

# METHODS OF REPRESENTATION THEORY

WITH APPLICATIONS TO FINITE GROUPS  
AND ORDERS

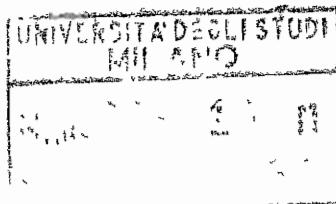
**CHARLES W. CURTIS**

*University of Oregon*

**IRVING REINER**

*University of Illinois at Urbana-Champaign*

**VOLUME II**



A WILEY-INTERSCIENCE PUBLICATION

**JOHN WILEY & SONS**

New York · Chichester · Brisbane · Toronto · Singapore

Copyright © 1987 by John Wiley & Sons, Inc.

All rights reserved. Published simultaneously in Canada.

Reproduction or translation of any part of this work beyond that permitted by Section 107 or 108 of the 1976 United States Copyright Act without the permission of the copyright owner is unlawful. Requests for permission or further information should be addressed to the Permissions Department, John Wiley & Sons, Inc.

*Library of Congress Cataloging in Publication Data:*

Curtis, Charles W.

Methods of representation theory—with applications to finite groups and orders.

(Pure and applied mathematics, ISSN 0079-8185)

“A Wiley-Interscience publication.”

Includes bibliographies and indexes.

1. Representations of groups. 2. Finite groups.

I. Reiner, Irving. II. Title. III. Series: Pure and applied mathematics (John Wiley & Sons)

QA171.C85 512'.2 81-7416

ISBN 0-471-18994-4 (v. 1)

ISBN 0-471-88871-0 (v. 2)

Printed in the United States of America

10 9 8 7 6 5 4 3 2 1

*To our sons,  
David and Peter,  
Timothy, Daniel, and Robert.*



# PREFACE

In this volume, the reader can follow each of the main directions in the current work on the representation theory of finite groups. The subject owes much of its present vitality to the achievements of R. Brauer, J. A. Green, G. Lusztig, and R. G. Swan. Their work not only has set the foundations, but also has established close ties between representation theory and the theory of finite groups, algebraic number theory, and algebraic geometry and topology. Our main objective has been to present an accessible, self-contained, and detailed introduction to their contributions, so that the reader can find in one place all that is needed for a thorough understanding of the main results, along with concrete information on how the ideas are applied.

As a supplement to the table of contents, we include here some remarks about the chapters in this volume and the earlier parts of the book they depend on. It has been our intention that the chapters can be read independently of one another.

Chapter 5 is a comprehensive introduction to low-dimensional algebraic  $K$ -theory. We present the basic properties of the groups  $K_0$ ,  $K_1$ , and  $K_2$ , together with information on methods of computing them for integral group rings and orders. Prerequisites include homological algebra, from the Introduction to Volume I, and other parts of Volume I, which are reviewed as they occur in the discussion.

Chapter 6, on class groups, is a culmination of integral representation theory. It contains a representative collection of explicit calculations of locally free class groups of integral group rings, including a discussion of the algebraic number theory needed to carry them out. This requires a good understanding of parts of Chapters 3 and 4, as well as a portion of the Introduction to Volume I. Chapters 5 and 6 also contain several references to the book *Maximal Orders* (Reiner [75]), cited as MO in the text.

Chapter 7 is devoted to Brauer's theory of blocks. It contains the basic results pertaining to blocks of modules over the group algebras  $KG$ ,  $RG$ , and  $kG$  for a  $p$ -modular system  $(K, R, k)$ . A main theme is the new approach to the foundations of block theory provided by Green's work on indecomposable modules and  $G$ -algebras. For this chapter, a thorough understanding of Chapters 1 and 2 is essential. We note incidentally that the character theory of finite groups with self-centralizing, cyclic Sylow  $p$ -subgroups that are  $TI$ -sets, from §§ 14 and 20, is reconsidered in the context of block theory in §§ 60 and 62. The chapter also contains several comparisons with the earlier account of block theory, Curtis-Reiner [62], cited throughout as CR.

Finite groups of Lie type occupy a special place in finite group theory, as the

classification of finite simple groups has shown. The contributions of Lusztig to the solution of many challenging problems concerning their representations have been responsible for a surge of interest in all aspects of the character theory of these groups. His work is based on the theory of reductive algebraic groups over finite fields, and their actions on certain algebraic varieties. Our purpose in Chapter 8 has been to give a self-contained introduction, for persons coming to the subject from other parts of representation theory, to topics that can be understood without extensive background on algebraic groups and  $l$ -adic cohomology, and that nevertheless are important in Lusztig's theory. Prerequisites for this chapter are Chapter 1, especially §11D on Hecke algebras, and Chapter 2, as preparation for §72.

Chapter 9, on rationality questions, begins with a section on the Frobenius-Schur classification of irreducible complex-valued characters, from the point of view of realizability of the representations over  $\mathbb{R}$ , which belongs in every first course in character theory. The prerequisite for the entire chapter is Chapter 1 and the theory of splitting fields from the Introduction to Volume I.

Chapter 10 takes up some new directions in the classification of indecomposable representations, including Gabriel's theorem on representations of graphs, and an introduction to the theory of Auslander-Reiten sequences. As an application of the latter topic, we present Yamagata's proof of Roiter's theorem on the Brauer-Thrall conjecture. An account of some earlier work on the classification of indecomposable modules over artinian rings was given in CR, Chapters 8 and 9.

The last chapter is devoted to Burnside rings and representation rings, which give a new perspective to the induction theorems discussed in Chapters 1 and 2, and to the problem of classifying indecomposable modules over non-semisimple group algebras.

Although it has resulted in a longer book, we have not hesitated to review basic concepts and proofs each time they are applied, so that the book can be picked up and read locally, without too great penalties for skipping from one part to another.

This volume is, to a great extent, a personal odyssey, containing much of what we know ourselves about the research problems we have worked on during the last twenty years. Chapters 5–8 have each been a basis of graduate courses and seminars we have given.

While the progress in representation theory made since the publication of CR encouraged us to undertake this project, its size and scope have been a surprise to us. Perhaps it is not out of place to express the hope that this book will be a useful guide, as CR was in its time, during a period of continuing activity in representation theory and its applications.

It remains to thank those persons and institutions whose help has been essential for the completion of this volume: Dan Grayson, Steve Ullom, Mike Stein, Gerald Cliff, Dean Alvis, Jerry Janusz, and Peter Webb for their help with the manuscript and the proof reading; the National Science Foundation for research support; and Hilda K. Britt for her tireless efforts devoted to the preparation of the manuscript. We also extend our thanks to the many friends,

colleagues, and students whom we have consulted on various points connected with the project. Once again, we add a special note of appreciation to our wives, Betsy and Irma, for their affection and encouragement.

CHARLES W. CURTIS  
IRVING REINER

*Eugene, Oregon  
Urbana, Illinois  
August 1986*

---

**Addendum to the Preface**

*Irving Reiner died in October, 1986, while the book was in production. I deeply regret that he did not live to see the book in print. We had completed together the manuscript and the preface, and sent them to the publisher earlier in 1986. Along with the persons mentioned in the Preface, I want to thank Irma Reiner for her help with the proof reading.*

CHARLES W. CURTIS

---

*Eugene, Oregon  
May, 1987*

---



# CONTENTS

<b>Chapter 5. Algebraic <math>K</math>-theory</b>	<b>1</b>
§ 38. Grothendieck groups	2
§ 38A. <i>Grothendieck groups. Frobenius functors</i>	2
§ 38B. <i>Grothendieck groups and projective class groups</i>	14
§ 38C. <i>Regular rings</i>	19
§ 38D. <i>Localization sequences</i>	31
§ 39. Grothendieck groups of integral group rings	44
§ 39A. <i>Localization sequences</i>	45
§ 39B. <i>Explicit calculations</i>	54
§ 40. Whitehead groups	61
§ 40A. <i>Introduction</i>	61
§ 40B. <i>Localization sequences</i>	65
§ 40C. <i>Elementary matrices</i>	73
§ 40D. <i>Unimodular rows and stably free modules</i>	77
§ 41. Basic elements, stable range, and cancellation	83
§ 42. Mayer-Vietoris sequences	101
§ 43. $K$ -theory of polynomial rings	112
§ 44. Relative $K$ -theory	120
§ 45. $SK_1$ of orders	138
§ 45A. <i>Reduced norms</i>	138
§ 45B. <i>Maximal orders</i>	142
§ 45C. <i>Finiteness of <math>SK_1</math></i>	151
§ 45D. <i>Profinite groups</i>	156
§ 46. Whitehead groups of integral group rings	163
§ 47. Milnor's $K_2$ -group	184
§ 47A. <i>Steinberg groups and <math>K_2</math></i>	184
§ 47B. <i>Relative <math>K</math>-theory</i>	190
§ 47C. <i>Symbols</i>	197
§ 48. $SK_1$ of integral group rings	210

<b>Chapter 6. Class groups of integral group rings and orders</b>	<b>216</b>
§49. Locally free class groups	217
§ 49A. <i>Basic formulas</i>	217
§ 49B. <i>Functorial properties and the kernel group</i>	229
§ 49C. <i>Frobenius functor properties for class groups of group rings</i>	238
§50. Class groups of integral group rings	243
§ 50A. <i>Cyclic groups of squarefree order</i>	243
§ 50B. <i>The kernel group for p-groups</i>	254
§ 50C. <i>Metacyclic groups</i>	259
§ 50D. <i>Dihedral and quaternion 2-groups</i>	266
§ 50E. <i>An involution on class groups and kernel groups</i>	274
§ 50F. <i>Cyclic p-groups</i>	283
§ 50G. <i>Twisted group rings and crossed-product orders</i>	291
§51. Jacobinski's Cancellation Theorem and the Eichler condition	303
§ 51A. <i>The Eichler condition</i>	304
§ 51B. <i>The Eichler-Swan Theorem</i>	306
§ 51C. <i>Locally free cancellation</i>	322
§52. The Hom description of the class group	329
§53. The Swan subgroup of the class group	343
§ 53A. <i>The Swan subgroup</i>	343
§ 53B. <i>Rings of integers in tame extensions</i>	351
§ 53C. <i>Generalized Swan subgroups</i>	353
§54. <i>p</i> -Adic logarithms and Taylor's Theorem	356
§55. Picard groups	369
§ 55A. <i>Basic properties</i>	369
§ 55B. <i>Picard groups of orders</i>	376
§ 55C. <i>Locally free Picard groups</i>	382
§ 55D. <i>Radical reduction</i>	391
§ 55E. <i>Picard groups of group rings</i>	396
<b>Chapter 7. The theory of blocks</b>	<b>406</b>
§56. Introduction to block theory	407
§ 56A. <i>Background and notation for block theory</i>	407
§ 56B. <i>Definition of p-blocks for a finite group G</i>	412
§ 56C. <i>A criterion for P.I.M.'s to belong to the same p-block</i>	414
§ 56D. <i>Central characters and blocks of KG-modules</i>	416
§ 56E. <i>The defect of a block</i>	422

§ 57. The defect group of a $p$ -block	429
§ 57A. <i>G-algebras, the trace map, and defect groups</i>	429
§ 57B. <i>Defect groups as vertices</i>	437
§ 57C. <i>Defect groups as Sylow intersections</i>	440
§ 58. The Brauer Correspondence	445
§ 58A. <i>The Brauer map</i>	445
§ 58B. <i>Brauer's First Main Theorem</i>	448
§ 58C. <i>The Brauer Correspondence</i>	451
§ 59. Applications of blocks to character theory	462
§ 59A. <i>The Nagao Decomposition</i>	463
§ 59B. <i>Brauer's Second Main Theorem</i>	467
§ 60. $p$ -Sections and characters in blocks	471
§ 60A. <i>Block orthogonality and <math>p</math>-sections</i>	471
§ 60B. <i>Determination of the principal block using block orthogonality</i>	473
§ 60C. <i>Applications to the classification of transitive permutation groups of degree <math>p</math></i>	478
§ 61. Refinements of the Brauer Correspondence	484
§ 61A. <i>Blocks and normal subgroups</i>	484
§ 61B. <i>An extension of Brauer's First Main Theorem</i>	489
§ 61C. <i>Brauer's Third Main Theorem</i>	494
§ 62. Blocks with cyclic defect groups	495
§ 62A. <i>Preliminary results from homological algebra</i>	496
§ 62B. <i>Functorial properties of the Green Correspondence</i>	499
§ 62C. <i>Uniserial algebras and blocks of finite representation type</i>	504
§ 62D. <i>Modular representations in blocks with cyclic defect groups</i>	512
§ 62E. <i>Periodic projective resolutions in blocks with cyclic defect groups</i>	522
§ 63. Applications to group theory	530
§ 63A. <i>The kernel of the principal block</i>	530
§ 63B. <i>The Brauer-Suzuki Theorem on quaternion Sylow 2-subgroups</i>	532
§ 63C. <i>Glauberman's Z*-Theorem</i>	545
<b>Chapter 8. The representation theory of finite groups of Lie type</b>	<b>549</b>
§ 64. Root systems and finite reflection groups	550
§ 64A. <i>Finite groups generated by reflections. Root systems</i>	550
§ 64B. <i>Coxeter groups</i>	561
§ 64C. <i>Parabolic subgroups of finite Coxeter groups</i>	570

§65. Finite groups with <i>BN</i> -pairs	576
§ 65A. <i>The Bruhat decomposition</i>	576
§ 65B. <i>Examples of BN-pairs</i>	580
§ 65C. <i>Parabolic subgroups of finite groups with BN-pairs</i>	583
§66. Homology representations of finite groups with <i>BN</i> -pairs	586
§ 66A. <i>Homology representations of finite groups</i>	586
§ 66B. <i>The Coxeter poset of a finite g.r.</i>	600
§ 66C. <i>The combinatorial building and the Steinberg representation of a finite group with a BN-pair</i>	605
§67. The Hecke algebra $\mathcal{H}(G, B)$ and the decomposition of $(1_B)^G$	609
§ 67A. <i>The structure of the Hecke algebra <math>\mathcal{H}(G, B)</math></i>	609
§ 67B. <i>The sign representation of <math>\mathcal{H}</math> and the Steinberg representation of <math>G</math></i>	614
§ 67C. <i>Representations of the Hecke algebra <math>\mathcal{H}</math> for a BN-pair of rank 2</i>	619
§ 67D. <i>The Feit-Higman Theorem on generalized polygons</i>	623
§ 67E. <i>The reflection representation of the Hecke algebra <math>\mathcal{H}</math></i>	630
§68. Generic algebras and finite Coxeter groups	635
§ 68A. <i>Generic algebras and the Deformation Theorem</i>	635
§ 68B. <i>Parametrization of characters in <math>(1_B)^G</math></i>	643
§ 68C. <i>Generic degrees</i>	648
§69. Finite groups with split <i>BN</i> -pairs	653
§ 69A. <i>The Levi Decomposition</i>	653
§ 69B. <i>Intersections of parabolic subgroups</i>	662
§70. Cuspidal characters	666
§ 70A. <i>Generalized restriction and induction</i>	666
§ 70B. <i>The philosophy of cusp forms</i>	676
§ 70C. <i>Formulas for character values</i>	681
§71. A Duality Operation in $\text{ch } CG$ .	688
§ 71A. <i>Definition and basic properties of <math>D_G</math></i>	689
§ 71B. <i>The effects of <math>D_G</math> on character degrees</i>	692
§ 71C. <i>The values of the Steinberg character</i>	697
§72. Modular representations of finite groups of Lie type	700
§ 72A. <i>The Ballard-Lusztig Theorem on characters of P.I.M.'s</i>	700
§ 72B. <i>The simple <math>kG</math>-modules</i>	706
<b>Chapter 9. Rationality questions</b>	<b>719</b>
§73. Unitary, orthogonal, and symplectic $CG$ -modules	720
§ 73A. <i>Rationality questions over the real field <math>\mathbb{R}</math></i>	720

<i>§ 73B. Induction theorems for real-valued characters</i>	727
<b>§ 74. The Schur Index</b>	732
<i>§ 74A. General theory</i>	732
<i>§ 74B. Schur indices for group algebras</i>	740
<i>§ 74C. The Benard-Schacher Theorem</i>	746
<b>§ 75. Representations and characters of the symmetric group</b>	762
<i>§ 75A. Specht modules and simple <math>FS_n</math>-modules</i>	762
<i>§ 75B. Solomon's Theorem and the irreducible characters of <math>S_n</math></i>	774
<b>§ 76. The Artin exponent</b>	782
<b>Chapter 10. Indecomposable modules</b>	790
<b>§ 77. Representations of graphs and Gabriel's Theorem</b>	790
<i>§ 77A. Representations of graphs and Coxeter functors</i>	790
<i>§ 77B. Representation categories of finite type (Gabriel's Theorem)</i>	799
<b>§ 78. Auslander-Reiten sequences</b>	806
<i>§ 78A. The Heller loop-space operator</i>	807
<i>§ 78B. Auslander-Reiten sequences for group algebras</i>	815
<i>§ 78C. Auslander-Reiten sequences for algebras</i>	822
<b>§ 79. Algebras of finite representation type</b>	830
<b>Chapter 11. The Burnside ring and the representation ring of a finite group</b>	837
<b>§ 80. Permutation representations and Burnside rings</b>	838
<i>§ 80A. Burnside rings</i>	838
<i>§ 80B. G-sets and induction maps</i>	846
<i>§ 80C. Tensor induction and algebraic maps</i>	852
<i>§ 80D. Conlon's Induction Theorem</i>	859
<b>§ 81. Representation rings</b>	868
<i>§ 81A. Preliminary results</i>	869
<i>§ 81B. Conlon's Theorems</i>	878
<i>§ 81C. Species</i>	891
<i>§ 81D. Dual elements in the Green algebra</i>	898
<i>§ 81E. Semisimplicity of representation algebras</i>	906
<i>§ 81F. Nilpotent elements in representation algebras</i>	912
<b>Bibliography</b>	921
<b>Notation index</b>	943
<b>Subject index</b>	947



# METHODS OF REPRESENTATION THEORY

## CHAPTER 5

# Algebraic $K$ -Theory

The aim of this chapter is to provide a self-contained introduction to “classical” algebraic  $K$ -theory, with special emphasis on the  $K$ -theory of integral group rings. We shall concentrate here on the Grothendieck group  $K_0(\mathcal{C})$  of the category  $\mathcal{C}$ , the Whitehead group  $K_1(A)$  of the ring  $A$ , and the Milnor group  $K_2(A)$ . In adopting this nomenclature, we have followed the books on algebraic  $K$ -theory by Bass [68], Milnor [71], Swan [68], and Swan-Evans [70], as well as the Battelle Conference Notes (Bass [73a–c]).

Other authors occasionally use different terminology. In particular, for a finite group  $G$  there is also a “Whitehead group”  $\text{Wh}(ZG)$ , discussed at length in §46. It will be clear from the context whether the term “Whitehead group” refers to  $K_1(ZG)$  or  $\text{Wh}(ZG)$ .

We have already encountered, in §16B, the definitions of the Grothendieck group  $G_0(RG)$  and the projective class group  $K_0(RG)$ , where  $R$  is a commutative ring and  $G$  a finite group. After recalling their definitions in §38A, we relate them to T. Y. Lam’s axiomatic theory of Frobenius functors. In §38B we treat  $G_0(A)$  and  $K_0(A)$  for an arbitrary ring  $A$ . As shown in §39C, we have  $G_0(A) \cong K_0(A)$  whenever the ring  $A$  is regular (that is, each f.g.  $A$ -module has finite homological dimension). The section ends with a discussion of localization sequences, an important topic which reappears in §39A and §40B.

Section 39 is devoted to Swan’s results on the Grothendieck group  $G_0(RG)$ , and its calculation by a formula due to Heller-Reiner when  $R$  is a Dedekind domain in an algebraic number field. In §40, we treat  $K_1(A)$ , and begin by showing that the determinantal version  $K_{\det}(A)$ , in §38, agrees with the definition here, namely  $K_1(A) \cong GL(A)/GL'(A)$ . After discussing localization sequences, we come to the important concepts of elementary matrices, Steinberg relations, and stable range. This last concept plays a central role in §41, where we give the Eisenbud-Evans theory of basic elements, which in turn yields Bass’s fundamental Stable Range Theorem.

In §42 we give Milnor’s exact sequence of  $K$ -groups, arising from a suitable fiber product of rings. This “Mayer-Vietoris sequence” is of the utmost importance in calculations of  $K$ -groups. As shown in §47, under suitable hypotheses it can be extended to the left by  $K_2$ -groups.

Section 43 briefly considers the  $K$ -theory of polynomial rings and gives Seshadri’s proof of a special case of Serre’s conjecture. Section 44 is a rather

technical one on relative  $K$ -theory, and its results are fundamental for our discussion of  $SK_1$  in §45C, as well as for the proof in §47 of Milnor's extended Mayer-Vietoris sequence.

Now let  $\Lambda$  be an order in an algebra  $A$ , and define  $SK_1(\Lambda)$  as the kernel of the map  $K_1(\Lambda) \rightarrow K_1(A)$ . In §45B we give Keating's formula for  $SK_1(\Lambda)$  when  $\Lambda$  is a maximal order; his proof uses the extended localization sequence from Quillen's  $K$ -theory. Using Keating's result, and some facts on relative  $K$ -theory from §44, we give a new proof of Bass' important theorem that  $SK_1(\Lambda)$  is finite when  $A$  is a f.d. separable algebra over a global field. The section concludes with a discussion of profinite groups, in preparation for §46.

Section 46 gives Wall's theorems on  $SK_1(RG)$  and the Whitehead group  $Wh(RG)$  of an integral group ring. The most striking result is that when  $R$  is the ring of algebraic integers in a number field, the torsion subgroup of  $K_1(RG)$  is precisely

$$(\text{torsion subgroup of } R^\times) \times G^{ab} \times SK_1(RG).$$

This may be viewed as a far-reaching generalization of G. Higman's theorem on torsion units in  $RG$  when  $G$  is abelian.

In §47 we give a brief introduction to  $K_2$ , following the treatment in Milnor [71], and occasionally referring the reader to that reference for some of the proofs. The section includes a discussion of "symbols" and their relation to reciprocity laws in number theory. In §48 we summarize (without proof) the known results on  $SK_1(RG)$ .

As can be seen from the above, we have largely omitted Quillen's higher  $K$ -theory, an important new approach which lies outside the scope of our book. So too do the connections between algebraic  $K$ -theory and topology, though we have listed some references for this subject at the end of the introduction to Chapter 6. For further reading on these omitted topics, we refer the reader to the "standard" references on algebraic  $K$ -theory, namely, Milnor [66], [71], Bass [73a–c], Stein [76], [78], Friedlander-Stein [81], Dennis [82], and Bak [84]. See also the useful books by McDonald [84] and Sylvester [81].

## §38. GROTHENDIECK GROUPS

### §38A. Grothendieck Groups and Frobenius Functors

Let  $R$  be a commutative ring, and let  $G$  be a finite group. We recall from §16B that the Grothendieck group  $G_0(RG)$  of the group ring  $RG$  is the additive group generated by symbols  $[M]$  corresponding to isomorphism classes  $(M)$  of f.g. left  $RG$ -modules, with defining relations

$$[M] = [M'] + [M''],$$

for each ses (short exact sequence)

$$0 \rightarrow M' \rightarrow M \rightarrow M'' \rightarrow 0$$

of f.g. left  $RG$ -modules.

In case  $R$  is a field  $K$ , we proved in §16B that  $G_0(KG)$  has the structure of a commutative ring. The multiplication in  $G_0(KG)$  was defined in such a way that

$$[M][N] = [M \otimes_K N]$$

for f.g. left  $KG$ -modules  $M$  and  $N$ , where  $M \otimes_K N$  is the inner tensor product (see Definition 10.15).

When  $\text{char } K = 0$ , we proved in (16.10) that there is an isomorphism of rings

$$G_0(KG) \cong \text{ch } KG,$$

where  $\text{ch } KG$  is the ring of virtual  $K$ -characters of  $G$ . The isomorphism is given by  $[M] \rightarrow \mu$ , for a left  $KG$ -module  $M$ , where  $\mu$  is the  $K$ -character of  $G$  afforded by  $M$ .

A similar result was established in §17 for  $G_0(kG)$ , where  $k$  is a field of characteristic  $p > 0$  associated with a  $p$ -modular system in which  $K$  is sufficiently large (see §16). As shown in Proposition 17.14, we have an isomorphism of rings,

$$G_0(kG) \cong \text{Bch } kG,$$

which maps an element  $t \in G_0(kG)$  onto the virtual Brauer character associated with it.

In the cases described above, Grothendieck groups provide no more than a reformulation of results about character rings. The same is true, at a deeper level, for the induction theorems of §§15 and 21. A typical induction theorem asserts that, for a field  $K$ , we have

$$G_0(KG) = \sum_{H \in \mathcal{E}_K} \text{ind}_H^G(G_0(KH)),$$

where  $\mathcal{E}_K$  is a family of subgroups of  $G$  depending on  $K$ , and  $\text{ind}_H^G$  is the induction map from  $KH$ -modules to  $KG$ -modules. These theorems describe the *additive* structure of Grothendieck groups  $G_0(KG)$ , but their proofs use the *multiplicative* structure. In particular, they depend on the fact that  $\sum_{H \in \mathcal{E}_K} \text{ind}_H^G(G_0(KH))$  is an ideal in the ring  $G_0(KG)$ ; this follows from the identity in the ring  $G_0(KG)$ , proved in (21.14), that

$$(\text{ind}_H^G u)v = \text{ind}_H^G(u \cdot \text{res}_H^G v), \quad u \in G_0(KH), \quad v \in G_0(KG).$$

In turn, this formula extends the identity (15.5) for complex-valued class functions:

$$\psi^G \cdot \zeta = (\psi \cdot \zeta_H)^G, \quad \psi \in \text{cf}_C(H), \quad \zeta \in \text{cf}_C(G).$$

Algebraic K-theory begins with the study of Grothendieck groups  $G_0(RG)$ , for commutative rings  $R$  which are not necessarily fields. Among other things, we would like to have induction theorems like those in §§15 and 21, which depend on introducing multiplicative structures on Grothendieck groups.

In this subsection, we present an axiomatic approach to these ideas, due to T. Y. Lam [68a] (see also Swan-Evans [70]). Extensions and variations of the results of this section, by Green [71] and Dress [73], will be taken up later, in Chapter 11. We start with Lam's axiomatization of the functor  $G \rightarrow G_0(RG)$ , and its relation to induction and restriction, in cases where  $G_0(RG)$  is a commutative ring.

**(38.1) Definition.** A *Frobenius functor*  $F$  consists of the data:

- (i) There is a correspondence  $G \rightarrow F(G)$ , which assigns to each finite group  $G$  a commutative ring  $F(G)$
- (ii) (*Restriction*) For each inclusion  $i: H \leq G$  of groups, there exists a homomorphism of commutative rings

$$i^*: F(G) \rightarrow F(H).$$

These ring homomorphisms satisfy the condition that

$$(ji)^* = i^* j^*$$

for each composition of inclusions  $H \leq_i K \leq_j G$ . Further, if  $H = G$ , and  $i: H \leq G$  is the identity map, then  $i^*$  is also the identity map.

- (iii) (*Induction*) For each inclusion  $i: H \leq G$ , there exists a homomorphism of additive groups

$$i_*: F(H) \rightarrow F(G)$$

such that  $i_* = \text{id}$  if  $H = G$ , and

$$(ji)_* = j_* i_*$$

for each composite inclusion as in (ii).

- (iv) (*Frobenius identity*) For each inclusion  $i: H \leq G$ , we have the identity in the ring  $F(G)$ :

$$x \cdot i_* y = i_*((i^* x) \cdot y), \quad x \in F(G), \quad y \in F(H).$$

**Remark.** It is useful to understand Definition 38.1 in terms of category theory (see §2C). Let  $\mathcal{G}$  be the category of all finite groups, with morphisms given by inclusions (that is, monomorphisms). When the conditions of (38.1) hold, we have two functors defined on  $\mathcal{G}$ :

- (i) The first is a contravariant functor from  $\mathcal{G}$  into the category of commutative rings  $\mathcal{R}$  (with ring homomorphisms as morphisms). This functor, called *restriction*, maps each object  $G \in \mathcal{G}$  onto an object  $F(G) \in \mathcal{R}$ , and carries each inclusion  $i: H \leq G$  onto a homomorphism of rings  $i^*: F(G) \rightarrow F(H)$ .
- (ii) The second is a covariant functor from  $\mathcal{G}$  into  $\mathcal{AB}$ , the category of abelian groups. This functor, called *induction*, maps each  $G \in \mathcal{G}$  onto  $F(G) \in \mathcal{AB}$ , and carries each inclusion  $i: H \leq G$  onto a homomorphism of additive groups  $i_*: F(H) \rightarrow F(G)$ .

The superscript on  $i^*$  indicates that the functor involved (in this case, restriction) is contravariant. The subscript on  $i_*$  means that the induction functor is covariant.

By the remarks preceding (38.1), we have as our first example:

**(38.2) Proposition.** *Let  $K$  be an arbitrary field. Then  $G_0(KG)$  is a commutative ring for each finite group  $G$ . The operations  $\text{res}_H^G$  and  $\text{ind}_H^G$  on  $KH$ -modules and  $KG$ -modules extend to maps  $i^*: G_0(KG) \rightarrow G_0(KH)$  and  $i_*: G_0(KH) \rightarrow G_0(KG)$  whenever  $H \leq G$ . The data*

$$\{F(G) = G_0(KG), i^*, i_*\}$$

define a Frobenius functor.

We omit the proof, which is straightforward, using the results mentioned earlier. In particular, the extensions of the operations  $\text{res}_H^G$  and  $\text{ind}_H^G$  to Grothendieck groups, and the Frobenius identity, have already been explained in §21B.

The extension of Proposition 38.2 to  $G_0(RG)$ , for a commutative ring  $R$ , is not immediate; indeed, as we shall see,  $G_0(RG)$  is not necessarily a commutative ring. To avoid this difficulty, we introduce the concept of an *RG-lattice*, that is a left  $RG$ -module which is  $R$ -projective and f.g./ $R$  (see §10D).

**(38.3) Definition.** Let  $R$  be a commutative ring, and  $G$  a finite group. We define  $G_0^R(RG)$  to be the Grothendieck group associated (as in §16B) with the category of left  $RG$ -lattices.

**(38.4) Proposition.** *The Grothendieck group  $G_0^R(RG)$ , for a finite group  $G$  and a commutative ring  $R$ , is a commutative ring. Multiplication is given by*

$$[M][N] = [M \otimes_R N]$$

for  $RG$ -lattices  $M$  and  $N$ , where  $M \otimes_R N$  is the inner tensor product.

*Proof.* The argument is essentially the same as that given in §16B, showing that  $G_0(KG)$  is a commutative ring when  $K$  is a field. Let us point

out a few main steps which must be considered in the more general situation.

First of all, if  $M$  and  $N$  are  $RG$ -lattices, then so is their inner tensor product  $M \otimes_R N$ . It is clear that this tensor product is an f.g. left  $RG$ -module. But it is also an  $R$ -lattice, since if  $M$  and  $N$  are  $R$ -lattices, then so is  $M \otimes_R N$ . For we may choose  $R$ -modules  $M'$  and  $N'$  such that  $M \oplus M'$  and  $N \oplus N'$  are  $R$ -free, and then use (2.17) and the fact that  $R \otimes_R R \cong R$  (see (2.16)).

Second, given any ses

$$(38.5) \quad 0 \rightarrow N' \rightarrow N \rightarrow N'' \rightarrow 0$$

of  $RG$ -lattices, and an arbitrary  $RG$ -lattice  $M$ , the sequence

$$(38.6) \quad 0 \rightarrow M \otimes_R N' \rightarrow M \otimes_R N \rightarrow M \otimes_R N'' \rightarrow 0$$

is also an exact sequence of  $RG$ -lattices. This follows, since  $M$  is  $R$ -projective and hence  $R$ -flat, by (2.28).

We then let  $\mathbf{F}$  be the free abelian group with a basis  $\{(M)\}$  consisting of isomorphism classes  $(M)$  of  $RG$ -lattices. The operation of inner tensor product clearly gives  $\mathbf{F}$  the structure of a commutative ring. The kernel of the natural map from  $\mathbf{F}$  to  $G_0^R(RG)$ , given by  $(M) \rightarrow [M]$ , is generated by all elements  $(N) - (N') - (N'')$  arising from ses's (38.5) as above. The exactness of (38.6) shows that the kernel is an ideal in the commutative ring  $\mathbf{F}$ , and hence  $G_0^R(RG)$  is also a commutative ring, with the required multiplication.

The above argument fails to show that  $G_0(RG)$  is a commutative ring, for an arbitrary commutative ring  $R$ , since the sequence (38.6) may not be exact if  $M$  is not  $R$ -projective. The proof given above does show, however, that for each ses (38.5) of f.g.  $RG$ -modules, and an arbitrary  $RG$ -lattice  $M$ , the sequence (38.6) is exact. Thus multiplication by  $[M]$ , for an  $RG$ -lattice  $M$ , is a well-defined operation in  $G_0(RG)$ . Therefore,  $G_0(RG)$  becomes a module over the commutative ring  $G_0^R(RG)$ , with

$$[M] \cdot [N] = [M \otimes_R N], \quad M \in G_0^R(RG), \quad N \in G_0(RG).$$

This leads us to the following:

**(38.7) Definition.** A *Frobenius module*  $M$  over a Frobenius functor  $F$  consists of the data:

(i) There is a correspondence which assigns to each finite group  $G$  an  $F(G)$ -module  $M(G)$ .

(ii) For each inclusion  $i: H \leq G$ , there exist a pair of homomorphisms of additive groups

$$\begin{aligned} \text{and} \quad i^*: M(G) &\rightarrow M(H) && \text{(restriction)} \\ i_*: M(H) &\rightarrow M(G) && \text{(induction)} \end{aligned}$$

such that  $i^* = i_*$  = identity map, in case  $H = G$ , and satisfying the same transitivity laws as in (38.1) for composite inclusions.

(iii) For each inclusion  $i: H \leq G$ , we have

$$i^*(xm) = i^*(x)i^*(m), \quad x \in F(G), \quad m \in M(G),$$

as well as the Frobenius identities,

$$x \cdot i_*(m') = i_*((i^*x) \cdot m'), \quad x \in F(G), \quad m' \in M(H),$$

and

$$(i_*x') \cdot m = i_*(x' \cdot i^*m), \quad x' \in F(H), \quad m \in M(G).$$

We then have:

**(38.8) Proposition.** *Let  $R$  be an arbitrary commutative ring. The correspondence  $G \rightarrow G_0^R(RG)$ , for each finite group  $G$ , together with the usual restriction and induction maps, is a Frobenius functor. The correspondence  $G \rightarrow G_0(RG)$ , together with restriction and induction, and the operation  $G_0^R(RG) \times G_0(RG) \rightarrow G_0(RG)$  given by*

$$[M] \cdot [N] = [M \otimes_R N]$$

for each  $RG$ -lattice  $M$  and each f.g.  $RG$ -module  $N$ , is a Frobenius module over the Frobenius functor  $G \rightarrow G_0^R(RG)$ .

The proof is routine, after what has been said, except for the Frobenius identities. These follow from (10.20), which asserts that for each  $RG$ -module  $N$  and each  $RH$ -module  $M$ , there is an isomorphism of  $RG$ -modules:

$$M^G \otimes_R N \cong (M \otimes_R N_H)^G,$$

where  $\otimes_R$  denotes inner tensor products of  $RG$ -modules and  $RH$ -modules, respectively. The rest of the proof of (38.8) is left as an exercise for the reader.

**(38.9) Definition.** Let  $F_1$  and  $F_2$  be Frobenius functors. A *morphism of Frobenius functors*  $\varphi: F_1 \rightarrow F_2$  consists of a family of homomorphisms of commutative rings

$$\varphi_G: F_1(G) \rightarrow F_2(G),$$

one for each finite group  $G$ , which commute with restriction and induction. This means that for each inclusion  $i: H \leq G$ , the following diagrams commute:

$$\begin{array}{ccc} F_1(H) & \xrightarrow{\varphi_H} & F_2(H) \\ i_* \downarrow & & \downarrow i_* \\ F_1(G) & \xrightarrow{\varphi_G} & F_2(G), \end{array} \quad \begin{array}{ccc} F_1(H) & \xrightarrow{\varphi_H} & F_2(H) \\ i^* \uparrow & & \uparrow i^* \\ F_1(G) & \xrightarrow{\varphi_G} & F_2(G). \end{array}$$

Similarly, for Frobenius modules  $M_1$  and  $M_2$  over a Frobenius functor  $F$ , a *morphism of Frobenius modules*  $\mu: M_1 \rightarrow M_2$  consists of a family of homomorphisms of  $F(G)$ -modules

$$\mu_G: M_1(G) \rightarrow M_2(G),$$

one for each finite group  $G$ , such that  $\mu$  commutes with  $i_*$  and  $i^*$  in an analogous manner.

**(38.10) Examples of Frobenius Modules and Morphisms.** Let  $R$  denote an arbitrary commutative ring. By (38.8), the correspondence  $G \rightarrow G_0^R(RG)$  is a Frobenius functor, which we shall call  $G_0^R$ . Similarly, the correspondence  $G \rightarrow G_0(RG)$  is a Frobenius module over  $G_0^R$ , which we shall call  $G_0$ . We now give some other examples.

- (i) The Frobenius functor  $G_0^R$  is a Frobenius module over itself, in an obvious way.
- (ii) We have already pointed out that  $G_0$  is a Frobenius module over the Frobenius functor  $G_0^R$ . Another example of a Frobenius module over the Frobenius functor  $G_0^R$  is given by  $M: G \rightarrow K_0(RG)$ , where  $K_0(RG)$  is the Grothendieck group of the category  $\mathcal{P}(RG)$  consisting of all f.g. projective  $RG$ -modules (see §16B). There are three main points to verify:
  - (a) For each  $RG$ -lattice  $L$  and each  $P \in \mathcal{P}(RG)$ , the inner tensor product  $L \otimes_R P$  also lies in  $\mathcal{P}(RG)$ . We prove this, writing  $\otimes$  in place of  $\otimes_R$  for brevity. Since  $P$  is a direct summand of  $(RG)^{(k)}$  for some  $k$ ,  $L \otimes P$  is a direct summand of  $L \otimes (RG)^{(k)}$ . The latter is  $RG$ -projective by Exercise 10.19, and thus  $L \otimes P \in \mathcal{P}(RG)$ , as claimed.
  - (b) The proposed multiplication preserves relations in  $G_0^R(RG)$ , that is, for each ses of  $RG$ -lattices
 
$$0 \rightarrow L' \rightarrow L \rightarrow L'' \rightarrow 0,$$
 and each  $P \in \mathcal{P}(RG)$ , we have
 
$$[L \otimes P] = [L' \otimes P] + [L'' \otimes P] \quad \text{in } K_0(RG).$$
  - (c) Relations in  $K_0(RG)$  are preserved, that is,
 
$$[L \otimes (P \oplus P')] = [L \otimes P] + [L \otimes P'] \quad \text{in } K_0(RG)$$

But this is clear since

$$0 \rightarrow L' \otimes P \rightarrow L \otimes P \rightarrow L'' \otimes P \rightarrow 0$$

is  $RG$ -exact, and splits over  $RG$  because  $L'' \otimes P \in \mathcal{P}(RG)$ .

- (c) Relations in  $K_0(RG)$  are preserved, that is,

$$[L \otimes (P \oplus P')] = [L \otimes P] + [L \otimes P'] \quad \text{in } K_0(RG)$$

for each RG-lattice  $L$ , and for  $P, P' \in \mathcal{P}(RG)$ . This is obvious from the isomorphism

$$L \otimes (P \oplus P') \cong (L \otimes P) \oplus (L \otimes P').$$

Now let  $i^*$  and  $i_*$  be given by restriction and induction, respectively. It follows that  $M$  is a Frobenius module over  $G_0^R$ .

- (iii) The *Cartan map*  $c: K_0(RG) \rightarrow G_0(RG)$  is the homomorphism of additive groups, which assigns to  $[M] \in K_0(RG)$ , for  $M \in \mathcal{P}(RG)$ , the corresponding element  $[M]$  in  $G_0(RG)$  (see Definition 18.4). It is easily verified that the Cartan map is a morphism of Frobenius modules over the Frobenius functor  $G_0^R$ .
- (iv) Let  $\mu: M_1 \rightarrow M_2$  be a morphism of Frobenius modules over the Frobenius functor  $F$ . Then  $\ker \mu$  and  $\text{coker } \mu$ , defined in the obvious way, are also Frobenius modules over  $F$ .
- (v) Let  $f: R \rightarrow S$  be a homomorphism of commutative rings. We shall obtain morphisms of Frobenius modules from the operations of tensoring and restriction, using the homomorphism  $f$ . For example,  $S \otimes_R M$  is an SG-lattice, for an RG-lattice  $M$ , where  $S$  is an  $R$ -module through the homomorphism  $f: R \rightarrow S$ . Moreover,  $f$  defines a homomorphism of rings  $RG \rightarrow SG$  for each finite group  $G$ , so that by restriction of scalars (§10A), each SG-module can be viewed as an RG-module. In general, however, the map  $[M] \rightarrow [S \otimes_R M]$  is not a morphism of Frobenius modules over the Frobenius functor  $G_0^R$ , because tensoring with  $S$  need not preserve exactness of sequences of RG-modules, without some additional hypothesis, such as the assumption that  $S$  is flat over  $R$ . We shall now summarize several cases where tensoring and restriction define morphisms of Frobenius modules.

**(38.11) Proposition.** *Let  $f: R \rightarrow S$  be a homomorphism of commutative rings, and let  $G_0^R$  denote the Frobenius functor  $G \rightarrow G_0^R(RG)$ . Then*

- (i) *The map  $M \rightarrow S \otimes_R M$ , from RG-modules to SG-modules, defines a morphism of Frobenius modules over the Frobenius functor  $G_0^R$ , in the following cases:*

$$\begin{aligned} G_0^R(RG) &\rightarrow G_0^S(SG); \\ G_0^R(RG) &\rightarrow G_0(SG) \quad \text{if } S \text{ is a flat } R\text{-module;} \\ K_0(RG) &\rightarrow K_0(SG). \end{aligned}$$

*In particular, the right-hand side is a Frobenius module over  $G_0^R$  in each case.*

- (ii) *The map given by restriction of scalars, from SG-modules to RG-modules, using the homomorphism  $f: RG \rightarrow SG$ , defines a morphism of Frobenius modules*

over the Frobenius functor  $G_0^R$ , in the following cases:

$$\begin{aligned} G_0^S(SG) &\rightarrow G_0^R(RG) \quad \text{if } S \text{ is an } R\text{-lattice;} \\ G_0(SG) &\rightarrow G_0(RG) \quad \text{if } S \text{ is f.g./}R; \\ K_0(SG) &\rightarrow K_0(RG) \quad \text{if } S \text{ is an } R\text{-lattice.} \end{aligned}$$

The proof will be left to the reader.

As mentioned earlier, one reason for introducing Frobenius functors and Frobenius modules is to prove induction theorems in more general situations than those arising from character rings. To put it another way, we wish to compute Frobenius functors  $F(G)$  (or Frobenius modules  $M(G)$ ) in terms of information about  $F(H)$ , for  $H$  some manageable type of subgroup (cyclic, elementary, etc.) of  $G$ .

**(38.12) Definition.** For each finite group  $G$ , let  $\mathcal{C}(G)$  denote a family of subgroups of  $G$ . Let  $F$  be a Frobenius functor, and  $M$  a Frobenius module over  $F$ . For each subgroup  $H \leq G$ , let  $i_H^*: F(G) \rightarrow F(H)$  (or  $M(G) \rightarrow M(H)$ ) denote the restriction map, and let  $(i_H)_*$  denote the induction map. Define

$$F(G)_{\mathcal{C}} = \sum_{H \in \mathcal{C}(G)} (i_H)_* F(H), \quad M(G)_{\mathcal{C}} = \sum_{H \in \mathcal{C}(G)} (i_H)_* M(H).$$

Also define the dual objects

$$F(G)^{\mathcal{C}} = \bigcap_{H \in \mathcal{C}(G)} \ker i_H^*, \quad M(G)^{\mathcal{C}} = \bigcap_{H \in \mathcal{C}(G)} \ker i_H^*.$$

**(38.13) Proposition.** *With the notation as above, we have for each finite group  $G$ :*

- (i)  $F(G)_{\mathcal{C}}$  and  $F(G)^{\mathcal{C}}$  are ideals of  $F(G)$ .
- (ii)  $M(G)_{\mathcal{C}}$  and  $M(G)^{\mathcal{C}}$  are  $F(G)$ -submodules of  $M(G)$ .
- (iii)  $F(G)_{\mathcal{C}} \cdot M(G)^{\mathcal{C}} = 0$ ,  $F(G)^{\mathcal{C}} \cdot M(G)_{\mathcal{C}} = 0$ ,  $F(G)_{\mathcal{C}} \cdot F(G)^{\mathcal{C}} = 0$ .
- (iv)  $M(G)/M(G)_{\mathcal{C}}$  and  $M(G)^{\mathcal{C}}$  are modules over the ring  $F(G)/F(G)_{\mathcal{C}}$ .
- (v) For each  $i: H \leq G$ , we have  $(i_H)_*(M(H)_{\mathcal{C}}) \subseteq M(G)_{\mathcal{C}}$ .

*Proof.* We first prove (ii), and obtain (i) by taking  $M(G)$  equal to  $F(G)$  in (ii). Clearly  $M(G)_{\mathcal{C}}$  and  $M(G)^{\mathcal{C}}$  are additive subgroups of  $M(G)$ . Now let  $x \in F(G)$ ,  $m \in M(H)$  and  $n \in M(G)^{\mathcal{C}}$ , for some subgroup inclusion  $i: H \leq G$ , where  $H \in \mathcal{C}(G)$ . Then by (38.7iii) we have

$$x \cdot i_* m = i_*(i_H^* x \cdot m) \in M(G)_{\mathcal{C}}, \quad i_H^*(x \cdot n) = i_H^* x \cdot i_H^* n = 0,$$

so (ii) follows, and hence (i), by the first remark.

Next, for  $i: H \leq G$ ,  $H \in \mathcal{C}(G)$ ,  $y \in F(H)$ ,  $n \in M(G)^\mathcal{C}$ , we have by another part of (38.7iii),

$$i_* y \cdot n = i_*(y \cdot i_H^* n) = 0,$$

proving the first statement of (iii). For the second, let  $x \in F(G)$ ,  $m \in M(H)$ ; then

$$x \cdot i_* m = i_*(i_H^* x \cdot m) = 0.$$

The third follows from the first by taking  $M = F$ .

Statement (iv) follows easily from (iii), together with the formula

$$F(G)_\mathcal{C} \cdot M(G) \subseteq M(G)_\mathcal{C},$$

which also follows from the Frobenius identities.

The last statement follows from the transitivity of  $i_*$  over composite inclusions, and the proof is completed.

### (38.14) Corollary.

- (i) If  $F(G)_\mathcal{C} = F(G)$ , then  $M(G)^\mathcal{C} = 0$ .
- (ii) If an integer  $n$  annihilates  $F(G)/F(G)_\mathcal{C}$ , it also annihilates  $M(G)/M(G)_\mathcal{C}$  and  $M(G)^\mathcal{C}$ .

The proof of (ii) follows from (38.13iv) and the observation that if  $n \cdot S = 0$  for a ring  $S$ , then  $n \cdot M = 0$  for any module  $M$  over  $S$ . The first result follows from the second by taking  $n = 1$ .

We conclude this subsection with two applications of the preceding ideas. The first is an extension of the Witt-Berman Theorem at characteristic  $p$  (see §21B), and the second is another proof that the cokernel of the Cartan map is annihilated by a power of  $p$ .

**(38.15) Proposition.** Let  $(K, R, k)$  be a  $p$ -modular system, where  $K$  and  $k$  are fields with  $\text{char } K = 0$ ,  $\text{char } k = p > 0$ . For each finite group  $G$ , let  $\mathcal{E}_K(G)$  be the family of  $K$ -elementary subgroups of  $G$ . Then

- (i)  $K_0(kG)_{\mathcal{E}_K} = K_0(kG)$ .
- (ii) Let  $x \in K_0(kG)$ . If  $i_H^* x = 0$  for each subgroup inclusion  $i_H: H \leq G$ , with  $H \in \mathcal{E}_K$ , then  $x = 0$ .
- (iii) Let  $c: K_0(kG) \rightarrow G_0(kG)$  be the Cartan map. Then  $\text{cok } c$  is annihilated by a power of  $p$ .

*Proof.* In the terminology of Definition 38.12, Theorem 21.15 gives

$$G_0(kG) = G_0(kG)_{\mathcal{E}_K}.$$

Then the integer 1 annihilates  $G_0(kG)/G_0(kG)_{\mathcal{E}_K}$ , and hence also annihilates  $K_0(kG)/K_0(kG)_{\mathcal{E}_K}$  by (38.14ii), since  $K_0$  is a Frobenius module over the Frobenius functor  $G_0$  by (38.10ii). (In this case we have  $G_0(kG) = G_0^k(kG)$  for each finite group  $G$ , because  $k$  is a field.) The second statement follows from Corollary 38.14i, and the above remarks.

For the third statement, we first assume that  $K$  is sufficiently large. By (38.10iii), the Cartan map  $c: K_0(kG) \rightarrow G_0(kG)$  is a morphism of Frobenius modules over the Frobenius functor  $G \rightarrow G_0(kG)$ . By (38.10iv),  $\text{cok } c$  is also a Frobenius module over  $G_0(kG)$ . Since  $K$  is sufficiently large, the family  $\mathcal{E}_K$  of  $K$ -elementary subgroups of  $G$  coincides with the family  $\mathcal{E}$  of elementary subgroups of  $G$ , and Theorem 21.15 becomes

$$G_0(kG) = G_0(kG)_{\mathcal{E}}.$$

By the same argument used to prove part (i), it follows that

$$\text{cok } c = (\text{cok } c)_{\mathcal{E}}.$$

By Exercise 18.7, we have  $|G|_p \cdot (\text{cok } c)_{\mathcal{E}} = 0$ , and hence  $|G|_p \cdot \text{cok } c = 0$ . The extension to an arbitrary field  $K$  is then carried out by the same argument used in the proof of (21.22).

The preceding result extends an induction theorem from  $G_0(kG)$  to  $K_0(kG)$ , and really does no more than reinterpret an earlier argument concerning the cokernel of the Cartan map. (The results can, of course, be obtained without the machinery of Frobenius functors.) Our final result, due to Swan [60], will be proved later. Here, we shall use it to derive several new induction theorems for  $G_0^R(RG)$ , for an arbitrary commutative ring  $R$ .

**(38.16) Theorem (Swan).** *Let  $R$  be a Dedekind ring with quotient field  $K$ , and let  $\bar{R} = R/P$ , for a maximal ideal  $P$  in  $R$ . Let  $\mathcal{C}(G)$  be a family of subgroups of  $G$ , for each finite group  $G$ . Let  $n \in \mathbb{Z}$  be such that*

$$n[G_0(KG)/G_0(KG)_{\mathcal{E}}] = 0.$$

*Then also*

$$n[G_0(\bar{R}G)/G_0(\bar{R}G)_{\mathcal{E}}] = 0 \quad \text{and} \quad n^2[G_0(RG)/G_0(RG)_{\mathcal{E}}] = 0.$$

A proof will be given in (39.6).

We next apply (38.16) to obtain extensions of the Artin Induction Theorem 15.4 and the Witt-Berman Theorem 21.6.

**(38.17) Corollary.** *For each finite group  $G$ , let  $\mathcal{C}(G)$  be the family of cyclic subgroups of  $G$ . Then*

$$(i) \quad |G|^2 [G_0^R(RG)/G_0^R(RG)_\mathcal{C}] = 0,$$

for an arbitrary commutative ring  $R$ , and

$$(ii) \quad |G| [G_0^R(RG)/G_0^R(RG)_\mathcal{C}] = 0,$$

for any commutative ring  $R$  of nonzero prime characteristic.

*Proof.* By Artin's Induction Theorem 15.4, and (38.16), it follows that  $|G|$  annihilates  $G_0^Z(ZG)/G_0^Z(ZG)_\mathcal{C}$ . For an arbitrary commutative ring  $R$ , there is a homomorphism of rings  $\mathbb{Z} \rightarrow R$ , making  $G_0^R$  into a Frobenius module over  $G_0^Z$ , by (38.11i). The first statement follows by Corollary 38.14. Further, if  $\bar{\mathbb{Z}} = \mathbb{Z}/p\mathbb{Z}$ , then  $|G|$  annihilates  $G_0(\bar{\mathbb{Z}}G)/G_0(\bar{\mathbb{Z}}G)_\mathcal{C}$ , for each finite group  $G$ , by (38.16). Then (ii) is immediate, since there exists a homomorphism of commutative rings  $\bar{\mathbb{Z}} \rightarrow R$  for any commutative ring  $R$  of characteristic  $p$ .

**(38.18) Corollary.** *Let  $\mathcal{H}(G)$  denote the family of hyper-elementary subgroups<sup>†</sup> of  $G$ . Then*

$$G_0^R(RG)_\mathcal{H} = G_0^R(RG), \quad G_0^R(RG)^{\mathcal{H}} = 0,$$

for every commutative ring  $R$ .

The proof is similar to the proof of (38.17). By the Solomon Induction Theorem 15.10, or by the Witt-Berman Theorem 21.6, we have

$$G_0(\mathbb{Q}G)_\mathcal{H} = G_0(\mathbb{Q}G),$$

for every finite group  $G$ . By (38.16), we have

$$G_0^Z(ZG)_\mathcal{H} = G_0^Z(ZG)$$

for each finite group  $G$ , and the result follows, using the existence of a homomorphism  $\mathbb{Z} \rightarrow R$ , as in (38.17).

**(38.19) Corollary.** *For each finite group  $G$  and commutative ring  $R$ , we have*

$$|G|^2 [K_0(RG)/K_0(RG)_\mathcal{C}] = 0,$$

where  $\mathcal{C}(G)$  is the family of cyclic subgroups of  $G$ . If  $R$  has nonzero prime characteristic, then for each  $G$  we have

$$|G| [K_0(RG)/K_0(RG)_\mathcal{C}] = 0.$$

The proof, which is an extension of the proof of (38.17), is left to the reader.

<sup>†</sup>See Volume I, p. 381.

For further results on Frobenius functors and Frobenius modules, see Exercise 39.5, Theorems 46.18–46.21, and §49C.

### §38B. Grothendieck Groups and Projective Class Groups

Here we shall derive some basic properties of the Grothendieck group  $G_0(A)$  and the projective class group  $K_0(A)$  of an arbitrary ring  $A$ . We shall also introduce the Whitehead group  $K_1(A)$ , to be studied in more detail in §40. While we are mainly interested in the case where  $A$  is an integral group ring  $RG$  of a finite group  $G$  over some domain  $R$ , as in §38A, it is nevertheless necessary to treat some of the topics in greater generality.

As in §38A (see Definition 16.5), the Grothendieck group  $G_0(A)$  is the additive group generated by expressions  $[M]$ , one for each isomorphism class  $(M)$  of f.g. left  $A$ -modules  $M$ , with relations  $[M] = [M'] + [M'']$  for each ses (short exact sequence)  $0 \rightarrow M' \rightarrow M \rightarrow M'' \rightarrow 0$  of f.g. left  $A$ -modules. Our first result gives a simple criterion for deciding when two  $A$ -modules yield the same element in  $G_0(A)$ .

**(38.20) Proposition.** *Let  $A$  be an arbitrary ring, and let  $M, N$  be f.g. left  $A$ -modules. Then  $[M] = [N]$  in  $G_0(A)$  if and only if there exist a pair of ses's (of f.g. left  $A$ -modules) of the form*

$$0 \rightarrow X_1 \rightarrow X_2 \oplus M \rightarrow X_3 \rightarrow 0, \quad 0 \rightarrow X_1 \rightarrow X_2 \oplus N \rightarrow X_3 \rightarrow 0.$$

*Proof.* Clearly  $[M] = [N]$  in  $G_0(A)$  whenever two such ses's exist. Suppose conversely that  $[M] = [N]$  in  $G_0(A)$ , and write  $G_0(A) = \mathbf{F}/\mathbf{F}_0$  as in (16.3). Then  $(M) - (N) \in \mathbf{F}_0$ , so we may write

$$(M) - (N) = \sum_i \{(X_i) - (X'_i) - (X''_i)\} - \sum_j \{(Y_j) - (Y'_j) - (Y''_j)\},$$

where either summation may be empty, and where

$$0 \rightarrow X'_i \rightarrow X_i \rightarrow X''_i \rightarrow 0, \quad 0 \rightarrow Y'_j \rightarrow Y_j \rightarrow Y''_j \rightarrow 0$$

are ses's of f.g.  $A$ -modules. Put  $X = \coprod_i X_i$ ,  $X' = \coprod_i X'_i$ , etc., so there are ses's

$$(38.21) \quad 0 \rightarrow X' \rightarrow X \rightarrow X'' \rightarrow 0, \quad 0 \rightarrow Y' \rightarrow Y \rightarrow Y'' \rightarrow 0$$

of f.g.  $A$ -modules. Since

$$(M) + \Sigma \{(X'_i) + (X''_i)\} + \Sigma(Y_j) = (N) + \Sigma(X_i) + \Sigma \{(Y'_j) + (Y''_j)\}$$

in  $\mathbf{F}$ , it follows that

$$M \oplus X' \oplus X'' \oplus Y \cong N \oplus X \oplus Y' \oplus Y''.$$

Let us denote the direct sum on the right-hand side above by  $S$ . Since  $M \oplus X' \oplus X'' \oplus Y \cong S$ , it follows from (38.21) that there exists a ses

$$0 \rightarrow X' \oplus Y' \rightarrow S \rightarrow M \oplus X'' \oplus Y'' \rightarrow 0.$$

There is thus a ses

$$0 \rightarrow X' \oplus Y' \rightarrow S \oplus N \rightarrow M \oplus X'' \oplus Y'' \oplus N \rightarrow 0.$$

Likewise, there is a ses of the same form, with middle term  $S \oplus M$ . This gives the desired result.

The same type of argument applies to the projective class group  $K_0(A)$ , which is the Grothendieck group of the category  $\mathcal{P}(A)$  of f.g. projective left  $A$ -modules (see (16.5)). Recall that  $K_0(A)$  is generated by expressions  $[P]$ , one for each isomorphism class  $(P)$  of f.g. projective left  $A$ -modules  $P$ , with relations  $[P \oplus P'] = [P] + [P']$  for all  $P, P' \in \mathcal{P}(A)$ . In the analogous version of the proof of (38.20), all the ses's which occur are split sequences, so we obtain:

**(38.22) Proposition.** *Let  $M, N \in \mathcal{P}(A)$ . Then  $[M] = [N]$  in  $K_0(A)$  if and only if*

$$(38.23) \quad M \oplus X \cong N \oplus X \quad \text{for some } X \in \mathcal{P}(A).$$

If (38.23) holds, then choosing  $Y \in \mathcal{P}(A)$  such that  $X \oplus Y$  is a free  $A$ -module  $A^{(k)}$ , we obtain

$$M \oplus A^{(k)} \cong N \oplus A^{(k)} \quad \text{for some } k.$$

We call  $M$  and  $N$  *stably isomorphic* when this occurs. We have thus shown that for  $M, N \in \mathcal{P}(A)$ ,  $[M] = [N]$  in  $K_0(A)$  if and only if  $M$  is stably isomorphic to  $N$ .

In many cases, stable isomorphism implies isomorphism. For example, if the K-S-A Theorem 6.12 is valid for f.g. projective  $A$ -modules, then from  $M \oplus A^{(k)} \cong N \oplus A^{(k)}$  we may conclude that  $M \cong N$ . In particular, if  $A$  is a left artinian ring, or if  $A$  is an algebra over a complete d.v.r., then (6.12) may be applied, and we conclude that stable isomorphism is identical with ordinary isomorphism in these cases. We shall have much more to say about this “cancellation” problem later on (see (41.20)).

We shall now introduce two new groups  $K_1(A)$  and  $G_1(A)$ , associated with an arbitrary ring  $A$ . As we shall see later, the group  $K_1(A)$  is closely related to the group of units  $A^\times$  of  $A$ . It has important applications to topology when  $A$  is an integral group ring. On the other hand, the group  $G_1(A)$  is often easier to compute, and there is a Cartan homomorphism  $K_1(A) \rightarrow G_1(A)$ , analogous to the Cartan map  $K_0(A) \rightarrow G_0(A)$ , which was studied extensively in §18.

To begin with, let  $\mathcal{C}$  be some category of left  $A$ -modules; the two cases of interest are those where  $\mathcal{C} = \mathcal{P}(A)$  and  $\mathcal{C} = {}_A\text{mod}$ , the category of all f.g. left  $A$ -modules. We intend to define  $K_1(\mathcal{C})$  by means of generators and relations,

just as we did in defining the Grothendieck group  $K_0(\mathcal{C})$ . For each  $M \in \mathcal{C}$ , let  $\text{Aut } M$  denote the group of all  $A$ -automorphisms of  $M$ . Consider the set of ordered pairs  $(M, \mu)$  with  $M \in \mathcal{C}$  and  $\mu \in \text{Aut } M$ . These pairs will be the generators of  $K_1(\mathcal{C})$ , and will be required to satisfy two types of relations. In case  $A$  is a field, and  $\mathcal{C}$  is the category of f.d. vector spaces over  $A$ , the relations become the familiar axiomatic description of the determinant map for automorphisms of a vector space. For this reason, for an arbitrary category  $\mathcal{C}$ , we often call  $K_1(\mathcal{C})$  the *determinantal*  $K_1$ , and write it as  $K_{\det}(\mathcal{C})$ .

Consider now the collection of all ordered pairs  $(M, \mu)$ , with  $M \in \mathcal{C}$  and  $\mu \in \text{Aut } M$ . A *morphism*  $f: (M, \mu) \rightarrow (N, v)$  is, by definition, an element  $f \in \text{Hom}_A(M, N)$  for which the diagram

$$\begin{array}{ccc} M & \xrightarrow{f} & N \\ \mu \downarrow & & \downarrow v \\ M & \xrightarrow{f} & N \end{array}$$

commutes. This collection of pairs, with morphisms defined as above, constitutes a category of modules.<sup>†</sup> A ses in this category

$$(38.24) \quad 0 \rightarrow (L, \lambda) \xrightarrow{f} (M, \mu) \xrightarrow{g} (N, v) \rightarrow 0$$

is a sequence in which  $f$  and  $g$  are morphisms, such that the sequence of  $A$ -modules

$$0 \rightarrow L \xrightarrow{f} M \xrightarrow{g} N \rightarrow 0$$

is exact. If we think of  $f$  as an embedding of  $L$  into  $M$ , and  $g$  as a natural surjection, the exactness of (38.24) means that the automorphism  $\mu$  of  $M$  induces an automorphism  $\lambda$  on the submodule  $L$ , and also induces an automorphism  $v$  on the factor module  $N = M/L$ .

Now write  $(M, \mu) \cong (N, v)$  if there exists a morphism  $f: (M, \mu) \rightarrow (N, v)$  such that  $f: M \cong N$ . Let  $\mathbf{G}$  be the free abelian group generated by all isomorphism classes of ordered pairs  $(M, \mu)$ . Let  $\mathbf{G}_0$  be the subgroup of  $\mathbf{G}$  generated by all expressions

$$(38.25) \quad (M, \mu) - (L, \lambda) - (N, v),$$

one for each ses (38.24), together with all expressions

$$(38.26) \quad (M, \mu\mu') - (M, \mu) - (M, \mu') \quad \text{for all } M \in \mathcal{C}, \quad \mu, \mu' \in \text{Aut } M.$$

<sup>†</sup>Let  $A' = A[x]$  be a polynomial ring over  $A$ , where  $x$  is an indeterminate commuting with all elements of  $A$ . Then  $(M, \mu)$  may be viewed as a left  $A'$ -module  $M$ , on which  $x$  acts as  $\mu$ . A morphism  $f: (M, \mu) \rightarrow (N, v)$  is then just an  $A'$ -homomorphism  $f: M \rightarrow N$ . This interpretation will be used in our proof of (38.45) below.

Let  $[M, \mu]$  denote the image of  $(M, \mu)$  in the quotient group  $\mathbf{G}/\mathbf{G}_0$ . We set

$$(38.27) \quad K_{\det}(\mathcal{C}) = \mathbf{G}/\mathbf{G}_0,$$

and call  $K_{\det}(\mathcal{C})$  the *determinantal K-group* of the category  $\mathcal{C}$ . We note that  $K_{\det}(\mathcal{C})$  is a homomorphic image of the Grothendieck group of the category of pairs  $(M, \mu)$  defined above. Further, since  $[M, \mu^{-1}] = -[M, \mu]$  in  $K_{\det}(\mathcal{C})$ , it follows that every element of  $K_{\det}(\mathcal{C})$  is expressible as  $[M, \mu]$  for some  $M \in \mathcal{C}$  and some  $\mu \in \text{Aut } M$ .

**(38.28) Definition.** The *Whitehead group*  $K_1(A)$  is the additive group  $K_{\det}(\mathcal{C})$ , where  $\mathcal{C}$  is the category  $\mathcal{P}(A)$ . On the other hand, define  $G_1(A)$  to be  $K_{\det}(\mathcal{C})$ , with  $\mathcal{C} = {}_A\text{mod}$ .

(Some authors use the term “Whitehead group” to refer to the group  $\text{Wh}(G) = K_1(\mathbb{Z}G)/\{\pm G^{ab}\}$ , where  $G$  is a finite group. The group  $\text{Wh}(G)$  will be discussed in §46.)

Now let  $A$  be a semisimple ring. It is clear that  $K_0(A) \cong G_0(A)$ , and the latter is a free abelian group on  $s$  generators, where  $s$  is the number of distinct simple left  $A$ -modules. We conclude this subsection with the computation of  $K_1(A)$ . This result is of intrinsic interest, and will be used repeatedly in later discussion. Let  $A = \bigoplus A_i$ , where the  $\{A_i\}$  are the Wedderburn components of  $A$ . Each  $M \in \mathcal{P}(A)$  decomposes into a direct sum  $M = \bigoplus M_i$ , with  $M_i \in \mathcal{P}(A_i)$ , and each  $\mu \in \text{Aut } M$  has a corresponding decomposition. It follows at once that

$$(38.29) \quad K_1(A) \cong \coprod_i K_1(A_i),$$

so the problem of evaluating  $K_1$  reduces to the case of simple artinian rings.

Changing notation, let  $A$  be a simple artinian ring. Then (see (3.55))  $A$  is Morita equivalent to a division ring  $D$ , and we have

$$(38.30) \quad K_1(D) \cong K_1(A).$$

Explicitly, write  $A = \text{End}_D V$  where  $V$  is a f.d. right vector space over  $D$ . There is a bijection between the isomorphism classes in  $\mathcal{P}(D)$  and  $\mathcal{P}(A)$ , which is given by mapping  $M \in \mathcal{P}(D)$  onto  $V \otimes_D M \in \mathcal{P}(A)$ . This bijection yields an isomorphism

$$\text{Aut}_D M \cong \text{Aut}_A(V \otimes_D M).$$

The isomorphism in (38.30) is then given by

$$[M, \mu] \rightarrow [V \otimes_D M, 1 \otimes \mu] \quad \text{for } M \in \mathcal{P}(D), \quad \mu \in \text{Aut}_D M.$$

In order to calculate  $K_1(D)$ , where  $D$  is a skewfield, we make use of Dieudonné determinants (see the discussion in §7 following (7.41)). Let  $D^* = D - \{0\}$ , and set

$$(38.31) \quad D^\# = D^\cdot / [D^\cdot, D^\cdot],$$

an abelian multiplicative group.

**(38.32) Theorem.** *The Dieudonné determinant gives an isomorphism of groups*

$$K_1(D) \cong D^\#$$

for every skewfield  $D$ .

*Proof.* Consider an ordered pair  $(M, \mu)$ , where  $M \in \mathcal{P}(D)$  and  $\mu \in \text{Aut}_D M$ . Each  $M \in \mathcal{P}(D)$  has a finite  $D$ -basis, relative to which  $\mu$  may be represented by a matrix  $\mathbf{X} \in GL_n(D)$ , where  $n = \dim_D M$ . Change of basis replaces  $\mathbf{X}$  by  $\mathbf{T}\mathbf{X}\mathbf{T}^{-1}$  for some  $\mathbf{T} \in GL_n(D)$ . If “det” denotes the Dieudonné determinant of a matrix, then  $\det \mathbf{X} \in D^\#$ , and

$$\det \mathbf{X} = \det \mathbf{T}\mathbf{X}\mathbf{T}^{-1}.$$

Setting  $\det \mu = \det \mathbf{X} \in D^\#$ , the Dieudonné determinant  $\det \mu$  is thus well defined.

Now let (38.24) be a ses, where  $L, M, N$  are  $D$ -spaces; we may choose a  $D$ -basis of  $M$  so that the matrix  $\mathbf{X}$  representing  $\mu$  has the form

$$\mathbf{X} = \begin{pmatrix} \mathbf{X}_1 & * \\ \mathbf{0} & \mathbf{X}_2 \end{pmatrix},$$

where  $\mathbf{X}_1$  is the matrix of  $\lambda$ , and  $\mathbf{X}_2$  that of  $v$ . Then  $\det \mathbf{X} = (\det \mathbf{X}_1)(\det \mathbf{X}_2)$ , that is,

$$\det \mu = (\det \lambda)(\det v).$$

Likewise,

$$\det \mu\mu' = (\det \mu)(\det \mu') \quad \text{for } \mu, \mu' \in \text{Aut } M.$$

It follows that there is a well-defined homomorphism

$$\det: K_1(D) \rightarrow D^\#,$$

which maps  $[M, \mu]$  onto  $\det \mu$ . The map is obviously surjective. To show it is injective, suppose that  $\det \mu = 1$ , and let  $\mu$  be represented by some matrix  $\mathbf{X}$ . Then we can find products  $\mathbf{P}$  and  $\mathbf{Q}$  of elementary matrices over  $D$ , such that

$$\mathbf{P}\mathbf{X}\mathbf{Q} = \text{diag}(1, \dots, 1, d)$$

for some  $d \in [D^\cdot, D^\cdot]$ . But every elementary matrix  $\mathbf{E}$  represents the zero element

of  $K_1(D)$ , since  $\mathbf{E}$  is of the form

$$\begin{pmatrix} \mathbf{I} & * \\ \mathbf{0} & \mathbf{I} \end{pmatrix} \quad \text{or} \quad \begin{pmatrix} \mathbf{I} & \mathbf{0} \\ * & \mathbf{I} \end{pmatrix},$$

and hence corresponds to some ses

$$0 \rightarrow (X_1, 1) \rightarrow (X_2, *) \rightarrow (X_3, 1) \rightarrow 0,$$

with  $[X_1, 1] = [X_3, 1] = 0$  in  $K_1(D)$ . Finally,  $\text{diag}(1, \dots, 1, d)$  represents the zero element in  $K_1(D)$ , since  $d \in [D^*, D^*]$  and  $K_1(D)$  is abelian. Thus, if  $\det \mu = 1$ , then  $[M, \mu] = 0$  in  $K_1(D)$ . This completes the proof that  $\det: K_1(D) \cong D^\#$ .

**Remarks.** (i) The above argument also shows that every element of  $K_1(D)$  has the form  $[D, d_r]$  for some  $d \in D^*$ , where  $d_r$  is right multiplication by  $d$ .

(ii) Klingenberg [62] has extended this theory to the case of a local ring  $R$ , not necessarily commutative. Set  $R^\# = R^*/[R^*, R^*]$ , where  $R^*$  is the group of units of  $R$ . There is a well-defined isomorphism  $\det: K_1(R) \cong R^\#$ , similar to that above.

### §38C. Regular Rings

In §38A, we needed to distinguish between the Grothendieck groups  $G_0(RG)$  and  $G_0^R(RG)$ , the first of which was associated with the category of all f.g.  $RG$ -modules, and the second with the category of  $RG$ -lattices. We shall see here that under suitable conditions on  $R$ , there is an isomorphism  $G_0(RG) \cong G_0^R(RG)$  of additive groups, a result which will be extremely useful. It will be convenient to treat a somewhat more general situation, rather than that of group rings.

Throughout this subsection,  $\Lambda$  denotes an arbitrary left noetherian ring<sup>†</sup>. All  $\Lambda$ -modules considered are assumed to be f.g. left  $\Lambda$ -modules. Let  $\mathcal{P}(\Lambda)$  denote the category of (f.g.) projective  $\Lambda$ -modules. Given any  $\Lambda$ -module  $M$ , and any integer  $n \geq 1$ , we can always find a  $\Lambda$ -exact sequence<sup>‡</sup>:

$$(38.33) \quad 0 \rightarrow L \rightarrow P_{n-1} \xrightarrow{\varphi_{n-1}} \cdots \xrightarrow{\varphi_1} P_0 \xrightarrow{\varphi_0} M \rightarrow 0, \quad P_i \in \mathcal{P}(\Lambda),$$

with  $L$  some  $\Lambda$ -module (see §8A).

**(38.34) Definition.** The  $\Lambda$ -module  $M$  has *finite homological dimension*  $\text{hd}_\Lambda(M)$  if there exists a  $\Lambda$ -exact sequence (38.33) in which  $L$  is  $\Lambda$ -projective. We write  $\text{hd}_\Lambda(M) \leq n$  in this case. If  $n$  is the least nonnegative integer for which  $\text{hd}_\Lambda(M) \leq n$ , we write  $\text{hd}_\Lambda(M) = n$ . Finally, write  $\text{hd}_\Lambda(M) = \infty$  if  $M$  does not have finite homological dimension.

<sup>†</sup>Some of the results are true even when  $\Lambda$  is not noetherian.

<sup>‡</sup>This means an exact sequence of  $\Lambda$ -modules.

We have previously encountered this concept in Volume I (p. 569), and we prove first that the above definition agrees with our earlier one. Of course,

$$(38.35) \quad \text{hd}_\Lambda(M) = 0 \Leftrightarrow M \in \mathcal{P}(\Lambda) \Leftrightarrow \text{Ext}_\Lambda^k(M, *) = 0 \quad \text{for } k \geq 1.$$

The first equivalence is clear, while the second follows from (8.4v). We now prove

**(38.36) Proposition.** *Let  $M$  be a  $\Lambda$ -module. Then*

$$\text{hd}_\Lambda(M) \leq n \quad \text{if and only if} \quad \text{Ext}_\Lambda^k(M, *) = 0 \quad \text{for } k \geq n + 1.$$

*Proof.* Suppose  $\text{hd}(M) \leq n$  (we omit the subscript  $\Lambda$  for convenience). Then the module  $L$  in some sequence (38.33) is  $\Lambda$ -projective, and the sequence is a projective resolution of  $M$ . It follows from (8.3) that  $\text{Ext}^k(M, *) = 0$  whenever  $k \geq n + 1$ .

Conversely, suppose that  $\text{Ext}^{n+1}(M, *) = 0$ , and let us prove that in any  $\Lambda$ -exact sequence (38.33), the module  $L$  must be projective. The case  $n = 0$  has already been settled, so let  $n \geq 1$ . We may break (38.33) into a succession of ses's:

$$0 \rightarrow L_0 \rightarrow P_0 \xrightarrow{\varphi_0} M \rightarrow 0, \quad 0 \rightarrow L_1 \rightarrow P_1 \xrightarrow{\varphi_1} L_0 \rightarrow 0, \dots, 0 \rightarrow L \rightarrow P_{n-1} \rightarrow L_{n-2} \rightarrow 0$$

where  $L_0 = \ker \varphi_0$ ,  $L_1 = \ker \varphi_1$ , and so on. From (8.8) we obtain readily

$$\text{Ext}^{n+1}(M, X) \cong \text{Ext}^n(L_0, X) \cong \text{Ext}^{n-1}(L_1, X) \cong \dots \cong \text{Ext}^1(L, X),$$

for each  $\Lambda$ -module  $X$ . Thus,  $\text{Ext}^1(L, *) = 0$ , so  $L$  is projective.

The preceding result implies that if there exists one sequence (38.33) in which the left-most term  $L$  is projective, then the left-most term  $L$  is necessarily projective in *every* such sequence. This also follows from

**(38.37) Generalized Schanuel's Lemma.** *Given a pair of  $\Lambda$ -exact sequences*

$$0 \rightarrow L \rightarrow P_{n-1} \rightarrow \dots \rightarrow P_0 \rightarrow M \rightarrow 0, \quad 0 \rightarrow L' \rightarrow P'_{n-1} \rightarrow \dots \rightarrow P'_0 \rightarrow M \rightarrow 0,$$

*with each  $P_i$  and  $P'_i$  projective, we have an isomorphism*<sup>†</sup>

$$L \oplus P'_{n-1} \oplus P_{n-2} \oplus P'_{n-3} \oplus \dots \cong L' \oplus P_{n-1} \oplus P'_{n-2} \oplus P_{n-3} \oplus \dots$$

*Proof.* This follows from Schanuel's Lemma 2.24, together with the decomposition of a long exact sequence into ses's, as in the preceding proof. The details are left to the reader.

<sup>†</sup>The final terms in the isomorphism are  $P_0$  and  $P'_0$ , and these occur on opposite sides, depending on the parity of  $n$ .

Suppose now that we are given an exact sequence of  $\Lambda$ -modules

$$(38.38) \quad 0 \rightarrow M' \rightarrow M \rightarrow M'' \rightarrow 0.$$

We wish to compare projective resolutions and homological dimensions of these modules. The comparison of homological dimension is an easy consequence of (8.6); see Exercise 38.11. However, the approach by means of projective resolutions yields more information, which will be needed for the proofs of the basic theorems (38.42) and (38.45) below. We shall start with partial projective resolutions of  $M'$  and  $M''$ , and show how to combine them to give such a resolution of  $M$ . We have

**(38.39) Horseshoe Lemma.** *Consider a “horseshoe” diagram of  $\Lambda$ -modules*

$$\begin{array}{ccccccc} & & & & 0 & & \\ & & & & \downarrow & & \\ 0 \rightarrow K' \rightarrow P'_n \rightarrow \cdots \rightarrow P'_0 \rightarrow M' \rightarrow 0 & & & & & & \\ & & & & \downarrow f & & \\ & & & & M & & \\ & & & & \downarrow g & & \\ 0 \rightarrow K'' \rightarrow P''_n \rightarrow \cdots \rightarrow P''_0 \rightarrow M'' \rightarrow 0 & & & & & & \\ & & & & \downarrow & & \\ & & & & 0 & & \end{array}$$

where the column is exact (as in (38.38)), and where the rows are exact, with each  $P'_i, P''_i$  projective. Then there exist a  $\Lambda$ -module  $K$  and maps for which the following diagram commutes, and has exact rows and exact columns:

$$\begin{array}{ccccccc} 0 \rightarrow K' \rightarrow & P'_n & \rightarrow \cdots \rightarrow & P'_0 & \rightarrow M' \rightarrow 0 \\ \downarrow & \downarrow & & & \downarrow & & \downarrow f \\ 0 \rightarrow K \rightarrow P'_n \oplus P''_n \rightarrow \cdots \rightarrow P'_0 \oplus P''_0 \rightarrow M \rightarrow 0 \\ \downarrow & \downarrow & & & \downarrow & & \downarrow g \\ 0 \rightarrow K'' \rightarrow & P''_n & \rightarrow \cdots \rightarrow & P''_0 & \rightarrow M'' \rightarrow 0. \end{array}$$

Each upper vertical arrow is injective, each lower one surjective.

*Proof.* Left as exercise for the reader. Use induction on  $n$ .

**(38.40) Definition.** The (left) global dimension  $\text{gl. dim. } \Lambda$  of a ring  $\Lambda$  is defined by

$$\text{gl. dim. } \Lambda = \sup \{ \text{hd}_\Lambda(M) : M = \Lambda\text{-module} \}.$$

As shown by M. Auslander, one can compute  $\text{gl. dim. } \Lambda$  by studying f.g.

$\Lambda$ -modules, and indeed even just *cyclic* modules. This follows from the formula

$$\text{gl. dim. } \Lambda = \sup \{ \text{hd}_\Lambda(\Lambda/L) : L = \text{left ideal of } \Lambda \}$$

(see Rotman [79, Theorem 9.12] for a proof).

We remark that  $\text{gl. dim. } \Lambda = 0$  if and only if every left  $\Lambda$ -module is projective, or equivalently, if and only if  $\Lambda$  is a semisimple ring. Next, we note that  $\text{gl. dim. } \Lambda \leq 1$  if and only if  $\Lambda$  is left hereditary. For, if  $\text{gl. dim. } \Lambda \leq 1$ , then consider the sequence  $0 \rightarrow M \rightarrow \Lambda \rightarrow \Lambda/M \rightarrow 0$ , where  $M$  is any left ideal of  $\Lambda$ . Since  $\text{hd}_\Lambda(\Lambda/M) \leq 1$ , it follows that  $M$  must be  $\Lambda$ -projective, and so  $\Lambda$  is left hereditary. Conversely, if  $\Lambda$  is left hereditary, then every submodule of a free  $\Lambda$ -module is projective (see (4.3)), which easily implies that  $\text{gl. dim. } \Lambda \leq 1$ .

In particular, by (4.6) every Dedekind domain  $R$  is hereditary, and thus  $\text{gl. dim. } R \leq 1$ . (Indeed,  $\text{gl. dim. } R = 1$  if  $R$  is not a field!)

**(38.41) Definition.** A left noetherian ring  $\Lambda$ , such that every f.g. left  $\Lambda$ -module  $M$  has finite homological dimension, is called a (left) *regular* ring.

All semisimple rings and all hereditary noetherian rings are regular. In particular, every Dedekind domain is a regular ring.

(We caution the reader that there exist regular rings  $\Lambda$  for which  $\text{gl. dim. } \Lambda = \infty$ . However, if  $\Lambda$  is noetherian and  $\text{gl. dim. } \Lambda$  is finite, then, of course,  $\Lambda$  is a regular ring.)

From now on, let  $R$  be a commutative regular ring, so  $R$  is noetherian, and every f.g.  $R$ -module has finite homological dimension. Let  $\Lambda$  be an  $R$ -algebra (see §1A), and assume always that  $\Lambda$  is f.g. and projective as  $R$ -module. (This certainly holds in case  $\Lambda$  is a group ring  $RG$ , where  $G$  is a finite group.) As usual, a  $\Lambda$ -lattice is a left  $\Lambda$ -module which is f.g. and projective as  $R$ -module (see §23).

Let  $G_0(\Lambda)$ ,  $G_1(\Lambda)$  be defined as in §38B. Let  $G_0^R(\Lambda)$  and  $G_1^R(\Lambda)$  be defined analogously, by restricting our attention to  $\Lambda$ -lattices rather than arbitrary f.g.  $\Lambda$ -modules. Our aim here is to establish the isomorphisms

$$G_0(\Lambda) \cong G_0^R(\Lambda), \quad G_1(\Lambda) \cong G_1^R(\Lambda),$$

whenever  $R$  is regular.

**(38.42) Theorem.** *Let  $R$  be a commutative regular ring, and let  $\Lambda$  be an  $R$ -algebra, f.g. and projective as  $R$ -module. Then there is an isomorphism*

$$f: G_0^R(\Lambda) \cong G_0(\Lambda),$$

defined by  $f[M] = [M]$  for every  $\Lambda$ -lattice  $M$ .

*Proof.* The map  $f$  is a well-defined homomorphism, and we need only construct an inverse map  $g$ . Given any f.g.  $\Lambda$ -module  $M$ , let  $n$  be such that  $\text{hd}_R(M) \leq n$ ,

and choose a  $\Lambda$ -exact sequence (38.33) with each  $P_i \in \mathcal{P}(\Lambda)$ . Since  $\Lambda$  is  $R$ -projective, so is each  $P_i$ . Therefore  $L$  is also  $R$ -projective, and is thus a  $\Lambda$ -lattice. We now put

$$g[M] = [P_0] - [P_1] + \cdots + (-1)^{n-1}[P_{n-1}] + (-1)^n[L] \in G_0^R(\Lambda).$$

It follows at once from the Generalized Schanuel's Lemma that  $g[M]$  does not depend on the choice of the sequence (38.33). Further, given (38.38), we first choose partial resolutions of  $M'$  and  $M''$ , and then use the Horseshoe Lemma to obtain one of  $M$ . It is then clear that  $g[M] = g[M'] + g[M'']$ , so  $g$  is a well-defined homomorphism from  $G_0(\Lambda)$  into  $G_0^R(\Lambda)$ . It is straightforward to check that  $gf = 1$  and  $fg = 1$ , so both  $f$  and  $g$  are isomorphisms, and the theorem is proved.

In the special case where  $\Lambda = R$ , a  $\Lambda$ -lattice  $M$  is just a module  $M \in \mathcal{P}(\Lambda)$ . Thus, the theorem gives

$$K_0(R) \cong G_0(R)$$

whenever  $R$  is a commutative regular ring. As we shall see in (38.51) below, this isomorphism holds for an arbitrary regular ring, not necessarily commutative.

We shall apply Theorem 38.42 to study the behavior of  $G_0$  and  $K_0$  under ground ring extension. Given any ring homomorphism  $\varphi: \Lambda \rightarrow \Gamma$ , there is an additive homomorphism  $K_0(\Lambda) \rightarrow K_0(\Gamma)$ , given by  $\Gamma \otimes_{\Lambda} *$ . This means that we use  $\varphi$  to make  $\Gamma$  into a right  $\Lambda$ -module, and then the map  $K_0(\Lambda) \rightarrow K_0(\Gamma)$  is given by  $[M] \rightarrow [\Gamma \otimes_{\Lambda} M]$ , for  $M \in \mathcal{P}(\Lambda)$ . There is no corresponding map  $G_0(\Lambda) \rightarrow G_0(\Gamma)$  in general, although such a map is well defined whenever  $\Gamma$  is flat as right  $\Lambda$ -module.

Suppose in particular that  $\Lambda$  is an  $R$ -algebra, and that  $f: R \rightarrow S$  is a homomorphism of commutative rings. Then there is a homomorphism

$$S \otimes_R *: K_0(\Lambda) \rightarrow K_0(S \otimes_R \Lambda).$$

As remarked earlier, this need not define a map on  $G_0$ , since  $S$  need not be  $R$ -flat. Nevertheless, we have

**(38.43) Proposition.** *Let  $R$  be a commutative regular ring, and let  $\Lambda$  be an  $R$ -algebra, f.g. and projective as  $R$ -module. Let  $f: R \rightarrow S$  be a homomorphism of commutative rings. Then there is an additive homomorphism*

$$\varphi: G_0(\Lambda) \rightarrow G_0(S \otimes_R \Lambda),$$

defined by composition of maps

$$G_0(\Lambda) \xrightarrow{\alpha} G_0^R(\Lambda) \xrightarrow{\beta} G_0^S(S \otimes \Lambda) \xrightarrow{\gamma} G_0(S \otimes \Lambda),$$

where  $\otimes$  means  $\otimes_R$ .

*Proof.* The map  $\alpha$  is the isomorphism defined in (38.42), while  $\gamma$  is the obvious map (taking lattices to modules). Finally,  $\beta$  is well-defined, since each ses of  $\Lambda$ -lattices (38.38) is  $R$ -split; therefore  $S \otimes *$  preserves exactness (and splitting!).

**Caution.** (i) If  $M$  is an arbitrary f.g.  $\Lambda$ -module, then  $\varphi[M]$  need not equal  $[S \otimes M]$  in  $G_0(S \otimes \Lambda)$ . In order to compute  $\varphi[M]$ , we first choose a sequence (38.33), and then

$$\varphi[M] = [S \otimes P_0] - [S \otimes P_1] + \cdots + (-1)^n [S \otimes L] \in G_0(S \otimes \Lambda).$$

(ii) Suppose for the moment that  $\Lambda = RG$ , where  $R$  is any commutative ring, and  $G$  is a finite group. As remarked in §38A,  $G_0^R(\Lambda)$  is a commutative ring, with multiplication given by

$$(38.44) \quad [M][N] = [M \otimes_R N],$$

where  $M \otimes_R N$  is the inner tensor product of the  $\Lambda$ -lattices  $M$  and  $N$ . The identity element of  $G_0^R(\Lambda)$  is the  $G$ -trivial  $\Lambda$ -lattice  $R$ . If  $R$  is regular, we can use the additive isomorphism  $G_0(\Lambda) \cong G_0^R(\Lambda)$  to make  $G_0(\Lambda)$  into a commutative ring as well. However, if  $M$  and  $N$  are arbitrary f.g.  $\Lambda$ -modules, then formula (38.44) need not be valid inside  $G_0(\Lambda)$ .

Next, we establish the analogue of Theorem 38.42 for  $G_1$  in place of  $G_0$ . For an  $R$ -algebra  $\Lambda$ , we define  $G_1(\Lambda)$  as in (38.28). Also, we define  $G_1^R(\Lambda)$  by using the category of all  $\Lambda$ -lattices. We have

**(38.45) Theorem.** *Let  $R$  be a commutative regular ring, and let  $\Lambda$  be an  $R$ -algebra, f.g. and projective as  $R$ -module. Then there is an isomorphism*

$$G_1^R(\Lambda) \cong G_1(\Lambda),$$

given by  $[M, \mu] \rightarrow [M, \mu]$  for each  $\Lambda$ -lattice  $M$  and each  $\mu \in \text{Aut } M$ .

*Proof.* Step 1. For  $n \geq 0$ , let

$$\mathcal{C}_n = \{M : M = \text{f.g. left } \Lambda\text{-module, } \text{hd}_R(M) \leq n\}.$$

Thus  $\mathcal{C}_0$  is the category of all  $\Lambda$ -lattices, and every f.g.  $\Lambda$ -module belongs to  $\mathcal{C}_n$  for all sufficiently large  $n$ . Let  $H_n$  be the abelian group generated by all symbols  $[M, \mu]$ ,  $M \in \mathcal{C}_n$ , subject to the standard relations arising from (38.25) and (38.26). The inclusion  $\mathcal{C}_n \subseteq \mathcal{C}_{n+1}$  induces a homomorphism  $H_n \rightarrow H_{n+1}$ , and we may identify  $G_1(\Lambda)$  with the direct limit  $\lim H_n$ . This means that every element of  $G_1(\Lambda)$  lies in some  $H_n$ , and that if  $x \in H_n$ ,  $y \in H_m$ , then  $x = y$  in  $G_1(\Lambda)$  if and only if  $x$  and  $y$  have the same images in some  $H_r$ , where  $r \geq m$  and  $r \geq n$ . Now  $H_0 = G_1^R(\Lambda)$ , and we shall prove that for each  $n$ , the inclusion  $\mathcal{C}_n \subseteq \mathcal{C}_{n+1}$  yields an isomorphism  $H_n \cong H_{n+1}$ . It will then follow that  $H_0 \cong H_1 \cong \cdots \cong \lim H_n = G_1(\Lambda)$ , and the theorem will be established.

*Step 2.* We claim that for each f.g.  $\Lambda$ -module  $M$ , there exists a surjection

$$f_0: P_0 \rightarrow M, \quad \text{where } P_0 \in \mathcal{P}(\Lambda),$$

such that every automorphism  $\mu$  of  $M$  lifts to an automorphism  $\pi_0$  of  $P_0$ . In other words, there exists a morphism  $f_0$  of  $(P_0, \pi_0)$  onto  $(M, \mu)$ .

To begin with, let  $f: P \rightarrow M$  be a surjection, with  $P \in \mathcal{P}(\Lambda)$ . Set  $P_0 = P \oplus P$ , and let  $f_0: P_0 \rightarrow M$  be the map defined by composition

$$P_0 = P \oplus P \xrightarrow{(f,f)} M \oplus M \xrightarrow{(1,0)} M,$$

so  $f_0$  is surjective. Given any  $\mu \in \text{Aut } M$ , consider the following commutative diagram, to be solved for  $\pi_0 \in \text{Aut } P_0$ :

$$\begin{array}{ccc} P_0 = P \oplus P & \xrightarrow{(f,f)} & M \oplus M \xrightarrow{(1,0)} M \\ \pi_0 \downarrow & & \downarrow (\mu, \mu^{-1}) \\ P_0 = P \oplus P & \xrightarrow{(f,f)} & M \oplus M \xrightarrow{(1,0)} M. \end{array}$$

Such a  $\pi_0$  will be a lifting of  $\mu$ , as required.

Let  $\Gamma = \text{End}_\Lambda M$ , and view the map  $(\mu, \mu^{-1})$  as a matrix  $\text{diag}(\mu, \mu^{-1}) \in GL_2(\Gamma)$ . This matrix can be written as a product of elementary matrices, as in (34.20), and it suffices to show that each of these elementary matrices can be lifted to an automorphism of  $P_0$ . Consider, for example, the matrix

$$\begin{pmatrix} 1 & \alpha \\ 1 & 1 \end{pmatrix}, \quad \text{where } \alpha \in \Gamma.$$

It acts on  $M \oplus M$  according to the rule

$$(m_1, m_2) \mapsto (m_1, m_2 + \alpha m_1), \quad m_i \in M.$$

Symbolically, the automorphism of  $M \oplus M$  given thus may be written as

$$\begin{array}{ccc} M \oplus M & & \\ 1 \downarrow \alpha \swarrow 1 \downarrow & & \\ M \oplus M. & & \end{array}$$

Since  $f: P \rightarrow M$  is surjective, we can lift  $\alpha$  to an endomorphism  $\theta$  of  $P$ , by (2.22iii). There is then a commutative diagram

$$\begin{array}{ccc} P \oplus P & \xrightarrow{(f,f)} & M \oplus M \\ 1 \swarrow \theta \searrow 1 \downarrow & & 1 \downarrow \alpha \swarrow 1 \downarrow \\ P \oplus P & \xrightarrow{(f,f)} & M \oplus M, \end{array}$$

so  $\begin{pmatrix} 1 & \theta \\ 0 & 1 \end{pmatrix}$  is the desired lifting of  $\begin{pmatrix} 1 & \alpha \\ 0 & 1 \end{pmatrix}$ . A similar argument holds for  $\begin{pmatrix} 1 & 0 \\ \alpha & 1 \end{pmatrix}$ , and we have now established the claim made at the start of this step.

*Step 3.* Now let  $n \geq 1$ , and let  $\varphi: H_{n-1} \rightarrow H_n$  be induced by  $\mathcal{C}_{n-1} \subseteq \mathcal{C}_n$ . We show that  $\varphi$  is an isomorphism, by constructing an inverse map  $\psi: H_n \rightarrow H_{n-1}$ . For this purpose, we shall view the category of ordered pairs  $(M, \mu)$  as a category of modules. Specifically, consider the polynomial ring  $\Lambda[x]$ , where  $x$  is an indeterminate which commutes with the elements of  $\Lambda$ . Then  $(M, \mu)$  may be viewed as a left  $\Lambda[x]$ -module  $M$ , on which  $x$  acts as  $\mu$ . We can thus apply module-theoretic arguments to such pairs.

Given  $M \in \mathcal{C}_n$ , choose a surjection  $f: P \rightarrow M$  with  $P \in \mathcal{P}(\Lambda)$ , such that every automorphism  $\mu$  of  $M$  lifts to an automorphism  $\pi$  of  $P$ . Letting  $X = \ker f$ , we see from (38.37) that  $X \in \mathcal{C}_{n-1}$ . Further, if  $\xi = \pi|_X$ , then  $\xi \in \text{Aut } X$ , and the sequence

$$(38.46) \quad 0 \rightarrow (X, \xi) \rightarrow (P, \pi) \xrightarrow{f} (M, \mu) \rightarrow 0$$

is exact. But then

$$(38.47) \quad [M, \mu] = [P, \pi] - [X, \xi] \quad \text{in } H_n,$$

which proves that  $\varphi$  maps  $H_{n-1}$  onto  $H_n$ . We now define

$$\psi[M, \mu] = [P, \pi] - [X, \xi],$$

so  $\psi$  is a map from  $H_n$  to  $H_{n-1}$ . In order to verify that  $\psi$  is a well-defined homomorphism, we must prove:

- (a)  $\psi[M, \mu]$  is independent of the choice of the sequence (38.46).
- (b) For  $\mu_1, \mu_2 \in \text{Aut } M$ ,

$$\psi[M, \mu_1 \mu_2] = \psi[M, \mu_1] + \psi[M, \mu_2].$$

- (c) For each exact sequence

$$(38.48) \quad 0 \rightarrow (M', \mu') \xrightarrow{g} (M, \mu) \xrightarrow{h} (M'', \mu'') \rightarrow 0,$$

where each module lies in  $\mathcal{C}_n$ , we have

$$(38.49) \quad \psi[M, \mu] = \psi[M', \mu'] + \psi[M'', \mu''].$$

To prove (a), consider another exact sequence

$$0 \rightarrow (X', \xi') \rightarrow (P', \pi') \xrightarrow{f'} (M, \mu) \rightarrow 0,$$

with  $P' \in \mathcal{P}(\Lambda)$ . We now imitate the proof of Schanuel's Lemma, viewing the ordered pairs as  $\Lambda[x]$ -modules. Let  $(Y, \eta)$  be the pullback of the pair of maps  $f, f'$ . Then there is a commutative diagram of  $\Lambda[x]$ -modules, with exact rows and columns:

$$\begin{array}{ccccccc}
 & & & 0 & & & \\
 & & & \downarrow & & & \\
 & & & (X, \xi) & & & \\
 & & & \downarrow & & & \\
 0 \rightarrow (X', \xi') \rightarrow (Y, \eta) & \longrightarrow & (P, \pi) \rightarrow 0 & & & & \\
 & & \downarrow & & f \downarrow & & \\
 & & (P', \pi') & \xrightarrow{f'} & (M, \mu) \rightarrow 0 & & \\
 & & \downarrow & & & & \\
 & & 0 & & & & 
 \end{array}$$

Then  $0 \rightarrow X \rightarrow Y \rightarrow P' \rightarrow 0$  is a  $\Lambda$ -exact sequence, and so  $Y \cong X \oplus P' \in \mathcal{C}_{n-1}$ . Further, since  $\pi$  and  $\xi'$  are automorphisms, so is  $\eta$  (by the Snake Lemma). Using exactness of rows and columns above, we obtain two identities in  $H_{n-1}$ :

$$[Y, \eta] = [X, \xi] + [P', \pi'], \quad [Y, \eta] = [X', \xi'] + [P, \pi].$$

This yields

$$[P, \pi] - [X, \xi] = [P', \pi'] = [X', \xi'],$$

and completes the proof of (a).

For (b), choose  $f: P \rightarrow M$  as in (38.46). Given  $\mu_1, \mu_2 \in \text{Aut } M$ , we may find  $\pi_i \in \text{Aut } P, \xi_i \in \text{Aut } X, i = 1, 2$ , such that  $\pi_i$  lifts  $\mu_i$ . Then  $\pi_1 \pi_2$  lifts  $\mu_1 \mu_2$ , and we have

$$\begin{aligned}
 \psi[M, \mu_1 \mu_2] &= [P, \pi_1 \pi_2] - [X, \xi_1 \xi_2] \\
 &= [P, \pi_1] + [P, \pi_2] - [X, \xi_1] - [X, \xi_2] \quad \text{in } H_{n-1},
 \end{aligned}$$

which proves (b).

Finally, we prove (c) by giving the first step in the proof of the Horseshoe Lemma in the present context. Starting with (38.48), choose surjections  $f': P' \rightarrow M', f'': P'' \rightarrow M'',$  where  $P', P'' \in \mathcal{P}(\Lambda)$ , with the lifting property for automorphisms. There is an exact sequence

$$0 \rightarrow (X', \xi') \rightarrow (P', \pi') \xrightarrow{f'} (M', \mu') \rightarrow 0,$$

where  $X' = \ker f'$ . Choose  $f: P \rightarrow M$  as in (38.46), and define a pair of morphisms:

$$(P', \pi') \xrightarrow{gf'} (M, \mu), \quad (P, \pi) \xrightarrow{hf} (M'', \mu'').$$

Now pick  $(X_0, \xi_0)$  so that

$$0 \rightarrow (X_0, \xi_0) \rightarrow (P', \pi') \oplus (P, \pi) \xrightarrow{(gf', f)} (M, \mu) \rightarrow 0$$

is exact. Likewise, choose  $(X'', \xi'')$  so that

$$0 \rightarrow (X'', f'') \rightarrow (P, \pi) \xrightarrow{hf} (M'', \mu'') \rightarrow 0$$

is exact. Clearly each of  $X_0$ ,  $X'$ , and  $X''$  lies in  $\mathcal{C}_{n-1}$ , and there is a commutative diagram with exact rows and columns:

$$\begin{array}{ccc} 0 & 0 & 0 \\ \downarrow & \downarrow & \downarrow \\ (X', \xi') & (X_0, \xi_0) & (X'', \xi'') \\ \downarrow & \downarrow & \downarrow \\ 0 \rightarrow (P', \pi') \xrightarrow{(1,0)} (P', \pi') \oplus (P, \pi) \xrightarrow{(0,1)} (P, \pi) \rightarrow 0 \\ \downarrow f' & \downarrow (gf', f) & \downarrow hf \\ 0 \rightarrow (M', \mu') \longrightarrow (M, \mu) \longrightarrow (M'', \mu'') \rightarrow 0 \\ \downarrow & \downarrow & \downarrow \\ 0 & 0 & 0 \end{array}$$

Viewing the pairs as  $\Lambda[x]$ -modules, the Snake Lemma yields an exact sequence

$$0 \rightarrow (X', \xi') \rightarrow (X_0, \xi_0) \rightarrow (X'', \xi'') \rightarrow 0.$$

Therefore

$$[X_0, \xi_0] = [X', \xi'] + [X'', \xi''] \quad \text{in } H_{n-1}.$$

(The Snake Lemma also shows that  $\xi''$  and  $\xi_0$  are automorphisms.) Now

$$\psi[M, \mu] = [P', \pi'] + [P, \pi] - [X_0, \xi_0],$$

$$\psi[M', \mu'] = [P', \pi'] - [X', \xi'], \quad \psi[M'', \mu''] = [P, \pi] - [X'', \xi''],$$

and so we obtain the desired formula (38.49).

We have thus verified (a)–(c), so  $\psi: H_n \rightarrow H_{n-1}$  is a well-defined homomorphism. Next, if  $M \in \mathcal{C}_{n-1}$  then (38.47) holds in  $H_{n-1}$  as well as in  $H_n$ . This implies that  $\psi\varphi = 1$ , so  $\varphi$  is injective. We have shown above that  $\varphi$  is surjective, so we conclude that  $\varphi$  is an isomorphism, and the theorem is proved.

In the above proof, we have followed the treatment in Swan [68]. For more general theorems of the above type, see Swan [68, pages 224–247, and especially (16.15)–(16.17)].

For an arbitrary category  $\mathcal{C}$  of modules, we have defined  $K_0(\mathcal{C})$  in (16.3); it is generated by symbols  $[M]$ ,  $M \in \mathcal{C}$ , with relations arising from ses's of modules in  $\mathcal{C}$ . Also, we defined  $K_{\det}(\mathcal{C})$  in (38.27); it is generated by symbols  $[M, \mu]$ ,

$M \in \mathcal{C}$ ,  $\mu \in \text{Aut } M$ , with relations of the types (38.25) and (38.26). In the special case where  $\mathcal{C} = \mathcal{P}(\Lambda)$ , the category of f.g. projective  $\Lambda$ -modules, we defined

$$K_0(\Lambda) = K_0(\mathcal{P}(\Lambda)), \quad K_1(\Lambda) = K_{\det}(\mathcal{P}(\Lambda)).$$

Following this review, we give some easy consequences of the proofs of Theorems 38.42 and 38.45, namely:

**(38.50) Theorem.** *Let  $\Lambda$  be an arbitrary noetherian ring, and let  $\mathcal{C}$  be the category of all f.g. left  $\Lambda$ -modules  $M$  for which  $\text{hd}_\Lambda(M)$  is finite. Then there exist isomorphisms*

$$K_0(\Lambda) \cong K_0(\mathcal{C}), \quad K_1(\Lambda) \cong K_{\det}(\mathcal{C}).$$

*Proof.* Let  $\mathcal{C}_n$  be the category of all f.g.  $\Lambda$ -modules  $M$  with  $\text{hd}_\Lambda(M) \leq n$ . The proof of (38.45) shows that the inclusion  $\mathcal{C}_{n-1} \subseteq \mathcal{C}_n$  induces an isomorphism  $K_{\det}(\mathcal{C}_{n-1}) \cong K_{\det}(\mathcal{C}_n)$ . This implies that

$$K_1(\Lambda) = K_{\det}(\mathcal{C}_0) \cong K_{\det}(\mathcal{C}_1) \cong \cdots \cong K_{\det}(\mathcal{C}).$$

If we omit all of the automorphisms, we get likewise  $K_0(\Lambda) \cong K_0(\mathcal{C})$ , and the theorem is proved.

We have at once:

**(38.51) Corollary.** *If  $\Lambda$  is a left regular ring, then*

$$K_0(\Lambda) \cong G_0(\Lambda), \quad K_1(\Lambda) \cong G_1(\Lambda).$$

In the remarks following (38.42), we already pointed out that  $K_0(\Lambda) \cong G_0(\Lambda)$  for  $\Lambda$  a commutative regular ring.

Our last topic in this subsection is the computation of the group  $K_0(R)$  for a Dedekind domain  $R$ . More precisely, we shall express  $K_0(R)$  in terms of the ideal class group  $\text{Cl}(R)$  defined in §4F.

**(38.52) Theorem.** *Let  $R$  be a Dedekind domain. Then*

$$K_0(R) \cong \mathbb{Z} \oplus \text{Cl}(R),$$

that is,  $K_0(R)$  is the direct product of the additive group  $\mathbb{Z}$  and the multiplicative group  $\text{Cl}(R)$ .

*Proof.* Steinitz's Theorem tells us that each  $M \in \mathcal{P}(R)$  is expressible as an external direct sum

$$(38.53) \quad M = \coprod_{i=1}^r J_i,$$

with each  $J_1$  a nonzero ideal of  $R$ . The isomorphism class of  $M$  is uniquely determined by the rank  $r = r(M)$  and the ideal class of the product  $J_1 \cdots J_r$ . This ideal class is called the *Steinitz class* of  $M$ , and we shall denote it for the moment by  $\text{St}(M)$ .

Now  $K_0(R)$  is generated by stable isomorphism classes  $[X]$  of modules  $X \in \mathcal{P}(R)$ . However, for  $X, Y \in \mathcal{P}(R)$ ,

$$X \oplus R^{(k)} \cong Y \oplus R^{(k)} \Rightarrow X \cong Y,$$

by Steinitz's Theorem. Thus,  $K_0(R)$  is generated by symbols  $[X]$ ,  $X \in \mathcal{P}(R)$ , and  $[X] = [Y]$  in  $K_0(R)$  if and only if  $X \cong Y$ . The relations in  $K_0(R)$  are given by  $[X] + [X'] = [X \oplus X']$ , for  $X, X' \in \mathcal{P}(R)$ .

For each  $M \in \mathcal{P}(R)$ , put

$$\psi[M] = (r(M), \text{St}(M)) \in \mathbb{Z} \oplus \text{Cl}(R).$$

Then  $\psi$  gives a well defined homomorphism  $\psi: K_0(R) \rightarrow \mathbb{Z} \oplus \text{Cl}(R)$ , since for  $M, M' \in \mathcal{P}(R)$ , we have

$$r(M \oplus M') = r(M) \oplus r(M'), \quad \text{St}(M \oplus M') = \text{St}(M) \cdot \text{St}(M').$$

It is easily verified that  $\psi$  is the desired isomorphism. (If the quotient field of  $R$  is a global field, the result is a special case of Theorem 38.67 below.)

The computation of  $K_1(R)$  lies considerably deeper, and we begin by defining a homomorphism

$$\det: K_1(R) \rightarrow R^*,$$

where  $R^*$  is the group of units of  $R$ . Consider an ordered pair  $(M, \mu)$ , where  $M \in \mathcal{P}(R)$  is as in (38.53), and where  $\mu \in \text{Aut}_R M$ . Let  $F$  be the quotient field of  $R$ , so  $F \otimes_R M$  is an  $r$ -dimensional vector space over  $F$ , where  $r$  is the rank of  $M$ . The automorphism  $\mu$  of  $M$  defines an invertible linear transformation  $1 \otimes \mu$  on  $F \otimes_R M$ , and we now set

$$\det(M, \mu) = \det(1 \otimes \mu).$$

In order to verify that  $\det$  is well defined on  $K_1(R)$ , we must show that

$$\det(M, \mu\mu') = \det(M, \mu) \cdot \det(M, \mu') \quad \text{for } \mu, \mu' \in \text{Aut } M,$$

and also that

$$\det(M, \mu) = \det(L, \lambda) \det(N, v),$$

using the notation in (38.25) and (38.26). Both of these verifications are straightforward, and are left to the reader.

We now define a homomorphism

$$\theta: R^\times \rightarrow K_1(R), \quad \text{by} \quad u \mapsto [R, u_r], \quad u \in R^\times,$$

where  $u_r$  denotes right multiplication by  $u$  on  $R$ . Clearly,

$$\det [R, u_r] = u,$$

so the map  $\theta$  splits the surjection  $\det: K_1(R) \rightarrow R^\times$ . Therefore

$$(38.54) \quad K_1(R) \cong R^\times \times SK_1(R),$$

where  $SK_1(R) = \ker \theta$ . The notation  $SK_1$  is suggested by analogy with the notation  $SL$  for the special linear group.

As we shall see in (40.27), this same decomposition (38.54) holds for every commutative ring  $R$ . The computation of  $SK_1(R)$  is often difficult, however. We now state without proof the following basic theorem:

**(38.55) Bass-Milnor-Serre Theorem.** *Let  $R$  be a Dedekind domain whose quotient field  $F$  is any global field. Then  $SK_1(R) = 1$ , and there is an isomorphism*

$$\det: K_1(R) \cong R^\times.$$

For a proof, see Bass-Milnor-Serre [67] or Milnor [71].

### §38D. Localization Sequences

We have seen in (16.6) that when  $\Lambda$  is a left artinian ring, the Grothendieck group  $G_0(\Lambda)$  is a free  $\mathbb{Z}$ -module with basis  $[S_1], \dots, [S_n]$ , where the  $\{S_i\}$  are a basic set of simple left  $\Lambda$ -modules. The situation is much more complicated when  $\Lambda$  is a noetherian ring which is not artinian, and one method of calculating  $G_0(\Lambda)$  is to reduce the problem to easier cases, by means of a localization sequence. The basic ideas originated with Grothendieck and Gabriel, while the special cases occurring below are due to Swan and Heller-Reiner.

To begin with, let  $R$  be a commutative noetherian ring, and let  $\Lambda$  be an  $R$ -algebra which is f.g. as  $R$ -module. Since every left ideal of  $\Lambda$  is also an  $R$ -submodule of  $\Lambda$ , it follows at once that  $\Lambda$  is a noetherian ring. Now let  $S$  be any multiplicative subset of  $R$ , and let us form the ring of quotients  $R' = S^{-1}R$  (see §4A). Then  $R'$  is also a commutative noetherian ring, and by §4A (see also MO(3.8)),  $R'$  is flat as  $R$ -module (that is,  $R' \otimes_R *$  preserves exactness of sequences of  $R$ -modules). We now set

$$\Lambda' = R' \otimes_R \Lambda = S^{-1}\Lambda, \quad \text{and} \quad M' = S^{-1}M = R' \otimes_R M = \Lambda' \otimes_{\Lambda} M,$$

for any left  $\Lambda$ -module  $M$ . Then  $\Lambda'$  is an  $R'$ -algebra, f.g. as  $R'$ -module, and every  $\Lambda$ -module  $M$  gives rise to a  $\Lambda'$ -module  $M'$ . If  $M$  is f.g./ $\Lambda$ , then  $M'$  is f.g./ $\Lambda'$ .

Our first localization sequence relates the Grothendieck groups  $G_0(\Lambda)$  and  $G_0(\Lambda')$ . There is an additive homomorphism

$$\varphi: G_0(\Lambda) \rightarrow G_0(\Lambda'), \quad \text{given by } \varphi[M] = [M'],$$

for each f.g.  $\Lambda$ -module  $M$ , where  $M'$  is as above. To see that  $\varphi$  is well defined, we need only observe that for each ses  $0 \rightarrow M_1 \rightarrow M_2 \rightarrow M_3 \rightarrow 0$  of  $\Lambda$ -modules, the corresponding sequence of  $\Lambda'$ -modules  $0 \rightarrow M'_1 \rightarrow M'_2 \rightarrow M'_3 \rightarrow 0$  is also exact, since  $R'$  is  $R$ -flat. We now prove:

**(38.56) Localization Sequence (Swan [63]).** *There exists an exact sequence of additive groups*

$$(38.57) \quad G_0^t(\Lambda) \xrightarrow{\psi} G_0(\Lambda) \xrightarrow{\varphi} G_0(\Lambda') \rightarrow 0,$$

where  $G_0^t(\Lambda)$  is the Grothendieck group of the category of all f.g.  $S$ -torsion<sup>†</sup>  $\Lambda$ -modules, and where  $\psi$  is defined by  $\psi[L] = [L]$  for each such module  $L$ .

Furthermore, if  $R$  is a Dedekind domain,<sup>††</sup> then

$$(38.58) \quad G_0^t(\Lambda) \cong \coprod_{\substack{P \\ P \cap S \neq \emptyset}} G_0(\Lambda/P\Lambda),$$

where  $P$  ranges over all prime ideals of  $R$  such that  $P \cap S$  is nonempty.

*Proof.* Step 1. If  $L$  is any f.g.  $S$ -torsion  $\Lambda$ -module, then  $sL = 0$  for some  $s \in S$ . Therefore

$$\varphi\psi[L] = [R' \otimes_R L] = [s^{-1}R' \otimes_R sL] = 0,$$

so  $\varphi\psi = 0$ , and  $\text{im } \psi \subseteq \ker \varphi$ . Furthermore, the proof of (23.13) remains valid even when  $R$  is not a domain, and so  $\varphi$  is a surjection.

The homomorphism  $\varphi: G_0(\Lambda) \rightarrow G_0(\Lambda')$  induces a homomorphism (also denoted by  $\varphi$ )

$$\varphi: G_0(\Lambda)/\text{im } \psi \rightarrow G_0(\Lambda').$$

To prove the exactness of (38.57), we shall construct a map  $\rho: G_0(\Lambda') \rightarrow G_0(\Lambda)/\text{im } \psi$  for which both  $\rho\varphi$  and  $\varphi\rho$  are the identity maps. Given any  $\Lambda$ -module  $M$ , we shall denote  $R' \otimes_R M$  by  $R'M$ , for brevity. However, the map  $M \rightarrow R'M$  given by  $m \in M \mapsto 1 \otimes m \in R'M$  is not necessarily injective, so we should not identify  $M$  with its image  $1 \otimes M$  in  $M'$ .

<sup>†</sup>An  $S$ -torsion  $\Lambda$ -module  $X$  is one such that for each  $x \in X$ , we have  $sx = 0$  for some  $s \in S$ .

<sup>††</sup>In fact, (38.58) holds for rings of Krull dimension  $\leq 1$  (see p. 93).

We proceed to define

$$\rho: G_0(\Lambda') \rightarrow G_0(\Lambda)/\text{im } \psi,$$

as follows. Each f.g.  $\Lambda'$ -module  $X$  may be written as  $X = R'M$  for some f.g.  $\Lambda$ -module  $M$  contained in  $X$ , by the proof of (23.13). We set  $\rho[X] = [M] + \text{im } \psi$ , and must verify that  $\rho$  is a well-defined homomorphism. First, we claim that  $\rho[X]$  is independent of the choice of  $M$ . For if also  $X = R'N$ , we choose  $s \in S$  such that  $sM \subseteq N$ . Since  $[M] - [sM] = \psi[M/sM] \in \text{im } \psi$ , we may replace  $M$  by  $sM$  without affecting  $[X]$ . Changing notation, we may now assume that  $M \subseteq N \subseteq X$ , and  $R'M = R'N = X$ . Then  $R'(N/M) = 0$ . Setting  $T = N/M$ , we see that  $T$  is an  $S$ -torsion  $\Lambda$ -module, and  $[N] = [M] + [T]$  in  $G_0(\Lambda)$ . Thus  $[M]$  and  $[N]$  differ by an element in  $\text{im } \psi$ , and we have shown that  $\rho[X]$  is independent of the choice of  $M$ .

We must also prove that  $\rho$  preserves the defining relations of  $G_0(\Lambda')$ : that is, given any  $\Lambda'$ -exact sequence

$$0 \rightarrow X_1 \xrightarrow{f} X_2 \xrightarrow{g} X_3 \rightarrow 0,$$

we have  $\rho[X_2] = \rho[X_1] + \rho[X_3]$ . Let  $X_2 = R'M_2$  for some f.g.  $\Lambda$ -submodule  $M_2$  of  $X_2$ ; then  $X_3 = R'g(M_2)$ , so we have

$$\rho[X_2] = [M_2] + \text{im } \psi, \quad \rho[X_3] = [M_3] + \text{im } \psi,$$

where  $M_3 = g(M_2)$ . Defining  $M_1 = \{x \in X_1 : f(x) \in M_2\}$ , we obtain a  $\Lambda$ -exact sequence

$$0 \rightarrow M_1 \xrightarrow{f} M_2 \xrightarrow{g} M_3 \rightarrow 0.$$

Tensoring with  $R'$ , and using the fact that  $R'M_i = X_i$ ,  $i = 1, 2$ , we obtain the exact sequence

$$0 \rightarrow R'M_1 \xrightarrow{f} X_2 \xrightarrow{g} X_3 \rightarrow 0.$$

Therefore,  $X_1 = R'M_1$ , and so  $\rho[X_1] = [M_1] + \text{im } \psi$ . But  $[M_2] = [M_1] + [M_3]$  in  $G_0(\Lambda)$ , and therefore  $\rho[X_2] = \rho[X_1] + \rho[X_3]$ , as desired. This proves that  $\rho$  is a well-defined homomorphism from  $G_0(\Lambda')$  into  $G_0(\Lambda)/\text{im } \psi$ . It is clear that  $\varphi\rho[X] = [X]$  for each  $[X] \in G_0(\Lambda')$ .

Finally, let  $[M] \in G_0(\Lambda)$ , and set  $X = R' \otimes M = R'N$ , where  $N = 1 \otimes M \subseteq X$ . Then  $\varphi[M] = [X]$ , and  $\rho\varphi[M] = \rho[X] = N + \text{im } \psi$ . But there is a  $\Lambda$ -exact sequence

$$0 \rightarrow M_0 \rightarrow M \rightarrow N \rightarrow 0,$$

where  $M_0$  is the kernel of the map  $M \rightarrow N$ , that is,  $M_0$  is the  $S$ -torsion submodule of  $M$  (see §4A). Therefore  $[M] = [N] + [M_0]$ , and  $[M_0] \in \text{im } \psi$ , which proves that  $\rho\varphi[M] = [M] + \text{im } \psi$ . This completes the proof that  $G_0(\Lambda)/\text{im } \psi \cong G_0(\Lambda')$ , and establishes (38.57).

*Step 2.* In order to prove (38.58), let  $M$  be any f.g.  $\Lambda$ -module. We show that there is a filtration

$$(38.59) \quad M = M_n \supset M_{n-1} \supset \cdots \supset M_1 \supset M_0 = 0,$$

where each factor  $M_i/M_{i-1}$  is a cyclic  $\Lambda$ -module whose  $R$ -annihilator is a prime ideal of  $R$ . We first write  $M = \sum_{i=1}^r \Lambda m_i$ , and note that  $M$  has a filtration

$$M = \sum_{i=1}^r \Lambda m_i \supseteq \sum_{i=1}^{r-1} \Lambda m_i \supseteq \cdots \supseteq \Lambda m_1 \supseteq 0,$$

with cyclic factors. We wish to refine this filtration to obtain one of the desired type, and so it suffices to prove the result for cyclic  $\Lambda$ -modules. If the result is false, let  $X = \Lambda x$  be a nonzero counterexample for which the annihilator ideal  $\text{ann}_R X$  is as large as possible (among all counterexamples  $X$ ). Set  $I = \text{ann}_R X$ , a proper ideal of  $R$ . If  $I$  is a prime ideal of  $R$ , then  $X \supset 0$  is a filtration of  $X$  whose factor module  $X$  has prime annihilator  $I$ , contrary to assumption. Thus  $I$  is not prime, so there exist elements  $a, b \in R$  with  $ab \in I$ ,  $a \notin I$ ,  $b \notin I$ . In the filtration  $X \supset aX \supset 0$ , the factors are  $X/aX$  and  $aX$ . Since

$$\text{ann}_R X/aX \supseteq I + Ra \supset I, \quad \text{ann}_R aX \supseteq I + Rb \supset I,$$

neither  $X/aX$  nor  $aX$  can be a counterexample. Thus both of them have filtrations whose factor modules have prime ideal annihilators. The same is therefore true of  $X$ . This proves that no counterexamples exist, and shows that every f.g.  $\Lambda$ -module  $M$  has a filtration (38.59) for which, for each  $i$ ,

$$\text{ann}_R(M_i/M_{i-1}) = P_i = \text{prime ideal of } R, \quad 1 \leq i \leq n.$$

Now let  $M$  be a f.g.  $S$ -torsion  $\Lambda$ -module, and let (38.59) be a filtration as above. Since each factor  $M_i/M_{i-1}$  is an  $S$ -torsion module, it follows that  $P_i \cap S \neq \emptyset$  for each  $i$ . Clearly  $[M] = \Sigma[M_i/M_{i-1}]$  in  $G_0^t(\Lambda)$ , and the map

$$[M] \rightarrow \sum_{i=1}^n [M_i/M_{i-1}] \in \coprod_P G_0(\Lambda/P\Lambda)$$

gives the desired isomorphism (38.58). (Since  $R$  is Dedekind, the modules  $\{M_i/M_{i-1}\}$  are simple, and the proposed map is independent of the choice of the filtration, by the Jordan-Hölder Theorem. It also has to be checked that the map preserves the defining relations of  $G_0^t(\Lambda)$ ) This completes the proof of Theorem 38.56 (See also Exercise 38.17).

For the remainder of this section, let  $R$  be a Dedekind domain with quotient field  $K$ . We recall from §23 that an  $R$ -order is an  $R$ -algebra  $\Lambda$  which is f.g. and projective as  $R$ -module. For such an  $R$ -order  $\Lambda$ , we set  $A = K \otimes_R \Lambda$ . Since  $R$  is a domain and  $\Lambda$  is  $R$ -torsionfree, we may identify  $\Lambda$  with its image  $1 \otimes \Lambda$  in  $A$ . Then we may write  $A = K\Lambda$ , viewed as the algebra of  $K$ -linear combinations of the elements of the  $R$ -algebra  $\Lambda$ . Our aim here is to calculate the Grothendieck group  $G_0(\Lambda)$ , and for this purpose we shall extend the Localization Sequence 38.57 to the left, by means of an additional term  $K_1(A)$ , the Whitehead group of  $A$  defined in (38.28).

Let us first review some ideas from the theory of orders. For each  $R$ -module  $M$ , there is an  $R$ -homomorphism  $M \rightarrow K \otimes_R M$  given by  $m \mapsto 1 \otimes m$ ,  $m \in M$ , whose kernel is the  $R$ -torsion submodule of  $M$ . If  $M$  is  $R$ -torsionfree, this map is an embedding, and we identify  $M$  with its image  $1 \otimes M$  in  $K \otimes_R M$ ; the latter can then be written as  $KM$ .

As in §23, a  $\Lambda$ -lattice is a left  $\Lambda$ -module  $M$  which is f.g. and projective as  $R$ -module (or equivalently, f.g. and torsionfree as  $R$ -module). For each  $\Lambda$ -lattice  $M$ ,  $KM$  is an f.g.  $A$ -module; conversely, every f.g.  $A$ -module  $V$  contains  $\Lambda$ -lattices  $M$  for which  $KM = V$ , and we call  $M$  a full  $\Lambda$ -lattice in  $V$ .

Now let  $\Lambda$  be an  $R$ -order in an f.d.  $K$ -algebra  $A$ . Since  $K = S^{-1}R$ , where  $S$  is the multiplicative set  $R - \{0\}$ , the Localization Sequence 38.57 becomes

$$G_0^t(\Lambda) \xrightarrow{\psi} G_0(\Lambda) \xrightarrow{\varphi} G_0(A) \rightarrow 0.$$

Here,  $G_0^t(\Lambda)$  is the Grothendieck group of the category of f.g.  $R$ -torsion  $\Lambda$ -modules. By (38.58), we have

$$(38.60) \quad G_0^t(\Lambda) \cong \coprod_P G_0(\Lambda/P\Lambda),$$

where  $P$  ranges over all nonzero prime ideals of  $R$ .

We are now ready to give a longer localization sequence, due to Heller-Reiner [64], [65]:

**(38.61) Theorem.** *Let  $R$  be a Dedekind domain with quotient field  $K$ , and let  $\Lambda$  be an  $R$ -order in a f.d. semisimple  $K$ -algebra  $A$ . There is an exact sequence of groups*

$$(38.62) \quad K_1(A) \xrightarrow{\delta} G_0^t(\Lambda) \xrightarrow{\psi} G_0(\Lambda) \xrightarrow{\varphi} G_0(A) \rightarrow 0.$$

*Proof.* Step 1. The preceding discussion shows that we need only define the homomorphism  $\delta$ , and prove that  $\text{im } \delta = \ker \psi$ . As a preliminary step, we carry out some elementary manipulations with  $\Lambda$ -lattices. Let  $M$  and  $N$  be  $\Lambda$ -lattices for which  $KM = KN$ . Then  $M \cap N$  is a full  $\Lambda$ -lattice in  $KM$ , and  $M/(M \cap N)$  is an  $R$ -torsion  $\Lambda$ -module. We now define

$$[M//N] = [M/(M \cap N)] - [N/(M \cap N)] \in G_0^t(\Lambda).$$

If  $L$  is another  $\Lambda$ -lattice for which  $KL = KM$ , we show that

$$(38.63) \quad [L//M] + [M//N] = [L//N] \text{ in } G_0^t(\Lambda).$$

To see this, let  $T = L \cap M \cap N$ ; from the exact sequence

$$0 \rightarrow (M \cap N)/T \rightarrow M/T \rightarrow M/(M \cap N) \rightarrow 0,$$

and the corresponding ses with  $M$  and  $N$  interchanged, we obtain  $[M//N] = [M/T] - [N/T]$ . Corresponding formulas hold with  $M$  replaced by  $L$ , and so on, which gives (38.63) at once.

Next, suppose we are given a diagram of  $\Lambda$ -lattices

$$\begin{array}{ccccccc} 0 & \longrightarrow & L_1 & \xrightarrow{f_1} & M_1 & \xrightarrow{g_1} & N_1 \longrightarrow 0 \\ & & \downarrow \lambda & & \downarrow \mu & & \downarrow \nu \\ 0 & \longrightarrow & L_2 & \xrightarrow{f_2} & M_2 & \xrightarrow{g_2} & N_2 \longrightarrow 0, \end{array}$$

in which each row is exact, and where the dotted arrows denote  $A$ -isomorphisms  $KL_1 \cong KL_2$ , etc., which commute with the horizontal maps  $KL_1 \rightarrow KM_1$ , etc. As in the Snake Lemma, we find readily that there is an exact sequence of  $R$ -torsion  $\Lambda$ -modules:

$$0 \rightarrow \frac{L_2}{L_2 \cap \lambda L_1} \rightarrow \frac{M_2}{M_2 \cap \mu M_1} \rightarrow \frac{N_2}{N_2 \cap \nu N_1} \rightarrow 0.$$

Therefore we have

$$\left[ \frac{M_2}{M_2 \cap \mu M_1} \right] = \left[ \frac{L_2}{L_2 \cap \lambda L_1} \right] + \left[ \frac{N_2}{N_2 \cap \nu N_1} \right]$$

in  $G_0^t(\Lambda)$ . An analogous formula holds with the numerators  $M_2, L_2, N_2$  replaced by  $\mu M_1, \lambda L_1, \nu N_1$ , respectively. Using (38.63), we obtain

$$(38.64) \quad [M_2//\mu M_1] = [L_2//\lambda L_1] + [N_2//\nu N_1] \text{ in } G_0^t(\Lambda).$$

*Step 2.* We are now ready to construct a map  $\delta: K_1(A) \rightarrow G_0^t(\Lambda)$ . Since  $K_1(A)$  is generated by ordered pairs  $(X, \mu)$  with  $X \in \mathcal{P}(A)$  and  $\mu \in \text{Aut}_A X$ , we need to define  $\delta(X, \mu)$ , and to show that this definition preserves the defining relations of  $K_1(A)$ . Given an ordered pair  $(X, \mu)$ , choose any full  $\Lambda$ -lattice  $M$  in  $X$ , and set

$$\delta(X, \mu) = [M//\mu(M)] \in G_0^t(\Lambda).$$

If also  $X = KN$  for some  $\Lambda$ -lattice  $N$ , then by (38.62) we have

$$[M/\!/ \mu M] - [N/\!/ \mu N] = [M/\!/ N] - [\mu M/\!/ \mu N] \text{ in } G_0^r(\Lambda).$$

But  $\mu$  maps  $M$  isomorphically onto  $\mu M$ , and  $N$  onto  $\mu N$ , so  $[M/\!/ N] = [\mu M/\!/ \mu N]$  in  $G_0^r(\Lambda)$ . This readily implies that  $\delta(X, \mu)$  is independent of the choice of the full  $\Lambda$ -lattice  $M$  in  $X$ .

We show next that  $\delta$  is well-defined on  $K_1(A)$ . First, let  $X \in \mathcal{P}(A)$  and let  $\mu, \mu' \in \text{Aut}_A X$ . Choosing a full  $\Lambda$ -lattice  $M$  in  $X$ , we have

$$\begin{aligned} \delta(X, \mu\mu') &= [M/\!/ \mu\mu' M] = [M/\!/ \mu M] + [\mu M/\!/ \mu\mu' M] \\ &= [M/\!/ \mu M] + [M/\!/ \mu' M] = \delta(X, \mu) + \delta(X, \mu'). \end{aligned}$$

Next, consider an exact sequence of ordered pairs (see (38.25)):

$$0 \rightarrow (X_1, \lambda) \rightarrow (X_2, \mu) \rightarrow (X_3, \nu) \rightarrow 0.$$

Let  $L, M, N$  be full  $\Lambda$ -lattices in  $X_1, X_2$ , and  $X_3$ , respectively. Then (38.64) is precisely the assertion that

$$\delta(X_2, \mu) = \delta(X_1, \lambda) + \delta(X_3, \nu).$$

This completes the proof that  $\delta$  is well defined on  $K_1(A)$ , and we write  $\delta[X, \mu]$  instead of  $\delta(X, \mu)$  hereafter.

*Step 3.* It remains for us to prove that  $\text{im } \delta = \ker \psi$  in the sequence (38.62). For  $[X, \mu] \in K_1(A)$ , let  $X = KM$  for some  $\Lambda$ -lattice  $M$ . Then

$$\begin{aligned} \psi \delta[X, \mu] &= \psi[M/\!/ \mu M] = \{[M] - [M \cap \mu M]\} - \{[\mu M] - [M \cap \mu M]\} \\ &= [M] - [\mu M] = 0, \end{aligned} \quad .$$

since  $\mu M \cong M$ . Therefore,  $\text{im } \delta \subseteq \ker \psi$ .

To prove the reverse inclusion, let  $\xi = [T_1] - [T_2] \in \ker \psi$ , where  $T_1$  and  $T_2$  are f.g.  $S$ -torsion  $\Lambda$ -modules. Choose  $\Lambda$ -exact sequences

$$0 \rightarrow L_i \rightarrow M_i \rightarrow T_i \rightarrow 0, \quad i = 1, 2,$$

with  $L_i$  and  $M_i$   $\Lambda$ -lattices; then  $\psi[T_i] = [M_i] - [L_i] \in G_0(\Lambda)$ . Therefore,

$$0 = \psi(\xi) = [M_1] - [L_1] - [M_2] + [L_2] \text{ in } G_0(\Lambda),$$

and so

$$[L_1 \oplus M_2] = [L_2 \oplus M_1] \text{ in } G_0(\Lambda).$$

Using the isomorphism  $G_0(\Lambda) \cong G_0^R(\Lambda)$  established in (38.42), and the analogue

of (38.20) for  $G_0^R(\Lambda)$ , it follows that there exist  $\Lambda$ -lattices  $U, V, W$ , and a pair of ses's:

$$0 \rightarrow U \rightarrow L_1 \oplus M_2 \oplus V \rightarrow W \rightarrow 0, \quad 0 \rightarrow U \rightarrow L_2 \oplus M_1 \oplus V \rightarrow W \rightarrow 0.$$

Applying  $K \otimes_R *$  to both of these, we obtain a pair of ses's of  $A$ -modules. These sequences are split since  $A$  is semisimple. Therefore, we can find an  $A$ -isomorphism

$$\mu: K(L_1 \oplus M_2 \oplus V) \cong K(L_2 \oplus M_1 \oplus V)$$

which yields the identity map on both  $KU$  and  $KW$ . Applying (38.64), it follows that

$$(38.65) \quad [(L_2 \oplus M_1 \oplus V) // \mu(L_1 \oplus M_2 \oplus V)] = 0 \text{ in } G_0^t(\Lambda).$$

On the other hand, from (38.63) we obtain (in  $G_0^t(\Lambda)$ ):

$$\xi = [T_1] - [T_2] = [M_1/L_1] - [M_2/L_2] = [(M_1 \oplus L_2 \oplus V) // (M_2 \oplus L_1 \oplus V)].$$

Using (38.65), we then have

$$\begin{aligned} \xi &= [(M_1 \oplus L_2 \oplus V) // (M_2 \oplus L_1 \oplus V)] - [(M_1 \oplus L_2 \oplus V) // \mu(M_2 \oplus L_1 \oplus V)] \\ &= -[(M_2 \oplus L_1 \oplus V) // \mu(M_2 \oplus L_1 \oplus V)] \in \text{im } \delta. \end{aligned}$$

This completes the proof that  $\text{im } \delta = \ker \psi$ , and establishes the theorem.

Since  $A$  is an artinian ring,  $G_0(A)$  is a free  $\mathbb{Z}$ -module with  $\mathbb{Z}$ -basis  $\{[S_1], \dots, [S_n]\}$ , where the  $\{S_i\}$  are a basic set of simple left  $A$ -modules. Since  $G_0(A)$  is  $\mathbb{Z}$ -free, the sequence (38.62) is  $\mathbb{Z}$ -split, and therefore,

$$(38.66) \quad G_0(\Lambda) \cong G_0(A) \oplus \text{cok } \delta, \quad \text{where } \text{cok } \delta = G_0^t(\Lambda) / \text{im } \delta.$$

Thus, the problem of determining the additive group  $G_0(\Lambda)$  is reduced to the calculation of  $G_0^t(\Lambda) / \text{im } \delta$ . This is a much simpler problem, which we shall treat in detail in §39. As a preliminary step, we now discuss an important special case:

**(38.67) Theorem.** *Let  $R$  be a Dedekind domain whose quotient field  $K$  is a global field. Let  $A$  be a central simple  $K$ -algebra, and let  $\Lambda$  be a maximal  $R$ -order in  $A$ . Then*

$$G_0(\Lambda) \cong \mathbb{Z} \oplus \text{Cl}_A R, \quad \text{where } \text{Cl}_A R = I(R)/P_A(R).$$

Here,  $I(R)$  denotes the group of fractional  $R$ -ideals in  $K$ , and  $P_A(R)$  is the subgroup

of  $I(R)$  consisting of all principal ideals  $\{R\alpha : \alpha \in K^+\}$ , where\*

$$K^+ = \{\alpha \in K : \alpha_P > 0 \text{ at every infinite real prime } P \text{ of } K \text{ at which } A \text{ is ramified}\}.$$

*Proof.* There is only one isomorphism class of simple left  $A$ -modules in this case, since  $A$  is a simple artinian ring, and therefore  $G_0(A) \cong \mathbb{Z}$ . Thus, it suffices to show that  $\text{cok } \delta \cong \text{Cl}_A R$ , and we begin by establishing an isomorphism

$$(38.68) \quad \tau: G'_0(\Lambda) \cong I(R).$$

To define  $\tau$ , let  $X$  be any f.g.  $R$ -torsion  $\Lambda$ -module. Then  $\alpha X = 0$  for some nonzero  $\alpha \in R$ , so  $X$  is a f.g. module over the ring  $\Lambda/\alpha\Lambda$ ; this ring is artinian and noetherian, and therefore so is  $X$ . This shows that the  $\Lambda$ -module  $X$  has a composition series. Let the composition factors be  $\{X_1, \dots, X_n\}$ . We now define

$$\tau[X] = \prod_{i=1}^n \text{ann}_R(X_i) \in I(R).$$

Since  $\tau$  is multiplicative on ses's of f.g.  $R$ -torsion  $\Lambda$ -modules, it follows that  $\tau$  is a well-defined homomorphism from  $G'_0(\Lambda)$  into  $I(R)$ .

The theorem is trivially true when  $R = K$ , so we exclude this case for the remainder of the proof. Let  $P$  range over the maximal ideals of  $R$ ; by (38.60),

$$G'_0(\Lambda) \cong \coprod_P G_0(\Lambda/P\Lambda).$$

For each  $[X] \in G'_0(\Lambda)$ , its image in  $G_0(\Lambda/P\Lambda)$  is precisely  $\sum_i [X_i]$ , the sum extending over all  $\Lambda$ -composition factors  $\{X_i\}$  of  $X$  for which  $PX_i = 0$ . (This follows readily from Step 2 of the proof of (38.56).) On the other hand,  $I(R)$  is the free abelian group generated by the set of all maximal ideals  $P$  of  $R$ . Thus, to prove (38.68) it suffices to show that  $\tau$  gives rise to an isomorphism

$$\tau_P: G_0(\Lambda/P\Lambda) \cong \langle P \rangle \quad \text{for each } P,$$

where  $\langle P \rangle$  is the infinite cyclic subgroup of  $I(R)$  generated by  $P$ .

Let  $\Lambda_P$  denote the localization of  $\Lambda$  at  $P$ . Then

$$\Lambda/P\Lambda \cong \Lambda_P/P\Lambda_P,$$

and by (5.22) we have

$$(\Lambda_P/P\Lambda_P)/\text{rad}(\Lambda_P/P\Lambda_P) \cong \Lambda_P/\text{rad} \Lambda_P.$$

The right-hand expression is a simple artinian ring, since  $\Lambda_P$  is a maximal

\*see (7.47).

$R$ -order in a central simple  $K$ -algebra (see (26.24ii)). Therefore, the artinian ring  $\Lambda/P\Lambda$  has a simple left module, unique up to isomorphism, which we denote temporarily by  $S(P)$ . It now follows that  $G_0(\Lambda/P\Lambda)$  is a free  $\mathbb{Z}$ -module with a single basis element  $[S(P)]$ . Furthermore, by (26.24ii) we have

$$\text{ann}_R S(P) = P.$$

This shows that  $\tau_P[S(P)] = P$ , so  $\tau_P: G_0(\Lambda/P\Lambda) \cong \langle P \rangle$  as desired, and we have completed the proof of (38.68).

Now let  $a \in \Lambda \cap A^\circ$ ; then  $\Lambda/\Lambda a$  is an  $R$ -torsion  $\Lambda$ -module, and we need to know the ideal  $\tau(\Lambda/\Lambda a)$  in  $R$ . However, by [MO, (24.14)], the product of the  $R$ -annihilators of the  $\Lambda$ -composition factors of  $\Lambda/\Lambda a$  is precisely the principal ideal  $R \cdot \text{nr}(a)$ , where  $\text{nr}$  is the reduced norm map  $\text{nr}_{A/K}$  from  $A$  to  $K$  (see §7D). Thus

$$\tau(\Lambda/\Lambda a) = R \cdot \text{nr}(a), \quad a \in \Lambda \cap A^\circ.$$

Using the isomorphism (38.68), we have

$$\text{cok } \delta = G_0^r(\Lambda)/\text{im } \delta \cong I(R)/\text{im } \tau\delta,$$

so to complete the proof of the theorem, we need only establish that  $\text{im } \tau\delta = P_A(R)$ , where  $P_A(R)$  is the subgroup of  $I(R)$  defined in the statement of the theorem.

By Exercise 38.14, each element of  $K_1(A)$  can be written as  $[A, a_r]$  for some  $a \in A^\circ$ , where  $a_r$  denotes right multiplication on  $A$  by  $a$ . Each  $a \in A^\circ$  is expressible as a quotient  $a = bc^{-1}$ , with  $b, c \in \Lambda \cap A^\circ$  (indeed, we can choose  $c \in R$  if desired), and therefore  $\tau\delta(K_1(A))$  is the multiplicative subgroup of  $I(R)$  generated by

$$\{\tau\delta[A, a_r] : a \in \Lambda \cap A^\circ\}.$$

In order to calculate  $\delta[A, a_r]$ , we must choose a full  $\Lambda$ -lattice  $M$  in  $A$ , and then  $\delta[A, a_r] = [M//Ma] \in G_0^r(\Lambda)$ . Choosing  $M = \Lambda$ , we obtain

$$\tau\delta[A, a_r] = \tau[\Lambda/\Lambda a] = R \cdot \text{nr}(a).$$

Thus

$$\text{im } \tau\delta = \langle \{R \cdot \text{nr}(a) : a \in \Lambda \cap A^\circ\} \rangle = \{R \cdot \text{nr}(x) : x \in A^\circ\}.$$

But by the Hasse-Schilling-Maass Norm Theorem 7.48,

$$\{\text{nr}(x) : x \in A^\circ\} = K^+.$$

This proves that  $\text{im } \tau\delta = P_A(R)$ , as claimed, and the theorem is established.

**(38.69) Remarks.** (i) By (38.42), we have  $G_0(\Lambda) \cong G_0^R(\Lambda)$ . Since  $\Lambda$  is a maximal  $R$ -order, every  $\Lambda$ -lattice is  $\Lambda$ -projective. Therefore  $G_0^R(\Lambda) = K_0(\Lambda)$ , so from

Theorem 38.67 we obtain

$$K_0(\Lambda) \cong \mathbb{Z} \oplus \text{Cl}_A R.$$

This result was proved in a somewhat different fashion by Swan [62].

(ii) For any global field  $K$ , and any central simple  $K$ -algebra  $A = M_n(D)$ , where  $D$  is a division algebra with center  $K$ , there are isomorphisms

$$K_1(A) \cong K_1(D) \cong D^\# \cong \text{nr}(D^\circ) \cong K^+.$$

On the other hand, every element of  $K_1(A)$  is of the form  $[A, a_r]$  with  $a \in A^\circ$ . Further,

$$[A, a_r] + [A, b_r] = [A, (ab)_r] \quad \text{for } a, b \in A^\circ,$$

so there is a surjective homomorphism

$$A^\circ \rightarrow K_1(A), \quad \text{given by } a \mapsto [A, a_r], \quad a \in A^\circ.$$

Since  $K_1(A)$  is commutative, this yields a surjection

$$A^\circ/[A^\circ, A^\circ] \rightarrow K_1(A).$$

However,  $\text{nr}_{A/K}(A^\circ) = \text{nr}_{D/K}(D^\circ)$ , and there is a commutative diagram

$$\begin{array}{ccc} A^\circ/[A^\circ, A^\circ] & \xrightarrow{\quad} & K_1(A) \\ \downarrow & & \downarrow \\ \text{nr}_{A/K}(A^\circ) & \longrightarrow & \text{nr}_{D/K}(D^\circ). \end{array}$$

Both vertical arrows are isomorphisms, by the Wang-Platonov Theorem, and so we obtain

$$K_1(A) \cong A^\circ/[A^\circ, A^\circ].$$

(The result need not hold for arbitrary central simple algebras. For instance, if  $A = M_2(F)$ ,  $F = \mathbb{Z}/2\mathbb{Z}$ , then  $K_1(A) \cong F^\circ$  while  $A^\circ/[A^\circ, A^\circ]$  has order 3.)

## §38. Exercises

1. Calculate  $K_0(F)$  for  $F$  a field, skewfield, or local ring. What can be said about  $G_0(F)$  in the first two cases? Calculate  $G_0(R)$  for  $R$  a local left regular ring.
2. Show that each ring homomorphism  $\varphi: A \rightarrow B$  induces an additive homomorphism  $K_i(A) \rightarrow K_i(B)$ ,  $i = 0, 1$ . Further, if  $B$  is a flat right  $A$ -module (via  $\varphi$ ), there are homomorphisms  $G_i(A) \rightarrow G_i(B)$ ,  $i = 0, 1$ .

3. Verify the assertions in (38.10).
4. Show that Morita equivalent rings have the same  $K_0$  and the same  $G_0$ . Does this also hold for  $K_1$  and  $G_1$ ?
5. Let  $N$  be a nilpotent two-sided ideal of a left noetherian ring  $A$ . Prove that there is an isomorphism  $\theta: G_0(A/N) \cong G_0(A)$ , given by  $\theta[X] = [X]$  for each f.g.  $(A/N)$ -module  $X$ .

[Hint: Define an inverse  $\psi: G_0(A) \rightarrow G_0(A/N)$  by setting

$$\psi[Y] = \sum_i [N^{i-1}Y/N^iY]$$

for each f.g.  $A$ -module  $Y$ . To show that  $\psi$  is well defined, it suffices to show that for  $X$  any  $A$ -submodule of  $Y$ , we have

$$(*) \quad \sum [N^{i-1}Y/N^iY] = \sum \{[N^{i-1}X/N^iX] + [N^{i-1}(Y/X)/N^i(Y/X)]\}$$

in  $G_0(A/N)$ . By Zassenhaus's Lemma, the finite chains

$$Y \supseteq X \supseteq 0, \quad Y \supseteq NY \supseteq N^2Y \supseteq \cdots \supseteq N^kY = 0$$

have equivalent refinements. Thus there exists a chain of  $\Lambda$ -modules

$$Y = Y_0 \supseteq Y_1 \supseteq \cdots \supseteq Y_s = 0$$

with some  $Y_m = X$ , and with  $N(Y_{j-1}/Y_j) = 0$  for each  $i$ . But in  $G_0(\Lambda/N)$ , both sides of formula  $(*)$  are equal to  $\sum [Y_{j-1}/Y_j]$ .

6. Prove that  $G_0(A) \cong G_0(A/\text{rad } A) \cong K_0(A)$  for every left artinian ring  $A$ .
7. Suppose that  $\Lambda$  is either a left artinian ring, or an  $R$ -algebra f.g./ $R$  as  $R$ -module, where  $R$  is a complete noetherian local ring. Let  $N$  be a two-sided ideal of  $\Lambda$  contained in  $\text{rad } \Lambda$ , and set  $\bar{\Lambda} = \Lambda/N$ . Show that there is an isomorphism

$$K_0(\Lambda) \cong K_0(\bar{\Lambda}), \quad \text{given by } [X] \rightarrow [X/NX]$$

for each  $X \in \mathcal{P}(\Lambda)$ . Show further that  $K_0(\bar{\Lambda}) \cong G_0(\bar{\Lambda})$  when  $N = \text{rad } \Lambda$ .

8. Prove that for an arbitrary ring  $A$ , each  $x \in K_0(A)$  is of the form  $x = [A^{(n)}] - [X]$  for some  $n$  and some  $X \in \mathcal{P}(A)$ .
9. Let  $A$  be an arbitrary ring,  $M$  a left  $A$ -module, and  $E = \text{End}_A M$ , where  $E$  acts from the right on  $M$ . Let  $\mathcal{C}$  be the category of  $A$ -direct summands of  $M^{(k)}$ ,  $k = 1, 2, \dots$ , and let  $K_0(\mathcal{C}, \oplus)$  be the additive group generated by symbols  $(X)$ ,  $X \in \mathcal{C}$ , with relations  $(X \oplus X') = (X) + (X')$  for  $X, X' \in \mathcal{C}$ . Prove that

$$K_0(\mathcal{C}, \oplus) \cong K_0(E).$$

[Hint: Use (6.3). The desired isomorphism is given by

$[N] \rightarrow [\text{Hom}_A(A M_E, A N)]$  for  $N \in \mathcal{C}.$

10. Keep the hypotheses of (38.42), and let

$$0 \rightarrow L \rightarrow M \rightarrow X \rightarrow 0$$

be an exact sequence of f.g.  $\Lambda$ -modules, where  $L$  and  $M$  are  $\Lambda$ -lattices. Prove that the isomorphism  $G_0(\Lambda) \cong G_0^R(\Lambda)$  maps  $[X]$  onto  $[M] - [L]$ .

11. Let  $A$  be an arbitrary ring, and let  $0 \rightarrow L \rightarrow M \rightarrow N \rightarrow 0$  be an exact sequence of  $A$ -modules. Prove that

$$\begin{aligned} \text{hd } M &\leq \text{Max}(\text{hd } L, \text{hd } N), \quad \text{hd } L \leq \text{Max}(\text{hd } M, \text{hd } N), \\ \text{hd } N &\leq \text{Max}(\text{hd } L, 1 + \text{hd } M). \end{aligned}$$

[Hint: Use (38.37) or (8.6).]

12. Let  $G$  be a finite group, and let  $M$  be any f.g. left  $\mathbb{Z}G$ -module of finite homological dimension. Prove that  $\text{hd}(M) \leq 1$  always, and that  $\text{hd}(M) = 0$  if  $M$  is a  $\mathbb{Z}G$ -lattice.

[Hint (S. Chase): Suppose  $\text{hd}(M) = n > 1$ , and consider a projective resolution

$$0 \rightarrow P_n \rightarrow P_{n-1} \rightarrow \cdots \rightarrow P_1 \rightarrow P_0 \rightarrow M \rightarrow 0$$

with each  $P_i \in \mathcal{P}(\mathbb{Z}G)$ . As in the proof of (38.36), the above sequence may be broken up into a collection of ses's:

$$0 \rightarrow L_0 \rightarrow P_0 \rightarrow M \rightarrow 0, \quad 0 \rightarrow L_1 \rightarrow P_1 \rightarrow L_0 \rightarrow 0, \dots, 0 \rightarrow P_n \rightarrow P_{n-1} \rightarrow L_{n-2} \rightarrow 0.$$

By Exercise 10.25, each of these sequences (except the first one) is  $\mathbb{Z}G$ -split. Thus  $L_0 \in \mathcal{P}(\mathbb{Z}G)$ , so  $\text{hd}(M) \leq 1$ . If  $M$  is a  $\mathbb{Z}G$ -lattice, then the sequence  $0 \rightarrow L_0 \rightarrow P_0 \rightarrow M \rightarrow 0$  is  $\mathbb{Z}G$ -split, so  $M \in \mathcal{P}(\mathbb{Z}G)$ .]

13. Let  $G$  be a finite group,  $G \neq \{1\}$ . Prove that the global dimension of  $\mathbb{Z}G$  must be infinite.

[Hint: If not, then  $\text{hd}_{\mathbb{Z}G}(\mathbb{Z}) = 0$ , where  $G$  acts trivially on  $\mathbb{Z}$ . But then  $\mathbb{Z}$  is  $\mathbb{Z}G$ -projective, which is impossible.]

14. Let  $A$  be a semisimple ring. Show that every element of  $K_1(A)$  is of the form  $[A, a_r]$ , where  $a_r$  is right multiplication on  $A$  by an element  $a \in A^\times$ .

[Hint: It suffices to treat the case where  $A$  is a simple artinian ring, say  $A = \text{End}_D V$ , as in the discussion following (38.30). By (38.32), each element of  $K_1(D)$  is of the form  $[D, d_r]$  for some  $d \in D^\times$ . Under the isomorphism (38.30), its image in  $K_1(A)$  is  $[V, \alpha]$  for some  $\alpha \in \text{Aut}_A V$ . Choose an  $A$ -module  $V'$  with  $V \oplus V' \cong A$ ; then in  $K_1(A)$ ,

$$[V, \alpha] = [V \oplus V', \alpha \oplus 1] = [A, a_r]$$

for some  $a \in A^\times$ .]

15. Let  $D$  be a skewfield. Calculate the Dieudonné determinant of the matrix  $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(D)$ .

(Hint: Treat separately the cases  $a \neq 0$  and  $a = 0$ .)

16. Is it true that a homomorphic image of a left regular ring must also be left regular?

17. Prove the following generalization of the Localization Sequence (38.56): *Let  $\Lambda$  be a left noetherian ring, and let  $S$  be any multiplicative subset of the center of  $\Lambda$ . Then (38.57) is an exact sequence, where now  $\Lambda' = S^{-1}\Lambda$ .*

### §39. GROTHENDIECK GROUPS OF INTEGRAL GROUP RINGS

Throughout this section, let  $\Lambda = RG$ ,  $A = KG$ , where  $G$  is a finite group of order  $n$ , and  $R$  is a Dedekind domain with quotient field  $K$ . We shall determine the additive structure of the Grothendieck group  $G_0(\Lambda)$  explicitly (see Definition 16.5). We begin by listing the key ideas underlying this computation.

- (39.1) A *hyper-elementary* group is a semidirect product  $C \rtimes H$  of a cyclic  $p'$ -group  $C$  and a  $p$ -group  $H$ , for some prime  $p$ . Let  $\mathcal{H}$  be the set of all hyper-elementary subgroups of a given group  $G$ . Solomon's Induction Theorem 15.10 gives<sup>†</sup>

$$G_0(QG) = \sum_{H \in \mathcal{H}} \text{ind}_H^G G_0(QH).$$

- (39.2) The Grothendieck group  $G_0^R(\Lambda)$ , associated with the category of left  $\Lambda$ -lattices, is a commutative ring with identity. Multiplication is defined by

$$[M][N] = [M \otimes_R N] \quad \text{for } \Lambda\text{-lattice } M \text{ and } N,$$

where  $M \otimes_R N$  is the inner tensor product of  $M$  and  $N$ . Since in this case  $R$  is a commutative regular ring, then by (38.42) there is an additive isomorphism

$$G_0^R(\Lambda) \cong G_0(\Lambda).$$

- (39.3) Let  $\bar{R} = R/P$ , where  $P$  is a maximal ideal of  $R$ . By (16.16), there is a commutative diagram

$$\begin{array}{ccc} G_0^R(RG) & \xrightarrow{\varphi} & G_0(KG) \\ \gamma \downarrow & & \nearrow \gamma' \\ G_0(\bar{R}G) & & \end{array}$$

\*See also the Witt-Berman Induction Theorem 21.6.

in which  $\varphi$  and  $\gamma$  are ring homomorphisms defined by change of ground ring, while  $\gamma'$  is the ring homomorphism given by the decomposition map.

(39.4) There is an exact sequence of groups (see (38.61) and (38.58))

$$K_1(A) \xrightarrow{\delta} \coprod_P G_0(\Lambda/P\Lambda) \xrightarrow{\psi} G_0^R(\Lambda) \xrightarrow{\varphi} G_0(A) \rightarrow 0,$$

where  $P$  ranges over all nonzero maximal ideals of  $R$ .

(39.5) Assume that  $\text{char } K = 0$ , and that each rational prime divisor of  $n$  is a nonunit in  $R$ . Then by Swan's Theorem 32.11, for each projective  $\Lambda$ -lattice  $M$ , we have

$$KM \cong A^{(r)}, \quad M_P \cong \Lambda_P^{(r)}, \quad M/PM \cong ((R/P)G)^{(r)}$$

for some  $r$ . Here,  $P$  can be any maximal ideal of  $R$ , and the subscript  $P$  indicates localization at  $P$ .

These facts will be used in §39A, together with the techniques of Frobenius functors (see §38A), to obtain Swan's refinement of the localization sequence (39.4). The key step is the proof that  $\varphi$  is an isomorphism whenever  $R$  is semilocal (that is,  $R$  has finitely many maximal ideals). Another interesting point in §39A is the introduction of the locally free class group  $\text{Cl } \Lambda$  (see (39.12)), which is used to study the kernel of the map  $\varphi$  in (39.4).

If §39B, we shall prove the Heller-Reiner formula for the additive structure of  $G_0(\Lambda)$ . We shall then apply this formula to the case of cyclic and abelian groups, to obtain some results of Lenstra [81].

### §39A. Localization Sequences

As in the preceding introduction, let  $G$  be a finite group, and let  $\Lambda = RG$ ,  $A = KG$ , where  $R$  is a Dedekind domain with quotient field  $K$ . Let  $H$  be a subgroup of  $G$ , and denote by  $\text{res}_H^G$ ,  $\text{ind}_H^G$  the restriction and induction maps defined in §38A:

$$\begin{aligned} \text{res}_H^G: G_0(RG) &\rightarrow G_0(RH), & G_0^R(RG) &\rightarrow G_0^R(RH), \\ \text{ind}_H^G: G_0(RH) &\rightarrow G_0(RG), & G_0^R(RH) &\rightarrow G_0^R(RG). \end{aligned}$$

Note that  $G_0^R(RG)$  is a commutative ring with identity element  $[R]$ , where  $G$  acts trivially on  $R$ . The map  $G_0^R(RG) \rightarrow G_0(RG)$  identifies the ring  $G_0^R(RG)$  with the additive group  $G_0(RG)$ . If  $X$  is some ideal of  $G_0^R(RG)$ , and  $m \in \mathbb{Z}$ , we write  $m \cdot [R] \in X$  to indicate that  $m \cdot [R] \in X$ . Equivalently, this means that  $m$  annihilates the additive group  $G_0^R(RG)/X$ .

We shall be using properties of the Frobenius functor  $G_0^R$  established in §38A. Given any homomorphism  $R \rightarrow S$ , where  $S$  is a commutative ring, there is a

“change of ground ring” map

$$G_0^R(RG) \rightarrow G_0^S(SG),$$

which commutes with restriction and induction maps, and is a ring homomorphism.

Letting  $\mathcal{C}$  denote some collection of subgroups of  $G$ , we have defined

$$G_0(RG)_{\mathcal{C}} = \sum_{H \in \mathcal{C}} \text{ind}_H^G G_0(RH).$$

We are now ready to prove

**(39.6) Lemma** (Swan [60]). *Let  $\mathcal{C}$  be any collection of subgroups of  $G$ , and let  $m$  be a positive integer such that  $m \in G_0(KG)_{\mathcal{C}}$ . Then*

$$m^2 \in G_0(RG)_{\mathcal{C}}, \quad m \in G_0((R/P)G)_{\mathcal{C}},$$

for each maximal ideal  $P$  of  $R$ .

*Proof.* Let  $\bar{R} = R/P$ , where  $P$  is a maximal ideal of  $R$ . Let  $\gamma$  and  $\gamma'$  be the maps occurring in (39.3). Since induction commutes with change of ground ring, we have

$$\gamma\{G_0(RG)_{\mathcal{C}}\} \subseteq G_0(\bar{R}G)_{\mathcal{C}}, \quad \gamma'\{G_0(KG)_{\mathcal{C}}\} \subseteq G_0(\bar{R}G)_{\mathcal{C}}.$$

Since  $\gamma'$  is a ring homomorphism, it follows that  $m \in G_0(\bar{R}G)_{\mathcal{C}}$ , as desired.

Next, the map  $\varphi: G_0^R(RG)_{\mathcal{C}} \rightarrow G_0(KG)_{\mathcal{C}}$  is surjective, since the corresponding map  $G_0^R(RH) \rightarrow G_0(KH)$  is surjective for each  $H \in \mathcal{C}$ . We may therefore choose  $x \in G_0^R(RG)_{\mathcal{C}}$  with  $\varphi(x) = m$ . Then  $\varphi(x - m) = 0$ , so by (39.4),

$$x - m = \psi(y) \quad \text{for some } y \in \coprod_P G_0(\Lambda/P\Lambda).$$

But  $my \in \coprod_P G_0(\Lambda/P\Lambda)_{\mathcal{C}}$  by (38.1iv) and the first part of this proof, since  $\Lambda/P\Lambda = (R/P)G$ . Therefore

$$mx - m^2 = \psi(my) \in G_0^R(RG)_{\mathcal{C}}.$$

Since  $mx$  lies in  $G_0^R(RG)_{\mathcal{C}}$ , so does  $m^2$ , and we are done.

We apply this to obtain:

**(39.7) Theorem** (Swan [60]). *Letting  $\mathcal{H}$  denote the set of all hyperelementary subgroups of  $G$ , we have*

$$(39.8) \quad G_0^R(RG) = G_0^R(RG)_{\mathcal{H}} = \sum_{H \in \mathcal{H}} \text{ind}_H^G G_0^R(RH).$$

*Proof.* Since  $1 \in G_0(QG)_{\mathcal{H}}$  by (39.1), we have by (39.6)

$$1 \in G_0^Z(ZG)_{\mathcal{H}}, \quad 1 \in G_0((Z/pZ)G)_{\mathcal{H}}$$

for each rational prime  $p$ . If  $\text{char } R = 0$ , the ring homomorphism  $Z \rightarrow R$  induces a homomorphism  $G_0^Z(ZG)_{\mathcal{H}} \rightarrow G_0^R(RG)_{\mathcal{H}}$ , so the latter group contains 1. If  $\text{char } R = p > 0$ , there is a ring homomorphism  $Z/pZ \rightarrow R$ , and so  $1 \in G_0^R(RG)_{\mathcal{H}}$  once more. Now use (38.13i) to finish the proof.

The above theorem, which depends on the Solomon Induction Theorem and the theory of Frobenius functors, will be vital for our later discussion. It will permit us to prove various identities by reducing the problem to the case of hyper-elementary groups. As a first step in this direction, we prove

**(39.9) Corollary.** *Suppose that for each hyper-elementary subgroup  $H$  of  $G$ , the change of ground ring map*

$$\varphi_H: G_0^R(RH) \rightarrow G_0(KH)$$

*is an isomorphism. Then we have an isomorphism*

$$\varphi_G: G_0^R(RG) \cong G_0(KG).$$

*Proof.* By (39.4),  $\varphi_G$  is surjective. To prove  $\varphi_G$  injective, let  $\varphi_G(x) = 0$ . Since  $\text{res}_H^G$  commutes with the change of ground ring map  $\varphi_G$ , and since  $\varphi_H$  is injective for each  $H \in \mathcal{H}$ , it follows that  $\text{res}_H^G(x) = 0$  for each  $H \in \mathcal{H}$ . But then (38.13) shows that  $x = 0$ , as desired.

A Dedekind domain  $R$  is called *semilocal* if  $R$  has only finitely many maximal ideals. (For example, the localization  $R_P$  of  $R$  at a maximal ideal  $P$  is a local ring, and is thus automatically semilocal as well.) We are now ready to prove the following remarkable theorem due to Swan [63], which will be the key to the global situation:

**(39.10) Theorem.** *For each semilocal Dedekind domain  $R$ , the change of ground ring map gives an isomorphism of rings*

$$\varphi: G_0^R(RG) \cong G_0(KG).$$

*Proof.* We need only show that  $\varphi$  is injective, since we already know that  $\varphi$  is surjective by (39.4). It suffices by (39.4) to show that  $\psi(G_0((R/P)G)) = 0$  for each nonzero maximal ideal  $P$  of  $R$ . To avoid trivialities, assume  $R \neq K$ .

Suppose first that  $P \neq n$ , where  $n = |G|$ . Then  $\text{char } K \neq n$ , so  $KG$  is a separable  $K$ -algebra by Maschke's Theorem. Let  $X$  be any f.g.  $(\Lambda/P\Lambda)$ -module. Then there exists a  $\Lambda$ -exact sequence

$$0 \rightarrow M \rightarrow N \rightarrow X \rightarrow 0$$

in which  $M$  and  $N$  are  $\Lambda$ -lattices, and so  $\psi[X] = [N] - [M]$ . Since  $\text{ann}_R X = P$ , we have  $X_Q = 0$  for each maximal ideal  $Q$  of  $R$  distinct from  $P$ . Therefore  $M_Q \cong N_Q$  for  $Q$  dividing  $n$ , so  $M$  and  $N$  are in the same genus by (31.2). But then  $M_Q \cong N_Q$  for every maximal ideal  $Q$  of  $R$ , and therefore by (31.15)  $M \cong N$  since  $R$  is semilocal. Thus  $\psi[X] = 0$  as desired.

For the remainder of the proof, suppose that  $P|n$ , and set  $\bar{R} = R/P$ . We must show that  $\psi(G_0(\bar{R}G)) = 0$ , or equivalently, that  $\psi[M] = 0$  for each simple  $\bar{R}G$ -module  $M$ . It suffices to treat the case where  $G$  acts faithfully on  $M$ ; for let

$$H = \{x \in G : xm = m \text{ for all } m \in M\}, \quad \tilde{G} = G/H,$$

and view  $M$  as an  $\bar{R}\tilde{G}$ -module. There is a commutative diagram

$$\begin{array}{ccc} G_0(\bar{R}\tilde{G}) & \xrightarrow{\tilde{\psi}} & G_0(R\tilde{G}) \\ \downarrow & & \downarrow \\ G_0(\bar{R}G) & \xrightarrow{\psi} & G_0(RG), \end{array}$$

where the vertical arrows come from viewing each  $\tilde{G}$ -module as  $G$ -module. Now  $\tilde{G}$  acts faithfully on  $M$ , and if  $\tilde{\psi}[M] = 0$ , then also  $\psi[M] = 0$ .

It thus suffices to prove that  $\psi[M] = 0$  when  $M$  is a simple  $\bar{R}G$ -module on which  $G$  acts faithfully. Further, we need only treat the case where  $G$  is hyper-elementary, by (39.9). So now let  $G = C \times H$ , where  $C = \langle x \rangle$  is cyclic of order  $c$  with  $(p, c) = 1$ , and  $H$  is a  $p$ -group. If  $P|c$ , then  $\text{char } \bar{R} = q$  for some rational prime  $q$  dividing  $c$ . The Sylow  $q$ -subgroup of  $C$  is then normal in  $G$ , and acts trivially on  $M$  by (17.16), contradicting the assumption that  $G$  acts faithfully on  $M$ .

We are thus left with the case where  $\text{char } \bar{R} = p$ , and where (as above)  $G$  contains no nontrivial normal  $p$ -subgroup. Suppose first that  $\bar{R}$  contains  $\omega$ , a primitive  $c$ -th root of 1. We shall show that  $M$  is  $\bar{R}G$ -projective. By Exercise 21.5, every simple  $\bar{R}C$ -module is one-dimensional over  $\bar{R}$ . Let  $V$  be a simple  $\bar{R}C$ -submodule of  $M$ . We have  $\sum yV \subseteq M$ , where  $y$  ranges over all elements of  $H$ , and the sum is an  $\bar{R}G$ -submodule of  $M$ . Therefore  $M = \sum yV$ , and we now show that the sum is direct, that is,  $M \cong V^G$ . We need only show that the  $G$ -conjugates  $\{yV\}$  of  $V$  are mutually nonisomorphic  $\bar{R}C$ -modules. Since  $M$  is  $G$ -faithful, it is easily seen that  $V$  is faithful as  $C$ -module.

Now let  $yV \cong V$  as  $\bar{R}C$ -modules, where  $y \in H$ . Since  $C$  acts faithfully on  $V$ , this implies that  $x = y^{-1}xy$ . Put

$$H_1 = \{y \in H : x = y^{-1}xy\},$$

the centralizer of  $C$  in  $H$ . For each  $t \in G$ , we have  $C = \langle x^t \rangle$ , so for each  $y \in H_1$  it follows that  $y^t$  commutes with  $x$ . Write  $y^t = zh$ ,  $z \in C$ ,  $h \in H$ ; then  $h$  centralizes  $C$ , and commutes with  $z$ . Since  $y^t$  has  $p$ -power order, it follows that  $z = 1$  and  $y^t = h$ , so  $y^t \in H_1$ . Therefore  $H_1$  is a normal  $p$ -subgroup of  $G$ , and hence  $H_1 = 1$ .

This completes the proof that  $M \cong V^G$ . Since  $V$  is a direct summand of  $\bar{R}C$ ,  $M$  is a direct summand of  $\bar{R}G$ , and is therefore projective.

We reached the above conclusion under the simplifying assumption that  $\omega \in \bar{R}$ . Dropping this hypothesis, put  $E = \bar{R}(\omega)$  and form the  $EG$ -module  $L = E \otimes_R M$ . We have

$$L \cong M^{\dim_{\bar{R}} E} \quad \text{as } \bar{R}G\text{-modules.}$$

Now let  $\{M_i\}$  be the set of composition factors of the  $EG$ -module  $L$ . Then each  $\bar{R}G$ -composition factor of  $M_i|_{RG}$  is isomorphic to  $M$ , so  $M_i$  is a  $G$ -faithful simple  $EG$ -module (for each  $i$ ), and thus  $M_i$  is  $EG$ -projective by the preceding argument.

Next, if  $M_j$  is a simple factor module of  $L$ , the surjection  $L \rightarrow M_j$  must split since  $M_j$  is projective. Repeating this argument, it follows that  $L \cong \prod_i M_i$ , so  $L$  is  $EG$ -projective. Restricting the operator domain to  $\bar{R}G$ , it follows that  $M$  is  $\bar{R}G$ -projective, as claimed.<sup>†</sup>

We have now shown that every  $G$ -faithful simple  $\bar{R}G$ -module  $M$  must be  $\bar{R}G$ -projective, whether or not  $\omega \in \bar{R}$ . Since  $M$  is simple, it is a homomorphic image of  $\bar{R}G$ , so  $\bar{R}G \cong M \oplus N$  for some  $\bar{R}G$ -module  $N$ . Now choose  $\Lambda$ -exact sequences

$$0 \rightarrow X \rightarrow \Lambda \rightarrow M \rightarrow 0, \quad 0 \rightarrow Y \rightarrow \Lambda \rightarrow N \rightarrow 0.$$

We obtain a pair of  $\Lambda$ -exact sequences

$$0 \rightarrow X \oplus Y \rightarrow \Lambda^{(2)} \rightarrow M \oplus N \rightarrow 0, \quad 0 \rightarrow \Lambda \xrightarrow{\pi} \Lambda \rightarrow \bar{R}G \rightarrow 0,$$

where the arrow  $\pi$  is multiplication by the prime element  $\pi$  of  $P$ . Schanuel's Lemma then shows that  $X$  is  $\Lambda$ -projective. Further,  $KX \cong KG$  since  $M$  is an  $R$ -torsion module. By Swan's Theorem 32.11, we conclude that  $X$  lies in the genus of  $\Lambda$ , so  $X \cong \Lambda$  because  $R$  is semilocal. Therefore  $\psi[M] = [\Lambda] - [X] = 0$ , which completes the proof of Theorem 39.10.

We are now ready to derive a number of important corollaries, and begin by strengthening the localization sequence for the integral group ring case;

**(39.11) Theorem (Swan [63]).** *Let  $R$  be an arbitrary Dedekind domain, and let  $\Omega$  be any finite set of maximal ideals of  $R$ . Then there is an exact sequence of groups*

$$\coprod_{P \notin \Omega} G_0((R/P)G) \xrightarrow{\psi} G_0^R(RG) \xrightarrow{\varphi} G_0(KG) \rightarrow 0,$$

where the sum extends over all nonzero maximal ideals of  $R$  such that  $P \notin \Omega$ .

<sup>†</sup>If  $R$  is a complete d.v.r. with maximal ideal  $p$ , the above shows that  $M \cong M_0/pM_0$  for some projective  $RG$ -lattice  $M_0$ . This gives another proof of the main step in establishing (21.18).

*Proof.* Let  $\Omega = \{P_1, \dots, P_m\}$ , and let  $S$  be the multiplicative set

$$S = R - \{P_1 \cup \dots \cup P_m\}.$$

If  $R' = S^{-1}R$ , then  $R'$  is a semilocal Dedekind domain whose maximal ideals are  $\{P_i R' : 1 \leq i \leq m\}$  (see §4A). By (39.10), there is an isomorphism

$$\varphi' : G_0^{R'}(R'G) \cong G_0(KG).$$

On the other hand, (38.56) gives the exact sequence

$$\coprod_P G_0((R/P)G) \xrightarrow{\psi} G_0^R(RG) \rightarrow G_0^{R'}(R'G) \cong G_0(KG),$$

where  $P$  ranges over all prime ideals of  $R$  such that  $P \cap S \neq \emptyset$ . Thus  $P$  ranges over the nonzero maximal ideals of  $R$  outside of  $\Omega$ , and the proof is complete.

If  $R = K$ , then of course the sum  $\coprod_P$  is vacuous. If  $R \neq K$ , the result says that in the exact sequence (38.56), we may omit any preassigned finite set of summands from the first term.

We have already remarked in (38.66) that the additive group  $G_0(KG)$  is  $\mathbb{Z}$ -free, and so

$$G_0^R(RG) \cong G_0(KG) \oplus \ker \varphi.$$

We intend to show that  $\ker \varphi$  is a finite group whenever  $K$  is a global field such that  $\text{char } K \nmid n$ . In addition to the basic Theorem 39.11, we shall need the locally free class group  $\text{Cl } RG$ , which we now define for arbitrary orders.

**(39.12) Definition.** Let  $R$  be a Dedekind domain with quotient field  $K$ , and let  $\Lambda$  be an arbitrary order in a f.d.  $K$ -algebra  $A$ . For each maximal ideal  $P$  of  $R$ , let  $\Lambda_P$  be the localization of  $\Lambda$  at  $P$ , and let  $K_0(\Lambda) \rightarrow K_0(\Lambda_P)$  be the map induced by ground ring extension. The *locally free class group*  $\text{Cl } \Lambda$  is the kernel of the homomorphism

$$K_0(\Lambda) \rightarrow \prod_P K_0(\Lambda_P),$$

where  $P$  ranges over all maximal ideals of  $R$ .

Each  $x \in K_0(\Lambda)$  is of the form  $x = [F] - [X]$  with  $F$   $\Lambda$ -free and  $X \in \mathcal{P}(\Lambda)$ . Then  $x \in \text{Cl } \Lambda$  if and only if  $[F_P] = [X_P]$  for all  $P$ , or equivalently, if and only if  $F_P$  is stably isomorphic to  $X_P$ . By Exercise 39.1, this occurs if and only if  $F_P \cong X_P$  for all  $P$ , that is,  $X$  and  $F$  lie in the same genus. If  $F \cong \Lambda^{(k)}$ , then by (31.14) we have  $X \cong \Lambda^{(k-1)} \oplus M$  for some left ideal  $M$  in the genus of  $\Lambda$ . Therefore

$$(39.13) \quad \text{Cl } \Lambda = \{[\Lambda] - [M] \in K_0(\Lambda) : M = \text{locally free left ideal of } \Lambda\}.$$

If  $K$  is a global field and  $A$  is a semisimple  $K$ -algebra, the Jordan-Zassenhaus Theorem shows that there are only finitely many isomorphism classes of left ideals of  $\Lambda$ . Therefore we have.

**(39.13) Proposition.** *For any order  $\Lambda$  in a semisimple f.d.  $K$ -algebra, the locally free class group  $\text{Cl } \Lambda$  is finite.*

In Chapter 6, we shall investigate  $\text{Cl } \Lambda$  in more detail. Here, we use it to finish our discussion of the map  $\varphi: G_0^R(RG) \rightarrow G_0(KG)$ .

**(39.14) Theorem.** *Let  $\Lambda = RG$ ,  $A = KG$ , where  $G$  is a finite group of order  $n$ , and  $K$  is a global field for which  $\text{char } K \nmid n$ . Then there is an exact sequence of groups*

$$\text{Cl } \Lambda \xrightarrow{\mu} G_0^R(\Lambda) \xrightarrow{\varphi} G_0(A) \rightarrow 0,$$

where  $\mu$  is defined by viewing each  $X \in \mathcal{P}(\Lambda)$  as  $\Lambda$ -lattice. Thus

$$G_0^R(\Lambda) \cong G_0(A) \oplus \ker \varphi,$$

and  $\ker \varphi$  is a finite abelian group.

*Proof.* Clearly  $\varphi\mu = 0$ . Now let  $\Omega$  be the finite set of maximal ideals of  $R$  which divide  $n$ . By (39.11), to prove that  $\ker \varphi = \text{im } \mu$ , it suffices to show that

$$\psi\{G_0((R/P)G)\} \subseteq \text{im } \mu$$

for each  $P \notin \Omega$ .

Let  $M$  be any f.g.  $(R/P)G$ -module, and choose a  $\Lambda$ -exact sequence

$$0 \rightarrow X \rightarrow F \rightarrow M \rightarrow 0,$$

with  $F$   $\Lambda$ -free. Then  $M_Q = 0$  for each maximal ideal  $Q$  of  $R$  containing  $n$ , so  $X_Q = F_Q$  for each such  $Q$ . But then  $X$  lies in the genus of  $F$  by (31.2), and thus  $[F] - [X] \in \text{Cl } \Lambda$ . This gives  $\psi[M] = [F] - [X] \in \text{im } \mu$ , as desired. The remaining assertions in the theorem are then obvious. The fact that  $K$  is a global field is used only to insure that  $\text{Cl } \Lambda$  is finite.

Our next step in the computation of  $G_0(\Lambda)$  is the comparison of the localization sequences of  $\Lambda$  and  $\Lambda'$ , where  $\Lambda'$  is a maximal order in  $A$  containing  $\Lambda$ . As shown by Swan [63], we have

**(39.15) Theorem.** *Let  $G$  be a finite group of order  $n$ , and  $R$  a Dedekind domain with quotient field  $K$  such that  $\text{char } K \nmid n$ . Let  $\Lambda = RG$ ,  $A = KG$ , and let  $\Lambda'$  be a maximal order in  $A$  containing  $\Lambda$ . Then there is a commutative diagram of groups, with exact rows:*

$$\begin{array}{ccccccc}
 \text{Cl } \Lambda & \xrightarrow{\mu} & G_0^R(\Lambda) & \xrightarrow{\varphi} & G_0(A) & \longrightarrow 0 \\
 \rho \downarrow & & \alpha \uparrow & & 1 \uparrow & \\
 0 \longrightarrow \text{Cl } \Lambda' & \xrightarrow{\mu'} & G_0^R(\Lambda') & \xrightarrow{\varphi'} & G_0(A) & \longrightarrow 0,
 \end{array}$$

where  $\rho$  is the map defined by  $\Lambda' \otimes_{\Lambda} *$ , and  $\alpha$  is defined by restriction of operators from  $\Lambda'$  to  $\Lambda$ . Further, both  $\rho$  and  $\alpha$  are surjective.

*Proof.* By (26.5), the order  $\Lambda$  may be embedded in a maximal order  $\Lambda'$ . Each  $\Lambda'$ -lattice is  $\Lambda'$ -projective by (26.12), so  $G_0^R(\Lambda') = K_0(\Lambda')$ . Let  $x = [F] - [X] \in \ker \varphi'$ , where  $F$  is  $\Lambda'$ -free and  $X$  is a  $\Lambda'$ -lattice. Since  $\varphi'(x) = 0$ , we have  $[KF] = [KX]$  in  $G_0(A)$ , and thus  $KF \cong KX$ . But then  $F$  and  $X$  are in the same genus by (32.1), so  $x \in \text{Cl } \Lambda'$ . This shows that the bottom row of the above diagram is exact.

The right-hand square is clearly commutative. For the left-hand square, let  $\xi \in \text{Cl } \Lambda$ , and write  $\xi = [\Lambda] - [M]$  with  $M$  a left ideal of  $\Lambda$  in the genus of  $\Lambda$ . By Exercise 31.10, we have

$$[\Lambda] - [M] = [\Lambda'] - [\Lambda' \otimes_{\Lambda} M] \quad \text{in } G_0(\Lambda).$$

Therefore  $\mu(\xi) = (\alpha \mu' \rho)(\xi)$  in  $G_0(\Lambda)$ . Since  $G_0(\Lambda) \cong G_0^R(\Lambda)$ , it follows that  $\mu = \alpha \mu' \rho$ , as desired.

To show that  $\rho$  is surjective, let  $x' = [\Lambda'] - [X] \in \text{Cl } \Lambda'$ , where  $X$  is a left ideal in  $\Lambda'$ . Let  $P$  range over all maximal ideals of  $R$ ; for each  $P$  we have  $X_P \cong \Lambda'_P$ , so  $X_P = \Lambda'_P \beta_P$  for some  $\beta_P \in A$ , with  $\beta_P = 1$  a.e. Set

$$M = A \cap \left\{ \bigcap_P \Lambda_P \beta_P \right\},$$

and then  $M$  is a full left  $\Lambda$ -lattice in  $A$  for which  $M_P = \Lambda_P \beta_P$  for all  $P$ . Thus  $M$  lies in the genus of  $\Lambda$ , and  $x = [\Lambda] - [M] \in \text{Cl } \Lambda$ . In order to prove that  $\rho(x) = x'$ , we need only show that  $\Lambda' \otimes_{\Lambda} M \cong X$ . But for each  $P$ ,

$$(\Lambda' \otimes_{\Lambda} M)_P = \Lambda'_P \otimes_{\Lambda_P} M_P \cong \Lambda'_P \beta_P = X_P,$$

so the map  $\Lambda' \otimes_{\Lambda} M \rightarrow \Lambda' M \subseteq A$  is the desired isomorphism. Thus  $\rho$  is surjective.

Finally,  $\alpha$  is surjective by “diagram-chasing”: let  $x \in G_0^R(\Lambda)$ , and choose  $y \in G_0^R(\Lambda')$  with  $\varphi'(y) = \varphi(x)$ . Then  $\varphi(x - \alpha y) = 0$ , so  $x - \alpha y = \mu z$  for some  $z \in \text{Cl } \Lambda$ . Therefore

$$x = \alpha y + \mu z = \alpha y + \alpha \mu' \rho z \in \text{im } \alpha.$$

Thus  $\alpha$  is surjective, and the theorem is proved.

At the end of §39B we shall show by example that the map  $\alpha$  in (39.15)

need not be an isomorphism. Further (see (49.33) and §50)  $\text{Cl}\Lambda$  is usually larger than  $\text{Cl}\Lambda'$ , so the maps  $\rho$  and  $\mu$  need not be injective.

We conclude this subsection with a brief discussion of the ring structure of  $G_0^R(\Lambda)$ . The main result, due to Swan [63], is as follows:

**(39.16) Theorem.** *Assume that  $\text{char } K/n$ , and let  $\varphi: G_0^R(\Lambda) \rightarrow G_0(A)$  as in (39.14). Then  $\ker \varphi$  is an ideal of  $G_0^R(\Lambda)$  such that  $(\ker \varphi)^2 = 0$ . Furthermore,*

$$\ker \varphi = \{x \in G_0^R(\Lambda) : x^2 = 0\}.$$

*Proof.* If  $x \in G_0^R(\Lambda)$  is such that  $x^2 = 0$ , then  $(\varphi(x))^2 = 0$  in  $G_0(A)$ . But  $G_0(A)$  has no nonzero nilpotent elements by Exercise 17.4, so  $x \in \ker \varphi$ . We show next that for  $x, y \in \ker \varphi$ , we have  $xy = 0$ . Write

$$x = [\Lambda] - [L], \quad y = [\Lambda] - [M],$$

where  $L, M$  are locally free left ideals of  $\Lambda$ . By definition of multiplication,

$$xy = [\Lambda \otimes \Lambda] - [L \otimes \Lambda] - [\Lambda \otimes M] + [L \otimes M],$$

where  $\otimes$  means inner tensor product over  $R$ . There is a  $\Lambda$ -exact sequence  $0 \rightarrow L \rightarrow \Lambda \rightarrow T \rightarrow 0$ , with  $T$  an  $R$ -torsion  $\Lambda$ -module. Since both  $M$  and  $\Lambda$  are  $R$ -flat, we obtain  $\Lambda$ -exact sequences

$$0 \rightarrow L \otimes M \rightarrow \Lambda \otimes M \rightarrow T \otimes M \rightarrow 0, \quad 0 \rightarrow L \otimes \Lambda \rightarrow \Lambda \otimes \Lambda \rightarrow \Lambda \otimes T \rightarrow 0.$$

But the inclusion  $M \subseteq \Lambda$  gives a map  $T \otimes M \rightarrow T \otimes \Lambda$ , which must be an isomorphism because both are  $R$ -torsion  $\Lambda$ -modules, and for each maximal ideal  $P$  of  $R$ ,  $(T \otimes M)_P \cong T_P \otimes M_P \cong T_P \otimes \Lambda_P \cong (T \otimes \Lambda)_P$ .

We now have  $T \otimes M \cong T \otimes \Lambda \cong \Lambda \otimes T$ , and both  $\Lambda \otimes M$  and  $\Lambda \otimes \Lambda$  are  $\Lambda$ -projective (by Exercise 10.19), so applying Schanuel's Lemma we obtain

$$(L \otimes M) \oplus (\Lambda \otimes \Lambda) \cong (L \otimes \Lambda) \oplus (\Lambda \otimes M).$$

Thus  $xy = 0$ , and the theorem is proved.

In the cases where the ring structure of  $G_0^R(\Lambda)$  has been worked out, one begins by finding a *ring* homomorphism  $\sigma: G_0(A) \rightarrow G_0^R(\Lambda)$  for which  $\varphi\sigma = 1$ . One may then view  $G_0(A)$  as a subring of  $G_0^R(\Lambda)$ , and the problem reduces to calculating its action on the ideal  $\ker \varphi$ . This calculation has been performed for  $\Lambda = ZG$  when  $G$  is cyclic (see Stancl [67], Swan [63]), and for  $G$  an elementary abelian  $p$ -group (Stancl [67]). For further results, see Obayashi [66], Uchida [67], and Matchett [76]; the work of Santa-Pietro [72] contains some errors, however.

One important application of Theorem 39.16 is as follows: the ring  $G_0^R(RG)$  acts on various abelian groups, such as  $K_0(RG)$  for example. In some cases

this action can be extended to an action of the ring  $G_0(KG)$  on such abelian groups, by verifying that  $\ker \varphi$  acts trivially. Thus we shall see in (49.48) that  $G_0(\mathbb{Q}G)$  acts on  $K_0(\mathbb{Z}G)$ ; see §49C for other results of this nature.

### §39B. Explicit Calculations

Here we shall derive the Heller-Reiner formula (39.20) for  $G_0^R(\Lambda)$ , where  $\Lambda = RG$ , with  $R$  a Dedekind domain whose quotient field  $K$  is an algebraic number field. As before, let  $|G| = n$ , and assume  $R \neq K$  to avoid trivialities.

Let  $A = KG$ , and let  $\Lambda'$  be a maximal  $R$ -order in  $A$  containing  $\Lambda$ . By (26.20) we may write

$$(39.17) \quad A = \bigoplus_{i=1}^s A_i, \quad \Lambda' = \bigoplus_{i=1}^s \Lambda_i,$$

where the  $\{\Lambda_i\}$  are maximal  $R$ -orders in the Wedderburn components  $\{A_i\}$  of  $A$ . Let

$$K_i = \text{center of } A_i, \quad R_i = \text{integral closure of } R \text{ in } K_i, \quad 1 \leq i \leq s,$$

so  $A_i$  is a central simple  $K_i$ -algebra, and  $\Lambda_i$  is a maximal  $R_i$ -order in  $A_i$ . As in §39A, let  $G_0^t(\Lambda')$  be the Grothendieck group of the category of f.g.  $R$ -torsion  $\Lambda'$ -modules. Since such modules decompose the same way as  $\Lambda'$ , we have

$$G_0^t(\Lambda') \cong \prod_{i=1}^s G_0^t(\Lambda_i),$$

noting that for a  $\Lambda_i$ -module,  $R$ -torsion coincides with  $R_i$ -torsion by Exercise 23.9. Using (38.68), we obtain an isomorphism

$$\tau: G_0^t(\Lambda') \cong \prod_{i=1}^s I(R_i),$$

where  $I(R_i)$  is the group of  $R_i$ -ideals in  $K_i$ . Let  $P_{A_i}(R_i)$  be the subgroup of  $I(R_i)$  defined as in (38.67), and let  $\delta': K_1(A) \rightarrow G_0^t(\Lambda')$  be the map occurring in the localization sequence for  $\Lambda'$ . Then

$$\text{im } \tau \delta' = \prod_{i=1}^s P_{A_i}(R_i).$$

Next, by (38.61) there is a commutative diagram of groups, with exact rows:

$$\begin{array}{ccccccc} K_1(A) & \xrightarrow{\delta'} & G_0^t(\Lambda') & \xrightarrow{\psi'} & G_0(\Lambda') & \xrightarrow{\varphi'} & G_0(A) \longrightarrow 0 \\ 1 \downarrow & & \beta \downarrow & & \alpha \downarrow & & 1 \downarrow \\ K_1(A) & \xrightarrow{\delta} & G_0^t(\Lambda) & \xrightarrow{\psi} & G_0(\Lambda) & \xrightarrow{\varphi} & G_0(A) \longrightarrow 0, \end{array}$$

where  $\alpha$  and  $\beta$  come from restriction of operators from  $\Lambda'$  to  $\Lambda$ . By (39.16),  $\alpha$  is surjective. An easy “diagram-chase” then shows that  $\beta$  is also surjective, and that

$$(39.18) \quad \ker \varphi \cong \text{cok } \delta \cong G_0^t(\Lambda') / (\text{im } \delta' + \ker \beta).$$

Since  $G_0(A)$  is  $\mathbb{Z}$ -free, we have

$$G_0(\Lambda) \cong G_0(A) \oplus \ker \varphi,$$

so the additive structure of  $G_0(\Lambda)$  and  $G_0^R(\Lambda)$  is determined by the group  $\ker \varphi$ . This is a finite abelian group, by (39.14).

Using the above isomorphism  $\tau$ , we have

$$\text{cok } \delta \cong \left( \prod_{i=1}^s I(R_i) \right) \Big/ \left( \prod_{i=1}^s P_{A_i}(R_i) \right) \cdot \tau(\ker \beta),$$

and it remains for us to describe  $\tau(\ker \beta)$ . By (38.60) we may write  $\beta = \bigoplus \beta_P$ , where

$$\beta_P: G_0(\Lambda'/P\Lambda') \rightarrow G_0(\Lambda/P\Lambda),$$

and where  $P$  ranges over the maximal ideals of  $R$ . Since  $\beta$  is surjective, so is each  $\beta_P$ . If  $P \nmid n$ , then by (27.1) we have  $\Lambda_P = \Lambda'_P$ , and  $\beta_P$  is an isomorphism. Therefore

$$\tau(\ker \beta) = \prod_{P \mid n} W_P, \quad \text{where} \quad W_P = \tau(\ker \beta_P).$$

We now introduce additional notation, to help us describe  $W_P$  explicitly. For each maximal ideal  $P$  of  $R$  dividing  $n$ , we write

$$PR_i = \prod_{j=1}^{t_i} P_{ij}^{e_{ij}}, \quad P_{ij} = \text{distinct prime ideals of } R_i, \quad 1 \leq i \leq s,$$

with the  $\{e_{ij}\}$  positive integers. For fixed  $i$  and  $j$ , we have

$$G_0(\Lambda_i/P_{ij}^{e_{ij}}\Lambda_i) \cong G_0(\Lambda_i/P_{ij}\Lambda_i) \cong \mathbb{Z},$$

since the two artinian factor rings above have the same unique simple module, hereafter denoted by  $S_{ij}$  (see proof of (38.67)). Therefore

$$\begin{aligned} G_0(\Lambda'/P\Lambda') &\cong \coprod_{i=1}^s G_0(\Lambda_i/P\Lambda_i) \cong \coprod_{i=1}^s \coprod_{j=1}^{t_i} G_0(\Lambda_i/P_{ij}^{e_{ij}}\Lambda_i) \\ &\cong \coprod_{i,j} G_0(\Lambda_i/P_{ij}\Lambda_i) = \coprod_{i,j} \mathbb{Z}[S_{ij}]. \end{aligned}$$

The isomorphism  $\tau$  carries  $[S_{ij}]$  onto its  $R_i$ -annihilator  $P_{ij} \in I(R_i)$ . Since  $P \supseteq P_{ij}$ , we may view  $S_{ij}$  as a  $(\Lambda/P\Lambda)$ -module. We thus obtain

$$(39.19) \quad W_P = \tau(\ker \beta_P) = \left\{ \prod_{i,j} P_{ij}^{n_{ij}} : \sum_{i,j} n_{ij} [S_{ij}] = 0 \text{ in } G_0(\Lambda/P\Lambda) \right\}.$$

Combining all of this information, we obtain the formula

$$(39.20) \quad G_0(\Lambda) \cong G_0(A) \oplus \left( \prod_{i=1}^s I(R_i) \right) / \left( \prod_{i=1}^s P_{A_i}(R_i) \right) \cdot \prod_{P|n} W_P,$$

due to Heller-Reiner [64, 65].

As our first application of this formula, we treat the case where  $G$  is cyclic, and  $\Lambda = \mathbb{Z}G$ . The result is due independently to Bass [79], Lenstra [81], and Reiner (see Reiner-Roggenkamp [79], p. 97).

**(39.21) Theorem.** *Let  $G$  be a cyclic group of order  $n$ , and let  $\Lambda = \mathbb{Z}G$ . For each  $d$  dividing  $n$ , let  $\zeta_d$  be a primitive  $d$ -th root of 1 over  $\mathbb{Q}$ , and set*

$$K_d = \mathbb{Q}(\zeta_d), \quad R_d = \mathbb{Z}[\zeta_d] = \text{alg. int. } \{K_d\}.$$

Then

$$G_0(\Lambda) \cong G_0(A) \oplus \prod_{d|n} \text{Cl} R_d[d^{-1}].$$

*Proof.* The unique maximal order in  $A$  is given by  $\Lambda' = \coprod R_d$ , and we have  $A = \coprod K_d$ . If  $G = \langle x \rangle$ , then  $x$  acts on each  $K_d$  and  $R_d$  as multiplication by  $\zeta_d$ . Let us calculate  $W_p$ , where  $p$  is a prime divisor of  $n$ . Write

$$pR_d = \prod_j P_{dj}^{e_{dj}}, \quad \{P_{dj}\} \text{ distinct prime ideals of } R_d,$$

for each  $d$  dividing  $n$ . The unique simple  $(\Lambda_d/P_{dj}\Lambda_d)$ -module is just  $R_d/P_{dj}$ , for each  $j$ . Thus, by (39.19),

$$W_P = \left\{ \prod_{d,j} P_{dj}^{n_{dj}} : \sum n_{dj} [R_d/P_{dj}] = 0 \text{ in } G_0(\Lambda/p\Lambda) \right\}.$$

For each  $d$ , write  $d = ap^u$ , where  $(p, a) = 1$ . By (4.40), in the extension  $K_a/\mathbb{Q}$ , the rational prime  $p$  splits into distinct prime ideals  $\{P_{aj}\}$  of  $R_a$ ; in the extension  $K_d/K_a$ , each  $P_{aj}$  is completely ramified:

$$(39.22) \quad P_{aj}R_d = P_{aj}^{ap^u}, \quad R_d/P_{dj} \cong R_a/P_{aj} \quad \text{for each } j.$$

The above isomorphism is a  $(\Lambda/P\Lambda)$ -isomorphism, so  $W_p$  contains all products  $P_{dj}P_{aj}^{-1}$ , with  $d, j$  varying.

We show next that  $W_p$  is generated by all such products, and for this purpose

we compute  $G_0(\Lambda/p\Lambda)$ . Let  $n = mp^k$ ,  $p \nmid m$ , and put  $\bar{Z} = Z/pZ$ . Then

$$\Lambda/p\Lambda \cong \bar{Z}[x]/(x^n - 1) \cong \bar{Z}[x]/(x^m - 1)^{p^k},$$

so

$$G_0(\Lambda/p\Lambda) \cong G_0(\bar{Z}[x]/(x^m - 1)).$$

But

$$\bar{Z}[x]/(x^m - 1) \cong \coprod_{a|m} \bar{Z}[x]/(\Phi_a(x)) \cong \coprod_{a|m} R_a/pR_a \cong \coprod_{a|m} \coprod_j R_a/P_{aj}.$$

The modules  $\{R_a/P_{aj}\}$  are nonisomorphic as  $\bar{Z}[x]/(x^m - 1)$ -modules, hence also as  $(\Lambda/p\Lambda)$ -modules, and we have

$$G_0(\Lambda/p\Lambda) = \coprod_{a,j} \bar{Z}[R_a/P_{aj}].$$

It follows at once that the products  $\{P_{dj}P_{aj}^{-1}\}$  generate  $W_p$ , as claimed. Note that such generators occur only when  $d$  is a multiple of  $p$ .

In formula (39.20), the subgroup  $P_{K_d}(R_d)$  of the ideal group  $I(R_d)$  is just the usual subgroup of principal ideals  $P(R_d)$ , so now

$$(39.23) \quad \ker \varphi \cong \left( \prod_{d|n} I(R_d) \right) / \left( \prod_{d|n} P(R_d) \right) \left( \prod_{p|n} (W_p) \right).$$

To simplify this expression, let  $N_{d/e}$  denote the norm map  $N_{K_d/K_e}$  whenever  $e|d$ . We now define an endomorphism  $\varepsilon$  of the group  $\prod_{d|n} I(R_d)$ , by setting

$$\varepsilon(X_d) = \prod_{\substack{e|d \\ (e,d/e)=1}} N_{d/e}(X_d), \quad \text{for } X_d \in I(R_d), \quad d|n.$$

Since the divisors of  $n$  form a partially ordered set with respect to divisibility, and since  $\varepsilon(X_d) = X_d \cdot (\text{elements of "lower" order})$ , it follows that  $\varepsilon$  is an *automorphism* of  $\prod_{d|n} I(R_d)$ . Clearly  $\varepsilon$  carries  $\prod_{d|n} P(R_d)$  onto itself.

We now show that

$$(*) \quad \prod_{p|n} \varepsilon(W_p) = \prod_{d|n} Y_d,$$

where  $Y_d$  is the subgroup of  $I(R_d)$  generated by the prime ideal divisors of  $d$  in  $R_d$ . Consider a generator  $P_{dj}P_{aj}^{-1}$  of  $W_p$ , where  $d = p^u a$ ,  $p/a$ . Then

$$\varepsilon(P_{dj}P_{aj}^{-1}) = \prod_e N_{d/e}(P_{dj}) \cdot \prod_c N_{a/c}(P_{aj})^{-1},$$

where  $e|d$ ,  $(e, d/e) = 1$  and  $c|a$ ,  $(c, a/c) = 1$ . The choices for  $e$  are  $p^u c$  and  $c$ , with  $c$  as above. Since

$$N_{d/c}(P_{dj}) = N_{a/c} N_{d/a}(P_{dj}) = N_{a/c}(P_{aj}),$$

we obtain

$$\varepsilon(P_{d_j} P_{aj}^{-1}) = \prod_c N_{d/p^u c}(P_{d_j}).$$

This shows that the left side of formula (\*) is contained in the right side. To prove the reverse inclusion, we use induction on the total number of prime factors of  $d$  to establish that

$$(**) \quad Y_d \subseteq \prod_{\substack{q|n \\ q \text{ prime}}} \varepsilon(W_q) \quad \text{whenever } d|n.$$

This is clear when  $d = p$ , since  $\varepsilon(P_{d_j} P_{aj}^{-1}) = P_{d_j}$  for each  $j$ . Now let  $d = p^u a$ ,  $u \geq 1$ ; then

$$\varepsilon(P_{d_j} P_{aj}^{-1}) = P_{d_j} \cdot \prod_c N_{d/p^u c}(P_{d_j}),$$

where  $c$  ranges over all proper divisors of  $a$  such that  $(c, a/c) = 1$ . However,  $\prod_c \varepsilon(W_q) \subseteq \prod \varepsilon(W_q)$  by the induction hypothesis, and therefore also  $P_{d_j} \subseteq \prod \varepsilon(W_q)$ . This proves (\*\*), and also (\*).

We thus obtain

$$\ker \varphi \cong \prod_{d|n} \{I(R_d)/P(R_d)Y_d\} \cong \prod_{d|n} \mathrm{Cl}(R_d)/V_d,$$

where  $V_d$  is the subgroup of the ideal class group  $\mathrm{Cl} R_d$  generated by the classes of all prime ideal divisors  $\{P_{d_j}\}$  of  $d$ . By Exercise 39.2, we have

$$\mathrm{Cl}(R_d)/V_d \cong \mathrm{Cl} R_d[d^{-1}],$$

where  $R_d[d^{-1}]$  consists of all expressions  $\{\alpha/d^k : \alpha \in R_d, k \geq 0\}$ . This completes the proof of the theorem.

**(39.24) Remarks.** (i) Keeping the above notation, let  $\Lambda' = \coprod_{d|n} R_d$  be the maximal order in  $A$ . The restriction map  $\alpha : G_0(\Lambda') \rightarrow G_0(\Lambda)$  is given by

$$\alpha : \coprod \mathrm{Cl} R_d \oplus G_0(A) \rightarrow \coprod \mathrm{Cl} R_d[d^{-1}] \oplus G_0(A),$$

where  $\mathrm{Cl} R_d \rightarrow \mathrm{Cl} R_d[d^{-1}]$  is the surjection discussed above. Hence, if we choose a positive integer  $d$  such that some prime ideal divisor of  $d$  in  $R_d$  is not principal, we obtain an example in which the map  $\alpha$  is not monic. For example, let  $n = pq$  be a product of two distinct odd primes, chosen so that some prime ideal divisor  $Q$  of  $q$  in  $R_p$  is not principal. Since  $Q$  ramifies completely in the extension  $R_n/R_p$ , it follows that  $QR_n = Q_0^{q-1}$  for some nonprincipal ideal  $Q_0$  of  $R_n$  dividing  $q$ . Thus the map  $\mathrm{Cl} R_n \rightarrow \mathrm{Cl} R_n[n^{-1}]$  is not monic, and so  $\alpha$  is also not monic.

(ii) Let  $n = p^k$  be a prime power, and let  $d|n$ . By (4.38), the prime  $p$  ramifies

completely in  $R_d$ , and is a power of a principal ideal. Thus  $\text{Cl } R_d = \text{Cl } R_d[d^{-1}]$  in this case, so we obtain  $G_0(\Lambda) \cong G_0(\Lambda')$ . As we shall see below, this same isomorphism holds more generally when  $\Lambda = \mathbb{Z}G$ , with  $G$  any abelian  $p$ -group.

Now let  $A = \mathbb{Q}G$ ,  $\Lambda = \mathbb{Z}G$ , where  $G$  is any finite abelian group. We shall obtain a formula due to Lenstra [81] for  $G_0(\Lambda)$ . Let  $\{G_1, \dots, G_t\}$  be the set of all subgroups of  $G$  for which the factor group  $G/G_i$  is cyclic. Put

$$H_i = G/G_i = \langle x_i \rangle, \quad |H_i| = n_i, \quad 1 \leq i \leq t,$$

and let

$$K_{n_i} = \mathbb{Q}(\zeta_{n_i}), \quad R_{n_i} = \mathbb{Z}[\zeta_{n_i}], \quad \text{where } \zeta_{n_i} = \text{primitive } n_i\text{-th root of 1 over } \mathbb{Q}.$$

By Exercise 39.4, we Wedderburn decomposition of  $A$  is given by

$$A = \coprod_{i=1}^t K_{n_i},$$

and  $G$  acts on  $K_{n_i}$  by means of the surjection  $G \rightarrow H_i$ , and the faithful action of  $H_i$  on  $K_{n_i}$  in which  $x_i$  acts as multiplication by  $\zeta_{n_i}$ . The unique maximal order  $\Lambda'$  in  $A$  is  $\coprod R_{n_i}$ . We have by (39.20)

$$G_0(\Lambda) \cong G_0(A) \oplus \left( \prod_{i=1}^t I(R_{n_i}) \right) / \left( \prod_{i=1}^t P(R_{n_i}) \right) \left( \prod_{p|n} W_p \right).$$

For each prime  $p$  dividing  $n$ , and each  $i$ , let  $P_{ij}$  range over all prime ideal divisors of  $p$  in  $R_{n_i}$ . Then  $\{R_{n_i}/P_{ij}\}$  gives a basic set of simple  $(\Lambda'/p\Lambda)$ -modules, and we have, as before,

$$W_p = \left\{ \prod_{i,j} P_{ij}^{b_{ij}} : \sum_{i,j} b_{ij} [R_{n_i}/P_{ij}] = 0 \text{ in } G_0(\Lambda/p\Lambda) \right\}.$$

For each  $i$ , write  $n_i = m_i p^{k_i}$  where  $p \nmid m_i$ . Then as in (39.22),

$$R_{n_i}/P_{ij} \cong R_{m_i}/P_{ij}^*, \quad \text{where } P_{ij}^* = R_{m_i} \cap P_{ij}.$$

Apart from this, there are no other relations in  $G_0(\Lambda/p\Lambda)$ , since  $H_{m_i}$  is the unique cyclic factor group of  $G$  which acts faithfully on the module  $R_{m_i}/P_{ij}^*$ . It follows at once that

$$(39.25) \quad G_0(\mathbb{Z}G) \cong \prod_{i=1}^t G_0(\mathbb{Z}H_i),$$

with  $G_0(\mathbb{Z}H_i)$  given by Theorem 39.21. This is Lenstra's formula for  $G_0(\mathbb{Z}G)$ ; for further discussion of this topic, and for its topological significance, see Bass

[79] and Lenstra [81]. There is an analogous formula, somewhat more complicated, for the group  $G_1(\mathbb{Z}G)$  defined as in (38.28); for details, see Liu [82].

**(39.26) Corollary.** *For any abelian  $p$ -group  $G$ , we have*

$$G_0(\mathbb{Z}G) \cong G_0(\Lambda'),$$

where  $\Lambda'$  is the maximal order of  $\mathbb{Q}G$ .

The above corollary has been generalized by David Webb [83], by using Frobenius functors. He showed that if  $G$  is an arbitrary group which does not contain a pair of commuting elements of relatively prime order, then  $G_0(\mathbb{Z}G) \cong G_0(\Lambda')$ , where  $\Lambda'$  is a maximal order in  $\mathbb{Q}G$ . He also computed  $G_0(\mathbb{Z}G)$  for  $G$  dihedral. (Also see Sumioka [73].)

### §39. Exercises

1. Let  $R$  be a d.v.r., not necessarily complete, and let  $\Lambda$  be an  $R$ -algebra, f.g./ $R$  as module. Let  $L, M, N$  be f.g. left  $\Lambda$ -modules. Show that for  $k \geq 1$ ,

$$L^{(k)} \cong M^{(k)} \Rightarrow L \cong M \quad \text{and} \quad L \oplus M \cong L \oplus N \Rightarrow M \cong N.$$

[Hint: Use (30.7) and (30.17).]

2. Let  $m$  be a nonzero element of a Dedekind domain  $R$ , and let  $\{P_i\}$  be the set of prime ideal divisors of  $m$  in  $R$ . Let  $V$  be the subgroup of the ideal class group  $\text{Cl } R$  generated by the classes  $[P_i]$ . Prove that  $\text{Cl}(R)/V \cong \text{Cl } R[m^{-1}]$ .

[Hint: Let  $R' = R[m^{-1}]$ ; extension of ground ring from  $R$  to  $R'$  gives a homomorphism of ideal groups  $I(R) \rightarrow I(R')$ , which induces the desired isomorphism.]

3. Let  $\Lambda$  be an arbitrary  $R$ -order in a f.d.  $K$ -algebra  $A$ , and let  $e$  be a central idempotent of  $A$ . Prove that there is a surjection

$$G_0(\Lambda e) \oplus G_0(\Lambda(1 - e)) \rightarrow G_0(\Lambda).$$

Deduce from this that if  $\Lambda = \mathbb{Z}G$  with  $G$  abelian, then the map  $\alpha$  in (39.15) is surjective. (See also Exercise 42.8.)

4. Let  $G$  be a finite abelian group, and let  $\{G_1, \dots, G_t\}$  be the set of all subgroups of  $G$  for which  $G/G_i$  is cyclic. Set

$$H_i = G/G_i, \quad n_i = |H_i|, \quad H_i = \langle x_i \rangle, \quad 1 \leq i \leq t.$$

Let  $K_{n_i} = \mathbb{Q}(\zeta_{n_i})$ , where  $\zeta_{n_i}$  is a primitive  $n_i$ -th root of 1 over  $\mathbb{Q}$ . Prove that

$$\mathbb{Q}G \cong \coprod_{i=1}^t K_{n_i},$$

where the  $i$ -th projection map is given by composition

$$QG \rightarrow QH_i \rightarrow K_{n_i}.$$

[Hint: Each Wedderburn component of  $QG$  is a field  $F = \mathbb{Q}(\theta(G))$ , where  $\theta: G \rightarrow F^*$  is a homomorphism. Then  $\ker \theta = G_i$  for some  $i$ , and  $\theta: H_i \rightarrow F^*$  is a faithful representation of the cyclic group  $H_i = G/G_i$ . This gives  $F = \mathbb{Q}(\theta(x_i))$ , where  $\langle x_i \rangle = H_i$ , so  $F \cong K_{n_i}$ . Further, there is a unique simple  $QH_i$ -module on which  $H_i$  acts faithfully, namely  $K_{n_i}$ , so the Wedderburn components of  $QG$  are in bijection with the set  $\{H_i : 1 \leq i \leq t\}$ .]

5. Let  $\Lambda = RG$  where  $G$  is a finite group and  $R$  is a commutative ring. Prove that  $K_1(\Lambda)$  is a Frobenius module over the Frobenius functor  $G_0^R(\Lambda)$ .

[Hint: Given  $M \in \mathcal{P}(\Lambda)$  and  $\mu \in \text{Aut}_\Lambda M$ , and any  $\Lambda$ -lattice  $X$ , define

$$[X] \cdot [M, \mu] = [X \otimes_R M, 1 \otimes \mu].$$

Show that this gives a well-defined action of  $G_0^R(\Lambda)$  on  $K_1(\Lambda)$ .]

## §40. WHITEHEAD GROUPS

In this section we give another definition of the Whitehead group  $K_1(\Lambda)$  of an arbitrary ring  $\Lambda$ , and show that the new definition agrees with that in (38.28). We then obtain a localization sequence for  $K_0$  and  $K_1$  analogous to that in (38.56). The section concludes with a discussion of elementary matrices and stability theorems.

### §40A. Introduction

Let  $\Lambda$  be an arbitrary ring. For each integer  $n \geq 1$ , let  $GL_n(\Lambda)$  be the group of all invertible  $n \times n$  matrices over  $\Lambda$ . We embed  $GL_n(\Lambda)$  in  $GL_{n+1}(\Lambda)$  by means of the homomorphism

$$\alpha \rightarrow \begin{pmatrix} \alpha & 0 \\ 1 & 1 \end{pmatrix}, \quad \alpha \in GL_n(\Lambda).$$

Now define the *general linear group*  $GL(\Lambda)$  by

$$(40.1) \quad GL(\Lambda) = \bigcup_{n=1}^{\infty} GL_n(\Lambda) = \varinjlim GL_n(\Lambda).$$

Thus, each element of  $GL(\Lambda)$  is represented by a matrix  $\alpha \in GL_n(\Lambda)$  for some  $n$ . If  $\beta \in GL_m(\Lambda)$  where  $m \geq n$ , then  $\alpha = \beta$  in  $GL(\Lambda)$  if and only if  $\beta = \text{diag}(\alpha, 1, \dots, 1)$  in  $GL_m(\Lambda)$ .

Now let

$$GL'(\Lambda) = [GL(\Lambda), GL(\Lambda)]$$

be the commutator subgroup of  $GL(\Lambda)$ . We set

$$(40.2) \quad K_1(\Lambda) = GL(\Lambda)/GL'(\Lambda),$$

an abelian multiplicative group called the *Whitehead group* of  $\Lambda$  (see the remark following (38.28)). Our first task is to establish an isomorphism between this  $K_1(\Lambda)$  and the group defined in (38.28), which we shall denote by  $K_{\det}(\Lambda)$  for convenience.

Let us recall from §38 that  $K_{\det}(\Lambda)$  is the additive group generated by ordered pairs  $[M, \mu]$  with  $M \in \mathcal{P}(\Lambda)$ ,  $\mu \in \text{Aut}_{\Lambda} M$ , modulo the subgroup generated by all expressions

$$(40.3) \quad [M, \mu\mu'] - [M, \mu] - [M, \mu'] \quad \text{for all } M \in \mathcal{P}(\Lambda), \mu, \mu' \in \text{Aut } M,$$

$$(40.4) \quad [M, \mu] - [L, \lambda] - [N, v]$$

for each ses

$$(40.5) \quad 0 \rightarrow (L, \lambda) \xrightarrow{f} (M, \mu) \xrightarrow{g} (N, v) \rightarrow 0$$

(see (38.25)). We are now ready to prove

**(40.6) Theorem.** *There is an isomorphism  $K_1(\Lambda) \cong K_{\det}(\Lambda)$ , which is induced by mapping each  $\mathbf{T} \in GL_n(\Lambda)$  onto  $\theta(\mathbf{T}) = [F, \varphi]$ , where  $F = \Lambda^{(n)}$  and where  $\varphi \in \text{Aut } F$  is determined by the matrix  $\mathbf{T}$ .*

*Proof.* We show first that  $\theta$  induces a homomorphism  $K_1(\Lambda) \rightarrow K_{\det}(\Lambda)$ , also denoted by  $\theta$ . To begin with,

$$\theta \begin{pmatrix} \mathbf{T} & \mathbf{0} \\ \mathbf{0} & 1 \end{pmatrix} = [F \oplus \Lambda, \varphi \oplus 1] = [F, \varphi] + [\Lambda, 1] = \theta(\mathbf{T}),$$

since  $[\Lambda, 1] = 0$  in  $K_{\det}(\Lambda)$  by (40.4). Therefore  $\theta$  induces a map  $GL(\Lambda) \rightarrow K_{\det}(\Lambda)$ , which is a homomorphism by (40.3). Further,  $\theta(GL'(\Lambda)) = 0$  since  $K_{\det}(\Lambda)$  is abelian, so we now have a homomorphism  $\theta: K_1(\Lambda) \rightarrow K_{\det}(\Lambda)$ .

We shall construct an inverse map  $\theta'$ . To begin with, consider a pair  $(M, \mu)$  with  $M \in \mathcal{P}(\Lambda)$ ,  $\mu \in \text{Aut } M$ . Choose  $N \in \mathcal{P}(\Lambda)$  so that  $M \oplus N = F$  is  $\Lambda$ -free, and then  $\mu \oplus 1 \in \text{Aut } F$ . Relative to some  $\Lambda$ -basis of  $F$ , this automorphism  $\mu \oplus 1$  determines a matrix  $\mathbf{T} \in GL(\Lambda)$ , and we define

$$\theta'(M, \mu) = \text{image of } \mathbf{T} \text{ in } K_1(\Lambda).$$

Changing the basis of  $F$  replaces  $\mathbf{T}$  by  $\mathbf{U}\mathbf{T}\mathbf{U}^{-1}$  for some  $\mathbf{U} \in GL(\Lambda)$ , and thus has no effect on the image of  $\mathbf{T}$  in  $K_1(\Lambda)$ .

Suppose now that  $M \oplus N = F'$  is free, and form  $\mu \oplus 1' \in \text{Aut } F'$ , which determines an element  $T' \in K_1(\Lambda)$ . In order to verify that  $T = T'$  in  $K_1(\Lambda)$ , we consider the pairs

$$(M \oplus N \oplus M \oplus N', \mu \oplus 1 \oplus 1 \oplus 1') \quad \text{and} \quad (M \oplus N \oplus M \oplus N', 1 \oplus 1 \oplus \mu \oplus 1').$$

In both pairs, the module which occurs is precisely  $F \oplus F'$ , and there is an isomorphism from one pair to the other, given by the map  $\mu^{-1} + 1 + \mu + 1'$ .

The first pair determines a matrix  $\begin{pmatrix} \mathbf{T} & \mathbf{0} \\ \mathbf{0} & \mathbf{I} \end{pmatrix}$ , the second  $\begin{pmatrix} \mathbf{I} & \mathbf{0} \\ \mathbf{0} & \mathbf{T}' \end{pmatrix}$ , so now we have

$$\begin{pmatrix} \mathbf{T} & \mathbf{0} \\ \mathbf{0} & \mathbf{I} \end{pmatrix} = \mathbf{U} \begin{pmatrix} \mathbf{I} & \mathbf{0} \\ \mathbf{0} & \mathbf{T}' \end{pmatrix} \mathbf{U}^{-1}$$

for some invertible  $\mathbf{U}$ . Therefore  $\begin{pmatrix} \mathbf{T} & \mathbf{0} \\ \mathbf{0} & \mathbf{I} \end{pmatrix}$  and  $\begin{pmatrix} \mathbf{I} & \mathbf{0} \\ \mathbf{0} & \mathbf{T}' \end{pmatrix}$  have the same image in  $K_1(\Lambda)$ , and consequently so do  $\mathbf{T}$  and  $\mathbf{T}'$ . This shows that  $\theta'(M, \mu)$  is well defined, independently of the choice of the complement of  $M$ .

It is obvious that

$$\theta'(M, \mu_1 \mu_2) = \theta'(M, \mu_1) \theta'(M, \mu_2), \quad \mu_i \in \text{Aut } M,$$

so it remains to check the behavior of  $\theta'$  on an expression of the form (40.4). Consider an exact sequence (40.5); complementing each of the modules so as to obtain a free module, we obtain a new exact sequence in which  $L, M$ , and  $N$  are  $\Lambda$ -free of finite rank, and we are trying to prove that  $\theta'$  annihilates the expression (40.4). Since the sequence  $0 \rightarrow L \rightarrow M \rightarrow N \rightarrow 0$  is  $\Lambda$ -split, we may write  $M = \bigoplus_{i=1}^m \Lambda e_i$ , where  $\{e_1, \dots, e_t\}$  are a basis for  $L$ , and the images of  $\{e_{t+1}, \dots, e_m\}$  are a basis for  $N$ . We now view  $f$  as an embedding, and  $g$  as a canonical surjection. The fact that  $f$  and  $g$  commute with the automorphisms of the free modules means that  $\mu$  can be represented by a matrix of the form

$$\mathbf{T} = \begin{pmatrix} \mathbf{T}_1 & \mathbf{U} \\ \mathbf{0} & \mathbf{T}_2 \end{pmatrix},$$

where  $\mathbf{T}_1$  represents  $\lambda$ , and  $\mathbf{T}_2$  represents  $v$ . But it is easily verified that both

$$\begin{pmatrix} \mathbf{T}_2 & \mathbf{0} \\ \mathbf{0} & \mathbf{T}_2^{-1} \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} \mathbf{I} & * \\ \mathbf{0} & \mathbf{I} \end{pmatrix}$$

lie in  $GL(\Lambda)$ . Therefore mod  $GL(\Lambda)$  we have (multiplicatively)

$$\mathbf{T} \equiv \begin{pmatrix} \mathbf{T}_1 \mathbf{T}_2 & \mathbf{0} \\ \mathbf{0} & \mathbf{I} \end{pmatrix} \equiv \mathbf{T}_1 \mathbf{T}_2.$$

Thus  $\mathbf{T} = \mathbf{T}_1 \mathbf{T}_2$  in  $K_1(\Lambda)$ , that is

$$\theta'(M, \mu) = \theta'(L, \lambda) \cdot \theta'(N, \nu)$$

for each ses (40.5). It thus follows that  $\theta'$  induces a well-defined homomorphism  $K_{\det}(\Lambda) \rightarrow K_1(\Lambda)$ . Since each element of  $K_{\det}(\Lambda)$  is of the form  $[F, \varphi]$  with  $F$  free, it is straightforward to prove that  $\theta$  and  $\theta'$  are inverses of one another, and the proof is complete.

**(40.7) Remarks.** (i) In some proofs involving  $K_1$ , it will be necessary to use the determinantal version as well as that given by (40.2).

(ii) Since  $K_{\det}(\Lambda)$  is defined categorically (see Exercise 3.12), so also is  $K_1(\Lambda)$ . In particular,  $K_1(\Lambda) \cong K_1(\Gamma)$  whenever the rings  $\Lambda$  and  $\Gamma$  are Morita equivalent. As a special case of this fact, an isomorphism  $\theta: \Lambda \cong M_r(\Gamma)$  induces an isomorphism  $\theta_*: K_1(\Lambda) = K_1(\Gamma)$ , defined by mapping each matrix  $(x_{ij}) \in GL_n(\Lambda)$  onto the matrix  $(\theta(x_{ij})) \in GL_{rn}(\Gamma)$ .

(iii) Given any ring homomorphism  $\varphi: \Lambda \rightarrow \Gamma$ , there is a commutative diagram

$$\begin{array}{ccc} K_1(\Lambda) & \xrightarrow{\varphi_*} & K_1(\Gamma) \\ \downarrow & & \downarrow \\ K_{\det}(\Lambda) & \xrightarrow{\varphi'} & K_{\det}(\Gamma) \end{array}$$

where the vertical arrows are the isomorphisms obtained in Theorem 40.6. Here,  $\varphi_*$  is induced by the map  $GL(\Lambda) \rightarrow GL(\Gamma)$ , and

$$\varphi'[M, \mu] = [\Gamma \otimes M, 1 \otimes \mu] \quad \forall \quad M \in \mathcal{P}(\Lambda), \quad \mu \in \text{Aut}_{\Lambda} M.$$

We leave the proof as an exercise for the reader.

(iv) By (38.51),  $K_1(\Lambda) \cong G_1(\Lambda)$  for any left regular ring  $\Lambda$ . More generally, let  $\Lambda$  be arbitrary, and let  $\mathcal{C}$  be the category of all f.g.  $\Lambda$ -modules of finite homological dimension. Then  $K_1(\Lambda) \cong K_{\det}(\mathcal{C})$  by (38.51).

(v) Let  $D$  be a division ring,  $D^{\#} = D^{\circ}/[D^{\circ}, D^{\circ}]$  (see (38.31)). The Dieudonné determinant induces an isomorphism  $K_1(D) \cong D^{\#}$ . If  $A = M_n(D)$  for some  $n$ , then

$$K_1(A) \cong K_1(D) \cong D^{\#}$$

(see (38.30)–(38.32)).

As a consequence of (40.6), we note

**(40.8) Corollary.** *For  $X, Y \in GL(\Lambda)$ , we have*

$$\begin{pmatrix} X & * \\ \mathbf{0} & Y \end{pmatrix} = \begin{pmatrix} X & \mathbf{0} \\ * & Y \end{pmatrix} = XY \quad \text{in } K_1(\Lambda).$$

### §40B. Localization Sequences

Our aim here is to obtain a localization sequence for  $K_0$  and  $K_1$  analogous to that given in (38.61) for Grothendieck groups. The sequence (38.62) played an important role in the calculation of Grothendieck groups of integral group rings. As we shall see, the corresponding sequence for  $K_1$  will be vital in the calculation of the locally free class group  $\text{Cl}(RG)$  of an integral group ring.

Throughout this section, let  $\Lambda$  be a left noetherian ring, and let  $S$  be a multiplicatively closed subset of the center of  $\Lambda$ , such that  $0 \notin S$  and  $1 \in S$ . We assume that  $\Lambda$  is  $S$ -torsionfree, and we let  $\Lambda' = S^{-1}\Lambda$ , the ring of quotients of  $\Lambda$  with denominators in  $S$ . Thus, the elements of  $\Lambda'$  are of the form  $x/s$ ,  $x \in \Lambda$ ,  $s \in S$ , with  $x/s = x_1/s_1$  if and only if  $s_1x = sx_1$  in  $\Lambda$ . The map  $x \rightarrow x/1$ ,  $x \in \Lambda$ , gives a ring monomorphism of  $\Lambda$  into  $\Lambda'$ , which we treat as an inclusion from now on.

(The reader should keep in mind the situation where  $\Lambda$  is an  $R$ -order over a Dedekind domain  $R$ , and  $S$  is a multiplicative subset of  $R$ . The hypotheses of the preceding paragraph are then automatically satisfied.)

The inclusion  $\Lambda \rightarrow \Lambda'$  induces homomorphisms of groups

$$K_0(\Lambda) \rightarrow K_0(\Lambda'), \quad K_1(\Lambda) \rightarrow K_1(\Lambda').$$

Let us define  $\mathcal{T}_d$  as the category of all f.g.  $S$ -torsion  $\Lambda$ -modules  $M$  such that  $\text{hd}_\Lambda(M) \leq d$ , and let

$$\mathcal{T} = \bigcup_{d=1}^{\infty} \mathcal{T}_d.$$

Thus  $\mathcal{T}$  is the category of all f.g.  $S$ -torsion  $\Lambda$ -modules of finite homological dimension over  $\Lambda$ . We form  $K_0(\mathcal{T})$ , the Grothendieck group of the category  $\mathcal{T}$ , generated by symbols  $[M]$  with  $M \in \mathcal{T}$ , and relations arising from all ses's from  $\mathcal{T}$ . We intend to prove

**(40.9) Localization Sequence.** *There is an exact sequence*

$$K_1(\Lambda) \xrightarrow{i_1} K_1(\Lambda') \xrightarrow{\delta} K_0(\mathcal{T}) \xrightarrow{i} K_0(\Lambda) \xrightarrow{i_0} K_0(\Lambda'),$$

where  $i_0, i_1$  are the maps induced by the inclusion  $\Lambda \rightarrow \Lambda'$ .

We begin the proof by establishing the following analogue of (38.50):

**(40.10) Lemma.** *For each  $d \geq 1$ , the inclusion  $\mathcal{T}_d \subseteq \mathcal{T}_{d+1}$  induces an iso-*

*morphism*

$$K_0(\mathcal{T}_d) \cong K_0(\mathcal{T}_{d+1}).$$

Thus there are isomorphisms

$$K_0(\mathcal{T}_1) \cong K_0(\mathcal{T}_2) \cong \cdots \cong K_0(\mathcal{T}).$$

*Proof.* Note that  $\mathcal{T}_0$  is empty, since each  $P \in \mathcal{P}(\Lambda)$  is  $S$ -torsionfree. Now let  $d \geq 1$ , and let

$$\varphi: K_0(\mathcal{T}_d) \rightarrow K_0(\mathcal{T}_{d+1})$$

come from the inclusion  $\mathcal{T}_d \subseteq \mathcal{T}_{d+1}$ . We shall construct a map

$$\psi: K_0(\mathcal{T}_{d+1}) \rightarrow K_0(\mathcal{T}_d)$$

inverse to  $\varphi$ , following the procedure in Step 3 of the proof of (38.45). Given  $M \in \mathcal{T}_{d+1}$ , choose  $s \in S$  so that  $sM = 0$ . Let

$$0 \rightarrow X \rightarrow F \xrightarrow{\theta} M \rightarrow 0$$

be  $\Lambda$ -exact, where  $F \cong \Lambda^{(k)}$ . Since  $\theta(sF) = 0$ ,  $\theta$  gives a map  $F/sF \rightarrow M$ , and there is a new exact sequence

$$(40.11) \quad 0 \rightarrow N \rightarrow F/sF \rightarrow M \rightarrow 0, \quad \text{where } N = X/(X \cap sF).$$

Then  $N$  is a f.g.  $S$ -torsion  $\Lambda$ -module (indeed,  $sN = 0$ ), and we claim that  $\text{hd}_\Lambda(N) \leq d$ . Consider the exact sequence

$$\cdots \rightarrow \text{Ext}^{d+1}(F/sF, *) \rightarrow \text{Ext}^{d+1}(N, *) \rightarrow \text{Ext}^{d+2}(M, *) \rightarrow \cdots.$$

The last term is 0 since  $\text{hd}_\Lambda(M) \leq d + 1$ . Also, the exactness of

$$0 \rightarrow F \xrightarrow{s} F \rightarrow F/sF \rightarrow 0$$

shows that  $\text{hd}(F/sF) \leq 1$ , and therefore  $\text{Ext}^{d+1}(F/sF, *) = 0$  because  $d \geq 1$ . This shows that  $\text{Ext}^{d+1}(N, *) = 0$ , so  $\text{hd}_\Lambda(N) \leq d$ .

We intend to define  $\psi$  by setting

$$(40.12) \quad \psi[M] = [F/sF] - [N] \in K_0(\mathcal{T}_d).$$

We must verify that  $\psi$  is well-defined. First of all, for fixed  $s$  the above expression for  $\psi[M]$  is independent of the choice of the sequence  $0 \rightarrow X \rightarrow F \rightarrow M \rightarrow 0$ , as

follows readily from Schanuel's Lemma applied to the sequence (40.11) of  $(\Lambda/s\Lambda)$ -modules. Next, to prove  $\psi[M]$  independent of  $s$ , suppose that  $t \in S$  is such that  $tM = 0$ . Using the same  $\theta$  as above, we obtain a new exact sequence

$$0 \rightarrow L \rightarrow F/stF \rightarrow M \rightarrow 0.$$

Now consider the commutative diagram with exact rows:

$$\begin{array}{ccccccc} 0 & \longrightarrow & L & \longrightarrow & F/stF & \longrightarrow & M \longrightarrow 0 \\ & & \alpha \downarrow & & \beta \downarrow & & 1 \downarrow \\ 0 & \longrightarrow & N & \longrightarrow & F/sF & \longrightarrow & M \longrightarrow 0. \end{array}$$

Since  $\beta$  is surjective, the Snake Lemma shows that  $\ker \alpha \cong \ker \beta$ , and also  $\alpha$  is surjective. But then

$$[L] - [N] = [F/stF] - [F/sF] \text{ in } K_0(\mathcal{T}_d).$$

(We have implicitly used the fact that  $\ker \alpha \in T_d$ ; see Exercise 38.11.) We obtain

$$\psi[M] = [F/sF] - [N] = [F/stF] - [L],$$

which shows that the image  $\psi[M]$  computed using  $s$  concides with that computed from  $st$ . This completes the proof that  $\psi[M]$  is independent of  $s$  and of the choice of the sequence  $0 \rightarrow X \rightarrow F \rightarrow M \rightarrow 0$ . Finally, the Horseshoe Lemma 38.39 shows that  $\psi$  preserves the relations which define  $K_0(\mathcal{T}_{d+1})$ , so  $\psi$  is a well-defined homomorphism from  $K_0(\mathcal{T}_{d+1})$  into  $K_0(\mathcal{T}_d)$ .

For  $M \in \mathcal{T}_d$ , formula (40.12) is just the assertion that  $\psi\varphi = 1$  on  $K_0(\mathcal{T}_d)$ , and so  $\varphi$  is injective. On the other hand, for  $M \in \mathcal{T}_{d+1}$ , the same formula shows that  $[M] \in \text{im } \varphi$ , whence  $\varphi$  is surjective. This completes the proof that  $\varphi$  is an isomorphism. The second assertion of the lemma is an immediate consequence of the first, and the lemma is established.

Continuing with the proof of (40.9), we note that each  $P \in \mathcal{P}(\Lambda)$  gives rise to a module  $P' \in \mathcal{P}(\Lambda')$ , where  $P' = \Lambda' \otimes_{\Lambda} P = S^{-1}P$ . Since  $P$  is  $S$ -torsionfree, the  $\Lambda$ -homomorphism  $P \rightarrow P'$  (given by  $p \mapsto 1 \otimes p$ ) is a monomorphism. We shall thus view  $P$  as a  $\Lambda$ -submodule of  $P'$  for which  $\Lambda'P = P'$ . To define the map  $\lambda: K_0(\mathcal{T}) \rightarrow K_0(\Lambda)$ , let  $M \in \mathcal{T}$  and write a  $\Lambda$ -exact sequence

$$(40.13) \quad 0 \rightarrow P_n \rightarrow \cdots \rightarrow P_0 \rightarrow M \rightarrow 0, \quad P_i \in \mathcal{P}(\Lambda).$$

Then put

$$\lambda[M] = [P_0] - [P_1] + \cdots \pm [P_n] \in K_0(\Lambda).$$

As in the proof of (38.42),  $\lambda$  is a well-defined homomorphism. Furthermore,  $\Lambda'$

is a flat  $\Lambda$ -module, and  $\Lambda' \otimes_{\Lambda} M = 0$  since  $M$  is a  $S$ -torsion module, so

$$0 \rightarrow P'_n \rightarrow \cdots \rightarrow P'_0 \rightarrow 0$$

is a  $\Lambda'$ -exact sequence. This proves that  $i_0 \lambda = 0$  in the Localization Sequence.

Next, let  $x = [P] - [Q] \in \ker i_0$ , where  $P, Q \in \mathcal{P}(\Lambda)$ . Then  $[P'] = [Q']$  in  $K_0(\Lambda')$ , so  $P'$  is stably isomorphic to  $Q'$ . Increasing both  $P$  and  $Q$  by  $\Lambda^{(k)}$  for some  $k$ , we may then assume that  $P' \cong Q'$ . Replacing  $P$  by an isomorphic copy, we may further suppose that  $P' = Q'$ . But then  $S^{-1}P = S^{-1}Q$ , so  $sP \subseteq Q$  for some  $s \in S$ . Then we have

$$x = [P] - [Q] = \lambda \{ [P/sP] - [Q/sP] \},$$

so  $\ker i_0 \subseteq \text{im } \lambda$ . This completes the proof that the sequence is exact at  $K_0(\Lambda)$ .

Now let  $P, Q \in \mathcal{P}(\Lambda)$  be such that  $P' = Q'$ , and let  $s \in S$  be such that  $sP \subseteq Q$ . We define

$$[P//Q] = [P/sP] - [Q/sP] \in K_0(\mathcal{T}).$$

If also  $tP \subseteq Q$  with  $t \in S$ , consider the  $\Lambda$ -exact sequences

$$0 \rightarrow sP/stP \rightarrow P/stP \rightarrow P/sP \rightarrow 0, \quad 0 \rightarrow sP/stP \rightarrow Q/stP \rightarrow Q/sP \rightarrow 0.$$

These give

$$[P/stP] - [Q/stP] = [P/sP] - [Q/sP] \quad \text{in } K_0(\mathcal{T}),$$

which shows that  $[P//Q]$  is independent of the choice of  $s \in S$  such that  $sP \subseteq Q$ . We note also that if  $R \in \mathcal{P}(\Lambda)$  is such that  $P' = Q' = R'$ , then

$$(40.14) \quad [P//Q] + [Q//R] = [P//R],$$

as is easily verified.

We are now ready to define the map  $\partial: K_1(\Lambda') \rightarrow K_0(\mathcal{T})$ . Let  $f \in GL_n(\Lambda')$  be viewed as an automorphism of  $(\Lambda')^n$  (the direct sum of  $n$  copies of  $\Lambda'$ ). We may then compute  $f\Lambda^n$ , by viewing  $\Lambda^n$  as submodule of  $(\Lambda')^n$ . Clearly  $f\Lambda^n \cong \Lambda^n$  as  $\Lambda$ -modules, and

$$S^{-1} \cdot f\Lambda^n = f(S^{-1}\Lambda^n) = f((\Lambda')^n) = (\Lambda')^{(n)}.$$

Thus  $\Lambda^n$  and  $f\Lambda^n$  lie in  $\mathcal{P}(\Lambda)$ , and generate the same  $\Lambda'$ -module, so  $[\Lambda^n//f\Lambda^n] \in K_0(\mathcal{T})$  is well-defined, by the earlier remarks. Let us put

$$\partial(f) = [\Lambda^n//f\Lambda^n], \quad f \in GL_n(\Lambda').$$

It is easily checked that  $\partial \begin{pmatrix} f & 0 \\ 0 & 1 \end{pmatrix} = \partial(f)$ , so  $\partial$  is well-defined on  $GL(\Lambda')$ . From

(40.14), we find at once that  $\partial$  is a homomorphism of groups. Since  $K_0(\mathcal{T})$  is abelian, there is thus a well-defined homomorphism  $\partial: K_1(\Lambda') \rightarrow K_0(\mathcal{T})$ , and obviously  $\partial$  annihilates  $\text{im } i_1$ , where  $i_1: K_1(\Lambda) \rightarrow K_1(\Lambda')$ .

Let us check next that  $\ker \lambda \subseteq \text{im } \partial$ , the reverse inclusion being obvious. Let  $x \in \ker \lambda$ ; using the isomorphism  $K_0(\mathcal{T}) \cong K_0(\mathcal{T}_1)$ , we may write

$$x = [P/Q] - [P_1/Q_1],$$

where all of the modules  $P, P_1, Q, Q_1 \in \mathcal{P}(\Lambda)$ , and where  $P' = Q', P'_1 = Q'_1$ . Then

$$0 = \lambda(x) = [P] + [Q_1] - [P_1] - [Q],$$

so  $P \oplus Q_1$  is stably isomorphic to  $P_1 \oplus Q$ . Increasing both  $P$  and  $Q$  by the same element of  $\mathcal{P}(\Lambda)$ , we may in fact assume that  $P \oplus Q_1$  is  $\Lambda$ -free, and that  $P \oplus Q_1 \cong P_1 \oplus Q$ . This isomorphism extends to an isomorphism  $f: P' \oplus Q'_1 \cong P'_1 \oplus Q'$ , so  $f$  is an automorphism of a free  $\Lambda'$ -module. We have then

$$x = [(P \oplus Q_1)/(P_1 \oplus Q)] = \partial(f),$$

which shows that  $\ker \lambda \subseteq \text{im } \partial$ , and that the Localization Sequence is exact at  $K_0(\mathcal{T})$ .

It remains for us to prove exactness at  $K_1(\Lambda')$ . Let  $f \in GL_n(\Lambda')$  be such that  $\partial(f) = 0$ , that is,  $[\Lambda^n // f\Lambda^n] = 0$  in  $K_0(\mathcal{T})$ . Choose  $s \in S$  such that  $sf\Lambda^n \subseteq \Lambda^n$ . Then

$$0 = [\Lambda^n // f\Lambda^n] = [\Lambda^n / sf\Lambda^n] - [\Lambda^n / s\Lambda^n]$$

by (40.14). We follow the approach in Bass [74, §10]: put  $Q = \Lambda^n$ ,  $g = sf \in \text{End}_{\Lambda} Q$ , so now

$$(40.15) \quad [Q/gQ] = [Q/sQ] \quad \text{in } K_0(\mathcal{T}_1), \quad \text{and} \quad f = g/s \quad \text{in } K_1(\Lambda').$$

*Case 1:* Suppose first that there is a  $\Lambda$ -isomorphism  $\gamma: Q/gQ \cong Q/sQ$ , and set  $P = Q \oplus Q$ . Let

$$g' = g \oplus 1, \quad s' = s \oplus 1, \quad \text{so} \quad P/g'P \cong Q/gQ, \quad P/s'P \cong Q/sQ,$$

and  $\gamma$  gives rise to an isomorphism  $\gamma': P/g'P \cong P/s'P$ . As in Step 2 of the proof of (38.45), the isomorphism  $\gamma'$  lifts to a pair of isomorphisms  $\gamma_1$  and  $\gamma_0$  such that the following diagram commutes:

$$\begin{array}{ccccccc} 0 & \longrightarrow & P & \xrightarrow{g'} & P & \longrightarrow & P/g'P \longrightarrow 0 \\ & & \downarrow \gamma_1 & & \downarrow \gamma_0 & & \downarrow \gamma' \\ 0 & \longrightarrow & P & \xrightarrow{s'} & P & \longrightarrow & P/s'P \longrightarrow 0. \end{array}$$

Thus

$$s'\gamma_1 = \gamma_0 g' \quad \text{in} \quad K_1(\Lambda'),$$

and so

$$s\gamma_1 = \gamma_0 g \quad \text{in} \quad K_1(\Lambda') \quad \text{since} \quad s' = s \oplus 1, \quad g' = g \oplus 1.$$

Therefore we have

$$f = g/s = \gamma_1/\gamma_0 \in \text{image of } i_1,$$

as desired.

*Case 2:* We are now ready to treat the general case. From (40.15) and Proposition 38.21, it follows that there exists a pair of  $\Lambda$ -exact sequences (of modules in  $\mathcal{T}_1$ ):

$$0 \rightarrow X_1 \rightarrow X \rightarrow X_2 \rightarrow 0, \quad 0 \rightarrow X_1 \rightarrow Y \rightarrow X_2 \rightarrow 0,$$

such that

$$(40.16) \quad X \oplus (Q/gQ) \cong Y \oplus (Q/sQ).$$

Since  $X_1 \in \mathcal{T}_1$ , we may write  $X_1 = P_0/P_1$ , where  $P_0, P_1 \in \mathcal{P}(\Lambda)$  and  $P_1 \subseteq P_0$ . Then  $tP_0 \subseteq P_1$  for some  $t \in S$ , since  $X$  is  $S$ -torsion. Put  $P = P_0 \oplus P_1$ , and let  $\alpha \in \text{End}_\Lambda P$  be defined by

$$\alpha(p_0, p_1) = (p_1, sp_0), \quad p_i \in P_i.$$

Then  $\alpha$  is injective, and

$$P/\alpha P \cong (P_0/P_1) \oplus (P_1/sP_0) = X_1 \oplus \tilde{X}_1, \quad \text{say},$$

where  $\tilde{X}_1 = P_1/sP_0 \in \mathcal{T}_1$ . Increasing  $X_1, X$  and  $Y$  by the summand  $\tilde{X}_1$  and changing notation, we may now assume that  $X_1 = P_1/\alpha_1 P_1$  for some  $P_1 \in \mathcal{P}(\Lambda)$  and  $\alpha_1 \in \text{End } P_1$ . Likewise, we may assume that  $X_2 = P_2/\alpha_2 P_2$  for some  $P_2 \in \mathcal{P}(\Lambda)$  and  $\alpha_2 \in \text{End } P_2$ . By the Horseshoe Lemma, we can then construct projective resolutions of  $X$  and  $Y$ , obtaining a pair of commutative diagrams:

$$\begin{array}{ccccc} P_1 & \longrightarrow & P & \longrightarrow & P_2 \\ \alpha_1 \downarrow & & \gamma \downarrow & & \alpha_2 \downarrow \\ P_1 & \longrightarrow & P & \longrightarrow & P_2 \\ \downarrow & & \downarrow & & \downarrow \\ X_1 & \longrightarrow & X & \longrightarrow & X_2, & \quad & P_1 & \longrightarrow & P & \longrightarrow & P_2 \\ & & & & & & \alpha_1 \downarrow & & \delta \downarrow & & \alpha_2 \downarrow \\ & & & & & & P_1 & \longrightarrow & P & \longrightarrow & P_2 \\ & & & & & & \downarrow & & \downarrow & & \downarrow \\ & & & & & & X_1 & \longrightarrow & Y & \longrightarrow & X_2, \end{array}$$

where for each consecutive pair of horizontal (or vertical) arrows, the first arrow is injective and the second surjective. Identifying  $K_1(\Lambda')$  with the additive group

$K_{\det}(\Lambda')$ , we then obtain

$$[\gamma] = [\alpha_1] + [\alpha_2] = [\delta] \quad \text{in} \quad K_{\det}(\Lambda').$$

We now have a pair of  $\Lambda$ -exact sequences

$$0 \longrightarrow P \oplus Q \xrightarrow{\gamma \oplus g} P \oplus Q \longrightarrow X \oplus (Q/gQ) \longrightarrow 0,$$

$$0 \longrightarrow P \oplus Q \xrightarrow{\delta \oplus s} P \oplus Q \longrightarrow Y \oplus (Q/sQ) \longrightarrow 0,$$

in which the last terms are isomorphic by (40.16). It follows from Case 1 that the elements  $[\gamma] + [g]$  and  $[\delta] + [s]$  in  $K_{\det}(\Lambda')$  are such that their difference lies in  $\text{im } i_1$ . But then

$$[f] = [g] - [s] = [g] + [\gamma] - [s] - [\delta] \in \text{im } i_1,$$

which completes the proof that  $\ker \partial \subseteq \text{im } i_1$ . This establishes the exactness of the Localization Sequence.

**(40.17) Corollary.** *Let  $S$  be a multiplicative subset of the commutative ring  $R$ , let  $\Lambda$  be an  $R$ -algebra which is  $S$ -torsionfree and is a left noetherian ring,\* and set  $\Lambda' = S^{-1}\Lambda$ . Then the sequence*

$$K_1(\Lambda) \rightarrow K_1(\Lambda') \rightarrow K_0(\mathcal{T}) \rightarrow K_0(\Lambda) \rightarrow K_0(\Lambda')$$

*is exact, where  $\mathcal{T}$  is the category of all f.g.  $S$ -torsion  $\Lambda$ -modules of finite homological dimension over  $\Lambda$ .*

**(40.18) Remark.** Quillen [73] has defined a sequence of groups  $\{K_n^Q(\mathcal{C}) : n = 0, 1, \dots\}$  for certain categories  $\mathcal{C}$ . When  $\mathcal{C} = \mathcal{P}(\Lambda)$ , his  $K_n$  coincides with our  $K_n(\Lambda)$ ,  $n = 0, 1$ . On the other hand, when  $\mathcal{C} = {}_{\Lambda}^{\text{mod}}$ , his  $K_0^Q$  coincides with our  $G_0(\Lambda)$ , but  $K_1^Q$  need not coincide with our  $G_1(\Lambda)$ . It turns out that our Localization Sequence 40.9 is a special case of the following Localization Sequence due to Quillen:

$$\begin{aligned} \cdots &\rightarrow K_2(\mathcal{T}) \rightarrow K_2(\Lambda) \rightarrow K_2(\Lambda') \rightarrow K_1(\mathcal{T}) \rightarrow K_1(\Lambda) \rightarrow K_1(\Lambda') \\ &\rightarrow K_0(\mathcal{T}) \rightarrow K_0(\Lambda) \rightarrow K_0(\Lambda'). \end{aligned}$$

For details, we refer the reader to Stein [76], and in particular to the theorem on p. 233 in Grayson's exposition of Quillen's work.

**(40.19) Remark.** The sequence (40.9) is also a special case of a more general

\*This hypothesis certainly holds if  $\Lambda$  is f.g./R and  $R$  is noetherian.

result due to Swan (see Swan [68]). (However, this general result does *not* usually extend to the higher  $K$ -theory.) Swan's work deals with the following situation: let  $\varphi: \Lambda \rightarrow \Lambda'$  be any homomorphism of rings. Then  $\varphi$  induces homomorphisms

$$K_0(\Lambda) \rightarrow K_0(\Lambda'), \quad K_1(\Lambda) \rightarrow K_1(\Lambda'),$$

by means of the “change of rings” map  $\Lambda' \otimes_{\Lambda} *$ . Then there is an exact sequence of groups

$$(40.20) \quad K_1(\Lambda) \rightarrow K_1(\Lambda') \xrightarrow{\vartheta} K_0(\Lambda, \varphi) \xrightarrow{\lambda} K_0(\Lambda) \rightarrow K_0(\Lambda'),$$

where  $K_0(\Lambda, \varphi)$  is a “relative”  $K_0$ . The relative group is defined by generators and relations, as follows. Consider triples  $(M, f, N)$  with  $M, N \in \mathcal{P}(\Lambda)$ ,  $f: \Lambda' \otimes_{\Lambda} M \cong \Lambda' \otimes_{\Lambda} N$ . For brevity, let  $M' = \Lambda' \otimes_{\Lambda} M$ , etc. A *morphism*

$$(\mu, v): (M, f, N) \rightarrow (M_1, f_1, N_1)$$

consists of a pair of maps  $\mu, v$ , where  $\mu \in \text{Hom}_{\Lambda}(M, M_1)$ ,  $v \in \text{Hom}_{\Lambda}(N, N_1)$ , such that the diagram

$$\begin{array}{ccc} M' & \xrightarrow{f} & N' \\ 1 \otimes \mu \downarrow & & \downarrow 1 \otimes v \\ M'_1 & \xrightarrow{f_1} & N'_1 \end{array}$$

commutes. If both  $\mu$  and  $v$  are isomorphisms, we write  $(M, f, N) \cong (M_1, f_1, N_1)$ .

A *short exact sequence* (ses) of triples is a sequence

$$(40.21) \quad 0 \rightarrow (M_1, f_1, N_1) \xrightarrow{(\mu_1, v_1)} (M_2, f_2, N_2) \xrightarrow{(\mu_2, v_2)} (M_3, f_3, N_3) \rightarrow 0$$

such that each pair  $(\mu_i, v_i)$  is a morphism, and where

$$0 \rightarrow M_1 \xrightarrow{\mu_1} M_2 \xrightarrow{\mu_2} M_3 \rightarrow 0, \quad 0 \rightarrow N_1 \xrightarrow{v_1} N_2 \xrightarrow{v_2} N_3 \rightarrow 0$$

are  $\Lambda$ -exact.

Given a pair of triples  $(L, f, M)$  and  $(M, g, N)$ , we may form a new triple  $(L, gf, N)$ . We now define  $K_0(\Lambda, \varphi)$  as the free abelian group generated by all isomorphism classes of triples, modulo the relations

$$(L, gf, N) = (L, f, M) + (M, g, N)$$

and

$$(M_2, f_2, N_2) = (M_1, f_1, N_1) + (M_3, f_3, N_3)$$

for each ses (40.21).

The map  $\lambda$  in (40.20) is defined by

$$\lambda[M, f, N] = [M] - [N],$$

while the map  $\partial$  is given by

$$\partial(f) = [\Lambda^n, f, \Lambda^n] \quad \text{for } f \in GL_n(\Lambda'),$$

and where brackets denote elements in  $K_0(\Lambda, \varphi)$  corresponding to triples.

We leave it as an exercise for the reader to verify that the sequence (40.20) is exact. The reader may also check that in the special case where  $\varphi: \Lambda \rightarrow \Lambda'$  with  $\Lambda' = S^{-1}\Lambda$ , the group  $K_0(\mathcal{T})$  occurring in (40.9) is isomorphic to the relative group  $K_0(\Lambda, \varphi)$ .

We shall encounter the sequence (40.20) again in §44, in our discussion of relative  $K$ -theory.

#### §40C. Elementary Matrices

Let  $R$  be an arbitrary ring. As usual, an *elementary matrix* in  $GL_n(R)$  is a matrix obtained from the identity matrix by replacing some off-diagonal zero entry by some element of  $R$ . Let  $E_n(R)$  be the subgroup of  $GL_n(R)$  generated by all elementary matrices. We define

$$GL(R) = \bigcup_{n=1}^{\infty} GL_n(R), \quad E(R) = \bigcup_{n=1}^{\infty} E_n(R),$$

where the embedding of  $GL_n(R)$  into  $GL_{n+1}(R)$  is given by  $\alpha \rightarrow \begin{pmatrix} \alpha & 0 \\ 0 & 1 \end{pmatrix}$ ,  $\alpha \in GL_n(R)$ . Call  $E(R)$  the *elementary subgroup* of the general linear group  $GL(R)$ .

We set

$$(40.22) \quad E_{ij}(a) = \mathbf{I} + a\mathbf{e}_{ij} \quad \text{for } 1 \leq i, j \leq n, \quad i \neq j, \quad a \in R,$$

where  $\mathbf{e}_{ij}$  is the matrix unit with 1 at position  $(i, j)$  and zeros elsewhere. (We have suppressed the symbol  $n$  indicating the sizes of the matrices.) Put

$$[\mathbf{X}, \mathbf{Y}] = \mathbf{XYX}^{-1}\mathbf{Y}^{-1} = \text{commutator of } \mathbf{X} \text{ and } \mathbf{Y}, \quad \text{for } \mathbf{X}, \mathbf{Y} \in GL(R).$$

It is easily checked that the elementary matrices  $\{E_{ij}(a)\}$  satisfy the following *Steinberg relations*, for  $a, b \in R$  and  $1 \leq i, j, k, l \leq n$ :

$$(40.23) \quad \begin{cases} E_{ij}(a)E_{ij}(b) = E_{ij}(a+b), & i \neq j, \\ [E_{ij}(a), E_{kl}(b)] = 1 & \text{if } i \neq j, \quad k \neq l \quad \text{and} \quad j \neq k, \quad i \neq l, \\ [E_{ij}(a), E_{jk}(b)] = E_{ik}(ab) & \text{if } i, j, k \text{ are distinct.} \end{cases}$$

The third relation gives

$$[E_n(R), E_n(R)] = E_n(R) \quad \text{if } n \geq 3.$$

Thus, for  $n \geq 3$ ,  $E_n(R)$  is a *perfect* group (that is, it coincides with its commutator subgroup). It follows at once that  $E(R)$  is also a perfect group.

**(40.24) Whitehead's Lemma.** *We have  $E(R) = GL'(R)$ .*

*Proof.* For  $n \geq 3$ ,  $E_n(R) = [E_n(R), E_n(R)] \subseteq GL'(R)$ . For the reverse inclusion, let  $\alpha, \beta \in GL_n(R)$ ; then

$$\begin{pmatrix} \alpha\beta\alpha^{-1}\beta^{-1} & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} \alpha & 0 \\ 0 & \alpha^{-1} \end{pmatrix} \begin{pmatrix} \beta & 0 \\ 0 & \beta^{-1} \end{pmatrix} \begin{pmatrix} (\beta\alpha)^{-1} & 0 \\ 0 & \beta\alpha \end{pmatrix}.$$

Now use the identity

$$(40.25) \quad \begin{pmatrix} \varphi & 0 \\ 0 & \varphi^{-1} \end{pmatrix} = \begin{pmatrix} 1 & \varphi^{-1} \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & \varphi^{-1}-1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ -\varphi & 1 \end{pmatrix}$$

for each  $\varphi \in GL_n(R)$ . Then we have

$$GL'_n(R) \subseteq E_{2n}(R) \quad \text{for all } n \geq 1,$$

whence  $GL'(R) \subseteq E(R)$  as desired.

**(40.26) Corollary.** *For each  $R$ ,  $E(R) \trianglelefteq GL(R)$  and*

$$K_1(R) \cong GL(R)/E(R).$$

**Remarks.** It is easy to give examples in which  $E_2(R)$  is not normal in  $GL_2(R)$ . Suslin recently proved, however, that

$$E_n(R) \trianglelefteq GL_n(R) \quad \text{if } n \geq 3 \quad \text{and } R \text{ is commutative.}$$

For a proof, see McDonald [84, Th. I. 17].

Each element  $x$  of  $K_1(R)$  can be represented by a matrix  $X \in GL_n(R)$  for some  $n$ . If  $P$  and  $Q$  are products of elementary matrices, then by (40.26) we have  $X = PQ$  in  $K_1(R)$ . We may try to choose  $P$  and  $Q$  so that  $PQ$  has a simpler form than  $X$ ; for example, if  $PQ = \begin{pmatrix} Y & \mathbf{0} \\ \mathbf{0} & 1 \end{pmatrix}$  for some  $Y \in GL_{n-1}(R)$ , then  $x$  is also represented by the element  $Y$ . For later calculations, it will be important to know how to choose  $n$  so that every element of  $K_1(R)$  is represented by an element of  $GL_n(R)$ . In other words, we wish to find  $n$  such that the map  $GL_n(R) \rightarrow$

$K_1(R)$ , given by  $GL_n(R) \rightarrow GL(R) \rightarrow K_1(R)$ , is a surjection. We have also the difficult question of finding the kernel of this surjection.

Suppose for the moment that  $R$  is a commutative ring, and let  $R^\times$  denote its group of units. The determinant map  $\det: GL_n(R) \rightarrow R^\times$  obviously extends to a surjective homomorphism

$$\det: K_1(R) \rightarrow R^\times.$$

Let  $SK_1(R)$  denote the kernel of this map; this notation is suggested by the usual notation  $SL(R)$  for the *special linear group*:

$$SL(R) = \{\mathbf{X} \in GL(R) : \det \mathbf{X} = 1\}.$$

The surjection  $\det: K_1(R) \rightarrow R^\times$  is split by the homomorphism

$$\theta: R^\times \rightarrow K_1(R), \quad \text{given by } \theta(x) = (x), \quad x \in R^\times,$$

and  $\theta$  is obviously injective. We have then

$$(40.27) \quad K_1(R) \cong R^\times \times SK_1(R)$$

for any commutative ring  $R$ . For those cases where the map  $\theta$  is also surjective, we obtain

$$(40.28) \quad K_1(R) \cong R^\times, \quad SK_1(R) = 1.$$

For example, this holds for any (commutative) euclidean domain  $R$ , since each  $\mathbf{X} \in GL_n(R)$  can be diagonalized by elementary row and column operations. Therefore each  $x \in K_1(R)$  is representable by a diagonal matrix  $\text{diag}(a_1, \dots, a_n)$ ,  $a_i \in R^\times$ , for some  $n$ . Since

$$(40.29) \quad \text{diag}(a_1, \dots, a_n) = \text{diag}(1, \dots, 1, a_1 \cdots a_n) = a_1 \cdots a_n \text{ in } K_1(R)$$

by virtue of (40.24), it follows that  $R^\times$  maps onto  $K_1(R)$ , and so (40.28) holds in this case.

Returning to the case where  $R$  is any commutative ring, we note finally that

$$SK_1(R) \cong SL(R)/E(R).$$

**(40.30) Remark.** A deep theorem of Bass-Milnor-Serre (see (38.55)) asserts that  $SK_1(R) = 1$  for every Dedekind domain  $R$  whose quotient field is a global field. On the other hand, there are examples of P.I.D.'s  $R$  for which  $SK_1(R) \neq 1$ , so the calculation of  $SK_1$  may be rather complicated, even for relatively well-behaved domains  $R$ .

We now drop the assumption that  $R$  is commutative, and consider the

question as to when  $R^\cdot \rightarrow K_1(R)$  is surjective. We have seen in §7D that this is the case when  $R$  is any skewfield. We shall now establish Bass's generalization of this result:

**(40.31) Theorem.** *Let  $R$  be a semilocal ring, that is, a ring for which  $R/\text{rad } R$  is semisimple artinian. Then the map  $R^\cdot \rightarrow K_1(R)$  is surjective, that is, each element of  $K_1(R)$  is of the form  $(u)$  for some  $u \in R^\cdot$ .*

*Proof.* Suppose that  $R = L + Rb$  for some left ideal  $L$  of  $R$  and some  $b \in R$ . If bars denote reduction mod  $\text{rad } R$ , then  $\bar{R}$  is a semisimple ring, and  $\bar{R} = \bar{L} + \bar{R}b$ . By Exercise 40.1, there exists an element  $y \in \bar{L}$  with  $y + \bar{b} \in \bar{R}^\cdot$ . Therefore  $x + b \in R^\cdot$  for some  $x \in L$ , by Exercise 5.2. We shall use these facts below.

An  $n$ -tuple  $\mathbf{a} = {}^t(a_1, \dots, a_n)$  of elements of  $R$  is called *unimodular* if  $\sum_{i=1}^n Ra_i = R$ . If  $\mathbf{X} \in GL_n(R)$ , then from  $\mathbf{X}^{-1}\mathbf{X} = \mathbf{I}$  it follows that every column of  $\mathbf{X}$  is unimodular. If  $\mathbf{x} = {}^t(x_1, \dots, x_n)$  is the first column of  $\mathbf{X}$ , and  $\mathbf{E}_{ij}(a)$  is as in (40.22), the first column of  $\mathbf{E}_{ij}(a)\mathbf{X}$  is

$${}^t(x_1, \dots, x_{i-1}, x_i + ax_j, x_{i+1}, \dots, x_n).$$

We write  $\mathbf{x} \sim \mathbf{x}'$  if the vector  $\mathbf{x}'$  can be obtained from  $\mathbf{x}$  by a finite number of such elementary (row) operations. If  $n \geq 2$  and  $x_1 \in R^\cdot$ , it is clear from (40.25) that

$$(40.32) \quad {}^t(x_1, \dots, x_n) \sim {}^t(1, 0, \dots, 0).$$

We use these ideas to show that when  $R$  is semilocal, every unimodular  $\mathbf{x} = {}^t(x_1, \dots, x_n)$  is equivalent to  ${}^t(1, 0, \dots, 0)$  if  $n \geq 2$ . By hypothesis,  $Rx_1 + \dots + Rx_n = R$ ; by the first step in the proof, we obtain

$$a_1x_1 + \dots + a_{n-1}x_{n-1} + x_n \in R^\cdot$$

for some elements  $a_i \in R$ . Then

$$\mathbf{x} \sim {}^t(x_1, \dots, x_{n-1}, a_1x_1 + \dots + a_{n-1}x_{n-1} + x_n) \sim {}^t(1, 0, \dots, 0).$$

as desired.

In matrix form, let  $\mathbf{X} \in GL_n(R)$  with  $n \geq 2$ . By the above, there exists a product  $\mathbf{E}$  of elementary matrices, such that

$$\mathbf{EX} = \begin{pmatrix} 1 & * \\ \mathbf{0} & \mathbf{X}_1 \end{pmatrix} \quad \text{for some } \mathbf{X}_1 \in GL_{n-1}(R).$$

But then  $\mathbf{X}$  and  $\mathbf{X}_1$  represent the same element of  $K_1(R)$ , by (40.8). Continuing this procedure with  $\mathbf{X}_1$  (if  $n \geq 3$ ), we eventually obtain  $\mathbf{X} = (u)$  in  $K_1(R)$  for some  $u \in R^\cdot$ . This completes the proof.

**(40.32) Remarks.** (i) If  $R$  is semilocal, the surjection  $R^\cdot \rightarrow K_1(R)$  induces a

surjection

$$R^\# = R^\cdot / [R^\cdot, R^\cdot] \rightarrow K_1(R).$$

If  $R$  is a skewfield, or more generally a local ring, this surjection is an isomorphism, with inverse the Dieudonné determinant (see remarks at the end of §38B).

(ii) Vaserstein [69] proved that if  $R$  is semilocal, the kernel of the surjection  $R^\cdot \rightarrow K_1(R)$  is the subgroup of  $R^\cdot$  generated by all expressions  $(1 + xy)(1 + yx)^{-1}$  in  $R^\cdot$  (for  $x, y \in R$ ). A proof is given in Silvester [81, Prop. 53]; see also Swan [71, §2].

#### §40D. Unimodular Rows and Stably Free Modules

We shall introduce here the concept of the stable range of an arbitrary ring  $A$ . As we shall see, if  $A$  has stable range  $d$  then every element of  $K_1(A)$  can be represented by a matrix in  $GL_d(A)$ . Every semilocal ring has stable range 1, while a Dedekind domain  $R$  has stable range  $\leq 2$ . Further, every  $R$ -order also has stable range  $\leq 2$ .

We denote the external direct sum of  $n$  copies of  $A$  by  $A^n$  rather than  $A^{(n)}$ , for convenience. Let

$$\mathbf{e}_i = (0, \dots, 0, 1, 0, \dots, 0), \quad 1 \text{ in } i\text{-th place}, \quad 1 \leq i \leq n,$$

so  $A^n = \bigoplus \mathbf{e}_i A$  as right  $A$ -modules. An element  $\mathbf{a} = (a_1, \dots, a_n) \in A^n$  is *unimodular* if  $\sum_{i=1}^n Aa_i = A$ .

**(40.33) Lemma.** *Let  $\mathbf{a} \in A^n$ . Then  $\mathbf{a}$  is unimodular if and only if  $\mathbf{a}A$  is a free direct summand of  $A^n$  of rank 1.*

*Proof.* If  $\mathbf{a}$  is unimodular, there exist elements  $b_i \in A$  with  $\sum b_i a_i = 1$ . The inclusion  $\mathbf{a}A \subseteq A^n$  is split by the map  $\varphi: A^n \rightarrow \mathbf{a}A$ , where  $\varphi(\mathbf{e}_i) = \mathbf{a}b_i$ ,  $1 \leq i \leq n$ . Thus  $\mathbf{a}A$  is a direct summand of  $A^n$ . Further, the surjection  $A \rightarrow \mathbf{a}A$  is monic, since if  $\mathbf{ax} = 0$  with  $x \in A$ , then  $x = \sum b_i a_i x = 0$ . Thus  $\mathbf{a}A$  is  $A$ -free of rank 1.

Conversely, suppose  $\mathbf{a}A$  is a free summand of  $A^n$ , and let  $\varphi: A^n \rightarrow \mathbf{a}A$  split the inclusion map. Setting  $\varphi(\mathbf{e}_i) = \mathbf{a}b_i$ ,  $1 \leq i \leq n$ , we find that  $\mathbf{a} = \mathbf{a} \cdot \sum b_i a_i$ , so  $\sum b_i a_i = 1$  because  $\mathbf{a}A \cong A$ . Thus  $\mathbf{a}$  is unimodular.

Suppose now that  $\mathbf{a} \in A^n$  is unimodular, and write

$$A^n = \mathbf{a}A \oplus P \quad \text{for some } P \in \mathcal{P}(A).$$

Obviously  $P \cong A^n/\mathbf{a}A$ , and we wish to decide whether  $P \cong A^{n-1}$ . We now show

**(40.34) Proposition.** *Let  $A^n = \mathbf{a}A \oplus P$ , where  $\mathbf{a}$  is a unimodular row vector. Then  $P \cong A^{n-1}$  if and only if  $'\mathbf{a}$  can be completed to a matrix in  $GL_n(A)$ .*

*Proof.* If  $P = \bigoplus_{i=2}^n \mathbf{e}'_i A$  is  $A$ -free, then  $A^n$  has two sets of free generators, namely,

$$\{\mathbf{e}_1, \dots, \mathbf{e}_n\} \quad \text{and} \quad \{\mathbf{a}, \mathbf{e}'_2, \dots, \mathbf{e}'_n\}.$$

Hence there exists an  $f \in \text{Aut } A^n$  such that

$$f(\mathbf{e}_1) = \mathbf{a}, \quad f(\mathbf{e}_2) = \mathbf{e}'_2, \dots, \quad f(\mathbf{e}_n) = \mathbf{e}'_n.$$

Let  $f(\mathbf{e}_i) = \sum_j \mathbf{e}_j a_{ij}$ , and put  $\mathbf{F} = (a_{ij}) \in GL_n(A)$ . Then ' $\mathbf{a}$ ' is the first column of the invertible matrix  $\mathbf{F}$ .

Conversely, if ' $\mathbf{a} = \mathbf{F}' \mathbf{e}_1$  for some  $\mathbf{F} \in GL_n(A)$ , then there exists an  $f \in \text{Aut } A^n$  such that  $f(\mathbf{e}_1) = \mathbf{a}$ . Therefore

$$P \cong A^n / \mathbf{a} A \cong f(A^n) / f(\mathbf{a} A) = A^n / \mathbf{e}_1 A \cong A^{n-1},$$

as desired.

**Caution.** For  $A$  noncommutative,  $\mathbf{X} \in GL_n(A)$  need not imply that ' $\mathbf{X} \in GL_n(A)$ .

In order to simplify our discussion, we assume once and for all that the ring  $A$  has the *invariant basis number* property, that is, for positive integers  $m$  and  $n$ ,

$$A^m \cong A^n \Rightarrow m = n.$$

This is certainly the case when  $A$  is any right artinian ring. It also holds when  $A$  is an  $R$ -algebra, f.g./ $R$  as module, where  $R$  is a commutative ring. To prove this, let  $P$  be any maximal ideal of  $R$ , so the localization  $R_P$  is a local ring with residue class field  $\bar{R} = R/P$ . Then  $A_P$  is an  $R_P$ -algebra, and by (5.22)  $\bar{A} = A_P/\text{rad } A_P$  is an f.d. semisimple  $\bar{R}$ -algebra. Then

$$A^m \cong A^n \Rightarrow \bar{A}^m \cong \bar{A}^n \Rightarrow m = n.$$

Let  $P, Q \in \mathcal{P}(A)$ ; call  $P$  and  $Q$  *stably isomorphic* if

$$(40.35) \quad P \oplus A^n \cong Q \oplus A^n \quad \text{for some } n.$$

We cannot conclude in general that  $P \cong Q$ , not even when  $A$  is commutative. A counterexample due to Kaplansky is given as follows. Let

$$A = \mathbb{R}[x, y, z]/(x^2 + y^2 + z^2 - 1), \quad \mathbb{R} = \text{real field}.$$

Here, the triple  $\mathbf{a} = (x, y, z)$  is unimodular, but cannot be completed to a matrix in  $GL_3(A)$ . Thus we have  $P \cong A^3 / \mathbf{a} A$ ,  $A^3 \cong \mathbf{a} A \oplus P \cong A \oplus P$ , but  $P$  is not  $A$ -free.

A module  $P \in \mathcal{P}(A)$  is called *stably free* if  $P \oplus A^m \cong A^n$  for some  $m, n$ . The preceding example shows that stably free modules need not be free.

On the other hand, if  $A$  is any semisimple ring, or more generally any semilocal ring, then stable isomorphism implies isomorphism, as we now prove. Let bars denote reduction modulo  $\text{rad } A$ , so  $\bar{A}$  is a semisimple artinian ring. From (40.35) we obtain

$$\bar{P} \oplus \bar{A}^n \cong \bar{Q} \oplus \bar{A}^n,$$

where  $\bar{P} \cong \bar{Q}$  since  $\bar{A}$  is artinian. But then  $P \cong Q$  by (6.6). We may further note that for each unimodular row  $\mathbf{a} \in A^{(n)}$ , there exists an  $\mathbf{E} \in E_n(A)$  such that  $\mathbf{E}'\mathbf{a} = {}^t\mathbf{e}_1$ , by the proof of (40.31), stated in terms of rows rather than columns. Thus  $'\mathbf{a}$  is the first column of  $\mathbf{E}^{-1}$ , so by (40.34) it follows from  $A^n \cong A \oplus P$  that  $P \cong A^{(n-1)}$ . This implies at once that every stably free  $A$ -module is free, for this case where  $A$  is semilocal.

The proof of (40.31) suggests a possible technique for attempting to complete a unimodular row  $\mathbf{a}$  to an invertible matrix. We consider operations of the form

$$(40.36) \quad (a_1, \dots, a_n) \rightarrow (a_1, \dots, a_i + xa_j, \dots, a_n), \quad x \in A, \quad i \neq j.$$

Such *elementary operations* on  $n$ -tuples do not affect the left ideal generated by their entries, and so preserve unimodularity. We write  $\mathbf{a} \sim \mathbf{b}$  if  $\mathbf{b}$  is obtained from  $\mathbf{a}$  by a sequence of such transformations. This gives

$$\mathbf{a} \sim \mathbf{b} \text{ if and only if } {}^t\mathbf{b} = \mathbf{E}'\mathbf{a} \text{ for some } \mathbf{E} \in E_n(A).$$

In particular,  $'\mathbf{a}$  is the first column of a matrix in  $GL_n(A)$  if and only if the same holds true for  $'\mathbf{b}$ .

We note next that for  $n \geq 2$ ,

$$(40.37) \quad (y_1, \dots, y_n) \sim (1, 0, \dots, 0) \quad \text{if some } y_i \in A^\perp.$$

This is almost obvious, apart from the question of permuting entries by elementary operations. But this can be done, by use of the identity

$$(40.38) \quad \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in E_2(R),$$

together with (40.25).

**(40.39) Definition.** We say that an arbitrary ring  $A$  satisfies the *stable range condition*  $S_{d+1}(A)$ , or that  $A$  has *stable range*  $d$ , if for each  $n \geq d+1$  and each unimodular  $\mathbf{a} = (a_1, \dots, a_n) \in A^n$ , there exist  $x_1, \dots, x_{n-1} \in A$  for which

$$(40.40) \quad \mathbf{a}' = (a_1 + x_1 a_n, a_2 + x_2 a_n, \dots, a_{n-1} + x_{n-1} a_n)$$

is unimodular. In this case we obtain

$$\mathbf{a} \sim (\mathbf{a}', a_n) \sim (\mathbf{a}', 1) \sim \mathbf{e}_1,$$

so for  $n \geq d + 1$  all unimodular  $n$ -tuples are equivalent to  $\mathbf{e}_1$ .

By (40.31), every semilocal ring has stable range 1. On the other hand, if  $R$  is a Euclidean domain, the Euclidean algorithm allows us to transform a unimodular pair  $(a_1, a_2)$  into  $(1, 0)$  by elementary operations. However, this does not imply that  $R$  has stable range 1. For example, when  $R = \mathbb{Z}$ , for the unimodular pair  $(3, 7)$  there is no  $x \in R$  such that  $3 + 7x \in R^\times$ . In fact,  $\mathbb{Z}$  has stable range 2.

Suppose next that  $R$  is a Dedekind domain. There are many examples where  $R$  is not Euclidean, nor even a P.I.D. Even when  $R$  is a P.I.D., however, there are examples in which some unimodular row  $(a, b)$  over  $R$  is not equivalent to  $(1, 0)$  under elementary row operations (see P. M. Cohn [66]). Nevertheless, we shall now show that every Dedekind domain  $R$  has stable range 2. (As pointed out above, this implies that for  $n \geq 3$ , every unimodular  $n$ -tuple over  $R$  is equivalent to  $(1, 0, \dots, 0)$ .)

Let  $R$  be a Dedekind domain, and let  $n > 2$ . Given any unimodular row  $\mathbf{a} = (a_1, \dots, a_n) \in R^n$ , we must show the existence of elements  $x_i \in R$  such that the vector  $\mathbf{a}'$  in (40.40) is unimodular. If some  $a_i = 0$ , where  $1 \leq i \leq n - 1$ , it suffices to add  $a_n$  to that  $a_i$  to achieve the desired result. Therefore we need only consider the case where the ideal  $Ra_1 + \dots + Ra_{n-2}$  is nonzero. Let  $\{P_i : 1 \leq i \leq k\}$  be the distinct maximal ideals of  $R$  containing that ideal. For each  $i$ , we can choose  $b_i \in R$  such that

$$a_{n-1} \not\equiv b_i a_n \pmod{P_i}.$$

In fact, if  $a_n \in P_i$  then  $a_{n-1} \notin P_i$ , and any  $b_i$  will work. On the other hand, if  $a_n \notin P_i$  then the congruence  $a_n x \equiv a_{n-1} \pmod{P_i}$  has a unique solution  $x_i \pmod{P_i}$ , and we then choose  $b_i = x_i + 1$ . Having determined these elements  $b_1, \dots, b_k \in R$ , we may use the Chinese Remainder Theorem to find  $b \in R$  such that  $b \equiv b_i \pmod{P_i}$  for each  $i$ . For this  $b$ , we have

$$a_{n-1} - ba_n \notin P_i, \quad 1 \leq i \leq k.$$

Therefore  $(a_1, a_2, \dots, a_{n-2}, a_{n-1} - ba_n)$  is a unimodular row, which completes the proof that  $R$  has stable range 2.

In (41.22) we shall prove the following far-reaching generalization of the preceding remarks:

**(40.41) Theorem (Bass).** *Let  $R$  be a Dedekind domain, and let  $A$  be an  $R$ -algebra, f.g./ $R$  as module. Then  $A$  has stable range 2.*

If  $A$  is an arbitrary ring with stable range  $d$ , then for any  $X \in GL_n(A)$ , where

$n \geq d + 1$ , we may find  $\mathbf{E} \in E_n(A)$  such that

$$\mathbf{EX} = \begin{pmatrix} 1 & * \\ \mathbf{0} & \mathbf{X}_1 \end{pmatrix} \quad \text{for some } \mathbf{X}_1 \in GL_{n-1}(A).$$

Since  $\mathbf{X}$  and  $\mathbf{EX}$  have the same image in  $K_1(A)$ , we obtain:

**(40.42) Surjective Stability Theorem.** *If  $A$  has stable range  $d$ , then there is a surjection*

$$GL_d(A) \rightarrow K_1(A).$$

It follows at once that

$$(40.43) \quad GL_d(A)/(GL_d(A) \cap E(A)) \cong K_1(A),$$

and clearly  $E_d(A) \subseteq GL_d(A) \cap E(A)$ . However, the inclusion may be proper. In (44.17), we shall prove:

**(40.44) Injective Stability Theorem (Bass, Vaserstein).** *If the ring  $A$  has stable range  $d$ , then  $E_n(A) = GL_n(A) \cap E(A) \trianglelefteq GL_n(A)$  for  $n \geq d + 1$ , and there is an isomorphism*

$$GL_n(A)/E_n(A) \cong K_1(A).$$

The map  $GL_n(A) \rightarrow K_1(A)$  is obviously surjective for  $n \geq d + 1$ , and the entire difficulty lies in determining the kernel. In (44.17) we shall prove a more general Injectivity Stability Theorem, which includes the above as a special case. The more general version will play a vital role in our study of  $SK_1$  of orders; see in particular the proof of (45.18). (For other treatments of the preceding theorem, see also Bass [68], Vaserstein [69], or Suslin-Tulenbaev [76].)

In special cases, the Injective Stability Theorem may be strengthened. Let  $R = \text{alg. int. } \{K\}$ , where  $K$  is an algebraic number field with  $r$  real primes and  $s$  complex primes. By the Dirichlet Unit Theorem, the group of units  $R^\times$  of  $R$  has rank  $r + s - 1$ . Thus  $R^\times$  is infinite, except when  $K = \mathbb{Q}$  or  $K = \mathbb{Q}(\sqrt{-d})$ ,  $d > 0$ . A remarkable theorem due to Vaserstein (see also Liehl [81]) is as follows:

**(40.45) Theorem.** *Let  $R$  be a Dedekind domain whose quotient field  $K$  is a global field, and assume  $R^\times$  infinite. Then*

$$SL_2(R) = E_2(R),$$

and the inclusion  $GL_2(R) \rightarrow GL(R)$  gives rise to an isomorphism

$$GL_2(R)/E_2(R) \cong GL(R)/E(R) = K_1(R).$$

Further

$$GL_2(R)/E_2(R) \cong GL_2(R)/SL_2(R) \cong R^\times.$$

**Remarks.** (i) The key is to prove that  $SL_2(R) = E_2(R)$ ; the rest is then obvious. The result implies that  $SK_1(R) = 1$ , a fact already pointed out in (38.55).

(ii) The theorem does *not* assert that  $R$  has stable range 1. It shows only that every unimodular pair  $(a, b)$  is the first row of some  $E \in E_2(R)$ . This does not imply that  $a + xb \in R^\times$  for some  $x \in R$ .

**Notes.** For any ring  $A$ , the opposite ring  $A^\circ$  has the same stable range as  $A$ .

**Reference:** Vaserstein [71]; (see Dennis [73a], p. 88).

## §40. Exercises

1. Let  $A$  be a semisimple ring, and suppose that  $A = Ax + M$  for some left ideal  $M$  of  $A$  and some  $x \in A$ . Show that  $x + m \in A^\times$  for some  $m \in M$ .

[Hint: Since  $A = Ax \oplus M_0$  for some left ideal  $M_0 \subseteq M$ , change notation and assume that  $A = Ax \oplus M$ . Let  $M' = \{a \in A : ax = 0\} = Ae$  for some idempotent  $e \in A$ . From the exact sequence  $0 \rightarrow M' \rightarrow A \rightarrow Ax \rightarrow 0$ , we get  $M' \cong M$ , so  $M = M'z$  for some  $z$  such that  $ez = z$ . Then (since  $ex = 0$ )

$$A(x + z) = (A(1 - e) + Ae)(x + z) = Ax \oplus M = A,$$

so  $x + z \in A^\times$ . But  $z = ez \in Ae = M$ .]

2. Prove the exactness of the sequence (40.20).

3. Let  $E \subseteq E'$  be global fields or completions thereof, let  $A$  be a f.d. separable  $E$ -algebra, and set  $A' = E' \otimes_E A$ . Show that the map  $K_1(A) \rightarrow K_1(A')$  is injective.

[Hint: If  $C = \text{center of } A$ , then

$$C' = \text{center of } A' = E' \otimes_E C.$$

There is a commutative diagram (see (45.3))

$$\begin{array}{ccc} K_1(A) & \xrightarrow{\text{nr}_{A/C}} & C^+ \\ \alpha \downarrow & & \beta \downarrow \\ K_1(A') & \xrightarrow{\text{nr}_{A'/C'}} & (C')^+ \end{array}$$

since  $\text{nr}$  commutes with field extension (see MO 9.29). The horizontal maps are isomorphisms, and  $\beta$  is injective, hence so is  $\alpha$ .]

4. Give an example of a left artinian ring  $A$  for which  $K_1(A)$  and  $K_1(A/\text{rad } A)$  are not isomorphic. Thus, the  $K_1$ -analogue of Exercise 38.7 need not hold.

[Hint: For  $A$  a commutative artinian ring,  $K_1(A) \cong A^\wedge$ . For suitable  $A$ ,  $A^\wedge$  is not isomorphic to  $(A/\text{rad } A)^\wedge$ .]

## §41. BASIC ELEMENTS, STABLE RANGE, AND CANCELLATION

Before plunging into some rather complicated proofs, let us state some of the main results of this section for the special case in which  $\Lambda$  is an  $R$ -order in a f.d.  $K$ -algebra  $A$ , where  $R$  is a Dedekind domain with quotient field  $K \neq R$ . Let  $P$  range over the maximal ideals of  $R$ , and let  $R_P$  denote localization at  $P$ . For  $M, N$   $\Lambda$ -modules, write  $M|N$  to indicate that  $M$  is a direct summand of  $N$  (up to isomorphism).

(1) (**Serre's Theorem**).<sup>\*</sup> *Let  $M \in \mathcal{P}(\Lambda)$  be such that*

$$\Lambda_P|M_P \text{ for each } P, \text{ and } A^{(2)}|KM$$

*Then  $\Lambda|M$ .*

(2) (**Bass Cancellation Theorem**).<sup>†</sup> *Let  $M \in \mathcal{P}(\Lambda)$  be as above, and let  $L, N \in \mathcal{P}(\Lambda)$ . Then*

$$L \oplus N \cong M \oplus N \Rightarrow L \cong M.$$

(3) (**Swan-Forster Theorem**). *Let  $\mu_\Lambda(M)$  denote the minimal number of generators of an arbitrary f.g.  $\Lambda$ -module  $M$ . Then*

$$\mu_\Lambda(M) \leq \max_P \{\mu_{\Lambda_P}(M_P), 1 + \mu_A(K \otimes_R M)\}.$$

(4) (**Bass Stable Range Theorem**).  *$\Lambda$  has stable range 2.*

As we shall see below, these results are special cases of more general theorems, dealing with the case where  $R$  is a commutative ring of finite Krull dimension, and  $\Lambda$  is an  $R$ -algebra, f.g./ $R$  as module. Some of the proofs will be carried out in the more general situation, but on the whole we shall avoid the machinery of commutative ring theory, and restrict attention to the Dedekind domain case when it seems appropriate. Our approach is by means of basic elements, as developed in Eisenbud-Evans [73]. The authors wish to thank Michael Fry for helpful comments on the material in this section.

Throughout this section we assume that all modules are f.g. If  $M$  is a  $B$ -module for some ring  $B$ , let

$$(41.1) \quad \begin{cases} \mu_B(M) = \text{minimal number of generators of } M, \\ \lambda_B(M) = \text{length of a composition series of } M, \end{cases}$$

<sup>\*</sup> When  $A$  is a separable  $K$ -algebra over a global field  $K$ , much stronger versions of these theorems are available. The Roiter-Jacobinski Theorem 31.32 improves Serre's Theorem, while the Jacobinski Cancellation Theorem is stronger than that of Bass.

assuming  $M$  has a composition series. We often omit the subscript  $B$  when there is no danger of confusion.

**(41.2) Definition.** Let  $M' \subseteq M$  be  $A$ -modules, where  $A$  is a semisimple ring. Call  $M'$  *t-fold basic* in  $M$  if

$$\mu(M/M') \leq \mu(M) - t.$$

We say  $M'$  is *basic* in  $M$  if  $M'$  is 1-fold basic in  $M$ . An element  $x \in M$  is *basic* in  $M$  if

$$\mu(M/Ax) < \mu(M),$$

or equivalently,

$$\mu(M/Ax) = \mu(M) - 1.$$

Thus,  $x$  is a basic element of  $M$  if and only if  $Ax$  is a basic submodule of  $M$ . Basic elements are important because, under suitable hypotheses, a basic element of a free module  $F$  generates a free direct summand of  $F$ . See Exercise 41.3.

**(41.3) Lemma.** Let  $M$  be a nonzero module over a simple artinian ring  $A$ . Let

$$\lambda(A) = \lambda_0, \quad \text{and} \quad \lambda(M) = p\lambda_0 + q \quad \text{where } 0 < q \leq \lambda_0.$$

Then

- (i)  $\mu(M) = p + 1$ ,
- (ii)  $M$  is a cyclic  $A$ -module if and only if  $\lambda(M) \leq \lambda_0$ ,
- (iii) An element  $x \in M$  is basic in  $M$  if and only if  $\lambda(Ax) \geq q$ .

*Proof.* Parts (i) and (ii) are trivial. For (iii), we have

$$\begin{aligned} x \text{ basic in } M &\Leftrightarrow \mu(M/Ax) \leq \mu(M) - 1 = p \\ &\Leftrightarrow \lambda(M/Ax) \leq p\lambda_0 \Leftrightarrow \lambda(Ax) \geq \lambda(M) - p\lambda_0 = q. \end{aligned}$$

**(41.4) Lemma.** Let  $A$  be a simple artinian ring, and let  $M = Am_1 \oplus Am_2$  be a cyclic  $A$ -module such that  $Am_2$  is simple. Let  $a \in A$  be such that

$$\lambda(A(a, m_1)) \geq \lambda(M),$$

where  $A(a, m_1)$  is the submodule of  $A \oplus M$  generated by  $(a, m_1)$ . Then there exists an element  $a' \in A$  such that for each central unit  $r \in A$ , we have

$$M = Am_1 \oplus Aaa'rm_2 = A(m_1 + aa'rm_2).$$

*Proof.* Consider the exact sequence of left  $A$ -modules

$$0 \rightarrow (\text{ann } m_1)a \rightarrow A(a, m_1) \xrightarrow{\pi} Am_1 \rightarrow 0,$$

where  $\pi$  is the projection map, and  $\text{ann}$  means  $A$ -annihilator. Then

$$\lambda(Am_1) = \lambda(M) - 1 \leq \lambda(A(a, m_1)) - 1,$$

whence  $(\text{ann } m_1)a \neq 0$ . But then  $A = (\text{ann } m_1)aA$ , since the right-hand expression is a nonzero two-sided ideal of  $A$ . Therefore

$$(\text{ann } m_1)aA \not\subseteq \text{ann } m_2,$$

so we may choose  $b \in \text{ann } m_1$ ,  $c \in A$ , such that  $bac \notin \text{ann } m_2$ . Therefore  $bacm_2 \neq 0$ , and since  $Am_2$  is simple, we obtain

$$Am_2 = Abacm_2 = Abacrm_2$$

for each central unit  $r \in A$ . Furthermore,  $bm_1 = 0$  gives

$$Am_2 = Ab(m_1 + acrm_2) \subseteq A(m_1 + acrm_2),$$

so  $A(m_1 + acrm_2)$  contains  $m_2$ , and hence also  $m_1$ . Therefore  $M = A(m_1 + acrm_2)$ , as desired. Finally, the sum

$$Am_1 + Aacrm_2$$

is direct, since the second expression lies in  $Am_2$ . The sum contains  $m_1 + acrm_2$ , hence coincides with  $M$ . Choosing  $a' = c$ , the proof is complete.

**(41.5) Lemma.** *Let  $A$  be a simple artinian ring,  $M \neq 0$  an  $A$ -module, and let  $b \in A$ ,  $x, y \in M$  be given. Then there exists an  $a \in A$  such that*

$$(41.6) \quad A(x + bay) = Ax \oplus Abay,$$

and

$$(41.7) \quad \text{either } y \in A(x + bay) \quad \text{or} \quad \lambda(A(x + bay)) \geq \lambda(A(b, x)),$$

where  $(b, x) \in A \oplus M$ .

*Proof.* We put  $d = \lambda(A(b, x)) - \lambda(Ax)$ . If  $d \leq 0$  we pick  $a = 0$ . Suppose now that  $d > 0$ , and use induction on  $d$ . If  $y \in Ax$  we may again choose  $a = 0$ , so let us consider the case where  $y \notin Ax$ , this is,  $Ax + Ay \supsetneq Ax$ . We may write  $Ab$  as a sum of simple  $A$ -modules  $Az$ , and then  $Ax + Az \supsetneq Ax$  for some  $z$ . Since  $z \in Ay$ ,

we may write  $z = cy$  for some  $c \in A$ , so we now have

$$Ax \oplus Acy \supset Ax, \quad Acy = \text{simple } A\text{-module}.$$

Now  $d > 0$  implies

$$\lambda(Ax \oplus Acy) = \lambda(Ax) + 1 \leq \lambda(A(b, x)) \leq \lambda_0.$$

Therefore  $Ax \oplus Acy$  is a cyclic  $A$ -module by (41.3), and we may thus apply (41.4) to the case where  $M = Ax \oplus Acy$ ,  $m_1 = x$ ,  $m_2 = cy$ . Hence there exists an element  $c' \in A$  such that

$$Ax \oplus Acy = A(x + bc'cy) = Ax \oplus Abc'cy.$$

Put  $x' = x + bc'cy$ , so

$$Ax \oplus Acy = Ax' = Ax \oplus Abc'cy.$$

Let

$$d' = \lambda(A(b, x')) - \lambda(Ax');$$

then  $d' = d - 1$ , since  $\lambda(Ax') = \lambda(Ax) + 1$ , while  $\lambda(A(b, x)) = \lambda(A(b, x'))$  by Exercise 41.2.

By the induction hypothesis, there exists an  $a' \in A$  such that

$$A(x' + ba'y) = Ax' \oplus Aba'y,$$

and

(\*) either  $y \in A(x' + ba'y)$  or  $\lambda(A(x' + ba'y)) \geq \lambda(A(b, x')) = \lambda(A(b, x))$ .

We set

$$x'' = x' + ba'y = x + bay, \quad \text{where } a = c'c + a',$$

and claim that this  $a$  has the desired properties. First,

$$\begin{aligned} Ax'' &= A(x' + ba'y) = Ax' \oplus Aba'y = Ax \oplus Abc'cy \oplus Aba'y \\ &= Ax \oplus (Abc'cy \oplus Aba'y) \supseteq Ax \oplus Abay \supseteq Ax'', \end{aligned}$$

so (41.6) holds. Finally, by (\*) either  $y \in Ax''$  or else  $\lambda(Ax'') \geq \lambda(A(b, x))$ . This establishes (41.7) and completes the proof.

We must now carry this information over to the semisimple case, and begin with an easy preliminary result:

**(41.8) Lemma.** *Let  $A = \coprod A_i$  be the Wedderburn decomposition of the semisimple artinian ring  $A$ , and let  $M$  be any f.g.  $A$ -module. Write  $M = \coprod M_i$ , where  $M_i = A_i M$ .*

Then

$$\mu_A(M) = \operatorname{Max}_i \mu_{A_i}(M_i), \quad \mu_A(A \oplus M) = \mu_A(M) + 1,$$

and  $(1, m)$  is basic in  $A \oplus M$  for each  $m \in M$ .

*Proof.* The formula for  $\mu_A(M)$  is obvious, while that for  $\mu_A(A \oplus M)$  follows from (41.3) whenever  $A$  is simple. For semisimple  $A$ , we have

$$\mu(A \oplus M) = \operatorname{Max}_i \mu(A_i \oplus M_i) = \operatorname{Max}_i \mu(M_i) + 1 = \mu(M) + 1.$$

Finally, for  $m \in M$  there is a surjection  $M \rightarrow (A \oplus M)/A(1, m)$ , and therefore

$$\mu((A \oplus M)/A(1, m)) \leq \mu(M) = \mu(A \oplus M) - 1,$$

so  $(1, m)$  is basic in  $A \oplus M$ .

**(41.9) Corollary.** *Keep the above notation, and let  $N$  be a submodule of  $M$ . Put*

$$J = \{i : \mu_A(M) = \mu_{A_i}(M_i)\},$$

so  $J$  is nonempty. Then

- (a)  $N$  is basic in  $M$  if and only if  $N_j$  is basic in  $M_j$  for all  $j \in J$ .
- (b) Let  $b \in A, m \in M$ , and let  $b_j, m_j$  denote images of  $b, m$ , respectively, under the projections  $A \rightarrow A_j, M \rightarrow M_j$ . Then  $(b, m)$  is basic in  $A \oplus M$  if and only if  $(b_j, m_j)$  is basic in  $A_j \oplus M_j$  for all  $j \in J$ .

*Proof.* Assume  $N$  basic in  $M$ ; then for all  $j \in J$ ,

$$\mu(M_j/N_j) \leq \mu(M/N) < \mu(M) = \mu(M_j),$$

so  $N_j$  is basic in  $M_j$ . Conversely, if  $N_j$  is basic in  $M_j$  for all  $j \in J$ , then for  $i \notin J$  we have

$$\mu(M_i/N_i) \leq \mu(M_i) < \mu(M).$$

Hence

$$\mu(M/N) = \operatorname{Max}_k \{\mu(M_k/N_k)\} < \mu(M),$$

so  $N$  is basic in  $M$ . Assertion (b) is a special case of (a).

**(41.10) Proposition.** *Let  $M$  be a f.g. module over a semisimple ring  $B$ , and let  $m_1, \dots, m_n \in M, b \in B$ , be such that*

$$\sum_1^n Bm_i \text{ is basic in } M, \quad \text{and} \quad (b, m_1) \text{ is basic in } B \oplus M.$$

Then there exist  $a_2, \dots, a_n \in B$  such that

$$m' = m_1 + b(a_2 m_2 + \dots + a_n m_n)$$

is basic in  $M$ , and

$$Bm' = Bm_1 \oplus \coprod_{i=2}^n Bba_i m_i.$$

*Proof.* Step 1. (Reduction to the simple case). Let superscripts denote projections onto simple components, and put

$$J = \{j : \mu_B(M) = \mu_{B^{(j)}}(M^{(j)})\}.$$

By the preceding results, the hypotheses carry over to the  $B^{(j)}$ -module  $M^{(j)}$ . Assuming that the proposition is valid for simple algebras, for each  $j \in J$  we can find elements  $a_2^{(j)}, \dots, a_n^{(j)} \in B^{(j)}$  such that

$$x^{(j)} = m_1^{(j)} + b^{(j)} \sum_{i=2}^n a_i^{(j)} m_i^{(j)}$$

is basic in  $M^{(j)}$ , and

$$B^{(j)} x^{(j)} = B^{(j)} m_1^{(j)} \oplus \coprod_{i=2}^n B^{(j)} (ba_i m_i)^{(j)}.$$

We need only choose  $a_i = \sum_{j \in J} a_i^{(j)}$ ,  $2 \leq i \leq n$ , and the desired result follows from (41.9).

Step 2. Assume now that  $B$  is simple artinian, and use induction on  $n$ . There is nothing to prove when  $n = 1$ , so let  $n > 1$  and assume the result holds at  $n - 1$ . By (41.5), there exists an element  $a_n \in B$  such that

$$Bx = Bm_1 \oplus Bba_n m_n, \quad \text{where } x = m_1 + ba_n m_n,$$

and either  $m_n \in Bx$  or else  $\lambda(Bx) \geq \lambda(B(b, m_1))$ . If  $m_n \in Bx$ , then  $Bx = Bm_1 + Bm_n$ , so  $Bx + Bm_2 + \dots + Bm_{n-1}$  is basic in  $M$ . Further, since  $(b, m_1)$  is basic in  $B \oplus M$ , so is  $(b, x)$  by Exercise 41.1. Applying the induction hypothesis, we may then choose  $a_2, \dots, a_{n-1} \in B$  such that

$$m' = x + b(a_2 m_2 + \dots + a_{n-1} m_{n-1}) \quad \text{is basic in } M,$$

and

$$Bm' = Bx \oplus \coprod_{i=2}^{n-1} Bba_i m_i = Bm_1 \oplus \coprod_{i=2}^n Bba_i m_i,$$

so we are through in this case.

On the other hand, suppose that the alternative  $\lambda(Bx) \geq \lambda(B(b, m_1))$  occurs. As in (41.3), write  $\lambda(M) = p\lambda_0 + q$ , where  $0 < q \leq \lambda_0$ . Then

$$\lambda(B \oplus M) = (p+1)\lambda_0 + q.$$

But  $(b, m_1)$  basic in  $B \oplus M$  implies  $\lambda(B(b, m_1)) \geq q$  by (41.3). We thus have  $\lambda(Bx) \geq q$ , so  $x$  is basic in  $M$ . Thus, in this case we just choose  $a_2 = \dots = a_{n-1} = 0$ . This completes the proof.

**(41.11) Corollary.** *Let  $M$  be a f.g. module over a semisimple ring  $B$ , and let  $m_1, \dots, m_n \in M$ ,  $b \in B$ , be such that*

$$\sum_1^n Bm_i \text{ is basic in } M, \quad \text{and} \quad (b, m_1) \text{ is basic in } B \oplus M.$$

*Then there exist  $a_2, \dots, a_n \in B$  such that for all central units  $r_2, \dots, r_n \in B$ , the element*

$$m'' = m_1 + b(a_2r_2m_2 + \dots + a_nr_nm_n)$$

*is basic in  $M$ , and*

$$Bm'' = Bm_1 \oplus \coprod_2^n Bba_im_i.$$

*Proof.* Let  $m'$  be as in (41.10), let  $\{r_i\}$  be a set of central units of  $B$ , and define  $m''$  as above. Clearly  $Bm'' \subseteq Bm'$ , and we claim that equality holds. Consider the  $B$ -homomorphisms

$$B \xrightarrow{m'} Bm_1 \oplus \coprod_2^n Bba_im_i \xrightarrow{(1, r_2, \dots, r_n)} Bm_1 \oplus \coprod_2^n Bba_im_i,$$

where the arrow labeled  $m'$  is right multiplication by  $m'$ . Each map is surjective, whence so is the composite. This composite is right multiplication by  $m''$ , and thus  $Bm'' = Bm'$  as claimed. Finally,

$$\mu(M/Bm'') = \mu(M/Bm') < \mu(M),$$

so  $m''$  is basic in  $M$ .

The following basic proposition is due to Eisenbud-Evans [73].

**(41.12) Proposition.** *Let  $M$  be a nonzero f.g.  $B$ -module, where  $B$  is semisimple. Let  $m_1, \dots, m_n \in M$ ,  $b \in B$ , be such that*

$$\sum_1^n Bm_i \text{ is } t\text{-fold basic in } M, \quad \text{and} \quad (b, m_1) \text{ is basic in } B \oplus M,$$

where  $t < n$ . Then there exist elements  $a_1, \dots, a_{n-1} \in B$  such that for all central units  $r_i \in B$ , the module  $N$  generated by

$$m_1 + ba_1r_n m_n, \quad m_2 + a_2r_2 m_n, \dots, m_{n-1} + a_{n-1}r_{n-1} m_n$$

is  $t$ -fold basic in  $M$ , and is independent of the choice of  $r$ 's.

*Proof.* If  $t = 0$ , choose each  $a_i = 0$ . Now let  $t = 1$ , and use (41.11); then there exist  $c_2, \dots, c_n \in B$  such that for all central units  $r_2, \dots, r_n \in B$ , the element

$$x = m_1 + b(c_2r_2 m_2 + \dots + c_n r_n m_n)$$

is basic in  $M$ , and such that the module  $Bx$  does not depend on the choice of  $r$ 's. Hence  $x, m_2, \dots, m_{n-1}$  generate a basic submodule  $N$  of  $M$ ; but  $N$  is also generated by

$$m_1 + bc_n r_n m_n, \quad m_2, \dots, m_{n-1},$$

so we need only choose  $a_1 = c_n$ ,  $a_2 = 0, \dots, a_{n-1} = 0$ . This completes the proof when  $t = 1$ .

Now let  $t > 1$ , and use induction. Construct  $x$  as above, and set  $\bar{M} = M/Bx$ . Then  $\mu(\bar{M}) < \mu(M)$  since  $x$  is basic in  $M$ , and thus  $\mu(\bar{M}) = \mu(M) - 1$ . If bars denote images in  $\bar{M}$ , we have

$$\mu\left(\bar{M} \left/ \sum_2^n B\bar{m}_i\right.\right) = \mu\left(M \left/ \sum_1^n Bm_i\right.\right) \leq \mu(M) - t = \mu(\bar{M}) - (t-1),$$

so  $\bar{m}_2, \dots, \bar{m}_n$  generate a  $(t-1)$ -fold basic submodule of  $\bar{M}$ . By (41.10),  $(1, \bar{m}_2)$  is basic in  $B \oplus \bar{M}$ . The induction hypothesis thus guarantees the existence of elements  $a_2, \dots, a_{n-1} \in B$  such that

$$\bar{m}_2 + a_2 r_2^{-1} r_n \bar{m}_n, \dots, \bar{m}_{n-1} + a_{n-1} r_{n-1}^{-1} r_n \bar{m}_n$$

generate a  $(t-1)$ -fold basic submodule  $\bar{L}$  of  $\bar{M}$ , which is independent of the  $r$ 's. Let  $L$  be the submodule of  $M$  defined as the inverse image of  $\bar{L}$  under the canonical mapping  $M \rightarrow \bar{M}$ . Since  $M/L \cong \bar{M}/\bar{L}$ , it follows that  $L$  is  $t$ -fold basic in  $M$ , and  $L$  is independent of the choice of  $r$ 's. Now  $L$  is generated by

$$x, \quad m_2 + a_2 r_2^{-1} r_n m_n, \dots, m_{n-1} + a_{n-1} r_{n-1}^{-1} r_n m_n,$$

hence also by

$$m_1 + ba_1 r_n m_n, \quad m_2 + a_2 r_2^{-1} r_n m_n, \dots, m_{n-1} + a_{n-1} r_{n-1}^{-1} r_n m_n,$$

for suitably chosen  $a_1$  (take  $a_1 = c_n - \sum_{i=2}^{n-1} c_i a_i$ ). These  $\{a_i\}$  are the desired elements of  $B$ , and the proof is complete.

We are interested in basic elements for  $R$ -algebras over a commutative ring  $R$ . For  $P$  a prime ideal of  $R$ , let  $R_P$  denote the localization of  $R$  at  $P$ .

**(41.13) Definition.** Let  $\Lambda$  be an  $R$ -algebra, f.g./ $R$  as module, and let  $M$  be a f.g.  $\Lambda$ -module. A submodule  $M'$  of  $M$  is called *t-fold basic at P* if

$$\mu(M_P/M'_P) \leq \mu(M_P) - t,$$

where  $\mu(M_P)$  is the minimal number of generators of  $M_P$  as  $\Lambda_P$ -module. *Basic* means “1-fold basic.” If the condition holds for each prime ideal  $P$  of  $R$ , we omit the words “at  $P$ ”, and call  $M'$  *t-fold basic* in  $M$ . An element  $m \in M$  is *basic* if  $\mu(M_P/\Lambda_P m) < \mu(M_P)$  for each  $P$ .

We shall use our results on modules over semisimple rings to prove:

**(41.14) Proposition.** Let  $\Lambda$  be an  $R$ -algebra f.g./ $R$ , and let  $P_1, \dots, P_k$  be a set of distinct prime ideals of  $R$ . Let  $M$  be a f.g.  $\Lambda$ -module, and let  $N = \sum_i^n \Lambda m_i \subseteq M$ . Suppose that for some  $a \in \Lambda$  we have for each  $i$ :

$$\begin{cases} N \text{ is } t_i\text{-fold basic in } M \text{ at } P_i, \\ (a, m_1) \text{ is basic in } \Lambda \oplus M \text{ at } P_i. \end{cases}$$

Then there exist  $a_1, \dots, a_{n-1} \in \Lambda$  such that

$$(41.15) \quad (a, m_1 + aa_1 m_n) \text{ is basic in } \Lambda \oplus M \text{ at each } P_i,$$

and such that the submodule of  $M$  generated by

$$m_1 + aa_1 m_n, \quad m_2 + a_2 m_n, \dots, m_{n-1} + a_{n-1} m_n$$

is  $\min(t_i, n-1)$ -fold basic in  $M$  at  $P_i$ ,  $1 \leq i \leq k$ .

*Proof.* Exercise 41.1 yields (41.15) for any choice of the  $\{a_j\}$ . Next, suppose that  $t_i \geq n$  for some  $i$ , so  $\sum_i^n \Lambda m_i$  is  $t_i$ -fold basic (and hence  $n$ -fold basic) in  $M$  at  $P_i$ . Then for any choice of  $a$ 's, the elements

$$m_n, \quad m_1 + aa_1 m_n, \quad m_2 + a_2 m_n, \dots, m_{n-1} + a_{n-1} m_n$$

generate a submodule of  $M$  which is  $n$ -fold basic in  $M$  at  $P_i$ . It follows from Exercise 41.5 that the submodule generated by the last  $n-1$  of these elements is  $(n-1)$ -fold basic in  $M$  at  $P_i$ , so again any choice of  $a$ 's will work for these  $\{P_i\}$  where  $t_i \geq n$ .

It remains for us to consider those  $P_i$  at which  $t_i < n$ , say  $\{P_1, \dots, P_l\}$ , numbered so that  $P_1$  is a minimal element of this set. Then  $P_1 \not\supseteq (P_2 \cap \dots \cap P_l)$ ,

so we may choose  $r \in R$  such that

$$r \notin P_1, \quad r \in P_2 \cap \cdots \cap P_l.$$

We use induction on  $l$ , and take  $l > 0$  and assume the result holds at  $l - 1$ . Then there exist  $a'_1, \dots, a'_{n-1} \in \Lambda$  such that the elements

$$m'_1 = m_1 + aa'_1 m_n, \quad m'_2 = m_2 + a'_2 m_n, \dots, m'_{n-1} = m_{n-1} + a'_{n-1} m_n$$

generate a submodule of  $M$  which is  $t_i$ -fold basic at  $P_i$ ,  $2 \leq i \leq l$ . We intend to choose  $b_1, \dots, b_{n-1} \in \Lambda$  so that the elements

$$(41.16) \quad m'_1 + ab_1 rm_n, \quad m'_2 + b_2 rm_n, \dots, m'_{n-1} + b_{n-1} rm_n$$

generate a submodule  $M_0$  of  $M$  which is  $t_1$ -fold basic at  $P_1$ . By Exercise 41.7,  $M_0$  will also be  $t_i$ -fold basic at  $P_i$ ,  $2 \leq i \leq l$ .

We now let

$$\bar{\Lambda} = \Lambda_{P_1}/\text{rad } \Lambda_{P_1}, \quad \bar{M} = M_{P_1}/(\text{rad } \Lambda_{P_1})M_{P_1}.$$

By Exercise 41.7, it follows that

$$\sum_1^n \bar{\Lambda} \bar{m}_i \text{ is } t_1\text{-fold basic in } \bar{M}, \quad \text{and} \quad (\bar{a}, \bar{m}_1) \text{ is basic in } \bar{\Lambda} \oplus \bar{M}.$$

As pointed out earlier,  $(\bar{a}, \bar{m}'_1)$  is also basic in  $\bar{\Lambda} \oplus \bar{M}$ . Also,

$$\sum_1^n \bar{\Lambda} \bar{m}_i = \sum_1^{n-1} \bar{\Lambda} \bar{m}'_i + \overline{\bar{\Lambda} rm_n} = t_1\text{-fold basic submodule of } \bar{M}.$$

where  $t_1 < n$ . By virtue of (41.12), there exist  $a_1, \dots, a_{n-1} \in \Lambda_{P_1}$  such that for each  $s \in R - P_1$ , the elements

$$\bar{m}'_1 + \overline{aa_1 srm_n}, \quad \bar{m}'_2 + \overline{a_2 srm_n}, \dots, \bar{m}'_{n-1} + \overline{a_{n-1} srm_n}$$

generate a  $\bar{\Lambda}$ -submodule of  $\bar{M}$  which is  $t_1$ -fold basic in  $\bar{M}$ . Choose  $s$  so that each  $sa_i$  lies in the image of  $\Lambda$  in  $\Lambda_{P_1}$ ; then there exist elements  $\{b_i\}$  in  $\Lambda$  so that the images of

$$m'_1 + ab_1 rm_n, \quad m'_2 + b_2 rm_n, \dots, m'_{n-1} + b_{n-1} rm_n$$

in  $\bar{M}$  generate a  $t_1$ -fold basic submodule. But then these elements generate a  $t_1$ -fold basic submodule of  $M$  at  $P_1$ , as desired in (41.16). This completes the proof of the proposition.

We are now going to specialize our discussion to the case where  $R$  is a

Dedekind ring with quotient field  $K$ , in order to avoid some arguments from commutative ring theory. All of the results carry over, with modifications in the statements and proofs, to the case where  $R$  is a commutative ring of finite Krull dimension. (We say that  $R$  has *Krull dimension  $n$*  if the length of a maximal chain of strictly increasing prime ideals of  $R$  equals  $n+1$ . Thus, if  $R$  is a Dedekind domain and *not* a field, then  $R$  has Krull dimension 1.) We assume once and for all that  $R \neq K$ , to avoid unnecessary complications in the statements of results. For  $M$  any  $R$ -module, denote  $K \otimes_R M$  by  $KM$  for brevity (even though the map  $M \rightarrow KM$  need not be a monomorphism!).

**(41.17) Lemma.** *Let  $R$  be a Dedekind domain with quotient field  $K$ ,  $\Lambda$  an  $R$ -algebra f.g./ $R$ , and  $N \subseteq M$  a pair of f.g.  $\Lambda$ -modules. If  $KN$  is  $t$ -fold basic in  $KM$ , then  $N$  is  $t$ -fold basic in  $M$  at almost all maximal ideals  $P$  of  $R$ .*

*Proof.* For  $n \geq 0$ , let

$$I_n(M) = \sum_{M'} \text{ann}_R(M/M'),$$

where  $M'$  ranges over all submodules of  $M$  which can be generated by  $n$  elements or fewer. Then  $I_0(M) \subseteq I_1(M) \subseteq \dots$ , and

$$I_k(M) = R \quad \text{whenever } \mu(M) \leq k.$$

Next, for any  $P$ , we have

$$(*) \quad P \supseteq I_k(M/N) \Leftrightarrow \mu(M_P/N_P) > k.$$

Now let  $k = \mu(M/N)$ , and consider the chain

$$(**) \quad I_0(M/N) \subseteq \dots \subseteq I_{k-1}(M/N) \subseteq I_k(M/N) = R.$$

Let  $P$  be a (nonzero) maximal ideal of  $R$ , and suppose that  $\mu(M_P/N_P) = n$ . Then

$$P \supseteq I_{n-1}(M/N), \quad P \not\supseteq I_n(M/N).$$

If  $I_{n-1} = 0$ , then  $(*)$  shows that  $\mu(KM/KN) \geq n$ , whence  $\mu(KM/KN) = n$ . But then

$$\mu(M_P/N_P) = \mu(KM/KN) \leq \mu(KM) - t \leq \mu(M_P) - t,$$

so  $N$  is  $t$ -fold basic in  $M$  at  $P$ . On the other hand, if  $I_{n-1} \neq 0$  there are only finitely many  $P$ 's containing it. Thus,  $N$  is  $t$ -fold basic in  $M$  at each nonzero  $P$ , with the possible exception of those  $P$ 's which contain at least one nonzero ideal in the chain  $(**)$ . This proves the lemma.

We are now ready to prove one of the main results of Eisenbud-Evans:

**(41.18) Theorem.** Let  $R$  be a Dedekind domain with quotient field  $K \neq R$ , let  $\Lambda$  be an  $R$ -algebra f.g./ $R$  as module, and let  $M$  be any f.g.  $\Lambda$ -module. Denote  $K \otimes_R M$  by  $KM$ , for brevity. Then:

(i) If  $\mu(KM) \geq 2$ , then  $M$  contains a basic element.

(ii) Let  $N = \sum_1^n \Lambda m_i \subseteq M$ ,  $a \in \Lambda$ , and assume

$$\begin{cases} (a, m_1) \text{ is basic in } \Lambda \oplus M, \\ N \text{ is basic in } M \text{ at each maximal ideal } P \text{ of } R, \text{ and} \\ KN \text{ is 2-fold basic in } KM. \end{cases}$$

Then  $M$  contains a basic element of the form  $m_1 + am'$ , with  $m' \in \sum_2^n \Lambda m_i$ .

*Proof.* Since  $KN$  is 2-fold basic in  $KM$ , surely  $n \geq 2$ . By (41.17),  $N$  is 2-fold basic in  $M$  at all but finitely many maximal ideals  $\{P_1, \dots, P_k\}$  of  $R$ . By hypothesis,  $N$  is basic in  $M$  at each  $P_i$ , so by (41.14) there exist elements  $a_1, \dots, a_{n-1} \in \Lambda$  such that the  $\Lambda$ -module  $N'$  generated by the elements

$$m'_1 = m_1 + aa_1 m_n, \quad m'_2 = m_2 + a_2 m_n, \dots, m'_{n-1} = a_{n-1} m_n,$$

is basic in  $M$  at each  $P_i$ , and is  $\min(n-1, 2)$ -fold basic in  $M$  at the ideal  $P_0 = \{0\}$ . Further,  $(a, m'_1)$  is basic in  $\Lambda \oplus M$  by Exercise 41.1. We claim that  $N'$  is basic in  $M$  at each maximal ideal  $P$ , and it suffices to check this when  $P \notin \{P_1, \dots, P_k\}$ . For such  $P$ ,  $N' + \Lambda m_n$  is 2-fold basic in  $M$  at  $P$ , whence surely  $N'$  is 1-fold basic in  $M$  at  $P$ , as desired.

Thus, if  $n > 2$  we have a new submodule  $N'$  of  $M$ , generated by  $n-1$  elements, and satisfying the same conditions as does  $N$ . Hence we may iterate the procedure until we reach the case  $n=2$ , at which point  $n-1=1$ , and the element  $m'_1$  above is basic in  $M$ . This completes the proof of (ii). But then (i) is clear, since we need only choose  $N = M$  and  $a = 1$  (see Exercise 41.8).

**Remarks.** (1) Let  $R$  be a commutative noetherian ring of finite Krull dimension  $d$ . For each prime ideal  $P$  of  $R$ , let  $\dim P$  be the largest integer  $m$  for which there exists a chain of prime ideals of  $R$

$$P \subset P_1 \subset \dots \subset P_m.$$

Let  $\Lambda$  be an  $R$ -algebra, f.g./ $R$  as module, and let  $M$  be an f.g.  $\Lambda$ -module. Then the generalization of the preceding theorem is as follows:

(i) If  $\mu(M_P) > d$  for each minimal  $P$ , then  $M$  contains a basic element.

(ii) Let  $N = \sum_1^n \Lambda m_i \subseteq M$ ,  $a \in \Lambda$ , and assume

$$\begin{cases} (a, m_1) \text{ is basic in } \Lambda \oplus M, \text{ and} \\ N \text{ is } (\dim P + 1)\text{-fold basic in } M \text{ for each prime ideal } P \text{ of } R. \end{cases}$$

Then  $M$  contains a basic element of the form  $m_1 + am'$ , with  $m' \in \sum_2^n \Lambda m_i$ .

(2) The hypothesis that  $R$  be noetherian of finite Krull dimension can be replaced by the weaker hypothesis that  $m\text{-spec } R$  is noetherian and of dimension  $d$ .

(3) The hypothesis that  $(a, m_1)$  be basic in  $\Lambda \oplus M$  is always fulfilled when  $a = 1$ .

We are now ready to show that the Eisenbud-Evans Theorem gives the four main results stated at the start of this section. In fact, we obtain these results not only for  $R$ -orders, but more generally for  $R$ -algebras, f.g./ $R$  as module. We begin with:

**(41.19) Theorem (Serre).** *Let  $\Lambda$  be an  $R$ -algebra as in (41.18), and let  $M$  be a f.g. projective  $\Lambda$ -module. Suppose that  $K\Lambda^{(2)}|KM$ , and that  $\Lambda_P|M_P$  for each maximal ideal  $P$  of  $R$ . Then  $\Lambda|M$ . Further, if  $M = \sum_1^n \Lambda m_i$ , the generator of the free summand of  $M$  may be chosen in the form  $m_1 + a_2 m_2 + \cdots + a_n m_n$ ,  $a_i \in \Lambda$ .*

*Proof.* The second assertion implies the first. Now choose a f.g. projective  $\Lambda$ -module  $L$  such that  $M \oplus L$  is  $\Lambda$ -free. At each maximal ideal  $P$  we have  $M_P = \Lambda_P \oplus X$  for some  $X$ , whence

$$\mu(M_P \oplus L_P) \geq 1 + \mu(L_P),$$

and so  $M$  is basic in  $M \oplus L$  at each  $P$ . Likewise,  $KM$  is 2-fold basic in  $K(M \oplus L)$ . Further,  $(1, m_1)$  is basic in  $\Lambda \oplus (M \oplus L)$ . It follows from Theorem 41.18 that  $M$  contains a basic element  $m$  of  $M \oplus L$  of the desired form. Then  $\Lambda m|(M \oplus L)$  by Exercise 41.3, whence  $\Lambda m|M$ , which proves the corollary.

In the same vein, we prove:

**(41.20) Bass Cancellation Theorem.** *Let  $M, \Lambda$  be as above, and let  $L, N$  be f.g. projective  $\Lambda$ -modules such that  $M \oplus N \cong L \oplus N$ . Then  $M \cong L$ .*

*Proof.* Increasing  $N$  by a suitable summand, we may assume that  $N$  is  $\Lambda$ -free. It then suffices to prove the result when  $N = \Lambda$ , so let

$$\alpha: \Lambda \oplus L \cong \Lambda \oplus M, \quad \alpha(1, 0) = (a, m_1),$$

be given. We shall set  $\beta = \psi\alpha$  for some suitable  $\psi \in \text{Aut}(\Lambda \oplus M)$ , chosen so that  $\beta|_\Lambda = 1$ . Then  $\beta: \Lambda \oplus L \cong \Lambda \oplus M$  induces an isomorphism  $L \cong M$ , and we are through.

Since  $(1, 0)$  is basic in  $\Lambda \oplus L$ , the element  $(a, m_1)$  is basic in  $\Lambda \oplus M$ . Write  $M = \sum_1^n \Lambda m_i$ ; the preceding results imply that  $M$  has a free direct summand  $\Lambda m$ , where  $m = m_1 + am'$  for some  $m' \in \sum_2^n \Lambda m_i$ . Now define  $\psi \in \text{Aut}(\Lambda \oplus M)$  by composition of maps:

$$\Lambda \oplus M \xrightarrow{\begin{pmatrix} l & 0 \\ f & 1 \end{pmatrix}} \Lambda \oplus M \xrightarrow{\begin{pmatrix} l & q \\ 0 & 1 \end{pmatrix}} \Lambda \oplus M \xrightarrow{\begin{pmatrix} 1 & 0 \\ h & 1 \end{pmatrix}} \Lambda \oplus M,$$

where the  $\Lambda$ -maps  $f, g, h$  are defined thus:

$$f(x) = xm', \quad h(x) = -xm, \quad x \in \Lambda,$$

and  $g \in \text{Hom}(M, \Lambda)$  is given by composition

$$M = \Lambda m \oplus M_0 \rightarrow \Lambda m \rightarrow \Lambda \rightarrow \Lambda(1-a).$$

Then we have  $g(m) = 1 - a$ , so

$$\begin{aligned} \psi(a, m_1) &= \begin{pmatrix} 1 & 0 \\ h & 1 \end{pmatrix} \begin{pmatrix} 1 & g \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ f & 1 \end{pmatrix} (a, m_1) \\ &= \begin{pmatrix} 1 & g \\ h & hg + 1 \end{pmatrix} (a, fa + m_1) = \begin{pmatrix} 1 & g \\ h & hg + 1 \end{pmatrix} (a, m) \\ &= (a + gm, ha + (hg + 1)m) = (1, 0). \end{aligned}$$

Then

$$\beta(1, 0) = \psi\alpha(1, 0) = \psi(a, m_1) = (1, 0).$$

so  $\beta|_{\Lambda} = 1$ , and the proof is finished.

**Remark.** The generalized versions of the preceding two theorems, for the case of a commutative noetherian ring  $R$  of finite Krull dimension  $d$ , are as follows:

In (41.19), the hypotheses should read:

$$\Lambda_P^{(1 + \dim P)} | M_P \text{ for each } P.$$

The conclusion is unchanged. The same change in hypothesis occurs in (41.20).

Our next consequence of Theorem 41.18 is:

**(41.21) Theorem (Swan-Forster).** Let  $\Lambda$  be an  $R$ -algebra as in (41.18), let  $P$  range over all maximal ideals of  $R$ , and put

$$t = \max_P \{\mu(M_P), 1 + \mu(KM)\}$$

(omit the term  $1 + \mu(KM)$  if  $KM = 0$ ). Then  $\mu(M) \leq t$ .

*Proof.* (In the special case where  $M$  is a nonzero ideal of  $R$ , we have  $\mu(M_P) = 1$  for each  $P$ , and  $1 + \mu(KM) = 2$ , so  $t = 2$ . We recover the classical result that  $M$  can be generated by 2 elements.)

Let  $n = \mu(M)$ ; we assume that  $n > t$ , and try to obtain a contradiction. There is an exact sequence

$$0 \rightarrow N \rightarrow F \rightarrow M \rightarrow 0, \quad \text{where } F \cong \Lambda^{(n)}.$$

At each maximal ideal  $P$  of  $R$ , we have

$$\mu(F_P/N_P) = \mu(M_P) = \mu(F_P) - (n - \mu(M_P)) \leq \mu(F_P) - 1,$$

so  $N$  is basic in  $F$  at  $P$ . A similar argument shows that  $KN$  is 2-fold basic in  $KF$ . By Theorem 41.18 it follows that  $N$  contains an element  $x$  which is basic in  $F$ . Then  $\Lambda x \cong \Lambda$ , and  $F = \Lambda x \oplus F'$  by Exercise 41.3. Thus we have

$$F = \Lambda^{(n-1)} \oplus \Lambda \cong F' \oplus \Lambda x.$$

If  $n \geq 3$ , the Bass Cancellation Theorem gives  $F' \cong \Lambda^{(n-1)}$ . But then

$$F' \cong F/\Lambda x \xrightarrow{\theta} F/N \cong M, \quad \text{with } \theta \text{ surjective,}$$

so  $F'$  maps onto  $M$ , whence  $\mu(M) \leq n - 1$ , a contradiction.

On the other hand, if  $n = 2$  then (assuming  $M \neq 0$ ) we have  $t = 1$  and necessarily  $KM = 0$ . If  $\mathfrak{a} = \text{ann}_R M$ , then  $\mathfrak{a}$  is nonzero; let

$$\bar{R} = R/\mathfrak{a}, \quad \bar{\Lambda} = \Lambda/\mathfrak{a}\Lambda,$$

so  $\bar{\Lambda}$  is an  $\bar{R}$ -algebra, and  $M$  is a  $\bar{\Lambda}$ -module. The preceding argument shows that  $F'$  maps onto  $M$ , whence also  $\bar{F}'$  maps onto  $M$ . But  $\bar{F} \cong \bar{F}' \oplus \bar{\Lambda}$ , and the Krull-Schmidt-Azumaya Theorem holds for f.g.  $\bar{\Lambda}$ -modules, whence  $\bar{F}' \cong \bar{\Lambda}^{(n-1)}$ . This shows again that  $\mu(M) \leq n - 1$ , a contradiction, and the proof is complete.

Finally, we prove Bass's result:

**(41.22) Bass Stable Range Theorem.** *Let  $\Lambda$  be an  $R$ -algebra as in (41.18), and suppose that*

$$\Lambda = \Lambda b_1 + \cdots + \Lambda b_n, \quad \text{where } n > 2.$$

*Then there exist  $x_1, \dots, x_{n-1} \in \Lambda$  such that*

$$\Lambda = \Lambda(b_1 + x_1 b_n) + \Lambda(b_2 + x_2 b_n) + \cdots + \Lambda(b_{n-1} + x_{n-1} b_n).$$

*Proof.* Let  $\mathbf{b} = (b_1, \dots, b_n)$ , so  $\mathbf{b}$  is unimodular by hypothesis. By (40.33), this is equivalent to the assertion that  $\mathbf{b}\Lambda$  is a free direct summand of the right  $\Lambda$ -module  $\Lambda^{(n)}$ , or equivalently (see Exercises 41.3, 41.4), that  $\mathbf{b}$  is basic in  $\Lambda^{(n)}$  at each maximal ideal  $P$  of  $R$ .

We now set  $M = \Lambda^{(n-1)}$ . Since  $n - 1 \geq 2$ , it follows that  $M$  is 2-fold basic in  $\Lambda^{(n)}$  at every maximal ideal  $P$  of  $R$ , and also at the zero ideal. We put

$$m_1 = (b_1, \dots, b_{n-1}), \quad m_2 = (1, 0, \dots, 0), \dots, m_n = (0, \dots, 0, 1),$$

viewed as elements of  $M$ . Then  $(b_n, m_1) \in \Lambda \oplus M$ , and  $(b_n, m_1)$  is unimodular, hence

basic in  $\Lambda \oplus M$ . It follows from Theorem 41.18 that there exist  $x_1, \dots, x_{n-1} \in \Lambda$  such that

$$m' = m_1 + (m_2 x_1 + \dots + m_n x_{n-1}) b_n$$

is basic in  $M$ . Hence this  $m'$  is also unimodular. But

$$m' = (b_1 + x_1 b_n, b_2 + x_2 b_n, \dots, b_{n-1} + x_{n-1} b_n),$$

so we have obtained our desired unimodular  $(n-1)$ -tuple. This completes the proof.

**(41.23) Corollary. (Surjective Stability).** *Let  $\Lambda$  be an  $R$ -algebra, f.g./ $R$  as module, where  $R$  is a Dedekind domain. Then  $\Lambda$  has stable range 2, and the map*

$$GL_2(\Lambda) \rightarrow K_1(\Lambda)$$

*is surjective.*

**Remarks.** For the case where  $R$  is any commutative noetherian ring of Krull dimension  $d$ , the generalized versions of the preceding results are as follows:

**(41.24) Theorem (Swan-Forster).** *Let  $R$  have Krull dimension  $d$ , and let  $\Lambda$  be an  $R$ -algebra, f.g./ $R$  as module. Let  $M$  be any f.g.  $\Lambda$ -module, and set*

$$t = \text{Max} \{ \mu(M_P) + \dim P \},$$

*where  $P$  ranges over all prime ideals of  $R$  such that  $M_P \neq 0$ . Then*

$$\mu(M) \leq t.$$

**(41.25) Bass Stable Range Theorem.** *Let  $\Lambda$  be as above, and suppose that*

$$\Lambda = \Lambda b_1 + \dots + \Lambda b_n, \quad \text{where } n > d + 1.$$

*Then there exist  $x_1, \dots, x_{n-1} \in \Lambda$  such that*

$$\Lambda = \Lambda(b_1 + x_1 b_n) + \Lambda(b_2 + x_2 b_n) + \dots + \Lambda(b_{n-1} + x_{n-1} b_n).$$

*In other words,  $\Lambda$  has stable range  $d + 1$ , and the map*

$$GL_n(\Lambda) \rightarrow K_1(\Lambda)$$

*is surjective for  $n \geq d + 1$ .*

**Notes.** (1) Let  $\Lambda = \mathbb{Z}G$ , where  $|G| = n$ . Let  $M$  and  $N$  be  $\Lambda$ -lattices such that

$$M \oplus \Lambda^{(k)} \cong N \oplus \Lambda^{(k)}$$

for some  $k$ . Suppose that neither  $M$  nor  $N$  is a cyclic  $\Lambda$ -module. Then (see Cohen [78])  $\mu_\Lambda(M) = \mu_\Lambda(N)$ .

Further,  $M$  contains a sublattice  $L$  such that

$$\mu_\Lambda(L) = \operatorname{Max}_{p|n} \{\mu_{\Lambda_p}(M_p)\}.$$

(Compare with the Swan-Forster Theorem 41.21.)

(2) Let  $M$  be a  $\Lambda$ -lattice, where  $\Lambda = \mathbb{Z}G$ , and let  $|G| = n$ . Set

$$t = \operatorname{Max}_{p|n} \{\mu_{\Lambda_p}(M_p)\},$$

and assume that  $t \geq 2$ . Suppose that every simple  $\mathbb{Q}G$ -module (except possibly the trivial module  $\mathbb{Q}$ ) occurs more often in  $(\mathbb{Q}G)^{(t)}$  than in  $\mathbb{Q}M$ . Then  $\mu_\Lambda(M) = t$ . The result is due to Swan [65], Lemma 4.4; see also Gruenberg [76], Theorem 7.3.

## §41. Exercises

1. Let  $M$  be a f.g.  $A$ -module, where  $A$  is any ring, and let  $(a, m) \in A \oplus M$  be such that

$$\mu((A \oplus M)/A(a, m)) < \mu(A \oplus M).$$

Show that this same inequality holds when  $m$  is replaced by  $m + am'$ , for any  $m' \in M$ .

[Hint: The map

$$(a, x) \rightarrow (a, x + am'), \quad a \in A, \quad x \in M,$$

is an  $A$ -automorphism of  $A \oplus M$  carrying  $(a, m)$  onto  $(a, m + am')$

2. Let  $M$  be a f.g.  $A$ -module, where  $A$  is an artinian ring, and let  $a \in A, m, m' \in M$ . Show that the submodules  $A(a, m)$  and  $A(a, m + am')$  of  $A \oplus M$  have the same composition length.

[Hint: There is an  $A$ -exact sequence

$$0 \rightarrow \operatorname{ann}(a, m) \rightarrow A \rightarrow A(a, m) \rightarrow 0,$$

and another in which  $m$  is replaced by  $m + am'$ . But  $(a, m)$  and  $(a, m + am')$  have the same annihilator.]

3. Let  $\Lambda$  be an  $R$ -algebra f.g./ $R$ , where  $R$  is any commutative ring. Let  $F \cong \Lambda^{(n)}$  be  $\Lambda$ -free of rank  $n$ , and let  $x \in F$  be basic in  $F$  at each maximal ideal  $P$  of  $R$  (that is,

$$\mu(F_P/\Lambda_P x) < \mu(F_P) \text{ for each } P.$$

Show that  $\Lambda x$  is a free direct summand of  $F$ .

[Hint: We must show that  $F/\Lambda x$  is projective, and that the surjection  $\alpha: \Lambda \rightarrow \Lambda x$  is an

isomorphism. It suffices to establish these facts at each  $P$ , so after localizing at  $P$ , we may assume  $R$  is local and  $\mu(F/\Lambda x) = \mu(F) - 1$ . Hence there is a surjection  $\gamma: \Lambda^{(n-1)} \rightarrow F/\Lambda x$ . Using the Horseshoe Lemma, we obtain a commutative diagram with exact rows:

$$\begin{array}{ccccccc} 0 & \rightarrow & \Lambda & \rightarrow & \Lambda^{(n)} & \rightarrow & \Lambda^{(n-1)} \rightarrow 0 \\ & & \alpha \downarrow & & \beta \downarrow & & \gamma \downarrow \\ 0 & \rightarrow & \Lambda x & \rightarrow & F & \rightarrow & F/\Lambda x \rightarrow 0. \end{array}$$

Now use the Snake Lemma to show that  $\alpha, \beta$  and  $\gamma$  are isomorphisms.]

4. Keep the notation of Exercise 3. Show that every free direct summand of  $\Lambda^{(n)}$  is basic in  $\Lambda^{(n)}$  (at each  $P$ ).
5. Let  $M$  be a f.g.  $A$ -module, where  $A$  is any ring, and let  $m_1, \dots, m_n \in M$ . Show that

$$\mu\left(M \left/ \sum_1^n Am_i\right.\right) \geq \mu(M) - n.$$

Further, if equality holds, then also

$$\mu\left(M \left/ \sum_1^r Am_i\right.\right) = \mu(M) - r$$

for  $1 \leq r \leq n$ .

6. Let  $M$  be a f.g.  $A$ -module, where  $A$  is any ring, and let  $\bar{A} = A/\text{rad } A$ ,  $\bar{M} = M/(\text{rad } A)M$ . Show that  $\mu_A(M) = \mu_{\bar{A}}(\bar{M})$ , where  $\mu$  denotes minimal number of generators.
7. Let  $R$  be a commutative local ring with maximal ideal  $P$ , and  $\Lambda$  an  $R$ -algebra f.g./ $R$  as module. Let  $M$  be an f.g.  $\Lambda$ -module, and let bars denote reduction modulo  $\text{rad } \Lambda$ . Let  $\tilde{\Lambda} = \Lambda/P\Lambda$ ,  $\tilde{M} = M/PM$ . Show that

$$\mu_{\Lambda}(M) = \mu_{\tilde{\Lambda}}(\tilde{M}) = \mu_{\tilde{\Lambda}}(\tilde{M}).$$

If  $N = \sum_1^k \Lambda m_i$  is a submodule of  $M$ , and  $N' = \sum_1^k \Lambda m'_i$  another submodule such that  $m'_i \equiv m_i \pmod{PM}$  for each  $i$ , show that

$$\mu(M/N) = \mu(M/N').$$

8. Let  $\Lambda$  be an  $R$ -algebra f.g./ $R$ , where  $R$  is commutative, and let  $M$  be any f.g.  $\Lambda$ -module. Show that for any  $m \in M$ , the element  $(1, m)$  is basic in  $\Lambda \oplus M$  at every prime ideal of  $R$ .
9. Give an example of a f.g.  $A$ -module  $M$  (for some suitably chosen ring  $A$ ) such that  $\mu(A \oplus M) \neq \mu(M) + 1$ .

## §42. MAYER-VIETORIS SEQUENCES

Let

$$(42.1) \quad \begin{array}{ccc} A & \xrightarrow{f_1} & A_1 \\ f_2 \downarrow & & \downarrow g_1 \\ A_2 & \xrightarrow{g_2} & \bar{A} \end{array}$$

be a fiber product of rings and ring homomorphisms (see end of §2A). This means that there is a ring isomorphism

$$A \cong \{(a_1, a_2) : a_i \in A_i, g_1(a_1) = g_2(a_2)\},$$

or equivalently, an exact sequence (of rings)

$$(42.2) \quad 0 \rightarrow A \xrightarrow{(f_1, f_2)} A_1 \oplus A_2 \xrightarrow{(g_1, -g_2)} \bar{A}.$$

Our object is to study properties of the ring  $A$ , and in particular the category  $\mathcal{P}(A)$ , in terms of corresponding properties of  $A_1, A_2$ , and  $\bar{A}$ . We shall be especially interested in the relation between the  $K$ -theory of  $A$  and that of the other rings. This relation, called a *Mayer-Vietoris sequence*, is as follows: if either  $g_1$  or  $g_2$  is surjective, there is an exact sequence of groups

$$K_1(A) \rightarrow K_1(A_1) \times K_1(A_2) \rightarrow K_1(\bar{A}) \rightarrow K_0(A) \rightarrow K_0(A_1) \oplus K_0(A_2) \rightarrow K_0(\bar{A}).$$

The result, due to Milnor, is of the utmost importance in calculations of  $K$ -groups. Further, if both  $g_1$  and  $g_2$  are surjective, the sequence can be extended to the left by means of  $K_2$  terms, where  $K_2(A)$  is the Milnor group of  $A$  (see §47B).

**(42.3) Example.** Let  $I$  and  $J$  be two-sided ideals of  $A$ . Then there is a fiber product

$$\begin{array}{ccc} A/(I \cap J) & \longrightarrow & A/I \\ \downarrow & & \downarrow \\ A/J & \longrightarrow & A/(I + J). \end{array}$$

As an illustration, consider Example 7.39 where  $A = \mathbb{Z}G$ , with

$$G = \langle x, y : x^n = 1, y^2 = 1, yxy^{-1} = x^{-1} \rangle, \quad H = \langle x \rangle \trianglelefteq G.$$

Let

$$I = (x - 1)A, \quad J = (x^{n-1} + x^{n-2} + \cdots + x + 1)A,$$

a pair of two-sided ideals of  $A$ . Since  $A$  is free as  $\mathbb{Z}H$ -module, and

$$(x - 1)\mathbb{Z}H \cap (x^{n-1} + \cdots + x + 1)\mathbb{Z}H = 0,$$

we obtain

$$I \cap J = 0, \quad I + J = nA + (x - 1)A.$$

The fiber product becomes

$$(42.4) \quad \begin{array}{ccc} \mathbb{Z}G & \longrightarrow & \mathbb{Z}[y] \\ \downarrow & & \downarrow \\ R^\circ[y] & \longrightarrow & \bar{\mathbb{Z}}[y], \end{array}$$

where  $\bar{\mathbb{Z}} = \mathbb{Z}/n\mathbb{Z}$ , and  $R^\circ[y]$ , is the twisted group ring of the cyclic group  $\langle y \rangle$  of order 2 over the commutative ring

$$R = \mathbb{Z}[x]/(x^{n-1} + \cdots + x + 1)$$

(see (28.1)). The action of  $y$  on  $\bar{R}$  is given by

$$y\alpha = \bar{\alpha}y, \quad \alpha \in R,$$

where the bar denotes the automorphism of  $R$  defined by  $x \rightarrow x^{-1}$ .

Since  $\mathbb{Q}$  is  $\mathbb{Z}$ -flat, tensoring with  $\mathbb{Q}$  over  $\mathbb{Z}$  gives a new fiber product (see (42.2))

$$\begin{array}{ccc} \mathbb{Q}G & \longrightarrow & \mathbb{Q}[y] \\ \downarrow & & \downarrow \\ K^\circ[y] & \longrightarrow & 0, \end{array}$$

where

$$K = \mathbb{Q}[x]/(x^{n-1} + \cdots + x + 1) \cong \coprod_{\substack{d|n \\ d>1}} \mathbb{Q}[x]/(\Phi_d(x)) = \coprod_{d|n} K_d.$$

Here,  $\Phi_d(x)$  is the  $d$ -th cyclotomic polynomial. Thus we obtain

$$\mathbb{Q}G \cong \mathbb{Q}[y] \oplus \coprod_{\substack{d|n \\ d>1}} K_d^\circ[y],$$

which agrees with the formula in (7.39). In this connection, see also (34.43).

**(42.5) Example (Wall square; see C. T. C. Wall [74b]).** Let  $R$  be a Dedekind domain with quotient field  $K \neq R$ , and let  $\Lambda$  be an  $R$ -order in a f.d.  $K$ -algebra  $A$ . For each maximal ideal  $P$  of  $R$ , let  $\Lambda_P, A_P$ , etc., denote  $P$ -adic completions.

The *adèle ring*  $\hat{A}$  is defined as

$$\hat{A} = \{(a_P) \in \prod_P A_P : a_P \in \Lambda_P \text{ a.e.}\}.$$

The diagonal mapping  $A \rightarrow \hat{A}$  is a ring homomorphism. Define

$$\hat{\Lambda} = \prod_P \Lambda_P = \text{ring of integral adèles},$$

a subring of  $\hat{A}$ . By (4.21) we have  $A \cap \hat{\Lambda} = \Lambda$ , so there is a fiber product

$$\begin{array}{ccc} \Lambda & \rightarrow & \hat{\Lambda} \\ \downarrow & & \downarrow \\ A & \rightarrow & \hat{A}, \end{array}$$

called a *Wall square*.

Returning to the general fiber product (42.1), we note that each  $A_i$ -module can be viewed as  $A$ -module via  $f_i$ , and likewise each  $\bar{A}$ -module becomes an  $A_i$ -module via  $g_i$ , for  $i = 1, 2$ . Given any  $P \in \mathcal{P}(A)$ , applying  $* \otimes_A P$  to (42.2) yields a new ses, and thus we obtain a fiber product of left  $A$ -modules:

$$(42.6) \quad \begin{array}{ccc} P & \longrightarrow & A_1 \otimes_A P = P_1 \\ \downarrow & & \downarrow \\ P_2 = A_2 \otimes_A P & \longrightarrow & \bar{A} \otimes_A P. \end{array}$$

Then  $P_i \in \mathcal{P}(A_i)$ , and there is a canonical  $\bar{A}$ -isomorphism

$$\kappa: \bar{A} \otimes_{A_1} P_1 \cong \bar{A} \otimes_{A_2} P_2.$$

Then we have

$$(42.7) \quad P \cong \{(x_1, x_2) : x_i \in P_i, \kappa(\bar{x}_1) = \bar{x}_2\}$$

where bars denote images in  $\bar{A} \otimes P$ .

We wish to reverse this procedure: starting with a pair of projective modules  $P_i \in \mathcal{P}(A_i)$ ,  $i = 1, 2$ , and with some  $\bar{A}$ -isomorphism  $\varphi: \bar{P}_1 \cong \bar{P}_2$  (where  $\bar{P}_i$  means  $\bar{A} \otimes P_i$ ), we want to find a module  $P \in \mathcal{P}(A)$  for which  $A_i \otimes_A P \cong P_i$ ,  $i = 1, 2$ . For this purpose, we define

$$(42.8) \quad (P_1, P_2, \varphi) = \{(x, y) : x \in P_1, y \in P_2, \varphi(\bar{x}) = \bar{y}\}.$$

Then  $(P_1, P_2, \varphi)$  is an  $A$ -module, since for  $a \in A$ ,  $(x, y) \in (P_1, P_2, \varphi)$ , we have  $a(x, y) = (ax, ay)$ , and

$$\varphi(\overline{ax}) = \bar{a}\varphi(\bar{x}) = \overline{ay}.$$

Thus, (42.7) is just the assertion that  $P \cong (P_1, P_2, \kappa)$ . We note that  $A = (A_1, A_2, 1)$ , and that

$$(P_1, P_2, \varphi) \oplus (Q_1, Q_2, \psi) \cong (P_1 \oplus Q_1, P_2 \oplus Q_2, \varphi \oplus \psi).$$

Further, each map  $f_i: P_i \rightarrow Q_i$  in  $\mathcal{P}(A_i)$  yields a map  $\bar{f}_i: \bar{P}_i \rightarrow \bar{Q}_i$ . We now define a *morphism* of triples

$$(f, g): (P_1, P_2, \varphi) \rightarrow (Q_1, Q_2, \psi)$$

to consist of a pair  $f: P_1 \rightarrow Q_1$ ,  $g: P_2 \rightarrow Q_2$ , such that  $\bar{g}\varphi = \psi\bar{f}$ . As anticipated by the notation, the pair  $(f, g)$  induces an  $A$ -homomorphism of triples, by means of

$$(f, g)(x, y) = (fx, gy) \quad \text{for } (x, y) \in (P_1, P_2, \varphi).$$

Indeed, we have

$$\psi(\bar{f}x) = \psi\bar{f}(\bar{x}) = \bar{g}\varphi(\bar{x}) = \bar{g}\bar{y} = \overline{gy}.$$

Further,  $(f, g)$  is an isomorphism if and only if both  $f$  and  $g$  are isomorphisms. However, the module  $(P_1, P_2, \varphi)$  defined in (42.8) need not be  $A$ -projective, and we shall impose some additional hypotheses to ensure this.

For convenience, we shall denote  $A^{(n)}$  simply by  $A^n$ . Further, we set

$$\bar{A}_i = \bar{A} \otimes_{A_i} A_i \cong \bar{A}, \quad i = 1, 2,$$

and we identify both  $\bar{A}_1$  and  $\bar{A}_2$  with  $\bar{A}$  hereafter. We need two easy lemmas:

**(42.9) Lemma.** *Let  $\psi, \psi' \in GL_n(\bar{A})$  be such that*

$$\psi' = \bar{\varphi}_2 \psi \bar{\varphi}_1 \quad \text{for some } \varphi_i \in GL_n(A_i), \quad i = 1, 2.$$

*Then there is an isomorphism of  $A$ -modules*

$$(A_1^n, A_2^n, \psi) \cong (A_1^n, A_2^n, \psi').$$

*Proof.* The isomorphism is given by

$$(x, y) \in (A_1^n, A_2^n, \psi) \rightarrow (\varphi_1^{-1}x, \varphi_2y) \in (A_1^n, A_2^n, \psi').$$

As we shall see in (42.13), the converse of the lemma holds under the additional hypothesis that either  $g_1$  or  $g_2$  is surjective.

**(42.10) Lemma.** *Suppose that in the fiber product (42.1), either  $g_1$  or  $g_2$  is*

surjective. Then

(i) For all  $\varphi \in E(n, \bar{A})$ ,

$$(A_1^n, A_2^n, \varphi) \cong A^n.$$

(ii) For all  $\varphi \in GL_n(\bar{A})$ , we have

$$(A_1^n, A_2^n, \varphi) \oplus (A_1^n, A_2^n, \varphi^{-1}) \cong A^{2n},$$

and therefore

$$(A_1^n, A_2^n, \varphi) \in \mathcal{P}(A).$$

*Proof.* If (say)  $g_1$  is surjective, every elementary matrix over  $\bar{A}$  lifts to one over  $A_1$ , so (i) follows from (42.9). Then (ii) is immediate, using the identity (40.25).

We are now ready to prove

**(42.11) Theorem (Milnor).** Suppose that in the fiber product (42.1), either  $g_1$  or  $g_2$  is surjective. Let  $P_i \in \mathcal{P}(A_i)$ ,  $i = 1, 2$ , and let  $\varphi: \bar{P}_1 \cong \bar{P}_2$  be an  $\bar{A}$ -isomorphism, where  $\bar{P}_i = \bar{A} \otimes_{A_i} P_i$ . Then the  $A$ -module

$$(P_1, P_2, \varphi) = \{(x, y) : x \in P_1, y \in P_2, \varphi(\bar{x}) = \bar{y}\}$$

lies in  $\mathcal{P}(A)$ . Further,

$$(42.12) \quad A_i \otimes_A (P_1, P_2, \varphi) \cong P_i, \quad i = 1, 2.$$

Finally, let  $Q_i \in \mathcal{P}(A_i)$ ,  $i = 1, 2$ , and let  $\varphi': \bar{Q}_1 \cong \bar{Q}_2$  be an  $\bar{A}$ -isomorphism. Then  $(P_1, P_2, \varphi) \cong (Q_1, Q_2, \varphi')$  as  $A$ -modules if and only if

$$\varphi' = \bar{v}\varphi\bar{\mu}^{-1} \text{ for some isomorphisms } \mu: P_1 \cong Q_1, \quad v: P_2 \cong Q_2.$$

*Proof.* Choose  $N_i \in \mathcal{P}(A_i)$  with  $P_i \oplus N_i \cong A_i^n$ ,  $i = 1, 2$ . Then  $\varphi$  gives rise to an isomorphism  $\psi$ , defined by composition of maps:

$$\bar{A}^n \oplus \bar{N}_1 \cong \overline{P_2 \oplus N_2 \oplus N_1} \cong \overline{P_1 \oplus N_2 \oplus N_1} \cong \bar{A}^n \oplus \bar{N}_2.$$

Therefore by (42.10),

$$(P_1, P_2, \varphi) \oplus (A_1^n \oplus N_1, A_2^n \oplus N_2, \psi) \cong (A_1^{2n}, A_2^{2n}, \varphi \oplus \psi) \in \mathcal{P}(A).$$

This shows that  $(P_1, P_2, \varphi) \in \mathcal{P}(A)$ . Also, since (42.12) holds for triples of the form  $(A_1^{2n}, A_2^{2n}, \varphi \oplus \psi)$ , it also holds for direct summands of such triples.

To complete the proof, let  $M = (P_1, P_2, \varphi)$ ,  $N = (Q_1, Q_2, \psi)$ . If  $\varphi' = \bar{v}\varphi\bar{\mu}^{-1}$  for some  $\mu, v$ , then  $(\mu, v): M \cong N$  is the desired  $A$ -isomorphism. Conversely, given

an  $A$ -isomorphism  $\rho: M \cong N$ , let

$$\sigma_i: A_i \otimes_A M \cong P_i, \quad \tau_i: A_i \otimes_A N \cong Q_i, \quad i = 1, 2,$$

be the isomorphisms in (42.12). Consider the commutative diagram

$$\begin{array}{ccccccc} P_1 = \bar{A} \otimes_{A_1} P_1 & \xrightarrow{1 \otimes \sigma_1^{-1}} & \bar{A} \otimes_{A_1} A_1 \otimes_A M & \xrightarrow{1 \otimes 1 \otimes \rho} & \bar{A} \otimes_{A_1} A_1 \otimes_A N & \xrightarrow{1 \otimes \tau_1} & \bar{A} \otimes_{A_1} Q_1 = \bar{Q}_1 \\ \varphi \downarrow & & \downarrow & & \downarrow & & \varphi' \downarrow \\ \bar{P}_2 = \bar{A} \otimes_{A_2} P_2 & \xrightarrow{1 \otimes \sigma_2^{-1}} & \bar{A} \otimes_{A_2} A_2 \otimes_A M & \xrightarrow{1 \otimes 1 \otimes \rho} & \bar{A} \otimes_{A_2} A_2 \otimes_A N & \xrightarrow{1 \otimes \tau_2} & \bar{A} \otimes_{A_2} Q_2 = \bar{Q}_2 \end{array}$$

Define

$$\mu = \tau_1(1 \otimes \rho)\sigma_1^{-1}: P_1 \rightarrow Q_1, \quad \text{and} \quad \nu = \tau_2(1 \otimes \rho)\sigma_2^{-1}: P_2 \rightarrow Q_2.$$

Then  $\mu, \nu$  are isomorphisms for which  $\varphi'\bar{\mu} = \bar{\nu}\varphi$ , as desired.

The main result of the section is as follows:

**(42.13) Milnor's Theorem.** *Given a fiber product (42.1) in which at least one of the maps  $g_1$  and  $g_2$  is surjective, there is an exact Mayer-Vietoris sequence*

$$\begin{aligned} (42.14) \quad K_1(A) &\xrightarrow{(f_1, f_2)} K_1(A_1) \times K_1(A_2) \xrightarrow{g_1 \times (1/g_2)} K_1(\bar{A}) \\ &\xrightarrow{\partial} K_0(A) \xrightarrow{(f_1, f_2)} K_0(A_1) \oplus K_0(A_2) \xrightarrow{g_1 - g_2} K_0(\bar{A}), \end{aligned}$$

where  $g_1 \times (1/g_2): (x, y) \rightarrow g_1(x)/g_2(y)$ .

*Proof.* A ring homomorphism  $\varphi: A \rightarrow B$  induces homomorphisms of groups  $K_i(A) \rightarrow K_i(B)$ ,  $i = 0, 1$ , so all of the above maps are well-defined, except that we must describe the connecting homomorphism  $\partial$ . Identifying  $\bar{A}_1$  with  $\bar{A}_2$ , each  $\varphi: \bar{A}_1^n \cong \bar{A}_2^n$  may be viewed as an element of  $GL_n(\bar{A})$ . Put

$$M(\varphi) = (\bar{A}_1^n, \bar{A}_2^n, \varphi) \in \mathcal{P}(A).$$

By (42.10),  $M(\varphi) \cong A^n$  if  $\varphi \in E_n(\bar{A})$ . We now define

$$\partial: K_1(\bar{A}) \rightarrow K_0(A) \quad \text{by} \quad \partial(\varphi) = [M(\varphi)] - [A^n] \quad \text{for } \varphi \in GL_n(A).$$

Since  $\partial \begin{pmatrix} \varphi & 0 \\ 0 & 1 \end{pmatrix} = \partial(\varphi)$ , and since  $\partial$  is trivial on  $E(\bar{A})$ , it follows that  $\partial$  is well-defined on  $K_1(\bar{A})$ . To show that  $\partial$  is a homomorphism, let  $\varphi, \psi \in GL_n(\bar{A})$ .

Then

$$\begin{aligned}\partial \begin{pmatrix} \varphi & 0 \\ 0 & \psi \end{pmatrix} &= \left[ M \begin{pmatrix} \varphi & 0 \\ 0 & \psi \end{pmatrix} \right] - [A^{2n}] = [M(\varphi)] - [A^n] + [M(\psi)] - [A^n] \\ &= \partial(\varphi) + \partial(\psi).\end{aligned}$$

However,

$$\begin{pmatrix} \varphi & 0 \\ 0 & \psi \end{pmatrix} = \begin{pmatrix} \varphi\psi & 0 \\ 0 & 1 \end{pmatrix} \text{ in } K_1(\bar{A})$$

by (40.25), so  $\partial(\varphi\psi) = \partial(\varphi) + \partial(\psi)$  as desired. Using (42.9)–(42.11), it is easily verified that the composite of two successive maps in (42.14) is 0.

We proceed to verify exactness at each position. First, let  $(x_1, x_2) \in \ker(g_1 - g_2)$ . We may write

$$x_i = [P_i] - [A_i^n], \quad P_i \in \mathcal{P}(A_i), \quad i = 1, 2,$$

where  $n$  is independent of  $i$ . Then  $[\bar{P}_1] = [\bar{P}_2]$  in  $K_0(\bar{A})$ , so  $\bar{P}_1$  is stably isomorphic to  $\bar{P}_2$  as  $\bar{A}$ -module. Increasing  $P_1$  and  $P_2$ , we may assume (after changing notation) that  $\bar{P}_1 \cong \bar{P}_2$ . By (42.11), there exists a module  $P \in \mathcal{P}(A)$  such that  $P_i = A_i \otimes_A P$ ,  $i = 1, 2$ ; then  $(x_1, x_2) = (f_1, f_2)[P]$ , so  $\ker(g_1 - g_2) = \text{im}(f_1, f_2)$ .

Next, let  $x = [P] - [A^n] \in \ker(f_1, f_2)$ , where  $P \in \mathcal{P}(A)$ . Writing  $P_i = A_i \otimes P$ , we have  $[P_i] = [A_i^n]$  in  $K_0(A_i)$ ,  $i = 1, 2$ . Increasing  $P$  and changing notation, we may assume that  $P_i \cong A_i^n$ ,  $i = 1, 2$ . If  $\kappa: \bar{P}_1 \cong \bar{P}_2$  is the canonical isomorphism, there is a commutative diagram

$$\begin{array}{ccc} \bar{P}_1 & \cong & \bar{A}_1^n \\ \kappa \downarrow & & \varphi \downarrow \\ \bar{P}_2 & \cong & \bar{A}_2^n \end{array}$$

for some  $\varphi \in GL_n(\bar{A})$ . Therefore  $P = (P_1, P_2, \kappa) \cong (A_1^n, A_2^n, \varphi)$ , so  $x = [M(\varphi)] - [A^n] = \partial(\varphi)$ , as desired.

We suppose next that  $\varphi \in GL_n(\bar{A})$  is such that  $\partial(\varphi) = 0$ , that is,  $[M(\varphi)] = [A^n]$  in  $K_0(A)$ . Replacing  $\varphi$  by  $\begin{pmatrix} \varphi & \mathbf{0} \\ \mathbf{0} & \mathbf{I} \end{pmatrix}$  if need be, and changing notation, we may then assume that  $M(\varphi) \cong A^n$ , that is,

$$(A_1^n, A_2^n, \varphi) \cong (A_1^n, A_2^n, 1).$$

Then  $\varphi \in \text{im } g_1 \times 1/g_2$  by (42.11).

Finally, let  $\alpha_i \in GL_n(A_i)$ ,  $i = 1, 2$ , be such that  $\bar{\alpha}_1 = \bar{\alpha}_2$  in  $K_1(\bar{A})$ . Then

$$\begin{pmatrix} \bar{\alpha}_1 & \mathbf{0} \\ \mathbf{0} & \mathbf{I} \end{pmatrix} \in \begin{pmatrix} \bar{\alpha}_2 & \mathbf{0} \\ \mathbf{0} & \mathbf{I} \end{pmatrix} \cdot E_m(\bar{A}).$$

for some  $m$  and some identity matrix  $\mathbf{I}$ . Replacing  $\alpha_i$  by  $\begin{pmatrix} \alpha_i & \mathbf{0} \\ \mathbf{0} & \mathbf{I} \end{pmatrix}$  leaves the image of  $\alpha_i$  in  $K_1(A_i)$  unchanged, and elements of  $E_m(\bar{A})$  are trivial in  $K_1(\bar{A})$ , so we now assume (after changing notation) that  $\bar{\alpha}_1 = \bar{\alpha}_2$ . It follows at once from the fiber product

$$(42.15) \quad \begin{array}{ccc} GL_n(A) & \longrightarrow & GL_n(A_1) \\ \downarrow & & \downarrow \\ GL_n(A_2) & \longrightarrow & GL_n(\bar{A}) \end{array}$$

that the pair  $(\alpha_1, \alpha_2)$  lifts to an element  $\alpha \in GL_n(A)$ . Thus the sequence (42.14) is exact at  $K_1(A_1) \times K_1(A_2)$ , and the proof is complete.

As an illustration, we give a calculation due to Rim [59]:

**(42.16) Example.** Let  $G = \langle x : x^p = 1 \rangle$ ,  $p$  prime, and put

$$\bar{\mathbb{Z}} = \mathbb{Z}/p\mathbb{Z}, \quad R = \mathbb{Z}[x]/(\Phi_p(x)) = \mathbb{Z}[\omega],$$

where  $\omega$  is a primitive  $p$ -th root of 1. There is a fiber product

$$\begin{array}{ccc} \mathbb{Z}G & \longrightarrow & R \\ \downarrow & & \downarrow \\ \mathbb{Z} & \longrightarrow & \mathbb{Z} \end{array}$$

in which all maps are surjective. The Mayer-Vietoris sequence becomes

$$K_1(\mathbb{Z}G) \rightarrow K_1(\mathbb{Z}) \times K_1(R) \xrightarrow{h} K_1(\bar{\mathbb{Z}}) \rightarrow K_0(\mathbb{Z}G) \rightarrow K_0(\mathbb{Z}) \oplus K_0(R) \rightarrow K_0(\bar{\mathbb{Z}}).$$

Now  $K_1(\bar{\mathbb{Z}}) \cong \bar{\mathbb{Z}}$ ; and  $R \rightarrow \bar{\mathbb{Z}}$  is surjective by the proof of (34.31), so  $h$  is surjective. Thus the sequence

$$0 \rightarrow K_0(\mathbb{Z}G) \rightarrow \mathbb{Z} \oplus K_0(R) \rightarrow \mathbb{Z} \rightarrow 0$$

is exact, and so  $K_0(\mathbb{Z}G) \cong K_0(R)$ . Finally,  $K_0(R) \cong \mathbb{Z} \oplus \text{Cl } R$  by (38.52). For more complicated calculations of this type, see Chapter 6.

**(42.17) Remark.** In §47 we shall define a Milnor group  $K_2(A)$ , and shall prove that starting with a fiber product (42.1) in which both  $g_1$  and  $g_2$  are surjective, the exact sequence (42.14) can be extended to the left:

$$K_2(A) \rightarrow K_2(A_1) \times K_2(A_2) \rightarrow K_2(\bar{A}) \rightarrow K_1(A) \rightarrow K_1(A_1) \times K_1(A_2) \rightarrow \dots$$

However, as shown by Swan [71], the sequence does not in general extend further to the left, despite the existence of higher K-groups  $K_n$ ,  $n \geq 3$ .

We conclude this section by showing that for a Wall square as in (42.5), the analogues of (42.10)–(42.13) remain valid, despite the fact that neither of the maps  $A \rightarrow \hat{A}$  and  $\Lambda \rightarrow \hat{\Lambda}$  is surjective. We shall follow the treatment of this topic given by Swan [80].

Keeping the notation of (42.5), set

$$\hat{R} = \prod_P R_P, \quad \hat{K} = \{(\alpha_P) \in \prod_P A_P : \alpha_P \in R_P \text{ a.e.}\},$$

where  $P$  ranges over all maximal ideals of  $R$ . Since  $\Lambda$  is an  $R$ -lattice, and  $A$  is  $K$ -free, we have

$$\hat{\Lambda} = \hat{R} \otimes_R \Lambda, \quad \hat{A} = \hat{K} \otimes_K A.$$

For each  $P$ , the ring  $\Lambda_P$  has its natural  $P$ -adic topology, in which  $\{P^n \Lambda_P : n \geq 0\}$  is a fundamental system of neighborhoods of 0. Since  $\hat{\Lambda} = \prod_P \Lambda_P$ , it acquires the product topology. We then topologize  $\hat{A}$  by requiring  $\hat{\Lambda}$  to be an open subgroup of  $\hat{A}$ . Note that  $K$  is dense in  $\hat{K}$  (by the Strong Approximation Theorem), and that  $\hat{R}$  is an open subgroup of  $\hat{K}$ .

The topology on  $\hat{A}$  extends to a topology on  $\hat{A}^n$  for each  $n$ , and hence to each summand of  $\hat{A}^n$ . Thus, each  $Y \in \mathcal{P}(\hat{A})$  has a topology, and likewise so does each  $X \in \mathcal{P}(\hat{\Lambda})$ .

**(42.18) Proposition.** *Given a Wall square (42.5), let  $V \in \mathcal{P}(A)$  and  $X \in \mathcal{P}(\hat{\Lambda})$  be such that*

$$\hat{K} \otimes_K V \cong \hat{K} \otimes_{\hat{R}} X$$

*as  $\hat{A}$ -modules. Then there exists an  $M \in \mathcal{P}(\Lambda)$  such that*

$$K \otimes_R M \cong V, \quad \hat{R} \otimes_R M \cong X,$$

*these isomorphisms being consistent with the given isomorphism.*

*Proof.* Replacing  $V$  by an isomorphic copy, we may assume that

$$\hat{K} \otimes_{\hat{R}} X = \hat{K} \otimes_K V = \hat{V},$$

with both  $V$  and  $X$  embedded in  $\hat{V}$ . Define  $M = X \cap V$ . Now  $V$  is dense in  $\hat{V}$ , since  $K$  is dense in  $\hat{K}$ . Also,  $X$  is an open subset of  $\hat{V}$  since  $\hat{R}$  is an open subgroup of  $\hat{K}$ . It follows at once that  $M$  is dense in  $X$ , and therefore  $\hat{R}M = X$ . Since  $\hat{V} = \hat{K}X = \hat{K} \cdot KM$ , we conclude that  $KM = V$ .

It remains for us to check that  $M \in \mathcal{P}(\Lambda)$ . We may choose a finite set of elements  $\{m_i\}$  from  $M$  such that  $\Sigma \hat{R}m_i = X$ . Then

$$\hat{R} \otimes_R (M / \Sigma Rm_i) = 0,$$

so  $M = \Sigma Rm_i$  because  $\hat{R}$  is faithfully flat as  $R$ -module. Therefore  $M$  is a  $\Lambda$ -lattice, and then  $M \in \mathcal{P}(\Lambda)$  by (8.19). This completes the proof. (The result should be compared with (4.21iv) and MO(5.2ii).)

Having established the analogue of (42.11), we now obtain

**(42.19) Theorem (C. T. C. Wall).** *Given a Wall square (42.5), there is an exact Mayer-Vietoris sequence*

$$(40.20) \quad K_1(\Lambda) \rightarrow K_1(A) \times K_1(\hat{\Lambda}) \rightarrow K_1(\hat{A}) \rightarrow K_0(\Lambda) \rightarrow K_0(A) \oplus K_0(\hat{\Lambda}) \rightarrow K_0(\hat{A}).$$

*Proof.* The proof of (42.13) carries over to the present case, except for that part of the argument which shows that  $M(\varphi) \cong A^n$  whenever  $\varphi \in E(n, \hat{A})$ .

Replacing  $\varphi$  by  $\begin{pmatrix} \varphi & 0 \\ 0 & 1 \end{pmatrix}$  if need be, and changing notation, we may assume that  $n \geq 3$ . Let  $E(\hat{A})$ ,  $E(A)$ , etc., be the elementary subgroups defined in §40C, and keep the notation of (40.22) and (40.23). We are going to show that the Wall square is *E-surjective* in the sense of Bass [68, page 360, Def. 3.3], that is,

$$(42.21) \quad \varphi = \varphi_1 \varphi_2 \quad \text{for some } \varphi_1 \in E(A), \quad \varphi_2 \in E(\hat{\Lambda}).$$

Once this is known, we obtain  $[M(\varphi)] = [A^n]$  in  $K_0(\hat{\Lambda})$  by (42.9).

To prove (42.21), we note that  $\hat{A} = A + \hat{\Lambda}$  by Exercise 42.5, and therefore  $E(\hat{A})$  is generated by its subgroups  $E(A)$  and  $E(\hat{\Lambda})$ . Set

$$E(A)E(\hat{\Lambda}) = \{\mathbf{XY} : \mathbf{X} \in E(A), \mathbf{Y} \in E(\hat{\Lambda})\}.$$

It suffices to prove that for each  $\mathbf{X} \in E(A)$  and each elementary matrix  $\mathbf{E}_{ij}(y)$ ,  $y \in \hat{\Lambda}$ , we have

$$\mathbf{X}^{-1}\mathbf{E}_{ij}(y)\mathbf{X} \in E(A)E(\hat{\Lambda}).$$

Choose a nonzero  $r \in R$  such that both  $r\mathbf{X}$  and  $r\mathbf{X}^{-1}$  have entries in  $\Lambda$ . Since  $\Lambda/r^4\Lambda \cong \hat{\Lambda}/r^4\hat{\Lambda}$ , we may write  $y = z + r^4w$ ,  $z \in \Lambda$ ,  $w \in \hat{\Lambda}$ . Then

$$\mathbf{X}^{-1}\mathbf{E}_{ij}(y)\mathbf{X} = (\mathbf{X}^{-1}\mathbf{E}_{ij}(z)\mathbf{X})(\mathbf{X}^{-1}\mathbf{E}_{ij}(r^4w)\mathbf{X}),$$

and the first factor on the right surely lies in  $E(A)$ . To handle the second factor, choose  $k \neq i, j$ , and use formula (40.23) to obtain

$$\mathbf{X}^{-1}\mathbf{E}_{ij}(r^4w)\mathbf{X} = [\mathbf{X}^{-1}\mathbf{E}_{ik}(r^2)\mathbf{X}, \mathbf{X}^{-1}\mathbf{E}_{kj}(r^2w)\mathbf{X}].$$

Using the notation of (40.22), we have

$$\mathbf{X}^{-1}\mathbf{E}_{ik}(r^2)\mathbf{X} = \mathbf{I} + (r\mathbf{X}^{-1})\mathbf{e}_{ik}(r\mathbf{X}) \in GL(\Lambda),$$

where  $\mathbf{I}$  is the identity matrix. Likewise,  $\mathbf{X}^{-1}\mathbf{E}_{kj}(r^2w)\mathbf{X} \in GL(\hat{\Lambda})$ , so the above commutator lies in the commutator subgroup  $GL(\hat{\Lambda})$ , that is, in  $E(\hat{\Lambda})$ . This completes the proof of (42.21), as well as that of Wall's Theorem 42.19.

**(42.22) Remarks.** (i) Let  $\varphi: A \rightarrow B$  be a homomorphism of arbitrary rings, and let  $S$  be a multiplicative subset of the center of  $A$  such that no element of  $S$  is a zero divisor in  $A$ . Suppose that  $\varphi(S)$  lies in the center of  $B$ , and consists only of non-zero divisors in  $B$ . Let  $S^{-1}A$  denote the quotient ring of  $A$  relative to  $S$  (see §4A), and  $S^{-1}B$  that of  $B$  relative to  $\varphi(S)$ . Assume further that for each  $s \in S$ ,  $\varphi$  induces an isomorphism (of  $A$ -modules)  $A/sA \cong B/sB$ . The square

$$\begin{array}{ccc} A & \longrightarrow & B \\ \downarrow & & \downarrow \\ S^{-1}A & \longrightarrow & S^{-1}B \end{array}$$

is called a *Karoubi square*. (For example, the Wall square (42.5) is of this form, if we take  $S = R - \{0\}$ .)

Karoubi proved that such squares always yield Mayer-Vietoris sequences of type (42.14), and Murthy showed that every Karoubi square is  $E$ -surjective. For proofs and generalizations, see Swan [80].

(ii) Given a Wall square (42.5), there is an exact sequence  $\cdots \rightarrow K_n(\Lambda) \rightarrow K_n(A) \oplus K_n(\hat{\Lambda}) \rightarrow K_n(\hat{A}) \rightarrow K_{n-1}(\Lambda) \rightarrow \cdots \rightarrow K_0(\hat{A})$ , where the  $\{K_n\}$  are the Quillen  $K$ -groups. This follows from Quillen's Localization Sequence in (40.18); for details, see Swan [80, §5].

## §42. Exercises

1. Let  $S$  and  $T$  be multiplicatively closed subsets of the center of ring  $A$  such that  $As + At = A$  for all  $s \in S$ ,  $t \in T$ , and let  $ST = \{st: s \in S, t \in T\}$ . Show that there is a fiber product diagram

$$\begin{array}{ccc} A & \longrightarrow & S^{-1}A \\ \downarrow & & \downarrow \\ T^{-1}A & \longrightarrow & (ST)^{-1}A. \end{array}$$

2. Let  $P = (P_1, P_2, \varphi)$ ,  $P' = (P'_1, P'_2, \varphi')$  as in (42.8). Show that  $P \cong P'$  if  $\varphi'\bar{\alpha}_1 = \bar{\alpha}_2\varphi$  for some  $\alpha_i: P_i \cong P'_i$ ,  $i = 1, 2$ .

3. Assume  $g_1$  surjective in (42.1), and let  $\varphi \in GL_n(\bar{A})$ . Let  $\mu \in E_{2n}(A_1)$  be such that  $\bar{\mu} = \begin{pmatrix} \varphi & 0 \\ 0 & \varphi^{-1} \end{pmatrix}$ , and let  $\mathbf{e}_i = \begin{pmatrix} \mathbf{I} & 0 \\ 0 & 0 \end{pmatrix} \in M_{2n}(A_i)$ ,  $\mathbf{e} = (\mu^{-1}\mathbf{e}_1\mu, \mathbf{e}_2) \in M_{2n}(A_1) \oplus M_{2n}(A_2)$ . Show that there is a fiber product diagram

$$\begin{array}{ccc} M_{2n}(A) & \longrightarrow & M_{2n}(A_1) \\ \downarrow & & \downarrow \\ M_{2n}(A_2) & \longrightarrow & M_{2n}(\bar{A}), \end{array}$$

and that  $\mathbf{e} \in M_{2n}(A)$  is an idempotent for which

$$M(\varphi) \cong A^{2n} \cdot \mathbf{e}.$$

4. Let  $k$  be a field,  $A = k + x^2k[x]$ , where  $x$  is an indeterminate over  $k$ . Use the fiber product

$$\begin{array}{ccc} A & \longrightarrow & k[x] \\ \downarrow & & \downarrow \\ k & \longrightarrow & k[x]/(x^2) \end{array}$$

to prove that

$$K_0(A) \cong \mathbb{Z} \oplus k^+, \quad k^+ = \text{additive group of } k.$$

5. In the Wall square (42.5), prove that  $A + \hat{\Lambda} = \hat{A}$ .

[Hint: Use the Strong Approximation Theorem 4.8.]

6. Given a Wall square (42.5), deduce the exactness of

$$K_1(A) \times K_1(\hat{\Lambda}) \rightarrow K_1(\hat{A}) \xrightarrow{\partial'} K_0(\Lambda) \rightarrow K_0(A) \oplus K_0(\hat{\Lambda}) \rightarrow K_0(\hat{A})$$

directly from the Localization Sequence 40.17

$$K_1(\Lambda) \rightarrow K_1(A) \xrightarrow{\partial} K_0(\mathcal{T}) \rightarrow K_0(\Lambda) \rightarrow K_0(A).$$

[Hint (Swan [80], pages 165–166): For  $\varphi \in GL_n(\hat{A})$ ,  $\partial'(\varphi) = [\Lambda^n] - [(\hat{\Lambda}^n, A^n, \varphi)]$ , where the triple  $(\Lambda^n, A^n, \varphi)$  is defined as in (42.8), and is isomorphic to  $A^n \cap \varphi(\hat{\Lambda}^n)$ .]

7. Consider a fiber product as in Exercise 1, in which no element of  $S$  is a zero divisor. Show that the analogues of (42.18)–(42.21) are valid for this case.

[Hint: The result is due to Murthy; see Gersten [73, Problem 4].] (Ref. in Swan [80, p. 164].)

8. Given a fiber product (42.3) in which the ring  $A$  is left noetherian, show that there exists an exact sequence of groups

$$G_0(A/(I+J)) \rightarrow G_0(A/I) \oplus G_0(A/J) \rightarrow G_0(A/(I \cap J)) \rightarrow 0.$$

[Hint: See Bass [81, Th. 4.2]. The result can be used to provide a proof of Lenstra's formula (39.25).]

### §43. $K$ -THEORY OF POLYNOMIAL RINGS

Let  $R$  be a left noetherian ring of finite global dimension, and let  $R' = R[x_1, \dots, x_n]$ , where the  $\{x_i\}$  are indeterminates which commute with each other and with all

elements of  $R$ . Ground ring extension  $R' \otimes_R *$  gives rise to homomorphisms  $K_i(R) \rightarrow K_i(R')$ ,  $i = 0, 1$ . Here, we shall use the ideas of §38C to prove:

**(43.1) Theorem (Grothendieck).**  $K_0(R) \cong K_0(R')$ .

**(43.2) Theorem (Bass-Heller-Swan).**  $K_1(R) \cong K_1(R')$ .

When  $R$  is a P.I.D., this gives  $K_0(R') \cong K_0(R) \cong \mathbb{Z}$ , and therefore every  $P \in \mathcal{P}(R')$  is stably free. This result led Serre to conjecture that each such  $P$  is in fact free. Seshadri [58] proved a special case of this conjecture (see (43.8)), and the general result was established independently by Quillen and Suslin. They proved a stronger result:

**Quillen-Suslin Theorem.** *Let  $R$  be a Dedekind domain, and let  $R' = R[x_1, \dots, x_n]$  be a polynomial domain over  $R$ . Then each  $P \in \mathcal{P}(R')$  is of the form  $P = R' \otimes_R X$  for some  $X \in \mathcal{P}(R)$ . If  $R$  is a P.I.D., each  $P \in \mathcal{P}(R')$  is  $R'$ -free.*

We shall content ourselves with a proof of Seshadri's Theorem. For a proof of the Quillen-Suslin Theorem, see Lam [78] or Rotman [79].

Our first task is to establish that  $K_0(R) \cong K_0(R')$  whenever  $R$  is a left noetherian ring of finite global dimension. We need to know that  $R'$  inherits these properties from  $R$ . Let us recall a well-known result (see, e.g., Jacobson [80, §7.9]):

**(43.3) Hilbert Basis Theorem.** *If  $R$  is a left noetherian ring, then so is  $R[x_1, \dots, x_n]$ .*

Thus, if  $R$  is left noetherian, so is  $R'$ . Our next step is to show that if  $R$  has finite global dimension, then so does  $R'$ . The proof of this result depends on the characteristic sequence of an endomorphism, as we now explain. Suppose that  $R$  is arbitrary, and let  $R' = R[x]$ . For each  $R$ -module  $M$ , define  $M' = R' \otimes_R M$ . Each  $m' \in M'$  is uniquely expressible as a finite sum

$$m' = \sum_0^{\infty} x^i \otimes m_i, \quad m_i \in M, \quad m_i = 0 \text{ a.e.}$$

Now let  $\alpha \in \text{End}_R M$ , and make  $M$  into a left  $R'$ -module by letting  $x$  act as  $\alpha$  on  $M$ . We may then define an  $R'$ -homomorphism  $\alpha^*: M' \rightarrow M$  by

$$\alpha^*(h(x) \otimes m) = h(x)m = h(\alpha)m, \quad \text{for all } h(x) \in R', \quad m \in M.$$

There is also an  $R'$ -homomorphism

$$x - \alpha: M' \rightarrow M', \quad \text{where } (x - \alpha)(h(x) \otimes m) = xh(x) \otimes m - h(x) \otimes \alpha m.$$

The relation between the maps  $\alpha^*$  and  $x - \alpha$  is given by:

**(43.4) Characteristic Sequence of an Endomorphism.** *For each  $\alpha \in \text{End}_R M$ , there is an  $R'$ -exact sequence*

$$0 \rightarrow M' \xrightarrow{x - \alpha} M' \xrightarrow{\alpha^*} M \rightarrow 0,$$

*the characteristic sequence of  $\alpha$ .*

*Proof.* It is trivial to check that  $\alpha^* \circ (x - \alpha) = 0$ . Next, let  $\sum x^i \otimes m_i \in M'$ , where  $m_i = 0$  a.e., and let us try to solve

$$\sum_0^\infty x^i \otimes m_i = (x - \alpha) \sum x^i \otimes v_i = \sum_0^\infty (x^{i+1} \otimes v_i - x^i \otimes \alpha v_i)$$

for elements  $v_i \in M$ . Supposing that  $v_k = v_{k+1} = \dots = 0$ , we obtain a system of equations

$$m_0 = -\alpha v_0, \quad m_1 = -\alpha v_1 + v_0, \dots, m_k = v_{k-1},$$

and  $m_{k+1} = m_{k+2} = \dots = 0$ . Using the last  $k - 1$  equations above, we solve successively for  $v_{k-1}, \dots, v_0$ . Substituting into the first equation, we obtain

$$\alpha^k m_k + \alpha^{k-1} m_{k-1} + \dots + \alpha m_1 + m_0 = 0,$$

that is,  $\alpha^*(\sum x^i \otimes m_i) = 0$ . This condition is necessary and sufficient that  $\sum x^i \otimes m_i \in \text{im}(x - \alpha)$ , so  $\ker \alpha^* = \text{im}(x - \alpha)$ . Finally, the above formulas also show that if each  $m_i = 0$ , then each  $v_j = 0$ , and thus the map  $x - \alpha$  is injective. This completes the proof.

In (38.40), we defined the (left) global dimension of the ring  $R$ . We now prove a weak version of the Hilbert Syzygy Theorem:

**(43.5) Theorem.** *For any ring  $R$ ,*

$$\text{gl. dim. } R[x] \leq 1 + \text{gl. dim. } R.$$

*Therefore*

$$\text{gl. dim. } F[x_1, \dots, x_n] \leq n$$

*for any field  $F$  and any  $n \geq 1$ .*

*Proof.* Let  $R' = R[x]$ , and let  $\text{gl. dim. } R = m$ . Then for each  $R$ -module  $M$ , there exists an  $R$ -exact sequence

$$0 \rightarrow P_m \rightarrow \dots \rightarrow P_0 \rightarrow M \rightarrow 0, \quad \text{where } P_i \text{ is } R\text{-projective.}$$

Since  $R'$  is  $R$ -free,  $R' \otimes_R$  preserves exactness, and we obtain an  $R'$ -exact sequence

$$0 \rightarrow P'_m \rightarrow \dots \rightarrow P'_0 \rightarrow M' \rightarrow 0.$$

This shows that

$$(*) \quad \text{hd}_R M' \leq m \quad \text{for every } R\text{-module } M.$$

Now let  $M$  be any  $R'$ -module, and define  $\alpha \in \text{End}_R M$  as left multiplication by  $x$ . Viewing  $M$  as an  $R$ -module, and making it into an  $R'$ -module by letting  $x$  act as  $\alpha$ , we recover the original  $R'$ -module  $M$ . Consider now the characteristic sequence (43.4). By  $(*)$  and Exercise 38.11, we obtain

$$\text{hd}_{R'} M \leq \text{Max}(\text{hd}_{R'} M', 1 + \text{hd}_{R'} M') \leq m + 1.$$

This shows that  $\text{gl. dim. } R' \leq 1 + \text{gl. dim. } R$ . Since  $\text{gl. dim. } F = 0$ , the rest of the theorem is clear.

It is not hard to prove a stronger version of the above theorem:

$$\text{gl. dim. } R[x] = 1 + \text{gl. dim. } R,$$

for  $R$  left noetherian of finite global dimension (see Rotman [79, Th. 9.34]). Thus

$$\text{gl. dim. } F[x_1, \dots, x_n] = n, \quad \text{gl. dim. } R[x_1, \dots, x_n] = n + 1,$$

for  $F$  a field, and  $R$  a Dedekind domain not a field.

Now let  $R$  be any left noetherian ring of finite global dimension, and let  $R' = R[x_1, \dots, x_n]$ . Then  $R'$  has the same properties, by (43.3) and (43.5). In order to prove Grothendieck's result that  $K_0(R) \cong K_0(R')$ , it suffices to treat the case  $n = 1$ , so hereafter let  $R' = R[x]$ . The following proof was supplied to the authors by Swan.

The inclusion  $R \subseteq R'$  gives a commutative diagram

$$\begin{array}{ccc} K_0(R) & \xrightarrow{\varphi} & K_0(R') \\ \downarrow & & \downarrow \\ G_0(R) & \xrightarrow{\psi} & G_0(R'). \end{array}$$

The vertical maps are isomorphisms, by (38.51). Next, the surjection  $R' \rightarrow R'/xR' = R$  induces a map  $\varphi': K_0(R') \rightarrow K_0(R)$ . Clearly  $\varphi'\varphi = 1$ , so  $\varphi$  is injective, and it remains for us to show that  $\psi$  (and hence also  $\varphi$ ) is surjective.

Given any f.g.  $R'$ -module  $Y$ , there is an  $R'$ -exact sequence

$$0 \rightarrow L \rightarrow R' \otimes F \rightarrow Y \rightarrow 0,$$

where  $F = R^{(k)}$  for some finite  $k$ , and  $\otimes$  means  $\otimes_R$ . Then  $[Y] = [R' \otimes F] - [L]$

in  $G_0(R')$ , and we must show that  $[L] \in \text{im } \psi$ . Define

$$M = L \cap \bigoplus_{i=0}^n (x^i \otimes F) \supseteq N = L \cap \bigoplus_{i=0}^{n-1} (x^i \otimes F),$$

where  $L$  is viewed as  $R'$ -submodule of  $R' \otimes F = \bigoplus_0^\infty (x^i \otimes F)$ , and where  $n$  is chosen large enough that  $M$  contains a set of  $R'$ -generators of  $L$ . Note that  $M$  and  $N$  are f.g.  $R$ -submodules of  $L$ , and that

$$(*) \quad m \in M, \quad xm \in M \Rightarrow m \in N.$$

Now define  $\alpha \in \text{End}_R L$  as left multiplication by  $x$ . Since  $xN \subseteq M$ , the characteristic sequence (43.4), for  $\alpha$  acting on  $L$ , yields a sequence of  $R'$ -modules

$$(43.6) \quad 0 \rightarrow R' \otimes N \xrightarrow{x-\alpha} R' \otimes M \xrightarrow{\alpha^*} L \rightarrow 0.$$

The map  $\alpha^*$  is surjective, while  $x - \alpha$  is injective. We claim that the sequence (43.6) is exact, and it suffices to show that  $\ker \alpha^* \subseteq \text{im}(x - \alpha)$ , the reverse inclusion being obvious. Let

$$u = \sum_{i=0}^k x^i \otimes m_i \in \ker \alpha^*, \quad m_i \in M.$$

As in the proof of (43.4), we obtain

$$m_0 = -xv_0, \quad m_1 = -xv_1 + v_0, \dots, m_k = v_{k-1},$$

and clearly each  $v_i \in M$ . These equations show that also each  $xv_i \in M$ , so by  $(*)$  above, it follows that each  $v_i \in N$ . Thus  $u \in \text{im}(x - \alpha)$ , which completes the proof that (43.6) is exact. But then

$$[L] = [R' \otimes M] - [R' \otimes N] \in \psi\{G_0(R)\},$$

and so we have proved that  $K_0(R) \cong K_0(R')$ .

Turning next to the proof of the Bass-Heller-Swan Theorem 43.2, we need only treat the case  $n = 1$ , so let  $R' = R[x]$ . A matrix  $\mathbf{N} \in M_n(R)$  is *nilpotent* if  $\mathbf{N}^d = 0$  for some  $d$ ; then  $1 + \mathbf{N}$  is called *unipotent*, and lies in  $GL_n(R)$ . We now show that

$$(*) \quad \mathbf{N} \in M_n(R), \quad 1 + x\mathbf{N} \in GL_n(R') \Rightarrow \mathbf{N} \text{ nilpotent.}$$

Indeed, embed  $R'$  in the ring  $R'' = R[[x]]$  of formal power series in  $x$ . Then

$$(1 + x\mathbf{N})^{-1} = 1 - x\mathbf{N} + x^2\mathbf{N}^2 - \dots \in GL_n(R'').$$

But the left-hand side lies in  $GL_n(R')$ , so  $\mathbf{N}^d = 0$  for all sufficiently large  $d$ .

Let  $\tau: K_1(R) \rightarrow K_1(R')$  be  $R' \otimes *$ , where  $\otimes$  means  $\otimes_{R'}$ . Since the composite of the ring homomorphisms

$$R \rightarrow R' \rightarrow R'/xR' = R$$

is the identity map, we see at once that  $\tau$  is injective. The difficulty lies in proving  $\tau$  surjective.

For  $\mathbf{M}(x) \in GL_n(R')$ , let  $\mathbf{M}(0)$  be the matrix obtained from  $\mathbf{M}(x)$  by setting  $x = 0$  in each entry of  $\mathbf{M}(x)$ . Clearly  $\mathbf{M}(0) \in GL_n(R)$ . Setting

$$\mathbf{T} = \mathbf{M}(0)^{-1}\mathbf{M}(x) = 1 + x\mathbf{T}_1 + \cdots + x^k\mathbf{T}_k \in GL_n(R'),$$

where each  $\mathbf{T}_i \in M_n(R)$ , we need only show that  $\mathbf{T} \in \text{im } \tau$ . If  $\mathbf{I}$  denotes the  $n \times n$  identity matrix, then  $\mathbf{T} = \begin{pmatrix} \mathbf{T} & \mathbf{0} \\ \mathbf{0} & \mathbf{I} \end{pmatrix}$  in  $K_1(R')$ . Elementary row and column operations in  $GL_{2n}(R')$  give

$$\begin{pmatrix} \mathbf{T} & \mathbf{0} \\ \mathbf{0} & \mathbf{I} \end{pmatrix} \sim \begin{pmatrix} \mathbf{T} & x\mathbf{I} \\ \mathbf{0} & \mathbf{I} \end{pmatrix} \sim \begin{pmatrix} \mathbf{T} - x\mathbf{A} & x\mathbf{I} \\ -\mathbf{A} & \mathbf{I} \end{pmatrix}$$

for any  $\mathbf{A} \in M_n(R')$ . Assuming  $k > 1$ , choose  $\mathbf{A} = x^{k-1}\mathbf{T}_k$ . Then in  $K_1(R')$  we have  $\mathbf{T} = \mathbf{T}^*$ , where  $\mathbf{T}^*$  has no terms of degree  $\geq k$ . Continuing with  $k-1$  in place of  $k$ , we find eventually that in  $K_1(R')$  we have  $\mathbf{T} = 1 + x\mathbf{N}$  for some  $\mathbf{N} \in M_m(R)$  for some  $m$ . We are trying to prove that  $\mathbf{T} \in \text{im } \tau$ , and it suffices to show that  $1 + x\mathbf{N}$  is the trivial element of  $K_1(R')$ . Note that  $\mathbf{N}$  is nilpotent by (\*) above, so  $1 + x\mathbf{N}$  is a unipotent matrix in  $GL_m(R')$ .

Let  $F$  be the free  $R'$ -module of rank  $m$  on which  $1 + x\mathbf{N}$  acts, and let  $\theta$  be the nilpotent endomorphism of  $F$  corresponding to the matrix  $x\mathbf{N}$ . If  $\theta^d = 0$ , there is a descending chain of  $R'$ -modules

$$F \supset \theta(F) \supset \theta^2(F) \supset \cdots \supset \theta^d(F) = 0,$$

and  $1 + \theta$  acts as identity on each quotient factor. But then  $[F, 1 + \theta]$  is the trivial element of the group  $G_1(R')$  defined in (38.28). However,  $G_1(R') \cong K_1(R')$  by (38.51), since the ring  $R'$  is left regular. This shows that  $1 + \theta$  is trivial in  $K_1(R')$ , as desired, and the proof of (43.2) is completed.

**(43.7) Remarks.** (i) Quillen showed that  $K_n(R) \cong K_n(R')$  for  $n \geq 0$ , where  $R'$  is as in (43.1). (See Quillen [73], page 114, Corollary of Theorem 8.)

(ii) The proofs of (43.1) and (43.2) work equally well whenever the ring  $R$  is left regular (see (38.41)).

(iii) If  $R$  is any left regular ring, then

$$K_1(R[x, x^{-1}]) \cong K_1(R) \oplus K_0(R).$$

For a proof, see Swan [68, (16.5)].

(iv) Let  $R$  be left regular, and let  $X$  be a set of noncommuting indeterminates, each of which commutes with all elements of  $R$ . Let  $R' = R\{X\}$  be the ring of all polynomials in the variables in  $X$ , with coefficients in  $R$ . Then the inclusion  $R \subseteq R\{X\}$  gives an isomorphism  $K_1(R) \cong K_1(R\{X\})$ . The result is due to Gersten; see Exercise 43.2.

We conclude this section with

**(43.8) Theorem** (Seshadri [58]). *Let  $R$  be a Dedekind domain with quotient field  $F$ , and let  $R' = R[x]$  where  $x$  is an indeterminate. Then every  $Y \in \mathcal{P}(R')$  is an extended module, that is,*

$$Y \cong R' \otimes_R M \quad \text{for some } M \in \mathcal{P}(R).$$

*Proof.* Clearly, every extended module  $R' \otimes_R M$  lies in  $\mathcal{P}(R')$ . Conversely, let  $Y \in \mathcal{P}(R')$  be embedded in  $FY = F \otimes_R Y$ . Then  $FY \cong F[x] \otimes_{R'} Y \in \mathcal{P}[F[x]]$ . Since  $F[x]$  is a P.I.D.,  $FY$  is a free  $F[x]$ -module, and we may write

$$FY = \bigoplus_{i=1}^n F[x]y_i, \quad \text{with each } y_i \in Y.$$

Put  $V = \bigoplus R'y_i$ , a free  $R'$ -submodule of  $Y$ . Then  $V$  is of course an extended module, and  $Y/V$  is an  $R$ -torsion  $R'$ -module. Thus  $IY \subseteq V \subseteq Y$  for some nonzero ideal  $I$  of  $R$ . We now show, by induction on the number of prime ideal factors of  $I$ , that  $Y$  is also an extended module. (The case  $R = F$  is trivial, and excluded from the argument.) It suffices to prove:

**Lemma.** *Suppose we are given  $Y \in \mathcal{P}(R')$  and inclusions  $IPY \subseteq V \subseteq Y$ , where  $P$  is a maximal ideal of  $R$ ,  $I$  any nonzero ideal of  $R$ , and  $V$  an extended module. Then there exists an extended module  $W$  such that  $IY \subseteq W \subseteq Y$ .*

To prove the lemma, suppose that  $V = R' \otimes_R M$  for some  $M \in \mathcal{P}(R)$ . By Steinitz's Theorem 4.13 we can express  $M$  as an external direct sum of nonzero ideals  $\{A_i\}$  of  $R$ , and then

$$V = \bigoplus_{i=1}^n (R' \otimes_R A_i)v_i = \bigoplus_{i=1}^n A_i[x]v_i,$$

where (after replacing  $A_i$  by  $\alpha A_i$  for some  $\alpha \in F$ ) we may assume each  $v_i \in V$ . Let bars denote reduction mod  $P$ . Then

$$\bar{V} = V/PV = \bigoplus \bar{A}_i[x]\bar{v}_i \cong \bigoplus \bar{R}[x]\bar{v}_i,$$

since  $\bar{A}_i \cong \bar{R}$  by (4.15).

The inclusion  $V \subseteq Y$  induces an  $\bar{R}[x]$ -homomorphism  $f: \bar{V} \rightarrow \bar{Y}$  with kernel

$$U_1 = \frac{V \cap PY}{PV} \subseteq \bar{V}.$$

If  $U_1 = 0$  then

$$IY \subseteq V \cap PY = PV \Rightarrow IY \subseteq V,$$

so we may choose  $W = V$  and we are done. Suppose for the rest of the proof that  $U_1 \neq 0$ . Since  $f(\bar{V})$  is an  $\bar{R}[x]$ -submodule of  $\bar{Y}$ , it is  $\bar{R}[x]$ -free by (4.3), and therefore the sequence

$$0 \rightarrow U_1 \rightarrow \bar{V} \rightarrow f(\bar{V}) \rightarrow 0$$

is split. Thus  $\bar{V} = U_1 \oplus U_2$ , and  $U_1$  is a free  $\bar{R}[x]$ -module of rank  $r$ , for some positive integer  $r \leq n$ .

By the Structure Theorem for modules over a P.I.D., we can find an  $\varepsilon \in \text{Aut}_{\bar{R}[x]} \bar{V}$  such that

$$\varepsilon \left\{ \bigoplus_{i=1}^r \bar{R}[x] \bar{v}_i \right\} = U_1, \quad \varepsilon \left\{ \bigoplus_{i=r+1}^n \bar{R}[x] \bar{v}_i \right\} = U_2.$$

Relative to the basis  $\{\bar{v}_i\}$  of  $\bar{V}$ , we may represent  $\varepsilon$  by a matrix over  $\bar{R}[x]$ , and then we may write  $\varepsilon = \alpha\beta$  where  $\alpha \in E_n(R[x])$  and  $\beta$  is diagonal. Therefore

$$U_1 = \alpha\beta \left\{ \bigoplus \bar{R}[x] \bar{v}_i \right\} = \alpha \left\{ \bigoplus \bar{R}[x] \bar{v}_i \right\}.$$

Lifting  $\alpha$  to an element  $h \in E_n(R')$ , where  $R' = R[x]$ , we obtain an element  $h \in \text{Aut}_{R'} V$  such that

$$V = V_1 \oplus V_2, \quad V_1 = \bigoplus_{i=1}^r A_i[x] v_i, \quad V_2 = \bigoplus_{i=r+1}^n A_i[x] v_i, \quad h(\bar{V}_i) = U_i, \quad i = 1, 2.$$

We now choose

$$W = P^{-1}h(V_1) \oplus h(V_2),$$

and we claim that  $IY \subseteq W \subseteq Y$ . First,  $h(V_1)$  and  $V \cap PY$  have the same image in  $\bar{V}$ , so

$$h(V_1) + PV = V \cap PY,$$

and therefore  $h(V_1) \subseteq PY$ , so  $W \subseteq Y$ . Furthermore,

$$IY \subseteq V \Rightarrow IY \subseteq (P^{-1}V \cap Y) = P^{-1}(V \cap PY) = P^{-1}(h(V_1) + PV) = W.$$

Finally, both of the summands  $P^{-1}h(V_1)$  and  $h(V_2)$  are extended modules, since

$$P^{-1}h(V_1) \cong \bigoplus_{i=1}^r P^{-1}A_i[x]v_i \cong R' \otimes_R \coprod_{i=1}^r P^{-1}A_i,$$

with a similar formula for  $h(V_2)$ . This completes the proof of the lemma, and of Seshadri's Theorem.

**(43.9) Corollary.** *Let  $R' = F[x_1, x_2]$ , where  $F$  is a field. Then every f.g. projective  $R'$ -module is free.*

### §43. Exercises

1. Let  $M = R^{(n)}$  be  $R$ -free, where  $R$  is a commutative ring. Let  $\alpha \in \text{End}_R M$ . Use (43.4) to prove the **Cayley-Hamilton Theorem**:

The equation  $\det(x - \alpha) = 0$  has  $x = \alpha$  as a matrix root.

[Hint: Let  $R' = R[x]$ , and view  $x - \alpha$  as a matrix over  $R'$ . To show that  $\{\det(x - \alpha)\}M = 0$ , use (43.4) and establish that, more generally,  $(\det \varphi)(\text{cok } \varphi) = 0$  for any endomorphism  $\varphi$  of a free  $R'$ -module of finite rank.]

2. Prove (43.7iv).

[Hint (Gersten): Let  $R' = R\{X\}$ ,  $\tau: K_1(R) \rightarrow K_1(R')$  the map induced by the inclusion  $R \subset R'$ . There is a surjection  $R' \rightarrow R$  which is the identity on  $R$ , so  $\tau$  is injective. As in the proof of (43.2), each element of  $\text{cok } \tau$  can be represented by a matrix  $1 + \mathbf{N}$ , where  $\mathbf{N} = \sum_{i=1}^r x_i \mathbf{N}_i$ ,  $x_i \in X$ , with the  $\{\mathbf{N}_i\}$  matrices over  $R$ .

Then  $\mathbf{N}$  is nilpotent, so there exists an integer  $d$  such that  $\mathbf{N}_{i_1} \cdots \mathbf{N}_{i_d} = 0$  for all indices between 1 and  $r$ . Further,

$$(1 + \mathbf{N})(1 - x_1 \mathbf{N}_1) \cdots (1 - x_r \mathbf{N}_r) = 1 + \sum x_i x_j \mathbf{N}_{ij}$$

$$(1 + \mathbf{N})(1 - x_1 \mathbf{N}_1) \cdots (1 - x_r \mathbf{N}_r) \prod_{i,j} (1 - x_i x_j \mathbf{N}_{ij}) = 1 + \sum x_i x_j x_k \mathbf{N}_{ijk},$$

and so on, with each  $\mathbf{N}_{ij}$ ,  $\mathbf{N}_{ijk}$  a matrix over  $R$ . Thus  $(1 + \mathbf{N})^{-1}$  is a product of factors of the form  $1 + y\mathbf{M}$  where  $y$  is a product of  $x$ 's and  $\mathbf{M}$  a product of  $\mathbf{N}_i$ 's. But  $1 + y\mathbf{M}$  is trivial in  $K_1(R[y])$ , hence also in  $K_1(R')$ .]

### §44. RELATIVE $K$ -THEORY

Let  $J$  be a two-sided ideal of the ring  $A$ , and let  $\bar{A} = A/J$ . The surjection  $A \rightarrow \bar{A}$  induces maps

$$K_1(A) \rightarrow K_1(\bar{A}), K_0(A) \rightarrow K_0(\bar{A}),$$

and we wish to compare the  $K$ -theory of  $A$  with that of  $\bar{A}$ . As pointed out in

(40.19), there is an exact sequence

$$(44.1) \quad K_1(A) \rightarrow K_1(\bar{A}) \rightarrow K_0(A, J) \rightarrow K_0(A) \rightarrow K_0(\bar{A})$$

involving  $K_0(A, J)$ , the *relative  $K_0$ -group* of  $A$  relative to  $J$ . We shall see here that the sequence can be extended to the left by a relative  $K_1(A, J)$ . Later, in §47, we shall obtain a further extension to the left by means of  $K_2$  terms.

The relative group  $K_0(A, J)$ , as described in (40.19), is generated by expressions  $[M, f, N]$  with  $M, N \in \mathcal{P}(A)$  and where  $f: \bar{A} \otimes_A M \cong \bar{A} \otimes_A N$ . These expressions satisfy certain defining relations, which we now recall. For each  $M \in \mathcal{P}(A)$ , put  $\bar{M} = M/JM \cong \bar{A} \otimes_A M$ . Then:

- (i) Given  $L, M, N \in \mathcal{P}(A)$  and  $\bar{A}$ -isomorphisms  $f: \bar{L} \cong \bar{M}$ ,  $g: \bar{M} \cong \bar{N}$ , we have

$$[L, gf, N] = [L, f, M] + [M, g, N].$$

- (ii) Given  $A$ -exact sequences

$$0 \rightarrow M_1 \rightarrow M_2 \rightarrow M_3 \rightarrow 0, \quad 0 \rightarrow N_1 \rightarrow N_2 \rightarrow N_3 \rightarrow 0, \quad \text{where } M_i, N_i \in \mathcal{P}(A),$$

and given  $\bar{A}$ -isomorphisms  $f_i: \bar{M}_i \cong \bar{N}_i$  ( $i = 1, 2, 3$ ) which commute with the maps associated with the given sequences, we have

$$[M_2, f_2, N_2] = [M_1, f_1, N_1] + [M_3, f_3, N_3].$$

The map  $K_1(\bar{A}) \rightarrow K_0(A, J)$  assigns to each  $f \in GL_n(\bar{A})$  the triple  $[A^n, f, A^n] \in K_0(A, J)$ . Further, the map  $K_0(A, J) \rightarrow K_0(A)$  carries  $[M, f, N]$  onto  $[M] - [N]$ , for  $M, N \in \mathcal{P}(A)$  and  $f: \bar{M} \cong \bar{N}$ .

Now let  $A \subseteq B$  be an inclusion of rings, and let  $J$  be a two-sided ideal of  $B$  contained in  $A$ . Setting  $\bar{A} = A/J$ ,  $\bar{B} = B/J$ , we have  $\bar{A} \subseteq \bar{B}$ , and there is a commutative diagram with exact rows

$$(44.2) \quad \begin{array}{ccccccc} K_1(A) & \rightarrow & K_1(\bar{A}) & \rightarrow & K_0(A, J) & \rightarrow & K_0(A) \\ \downarrow & & \downarrow & & \theta \downarrow & & \downarrow \\ K_1(B) & \rightarrow & K_1(\bar{B}) & \rightarrow & K_0(B, J) & \rightarrow & K_0(\bar{B}) \end{array}$$

We shall now prove the Excision Theorem, which states that the map  $\theta$  is an isomorphism. The authors wish to thank H. Bass for supplying the proof, as well as for many other helpful comments on this chapter.

**(44.3) Excision Theorem.** *Let  $A$  be a subring of  $B$ , and let  $J$  be a two-sided ideal of  $B$  contained in  $A$ . Then the map  $B \otimes_A *$  gives an isomorphism*

$$\theta: K_0(A, J) \cong K_0(B, J).$$

*Proof.* Each  $M \in \mathcal{P}(A)$  will be identified with its image  $1 \otimes M$  in  $B \otimes_A M$ , and

the tensor product will be written as  $BM$ . Note that  $J \cdot BM = JM$ , so

$$\overline{BM} = BM/JBM = BM/JM = \bar{B}\bar{M},$$

where bars denote reduction mod  $J$ .

To prove  $\theta$  surjective, let  $x = [P, f, Q] \in K_0(B, J)$ , where  $P, Q \in \mathcal{P}(B)$  and  $f: \bar{P} \cong \bar{Q}$ . Now

$$x = [P \oplus P', f \oplus 1, Q \oplus P']$$

for  $P' \in \mathcal{P}(B)$ . Choose  $P'$  so that  $P \oplus P'$  is  $B$ -free. Changing notation, we may now assume that  $P$  is  $B$ -free, and so  $P = BM$  for some free  $A$ -module  $M$ . Define  $N$  as the pullback of the maps  $Q \rightarrow \bar{Q}$ ,  $\bar{M} \rightarrow \bar{B}\bar{M} \cong \bar{Q}$ . Then  $N \in \mathcal{P}(A)$  by (42.10ii). In the commutative diagram

$$\begin{array}{ccc} N & \xrightarrow{i} & Q \\ h \downarrow & & \downarrow \\ \bar{M} & \longrightarrow & \bar{Q} \end{array}$$

the map  $i$  is injective,  $h$  is surjective, and  $\ker h \cong JQ$  (see Exercise 2.3). Viewing  $N$  as an  $A$ -submodule of  $Q$ , we have  $JQ \subseteq N \subseteq Q$ . Since  $h(BN) = \bar{B}\bar{M} \cong \bar{Q}$ , we obtain  $Q = BN + JQ = BN$ , and then  $JQ = JN$ . Thus  $h$  induces an  $\bar{A}$ -isomorphism  $g: \bar{N} \cong \bar{M}$ , and  $g^{-1} = f$ . It follows that  $x = \theta[M, g^{-1}, N]$ , and therefore  $\theta$  is surjective.

Turning to the proof that  $\theta$  is injective, let  $x = [M, f, N] \in \ker \theta$ , where  $M, N \in \mathcal{P}(A)$  and  $f: \bar{M} \cong \bar{N}$ . As above, we may assume that  $M$  is  $A$ -free. If  $f$  can be lifted to an  $A$ -isomorphism  $\varphi: M \cong N$ , then by the discussion preceding (40.21) there is an isomorphism of triples

$$(\varphi, 1): (M, f, N) \cong (N, \text{id}_{\bar{N}}, N).$$

Then  $x = [N, \text{id}, N] = 0$  in  $K_0(A, J)$ , as desired. We must still show how to lift  $f$ .

Let  $f$  induce  $f^*: \bar{B}\bar{M} \cong \bar{B}\bar{N}$ ; then

$$0 = \theta(x) = [BM, f^*, BN] \in K_0(B, J).$$

The map  $K_0(B, J) \rightarrow K_0(B)$  carries the above triple to  $[BM] - [BN]$ , so  $BM$  is stably isomorphic to  $BN$ . Replacing  $x$  by  $x + [F, \text{id}, F]$  with  $F$   $A$ -free, and changing notation, we may assume hereafter that  $BM \cong BN = V$ , say, where  $V$  is  $B$ -free of rank  $r$ . We now view  $M$  and  $N$  as  $A$ -submodules of  $V$  such that

$$BM = BN = V, \quad JM = JN = JV, \quad \bar{M} = M/JM \cong V/JV = \bar{V},$$

and likewise  $\bar{N} \subseteq \bar{V}$ . Thus there is a commutative diagram

$$\begin{array}{ccc} \bar{M} & \xrightarrow{f} & \bar{N} \\ \downarrow & & \downarrow \\ \bar{V} & \xrightarrow{f^*} & \bar{V}, \end{array}$$

where the vertical maps are inclusions, and where  $f^* \in \text{Aut}_B \bar{V} = GL_r(\bar{B})$ . Viewing  $f^*$  as representing an element of  $K_1(\bar{B})$ , its image in  $K_0(B, J)$  is the zero element  $[V, f^*, V]$ , so by (44.1) with  $A$  replaced by  $B$ , there exists an element  $g \in GL(B)$  with image  $f^*$  in  $K_1(\bar{B})$ . Stabilizing and changing notation once more, we may assume that  $g \in \text{Aut}_B V$  induces the map  $f^* \in \text{Aut}_{\bar{B}} \bar{V}$ .

Now consider the diagrams

$$\begin{array}{ccc} M \subseteq V & \quad \bar{M} \subseteq \bar{V} \\ g \downarrow & f \downarrow & f^* \downarrow \\ N \subseteq V, & \bar{N} \subseteq \bar{V}, & \end{array}$$

where  $f^* = \bar{g}$ . Since  $\bar{g}(\bar{M}) = f(\bar{M}) = \bar{N}$ , we obtain  $g(M) = N + JV$ , so  $g(M) = N$ . Also,  $g$  is injective on  $V$ , hence also on  $M$ , so  $g|_M$  is the desired lifting of  $f$ , and the proof is complete.

(See Remark 44.16 below, concerning the analogue of (44.3) for  $K_1$ .)

Just as in homological algebra, many computations in algebraic  $K$ -theory depend on the existence of various types of exact sequences: localization, Mayer-Vietoris, and relative  $K$ -theory sequences. We show next how to extend (44.1) one term to the left, by means of a relative group  $K_1(A, J)$ , defined below.

Let  $\bar{A} = A/J$ , where  $J$  is a two-sided ideal of the ring  $A$ . There is a homomorphism  $GL_n(A) \rightarrow GL_n(\bar{A})$  for each  $n$ , defined by reduction mod  $J$ . Let  $GL_n(A, J)$  be the kernel, so there is an exact sequence

$$(44.4) \quad 1 \rightarrow GL_n(A, J) \rightarrow GL_n(A) \rightarrow GL_n(\bar{A}).$$

Now set

$$GL(A, J) = \varinjlim GL_n(A, J) \trianglelefteq GL(A).$$

Now let  $\{\mathbf{E}_{ij}(a)\}$  be the elementary matrices defined in (40.22). For each  $n \geq 1$ , let  $E_n(A)$  be the subgroup of  $GL_n(A)$  generated by elementary matrices. Further, set

$$(44.5) \quad E_n(A, J) = \text{normal subgroup of } E_n(A) \text{ generated by}$$

$$\{\mathbf{E}_{ij}(a) : a \in J, 1 \leq i, j \leq n\}.$$

Put

$$E(A) = \varinjlim E_n(A), E(A, J) = \varinjlim E_n(A, J),$$

so  $E(A, J) \leq GL(A, J)$ . We shall show below that  $E(A, J) \trianglelefteq GL(A, J)$ ; taking this for granted for the moment, let us define

$$(44.6) \quad K_1(A, J) = GL(A, J)/E(A, J).$$

Note that  $K_1(A, A) = K_1(A)$ , while  $K_1(A, 0)$  is trivial.

**(44.7) Theorem (Bass).** *Let  $J$  be a two-sided ideal of  $A$ . Then*

- (i)  $E(A, J) = [E(A), E(A, J)] = [GL(A), GL(A, J)] \trianglelefteq GL(A)$ .
- (ii) *The group  $K_1(A, J)$  is abelian, and equals the center of  $GL(A)/E(A, J)$ .*

*Proof.* We use the formulas (40.23). For  $i, j, k$  distinct, we have

$$[E_{ik}(1), E_{kj}(a)] = E_{ij}(a), \quad a \in A.$$

Choosing  $a \in J$ , this gives

$$E_{ij}(a) \in [E(A), E(A, J)] \trianglelefteq E(A).$$

Therefore

$$E(A, J) = [E(A), E(A, J)] \leq [GL(A), GL(A, J)],$$

and we must prove that equality holds. Let

$$\mathbf{x} \in GL_n(A), \quad \mathbf{y} \in GL_n(A, J), \quad \mathbf{y} = 1 + \mathbf{z},$$

where  $\mathbf{z}$  has entries in  $J$ . It is easily checked that

$$(*) \quad \begin{pmatrix} \mathbf{y}\mathbf{x} & \mathbf{0} \\ \mathbf{0} & 1 \end{pmatrix} \begin{pmatrix} 1 & (\mathbf{y}\mathbf{x})^{-1}\mathbf{z} \\ \mathbf{0} & 1 \end{pmatrix} \cdot \mathbf{P} \cdot \begin{pmatrix} 1 & \mathbf{0} \\ -\mathbf{y}^{-1}\mathbf{z}\mathbf{x} & 1 \end{pmatrix} = \begin{pmatrix} \mathbf{x} & 0 \\ 0 & \mathbf{y} \end{pmatrix},$$

where

$$\mathbf{P} = \begin{pmatrix} 1 & \mathbf{0} \\ -\mathbf{x} & 1 \end{pmatrix} \begin{pmatrix} 1 & -\mathbf{x}^{-1}\mathbf{z} \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & \mathbf{0} \\ \mathbf{x} & 1 \end{pmatrix}.$$

Then  $\mathbf{P} \in E_{2n}(A, J)$  since  $E_{2n}(A, J) \trianglelefteq E_{2n}(A)$ . Thus  $(*)$  gives

$$\begin{pmatrix} \mathbf{y}\mathbf{x} & \mathbf{0} \\ \mathbf{0} & 1 \end{pmatrix} \in \begin{pmatrix} \mathbf{x} & \mathbf{0} \\ \mathbf{0} & \mathbf{y} \end{pmatrix} E_{2n}(A, J).$$

For  $x = 1$ , this yields  $\begin{pmatrix} y & \mathbf{0} \\ \mathbf{0} & y^{-1} \end{pmatrix} \in E_{2n}(A, J)$  for all  $y \in GL_n(A, J)$ . Further, letting  $x \in GL_n(A)$  be arbitrary, we obtain

$$\begin{pmatrix} xy & \mathbf{0} \\ \mathbf{0} & 1 \end{pmatrix} = \begin{pmatrix} x & \mathbf{0} \\ \mathbf{0} & y \end{pmatrix} \begin{pmatrix} y & \mathbf{0} \\ \mathbf{0} & y^{-1} \end{pmatrix} \in \begin{pmatrix} x & \mathbf{0} \\ \mathbf{0} & y \end{pmatrix} E_{2n}(A, J),$$

and so

$$\begin{aligned} \begin{pmatrix} xyx^{-1}y^{-1} & \mathbf{0} \\ \mathbf{0} & 1 \end{pmatrix} &= \begin{pmatrix} x & \mathbf{0} \\ \mathbf{0} & 1 \end{pmatrix} \begin{pmatrix} yx^{-1}y^{-1} & \mathbf{0} \\ \mathbf{0} & 1 \end{pmatrix} \in \begin{pmatrix} x & \mathbf{0} \\ \mathbf{0} & 1 \end{pmatrix} \begin{pmatrix} x^{-1}y^{-1} & \mathbf{0} \\ \mathbf{0} & y \end{pmatrix} E_{2n}(A, J) \\ &\leq E_{2n}(A, J). \end{aligned}$$

This shows that  $[GL(A), GL(A, J)] \leq E(A, J)$ , and establishes (i).

To prove (ii), observe first that  $K_1(A, J)$  is abelian since  $E(A, J)$  contains the commutator subgroup of  $GL(A, J)$ . Further, if  $u$  lies in the center of  $GL(A)/E(A, J)$ , its image  $\bar{u} \in GL(\bar{A})/E(\bar{A})$  is also central. This latter quotient is a subgroup of  $GL(\bar{A})$  containing  $E(\bar{A})$ . But the centralizer of  $E(\bar{A})$  in  $GL(\bar{A})$  is 1, so  $\bar{u} = 1$  and therefore  $u \in GL(A, J)$ . This completes the proof of the theorem.

**(44.8) Corollary.** *Let  $J$  be a two-sided ideal of the ring  $A$ , and let  $K_1(A, J)$  be defined as above. Then there is an exact sequence*

$$K_1(A, J) \rightarrow K_1(A) \rightarrow K_1(\bar{A}) \rightarrow K_0(A, J) \rightarrow K_0(A) \rightarrow K_0(\bar{A}).$$

*Proof.* It suffices to prove exactness at  $K_1(A)$ . Consider the commutative diagram with exact rows:

$$\begin{array}{ccccccc} 1 & \rightarrow & E(A) \cap GL(A, J) & \rightarrow & E(A) & \rightarrow & E(\bar{A}) \rightarrow 1 \\ & & \downarrow & & \downarrow & & \downarrow \\ 1 & \rightarrow & GL(A, J) & \longrightarrow & GL(A) & \rightarrow & GL(\bar{A}). \end{array}$$

The vertical maps are inclusions, so the Snake Lemma for Groups (see Exercise 44.3) gives an exact sequence

$$1 \rightarrow GL(A, J)/(E(A) \cap GL(A, J)) \rightarrow K_1(A) \rightarrow K_1(\bar{A}).$$

Since  $E(A, J) \leq E(A) \cap GL(A, J)$ , it follows from the above and formula (44.6) that

$$K_1(A, J) \rightarrow K_1(A) \rightarrow K_1(\bar{A})$$

is exact. This completes the proof.

We now give another approach to relative K-theory, due to Bass and Stein,

which is based on the use of an appropriate Mayer-Vietoris sequence. The advantages of this approach are its simplicity, and the fact that it extends readily to the  $K_2$  terms. However, the description of the relative groups  $K_0(A, J)$  and  $K_1(A, J)$  is not so intuitively satisfying. We follow the treatment in Milnor's book [71].

As above, let  $\bar{A} = A/J$ , where  $J$  is a two-sided ideal of  $A$ . The *double* of  $A$  along  $J$  is the ring  $D$  defined by the fiber product

$$(44.9) \quad \begin{array}{ccc} D & \xrightarrow{f} & A \\ g \downarrow & & f' \downarrow \\ A & \longrightarrow & \bar{A}, \\ & & g' \end{array}$$

where  $f' = g'$  is the canonical surjection  $A \rightarrow \bar{A}$ . Thus,

$$D = \{(x, y) \in A \oplus A : \bar{x} = \bar{y} \text{ in } \bar{A}\}.$$

The Mayer-Vietoris sequence (42.14) gives us an exact sequence

$$(44.10) \quad \begin{aligned} K_1(D) &\xrightarrow{(f, g)} K_1(A) \times K_1(A) \xrightarrow{(f', 1/g')} K_1(\bar{A}) \\ &\xrightarrow{\partial} K_0(D) \xrightarrow{(f, g)} K_0(A) \oplus K_0(A) \xrightarrow{(f', -g')} K_0(\bar{A}). \end{aligned}$$

(The map  $(f', 1/g')$  is defined by

$$(f', 1/g')(x, y) = f'(x)/g'(y) \quad \text{for } x, y \in K_1(A).$$

We note that

$$\text{im}(f', 1/g') = \text{im } g' \text{ in } K_1(\bar{A}), \quad \text{im}(f', -g') = \text{im } g' \text{ in } K_0(\bar{A}).$$

Now let  $x \in K_1(A)$ ; then

$$\begin{aligned} x \in \ker g' &\Leftrightarrow (0, x) \in \ker(f', 1/g') \Leftrightarrow (0, x) = (fy, gy) \quad \text{for some } y \in K_1(D) \\ &\Leftrightarrow x = gy \quad \text{for some } y \in \ker f. \end{aligned}$$

An analogous result holds for the case where  $x \in K_0(A)$ . Put

$$(44.11) \quad K_i(A, J) = \{y \in K_i(D) : f(y) = 0\}, \quad i = 0, 1.$$

We have thus shown that

$$K_i(A, J) \xrightarrow{g} K_i(A) \xrightarrow{g'} K_i(\bar{A}), \quad i = 0, 1,$$

is exact. Since  $(f, g) \cdot (\text{im } \partial) = 0$ , it follows readily that there is an exact sequence

$$(44.12) \quad K_1(A, J) \xrightarrow{g} K_1(A) \xrightarrow{g'} K_1(\bar{A}) \xrightarrow{\partial} K_0(A, J) \xrightarrow{g} K_0(A) \xrightarrow{g'} K_0(\bar{A}),$$

as desired.

**(44.13) Remarks.** (i) When  $J = A$  we obtain  $\bar{A} = 0$ ,  $D = A \times A$ , and then

$$K_i(A, A) \cong K_i(A), \quad i = 0, 1.$$

At the other extreme where  $J = 0$ , we get  $D = A$ , and then  $K_i(A, 0) = 0$ ,  $i = 0, 1$ .

(ii) Let  $\Delta: A \rightarrow D$  be the diagonal map  $\Delta(a) = (a, a)$ ,  $a \in A$ . Then  $\Delta$  splits the surjection  $f: D \rightarrow A$ , so the sequence

$$0 \rightarrow K_0(A, J) \rightarrow K_0(D) \xrightarrow{f} K_0(A) \rightarrow 0$$

is split exact. (Indeed,  $\Delta$  induces a splitting  $K_i(A) \rightarrow K_i(D)$ .) This shows that

$$K_0(D) \cong K_0(A) \oplus K_0(A, J).$$

In the same manner, we obtain

$$K_1(D) \cong K_1(A) \times K_1(A, J).$$

We leave it as an exercise to the reader to establish an isomorphism between this version of  $K_0(A, J)$  and the preceding version. However, we shall now prove that the two definitions of  $K_1(A, J)$  agree.

**(44.14) Proposition.** *Let  $J$  be a two-sided ideal of  $A$ , and let  $D$  be the double of  $A$  along  $J$ , as in (44.9). Set*

$$K_1^*(A, J) = \{y \in K_1(D) : f(y) = 0\},$$

where  $f: D \rightarrow A$ . Then there is an isomorphism

$$K_1^*(A, J) \cong K_1(A, J),$$

where, as in (44.6),

$$K_1(A, J) = GL(A, J)/E(A, J).$$

*Proof.* From (44.9) we obtain a fiber product of groups

$$\begin{array}{ccc} GL(D) & \xrightarrow{f} & GL(A) \\ g \downarrow & & \downarrow g' \\ GL(A) & \xrightarrow{f'} & GL(\bar{A}), \end{array}$$

where  $f$  is viewed as a projection onto the first component. Clearly

$$\ker f = 1 \times GL(A, J).$$

Next, the surjection  $f: D \rightarrow A$  induces a surjection  $E(D) \rightarrow E(A)$ , also denoted by  $f$ . We shall prove that the sequence of groups

$$(44.15) \quad 1 \rightarrow 1 \times E(A, J) \rightarrow E(D) \xrightarrow{f} E(A) \rightarrow 1$$

is exact. By (44.5),  $E(A, J)$  is the subgroup of  $E(A)$  generated by all expressions  $\mathbf{S}\mathbf{T}\mathbf{S}^{-1}$ ,  $\mathbf{S} \in E(A)$ , where  $\mathbf{T}$  ranges over all elementary matrices for which  $\bar{\mathbf{T}} = 1$  in  $E(\bar{A})$ . Now

$$(1, \mathbf{S}\mathbf{T}\mathbf{S}^{-1}) = (\mathbf{S}, \mathbf{S})(1, \mathbf{T})(\mathbf{S}, \mathbf{S})^{-1} \text{ in } GL(D),$$

and  $(1, \mathbf{T}) \in E(D)$ , so  $(1, \mathbf{S}\mathbf{T}\mathbf{S}^{-1}) \in E(D)$ . Thus,  $1 \times E(A, J)$  is a subgroup of  $E(D)$  contained in  $\ker f$ , and it remains for us to prove the reverse inclusion.

Each element of  $E(D)$  in  $\ker f$  must be of the form  $(1, \mathbf{X})$ , with  $\mathbf{X} \in E(A)$  and  $\bar{\mathbf{X}} = 1$  in  $E(\bar{A})$ . On the other hand, every element of  $E(D)$  is a product of elementary matrices over  $D$ , and each such elementary matrix is of the form

$$(\mathbf{E}_{ij}(r), \mathbf{E}_{ij}(s)), r, s \in A, \quad r \equiv s \pmod{J}.$$

We may thus write

$$(1, \mathbf{X}) = \prod_{i=1}^k (\mathbf{S}_i, \mathbf{S}_i \mathbf{T}_i) \text{ in } E(D),$$

where for each  $i$ ,  $\mathbf{S}_i, \mathbf{T}_i$  are elementary matrices over  $A$  and  $\bar{\mathbf{T}}_i = 1$ . Then  $\prod \mathbf{S}_i = 1$ , and

$$\mathbf{X} = \prod_{i=1}^k (\mathbf{S}_i \mathbf{T}_i) = (\mathbf{S}_1 \mathbf{T}_1 \mathbf{S}_1^{-1})(\mathbf{S}_1 \mathbf{S}_2 \mathbf{T}_2 (\mathbf{S}_1 \mathbf{S}_2)^{-1}) \cdots (\mathbf{S}_1 \cdots \mathbf{S}_k \mathbf{T}_k (\mathbf{S}_1 \cdots \mathbf{S}_k)^{-1}).$$

The right-hand expression lies in  $E(A, J)$  by the preceding remarks, so  $(1, \mathbf{X}) \in 1 \times E(A, J)$ , and we have proved the exactness of (44.15).

Now consider the commutative diagram with exact rows and columns:

$$\begin{array}{ccccccc}
 1 & \longrightarrow & E(A, J) & \longrightarrow & GL(A, J) & \longrightarrow & K_1^*(A, J) \\
 & & g_1 \downarrow & & g_2 \downarrow & & \downarrow \\
 1 & \longrightarrow & E(D) & \longrightarrow & GL(D) & \longrightarrow & K_1(D) \longrightarrow 1 \\
 & & f_1 \downarrow & & f_2 \downarrow & & f_3 \downarrow \\
 1 & \longrightarrow & E(A) & \longrightarrow & GL(A) & \longrightarrow & K_1(A) \longrightarrow 1.
 \end{array}$$

Here, the  $\{f_i\}$  are induced by  $f$ , while the  $g_i$  arise from the map  $g(x) = (1, x)$ ,  $x \in GL(A, J)$ . The last column is the split exact sequence described in Remark 44.13ii. The Remark also shows that both  $f_1$  and  $f_2$  are surjective. The Snake Lemma for Groups (Exercise 44.3) then gives an exact sequence

$$1 \rightarrow E(A, J) \rightarrow GL(A, J) \rightarrow K_1^*(A, J) \rightarrow 1$$

so  $K_1(A, J) \cong K_1^*(A, J)$ , and the proposition is proved.

**(44.16) Remark.** It is natural to ask whether the analogue of the Excision Theorem is valid for  $K_1$  as well as for  $K_0$ . In other words, under the hypotheses of (44.3), is there an isomorphism  $K_1(A, J) \cong K_1(B, J)$ ? As shown by Swan [71], this need not be the case in general. It does hold under suitable hypotheses, however; see (47.20).

We conclude this section by proving a theorem on injective stability for  $K_1(A, J)$ . Since  $K_1(A, A) = K_1(A)$ , the result includes the Bass-Vaserstein Theorem 40.44 as a special case. The more general result will be vital in our discussion of  $SK_1$  of orders (see §45C, and especially the proof of (45.18)). The authors wish to thank W. van der Kallen for supplying the following proof, which is adapted from work of K. Dennis.

**(44.17) Theorem (Injective Stability for Relative  $K$ -Theory).** *Let  $A$  be a ring with stable range  $d$ , and let  $J$  be any two-sided ideal of  $A$ . Then for any  $n \geq d + 1$ , the following hold true:*

- (i)  $E_n(A, J)$  is a normal subgroup of  $GL_n(A)$ , and in fact

$$(44.18) \quad E_n(A, J) = GL_n(A) \cap E(A, J).$$

- (ii) The homomorphism  $GL_n(A, J) \rightarrow K_1(A, J)$  induces an isomorphism

$$(44.19) \quad GL_n(A, J)/E_n(A, J) \cong K_1(A, J).$$

- (iii) In the “absolute” case where  $A = J$ , we have

$$(44.20) \quad E_n(A) = GL_n(A) \cap E(A) \quad \text{and} \quad GL_n(A)/E_n(A) \cong K_1(A).$$

*Proof.* Step 1. We begin by showing that the relative case can be deduced from the absolute case. Suppose for the moment that (iii) has been proved, and let us deduce assertions (i) and (ii). Let  $D$  be the double of  $A$  along  $J$ . As will be shown in (44.25) below,  $D$  also has stable range  $d$ .

Now let  $n \geq d + 1$ ; the proof of (44.14) shows that the sequence

$$(44.21) \quad 1 \rightarrow E_n(A, J) \xrightarrow{g} E_n(D) \xrightarrow{f} E_n(A) \rightarrow 1$$

is exact, and also that there is a commutative diagram with exact rows:

$$\begin{array}{ccccccc} 1 & \longrightarrow & GL_n(A, J) & \longrightarrow & GL_n(D) & \longrightarrow & GL_n(A) & \longrightarrow 1 \\ & & \downarrow & & \downarrow & & \downarrow & \\ 1 & \longrightarrow & K_1(A, J) & \longrightarrow & K_1(D) & \longrightarrow & K_1(A) & \longrightarrow 1. \end{array}$$

In order to prove (i), we observe that  $E(A, J) \trianglelefteq GL(A)$ , so it suffices to establish (44.18). Furthermore, we need only show that  $GL_n(A) \cap E(A, J) \subseteq E_n(A, J)$ , the reverse inclusion being obvious. Given any  $\mathbf{x} \in GL_n(A) \cap E(A, J)$ , the map  $g$  defined in (44.21) carries  $\mathbf{x}$  onto  $g(\mathbf{x}) \in GL_n(D) \cap E(D)$ . By virtue of (iii), applied to the ring  $D$  rather than  $A$ , we deduce that  $g(\mathbf{x}) \in E_n(D)$ . But then  $\mathbf{x} \in E_n(A, J)$  as desired, by the exactness of (44.21).

We have thus shown (assuming (iii)) that  $E_n(A, J) \trianglelefteq GL_n(A, J)$ , and so we obtain a commutative diagram with exact rows

$$\begin{array}{ccccccc} 1 & \longrightarrow & GL_n(A, J)/E_n(A, J) & \longrightarrow & GL_n(D)/E_n(D) & \longrightarrow & GL_n(A)/E_n(A) & \longrightarrow 1 \\ & & \alpha \downarrow & & \beta \downarrow & & \gamma \downarrow & \\ 1 & \longrightarrow & K_1(A, J) & \longrightarrow & K_1(D) & \longrightarrow & K_1(A) & \longrightarrow 1. \end{array}$$

By (40.42), both  $\beta$  and  $\gamma$  are surjective. It then follows from the Snake Lemma for Groups (see Exercise 44.3) that if  $\beta$  and  $\gamma$  are isomorphisms, then so is  $\alpha$ . Thus, (ii) follows from (iii), as claimed.

Step 2. We now begin the proof of (iii). Since  $GL_n(A) \rightarrow K_1(A)$  is a surjection with kernel  $GL_n(A) \cap E(A)$ , we need only prove the first part of (44.20). Further,  $E(A) = \varinjlim E_m(A)$ , and thus it suffices to show

$$(44.22) \quad GL_n(A) \cap E_{n+1}(A) = E_n(A) \quad \text{for } n \geq d + 1.$$

For the remainder of the proof, write  $GL_n$  and  $E_n$  in place of  $GL_n(A)$  and  $E_n(A)$ , respectively. Let  $n \geq d + 1$ . An element  $\mathbf{x} \in GL_{n+1}$  is said to be in *normal form* if it is expressed as a product

$$(44.23) \quad \mathbf{x} = \begin{pmatrix} \mathbf{P} & \mathbf{0} \\ \mathbf{0} & 1 \end{pmatrix} \begin{pmatrix} \mathbf{I}_n & \mathbf{0} \\ \mathbf{b} & 1 \end{pmatrix} \begin{pmatrix} \mathbf{I}_n & \mathbf{c} \\ \mathbf{0} & 1 \end{pmatrix} \begin{pmatrix} 1 & \mathbf{0} \\ \mathbf{d} & \mathbf{I}_n \end{pmatrix} \begin{pmatrix} 1 & \mathbf{0} \\ \mathbf{0} & \mathbf{Q} \end{pmatrix}, \quad \text{with } \mathbf{P}, \mathbf{Q} \in E_n,$$

where  $\mathbf{0}, \mathbf{b}, \mathbf{c}, \mathbf{d}$  represent row or column vectors over  $A$  of length  $n$ . Note that the

middle factors are upper or lower triangular matrices. The normal form of  $\mathbf{x}$  is usually not unique, a fact which will be useful below.

Let us set

$$\mathcal{N} = \{\mathbf{x} \in E_{n+1} : \mathbf{x} \text{ can be written in normal form}\}.$$

The object of this step is to show that  $\mathcal{N} = E_{n+1}$ , that is, each  $\mathbf{x} \in E_{n+1}$  has a normal form. For this, it suffices to prove that for each  $\mathbf{x} \in E_{n+1}$  of the type (44.23), and each generator  $\mathbf{E}_{ij}(a)$ ,  $a \in A$ , the product  $\mathbf{E}_{ij}(a)\mathbf{x}$  also has a normal form.

We shall use repeatedly the following formula: for  $\mathbf{P} \in GL_r$ ,  $\mathbf{S} \in GL_s$ , we have

$$\begin{pmatrix} \mathbf{P} & \mathbf{0} \\ \mathbf{0} & \mathbf{S} \end{pmatrix} \begin{pmatrix} \mathbf{I}_r & \mathbf{Q} \\ \mathbf{0} & \mathbf{I}_s \end{pmatrix} = \begin{pmatrix} \mathbf{P} & \mathbf{PQ} \\ \mathbf{0} & \mathbf{S} \end{pmatrix} = \begin{pmatrix} \mathbf{I}_r & \mathbf{Q}' \\ \mathbf{0} & \mathbf{I}_s \end{pmatrix} \begin{pmatrix} \mathbf{P} & \mathbf{0} \\ \mathbf{0} & \mathbf{S} \end{pmatrix},$$

where  $\mathbf{PQ} = \mathbf{Q}'\mathbf{S}$ . Thus, we can shift the factor  $\begin{pmatrix} \mathbf{P} & \mathbf{0} \\ \mathbf{0} & \mathbf{S} \end{pmatrix}$  from one side of  $\begin{pmatrix} \mathbf{I} & \mathbf{Q} \\ \mathbf{0} & \mathbf{I} \end{pmatrix}$  to the other side, by changing the corner matrix  $\mathbf{Q}$ .

Now consider

(44.24)

$$\mathbf{x}' = \mathbf{E}_{ij}(a)\mathbf{x} = \mathbf{E}_{ij}(a) \begin{pmatrix} \mathbf{P} & \mathbf{0} \\ \mathbf{0} & 1 \end{pmatrix} \begin{pmatrix} \mathbf{I} & \mathbf{0} \\ \mathbf{b} & 1 \end{pmatrix} \begin{pmatrix} \mathbf{I} & \mathbf{c} \\ \mathbf{0} & 1 \end{pmatrix} \begin{pmatrix} 1 & \mathbf{0} \\ \mathbf{d} & \mathbf{I} \end{pmatrix} \begin{pmatrix} 1 & \mathbf{0} \\ \mathbf{0} & \mathbf{Q} \end{pmatrix}, \quad \mathbf{P}, \mathbf{Q} \in E_n.$$

Here,  $\mathbf{E}_{ij}(a)$  is the  $(n+1) \times (n+1)$  matrix, obtained from  $\mathbf{I}_{n+1}$  by placing the element  $a$  in position  $(i, j)$ , where  $i \neq j$ . If both  $i \leq n$  and  $j \leq n$ , then

$$\mathbf{E}_{ij}(a) \begin{pmatrix} \mathbf{P} & \mathbf{0} \\ \mathbf{0} & 1 \end{pmatrix} = \begin{pmatrix} \mathbf{P}' & \mathbf{0} \\ \mathbf{0} & 1 \end{pmatrix}$$

for some  $\mathbf{P}' \in E_n$ , so  $\mathbf{x}' \in \mathcal{N}$ , as desired.

Next, suppose that  $i = n + 1$ ; then

$$\mathbf{E}_{ij}(a) = \begin{pmatrix} \mathbf{I} & \mathbf{0} \\ \mathbf{e}_j a & 1 \end{pmatrix}, \quad \text{where } \mathbf{e}_j = (0 \cdots 1 \ 0 \cdots 0).$$

Therefore

$$\begin{aligned} \mathbf{E}_{ij}(a) \begin{pmatrix} \mathbf{P} & \mathbf{0} \\ \mathbf{0} & 1 \end{pmatrix} \begin{pmatrix} \mathbf{I} & \mathbf{0} \\ \mathbf{b} & 1 \end{pmatrix} &= \begin{pmatrix} \mathbf{I} & \mathbf{0} \\ \mathbf{e}_j a & 1 \end{pmatrix} \begin{pmatrix} \mathbf{P} & \mathbf{0} \\ \mathbf{0} & 1 \end{pmatrix} \begin{pmatrix} \mathbf{I} & \mathbf{0} \\ \mathbf{b} & 1 \end{pmatrix} \\ &= \begin{pmatrix} \mathbf{P} & \mathbf{0} \\ \mathbf{0} & 1 \end{pmatrix} \begin{pmatrix} \mathbf{I} & \mathbf{0} \\ \mathbf{u} & 1 \end{pmatrix} \begin{pmatrix} \mathbf{I} & \mathbf{0} \\ \mathbf{b} & 1 \end{pmatrix} = \begin{pmatrix} \mathbf{P} & \mathbf{0} \\ \mathbf{0} & 1 \end{pmatrix} \begin{pmatrix} \mathbf{I} & \mathbf{0} \\ \mathbf{b}' & 1 \end{pmatrix} \end{aligned}$$

for some  $\mathbf{u}$  and  $\mathbf{b}'$ , so again  $\mathbf{x}' \in \mathcal{N}$ .

We are left with the most difficult case, that where  $j = n + 1$ . Here we have

$$E_{ij}(a) = \begin{pmatrix} I_n & ea \\ \mathbf{0} & 1 \end{pmatrix}, \quad \text{where } \mathbf{e} = {}^t(0 \cdots 1 \ 0 \cdots 0).$$

Then

$$E_{ij}(a) \begin{pmatrix} \mathbf{P} & \mathbf{0} \\ \mathbf{0} & 1 \end{pmatrix} = \begin{pmatrix} \mathbf{P} & \mathbf{0} \\ \mathbf{0} & 1 \end{pmatrix} \begin{pmatrix} \mathbf{I} & va \\ \mathbf{0} & 1 \end{pmatrix},$$

where  $\mathbf{v} = \mathbf{P}^{-1}\mathbf{e}$  is unimodular. Since  $n \geq d + 1$  and  $A$  has stable range  $d$ , we can find a column vector  $\mathbf{w}$  of length  $n - 1$  such that

$$\begin{pmatrix} 1 & \mathbf{0} \\ -\mathbf{w} & I_{n-1} \end{pmatrix} \mathbf{v} = \mathbf{p} = {}^t(p_1, \dots, p_n),$$

where  ${}^t(p_2, \dots, p_n)$  is unimodular. Now let  $\mathbf{X} = \begin{pmatrix} 1 & \mathbf{0} \\ \mathbf{w} & \mathbf{I} \end{pmatrix}$ ; then

$$\begin{pmatrix} 1 & \mathbf{0} \\ \mathbf{d} & \mathbf{I} \end{pmatrix} = \begin{pmatrix} \mathbf{X} & \mathbf{0} \\ \mathbf{0} & 1 \end{pmatrix} \begin{pmatrix} 1 & \mathbf{0} \\ \mathbf{d}_1 & \mathbf{I} \end{pmatrix}$$

for some  $\mathbf{d}_1$ . Making this substitution in (44.24), we may then push the factor  $\begin{pmatrix} \mathbf{X} & \mathbf{0} \\ \mathbf{0} & 1 \end{pmatrix}$  to the left and absorb it into  $\begin{pmatrix} \mathbf{P} & \mathbf{0} \\ \mathbf{0} & 1 \end{pmatrix}$ , obtaining

$$\mathbf{x}' = \begin{pmatrix} \mathbf{P}_1 & \mathbf{0} \\ \mathbf{0} & 1 \end{pmatrix} \begin{pmatrix} I_n & \mathbf{X}^{-1}\mathbf{v}a \\ \mathbf{0} & 1 \end{pmatrix} \begin{pmatrix} \mathbf{I} & \mathbf{0} \\ \mathbf{b}_1 & 1 \end{pmatrix} \begin{pmatrix} \mathbf{I} & \mathbf{c}_1 \\ \mathbf{0} & 1 \end{pmatrix} \begin{pmatrix} 1 & \mathbf{0} \\ \mathbf{d}_1 & \mathbf{I} \end{pmatrix} \begin{pmatrix} 1 & \mathbf{0} \\ \mathbf{0} & \mathbf{Q} \end{pmatrix}$$

for some  $\mathbf{P}_1 \in E_n$ , and some vectors  $\mathbf{b}_1$ ,  $\mathbf{c}_1$ , and  $\mathbf{d}_1$ . Now  $\mathbf{X}^{-1}\mathbf{v}a = \mathbf{p}a$ , where  $\mathbf{p}$  is a column vector with  $n$  components, whose lower  $n - 1$  components form a unimodular vector. In the above expression for  $x'$ , we replace the first two factors by

$$\begin{pmatrix} \mathbf{P}_2 & \mathbf{0} \\ \mathbf{0} & 1 \end{pmatrix} \begin{pmatrix} 1 & \mathbf{q} & 0 \\ \mathbf{0} & I_{n-1} & \mathbf{0} \\ 0 & \mathbf{0} & 1 \end{pmatrix} \begin{pmatrix} I_n & \mathbf{X}^{-1}\mathbf{v}a \\ \mathbf{0} & 1 \end{pmatrix}$$

for some  $\mathbf{P}_2 \in E_n$  and some vector  $\mathbf{q}$ . By the preceding remarks, we may choose  $\mathbf{q}$  so that the top entry of the column vector

$$\begin{pmatrix} 1 & \mathbf{q} \\ \mathbf{0} & I_{n-1} \end{pmatrix} \mathbf{X}^{-1}\mathbf{v}a$$

is 0. We may then write

$$\mathbf{x}' = \begin{pmatrix} \mathbf{P}_2 & \mathbf{0} \\ \mathbf{0} & 1 \end{pmatrix} \begin{pmatrix} 1 & \mathbf{0} & 0 \\ \mathbf{0} & \mathbf{I}_{n-1} & \mathbf{r} \\ 0 & \mathbf{0} & 1 \end{pmatrix} \begin{pmatrix} 1 & \mathbf{q} & 0 \\ \mathbf{0} & \mathbf{I}_{n-1} & \mathbf{0} \\ 0 & \mathbf{0} & 1 \end{pmatrix} \begin{pmatrix} \mathbf{I} & \mathbf{0} \\ \mathbf{b}_1 & 1 \end{pmatrix} \begin{pmatrix} \mathbf{I} & \mathbf{c}_1 \\ \mathbf{0} & 1 \end{pmatrix} \begin{pmatrix} 1 & \mathbf{0} \\ \mathbf{d}_1 & \mathbf{I} \end{pmatrix} \begin{pmatrix} 1 & \mathbf{0} \\ \mathbf{0} & \mathbf{Q} \end{pmatrix}.$$

The product of the middle three factors can be written as

$$\begin{pmatrix} \mathbf{I}_n & \mathbf{0} \\ \mathbf{b}_2 & 1 \end{pmatrix} \begin{pmatrix} 1 & \mathbf{q} & 0 \\ \mathbf{0} & \mathbf{I}_{n-1} & \mathbf{0} \\ 0 & \mathbf{0} & 0 \end{pmatrix} \begin{pmatrix} \mathbf{I}_n & \mathbf{c}_1 \\ \mathbf{0} & 1 \end{pmatrix} = \begin{pmatrix} \mathbf{I}_n & \mathbf{0} \\ \mathbf{b}_2 & 1 \end{pmatrix} \begin{pmatrix} 1 & \mathbf{c}_2 \\ \mathbf{0} & \mathbf{I}_n \end{pmatrix} \begin{pmatrix} 1 & \mathbf{0} \\ \mathbf{0} & \mathbf{U} \end{pmatrix}$$

for some vectors  $\mathbf{b}_2, \mathbf{c}_2$ , and some  $\mathbf{U} \in E_n$ . The factor  $\begin{pmatrix} 1 & \mathbf{0} \\ \mathbf{0} & \mathbf{U} \end{pmatrix}$  can be pushed to the right and absorbed into the last factor of  $x'$ , to give

$$\mathbf{x}' = \begin{pmatrix} \mathbf{P}_2 & \mathbf{0} \\ \mathbf{0} & 1 \end{pmatrix} \begin{pmatrix} 1 & \mathbf{0} & 0 \\ \mathbf{0} & \mathbf{I}_{n-1} & \mathbf{r} \\ 0 & \mathbf{0} & 1 \end{pmatrix} \begin{pmatrix} \mathbf{I}_n & \mathbf{0} \\ \mathbf{b}_2 & 1 \end{pmatrix} \begin{pmatrix} 1 & \mathbf{c}_2 \\ \mathbf{0} & \mathbf{I}_n \end{pmatrix} \begin{pmatrix} 1 & \mathbf{0} \\ \mathbf{d}_2 & \mathbf{I}_n \end{pmatrix} \begin{pmatrix} 1 & \mathbf{0} \\ \mathbf{0} & \mathbf{Q}_1 \end{pmatrix}$$

for some vector  $\mathbf{d}_2$  and some  $\mathbf{Q}_1 \in E_n$ .

Now  $n \geq 2$ , so we may write

$$\begin{pmatrix} \mathbf{I}_n & \mathbf{0} \\ \mathbf{b}_2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & \mathbf{0} & 0 \\ \mathbf{0} & \mathbf{I}_{n-1} & \mathbf{0} \\ s & \mathbf{y} & 1 \end{pmatrix} = \begin{pmatrix} 1 & \mathbf{0} & 0 \\ \mathbf{0} & \mathbf{I}_{n-1} & \mathbf{0} \\ s & \mathbf{0} & 1 \end{pmatrix} \begin{pmatrix} 1 & \mathbf{0} \\ \mathbf{0} & \mathbf{v} \end{pmatrix},$$

where

$$\mathbf{v} = \begin{pmatrix} \mathbf{I}_{n-1} & \mathbf{0} \\ \mathbf{y} & 1 \end{pmatrix} \in E_n,$$

and where  $s$  is scalar,  $\mathbf{y}$  a vector. Pushing the factor  $\begin{pmatrix} 1 & \mathbf{0} \\ \mathbf{0} & \mathbf{v} \end{pmatrix}$  to the right, we obtain

$$\mathbf{x}' = \begin{pmatrix} \mathbf{P}_2 & \mathbf{0} \\ \mathbf{0} & 1 \end{pmatrix} \begin{pmatrix} 1 & \mathbf{0} & 0 \\ \mathbf{0} & \mathbf{I}_{n-1} & \mathbf{r} \\ 0 & \mathbf{0} & 1 \end{pmatrix} \begin{pmatrix} 1 & \mathbf{0} & 0 \\ \mathbf{0} & \mathbf{I}_{n-1} & \mathbf{0} \\ s & \mathbf{0} & 1 \end{pmatrix} \begin{pmatrix} 1 & \mathbf{c}_3 \\ \mathbf{0} & \mathbf{I} \end{pmatrix} \begin{pmatrix} 1 & \mathbf{0} \\ \mathbf{d}_3 & \mathbf{I} \end{pmatrix} \begin{pmatrix} 1 & \mathbf{0} \\ \mathbf{0} & \mathbf{Q}_2 \end{pmatrix}.$$

However, we have

$$\begin{pmatrix} 1 & \mathbf{0} & 0 \\ \mathbf{0} & \mathbf{I} & \mathbf{r} \\ 0 & \mathbf{0} & 1 \end{pmatrix} \begin{pmatrix} 1 & \mathbf{0} & 0 \\ \mathbf{0} & \mathbf{I} & \mathbf{0} \\ s & \mathbf{0} & 1 \end{pmatrix} = \begin{pmatrix} 1 & \mathbf{0} & 0 \\ \mathbf{r}s & \mathbf{I} & \mathbf{0} \\ 0 & \mathbf{0} & 1 \end{pmatrix} \begin{pmatrix} 1 & \mathbf{0} & 0 \\ \mathbf{0} & \mathbf{I} & \mathbf{0} \\ s & \mathbf{0} & 1 \end{pmatrix} \begin{pmatrix} 1 & \mathbf{0} & 0 \\ \mathbf{0} & \mathbf{I} & \mathbf{r} \\ 0 & \mathbf{0} & 1 \end{pmatrix}.$$

Substitute into the formula for  $x'$ , and write

$$\begin{pmatrix} \mathbf{P}_2 & \mathbf{0} \\ \mathbf{0} & 1 \end{pmatrix} \begin{pmatrix} 1 & \mathbf{0} & 0 \\ rs & \mathbf{I} & \mathbf{0} \\ 0 & \mathbf{0} & 1 \end{pmatrix} = \begin{pmatrix} \mathbf{P}_3 & \mathbf{0} \\ \mathbf{0} & 1 \end{pmatrix}, \quad \text{where } \mathbf{P}_3 \in E_n.$$

Then

$$\begin{aligned} \mathbf{x}' &= \begin{pmatrix} \mathbf{P}_3 & \mathbf{0} \\ \mathbf{0} & 1 \end{pmatrix} \begin{pmatrix} 1 & \mathbf{0} & 0 \\ \mathbf{0} & \mathbf{I} & \mathbf{0} \\ s & \mathbf{0} & 1 \end{pmatrix} \begin{pmatrix} 1 & \mathbf{0} & 0 \\ \mathbf{0} & \mathbf{I} & r \\ 0 & \mathbf{0} & 1 \end{pmatrix} \begin{pmatrix} 1 & \mathbf{c}_3 \\ \mathbf{0} & \mathbf{I} \end{pmatrix} \begin{pmatrix} 1 & \mathbf{0} \\ \mathbf{d}_3 & \mathbf{I} \end{pmatrix} \begin{pmatrix} 1 & \mathbf{0} \\ \mathbf{0} & \mathbf{Q}_2 \end{pmatrix} \\ &= \begin{pmatrix} \mathbf{P}_3 & \mathbf{0} \\ \mathbf{0} & 1 \end{pmatrix} \begin{pmatrix} 1 & \mathbf{0} & 0 \\ \mathbf{0} & \mathbf{I} & \mathbf{0} \\ s & \mathbf{0} & 1 \end{pmatrix} \begin{pmatrix} 1 & \mathbf{c}_4 \\ \mathbf{0} & \mathbf{I} \end{pmatrix} \begin{pmatrix} 1 & \mathbf{0} \\ \mathbf{d}_4 & \mathbf{I} \end{pmatrix} \begin{pmatrix} 1 & \mathbf{0} \\ \mathbf{0} & \mathbf{Q}_3 \end{pmatrix}, \end{aligned}$$

for some  $\mathbf{c}_4, \mathbf{d}_4$  and some  $\mathbf{Q}_3 \in E_n$ .

Finally, we have

$$\begin{pmatrix} 1 & \mathbf{c}_4 \\ \mathbf{0} & \mathbf{I} \end{pmatrix} = \begin{pmatrix} \mathbf{W} & \mathbf{0} \\ \mathbf{0} & 1 \end{pmatrix} \begin{pmatrix} \mathbf{I} & \mathbf{f} \\ \mathbf{0} & 1 \end{pmatrix}$$

for some  $\mathbf{W} \in E_n$  and some vector  $\mathbf{f}$ . Pushing the factor  $\begin{pmatrix} \mathbf{W} & \mathbf{0} \\ \mathbf{0} & 1 \end{pmatrix}$  to the left, we obtain

$$\mathbf{x}' = \begin{pmatrix} \mathbf{P}_4 & \mathbf{0} \\ \mathbf{0} & 1 \end{pmatrix} \begin{pmatrix} \mathbf{I} & \mathbf{0} \\ t & 1 \end{pmatrix} \begin{pmatrix} \mathbf{I} & \mathbf{f} \\ \mathbf{0} & 1 \end{pmatrix} \begin{pmatrix} 1 & \mathbf{0} \\ \mathbf{d}_4 & \mathbf{I} \end{pmatrix} \begin{pmatrix} 1 & \mathbf{0} \\ \mathbf{0} & \mathbf{Q}_3 \end{pmatrix}$$

with  $\mathbf{P}_4 \in E_n$ . This shows that  $\mathbf{x}'$  can be written in normal form. We have thus proved that every vector  $\mathbf{x} \in E_{n+1}$  can be written in the normal form (44.20).

*Step 3.* We now prove (44.22), so let  $n \geq d + 1$  and let  $\mathbf{X} \in GL_n(A)$  be such that  $\begin{pmatrix} \mathbf{X} & \mathbf{0} \\ \mathbf{0} & 1 \end{pmatrix} \in E_{n+1}(A)$ . We must prove that  $\mathbf{X} \in E_n(A)$ . By Step 2, we may write

$$\begin{pmatrix} \mathbf{X} & \mathbf{0} \\ \mathbf{0} & 1 \end{pmatrix} = \begin{pmatrix} \mathbf{P} & \mathbf{0} \\ \mathbf{0} & 1 \end{pmatrix} \begin{pmatrix} \mathbf{I}_n & \mathbf{0} \\ \mathbf{b} & 1 \end{pmatrix} \begin{pmatrix} \mathbf{I}_n & \mathbf{c} \\ \mathbf{0} & 1 \end{pmatrix} \begin{pmatrix} 1 & \mathbf{0} \\ \mathbf{d} & \mathbf{I}_n \end{pmatrix} \begin{pmatrix} 1 & \mathbf{0} \\ \mathbf{0} & \mathbf{Q} \end{pmatrix}$$

with  $\mathbf{P}, \mathbf{Q} \in E_n(A)$ . Replacing  $\mathbf{X}$  by  $\mathbf{P}^{-1}\mathbf{X}$  and changing notation, we may take  $\mathbf{P} = \mathbf{I}_n$  for the rest of the proof. Next,

$$\begin{pmatrix} 1 & \mathbf{0} \\ \mathbf{d} & \mathbf{I}_n \end{pmatrix} \begin{pmatrix} 1 & \mathbf{0} \\ \mathbf{0} & \mathbf{Q} \end{pmatrix} = \begin{pmatrix} 1 & \mathbf{0} \\ \mathbf{0} & \mathbf{Q} \end{pmatrix} \begin{pmatrix} 1 & \mathbf{0} \\ \mathbf{d}' & \mathbf{I}_n \end{pmatrix}$$

for some  $\mathbf{d}'$ , so we obtain

$$\begin{pmatrix} \mathbf{I}_n & \mathbf{0} \\ -\mathbf{b} & 1 \end{pmatrix} \begin{pmatrix} \mathbf{X} & \mathbf{0} \\ \mathbf{0} & 1 \end{pmatrix} \begin{pmatrix} 1 & \mathbf{0} \\ -\mathbf{d}' & \mathbf{I}_n \end{pmatrix} = \begin{pmatrix} \mathbf{I}_n & \mathbf{c} \\ \mathbf{0} & 1 \end{pmatrix} \begin{pmatrix} 1 & \mathbf{0} \\ \mathbf{0} & \mathbf{Q} \end{pmatrix}.$$

This gives

$$\begin{pmatrix} \mathbf{X}' & \mathbf{0} \\ \mathbf{b}' & 1 \end{pmatrix} = \begin{pmatrix} 1 & \mathbf{e} \\ \mathbf{0} & \mathbf{Q}' \end{pmatrix}$$

for some new matrices  $\mathbf{X}', \mathbf{Q}'$  and vectors  $\mathbf{b}', \mathbf{e}$ , where

$$\mathbf{X}' \equiv \mathbf{X}, \mathbf{Q}' \equiv \mathbf{Q} \pmod{E_n(A)}.$$

Comparing the above two matrices, we obtain

$$\begin{pmatrix} \mathbf{X}' & \mathbf{0} \\ \mathbf{b}' & 1 \end{pmatrix} = \begin{pmatrix} 1 & \mathbf{u} & 0 \\ \mathbf{0} & \mathbf{M} & \mathbf{0} \\ 0 & \mathbf{v} & 1 \end{pmatrix} = \begin{pmatrix} 1 & \mathbf{e} \\ \mathbf{0} & \mathbf{Q}' \end{pmatrix},$$

for some vectors  $\mathbf{u}, \mathbf{v}$  and some matrix  $\mathbf{M}$ . Then

$$\begin{pmatrix} \mathbf{M} & \mathbf{0} \\ \mathbf{0} & 1 \end{pmatrix} = \begin{pmatrix} \mathbf{M} & \mathbf{0} \\ \mathbf{v} & 1 \end{pmatrix} \begin{pmatrix} \mathbf{I} & \mathbf{0} \\ -\mathbf{v} & 1 \end{pmatrix} = \mathbf{Q}' \begin{pmatrix} \mathbf{I} & \mathbf{0} \\ -\mathbf{v} & 1 \end{pmatrix} \in E_n(A).$$

Also,

$$\mathbf{X}' = \begin{pmatrix} 1 & \mathbf{u} \\ \mathbf{0} & \mathbf{M} \end{pmatrix} = \begin{pmatrix} 1 & \mathbf{0} \\ \mathbf{0} & \mathbf{M} \end{pmatrix} \begin{pmatrix} 1 & \mathbf{u} \\ \mathbf{0} & \mathbf{I} \end{pmatrix}.$$

But

$$\begin{pmatrix} 1 & \mathbf{0} \\ \mathbf{0} & \mathbf{M} \end{pmatrix} \in E_n(A),$$

since  $\begin{pmatrix} \mathbf{M} & \mathbf{0} \\ \mathbf{0} & 1 \end{pmatrix} \in E_n(A)$ , and  $E_n(A)$  is invariant under conjugation by permutation matrices. It follows that  $\mathbf{X} \in E_n(A)$ , which completes the proof of the theorem.

It remains for us to verify the following result, whose proof was also supplied by W. van der Kallen.

**(44.25) Lemma.** *Let  $D$  be the double of  $A$  along  $J$ , and suppose that  $A$  has stable range  $d$ . Then  $D$  also has stable range  $d$ .*

*Proof.* Let  $n \geq d + 1$ , and let

$$\mathbf{v} = [(a_1, b_1), \dots, (a_n, b_n)] \in D^{(n)}$$

be a unimodular row over  $D$ . We must show that by subtracting left multiples of the last entry  $(a_n, b_n)$  from the first  $(n - 1)$  components of  $\mathbf{v}$ , we can make the first  $n - 1$  components into a unimodular row. Call this process “reduction.”

Since  $(a_1, \dots, a_n)$  is unimodular over  $A$ , and  $n \geq d + 1$ , there exist elements  $\{x_i\}$

from  $A$  for which

$$(a_1 + x_1 a_n, a_2 + v_2 a_n, \dots, a_{n-1} + x_{n-1} a_n)$$

is unimodular. Put

$$c_i = a_i + x_i a_n, \quad d_i = b_i + x_i b_n, \quad 1 \leq i \leq n-1.$$

Then the row

$$\mathbf{w} = [(c_1, d_1), \dots, (c_{n-1}, d_{n-1}), (a_n, b_n)] \in D^{(n)}$$

is unimodular, and comes from  $\mathbf{v}$  by “reduction,” so it suffices to show how to “reduce”  $\mathbf{w}$ . Now  $(c_1, \dots, c_{n-1})$  is unimodular, so we may choose  $\{y_i\}$  from  $A$  so that  $\sum_{i=1}^{n-1} y_i c_i = 1$ , and then

$$\sum_{i=1}^{n-1} y_i d_i = 1 + x \quad \text{for some } x \in J.$$

Let us write

$$S = \sum_{i=1}^{n-1} D(c_i, d_i),$$

a left ideal of  $D$  containing  $(1, 1+x)$ . Since  $\mathbf{w}$  is unimodular, there exists  $(t, u) \in D$  such that

$$(1, 1) \equiv (t, u)(a_n, b_n) \pmod{S}.$$

Multiplying on the left by  $(0, x) \in D$ , we obtain

$$(0, x) \equiv (0, xub_n) \pmod{S},$$

and therefore

$$(1, 1) = (1, 1+x) - (0, x) \equiv (0, -xub_n) \pmod{S}.$$

But then

$$\mathbf{y} = [(c_1, d_1), \dots, (c_{n-1}, d_{n-1}), (0, -xub_n)] \in D^{(n)}$$

is unimodular, and since  $(0, -xub_n)$  is a left multiple of  $(a_n, b_n)$ , it suffices to “reduce” the vector  $\mathbf{y}$ . Subtracting suitable left multiples of  $(0, -xub_n)$  from the first  $n-1$  components of  $\mathbf{y}$ , we obtain a new vector

$$\mathbf{z} = [(c_1, e_1), \dots, (c_{n-1}, e_{n-1}), (0, -xub_n)]$$

in which  $(e_1, \dots, e_{n-1}) \in A^{(n-1)}$  is unimodular.

Now let

$$S' = \sum_{i=1}^{n-1} D(c_i, e_i).$$

Then there exist  $\{g_i\} \in A$  with

$$\sum_{i=1}^{n-1} g_i c_i = 1, \quad \sum_{i=1}^{n-1} g_i e_i = 1 + x',$$

with  $x' \in J$ . Then  $(1, 1 + x') \in S'$ . But  $S'$  contains an element  $(*, 1)$ , so multiplying on the left by  $(0, x')$ , we see that  $(0, x') \in S'$ . Therefore  $(1, 1) \in S'$ , which shows that the first  $n - 1$  components of  $\mathbf{z}$  form a unimodular row. This completes the proof of the lemma.

For future reference, we list a special case of Theorem 44.17:

**(44.26) Corollary.** (i) *Let  $R$  be a Dedekind domain, and let  $A$  be an  $R$ -algebra,  $f.g./R$  as module. Let  $J$  be any two-sided ideal of  $A$ . Then for  $n \geq 3$  there is an isomorphism*

$$GL_n(A, J)/E_n(A, J) \cong K_1(A, J),$$

*induced by the surjection  $GL_n(A, J) \rightarrow K_1(A, J)$ .*

(ii) *More generally, let  $R$  be a commutative noetherian ring of Krull dimension  $d$ . Then the above isomorphism holds whenever  $n \geq d + 2$ .*

The result is immediate from (44.17), by virtue of the “surjective stability” theorems (41.23) and (41.25).

## §44. Exercises

1. Let  $A$  be a commutative ring, and let  $K_0(A)$  be made into a ring with multiplication defined via  $\otimes_A$  (see (38.4) with  $G = 1$ ). Then for the ring  $D$  defined by (44.9),  $K_0(D)$  is also a commutative ring. Show that the map  $f_*: K_0(D) \rightarrow K_0(A)$  induced by  $f$  is a ring homomorphism. Prove further that the diagonal map  $\Delta: A \rightarrow D$  induces a ring homomorphism  $\Delta_*$  which splits  $f_*$ . Using the exact sequence

$$0 \rightarrow K_0(A, J) \rightarrow K_0(D) \xrightarrow{f_*} K_0(A) \rightarrow 0,$$

deduce that  $K_0(A, J)$  is a module over the ring  $K_0(A)$ .

2. Keep the above notation. Show that  $K_1(A, J)$  is a  $K_0(A)$ -module, where each  $x \in K_0(A)$  acts as  $\Delta_*(x)$ , using the action of  $K_0(D)$  on  $K_1(D)$  (see Exercise 39.5 with  $G = 1$ ).

Show also that there is a pairing

$$K_0(A, J) \times K_1(A) \rightarrow K_1(A, J),$$

given by

$$(x, y) \rightarrow x \cdot \Delta_*(y), \quad \text{where } \Delta_*: K_1(A) \rightarrow K_1(D).$$

3. (Snake Lemma for Groups.) Let

$$\begin{array}{ccccccc} & A & \xrightarrow{\rho} & B & \longrightarrow & C & \longrightarrow 1 \\ & \alpha \downarrow & & \beta \downarrow & & \gamma \downarrow & \\ 1 & \longrightarrow & A' & \longrightarrow & B' & \xrightarrow{\sigma} & C' \end{array}$$

be a commutative diagram of groups, with exact rows, and assume that  $\text{im } \rho \trianglelefteq B$ ,  $\text{im } \alpha \trianglelefteq A'$ , and so on. Then there is an exact sequence of groups

$$\ker \alpha \xrightarrow{\rho_*} \ker \beta \rightarrow \ker \gamma \rightarrow \text{cok } \alpha \rightarrow \text{cok } \beta \xrightarrow{\sigma_*} \text{cok } \gamma.$$

Further, if  $\rho$  is surjective, so is  $\rho_*$ ; if  $\sigma$  is surjective, so is  $\sigma_*$ .

## §45. $SK_1$ OF ORDERS

In order to study  $K_1(\mathbb{Z}G)$  in §46, we shall need some general facts about  $K_1$  and  $SK_1$  of an arbitrary order. We assume throughout this section that  $K$  is either a global field, or the completion of a global field at a finite or infinite prime  $P$ . Further,  $R$  is a Dedekind domain with quotient field  $K$ , and  $\Lambda$  is an  $R$ -order in a f.d. separable  $K$ -algebra  $A$ .

### §45A. Reduced Norms

The calculation of  $K_1(A)$  reduces to the case of simple algebras, by (38.29). Until further notice, let  $A$  be a central simple  $K$ -algebra. As in (7.46) and (7.47), we define

$$(45.1) \quad K^+ = \{\alpha \in K : \alpha_P > 0 \text{ at each real prime } P \text{ of } K \text{ ramified in } A\}.$$

Letting  $\text{nr}: A^\times \rightarrow K^\times$  be the reduced norm map  $\text{nr}_{A/K}$  defined in §7D, we have

$$(45.2) \quad \text{nr } A^\times = K^+.$$

This is the Hasse-Schilling-Maass Norm Theorem 7.48 when  $K$  is a global field, while it is an easy exercise (see (7.44), (7.45)) when  $K$  is a complete field.

The notation  $K^+$  is somewhat ambiguous, since  $K^+$  depends not only on  $K$ , but on the algebra  $A$  as well. In practice, it will be clear from the context what is intended.

We now amplify Remark 38.69ii, where we pointed out the isomorphism  $K_1(A) \cong K^+$ .

**(45.3) Theorem.** *Let  $A$  be a central simple  $K$ -algebra. Then the reduced norm  $\text{nr}_{A/K}$  induces an isomorphism*

$$\text{nr}: K_1(A) \cong K^+.$$

Further, if  $K$  is a complete field, then  $K^+ = K^\circ$  except when  $K = \mathbb{R}$  and  $A \cong M_n(\mathbb{H})$ ,  $\mathbb{H} = \text{real quaternions}$ .

*Proof.* The exercises in §7 show that for  $n \geq 1$ ,

$$\text{nr } GL_n(A) = \text{nr } A^\circ \subseteq K^\circ.$$

Further, for  $\alpha \in GL_n(A)$ , we have  $\text{nr} \begin{pmatrix} \alpha & 0 \\ 0 & 1 \end{pmatrix} = \text{nr } \alpha$ . Thus the homomorphism

$$\text{nr}: GL(A) \rightarrow K^\circ$$

is well defined. Its kernel contains  $GL'(A)$ , so there is a homomorphism  $\text{nr}: K_1(A) \rightarrow K^\circ$ . By (7.44)–(7.48) we have  $\text{nr } K_1(A) = K^+$ .

To prove  $\text{nr}$  injective, note that each element of  $K_1(A)$  can be represented by a  $1 \times 1$  matrix  $(a)$ , where  $a \in A^\circ$  (see Exercise 38.14 or Theorem 40.31). If  $\text{nr}(a) = 1$ , then  $a \in [A^\circ, A^\circ]$  by (7.49), (7.51), and Exercise 7.7. But then  $(a) = 1$  in  $K_1(A)$ , as desired.

Before turning to the calculation of  $K_1(\Lambda)$ , where  $\Lambda$  is a maximal order, we need some information about the Eichler condition. Let  $K$  be a global field; by a *prime*  $P$  of  $K$  we mean an equivalence class of valuations of  $K$  (see §4C), always excluding the trivial valuation.

**(45.4) Definitions.** Let  $K$  be a global field, and  $R$  a Dedekind domain with quotient field  $K$ . A prime  $P$  of  $K$ , which does *not* arise from a valuation of  $K$  associated with a maximal ideal of  $R$ , will be called a “non- $R$ ” prime of  $K$ .

Let  $A$  be a simple f.d.  $K$ -algebra. We say that  $A$  satisfies the *Eichler condition relative to  $R$* , and use the notation  $A = \text{Eichler}/R$ , if there exists at least one non- $R$  prime  $P$  of  $K$  such that at least one Wedderburn component of the  $P$ -adic completion  $A_P$  is not a noncommutative division algebra. In other words,  $A = \text{Eichler}/R$  except when  $A_P$  is a direct sum of noncommutative skewfields for every non- $R$  prime  $P$  of  $K$ .

Let  $F$  be the center of  $A$ , and  $S$  the integral closure of  $R$  in  $F$ . By Exercise 45.1 below,

$$A = \text{Eichler}/R \Leftrightarrow A = \text{Eichler}/S.$$

Further, for each prime  $Q$  of  $F$ , the  $Q$ -adic completion  $A_Q$  is a simple algebra with center  $F_Q$ . Therefore,  $A = \text{Eichler}/S$  except when  $A_Q$  is a noncommutative division algebra for every non- $S$  prime  $Q$  of  $F$ .

Next, let  $A$  be a f.d. semisimple  $K$ -algebra, with Wedderburn components  $A_1, \dots, A_s$ . We shall say that  $A$  satisfies the *Eichler condition relative to  $R$*  if  $A_i = \text{Eichler}/R$  for each  $i$ .

**(45.5) Remarks.** (i) If  $K$  is an algebraic number field and  $R = \text{alg. int. } \{K\}$ ,

then a central simple  $K$ -algebra  $A$  satisfies the Eichler condition over  $R$  except when  $A$  is a totally definite quaternion algebra (see Volume I, p. 718).

(ii) The preceding version (45.4) of the Eichler condition was first introduced by Swan [80]. It coincides with the usual version when  $K$  is an algebraic number field, but is a weaker restriction on  $A$  when  $K$  is a global function field (see, e.g., MO (Definition 34.3)). As shown by Swan, whose proof will be given in (51.22) below, this weaker condition on  $A$  is sufficient for the validity of the following fundamental result:

**(45.6) Theorem.** *Let  $K$  be a global field, and let  $\Lambda$  be a maximal  $R$ -order in a central simple  $K$ -algebra  $A$ , where  $A = \text{Eichler}/R$ . Then*

$$\text{nr}_{A/K} \Lambda^\cdot = R^\cdot \cap K^+.$$

From this, we derive readily:

**(45.7) Theorem.** *Let  $K$  be a global field, and  $\Lambda$  a maximal  $R$ -order in a central simple  $K$ -algebra  $A$ . Then*

$$\text{nr } K_1(\Lambda) = R^\cdot \cap K^+.$$

*Proof.* Since  $\text{nr}$  is multiplicative, we have

$$\text{nr } GL_n(\Lambda) \subseteq R^\cdot \cap K^+, \quad n \geq 1.$$

Further,  $M_2(\Lambda)$  is a maximal  $R$ -order in  $M_2(A)$ . Now  $M_2(A)$  is a central simple  $K$ -algebra which is always Eichler/ $R$ , whether or not  $A$  is Eichler/ $R$ . Therefore  $\text{nr } GL_2(\Lambda) = R^\cdot \cap K^+$  by (45.6), which establishes the theorem.

**Remark.** The reader may easily verify that  $R^\cdot \cap K^+$  is a subgroup of  $R^\cdot$  of finite index.

The local version of the preceding is much easier to prove:

**(45.8) Proposition.** *Let  $R$  be a complete d.v.r. with quotient field  $K$  and finite residue class field  $\bar{R}$ . Let  $\Lambda$  be a maximal  $R$ -order in a central simple  $K$ -algebra  $A$ . Then*

$$\text{nr } K_1(\Lambda) = \text{nr } \Lambda^\cdot = R^\cdot.$$

*Proof.* Let  $A = M_k(D)$ , where  $D$  is a division algebra with center  $K$ , and let  $\Delta$  be the unique maximal  $R$ -order in  $D$  (see (26.22)). By (26.23) we have  $\Lambda = M_k(\Delta)$  (up to conjugacy), and then (see Exercise 7.5)

$$K_1(\Lambda) \cong K_1(\Delta), \quad \text{nr}_{A/K} \Lambda^\cdot = \text{nr}_{D/R} \Delta^\cdot.$$

It suffices to show that  $\text{nr } \Delta^\cdot = R^\cdot$ , where now  $\text{nr}$  means  $\text{nr}_{D/K}$ .

By MO (§14),  $D$  contains an *inertia subfield*  $W$ , unique up to conjugacy, such that  $W$  is a maximal subfield of  $D$  and  $W$  is unramified over  $K$ . Further, by MO (Exercise 14.5),

$$\text{nr}_{D/K} \alpha = N_{W/K} \alpha \quad \text{for all } \alpha \in W.$$

If  $\mathfrak{o}_W$  denotes the integral closure of  $R$  in  $W$ , then  $\mathfrak{o}_W \subseteq \Delta$ , and thus  $\text{nr } \Delta \supseteq N_{W/K}(\mathfrak{o}_W)$ . But the latter contains  $R^\cdot$  by MO (14.1), and thus  $\text{nr } \Delta \supseteq R^\cdot$ . But if  $x \in \Delta$  is such that  $\text{nr } x \in R^\cdot$ , it follows that also  $N_{D/K}(x) \in R^\cdot$ , so  $x \in \Delta^\cdot$  by (26.22) or (26.2). This completes the proof that  $\text{nr } \Delta^\cdot = R^\cdot$ , and establishes the proposition.

**Remark.** As we shall see in (45.13), the surjection  $\text{nr}: K_1(\Lambda) \rightarrow R^\cdot \cap K^+$  is seldom an isomorphism.

To conclude this subsection, we briefly discuss the case of semisimple algebras. Let  $A$  be an f.d. separable  $K$ -algebra, with Wedderburn components  $\{A_i: 1 \leq i \leq s\}$ . Let  $C$  be the center of  $A$ , and write

$$C = \bigoplus_{i=1}^s F_i, \quad F_i = \text{center of } A_i.$$

We now define

$$(45.9) \quad C^+ = \bigoplus_{i=1}^s (F_i)^+,$$

so by (45.2) and (45.3) we obtain

$$\text{nr}: K_1(A) \cong C^+, \quad \text{nr}_{A/C} A^\cdot = C^+.$$

We now define

$$(45.10) \quad SK_1(\Lambda) = \{x \in K_1(\Lambda): \text{nr}_{A/C} x = 1\},$$

so there is an exact sequence

$$(45.11) \quad 1 \rightarrow SK_1(\Lambda) \rightarrow K_1(\Lambda) \rightarrow K_1(A).$$

When  $\Lambda$  is commutative, then  $\text{nr}_{A/C}$  is the usual determinant map  $\det: K_1(A) \rightarrow A^\cdot$ . Therefore

$$SK_1(\Lambda) = \{x \in K_1(\Lambda): \det x = 1\} \quad \text{if } \Lambda \text{ is commutative.}$$

The surjection  $\det: K_1(A) \rightarrow A^\cdot$  is split by the homomorphism  $u \mapsto (u)$ ,  $u \in A^\cdot$ , and

therefore

$$K_1(\Lambda) \cong \Lambda^\cdot \times SK_1(\Lambda)$$

whenever  $\Lambda$  is commutative. Thus, definitions (45.10) and (40.27) agree in the commutative case. We also have:

**(45.12) Proposition.** *Let  $\Lambda$  be a commutative semilocal ring. Then*

$$SK_1(\Lambda) = 1, \quad K_1(\Lambda) \cong \Lambda^\cdot.$$

*Proof.* Immediate from (40.31) and the preceding remarks.

### §45B. Maximal Orders

We show here how to compute  $K_1(\Lambda)$  and  $SK_1(\Lambda)$ , where  $\Lambda$  is a maximal order in a separable  $K$ -algebra  $A$  over a global field  $K$ . Of course, it suffices to treat the case where  $A$  is a central simple  $K$ -algebra. Further, let  $A \cong M_n(D)$ , with  $D$  a skewfield, and let  $\Delta$  be a maximal order in  $D$ . Then every maximal order  $\Lambda$  in  $A$  is Morita equivalent to the maximal order  $M_n(\Delta)$ , and we have

$$K_1(A) \cong K_1(D), \quad K_1(\Lambda) \cong K_1(\Delta), \quad SK_1(\Lambda) \cong SK_1(\Delta),$$

so the problem reduces to the case of a maximal order in a skewfield.

We begin with the local calculation, due to Kuku [76] and Keating [76].

**(45.13) Theorem.** *Let  $R$  be a complete d.v.r. with finite residue class field  $\bar{R} = R/P$  and quotient field  $K$ . Let  $D$  be a division algebra of dimension  $m^2$  over its center  $K$ , and let  $\Delta$  be a maximal  $R$ -order in  $D$ . Then  $SK_1(\Delta)$  is a cyclic group of order  $(q^m - 1)/(q - 1)$ , where  $q = |\bar{R}|$ , and there is an exact sequence of abelian groups*

$$1 \rightarrow SK_1(\Delta) \rightarrow K_1(\Delta) \xrightarrow{\text{nr}} R^\cdot \rightarrow 1,$$

where  $\text{nr}$  means  $\text{nr}_{D/K}$ .

*Proof.* We already know that  $\text{nr } K_1(\Delta) = R^\cdot$  by (45.8), and by definition  $SK_1(\Delta)$  is the kernel of  $\text{nr}$ . We must prove that  $SK_1(\Delta)$  is a cyclic group of order  $(q^m - 1)/(q - 1)$ . Let  $W$  be an inertia subfield of  $D$ , as in the proof of (45.8). As shown in MO (§14), we may write  $W = K(\omega)$ , where  $\omega$  is a primitive  $(q^m - 1)$ -st root of 1 over  $K$ . Then

$$\bar{\Delta} = \Delta/\text{rad } \Delta = \bar{R}(\bar{\omega}),$$

a field extension of  $\bar{R}$  of degree  $m$ . Here,  $\bar{\omega}$  is the image of  $\omega$  in  $\bar{\Delta}$ , and is a primitive  $(q^m - 1)$ -st root of 1 over  $\bar{R}$ ; it generates the cyclic group  $\bar{\Delta}^\cdot$ .

Let  $\pi_D$  denote a prime element of  $\Delta$ . Then (see MO (14.6))

$$\text{rad } \Delta = \pi_D \Delta = \Delta \pi_D, \quad \pi_D \omega \pi_D^{-1} = \omega^q$$

for some integer  $r$  with  $(r, m) = 1$ . It is easily seen that  $\omega^{qr-1}$  has order  $(q^m - 1)/(q - 1)$ ; the same holds with  $\bar{\omega}$  in place of  $\omega$ . Further,

$$\omega^{qr-1} = \pi_D \omega \pi_D^{-1} \omega^{-1},$$

so  $\text{nr } \omega^{qr-1} = 1$ . Thus, the cyclic group  $\langle \omega^{qr-1} \rangle$  maps into  $SK_1(\Delta)$ , and we claim the map is an embedding. Indeed, the homomorphism  $K_1(\Delta) \rightarrow K_1(\bar{\Delta})$  carries  $\langle \omega \rangle$  onto  $\langle \bar{\omega} \rangle$ . Since  $K_1(\bar{\Delta}) = \langle \bar{\omega} \rangle$ , this shows that the group  $\langle \omega \rangle$  is embedded in  $K_1(\Delta)$ , and therefore  $\langle \omega^{qr-1} \rangle$  is embedded in  $SK_1(\Delta)$ . Note that  $\langle \omega^{qr-1} \rangle$  is cyclic of order  $(q^m - 1)/(q - 1)$ , and we must show that it coincides with  $SK_1(\Delta)$ .

We next observe that there is an exact localization sequence

$$K_1(\mathcal{T}) \xrightarrow{\varepsilon} K_1(\Delta) \rightarrow K_1(D),$$

where  $\mathcal{T}$  is the category of all f.g.  $R$ -torsion  $\Delta$ -modules of finite homological dimension. The last restriction is superfluous since  $\text{gl. dim. } \Delta \leq 1$ , because the ring  $\Delta$  is hereditary. To describe the map  $\varepsilon$ , note that each element of  $K_1(\mathcal{T})$  is of the form  $[T, \tau]$  with  $T \in \mathcal{T}$  and  $\tau \in \text{Aut}_\Delta T$ . Since the homological dimension of  $T$  is  $\leq 1$ , we can then find  $Q_i \in \mathcal{P}(\Delta)$  and  $\varphi_i \in \text{Aut}_\Delta Q_i$ ,  $i = 1, 2$ , for which the sequence of pairs

$$0 \rightarrow (Q_1, \varphi_1) \rightarrow (Q_2, \varphi_2) \rightarrow (T, \tau) \rightarrow 0$$

is exact. Then

$$\varepsilon[T, \tau] = [Q_2, \varphi_2] - [Q_1, \varphi_1] \in K_1(\Delta).$$

(Note that we have used the determinantal version of  $K_1(\mathcal{T})$ , as given in the discussion preceding (38.28)).

Next, each  $T \in \mathcal{T}$  has a filtration

$$T \supset \pi_D T \supset \pi_D^2 T \supset \cdots \supset \pi_D^l T = 0$$

for some  $l$ . Each factor is a left  $\bar{\Delta}$ -module, so as in §38D we obtain  $K_1(\mathcal{T}) \cong K_1(\bar{\Delta})$ . Note that  $K_1(\bar{\Delta}) \cong \bar{\Delta}^\cdot = \langle \bar{\omega} \rangle$ , and we shall now compute  $\varepsilon \langle \bar{\omega} \rangle$  in  $K_1(\Delta)$ . For this purpose, we note that the element  $(\bar{\omega}) \in K_1(\bar{\Delta})$  corresponds to the pair  $[\bar{\Delta}, \bar{\omega}]$ . There is an exact sequence

$$0 \rightarrow (\pi_D \Delta, \omega) \rightarrow (\Delta, \omega) \rightarrow (\bar{\Delta}, \bar{\omega}) \rightarrow 0,$$

and therefore

$$\varepsilon(\bar{\omega}) = [\Delta, \omega] - [\pi_D \Delta, \omega] \in K_1(\Delta).$$

However,

$$(\pi_D \Delta, \omega) \cong (\Delta, \pi_D^{-1} \omega \pi_D),$$

as follows from the commutative diagram (of right multiplications)

$$\begin{array}{ccc} \pi_D \Delta & \xrightarrow{\pi_D^{-1}} & \Delta \\ \omega \downarrow & & \downarrow \pi_D \omega \pi_D^{-1} \\ \pi_D \Delta & \xrightarrow{\pi_D^{-1}} & \Delta. \end{array}$$

Therefore

$$\varepsilon(\bar{\omega}) = (\omega \pi_D^{-1} \omega^{-1} \pi_D) = (\omega^{1-q^r}) \in K_1(\Delta).$$

Since  $\text{im } \varepsilon = SK_1(\Delta)$ , we have now shown that  $SK_1(\Delta)$  coincides with the cyclic group  $\langle \omega^{q^r-1} \rangle$  of order  $(q^m - 1)/(q - 1)$ , and the theorem is established.

The global version of the preceding theorem is considerably deeper. We follow the treatment in Keating [76], which uses the Bass-Milnor-Serre Theorem and Quillen's Localization Sequence. We begin by recalling some notation. Let  $D$  be a skewfield with center  $K$ . For each prime  $P$  of  $K$ , let  $D_P$  be its  $P$ -adic completion. Then we may write

$$(45.14) \quad D_P \cong M_{\kappa_P}(\Omega_P), \quad \dim_{K_P} \Omega_P = m_P^2,$$

where  $\Omega_P$  is a skewfield with center  $K_P$  and index  $m_P$ . We call  $\kappa_P$  the *local capacity* of  $D$  at  $P$ , and  $m_P$  the *local index*. We say that  $P$  is *ramified* in  $D$  if  $m_P > 1$ , and *unramified* if  $m_P = 1$ . Then  $m_P = 1$  a.e. (see MO(32.1)). We are now ready to prove:

**(45.15) Theorem** (Keating [76]). *Let  $\Delta$  be a maximal  $R$ -order in a division algebra  $D$  with center  $K$  a global field. For each maximal ideal  $P$  of  $R$ , let  $m_P$  be the local index of  $D$  at  $P$ , and let  $q_P = |R/P|$ . Then*

$$SK_1(\Delta) \cong \prod_P SK_1(\Delta_P),$$

and  $SK_1(\Delta_P)$  is a cyclic group of order  $(q_P^{m_P} - 1)/(q_P - 1)$ , which is trivial a.e. Further, there is an exact sequence

$$1 \rightarrow SK_1(\Delta) \rightarrow K_1(\Delta) \rightarrow R^\times \cap K^+ \rightarrow 1,$$

where  $K^+$  is defined as in (45.1),

*Proof.* Step 1. Let  $\mathcal{T}$  be the category of f.g.  $R$ -torsion  $\Delta$ -modules; each  $T \in \mathcal{T}$

has finite homological dimension, since  $\Delta$  is hereditary. By Quillen's Localization Sequence (40.18), there is an exact sequence\*

$$K_2(D) \xrightarrow{\theta} K_1(\mathcal{T}) \rightarrow K_1(\Delta) \rightarrow K_1(D),$$

so  $SK_1(\Delta) \cong \text{cok } \theta$ , and it remains to compute  $\text{cok } \theta$ . Note that  $\text{nr } K_1(\Delta) = R^\times \cap K^+$  by Theorem 45.7.

As in the proof of (45.13), we have

$$K_1(\mathcal{T}) \cong \coprod_P K_1(\mathcal{T}_P), \quad \text{where } \mathcal{T}_P = \text{category of } P\text{-torsion modules in } \mathcal{T}.$$

Next, for fixed  $P$ , each  $T \in \mathcal{T}_P$  is a  $\Delta_P$ -module having a  $\Delta_P$ -composition series, and therefore  $K_1(\mathcal{T}_P) \cong K_1(\Delta_P/\text{rad } \Delta_P)$ . But (see (45.14))

$$\Delta_P \cong M_{\kappa_P}(\Gamma_P), \quad \Delta_P/\text{rad } \Delta_P \cong M_{\kappa_P}(\bar{\Gamma}_P), \quad \text{where } \bar{\Gamma}_P \cong \Gamma_P/\text{rad } \Gamma_P.$$

Note that  $\bar{\Gamma}_P$  is a field extension of  $R/P$  of degree  $m_P$ , so now

$$(45.16) \quad K_1(\mathcal{T}_P) \cong K_1(\bar{\Gamma}_P) \cong (\bar{\Gamma}_P)^\circ,$$

a cyclic group of order  $q_P^{m_P} - 1$ . Therefore  $K_1(\mathcal{T}) \cong \coprod_P (\bar{\Gamma}_P)^\circ$ , and it thus suffices to prove that

$$\theta(K_2(D)) = \coprod_P (R/P)^\circ \quad \text{in } \coprod_P (\bar{\Gamma}_P)^\circ.$$

For each maximal ideal  $P_0$  of  $R$ , there is a commutative diagram

$$\begin{array}{ccc} K_2(D) & \xrightarrow{\theta} & \coprod_P K_1(\bar{\Gamma}_P) \\ \downarrow & & \downarrow \\ K_2(D_{P_0}) & \xrightarrow{\theta_0} & K_1(\bar{\Gamma}_{P_0}). \end{array}$$

But  $\text{im } \theta_0 \subseteq (R/P_0)^\circ$  by (45.13), and so we obtain

$$\theta(K_2(D)) \subseteq \coprod_P (R/P)^\circ \quad \text{in } \coprod_P K_1(\bar{\Gamma}_P).$$

The entire difficulty lies in establishing the reverse inclusion.

\*For an explicit description of the map  $\theta$  when  $D$  is a global field, see the discussion of tame symbols in §47C.

Let  $x = (x_P) \in \Pi(R/P)^*$ , where  $x_P = 1$  a.e. Let  $\mathcal{S}$  be a finite set of primes of  $K$  (including possibly some of the infinite primes), such that for  $P \notin \mathcal{S}$  we have  $x_P = 1$  and  $m_P = 1$ . In Step 2, we shall construct a maximal subfield  $L$  of  $D$ , which depends on the set  $\mathcal{S}$ , with certain properties. Let  $S$  be the integral closure of  $R$  in  $L$ . Since we may replace  $\Delta$  by any other maximal order  $\Delta'$  in  $D$  without affecting the remainder of the argument, and since  $K_1(\Delta_P/\text{rad } \Delta_P) \cong K_1(\Delta'_P/\text{rad } \Delta'_P)$  for each  $P$ , we may assume that  $S \subseteq \Delta$ . The inclusions  $S \subseteq \Delta$ ,  $L \subseteq D$ , give rise to a commutative diagram with exact rows:

$$\begin{array}{ccccccc} K_2(L) & \xrightarrow{\theta'} & \coprod_Q K_1(S/Q) & \longrightarrow & K_1(S) & \longrightarrow & K_1(L) \\ \downarrow & & \downarrow \psi & & \downarrow & & \downarrow \\ K_2(D) & \xrightarrow{\theta} & \coprod_P K_1(\mathcal{F}_P) & \longrightarrow & K_1(\Delta) & \longrightarrow & K_1(D). \end{array}$$

Here,  $Q$  ranges over all maximal ideals of  $S$ . The Bass-Milnor-Serre Theorem tells us that  $SK_1(S) = 1$ , or equivalently, that  $\theta'$  is surjective. It therefore suffices to prove that  $x \in \text{im } \psi$ .

*Step 2.* Let  $m$  be the index of the skewfield  $D$ , so  $\dim_K D = m^2$ . By (45.14) we have  $m_P \kappa_P = m$  for each prime  $P$  of  $K$ . As above, let  $\mathcal{S}$  be a finite set of primes  $P$  of  $K$ , including all those for which  $x_P \neq 1$  or  $m_P > 1$ . By the Grunwald-Wang Theorem (see MO(32.18)), we may choose a field  $L$  which is a Galois extension of  $K$  with cyclic Galois group of order  $m$ , such that

$$\dim_{K_P} L_{P_i} = m_P \text{ for each } P \in \mathcal{S} \text{ and each prime } P_i \text{ of } L \text{ extending } P.$$

Then  $L$  is a splitting field for  $D$  over  $K$  (see MO(32.15)), and since  $\dim_K L = m$ , we can embed  $L$  as a maximal subfield of  $D$  (see MO(28.10)).

Let  $S$  be the integral closure of  $R$  in  $L$ ; for each maximal ideal  $P$  of  $R$  such that  $x_P \neq 1$ , let  $P_i$  range over the maximal ideals of  $S$  containing  $P$ . It suffices to show that the image of the map

$$\psi_P: \coprod_i (S/P_i)^* \rightarrow K_1(\bar{\Gamma}_P)$$

is precisely  $(R/P)^*$ , using the identifications in (45.16). The problem is thus reduced to a local situation, but one in which  $R$  is not complete. There is no loss of generality in assuming that  $R$  is a d.v.r. from this point on.

Let us write

$$PS = \prod_{i=1}^{\kappa} P_i^{e_i}, \quad f_i = \dim_R(S/P_i),$$

where  $\bar{R} = R/P$ . Then  $e_i f_i = \dim_{K_P} L_i = m_P$ , where  $L_i$  is an abbreviation for  $L_{P_i}$ .

We have

$$m = \dim_{K_P} L_P = \sum_{i=1}^{\kappa} \dim_{K_P} L_i = m_P \kappa,$$

so  $\kappa = \kappa_P$ . For the remainder of the proof, we simplify the notation by writing

$$D_P \cong M_\kappa(\Omega), \quad \Delta_P = M_\kappa(\Gamma), \quad \bar{\Gamma} = \Gamma/\text{rad } \Gamma, \quad \bar{S} = S/P_1, \quad q = |\bar{R}|.$$

The isomorphism  $L_P \cong \coprod L_i$  may be written as

$$L_P = \bigoplus_{i=1}^{\kappa} L_i \varepsilon_i,$$

where  $1 = \varepsilon_1 + \dots + \varepsilon_\kappa$  is a decomposition into orthogonal primitive idempotents. Then  $D_P = \bigoplus D_P \varepsilon_i$  is a decomposition of  $D_P$  into minimal left ideals, and we may thus identify  $\varepsilon_i$  with the diagonal matrix  $\text{diag}(0, \dots, 0, 1, 0, \dots, 0)$ , with 1 in  $i$ -th position, this for  $1 \leq i \leq \kappa$ .

Let  $u \in \bar{S}^*$ , viewed as an element  $[\bar{S}, u] \in K_1(\bar{S})$ . Then

$$\psi_P(u) = [\Delta \otimes_{\bar{S}} (S/P_1), 1 \otimes u] = [\Delta/\Delta P_1, 1 \otimes u] \in K_1(\Delta/P\Delta),$$

and in these formulas we may replace  $\Delta$  by its completion  $\Delta_P$ . In order to identify  $\psi_P(u)$  as an element of  $K_1(\bar{\Gamma})$ , we need a  $\Delta_P$ -composition series for  $\Delta/\Delta P_1$ . Now we have

$$S_P = \bigoplus_{i=1}^{\kappa} S_i \varepsilon_i, \quad P_1 S_P = P_1 S_1 \varepsilon_1 \bigoplus \left( \bigoplus_{i=2}^{\kappa} S_i \varepsilon_i \right),$$

where  $S_i$  is the  $P_i$ -adic completion of  $S$ . Therefore

$$\Delta_P/\Delta_P P_1 \cong M_\kappa(\Gamma/\Gamma P_1) \cdot \varepsilon_1.$$

Note that

$$\Gamma \cong \varepsilon_1 \Delta_P \varepsilon_1, \quad S_1 = S_P \varepsilon_1 = \varepsilon_1 S_P,$$

so  $\Gamma$  is a two-sided  $S_1$ -module, and  $S_1 \subset \Gamma$ .

Let  $\pi, \pi_1$ , and  $\xi$  denote prime elements, with

$$P = \pi R, \quad P_1 = \pi_1 S, \quad \text{rad } \Gamma = \xi \Gamma = \Gamma \xi.$$

Then up to unit factors we have

$$\pi = \xi^{m_P}, \quad \pi = \pi_1^{e_1}, \quad \text{so} \quad \pi_1 = \xi^{f_1},$$

using the fact that  $e_1 f_1 = m_P$ . Therefore  $\Gamma/\Gamma P_1 = \Gamma/\Gamma \xi^{f_1}$ , so  $\Delta_P/\Delta_P P_1 \cong$

$(\Gamma/\Gamma\xi^{f_1})^{(\kappa)}$ , the left  $\Gamma$ -module consisting of all  $\kappa \times 1$  column vectors with entries in  $\Gamma/\Gamma\xi^{f_1}$ . As in the proof of (45.13), we may write

$$\xi u \xi^{-1} = u^{qr} \quad \text{in } \bar{S},$$

for some  $r$  relatively prime to  $m_p$ . We obtain

$$\begin{aligned} \psi_P(u) &= [(\Gamma/\Gamma\xi^{f_1})^{(\kappa)}, 1 \otimes u] = \sum_{i=0}^{f_1-1} [(\Gamma\xi^i/\Gamma\xi^{i+1})^{(\kappa)}, 1 \otimes u] \\ &= \sum_i [(\Gamma/\Gamma\xi)^{(\kappa)}, \xi^i(1 \otimes u)\xi^{-i}] \in K_1(\mathcal{T}_P). \end{aligned}$$

Now  $\Gamma/\Gamma\xi = \bar{\Gamma}$ , and  $\bar{\Gamma}^{(\kappa)}$  is a simple left  $M_\kappa(\bar{\Gamma})$ -module. Identifying  $K_1(\mathcal{T}_P)$  with  $K_1(\bar{\Gamma})$ , the image of  $\psi_P(u)$  in  $\bar{\Gamma}^*$  becomes

$$\prod_{i=0}^{f_1-1} u^{qr} \in \bar{S}.$$

However,  $\bar{S}$  is a Galois extension of  $\bar{R}$  of degree  $f_1$ , with cyclic Galois group generated by the Frobenius automorphism  $\sigma: \alpha \mapsto \alpha^q, \alpha \in \bar{S}$ . Then  $\sigma^r$  also generates this Galois group, and so

$$\psi_P(u) = \prod_{i=0}^{f_1-1} \sigma^i(u) = N_{\bar{S}/\bar{R}}(u) \in \bar{R}^*.$$

Moreover,  $N_{\bar{S}/\bar{R}}$  maps  $\bar{S}$  onto  $\bar{R}$  (see MO(14.1)), and it follows that

$$\psi_P \left\{ \prod_{i=1}^\kappa (S/P_i)^* \right\} = \bar{R}^* \subseteq \bar{\Gamma}^*,$$

as desired. This completes the proof of the theorem.

The preceding theorem generalizes to the case of hereditary orders, as shown by Oliver [80b]. Since a hereditary order  $\Lambda$  in a  $K$ -algebra  $A$  decomposes according to the Wedderburn decomposition of  $A$  (see (26.20a)), it suffices to treat the case where  $A$  is a central simple  $K$ -algebra. The main result is as follows:

**(45.17) Theorem (Oliver).** *Let  $\Lambda$  be a hereditary  $R$ -order in a central simple  $K$ -algebra  $A$ , where  $K$  is a global field. Then*

$$SK_1(\Lambda) \cong \coprod_P SK_1(\Lambda_P),$$

where  $P$  ranges over the maximal ideals of  $R$ , and  $\Lambda_P$  is the  $P$ -adic completion of  $\Lambda$ . The terms  $SK_1(\Lambda_P)$  are zero for almost all  $P$ .

Further, for each  $P$  we may write

$$(45.17a) \quad \Lambda_P/\text{rad } \Lambda_P \cong \coprod_{i=1}^r M_{n_i}(\bar{\Delta})$$

for some field  $\bar{\Delta}$  containing  $\bar{R}$ , where  $\bar{R} = R/P$  (see (26.28ii)). Then

$$SK_1(\Lambda_P) \cong \left( \prod_{i=1}^r \bar{\Delta}^\cdot \right) / \bar{R}^\cdot,$$

with  $\bar{R}^\cdot$  embedded diagonally in the product.

*Proof.* Let  $\Lambda \subseteq \Gamma =$  maximal  $R$ -order in  $A$ . Then  $\Lambda_P = \Gamma_P$  for almost all  $P$ , and therefore  $SK_1(\Lambda_P) = 1$  a.e. by (45.15). To simplify the proof, we shall use a few results from §49A Appendix. As shown there, we have a surjection

$$SK_1(\Lambda) \rightarrow \coprod_P SK_1(\Lambda_P),$$

whose kernel is denoted by  $\text{Cl}_1\Lambda$ . From Keating's Theorem we obtain  $\text{Cl}_1\Gamma = 1$ , and we must prove here that  $\text{Cl}_1\Lambda = 1$ .

From §49A Appendix, there is a commutative diagram with exact rows:

$$\begin{array}{ccccccc} K_2(A) & \rightarrow & \coprod_P K_2(A_P)/\text{im } K_2(\Lambda_P) & \rightarrow & \text{Cl}_1\Lambda & \rightarrow & 1 \\ 1 \downarrow & & \downarrow & & \downarrow & & \\ K_2(A) & \rightarrow & \coprod_P K_2(A_P)/\text{im } K_2(\Gamma_P) & \rightarrow & \text{Cl}_1\Gamma & \rightarrow & 1. \end{array}$$

To prove that  $\text{Cl}_1\Lambda = 1$ , it thus suffices to verify that

$$(45.17b) \quad \text{im } K_2(\Lambda_P) = \text{im } K_2(\Gamma_P) \quad \text{in } K_2(A_P)$$

for each  $P$ .

Changing notation for the rest of the proof, we now assume that  $R$  is a complete d.v.r. with finite residue class field  $\bar{R}$ . The Quillen Localization Sequence gives an exact sequence

$$1 \rightarrow K_2(A)/\text{im } K_2(\Lambda) \rightarrow K_1(\mathcal{T}) \rightarrow SK_1(\Lambda) \rightarrow 1,$$

where  $\mathcal{T}$  is the category of f.g.  $R$ -torsion  $\Lambda$ -modules of finite homological dimension. But every  $\Lambda$ -module has finite homological dimension, since  $\Lambda$  is hereditary. The proof of (49.13) then shows that  $K_1(\mathcal{T}) \cong K_1(\Lambda/\text{rad } \Lambda)$ . We thus

obtain a commutative diagram with exact rows:

$$\begin{array}{ccccccc} 1 \rightarrow K_2(A)/\text{im } K_2(\Lambda) & \xrightarrow{\theta} & K_1(\Lambda/\text{rad } \Lambda) & \longrightarrow & SK_1(\Lambda) & \longrightarrow & 1 \\ \downarrow & & \downarrow & & \downarrow & & \\ 1 \rightarrow K_2(A)/\text{im } K_2(\Gamma) & \xrightarrow{\theta'} & K_1(\Gamma/\text{rad } \Gamma) & \longrightarrow & SK_1(\Gamma) & \rightarrow & 1. \end{array}$$

One easily verifies that in order to prove (45.17b), it suffices to establish

$$(45.17c) \quad |SK_1(\Lambda)| \geq |K_1(\Lambda/\text{rad } \Lambda)| / |\text{im } \theta'|.$$

From the proof of (45.15) we have  $\text{im } \theta' \cong \bar{R}^*$ . Then as in (45.17a) we may write

$$\Lambda/\text{rad } \Lambda \cong \coprod_{i=1}^r M_{n_i}(\bar{\Delta}),$$

with  $\bar{\Delta}$  some finite field extension of  $\bar{R}$ . (Indeed, we have  $\Gamma/\text{rad } \Gamma \cong M_n(\bar{\Delta})$  for some  $n$ , and  $\dim_{\bar{R}} \bar{\Delta}$  is the index of the skewfield part of  $A$ .) We thus obtain

$$K_1(\Lambda/\text{rad } \Lambda) \cong \prod_{i=1}^r K_1(M_{n_i}(\bar{\Delta})) \cong \prod_{i=1}^r \bar{\Delta}^*,$$

a finite  $p'$ -group. It follows that  $SK_1(\Lambda)$  is also a  $p'$ -group.

Consider next the isomorphism

$$\text{nr}: K_1(A) \cong K^*$$

given in (45.3). Identifying  $K_1(A)$  with  $K^*$ , it follows as in (45.8) that  $\text{nr } K_1(\Lambda) \subseteq R^*$ , and there is an exact sequence

$$1 \rightarrow SK_1(\Lambda) \rightarrow K_1(\Lambda) \xrightarrow{\text{nr}} R^*.$$

By (45.31), we may write

$$K_1(\Lambda) \cong K_1(\Lambda/\text{rad } \Lambda) \times V_0, \quad \text{and} \quad R^* \cong R^* \times V_1,$$

where  $V_0$  and  $V_1$  are pro- $p$ -groups. Since  $SK_1(\Lambda)$  has already been shown to be a  $p'$ -group, it follows that there is an exact sequence

$$1 \rightarrow SK_1(\Lambda) \rightarrow K_1(\Lambda/\text{rad } \Lambda) \rightarrow \bar{R}^*.$$

But this implies (45.17c), and completes the proof of the first assertion of the theorem.

Finally, we obtain (in the local case)

$$SK_1(\Lambda) \cong K_1(\Lambda/\text{rad } \Lambda)/\text{im } \theta \cong \left( \prod_{i=1}^r \bar{\Delta}^\cdot \right) / \bar{R},$$

where  $\bar{R}^\cdot$  is embedded diagonally in the product. This completes the proof of Oliver's Theorem.

### §45C. Finiteness of $SK_1$

Throughout this subsection, let  $\Lambda$  be an  $R$ -order in an f.d. separable  $K$ -algebra  $A$ , where  $K$  is either a global field or a non-archimedean completion of a global field. Let  $\Lambda'$  be a maximal  $R$ -order in  $A$  containing  $\Lambda$ , so  $SK_1(\Lambda')$  is a finite group by §45B. By comparing  $SK_1(\Lambda)$  with  $SK_1(\Lambda')$ , we shall establish the fundamental result (due to Bass) that  $SK_1(\Lambda)$  is also a finite group.

We begin with a preliminary result, which is valid in a somewhat more general situation.

**(45.18) Theorem.** *Let  $\Lambda \subset \Gamma$  be  $R$ -orders in a f.d.  $K$ -algebra  $A$ , where  $R$  is any Dedekind domain with finite residue class fields. Let*

$$\theta: K_1(\Lambda) \rightarrow K_1(\Gamma)$$

*be the homomorphism induced by the inclusion  $\Lambda \subset \Gamma$ . Then  $\ker \theta$  and  $\text{cok } \theta$  are finite.*

*Proof.* Step 1. Choose a nonzero  $r \in R$  with  $r\Gamma \subseteq \Lambda$ , and let  $n \geq 3$ . Then (see (44.4)) we have

$$GL_n(\Gamma, r\Gamma) \subseteq GL_n(\Lambda) \subseteq GL_n(\Gamma),$$

and  $|GL_n(\Gamma): GL_n(\Gamma, r\Gamma)|$  is finite (since  $\Gamma/r\Gamma$  is a finite ring). Thus the map

$$\alpha: GL_n(\Lambda) \rightarrow GL_n(\Gamma)$$

has finite cokernel. But  $GL_n(\Gamma)$  maps onto  $K_1(\Gamma)$  by (41.23), so  $\text{cok } \alpha$  maps onto  $\text{cok } \theta$ . Therefore  $\text{cok } \theta$  is finite, as claimed.

Now let  $J$  be any two-sided ideal of  $\Lambda$  for which  $K \cdot J = A$ . By (44.6) and (44.8), there is an exact sequence

$$(45.19) \quad K_1(\Lambda, J) \xrightarrow{\varphi} K_1(\Lambda) \rightarrow K_1(\Lambda/J),$$

where  $K_1(\Lambda, J) = GL(\Lambda, J)/E(\Lambda, J)$ . Since  $\Lambda/J$  is a finite ring,  $K_1(\Lambda/J)$  is finite by (40.31), and therefore  $\text{cok } \varphi$  is a finite group. Since  $n \geq 3$ , it follows from (44.26)

that

$$K_1(\Lambda, J) \cong GL_n(\Lambda, J)/E_n(\Lambda, J), \quad K_1(\Lambda) \cong GL_n(\Lambda)/E_n(\Lambda).$$

We shall use these formulas to prove that  $\ker \varphi$  is finite.

*Step 2.* We set

$$G = GL_n(\Lambda), \quad N = GL_n(\Lambda, J) \trianglelefteq G.$$

Then by (44.7) and (44.17)

$$K_1(\Lambda, J) = N/[G, N], \quad K_1(\Lambda) = G/[G, G].$$

Note that  $G/N \leq GL_n(\Lambda/J)$ , so  $G/N$  is finite. Let  $\bar{G} = G/N$ , and let  $Z$  be the trivial  $G$ -module. There is an exact sequence of homology groups<sup>†</sup>

$$H_2(G, Z) \rightarrow H_2(\bar{G}, Z) \rightarrow H_1(N, Z)/I_{\bar{G}} \cdot H_1(N, Z) \xrightarrow{\psi} H_1(G, Z) \rightarrow H_1(\bar{G}, Z),$$

where  $I_{\bar{G}}$  is the augmentation ideal of  $Z\bar{G}$ . By Exercise 8.1,

$$H_1(G, Z) \cong G/[G, G], \quad H_1(N, Z) \cong N/[N, N].$$

Put  $T = N/[N, N]$ , viewed as  $\bar{G}$ -module. For  $\bar{x} - 1 \in I_{\bar{G}}$ , where  $x \in G$ , we have

$$(\bar{x} - 1)n = xn x^{-1} n^{-1} = [x, n], \quad n \in T.$$

Therefore

$$H_1(N, Z)/I_{\bar{G}} \cdot H_1(N, Z) \cong N/[G, N],$$

and we may identify  $\psi$  with the map  $\varphi$  occurring in Step 1. Thus, we need only show that the groups  $H_2(\bar{G}, Z)$  and  $H_1(\bar{G}, Z)$  are finite.

However,  $H_1(\bar{G}, Z) \cong \bar{G}/[\bar{G}, \bar{G}]$ , a finite group. Also we have (see Rotman [79, Theorem 10.31])

$$H_2(G, Z) \cong H^2(\bar{G}, Q/Z) \cong \text{Schur multiplier of } G,$$

which is finite by (11.38). This completes the proof that the map  $\varphi$  in (45.19) has finite kernel and cokernel.

*Step 3.* With  $r$  as in Step 1, put  $I = r\Gamma$ ,  $J = r^2\Gamma$ , a pair of two-sided  $\Gamma$ -ideals in  $\Lambda$ . For each  $n$ , every matrix in  $GL_n(\Lambda, J)$  is  $\equiv \mathbf{I}_n \pmod{J}$ , and so

$$GL_n(\Lambda, J) = GL_n(\Gamma, J), \quad E_n(\Lambda, J) \leq E_n(\Gamma, J), \quad n \geq 3.$$

<sup>†</sup>This is the Hochschild-Serre-Lyndon sequence of homology groups; see Rotman [79, Theorem 11.6].

Hence (see (45.19)) there is a map  $\sigma$  giving rise to a commutative diagram

$$\begin{array}{ccc} K_1(\Lambda, J) & \xrightarrow{\varphi} & K_1(\Lambda) \\ \sigma \downarrow & & \theta \downarrow \\ K_1(\Gamma, J) & \xrightarrow{\varphi'} & K_1(\Gamma). \end{array}$$

Since both  $\varphi$  and  $\varphi'$  have finite kernels and cokernels, we need only prove that  $\ker \sigma$  is finite, which will imply that  $\ker \theta$  is finite.

Using the third formula in (40.23) with  $a, b \in I$ , and using the equality  $J = I^2$ , we obtain from (44.7):

$$\begin{aligned} E_n(\Gamma, J) &\leq [E_n(\Gamma, I), E_n(\Gamma, I)] \leq [GL_n(\Gamma, I), GL_n(\Gamma, I)] \\ &= [GL_n(\Lambda, I), GL_n(\Lambda, I)] \leq E_n(\Lambda, I) \leq E_n(\Lambda). \end{aligned}$$

Therefore

$$\ker \sigma \cong E_n(\Gamma, J)/E_n(\Lambda, J) \leq E_n(\Lambda)/E_n(\Lambda, J) = [G, G]/[G, N].$$

By Step 2, the quotient  $[G, G]/[G, N]$  is finite, since both  $G/N$  and  $\ker \varphi$  are finite. Thus  $\ker \sigma$  is finite, and the theorem is proved.

We may now prove the basic result:

**(45.20) Theorem (Bass).** *Let  $\Lambda$  be an R-order in a f.d. separable K-algebra A, where K is either a global field or its completion at a non-archimedean prime. Then  $SK_1(\Lambda)$  is a finite abelian group.*

*Proof.* Let  $\Lambda'$  be a maximal R-order in A containing  $\Lambda$ . There is a commutative diagram

$$\begin{array}{ccccc} 1 & \rightarrow & SK_1(\Lambda) & \rightarrow & K_1(\Lambda) & \rightarrow & K_1(A) \\ & & \theta' \downarrow & & \theta \downarrow & & 1 \downarrow \\ 1 & \rightarrow & SK_1(\Lambda') & \rightarrow & K_1(\Lambda') & \rightarrow & K_1(A), \end{array}$$

so  $\ker \theta' = \ker \theta$ . But  $\ker \theta$  is finite by the preceding theorem, while  $SK_1(\Lambda')$  is finite by §45B. Therefore  $SK_1(\Lambda)$  is also finite.

The rank of the abelian group  $K_1(\Lambda)$  is defined as  $\dim_{\mathbb{Q}}(\mathbb{Q} \otimes_{\mathbb{Z}} K_1(\Lambda))$ . We obtain at once:

**(45.21) Theorem (Bass [66]).** *Let A be a f.d. semisimple  $\mathbb{Q}$ -algebra, and let  $\Lambda$  be a  $\mathbb{Z}$ -order in A. Then*

(i) The rank of  $K_1(\Lambda)$  equals  $r - q$ , where  $q$  is the number of Wedderburn components of  $A$ , and  $r$  the number of Wedderburn components of  $R \otimes_{\mathbb{Q}} A$ .

(ii) Let  $\Lambda = \mathbb{Z}G$ , where  $G$  is a finite group. Then  $\text{rank } K_1(\Lambda) = r - q$ , where  $r$  is the number of nonisomorphic simple  $RG$ -modules, and  $q$  the corresponding number of  $\mathbb{Q}G$ -modules.

*Proof.* By (45.18),

$$\text{rank } K_1(\Lambda) = \text{rank } K_1(\Lambda'),$$

where  $\Lambda'$  is a maximal  $\mathbb{Z}$ -order in  $A$  containing  $\Lambda$ . Let  $C$  be the center of  $A$ , and  $\mathfrak{O}$  the integral closure of  $\mathbb{Z}$  in  $C$ . Then we may write

$$C = \prod_{i=1}^q F_i, \quad \mathfrak{O} = \prod_{i=1}^q R_i, \quad R_i = \text{alg.int.}\{F_i\},$$

where  $F_i$  is the center of the  $i$ -th Wedderburn component of  $A$ . By (45.7) and (45.20),

$$\text{rank } K_1(\Lambda') = \text{rank}(\mathfrak{O}^\times \cap C^\times) = \text{rank } \mathfrak{O}^\times = \sum_{i=1}^q \text{rank } R_i^\times.$$

Let  $n_i$  be the number of infinite primes of  $F_i$ ,  $1 \leq i \leq q$ . Then  $R \otimes_{\mathbb{Q}} F_i$  is a direct sum of  $n_i$  fields, each summand being either  $R$  or  $C$ . It follows that  $r = \sum_{i=1}^q n_i$ . On the other hand,  $\text{rank } R_i^\times = n_i - 1$  by the Dirichlet Unit Theorem (see Weiss [63, Theorem 5.3.10], for example). Thus

$$\text{rank } K_1(\Lambda') = \sum_{i=1}^q (n_i - 1) = r - q,$$

which establishes (i). Assertion (ii) is a special case of (i).

We shall now give C. T. C. Wall's proof of the  $p$ -adic version of (45.20) (see Wall [73], Kuku [76]). The methods used will be needed for a finer investigation of the structure of  $K_1(\Lambda)$  and  $SK_1(\Lambda)$ . The proof uses some easy facts about topological groups, and relies on a theorem of Borel about subgroups of  $SL_n(A)$ , rather than on the Injective Stability Theorem and relative  $K$ -theory.

**(45.22) Theorem.** Let  $K$  be a finite extension of the  $p$ -adic field  $\mathbb{Q}_p$ ,  $R$  its d.v.r., and let  $\Lambda$  be an  $R$ -order in a f.d. semisimple  $K$ -algebra  $A$ . Then  $SK_1(\Lambda)$  is finite.

*Proof.* Let  $n \geq 2$ , and topologize both the group  $GL_n(A)$ , and its subgroup  $GL_n(\Lambda)$ , by choosing as basis for the open neighborhoods of 1 the normal subgroups  $\{1 + p^k M_n(\Lambda) : k = 1, 2, \dots\}$ . Note that

$$1 + p^k M_n(\Lambda) = \{1 + x : x \in p^k M_n(\Lambda)\},$$

by definition. The center  $C$  of  $A$  is a direct sum of  $p$ -adic fields, and so  $C^\circ$  may be topologized in a similar manner.

The reduced norm  $\text{nr}_{A/C}$  induces a continuous homomorphism of topological groups

$$\text{nr}: GL_n(A) \rightarrow C^\circ,$$

whose kernel  $SL_n(A)$  is a closed normal subgroup of  $GL_n(A)$ . We have

$$SL_n(A) = [GL_n(A), GL_n(A)], \quad K_1(A) = GL_n(A)/SL_n(A)$$

by §45A. Then  $K_1(A)$  is a topological group, with the topology induced from that of  $GL_n(A)$ .

The homomorphism  $\theta$  defined by composition of maps

$$GL_n(\Lambda) \rightarrow GL_n(A) \rightarrow K_1(A)$$

is also a continuous map. Set

$$W_n = \ker \theta = GL_n(\Lambda) \cap SL_n(A).$$

Then there is a commutative diagram with exact rows:

$$\begin{array}{ccccccc} 1 & \longrightarrow & W_n & \longrightarrow & GL_n(\Lambda) & \xrightarrow{\theta} & K_1(A) \\ & & \alpha \downarrow & & \beta \downarrow & & 1 \downarrow \\ 1 & \longrightarrow & SK_1(\Lambda) & \longrightarrow & K_1(\Lambda) & \longrightarrow & K_1(A). \end{array}$$

Clearly  $\ker \alpha \leq \ker \beta \leq \ker \theta$ , so we have  $\ker \alpha = \ker \beta$ . Furthermore, since  $\beta$  is surjective, so is  $\alpha$ .

Now  $SL_n(A)$  is a closed subgroup of  $GL_n(A)$ , and  $GL_n(\Lambda)$  is a compact open subgroup of  $GL_n(A)$ , so  $W_n$  is a compact open subgroup of  $SL_n(A)$ . By a theorem\* of Borel (the proof is given in the article by Riehm [70]), every noncentral normal subgroup of an open subgroup of  $SL_n(A)$  is also open. Thus  $\ker \alpha$  is an open subgroup of  $SL_n(A)$ , and is therefore also open in  $W_n$ . This implies that  $W_n/\ker \alpha$  is a discrete group. On the other hand, since  $\ker \alpha$  is open in  $W_n$ , it is also closed in  $W_n$ . Since  $W_n$  is compact, therefore so is  $W_n/\ker \alpha$ . But then  $SK_1(\Lambda) \cong W_n/\ker \alpha$  is a compact discrete group, and must therefore be finite.

**(45.23) Corollary.** *Let  $n \geq 2$ , and let  $\beta: GL_n(\Lambda) \rightarrow K_1(\Lambda)$ . Then  $\ker \beta$  is a closed normal subgroup of  $GL_n(\Lambda)$ .*

*Proof.* Using the notation of the preceding proof, we have shown that  $\ker \beta$  is open (and hence closed) in  $W_n$ . But  $W_n$  is the kernel of the continuous homomorphism  $\theta$ , so  $W_n$  is closed in  $GL_n(\Lambda)$ . Therefore  $\ker \beta$  is closed in  $GL_n(\Lambda)$ .

\*This uses the hypothesis  $n \geq 2$ .

### §45D. Profinite Groups

We shall give here a brief summary of the theory of profinite groups; for more details, see the article by Gruenberg (Chapter V of Cassels-Fröhlich [67]), and also Ribes [70]. Topological background is given in Eilenberg-Steenrod [52] and Pontrjagin [39], while results on inverse limits can be found in Rotman [79]. Some of the ideas in this subsection will be needed for a finer discussion of  $K_1$  and  $SK_1$  of  $p$ -adic orders, and also in §49 on locally free class groups.

**(45.24) Definition.** An *inverse system* of groups  $\{G_i\}$  and homomorphisms  $\{\varphi_{ji}\}$ , where

$$\varphi_{ji}: G_j \rightarrow G_i, \quad \text{for } 1 \leq i \leq j,$$

is a collection of groups and homomorphisms such that

$$\varphi_{ii} = 1 \quad \text{for all } i, \quad \varphi_{ji}\varphi_{ki} = \varphi_{ki} \quad \text{for } 1 \leq i \leq j \leq k.$$

An element  $\langle x_1, x_2, \dots \rangle \in \prod_{i=1}^{\infty} G_i$  is *coherent* if

$$\varphi_{ji}(x_j) = x_i \quad \text{for } 1 \leq i \leq j.$$

The set  $G$ , consisting of all coherent elements of the direct product  $\prod_{i=1}^{\infty} G_i$ , is a subgroup of  $\prod_i G_i$ , called the *inverse limit* (or *projective limit*) of the inverse system. We write

$$G = \varprojlim G_i.$$

There is a canonical projection  $\pi_i: G \rightarrow G_i$ , mapping each element of  $G$  onto its  $i$ -th coordinate. As shown in Exercise 45.6, the inverse limit may be characterized in terms of a universal mapping property.

**Remarks.** It is sometimes more convenient to partially order the integers by divisibility, rather than by size. In this situation, an inverse system  $\{G_i, \varphi_{ji}\}$  consists of groups and homomorphisms  $\{\varphi_{ji}\}$  for  $i$  dividing  $j$ , satisfying obvious compatibility requirements.

More generally, let  $I$  be any directed set with respect to an order relation  $\prec$  (which is transitive and reflexive). This means that for any  $i, j \in I$ , there exists  $k \in I$  such that  $i \prec k$  and  $j \prec k$ . We can then define  $\varprojlim$  in the same way as above.

Suppose now that each  $G_i$  is a Hausdorff topological group (see Eilenberg-Steenrod [52]), and that for  $i \leq j$ ,  $\varphi_{ji}: G_j \rightarrow G_i$  is a continuous surjection. Then  $G = \varprojlim G_i$  is also a topological group, whose topology is given as follows: the direct product  $\prod_{i=1}^{\infty} G_i$  has a *product topology*, in which a fundamental system of neighborhoods of 1 in  $\prod_i G_i$  is given by all products  $\prod N_i$ , where  $N_i = G_i$  a.e. (almost everywhere, that is, for all but a finite number of subscripts  $i$ ), and where for those exceptional values of  $i$ ,  $N_i$  is a neighborhood of 1 in  $G_i$ . If each  $G_i$  is compact, then so is  $\prod_i G_i$  in the product topology.

Let  $G = \varprojlim G_i$ ; then  $G$  is a closed subgroup of  $\prod G_i$ , and  $G$  inherits a topology from  $\prod G_i$ , namely, the open sets in  $G$  are given by  $\{G \cap U : U = \text{open set in } \prod G_i\}$ . If each  $G_i$  is compact, then since  $G$  is closed in  $\prod G_i$ , the group  $G$  is also compact.

**(45.25) Definition.** A *profinite group* is a projective limit

$$G = \varprojlim G_i$$

of an inverse system of discrete finite groups  $\{G_i\}$ . (If  $p$  is a prime and each  $G_i$  is a finite  $p$ -group, we call  $G$  a *pro- $p$ -group*.)

Let  $\pi_i: G \rightarrow G_i$  be the canonical projection map, and put  $U_i = \ker \pi_i$ . Then the  $\{U_i\}$  are a basis for the neighborhoods of 1 in  $G$ , and are open normal subgroups of  $G$ . It is easily seen that  $G = \varprojlim G/U_i$ . In fact, there is no loss of generality in assuming each  $\varphi_{ji}$  surjective, since otherwise we may replace  $G_i$  by  $\bigcap_{j \geq i} \text{im } \varphi_{ji}$ . But then each  $\pi_i$  is surjective, and  $G/U_i \cong G_i$ . We note that the profinite group  $G$  is compact, since each  $G_i$  is compact. (It can be shown that a topological group  $G$  is profinite if and only if  $G$  is Hausdorff, compact, and totally disconnected (see Gruenberg, loc. cit.).)

**Example.** Let  $R$  be a complete d.v.r. with maximal ideal  $P$ , and finite residue class field  $R/P$ . Let  $G_i = R/P^i$ ,  $i \geq 1$ , and let  $\varphi_{ji}$  be the canonical surjection  $G_j \rightarrow G_i$  for  $j \geq i$ . A coherent element  $\langle x_1, x_2, \dots \rangle$  is a sequence of elements of  $R$ , with  $x_i$  unique mod  $P^i$ , such that

$$x_{i+1} \equiv x_i \pmod{P^i}, \quad i \geq 1.$$

Such a coherent element defines a unique element of  $R$ , since  $R$  is complete in the  $P$ -adic topology. Conversely, each  $y \in R$  yields a coherent element  $\langle y_1, y_2, \dots \rangle$ , where  $y_i$  is the image of  $y$  in  $G_i$ . Thus we have

$$R = \varprojlim R/P^i.$$

Further, the additive subgroups  $\{P^i\}$  are a basis for the neighborhoods of 0 in  $R$ , so the  $P$ -adic and profinite topologies of  $R$  are the same.

Suppose now that  $G = \varprojlim G_i$  is any profinite group. Each open subgroup  $U$  of  $G$  contains a subgroup  $U_i$  for some  $i$ , where  $U_i = \ker \pi_i$ , and so the index  $|G:U|$  is necessarily finite. Further, the coset decomposition  $G = \bigcup_i (x_i U)$  shows that the complement of  $U$  in  $G$  is open, so  $U$  must be closed in  $G$ . Let  $\{H_j\}$  be the collection of open normal subgroups of  $G$ , partially ordered by reverse inclusion:  $j \leq k$  whenever  $H_j \supseteq H_k$ . For  $j \leq k$ , there is a natural surjection  $G/H_k \rightarrow G/H_j$ . Then we have:

**(45.26) Proposition.** Let  $\{H_j\}$  be the collection of all open normal subgroups of  $G$ , ordered by reverse inclusion. Then there is an isomorphism of topological

groups

$$G = \varprojlim G/H_j,$$

and each  $H_j$  is a closed subgroup of  $G$  of finite index.

For the proof of the above, and also for that of (45.27) below, see Gruenberg, loc. cit. Further, we have:

**(45.27) Proposition.** *Let  $H$  be any closed subgroup of a profinite group  $G$ , and let  $U$  range over all open normal subgroups of  $G$  of finite index. Then*

(i)  $H$  is profinite, and

$$H \cong \varprojlim H/(H \cap U).$$

(ii) If  $H \trianglelefteq G$ , then

$$G/H \cong \varprojlim G/HU$$

is profinite.

In the above, we can replace the system  $\{U\}$  by the system  $\{U_i\}$ , where  $U_i = \ker \pi_i$ .

We now give some more examples of profinite groups.

**(45.28) Example.** Let

$$\hat{\mathbb{Z}} = \varprojlim \mathbb{Z}/n\mathbb{Z},$$

where the set of subgroups  $\{n\mathbb{Z}: n \geq 1\}$  is ordered by reverse inclusion. Then  $\hat{\mathbb{Z}}$  is the *profinite completion* of  $\mathbb{Z}$ , and there is an isomorphism

$$\hat{\mathbb{Z}} \cong \prod_p \mathbb{Z}_p,$$

where  $p$  ranges over all primes, and  $\mathbb{Z}_p$  is the ring of  $p$ -adic integers. Note that

$$\mathbb{Z}_p = \varprojlim \mathbb{Z}/p^i\mathbb{Z}$$

is a pro- $p$ -group.

**(45.29) Example.** Let  $R$  be a complete d.v.r. with maximal ideal  $P$  and finite residue class field  $\bar{R}$  of characteristic  $p$ . Let  $\Lambda$  be an  $R$ -order, and put  $J = \text{rad } \Lambda$ , so  $\Lambda/J$  is a f.d. semisimple  $\bar{R}$ -algebra, and is therefore a finite  $p$ -group. By (6.8),  $\Lambda$  is complete in the  $J$ -adic topology, so

$$\Lambda = \varprojlim \Lambda/J^n.$$

For each  $n$ , there is a filtration

$$\Lambda/J^n \supseteq J/J^n \supseteq J^2/J^n \supseteq \dots$$

whose factors  $J^i/J^{i+1}$  are  $(\Lambda/J)$ -modules, and are thus finite  $p$ -groups. This shows that each  $\Lambda/J^n$  is a  $p$ -group, and so  $\Lambda$  is a pro- $p$ -group.

Now put

$$1 + J^n = \{1 + x : x \in J^n\}, \quad n \geq 1,$$

a subgroup of the group of units  $\Lambda^\times$  of  $\Lambda$ . We topologize  $\Lambda^\times$  by choosing the groups  $\{1 + J^n\}$  as basis for the neighborhoods of 1 in  $\Lambda^\times$ . Then  $\Lambda^\times$  is complete in this topology (since  $\Lambda$  is complete in the  $J$ -adic topology), and we have

$$\Lambda^\times = \varprojlim \Lambda^\times / (1 + J^n).$$

Further,

$$1 + J = \varprojlim (1 + J) / (1 + J^n).$$

Now for each  $n$  there is a chain

$$(1 + J) / (1 + J^n) \supseteq (1 + J^2) / (1 + J^n) \supseteq \dots,$$

with factors  $(1 + J^i) / (1 + J^{i+1})$ . However, there is an isomorphism

$$(1 + J^i) / (1 + J^{i+1}) \cong J^i / J^{i+1}$$

where the left-hand side is a multiplicative group, the right-hand side an additive group. Thus  $(1 + J) / (1 + J^n)$  is a finite  $p$ -group, so  $1 + J$  is a pro- $p$ -group.

**(45.30) Example.** Let  $K \subseteq N$  be fields, with  $N$  a Galois extension of  $K$ , that is,  $N$  is an algebraic extension of  $K$  which is the splitting field of a set of separable polynomials over  $K$ . We do not assume  $\dim_K N$  finite. Let  $\text{Gal}(N/K)$  be the Galois group of  $N/K$ , that is, the group of  $K$ -automorphisms of  $N$ . We show that  $\text{Gal}(N/K)$  is a profinite group.

Let  $\{L_i\}$  range over all fields with  $K \subseteq L_i \subseteq N$ ,  $L_i/K$  finite Galois, and put  $G_i = \text{Gal}(L_i/K)$ . Partially order the fields  $\{L_i\}$  by inclusion, so for  $L_i \subseteq L_j$  there is a natural surjection  $G_j \rightarrow G_i$ . Each  $\sigma \in G$  is uniquely determined by its restrictions  $\sigma|_{L_i} \in G_i$  for all  $i$ , and  $\sigma$  determines a coherent element  $\langle \sigma|_{L_i} \rangle \in \prod_i G_i$ . Conversely, each coherent element  $\langle \sigma_i \rangle \in \prod_i G_i$  determines a unique  $\sigma \in G$ , so we have

$$G = \varprojlim G_i.$$

The kernel  $H_i$  of the surjection  $G \rightarrow G_i$  is given by

$$H_i = \text{Gal}(N/L_i),$$

for each  $i$ . These  $\{H_i\}$  form a basis for the neighborhoods of 1 in the profinite group  $G$ .

Each open subgroup  $U$  of  $G$  contains some  $H_i$ , and its fixed field  $N^U$  is then a subfield of  $L_i$ . We have

$$|G:U| = \dim_K N^U,$$

so  $|G:U|$  is finite. Conversely, given any finite extension  $L/K$ ,  $L \subseteq N$ , not necessarily Galois, let  $U = \text{Gal}(N/L)$ . Then  $U$  is an open subgroup of  $G$  (of finite index). The normal open subgroups of  $G$  are precisely the groups  $\{H_i\}$ .

We quote without proof the following result, which shows the significance of the topological structure of the profinite group  $\text{Gal}(N/K)$ : *Krull's Theorem*. Let  $N/K$  be a Galois extension. Then there is a lattice antiisomorphism  $H \leftrightarrow L$  between the set of closed subgroups  $H$  of the profinite group  $\text{Gal}(N/K)$ , and the set of fields  $L$  with  $K \subseteq L \subseteq N$ . The correspondence is given by

$$L = \text{subfield of } N \text{ fixed by } H, \quad \text{and } H = \text{Gal}(N/L).$$

We shall conclude this subsection with a result of Wall's on  $K_1$  of  $p$ -adic orders, which will be needed for the discussion of Whitehead groups in §46.

**(45.31) Theorem.** *Let  $R$  be a complete d.v.r. with maximal ideal  $P$  and finite residue class field  $\bar{R}$  of characteristic  $p$ . Let  $\Lambda$  be an  $R$ -order, and put  $\bar{\Lambda} = \Lambda/J$ , where  $J = \text{rad } \Lambda$ . Then there is an exact sequence*

$$(45.32) \quad 1 \rightarrow V \rightarrow K_1(\Lambda) \rightarrow K_1(\bar{\Lambda}) \rightarrow 1,$$

in which  $V$  is a pro- $p$ -group and  $K_1(\bar{\Lambda})$  is a finite group of order prime to  $p$ . The sequence has a canonical splitting, so

$$K_1(\Lambda) \cong V \times K_1(\bar{\Lambda}).$$

*Proof.* Since  $\bar{R}$  is finite, we may write

$$\bar{\Lambda} = \coprod_i M_{n_i}(F_i), \quad F_i = \text{finite field extension of } \bar{R}.$$

Then

$$K_1(\bar{\Lambda}) \cong \prod_i K_1(F_i) \cong \prod_i F_i^\times.$$

Each  $F_i$  is a finite group of order prime to  $p$ , so the same is true of  $K_1(\bar{\Lambda})$ .

Now let  $\Gamma = M_2(\Lambda)$ , so  $\text{rad } \Gamma = M_2(J)$ , and we set  $\bar{\Gamma} = \Gamma/\text{rad } \Gamma \cong M_2(\bar{\Lambda})$ . There is a commutative diagram with exact rows:

$$\begin{array}{ccccccc} 1 & \longrightarrow & 1 + \text{rad } \Gamma & \longrightarrow & \Gamma^\times & \xrightarrow{\gamma} & \Gamma^\times \longrightarrow 1 \\ & & \psi \downarrow & & \beta \downarrow & & \delta \downarrow \\ 1 & \longrightarrow & V & \longrightarrow & K_1(\Lambda) & \xrightarrow{\lambda} & K_1(\bar{\Lambda}) \longrightarrow 1, \end{array}$$

in which  $\beta, \gamma$  and  $\delta$  are surjective, and  $V = \ker \lambda$ . (Since  $\lambda\beta = \delta\gamma$ ,  $\lambda$  is also surjective. The map  $\psi$  is induced by  $\beta$ .)

Next, we have

$$\ker \beta \geq [\Gamma^*, \Gamma^*], \quad \ker \delta = [\bar{\Gamma}^*, \bar{\Gamma}^*],$$

so  $\gamma$  maps  $\ker \beta$  onto  $\ker \delta$ . The Snake Lemma then shows that  $\psi$  is surjective, so now

$$V \cong (1 + \text{rad } \Gamma) / \ker \psi.$$

From (45.29),  $1 + \text{rad } \Gamma$  is an open (and closed) subgroup of the profinite group  $\Gamma^*$ , and is itself a pro- $p$ -group. Further,  $\ker \beta$  is closed in  $\Gamma^*$  by (45.23). Since

$$\ker \psi = (\ker \beta) \cap (1 + \text{rad } \Gamma),$$

it follows that  $\ker \psi$  is a closed normal subgroup of  $1 + \text{rad } \Gamma$ . Therefore  $V$  is a pro- $p$ -group by (45.27ii). We leave it as an exercise to deduce that the sequence (45.32) has a canonical splitting (see Exercise 10).

## §45. Exercises

- Let  $K$  be a global field,  $R$  a Dedekind domain with quotient field  $K$ , and let  $A$  be a f.d. simple  $K$ -algebra with center  $F$ . Let  $S$  be the integral closure of  $R$  in  $F$ . Prove that  $A$  satisfies the Eichler condition (45.4) relative to  $R$  if and only if  $A$  satisfies the Eichler condition relative to  $S$ .

[Hint: Every  $P$ -adic valuation of  $K$  arising from a maximal ideal of  $R$  extends to a  $Q$ -adic valuation of  $F$  arising from a maximal ideal of  $S$ . Thus, the non- $R$  primes  $P$  of  $K$  extend to non- $S$  primes  $Q$  of  $F$ , with  $Q|_K = P$ . Let  $\{Q_i\}$  be the set of all primes of  $F$  which extend a given non- $R$  prime  $P$  of  $K$ . Then

$$K_P \otimes_K F = F_P \cong \coprod_i F_{Q_i},$$

so

$$A_P = K_P \otimes_K A \cong (K_P \otimes_K F) \otimes_F A \cong \coprod_i A_{Q_i}.$$

Thus, the Wedderburn components of  $A_P$  are the central simple  $F_{Q_i}$ -algebras  $A_{Q_i}$ .]

- Let  $R$  be a complete d.v.r. with quotient field  $K$  and finite residue class field  $\bar{R}$ . Let  $\Lambda$  be a maximal order in a central simple  $K$ -algebra  $A$ . Then show that  $\text{nr}_{A/K}(\Lambda) = R$ .

[Hint: Using the notation in the proof of (45.8), let  $\pi_D$  be a prime element of  $\Delta$ . Show that  $\text{nr}_{D/K}\pi_D = \pm \pi$ , where  $\pi$  is a prime element of  $R$ . Thus  $\text{nr } \Lambda$  contains  $\pm \pi$  and  $R^*$ , by (45.8).]

- Using the notation of (45.13), show that

$$SK_1(\Delta) \cong \bar{\Delta}^*/\bar{R}^*, \quad SK_1(\Delta) \cong [\Delta^*, D^*]/[\Delta^*, \Delta^*], \quad K_1(\Delta) \cong \Delta^*/[\Delta^*, \Delta^*].$$

- Let  $\Lambda$  be an  $R$ -order in a separable  $A$ . Define  $C^+$  as in (45.9), and let  $\mathfrak{O}$  be the integral

closure of  $R$  in  $C$ . Prove that  $\text{nr } K_1(\Lambda)$  is a subgroup of finite index in  $\mathfrak{O}^* \cap C^+$ , and is therefore also of finite index in  $\mathfrak{O}^*$ .

[Hint: Choose  $\Gamma$  a maximal order containing  $\Lambda$ , so  $\text{nr } K_1(\Gamma) = \mathfrak{O}^* \cap C^+$ . If  $\beta: K_1(\Lambda) \rightarrow K_1(\Gamma)$ , then

$$\text{nr}_{A/C}(\text{cok } \beta) = (\mathfrak{O}^* \cap C^+)/\text{nr } K_1(\Lambda).]$$

5. Let  $\Lambda \subset \Gamma$  be  $R$ -orders in a separable  $K$ -algebra  $A$ , and let  $r\Gamma \subset \Lambda$  where  $r \in R$ ,  $r \neq 0$ . Show that the map  $K_1(\Lambda) \rightarrow K_1(\Gamma)$  has finite cokernel, by using the Mayer-Vietoris sequence associated with the fiber product

$$\begin{array}{ccc} \Lambda & \longrightarrow & \Lambda/r\Gamma \\ \downarrow & & \downarrow \\ \Gamma & \longrightarrow & \Gamma/r\Gamma. \end{array}$$

6. Let  $\{G_i, \varphi_{ji}\}$  be an inverse system of groups and homomorphisms, and let  $G = \varprojlim G_i$ . Define  $\pi_i: G \rightarrow G_i$  as the canonical projection, for each  $i$ . Show that  $G$  satisfies the following universal mapping property, which characterizes  $G$  up to isomorphism:

For each group  $X$  and each family of homomorphisms  $\theta_i: X \rightarrow G_i$  such that  $\varphi_{ji}\theta_j = \theta_i$  whenever  $i \leq j$ , there is a unique homomorphism  $\theta: X \rightarrow G$  for which  $\theta_i = \pi_i\theta$  for all  $i$ .

7. Let  $\{M_i, \varphi_{ji}\}$  be an inverse system of  $A$ -modules and  $A$ -homomorphisms, where  $A$  is an arbitrary ring. Prove that for an  $A$ -module  $L$ ,

$$\varprojlim \text{Hom}_A(L, M_i) \cong \text{Hom}_A(L, \varprojlim M_i).$$

8. Prove that the inverse limit of an inverse system of profinite groups is again a profinite group. Show also that the direct product of profinite groups is profinite.

9. Show that a finite subgroup of a pro- $p$ -group must be a  $p$ -group. Show that any finite quotient group of a pro- $p$ -group must be a  $p$ -group.

[Hint: Let  $G = \varprojlim G_i$ , where each  $G_i$  is a finite  $p$ -group, and let  $\theta: G \rightarrow F$  be a surjection, with  $F$  a finite group of order  $p^k n$ , where  $p \nmid n$ . Each  $x \in G$  is of the form  $x = \langle x_i \rangle \in \prod G_i$ . For each  $i$ , there is a unique  $y_i \in G_i$  with  $x_i = \langle y_i \rangle^n$ . Then  $y = \langle y_i \rangle$  also lies in  $G$ , and  $x = y^n$ . Therefore  $\theta(x) = \theta(y)^n$ , so the order of  $\theta(x)$  is a divisor of  $p^k$ . This shows that every element of  $F$  has  $p$ -power order, so  $n = 1$ .]

10. Let  $p$  be prime, and let  $1 \rightarrow G \rightarrow A \rightarrow E \rightarrow 1$  be an exact sequence of abelian groups, in which  $G$  is a pro- $p$ -group and  $E$  is a finite  $p'$ -group. Prove that there is a canonical splitting of this sequence.

[Hint: Let

$$1 \rightarrow G \xrightarrow{\gamma} A \xrightarrow{\alpha} E \rightarrow 1$$

be an exact sequence of abelian groups, where  $G$  is a pro- $p$ -group and  $E$  is a finite  $p'$ -group. There is a unique homomorphism  $\varphi: A \rightarrow G$  which splits  $\gamma$ . To construct  $\varphi$ , suppose first that  $G$  is a finite  $p$ -group, and let  $e = |E|$ , so  $p \nmid e$ . Choose  $n \in \mathbb{Z}$  with

$$n \equiv 0 \pmod{e}, \quad n \equiv 1 \pmod{|G|}.$$

Then for  $a \in A$ , there is a unique  $g \in G$  with  $a^n = \gamma(g)$ , and we define  $\varphi(a) = g$ . It is easily checked that  $\varphi\gamma = \text{id}_G$ , and that  $\varphi$  is independent of the choice of  $n$ , and finally that  $\varphi$  is the unique splitting of  $\gamma$ .

Now let  $G = \varprojlim G_i$ , where for each  $i$  we have  $G_i = G/H_i =$  finite  $p$ -group. Given the above exact sequence, we obtain (for each  $i$ ) a commutative diagram of abelian groups, with exact rows:

$$\begin{array}{ccccccc} 1 & \longrightarrow & G & \xrightarrow{\gamma} & A & \xrightarrow{\alpha} & E \longrightarrow 1 \\ & & \downarrow & & \pi_i \downarrow & & \downarrow 1 \\ 1 & \longrightarrow & G/H_i & \xrightarrow{\gamma_i} & A/H_i & \xrightarrow{\alpha_i} & E \longrightarrow 1. \end{array}$$

Then there is a unique  $\varphi_i: A/H_i \rightarrow G/H_i$  which splits  $\gamma_i$ , and we define the required splitting  $\varphi: A \rightarrow G$  by the formula

$$\varphi(a) = \langle \varphi_i \pi_i(a): i = 1, 2, \dots \rangle.]$$

11. Let  $R$  be a complete d.v.r. with finite residue class field  $\bar{R}$ . Show that the surjection  $R^\times \rightarrow \bar{R}^\times$  has a canonical splitting

$$t: \bar{R}^\times \rightarrow R^\times \quad (\text{Teichmüller map}).$$

[Hint: If  $q = \text{card } \bar{R}$ , then  $R$  contains  $\omega$ , a primitive  $(q - 1)$ -st root of 1, and the map  $\langle \omega \rangle \rightarrow \langle \bar{\omega} \rangle$  is an isomorphism, whose inverse is  $t$ .]

12. Show that any homomorphism  $\Lambda \rightarrow \Delta$  of commutative rings induces a homomorphism of groups

$$SK_1(\Lambda) \rightarrow SK_1(\Delta).$$

13. Let  $\Lambda_i$  be an  $R$ -order in a separable  $K$ -algebra  $A_i$ ,  $i = 1, 2$ , where  $K$  is a global field which is the quotient field of a Dedekind domain  $R$ . Show that any  $K$ -algebra homomorphism  $A_1 \rightarrow A_2$ , which carries  $\Lambda_1$  into  $\Lambda_2$ , induces a homomorphism

$$SK_1(\Lambda_1) \rightarrow SK_1(\Lambda_2).$$

14. Let  $\Lambda$  be an  $R$ -order in a separable  $K$ -algebra  $A$  (as above), and let  $P$  be any maximal ideal of  $R$ . Then the inclusion  $\Lambda \rightarrow \Lambda_P$  induces a map  $SK_1(\Lambda) \rightarrow SK_1(\Lambda_P)$ .

## §46. WHITEHEAD GROUPS OF INTEGRAL GROUP RINGS

We present here C. T. C. Wall's results on the Whitehead group<sup>†</sup>  $\text{Wh}(RG)$ , where  $R$  is a commutative ring and  $G$  is a finite group. Let

$$G^{ab} = G/[G, G] = \text{commutator factor group of } G,$$

<sup>†</sup>We have previously referred to  $K_1$  as a "Whitehead group," but we shall avoid that terminology here.

and let  $RG^{ab}$  denote its group ring over  $R$ . The composite map

$$G \rightarrow (RG)^* \rightarrow K_1(RG)$$

induces a homomorphism  $G^{ab} \rightarrow K_1(RG)$ . Likewise, the inclusion  $\eta: R \rightarrow RG$  induces a homomorphism  $\eta_*: K_1(R) \rightarrow K_1(RG)$ . In order to define  $\text{Wh}(RG)$ , we need a preliminary result:

**(46.1) Proposition.** *The homomorphism*

$$\varphi: K_1(R) \times G^{ab} \rightarrow K_1(RG)$$

*is injective.*

*Proof.* The augmentation map  $\varepsilon: RG \rightarrow R$  induces  $\varepsilon_*: K_1(RG) \rightarrow K_1(R)$ . Since  $\varepsilon\eta = \text{id}_R$ , we have  $\varepsilon_*\eta_* = 1$ , so  $\eta_*$  is injective and  $\varepsilon_*$  is surjective. Since  $\varepsilon_*\{\varphi(G^{ab})\} = 1$  in  $K_1(R)$ , it follows that the product  $K_1(R) \times \varphi(G^{ab})$  in  $K_1(RG)$  is a direct product. We must still check that  $\varphi: G^{ab} \rightarrow K_1(RG)$  is injective. But there are homomorphisms

$$G^{ab} \xrightarrow{\varphi} K_1(RG) \longrightarrow K_1(RG^{ab}) \xrightarrow{\det} (RG^{ab})^*,$$

where composite is the inclusion  $G^{ab} \rightarrow (RG^{ab})^*$ . Therefore  $\varphi$  is injective, and the result is established.

From now on, we identify  $K_1(R) \times G^{ab}$  with its image in  $K_1(RG)$ , and define the *Whitehead group* as

$$(46.2) \quad \text{Wh}(RG) = K_1(RG)/(K_1(R) \times G^{ab})$$

When  $R = \mathbb{Z}$ , we write simply  $\text{Wh}(G)$ . Since  $K_1(\mathbb{Z}) = \{\pm 1\}$ , we have

$$(46.3) \quad \text{Wh}(G) = K_1(\mathbb{Z}G)/\pm G^{ab}.$$

Let us now recall (see Exercise 9.17 or CR §37):

**Theorem (G. Higman).** *Let  $R = \text{alg. int. } \{F\}$ , where  $F$  is an algebraic number field, and let  $G$  be a finite abelian group. Then every unit of  $RG$  of finite order is of the form  $\varepsilon x$ , with  $\varepsilon$  a root of unity in  $R$ , and  $x \in G$ . In other words,*

$$\text{torsion subgroup of } (RG)^* = (\text{torsion subgroup of } R^*) \times G.$$

C. T. C. Wall [74c] generalized this to an arbitrary finite group  $G$ , by proving a K-theoretic version in which  $(RG)^*$  is replaced by  $K_1(RG)$ . Of course,  $SK_1(RG)$  lies in the torsion subgroup of  $K_1(RG)$ . The aim of this section is to prove:

**(46.4) Wall's Theorem.** *Let  $R$  be the ring of all algebraic integers in an algebraic*

number field  $F$ , and let  $G$  be an arbitrary finite group. Then the torsion subgroup of  $K_1(RG)$  is precisely

$$(\text{torsion subgroup of } R^\times) \times G^{ab} \times SK_1(RG).$$

The proof of Wall's Theorem is based on the following steps:

1. It suffices to show that  $\text{Wh}^F(RG)$  is torsionfree, where (see below)

$$\text{Wh}^F(RG) = K_1(RG)/(SK_1(RG) \times K_1(R) \times G^{ab}).$$

2. To prove  $\text{Wh}^F(RG)$  torsionfree, it suffices to establish the result after extending or completing the ground field (Lemma 46.8)
3. For  $R = p$ -adic ring,  $SK_1(RG)$  is a finite  $p$ -group (Theorem 46.9).
4. For  $G = p$ -group and  $R = p$ -adic ring,  $\text{Wh}^F(RG)$  is  $p$ -torsionfree (Theorem 46.10).
5. For  $R = \text{alg. int. } \{F\}$ , induction techniques reduce the problem of  $p$ -torsion in  $\text{Wh}^F(RG)$  to the case where  $G$  is a  $p$ -hyper-elementary group (Prop. 46.22). This case is easily handled by using the results of the previous steps.

Our first step in the proof of Wall's Theorem is to reduce the problem to calculations in  $K_1(FG)$ . Let  $K_1^F(RG)$  denote the image of  $K_1(RG)$  in  $K_1(FG)$ , so the sequence

$$1 \rightarrow SK_1(RG) \rightarrow K_1(RG) \rightarrow K_1^F(RG) \rightarrow 1$$

is exact. There is a commutative diagram

$$(46.5) \quad \begin{array}{ccc} K_1(R) \times G^{ab} & \xrightarrow{\varphi} & K_1(RG) \\ & \searrow \varphi' & \downarrow \\ & & K_1^F(RG). \end{array}$$

The proof of (46.1) shows that the map  $K_1(F) \times G^{ab} \rightarrow K_1(FG)$  is injective. We define

$$\text{Wh}^F(RG) = K_1^F(RG)/(K_1^F(R) \times G^{ab}),$$

where  $K_1^F(R)$  is the image of  $K_1(R)$  in  $K_1(F)$ , that is,  $K_1^F(R) = R^\times$ . Since  $SK_1(R) = 1$  by the Bass-Milnor-Serre Theorem, we have  $K_1(R) \cong K_1^F(R) = R^\times$ . It follows that  $\varphi'$  is injective, the sequence

$$1 \rightarrow SK_1(RG) \rightarrow \text{Wh}(RG) \rightarrow \text{Wh}^F(RG) \rightarrow 1$$

is exact, and  $SK_1(RG) \times K_1(R) \times G^{ab}$  is a direct product in  $K_1(RG)$ . Wall's Theorem is therefore equivalent to each of the following equivalent assertions:

$$(46.6) \quad \begin{cases} \text{(i) torsion subgroup of } K_1^F(RG) = (\text{torsion subgroup of } R^\circ) \times G^{ab}. \\ \text{(ii) } \text{Wh}^F(RG) \text{ is torsionfree.} \end{cases}$$

We remark that (46.6) is trivially true when  $G = \{1\}$ . Next, let  $G$  be arbitrary. For any abelian group  $A$  and any prime  $p$ , define the

$$p\text{-torsion subgroup of } A = \{a \in A : p^n a = 0 \text{ for some } n \geq 0\}.$$

For  $\varphi$  and  $\varphi'$  as in (46.5), and for each prime  $p$ , it is easily seen that the following conditions are equivalent:

- (i)  $\text{im } \varphi \supseteq p\text{-torsion subgroup of } K_1(RG)$ .
- (ii)  $\varphi$  induces an isomorphism of  $p$ -torsion subgroups.
- (iii)  $\text{Wh}(RG)$  is  $p$ -torsionfree.

Further, the same remark holds with  $\varphi' K_1^F(RG)$ , and  $\text{Wh}^F(RG)$  in place of  $\varphi$ ,  $K_1(RG)$ , and  $\text{Wh}(RG)$ , respectively. We note also that

$$(46.7) \quad \text{Wh}(RG) \text{ is } p\text{-torsionfree} \Leftrightarrow \text{both } \text{Wh}^F(RG) \text{ and } SK_1(RG) \text{ are } p\text{-torsionfree.}$$

For the remainder of our discussion, either  $R = \text{alg. int. } \{F\}$  for  $F$  an algebraic number field, or else  $R$  is a d.v.r. in a  $p$ -adic field  $F$  (with  $\dim_{\mathbb{Q}_p} F < \infty$ ). Call  $R$  a  *$p$ -adic ring* in the latter case.

**Remarks.** (i) If the group  $G$  is abelian, then  $K_1^F(RG) \cong (RG)^\circ$ , so (46.6) gives Higman's Theorem, which is therefore a consequence of Wall's Theorem.

- (ii) If  $G$  is abelian and  $R$  is a  $p$ -adic ring, then by (45.12) we have

$$(RG)^\circ \cong K_1(RG) \cong K_1^F(RG), \quad SK_1(RG) = 1.$$

- (iii) If  $G$  is abelian and  $R = \text{alg. int. } \{F\}$ , then

$$(RG)^\circ \cong K_1^F(RG), \quad \text{but } SK_1(RG) \text{ may be nontrivial.}$$

**(46.8) Lemma.** *Let  $F \subseteq E$  be fields, with rings of integers  $R \subseteq S$ , such that one of the following holds:*

- (a) *Both fields are algebraic number fields.*
- (b) *Both are  $p_0$ -adic fields (for the same  $p_0$ ).*
- (c)  *$F$  is a number field, and  $E$  a  $p_0$ -adic field.*

*Then if  $\text{Wh}^E(SG)$  is  $p$ -torsionfree, so is  $\text{Wh}^F(RG)$ .*

*Proof.* Let  $C = \text{center of } FG$ , and define  $C^+$  as in (45.9). From the commutative diagram

$$\begin{array}{ccc} K_1(FG) & \xrightarrow{\text{nr}} & C^+ \\ \downarrow & & \downarrow \\ K_1(EG) & \xrightarrow{\text{nr}} & (E \otimes_F C)^+, \end{array}$$

it follows that the map  $K_1(FG) \rightarrow K_1(EG)$  is a monomorphism. Therefore so are the maps  $K_1^F(RG) \rightarrow K_1^E(SG)$  and  $K_1^F(R) \rightarrow K_1^E(S)$ . Now consider the commutative diagram

$$\begin{array}{ccccc} K_1^F(R) \times G^{ab} & \xrightarrow{\varphi} & K_1^F(RG) & \xrightarrow{\varepsilon_*} & K_1^F(R) \\ \downarrow & & \sigma \downarrow & & \sigma' \downarrow \\ K_1^E(S) \times G^{ab} & \xrightarrow{\varphi'} & K_1^E(SG) & \xrightarrow{\varepsilon'_*} & K_1^E(S), \end{array}$$

in which all vertical maps are monomorphisms. By hypothesis  $\text{Wh}^E(SG)$  is  $p$ -torsionfree, so all  $p$ -torsion elements of  $K_1^E(SG)$  lie in  $\text{im } \varphi'$ . If  $x \in K_1^F(RG)$  is a  $p$ -torsion element, then  $\sigma(x) = \varphi'(s, g)$  for some  $s \in S^*$ ,  $g \in G^{ab}$ . Then  $s = \varepsilon'_* \sigma(x) = \sigma' \varepsilon_*(x)$ , so  $s \in R^*$ . Therefore  $x \in \text{im } \varphi$ , which shows that  $\text{im } \varphi$  contains all  $p$ -torsion elements of  $K_1^F(RG)$ . This shows that  $\text{Wh}^F(RG)$  is  $p$ -torsionfree, as desired.

**(46.9) Theorem.** *Let  $R$  be a complete d.v.r. with residue class field  $k$  and quotient field  $F$ , where  $\dim_{\mathbb{Q}_p} F$  is finite. Then  $SK_1(RG)$  is a finite  $p$ -group, for any finite group  $G$ .*

*Proof.* Step 1. We set

$$\Lambda = RG, \quad \bar{\Lambda} = \Lambda/\text{rad } \Lambda \cong kG/\text{rad } kG.$$

By (45.31), there is a canonical injection  $\mu: K_1(\bar{\Lambda}) \rightarrow K_1(\Lambda)$ , and we have

$$K_1(\Lambda) = K_1(\bar{\Lambda}) \times V, \quad \text{where } V \text{ is a pro-}p\text{-group.}$$

Let  $\sigma: K_1(\Lambda) \rightarrow K_1(FG)$ , so  $SK_1(\Lambda) = \ker \sigma$ . We shall show below that the composite map  $\sigma \mu$  is injective. Taking this for granted for the moment, we obtain  $(\ker \sigma) \cap (\text{im } \mu) = 1$ , and so  $\ker \sigma \leq V$ . But any finite subgroup of a pro- $p$ -group is a  $p$ -group, so  $\ker \sigma$  is a finite  $p$ -group, and we are done.

Now let  $F'$  be a finite extension field of  $F$ , with d.v.r.  $R'$  and residue class field  $k'$ , such that  $F'$  and  $k'$  are splitting fields for  $G$ . We have

$$R'G/\text{rad } R'G \cong k'G/\text{rad } k'G \cong k' \otimes_k (kG/\text{rad } kG) \cong k' \otimes_k \bar{\Lambda},$$

using (5.22) and the proof of (7.10). Then there is a commutative diagram

$$\begin{array}{ccc} K_1(\bar{\Lambda}) & \xrightarrow{\sigma\mu} & K_1(FG) \\ \downarrow & & \downarrow \\ K_1(k' \otimes_k \bar{\Lambda}) & \xrightarrow{\sigma'\mu'} & K_1(F'G), \end{array}$$

in which both vertical maps are injective by Exercise 40.3. To prove  $\sigma\mu$  injective, it suffices to prove  $\sigma'\mu'$  injective. Changing notation, we may assume henceforth that both  $F$  and  $k$  are splitting fields for  $G$ .

*Step 2.* Since  $F$  is a splitting field for  $G$ , we may write

$$FG \cong \prod_{i=1}^s M_{n_i}(F), \quad \text{and} \quad \psi: K_1(FG) \cong \prod_{i=1}^s F^\times.$$

To describe  $\psi$  explicitly, let  $\{Z_1, \dots, Z_s\}$  be a basic set of simple left  $FG$ -modules. In the Morita equivalence  $M_{n_i}(F) \sim F$ , the simple modules  $Z_i$  and  $F$  correspond to each other. Thus  $\psi$  is given by

$$\sum_{i=1}^s [Z_i, a_i] \xrightarrow{\psi} (a_1, \dots, a_s) \in \prod_{i=1}^s F^\times.$$

On the other hand, we can construct the image of  $K_1(\bar{\Lambda})$  in  $K_1(\Lambda)$  explicitly, as follows. Let  $\{P_1, \dots, P_r\}$  be a full set of nonisomorphic indecomposable projective  $\Lambda$ -modules, and set  $\bar{P}_i = P_i / (\text{rad } \Lambda)P_i$ , so  $\{\bar{P}_1, \dots, \bar{P}_r\}$  are a basic set of simple left  $\bar{\Lambda}$ -modules. Let  $n = |k'|$ , where  $k$  is the residue class field of  $R$ . Via the Teichmüller map  $t: k' \rightarrow R^\times$  (see Exercise 45.11), we can find an  $n$ -th root of unity  $\omega \in R^\times$  such that  $k' = \langle \bar{\omega} \rangle$ . For each  $i$ ,  $[P_i, \omega^{a_i}] \in K_1(\Lambda)$  for  $a_i \in \mathbb{Z}$ , and its image in  $K_1(\bar{\Lambda})$  is  $[\bar{P}_i, \bar{\omega}^{a_i}]$ . Let  $W$  be the subgroup of  $K_1(\Lambda)$  consisting of all expressions

$$w = \sum_{i=1}^r [P_i, \omega^{a_i}], \quad a_i \in \mathbb{Z}.$$

The above shows that  $W \cong K_1(\bar{\Lambda})$ , and since  $K_1(\bar{\Lambda})$  is canonically embedded in  $K_1(\Lambda)$ ,  $W$  must be its image in  $K_1(\Lambda)$ .

We now show that

$$W \cap \ker \sigma = 1, \quad \text{where } \sigma: K_1(\Lambda) \rightarrow K_1(FG).$$

Consider the lifting homomorphism  $e: K_0(kG) \rightarrow K_0(FG)$  defined in §18, and let  $(e_{ij})^{r \times s}$  be its matrix representation relative to the bases  $\{\bar{P}_i\}, \{Z_j\}$ . Then in

$K_0(FG)$  we have

$$[F \otimes_R P_i] = \sum_{j=1}^s e_{ij}[Z_j], \quad 1 \leq i \leq r.$$

Now let  $w = \sum_{i=1}^r [P_i, \omega^{a_i}] \in \ker \sigma$ . Then

$$0 = \sigma(w) = \sum_{j=1}^s [Z_j, \omega^{\sum_i a_i e_{ij}}] \text{ in } K_1(FG),$$

so by the previous remarks we obtain

$$\sum_{i=1}^r a_i e_{ij} \equiv 0 \pmod{n} \quad \text{for } 1 \leq j \leq s.$$

But the map  $e$  is a split injection by (18.27), so we conclude that  $a_i \equiv 0 \pmod{n}$  for each  $i$ . Thus  $w = 1$ , so we have shown that  $W \cap \ker \sigma = 1$ . As remarked in Step 1 above, this implies that  $\ker \sigma \leq V$ , and so  $SK_1(\Lambda)$  is a finite  $p$ -group, as was to be shown. The authors thank K. Uno for pointing out this simplified version of the original proof.

**(46.10) Theorem.** *Let  $G$  be a  $p$ -group, where  $p$  is prime. Let  $R$  be a  $p$ -adic ring or a ring of algebraic integers, and let  $F$  be its quotient field. Then  $\text{Wh}^F(RG)$  is  $p$ -torsionfree<sup>†</sup>.*

*Proof.* Step 1. We may assume  $G \neq \{1\}$ , since otherwise the result is trivially true. Suppose first that  $R = \text{alg. int. } \{F\}$ , and let  $P$  be a prime ideal of  $R$  dividing  $p$ . Let  $E = F_P$ ,  $S = \text{d.v.r. in } E$ . By (46.8), if  $\text{Wh}^E(SG)$  is  $p$ -torsionfree, then so is  $\text{Wh}^F(RG)$ . For the rest of the proof, we may concentrate on the local case, in which  $R$  is a  $p$ -adic ring. Further, again by (46.8), we may extend the ground field  $F$ , if desired, so we may assume that  $R$  contains the  $|G|$ -th roots of 1.

Step 2. Here we shall prove the theorem for the special case where  $G$  is an abelian  $p$ -group, using induction on  $|G|$ . (This case could also be deduced from Higman's Theorem.) Let  $p^r$  be the exponent of  $G$ , so  $r > 0$  since  $G \neq \{1\}$ , and let  $\omega$  be a primitive  $p^r$ -th root of 1. By Step 1, we may assume that  $\omega \in R$ . Let  $v$  be the valuation on  $R$ , normalized (for convenience) so that  $v(p) = (p - 1)/p$ . By (4.38) we obtain  $v(1 - \omega) = 1/p^r$ .

Now in this case

$$K_1(RG) \cong K_1^F(RG) \cong (RG)^*, \quad K_1(R) \cong R^*,$$

and we must show that each  $p$ -torsion element  $x \in (RG)^*$  lies in  $R^* \times G$ .

Each irreducible character  $\psi \in \text{Irr}(FG)$  maps  $RG$  into  $R$ , and is a ring homomorphism. The trivial character  $\psi_1$  is just the augmentation map. If

<sup>†</sup>By Exercise 5,  $\text{Wh}^F(RG)$  is torsionfree if  $R$  is a  $p$ -adic ring and  $G$  is a  $p$ -group.

$x \in (RG)^\circ$  is a  $p$ -torsion element, then  $\psi_1(x) = r \in R^\circ$ . Replacing  $x$  by  $r^{-1}x$  and changing notation, we may now assume that  $\psi_1(x) = 1$ .

Choose an element  $g \in G$  of order  $p$ , and let  $\bar{G} = G/\langle g \rangle$ . There is an exact sequence

$$0 \rightarrow (1 - g)RG \rightarrow RG \rightarrow R\bar{G} \rightarrow 0,$$

and the ring surjection  $RG \rightarrow R\bar{G}$  induces a homomorphism  $(RG)^\circ \rightarrow (R\bar{G})^\circ$ . This map carries  $x$  onto a  $p$ -torsion element  $\bar{x} \in (R\bar{G})^\circ$ , and  $\bar{\psi}_1(\bar{x}) = \psi_1(x) = 1$ , where  $\bar{\psi}_1$  is the trivial character of  $\bar{G}$ . By the induction hypothesis, we may conclude that

$$x \equiv g_0 \pmod{(1 - g)RG}$$

for some  $g_0 \in G$ . Replacing  $x$  by  $g_0^{-1}x$  and changing notation, we may now assume that

$$(46.11) \quad x \equiv 1 \pmod{(1 - g)RG}.$$

Now let  $\theta$  be a character of  $G$  for which  $\theta(g) \neq 1$ , so  $\theta(g)$  is a  $p$ -th root of 1, and  $v(1 - \theta(g)) = 1/p$ . Extend  $\theta$  to a map  $RG \rightarrow R$ . Then

$$1 - \theta(x) = \theta(1 - x) = (1 - \theta(g)) \cdot \theta(y) \quad \text{for some } y \in RG.$$

Therefore  $v(1 - \theta(x)) \geq 1/p$ ; but  $\theta(x)$  is a  $p$ -power root of 1, since  $x$  is a  $p$ -torsion element. Therefore  $\theta(x)$  is either 1 or a  $p$ -th root of 1, and so  $\theta(x) = \theta(g^a)$  for some  $a$ . Replacing  $x$  by  $xg^{-a}$  and changing notation, we obtain a new  $x$  satisfying (46.11) for which  $\theta(x) = 1$ . Writing  $(1 - x) = (1 - g)y$ , where  $y \in RG$ , it follows that  $\theta(y) = 0$ , so

$$y \in \ker \theta, \quad \text{and} \quad \ker \theta = \bigoplus_{u \in G, u \neq 1} R(u - \theta(u)).$$

Now let  $\psi$  range over  $\text{Irr}(FG)$ ; then

$$1 - \psi(x) = (1 - \psi(g))\psi(y).$$

If  $\psi(g) = 1$ , then  $\psi(x) = 1$ . If  $\psi(g) \neq 1$ , then  $\psi(g)$  is a  $p$ -th root of 1, so  $v(1 - \psi(g)) = 1/p$ . Further,

$$v(\psi(u - \theta(u))) = v(\psi(u) - \theta(u)) > 0 \quad \text{for } u \in G,$$

so

$$v(1 - \psi(x)) > 1/p.$$

Since  $\psi(x)$  is a  $p$ -power root of 1, this gives  $\psi(x) = 1$ . We have now shown that  $\psi(x) = 1$  for all  $\psi \in \text{Irr}(FG)$ , whence  $x = 1$ . This completes the proof of the theorem when  $G$  is an abelian  $p$ -group.

*Step 3.* Now let  $G$  be an arbitrary  $p$ -group. The map  $G \rightarrow G^{ab}$  induces a homomorphism.

$$\tau: K_1^F(RG) \rightarrow K_1^F(RG^{ab})$$

which preserves torsion. Each element of  $K_1^F(RG)$  can be represented by an element of  $(RG)^*$ . Given a  $p$ -torsion element  $x \in (RG)^*$ , we must prove that  $x \in R^* \times G^{ab}$  in  $K_1^F(RG)$ . Since  $\tau(x)$  is a  $p$ -torsion element of  $K_1^F(RG^{ab})$ , by Step 2 we may write  $\tau(x) = rg$  for some  $r \in R^*$ ,  $g \in G$ . Replacing  $x$  by  $x(rg)^{-1}$  and changing notation, we may assume  $\tau(x) = 1$ . In order to prove that  $x = 1$  in  $K_1^F(RG)$ , it suffices to verify that  $\text{nr } x = 1$ , where the reduced norm  $\text{nr}$  carries  $K_1^F(RG)$  into the center of  $RG$ . The rest of the proof is devoted to showing, by induction on  $|G|$ , that

$$\tau(x) = 1 \Rightarrow \text{nr } x = 1.$$

Suppose to begin with that  $G$  contains an abelian normal subgroup  $H$  of index  $p$ , and let  $G = \langle H, g \rangle$ , where  $g^p = h_0 \in H$ . We may write

$$RG = \bigoplus_{i=0}^{p-1} (RH)g^i = \bigoplus_{i=0}^{p-1} g^i(RH),$$

a twisted group algebra of the cyclic group  $G/H$  over the commutative coefficient ring  $RH$ . The powers  $\{g^i\}$  act by conjugation on  $RH$ , and conjugation by  $g$  defines a ring automorphism  $\sigma$  of  $RH$ :

$$(46.12) \quad \sigma(\alpha) = g^{-1}\alpha g = \alpha^g, \quad \forall \alpha \in RH.$$

Note that  $\sigma^p = 1$  since  $g^p = h_0 \in H$ . There is an analogous decomposition  $FG = \bigoplus (FH)g^i$ .

Now let  $FG = \coprod A_j$  be the Wedderburn decomposition of  $FG$ . As pointed out in Step 1, we may assume that  $F$  is a splitting field for  $G$  and its subgroups. The  $p$ -torsion element  $x \in (RG)^*$  may be written as  $x = \sum x_j$ ,  $x_j \in A_j$ , and we must show that each  $\text{nr } x_j = 1$ . This is clear when  $A_j \cong F$ , that is,  $A_j$  corresponds to a linear character of  $FG$ ; for then  $\tau(x) = 1$  implies that  $x_j = 1$ . We are left with the case where  $A_j$  is a matrix algebra over  $F$ . Keep  $j$  fixed, and let  $S$  denote a simple left  $A_j$ -module. The character afforded by  $S$  is of the form  $\psi^G$ , where  $\psi$  is a linear character of  $H$  distinct from its  $G$ -conjugates. Let  $e$  be the central idempotent of  $FH$  corresponding to  $\psi$ , so

$$FH \cdot e = Fe, \quad \text{and} \quad he = \psi(h)e, \quad h \in H.$$

We obtain

$$S = FG \otimes_{FH} e = \bigoplus_{i=0}^{p-1} F(g^i \otimes e), \quad \text{and} \quad A_j \cong M_p(F).$$

In order to calculate  $\text{nr } x_j$ , we let  $x_S$  denote left multiplication by  $x$  on  $S$ . Relative to the  $F$ -basis  $\{g^i \otimes e\}$  of  $S$ ,  $x_S$  is represented by a matrix  $\mathbf{M}(x)$ , and then  $\text{nr } x_j = \det \mathbf{M}(x)$ . (This procedure works for all elements  $x \in FG$ .) Let us write

$$x = \alpha_0 + \alpha_1 g + \cdots + \alpha_{p-1} g^{p-1}, \quad \text{where } \alpha_i \in RH.$$

Then

$$\mathbf{M}(x) = \sum_{i=0}^{p-1} \mathbf{M}(\alpha_i) \mathbf{M}(g^i).$$

Next, we observe for  $\alpha \in RH$ :

$$\begin{aligned} \alpha(g^i \otimes e) &= g^i \otimes \alpha^{g^i} e = g^i \otimes \sigma^i(\alpha)e = \psi(\sigma^i(\alpha))\{g^i \otimes e\}, \quad 0 \leq i \leq p-1, \\ g(g^i \otimes e) &= \begin{cases} g^{i+1} \otimes e, & 0 \leq i \leq p-2, \\ \psi(h_0)\{1 \otimes e\}, & i = p-1. \end{cases} \end{aligned}$$

On the other hand, we may let  $x$  act from the left on  $\bigoplus(FH)g^i$ . Relative to the  $FH$ -basis  $\{g^i\}$ ,  $x$  is then represented by a matrix  $\mathbf{N}(x) \in M_p(FH)$ . The above formulas then show that

$$(46.13) \quad \psi(\det \mathbf{N}(x)) = \det \mathbf{M}(x) = \text{nr } x_j.$$

It will be vital to give another interpretation of the matrix  $\mathbf{N}(x)$ , where now  $x \in (RG)^*$ . Using the determinantal interpretation of  $K_1$ , the element  $x$  corresponds to the pair  $[RG, x_l]$ , where  $x_l$  is left multiplication by  $x$  on the right  $RG$ -module  $RG$ . But  $RG$  is also a free right  $RH$ -module on the  $p$  generators  $\{g^i\}$ , so  $x_l$  may be viewed as an automorphism of a free  $RH$ -module, and then  $[RG, x_l]$  is an element of  $K_1(RH)$ , represented by the matrix  $\mathbf{N}(x) \in M_p(RH)$ . Thus,  $\mathbf{N}$  is a homomorphism

$$\mathbf{N}: K_1(RG) \rightarrow K_1(RH),$$

and of course it carries  $K_1^F(RG)$  into  $K_1^F(RH)$ .

*Step 4.* Keeping the above notation, we study  $\mathbf{N}(x)$  in more detail, assuming for the moment that  $x$  is an arbitrary element of  $RG$ , not necessarily a unit. Let  $N^*(x) = \det \mathbf{N}(x)$ ,  $x \in RG$ . For  $\alpha \in RH$ , we have

$$N^*(\alpha) = \det \mathbf{N}(\alpha) = \prod_{i=0}^{p-1} \sigma^i(\alpha) = \text{norm of } \alpha.$$

This suggests the definitions

$$T(\alpha) = \sum_{i=0}^{p-1} \sigma^i(\alpha) = \text{trace of } \alpha, \quad \text{and} \quad T(RH) = \{T(\alpha): \alpha \in RH\}.$$

We call  $T(RH)$  the *trace subgroup* of  $RH$ ; it is an  $R$ -submodule of  $RH$ . We now prove that there is an additive homomorphism

$$RG \rightarrow RH/T(RH), \quad \text{given by } x \mapsto \det \mathbf{N}(x) \pmod{T(RH)}.$$

In order to avoid notational difficulties, we carry out the proof for the case  $p = 3$ , so now

$$x = \alpha_0 + \alpha_1 g + \alpha_2 g^2, \quad \text{and} \quad g^3 = h_0 \in H.$$

Then

$$\mathbf{N}(x) = \begin{bmatrix} \alpha_0 & h_0\alpha_2 & h_0\alpha_1 \\ \sigma(\alpha_1) & \sigma(\alpha_0) & h_0\sigma(\alpha_2) \\ \sigma^2(\alpha_2) & \sigma^2(\alpha_1) & \sigma^2(\alpha_0) \end{bmatrix}.$$

We find readily that

$$(46.14) \quad N^*(x) \equiv N^*(\alpha_0) + h_0 N^*(\alpha_1) + h_0^2 N^*(\alpha_2) \pmod{T(RH)}.$$

Likewise, for  $\alpha, \beta \in RH$ , we obtain

$$N^*(\alpha + \beta) \equiv N^*(\alpha) + N^*(\beta) \pmod{T(RH)}.$$

Together, these give

$$(46.15) \quad N^*(x + y) \equiv N^*(x) + N^*(y) \pmod{T(RH)}, \quad \text{for } x, y \in RG.$$

*Step 5.* We return to the situation in Step 3, where  $x \in (RG)^*$  is a  $p$ -torsion element such that  $\tau(x) = 1$ , and where  $G$  contains an abelian normal subgroup  $H$  of index  $p$ . Then  $\mathbf{N}(x)$  is a  $p$ -torsion element in  $K_1(RH)$ , hence is represented by  $rh_1$  for some  $r \in R^*$ ,  $h_1 \in H$ . Further,  $r = 1$  because  $\tau(x) = 1$ . Therefore we obtain

$$N^*(x) = h_1 \text{ in } (RH)^*,$$

since the isomorphism  $K_1(RH) \cong (RH)^*$  is given by the determinant map.

Put  $G' = [G, G]$ ; since  $G = \langle H, g \rangle$ , we find at once that

$$G' = \{h^{1-\sigma} : h \in H\}, \quad \text{where } h^{1-\sigma} = h\sigma^{-1}(h).$$

The elements  $\{\bar{g}^i\}$  in  $G'^{ab}$  are clearly distinct.

Let us write

$$x = \sum_{i=0}^{p-1} \sum_{h \in H} a_{ih} hg^i, \quad \text{so } \tau(x) = \sum \sum a_{ih} \overline{hg^i} \in RG^{ab}.$$

From  $\tau(x) = 1$ , we obtain, for each coset  $zG'$  in  $G$ ,

$$(46.16) \quad \sum_{h \in zG'} a_{ih} = \begin{cases} 1 & \text{if } i = 0 \text{ and } z \in G', \\ 0 & \text{otherwise.} \end{cases}$$

But also, by Step 4,

$$\begin{aligned} N^*(x) &\equiv \sum_{i,h} N^*(a_{ih}hg^i) \equiv \sum_{i,h} a_{ih}^p h_0^i N^*(h) \pmod{T(RH)}. \\ &\equiv \sum_z \left\{ \sum_i \sum_{h \in zG'} a_{ih}^p h_0^i N^*(h) \right\} \pmod{T(RH)}. \end{aligned}$$

However,  $N^*$  is trivial on commutators, so for  $h \in zG'$ , the value  $N^*(h)$  depends only on  $z$ . Furthermore,

$$\sum_{h \in zG'} a_{ih}^p \equiv \left( \sum_h a_{ih} \right)^p \pmod{pRH}.$$

Using (46.16), we thus obtain

$$N^*(x) \equiv 1 \pmod{(T(RH) + pRH)}, \quad \text{that is, } h_1 - 1 \in T(RH) + pRH.$$

However, the coefficient of 1 in  $T(\alpha)$ , for any  $\alpha \in RH$ , is a multiple of  $p$ . Therefore  $h_1$  must equal 1, which shows that  $N^*(x) = 1$ . Then by (46.13) we obtain

$$\text{nr } x_j = \psi(\det \mathbf{N}(x)) = \psi(N^*(x)) = 1,$$

which completes the proof of the theorem in case  $G$  has an abelian normal subgroup  $H$  of index  $p$ .

*Step 6.* Now let  $G$  be an arbitrary  $p$ -group,  $F$  a splitting field for  $G$ , and let  $x \in (RG)^*$  be a  $p$ -torsion element such that  $\tau(x) = 1$  in  $(RG^{ab})^*$ . We must prove that  $\text{nr } x = 1$ . Let  $A_j$  be a Wedderburn component of  $FG$ , and (as in Step 3) we need only show that  $\text{nr } x_j = 1$  whenever  $\dim_F A_j > 1$ . Let  $S$  be a simple left  $A_j$ -module. By Blichfeldt's Theorem 11.3, there exists a subgroup  $H \leq G$  of index  $p$ , and a simple left  $FH$ -module  $M$ , such that  $S = \text{ind}_H^G M$ . Just as in Step 3, we have  $G = \langle H, g \rangle$  for some  $g$  with  $g^p \in H$ , and again

$$RG = \bigoplus (RH)g^i, \quad S = \bigoplus g^i \otimes M.$$

Since  $G$  is a  $p$ -group and  $|G:H| = p$ , we have  $H \trianglelefteq G$ , and  $RG$  is a twisted group ring of the cyclic group  $G/H$  over the (possibly noncommutative) coefficient ring  $RH$ . We note further that

$$S|_H = \bigoplus_0^{p-1} (g^i \otimes M),$$

a sum of  $p$  distinct  $G$ -conjugates of  $M$ .

Just as in Step 3, there is a homomorphism  $\mathbf{N}: K_1(RG) \rightarrow K_1(RH)$ . To compute  $\text{nr } x_j$ , we use the formula

$$(46.17) \quad \text{nr } x_j = \text{nr } \mathbf{N}(x),$$

where the entries of  $\mathbf{N}(x)$  act on the  $FH$ -module  $M$ .

Now  $H' = [H, H]$  is characteristic in  $H$ , hence normal in  $G$ , and there is a commutative diagram

$$\begin{array}{ccccc} K_1^F(RG) & \xrightarrow{\theta} & K_1^F(R(G/H')) & \xrightarrow{\theta'} & K_1^F(RG^{ab}) \\ \mathbf{N} \downarrow & & \downarrow & & \downarrow \\ K_1^F(RH) & \xrightarrow{\rho} & K_1^F(RH^{ab}). & & \end{array}$$

The group  $G/H'$  has an abelian normal subgroup  $H/H'$  of index  $p$ , so we can apply the results of Steps 3–5 to it. In particular, since  $\theta'(\theta(x)) = \tau(x) = 1$ , it follows that  $\theta(x) = 1$ . But then  $\rho\mathbf{N}(x) = 1$ , so by the induction hypothesis (applied to  $H$ ) we conclude that  $\mathbf{N}(x) = 1$ . Therefore  $\text{nr } x_j = 1$  by (46.17), so  $x = 1$  in  $K_1^F(RG)$ , as desired. This completes the proof of (46.10).

Continuing with our proof of Wall's Theorem 46.4, we now use induction techniques to reduce the problem to the case of hyper-elementary groups. Let  $R$  be any commutative ring, and let  $G_0^R$  be the Frobenius functor which assigns to each finite group  $G$  the commutative ring  $G_0^R(RG)$  (see (38.10)). Let  $K_1$  be the Frobenius module over  $G_0^R$ , which assigns to each  $G$  the  $G_0^R(RG)$ -module  $K_1(RG)$ . As shown in Exercise 39.5, there is a well-defined action of  $G_0^R$  on  $K_1$ , namely,

$$[X][M, \mu] = [X \otimes_R M, 1 \otimes \mu]$$

for each  $RG$ -lattice  $X$ , each  $M \in \mathcal{P}(RG)$ , and each  $\mu \in \text{Aut}_{RG} M$ .

We investigate in more detail the behavior of  $K_1(RG)$  under induction and restriction. Let  $H \leq G$  be finite groups. The inclusion  $RH \subseteq RG$  induces a “change of rings” homomorphism

$$\text{ind}_H^G: K_1(RH) \rightarrow K_1(RG),$$

by mapping  $GL_n(RH)$  into  $GL_n(RG)$  for all  $n$ . On the other hand, the restriction map carries  $\mathcal{P}(RG)$  into  $\mathcal{P}(RH)$ , since  $RG$  is a free  $RH$ -module on  $|G:H|$  generators. Thus,

$$\text{res}_H^G: K_1(RG) \rightarrow K_1(RH)$$

is given by  $[M, \mu] \mapsto [M_H, \mu]$  for  $M \in \mathcal{P}(RG)$ ,  $\mu \in \text{Aut}_{RG} M$ .

**(46.18) Lemma.** *Let  $R$  be a P.I.D. Then the functors*

$$G \rightarrow G^{ab} \times R^\cdot \quad \text{and} \quad G \rightarrow G^{ab} \times SK_1(RG) \times K_1(R)$$

define  $G_0^R(RG)$ -submodules of the Frobenius module  $K_1(RG)$ .

*Proof.* Let  $H \leq G$ ; the induction map arises from the inclusion  $RH \subseteq RG$ , which induces a map  $H^{ab} \times R^\cdot \rightarrow G^{ab} \times R^\cdot$ . For the restriction map, consider an element  $x \in G$ ; its image in  $K_1(RG)$  can be represented as  $[RG, x_l]$ , where  $x_l$  is left multiplication by  $x$  on the right  $RG$ -module  $RG$ . Then

$$\text{res}_H^G[RG, x_l] = [RG|_{RH}, x_l].$$

If  $G = \dot{\cup} g_i H$ , then  $RG = \bigoplus g_i RH$ . Now  $x_l$  permutes the left cosets  $\{g_i H\}$ , and is therefore represented by a permutation matrix whose determinant is  $\epsilon(x) V_H^G(x)$ . Here,  $\epsilon(x)$  is the sign of the permutation, and  $V_H^G$  is the transfer map defined in (13.11) (compare (13.15i)). Thus in  $K_1(RH)$  we have

$$\text{res}_H^G(x) = \epsilon(x) V_H^G(x) \in R^\cdot \times H^{ab},$$

as desired. Clearly,  $\text{res}_H^G$  carries  $R$  and  $K_1(R)$  into themselves.

Next, we verify that for each right  $RG$ -lattice  $X = \bigoplus Rx_i$  and each  $g \in G$ , the product

$$[X][RG, g_l],$$

formed in  $K_1(RG)$ , lies in  $R^\cdot \times G^{ab}$ . This product is just

$$[X \otimes_R RG, 1 \otimes g_l].$$

But  $X \otimes_R RG$  is a free right  $RG$ -module with basis  $\{x_i \otimes 1\}$ , by Exercise 10.18, so we have

$$[X][RG, g_l] = g^{\text{rank}_R X} \text{ in } K_1(RG).$$

Finally, the map  $K_1(RG) \rightarrow K_1(FG)$  is a morphism of Frobenius modules over  $G_0^R(RG)$ , so the kernel  $SK_1(RG)$  is also a Frobenius module. This completes the proof of the lemma, which holds equally well for left modules.

**(46.19) Corollary.** *Let  $R = \text{alg. int. } \{F\}$ . Then  $\text{Wh}(RG)$  and  $\text{Wh}^F(RG)$  are Frobenius modules over the Frobenius functor  $G_0^Z(ZG)$ .*

*Proof.* We may make  $K_1(RG)$  into a Frobenius module over  $G_0^Z(ZG)$  as follows: for each  $ZG$ -lattice  $X$  and each  $[M, \mu] \in K_1(RG)$ , where  $M \in \mathcal{P}(RG)$   $\mu \in \text{Aut } M$ , define

$$[X][M, \mu] = [(R \otimes_Z X) \otimes_R M, 1 \otimes \mu],$$

where  $\otimes_R$  is the inner tensor product of a pair of  $RG$ -modules. The proof of Lemma 46.18 shows that  $K_1(R) \times G^{ab} \times SK_1(RG)$  is a Frobenius submodule of  $K_1(RG)$ , and likewise so is  $K_1(R) \times G^{ab}$ . Then by (38.10iv),  $\text{Wh}(RG)$  and  $\text{Wh}^F(RG)$  are also Frobenius modules over  $G_0^Z(ZG)$ .

In order to apply the above results, we need a modified version of Solomon's Induction Theorem 15.10, and Swan's application thereof in (39.7). Let  $p$  be a rational prime; recall from (39.1) that a  $p$ -hyper-elementary group is a semidirect product  $C \rtimes P$  of a cyclic  $p'$ -group  $C$  and a  $p$ -group  $P$ . Let us set

$$\mathbb{Z}_{(p)} = \{a/b : a, b \in \mathbb{Z}, (b, p) = 1\},$$

the *localization* of  $\mathbb{Z}$  at  $p$ , so all other rational primes are invertible in  $\mathbb{Z}_{(p)}$ . We now have

**(46.20) Theorem.** *Let  $p$  be prime, and let  $\mathcal{H}_p$  be the set of all  $p$ -hyper-elementary subgroups of a given finite group  $G$ . Then there exist rational numbers  $c_i \in \mathbb{Z}_{(p)}$  such that*

$$1_G = \sum_{H_i \in \mathcal{H}_p} c_i (1_{H_i})^G,$$

where both sides are viewed as  $\mathbb{Z}_{(p)}$ -valued class functions on  $G$ .

The result follows easily from the proof of (15.10), once we modify (15.11) so that it deals with  $\mathbb{Z}_{(p)}$ -valued functions. The details are left to the reader. Using the above theorem, we obtain

**(46.21) Corollary.** *Let  $p$  be prime, and let  $\mathcal{H}_p(G)$  be the set of all  $p$ -hyper-elementary subgroups of  $G$ . Let  $\Phi$  be the Frobenius functor which assigns to each group  $G$  the  $\mathbb{Z}_{(p)}$ -algebra*

$$\Phi(G) = \mathbb{Z}_{(p)} \otimes_Z G_0^Z(ZG).$$

Then

- (i)  $\Phi(G) = \sum_{H \in \mathcal{H}_p(G)} \text{ind}_H^G \Phi(H)$ .
- (ii) If  $M$  is any Frobenius module over  $\Phi$ , then for each  $x \in M(G)$ ,

$$\text{res}_H^G x = 0 \quad \text{for all } H \in \mathcal{H}_p(G) \Rightarrow x = 0.$$

The result follows easily from (46.20); see the proof of (38.14i).

We are now ready to apply these results to the study of torsion in Whitehead groups. As remarked earlier, Wall's Theorem 46.4 is equivalent to the assertion that  $\text{Wh}^F(RG)$  is torsionfree. The techniques of Frobenius functors allow us to reduce the problem to the case of hyper-elementary groups, as follows:

**(46.22) Proposition.** *Let  $p$  be a prime, and let  $R = \text{alg. int. } \{F\}$ . Then  $\text{Wh}(RG)$*

is  $p$ -torsionfree if and only if  $\text{Wh}(RG)$  is  $p$ -torsionfree for every  $p$ -hyper-elementary subgroup  $H$  of  $G$ . The same holds with  $\text{Wh}^F$  in place of  $\text{Wh}$ .

*Proof.* By (46.19), both  $\text{Wh}(RG)$  and  $\text{Wh}^F(RG)$  are Frobenius modules over the Frobenius functor  $G_0^Z(\mathbb{Z}G)$ . Now define

$$\Phi(G) = \mathbb{Z}_{(p)} \otimes_{\mathbb{Z}} G_0^Z(\mathbb{Z}G), \quad \Psi(G) = \mathbb{Z}_{(p)} \otimes_{\mathbb{Z}} \text{Wh}^F(RG),$$

where  $\mathbb{Z}_{(p)}$  is the localization of  $\mathbb{Z}$  at  $p$ , and where  $\text{Wh}^F(RG)$  is viewed as  $\mathbb{Z}$ -module. Then  $\Psi(G)$  has the same  $p$ -torsion as  $\text{Wh}^F(RG)$ , so it suffices to test whether  $\Psi(G)$  is  $p$ -torsionfree. As in (46.21),  $\Phi$  is a Frobenius functor, and  $\Psi$  is a Frobenius module over  $\Phi$ . Since the restriction of a  $p$ -torsion element is  $p$ -torsion, the proposition now follows from (46.21ii).

We remark that the above proof is valid for any commutative ring  $R$ .

To finish the proof of Wall's Theorem, we need one more preliminary result:

**(46.23) Lemma.** *Let  $p, q$  be distinct primes, and let  $R = \text{alg. int. } \{F\}$ . Let  $\bar{G} = G/H$ , where  $H$  is a normal  $q$ -subgroup of  $G$ . Then if  $\text{Wh}^F(R\bar{G})$  is  $p$ -torsionfree, so is  $\text{Wh}^F(RG)$ .*

*Proof.* Let  $\hat{R}$  be the  $Q$ -adic completion of  $R$  at some prime  $Q$  dividing  $q$ , so  $\hat{R}$  is a  $q$ -adic ring. By (5.26) we have

$$\hat{R}G/\text{rad } \hat{R}G \cong \hat{R}\bar{G}/\text{rad } \hat{R}\bar{G}.$$

Now  $K_1(\hat{R}G)$  and  $K_1(\hat{R}\bar{G})$  have finite Sylow  $p$ -subgroups, and by (45.31), the map

$$\rho: K_1(\hat{R}G) \rightarrow K_1(\hat{R}\bar{G})$$

induces an isomorphism of these Sylow  $p$ -subgroups. By (46.9), the same holds for the map

$$\rho': K_1^F(\hat{R}G) \rightarrow K_1^F(\hat{R}\bar{G})$$

Now consider the commutative diagram

$$\begin{array}{ccc} K_1^F(RG) & \xrightarrow{\rho_0} & K_1^F(R\bar{G}) \\ \downarrow & & \downarrow \\ K_1^F(\hat{R}G) & \xrightarrow{\rho'} & K_1^F(\hat{R}\bar{G}). \end{array}$$

Both vertical arrows are monomorphisms by Exercise 40.3, and  $\rho'$  gives an isomorphism of Sylow  $p$ -subgroups (which are finite, by the above discussion).

Therefore  $\rho_0$  maps the Sylow  $p$ -subgroup of  $K_1^F(RG)$  injectively into that of  $K_1^F(R\bar{G})$ .

On the other hand, the composite map

$$K_1^F(R) \times G^{ab} \xrightarrow{\rho_1} K_1^F(RG) \xrightarrow{\rho_0} K_1^F(R\bar{G})$$

is surjective on Sylow  $p$ -subgroups, by virtue of the equivalence of conditions (i)–(iii) below (46.6), since we are assuming that  $\text{Wh}^F(R\bar{G})$  is  $p$ -torsionfree. This implies that  $\rho_0$  is a surjection of Sylow  $p$ -subgroups, whence so is  $\rho_1$ . But then  $\text{Wh}^F(RG)$  is  $p$ -torsionfree, again by the conditions (i)–(iii). This completes the proof.

We are now ready to finish the proof of Wall's Theorem. Let  $R = \text{alg. int. } \{F\}$ , and let  $G$  be an arbitrary finite group. As remarked earlier, we must show that  $\text{Wh}^F(RG)$  is torsionfree. For this, it suffices to prove that, for each prime  $p$ ,  $\text{Wh}^F(RG)$  is  $p$ -torsionfree. By (46.22), we need only verify this when  $G$  is  $p$ -hyper-elementary, say  $G = C \rtimes P$  for some cyclic  $p'$ -group  $C$  and some  $p$ -group  $P$ . By repeated use of (46.23), we may peel off the  $q$ -primary components of  $C$  for each prime  $q$  dividing  $|C|$ , so the problem is reduced to showing that  $\text{Wh}^F(RP)$  is  $p$ -torsionfree. But this case has already been settled in Theorem 46.10, so the proof of Wall's Theorem is completed.

**Remark.** If  $R$  is a  $p$ -adic ring, the Whitehead group  $\text{Wh}^F(RG)$  may have  $p$ -torsion elements, even when  $G$  is  $p$ -hyper-elementary.

Turning next to  $SK_1$ , we prove:

**(46.24) Theorem (Wall).** *Let  $R$  be a  $p$ -adic ring, and suppose that  $G$  has an abelian Sylow  $p$ -subgroup. Then  $SK_1(RG) = 1$ .*

*Proof.* Step 1. By (46.9) we know that  $SK_1(RG)$  is a finite  $p$ -group, and so

$$SK_1(RG) \cong \mathbb{Z}_{(p)} \otimes_{\mathbb{Z}} SK_1(RG),$$

where  $\mathbb{Z}_{(p)}$  is the localization of  $\mathbb{Z}$  at  $p$ , and where  $SK_1$  is viewed as  $\mathbb{Z}$ -module. Then  $SK_1(RG)$  is a Frobenius module over the Frobenius functor  $\mathbb{Z}_{(p)} \otimes_{\mathbb{Z}} G_0^{\mathbb{Z}}(\mathbb{Z}G)$ . Just as in the proof of (46.22), it follows that if  $SK_1(RH) = 1$  for every  $p$ -hyper-elementary subgroup  $H$  of  $G$ , then necessarily  $SK_1(RG) = 1$ . (This part of the argument does not require the hypothesis on the Sylow  $p$ -subgroup of  $G$ .)

Step 2. Changing notation, we may now assume that

$$G = C \rtimes P, \quad \text{where } C = \text{cyclic group of order } n, p \nmid n,$$

and  $P$  is an abelian  $p$ -group. We proceed to study the group ring  $RG$ , and we

may write  $RG = (RC) \circ P$ , the twisted group ring (with trivial factor set) of the  $p$ -group  $P$  over the commutative coefficient ring  $RC$ . Note that  $P$  acts by conjugation on  $RC$ .

The decomposition of the ring  $RC$  is given in Exercise 21.5. We have (letting  $F$  be the quotient field of  $R$ )

$$FC = \coprod F_i, \quad RC = \coprod R_i,$$

where  $F_i$  is a Galois unramified extension of  $F$ , and  $R_i$  is the integral closure of  $R$  in  $F_i$ . The action of  $P$  on  $RC$  permutes the summands  $\{R_i\}$ , not necessarily in a transitive fashion. Let  $R_1, \dots, R_m$  be the distinct conjugates of  $R_1$  under the action of  $P$ ; then  $\Lambda = (R_1 \oplus \dots \oplus R_m) \circ P$  is a ring direct summand of  $RG$ , and  $RG$  decomposes into a direct sum of such  $\Lambda$ 's. Thus, we need only prove that  $SK_1(\Lambda) = 1$ .

*Step 3.* Put

$$S = R_1 \oplus \dots \oplus R_m = S\delta_1 \oplus \dots \oplus S\delta_m,$$

where the  $\{\delta_i\}$  are primitive orthogonal idempotents in  $S$ , and where  $P$  acts transitively on the  $\{\delta_i\}$ . These  $\{\delta_i\}$  are also orthogonal idempotents in the ring  $\Lambda = S \circ P$ , and therefore

$$\Lambda \cong M_m(\delta_1 \Lambda \delta_1)$$

by Exercise 46.2.

Next, we have

$$\delta_1 \Lambda \delta_1 = (S\delta_1) \circ P = (S\delta_1) \circ P_1 = R_1 \circ P_1,$$

where  $P_1 = \{x \in P : x\delta_1 x^{-1} = \delta_1\}$ . Of course,

$$SK_1(\Lambda) \cong SK_1(\delta_1 \Lambda \delta_1) \cong SK_1(R_1 \circ P_1),$$

and we must show that  $SK_1(R_1 \circ P_1) = 1$ .

Let

$$P_0 = \{x \in P_1 : x \text{ acts trivially on } R_1\},$$

and set  $H = P_1/P_0$ . Then  $H$  acts by conjugation on both  $R_1$  and  $P_0$ , and now we put

$$\Gamma = R_1 \circ P_1 = (R_1 P_0) \circ H.$$

Here,  $R_1 P_0$  is an ordinary group ring, and  $(R_1 P_0) \circ H$  is a twisted group ring of  $H$  with possibly nontrivial factor set  $f: H \times H \rightarrow P_0$ .

*Step 4.* The above group  $H$  may be viewed as a subgroup of  $\text{Gal}(F_1/F)$ , where  $F_1$  is the quotient field of  $R_1$ . Let  $F_0$  be the subfield of  $F_1$  fixed (elementwise)

by  $H$ , and let  $R_0$  be its d.v.r. Denote by  $\mathfrak{p}_i$  the prime ideal of  $R_i$ , and set  $\bar{R}_i = R_i/\mathfrak{p}_i$ ,  $i = 0, 1$ . Since  $F \subseteq F_0 \subseteq F_1$  and  $F_1$  is unramified over  $F$ , it follows that  $F_1$  is unramified over  $F_0$ , and that

$$H = \text{Gal}(F_1/F_0) \cong \text{Gal}(\bar{R}_1/\bar{R}_0)$$

(see the discussion in Exercise 21.5).

Since  $R_1$  is a  $p$ -adic ring and  $P_0$  is a  $p$ -group, we have

$$R_1 P_0 / \text{rad } R_1 P_0 \cong \bar{R}_1,$$

and  $R_1 P_0$  is a commutative local ring. Then

$$N = (\text{rad } R_1 P_0)^\circ H$$

is a two-sided ideal of  $\Gamma$  contained in  $\text{rad } \Gamma$ , and

$$\Gamma/N \cong \bar{R}_1^\circ H,$$

a crossed-product algebra (see (8.33i)). Since the factor set  $f$  takes values in  $P_0$ , and since  $x \equiv 1 \pmod{N}$  for every  $x \in P_0$ , the above algebra has trivial factor set. By (28.3), we obtain

$$\bar{R}_1^\circ H \cong M_t(\bar{R}_0), \quad \text{where } t = |H|.$$

This shows that in fact  $N = \text{rad } \Gamma$ .

By the Theorem on Lifting Idempotents 6.7, we may choose orthogonal idempotents  $e_1, \dots, e_t \in \Gamma$  with sum 1, whose images in  $\Gamma/N$  are a set of primitive orthogonal idempotents. Then

$$\Gamma = \bigoplus_{i=1}^t \Gamma e_i \cong M_t(e_1 \Gamma e_1)$$

by Exercise 46.2. Now  $\Gamma$  is a free left  $(R_1 P_0)$ -module of rank  $t$ , and  $\Gamma e_i \cong \Gamma e_1$  for each  $i$ , so  $\Gamma e_1$  is a free  $(R_1 P_0)$ -module of rank 1. Therefore

$$(e_1 \Gamma e_1)_\circ = \text{End}_\Gamma \Gamma e_1 \subseteq \text{End}_{R_1 P_0}(\Gamma e_1) \cong R_1 P_0.$$

This proves that  $e_1 \Gamma e_1$  is commutative, and in fact we see that

$$e_1 \Gamma e_1 = \text{subring of } R_1 P_0 \text{ on which } H \text{ acts trivially.}$$

We remark also that

$$e_1 \Gamma e_1 / \text{rad}(e_1 \Gamma e_1) \cong \bar{e}_1 (\Gamma / \text{rad } \Gamma) \bar{e}_1 \cong \bar{R}_0,$$

Combining our results, we obtain

$$\Lambda \cong M_m(\delta_1 \Lambda \delta_1) \cong M_m(R_1 \circ P_1) \cong M_{mt}(e_1 \Gamma e_1).$$

But then

$$SK_1(\Lambda) \cong SK_1(e_1 \Gamma e_1) = 1,$$

the latter step by virtue of (45.12). This completes the proof of Theorem 46.24.

**(46.25) Remarks.** (i) Let us record here the following result, proved above:

Let  $\Lambda = (R_1 \oplus \cdots \oplus R_m) \circ P$ , where  $P$  is a finite abelian  $p$ -group acting transitively on the  $p$ -adic rings  $\{R_i\}$ . Let  $P_1$  = stabilizer of  $R_1$  in  $P$ ,  $P_0$  = subgroup of  $P_1$  which acts trivially on  $R_1$ . Then, for some  $t$ ,

$$\Lambda \cong M_{mt}(\Delta),$$

where the commutative local ring  $\Delta$  is the subring of  $R_1 P_0$  fixed elementwise by  $P_1/P_0$ .

Furthermore, the above holds whenever  $P_0$  is abelian, whether or not  $P$  is abelian.

(ii) The preceding calculation has been generalized by DeMeyer-Janusz [83], as follows. Let  $R$  be an arbitrary commutative ring, and  $G$  a finite group with commutator subgroup  $G'$ . They proved that the group ring  $RG$  is an Azumaya algebra over its center (see Exercise 55.3) if and only if  $|G'|$  is a unit in  $R$ .

In particular, suppose that  $R$  is a  $p$ -adic ring, and that  $p$  does not divide  $|G'|$ . The ring direct summands of the center of  $RG$  have trivial Brauer group, since they are complete local rings with finite residue class fields. It follows that  $RG$  is a direct sum of matrix rings of the form  $M_n(\Gamma)$ , with  $\Gamma$  a commutative  $R$ -algebra, f.g./ $R$  as module. But then

$$SK_1(M_n(\Gamma)) \cong (SK_1(\Gamma)) = 1$$

by (45.12), which shows that  $SK_1(RG) = 1$  whenever  $|G'| \not\equiv 0 \pmod{p}$ . It is easily checked that this condition on  $|G'|$  is satisfied when  $G$  is a  $p$ -hyper-elementary group with abelian Sylow  $p$ -subgroup.

## §46. Exercises

1. Let  $\tau: u \rightarrow u^*$  be the involution of  $\mathbf{Z}G$  defined by  $g \rightarrow g^{-1}$ ,  $g \in G$ , extended by linearity. Prove that  $\tau$  acts trivially on the Whitehead group

$$\text{Wh}^0(\mathbf{Z}G) = K_1(\mathbf{Z}G) / (\pm G^{ab} \times SK_1(\mathbf{Z}G)).$$

[Hint (Wall): Let  $\mathbf{Q}G = \coprod A_j$  be the Wedderburn decomposition of  $\mathbf{Q}G$ ,  $F_j$  = center of  $A_j$ ,

and let  $u \in \mathbb{Q}G$  be expressed as  $u = \sum u_j, u_j \in A_j$ . Let  $\text{nr}_j$  be the reduced norm from  $A_j$  to  $F_j$ , extended to a map on  $GL(A_j)$ .

The reduced norm  $\text{nr} = \prod_j \text{nr}_j$  induces an isomorphism

$$\text{Wh}^0(\mathbb{Z}G) \cong C^+/\text{torsion subgroup of } C^+,$$

with  $C^+$  as in (45.9). It suffices to show that for fixed  $j$ , and any  $u \in GL(\mathbb{Z}G)$ ,

$$\text{nr}_j(u^*)_j = (\text{nr}_j(u_j)) \cdot \text{torsion element of } F_j.$$

For any absolutely irreducible complex representation  $\mathbf{M}$  of  $G$ , there exists an invertible matrix  $\mathbf{P}$  such that

$$\mathbf{M}(g^{-1}) = \overline{\mathbf{P} \mathbf{M}(g) \mathbf{P}^{-1}} \quad \text{for } g \in G,$$

where bar denotes complex conjugation. It follows that, up to similarity,  $\mathbf{M}(u^*)$  is the complex conjugate of  $\mathbf{M}(u)$ . Therefore

$$\text{nr}_j(u^*)_j = \overline{\text{nr}_j(u_j)}.$$

Let  $\theta_1, \dots, \theta_m$  be the inequivalent embeddings of  $F_j$  into  $\mathbb{C}$ , and define

$$\Phi(\alpha) = (\log|\theta_1(\alpha)|, \dots, \log|\theta_m(\alpha)|), \quad \text{for } \alpha \in F_j.$$

As in the proof of Dirichlet's Unit Theorem,  $\Phi$  is a homomorphism of  $F_j$  onto a free  $\mathbb{Z}$ -lattice of rank  $m - 1$ , and  $\ker \Phi$  is the torsion subgroup of  $F_j$ . This implies the desired result.]

2. Let  $1 = e_1 + \dots + e_m$  be a decomposition into orthogonal idempotents in a ring  $\Lambda$ , and suppose that for each  $i$ , there exists a unit  $u_i \in \Lambda^\times$  such that  $u_i e_i u_i^{-1} = e_i$ . Show that

$$\Lambda \cong M_m(e_1 \Lambda e_1).$$

[Hint: By Exercise 6.14, these  $\{u_i\}$  exist if and only if  $\Lambda e_i \cong \Lambda e_1$  for each  $i$ . Next, the hypothesis implies that  $\Lambda \cong (\Lambda e_1)^{(m)}$  as left  $\Lambda$ -modules. Therefore

$$\begin{aligned} \Lambda^\circ &\cong \text{End}_\Lambda(\Lambda \Lambda) \cong \text{End}_\Lambda((\Lambda e_1)^{(m)}) \cong M_m(\text{End}_\Lambda(\Lambda e_1)) \\ &\cong M_m((e_1 \Lambda e_1)^\circ) \cong \{M_m(e_1 \Lambda e_1)\}^\circ. \end{aligned}$$

3. Let  $G$  be a finite abelian group. Show that

$$K_1(\mathbb{Z}G) \cong (\mathbb{Z}G)^\times \times SK_1(\mathbb{Z}G),$$

and that there is a canonical decomposition

$$(\mathbb{Z}G)^\times \cong \{\pm 1\} \times G \times F$$

for some free abelian group  $F$ .

(References: Dennis [80], Roggenkamp-Scott [83].)

4. Let  $R = \text{alg. int. } \{F\}$ , and let  $\Lambda = RG$ , where  $G$  is a finite group. Let  $\Gamma$  be a maximal  $R$ -order in  $FG$  containing  $\Lambda$ . Prove that the sequence

$$1 \rightarrow SK_1(\Lambda) \rightarrow K_1(\Lambda) \rightarrow K_1(\Gamma)$$

is exact.

[Hint (Oliver): It suffices to show that  $SK_1(\Lambda) \rightarrow SK_1(\Gamma)$  is the zero map. By (45.15), this amounts to proving that

$$SK_1(\Lambda_P) \rightarrow SK_1(\Gamma_P)$$

is the zero map for each prime ideal  $P$  of  $R$ . But  $SK_1(\Gamma_P)$  is a  $p'$ -group where  $p$  is the rational prime in  $P$ , while  $SK_1(\Lambda_P)$  is a  $p$ -group.]

5. Prove that  $\text{Wh}^F(RG)$  is torsionfree if  $R$  is a  $p$ -adic ring and  $G$  is a  $p$ -group.

[Hint: By (45.31),  $K_1(RG) \cong (\text{pro-}p\text{-group}) \times \bar{R}^\times$ , where  $\bar{R}^\times$  is the group of roots of unity in the residue class field  $\bar{R}$  of  $R$ . This group  $\bar{R}^\times$  is isomorphic to the torsion subgroup of  $R^\times$ . Now let  $x \in K_1(RG)$  be a torsion element in  $\text{Wh}^F(RG)$ . Write  $x = x_1x_2$ , with  $x_1 \in \text{pro-}p\text{-group}$ ,  $x_2 = p'$ -element. Then  $x_2$  is a root of unity in  $R^\times$ , so  $x$  and  $x_1$  have the same image in  $\text{Wh}^F(RG)$ . Then  $x_1 = 1$  in  $\text{Wh}^F(RG)$ , since  $\text{Wh}^F(RG)$  is  $p$ -torsionfree.]

## §47. MILNOR'S $K_2$ -GROUP

In the proof of Keating's Theorem 45.15 on  $SK_1$  of a maximal order, we have already seen that important information about  $SK_1$  of orders can be obtained by using Quillen's Localization Sequence. This sequence involves  $K_2(A)$ , where  $A$  is an algebra, and indeed the full sequence involves all of the higher  $K$ -groups of Quillen.

The aim of this section is to give a brief introduction to  $K_2$ -groups, following the treatment in Milnor [71]. Other possible definitions of  $K_2$  were introduced by various authors in the past two decades, but it is beyond the scope of this book to examine their interrelationships. As pointed out by Milnor in [71, page viii], his version of  $K_2$  is based on the fundamental ideas of Steinberg [62], [67]. Since it is convenient to have a name for these  $K_2$ -groups, and since the terminology "Steinberg group" has another meaning (described below), we shall therefore refer to the  $K_2$ -group defined in this section as *Milnor's  $K_2$ -group*. This usage agrees with the terminology in *Algebraic K-theory II* (Bass [73b]), where Section C is titled "The Functor  $K_2$  of Milnor."

The authors wish to thank W. van der Kallen and M. Stein for many helpful comments during the preparation of this section.

### §47A. Steinberg Groups and $K_2$

Let  $A$  be an arbitrary ring, and let  $K_1(A) = GL(A)/E(A)$  as in §40C. Here,

$$GL(A) = \varinjlim GL_n(A), \quad E(A) = \varinjlim E_n(A),$$

with  $E_n(A)$  the subgroup of  $GL_n(A)$  generated by all elementary matrices  $\{\mathbf{E}_{ij}(a)\}$ . As we have seen, these matrices satisfy the Steinberg relations given in (40.23).

We now introduce the *Steinberg group*  $St_n(A)$  for  $n \geq 3$ , as the abstract group generated by elements satisfying these relations. Explicitly, for  $n \geq 3$ ,  $St_n(A)$  has generators

$$\{x_{ij}(a) : 1 \leq i, j \leq n, i \neq j, a \in A\},$$

and relations

$$(47.1) \quad \begin{cases} x_{ij}(a)x_{ij}(b) = x_{ij}(a+b), \\ [x_{ij}(a), x_{kl}(b)] = 1 \quad \text{unless } j=k \text{ or } i=l, \\ [x_{ij}(a), x_{jk}(b)] = x_{ik}(ab), \end{cases}$$

for all  $a, b \in A$ , and all choices of the indices between 1 and  $n$ . We agree once and for all that in expressions such as  $x_{ij}(a)$ ,  $\mathbf{E}_{ij}(a)$ , etc., the subscripts are such that  $i \neq j$ .

The Steinberg group  $St_{n+1}(A)$  has more generators and more relations than  $St_n(A)$ , and there is a homomorphism  $St_n(A) \rightarrow St_{n+1}(A)$ , defined by  $x_{ij}(a) \mapsto x_{ij}(a)$ , which need not be injective. Now define

$$\text{Steinberg group of } A = St(A) = \varinjlim St_n(A),$$

so  $St(A)$  has generators

$$\{x_{ij}(a) : i \geq 1, j \geq 1, a \in A\},$$

and relations (47.1).

There is a surjection

$$\varphi: St(A) \rightarrow E(A), \quad \text{where } \varphi(x_{ij}(a)) = \mathbf{E}_{ij}(a),$$

called the *evaluation map*. We put

$$\text{Milnor group of } A = K_2(A) = \ker \varphi,$$

so there is an exact sequence of groups

$$(47.2) \quad 1 \rightarrow K_2(A) \rightarrow St(A) \xrightarrow{\varphi} GL(A) \rightarrow K_1(A) \rightarrow 1.$$

Clearly  $K_2$  is a functor from rings to groups, and each ring homomorphism  $f: A \rightarrow A'$  induces a group homomorphism  $f_*: K_2(A) \rightarrow K_2(A')$ . The first important fact about  $K_2$  is:

**(47.3) Proposition.** *The Milnor group  $K_2(A)$  is the center of  $St(A)$ , and is therefore abelian.*

*Proof.* Step 1. We show that  $E(A)$  has trivial center. First, let  $n \geq 2$  and let  $\mathbf{z} = (z_{ij}) \in \text{center of } E_n(A)$ . Then

$$\mathbf{z} \cdot \mathbf{E}_{ij}(a) = \mathbf{E}_{ij}(a) \cdot \mathbf{z} \quad \text{for all } i, j, \quad 1 \leq i, j \leq n, \quad a \in A$$

(remember the convention that  $i \neq j$ ). Comparing the  $(i, j)$ -entries of both sides, and then the  $(i, i)$ -entries, we find readily that  $\mathbf{z} = t\mathbf{I}_n$  for some  $t \in \text{center of } A$ .

Now consider any element  $\xi \in \text{center of } E(A)$ ; we may represent  $\xi$  by a matrix  $\mathbf{z} \in E_{n-1}(A)$  for some  $n$ , and then  $\begin{pmatrix} \mathbf{z} & \mathbf{0} \\ \mathbf{0} & 1 \end{pmatrix} \in \text{center of } E_n(A)$ . Therefore  $\begin{pmatrix} \mathbf{z} & \mathbf{0} \\ \mathbf{0} & 1 \end{pmatrix} = t\mathbf{I}_n$  for some  $t$ , which shows that  $t = 1$  and  $\mathbf{z} = \mathbf{I}_{n-1}$ , that is,  $\xi = 1$ . We have thus proved that the center of  $E(A)$  is  $\{1\}$ .

Step 2. Now let  $x \in \text{center of } \text{St}(A)$ ; since  $\varphi$  maps  $\text{St}(A)$  onto  $E(A)$ , it follows that  $\varphi(x) \in \text{center of } E(A)$ , and so  $x \in K_2(A)$ . Conversely, let  $y \in K_2(A)$ , so  $\varphi(y) = 1$ . We must show that  $y$  commutes with each generator  $x_{ij}(a)$  of  $\text{St}(A)$ . Since  $y \in \text{St}(A)$ , we may express  $y$  as a finite product

$$y = \prod_m x_{i_m j_m}(a_m), \quad \text{where } a_m \in A.$$

Choosing  $n > \text{Max}_m\{i_m, j_m\}$ , surely  $\varphi(y) \in E_n(A)$ .

We now define

$$(47.4) \quad P_n = \text{subgroup of } \text{St}(A) \text{ generated by } \{x_{in}(a) : 1 \leq i < n, a \in A\},$$

and note that  $P_n$  is abelian by virtue of (47.1). Each  $p \in P_n$  is uniquely expressible as a product  $p = \prod_{i=1}^{n-1} x_{in}(a_i)$ , and then

$$\varphi(p) = \begin{bmatrix} 1 & 0 & \cdots & 0 & a_1 \\ 0 & 1 & \cdots & 0 & a_2 \\ \vdots & \ddots & \cdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 & 1 \end{bmatrix}.$$

Thus the evaluation map  $\varphi$  is a monomorphism on  $P_n$ . The same holds for  $Q_n$ , where

$$Q_n = \text{subgroup of } \text{St}(A) \text{ generated by } \{x_{ni}(a) : 1 \leq i < n, a \in A\}.$$

Note that  $Q_n$  is abelian by (47.1).

From the relations (47.1), we have

$$x_{ij}(a) \cdot P_n \cdot x_{ij}(a)^{-1} \subseteq P_n \quad \text{for } 1 \leq i, j \leq n-1, \quad a \in A.$$

Now return to the given  $y \in K_2(A)$ ; then  $yP_ny^{-1} \subseteq P_n$ , and we claim that  $y$

centralizes  $P_n$ . Indeed, since  $\varphi(y) = 1$ , we have

$$\varphi(ypy^{-1}) = \varphi(p) \quad \text{for all } p \in P_n,$$

and therefore  $ypy^{-1} = p$ , since  $\varphi$  is injective on  $P_n$ . Thus  $y$  centralizes  $P_n$  (and also  $Q_n$ , by similar reasoning). But

$$\mathrm{St}_n(A) = \langle P_n, Q_n \rangle, \quad n \geq 3,$$

since

$$x_{ij}(a) = [x_{in}(a), x_{nj}(1)] \quad \text{for } 1 \leq i, j < n, \quad i \neq j, \quad a \in A.$$

Thus  $y$  centralizes  $\mathrm{St}_n(A)$ , which completes the proof that  $K_2(A)$  is the center of  $\mathrm{St}(A)$ .

**Remark.** Let  $U$  be the *upper triangular subgroup* of  $\mathrm{St}(A)$ , generated by all

$$\{x_{ij}(a) : 1 \leq i < j, a \in A\}.$$

The preceding proof shows that each  $u \in U$  is uniquely expressible as a finite product

$$u = x_{12}(a)x_{13}(a') \cdots x_{1k}(a'')x_{23}(b)x_{24}(b') \cdots.$$

This implies at once that  $\varphi$  is a monomorphism from  $U$  into  $E(A)$ .

**(47.5) Definition.** An exact sequence of groups

$$1 \rightarrow C \rightarrow E \xrightarrow{\varphi} G \rightarrow 1$$

is a *central extension* if  $C \leq$  center of  $E$ . It is a *universal central extension* if for each central extension  $1 \rightarrow C_1 \rightarrow E_1 \rightarrow G \rightarrow 1$ , there exists a unique homomorphism  $E \rightarrow E_1$  making the diagram

$$\begin{array}{ccccccc} 1 & \longrightarrow & C & \longrightarrow & E & \xrightarrow{\varphi} & G \longrightarrow 1 \\ & & \downarrow & & \downarrow & & \downarrow \\ 1 & \longrightarrow & C_1 & \longrightarrow & E_1 & \longrightarrow & G \longrightarrow 1 \end{array}$$

commute. (Compare this concept with that of  $B$ -universal extensions defined in (11.35).) It is easily seen that if  $G$  has a universal central extension, it must be unique up to isomorphism.

The following criterion for the existence of a universal central extension is

due originally to Schur, generalized later by H. Hopf; for a proof, see Milnor [71, pages 43–46] or Kervaire [70].

**(47.6) Theorem.** *A group  $G$  has a universal central extension if and only if  $G$  is perfect, that is,  $G = [G, G]$ .*

The proof of this theorem gives a method of constructing a universal central extension of the group  $G$ , which we describe briefly. We consider any presentation of  $G$ :

$$1 \rightarrow R \rightarrow F \xrightarrow{\varphi} G \rightarrow 1,$$

where  $F$  is a free group, and  $R$  the normal subgroup of relations. Let  $F' = [F, F]$ . Then the exact sequence

$$(47.7) \quad 1 \rightarrow \frac{R \cap F'}{[R, F]} \rightarrow \frac{F'}{[R, F]} \xrightarrow{\varphi'} G \rightarrow 1,$$

where  $\varphi'$  is induced by  $\varphi$ , gives a universal central extension of  $G$ . Furthermore, we have

$$(R \cap F')/[R, F] \cong H_2(G, \mathbb{Z}),$$

the second homology group of  $G$  with coefficients in  $\mathbb{Z}$ . For a more detailed discussion of this topic, see Rotman [79, Theorems 10.12 and 11.7], or Gruenberg [70], Kervaire [70], or Hilton-Stammbach [71].

Now let  $A$  be any ring; by (40.23), the elementary group  $E(A)$  is perfect, and therefore has a universal central extension. The next major result, due to Kervaire [70] and Steinberg, gives the connection between  $K_2(A)$  and this extension:

**(47.8) Theorem.** *The exact sequence*

$$1 \rightarrow K_2(A) \rightarrow \text{St}(A) \xrightarrow{\varphi} E(A) \rightarrow 1$$

*is a universal central extension of  $E(A)$ . Consequently,*

$$(47.9) \quad K_2(A) \cong H_2(E(A), \mathbb{Z}).$$

**(47.10) Remarks.** (i) For a proof, we refer the reader to Milnor [71] or Kervaire [70].

(ii) Let  $F$  be a field, and put

$$SL(F) = \bigcup_{n=1}^{\infty} SL_n(F) = \{\mathbf{X} \in GL(F) : \det \mathbf{X} = 1\},$$

the *special linear group* over  $F$ . It follows readily from §40C, or from the discussion of Dieudonné determinants in §7D, that  $SL(F)$  coincides with the elementary group  $E(F)$ . Formula (47.9) thus yields information about the homology group  $H_2(SL(F), \mathbf{Z})$  in terms of  $K_2(F)$ . The latter can be calculated explicitly by other methods; see the discussion in §47C.

(iii) Let  $n \geq 3$ , and let  $A$  be any ring. We may define a group  $K_2(n, A)$  as the kernel of the surjection  $\varphi: St_n(A) \rightarrow E_n(A)$ , so there is an exact sequence

$$1 \rightarrow K_2(n, A) \rightarrow St_n(A) \xrightarrow{\varphi} E_n(A) \rightarrow 1.$$

It turns out that when  $A$  is a skewfield and  $n \geq 5$ , this sequence gives a universal central extension of  $E_n(A)$ . On the other hand, for an arbitrary *commutative* ring  $A$ , for  $n \geq 5$  the sequence again gives a universal central extension. This second result was proved by van der Kallen [77], using the previously known fact of “universality” (see Milnor [71, page 48]).

(iv) As an application of Theorem 47.8, we shall show below that for any commutative ring  $R$ , the abelian group  $K_2(R)$  may be made into a  $K_0(R)$ -module.

(v) The calculation of  $K_2(A)$  is by no means trivial, even in the simplest cases. For example,

$$K_2(\mathbf{Z}) \text{ is a cyclic group of order 2,}$$

but the proof requires either a presentation of  $GL_n(\mathbf{Z})$  by generators and relations, or else a topological argument. For details, see Milnor [71, §10].

To explain Remark (iv), we consider a commutative ring  $R$ . Since we may identify the additive group  $K_0(R)$  with the Grothendieck ring  $G_0^R(R)$ , it follows that  $K_0(R)$  is a commutative ring with identity element  $[R]$ , and with multiplication defined by  $\otimes_R$ . We have already seen how to make  $K_1(R)$  into a  $K_0(R)$ -module. Specifically, for each  $X \in \mathcal{P}(R)$  and each pair  $[M, \mu]$  with  $M \in \mathcal{P}(R)$  and  $\mu \in \text{Aut}_R M$ , we define

$$[X][M, \mu] = [X \otimes_R M, 1 \otimes \mu] \in K_1(R).$$

Next, we may use formula (47.9) to define an action of  $K_0(R)$  on  $K_2(R)$ , so as to make the abelian group  $K_2(R)$  into a  $K_0(R)$ -module. Given any  $X \in \mathcal{P}(R)$ , choose  $Y \in \mathcal{P}(R)$  so that  $X \oplus Y \cong R^{(k)}$  for some  $k$ . Now define a map

$$h_X: GL_n(R) \rightarrow GL_{kn}(R)$$

as follows: given  $\mu \in GL_n(R)$ , view it as element of  $\text{Aut } R^{(n)}$ , and define  $h_X(\mu)$  by the formula

$$h_X(\mu)\{(x + y) \otimes w\} = x \otimes \mu(w) + y \otimes w, \quad \text{for } x \in X, \quad y \in Y, \quad w \in R^{(n)}.$$

Then  $h_X(\mu) \in \text{Aut } R^{(kn)} \cong GL_{kn}(R)$ . The map  $h_X$  on  $GL(R)$  is unique up to inner automorphisms, and satisfies

$$h_{X \oplus X'} = h_X \cdot h_{X'} \quad \text{for } X, X' \in \mathcal{P}(R).$$

It follows readily that  $h_X$  depends only on the stable class of  $X \in \mathcal{P}(R)$ , and that  $h_X$  induces a homomorphism  $E_n(R) \rightarrow E(R)$  for  $n \geq 3$ . There is then a well-defined map

$$(h_X)_*: H_2(E_n(R), \mathbb{Z}) \rightarrow H_2(E(R), \mathbb{Z}),$$

additive in  $X$ . Since

$$H_2(E(R), \mathbb{Z}) = \varinjlim H_2(E_n(R), \mathbb{Z}),$$

we obtain a map  $\theta(X): H_2(E(R), \mathbb{Z}) \rightarrow H_2(E(R), \mathbb{Z})$ , which makes  $K_2(R)$  into a  $K_0(R)$ -module.

### §47B. Relative K-Theory

We return next to the relative K-theory developed in §44, so let  $J$  be a two-sided ideal of the ring  $A$ , and let  $\bar{A} = A/J$ . As shown in (44.8), there is an exact sequence

$$(47.11) \quad K_1(A, J) \rightarrow K_1(A) \rightarrow K_1(\bar{A}) \rightarrow K_0(A, J) \rightarrow K_0(A) \rightarrow K_0(\bar{A}),$$

involving two relative groups  $K_1(A, J)$  and  $K_0(A, J)$ . Our aim here is to extend the sequence to the left by  $K_2$  terms, and then to use this longer sequence to also extend Milnor's Mayer-Vietoris sequence (42.14) to the left.

Let  $D$  be the double of  $A$  along  $J$ , so as in (44.9) there is a fiber product

$$(47.12) \quad \begin{array}{ccc} D & \xrightarrow{f} & A \\ g \downarrow & & \downarrow f' \\ A & \xrightarrow{g'} & A, \end{array}$$

where the maps are ring surjections. As in (44.11), we set

$$K_i(A, J) = \{y \in K_i(D) : f(y) = 0\}, \quad i = 0, 1.$$

Then, as shown in the proof of (44.14), there is a commutative diagram with

exact rows and columns:

$$\begin{array}{ccccccc}
 1 & \longrightarrow & E(A, J) & \longrightarrow & GL(A, J) & \longrightarrow & K_1(A, J) & \longrightarrow 1 \\
 & & g \downarrow & & g \downarrow & & g \downarrow & \\
 1 & \longrightarrow & E(D) & \longrightarrow & GL(D) & \longrightarrow & K_1(D) & \longrightarrow 1 \\
 & & f \downarrow & & f \downarrow & & f \downarrow & \\
 1 & \longrightarrow & E(A) & \longrightarrow & GL(A) & \longrightarrow & K_1(A) & \longrightarrow 1,
 \end{array}$$

with the  $g$ 's injective and the  $f$ 's surjective.

Now define the *relative Steinberg group*  $\text{St}(A, J)$  as the kernel of the map  $\text{St}(D) \rightarrow \text{St}(A)$  induced by  $f: D \rightarrow A$ , so there is an exact sequence

$$1 \rightarrow \text{St}(A, J) \rightarrow \text{St}(D) \xrightarrow{f} \text{St}(A) \rightarrow 1.$$

**(47.13) Lemma.** *There is an exact sequence*

$$\text{St}(A, J) \xrightarrow{g} \text{St}(A) \xrightarrow{f'} \text{St}(\bar{A}) \rightarrow 1.$$

*Proof.* The map  $g: D \rightarrow A$  induces a map  $\text{St}(D) \rightarrow \text{St}(A)$ , and carries  $\text{St}(A, J)$  into  $\text{St}(A)$ . Further,  $f'$  maps the generators of  $\text{St}(A)$  onto those of  $\text{St}(\bar{A})$ , and  $f'g = 1$ . Thus, it remains to prove that  $\ker f' \leq \text{im } g$  in the above sequence.

To begin with, each generator of  $\text{St}(D)$  is of the form  $x_{ij}(a, b)$  with  $(a, b) \in D$ , that is,  $a \equiv b \pmod{J}$ . We may write

$$x_{ij}(a, b) = x_{ij}(a, a)x_{ij}(0, b - a) = (\Delta_* x_{ij}(a))x_{ij}(0, c),$$

where  $\Delta: A \rightarrow D$  is the diagonal map, and where  $c = b - a \in J$ . Now let  $w \in \text{St}(A, J)$ , so  $f(w) = 1$  in  $\text{St}(A)$ . We may write

$$w = \prod_m (\Delta_* x_{i_m j_m}(a_m))x_{i_m j_m}(0, c_m),$$

with each  $c_m \in J$ . Then

$$1 = f(w) = \prod_m x_{i_m j_m}(a_m) = \prod_m s_m,$$

with  $s_m = x_{i_m j_m}(a_m) \in \text{St}(A)$ . Therefore  $\prod_m \Delta_* s_m = 1$ , and  $w$  is expressible as a product of terms of the form

$$(47.14) \quad (\Delta_* s)x_{ij}(0, c) \cdot \Delta_*(s^{-1}), \quad \text{with } s \in \text{St}(A), \quad c \in J.$$

Therefore  $g(\text{St}(A, J))$  is generated by all expressions

$$\{sx_{ij}(c)s^{-1} : s \in \text{St}(A), c \in J\},$$

so  $\text{im}(g)$  is the normal closure in  $\text{St}(A)$  of the subgroup generated by  $\{x_{ij}(c) : c \in J\}$ . It follows that  $\text{cok}(g)$  is obtained from  $\text{St}(A)$  by imposing on the generators  $\{x_{ij}(a) : a \in A\}$  of  $\text{St}(A)$  the additional relations  $x_{ij}(c) = 1$  for  $c \in J$ . Therefore  $\text{cok}(g)$  is identical with the Steinberg group  $\text{St}(\bar{A})$ , which completes the proof.

**(47.15) Corollary.** *The composite map*

$$\text{St}(A, J) \xrightarrow{g} \text{St}(A) \xrightarrow{\varphi} E(A)$$

gives a surjection

$$\text{St}(A, J) \rightarrow E(A, J).$$

*Proof.* We have seen that  $g(\text{St}(A, J))$  is generated by all expressions

$$\{sx_{ij}(c)s^{-1} : s \in \text{St}(A), c \in J\}.$$

Since  $\varphi(\text{St}(A)) = E(A)$ , it follows that  $\text{im } \varphi g$  is the normal subgroup of  $E(A)$  generated by all  $\{E_{ij}(c) : c \in J\}$ . This is precisely  $E(A, J)$ , by (44.5).

**(47.16) Definition.** *The relative  $K_2$ -group  $K_2(A, J)$  is the kernel of the surjection  $\text{St}(A, J) \rightarrow E(A, J)$  given above.*

We thus obtain a commutative diagram with exact rows and columns:

$$\begin{array}{ccccccc} 1 & \longrightarrow & K_2(A, J) & \longrightarrow & \text{St}(A, J) & \longrightarrow & E(A, J) \longrightarrow 1 \\ & & \downarrow & & \downarrow & & \downarrow \\ 1 & \longrightarrow & K_2(D) & \longrightarrow & \text{St}(D) & \longrightarrow & E(D) \longrightarrow 1 \\ & & \downarrow & & \downarrow & & \downarrow \\ 1 & \longrightarrow & K_2(A) & \dashrightarrow & \text{St}(A) & \longrightarrow & E(A) \longrightarrow 1 \end{array}$$

with upper vertical arrows injective, lower ones surjective. Combining this diagram with the preceding one, we obtain a new diagram with the same properties:

$$\begin{array}{ccccccc} 1 & \longrightarrow & K_2(A, J) & \longrightarrow & \text{St}(A, J) & \longrightarrow & GL(A, J) \longrightarrow K_1(A, J) \longrightarrow 1 \\ & & \downarrow & & \downarrow & & \downarrow \\ 1 & \longrightarrow & K_2(D) & \longrightarrow & \text{St}(D) & \longrightarrow & GL(D) \longrightarrow K_1(D) \longrightarrow 1 \\ & & \downarrow & & \downarrow & & \downarrow \\ 1 & \longrightarrow & K_2(A) & \longrightarrow & \text{St}(A) & \longrightarrow & GL(A) \longrightarrow K_1(A) \longrightarrow 1. \end{array}$$

Applying the Snake Lemma to the diagram

$$\begin{array}{ccccccc} \text{St}(A, J) & \longrightarrow & \text{St}(A) & \longrightarrow & \text{St}(\bar{A}) & \longrightarrow & 1 \\ \downarrow & & \downarrow & & \downarrow & & \\ 1 & \longrightarrow & GL(A, J) & \longrightarrow & GL(A) & \longrightarrow & GL(\bar{A}), \end{array}$$

we obtain an exact sequence

$$(47.17) \quad K_2(A, J) \rightarrow K_2(A) \rightarrow K_2(\bar{A}) \rightarrow K_1(A, J) \rightarrow K_1(A) \rightarrow K_1(\bar{A}).$$

This sequence extends to the left the sequence given in (47.11). Once we prove the Excision Lemma 47.20 for the relative group  $K_1(A, J)$ , it will be a simple task to obtain Milnor's extended Mayer-Vietoris sequence (Theorem 47.22).

Before going further, however, we should point out that the relative groups  $\text{St}(A, J)$  and  $K_2(A, J)$ , as defined above, are not the “correct” ones, from a more advanced point of view. They are “too large” to allow the sequence (47.17) to be extended further to the left, as shown by Swan [71]. The correct relative groups were given independently by Keune [78] and Loday [78], and we now summarize some of their results.

Given any ring homomorphism  $\theta: A \rightarrow \bar{A}$ , it follows from Quillen's work that there is a long exact sequence of higher  $K$ -groups:

$$(47.18)$$

$$\cdots \rightarrow K_3(A) \rightarrow K_3(\bar{A}) \rightarrow K_2(\theta) \rightarrow K_2(A) \rightarrow K_2(\bar{A}) + K_1(\theta) \rightarrow K_1(A) \rightarrow \cdots,$$

where the  $K_i(\theta)$  are *relative  $K$ -groups*. In particular, suppose that

$$(47.19) \quad \theta: A \rightarrow A/J = \bar{A}$$

is the natural surjection, where  $J$  is a two-sided ideal of the ring  $A$ . We have already defined relative groups  $K_i(A, J)$  for  $i = 0, 1, 2$  (see (40.19), (44.6), and (47.16)). It turns out that  $K_i(A, J)$  coincides with  $K_i(\theta)$  for  $i = 0, 1$ , but *not* when  $i = 2$ .

We shall now define the “correct” relative group  $K_2(\theta)$ , following the approach of Keune and Loday. We begin by introducing a new *relative Steinberg group*  $\text{St}(\theta)$ , where  $\theta$  is as in (47.19). Let  $D$  be the double of  $A$  along  $J$ , as in (47.12). Changing notation for the moment, let  $f_*: \text{St}(D) \rightarrow \text{St}(A)$  be the surjection of Steinberg groups induced by the ring surjection  $f: D \rightarrow A$ ; likewise, let  $g$  induce  $g_*: \text{St}(D) \rightarrow \text{St}(\bar{A})$ . We had previously defined  $\text{St}(A, J)$  to be  $\ker f_*$ , and we now set<sup>†</sup>

$$\text{St}(\theta) = (\ker f_*) / [\ker f_*, \ker g_*],$$

<sup>†</sup>If  $H_1$  and  $H_2$  are subgroups of a group  $G$ , then  $[H_1, H_2]$  denotes the subgroup of  $G$  generated by all commutators  $[h_1, h_2]$  with  $h_i \in H_i$ .

a factor group of  $\text{St}(A, J)$ . The commutator group  $[\ker f_*, \ker g_*]$  lies in the kernel of the map  $\text{St}(A, J) \rightarrow E(A, J)$ , that is, in  $K_2(A, J)$ . We now define

$$K_2(\theta) = K_2(A, J)/[\ker f_*, \ker g_*].$$

With this choice for  $K_2(\theta)$ , Keune and Loday proved that the sequence (47.18) is exact, starting on the left with the term  $K_3(A)$ . For further discussion, we refer the reader to their articles.

We are now ready to return to our original task of extending the sequence (47.11) to the left, using the relative  $K_2(A, J)$  as defined in (47.16). We begin by proving the following “excision lemma” for relative  $K_1$ -groups, analogous to the  $K_0$ -excision theorem in (44.3):

**(47.20) Excision Lemma.** *Let  $\psi: A \rightarrow A'$  be a surjection of rings, and let  $J$  be a two-sided ideal of  $A$  such that  $J \cap \ker \psi = 0$ . Set  $J' = \psi(J)$ , a two-sided ideal of  $A'$ . Then  $\psi$  induces a surjection*

$$K_2(A, J) \rightarrow K_2(A', J')$$

and an isomorphism

$$K_1(A, J) \cong K_1(A', J').$$

*Proof.* Clearly  $J'$  is a two-sided ideal of  $A'$ , since  $\psi(A) = A'$ . We show now that  $\psi$  induces an isomorphism

$$\psi: GL(A, J) \cong GL(A', J').$$

Indeed, if  $\mathbf{X} \in GL_n(A, J)$  is such that  $\psi(\mathbf{X}) = \mathbf{I}_n$ , then  $\psi(\mathbf{X} - \mathbf{I}) = 0$ , and therefore  $\mathbf{X} - \mathbf{I} = 0$  since  $\psi$  is injective on  $J$ . To show  $\psi$  surjective, let  $\mathbf{U} \in GL_n(A', J')$  and set  $\mathbf{V} = \mathbf{U}^{-1}$ . Since  $\psi(J) = J'$ , we can find matrices  $\mathbf{X}$  and  $\mathbf{Y}$  with entries in  $J$ , such that

$$\psi(\mathbf{X}) = \mathbf{U} - \mathbf{I}, \quad \psi(\mathbf{Y}) = \mathbf{V} - \mathbf{I}.$$

Then  $(\mathbf{X} + \mathbf{I})(\mathbf{Y} + \mathbf{I}) - \mathbf{I}$  has entries in  $J$ , and is annihilated by  $\psi$ , hence must be 0. It follows that  $\mathbf{X} + \mathbf{I} \in GL_n(A, J)$  and  $\psi(\mathbf{X} + \mathbf{I}) = \mathbf{U}$ . Thus  $\psi$  is surjective, and we have established the desired isomorphism.

Next, the proof of (47.13) shows that  $\text{St}(A', J')$  is generated by expressions like those in (47.14), so  $\psi$  induces a surjection  $\alpha: \text{St}(A, J) \rightarrow \text{St}(A', J')$ . The lemma now follows by diagram-chasing, starting with the commutative diagram with exact rows:

$$\begin{array}{ccccccc} 1 & \longrightarrow & K_2(A, J) & \longrightarrow & \text{St}(A, J) & \longrightarrow & GL(A, J) \longrightarrow K_1(A, J) \longrightarrow 1 \\ & & \downarrow & & \alpha \downarrow & & \psi \downarrow \\ 1 & \longrightarrow & K_2(A', J') & \longrightarrow & \text{St}(A', J') & \longrightarrow & GL(A', J') \longrightarrow K_1(A', J') \longrightarrow 1, \end{array}$$

where  $\alpha$  is surjective and  $\psi$  is an isomorphism.

**(47.21) Corollary.** Keeping the hypotheses of (47.20), set  $\bar{A} = A/J$ ,  $\bar{A}' = A'/J'$ . Then there is an exact sequence of groups

$$K_2(A) \rightarrow K_2(A') \times K_2(\bar{A}) \rightarrow K_2(\bar{A}') \rightarrow K_1(A) \rightarrow K_1(A') \times K_1(\bar{A}) \rightarrow K_1(\bar{A}').$$

*Proof.* Comparing the relative sequences for the pairs  $(A, J)$  and  $(A', J')$ , we obtain a commutative diagram with exact rows:

$$\begin{array}{ccccccccc} K_2(A, J) & \xrightarrow{\alpha_1} & K_2(A) & \xrightarrow{\alpha_2} & K_2(\bar{A}) & \xrightarrow{\alpha_3} & K_1(A, J) & \xrightarrow{\alpha_4} & K_1(A) & \xrightarrow{\alpha_5} & K_1(\bar{A}) \\ \gamma_1 \downarrow & & \gamma_2 \downarrow & & \gamma_3 \downarrow & & \gamma_4 \downarrow & & \gamma_5 \downarrow & & \gamma_6 \downarrow \\ K_2(A', J') & \longrightarrow & K_2(A') & \longrightarrow & K_2(\bar{A}') & \longrightarrow & K_1(A', J') & \longrightarrow & K_1(A') & \longrightarrow & K_1(\bar{A}'). \\ \beta_1 & & \beta_2 & & \beta_3 & & \beta_4 & & \beta_5 & & \beta_6 \end{array}$$

Note that  $\gamma_1$  is surjective and  $\gamma_4$  is an isomorphism, by (47.20).

Now consider the sequence

$$\begin{aligned} K_2(A) &\xrightarrow{(\gamma_2, \alpha_2)} K_2(A') \times K_2(\bar{A}) \xrightarrow{(\beta_2, 1/\gamma_3)} K_2(\bar{A}') \xrightarrow{\alpha_4 \gamma_4^{-1} \beta_3} \\ K_1(A) &\xrightarrow{(\gamma_5, \alpha_5)} K_1(A') \times K_1(\bar{A}) \xrightarrow{(\beta_5, 1/\gamma_6)} K_1(\bar{A}), \end{aligned}$$

where, by definition,

$$(\gamma_2, \alpha_2): x \mapsto (\gamma_2 x, \alpha_2 x), \quad (\beta_2, 1/\gamma_3): (y, z) \mapsto \beta_2 y / \gamma_3 z,$$

and so on. It is easily checked that the composite of any two consecutive maps is 0.

Next, we verify that  $\ker(\beta_2, 1/\gamma_3) \subseteq \text{im}(\gamma_2, \alpha_2)$ . Let  $(y, z) \in \ker(\beta_2, 1/\gamma_3)$ , so  $\beta_2 y = \gamma_3 z$ . Then  $\beta_3 \gamma_3 z = 0$ , so  $\alpha_3 z = 0$  because  $\gamma_4$  is injective. Therefore  $z = \alpha_2 x$  for some  $x \in K_2(A)$ . This gives

$$\beta_2 y = \gamma_3 \alpha_2 x = \beta_2 \gamma_2 x,$$

so  $\beta_2(y^{-1} \cdot \gamma_2 x) = 0$ . Since  $\gamma_1$  is surjective, we obtain  $y = \gamma_2 \{x \cdot \alpha_1(w)\}$  for some  $w \in K_2(A, J)$ . This gives

$$(y, z) = (\gamma_2, \alpha_2) \{x \cdot \alpha_1(w)\} \in \text{im}(\gamma_2, \alpha_2),$$

as desired. We leave the remaining verifications to the reader.

We are now ready to establish:

**(47.22) Milnor's Theorem.** *Given a fiber product of rings*

$$\begin{array}{ccc} A & \xrightarrow{f_1} & A_1 \\ f_2 \downarrow & & g_1 \downarrow \\ A_2 & \xrightarrow{g_2} & \bar{A} \end{array}$$

in which both  $g_1$  and  $g_2$  are surjective, there is an exact Mayer-Vietoris sequence of groups:

$$\begin{aligned} K_2(A) \rightarrow K_2(A_1) \times K_2(A_2) \rightarrow K_2(\bar{A}) &\xrightarrow{\partial} K_1(A) \rightarrow K_1(A_1) \times K_1(A_2) \rightarrow K_1(\bar{A}) \\ &\xrightarrow{\partial} K_0(A) \rightarrow K_0(A_1) \oplus K_0(A_2) \rightarrow K_0(\bar{A}). \end{aligned}$$

The maps are given by

$$K_i(A) \xrightarrow{(f_1, f_2)} K_i(A_1) \times K_i(A_2), K_i(A_1) \times K_i(A_2) \xrightarrow{(g_1, 1/g_2)} K_i(\bar{A}),$$

for  $i = 1, 2$ , while for  $i = 0$  these become

$$K_0(A) \xrightarrow{(f_1, f_2)} K_0(A_1) \oplus K_0(A_2), K_0(A_1) \oplus K_0(A_2) \xrightarrow{(g_1, -g_2)} K_0(\bar{A}).$$

The connecting homomorphisms  $\partial$  are defined as in (47.21), and the sequence extends the Mayer-Vietoris sequence (42.14).

*Proof.* We remark first that since  $g_1$  and  $g_2$  are surjective, so are  $f_1$  and  $f_2$ . Thus we may write

$$A_1 = A/J, \quad \bar{A} = A_2/J',$$

for some two-sided ideals  $J$  and  $J'$  of  $A$  and  $A_2$ , respectively. From the fiber product, we find readily that  $f_2$  induces an isomorphism  $\ker f_1 \cong \ker g_2$ , that is,  $J \cong J'$ . The desired result now follows from (47.21) and (42.14), using the ring surjection  $A \rightarrow A_2$ .

As an example of the use of the above sequence, consider the integral group ring  $\mathbb{Z}G$  of a cyclic group  $G$  of prime order  $p$ . The fiber product in (42.16) gives an exact sequence

$$K_2(\bar{\mathbb{Z}}) \rightarrow K_1(\mathbb{Z}G) \xrightarrow{i} K_1(\mathbb{Z}) \times K_1(R) \xrightarrow{h} K_1(\bar{\mathbb{Z}}),$$

in which  $h$  is surjective. We shall see in §47C that  $K_2(F) = 0$  for any finite field  $F$ . Thus, the map  $i$  is injective. Furthermore,  $K_1(\mathbb{Z}) \cong \mathbb{Z}$  and  $K_1(R) \cong R^\times$ , the latter by virtue of the Bass-Milnor-Serre Theorem. It follows at once that

$$(47.23) \quad K_1(\mathbb{Z}G) \cong (\mathbb{Z}G)^\times \quad \text{and} \quad SK_1(\mathbb{Z}G) = 1.$$

As we shall see in §48, (47.23) is true for an arbitrary finite cyclic group  $G$ .

### §47C. Symbols

Throughout the discussion,  $A$  denotes an arbitrary ring, and  $R$  a commutative ring. One technique for calculating  $K_2(A)$  or  $K_2(R)$ , in special cases, is to introduce certain types of generators of these groups, satisfying some obvious relations. These special generators are called *symbols*, by analogy with the Legendre and Jacobi symbols of number theory, and in fact this similarity is by no means accidental.

For the case of a field  $F$ , the *Steinberg symbols*  $\{u, v\}$ , defined for  $u, v \in F^\times$ , will generate  $K_2(F)$ , and will satisfy some simple relations. If instead we consider a commutative local ring  $R$ , then  $K_2(R)$  will be generated by the *Dennis-Stein symbols*  $\langle a, b \rangle$ , defined for  $a, b \in R$  with  $1 - ab \in R^\times$ ; these symbols will satisfy a different set of defining relations.

In this survey, we shall follow closely the treatment in Milnor [71] and the two articles by Dennis and Stein in Bass [73b], omitting most of the proofs. Our aim is to give the reader a feeling for the flavor of the subject, and also to provide some insight into the homomorphism

$$\theta': K_2(L) \rightarrow \coprod_Q K_1(S/Q)$$

occurring in the proof of Keating's Theorem 45.15. Here,  $L$  is a global field which is the quotient field of a Dedekind domain  $S$ , and  $Q$  ranges over all maximal ideals of  $S$ .

To emphasize the importance of the Milnor group  $K_2$ , we shall present here Tate's calculation of  $K_2(\mathbb{Q})$ , which has as consequences the Hilbert Reciprocity Theorem and the Law of Quadratic Reciprocity!

We recall from §47A that for  $n \geq 3$ , the *Steinberg group*  $St_n(A)$  has generators  $\{x_\alpha(a) : a \in A\}$ , where  $\alpha$  ranges over all ordered pairs  $ij$  with  $1 \leq i, j \leq n$ ,  $i \neq j$ , and where these generators satisfy the Steinberg relations (47.1). For  $\alpha = ij$ , we define  $-\alpha = ji$ , the reversed pair (compare with Exercise 64.1).

Let  $\varphi: St_n(A) \rightarrow E_n(A)$  be the homomorphism given by the evaluation map, which carries each generator  $x_\alpha(a)$  onto the elementary matrix  $E_\alpha(a)$ . Let  $K_2(n, A) = \ker \varphi$ , so there is an exact sequence of groups

$$(47.24) \quad 1 \rightarrow K_2(n, A) \rightarrow St_n(A) \xrightarrow{\varphi} E_n(A) \rightarrow 1.$$

We now introduce certain combinations of generators of  $St_n(A)$ , whose images

under the map  $\varphi$  are especially useful types of matrices. Let  $u \in A^\circ$ , and set

$$(47.25) \quad w_\alpha(u) = x_\alpha(u)x_{-\alpha}(-u^{-1})x_\alpha(u), \quad \text{and} \quad h_\alpha(u) = w_\alpha(u)w_\alpha(-1),$$

for each  $\alpha = ij$  as above. For  $\alpha = 12$ , we find readily that

$$(47.26) \quad w_\alpha(u) \xrightarrow{\varphi} \begin{pmatrix} 0 & u \\ -u^{-1} & 0 \end{pmatrix} \oplus \mathbf{I}^{(n-2)}, \quad h_\alpha(u) \xrightarrow{\varphi} \begin{pmatrix} u & 0 \\ 0 & u^{-1} \end{pmatrix} \oplus \mathbf{I}^{(n-2)},$$

where  $\mathbf{I}$  denotes an identity matrix of appropriate size.

Likewise, if  $a, b$  are elements of a commutative ring  $R$  and  $1 - ab \in R^\circ$ , then for each  $\alpha$  we set

$$(47.27) \quad H_\alpha(a, b) = x_{-\alpha}(-b(1 - ab)^{-1})x_\alpha(-a)x_{-\alpha}(b)x_\alpha((1 - ab)^{-1}a) \in \mathrm{St}_n(R),$$

and we find readily that

$$H_\alpha(a, b) \xrightarrow{\varphi} \mathrm{diag}(1 - ab, (1 - ab)^{-1}) \oplus \mathbf{I}^{(n-2)} \in E_n(R).$$

Our next step is to introduce the *Weyl group*  $W_n$ , defined as the subgroup of  $\mathrm{St}_n(A)$  generated by all elements  $\{w_\alpha(u) : u \in A^\circ\}$ , where (as above)  $\alpha = ij$ , with  $1 \leq i \neq j \leq n$ , and where  $n \geq 3$ . From (47.26), we find readily that  $\varphi(W_n)$  consists precisely of all generalized permutation matrices, whose entries are in  $A^\circ$ , and whose determinant equals 1 (in  $A^\circ/[A^\circ, A^\circ]$ ); see Milnor [71, §9] for details. Now set

$$(47.28) \quad C_n = \{w \in W_n : \varphi(w) = 1\},$$

a subgroup of  $W_n$  and of  $\mathrm{St}_n(A)$ . Further, with  $n \geq 3$  as usual, it turns out that  $C_n$  lies in the center of  $\mathrm{St}_n(A)$ ; see Milnor [71, §9].

Let us now restrict our attention to the case of a commutative ring  $R$ , and let  $n \geq 3$ . For each  $\alpha = ij$  and each  $u \in R^\circ$ , we have  $h_\alpha(u) \in W_n$ . From (47.26) it follows at once that for each  $\alpha$ ,

$$(47.29) \quad \{u, v\} = h_\alpha(uv)h_\alpha(u)^{-1}h_\alpha(v)^{-1} \in C_n \quad \text{for } u, v \in R^\circ,$$

thereby defining elements  $\{u, v\} \in C_n \subseteq K_2(n, R)$ . It turns out that  $\{u, v\}$  is independent of the choice of  $\alpha$ . We call these elements  $\{u, v\}$  *Steinberg symbols*; they satisfy the following identities:

$$(47.30) \quad \{uu', v\} = \{u, v\}\{u', v\}, \quad \{u, v\} = \{v, u\}^{-1}, \quad \{u, -u\} = 1,$$

for  $u, u', v \in R^\circ$ . Furthermore,

$$(47.31) \quad \{u, 1 - u\} = 1 \quad \text{if both } u \in R^\circ \quad \text{and} \quad 1 - u \in R^\circ.$$

(see Milnor [71, §§8–9] for proofs of the above assertions.)

**(47.32) Remarks.** (i) The term “symbol” is also used to denote a map  $\{ \ , \ \}$  from  $R^\times \times R^\times$  into some abelian group, such that the identities (47.30) and (47.31) are valid. Thus, the map

$$(u, v) \in R^\times \times R^\times \rightarrow \{u, v\} \in C_n,$$

with  $C_n$  as in (47.28), yields a symbol on  $R$ .

(ii) As shown in Milnor [71, Theorem 9.11], the group  $C_n$  is generated by the set of all symbols  $\{u, v\}$  with  $u, v \in R^\times$ . On the other hand, if  $R$  is either a finite field or a residue class ring  $\mathbb{Z}/p^n\mathbb{Z}$ , with  $p$  an odd prime, it is easily shown that all symbols on  $R$  must be trivial (Exercise 47.6).

The importance of the Steinberg symbols  $\{u, v\} \in C_n$  is that they provide concrete elements of  $K_2(n, R)$ , for  $R$  commutative. For the case of fields and skewfields, even stronger results are known:

**(47.33) Theorem.** *Let  $A$  be a skewfield, and define  $K_2(n, A)$  as in (47.24). Then*

(i) *For  $n \geq 3$ ,*

$$K_2(n, A) = C_n \leq \text{center of } \text{St}_n(A),$$

*so  $K_2(n, A)$  is an abelian group.*

(ii) *For  $n \geq 5$ , the exact sequence (47.24) gives a universal central extension of  $E_n(A)$ .*

For a proof of (i), see Milnor [71, Theorem 9.12]. Assertion (ii) follows from the proof of (47.8); see Milnor [71, Theorem 5.10] and also Remark 47.10iii above.

**(47.34) Corollary.** *Let  $F$  be a field. Then  $K_2(F)$  is generated by the set of all Steinberg symbols  $\{u, v\}$ , with  $u, v \in F^\times$ . Further,  $K_2(F) = 1$  if  $F$  is a finite field.*

*Proof.* We have

$$K_2(F) = \varinjlim K_2(n, F),$$

and  $K_2(n, F) = C_n$  for  $n \geq 3$ . Now use the fact that  $C_n$  is generated by Steinberg symbols (see (47.32ii)). Finally,  $K_2(F) = 1$  since symbols on a finite field are trivial.

A much deeper result, fundamental to the entire theory, is as follows:

**(47.35) Matsumoto's Theorem.** *Let  $F$  be a field. Then the abelian group  $K_2(F)$  has a presentation with generators  $\{u, v\}$  with  $u, v \in F^\times$ , subject to the relations*

$$\{uu', v\} = \{u, v\}\{u', v\}, \{u, vv'\} = \{u, v\}\{u, v'\},$$

and also<sup>†</sup>

$$\{u, 1-u\} = 1 \quad \text{for } u \neq 0, 1.$$

Furthermore, with  $C_n$  as in (47.28),

$$C_3 \cong C_4 \cong \cdots \cong K_2(F).$$

A proof is given in Milnor [71, §12], and a simpler proof in Keune [75].

Matsumoto's Theorem can be generalized in two ways, one in which  $F$  is replaced by a skewfield  $D$ , and the other with  $F$  replaced by a commutative local ring  $R$ . For the skewfield case, we have (Rehmann [78]):

**(47.36) Rehmann's Theorem.** *Let  $D$  be a skewfield, and let  $\text{St}_1(D)$  be the group generated by elements  $c(u, v)$ , one for each pair of elements  $u, v \in D^\times$ , and subject to the defining relations*

$$\begin{aligned} c(uv, w) &= c(uvu^{-1}, uwu^{-1})c(u, w), \\ c(u, vw)c(v, wu)c(w, uv) &= 1, \quad c(u, 1-u) = 1, \end{aligned}$$

if  $u, v, w \in D^\times$  (and  $u \neq 1$  in the last relation). Then there is an exact sequence

$$1 \rightarrow K_2(D) \rightarrow \text{St}_1(D) \xrightarrow{f} [D^\times, D^\times] \rightarrow 1,$$

where  $f: c(u, v) \rightarrow [u, v]$  for  $u, v \in D^\times$ .

Indeed, there is an injection  $\text{St}_1(D) \rightarrow \text{St}(D)$ , given by

$$c(u, v) \rightarrow \{u, v\} \quad \text{for } u, v \in D^\times,$$

where  $\{u, v\}$  is defined as in (47.29), using  $\alpha = 12$ . This identifies  $\ker f$  with  $K_2(D)$ .

We turn next to the Dennis-Stein symbols  $\langle a, b \rangle$ , where  $a$  and  $b$  are elements of a commutative ring  $R$ , and are such that  $1 - ab \in R^\times$ . Let  $\alpha = ij$ , where  $1 \leq i \neq j \leq n$ , and where  $n \geq 3$ . We define

$$(47.37) \quad \langle a, b \rangle = H_\alpha(a, b)h_\alpha(1 - ab)^{-1},$$

with  $H_\alpha$  and  $h_\alpha$  as in (47.27) and (47.25), respectively. It turns out that  $\langle a, b \rangle$  lies in  $K_2(n, R)$ , and does not depend on the choice of  $\alpha$ . Dennis and Stein originally used  $\langle -a, b \rangle$  in place of our  $\langle a, b \rangle$ ; their original list of relations was considerably simplified by Maazen-Stienstra. Later, Silvester and Stienstra

<sup>†</sup>Any bimultiplicative map  $f: F^\times \times F^\times \rightarrow G$  (= abelian multiplicative group), such that  $f(u, 1-u) = 1$  for  $u \neq 0, 1$ , is necessarily a symbol on  $F$ . See Exercise 47.7.

independently observed that the new symbols satisfy identities of a more symmetric form, as compared to the original relations.

In the following discussion, we shall only use the Dennis-Stein symbol  $\langle a, b \rangle$  when  $1 - ab \in R^\times$ ; likewise, when we use the Steinberg symbol  $\{u, v\}$ , we assume automatically that  $u, v \in R^\times$ . The Dennis-Stein symbols satisfy the following identities in  $K_2(n, R)$ :

$$(47.38) \quad \begin{cases} \langle a, b \rangle \langle b, a \rangle = 1, \\ \langle a, b \rangle \langle a, c \rangle = \langle a, b + c - abc \rangle, \\ \langle a, bc \rangle = \langle ab, c \rangle \langle ac, b \rangle. \end{cases}$$

One can express Steinberg symbols  $\{u, v\}$  in terms of Dennis-Stein symbols  $\langle a, b \rangle$  (but not conversely, in certain examples!).

Dennis and Stein proved (see Dennis-Stein [73b, §2]):

**(47.39) Theorem.** *Let  $n \geq 3$  and let  $R$  be a commutative semilocal ring. Then  $K_2(n, R)$  and  $K_2(R)$  are generated by the set of all Dennis-Stein symbols. They are also generated by the set of all Steinberg symbols.*

It is in terms of Dennis-Stein symbols that one obtains a presentation of the group  $K_2(R)$ , for  $R$  a commutative local ring. This result provides a second generalization of Matsumoto's Theorem (which is used in the proof, in any case), and is based on the work of Dennis-Stein, Maazen-Stienstra, and van der Kallen (see van der Kallen [80]). We have

**(47.40) Theorem.** *Let  $R$  be a commutative local ring. Then  $K_2(R)$  has a presentation with generators all Dennis-Stein symbols  $\langle a, b \rangle$ , one for each pair  $a, b \in R$  such that  $1 - ab \in R^\times$ , and with relations (47.38) whenever all the symbols involved are defined.*

We now return to Matsumoto's Theorem, and show how to use it to obtain Tate's formula for  $K_2(\mathbb{Q})$ .

Matsumoto's Theorem implies at once that for any field  $F$ , the Steinberg symbol

$$\{ \quad , \quad \}: F^\times \times F^\times \rightarrow K_2(F),$$

defined in (47.29), is universal. Thus (see Exercise 47.7) every bimultiplicative map  $f$  from  $F^\times \times F^\times$  into an abelian group  $G$ , such that  $f(u, 1 - u) = 1$  for  $u \neq 0, 1$ , factors uniquely through  $K_2(F)$ . This means that there exists a unique homomorphism  $h: K_2(F) \rightarrow G$  such that

$$h\{x, y\} = f(x, y) \quad \text{for all } x, y \in F^\times.$$

Choosing  $f$  suitably, we may thus construct well-defined homomorphisms on

$K_2(F)$ . This idea lies at the heart of Tate's calculation of  $K_2(\mathbb{Q})$ , which we now give.

**(47.41) Tate's Theorem.** *There is an isomorphism*

$$K_2(\mathbb{Q}) \cong \{\pm 1\} \oplus \prod_{p \geq 3} GF(p)^*,$$

*the direct sum of a cyclic group of order 2 and cyclic groups of order  $p - 1$ , with  $p$  ranging over all odd primes.*

*Proof.* Step 1. We shall give the isomorphism explicitly in terms of certain symbols defined on  $\mathbb{Q}$ . First, let

$$t_\infty: \mathbb{R}^* \times \mathbb{R}^* \rightarrow \{\pm 1\}$$

be the bimultiplicative map defined by

$$t_\infty(a, b) = \begin{cases} 1 & \text{if } a > 0 \quad \text{or} \quad b > 0, \\ -1 & \text{if } a < 0 \quad \text{and} \quad b < 0. \end{cases}$$

Since  $t_\infty(a, 1-a) = 1$  for  $a \neq 0, 1$ , there is a well-defined homomorphism

$$t_\infty: K_2(\mathbb{R}) \rightarrow \{\pm 1\}, \quad \text{given by } \{a, b\} \mapsto t_\infty(a, b) \text{ for } a, b \in \mathbb{R}^*.$$

Since  $t_\infty\{-1, -1\} = -1$ , we conclude that  $\{-1, -1\} \neq 1$  in  $K_2(\mathbb{R})$ ; this inequality also holds in  $K_2(\mathbb{Q})$  and  $K_2(\mathbb{Z})$ , since  $t_\infty$  is also a symbol on every subring of  $\mathbb{R}$ .

Step 2. For each rational odd prime  $p$ , we introduce a *tame symbol*

$$t_p: \mathbb{Q}^* \times \mathbb{Q}^* \rightarrow GF(p)^*,$$

as follows. Each  $x \in \mathbb{Q}^*$  can be expressed as  $x = p^e a/b$ , where  $a, b \in \mathbb{Z}$  and  $p \nmid ab$ . Put  $v(x) = e$ , and call  $v$  the *exponential p-adic valuation* on  $\mathbb{Q}$ ; let  $v(0) = \infty$ . Since

$$v(x^{v(y)} / y^{v(x)}) = 0,$$

the quotient has a well-defined image  $\overline{x^{v(y)} / y^{v(x)}} \in GF(p)^*$ . Setting

$$t_p(x, y) = (-1)^{v(x)v(y)} \overline{x^{v(y)} / y^{v(x)}} \quad \text{for } x, y \in \mathbb{Q}^*,$$

we find readily that for each  $p$ ,  $t_p$  is a symbol on  $\mathbb{Q}$ . Thus there is a well-defined homomorphism

$$t_p: K_2(\mathbb{Q}) \rightarrow GF(p)^*, \quad \text{given by } \{a, b\} \mapsto t_p(a, b) \quad \text{for } a, b \in \mathbb{Q}^*.$$

We intend to prove that the map

$$\{a, b\} \in K_2(\mathbb{Q}) \rightarrow t_\infty(a, b) + \sum_{p \geq 3} t_p(a, b), \quad \text{for } a, b \in \mathbb{Q},$$

gives the desired isomorphism.

*Step 3.* For  $m \geq 1$ , let  $S_m$  be the subgroup of  $K_2(\mathbb{Q})$  generated by all symbols  $\{a, b\}$  with  $a, b \in \mathbb{Z}$ ,  $|a| \leq m$ ,  $|b| \leq m$ . Then

$$K_2(\mathbb{Q}) = \bigcup_{m=1}^{\infty} S_m = \varinjlim S_m.$$

Now  $S_1$  is cyclic of order 2, generated by  $\{-1, -1\}$ . Also  $S_2 = S_1$ , since

$$\{-1, 2\} = \{u, 1-u\} = 1 \quad (\text{with } u = -1), \quad \{2, 2\} = \{-1, 2\} \{-2, 2\} = 1.$$

Thus  $t_\infty: S_2 \cong \{\pm 1\}$ , with  $t_\infty$  as in Step 1.

We now show that for  $p \geq 3$ , the map  $t_p$  induces an isomorphism

$$(47.42) \quad t'_p: S_p/S_{p-1} \cong GF(p)^*.$$

Note that  $t'_p$  is well defined since  $t_p$  is trivial on  $S_{p-1}$ . Further, if  $a \in \mathbb{Z}$  is prime to  $p$ , then  $v(a) = 0$ ,  $v(p) = 1$ , so

$$t_p\{a, p\} = \bar{a} \in GF(p)^*.$$

Thus  $t'_p$  is surjective, so it remains for us to construct an inverse map

$$(47.43) \quad \theta: GF(p)^* \rightarrow S_p/S_{p-1}.$$

Let  $a \in \mathbb{Z}$ ,  $0 < a < p$ , and put

$$\theta(\bar{a}) = \{a, p\} \pmod{S_{p-1}},$$

viewed as element of the multiplicative group  $S_p/S_{p-1}$ . We shall now verify that

$$\theta(\bar{a})\theta(\bar{b}) = \theta(\bar{ab}) \quad \text{for } 0 < a, b < p.$$

Write

$$ab = rp + c, \quad \text{where } 0 \leq r \leq p-1, 0 < c < p.$$

If  $r = 0$ , then

$$\theta(\bar{ab}) = \{c, p\} = \{a, p\}\{b, p\}$$

as desired. On the other hand, let  $r > 0$ ; then

$$\left\{ \frac{rp}{ab}, \frac{c}{ab} \right\} = 1 \quad \text{because } \frac{rp}{ab} + \frac{c}{ab} = 1.$$

Consequently we obtain

$$\left\{ c, \frac{rp}{ab} \right\} = \left\{ ab, \frac{rp}{ab} \right\} = \left\{ ab, \frac{r}{ab} \right\} \{ab, p\} \equiv \{a, p\} \{b, p\} \pmod{S_{p-1}},$$

where the congruence is interpreted multiplicatively. But also

$$\left\{ c, \frac{rp}{ab} \right\} = \{c, p\} \left\{ c, \frac{r}{ab} \right\} \equiv \{c, p\} \pmod{S_{p-1}},$$

which completes the proof that  $\theta$  is a well-defined homomorphism. Clearly  $t'_p \theta$  is the identity map, and it remains to check that  $\theta$  is surjective. Now  $S_p/S_{p-1}$  has generators  $\{\pm p, \pm p\}$  and  $\{\pm b, \pm p\}$ , where  $0 < b \leq p - 1$ . However,

$$\begin{aligned} \{p, -p\} &= 1 = \{-p, p\}, \quad \{1-p, p\} = 1, \\ \{p, p\} &= \{-1, p\} \{-p, p\} = \{-1, p\} = \{p-1, p\} = \theta(\overline{p-1})^{-1}. \end{aligned}$$

Also, for  $0 < b \leq p - 1$ ,

$$\{-b, p\} = \{b, p\} \{-1, p\} \in \text{im } \theta.$$

Thus  $\theta$  is surjective, and is the inverse of  $t'_p$ , which proves (47.42).

*Step 4.* We are now ready to complete the proof, and begin by computing  $S_m$  explicitly. If  $m \geq 4$  is not prime, then of course  $S_m = S_{m-1}$ . We have already shown that  $t_\infty: S_2 \cong \{\pm 1\}$ . We now use induction on the prime  $p$  to show that

(47.44)

$$\tau_p: S_p \cong \{\pm 1\} \times GF(3)^\circ \times \cdots \times GF(p)^\circ, \quad \text{where } \tau_p = t_\infty \times t_3 \times \cdots \times t_p.$$

The results holds at  $p = 2$ , so let  $p \geq 3$  and assume the result true at all smaller primes. Let  $q$  be the largest prime  $< p$ , so  $S_{p-1} = S_q$ . Then there is a commutative diagram with exact rows

$$\begin{array}{ccccccc} 1 & \longrightarrow & S_q & \longrightarrow & S_p & \longrightarrow & GF(p)^\circ \longrightarrow 1 \\ & & \tau_q \downarrow & & \tau_p \downarrow & & 1 \downarrow \\ 1 & \rightarrow & \{\pm 1\} \times \cdots \times GF(q)^\circ & \rightarrow & \{\pm 1\} \times \cdots \times GF(q)^\circ \times GF(p)^\circ & \rightarrow & GF(p)^\circ \rightarrow 1. \end{array}$$

Since  $\tau_q$  is an isomorphism by the induction hypothesis, so is  $\tau_p$  by the Snake Lemma. This proves (47.44) for all  $p$ . However, we then obtain

$$K_2(\mathbb{Q}) = \varinjlim S_m = \{\pm 1\} \times \coprod_{p \geq 3} GF(p)^*,$$

and the proof of Tate's Theorem is completed.

Let us now sketch the connection between  $K_2(\mathbb{Q})$  and quadratic reciprocity. For  $p$  an odd prime, define the *Hilbert symbol*  $(a, b)_p$  by the formula

$$(47.45) \quad (a, b)_p = t_p(a, b)^{(p-1)/2} \in GF(p)^* \quad \text{for } a, b \in \mathbb{Q}^*.$$

Then  $(a, b)_p$  is bimultiplicative, and is unchanged if  $a$  is replaced by  $ax^2$  with  $x \in \mathbb{Q}^*$ . Further, for  $a, b \in \mathbb{Z}$  prime to  $p$ , we find that

$$(a, b)_p = 1, \quad (a, p)_p = \bar{a}^{(p-1)/2} = \begin{cases} 1 & \text{if } \bar{a} \text{ square in } GF(p), \\ -1 & \text{otherwise.} \end{cases}$$

Furthermore,

$$(p, p)_p = (-1)^{(p-1)/2}.$$

Thus, if  $a \in \mathbb{Z}$  is prime to  $p$ , then  $(a, p)_p$  is the usual Legendre symbol  $\left(\frac{a}{p}\right)$ .

We now define  $(a, b)_2 = \pm 1$ , for  $a, b \in \mathbb{Q}^*$ , according to whether the equation

$$ax^2 + by^2 = z^2, \quad \text{with } x, y, z \in \mathbb{Q}_2 \quad (= 2\text{-adic field}),$$

has a nontrivial solution or not (see Exercises 47.3, 47.4). Then  $(a, b)_2$  defines a symbol on  $\mathbb{Q}^*$ , the *Hilbert symbol* associated with the prime 2.

Since every symbol on  $\mathbb{Q}$  factors through  $K_2(\mathbb{Q})$  (according to the discussion preceding (47.41)), it follows from Tate's formula (47.41) that there exist homomorphisms

$$\varphi_\infty: \{\pm 1\} \rightarrow \{\pm 1\}, \quad \varphi_p: GF(p)^* \rightarrow \{\pm 1\}, \quad p \geq 3,$$

such that

$$(a, b)_2 = \varphi_\infty t_\infty(a, b) \cdot \prod_{p \geq 3} \varphi_p t_p(a, b) \quad \text{for all } a, b \in \mathbb{Q}^*.$$

Since the values of  $\varphi_p$  lie in  $\{\pm 1\}$ , we have  $\varphi_p(x^2) = 1$  for all  $x \in GF(p)^*$ , and therefore

$$\varphi_p(x) = x^{n_p(p-1)/2}, \quad x \in GF(p)^*,$$

with  $n_p = 0$  or 1. Thus we obtain

$$(a, b)_2 = t_\infty(a, b)^{n_\infty} \cdot \prod_{p \geq 3} (a, b)_p^{n_p} \quad \text{for all } a, b \in Q^\times,$$

where also  $n_\infty = 0$  or 1. Choosing  $a = b = -1$ , we see that  $n_\infty = 1$ .

It is convenient to write

$$t_\infty(a, b) = (a, b)_\infty,$$

so now

$$(47.46) \quad (a, b)_2 = (a, b)_\infty \cdot \prod_{p \geq 3} (a, b)_p^{n_p}.$$

We show that each  $n_p = 1$ . First, choose  $b = p = 8k \pm 3$ ,  $a = 2$ ; then

$$(2, p)_2 = -1, \quad (2, p)_\infty = 1, \quad (2, p)_q = 1 \quad \text{for } q = \text{odd prime}, \quad q \neq p.$$

This gives

$$-1 = (2, p)_p^{n_p}, \quad \text{whence } n_p = 1 \quad \text{and} \quad (2, p)_p = -1.$$

Second, choose  $b = p = 8k + 7$ ,  $a = -1$ , and then we get as above:

$$(-1, p)_p = -1 \quad \text{and} \quad n_p = 1.$$

Finally, we need (see Milnor [71], Lemma 11.9):

**(47.47) Lemma.** *Let  $p = 8k + 1$  be prime. Then there exists an odd prime  $q < \sqrt{p}$  such that  $p$  is a quadratic nonresidue mod  $q$ , that is,  $(p, q)_q = -1$ .*

Continuing with our discussion, suppose  $n_p \neq 1$  for some odd prime  $p$ , and let  $p$  be minimal such. Choose  $q$  as in the lemma, so  $n_q = 1$ . Then

$$(p, q)_\infty = 1, \quad (p, q)_2 = 1, \quad (p, q)_l = 1 \quad \text{for } l = \text{odd prime}, \quad l \neq p, q.$$

Therefore (47.46) gives

$$1 = (p, q)_q^{n_q} (p, q)_p^{n_p} = -1 \cdot (p, q)_p^{n_p},$$

so  $n_p = 1$ , a contradiction. We have thus proved:

**(47.48) Hilbert Reciprocity Theorem.** *For  $a, b \in Q^\times$ ,*

$$\prod_{2 < p < \infty} (a, b)_p = 1.$$

**(47.49) Corollary (Law of Quadratic Reciprocity).** *Let  $p$  and  $q$  be odd primes, and let  $\left(\frac{x}{p}\right)$  denote the Legendre symbol. Then*

$$\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}, \quad \left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8},$$

and

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{(p-1)(q-1)/4}.$$

*Proof.* We have

$$(-1, p)_\infty = 1, \quad (-1, p)_2 = (-1)^{(p-1)/2}, \quad (-1, p)_l = 1,$$

for  $l$  an odd prime,  $l \neq p$ . By (47.48) we obtain

$$\left(\frac{-1}{p}\right) = (-1, p)_p = (-1)^{(p-1)/2}.$$

A similar argument yields the formula for  $\left(\frac{2}{p}\right)$ .

Finally, we have

$$(p, q)_\infty = 1, \quad (p, q)_l = 1 \quad \text{for odd primes } l \neq p, q,$$

$$(p, q)_p = \left(\frac{q}{p}\right), \quad (p, q)_q = \left(\frac{p}{q}\right), \quad (p, q)_2 = (-1)^{(p-1)(q-1)/4}.$$

Combining these results, we obtain the desired formula for the product  $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right)$ , which completes the proof.

Suppose now that  $R$  is any Dedekind domain, and let  $F$  be its quotient field. As shown by Quillen (see Dennis-Stein [73a], page 246), there is an exact sequence

$$K_3(F) \rightarrow \coprod_P K_2(R/P) \rightarrow K_2(R) \rightarrow K_2(F) \rightarrow \coprod_P K_1(R/P) \rightarrow K_1(R)$$

$$\rightarrow K_1(F) \rightarrow \coprod_P K_0(R/P) \rightarrow K_0(R) \rightarrow K_0(F) \rightarrow 0,$$

where  $P$  ranges over all (nonzero) prime ideals of  $R$ .

Now assume that  $F$  is a global field; then each  $R/P$  is a finite field, so  $K_2(R/P) = 1$  by (47.34). Further, the map  $K_1(R) \rightarrow K_1(F)$  is injective, since the kernel  $SK_1(R)$  is trivial by the Bass-Milnor-Serre Theorem. The above sequence

thus breaks into two exact sequences

$$0 \rightarrow K_2(R) \rightarrow K_2(F) \xrightarrow{d} \coprod_P K_1(R/P) \rightarrow 0,$$

$$1 \rightarrow K_1(R) \rightarrow K_1(F) \rightarrow \coprod_P K_0(R/P) \rightarrow K_0(R) \rightarrow K_0(F) \rightarrow 0.$$

The second of these is our standard localization sequence (40.17).

The map  $d$  played a vital role in the proof of Keating's Theorem 45.15, and it is therefore of interest to give an explicit description of the map in the special case considered here. It will suffice to define the map

$$d_P: K_2(F) \rightarrow (R/P)^* \cong K_1(R/P)$$

for each  $P$ ; it will be clear from its definition that for each  $\xi \in K_2(F)$ ,  $d_P(\xi) = 1$  a.e.

Now  $K_2(F)$  is generated by Steinberg symbols  $\{x, y\}$  with  $x, y \in F^*$ . We define  $d_P$  by constructing a bimultiplicative map  $d_P: F^* \times F^* \rightarrow (R/P)^*$ , such that  $d_P(x, 1-x) = 1$  for  $x \neq 0, 1$ , and then factoring this map through  $K_2(F)$ . Let  $v_P$  be the *exponential P-adic valuation* on  $F$ , defined analogously to the valuation  $v$  occurring in Step 2 of the proof of Tate's Theorem (see also §4C). We now set

$$d_P\{x, y\} = (-1)^{v_P(x)v_P(y)} \overline{x^{v_P(y)}} / \overline{y^{v_P(x)}} \in (R/P)^* \quad \text{for } x, y \in F^*,$$

the right-hand side representing a *tame symbol* corresponding to  $P$ . (The reader will easily verify that this is indeed a symbol on  $F$ .)

We can now describe the map  $d$  in terms of these  $\{d_P\}$ , and we have

$$d: K_2(F) \rightarrow \coprod_P K_1(R/P),$$

where for  $x, y \in F^*$ ,

$$d\{x, y\} = - \coprod_P d_P\{x, y\}.$$

(The minus sign is used for technical reasons, which we shall not discuss here.)

## §47. Exercises

- Let  $R$  be a commutative ring, and  $K_0(R) = G_0^R(R)$  its Grothendieck ring, with multiplication given by  $\otimes_R$ . For each ideal  $J$  of  $R$ , show that the relative groups  $K_0(R, J)$  and  $K_1(R, J)$  can be made into  $K_0(R)$ -modules.
- Let  $F$  be a noetherian ring of finite global dimension, and let  $x, y$  be indeterminates which commute with all elements of  $F$  and with each other. Let  $A = F[x, y]/(xy)$ . Show

that there is a fiber product

$$\begin{array}{ccc} A & \longrightarrow & F[x] \\ \downarrow & & \downarrow \\ F[y] & \longrightarrow & F, \end{array}$$

and apply (47.17) to prove that  $K_1(A) \cong K_1(F)$ .

[Hint: Since there is a map  $F \rightarrow F[x]$  which splits the surjection  $F[x] \rightarrow F[x]/(x) = F$ , the maps  $K_i(F[x]) \rightarrow K_i(F)$ ,  $i = 1, 2$ , are surjective.]

3. Let  $p$  be an odd prime, and let  $(a, b)_p$  be the Hilbert symbol defined by (47.45). Let  $\mathbb{Q}_p$  be the  $p$ -adic field. Prove that  $(a, b)_p = 1$  if the equation

$$ax^2 + by^2 = 1 \quad \text{has a solution with } x, y \in \mathbb{Q}_p,$$

and  $(a, b)_p = -1$  otherwise. Show also that  $(a, b)_p = 1$  if and only if  $ax^2 + by^2 = z^2$  has a nontrivial solution with  $x, y, z \in \mathbb{Q}_p$ .

4. Define  $(a, b)_2$  analogously, for  $a, b \in \mathbb{Z}$ ,  $ab \neq 0$ . Prove that if  $2 \nmid ab$ , then

$$(a, b)_2 = (-1)^{(a-1)(b-1)/4}$$

Show also that

$$(a, 2)_2 = (-1)^{(a^2-1)/8}, \quad (2, 2)_2 = 1.$$

Prove that the map

$$\mathbb{Q}^\times \times \mathbb{Q}^\times \rightarrow \{\pm 1\}, \quad \text{given by } x \times y \mapsto (x, y)_2,$$

defines a symbol on  $\mathbb{Q}$ .

5. Prove the following version of the **Excision Lemma 47.20**:

Let  $B = B_1 \times \cdots \times B_n$  be a product of rings, and  $A$  a subring of  $B$  which projects onto each  $B_i$ . Let  $J$  be a two-sided ideal of  $B$  contained in  $A$ . Show that  $K_1(A, J) \cong K_1(B, J)$ , and that the map  $K_2(A, J) \rightarrow K_2(B, J)$  is surjective.

[Hint: See Bass [68], Theorem 5.8 on page 484, and Dennis [73b], pages 117–119.]

6. Let  $R = GF(q)$  or  $\mathbb{Z}/p^n\mathbb{Z}$ , with  $p$  odd. Show that all symbols on  $R$  are trivial.

[Hint: Consider the case  $R = GF(q)$ ,  $q$  odd. There must exist two squares  $a, b \in R^\times$  whose sum is a nonsequence, since otherwise the set of squares is a subfield of  $R$ . Therefore there exist nonsquares  $c, d \in R^\times$  with  $c + d = 1$ . If  $\{ , \}$  is a symbol on  $R$ , then  $\{c, d\} = 1$ . Now let  $R^\times = \langle x \rangle$ , so  $c$  and  $d$  are odd powers of  $x$ . Then  $\{x, x\}$  has odd order. But  $\{x, x\} = \{x, x\}^{-1}$ , so  $\{x, x\} = 1$ , and therefore  $\{u, v\} = 1$  for all  $u, v \in R^\times$ . Analogous arguments work for the other cases where  $q = 2$ , or where  $R = \mathbb{Z}/p^n\mathbb{Z}$ ,  $p$  odd.]

7. Let  $F$  be a field,  $G$  an abelian multiplicative group, and let  $f: F^\times \times F^\times \rightarrow G$  be any bimultiplicative map such that  $f(u, 1-u) = 1$  for  $u \neq 0, 1$ . Prove that  $f$  is a symbol on  $F$ .

[Hint: We must show that for  $u, v \in F^*$ ,

$$f(u, -u) = 1 \quad \text{and} \quad f(v, u) = f(u, v)^{-1}.$$

For the first of these, note that  $-u = (1-u)/(1-u^{-1})$  if  $u \neq 1$ . Therefore

$$f(u, -u) = f(u, 1-u)f(u, 1-u^{-1})^{-1} = f(u, 1-u)^{-1} = f(u^{-1}, 1-u^{-1}) = 1.$$

For the second identity, use

$$\begin{aligned} f(u, v) &= f(u, v)f(u, -u)f(uv, -uv)^{-1}f(v^{-1}, -v^{-1}) \\ &= f(v^{-1}, -uv)f(v^{-1}, -v^{-1}) = f(v^{-1}, u) = f(v, u)^{-1}. \end{aligned}$$

8. Let  $A$  be a finite  $p$ -torsion ring, where  $p$  is prime. Prove that  $K_2(A)$  is a finite  $p$ -group.

[Hint (Oliver): Since  $A$  is semilocal, it has stable range 1. The analogue of (40.42) for  $K_2$  shows that  $K_2(A)$  is f.g., so it suffices to prove that  $K_2(A)$  is a  $p$ -torsion group. For any group  $G$ , let  $H_2(G)$  denote its Schur multiplier  $H_2(G, \mathbb{Z})$ . Given  $N \trianglelefteq G$ , let  $\bar{G} = G/N$ . Then (see Rotman [79, page 356])  $H_2(G)$  has a filtration whose factor groups are subquotients of the groups

$$(*) \quad H_2(\bar{G}), \quad H_1(\bar{G}, H_1(N)), \quad H_0(\bar{G}, H_2(N)).$$

We apply this to the case where  $G = E(A)$ ,  $\bar{G} = E(\bar{A})$ , with  $\bar{A} = A/\text{rad } A$ , a direct sum of full matrix algebras over finite fields. Then  $H_2(\bar{G}) = K_2(\bar{A}) = 1$ , by (47.34). On the other hand,  $N$  is the kernel of the surjection  $E(A) \rightarrow E(\bar{A})$ , hence is the union of kernels of  $E_n(A) \rightarrow E_n(\bar{A})$  for  $n \geq 2$ . Each of these kernels lies in  $1 + (\text{rad } A)M_n(A)$  and is therefore a finite  $p$ -group. Thus  $N = \varinjlim N_i$ , with each  $N_i$  a finite  $p$ -group. Therefore  $H_1(N) = \varinjlim H_1(N_i)$  is a  $p$ -torsion group, and likewise so is  $H_2(N)$ . Thus the groups  $(*)$  are  $p$ -torsion, whence so is  $H_2(E(A)) (= K_2(A))$ .]

## §48. $SK_1$ OF INTEGRAL GROUP RINGS

Throughout this section,  $G$  denotes a finite group, and  $G_p$  a Sylow  $p$ -subgroup of  $G$  for each prime  $p$ . Let  $R$  be a Dedekind domain whose quotient field  $F$  is either an algebraic number field or else a finite extension of a  $p$ -adic field  $\mathbb{Q}_p$ . In the latter case,  $R$  is taken to be the valuation ring in  $F$ , and is called a  *$p$ -adic ring*.

Our purpose here is to describe some of the main results about  $SK_1(RG)$ . The proofs are beyond the scope of this book, since they involve a generalized version of the Bass-Milnor-Serre Theorem, as well as detailed calculations with  $K_2$ -groups. We begin by recalling some earlier results.

The inclusion  $RG \subset FG$  induces a map  $K_1(RG) \rightarrow K_1(FG)$ , whose kernel is denoted by  $SK_1(RG)$ . We have already established:

1.  $SK_1(RG)$  is a finite abelian group (Bass's Theorem 45.20).
2. If  $R$  is a  $p$ -adic ring, then  $SK_1(RG)$  is a finite  $p$ -group (Wall's Theorem 46.9).
3. If  $R$  is a  $p$ -adic ring, then  $SK_1(RG) = 1$  if  $G_p$  is abelian or if  $p$  does not divide  $|G'|$  (see (46.24) and (46.25ii)).

For  $G$  cyclic of prime order, we proved at the end of §47B that  $SK_1(ZG) = 1$ . More generally, the following holds true:

**(48.1) Bass-Milnor Theorem.**  $SK_1(ZG) = 1$  for every cyclic group  $G$ .

For a proof, see Bass-Milnor-Serre [67], Prop. 4.14. The theorem remains valid when  $Z$  is replaced by a ring  $R$  of algebraic integers, see Alperin-Dennis-Stein [85] and Alperin-Dennis-Oliver-Stein [86].

We next introduce the *induction* and *restriction* maps:

$$\text{ind}_H^G: K_1(RH) \rightarrow K_1(RG), \quad \text{res}_H^G: K_1(RG) \rightarrow K_1(RH).$$

These were discussed in §46 (see (46.18)), where we showed that  $K_1(RG)$  is a Frobenius module over the Frobenius functor  $G_0^R(RG)$ . Since  $\text{ind}$  and  $\text{res}$  commute with maps obtained by change of ground ring from  $R$  to  $F$ , it follows readily that  $SK_1(RG)$  is also a Frobenius module over  $G_0^R(RG)$ . We may therefore apply the induction theorems established in §38A.

For a prime  $p$ , let the subscript  $(p)$  denote localization at  $p$ . Then  $SK_1(RG)_{(p)}$  is precisely the  $p$ -torsion submodule of the finite abelian group  $SK_1(RG)$ :

$$SK_1(RG)_{(p)} = \{x \in SK_1(RG) : p^n x = 0 \text{ for some } n \geq 0\}.$$

As in (46.24), we see that  $SK_1(RG)_{(p)}$  is a Frobenius module over  $G_0^R(RG)_{(p)}$ , where

$$G_0^R(RG)_{(p)} = Z_{(p)} \otimes_Z G_0^R(RG).$$

On the other hand, starting with our given field  $F$ , we denote by  $\mathcal{H}_p$  the set of all subgroups  $H$  of  $G$  which are  $F$ -elementary at the prime  $p$  (see Volume I, page 492). Then we obtain

$$G_0(FG)_{(p)} = \sum_{H \in \mathcal{H}_p} \text{ind}_H^G G_0(FH)_{(p)},$$

by an easy modification of the proof of the Witt-Berman Theorem 21.6. As in the proof of (38.18), the above implies that

$$G_0^R(RG)_{(p)} = \sum_{H \in \mathcal{H}_p} \text{ind}_H^G G_0^R(RH)_{(p)}.$$

Therefore we obtain from (38.13):

$$SK_1(RG)_{(p)} = \sum_{H \in \mathcal{H}_p} \text{ind}_H^G SK_1(RH)_{(p)},$$

$$\bigcap_{H \in \mathcal{H}_p} \ker(\text{res}_H^G \text{ acting on } SK_1(RG)_{(p)}) = 0.$$

Thus, we may obtain information about  $SK_1(RG)$  from knowledge of

$SK_1(RH)$  for various  $F$ -elementary subgroups  $H$  of  $G$ . However, a much stronger result is true. We state without proof the following fundamental theorem, due to R. Oliver [81]:

**(48.2) Oliver's Theorem.** *Let  $p$  be prime, and let  $\mathcal{E}_p$  be the set of  $p$ -elementary subgroups of  $G$ , that is, subgroups which are a direct product of a  $p$ -group and a cyclic  $p$ -group. Then*

(i) *For  $R = \text{alg. int. } \{F\}$ , we have*

$$SK_1(RG)_{(p)} = \sum_{H \in \mathcal{E}_p} \text{ind}_H^G SK_1(RH)_{(p)}.$$

(ii) *If  $R$  is a  $p$ -adic ring, then*

$$SK_1(RG) = \sum_{H \in \mathcal{E}_p} \text{ind}_H^G SK_1(RH).$$

(iii) *There exist groups  $G$  for which*

$$\bigcap_{H \in \mathcal{E}_p} \ker(\text{res}_H^G \text{ acting on } SK_1(RG)_{(p)}) \neq 0.$$

This powerful theorem seems rather unexpected, and it also provides an instance where the induction and restriction properties are markedly different. Before applying Oliver's Theorem, we describe some induction theorems involving the set  $\mathcal{C}$  of all cyclic subgroups of a given group  $G$ . By definition, the Artin exponent  $A(G)$  (see also §76) is the least positive integer  $n$  such that

$$n \cdot G_0(QG) \subseteq \sum_{H \in \mathcal{C}} \text{ind}_H^G G_0(QH).$$

By Artin's Induction Theorem we know that  $A(G)$  divides  $|G|$ . Next, by (38.16) we obtain

$$A(G)^2 \cdot G_0^Z(ZG) \subseteq \sum_{H \in \mathcal{C}} \text{ind}_H^G G_0^Z(ZH),$$

and consequently

$$A(G)^2 \cdot SK_1(ZG) \subseteq \sum_{H \in \mathcal{C}} \text{ind}_H^G SK_1(ZH).$$

However, each term  $SK_1(ZH)$ ,  $H \in \mathcal{C}$ , is trivial by the Bass-Milnor Theorem. We have thus established:

**(48.3) Lam's Theorem.** *Let  $A(G)$  be the Artin exponent of  $G$ . Then*

$$A(G)^2 \cdot SK_1(ZG) = 0.$$

As shown by Alperin-Dennis-Oliver-Stein [86], the analogous result holds true when  $\mathbb{Z}$  is replaced by a ring of algebraic integers:

**(48.4) Theorem.** *Let  $R = \text{alg. int. } \{F\}$ , where  $F$  is an algebraic number field. Then*

$$A(G)^2 \cdot SK_1(RG) = 0,$$

where  $A(G)$  is the Artin exponent of  $G$ .

*Proof.* As shown in the proof of (38.17),  $SK_1(RG)$  is a Frobenius module over the Frobenius functor  $G_0^{\mathbb{Z}}(\mathbb{Z}G)$ . By the remarks preceding (48.3), we obtain

$$A(G)^2 \cdot SK_1(RG) \subseteq \sum_{H \in \mathcal{C}} \text{ind}_H^G SK_1(RH).$$

But  $SK_1(RH)$  is trivial for each cyclic group  $H$ , as pointed out in the remarks after (48.1). This gives the desired result.

As an immediate consequence of the above, we obtain:

**(48.5) Corollary.** *Let  $R = \text{alg. int. } \{F\}$ , and let  $p$  be prime. Then*

- (i) *If  $G$  is a  $p$ -group, then so is  $SK_1(RG)$ .*
- (ii) *If  $p \nmid |G|$ , then  $SK_1(RG)$  is  $p$ -torsionfree.*
- (iii) *If  $G$  has a cyclic normal Sylow  $p$ -subgroup, then  $SK_1(RG)$  is  $p$ -torsionfree.*

The first two assertions follow from (48.4), since  $A(G)$  divides  $|G|$ . Assertion (iii) is a consequence of a result of Lam [68b] (see (76.23)), which states that if  $G$  has a cyclic normal Sylow  $p$ -subgroup, then  $p \nmid A(G)$ .

We turn next to the question as to which groups  $G$  have trivial  $SK_1(\mathbb{Z}G)$ . This is a difficult question, even for abelian groups. The key result below is proved in Alperin-Dennis-Stein [85] and Alperin-Dennis-Oliver-Stein [86], and may be viewed as a far-reaching generalization of the Bass-Milnor Theorem. The proofs, beyond the scope of this book, use detailed facts about  $K_2$ -groups, as well as earlier calculations by various authors (Bass, Kervaire, Lam, Milnor). Also needed is the result<sup>†</sup> that a surjection of abelian groups  $G \rightarrow H$  induces a surjection  $SK_1(\mathbb{Z}G) \rightarrow SK_1(\mathbb{Z}H)$ .

**(48.6) Theorem (Alperin-Dennis-Oliver-Stein).** *Let  $G$  be an abelian group. Then  $SK_1(\mathbb{Z}G) = 1$  in precisely the following cases:*

- (i)  *$G$  = elementary abelian 2-group,*
- (ii) *All Sylow subgroups of  $G$  are cyclic,*
- (iii) *For each  $p$ , the Sylow  $p$ -subgroup of  $G$  has the form  $C_p \times C_{p^n}$  for some  $n \geq 1$ , where  $C_m$  denotes a cyclic group of order  $m$ .*

<sup>†</sup>This result holds even when  $G$  is non-abelian, provided  $H$  is abelian; see Magurn [78a]. However, as shown by Oliver, the result may fail without such hypothesis on  $H$ .

This theorem, used in conjunction with Oliver's Theorem and a result of Obayashi, allows us to prove the triviality of  $SK_1(\mathbb{Z}G)$  in most of the known cases. For example, we obtain:

**(48.7) Theorem** (Magurn [78b]). *For  $D_n$  the dihedral group of order  $2n$ , we have  $SK_1(\mathbb{Z}D_n) = 1$ .*

*Proof.* The elementary subgroups  $H$  of  $D_n$  are either cyclic or of the form  $C_2 \times C_2$ , or possibly a dihedral 2-group. In the first two cases we know that  $SK_1(\mathbb{Z}H) = 1$  by (48.6). For a dihedral 2-group  $H$  we again have  $SK_1(\mathbb{Z}H) = 1$  by Obayashi [73]. Therefore  $SK_1(\mathbb{Z}D_n) = 1$  by Oliver's Theorem 48.2.

**(48.8) Theorem.** *If  $p^3 \mid |G|$  then  $SK_1(\mathbb{Z}G)$  is  $p$ -torsionfree.*

*Proof.* Let  $G_p$  be a Sylow  $p$ -subgroup of  $G$ ; then  $|G_p| \leq p^2$ , so  $G_p$  is either  $C_{p^2}$  or  $C_p \times C_p$ . Each  $p$ -elementary subgroup  $H$  of  $G$  is therefore a subgroup of  $C \times G_p$  for some cyclic  $p'$ -group  $C$ . But then  $SK_1(\mathbb{Z}H) = 1$  by (48.6), so the desired result follows from Oliver's Theorem.

A similar argument yields another proof of (48.5iii) for the case  $R = \mathbb{Z}$ ; we have the details as an exercise for the reader.

Next, we list some cases where  $SK_1(\mathbb{Z}G)$  is known explicitly. The following results are stated in Stein [78]:

- (1) Let  $G$  be an elementary abelian  $p$ -group of rank  $k$ , where  $p$  is an odd prime. Then  $SK_1(\mathbb{Z}G)$  is also an elementary abelian  $p$ -group, of rank

$$\frac{p^k - 1}{p - 1} - \binom{p + k - 1}{p},$$

which is positive for  $k \geq 3$ . The proof is sketched in Alperin-Dennis-Stein [73]. For full details, see Alperin-Dennis-Oliver-Stein [86].

- (2) For  $G$  abelian, the calculation of  $SK_1(\mathbb{Z}G)$  can be reduced to that of  $SK_1(\mathbb{Z}G_p)$ , with  $G_p$  ranging over the Sylow subgroups of  $G$ . For the proof, see Alperin-Dennis-Stein [85].
- (3) Let  $C_n$  denote a cyclic group of order  $n$ , and  $p$  an odd prime. As shown in Alperin-Dennis-Oliver-Stein [86], the following table gives the structure of  $SK_1(\mathbb{Z}G)$ :

$G$	$SK_1(\mathbb{Z}G)$
$C_{p^2} \times C_{p^n}, \quad n \geq 1$	$C_p^{(p-1)(n-1)}$
$C_{p^n} \times C_p \times C_p, \quad n \geq 1$	$C_p^{np(p-1)/2}$
$C_{p^3} \times C_{p^3}$	$C_p^{(p^2-1)} \times C_{p^2}^{(p-1)}$
$C_3 \times C_9 \times C_9$	$C_3^{(15)} \times C_9^{(2)}$
$C_8 \times C_8$	$C_2^{(4)}$
$C_4 \times C_4$	$C_2$
$C_2 \times C_2 \times C_4$	$C_2$
$C_2 \times C_2 \times C_2 \times C_4$	$C_2^{(3)} \times C_4$

The cases where  $G = C_{p^n} \times C_p^{(3)}$  and  $G = C_{2^n} \times C_2^{(k)}$  have also been worked out explicitly in the above reference.

To conclude this brief survey, we quote some results of Oliver [80b].

- (4) For odd  $p$ , there exist groups  $G$  of order  $p^5$  for which  $SK_1(\mathbb{Z}_p G) \neq 1$ , where  $\mathbb{Z}_p$  is the ring of  $p$ -adic integers.  
For  $p = 2$ , there is a group  $G$  of order 64 with  $SK_1(\mathbb{Z}_2 G) \neq 1$ .
- (5) Let  $R$  be a  $p$ -adic ring, and  $G$  a  $p$ -group. Then

$$SK_1(RG) \cong H_2(G)/H_2^{ab}(G),$$

where  $H_2(G)$  is the Schur multiplier of  $G$ , and  $H_2^{ab}(G)$  is the subgroup of  $H_2(G)$  generated by the image of all  $\{H_2(A)\}$ , where  $A$  ranges over the abelian subgroups of  $G$ .

In particular,  $SK_1(RG)$  is independent of  $R$ .

# Class Groups of Integral Group Rings and Orders

In this chapter we shall define the locally free class group  $\text{Cl } \Lambda$  of an order  $\Lambda$ , with special emphasis on the case  $\Lambda = \mathbb{Z}G$ ,  $G$  a finite group. The class group  $\text{Cl } \mathbb{Z}G$  was introduced by Swan [60], as the kernel of the rank homomorphism  $K_0(\mathbb{Z}G) \rightarrow \mathbb{Z}$ . Most of the applications to topology and algebraic number theory, for which we refer the reader to the references listed at the end of this introduction, involve the group ring case. Further, most of the detailed calculations of class groups in §§50–54 are for this special case.

However, many of the techniques for determining  $\text{Cl } \mathbb{Z}G$  depend on reducing the problem to the calculation of  $\text{Cl } \Lambda$ , for various orders  $\Lambda$  which are *not* group rings. For more general orders,  $\text{Cl } \Lambda$  was first studied by Jacobinski [68] in his fundamental work on genera of lattices. His results were recast by Fröhlich [75] in terms of idèles, and it is this idèle version which we shall use most often. Fröhlich [76] later reformulated this approach, obtaining the “Hom formula” for  $\text{Cl } \Lambda$  given in §52.

This chapter is largely independent of Chapter 5, except that in §49A we derive the basic formulas for class groups by using the Localization Sequence 40.9 of algebraic  $K$ -theory. We shall also need some facts about reduced norms and their connection with  $K_1$ , as described in §45.

In §49A, we derive the main formulas for the locally free class group  $\text{Cl } \Lambda$  of an order  $\Lambda$  (in a f.d. separable algebra), and introduce the *kernel group*  $D(\Lambda)$  which measures the discrepancy between  $\text{Cl } \Lambda$  and  $\text{Cl } \Lambda'$ , where  $\Lambda'$  is a maximal order containing  $\Lambda$ . Since  $\text{Cl } \Lambda'$  is easily described in practice, much of the effort lies in determining  $D(\Lambda)$ . We briefly discuss the functorial properties of  $\text{Cl } \Lambda$  and  $D(\Lambda)$  in §49B, C.

The lengthy §50 gives many examples of the calculation of  $\text{Cl } \mathbb{Z}G$  and  $D(\mathbb{Z}G)$ , starting with the case in §50A where  $G$  is cyclic of squarefree order. In §50F, we treat the much harder case of cyclic  $p$ -groups. Metacyclic groups are studied in §50C, while §50D is devoted to dihedral and quaternion groups. The section concludes in §50G with the important result, due to Wilson, that  $D(\Lambda) = 0$  for  $\Lambda$  a twisted group ring, or more generally, a crossed-product order.

In §51A we prove the fundamental Jacobinski Cancellation Theorem, following a new approach by Swan [80]. Section 52 is devoted to Fröhlich’s

“Hom formula”  $\text{Cl } RG$ , which plays a key role in Taylor’s calculation of the Swan subgroup  $T(G)$  of  $\text{Cl } ZG$ , where  $G$  is any  $p$ -group (see §54). The chapter concludes with §55 on Picard groups of orders, where one studies invertible two-sided ideals of an order, rather than locally free one-sided ideals.

The reader will find that some of the calculations in §50 rely heavily on results from algebraic number theory. Even the special case of calculating  $D(ZG)$ , where  $G$  is a cyclic group of order  $p^2$ , already leads to difficult questions about cyclotomic fields (see §50F). On the other hand, the locally free class group  $\text{Cl } ZG$  (for arbitrary  $G$ ) has important applications to questions in algebraic number theory, especially those connected with the existence of normal integral bases (see (52.14) and §53B). For a systematic treatment of such applications, we refer the reader to the fundamental works of Fröhlich [83], [84], and to the references listed therein.

It is beyond the scope of this book to treat the many applications of locally free class groups to problems in algebraic topology. In the introduction to Chapter 5, we have already listed a number of references in which algebraic K-theory is applied to topological problems. Here, we list further references, more closely connected with topological applications of class groups. The authors wish to thank R. Oliver and J. Arnold for helpful comments.

To begin with, let  $X$  be a CW-complex with fundamental group  $G$ . There is a “Swan-Wall invariant”, with values in  $\text{Cl } ZG$ , measuring the obstruction to  $X$  being homotopy equivalent to a finite CW-complex. For details, see Swan [60b], Wall [65], [66].

The above problem is connected with that of determining which finite groups can act freely on a sphere. For this topic, see Swan [60b], Thomas [81], Milgram [81], [82], Madsen [83].

In some topological problems, there is an obstruction taking values in  $\text{Cl}(ZG)/T(G)$ , where  $T(G)$  is the Swan subgroup. In this connection, see Swan [60b], Endo-Miyata [73–74], Oliver [78].

## §49. LOCALLY FREE CLASS GROUPS

### §49A. Basic Formulas

Throughout this section, let  $\Lambda$  be an  $R$ -order in a f.d. separable  $K$ -algebra  $A$ , where  $R$  is a Dedekind domain with quotient field  $K$ . Usually  $K$  will be taken to be a global field. Let  $P$  range over the maximal ideals of  $R$ , and let  $\Lambda_P$ ,  $A_P$ , etc., denote  $P$ -adic completions (rather than localizations at  $P$ ). Further, we denote by  $\Lambda_P^\times$  the group of units of  $\Lambda_P$ , and by  $A_P^\times$  that of  $A_P$ .

Let us begin by reviewing some definitions and results from §31. A  $\Lambda$ -lattice is a left  $\Lambda$ -module which is f.g. and projective as  $R$ -module. For any  $\Lambda$ -lattice  $M$ , we identify  $M$  with its image  $1 \otimes M$  in  $K \otimes_R M$ ; then we may write  $K \otimes_R M = KM$ , a left  $A$ -module. Two  $\Lambda$ -lattices  $M$  and  $N$  are in the same genus, or are locally isomorphic, if  $M_P \cong N_P$  as  $\Lambda_P$ -modules for each  $P$ ; we write  $M \vee N$  in this case. If  $M \vee N$ , then after replacing  $N$  by an isomorphic copy, we may assume that  $KM = KN$ .

Now define

$$(49.1) \quad S(\Lambda) = \{P: \Lambda_P \neq \text{maximal } R_P\text{-order in } A_P\},$$

so  $S(\Lambda)$  is a finite set of maximal ideals of  $R$ , and  $S(\Lambda)$  is empty if and only if  $\Lambda$  is a maximal order. By (31.2), the genus of a  $\Lambda$ -lattice  $M$  is determined by the isomorphism classes of the modules  $\{M_P: P \in S(\Lambda)\}$ . If  $\Lambda$  is a maximal order, the genus of  $M$  is determined by the isomorphism class of  $KM$ .

In (31.7) we showed how to “add” lattices in a given genus:

**(49.2) Proposition.** *Let  $L, M$ , and  $N$  be  $\Lambda$ -lattices in the same genus. Then there exists a  $\Lambda$ -lattice  $L'$  in the genus, such that*

$$M \oplus N \cong L \oplus L'.$$

In the same vein, decomposability is a property of genera (see (31.13) and (31.14)):

**(49.3) Proposition.** *If  $L, M$ , and  $N$  are arbitrary  $\Lambda$ -lattices such that  $L \vee (M \oplus N)$ , then  $L \cong M' \oplus N'$  for some  $M' \vee M$  and some  $N' \vee N$ . In particular, if  $L \vee M^{(r)}$  for some  $r$ , then*

$$L \cong M^{(r-1)} \oplus M' \quad \text{for some } M' \vee M.$$

For most of the discussion, we shall concentrate on the *principal genus*<sup>†</sup>  $g(\Lambda)$ , consisting of all  $\Lambda$ -lattices in the genus of  $\Lambda$ . We do this because if  $M$  is an arbitrary  $\Lambda$ -lattice, the study of  $\Lambda$ -lattices in the genus<sup>†</sup>  $g(M)$  of  $M$  reduces at once to the study of locally free left ideals in the  $R$ -order  $\text{End}_\Lambda M$ . Thus, for the most part, it suffices to treat the genus associated with an *order*, rather than with a *lattice*.

Now let  $M \in g(\Lambda)$ ; after replacing  $M$  by an isomorphic copy if need be, we may assume that  $M \subset A$ . We call  $M$  a *locally free* left  $\Lambda$ -ideal in  $A$ . Each such  $M$  is projective as  $\Lambda$ -module, by (8.19). Let  $P$  range over the maximal ideals of  $R$ . For each  $P$ , we may write

$$M_P = \Lambda_P \alpha_P \quad \text{for some } \alpha_P \in A_P^\times.$$

Since  $M_P = \Lambda_P$  a.e., we have  $\alpha_P \in \Lambda_P^\times$  a.e. Let  $\alpha = (\alpha_P) \in \prod_P A_P^\times$  be an *idèle*, and view  $\alpha$  as an element of the *idèle group*

$$(49.4) \quad J(A) = \{(\alpha_P) \in \prod_P A_P^\times: \alpha_P \in \Lambda_P^\times \text{ a.e.}\}.$$

As remarked in the discussion following (31.17),  $J(A)$  does not depend on the

<sup>†</sup>*Caution:* The notation is different from that used in §31, where  $\Gamma_M$  denoted the genus of  $M$ , and where  $g(M)$  denoted the number of isomorphism classes in  $\Gamma_M$ .

choice of the  $R$ -order  $\Lambda$  in  $A$ . Further, given the idèle  $\alpha$ , we may recover the  $\Lambda$ -lattice  $M$  by the formula  $M = \Lambda\alpha$ , where by definition

$$(49.5) \quad \Lambda\alpha = A \cap \{\cap_p \Lambda_p \alpha_p\}.$$

As shown in (31.18), for  $\alpha, \beta \in J(A)$  we have

$$(49.6) \quad \Lambda\alpha \cong \Lambda\beta \text{ as } \Lambda\text{-lattices} \Leftrightarrow \beta \in U(\Lambda) \cdot \alpha \cdot u(A),$$

where

$$(49.7) \quad \begin{cases} U(\Lambda) = \text{group of unit idèles} = \prod_p \Lambda_p^*, \\ u(A) = \text{group of principal idèles} = \text{image of } A^\times \text{ in } J(A). \end{cases}$$

We shall return to this equivalence (49.6) later.

Our next step is to define the locally free class group of  $\Lambda$ , denoted by  $\text{Cl } \Lambda$ . We begin by observing that “addition” of lattices in the genus  $g(\Lambda)$ , as given in (49.2), can be put into a more appealing form using idèle notation. Up to isomorphism, each  $M \in g(\Lambda)$  is of the form  $M = \Lambda\alpha$ ,  $\alpha \in J(A)$ . As shown in (31.19), we have

$$(49.8) \quad \Lambda\alpha \oplus \Lambda\beta \cong \Lambda \oplus \Lambda\alpha\beta \quad \text{for } \alpha, \beta \in J(A).$$

Thus, the isomorphism classes of  $\Lambda\alpha$  and  $\Lambda\beta$  uniquely determine that of  $\Lambda \oplus \Lambda\alpha\beta$ . However, as pointed out at the end of §31B, an example due to Swan [62] shows that the isomorphism class of  $\Lambda\alpha\beta$  need not be uniquely determined, since “cancellation” need not hold. To overcome this difficulty, let us recall the concept of stable isomorphism, already encountered on pages 15 and 78.

For  $X, Y \in \mathcal{P}(\Lambda)$ , call  $X$  stably isomorphic to  $Y$  if

$$(49.9) \quad X \oplus \Lambda^{(k)} \cong Y \oplus \Lambda^{(k)} \quad \text{for some } k \geq 0,$$

or equivalently, if  $[X] = [Y]$  in  $K_0(\Lambda)$ . Let  $[X]$  denote the stable isomorphism class of  $X$ , and let

$$(49.10) \quad \text{Cl } \Lambda = \{[X] : X \in g(\Lambda)\} = \text{locally free class group of } \Lambda.$$

Note that by (6.15), stably isomorphic lattices must lie in the same genus. Now let  $X_1, X_2 \in g(\Lambda)$ ; by (49.2) we have

$$X_1 \oplus X_2 \cong \Lambda \oplus X_3 \quad \text{for some } X_3 \in g(\Lambda).$$

It is easily seen that the stable isomorphism class  $[X_3]$  is uniquely determined by the classes  $[X_1]$  and  $[X_2]$ . Indeed, let  $k$  be such that

$$X_i \oplus \Lambda^{(k)} \cong Y_i \oplus \Lambda^{(k)}, \quad i = 1, 2, \quad \text{and let} \quad Y_1 \oplus Y_2 \cong \Lambda \oplus Y_3.$$

Then

$$X_3 \oplus \Lambda^{(2k+1)} \cong X_1 \oplus X_2 \oplus \Lambda^{(2k)} \cong Y_1 \oplus Y_2 \oplus \Lambda^{(2k)} \cong Y_3 \oplus \Lambda^{(2k+1)},$$

so  $[X_3] = [Y_3]$  as claimed.

We now define a group law on  $\text{Cl } \Lambda$  by the formula

$$[X_1] + [X_2] = [X_3] \quad \text{whenever } X_1 \oplus X_2 \cong \Lambda \oplus X_3,$$

where  $X_1, X_2 \in g(\Lambda)$ . This is now a well-defined commutative and associative operation, with identity element  $[\Lambda]$ . Further, inverses exist since

$$\Lambda\alpha \oplus \Lambda\alpha^{-1} \cong \Lambda \oplus \Lambda \quad \text{for } \alpha \in J(A).$$

Thus,  $\text{Cl } \Lambda$  is an abelian additive group, and formula (49.8) now states that there is a surjective homomorphism

$$J(A) \rightarrow \text{Cl } \Lambda, \quad \text{given by } \alpha \in J(A) \mapsto [\Lambda\alpha] \in \text{Cl } \Lambda.$$

**(49.11) Remarks.** (i) By the Bass Cancellation Theorem 41.20, two lattices  $X, Y \in g(\Lambda)$  are stably isomorphic if and only if  $X \oplus \Lambda \cong Y \oplus \Lambda$ , so it suffices to take  $k = 1$  in (49.9). We shall give another proof of this fact in §51, when  $K$  is a global field, by using the Jacobinski Cancellation Theorem 51.24. We shall also see (in (51.24)) that when  $\Lambda$  satisfies the Eichler condition, then stable isomorphism implies isomorphism for lattices in  $g(\Lambda)$ .

(ii) For  $K$  a global field, the Jordan-Zassenhaus Theorem tells us that the number of isomorphism classes of left ideals of  $\Lambda$  is finite. Therefore  $\text{Cl } \Lambda$  is a finite abelian group in this case.

(iii) Our discussion shows that for arbitrary  $K$ , there is a surjective homomorphism

$$J(A) \rightarrow \text{Cl } \Lambda,$$

whose kernel contains both the unit idèles  $U(\Lambda)$  and the principal idèles  $u(A)$ . Since  $\text{Cl } \Lambda$  is abelian, the kernel must also contain the commutator group  $[J(A), J(A)]$ . We shall see in (49.22) that when  $K$  is a global field, we have

$$J(A)/J_0(A)A^\ast U(\Lambda) \cong \text{Cl } \Lambda,$$

where  $J_0(A)$  is the kernel of the reduced norm acting on  $J(A)$ .

(iv) The locally free class group was first introduced by Swan [60] for the special case where  $\Lambda$  is an integral group ring  $RG$ , with  $R = \text{alg. int. } \{K\}$ . Let  $SK_0(\Lambda)$  denote the kernel of the map  $K_0(\Lambda) \rightarrow K_0(A)$  defined by  $K \otimes_R *$ ; we shall call  $SK_0(\Lambda)$  the *reduced projective class group*. It is often denoted by  $\tilde{K}_0(\Lambda)$  in the literature.

For the case  $\Lambda = RG$ , we show at once that

$$\mathrm{Cl}\Lambda \cong SK_0(\Lambda).$$

Each  $x \in SK_0(\Lambda)$  is expressible as  $x = [\Lambda^{(r)}] - [M]$  for some  $r \geq 0$  and some  $M \in \mathcal{P}(\Lambda)$ , with  $KM \cong A^{(r)}$ . By Swan's Theorem 32.11, we have  $M \vee \Lambda^{(r)}$ , so by (49.3) we obtain  $M \cong \Lambda^{(r-1)} \oplus X$  for some  $X \vee \Lambda$ . Therefore  $x = [\Lambda] - [X]$ , and the isomorphism is given by

$$[X] \in \mathrm{Cl}\Lambda \rightarrow [\Lambda] - [X] \in SK_0(\Lambda).$$

Of course, we cannot expect such an isomorphism to hold for arbitrary orders  $\Lambda$  which are not group rings.

We now return to an arbitrary order  $\Lambda$ , and for brevity we shall call  $\mathrm{Cl}\Lambda$  the *class group* of  $\Lambda$ . For arbitrary  $\Lambda$ , this group was first defined by Jacobinski [68], in his fundamental work on genera of lattices. He used a deep result of Eichler to obtain an explicit formula for  $\mathrm{Cl}\Lambda$ . Later Fröhlich [75] gave an idèle-theoretic version of the formula, somewhat easier to use in practice. Wilson [77a] then used the Localization Sequence from algebraic  $K$ -theory to obtain a formula for  $\mathrm{Cl}\Lambda$  in terms of the idèle group  $JK_1(A)$ . For the case where  $K$  is a global field, the reduced norm map allows one to eliminate the  $K_1$ -groups and to obtain Fröhlich's formula. Another approach, given independently by C. T. C. Wall [74], obtains the formula by using the Mayer-Vietoris sequence associated with the Wall square (see (42.19)). More recently, Fröhlich [76] gave a "Hom" description of  $\mathrm{Cl}\Lambda$ , in terms of certain groups of homomorphisms (see §52). This version has played a fundamental role in applications of  $\mathrm{Cl}\Lambda$  to algebraic number theory (see Fröhlich [83]).

We now give the Wilson-Wall approach to  $\mathrm{Cl}\Lambda$  via algebraic  $K$ -theory. The Localization Sequence (40.9) gives an exact sequence

$$(49.12) \quad K_1(\Lambda) \rightarrow K_1(A) \rightarrow K_0(\mathcal{T}) \rightarrow K_0(\Lambda) \xrightarrow{\varphi} K_0(A),$$

where  $\mathcal{T}$  is the category of all f.g.  $R$ -torsion  $\Lambda$ -modules  $M$  of finite homological dimension. It should be stressed that the existence of such a sequence is a rather formal result, requiring little more than the definitions of the  $K$ -groups involved, and valid in much more general circumstances than the case of orders in algebras.

For each maximal ideal  $P$  of  $R$ , let  $\mathcal{T}_P$  be the category of f.g.  $P$ -torsion  $\Lambda_P$ -modules of finite homological dimension. Each  $M \in \mathcal{T}$  is expressible as a finite direct sum

$$M = \bigoplus_P M_P, \quad \text{where } M_P \in \mathcal{T}_P \quad \text{and} \quad M_P = 0 \quad \text{a.e.}$$

(Indeed,  $M_P$  is just the  $P$ -primary component of  $M$ .) This gives an isomorphism

$$\beta: K_0(\mathcal{T}) \cong \coprod_P K_0(\mathcal{T}_P)$$

We set

$$SK_0(\Lambda) = \ker \varphi, \quad \text{where } \varphi: K_0(\Lambda) \rightarrow K_0(A).$$

From (49.12) we obtain an exact sequence

$$1 \rightarrow K_1(A)/\text{im } K_1(\Lambda) \rightarrow K_0(\mathcal{T}) \rightarrow SK_0(\Lambda) \rightarrow 0.$$

Similarly, for each  $P$  there is such a sequence, with  $A, \Lambda$ , and  $\mathcal{T}$  replaced by  $A_P, \Lambda_P$ , and  $\mathcal{T}_P$ , respectively.

**(49.13) Lemma.** *There is a commutative diagram with exact rows:*

$$\begin{array}{ccccccc} 1 & \longrightarrow & K_1(A)/\text{im } K_1(\Lambda) & \longrightarrow & K_0(\mathcal{T}) & \longrightarrow & SK_0(\Lambda) & \longrightarrow 0 \\ & & \alpha \downarrow & & \beta \downarrow & & \gamma \downarrow & \\ 1 & \longrightarrow & \coprod_P K_1(A_P)/\text{im } K_1(\Lambda_P) & \longrightarrow & \coprod_P K_0(\mathcal{T}_P) & \longrightarrow & \coprod_P SK_0(\Lambda_P) & \longrightarrow 0. \end{array}$$

*Proof.* We have just seen that  $\beta$  is an isomorphism. To show that  $\gamma$  is well-defined, note that the map  $SK_0(\Lambda) \rightarrow SK_0(\Lambda_P)$  is defined for each  $P$ , and we must show that  $\gamma$  maps  $SK_0(\Lambda)$  into the direct sum of the  $\{SK_0(\Lambda_P)\}$ . Each  $x \in SK_0(\Lambda)$  is expressible as

$$x = [X] - [Y], \quad \text{with } X, Y \in \mathcal{P}(\Lambda) \quad \text{and} \quad KX = KY.$$

Then  $X_P = Y_P$  a.e., and

$$\gamma(x) = \sum_P ([X_P] - [Y_P]),$$

a finite sum. Thus  $\gamma$  and  $\beta$  are both well-defined, and induce a map  $\alpha$  as shown. By the Snake Lemma, it follows that  $\alpha$  is injective,  $\gamma$  is surjective, and  $\ker \gamma \cong \text{cok } \alpha$ , facts needed below.

**(49.14) Corollary.** *There is an exact sequence*

$$1 \rightarrow K_1(A)/\text{im } K_1(\Lambda) \xrightarrow{\alpha} \coprod_P K_1(A_P)/\text{im } K_1(\Lambda_P) \xrightarrow{\partial} \text{Cl } \Lambda \rightarrow 0,$$

with  $\partial$  defined below.

*Proof.* Keeping the notation of (49.13), it suffices to establish an isomorphism

$$(49.15) \quad \theta: \text{Cl } \Lambda \cong \ker \gamma.$$

By the final remark in the proof of (49.13), we have  $\ker \gamma \cong \text{cok } \alpha$ , so we need only use the machinery of the Snake Lemma to define the map  $\partial$ .

To begin with, there is an injective map  $\theta: \text{Cl } \Lambda \rightarrow \ker \gamma$ , given by  $\theta[M] = [\Lambda] - [M]$  for  $M \in g(\Lambda)$ . We show that  $\theta$  is a homomorphism: if  $M_1, M_2 \in g(\Lambda)$ , then in  $\text{Cl } \Lambda$  we have

$$[M_1] + [M_2] = [M_3], \quad \text{where } M_1 \oplus M_2 \cong \Lambda \oplus M_3.$$

It follows at once that  $\theta[M_1] + \theta[M_2] = \theta[M_3]$ , so  $\theta$  is a well-defined injective homomorphism. To show  $\theta$  surjective, let  $x = [\Lambda^{(k)}] - [Y] \in \ker \gamma$ , where  $Y \in \mathcal{P}(\Lambda)$ . From  $\gamma(x) = 0$  we obtain  $\Lambda_P^{(k)} \cong Y_P$  for all  $P$ , so  $Y \vee \Lambda^{(k)}$ , and therefore  $Y \cong \Lambda^{(k-1)} \oplus M$  for some  $M \in g(\Lambda)$ , by (49.3). But then  $x = [\Lambda] - [M] = \theta[M]$ , as desired.

The homomorphism  $\partial$  is obtained via composition of maps

$$\text{cok } \alpha \cong \ker \gamma \cong \text{Cl } \Lambda,$$

and can be described explicitly as follows. Since  $A_P^*$  maps onto  $K_1(A_P)$  by (40.31), each  $x$  in the domain of  $\partial$  can be represented as the class of a product  $\prod a_P$ , where  $a_P \in A_P^*$  for each  $P$ , and  $a_P = 1$  a.e. Let  $a = (a_P) \in J(A)$  be the corresponding idèle, and choose a nonzero  $r \in R$  such that  $b_P = r a_P \in \Lambda_P$  for each  $P$ . Set  $b = (b_P) \in J(A)$ . Then the image  $\partial(x)$  of  $x$  in  $\text{Cl } \Lambda$  is  $\partial(b) - \partial(r)$ , where  $b$  and  $r$  are viewed as elements in the domain of  $\partial$ . From the proof of (40.9), the image of  $b$  in  $\coprod_P K_0(\mathcal{T}_P)$  is  $\sum_P [\Lambda_P / \Lambda_P b_P]$ . We then have

$$\beta^{-1} \sum [\Lambda_P / \Lambda_P b_P] = [\Lambda / \Lambda b] \text{ in } K_0(\mathcal{T}),$$

with  $\Lambda b$  defined as in (49.5). The map  $K_0(\mathcal{T}) \rightarrow SK_0(\Lambda)$  carries  $[\Lambda / \Lambda b]$  onto  $[\Lambda] - [\Lambda b]$ , and  $\theta^{-1}$  maps this latter expression onto  $[\Lambda b] \in \text{Cl } \Lambda$ . This gives  $\partial(b) = [\Lambda b]$ , and similarly  $\partial(r) = [\Lambda r]$ . Therefore

$$\partial(x) = [\Lambda b] - [\Lambda r] = [\Lambda b r^{-1}] = [\Lambda a] \in \text{Cl } \Lambda,$$

by (49.8). In short, if  $x$  is the class of an idèle  $a \in J(A)$ , then  $\partial(x) = [\Lambda a] \in \text{Cl } \Lambda$ . This completes the proof.

**Remark.** We had previously defined the locally free class group  $\text{Cl } \Lambda$ , in (39.12), as the kernel of the homomorphism

$$K_0(\Lambda) \rightarrow \prod_P K_0(\Lambda_P).$$

It is easily seen that this kernel coincides with  $\ker \gamma$ , where  $\gamma$  is the map occurring in (49.13). Thus, the class group as defined in (39.12) is isomorphic to our current version (49.10), and we shall almost always use  $\text{Cl } \Lambda$  in the sense of (49.10) in this chapter.

In our earlier discussion of the class group  $\text{Cl } \Lambda$ , and again in proving (49.14),

the idèle group  $J(A)$  played a vital role. Our next aim is to refine (49.14) so as to obtain an explicit formula for  $\text{Cl}\Lambda$  in terms of the *idèle group*  $JK_1(A)$  of  $K_1(A)$  relative to  $R$ . Later, we shall use properties of reduced norms to eliminate the occurrences of the  $K_1$ -groups, in the special case where  $A$  is an algebra over a *global field*  $K$ .

By definition, the idèle group  $JK_1(A)$  of  $K_1(A)$  relative to  $R$  is given by

$$JK_1(A) = \left\{ (x_p) \in \prod_p K_1(A_p) : x_p \in \text{im } K_1(\Lambda_p) \text{ a.e.} \right\}.$$

This group is independent of the choice of the  $R$ -order  $\Lambda$  in  $A$ , since if  $\Lambda'$  is another such order, then  $\Lambda_p = \Lambda'_p$  a.e. We also introduce the group of *unit idèles*

$$UK_1(\Lambda) = \prod_p K_1(\Lambda_p).$$

The maps  $K_1(\Lambda_p) \rightarrow K_1(A_p)$ , as  $P$  varies, give rise to a homomorphism  $UK_1(\Lambda) \rightarrow JK_1(A)$ . Since

$$JK_1(A) = \left( \coprod_p K_1(A_p) \right) \cdot \text{im } UK_1(\Lambda),$$

we obtain

$$\frac{JK_1(A)}{\text{im } UK_1(\Lambda)} \cong \coprod_p \frac{K_1(A_p)}{\text{im } K_1(\Lambda_p)}.$$

Next, the maps  $A \rightarrow A_p$  (for each  $P$ ) yield a homomorphism from  $K_1(A)$  into the direct product  $\prod_p K_1(A_p)$ . Further, for  $x \in K_1(A)$ , we may represent  $x$  by a matrix  $X \in GL(A)$ , and then clearly  $X \in GL(\Lambda_p)$  a.e. Thus we obtain the homomorphism  $\alpha$  given in (49.14), carrying  $x$  onto the class of the principal idèle  $(x)$  in  $\coprod_p K_1(A_p)/\text{im } K_1(\Lambda_p)$ . Consequently, we may reformulate (49.14) as follows:

**(49.16) Proposition.** *There is an isomorphism of groups*

$$\frac{JK_1(A)}{\text{im } K_1(A) \cdot \text{im } UK_1(\Lambda)} \cong \text{Cl}\Lambda,$$

given by representing each element of the left-hand side by an idèle  $a \in J(A)$ , and then mapping the element onto the class  $[\Lambda a]$  of the locally free ideal  $\Lambda a$  defined as in (49.5).

The preceding results give formulas for  $\text{Cl}\Lambda$ , where  $\Lambda$  is an  $R$ -order in a f.d. separable  $K$ -algebra  $A$ , with arbitrary ground field  $K$ . In the case where  $K$  is a global field, however, we may obtain a simpler expression for the class group  $\text{Cl}\Lambda$ , by using reduced norms to get rid of the  $K_1$  groups. The following basic formula is due to Fröhlich [75], and is the idèle-theoretic version of an earlier formula of Jacobinski [68b]:

**(49.17) Theorem.** *Let  $K$  be a global field, and let  $\Lambda$  be an  $R$ -order in a separable f.d.  $K$ -algebra  $A$ . Let  $C$  be the center of  $A$ , and  $J(C)$  its idèle group defined as in (49.4). Then we have*

$$\text{Cl } \Lambda \cong \frac{J(C)}{C^+ \cdot \prod_P \text{nr } \Lambda_P^+},$$

where  $C^+$  is the subgroup of  $C^\circ$  (viewed as principal idèles) given in (45.9), and where  $\text{nr}$  is the reduced norm map.

*Proof.* The reduced norm map  $\text{nr}$  maps  $A^\circ$  onto  $C^+$ , by the Hasse-Schilling-Maass Theorem 7.48. On the other hand, for each  $P$ , it follows from Exercise 49.1 that  $A_P$  is a  $K_P$ -algebra with center  $C_P$ , so there is a reduced norm map  $A_P^\circ \rightarrow C_P^\circ$ , again denoted by  $\text{nr}$ . This map is surjective by (7.45).

As shown in §45A, the reduced norm map induces isomorphisms

$$(49.18) \quad \text{nr}: K_1(A) \cong C^+, \quad \text{nr}: K_1(A_P) \cong C_P^\circ$$

for each  $P$ . The first of these is a much deeper result, depending on the Wang-Platonov Theorem; see (45.3). However, we do not require the full force of this isomorphism, but only the weaker fact that  $\text{nr } K_1(A) = C^+$ ; this follows readily from the Hasse-Schilling-Maass Norm Theorem (see §45A). The isomorphism given in the local case is an immediate consequence of the Nakayama-Matsushima Theorem 7.49; see (45.3).

Next, let  $\mathfrak{O}$  be the integral closure of  $R$  in  $C$ , so

$$J(C) = \{(c_P) \in \prod C_P^\circ : c_P \in \mathfrak{O}_P^\circ \text{ a.e.}\}.$$

If  $\Gamma_P$  is a maximal  $R_P$ -order in  $A_P$ , then by (45.8) we have

$$(49.19) \quad \text{nr } K_1(\Gamma_P) = \text{nr } \Gamma_P^\circ = \mathfrak{O}_P^\circ$$

for each  $P$ .

It follows from the results (in the local case) that  $\text{nr}$  induces an isomorphism  $JK_1(A) \cong J(C)$ . In this isomorphism, the group of principal idèles  $K_1(A)$  maps onto  $C^+$ , while the group of unit idèles  $UK_1(\Lambda)$  maps onto  $\prod_P \text{nr } K_1(\Lambda_P)$ . Since each element of  $K_1(\Lambda_P)$  is represented by an element of  $\Lambda_P$ , we have  $\text{nr } K_1(\Lambda_P) = \text{nr } \Lambda_P^\circ$ . The desired formula for  $\text{Cl } \Lambda$  is now a direct consequence of (49.16).

**(49.20) Remark.** Let  $K$  be a global field, and keep the above notation. By (40.31), the elements of  $K_1(A_P)$ ,  $K_1(A)$ , and  $K_1(\Lambda_P)$  are representable by  $1 \times 1$  matrices with entries in  $A_P^\circ$ ,  $A^\circ$ , and  $\Lambda_P$ , respectively. It follows at once that there is a surjection  $J(A) \rightarrow JK_1(A)$ , whose kernel we denote by  $J_0(A)$ . Thus

$$(49.21) \quad JK_1(A) \cong J(A)/J_0(A).$$

Next, the reduced norm  $\text{nr}: A \rightarrow C$  induces a map of idèle groups, and there is a commutative diagram

$$\begin{array}{ccc} J(A) & \longrightarrow & JK_1(A) \\ \text{nr} \searrow & & \downarrow \text{nr} \\ & & J(C) \end{array}$$

in which the vertical map is an isomorphism by (49.18). It follows at once that

$$J_0(A) = \{x \in J(A) : \text{nr } x = 1\}.$$

Note that  $J_0(A) \supseteq [J(A), J(A)]$  since  $JK_1(A)$  is abelian.

In the isomorphism (49.21), the image of  $K_1(A)$  in  $JK_1(A)$  maps onto  $A^\times$ , considered as the group of principal idèles in  $J(A)$ . Likewise, the image of  $UK_1(\Lambda)$  in  $JK_1(A)$  maps onto the group of unit idèles  $U(\Lambda)$  in  $J(A)$ , defined as in (49.7). From (49.16) and the isomorphism (49.21), we therefore obtain:

**(49.22) Theorem.** *Let  $K$  be a global field, and let  $\Lambda$  be an  $R$ -order in a f.d. separable  $K$ -algebra  $A$ . Then*

$$\text{Cl } \Lambda \cong \frac{J(A)}{J_0(A)A^\times U(\Lambda)},$$

where  $J_0(A) = \{x \in J(A) : \text{nr } x = 1\}$ .

Of course, applying  $\text{nr}$  to the right-hand expression above yields (49.17) at once.

It is sometimes desirable to use both finite and infinite primes in the idèle group of  $A$ . We conclude this subsection with a brief discussion of what happens to the formulas in (49.17) and (49.22) in this new context. Let  $R = \text{alg. int. } \{K\}$ , and write  $P|\infty$  to indicate that  $P$  is an infinite (archimedean) prime of  $K$ . For each such  $P$ , let  $C_P^+$  be the subgroup of  $C_P$  (of index a power of 2) such that

$$\text{nr } A_P^\times = C_P^+.$$

This subgroup is defined just as in (7.46) and (7.47), by first reducing to the case of central simple algebras, and then using (7.47) for the single prime  $P$ . As in §45A, we have  $\text{nr } K_1(A_P) = C_P^+$  for  $P|\infty$ .

We now define

$$J^*(C) = J(C) \times C_\infty^\times, \quad \text{where } C_\infty = \prod_{P|\infty} C_P,$$

$$U^*(\Lambda) = U(\Lambda) \times A_\infty^\times, \quad \text{where } A_\infty = \prod_{P|\infty} A_P,$$

so now

$$\text{nr } A_\infty^+ = C_\infty^+ = \prod_{P|\infty} C_P^+.$$

There is an obvious embedding of  $J(C)$  into  $J^*(C)$ , given by  $a \rightarrow a \times 1$  for  $a \in J(C)$ . There are now two diagonal embeddings of  $C^*$ , one in  $J(C)$ , the other in  $J^*(C)$ . Denoting these by  $i$  and  $i^*$ , respectively, we may write for  $c \in C$ :

$$i^*(c) = i(c) \times i_\infty(c), \quad \text{where } i_\infty(c) \in C_\infty^+.$$

We are now ready to establish the following result of Fröhlich [75]:

**(49.23) Theorem.** *Keeping the above notation, we have*

$$\text{Cl } \Lambda \cong \frac{J^*(C)}{i^*(C^*) \text{nr } U^*(\Lambda)}.$$

**Proof.** The existence of the desired isomorphism will follow from (49.17) once we show that the embedding  $J(C) \rightarrow J^*(C)$  induces an isomorphism

$$\theta: \frac{J(C)}{i(C^+) \text{nr } U(\Lambda)} \cong \frac{J^*(C)}{i^*(C^*) \text{nr } U^*(\Lambda)}.$$

The right-hand expression may be written as

$$\frac{J(C) \times C_\infty^+}{\{i(c) \times i_\infty(c) : c \in C\} \{\text{nr } U(\Lambda)\} C_\infty^+}.$$

To show  $\theta$  well-defined, note that for  $c \in C^+$  we have  $i_\infty(c) \in C_\infty^+$ , so

$$i(C^+) \subseteq i^*(C^*) C_\infty^+.$$

We show next that  $\theta$  is surjective, by proving that

$$C_\infty^+ \subseteq J(C) i^*(C^*) \text{nr } U^*(\Lambda).$$

Indeed, given  $b \in C_\infty^+$ , it follows from the Weak Approximation Theorem in valuation theory (see, for example, Weiss [63]) that there exists an element  $c \in C$  with  $bi_\infty(c) \in C_\infty^+$ . But therefore  $b \in J(C)i^*(C^*)C^+$ , as desired.

Finally, we prove that  $\theta$  is injective. Let  $a \in J(C)$  be such that

$$a \times 1 = i(c) \times i_\infty(c)(\text{nr } u)v \quad \text{for some } c \in C, \quad u \in U(\Lambda), \quad v \in C_\infty^+.$$

Then

$$a = i(c) \text{nr } u, \quad 1 = i_\infty(c)v.$$

Therefore  $i(c) \in C^+$ , which means that  $c \in C^+$ , so  $a \in i(C^+) \cap U(\Lambda)$  as desired. This shows that  $\theta$  is an isomorphism, and completes the proof of the theorem.

Analogously, formula (49.22) takes the form

$$(49.24) \quad \text{Cl } \Lambda \cong \frac{J^*(A)}{\tilde{J}(A) \cdot U^*(\Lambda)},$$

where  $\tilde{J}(A) = \{x \in J^*(A); \text{nr } x = 1\}$ . Fröhlich showed that  $\tilde{J}(A)$  coincides with the closure of the commutator subgroup of  $J^*(A)$  in the standard idèle topology, (see Exercise 51.1).

### Appendix to §49A

We briefly consider a “higher” locally free class group  $\text{Cl}_1(\Lambda)$ , used by Oliver [80a, b] in his calculations of  $SK_1$  of integral group rings. We have already used this concept in the proof of Theorem 45.17 above.

Let  $\Lambda$  be an  $R$ -order in a f.d. separable  $K$ -algebra  $A$ , where  $R$  is a Dedekind domain whose quotient field  $K$  is a global field. The group  $SK_0(\Lambda)$  is (by definition) the kernel of the homomorphism  $K_0(\Lambda) \rightarrow K_0(A)$ . For each maximal ideal  $P$  of  $R$ , the group  $SK_0(\Lambda_P)$  is defined analogously. As shown in (49.15), the locally free class group  $\text{Cl } \Lambda$  is isomorphic to  $\ker \gamma$ , where

$$\gamma: SK_0(\Lambda) \rightarrow \prod_P SK_0(\Lambda_P).$$

It seems natural to study the map

$$(49.24a) \quad \gamma_1: SK_1(\Lambda) \rightarrow \prod_P SK_1(\Lambda_P),$$

when  $SK_1(\Lambda)$  is the kernel of the homomorphism  $K_1(\Lambda) \rightarrow K_1(A)$ , with  $SK_1(\Lambda_P)$  defined analogously. We have already seen in (45.17) that  $SK_1(\Lambda_P) = 1$  a.e. We shall show below that  $\gamma_1$  is surjective, and following Oliver, we define

$$\text{Cl}_1 \Lambda = \ker \gamma_1,$$

a “higher” locally free class group. Of course,  $\text{Cl}_1 \Lambda$  is a finite abelian group.

We keep the notation of (49.13). There is a commutative diagram with exact rows:

$$\begin{array}{ccccccc} 1 & \longrightarrow & K_2(A)/\text{im } K_2(\Lambda) & \longrightarrow & K_1(\mathcal{T}) & \longrightarrow & K_1(\Lambda) \longrightarrow K_1(A) \\ & & \downarrow & & \downarrow 1 & & \downarrow \\ 1 & \longrightarrow & \prod_P K_2(A_P)/\text{im } K_2(\Lambda_P) & \longrightarrow & K_1(\mathcal{T}) & \longrightarrow & \prod_P K_1(\Lambda_P) \longrightarrow \prod_P K_1(A_P). \end{array}$$

This yields a similar diagram

$$\begin{array}{ccccccc} 1 & \longrightarrow & K_2(A)/\text{im } K_2(\Lambda) & \longrightarrow & K_1(\mathcal{T}) & \longrightarrow & SK_1(\Lambda) \longrightarrow 1 \\ & & \downarrow & & \downarrow 1 & & \downarrow \\ 1 & \longrightarrow & \prod_P K_2(A_P)/\text{im } K_2(\Lambda_P) & \longrightarrow & K_1(\mathcal{T}) & \longrightarrow & \prod_P SK_1(\Lambda_P) \longrightarrow 1. \end{array}$$

It follows at once that  $\gamma_1$  is surjective. Further, as in (49.13) and (49.14), we obtain an exact sequence

$$(49.24b) \quad 1 \rightarrow K_2(A)/\text{im } K_2(\Lambda) \rightarrow \prod_P K_2(A_P)/\text{im } K_2(\Lambda_P) \rightarrow \text{Cl}_1 \Lambda \rightarrow 1,$$

since  $\text{Cl}_1 \Lambda = \ker \gamma_1$ .

Anticipating the discussion in §49B, and (49.25) in particular, we prove:

**(49.24c) Theorem.** *Let  $\Lambda, \Gamma$  be  $R$ -orders in f.d. separable  $K$ -algebras  $A, B$ , respectively. Let  $\varphi: A \rightarrow B$  be a surjection of  $K$ -algebras such that  $\varphi(\Lambda) \subseteq \Gamma$ . Then  $\varphi$  induces a surjection  $\text{Cl}_1 \Lambda \rightarrow \text{Cl}_1 \Gamma$ .*

*Proof.* Since  $\varphi: A \rightarrow B$  is a split surjection of  $K$ -algebras, the induced homomorphism  $K_2(A) \rightarrow K_2(B)$  is surjective (and split). The same holds for the map  $K_2(A_P) \rightarrow K_2(B_P)$  for each  $P$ , and the desired result now follows from (49.24b).

**(49.24d) Corollary.** (i) If  $\Lambda \subseteq \Gamma$  are  $R$ -orders in  $A$ , then  $\text{Cl}_1 \Lambda$  maps onto  $\text{Cl}_1 \Gamma$ .

(ii) A surjection  $G \rightarrow \bar{G}$  of finite groups induces a surjection  $\text{Cl}_1 RG \rightarrow \text{Cl}_1 R\bar{G}$ .

**Remarks.** (i) For any abelian group  $G$  and any maximal ideal  $P$  of  $R$ , we have  $SK_1(R_P G) = 1$  by (45.12). We conclude that

$$\text{Cl}_1 RG = SK_1(RG) \quad \text{whenever } G \text{ is abelian.}$$

(ii) For  $p$  prime, let  $(\text{Cl}_1)_{(p)}$  denote the  $p$ -torsion subgroup of  $\text{Cl}_1$ . Oliver [80a] showed that for each group  $G$ ,

$$(\text{Cl}_1 ZG)_{(p)} = \sum_H \text{ind}_H^G (\text{Cl}_1 ZH)_{(p)},$$

where  $H$  ranges over all  $p$ -elementary subgroups of  $G$ .

(iii) Some further results of Oliver [80a]:

1.  $\text{Cl}_1 ZG \neq 0$  if  $G$  is a non-abelian  $p$ -group, where  $p$  is odd.
2.  $\text{Cl}_1 ZG = 0$  for  $G$  a dihedral or generalized quaternion 2-group.
3.  $\text{Cl}_1 ZG = 0$  if  $RG$  is a direct sum of matrix algebras over  $R$ , that is, every complex representation of  $G$  is realizable over  $R$  (see §73).

## §49B. Functorial Properties and the Kernel Group

As above, let  $\Lambda$  be an  $R$ -order in a f.d. separable  $K$ -algebra  $A$ , where for the moment the field  $K$  may be arbitrary. Our aim here is to develop some functorial

properties of the class group  $\text{Cl } \Lambda$ , especially those arising from homomorphisms from one order to another. These properties, whose proofs use the  $K$ -theoretic description of  $\text{Cl } \Lambda$  given in (49.16), will yield techniques for calculation of class groups in specific cases.

We saw in (49.16) that there is an isomorphism

$$\frac{\text{JK}_1(A)}{\text{im } K_1(A) \cdot \text{im } UK_1(\Lambda)} \cong \text{Cl } \Lambda,$$

where (by definition)

$$\begin{cases} \text{JK}_1(A) = \{(x_P) : x_P \in K_1(A_P) \text{ for all } P, \text{ and } x_P \in \text{im } K_1(\Lambda_P) \text{ a.e.}\}, \\ \text{UK}_1(\Lambda) = \prod_P K_1(\Lambda_P), \text{im } K_1(A) = \text{group of principal idèles}. \end{cases}$$

As an immediate consequence of these formulas, we have (Fröhlich [75]):

**(49.25) Theorem.** *Let  $\Lambda, \Gamma$  be  $R$ -orders in separable  $K$ -algebras  $A, B$ , respectively, and let  $\varphi: A \rightarrow B$  be a homomorphism of  $K$ -algebras such that  $\varphi(\Lambda) \subseteq \Gamma$ . Then*

- (i) *The map  $\varphi$  induces a homomorphism  $\varphi_*: \text{Cl } \Lambda \rightarrow \text{Cl } \Gamma$ , given by  $[X] \mapsto [\Gamma \otimes_{\Lambda} X]$  for  $[X] \in \text{Cl } \Lambda$ .*
- (ii) *If  $\varphi$  is a surjection of  $A$  into  $B$ , then  $\varphi_*(\text{Cl } \Lambda) = \text{Cl } \Gamma$ .*
- (iii) *If  $\Lambda \subseteq \Gamma$  are  $R$ -orders in  $A$ , this inclusion induces a surjection of  $\text{Cl } \Lambda$  onto  $\text{Cl } \Gamma$ .*

*Proof.* The map  $\varphi: A \rightarrow B$  induces homomorphisms

$$\text{JK}_1(A) \rightarrow \text{JK}_1(B), \quad K_1(A) \rightarrow K_1(B), \quad UK_1(\Lambda) \rightarrow UK_1(\Gamma),$$

so by (49.15) there is a map  $\varphi_*: \text{Cl } \Lambda \rightarrow \text{Cl } \Gamma$ . We leave it to the reader to verify that  $\varphi_*$  agrees with the “change of rings” map  $\Gamma \otimes_{\Lambda} *$ .

If  $\varphi(A) = B$ , then  $\varphi$  maps  $\text{JK}_1(A)$  onto  $\text{JK}_1(B)$ , whence  $\varphi_*$  is also surjective. This proves assertion (ii), and finally (iii) is a special case of (ii).

For computational purposes, a special case of the Mayer-Vietoris sequence (42.14) is often useful. Consider a fiber product

$$(49.26) \quad \begin{array}{ccc} \Lambda & \longrightarrow & \Lambda_1 \\ \downarrow & & \downarrow g_1 \\ \Lambda_2 & \xrightarrow{g_2} & \bar{\Lambda}, \end{array}$$

in which  $\Lambda, \Lambda_1$ , and  $\Lambda_2$  are  $R$ -orders in  $K$ -algebras  $A, A_1$ , and  $A_2$ , respectively, and where  $\bar{\Lambda}$  is an  $R$ -torsion  $R$ -algebra. (As we shall see, such fiber products arise naturally in many cases.) We then obtain the following, first pointed out by Reiner-Ullom [74a]:

**(49.27) Theorem.** *Given a fiber product diagram (49.26) as above, in which either  $g_1$  or  $g_2$  is surjective, there is an exact “Mayer-Vietoris sequence”*

$$K_1(\Lambda_1) \times K_1(\Lambda_2) \rightarrow K_1(\bar{\Lambda}) \xrightarrow{\partial'} \text{Cl } \Lambda \rightarrow \text{Cl } \Lambda_1 \oplus \text{Cl } \Lambda_2 \rightarrow 0.$$

*Proof.* Applying  $K \otimes_R *$  to (49.26) and using the fact that  $K \otimes_R \bar{\Lambda} = 0$ , we see at once that  $A \cong A_1 \oplus A_2$ . Treating this isomorphism as an identification, we have

$$\Lambda = \{(x_1, x_2) \in \Lambda_1 \oplus \Lambda_2 : g_1(x_1) = g_2(x_2)\}.$$

The inclusion  $\Lambda \subseteq \Lambda_1 \oplus \Lambda_2$  then gives a surjection  $\text{Cl } \Lambda \rightarrow \text{Cl } \Lambda_1 \oplus \text{Cl } \Lambda_2$ , by Theorem 49.25.

From Milnor’s Theorem 42.13, we obtain an exact sequence

$$K_1(\Lambda_1) \times K_1(\Lambda_2) \rightarrow K_1(\bar{\Lambda}) \xrightarrow{\partial} K_0(\Lambda) \rightarrow K_0(\Lambda_1) \oplus K_0(\Lambda_2).$$

In our special case,  $\bar{\Lambda}$  is a semilocal ring, so each element of  $K_1(\bar{\Lambda})$  may be represented by a unit of  $\bar{\Lambda}$ . The connecting homomorphism  $\partial$  constructed in the proof of (42.13) can now be described more simply: for  $u \in \bar{\Lambda}^\times$ , we have

$$\partial(u) = [M(u)] - [\Lambda] \in K_0(\Lambda),$$

where, as in (42.8),

$$M(u) = (\Lambda_1, \Lambda_2, u) = \{(x_1, x_2) \in \Lambda_1 \oplus \Lambda_2 : \bar{x}_1 u = \bar{x}_2 \text{ in } \bar{\Lambda}\}.$$

Let us show that  $M(u) \vee \Lambda$ . For each prime  $P$  of  $R$ , we have

$$M(u)_P = ((\Lambda_1)_P, (\Lambda_2)_P, u).$$

If (say)  $g_1$  is surjective, then there is a surjection  $(\Lambda_1)_P \rightarrow \bar{\Lambda}_P$ , which yields a surjection of units by Exercise 5.12. But then we have  $M(u)_P \cong \Lambda_P$  by (42.9). We have now proved that the connecting homomorphism  $\partial$  carries  $K_1(\bar{\Lambda})$  into the kernel of the map

$$\gamma: SK_0(\Lambda) \rightarrow \coprod_P SK_0(\Lambda_P).$$

Since  $\ker \gamma \cong \text{Cl } \Lambda$  by (49.15), we obtain the desired exact sequence, where the map  $\partial': K_1(\bar{\Lambda}) \rightarrow \text{Cl } \Lambda$  is given by

$$\partial'(u) = [M(u)] \in \text{Cl } \Lambda \quad \text{for } u \in \bar{\Lambda}^\times.$$

This completes the proof.

See Exercise 53.1 for an explicit description of  $M(u)$  in terms of idèles.

In the special case where  $\bar{\Lambda}$  is commutative, we may identify  $K_1(\bar{\Lambda})$  with  $\bar{\Lambda}^\times$ , by (40.28). For  $i = 1, 2$ , the image of  $K_1(\Lambda_i)$  in  $\bar{\Lambda}^\times$  is given by

$$\{\det g_i(x) : x \in GL(\Lambda_i)\},$$

which contains  $g_i(\Lambda_i^\times)$  but need not coincide with it in general. However, if  $\Lambda_i$  is commutative, we have

$$\{\det g_i(x) : x \in GL(\Lambda_i)\} = g_i(\Lambda_i^\times).$$

This implies

**(49.28) Corollary.** *If the algebra  $A$  is commutative, the sequence*

$$1 \rightarrow \Lambda^\times \rightarrow \Lambda_1^\times \times \Lambda_2^\times \rightarrow \bar{\Lambda}^\times \rightarrow Cl\Lambda \rightarrow Cl\Lambda_1 \oplus Cl\Lambda_2 \rightarrow 0$$

*is exact.*

There is an analogous version when  $A$  is not necessarily commutative, under some mild restrictions. We begin with

**(49.29) Definition.** An order  $\Lambda$  has *locally free cancellation* if for any locally free  $\Lambda$ -modules  $X$  and  $Y$ ,

$$X \oplus \Lambda^{(k)} \cong Y \oplus \Lambda^{(k)} \quad \text{for some } k \Rightarrow X \cong Y.$$

By (49.3), this holds if and only if it holds for left ideals  $X, Y$  in  $g(\Lambda)$ . A commutative order  $\Lambda$  necessarily has this cancellation property, since for  $X \in g(\Lambda)$ , the  $(k+1)$ -st exterior power of  $X \oplus \Lambda^{(k)}$  is isomorphic to  $X$  (see the proof of (34.30)). As we shall see below, most noncommutative orders also have locally free cancellation; this is the case whenever  $A = Eichler/R$  (see (51.24)).

**(49.30) Corollary.** *Given a fiber product as in (49.26), assume that  $\Lambda$  is an order with locally free cancellation. Then there is an exact sequence*

$$1 \rightarrow W \rightarrow \bar{\Lambda}^\times \xrightarrow{\partial'} Cl\Lambda \rightarrow Cl\Lambda_1 \oplus Cl\Lambda_2 \rightarrow 0,$$

where

$$W = \{w_1 w_2 : w_i \in g_i(\Lambda_i), i = 1, 2\}.$$

*Proof.* The homomorphism  $\partial'$  is given as in (49.27), namely,

$$\partial'(u) = [M(u)], \quad \text{where } M(u) = (\Lambda_1, \Lambda_2, u), \quad \text{for } u \in \bar{\Lambda}^\times.$$

Since  $\Lambda$  is assumed to have locally free cancellation, we have  $\partial'(u) = 0$  if and

only if  $M(u) \cong \Lambda$ , that is,  $(\Lambda_1, \Lambda_2, u) = (\Lambda_1, \Lambda_2, 1)$ . The latter isomorphism holds if and only if  $u \in W$ , by (42.9).

The above implies also that

$$W = \{w_2 w_1 : w_i \in g_i(\Lambda_i)\},$$

as well as the unexpected fact that  $W \trianglelefteq \bar{\Lambda}^*$ .

The above result, and an analogous version (49.39) below, will be used in §50C to calculate the class group  $\text{Cl}_G$  of certain metacyclic groups  $G$ .

As in Chapters 3 and 4, we obtain information about nonmaximal orders by relating them to maximal orders. This technique is also important in studying class groups, and we shall begin by determining the class group of a maximal order  $\Lambda$  in a f.d. separable  $K$ -algebra  $A$ . Since  $\Lambda$  decomposes according to the Wedderburn decomposition of  $A$ , as in (26.20), it suffices to treat the case where  $A$  is a central simple  $K$ -algebra.

For the moment, let  $K$  be a global field, and recall some notation from §38:

$$(49.31) \quad \begin{cases} I(R) = \text{group of fractional } R\text{-ideals of } K, \\ K^+ = \{a \in K : a_P > 0 \text{ at every infinite prime } P \text{ of } K \text{ ramified in } A\}, \\ P_A(R) = \{Ra : a \in K^+\} = \text{subgroup of } I(R), \\ \text{Cl}_A R = I(R)/P_A(R). \end{cases}$$

In terms of this notation, we have:

**(49.32) Theorem.** *Let  $\Lambda$  be a maximal  $R$ -order in a central simple  $K$ -algebra  $A$ , where  $K$  is a global field. Then*

$$\text{Cl } \Lambda \cong SK_0(\Lambda) \cong \text{Cl}_A R.$$

*Proof.* To establish the first isomorphism, let  $P$  be a prime of  $R$ . If  $X, Y$  are projective  $\Lambda_P$ -lattices such that  $K_P X \cong K_P Y$  as  $A_P$ -modules, then  $X \cong Y$  by (26.24iii). This shows that  $SK_0(\Lambda_P) = 0$ , and therefore  $\text{Cl } \Lambda = SK_0(\Lambda)$  by (49.15).

Next, there is an exact sequence

$$0 \rightarrow SK_0(\Lambda) \rightarrow K_0(\Lambda) \rightarrow K_0(A) \rightarrow 0,$$

with  $K_0(A) \cong \mathbb{Z}$  since  $A$  is a simple algebra. The proof of (38.67) then gives  $SK_0(\Lambda) \cong \text{Cl}_A R$ , which establishes the theorem.

**Remarks.** (i) The theorem exhibits  $\text{Cl } \Lambda$  as a “restricted” ideal class group of  $R$ , where the restriction is placed on the kind of principal ideals used. The result shows that  $\text{Cl } \Lambda$  is independent of the choice of the maximal order  $\Lambda$ . This is clear in any case from the fact that any two such orders are Morita equivalent. See also Exercise 49.9.

(ii) We can also obtain the theorem by a more complicated argument based on (49.17). Indeed, from (49.17) and its proof we obtain

$$\text{Cl } \Lambda \cong J(K)/K^+ U(R), \quad \text{where } U(R) = \prod_p R_p^\times.$$

As in Example 31.24, we have  $J(K)/K^+ U(R) \cong \text{Cl}_A R$ .

Returning to the case where  $\Lambda$  is an arbitrary order, and  $K$  any field, let  $\Lambda'$  be a maximal  $R$ -order in  $A$  containing  $\Lambda$ . By (49.25), there is a surjection  $\text{Cl } \Lambda \rightarrow \text{Cl } \Lambda'$ , whose kernel  $D(\Lambda)$  is called the *kernel group of  $\Lambda$* . Thus, there is an exact sequence

$$(49.33) \quad 0 \rightarrow D(\Lambda) \rightarrow \text{Cl } \Lambda \rightarrow \text{Cl } \Lambda' \rightarrow 0.$$

We shall see in a moment that  $D(\Lambda)$  is independent of the choice of  $\Lambda'$ .

The problem of calculating  $\text{Cl } \Lambda$  reduces to that of calculating  $\text{Cl } \Lambda'$  and  $D(\Lambda)$ , and the former can be handled by the previous theorem (at least when  $K$  is a global field). In most cases,  $D(\Lambda)$  is harder to compute. There is also a secondary question, so far settled in very few cases: what is the nature of the extension (49.33) of  $\text{Cl } \Lambda'$  by  $D(\Lambda)$ ?

We begin our discussion of kernel groups with an easy criterion, due to Jacobinski, for a locally free ideal to give an element of  $D(\Lambda)$ :

**(49.34) Proposition.** *Let  $M \in g(\Lambda)$ . Then  $[M] \in D(\Lambda)$  if and only if*

$$M \oplus X \cong \Lambda \oplus X \quad \text{for some f.g. left } \Lambda\text{-module } X.$$

Consequently,  $D(\Lambda)$  is independent of the choice of  $\Lambda'$  in (49.33).

*Proof.* Given an isomorphism  $M \oplus X \cong \Lambda \oplus X$ , let  $t(X)$  be the  $R$ -torsion submodule of  $X$ , and put  $\bar{X} = X/t(X)$ , a  $\Lambda$ -lattice. The isomorphism must carry  $t(X)$  to itself, and so induces an isomorphism

$$M \oplus \bar{X} \cong \Lambda \oplus \bar{X}.$$

We shall use this observation soon.

Now let  $\Lambda \subseteq \Lambda' =$  maximal order. Since  $M \vee \Lambda$ , it follows from Exercise 31.10 that there is a  $\Lambda$ -isomorphism

$$M \oplus \Lambda' \cong \Lambda \oplus (\Lambda' \otimes M),$$

where  $\otimes$  means  $\otimes_\Lambda$ . If  $[M] \in D(\Lambda)$ , then  $[\Lambda' \otimes M] = 0$  in  $\text{Cl } \Lambda'$ , so  $\Lambda' \otimes M$  is stably isomorphic to  $\Lambda'$ . Adding copies of  $\Lambda'$  to both sides of the above isomorphism, we obtain  $M \oplus \Lambda'^{(k)} \cong \Lambda \oplus \Lambda'^{(k)}$  for some  $k$ , as desired.

Conversely, suppose  $M \oplus X \cong \Lambda \oplus X$  for some  $X$ ; apply  $\Lambda' \otimes *$  to both sides

and factor out the torsion submodules, obtaining a  $\Lambda'$ -isomorphism

$$(\Lambda' \otimes M) \oplus Y \cong \Lambda' \oplus Y \text{ for some } \Lambda'\text{-lattice } Y.$$

But  $Y$  is  $\Lambda'$ -projective by (26.12ii), so  $\Lambda' \otimes M$  is stably isomorphic to  $\Lambda'$ , that is,  $[\Lambda' \otimes M] = 0$  in  $\mathrm{Cl}\Lambda'$ . Thus  $[M] \in D(\Lambda)$ , as claimed.

**(49.35) Corollary.** *If  $\Lambda$  is any hereditary order in  $A$ , and  $\Lambda'$  is a maximal order, then  $\mathrm{Cl}\Lambda \cong \mathrm{Cl}\Lambda'$ .*

*Proof.* If  $[M] \in D(\Lambda)$ , then  $M \oplus X \cong \Lambda \oplus X$  for some  $\Lambda$ -lattice  $X$ . But  $X$  is  $\Lambda$ -projective by (4.3) and Exercise 23.1, so  $[M] = 0$ .

The idèle-theoretic formulas for  $\mathrm{Cl}\Lambda$  and  $\mathrm{Cl}\Lambda'$  combine to give a formula for  $D(\Lambda)$ , as follows:

**(49.36) Theorem.** *Let  $K$  be a global field, and let  $\mathfrak{O}$  be the integral closure of  $R$  in the center  $C$  of  $A$ . Then*

$$D(\Lambda) \cong \frac{C^+ \cdot \prod \mathfrak{O}_P^\times}{C^+ \cdot \prod \mathrm{nr} \Lambda_P^\times},$$

where  $P$  ranges over all prime ideals of  $R$ , and  $C^+$  is as in (49.17).

*Proof.* Let  $\Lambda'$  be a maximal order containing  $\Lambda$ . As pointed out in (49.19), we have  $\mathrm{nr}(\Lambda'_P) = \mathfrak{O}_P^\times$ . From (49.17) we then obtain

$$(49.37) \quad \mathrm{Cl}\Lambda' = J(C)/C^+ U(\mathfrak{O}), \quad \text{where } U(\mathfrak{O}) = \prod_P \mathfrak{O}_P^\times.$$

Comparing the above with formula (49.17) for  $\mathrm{Cl}\Lambda$ , the theorem follows.

**(49.38) Proposition.** *Let  $\varphi: A \rightarrow B$  be a homomorphism of  $K$ -algebras such that  $\varphi(\Lambda) \subseteq \Gamma$ , where  $\Lambda, \Gamma$  are  $R$ -orders in  $A, B$ , respectively. Then  $\varphi$  induces a map  $\varphi_*: D(\Lambda) \rightarrow D(\Gamma)$ , and  $\varphi_*$  is surjective whenever  $\varphi(A) = B$ .*

*Proof.* Let  $M \vee \Lambda$  be such that  $[M] \in D(\Lambda)$ ; then by (49.34)  $M \oplus X \cong \Lambda \oplus X$  for some f.g.  $\Lambda$ -module  $X$ . Applying  $\Gamma \otimes_\Lambda *$  to this isomorphism, it follows that  $[\Gamma \otimes_\Lambda M] \in D(\Gamma)$ , so  $\varphi_* D(\Lambda) \subseteq D(\Gamma)$ .

Now let  $\varphi(A) = B$ , so  $\varphi$  is a projection of  $A$  onto the sum of certain simple components of  $A$ . If  $\Lambda'$  is a maximal order in  $A$ , then  $\varphi(\Lambda')$  is a maximal order in  $B$ . However, we have

$$D(\Lambda) \cong \frac{\mathrm{im} K_1(A) \cdot \mathrm{im} UK_1(\Lambda')}{\mathrm{im} K_1(A) \cdot \mathrm{im} UK_1(\Lambda)}$$

by (49.16), where all of these images lie in  $JK_1(A)$ . It is then obvious that  $\varphi_*$  is surjective.

Next, we show how to use (49.27) to obtain information about kernel groups rather than class groups.

**(49.39) Theorem.** *Given a fiber product as in (49.27), there is an exact “Mayer-Vietoris sequence”*

$$K_1(\Lambda_1) \times K_1(\Lambda_2) \rightarrow K_1(\bar{\Lambda}) \xrightarrow{\partial'} D(\Lambda) \rightarrow D(\Lambda_1) \oplus D(\Lambda_2) \rightarrow 0.$$

Further, if  $\Lambda$  has locally free cancellation, the sequence

$$1 \rightarrow W \rightarrow \bar{\Lambda}^\cdot \rightarrow D(\Lambda) \rightarrow D(\Lambda_1) \oplus D(\Lambda_2) \rightarrow 0$$

is exact, where  $W$  is defined as in (49.30).

*Proof.* Let  $\Lambda'$  be a maximal order containing  $\Lambda_1 \oplus \Lambda_2$ . Since the diagram

$$\begin{array}{ccc} \text{Cl } \Lambda & \longrightarrow & \text{Cl } \Lambda' \\ \searrow & & \nearrow \\ \text{Cl } \Lambda_1 \oplus \text{Cl } \Lambda_2 & & \end{array}$$

commutes, it follows that in the sequence (49.27), we have  $\text{im } \partial' \subseteq D(\Lambda)$ . The remaining assertions are then trivial.

Returning to the case where  $K$  is a global field, we may simplify the formula in (49.36) for  $D(\Lambda)$  by using the set  $S = S(\Lambda)$  defined in (49.1). We prove

**(49.40) Theorem.** *Let  $K$  be a global field, and keep the notation of (49.36). Then*

$$D(\Lambda) \cong \frac{\prod_{P \in S} \mathfrak{O}_P^\cdot}{\mathfrak{O}^+ \prod_{P \in S} \text{nr } \Lambda_P^\cdot},$$

where  $\mathfrak{O}^+ = C^+ \cap \mathfrak{O}^\cdot$ , viewed as a subgroup of  $\prod_{P \in S} \mathfrak{O}_P^\cdot$ .

*Proof.* Let  $\Lambda \subseteq \Lambda' = \text{maximal } R\text{-order in } A$ ; then  $\Lambda_P = \Lambda'_P$  for  $P \notin S$ . From (49.36) we obtain

$$D(\Lambda) \cong \frac{\prod \mathfrak{O}_P^\cdot}{(\prod \text{nr } \Lambda_P^\cdot)(C^+ \cap \prod \mathfrak{O}_P^\cdot)},$$

where the products extend over all  $P$ . Now  $C^+ \cap \prod \mathfrak{O}_P^\cdot = C^+ \cap \mathfrak{O}^\cdot = \mathfrak{O}^+$ , so we

have

$$(49.41) \quad D(\Lambda) \cong \frac{\prod_p \mathfrak{O}_p^+}{\mathfrak{D}^+ \prod_p \text{nr } \Lambda_p^+}.$$

Setting  $Y = \prod_{p \notin S} \mathfrak{O}_p^+$ , the above may be written as

$$D(\Lambda) \cong \frac{\left( \prod_{p \in S} \mathfrak{O}_p^+ \right) \times Y}{\left( \prod_{p \in S} \text{nr } \Lambda_p^+ \right) Y \mathfrak{D}^+}.$$

There is an embedding  $i: \mathfrak{D}^+ \rightarrow \prod_{p \in S} \mathfrak{O}_p^+$ , and clearly  $Y \mathfrak{D}^+ = i(\mathfrak{D}^+) \times Y$ . This gives the desired formula for  $D(\Lambda)$ , once we identify  $\mathfrak{D}^+$  with  $i(\mathfrak{D}^+)$ .

Following the above approach, we now give Fröhlich's generalization of the Mayer-Vietoris sequence (49.39), valid when  $K$  is a global field. In addition to the notation in (49.40), we introduce the unit idèle groups

$$U(\mathfrak{D}) = \prod_p \mathfrak{O}_p^+, \quad U(\Lambda) = \prod_p \Lambda_p^+,$$

where  $P$  ranges over all maximal ideals of  $R$ . The reduced norm  $\text{nr}: A \rightarrow C$  induces a reduced norm map  $\text{nr}: U(\Lambda) \rightarrow U(\mathfrak{D})$ .

**(49.42) Theorem (Fröhlich [75]).** *Let  $K$  be a global field, and let*

$$A = A_1 \oplus A_2, \quad C = C_1 \oplus C_2, \quad \mathfrak{D} = \mathfrak{D}_1 \oplus \mathfrak{D}_2, \quad \Lambda \subseteq \Lambda_1 \oplus \Lambda_2,$$

*where  $A_1$  and  $A_2$  are direct sums of Wedderburn components of  $A$ , and where  $\Lambda_i$  is an  $R$ -order in  $A_i$ ,  $i = 1, 2$ . Then there is an exact sequence*

(49.43)

$$\text{nr } U(\Lambda) \rightarrow \frac{\mathfrak{D}_1^+ \text{nr } U(\Lambda_1)}{\mathfrak{D}_1^+} \times \frac{\mathfrak{D}_2^+ \text{nr } U(\Lambda_2)}{\mathfrak{D}_2^+} \rightarrow D(\Lambda) \rightarrow D(\Lambda_1) \oplus D(\Lambda_2) \rightarrow 0.$$

*Proof.* We note first that

$$U(\mathfrak{D}) = U(\mathfrak{D}_1) \times U(\mathfrak{D}_2), \quad \mathfrak{D}^+ = \mathfrak{D}_1^+ \times \mathfrak{D}_2^+, \quad \mathfrak{D}^+ = \mathfrak{D}_1^+ \times \mathfrak{D}_2^+.$$

Formula (49.41) takes the form

$$D(\Lambda) \cong \frac{U(\mathfrak{D})}{\mathfrak{D}^+ \text{nr } U(\Lambda)}.$$

There are analogous formulas for  $D(\Lambda_1)$  and  $D(\Lambda_2)$ . Since  $U(\mathfrak{D}) = U(\mathfrak{D}_1) \times U(\mathfrak{D}_2)$ , it follows that there is a surjection

$$\theta: \frac{U(\mathfrak{D})}{\mathfrak{D}^+ \text{ nr } U(\Lambda)} \rightarrow \frac{U(\mathfrak{D}_1)}{\mathfrak{D}_1^+ \text{ nr } U(\Lambda_1)} \times \frac{U(\mathfrak{D}_2)}{\mathfrak{D}_2^+ \text{ nr } U(\Lambda_2)}.$$

We have used the fact that for  $i = 1, 2$ , the projection map  $A \rightarrow A_i$  carries  $U(\mathfrak{D})$  to  $U(\mathfrak{D}_i)$ ,  $\mathfrak{D}^+$  to  $\mathfrak{D}_i^+$ , and  $\text{nr } U(\Lambda)$  to  $\text{nr } U(\Lambda_i)$ .

The kernel of  $\theta$  is clearly the image of

$$\frac{\mathfrak{D}_1^+ \text{ nr } U(\Lambda_1)}{\mathfrak{D}_1^+} \times \frac{\mathfrak{D}_2^+ \text{ nr } U(\Lambda_2)}{\mathfrak{D}_2^+}$$

in  $U(\mathfrak{D})/\mathfrak{D}^+ \text{ nr } U(\Lambda)$ . Finally, from the fact that

$$(49.44) \quad \frac{\mathfrak{D}_i^+ \text{ nr } U(\Lambda_i)}{\mathfrak{D}_i^+} \cong \frac{\text{nr } U(\Lambda_i)}{\mathfrak{D}_i^+ \cap \text{nr } U(\Lambda_i)}$$

for  $i = 1, 2$ , it is easily seen that the sequence (49.43) is exact. This completes the proof.

**(49.45) Remark.** A fiber product (49.26) gives rise to a decomposition  $A = A_1 \oplus A_2$  in which  $\Lambda \subseteq \Lambda_1 \oplus \Lambda_2$ , so the sequence (49.43) can be viewed as a modified version of the Mayer-Vietoris sequence (49.39).

### §49C. Frobenius Functor Properties for Class Groups of Group Rings

Throughout this subsection, let  $G$  be a finite group, and  $K$  a global field for which  $\text{char } K \nmid |G|$ . Let  $R$  be a Dedekind domain with quotient field  $K$ . In most applications we choose  $R = \text{alg. int. } \{K\}$ , but for the moment we shall not impose this hypothesis. The first result is due to Reiner [75] and Matchett [77]:

**(49.46) Theorem.** *Both  $\text{Cl } RG$  and  $D(RG)$  are Frobenius modules over the Frobenius functor  $G_0^K(RG)$ .*

*Proof.* For each  $G$ , we have defined  $G_0^K(RG)$  to be the Grothendieck group associated with the category of left  $RG$ -lattices, with multiplication given by inner tensor products (over  $R$ ) of  $RG$ -lattices (see (38.3)). As shown in (38.10), both  $K_0(RG)$  and  $K_0(KG)$  are Frobenius modules over the Frobenius functor  $G_0^K(RG)$ , and the map  $K_0(RG) \rightarrow K_0(KG)$  is a morphism of Frobenius modules. Its kernel  $SK_0(RG)$  is therefore also a Frobenius module over  $G_0^K(RG)$ .

By (49.15), there is an exact sequence

$$(49.46a) \quad 0 \rightarrow \text{Cl } RG \rightarrow SK_0(RG) \xrightarrow{\gamma} \coprod_p SK_0(R_p G) \rightarrow 0,$$

where  $P$  ranges over all maximal ideals of  $R$ . Since  $\gamma$  is also a morphism of Frobenius modules, it follows that  $\text{Cl } RG$  is itself a Frobenius module over  $G_0^R(RG)$ .

We show next that the kernel group  $D(RG)$ , defined as (49.33), is also a Frobenius module. The entire difficulty lies in showing that kernel groups behave properly under restriction and induction. For  $H \leq G$ , the inclusion  $RH \subseteq RG$  gives rise to maps

$$\text{res}_H^G: \text{Cl } RG \rightarrow \text{Cl } RH, \quad \text{ind}_H^G: \text{Cl } RH \rightarrow \text{Cl } RG.$$

It is clear from (49.34) that  $\text{ind}_H^G D(RH) \subseteq D(RG)$ , as desired.

Turning to the restriction map, let  $|G:H| = n$ , so  $RG \cong (RH)^{(n)}$  as  $RH$ -modules. Since  $K_0(RG)$  is spanned by f.g. projective  $RG$ -modules, it follows that  $\text{res}_H^G$  carries  $K_0(RG)$  into  $K_0(RH)$ . We now identify  $\text{Cl } RG$  with  $\ker \gamma$  as in (49.15), where  $\gamma$  is as in (49.46a). Let  $x \in D(RG)$  be expressed as  $x = [M] - [RG]$  where  $M \vee RG$  (since  $\gamma(x) = 0$ ). Then

$$\text{res}_H^G x = [M_H] - n[RH] \in SK_0(RH).$$

But  $M_H \vee (RH)^{(n)}$ , so by (49.3) we may write  $M_H \cong N \oplus (RH)^{(n-1)}$  for some  $N \vee RH$ . Therefore

$$\text{res}_H^G x = [N] - [RH] \in SK_0(RH).$$

On the other hand, since  $x \in D(RG)$  we have  $M \oplus X \cong RG \oplus X$  for some f.g.  $RG$ -module  $X$ , by (49.34). Restricting to  $H$ , it follows that  $N \oplus Y \cong RH \oplus Y$ , where  $Y = X_H \oplus (RH)^{(n-1)}$ , and therefore  $\text{res}_H^G x \in D(RH)$  as desired. We leave it as an exercise for the reader to verify that the induction and restriction maps between  $D(RH)$  and  $D(RG)$  satisfy the axioms in (38.7).

A somewhat surprising consequence is:

**(49.47) Corollary.** *Both  $\text{Cl } RG$  and  $D(RG)$  are Frobenius modules over the Frobenius functor  $G_0(KG)$ .*

*Proof.* Let  $\varphi: G_0^R(RG) \rightarrow G_0(KG)$  be the ring surjection induced by the inclusion map  $RG \subset KG$ , as in (39.14). It suffices to show that  $\ker \varphi$  annihilates  $\text{Cl } RG$ . By (39.14), every element of  $\ker \varphi$  has the form  $[RG] - [M]$  for some  $M \vee RG$ . But the typical element of  $\text{Cl } RG$  is of the form  $[RG] - [N]$ , with  $N \vee RG$ . However,

$$([RG] - [M])([RG] - [N]) = 0 \quad \text{in } K_0(RG)$$

by the proof of (39.16). Therefore  $(\ker \varphi) \cdot \text{Cl } RG = 0$ , as desired.

(Swan [60], [63] showed that  $\text{Cl } RG$  is a Frobenius module over  $G_0(KG)$ . The

corresponding result for  $D(RG)$  was established by Endo-Miyata [74] and Matchett [77]. For other results of this nature, see also Ullom [81].)

Along the same lines as the previous theorem, we have:

**(49.48) Proposition.**  $K_0(\mathbb{Z}G)$  is a Frobenius module over the Frobenius functor  $G_0(\mathbb{Q}G)$ .

*Proof.* By (32.12), each  $x \in K_0(\mathbb{Z}G)$  is of the form

$$x = m[\mathbb{Z}G] - [M] \quad \text{for some } m \in \mathbb{Z} \text{ and some } M \vee \mathbb{Z}G.$$

As above,

$$([\mathbb{Z}G] - [N])([\mathbb{Z}G] - [M]) = 0 \quad \text{in } K_0(\mathbb{Z}G)$$

for any  $N \vee \mathbb{Z}G$ . On the other hand,

$$([\mathbb{Z}G] - [N]) \cdot [\mathbb{Z}G] = [\mathbb{Z}G \otimes_{\mathbb{Z}} \mathbb{Z}G] - [N \otimes_{\mathbb{Z}} \mathbb{Z}G] = 0,$$

the last equality because  $N \otimes_{\mathbb{Z}} \mathbb{Z}G$  is  $\mathbb{Z}G$ -free of rank  $|G|$ , by Exercise 10.18. This shows that  $\ker \varphi$  annihilates  $K_0(\mathbb{Z}G)$ , where  $\varphi: G_0^{\mathbb{Z}}(\mathbb{Z}G) \rightarrow G_0(\mathbb{Q}G)$  is the ring surjection induced by the inclusion  $\mathbb{Z}G \subset \mathbb{Q}G$ . The rest is now clear.

## §49. Exercises

1. Let  $A$  be a f.d.  $K$ -algebra with center  $C$ , and let  $E$  be any extension field of  $K$ . Prove that  $E \otimes_K A$  is a f.d.  $E$ -algebra with center  $E \otimes_K C$ . In particular, if  $E$  is a  $P$ -adic completion  $K_P$  of a field  $K$  relative to some prime  $P$  of  $K$ , show that the center of  $A_P$  is  $C_P$  ( $= K_P \otimes_K C$ ).

[Hint: Let  $C'$  denote the center of  $E \otimes A$ , where  $\otimes$  means  $\otimes_K$ . Clearly  $C' \supseteq E \otimes C$ . Now write  $E = \bigoplus K e_i$ , so  $E \otimes A = \bigoplus (e_i \otimes A)$ . If  $x = \sum e_i \otimes a_i \in C'$ , then  $x$  commutes with  $1 \otimes a$  for each  $a \in A$ . Therefore each  $a_i \in C$ , so  $x \in E \otimes C$ .]

2. Let  $\Lambda$  be an  $R$ -order, and set  $\Gamma = M_n(\Lambda)$ . Show that

$$\mathrm{Cl}\Lambda \cong \mathrm{Cl}\Gamma, \quad D(\Lambda) \cong D(\Gamma).$$

3. Starting with a fiber product (49.26) with  $g_1$  or  $g_2$  surjective, there is a fiber product

$$\begin{array}{ccc} M_n(\Lambda) & \longrightarrow & M_n(\Lambda_1) \\ \downarrow & & h_1 \downarrow \\ M_n(\Lambda_2) & \xrightarrow{h_2} & M_n(\bar{\Lambda}) \end{array}$$

for  $n \geq 2$ . Deduce from (49.30), (49.39), and (51.24) that there are exact sequences

$$1 \rightarrow W \rightarrow GL_n(\bar{\Lambda}) \rightarrow Cl\Lambda \rightarrow Cl\Lambda_1 \oplus Cl\Lambda_2 \rightarrow 0$$

$\searrow D(\Lambda) \rightarrow D(\Lambda_1) \oplus D(\Lambda_2) \rightarrow 0,$

where

$$W = \{w_1 w_2 : w_i \in h_i(GL_n(\Lambda_i)), \quad i = 1, 2\}.$$

4. Keep the above notation and suppose that  $g_1$  maps  $\Lambda_1^*$  onto  $\bar{\Lambda}^*$ . Show that

$$Cl\Lambda \cong Cl\Lambda_1 \oplus Cl\Lambda_2, \quad D(\Lambda) \cong D(\Lambda_1) \oplus D(\Lambda_2).$$

[Hint: Since  $\bar{\Lambda}^*$  maps onto  $K_1(\bar{\Lambda})$ , so does  $K_1(\Lambda_1)$ .]

5. Starting with a fiber product (49.26) in which  $g_1$  or  $g_2$  is surjective, suppose that

$$g_1(\Lambda_1^*) = (g_1(\Lambda_1))^*.$$

Show that the surjections

$$Cl\Lambda \rightarrow Cl\Lambda_1, \quad D(\Lambda) \rightarrow D(\Lambda_1)$$

are split.

[Hint (Reiner-Ullom [74a]): If  $g_1(\Lambda_1) = \bar{\Lambda}$ , the result follows from Exercise 4. If  $g_1(\Lambda_1) \neq \bar{\Lambda}$ , then by hypothesis  $g_2(\Lambda_2) = \bar{\Lambda}$ . Setting  $\Lambda_3 = g_2^{-1}(g_1(\Lambda_1))$ , there is a fiber product

$$\begin{array}{ccc} \Lambda & \longrightarrow & \Lambda_1 \\ \downarrow & & \downarrow \\ \Lambda_3 & \longrightarrow & g_1(\Lambda_1). \end{array}$$

Then

$$Cl\Lambda \cong Cl\Lambda \oplus Cl\Lambda_3, \quad D(\Lambda) \cong D(\Lambda_1) \oplus D(\Lambda_3)$$

by the first case.]

6. Let  $\Lambda$  be an  $R$ -order, and let  $M, N \in \mathcal{P}(\Lambda)$  be such that  $M \oplus X \cong N \oplus X$  for some f.g.  $\Lambda$ -module  $X$  of finite homological dimension. Prove that  $[M] = [N]$  in  $K_0(\Lambda)$ .

[Hint: Use (38.50)]

7. Let  $\Lambda \subset \Lambda'$  be  $R$ -orders in  $A$ , and suppose that  $hd_{\Lambda} \Lambda'$  is finite. Deduce that  $Cl\Lambda \cong Cl\Lambda'$ .

8. Let  $X$  be a locally free  $\Lambda$ -lattice, and let  $\Lambda' \supset \Lambda$ . Show that the map

$$\Lambda' \otimes X \rightarrow \Lambda' X \subset KX$$

is an isomorphism. This also holds for  $X \in \mathcal{P}(\Lambda)$ .

9. Let  $\Lambda_1$  and  $\Lambda_2$  be a pair of maximal  $K$ -orders in  $A$ . Show that  $\Lambda_2 = \beta \Lambda_1 \beta^{-1}$  for some idèle  $\beta \in J(A)$ , and deduce that

$$J_0(A)A^*U(\Lambda_2) = J_0(A)A^*U(\Lambda_1),$$

which gives  $Cl\Lambda_1 \cong Cl\Lambda_2$  (see (49.32)).

10. Let  $\Lambda \subset \Gamma$  be a pair of  $R$ -orders in a f.d.  $K$ -algebra, and let  $I$  be a two-sided  $\Gamma$ -ideal contained in  $\Lambda$ , such that  $KI = A$ . There is a fiber product

$$\begin{array}{ccc} \Lambda & \longrightarrow & \Gamma \\ \downarrow & & \downarrow \\ \bar{\Lambda} & \longrightarrow & \bar{\Gamma} \end{array}$$

where  $\bar{\Lambda} = \Lambda/I$  and  $\bar{\Gamma} = \Gamma/I$ . Using Milnor's Theorem 42.13 and the ideas in the proof of (49.27), prove that these are exact sequences.

$$\begin{array}{ccccccc} K_1(\Lambda) & \rightarrow & K_1(\Gamma) \times K_1(\bar{\Lambda}) & \rightarrow & K_1(\bar{\Gamma}) & \rightarrow & \text{Cl } \Lambda \rightarrow \text{Cl } \Gamma \rightarrow 0 \\ & & & & \searrow & & \\ & & & & D(\Lambda) & \rightarrow & D(\Gamma) \rightarrow 0. \end{array}$$

In particular, if  $A$  is a commutative algebra and  $\Gamma$  is a maximal order, prove that

$$D(\Lambda) \cong \bar{\Gamma}^*/(\text{image of } \Gamma^*)(\text{image of } \bar{\Lambda}^*),$$

[Hint (Matchett [80]): Let  $P$  range over the maximal ideals of  $R$ . There is a commutative diagram with exact rows

$$\begin{array}{ccccccc} K_1(\bar{\Gamma}) & \xrightarrow{\partial} & K_0(\Lambda) & \longrightarrow & K_0(\Gamma) \oplus K_0(\bar{\Lambda}) & \longrightarrow & K_0(\bar{\Gamma}) \\ f_1 \downarrow & & f_2 \downarrow & & f_3 \downarrow & & f_4 \downarrow \\ \prod_p K_1(\bar{\Gamma}_P) & \xrightarrow{\partial'} & \prod_p K_0(\Lambda_P) & \longrightarrow & \prod_p K_0(\Gamma_P) \oplus \prod_p K_0(\bar{\Lambda}_P) & \longrightarrow & \prod_p K_0(\bar{\Gamma}_P). \end{array}$$

Since  $\bar{\Gamma}$  and  $\bar{\Lambda}$  are  $R$ -torsion  $R$ -algebras, we have

$$\bar{\Gamma} \cong \coprod_P \bar{\Gamma}_P, \quad \bar{\Lambda} \cong \coprod_P \bar{\Lambda}_P,$$

so  $f_1$ ,  $f_4$ , and  $f_5$  are isomorphisms. Further, for each  $P$  the map  $K_1(\bar{\Gamma}_P) \rightarrow K_0(\Lambda_P)$  is the zero map (since  $(\Gamma_P)^* \rightarrow (\bar{\Gamma}_P)^*$  is surjective; see proof of (49.27)). Thus  $\partial'$  is the zero map.

It follows easily that

$$K_1(\bar{\Gamma}) \rightarrow \ker f_2 \rightarrow \ker f_3 \rightarrow 0$$

is exact. Finally,  $\ker f_2 \cong \text{Cl } \Lambda$  and  $\ker f_3 \cong \text{Cl } \Gamma$ . Note also that  $\text{im } \partial \subseteq \ker(\text{Cl } \Lambda \rightarrow \text{Cl } \Gamma) \subseteq D(\Lambda)$ .

If  $A$  is commutative, then the determinant map gives an isomorphism  $\det: K_1(\bar{\Gamma}) \cong \bar{\Gamma}^*$ . Since

$$\begin{array}{ccc} K_1(\Gamma) & \longrightarrow & K_1(\bar{\Gamma}) \\ \det \downarrow & & \det \downarrow \\ \Gamma^* & \longrightarrow & \bar{\Gamma}^* \end{array}$$

commutes, it is clear that  $K_1(\Gamma)$  and  $\Gamma^*$  have the same image in  $\bar{\Gamma}^*$ .]

11. Given a surjection  $G \rightarrow \bar{G}$  of finite groups, show that there is a surjection

$$D(\mathbb{Z}G) \rightarrow D(\mathbb{Z}\bar{G}).$$

[Hint: Use (49.38).]

12. Let  $G = N \rtimes H$  be a semidirect product. Prove that there are split surjections

$$\text{Cl } \mathbb{Z}G \rightarrow \text{Cl } \mathbb{Z}H, \quad D(\mathbb{Z}G) \rightarrow D(\mathbb{Z}H).$$

## §50. CLASS GROUPS OF INTEGRAL GROUP RINGS

In this section we shall show how to compute the locally free class group  $\text{Cl } \mathbb{Z}G$  for various finite groups  $G$ . The methods often apply to the more general case  $\text{Cl } RG$ , with  $R$  a ring of algebraic integers. In most cases, we shall determine the kernel group  $D(\mathbb{Z}G)$ , which differs from the class group  $\text{Cl } \mathbb{Z}G$  by class groups of rings of algebraic integers. Furthermore, the kernel group  $D(\mathbb{Z}G)$  is usually calculated in terms of information about the distribution of units (in rings of algebraic integers) modulo certain ideals. Deeper investigation of units leads to difficult problems in algebraic number theory, which are usually beyond the scope of this book, and in any case are often unsolved.

### §50A. Cyclic Groups of Squarefree Order

Throughout this subsection,  $p$  denotes a rational prime,  $C_n$  a cyclic group of order  $n$ , and  $\omega_n$  a primitive  $n$ -th root of 1 over  $\mathbb{Q}$ . We set (see §4H)

$$(50.1) \quad K_n = \mathbb{Q}(\omega_n), \quad R_n = \text{alg. int. } \{K_n\} = \mathbb{Z}[\omega_n], \quad \pi_n = \prod_{p|n} (1 - \omega_p).$$

Let  $R_n^*$  be the group of units of  $R_n$ , and  $(R_n/\pi_n)^*$  the group of units of  $R_n/\pi_n$ , where we write  $R_n/\pi_n$  in place of  $R_n/\pi_n R_n$  for brevity. By Exercise 21.1, we may write

$$\text{QC}_n \cong \coprod_{d|n} K_d.$$

The unique maximal  $\mathbb{Z}$ -order  $\Lambda'$  in  $\text{QC}_n$  is therefore given by

$$\Lambda' \cong \coprod_{d|n} R_d,$$

and consequently

$$\text{Cl } \Lambda' \cong \coprod_{d|n} \text{Cl } R_d.$$

There is an exact sequence (see (49.33))

$$0 \rightarrow D(\mathbb{Z}C_n) \rightarrow \text{Cl } \mathbb{Z}C_n \rightarrow \text{Cl } \Lambda' \rightarrow 0,$$

and we shall usually study the *kernel group*  $D(\mathbb{Z}C_n)$  rather than  $\text{Cl } \mathbb{Z}C_n$ .

We begin with a “classical” result, due to Rim [59]:

**(50.2) Theorem.** *For each prime  $p$ ,*

$$\text{Cl } \mathbb{Z}C_p \cong \text{Cl } R, \quad D(\mathbb{Z}C_p) = 0$$

where  $R = \mathbb{Z}[\omega]$ , with  $\omega$  a primitive  $p$ -th root of 1 over  $\mathbb{Q}$ .

*Proof.* We have already proved this theorem in Example 42.16, but repeat the argument here with slightly different notation. By (4.38i) we have

$$R/\pi \cong \mathbb{Z}/p, \quad (R/\pi)^* \cong (\mathbb{Z}/p)^*, \quad \text{where } \pi = 1 - \omega.$$

Let  $C_p = \langle x : x^p = 1 \rangle$ , and consider the fiber product

$$(50.3) \quad \begin{array}{ccc} \mathbb{Z}C_p & \xrightarrow{f} & R \\ g \downarrow & & \downarrow \\ \mathbb{Z} & \xrightarrow{\frac{\cdot}{p}} & \mathbb{Z} \cong \frac{R}{\pi}, \end{array}$$

where  $f(x) = \omega$  and  $g(x) = 1$ . By (49.28) and (49.39), there are exact sequences

$$\begin{array}{ccccccc} 1 \rightarrow (\mathbb{Z}C_p)^* & \rightarrow \mathbb{Z}^* \times R^* & \xrightarrow{h} & (R/\pi)^* & \rightarrow \text{Cl } \mathbb{Z}C_p & \rightarrow \text{Cl } \mathbb{Z} \oplus \text{Cl } R & \rightarrow 0 \\ & & & & \searrow & & \\ & & & & D(\mathbb{Z}C_p) & \rightarrow D(\mathbb{Z}) \oplus D(R) & \rightarrow 0. \end{array}$$

Since  $D(\mathbb{Z}) = D(R) = \text{Cl } \mathbb{Z} = 0$ , it suffices to prove that  $h$  is surjective.

Each element of  $(R/\pi)^*$  is of the form  $\bar{n} = n + \pi R$  for some  $n \in \mathbb{Z}$  relatively prime to  $p$ . Since  $\omega$  is expressible as a power of  $\omega^n$ , it follows that

$$(1 - \omega^n)/(1 - \omega) \quad \text{and} \quad (1 - \omega)/(1 - \omega^n) \quad \text{lie in } R.$$

Therefore  $u = (1 - \omega^n)/(1 - \omega) \in R^*$ . Since  $\omega = 1 - \pi$ , we have

$$u = \frac{1 - (1 - \pi)^n}{\pi} \equiv n \pmod{\pi},$$

so  $h(u) = \bar{n}$ . This proves that  $h$  is surjective, and establishes Rim’s Theorem.

We note next that for  $m, n$  relatively prime integers,  $\omega_m \omega_n$  is a primitive  $mn$ -th root of 1 over  $\mathbb{Q}$ . This implies that

$$R_m \otimes_{\mathbb{Z}} R_n \cong R_{mn} \quad \text{when } (m, n) = 1,$$

a fact used repeatedly below. One consequence is an obvious extension of Rim's result:

**(50.4) Corollary.** *Let  $p$  be prime, and assume  $p \nmid m$ . Then.*

$$D(R_m C_p) \cong \text{cok}(R_{mp} \rightarrow (R_{mp}/\pi_p)^{\circ}),$$

using the notation of (50.1).

*Proof.* Applying  $R_m \otimes_{\mathbb{Z}} *$  to (50.3), we obtain a fiber product

$$(50.5) \quad \begin{array}{ccc} R_m C_p & \longrightarrow & R_{mp} \\ \downarrow & & \downarrow \\ R_m & \xrightarrow{\quad R_m \quad} & \frac{R_{mp}}{p} \cong \frac{R_{mp}}{\pi_p}. \end{array}$$

(The isomorphism occurring in this diagram follows from (4.40ii). But the corollary is now an immediate consequence of the Mayer-Vietoris sequence (49.39).

We now turn to a consideration of  $D(\mathbb{Z}C_n)$  for squarefree  $n$ . The case where  $n = 2p$ , with  $p$  an odd prime, is due to Ullom [70]. The general case was treated independently by Cassou-Noguès [72], [74] and Matchett [80]. We follow Matchett's approach, somewhat modified. The symbol  $p$  always denotes a prime (not necessarily odd), and as in (50.1)  $R_p$  means  $\mathbb{Z}[\omega_p]$ , rather than the  $p$ -adic completion of a ring  $R$ . Further, we set  $\pi_p = 1 - \omega_p$ , and

$$\pi_d = \prod_{p|d} (1 - \omega_p) \in R_d.$$

We write  $R_d/\pi_d$  instead of  $R_d/\pi_d R_d$ , for brevity; likewise,  $R_d/p$  means  $R_d/p R_d$ .

The main result exhibits the order of  $D(\mathbb{Z}C_n)$  as a product of the orders of certain cokernels. The explicit calculation of these orders leads to complicated questions in algebraic number theory, concerning the distribution of units of cyclotomic rings  $R_d$  among the residue classes mod  $\pi_d$ . We shall prove:

**(50.6) Theorem.** *Let  $C_n$  be a cyclic group of squarefree order  $n$ . Then*

$$|D(\mathbb{Z}C_n)| = \prod_{d|n} |\text{cok} \{R_d \rightarrow (R_d/\pi_d)^{\circ}\}|,$$

using the notation (50.1) and setting  $\pi_1 = 1$ . In particular, if  $n = pq$  where  $p, q$  are

*distinct primes, then*

$$|D(\mathbb{Z}C_n)| = |\text{cok } \{R_n^\times \rightarrow (R_n/\pi_n)^\times\}|.$$

*Proof.* Step 1. Let  $\Lambda = \mathbb{Z}C_n$ , and let  $\Lambda'$  be the unique maximal  $\mathbb{Z}$ -order in  $A$ , where  $A = QC_n$ . As pointed out at the beginning of this subsection,

$$A \cong \coprod_{d|n} K_d, \quad \Lambda' \cong \coprod_{d|n} R_d,$$

where  $d$  ranges over all positive divisors of  $n$ . Since  $n\Lambda'$  is a two-sided ideal of  $\Lambda$  by (27.1), there is a fiber product

$$\begin{array}{ccc} \Lambda & \longrightarrow & \Lambda' \\ \downarrow & & \downarrow \\ \Lambda/n\Lambda' & \longrightarrow & \Lambda'/n\Lambda'. \end{array}$$

From Exercise 49.10, we obtain an exact sequence

$$1 \rightarrow \Lambda^\times \rightarrow (\Lambda/n\Lambda')^\times \times (\Lambda')^\times \rightarrow (\Lambda'/n\Lambda')^\times \rightarrow D(\Lambda) \rightarrow 0.$$

On the other hand, there is a commutative diagram

$$\begin{array}{ccc} (\Lambda/n\Lambda')^\times & & \\ \psi \downarrow & \searrow \alpha & \\ (\Lambda/n\Lambda')^\times & \xrightarrow{\alpha'} & (\Lambda'/n\Lambda')^\times. \end{array}$$

The map  $\psi$  is surjective, by virtue of the following useful result:

**(50.7) Lemma.** *Let  $\Gamma$  be any semilocal ring<sup>†</sup> (not necessarily commutative) and let  $I$  be any two-sided ideal of  $\Gamma$ . Then the surjection of rings  $\Gamma \rightarrow \Gamma/I$  induces a surjection  $\Gamma^\times \rightarrow (\Gamma/I)^\times$  of groups of units.*

*Proof.* The factor ring  $\Gamma/\text{rad } \Gamma$  is semisimple artinian, by hypothesis. The proof of Exercise 5.12 carries over directly to the present situation, using  $\Gamma$  in place of the ring  $A$  in that exercise.

Step 2. Returning to the proof of the theorem, we observe that since  $\psi$  is surjective, the maps  $\alpha$  and  $\alpha'$  above have the same image in  $(\Lambda'/n\Lambda')^\times$ . Thus there is an exact sequence

$$(\Lambda/n\Lambda')^\times \times (\Lambda')^\times \xrightarrow{(\alpha, \beta)} (\Lambda'/n\Lambda')^\times \rightarrow D(\Lambda) \rightarrow 0,$$

<sup>†</sup>This means that  $\Gamma/\text{rad } \Gamma$  is a semisimple artinian ring. See the discussion in (5.28).

and so  $D(\Lambda) \cong \text{cok } (\alpha, \beta)$ . We shall calculate  $\text{cok } (\alpha, \beta)$  by first determining  $\text{cok } \alpha$ , and then factoring out the image of  $\beta$  in  $\text{cok } \alpha$ .

Consider the natural maps

$$f: \frac{\Lambda}{n\Lambda} \rightarrow \frac{\Lambda'}{n\Lambda'}, \quad \alpha: \left( \frac{\Lambda}{n\Lambda} \right)^* \rightarrow \left( \frac{\Lambda'}{n\Lambda'} \right)^*.$$

Since  $n$  is squarefree, there are decompositions

$$\frac{\Lambda}{n\Lambda} \cong \coprod_{p|n} \frac{\Lambda}{p\Lambda}, \quad \frac{\Lambda'}{n\Lambda'} \cong \coprod_{p|n} \frac{\Lambda'}{p\Lambda'},$$

where  $p$  ranges over the prime divisors of  $n$ . Then  $f = \coprod f_p$ ,  $\alpha = \coprod \alpha_p$ , where

$$f_p: \frac{\Lambda}{p\Lambda} \rightarrow \frac{\Lambda'}{p\Lambda'}, \quad \alpha_p: \left( \frac{\Lambda}{p\Lambda} \right)^* \rightarrow \left( \frac{\Lambda'}{p\Lambda'} \right)^*.$$

Using these maps, we now establish:

**(50.8) Lemma.** *Keeping the above notation, we have*

$$\text{cok } \alpha \cong \prod_{m|n} (R_m/\pi_m)^*.$$

*Proof.* Since  $\Lambda' \cong \coprod_{d|n} R_d$ , we may write (for each prime  $p$  dividing  $n$ )

$$f_p: \frac{\Lambda}{p\Lambda} \rightarrow \coprod_{d|n} \frac{R_d}{p}, \quad \alpha_p: \left( \frac{\Lambda}{p\Lambda} \right)^* \rightarrow \prod_{d|n} \left( \frac{R_d}{p} \right)^*,$$

where (as usual),  $R_d/p$  is an abbreviation for  $R_d/pR_d$ . Let  $\tilde{\Lambda}$  denote the localization of  $\Lambda$  at  $p$ , and  $\tilde{R}_d$  that of  $R_d$ , for  $d|n$ . As in §40, we have

$$\tilde{\Lambda}/p\tilde{\Lambda} \cong \Lambda/p\Lambda, \quad \tilde{R}_d/p\tilde{R}_d \cong R_d/p,$$

so in computing  $\text{cok } f_p$  and  $\text{cok } \alpha_p$ , we may replace  $\Lambda$  and each  $R_d$  by their localizations at  $p$ .

Since localization preserves exactness (see (4.2ii)), the pullback diagram (50.3) yields a fiber product

$$\begin{array}{ccc} \tilde{\mathbb{Z}}C_p & \longrightarrow & \tilde{R}_p \\ \downarrow & & \downarrow \\ \tilde{\mathbb{Z}} & \longrightarrow & \frac{\tilde{\mathbb{Z}}}{p} \cong \frac{\tilde{R}_p}{\pi_p}. \end{array}$$

We apply the exact functor  $\tilde{\mathbb{Z}}C_q \otimes_{\tilde{\mathbb{Z}}} *$  to the above, where  $q = n/p$ . This gives a new

fiber product

$$\begin{array}{ccc} \tilde{\mathbb{Z}}C_n & \longrightarrow & \tilde{R}_p C_q \\ \downarrow & & \downarrow \\ \tilde{\mathbb{Z}}C_q & \xrightarrow[p]{\tilde{\mathbb{Z}}} & \frac{\tilde{R}_p}{\pi_p} C_q \cong \tilde{R}_p C_q. \end{array}$$

But  $q$  is a unit in  $\tilde{R}_p$ , so  $\tilde{R}_p C_q$  is a maximal  $\tilde{R}_p$ -order in  $K_p C_q$ . Therefore we may write

$$\tilde{\mathbb{Z}}C_q \cong \coprod_{d|q} \tilde{R}_d, \quad \tilde{R}_p C_q \cong \coprod_{d|q} \tilde{R}_{pd},$$

where, for the latter formula, we have used the obvious fact that

$$R_p \otimes_{\mathbb{Z}} R_q = \mathbb{Z}[\omega_p] \otimes_{\mathbb{Z}} \mathbb{Z}[\omega_q] \cong \mathbb{Z}[\omega_{pq}]$$

whenever  $(p, q) = 1$ .

The preceding fiber product diagram can thus be written as an exact sequence

$$(50.9) \quad 0 \rightarrow \mathbb{Z}C_n \rightarrow \coprod_{d|q} \{\tilde{R}_d \oplus \tilde{R}_{pd}\} \rightarrow \coprod_{d|q} \tilde{R}_{pd}/\pi_p \rightarrow 0.$$

Viewing  $\mathbb{Z}C_n$  as embedded in  $\tilde{\Lambda}'$ , we may thus describe  $\tilde{\mathbb{Z}}C_n$  as the set of all vectors

$$\langle x_m \in \tilde{R}_m : m|n \rangle$$

satisfying the congruence conditions

$$x_d \equiv x_{pd} \pmod{\pi_p \tilde{R}_{pd}} \quad \text{for each } d \text{ dividing } n/p.$$

On the other hand,  $\mathbb{Z}C_n$  is the intersection of its localizations  $\tilde{\mathbb{Z}}C_n$  as  $p$  ranges over all rational primes. The only restrictions arise from primes  $p$  dividing  $n$ , so we have the useful formula

$$(50.10) \quad \mathbb{Z}C_n = \{ \langle x_m \in R_m : m|n \rangle : x_d \equiv x_{pd} \pmod{\pi_p R_{pd}} \quad \text{for each prime } p \text{ dividing } n, \text{ and each } d \text{ dividing } n/p \}.$$

Passing over to groups of units, we have

$$(50.11) \quad (\mathbb{Z}C_n)^* = \{ \langle x_m \rangle \in \prod_{m|n} R_m^* : x_d x_{pd}^{-1} \equiv 1 \pmod{\pi_p R_{pd}} \text{ for } p|n, d|(n/p) \}.$$

We now apply the right exact functor  $(\tilde{\mathbb{Z}}/p) \otimes_{\mathbb{Z}} *$  to (50.9), obtaining a new exact

sequence

$$\frac{\mathbb{Z}}{p} C_n \rightarrow \coprod_{d|q} \left\{ \frac{\tilde{R}_d}{p} \oplus \frac{\tilde{R}_{pd}}{p} \right\} \rightarrow \coprod_{d|q} \left\{ \frac{\mathbb{Z}}{p} \otimes_{\mathbb{Z}} \frac{\tilde{R}_{pd}}{\pi_p} \right\} \rightarrow 0.$$

But

$$(\tilde{\mathbb{Z}}/p) \otimes_{\mathbb{Z}} (\tilde{R}_{pd}/\pi_p) \cong \tilde{R}_{pd}/\pi_p, \quad \text{since } p \in \pi_p \tilde{R}_{pd}.$$

Passing over to groups of units, we obtain an exact sequence

$$\left( \frac{\Lambda}{p\Lambda} \right)^\cdot \rightarrow \prod_{d|q} \left\{ \left( \frac{R_d}{p} \right)^\cdot \times \left( \frac{R_{pd}}{p} \right)^\cdot \right\} \xrightarrow{\theta} \prod_{d|q} \left( \frac{R_{pd}}{\pi_p} \right)^\cdot \rightarrow 1.$$

Note that we can specify  $\theta$  by the formulas

$$\theta(x_d) = x_d^{-1} \pmod{\pi_p R_{pd}}, \quad \theta(x_{pd}) \equiv x_{pd} \pmod{\pi_p R_{pd}}, \quad \text{for } x_d \in R_d, \quad x_{pd} \in R_{pd}.$$

The last exact sequence can be rewritten thus:

$$\left( \frac{\Lambda}{p\Lambda} \right)^\cdot \xrightarrow{\alpha_p} \prod_{m|n} \left( \frac{R_m}{p} \right)^\cdot \xrightarrow{\theta} \prod_{d|q} \left( \frac{R_{pd}}{\pi_p} \right)^\cdot \rightarrow 1,$$

and consequently we obtain

$$\text{cok } \alpha_p \cong \prod_{d|q} (R_{pd}/\pi_p)^\cdot,$$

where  $q = n/p$ .

We are now ready to complete the proof of Lemma 50.8. We have

$$\text{cok } \alpha = \prod_{p|n} \text{cok } \alpha_p = \prod_{p|n} \prod_{d|n/p} (R_{pd}/\pi_p)^\cdot.$$

Each divisor  $m$  of  $n$ ,  $m > 1$ , occurs as a subscript  $pd$  for some  $p$  and  $d$ . Thus

$$\text{cok } \alpha \cong \prod_{\substack{m|n \\ m>1}} \left\{ \prod_{p|m} \left( \frac{R_m}{\pi_p} \right)^\cdot \right\}.$$

By the Chinese Remainder Theorem we have

$$R_m/\pi_m \cong \coprod_{p|m} R_m/\pi_p,$$

so we obtain

$$\text{cok } \alpha \cong \prod_{\substack{m|n \\ m>1}} (R_m/\pi_m)^\cdot,$$

which yields (50.8) at once.

Step 3. Let  $\beta: (\Lambda')^\cdot \rightarrow (\Lambda'/n\Lambda')^\cdot$ . We have shown in Step 1 that

$$D(\Lambda) \cong \text{cok } \alpha / (\text{image of } \beta \text{ in cok } \alpha),$$

and we must compute the denominator on the right side. We have seen that

$$\text{cok } \alpha \cong \prod_{p|n} \text{cok } \alpha_p, \quad \text{and} \quad \text{cok } \alpha_p \cong \prod_{k|n/p} (R_{pk}/\pi_p)^\cdot.$$

We shall calculate the image of  $\beta$  in each  $\text{cok } \alpha_p$ , and for this it suffices to find the image of an element  $x_d \in R_d^\cdot$ , where  $d|n$ . If  $p \nmid d$ , then by Step 2 we have

$$x_d \in R_d^\cdot \rightarrow x_d^{-1} \in (R_{pd}/\pi_p)^\cdot \cong (R_{pd}/\pi_p)^\cdot,$$

so the image of  $x_d$  in  $\text{cok } \alpha_p$  is precisely  $x_d^{-1} \in (R_{pd}/\pi_p)^\cdot$ , that is, the image is

$$\{1, \dots, x_d^{-1}, 1, \dots, 1\} \in \prod_{k|n/p} (R_{pk}/\pi_p)^\cdot.$$

On the other hand, if  $p|d$  and we write  $d = pd'$ , then  $x_d \in R_d^\cdot$  maps onto  $x_d \pmod{R_{pd}/\pi_p}$ , with all other components 1.

Combining  $p$ -parts for all primes  $p$  dividing  $n$ , we see that the map

$$\gamma: (\Lambda')^\cdot \rightarrow \text{cok } \alpha$$

is given by  $\gamma = \prod_{d|n} \gamma_d$ , where

$$\gamma_d: R_d^\cdot \rightarrow \left\{ \prod_{p|d} (R_{pd}/\pi_p)^\cdot \right\} \times \left\{ \prod_{p|n/d} (R_{pd}/\pi_p)^\cdot \right\},$$

and where the right-hand side is viewed as a direct factor of  $\text{cok } \alpha$ . The map  $\gamma_d$  carries an element  $x_d \in R_d^\cdot$  onto the congruence class of  $x_d$  in each of the first set of factors, and onto the class of  $x_d^{-1}$  in each of the second set of factors. We may therefore write

$$\gamma_d: R_d^\cdot \rightarrow (R_{pd}/\pi_p)^\cdot \times \prod_{p|n/d} (R_{pd}/\pi_p)^\cdot \leq \text{cok } \alpha,$$

where now for  $x_d \in R_d^\cdot$ ,

$$\gamma_d(x_d) = \langle x_d, x_d^{-1}, \dots, x_d^{-1}, 1, \dots, 1 \rangle \in \text{cok } \alpha.$$

It will be convenient to let  $\psi_d$  denote the natural map

$$\psi_d: R_d^\cdot \rightarrow (R_{pd}/\pi_p)^\cdot, \quad d|n.$$

Then of course  $\text{cok } \psi_1 = 1$ , and we are trying to prove that

$$(50.12) \quad |\text{cok } \gamma| = \prod_{d|n} |\text{cok } \psi_d|.$$

In order to use an induction argument, we begin by arranging the distinct positive divisors of  $n$  as a sequence

$$d_0 = 1, d_1, d_2, \dots, d_N = n,$$

in such a way that for  $i < j$ , the number of prime factors of  $d_i$  is  $\leq$  the corresponding number for  $d_j$ . For each  $i$ , put

$$B_i = \prod_{j \geq i} R_{d_j}, \quad Y_i = \prod_{j \geq i} (R_{d_j}/\pi_{d_j}).$$

Then  $\gamma(B_i) \leq Y_i$ , and we have

$$\text{cok } \gamma = \text{cok}(R_1^\bullet \times B_1 \rightarrow Y_1).$$

We shall prove that  $R_1^\bullet \times B_1$  and  $B_1$  have the same image in  $Y_1$ , and shall also show that

$$(50.13) \quad |\text{cok}(B_i \rightarrow Y_i)| = |\text{cok } \psi_{d_i}| |\text{cok}(B_{i+1} \rightarrow Y_{i+1})|.$$

These facts will imply the validity of formula (50.12), by taking  $i = 1, \dots, N - 1$  successively.

*Step 4.* Let us verify that  $\gamma(R_1^\bullet \times B_1) = \gamma(B_1)$  in  $Y_1$ . For any  $x_1 \in R_1^\bullet$ , we choose  $\xi = x_1 1_\Lambda \in \Lambda^\bullet$ . Since  $\gamma(\Lambda^\bullet) = 1$ , it follows that  $\gamma(\xi) = 1$ , and therefore

$$\gamma(x_1) = \gamma(\xi^{-1} x_1), \quad \text{and} \quad \xi^{-1} x_1 \in B_1.$$

This implies that  $\gamma(R_1^\bullet) \leq \gamma(B_1)$ , and establishes the claim.

Next we prove (50.13) for  $1 \leq i \leq N - 1$ . We have

$$\text{cok}(B_i \rightarrow Y_i) = \text{cok}(R_{d_i}^\bullet \times B_{i+1} \rightarrow (R_{d_i}/\pi_{d_i})^\bullet \times Y_{i+1}),$$

and  $\gamma(B_{i+1}) \leq Y_{i+1}$ . By Exercise 50.2 we obtain

$$|\text{cok}(B_i \rightarrow Y_i)| = |\text{cok}(R_{d_i}^\bullet \rightarrow (R_{d_i}/\pi_{d_i})^\bullet)| |\text{cok}(W \rightarrow Y_{i+1})|,$$

where

$$W = \{x \in R_{d_i}^\bullet : x \equiv 1 \pmod{\pi_{d_i}}\} \times B_{i+1}.$$

To complete the proof of (50.13), it remains to show that  $\gamma(W) = \gamma(B_{i+1})$  in  $Y_{i+1}$ .

Let  $x \in R_{d_i}^*$  be such that  $x \equiv 1 \pmod{\pi_{d_i}}$ , and define  $\xi = \langle \xi_{d_j} : 0 \leq j \leq N \rangle \in (\Lambda')$  by the formula

$$\xi_{d_j} = \begin{cases} x & \text{if } d_j \text{ is divisible by } d_i, \\ 1 & \text{otherwise.} \end{cases}$$

Then  $\xi^{-1}x \in B_{i+1}$  (viewed as direct factor of  $(\Lambda')$ ), and we shall show that  $\gamma(\xi) = 1$ . This will imply that  $\gamma(x) = \gamma(\xi^{-1}x) \in \gamma(B_{i+1})$ , so  $\gamma(R_{d_i}^*) \leq \gamma(B_{i+1})$ , as desired.

To prove that  $\gamma(\xi) = 1$ , it suffices to find the image of  $\gamma$  in each  $\text{cok } \alpha_p$ , where  $p$  ranges over the prime divisors of  $n$ , and where

$$\text{cok } \alpha_p = \prod_{d|n/p} (R_{pd}/\pi_p)^*$$

(see Step 2). If the prime  $p$  divides the given  $d_i$ , then  $\pi_p$  is a factor of  $\pi_{d_i}$ , and the image of  $\xi$  (under the map  $\gamma$ ) is 1 in each  $(R_{pd}/\pi_p)^*$ , since  $x \equiv 1 \pmod{\pi_p}$ . On the other hand, if  $p \nmid d_i$ , then the  $\{d_j\}$  which are multiples of  $d_i$  can be grouped into pairs  $\{d_j, pd_j\}$ , where  $p \nmid d_j$ ; then by definition of the map  $\gamma$ , the image  $\gamma(\xi)$  in  $\text{cok } \alpha_p$  is again equal to 1. This shows that  $\gamma(\xi) = 1$ , and completes the proof of (50.13), (50.12), and the first assertion of Theorem 50.6.

Finally, the special case where  $n = pq$  is an immediate consequence of the general case, since we have already shown in the proof of Theorem 50.2 that for each prime  $p$ , the map  $R_p^* \rightarrow (R_p/\pi_p)^*$  is surjective. This completes the proof of Theorem 50.6.

We remark that, just as in (50.4), Theorem 50.6 may be extended to the case in which  $Z$  is replaced by a cyclotomic ring  $R_m$ , with  $(m, n) = 1$ .

We may slightly refine the preceding theorem to obtain:

**(50.14) Theorem (Ullom [70]).** *For  $p$  an odd prime,*

$$D(ZC_{2p}) \cong \text{cok}(R_p^* \rightarrow (R_p/2R_p)^*).$$

*Proof.* From (50.6) we have

$$D(ZC_{2p}) \cong \text{cok}(R_p^* \rightarrow (R_p/2\pi_p)^*) = \text{cok}(R_p^* \rightarrow (R_p/2)^* \times (R_p/\pi_p)^*).$$

By Exercise 50.2, we obtain

$$|D(ZC_{2p})| = |\text{cok}(R_p^* \rightarrow (R_p/2)^*)| |(R_p/\pi_p)^* : \text{im } V|,$$

where

$$V = \{v \in R_p^* : v \equiv 1 \pmod{2R_p}\}.$$

It suffices to establish that  $\text{im } V = (R_p/\pi_p)^*$ , since the proof of Exercise 50.2 will then give the desired isomorphism in (50.14).

We have seen before that each unit of  $R_p/\pi_p$  is of the form  $\bar{u}$  for some unit  $u \in R_p$ . We shall construct a unit  $w \in R_p^\times$  such that

$$(50.15) \quad w \equiv u \pmod{2R_p}, \quad w \equiv 1 \pmod{\pi_p}.$$

For such  $w$  we have  $uw^{-1} \in V$ , and  $uw^{-1}$  has the same image as  $u$  in  $(R_p/\pi_p)^\times$ . Thus  $\text{im } V = (R_p/\pi_p)^\times$ , as desired.

It remains to construct  $w$ . Choose  $\theta \in \text{Gal}(\mathbb{Q}(\omega_p)/\mathbb{Q})$  such that  $\theta(\omega_p) = \omega_p^2$ . Then for all  $z \in R_p$  we have

$$\theta(z) \equiv z^2 \pmod{2} \quad \text{and} \quad \theta(z) \equiv z \pmod{\pi_p},$$

since these hold when  $z$  is any power of  $\omega_p$ , and hence also when  $z \in \mathbb{Z}[\omega_p]$ . Setting  $w = \theta(u)/u$ , it follows that  $w \in R_p^\times$  satisfies the congruences (50.15). This completes the proof.

**Remarks.** (1) For the cyclic group  $C_{2p}$  with  $p$  an odd prime, Ullom [70] obtained lower bounds for the order  $|D(\mathbb{Z}C_{2p})|$  of the kernel group. These results were generalized by Reiner-Ullom [74b] to the case  $C_{pq}$ , with  $p$  and  $q$  distinct primes. Their work was extended by Cassou-Noguès [72], who obtained lower bounds for  $|D(\mathbb{Z}C_{pq})|$  for various numerical values of  $p$  and  $q$ .

(2) If  $G \rightarrow \bar{G}$  is a surjection of finite groups, then by (49.38) there is an induced surjection  $D(\mathbb{Z}G) \rightarrow D(\mathbb{Z}\bar{G})$ , so  $|D(\mathbb{Z}\bar{G})|$  divides  $|D(\mathbb{Z}G)|$ . In particular, if  $G$  is an abelian group having a factor group of type  $C_{pq}$ , with  $p$  and  $q$  distinct primes, one obtains a lower bound for  $|D(\mathbb{Z}G)|$ . This is one of the key steps in proving:

**(50.16) Theorem** (Cassou-Noguès [72]). *For  $G$  a finite abelian group,  $D(\mathbb{Z}G) = 0$  precisely for the following groups  $G$ :*

- (i)  $G$  has prime order,
- (ii)  $G$  is cyclic of order 4, 6, 8, 9, 10, 14,
- (iii)  $G$  is an elementary group of type (2, 2).

Since  $D(\mathbb{Z}G)$  and  $\text{Cl } \mathbb{Z}G$  differ by class groups of rings of cyclotomic integers, and since  $|\text{Cl } R_p| > 1$  whenever  $p \geq 23$ , one obtains (Cassou-Noguès [72]):

**(50.17) Corollary.** *Let  $G$  be a finite abelian group. Then  $\text{Cl } \mathbb{Z}G = 0$  for precisely the following groups:*

- (i)  $G$  cyclic of order  $n$ ,  $1 \leq n \leq 11$
- (ii)  $G$  cyclic of order 13, 14, 17, 19
- (iii)  $G$  elementary abelian of type (2, 2).

### §50B. The Kernel Group for $p$ -Groups

The aim of this subsection is to prove the fundamental result that when  $G$  is a finite  $p$ -group, where  $p$  is prime, then the kernel group  $D(ZG)$  is also a  $p$ -group. Before starting the proof, we remark that the result depends strongly on the fact that the coefficient ring is  $\mathbb{Z}$ , rather than a more general ring of algebraic integers. Further, it is tempting to conjecture that for arbitrary  $G$ , each prime factor of  $|D(ZG)|$  must divide  $|G|$ . However, this conjecture is definitely false, as can be seen from the examples at the end of §50A. Indeed, let  $C_{2p}$  be a cyclic group of order  $2p$ . Then for suitably chosen odd primes  $p$ , it happens that  $|D(ZC_{2p})|$  has odd prime factors different from  $p$ .

The following theorem was proved first by Fröhlich [69] for the case of abelian  $p$ -groups, and then for the general case by Reiner-Ullom [72]:

**(50.18) Theorem.** *Let  $G$  be a  $p$ -group, where  $p$  is prime. Then  $D(ZG)$  is also a  $p$ -group.*

*Proof.* We revert to our earlier notation, in which the subscript  $p$  indicates  $p$ -adic completion. We shall give a simplified version of the Reiner-Ullom proof, by making use of Fröhlich's formula for kernel groups, and some easy facts about pro- $p$ -groups.

Let  $\Lambda = \mathbb{Z}G$ , where  $G$  is a  $p$ -group. The set  $S(\Lambda)$  in (49.1) consists of the single prime  $p$ . From (49.40) we obtain

$$D(\Lambda) \cong \mathfrak{O}_p^\times / \mathfrak{O}^+ \text{nr } \Lambda_p^\times,$$

where  $\mathfrak{O}$  is the integral closure of  $\mathbb{Z}$  in the center  $C$  of  $\mathbb{Q}G$ .

*Case 1.*  $p$  odd. By Schilling's Theorem 74.17, we may write

$$A = \mathbb{Q}G \cong \coprod M_{n_i}(F_i), \quad C = \coprod F_i, \quad \mathfrak{O} = \coprod R_i$$

where each  $F_i$  is a cyclotomic field  $\mathbb{Q}(\omega_i)$  for some  $p$ -power root of unity  $\omega_i$ . There is exactly one simple component  $A_i$  of  $A$  for which  $F_i = \mathbb{Q}$ , say  $A_1$ , and then  $A_1 = F_1 = \mathbb{Q}$ . By (4.38), there is a unique prime ideal  $P_i$  of  $R_i$  containing  $p$ , and we have  $R_i/P_i \cong \mathbb{Z}/p\mathbb{Z}$ . Further, the  $p$ -adic completion of  $R_i$  coincides with its  $P_i$ -adic completion, which we now denote by  $\hat{R}_i$ . Thus

$$\mathfrak{O}_p = \coprod \hat{R}_i, \quad \text{and} \quad \mathfrak{O}_p^\times = \coprod (\hat{R}_i)^\times.$$

On the other hand, no infinite primes ramify in this case, so  $C^+ = C$  and  $\mathfrak{O}^+ = \mathfrak{O}^\times$ . Thus we obtain

$$D(\Lambda) \cong \mathfrak{O}_p^\times / \mathfrak{O}^\times \text{nr } \Lambda_p^\times.$$

Now let  $\alpha = \sum \alpha_i \in \mathfrak{O}_p^\times$ , with  $\alpha_i \in (\hat{R}_i)^\times$  for each  $i$ . Then  $\alpha_i \equiv a_i \pmod{\hat{P}_i}$  for

some  $a_i \in \mathbb{Z}$ . Choose  $t \in \mathbb{Z}$  with  $(t, p) = 1$ , such that  $ta_1 \equiv 1 \pmod{\hat{P}_1}$ . Viewing  $t$  as element of  $\Lambda_p^\circ$ , we note that  $\text{nr}(t)$  has component  $t$  in  $\hat{A}_1$ . Replacing  $\alpha$  by  $\alpha \cdot \text{nr}(t)$ , which does not affect the image of  $\alpha$  in  $D(\Lambda)$ , we may hereafter assume that  $\alpha_1 \equiv 1 \pmod{\hat{P}_1}$ .

On the other hand, as shown in the proof of (50.2), for each  $i > 1$  there exists a unit  $u_i \in R_i^\circ$  with  $u_i a_i \equiv 1 \pmod{\hat{P}_i}$ . Replacing  $\alpha$  by  $\alpha \cdot \prod u_i$  again does not change its image in  $D(\Lambda)$ , so after changing notation, we may write

$$\alpha = \sum \alpha_i, \quad \text{where } \alpha_i \equiv 1 \pmod{\hat{P}_i} \text{ for each } i.$$

Thus there exists a surjection

$$1 + \coprod \hat{P}_i \rightarrow \mathfrak{O}_p^\circ / \mathfrak{O}^\circ \text{nr } \Lambda_p^\circ.$$

The left-hand expression is a pro- $p$ -group by (45.29), while the right side is a finite group, and is therefore a finite  $p$ -group (see Exercise 45.9).

*Case 2.*  $p = 2$ . By (74.18) we may write

$$A = \coprod A_i \text{ (simple components)}, \quad C = \coprod F_i, \quad F_i = \text{center of } A_i,$$

where for each  $i$ ,  $F_i$  is a subfield of  $E_i = \mathbb{Q}(\omega_i)$ , with  $\omega_i$  a 2-power root of unity. Let

$$R_i = \text{alg. int. } \{F_i\}, \quad S_i = \text{alg. int. } \{E_i\}.$$

Now we have

$$D(\Lambda) \cong \mathfrak{O}_2^\circ / \mathfrak{O}^+ \text{nr } \Lambda_2^\circ,$$

and  $\mathfrak{O}^\circ / \mathfrak{O}^+$  is a finite 2-group, so in order to prove that  $D(\Lambda)$  is a 2-group, it suffices to show that  $\mathfrak{O}_2^\circ / \mathfrak{O}^\circ \text{nr } \Lambda_2^\circ$  is a 2-group.

The prime 2 ramifies completely in  $E_i$ , and hence also in  $F_i$ . Let  $P_i$  and  $\mathfrak{P}_i$  be the unique prime ideals containing 2 in  $R_i$  and  $S_i$ , respectively. Then

$$S_i / \mathfrak{P}_i \cong R_i / P_i \cong \mathbb{Z}/2\mathbb{Z},$$

and the same isomorphisms hold when we pass to 2-adic completions. Now let  $\alpha = \sum \alpha_i \in \mathfrak{O}_2^\circ$ , with each  $\alpha_i \in \hat{R}_i$ . Since  $\hat{R}_i / \hat{P}_i \cong \mathbb{Z}/2\mathbb{Z}$ , we have  $\alpha_i \equiv 1 \pmod{\hat{P}_i}$ . But then, as in Case 1, there is a surjection

$$1 + \coprod \hat{P}_i \rightarrow \mathfrak{O}_2^\circ / \mathfrak{O}^\circ \text{nr } \Lambda_2^\circ,$$

and the left-hand expression is a pro-2-group. This completes the proof.

S. Ullom has pointed out another proof of Theorem 50.18. To begin with, a simplified version of the above proof shows that for each *cyclic*  $p$ -group  $C$ ,

the kernel group  $D(ZC)$  is a  $p$ -group. Now let  $G$  be an arbitrary  $p$ -group, and  $\mathcal{C}$  the set of cyclic subgroups of  $G$ . As in (38.12), define

$$D(ZG)_{\mathcal{C}} = \sum_{C \in \mathcal{C}} \text{ind}_C^G D(ZC).$$

Then  $D(ZG)_{\mathcal{C}}$  is a  $p$ -group, since each  $D(ZC)$  is a  $p$ -group. On the other hand, by (49.47),  $D(ZG)$  is a Frobenius module over the Frobenius functor  $G_0(\mathbb{Q}G)$ . The Artin Induction Theorem shows that

$$|G| \cdot G_0(\mathbb{Q}G) \subseteq G_0(\mathbb{Q}G)_{\mathcal{C}},$$

so by (38.14) we may conclude that

$$|G| \cdot D(ZG) \subseteq D(ZG)_{\mathcal{C}}.$$

Therefore  $D(ZG)$  is a  $p$ -group, as claimed.

As shown by Ullom [74], the proof of (50.18) can be refined so as to yield an upper bound on the exponent  $e(G)$  of the finite  $p$ -group  $D(ZG)$ . The main result is:

**(50.19) Theorem (Ullom [74]).** *Let  $G$  be a group of order  $p^n$ , where  $p$  is prime, and let  $e(G)$  be the exponent of the kernel group  $D(ZG)$ . Then*

- (i) *For odd  $p$ ,  $e(G)$  divides  $p^{n-1}$ .*
- (ii) *For  $p = 2$ ,  $e(G)$  divides  $2^{n-2}$ .*

*Proof.* We restrict our attention to the easier case of odd  $p$ . Keeping the notation of Case 1 in the proof of (50.18), we saw there that

$$(50.20) \quad D(\Lambda) \cong \mathfrak{O}_p^\times / \mathfrak{O}^\times \text{nr } \Lambda_p^\times,$$

and that each element of  $D(\Lambda)$  can be represented as the image of an element  $\alpha = \sum \alpha_i$ , where

$$\alpha_i \in (\hat{R}_i)^\times, \quad \alpha_i \equiv 1 \pmod{\hat{P}_i} \quad \text{for each } i.$$

On the other hand, since  $\Lambda_q' = \Lambda_q$  for each prime  $q \neq p$ , the formula for  $D(\Lambda)$  in the proof of (49.38) takes the form

$$(50.21) \quad D(\Lambda) \cong \frac{\text{im } K_1(A) \cdot \text{im } K_1(\Lambda_p')}{\text{im } K_1(A) \cdot \text{im } K_1(\Lambda_p)},$$

where all these images are contained in  $K_1(A_p)$ . Formula (49.40) is obtained

from the above by applying the reduced norm map

$$\text{nr}: K_1(A_p) \rightarrow C_p^*,$$

which induces isomorphisms

$$\text{im } K_1(A) \cong C^*, \quad \text{im } K_1(\Lambda'_p) \cong \mathfrak{D}_p^*, \quad \text{im } K_1(\Lambda_p) \cong \text{nr } \Lambda_p^*.$$

Further, in this situation  $A_p$  is a direct sum of matrix algebras over fields, and we have

$$A_p \cong \coprod_i M_{n_i}(\hat{F}_i), \quad \Lambda'_p = \coprod_i \Lambda_i, \quad \text{where } \Lambda_i \cong M_{n_i}(\hat{R}_i).$$

Here,  $\hat{F}_i$  and  $\hat{R}_i$  denote the  $p$ -adic completions of  $F_i$  and  $R_i$ , respectively. The reduced norm map in this case is just the usual determinant map, computed componentwise.

Let  $\xi \in D(\Lambda)$  be represented (via formula (50.20)) by an element  $\alpha = \sum \alpha_i$  as above. Define

$$\beta = \sum \beta_i, \quad \text{where } \beta_i = \text{diag}(1, \dots, 1, \alpha_i) \in \Lambda_i^*.$$

Then  $\text{nr } \beta = \alpha$ , and via formula (50.21)  $\beta$  represents the element  $\xi \in D(\Lambda)$ . Clearly

$$\beta_i \equiv 1 \pmod{\hat{P}_i \Lambda_i} \quad \text{for each } i.$$

and to prove the theorem, we need only show that these congruences imply that  $\beta^{p^{n-1}} \in \Lambda_p^*$ . In fact, since  $\beta \in (\Lambda'_p)^*$ , it suffices to show that  $\beta^{p^{n-1}} \in \Lambda_p$ . (We may assume  $n \geq 1$ , since the result is trivial when  $n = 0$ .)

Let  $(\Lambda':\Lambda)_l$  be the left conductor of  $\Lambda'$  into  $\Lambda$ . By Jacobinski's Theorem 27.8, we have

$$(\Lambda'_p:\Lambda_p)_l = \coprod_i (p^n/n_i) \mathfrak{D}_i^{-1} \subseteq \Lambda_p,$$

where  $\mathfrak{D}_i^{-1} = \mathfrak{D}^{-1}(\Lambda_i/\hat{Z})$  is the inverse different of  $\Lambda_i$  relative to  $\hat{Z}$ , defined in terms of the reduced trace. The proof of (27.13) gives

$$\mathfrak{D}^{-1}(\Lambda_i/\hat{Z}) = \mathfrak{D}^{-1}(\Lambda_i/\hat{R}_i) \cdot \mathfrak{D}^{-1}(\hat{R}_i/\hat{Z}).$$

However, since  $\Lambda_i \cong M_{n_i}(\hat{R}_i)$ , it is easily verified that  $\mathfrak{D}^{-1}(\Lambda_i/\hat{R}_i) = \Lambda_i$  (see MO(25.7), for example). We thus obtain

$$(\Lambda'_p:\Lambda_p)_l = \coprod_i (p^n/n_i) \mathfrak{D}^{-1}(\hat{R}_i/\hat{Z}) \Lambda_i \subseteq \Lambda_p.$$

It therefore suffices to show (for each  $i$ ) that

$$\alpha_i \in \widehat{R}_i, \quad \alpha_i \equiv 1 \pmod{\widehat{P}_i} \Rightarrow \alpha_i^{p^{n-1}} \equiv 1 \pmod{(p^n/n_i)\mathfrak{D}^{-1}(\widehat{R}_i/\widehat{Z})}.$$

To simplify the notation, drop the subscript  $i$ , and let

$$\widehat{F} = \widehat{\mathbb{Q}}(\omega), \quad \widehat{R} = \widehat{\mathbb{Z}}[\omega], \quad \widehat{P} = \pi\widehat{R}, \quad \text{where } \omega \text{ is a primitive } p^m\text{-th root of 1.}$$

Here, we have  $0 \leq m \leq n$ , and  $\pi = p$  if  $m = 0$ ,  $\pi = 1 - \omega$  if  $m > 0$ . By Exercise 50.8, we know that

$$\mathfrak{D}(\widehat{R}/\widehat{Z}) = \widehat{P}^t, \quad \text{where } t = m\varphi(p^m) - p^{m-1} \quad \text{if } m \geq 1.$$

It therefore suffices to prove

$$(50.22) \quad (1 + \pi z)^{p^{n-1}} \equiv 1 \pmod{p^n \pi^{-t} \widehat{R}} \quad \text{for } z \in \widehat{R}.$$

This is clear (by induction on  $n$ ) when  $m = 0$ , for then  $\pi = p$ ,  $\widehat{R} = \widehat{\mathbb{Z}}$ , and  $t = 0$ .

Now let  $m \geq 1$ . We shall show that

$$(50.23) \quad (1 + \pi z)^{p^{m-1}} \equiv 1 \pmod{p^m \pi^{-t} \widehat{R}} \quad \text{for } z \in \widehat{R}.$$

Once this is established, we may then deduce (50.22) by raising both sides of (50.23) to the  $p$ -th power  $n - m$  times. Let  $v$  be the exponential valuation on  $\widehat{F}$ , normalized so that  $v(\pi) = 1$ . Then

$$v(p^m \pi^{-t}) = mv(p) - t = m\varphi(p^m) - t = p^{m-1}.$$

Let  $X$  be an indeterminate, and define

$$g(X) = \{(1 + \pi X)^{p^{m-1}} - 1\}/X \in \widehat{R}[X].$$

It then suffices to prove that  $v(a_i) \geq p^{m-1}$  for each coefficient  $a_i$  of  $g(X)$ . Note that  $v(a_0) = p^{m-1}$ , where  $a_0$  is the leading coefficient of  $g(X)$ . We may assume  $m > 1$ , since  $g(X) = \pi$  when  $m = 1$ .

We shall use the Newton polygon of  $g(X)$  (see §51B). For each root  $\alpha$  of the equation  $g(X) = 0$ , we obtain

$$(1 + \pi\alpha)^{p^{m-1}} = 1, \quad \alpha \neq 0.$$

Therefore we may write

$$1 + \pi\alpha = \omega^{pk} \text{ for some } k, \quad \text{so } \alpha = (\omega^{pk} - 1)/\pi.$$

This implies that

$$v(\alpha) = v(\omega^{pk} - 1) - 1 \geq p - 1,$$

the inequality holding because  $\omega^{pk} - 1$  is a prime element in some proper cyclotomic subfield of  $\hat{F}$ . It follows that the slope of each side of the Newton polygon for  $g(X)$  is positive, so  $v(a_i) \geq v(a_0)$  for each coefficient  $a_i$  of  $g(X)$ . This proves (50.23), and completes the proof of the theorem for odd  $p$ .

The theorem is in some sense best possible, since Galovich [74] showed that for  $G$  cyclic of order  $p^n, p > 3$ , the exponent of the kernel group  $D(ZG)$  is precisely  $p^{n-1}$ .

### §50C. Metacyclic Groups

In this subsection we discuss the class group  $\text{Cl } ZG$  and kernel group  $D(ZG)$  for metacyclic groups  $G$ . We shall begin with a detailed treatment of the case in which

$$(50.24) \quad G = \langle x, y : x^p = 1, y^q = 1, yxy^{-1} = x^r \rangle,$$

where  $p$  is an odd prime,  $q$  is any divisor of  $p-1$ , and  $r$  is a primitive  $q$ -th root of  $1 \pmod{p}$ . Thus  $G$  is a semidirect product  $\langle x \rangle \rtimes \langle y \rangle$ , where the cyclic group  $\langle y \rangle$  acts faithfully on the cyclic subgroup  $\langle x \rangle$  by conjugation. Note that  $G$  has trivial center. We shall prove the following result of Galovich-Reiner-Ullom [72]:

**(50.25) Theorem.** *Let  $G$  be as above, and let  $\omega$  be a primitive  $p$ -th root of 1 over  $\mathbb{Q}$ . Set*

$$K = \mathbb{Q}(\omega), \quad R = \text{alg. int. } \{K\} = \mathbb{Z}[\omega].$$

*Let  $L$  be the unique subfield of  $K$  with  $\dim_L K = q$ , that is,  $L$  is the subfield of  $K$  fixed by the automorphism  $\sigma$  defined by  $\omega^\sigma = \omega^r$ . Let  $S = \text{alg. int. } \{L\}$ , and set  $H = \langle y : y^q = 1 \rangle$ .*

*Then there are exact sequences of finite abelian groups*

$$0 \rightarrow D_0 \rightarrow \text{Cl } ZG \rightarrow \text{Cl } S \oplus \text{Cl } ZH \rightarrow 0, \quad 0 \rightarrow D_0 \rightarrow D(ZG) \rightarrow D(ZH) \rightarrow 0,$$

*where  $D_0$  is a cyclic group, and where*

$$|D_0| = \begin{cases} q & \text{if } q \text{ is odd,} \\ q/2 & \text{if } q \text{ is even.} \end{cases}$$

*In particular, for  $q = 2$  and  $p$  an odd prime,  $G$  is the dihedral group of order  $2p$ , and*

$$\text{Cl } ZG \cong \text{Cl } S, \quad D(ZG) = 0, \quad \text{where } S = \mathbb{Z}[\omega + \omega^{-1}].$$

*Proof.* Step 1. The Galois group of  $K/\mathbb{Q}$  is cyclic of order  $p-1$ , and the

automorphism  $\sigma$  of  $K$  has order  $q$  in this group. Therefore the fixed field  $L$  of  $\langle \sigma \rangle$  is the unique subfield of  $K$  for which  $\dim_L K = q$ .

As in (34.43), there is a fiber product

$$\begin{array}{ccc} \Lambda = \mathbb{Z}G & \xrightarrow{f_1} & R \circ H \\ f_2 \downarrow & & g_1 \downarrow \\ \mathbb{Z}H & \xrightarrow{g_2} & \bar{\mathbb{Z}}H, \end{array}$$

where

$$\bar{\mathbb{Z}} = \mathbb{Z}/p\mathbb{Z} \cong R/(1 - \omega)R,$$

and where  $f_1(x) = \omega$ ,  $f_2(x) = 1$ . In the twisted group ring  $R \circ H$  we have

$$y\alpha = \alpha^\sigma y, \quad \alpha \in R,$$

where  $\sigma$  is the automorphism of  $R$  for which  $\omega^\sigma = \omega^r$ .

Next, we note that  $\mathbb{Q}G \cong \mathbb{Q}H \oplus K \circ H$ , so  $\mathbb{Q}G$  satisfies the Eichler condition. Therefore (see (51.24))  $\mathbb{Z}G$  has locally free cancellation, and by (49.30) we obtain an exact sequence

$$1 \rightarrow W \rightarrow (\bar{\mathbb{Z}}H)^* \rightarrow \text{Cl } \Lambda \rightarrow \text{Cl } R \circ H \oplus \text{Cl } \mathbb{Z}H \rightarrow 0,$$

where  $W$  is the subgroup of  $(\bar{\mathbb{Z}}H)^*$  generated by the images of  $(\mathbb{Z}H)^*$  and  $(R \circ H)^*$ . Since  $(\mathbb{Z}H)^* \leq (R \circ H)^*$ , the subgroup  $W$  is precisely the image of  $(R \circ H)^*$  in  $(\bar{\mathbb{Z}}H)^*$ .

Next, we recall the proof that  $R \circ H$  is a hereditary order (see §34E or (28.7)). In the extension  $K/L$ , there is a unique prime ideal  $P_0$  of  $S$  ramified in  $R$ , namely, the prime ideal containing  $p$ . Then  $P_0R = P^q$ , where  $P = (1 - \omega)R$  is the prime ideal of  $R$  containing  $p$ , and we have

$$S/P_0 \cong R/P \cong \bar{\mathbb{Z}} = \mathbb{Z}/p\mathbb{Z}.$$

Since  $p \nmid q$ , it follows from Exercise 4.12 that  $R$  is tamely ramified over  $S$ . Therefore  $R \circ H$  is hereditary, by (28.7) and the discussion following it.

By (49.35) we obtain

$$D(R \circ H) = 0, \quad \text{Cl } R \circ H \cong \text{Cl } \Gamma,$$

where  $\Gamma$  is a maximal  $\mathbb{Z}$ -order in the twisted group algebra  $K \circ H$ . But  $K \circ H \cong M_q(L)$  by (28.3), and  $S$  is the integral closure of  $\mathbb{Z}$  in the center  $L$  of  $K \circ H$ , so  $\text{Cl } \Gamma \cong \text{Cl } S$  by (49.32). Thus we have exact sequences

$$1 \rightarrow \text{image of } (R \circ H)^* \rightarrow (\bar{\mathbb{Z}}H)^* \rightarrow \text{Cl } \Lambda \rightarrow \text{Cl } S \oplus \text{Cl } \mathbb{Z}H \rightarrow 0$$

$\searrow D(\Lambda) \rightarrow D(\mathbb{Z}H) \rightarrow 0.$

Let

$$D_0 = (\bar{Z}H) / \text{image of } (R \circ H).$$

To complete the proof, we must show that  $D_0$  is cyclic of order  $q$  if  $q$  is odd, and of order  $q/2$  if  $q$  is even.

*Step 2.* The homomorphism  $S \rightarrow S/P_0 \cong \bar{Z}$  maps  $S^\circ$  into  $\bar{Z}^\circ$ . We show next that  $\bar{Z}^\circ/\text{im } S^\circ$  is cyclic of order  $q$  or  $q/2$ , depending on whether  $q$  is odd or even. We note first that  $L$  is a Galois extension of  $\mathbb{Q}$ , whose Galois group  $\text{Gal}(L/\mathbb{Q})$  is cyclic of order  $m$ , where

$$p - 1 = qm.$$

Each  $\tau \in \text{Gal}(L/\mathbb{Q})$  induces an element  $\bar{\tau} \in \text{Gal}(\bar{S}/\bar{Z})$ , where  $\bar{S} = S/P_0$ . Since  $\bar{S} \cong \bar{Z}$ , we obtain

$$u^\tau \equiv u \pmod{P_0} \quad \text{for all } u \in S^\circ.$$

Multiplying these congruences, where  $\tau$  ranges over  $\text{Gal}(L/\mathbb{Q})$ , we obtain

$$N_{L/\mathbb{Q}} u = \prod_{\tau} u^\tau \equiv u^m \pmod{P_0},$$

where  $N_{L/\mathbb{Q}}$  is the norm from  $L$  to  $\mathbb{Q}$  (see CR, §20B). Now suppose that  $u \in S^\circ$ ; then  $N_{L/\mathbb{Q}} u = \pm 1$ , and so we obtain

$$u^m \equiv \pm 1 \pmod{P_0} \quad \text{for all } u \in S^\circ.$$

Furthermore, the field  $K$  is totally imaginary, that is, there are no real primes of  $K$ . Hence any real prime of  $L$  must split into an even number of complex primes of  $K$ , so  $\dim_L K$  must be even if  $L$  has any real primes. Thus if  $q$  is odd, it follows that  $L$  is also totally imaginary, and therefore  $N_{L/\mathbb{Q}} u = +1$  for  $u \in S^\circ$ . Thus for  $q$  odd we have

$$u^m \equiv 1 \pmod{P_0} \quad \text{for all } u \in S^\circ.$$

*Case 1.*  $q$  even. Let

$$T = \{x \in \bar{Z}^\circ : x^{2m} = 1\},$$

a subgroup of  $\bar{Z}^\circ$  of order  $2m$ . We shall show that  $\text{im } S^\circ = T$ , so  $|\bar{Z}^\circ/\text{im } S^\circ| = (p-1)/2m = q/2$ , as desired. The preceding discussion shows that  $u^{2m} \equiv 1 \pmod{P_0}$  for every  $u \in S^\circ$ , and therefore  $\text{im } S^\circ \leq T$ .

For the reverse inclusion, let  $\bar{a} \in \bar{Z}^\circ$ , where  $a \in \mathbb{Z}$  is prime to  $p$ . Let  $K^+ = Q(\omega + \bar{\omega})$ ,  $R^+ = \text{alg. int. } \{K^+\}$ , so  $K^+$  is the maximal real subfield of  $K$ ,

and  $\dim_{K^+} K = 2$ . Since  $q$  is even,  $L$  is a subfield of  $K^+$ . Now set

$$\xi_a = (\omega^a - \omega^{-a})/(\omega - \omega^{-1}) \in (R^+).$$

As in the proof of (34.31), we have

$$\xi_a \equiv a \pmod{P^+}, \quad \text{where } P^+ = R^+ \cap P.$$

Let  $u_a = N_{K^+/L}\xi_a$ , so  $u_a \in S^\circ$ . Taking norms from  $K^+$  to  $L$  in the above congruence, we obtain

$$u_a \equiv a^{q/2} \pmod{P_0}.$$

Thus

$$\text{im } S^\circ \geq \{\bar{a}^{q/2} : \bar{a} \in \bar{Z}^\circ\} = T,$$

which completes the proof that  $Z^\circ/\text{im } S^\circ$  is cyclic of order  $q/2$  for  $q$  even.

*Case 2.*  $q$  odd. It suffices to show that  $\text{im } S^\circ = T_1$ , where

$$T_1 = \{x \in \bar{Z}^\circ : x^m = 1\}.$$

The earlier discussion shows that  $\text{im } S^\circ \leq T_1$ , so we need only prove the reverse inclusion. In this case, let  $\xi_a$  be as above, and set  $v_a = N_{K/L}\xi_a \in S^\circ$ . Then

$$v_a \equiv a^q \pmod{P_0},$$

so

$$\text{im } S^\circ \geq \{\bar{a}^q : \bar{a} \in \bar{Z}^\circ\} = T_1,$$

and we are through.

*Step 3.* To complete the proof of the theorem, we shall exhibit an isomorphism

$$(50.26) \quad \theta : \frac{(\bar{Z}H)^\circ}{\text{im } (R^\circ H)} \cong \frac{\bar{Z}^\circ}{\text{im } S^\circ},$$

which will be given by a determinant map. We shall compute  $(R^\circ H)^\circ$  by observing that this group of units is anti-isomorphic to the automorphism group of  $R^\circ H$  as left  $(R^\circ H)$ -module. Now we have an isomorphism

$$\varphi : (R^\circ H)/(P^\circ H) \cong \bar{Z}H = \text{direct sum of } q \text{ simple modules},$$

using the fact that  $\bar{Z}$  contains the  $q$ -th roots of 1. Furthermore,

$$R = \mathbb{Z}[\omega] = S[\omega] = S \oplus S\omega \oplus \cdots \oplus S\omega^{q-1},$$

a free  $S$ -module. The discussion in Volume I (pages 597–599) then shows that

$$R \circ H \cong R \oplus P \oplus P^2 \oplus \cdots \oplus P^{q-1}$$

as left  $(R \circ H)$ -modules. For each  $i$ ,  $P^i$  is the module on which  $R$  acts naturally, and the generator  $y$  of  $H$  acts as the automorphism  $\sigma \in \text{Gal}(K/L)$ . We use this isomorphism to establish:

**(50.27) Lemma.** *The group  $(R \circ H)^*$  is isomorphic to the group of all  $q \times q$  matrices  $(\alpha_{ij}) \in GL_q(S)$  whose entries below the main diagonal all lie in  $P_0$ .*

*Proof.* We compute  $\text{End}_{R \circ H}(R \circ H)$ , using the module structure of  $R \circ H$ , so

$$\text{End}(R \circ H) \cong \bigoplus_{i,j=0}^{q-1} \text{Hom}_{R \circ H}(P^i, P^j).$$

Now  $KP^i \cong KP^j \cong K$ , the unique simple  $(K \circ H)$ -module, and  $\text{End}_{K \circ H} K \cong L$ . Therefore

$$\text{Hom}_{R \circ H}(P^j, P^i) = L \cap P^{i-j} = \begin{cases} S, & i \leq j, \\ P_0, & i > j, \end{cases}$$

using the fact that  $P_0 R = P^q$ . Thus the units of  $\text{End } R \circ H$  are represented by matrices in  $GL_q(S)$  whose entries above the main diagonal lie in  $P_0$ . Now take transposes because of the anti-isomorphism between  $(R \circ H)^*$  and the units of  $\text{End } R \circ H$ , so the lemma is proved.

We shall use this description of  $(R \circ H)^*$  to calculate its image  $\varphi((R \circ H)^*)$  in  $(\bar{Z}H)^*$ . We have

$$\bar{Z}H \cong (R \circ H)/P(R \circ H) \cong \coprod_{i=0}^{q-1} (P^i/P^{i+1}),$$

and the  $\{P^i/P^{i+1}\}$  are a full set of simple  $\bar{Z}H$ -modules. Identifying  $\bar{Z}H$  with the endomorphism ring of the left regular module, we find that if  $u \in (R \circ H)^*$  is represented by a matrix  $(\alpha_{ij}) \in GL_q(S)$  as in the lemma, then  $\varphi(u)$  is represented by a matrix

$$\text{diag}(\bar{\alpha}_{11}, \dots, \bar{\alpha}_{qq}) \in GL_q(\bar{Z}),$$

where bars denote images in  $S/P_0$ . Therefore we may identify  $(\bar{Z}H)^*$  with the group of all diagonal matrices in  $GL_q(\bar{Z})$ , and  $\varphi(R \circ H)$  with those diagonal matrices which come from a matrix  $(\alpha_{ij}) \in GL_q(S)$  whose entries below the main diagonal lie in  $P_0$ .

Now consider the commutative diagram

$$\begin{array}{ccc} (R \circ H)^\cdot & \longrightarrow & (\bar{Z}H)^\cdot \\ \det \downarrow & & \det \downarrow \\ S^\cdot & \longrightarrow & \bar{Z}^\cdot. \end{array}$$

where the lower arrow arises from the map  $S \rightarrow S/P_0 \cong \bar{Z}$ . There is then an induced map  $\theta$  as in (50.26), which is surjective since  $\det: (\bar{Z}H)^\cdot \rightarrow \bar{Z}^\cdot$  is surjective. It remains to prove  $\theta$  injective, so let

$$x = \text{diag}(\beta_1, \dots, \beta_q) \in GL_q(\bar{Z})$$

be such that  $\theta(x) = 1$ , that is,  $\prod \beta_i \in \text{im } S^\cdot$ . Then  $\prod \beta_i = \bar{u}$  for some  $u \in S^\cdot$ ; choose elements  $\alpha_i \in S$  with  $\bar{\alpha}_i = \beta_i$ , and then  $\prod \alpha_i = u + \pi_0$  for some  $\pi_0 \in P_0$ . We now choose  $y \in M_q(S)$  as follows:

$$\begin{bmatrix} \alpha_1 & 1 & 0 & \cdots & 0 \\ 0 & \alpha_2 & 1 & \cdots & 0 \\ 0 & 0 & \alpha_3 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ (-1)^q \pi_0 & 0 & 0 & \cdots & \alpha_q \end{bmatrix}$$

(for  $q = 1$ , let  $y = (u)$ ). Then for  $q \geq 1$ ,

$$\det y = \prod_i \alpha_i - \pi_0 = u,$$

so  $y \in GL_q(S)$  represents an element of  $(R \circ H)^\cdot$ . We have  $x = \text{image of } y \text{ in } (\bar{Z}H)^\cdot$ , so  $\theta$  is injective, as desired. This completes the proof of the theorem.

The special case of Theorem 50.25, in which  $G$  is dihedral of order  $2p$ , is due originally to Reiner-Ullom [72]. We remark also that (in the general case) we have

$$D(\mathbb{Z}G) \cong D_0 \oplus D(\mathbb{Z}H),$$

since  $G$  is a semidirect product  $\langle x \rangle \rtimes H$  (see Exercise 49.12).

The theorem was generalized by Keating [74] as follows:

**(50.28) Theorem.** *Let  $p$  be a regular<sup>†</sup> odd prime,  $q$  a divisor of  $p-1$ , and let*

$$G_k = \langle x, y: x^{p^k} = 1, y^q = 1, yxy^{-1} = x^r \rangle, \quad k \geq 0,$$

where  $\langle y \rangle$  acts faithfully on  $\langle x \rangle$  by conjugation. Let  $\omega$  be a primitive  $p^k$ -th root

<sup>†</sup>This means that  $p$  does not divide the class number of  $\mathbb{Q}(\sqrt[p]{1})$ .

of 1, and let  $L_k$  be the unique subfield of  $\mathbb{Q}(\omega)$  for which  $\dim_{L_k} \mathbb{Q}(\omega) = q$ . Put  $S_k = \text{alg. int. } \{L_k\}$ .

Then there are exact sequences

$$1 \rightarrow C_{q'} \rightarrow \text{Cl } \mathbb{Z}G_k \rightarrow \text{Cl } \mathbb{Z}G_{k-1} \oplus \text{Cl } S_k \rightarrow 0, \quad 1 \rightarrow C_{q'} \rightarrow D(\mathbb{Z}G_k) \rightarrow D(\mathbb{Z}G_{k-1}) \rightarrow 0,$$

where  $C_{q'}$  is a cyclic group of order  $q' = q/(q, 2)$ .

Matchett [76] showed that under the above hypotheses,

$$D(\mathbb{Z}G_k) \cong (C_{q'})^{(k)},$$

a direct sum of  $k$  copies of  $C_{q'}$ .

A further generalization, due to Cassou-Noguès [75], showed that if the odd prime  $p$  is not assumed regular, then in fact

$$D(\mathbb{Z}G) \cong (C_{q'})^{(k)} \oplus \text{some } p\text{-group}.$$

We now give a brief description of some results of Cassou-Noguès [75] for the metacyclic group

$$G = \langle x, y : x^n = 1, y^q = 1, yxy^{-1} = x^r \rangle,$$

where  $n$  is odd, and where the cyclic group  $H = \langle y : y^q = 1 \rangle$  acts faithfully on the cyclic group  $C = \langle x : x^n = 1 \rangle$ . Keeping the notation of (50.1), let  $\sigma \in \text{Gal}(K_n/\mathbb{Q})$  be defined by  $(\omega_n)^\sigma = (\omega_n)^r$ . For each divisor  $d$  of  $n$ , we may view  $K_d$  as a subfield of  $K_n$ , and then define  $L_d$  as the subfield of  $K_d$  fixed by  $\sigma$ . Finally, let  $S_d = \text{alg. int. } \{L_d\}$ . Then

$$\mathbb{Q}G \cong \coprod_{d|n} K_d \circ H,$$

where for each  $d$ ,  $K_d \circ H$  is a twisted group algebra in which  $y$  acts as  $\sigma$  on  $K_d$ . It is easily verified that  $(q, n) = 1$ , so  $R_d \circ H$  is a maximal  $S_d$ -order in  $K_d \circ H$ . Since  $K_d \circ H \cong M_q(L_d)$ , we obtain

$$\text{Cl } R_d \circ H \cong \text{Cl } S_d \quad \text{when } d|n.$$

Cassou-Noguès showed that there are exact sequences

$$0 \rightarrow D_0(\mathbb{Z}G) \rightarrow \text{Cl } \mathbb{Z}G \rightarrow \text{Cl } \mathbb{Z}H \oplus \coprod_{d|n} \text{Cl } S_d \rightarrow 0,$$

$$0 \rightarrow D_0(\mathbb{Z}G) \rightarrow D(\mathbb{Z}G) \rightarrow D(\mathbb{Z}H) \rightarrow 0,$$

for some subgroup  $D_0(\mathbb{Z}G)$  of  $D(\mathbb{Z}G)$ . Further, the induction map  $\text{ind}_C^G$  gives rise to an additive homomorphism

$$f' : D_0(\mathbb{Z}C) \rightarrow D(\mathbb{Z}G),$$

whose cokernel is a direct sum of copies of the cyclic group  $C_{q'}$ , where  $q' = q/(q, 2)$ . The number of copies is equal to the total number of prime divisors of  $n$ , counting multiplicities. The problem of computing  $|D(ZG)|$  thus reduces to calculating  $|D(ZH)|$  and  $|\text{cok } f'|$ .

In the special case where  $q$  is an odd prime, we have  $D(ZH) = 0$ . Cassou-Noguès estimated  $|\text{cok } f'|$  for arbitrary  $q$ , and calculated  $|\text{cok } f'|$  explicitly in the special case where  $q \nmid h_d$  for each  $d$  dividing  $n$ , where  $h_d$  is the ideal class number of the ring of integers  $S_d$ .

For further results on  $\text{Cl}ZG$  and  $D(ZG)$  when  $G$  is metacyclic or dihedral, see Endo-Miyata-Sekiguchi [82, Prop. 4.4]. We conclude this subsection with a brief discussion as to which finite groups  $G$  have the property that the kernel group  $D(ZG)$  is trivial. The case of abelian groups is completely settled by Theorem 50.16. For non-abelian groups, we have:

**(50.29) Theorem (Endo-Hironaka [79]).** *A non-abelian group  $G$  for which  $D(ZG) = 0$  must be one of the groups  $D_n, A_4, A_5$ , or  $S_4$ .*

For  $G = A_4, A_5$ , or  $S_4$ , we have  $D(ZG) = 0$  by Reiner-Ullom [74b]. For  $G = D_n$ , the dihedral group of order  $2n$ , we know that  $D(ZG) = 0$  in the following cases:

- (i)  $n = \text{odd prime}$  (see (50.25)).
- (ii)  $n = \text{power of a regular odd prime}$  (see (50.28)).
- (iii)  $n = \text{power of 2}$  (see (50.31) below).

On the other hand, the results of Cassou-Noguès described above show that there exist infinitely many pairs of distinct odd primes  $p, q$  for which  $D(ZD_{pq}) \neq 0$ . It seems difficult to determine precisely those integers  $n$  for which  $D(ZD_n) = 0$ . The best result in this direction is:

**(50.30) Theorem (Endo-Miyata) [80].** *If  $D(ZD_n)$  has odd order (possibly 1), then  $n = 2^r p^s q^t$  for some  $r, s, t$  and some odd primes  $p, q$ . In particular,  $D(ZD_n) = 0$  for  $2 \leq n < 60$ , while  $D(ZD_{60})$  has order 2.*

## §50D. Dihedral and Quaternion 2-Groups

We begin with a discussion of dihedral 2-groups. The methods of §50C do not apply to this case, and the calculations needed are somewhat more subtle. The main result, due to Reiner-Ullom [74b] for the dihedral group of order 8, and to Fröhlich-Keating-Wilson [74] for the general case, is as follows:

**(50.31) Theorem.** *For  $G_n$  a dihedral group of order  $2^{n+2}$ , where  $n \geq 0$ , the kernel group  $D(ZG_n)$  is trivial.*

*Proof.* Step 1. For  $n = 0$ ,  $G_0$  is an elementary  $(2, 2)$ -group, so  $D(ZG_0) = 0$  (see Exercise 50.1). Now let  $n > 0$ , and let

$$G_n = \langle x, y : x^{2^{n+1}} = 1, y^2 = 1, yxy^{-1} = x^{-1} \rangle$$

be the dihedral group of order  $2^{n+2}$ . We set

$$K = \mathbb{Q}(\omega), \quad R = \mathbb{Z}[\omega], \quad L = \mathbb{Q}(\omega + \bar{\omega}), \quad S = \mathbb{Z}[\omega + \bar{\omega}] = \text{alg. int. } \{L\},$$

where  $\omega$  is a primitive  $2^{n+1}$ -st root of 1. Since  $x^{2^{n+1}} - 1 = (x^{2^n} - 1)(x^{2^n} + 1)$ , there is a fiber product

$$\begin{array}{ccc} \Lambda = \mathbb{Z}G_n & \xrightarrow{f_1} & \Delta = \mathbb{Z}G_{n-1} \\ f_2 \downarrow & & \downarrow \\ \Gamma = R \circ H & \longrightarrow & \Delta/2\Delta, \end{array}$$

where  $H = \langle y: y^2 = 1 \rangle$ . The maps  $f_1, f_2$  are given by

$$f_1(x) = x \in G_{n-1}, \quad f_2(x) = \omega \in R,$$

and  $\Gamma$  is the twisted group ring of  $H$  over  $R$ , in which  $y$  acts on  $R$  by complex conjugation:  $y\alpha = \bar{\alpha}y$ ,  $\alpha \in R$ .

Consider the display

$$\begin{array}{ccccc} & K & \longrightarrow & R & \pi_0 = 1 - \omega \\ & | & & | & | \\ 2 & L & \longrightarrow & S & \pi = (1 - \omega)(1 - \bar{\omega}) = \pi_0 \bar{\pi}_0 \\ & | & & | & | \\ 2^{n-1} & Q & \longrightarrow & Z & 2 \end{array}$$

Here,  $\dim_L K = 2$  and  $\dim_Q L = 2^{n-1}$ . The only rational prime which ramifies in the extension  $K/\mathbb{Q}$  is 2, and 2 is completely ramified (see §4H). Further,  $\pi_0 R$  and  $\pi S$  are prime ideals, and

$$2S = (\pi S)^{2^{n-1}}, \quad 2R = (\pi_0 R)^{2^n}, \quad \pi R = \pi_0^2 R; \quad R/\pi_0 R \cong S/\pi S \cong \mathbb{Z}/2\mathbb{Z}.$$

We observe that  $\Gamma$  is an  $S$ -order in the twisted group algebra  $K \circ H$ , but  $\Gamma$  is not hereditary, since  $K$  is not tamely ramified over  $L$ . Since  $K \circ H \cong M_2(L)$ , we may write

$$\mathbb{Q}G_n \cong K \circ H \oplus \mathbb{Q}G_{n-1}, \quad C \cong L \oplus \tilde{C}, \quad \mathfrak{O} = S \oplus \tilde{\mathfrak{O}},$$

where  $C, \tilde{C}$  are the centers of  $\mathbb{Q}G_n, \mathbb{Q}G_{n-1}$ , respectively, and where  $\mathfrak{O}, \tilde{\mathfrak{O}}$  are the integral closures of  $Z$  in  $C$  and  $\tilde{C}$ , respectively.

*Step 2.* By (49.42), there is an exact sequence

$$\frac{\text{nr } U(\Lambda)}{\text{nr } S} \rightarrow \frac{\mathfrak{O} \cdot \text{nr } U(\Gamma)}{\mathfrak{O} \cdot S} \times \frac{\tilde{\mathfrak{O}} \cdot \text{nr } U(\Delta)}{\tilde{\mathfrak{O}} \cdot S} \xrightarrow{g} D(\Lambda) \rightarrow D(\Gamma) \oplus D(\Delta) \rightarrow 0.$$

(Note that in this case, by (7.39), we have  $S^+ = S^-$  and  $\mathfrak{D}^+ = \mathfrak{D}^-$ .)

For each odd prime  $p$ , we see readily that  $\Lambda_p^\circ = \Gamma_p^\circ \times \Delta_p^\circ$ , so in the above sequence we may replace the groups of unit idèles by their 2-components. Thus, there is an exact sequence

$$(50.32) \quad \text{nr } \Lambda_2^\circ \xrightarrow{h} \frac{S^\circ \text{ nr } \Gamma_2^\circ}{S^\circ} \times \frac{\mathfrak{D}^\circ \text{ nr } \Delta_2^\circ}{\mathfrak{D}^\circ} \xrightarrow{g} D(\Lambda) \rightarrow D(\Gamma) \oplus D(\Delta) \rightarrow 0.$$

Proceeding by induction on  $n$ , it therefore suffices to show that  $D(\Gamma) = 0$  and that  $h$  is surjective.

Now  $\Gamma_p$  is a maximal order for each odd prime  $p$ , so from (49.40) we obtain

$$D(\Gamma) \cong S_2^\circ / S^\circ \text{ nr } \Gamma_2^\circ.$$

We now prove that  $\text{nr } \Gamma_2^\circ = S_2^\circ$ , and therefore  $D(\Gamma) = 0$ . By (7.39) we may write

$$\Gamma_2 = R_2 \oplus R_2 y, \quad \text{and} \quad \text{nr}_{\Gamma_2/S_2}(\alpha + \beta y) = \alpha\bar{\alpha} - \beta\bar{\beta} \quad \text{for } \alpha, \beta \in R_2.$$

(Note that for  $\alpha \in R_2$ ,  $\bar{\alpha}$  is the image of  $\alpha$  under the automorphism of  $R_2$  defined by  $\omega \mapsto \omega^{-1}$ .)

When  $n = 1$ , the argument is simple, since in this case  $S_2 = \mathbb{Z}_2$ , and each  $u \in S_2^\circ$  has the form  $u = 1 + 2v$  with  $v \in S_2$ . But then

$$\text{nr}((v+1) + vy) = (v+1)^2 - v^2 = u,$$

so  $\text{nr } \Gamma_2^\circ = S_2^\circ$ , as desired.

The proof when  $n > 1$  is not much harder. In this case for  $i \geq 1$  and  $\alpha, \beta \in R_2$ , we obtain

$$\text{nr}(1 + \pi^i(\alpha + \beta y)) \equiv 1 + \pi^i(\alpha + \bar{\alpha}) \equiv 1 \pmod{\pi^{i+1}S_2},$$

since  $\alpha \equiv \bar{\alpha} \pmod{\pi S_2}$ . This shows that  $\text{nr}(1 + \pi^i \Gamma_2) \subseteq 1 + \pi^{i+1} S_2$  for  $i \geq 1$ . On the other hand, for  $\pi_0 = 1 - \omega$  as above,

$$\text{nr}(1 + \pi^i \pi_0) = (1 + \pi^i \pi_0)(1 + \pi^i \bar{\pi}_0) \equiv 1 + \pi^{i+1} \pmod{\pi^{2i+1}}$$

for  $i \geq 1$ . Now each  $u \in 1 + \pi^2 S_2$  is of the form  $u = 1 + \sum_{i=2}^{\infty} a_i \pi^i$ , with  $a_i \in \{0, 1\}$ . Since  $R_2$  is complete, it follows from the above discussion that

$$\text{nr}(1 + \pi \Gamma_2) = 1 + \pi^2 S_2.$$

Therefore

$$|S_2^\circ : \text{nr } \Gamma_2^\circ| \leq |S_2^\circ : 1 + \pi^2 S_2| = 2.$$

However, since  $n > 1$  we have

$$\text{nr}(1 + \omega + y) = 1 + \omega + \bar{\omega} = 3 - \pi \equiv 1 + \pi \pmod{\pi^2 S_2},$$

and therefore  $\text{nr } \Gamma_2^* > 1 + \pi^2 S_2$ . It follows that  $\text{nr } \Gamma_2^* = S_2^*$ , which shows that  $D(\Gamma) = 0$ , as claimed.

*Step 3.* It remains for us to prove that the map  $h$  occurring in (50.32) is surjective. Consider the fiber product used in defining the map  $h$ , namely

$$\begin{array}{ccc} \Lambda_2 & \xrightarrow{f_1} & \Delta_2 \\ f_2 \downarrow & & \downarrow \\ \Gamma_2 & \longrightarrow & \Delta_2/2\Delta_2. \end{array}$$

Then

$$f_1\{1 + (x^{2^n} - 1)\Lambda_2\} = 1, \quad f_2\{1 + (x^{2^n} - 1)\Lambda_2\} = 1 + 2\Gamma_2,$$

and consequently

$$\text{im } h \geq \text{nr}(1 + 2\Gamma_2) \times 1.$$

On the other hand, the map  $\Lambda_2^* \rightarrow \Delta_2^*$  is surjective by (50.7), so  $\text{im}(h)$  covers the factor  $\mathfrak{O} \cdot \text{nr } \Delta_2^*/\mathfrak{O}^*$ . It therefore suffices to prove that

$$S^* \text{nr } \Gamma_2^* = S^* \text{nr}(1 + 2\Gamma_2).$$

But  $\text{nr } \Gamma_2^* = S_2^*$  and  $\text{nr}(1 + 2\Gamma_2) = 1 + 2\pi S_2$ , by Step 2. Thus we must show that

$$(50.33) \quad S_2^* = S^*(1 + 2\pi S_2).$$

This is obvious when  $n = 1$ , for the desired equality becomes  $Z_2^* = \{\pm 1\} \cdot (1 + 4Z_2)$ , which is clearly true. Now let  $n > 1$  and consider the map  $\rho: S^* \rightarrow S_2^*/(1 + 2\pi S_2)$ . We shall prove (50.33) by showing that  $\rho$  is surjective. The proof will require some deep results from algebraic number theory. Since there is a surjection

$$S_2^*/(1 + 4S_2) \rightarrow S_2^*/(1 + 2\pi S_2),$$

it suffices to prove the (harder) result that

$$\tau: S^* \rightarrow S_2^*/(1 + 4S_2)$$

is surjective.

To simplify the notation, we set

$$U = S_2 = \left\{ 1 + \sum_{i=1}^{\infty} a_i \pi^i : a_i = 0 \text{ or } 1 \right\}, \quad U^2 = \{u^2 : u \in U\}.$$

We wish to show that  $U = \tau(S^\circ)(1 + 4S_2)$ ; for this, it suffices to prove that

$$(50.34) \quad U = U^2\tau(S^\circ)(1 + 4S_2),$$

for then we obtain the desired result by applying Nakayama's Lemma to the finite 2-group  $U/(1 + 4S_2)$ .

We need an elementary result from local field theory:

**(50.35) Lemma.** *Keeping the above notation, set*

$$W = U/U^2(1 + 4S_2).$$

*Then  $W$  is an elementary abelian 2-group on  $2^{n-1}$  generators.*

*Proof.* The only roots of unity in  $\mathbb{Q}_2(\omega + \omega^{-1})$  are  $\pm 1$ , so the group structure of  $U$  is given by

$$U \cong \{\pm 1\} \times \{2^{n-1} \text{ copies of the additive group } \mathbb{Z}_2\}$$

(see, for example, Serre [62, p. 220, Prop. 10] or Long [77, p. 63, Th. 2.9]). It follows that  $U/U^2$  is an elementary abelian 2-group on  $2^{n-1} + 1$  generators, and we may view  $U/U^2$  as a vector space over  $\bar{\mathbb{Z}} (= \mathbb{Z}/2\mathbb{Z})$  of dimension  $2^{n-1} + 1$ . Further (see Long [77, p. 64, Prop. 2.11])

$$1 + 4S_2 \not\leq U^2, \quad \text{and} \quad 1 + 4\pi S_2 \leq U^2.$$

Since  $|1 + 4S_2 : 1 + 4\pi S_2| = |S_2 : \pi S_2| = 2$ , it then follows that  $\dim_{\bar{\mathbb{Z}}} W = 2^{n-1}$ , as desired.

*Step 4.* To complete the proof of the theorem, we must show that the natural map  $\varphi: S^\circ \rightarrow W$  is surjective. We shall use Hilbert symbols to construct a symmetric bilinear form  $F: W \times W \rightarrow \bar{\mathbb{Z}}$ , and we shall find  $2^{n-1}$  units  $\{u_i\}$  in  $S$  such that

$$F(\varphi(u_i), \varphi(u_j)) = \delta_{ij}, \quad 1 \leq i, j \leq 2^{n-1}.$$

The images  $\{\varphi(u_i)\}$  thus form an orthonormal  $\bar{\mathbb{Z}}$ -basis for  $W$ , and consequently  $\varphi$  is surjective.

We begin by reviewing some basic facts about Hilbert symbols, generalizing the discussion in §47C. For more details on these symbols, we refer the reader to Cassels-Fröhlich [67, pages 351–353]. For the moment, let  $K$  be an arbitrary algebraic number field, and let  $R = \text{alg. int. } \{K\}$ . For  $P$  ranging over the primes of  $\{K\}$ , finite or infinite, let  $K_P, R_P$  denote  $P$ -adic completions (with  $R_P = K_P$  for  $P$  infinite).

Given a prime  $P$  of  $K$ , there is a Hilbert symbol  $(a, b)_P$ , defined for  $a, b \in K_P$ ,

whose values are  $\pm 1$ . Specifically, we define

$$(a, b)_P = 1 \Leftrightarrow ax^2 + by^2 = 1 \text{ has a solution with } x, y \in K_P.$$

This symbol is a special case of the norm residue symbol, corresponding to Kummer extensions defined by square roots. Equivalently,

$$(a, b)_P = 1 \Leftrightarrow b \text{ is a norm from } K_P(\sqrt{a}) \text{ to } K_P.$$

This symbol satisfies the following identities:

$$(a, b)_P = (b, a)_P, \quad (aa', b)_P = (a, b)_P(a', b)_P, \quad (ax^2, b)_P = (a, b)_P$$

where  $a, a', b, x \in K_P^\times$ . Furthermore, we have:

- (1) Let  $P$  be a finite prime of  $K$ , and assume that  $q = \text{card } R/P$  is odd. Let  $v$  be the exponential  $P$ -adic valuation of  $K_P$ . For  $a, b \in K_P^\times$ , define

$$c = (-1)^{v(a)v(b)} a^{v(b)} / b^{v(a)} \in R_P^\times.$$

(Compare with the tame symbol defined on pages 202 and 203.) Then

$$(a, b)_P \equiv c^{(q-1)/2} \pmod{P}.$$

In particular, in this case

$$(a, b)_P = 1 \quad \text{for all } a, b \in R_P^\times.$$

- (2) For any prime  $P$  of  $K$ , let  $a \in K_P^\times$  be such that the prime  $P$  is unramified in the extension  $K_P(\sqrt{a})/K_P$ . Then every  $b \in R_P^\times$  is a norm from  $K_P(\sqrt{a})$ , and consequently

$$(a, b)_P = 1 \quad \text{for all } b \in R_P^\times.$$

- (3) (*Product Formula*) For  $a, b \in K^\times$  there is an identity

$$\prod_P (a, b)_P = 1,$$

where  $P$  ranges over all primes of  $K$ . (Compare with the Hilbert Reciprocity Theorem 47.48.) Further, if  $P$  is a non-archimedean prime which does not contain the rational prime 2, then  $(a, b)_P = 1$  for all  $a, b \in R^\times$ .

After these preliminaries, we are ready to return to our study of the  $\bar{\mathbb{Z}}$ -space  $W = U/U^2(1 + 4S_2)$ , where

$$L_2 = \Omega_2(\omega + \omega^{-1}), \quad S_2 = \mathbb{Z}_2[\omega + \omega^{-1}], \quad U = S_2^\times.$$

We are trying to show that the natural map  $\varphi: S \rightarrow W$  is a surjection. Let  $P_2 = \pi S_2$  be the prime ideal in the valuation ring in  $L_2$ . We intend to define a bilinear form  $F: W \times W \rightarrow \{\pm 1\}$  by setting

$$F(a, b) = (a, b)_{P_2} \quad \text{for } a, b \in U.$$

To prove that  $F$  is well-defined, we note first that  $F(a, b) = 1$  if either  $a \in U^2$  or  $b \in U^2$ . Next, let  $d \in 1 + 4S_2$ ,  $d \notin U^2$ ; then  $(1 \pm \sqrt{d})/2$  lies in the valuation ring of  $L_2(\sqrt{d})$ , and so  $P_2$  is unramified in the extension  $L_2(\sqrt{d})/L_2$ . It follows that  $(d, b)_{P_2} = 1$  for all  $b \in U$ . This shows that  $F$  is indeed well-defined (and bilinear).

We now make use of:

**Weber's Theorem.** *Let  $L = Q(\omega + \omega^{-1})$ ,  $S = \text{alg. int. } \{L\}$ , where  $\omega$  is a primitive  $2^n$ -th root of 1, and  $n \geq 1$ . Let  $\{\mathfrak{q}_i : 1 \leq i \leq 2^{n-1}\}$  be the infinite primes of  $L$  (necessarily real primes). Then for each  $i$ ,  $1 \leq i \leq 2^{n-1}$ , there exists a unit  $u_i \in S$  such that*

$$u_i < 0 \text{ in } L_{\mathfrak{q}_i}, \quad \text{and} \quad u_i > 0 \text{ in each } L_{\mathfrak{q}_j}, \quad j \neq i.$$

(See Hasse [52, p. 29].)

From the definition of the Hilbert symbol, it follows at once that

$$(u_i, u_i)_{\mathfrak{q}_i} = -1, \quad \text{and} \quad (u_i, u_j)_{\mathfrak{q}_k} = +1 \quad \text{if } i, j, k \text{ do not coincide.}$$

Since  $\pi S$  is the unique prime ideal of  $S$  containing 2, the Product Formula now gives

$$(u_i, u_j)_{P_2} = (-1)^{\delta_{ij}}, \quad 1 \leq i, j \leq 2^{n-1}.$$

This implies that the images  $\{\varphi(u_i) : 1 \leq i \leq 2^{n-1}\}$  form an orthonormal  $\bar{\mathbb{Z}}$ -basis of  $W$  relative to the form  $F$ . Therefore  $\varphi$  is surjective, which completes the proof of (50.34) and establishes the theorem.

**Remark.** For another proof of Theorem 50.31 for the case  $n = 1$ , see Wall [74c].

We turn next to the quaternion group

$$G_n = \langle x, y : x^{2^{n+1}} = 1, x^{2^n} = y^2, yxy^{-1} = x^{-1} \rangle$$

of order  $2^{n+2}$ . Fröhlich-Keating-Wilson [74] proved:

**(50.36) Theorem.** *Let  $G_n$  be the generalized quaternion group of order  $2^{n+2}$ , where  $n \geq 1$ . Then<sup>†</sup>  $|D(\mathbb{Z}G_n)| = 2$ .*

<sup>†</sup>The nontrivial element of  $D(\mathbb{Z}G_n)$  is represented by  $I + 3\mathbb{Z}G_n$ , where  $I$  is the augmentation ideal of  $\mathbb{Z}G_n$ ; see Swan [83, Remark 9.9], and (53.17).

*Proof.* The special case where  $G$  is the quaternion group of order 8 was first proved independently by Martinet [71] and Reiner-Ullom [72]. Other versions for this case are given by Keating [73], Reiner-Ullom [74b], and Wall [74c]. Here we shall prove the theorem only for this case, and refer the reader to the article by Fröhlich-Keating-Wilson [74] for the general case.

For  $G$  the quaternion group of order 8, we start with the fiber product

$$\begin{array}{ccc} \Lambda = \mathbb{Z}G & \xrightarrow{f_1} & \Delta = \mathbb{Z}H \\ f_2 \downarrow & & \downarrow \\ \Gamma = R \oplus Ry & \longrightarrow & \bar{\Delta} = \bar{\mathbb{Z}}H, \end{array}$$

where  $H = \langle x, y : x^2 = y^2 = 1, xy = yx \rangle$ ,  $\bar{\mathbb{Z}} = \mathbb{Z}/2\mathbb{Z}$ ,  $R = \mathbb{Z}[i]$ , and where  $\Gamma$  is the ring of integral quaternions, that is,

$$y^2 = -1, \quad y\alpha = \bar{\alpha}y \text{ in } \Gamma, \quad \text{for } \alpha \in R.$$

The maps  $f_j$  are given by  $f_1(x) = x$ ,  $f_2(x) = i$ ,  $f_1(y) = f_2(y) = y$ .

As in (50.32), there is an exact sequence

$$\mathrm{nr} \Lambda_2^+ \xrightarrow{h} \frac{\mathbb{Z}^+ \mathrm{nr} \Gamma_2^+}{\mathbb{Z}^+} \times \frac{\Delta^+ \Delta_2^+}{\Delta^+} \rightarrow D(\Lambda) \rightarrow D(\Gamma) \oplus D(\Delta) \rightarrow 0,$$

where  $\mathbb{Z}^+ = \mathbb{Z}^+ \cap \mathbb{Q}^+ = \{1\}$ . (We have used the fact that  $\mathrm{nr} \Delta_2^+ = \Delta_2^+$ .) We already know from Exercise 50.1 that  $D(\Delta) = 0$ . Next, we observe that  $D(\Gamma) \cong \mathbb{Z}_2^*/\mathrm{nr} \Gamma_2^+$ . But for  $\alpha + \beta y \in \Gamma_2$ , where  $\alpha = a_1 + a_2 i \in R_2$ ,  $\beta = b_1 + b_2 i \in R_2$ , with each  $a_j, b_j \in \mathbb{Z}_2$ , we have

$$\mathrm{nr}(\alpha + \beta y) = \bar{\alpha}\alpha + \bar{\beta}\beta = a_1^2 + a_2^2 + b_1^2 + b_2^2.$$

Thus,  $\mathrm{nr} \Gamma_2^+$  contains 1, 3, 5, 7. But also  $\mathrm{nr} \Gamma_2^+$  contains  $1 + 8\mathbb{Z}_2$  (see the argument in Step 2 of the proof of (50.31)). Therefore  $\mathrm{nr} \Gamma_2^+ = \mathbb{Z}_2^*$ , so  $D(\Gamma) = 0$ .

Finally, we must show that  $|\mathrm{cok} h| = 2$ . Since  $\mathrm{nr} \Lambda_2^+$  maps onto  $\Delta_2^+$ , it follows that

$$\mathrm{cok} h \cong \mathbb{Z}_2^*/\mathrm{im} X,$$

where  $X = \{u \in \Lambda_2^+ : f_1(u) = 1 \text{ in } \Delta_2^+\}$ . Then  $f_2(X) = 1 + 2\Gamma_2$ , and for  $\alpha, \beta \in R_2$  we have

$$\mathrm{nr}(1 + 2\alpha + 2\beta y) = (1 + 2\alpha)(1 + 2\bar{\alpha}) + 4\beta\bar{\beta} \in \mathbb{Z}_2^*.$$

This readily implies that  $\mathrm{nr}(1 + 2\Gamma_2) = 1 + 4\mathbb{Z}_2$ , so

$$\mathrm{cok} h \cong (1 + 2\mathbb{Z}_2)/(1 + 4\mathbb{Z}_2).$$

Therefore  $|\mathrm{cok} h| = 2$ , as claimed.

### §50E. An Involution on Class Groups and Kernel Groups

Let  $G$  be a finite group, and set

$$\Lambda = RG, A = KG, \quad \text{where } R = \text{alg. int. } \{K\}.$$

Let  $\tau$  be the involution of  $\Lambda$  defined by  $g \mapsto g^{-1}$ ,  $g \in G$ , extended by linearity. Then  $\tau$  is an anti-automorphism of  $\Lambda$ , and extends to an involution on  $A$  and on the idèle group  $J(A)$ . Further,  $\tau$  induces an automorphism on the center  $C$  of  $A$ , and its idèle group  $J(C)$ . Let us show that  $\tau$  acts on the class group  $\text{Cl } \Lambda$  and the kernel group  $D(\Lambda)$ .

For any left  $\Lambda$ -module  $M$ , let  $M^* = \text{Hom}_R(M, R)$  be its dual, viewed as right  $\Lambda$ -module. We make  $M^*$  into a left  $\Lambda$ -module  $\check{M}$ , the *contragredient* of  $M$ , by defining

$$x \cdot m^* = m^* \tau(x) \quad \text{for } x \in \Lambda, \quad m^* \in M^*.$$

By (10.21), we have  $M^* \cong \text{Hom}_{\Lambda}(M, \Lambda)$ , and we treat this isomorphism as an identification. In particular, when  $M = \Lambda a$  is principal, where  $a \in A'$ , then

$$M^* = \text{Hom}_{\Lambda}(\Lambda a, \Lambda) \cong a^{-1} \Lambda.$$

We claim that there is a left  $\Lambda$ -isomorphism

$$f: \check{M} \cong \Lambda \tau(a^{-1}), \quad \text{given by } f(a^{-1} \lambda) = \tau(\lambda) \tau(a^{-1}) \text{ for } \lambda \in \Lambda.$$

Indeed, for  $x \in \Lambda$  and for each  $\lambda \in \Lambda$ , we have

$$f(x \cdot a^{-1} \lambda) = f(a^{-1} \lambda \tau(x)) = \tau(\lambda \tau(x)) \tau(a^{-1}) = x \tau(\lambda) \tau(a^{-1}) = x f(a^{-1} \lambda).$$

Thus, the contragredient of  $\Lambda a$  is isomorphic to the left  $\Lambda$ -ideal  $\Lambda \tau(a^{-1})$ . Of course, the ideal  $\Lambda$  is self-contragredient.

Now let  $\alpha \in J(A)$ , and take  $M = \Lambda \alpha$ . Since  $\tau$  commutes with  $P$ -adic completion, the above remarks show that

$$\text{contragredient of } \Lambda \alpha \cong \Lambda \tau(\alpha^{-1}) = \Lambda \tau(\alpha)^{-1}, \quad \alpha \in J(A).$$

The action of the involution  $\tau$  on  $\text{Cl } \Lambda$  is given by

$$\tau[\Lambda \alpha] = [\Lambda \tau(\alpha)] \text{ for } \alpha \in J(A),$$

or equivalently,

$$\tau[M] = [\text{contragredient of } M^{-1}], \quad [M] \in \text{Cl } \Lambda,$$

where  $M^{-1}$  means the inverse of  $M$  in  $\text{Cl } \Lambda$ .

It follows readily that  $\tau$  acts as an involution on  $D(\Lambda)$ ; for if  $[M] \in D(\Lambda)$ , then also  $[M^{-1}] \in D(\Lambda)$ , and hence

$$M^{-1} \oplus X \cong \Lambda \oplus X$$

for some f.g.  $\Lambda$ -module  $X$ . Taking contragredients, and using the fact that  $\Lambda$  is self-contragredient, it follows at once that  $\tau[M] \in D(\Lambda)$ , as desired.

The involution  $\tau$  acts on the idèle group  $J(C)$ , where  $C$  is the center of  $A$ , and  $\tau$  commutes with the isomorphisms

$$\text{Cl } \Lambda \cong \frac{J(C)}{C^+ \prod_p \text{nr } \Lambda_P^\times}, \quad D(\Lambda) \cong \frac{C^+ \prod_p \mathfrak{O}_P^\times}{C^+ \prod_p \text{nr } \Lambda_P^\times}$$

given in (49.17) and (49.36).

We now concentrate on the case  $\Lambda = \mathbb{Z}G$ ,  $A = \mathbb{Q}G$ , and begin with an easy result:

**(50.37) Proposition.** *For  $A = \mathbb{Q}G$ , the involution  $\tau$  maps each simple component  $A_i$  of  $A$  onto itself, and induces the complex conjugation map on the center  $K_i$  of  $A_i$ .*

*Proof.* Let  $A_i$  afford the character  $\mu_i$  of  $G$ . Then  $\tau(A_i)$  is also a simple component of  $A$ , and affords the character

$$g \mapsto \bar{\mu}_i(g^{-1}), \quad g \in G.$$

But  $\mu_i(g^{-1}) = \bar{\mu}_i(g)$ ,  $g \in G$ , where bar denotes complex conjugation (see the discussion preceding (9.23)). Further,  $\bar{\mu}_i(g) = \mu_i(g)$  for all  $g \in G$ , since  $\mu_i$  takes values in  $\mathbb{Q}$ . It follows that  $\tau(A_i) = A_i$ , as claimed.

Furthermore, the center  $K_i$  of  $A_i$  is a subfield of a cyclotomic field  $\mathbb{Q}(\omega)$ , with  $\omega$  a root of unity. Then  $\tau$  induces an automorphism of  $K_i$  by means of the map  $\omega \mapsto \omega^{-1}$ , noting that  $\tau(K_i) = K_i$  since  $K_i$  is a Galois extension of  $\mathbb{Q}$ . This completes the proof.

**Example.** Let  $G$  be cyclic of order  $p$ , and keep the notation of (50.1). Each  $[M] \in \text{Cl } \mathbb{Z}G$  is represented by an ideal class  $[\alpha] \in \text{Cl } R$ , and  $[M^{-1}]$  by  $[\bar{\alpha}^{-1}]$ . If  $\check{M}$  denotes the contragredient of  $M$ , then the preceding discussion shows that

$$[\check{M}] \text{ corresponds to } [\bar{\alpha}^{-1}] \in \text{Cl } R,$$

where bar denotes complex conjugation. This result was pointed out by Reiner [68].

For any additive group  $D$  on which an involution  $\tau$  acts, we set

$$D^+ = \{x \in D : \tau(x) = x\} \quad \text{and} \quad D^- = \{x \in D : \tau(x) = -x\}.$$

We call  $D^+$  and  $D^-$  the “plus part” and “minus part” of  $D$ , respectively.

We shall now give Fröhlich's [72] calculation of the order of  $D^-(\Lambda)$ , where  $\Lambda = \mathbb{Z}G$  with  $G$  an abelian  $p$ -group and  $p$  an odd prime. Here,  $D^-(\Lambda)$  denotes the minus part of the kernel group  $D(\Lambda)$  on which the canonical involution  $\tau$  acts, where  $\tau$  is as above. This calculation generalizes earlier results of Kervaire-Murthy [77] for the case where  $G$  is a cyclic  $p$ -group; their work circulated in preprint form in the late 1960s.

Let  $A = \mathbb{Q}G$  where  $G$  is an abelian  $p$ -group,  $p$  odd. By Exercise 39.4, we may write

$$(50.38) \quad A = \coprod_{i=0}^m K_i, \quad \text{where } K_i = \mathbb{Q}(\omega_i), \quad \omega_i = p^{s_i}\text{-th root of 1.}$$

The simple component  $\mathbb{Q}$  occurs exactly once in  $A$ , and we set  $K_0 = \mathbb{Q}$ . Since  $A$  has no other  $G$ -trivial summands, we have  $s_i \geq 1$  for  $1 \leq i \leq m$ . By (50.37),  $\tau$  acts as the identity on  $K_0$ , and as complex conjugation on each  $K_i$ . There is a unique maximal  $\mathbb{Z}$ -order  $\Gamma$  in  $A$ , given by

$$(50.39) \quad \Gamma = \coprod_{i=0}^m R_i, \quad \text{where } R_i = \text{alg. int. } \{K_i\} = \mathbb{Z}[\omega_i] \text{ for each } i.$$

Clearly  $\tau(\Gamma) = \Gamma$ , and indeed  $\tau(R_i) = R_i$  for each  $i$ . As in §50B, the rational prime  $p$  ramifies completely in  $K_i$ , and thus

$$pR_i = P_i^{e_i}, \quad \text{where } e_i = \varphi(p^{s_i}), \quad 1 \leq i \leq m.$$

The  $p$ -adic and  $P_i$ -adic completions of  $R_i$  coincide, and will be denoted by  $\hat{R}_i$ , for each  $i$ .

In order to calculate  $|D^-(\Lambda)|$ , we shall use formula (50.20) for  $D(\Lambda)$ . In this case where  $A$  is commutative, the ring  $\mathfrak{O}$  coincides with  $\Gamma$ , and  $\mathfrak{O}^+$  with  $\Gamma^+$ . Further, the reduced norm map is the identity map, so we obtain

$$D(\Lambda) \cong \Gamma_p^\circ / \Gamma^\circ \Lambda_p^\circ.$$

We show at once that the sequence

$$(50.40) \quad 1 \rightarrow \Gamma^\circ / \Lambda^\circ \longrightarrow \Gamma_p^\circ / \Lambda_p^\circ \longrightarrow D(\Lambda) \rightarrow 0$$

is exact. In view of the preceding formula for  $D(\Lambda)$ , we need only prove that  $\Gamma^\circ \cap \Lambda_p^\circ = \Lambda^\circ$ . But this is clear, since  $\Lambda_q = \Gamma_q$  for primes  $q \neq p$ , so

$$\Gamma^\circ \cap \Lambda_p^\circ \subseteq \left( \bigcap_{q \neq p} \Lambda_q^\circ \right) \cap \Lambda_p^\circ = \Lambda^\circ.$$

Note that by Exercise 50.4, the quotient groups in (50.40) are finite. Further,  $D(\Lambda)$  is a finite  $p$ -group by Theorem 50.18.

Keeping the notation of (50.39), we have

$$(50.41) \quad \Gamma_p = \coprod \hat{R}_i, \quad N = \text{rad } \Gamma_p = \coprod \hat{P}_i.$$

Then  $\Gamma_p/N \cong \coprod \mathbb{Z}/p\mathbb{Z}$ , so  $(\Gamma_p/N)^\circ$  is a finite group of order prime to  $p$ . Therefore  $1+N$  is a subgroup of  $\Gamma_p^\circ$  of index prime to  $p$ . Since  $D(\Lambda)$  is a  $p$ -group, it follows from (50.40) that  $1+N$  maps onto  $D(\Lambda)$ , and there is an exact sequence

$$(50.42) \quad 1 \rightarrow \frac{\Gamma^\circ \cap (1+N)}{\Lambda_p^\circ \cap (1+N)} \longrightarrow \frac{1+N}{\Lambda_p^\circ \cap (1+N)} \longrightarrow D(\Lambda) \rightarrow 0.$$

Further,  $\tau$  acts on each of the groups  $\Gamma^\circ \cap (1+N)$ ,  $\Lambda_p^\circ \cap (1+N)$ , etc., in the above formula, and the maps in (50.42) commute with  $\tau$ . Since  $2$  acts invertibly on  $D(\Lambda)$ , it follows from Exercise 50.6 that

$$(50.43) \quad |D^-(\Lambda)| = k/l, \text{ where } k = \text{order of minus part of } \frac{1+N}{\Lambda_p^\circ \cap (1+N)},$$

$$l = \text{order of minus part of } \frac{\Gamma^\circ \cap (1+N)}{\Lambda_p^\circ \cap (1+N)}.$$

We shall proceed to calculate  $k$  and  $l$  explicitly, and begin with:

**(50.44) Lemma.** *Let  $N = \text{rad } \Gamma_p$  and  $M = \Lambda_p \cap N$ , viewed as additive groups on which the involution  $\tau$  acts. Then  $\Lambda_p^\circ \cap (1+N) = 1+M$ , and*

$$k = \text{order of the minus part of } N/M.$$

*Proof.* The equality  $\Lambda_p^\circ \cap (1+N) = 1 + (\Lambda_p \cap N)$  is obvious. Now set

$$G_r = 1 + N^r + M \quad \text{and} \quad H_r = N^r + M, \quad r \geq 1,$$

so  $G_r$  is a multiplicative subgroup of  $1+N$ , and  $H_r$  an additive subgroup of  $N$ . We have

$$G_1 = 1 + N, \quad G_s = 1 + M$$

for sufficiently large  $s$ , using the fact that  $N^s \subseteq \Lambda_p$  for large  $s$  (see (5.22)). Likewise,

$$H_1 = N, \quad H_s = M,$$

and  $\tau$  acts on all of the  $\{G_r\}$  and  $\{H_r\}$ . For  $r \geq 1$ , there is an isomorphism

$$\frac{H_r}{H_{r+1}} = \frac{N^r + M}{N^{r+1} + M} \cong \frac{1 + N^r + M}{1 + N^{r+1} + M} = \frac{G_r}{G_{r+1}},$$

given by  $\alpha \in H_r \rightarrow 1 + \alpha \in G_r$ . This isomorphism preserves the action of  $\tau$ . But  $H_r/H_{r+1}$  is a finite  $p$ -group since  $p \in N$ , whence so is  $G_r/G_{r+1}$ .

Now consider the filtrations

$$1 + N = G_1 \geq G_2 \geq \cdots \geq G_s = 1 + N^s + M, \quad N = H_1 \geq H_2 \geq \cdots \geq H_s = N^s + M.$$

The factor groups are finite groups of odd order, so by Exercise 50.6 we deduce that

$$|\{G_1/G_s\}^-| = \prod_{r=1}^{s-1} |\{G_r/G_{r+1}\}^-| = \prod_{r=1}^{s-1} |\{H_r/H_{r+1}\}^-| = |\{H_1/H_s\}^-|,$$

which proves the lemma.

We are trying to calculate the order  $k$  of the minus part of  $N/M$ ; by Exercise 50.6 we have

$$k = |N^-/M^-|,$$

since  $N/M$  is a finite  $p$ -group by the proof of the above lemma. The group  $N$  is given by (50.41). For each  $i$ ,  $1 \leq i \leq m$ , we have<sup>†</sup>

$$\alpha \equiv \bar{\alpha} \pmod{\hat{P}_i} \quad \text{for } \alpha \in \hat{R}_i.$$

Then

$$\hat{R}_i^- = \{\alpha \in \hat{R}_i : \tau(\alpha) = -\alpha\} = \{\alpha \in \hat{R}_i : \bar{\alpha} = -\alpha\} = \{\alpha \in \hat{P}_i : \bar{\alpha} = -\alpha\} = \hat{P}_i^-.$$

This shows that

$$N^- = (\Gamma_p)^- \quad \text{and} \quad M^- = (N \cap \Lambda_p)^- = (\Gamma_p)^- \cap (\Lambda_p)^- = (\Lambda_p)^-.$$

Since  $\Gamma_p/\Lambda_p$  is a finite  $p$ -group, we may apply Exercise 50.5 to conclude that

$$k = |\Gamma_p : \Lambda_p| / |\Gamma_p^+ : \Lambda_p^+|.$$

We intend to use discriminants to calculate these indices.

Let  $T: A_p \times A_p \rightarrow \mathbb{Q}_p$  be the bilinear trace form

$$(x, y) \mapsto \text{Tr}_{A_p/\mathbb{Q}_p}(xy) \quad \text{for } x, y \in A_p.$$

Then  $T$  is a nondegenerate symmetric bilinear form, extending the usual trace form  $A \times A \rightarrow \mathbb{Q}$ . If  $\Lambda_p = \bigoplus_1^t \hat{Z}x_i$ , we define the discriminant

$$d(\Lambda_p) = \det(T(x_i x_j))_{1 \leq i, j \leq t}.$$

<sup>†</sup>Here, bar denotes the unique involution in  $\text{Gal}(\hat{K}/\hat{\mathbb{Q}})$ . The congruence holds for  $\alpha = \omega_i$  since  $\hat{P}_i = (1 - \omega_i)\hat{R}_i$ , and hence it holds for all  $\alpha \in \hat{R}_i$  because  $\hat{R}_i = \hat{Z}[\omega_i]$ .

Then  $d(\Lambda_p)$  is uniquely determined up to a unit factor from the ring  $\mathbb{Z}$  of  $p$ -adic integers (see §4E). By (4.26) we have

$$|\Gamma_p : \Lambda_p|^2 = \text{power of } p \text{ in } d(\Lambda_p)/d(\Gamma_p).$$

Likewise,  $T$  restricts to a trace form  $T^+ : A_p^+ \times A_p^+ \rightarrow \mathbb{Q}_p$ , where  $A_p^+$  = plus part of  $A_p = \{x \in A_p : \tau(x) = x\}$ , and we have

$$|\Gamma_p^+ : \Lambda_p^+|^2 = \text{power of } p \text{ in } d(\Lambda_p^+)/d(\Gamma_p^+).$$

Thus we obtain

$$k^2 = p\text{-part of } \frac{d(\Lambda_p)}{d(\Gamma_p)} \cdot \frac{d(\Gamma_p^+)}{d(\Lambda_p^+)}.$$

We shall now compute the  $p$ -part of  $d(\Gamma_p^+)/d(\Gamma_p)$ , and for this it suffices to treat separately each summand  $\tilde{R}_i$  of  $\Gamma_p$ . Let  $1 \leq i \leq m$ , and keep the notation in (50.39). Since the discriminant  $d(R_i/\mathbb{Z})$  is a power of  $p$ , and is unaffected by passage to  $p$ -adic completion, it follows that

$$p\text{-part of } d(\Gamma_p^+)/d(\Gamma_p) = d(\Gamma^+)/d(\Gamma).$$

We now use (see Exercise 50.9 for proof):

**(50.45) Lemma.** *Let  $K = \mathbb{Q}(\omega)$ ,  $R = \mathbb{Z}[\omega]$ , where  $\omega$  is a primitive  $p^s$ -th root of 1, with  $p$  odd and  $s \geq 1$ . Let*

$$K_0 = \mathbb{Q}(\omega + \bar{\omega}), \quad R_0 = \mathbb{Z}[\omega + \bar{\omega}] = \text{alg. int. } \{K_0\},$$

so  $K_0$  is the unique maximal real subfield of  $K$ . Then

$$d(R)/d(R_0) = p^{f(s)}, \quad \text{where } f(s) = \frac{1}{2}(sp^s - (s+1)p^{s-1} + 1).$$

Now let us set

$$(50.46) \quad w_s = \text{number of cyclic subgroups of } G \text{ of order } p^s.$$

In view of the isomorphism  $G \cong \text{Hom}(G, \mathbb{C}^\times)$ , it follows that  $w_s$  is also the number of quotient groups of  $G$  which are cyclic of order  $p^s$ . Hence  $w_s$  equals the number of simple summands of  $\mathbb{Q}G$  which are isomorphic to  $\mathbb{Q}(\omega)$ ,  $\omega$  = primitive  $p^s$ -th root of 1. From (50.45) we obtain

$$d(\Gamma)/d(\Gamma^+) = p^e, \quad \text{where } e = \sum_{s \geq 1} w_s f(s).$$

We shall now carry out the same computation for  $d(\Lambda_p)$  and  $d(\Lambda_p^+)$ . By

(27.1) we know that

$$d(\Lambda) = (p^n)^{p^n}, \quad \text{where } |G| = p^n.$$

(Here, we use the  $\mathbb{Z}$ -basis of  $\Lambda$  consisting of the elements of  $G$ .) Thus,  $d(\Lambda)$  coincides with the  $p$ -part of  $d(\Lambda_p)$ ; likewise  $d(\Lambda^+)$  is the  $p$ -part of  $d(\Lambda_p^+)$ . To compute  $d(\Lambda^+)$ , note that

$$\Lambda^+ = \mathbb{Z} \cdot 1 \oplus (\bigoplus_x \mathbb{Z} u_x), \quad \text{where } u_x = x + x^{-1},$$

and where  $x$  ranges over  $(p^n - 1)/2$  elements of  $G$ , one for each unordered pair  $(x, x^{-1})$ ,  $x \in G - \{1\}$ . Then clearly

$$u_x u_y = u_{xy} + u_{xy^{-1}}, \quad \text{where } u_1 = 2.$$

Let  $T^+$  be the trace form on  $A^+$ ; then  $T^+(1) = (p^n + 1)/2 = \dim_{\mathbb{Q}} A^+$ . An easy calculation, left to the reader, shows that  $T^+(u_x) = 1$  for  $x \in G - \{1\}$ . Therefore we obtain for  $x, y \in G - \{1\}$ :

$$T^+(u_x u_y) = T^+(u_{xy}) + T^+(u_{xy^{-1}}) = \begin{cases} 2 & \text{if } (x, x^{-1}) \neq (y, y^{-1}), \\ p^n + 2 & \text{if } (x, x^{-1}) = (y, y^{-1}). \end{cases}$$

Consequently we have

$$d(\Lambda^+) = \left| \begin{array}{ccccc} (p^n + 1)/2 & 1 & 1 & \cdots & 1 \\ 1 & p^n + 2 & 2 & \cdots & 2 \\ 1 & 2 & p^n + 2 & \cdots & 2 \\ \cdot & \cdot & \cdot & \ddots & \cdot \\ 1 & 2 & 2 & \cdots & p^n + 2 \end{array} \right|.$$

Subtracting twice the first row from the other rows, we find readily that

$$d(\Lambda^+) = p^{n(p^n + 1)/2}.$$

Combining all of the above formulas, we obtain

$$k = p^z, \quad \text{where } z = n(p^n - 1)/4 - \sum_{s \geq 1} w_s f(s)/2.$$

We are ready to compute the integer  $l$  occurring in (50.43). The group  $\Gamma \cap (1 + N)$  decomposes into a direct product

$$(1) \times \prod_{i=1}^m \{\alpha \in R_i : \alpha \equiv 1 \pmod{P_i}\},$$

using the notation of (50.39) and (50.41). (Note that  $-1 \notin 1 + N$ .) Next, since  $\{\Gamma^\circ \cap (1 + N)\}/\{\Lambda^\circ \cap (1 + N)\}$  is a  $p$ -group, Exercise 50.5 tells us that its minus part is

$$\{\Gamma^\circ \cap (1 + N)\}^-/\{\Lambda^\circ \cap (1 + N)\}^-,$$

and we now calculate these minus parts. For this purpose, we need:

**(50.47) Kummer's Lemma.** *Let  $p$  be any prime,  $p \geq 2$ , and let  $\omega$  be a primitive  $p^s$ -th root of 1, where  $s \geq 1$ . (Assume  $s \geq 2$  if  $p = 2$ ). Let*

$$K = \mathbb{Q}(\omega), \quad R = \mathbb{Z}[\omega], \quad R_0 = \mathbb{Z}[\omega + \bar{\omega}],$$

where bars denote complex conjugation.

(i) If  $p$  is odd, then

$$R^\circ = \langle \omega \rangle \times R_0^\circ,$$

that is, every unit of  $R$  is uniquely expressible as a power of  $\omega$  times a real unit.

(ii) If  $p = 2$ , then  $R^\circ = \langle \omega \rangle R_0^\circ$ , and  $\langle \omega \rangle \cap R_0^\circ = \{\pm 1\}$ .

*Proof.* (Kervaire-Murthy [77]). It suffices to prove for  $p \geq 2$  that  $R^\circ = \langle \omega \rangle R_0^\circ$ . Let  $\mathfrak{G}$  denote the Galois group  $\text{Gal}(K/\mathbb{Q})$ , and view complex conjugation on  $K$  as an element of  $\mathfrak{G}$ . Given  $u \in R^\circ$ , let  $v = \bar{u}/u$ , so  $v \in R^\circ$ . Then for all  $\sigma \in \mathfrak{G}$ ,

$$|\sigma(v)| = |\overline{\sigma u}/\sigma u| = |\overline{\sigma u}/\sigma u| = 1,$$

using the fact that  $\mathfrak{G}$  is abelian. For fixed  $m \in \mathbb{Z}$ , it follows that  $|\sigma(v^m)| = 1$  for all  $\sigma \in \mathfrak{G}$ . Therefore the coefficients of min. pol. <sub>$\mathbb{Q}$</sub> ( $v^m$ ) are rational integers, bounded independently of  $m$ . Consequently there are only finitely many distinct elements in the set  $\{v, v^2, \dots\}$ , so  $v$  is a root of 1. Therefore

$$\bar{u}/u = \pm \omega^t \quad \text{for some } t \in \mathbb{Z}.$$

If  $\bar{u}/u = \omega^t$ , where  $t = 2r$  is even, then  $u\omega^r \in R_0^\circ$  and  $u = \omega^{-r} \cdot u\omega^r \in \langle \omega \rangle R_0^\circ$ , as desired. The rest of the argument is aimed at proving that  $\bar{u}/u$  must equal  $\omega^t$  for some even integer  $t$ .

*Case 1.*  $p$  odd. Since  $t$  is determined mod  $p^s$ , we may assume  $t$  even. We claim that the equation  $\bar{u}/u = -\omega^t$  cannot occur. Indeed, since  $\bar{u} \equiv u \pmod{(1 - \omega)R}$ , the equation would imply that  $1 \equiv -1 \pmod{(1 - \omega)R}$ , a contradiction.

*Case 2.*  $p = 2, s \geq 2$ . Since  $-1$  is a power of  $\omega$ , we may write  $\bar{u}/u = \omega^t$  for some  $t \in \mathbb{Z}$ , and we need only show  $t$  even. Let  $N$  denote the norm map from  $K$  to  $\mathbb{Q}(i)$ , where  $i^2 = -1$ . Then  $N(\omega) = \pm i$ , and since  $Nu$  is a unit in  $\mathbb{Z}[i]$ , we must

have  $Nu = \pm 1$  or  $\pm i$ . From  $\bar{u} = \omega^t u$  we obtain

$$\overline{Nu} = N\bar{u} = (N\omega)^t Nu = (\pm i)^t Nu.$$

This implies that  $t$  is even, and completes the proof of Kummer's Lemma.

We now return to our calculations of  $\{\Gamma^* \cap (1 + N)\}^-$  and  $\{\Lambda^* \cap (1 + N)\}^-$ , where  $p$  is an odd prime. The involution  $\tau$  acts as complex conjugation on  $R$  and acts trivially on  $R_0 = \mathbb{Z}[\omega + \bar{\omega}]$ . From Kummer's Lemma we deduce that

$$(R^*)^+ = R_0^*, \quad \text{and} \quad (R^*)^- = \{\pm 1\} \times \langle \omega \rangle.$$

Therefore we obtain

$$\{\Gamma^* \cap (1 + N)\}^- = \prod_{i=1}^m \langle \omega_i \rangle.$$

Since  $Q(p^s \sqrt{1})$  occurs  $w_s$  times as a simple summand of  $A$ , we thus have

$$|\{\Gamma^* \cap (1 + N)\}^-| = p^{z'}, \quad \text{where } z' = \sum_{s \geq 1} sw_s.$$

On the other hand,  $\{\Lambda^* \cap (1 + N)\}^-$  is a subgroup of  $\{\Gamma^* \cap (1 + N)\}^-$ , hence is finite. But the only units of  $\Lambda$  of finite order are  $\{\pm g : g \in G\}$ , by Higman's Theorem (see page 164). Further,  $-g \notin 1 + N$  and  $g \in 1 + N$ , for  $g \in G$ . Therefore

$$|\{\Lambda \cap (1 + N)\}^-| = |G| = p^n,$$

and so we obtain  $|D^-(ZG)| = p^{z' - n}$ . Combining all of our results, we have now established:

**(50.48) Theorem (Fröhlich [72]).** *Let  $G$  be an abelian  $p$ -group of order  $p^n$ , where  $p$  is an odd prime. For  $s \geq 1$  let  $w_s$  be the number of cyclic subgroups of  $G$  of order  $p^s$ . Then  $|D^-(ZG)| = p^r$ , where*

$$4r = n(p^n + 3) - \sum_{s \geq 1} w_s(sp^s - (s+1)p^{s-1} + 1 + 4s).$$

As our first consequence, we obtain:

**(50.49) Corollary (Kervaire-Murthy [77]).** *Let  $G$  be a cyclic group of order  $p^n$ . Then  $|D^-(ZG)| = p^r$ , where*

$$r = \frac{1}{2} \left\{ \frac{p^n - 1}{p - 1} - n^2 \right\}.$$

Second, we obtain:

**(50.50) Corollary.** *Let  $G$  be an elementary abelian  $p$ -group of order  $p^n$ . Then  $|D^-(\mathbb{Z}G)| = p^r$ , where*

$$4r = 3n + \{(n-1)p^{n+1} - (n+3)p^n + p + 3\}/(p-1).$$

These formulas have been generalized to arbitrary  $p$ -groups by Oliver. We state without proof:

**(50.51) Theorem** (Oliver [83c]). *Let  $G$  be a  $p$ -group, where  $p$  is odd. Let  $C$  range over a full set of nonconjugate cyclic subgroups of  $G$ , with  $1 < C \leq G$ . For each  $C$ , let*

$$|N_G(C):C| = p^{a(C)}, \quad |C| \cdot |Z_G(C)| / |N_G(C)| = p^{b(C)},$$

where  $Z_G(C)$  is the centralizer of  $C$  in  $G$ , and  $N_G(C)$  the normalizer. Then  $|D^-(\mathbb{Z}G)| = p^r$ , where

$$r = \log_p |G:[G,G]| + \frac{1}{4} \sum_C \{(a(C)-1)\varphi(p^{b(C)}) + p^{b(C)} - 4b(C) - 1\}.$$

## §50F. Cyclic $p$ -Groups

We shall discuss here the calculation of the locally free class group  $\text{Cl } \mathbb{Z}G$  of a cyclic  $p$ -group  $G$ , where  $p$  is prime. The main results are due to Kervaire-Murthy [77] and Galovich [74], with later refinements by Ullom [77, 78], and Oliver [83c]. The Kervaire-Murthy article circulated in preprint form in the late 1960s, though it was published much later.

As usual, there is an exact sequence of finite abelian groups

$$(50.52) \quad 0 \rightarrow D(\mathbb{Z}G) \rightarrow \text{Cl } \mathbb{Z}G \rightarrow \text{Cl } \Lambda' \rightarrow 0,$$

where  $\Lambda'$  is the unique maximal  $\mathbb{Z}$ -order in  $\mathbb{Q}G$ . Then  $\Lambda'$  is a direct sum  $\coprod R_i$  of rings of cyclotomic integers, and  $\text{Cl } \Lambda' \cong \prod \text{Cl } R_i$ . These class groups  $\text{Cl } R_i$  have been studied intensively in algebraic number theory, and we shall not consider them further in this subsection. Most of the research on  $\text{Cl } \mathbb{Z}G$  has been devoted to the calculation of the kernel group  $D(\mathbb{Z}G)$ .

By Rim's Theorem 50.2 we have  $D(\mathbb{Z}G) = 0$  for  $|G| = p$ , so the first case to be handled here is that where  $G$  is cyclic of order  $p^2$ . For  $p = 2$  it is easily seen that  $D(\mathbb{Z}G) = 0$  (see Exercise 50.1). For odd  $p$ , the determination of  $D(\mathbb{Z}G)$  leads to delicate problems concerning units in cyclotomic fields, and is surprisingly difficult. As we shall see below in (50.56), the formula for  $|D(\mathbb{Z}G)|$  depends on whether  $p$  is a regular odd prime or not.

In §50E we have already obtained a lower bound for the order of  $D(\mathbb{Z}G)$ , when  $G$  is a cyclic group of order  $p^n$  with  $p$  odd. There is a canonical involution  $\tau$  acting on  $\mathbb{Z}G$ , given by  $\tau(x) = x^{-1}$  for  $x \in G$ , and extended by

linearity. This involution  $\tau$  acts on  $D(\mathbb{Z}G)$ , and we define

$$D^+(\mathbb{Z}G) = \{\xi \in D(\mathbb{Z}G) : \tau(\xi) = \xi\}, \quad D^-(\mathbb{Z}G) = \{\xi \in D(\mathbb{Z}G) : \tau(\xi) = -\xi\}.$$

Since  $D(\mathbb{Z}G)$  has odd order, we have (Exercise 50.5)

$$D(\mathbb{Z}G) = D^+(\mathbb{Z}G) \oplus D^-(\mathbb{Z}G).$$

We have already calculated  $|D^-|$  in (50.49), where we found that if  $G$  is cyclic of order  $p^n$ , with  $p$  odd, then

$$|D^-(\mathbb{Z}G)| = p^r, \quad \text{with } r = \frac{1}{2} \left\{ \frac{p^n - 1}{p - 1} - n^2 \right\}.$$

In particular,

$$|D^-(\mathbb{Z}G)| = p^{(p-3)/2} \quad \text{for } G \text{ cyclic of order } p^2, \text{ with } p \text{ odd.}$$

Before stating one of the main results, let us recall the definition of a regular prime. By definition, an odd prime  $p$  is *regular* if  $p$  does not divide the ideal class number  $h_R$ , where  $R = \mathbb{Z}[\omega]$ , with  $\omega$  a primitive  $p$ -th root of 1. As general reference for results about regular and irregular primes, see Borevich-Shafarevich [66]. To test a prime for regularity, one considers the Bernoulli numbers<sup>†</sup>

$$(50.53) \quad B_2, B_4, \dots, B_{2p^*}, \quad \text{where } p^* = (p-3)/2.$$

The first few of these are

$$\begin{aligned} B_2 &= 1/6, & B_4 &= -1/30, & B_6 &= 1/42, & B_8 &= -1/30, \\ B_{10} &= 5/66, & B_{12} &= -691/2730. \end{aligned}$$

Then  $p$  is regular if and only if  $p$  does not divide the numerator of the  $\{B_i\}$  listed in (50.53). The first three irregular primes are 37, 59 and 67. Of the first 550 primes, 216 of them are irregular, and 334 are regular.

We shall now prove the following result, due independently to Kervaire-Murthy [77] and Galovich [74]:

**(50.54) Theorem.** *Let  $G$  be cyclic of order  $p^2$ , where  $p$  is a regular odd prime. Then*

$$|D(\mathbb{Z}G)| = p^{(p-3)/2}.$$

*Proof.* Step 1. Let  $G = \langle x : x^{p^2} = 1 \rangle$  and  $R = \mathbb{Z}[\omega]$ , where  $\omega$  is a primitive  $p$ -th

<sup>†</sup>We now follow the standard notation for Bernoulli numbers, rather than that used in Volume I (page 741).

root of 1. We shall follow Galovich's approach, and begin by proving that whether or not  $p$  is regular, there is an exact sequence

$$(50.55) \quad R^\cdot \xrightarrow{j} \bar{R}^\cdot \rightarrow D(ZG) \rightarrow 0, \quad \text{where } \bar{R} = R/pR.$$

Let  $\Phi_{p^i}(x)$  be the cyclotomic polynomial whose zeros are the primitive  $p^i$ -th roots of 1. There is a fiber product

$$\begin{array}{ccc} ZG & \longrightarrow & \Gamma = Z[x]/(\Phi_p(x)\Phi_{p^2}(x)) \\ \downarrow & & \downarrow \\ Z & \longrightarrow & Z/p^2Z \end{array}$$

(see (2.12)). From (49.28) and (49.39), we obtain an exact sequence

$$\Gamma^\cdot \times Z^\cdot \rightarrow (Z/p^2Z)^\cdot \rightarrow D(ZG) \rightarrow D(\Gamma) \rightarrow 0.$$

However,  $\Gamma^\cdot$  maps onto  $(Z/p^2Z)^\cdot$ , since if  $m \in Z$  is prime to  $p$ , then the element  $(1 - x^m)/(1 - x)$  is a unit in  $\Gamma$ , and has image  $m \pmod{p^2}$  in  $Z/p^2Z$ . Thus we obtain  $D(ZG) \cong D(\Gamma)$ .

Let  $R_2 = Z[\omega_2]$ , where  $\omega_2$  is a primitive  $p^2$ -th root of 1. Then  $\Gamma$  is given by a fiber product

$$\begin{array}{ccc} \Gamma & \longrightarrow & R_2 = Z[x]/(\Phi_{p^2}(x)) \\ \downarrow & & \downarrow \\ R = Z[x]/(\Phi_p(x)) & \rightarrow & \bar{R}, \quad \text{where } \bar{R} = R/pR. \end{array}$$

As above, we obtain an exact sequence

$$R_2^\cdot \times R^\cdot \rightarrow \bar{R}^\cdot \rightarrow D(\Gamma) \rightarrow 0.$$

But  $R_2^\cdot$  and  $R^\cdot$  have the same image in  $\bar{R}^\cdot$  by Exercise 34.4, which establishes the exactness of the sequence (50.55).

*Step 2.* We must now evaluate  $\text{cok } j$ , where  $j: R^\cdot \rightarrow \bar{R}^\cdot$ . Let  $S = Z[\omega + \bar{\omega}]$ , where  $\bar{\omega}$  is the complex conjugate of  $\omega$ . By Kummer's Lemma 50.47, we have

$$R^\cdot = \langle \omega \rangle \times S^\cdot,$$

which will help us compute the image of  $R^\cdot$  in  $\bar{R}^\cdot$ . We set

$$\pi = 1 - \omega, \quad \pi_0 = (1 - \omega)(1 - \bar{\omega}),$$

so by Exercise 50.9 we obtain

$$pR = \pi^{p-1}R, \quad pS = \pi_0^{(p-1)/2}S.$$

Then  $\bar{R} = R/pR \cong \bar{\mathbb{Z}}[\pi]/(\pi^{p-1})$ , where  $\bar{\mathbb{Z}} = \mathbb{Z}/p\mathbb{Z}$ . This gives

$$\bar{R}^* = \bar{\mathbb{Z}}^* \times \langle 1 + \pi \rangle \times \langle 1 + \pi^2 \rangle \times \cdots \times \langle 1 + \pi^{p-2} \rangle,$$

a direct product of a cyclic group  $\bar{\mathbb{Z}}^*$  of order  $p-1$ , and  $p-2$  cyclic groups  $\langle 1 + \pi^i \rangle$ , each of order  $p$ . Likewise, setting  $\bar{S} = S/pS$ , we have

$$\bar{S}^* \cong \bar{\mathbb{Z}}^* \times \langle 1 + \pi_0 \rangle \times \langle 1 + \pi_0^2 \rangle \times \cdots \times \langle 1 + \pi_0^{p^*} \rangle,$$

where  $p^* = (p-3)/2$ . Since  $pR \cap S = pS$ , the map  $\bar{S} \rightarrow \bar{R}$  is injective, whence so is the map  $\bar{S}^* \rightarrow \bar{R}^*$ . Further, for  $1 \leq i \leq p^*$ ,

$$1 + \pi_0^i = 1 + (1 - \omega)^i(1 - \bar{\omega})^i \equiv 1 + \pi^{2i}(-1)^i \pmod{\pi^{2i+1}}.$$

It follows from the above remarks that there is an exact sequence

$$1 \rightarrow \bar{S}^* \rightarrow \bar{R}^* \rightarrow \bar{\mathbb{Z}}^{(p-1)/2} \rightarrow 0,$$

where  $\bar{\mathbb{Z}}^{(p-1)/2}$  denotes the direct sum of  $(p-1)/2$  cyclic groups of order  $p$ .

Now consider the map  $j: R^* \rightarrow \bar{R}^*$ , whose cokernel is a direct sum of copies of  $\bar{\mathbb{Z}}$ . Now  $j(\omega) = 1 - \pi$ , which generates the subgroup  $\langle 1 + \pi \rangle$  of  $\bar{R}^*$ . Furthermore, we have  $R^* = \langle \omega \rangle \times S^*$ , and the map  $S^* \rightarrow \bar{R}^*$  factors through  $\bar{S}^*$ . It follows at once that  $\text{cok } j$  is a direct sum of at least  $(p-3)/2$  copies of  $\bar{\mathbb{Z}}$ .

*Step 3.* It remains for us to show that when  $p$  is a regular prime, then  $\text{cok } j$  is at most  $p^*$  copies of  $\bar{\mathbb{Z}}$ . The crucial tool is an old result of Hilbert [70, sec. 138, p. 281]:

**Proposition.** *Keep the above notation. There exist units  $u_i \in S^*$ ,  $1 \leq i \leq p^*$ , such that*

$$\begin{aligned} u_1 &= 1 + a_1 \pi^2 & (\text{mod } \pi^3), \\ u_2 &\equiv 1 + a_2 \pi^4 & (\text{mod } \pi^5), \\ &\dots \\ u_{p^*} &\equiv 1 + a_{p^*} \pi^{p-3} & (\text{mod } \pi^{p-2}), \end{aligned}$$

where each  $a_i \in \mathbb{Z}$ , and where  $p \mid a_i$  if and only if  $p$  divides the numerator of the  $2i$ -th Bernoulli number  $B_{2i}$ .

Taking this for granted, we now finish the proof of the theorem. Assume  $p$  is regular, so each  $a_i$  above is prime to  $p$ , where  $1 \leq i \leq p^*$ . We are trying to find an upper bound on the size of  $\text{cok } j$ , where  $j: R^* \rightarrow \bar{R}^*$ . The proof of (50.2) shows that  $\text{im } j$  contains the factor  $\bar{\mathbb{Z}}^*$  of  $\bar{R}$ . Furthermore,  $\text{im } j \supseteq \langle 1 + \pi \rangle$  since  $j(\omega) = 1 - \pi$ . But  $\text{im } j$  also contains the product  $\langle u_1 \rangle \times \langle u_2 \rangle \times \cdots \times \langle u_{p^*} \rangle$ , where the  $\{u_i\}$  are as above. It follows that  $\text{cok } j$  is a direct sum of at most

$(p - 3)/2$  copies of  $\bar{\mathbb{Z}}$ . Combining this fact with the results of the previous steps, we conclude that  $\text{cok } j$  is the direct sum of exactly  $(p - 3)/2$  copies of  $\bar{\mathbb{Z}}$ , and the theorem is proved.

The above theorem can be generalized to the case of certain (possibly all) irregular primes. An odd prime  $p$  is called *properly irregular* if

$$p|h_R \text{ but } p \nmid h_S, \quad \text{where } R = \mathbb{Z}[\omega], \quad S = \mathbb{Z}[\omega + \bar{\omega}],$$

with  $\omega$  a primitive  $p$ -th root of 1. In all cases known to this date, a prime is either regular or properly irregular.

Let us denote by  $\delta(p)$  the number of Bernoulli numbers in (50.53) whose numerators are divisible by  $p$ . As remarked earlier,

$$\delta(p) = 0 \quad \text{if and only if } p \text{ is a regular prime.}$$

If  $\delta(p) > 0$ , then  $\delta(p)$  of the units  $\{u_i\}$ , given in Hilbert's Proposition above, have image 1 in  $\bar{R}$ . We might therefore suspect that (50.54) no longer holds in this case. In fact, the following generalization was proved independently by Kervaire-Murthy [77] and Galovich [74]:

**(50.56) Theorem.** *Let  $G$  be cyclic of order  $p^2$ , where  $p$  is an odd prime which is either regular or properly irregular. Let  $\delta(p)$  be the number of Bernoulli numbers  $\{B_{2i}: 1 \leq i \leq (p - 3)/2\}$  with numerators divisible by  $p$ . Then*

$$D(\mathbb{Z}G) \cong D^-(\mathbb{Z}G) \oplus D^+(\mathbb{Z}G),$$

and

$$D^-(\mathbb{Z}G) \cong \bar{\mathbb{Z}}^{(p-3)/2}, \quad D^+(\mathbb{Z}G) \cong \bar{\mathbb{Z}}^{\delta(p)},$$

where  $\bar{\mathbb{Z}} = \mathbb{Z}/p\mathbb{Z}$ .

**Remarks.** (i) For another proof, see Ullom [77], [78].

(ii) As predicted by (50.19),  $D(\mathbb{Z}G)$  is a group of exponent  $p$ .

(iii) Ullom [77] showed that for  $p$  properly irregular and  $G$  cyclic of order  $p^n$ ,  $n \geq 2$ , the sequence (50.52) is *not* split.

We turn next to the case of cyclic groups of order  $p^n$ , where  $p \geq 2$  and  $n \geq 2$ . Let

$$G_n = \langle x: x^{p^n} = 1 \rangle, \quad G_{n-1} = \langle x: x^{p^{n-1}} = 1 \rangle,$$

and view  $G_{n-1}$  as a factor group of  $G_n$ . We calculate  $D(\mathbb{Z}G_n)$  by relating it to  $D(\mathbb{Z}G_{n-1})$  via a Mayer-Vietoris sequence. For each  $n$ , let us set

$$(50.57) \quad R_n = \mathbb{Z}[\omega_n], \quad K_n = \mathbb{Q}(\omega_n), \quad \bar{R}_n = R_n / (1 - \omega_n)^{p^{n-1}} R_n,$$

where  $\omega_n$  is a primitive  $p^n$ -th root of 1, and where  $\omega_{n-1} = \omega_n^p$ . Let  $\Phi_{p^n}(x) = \min.\text{pol.}_{\mathbb{Q}}(\omega_n)$ , the  $p^n$ -th cyclotomic polynomial. From the formula

$$x^{p^n} - 1 = \Phi_{p^n}(x) \cdot (x^{p^{n-1}} - 1),$$

we obtain a fiber product diagram

$$\begin{array}{ccc} \mathbb{Z}G_n & \longrightarrow & \mathbb{Z}G_{n-1} \\ \downarrow & & \downarrow \\ R_n & \longrightarrow & \bar{R}_n \cong \bar{\mathbb{Z}}G_{n-1}, \end{array}$$

where  $\bar{\mathbb{Z}} = \mathbb{Z}/p\mathbb{Z}$ . From (49.28) and (49.39), there is an exact sequence

$$1 \rightarrow (\mathbb{Z}G_n)^* \rightarrow R_n^* \times (\mathbb{Z}G_{n-1})^* \xrightarrow{j} \bar{R}_n^* \rightarrow D(\mathbb{Z}G_n) \rightarrow D(\mathbb{Z}G_{n-1}) \rightarrow 0.$$

The problem thus reduces to calculating  $\text{cok } j$ . Let us set<sup>†</sup>

$$(50.58) \quad V_n = \text{cok } j = \bar{R}_n^*/\text{image of } (R_n^* \times (\mathbb{Z}G_{n-1})^*).$$

Suppose first that  $p$  is odd, and let  $\tau$  be the canonical involution on  $\mathbb{Z}G_n$ , acting also on  $D(\mathbb{Z}G_n)$ ,  $D(\mathbb{Z}G_{n-1})$ , and  $V_n$ . There is then an exact sequence of “minus parts” relative to  $\tau$ :

$$0 \rightarrow V_n^- \rightarrow D^-(\mathbb{Z}G_n) \rightarrow D^-(\mathbb{Z}G_{n-1}) \rightarrow 0,$$

and (50.49) can be used to calculate the orders of those terms. The difficulty lies in determining  $V_n^+$ . We quote without proof the following result of Kervaire-Murthy, which depends on Iwasawa’s work on cyclotomic fields:

**(50.59) Theorem.** *Keep the above notation, and let  $p$  be an odd prime which is either regular or properly irregular. Then there is a canonical injection*

$$\text{character group of } V_n^+ \rightarrow p\text{-primary component of } (\text{Cl } R_{n-1})^-.$$

In particular, if the prime  $p$  is regular, then  $|\text{Cl } R_{n-1}|$  is prime to  $p$  for all  $n \geq 2$ , and therefore  $V_n^+ = 1$  whenever  $p$  is regular. This yields the important consequence, due to Kervaire-Murthy [77] and Galovich [74]:

**(50.60) Corollary.** *For  $p$  a regular odd prime and  $G$  cyclic of order  $p^n$ ,  $n \geq 1$ , we have  $D^+(\mathbb{Z}G) = 0$  and*

$$|D(\mathbb{Z}G)| = |D^-(\mathbb{Z}G)| = p^r, \quad \text{where } r = \frac{1}{2} \left( \frac{p^n - 1}{p - 1} - n^2 \right).$$

Kervaire-Murthy also settle the case  $p = 2$ :

<sup>†</sup>Kervaire-Murthy and Ullom choose  $G$  cyclic of order  $p^{n+1}$ . Our  $V_{n+1}$  is their  $V_n$ .

**(50.61) Theorem.** *Let  $G$  be cyclic of order  $2^n$ ,  $n \geq 1$ . Then*

$$|D(\mathbb{Z}G)| = 2^r, \quad \text{where } r = 2^{n-1} - \frac{1}{2}n(n-1) - 1.$$

We turn next to the refinements of these results, due to Ullom [77, 78] and Oliver [83c]. Let  $p$  be an odd prime, and let  $G$  be cyclic of order  $p^n$ ,  $n \geq 2$ . Then

$$\text{Aut } G \cong \text{Gal}(K_n/\mathbb{Q}) \cong \text{cyclic group of order } p^{n-1}(p-1).$$

Let  $\Delta$  be the unique subgroup of  $\text{Aut } G$  of order  $p-1$ , and identify  $\Delta$  with  $\text{Gal}(K_1/\mathbb{Q})$ . Then  $\Delta$  acts on  $\mathbb{Z}G$  and  $\Lambda'$ , inducing an action of  $\Delta$  on the groups  $D(\mathbb{Z}G)$ ,  $\text{Cl}\mathbb{Z}G$ , and  $\text{Cl}\Lambda'$ . Let  $\hat{\mathbb{Z}}$  denote the  $p$ -adic completion of  $\mathbb{Z}$ . Since  $D(\mathbb{Z}G)$  is a finite  $p$ -group, we may view it as a  $\hat{\mathbb{Z}}\Delta$ -module. Now  $\hat{\mathbb{Z}}$  contains a primitive  $(p-1)$ -st root of 1, say  $\theta$  (see Volume I, bottom of page 748), and there is a decomposition

$$\hat{\mathbb{Z}}\Delta \cong \coprod_{i=0}^{p-2} \hat{\mathbb{Z}}e_i,$$

where the  $\{e_i\}$  are primitive idempotents in  $\hat{\mathbb{Z}}\Delta$ , and where a generator  $\delta$  of  $\Delta$  acts as  $\theta^i$  on  $e_i$ . Each  $\hat{\mathbb{Z}}\Delta$ -module  $M$  then decomposes into a direct sum of eigenspaces:

$$M = \bigoplus_{i=0}^{p-2} e_i M, \quad \text{with } e_i M = \{m \in M : \delta m = \theta^i m\}, \quad 0 \leq i \leq p-2.$$

Let  $\tau$  be the canonical involution of  $\mathbb{Z}G$ , which acts on  $D(\mathbb{Z}G)$ . It is easily seen that

$$D^+(\mathbb{Z}G) = \bigoplus_{i \text{ even}} e_i D(\mathbb{Z}G), \quad D^-(\mathbb{Z}G) = \bigoplus_{i \text{ odd}} e_i D(\mathbb{Z}G),$$

and there are corresponding decompositions of the group  $V_n$  defined in (50.58).

Now consider the automorphism of  $G$  given by  $g \rightarrow g^{1+p}$ ,  $g \in G$ , which induces an automorphism  $\gamma$  of  $D(\mathbb{Z}G)$  for which  $\gamma^{p^{n-2}} = 1$ . Then  $D(\mathbb{Z}G)$  is a  $\hat{\mathbb{Z}}[\gamma]$ -module, on which  $\gamma - 1$  acts nilpotently. As in Iwasawa theory, we introduce the power series ring  $\Lambda = \hat{\mathbb{Z}}[[T]]$  in an indeterminate  $T$ . Then  $D(\mathbb{Z}G)$  can be made into a left  $\Lambda$ -module by letting  $T$  act as  $\gamma - 1$ . The map  $D(\mathbb{Z}G_n) \rightarrow D(\mathbb{Z}G_{n-1})$  is then a  $\Lambda$ -homomorphism, so  $V_n$  and its eigenspaces  $e_i V_n$  are also  $\Lambda$ -modules. Ullom [77] proved that each  $e_i V_n$  is a cyclic left  $\Lambda$ -module, whose generator can be given explicitly. From this he showed that for  $n \geq 2$ ,

$$\text{ann}_\Lambda e_i V_n = p \text{ann}_\Lambda e_i V_{n-1} + T^{p^{n-2} - \delta_{11}} \Lambda, \quad i \text{ odd}, 1 \leq i \leq p-2,$$

where  $\delta_{11}$  = Kronecker delta. (An analogous formula holds for  $p = 2$ .) From the

above, it follows that

$$e_i V_n \cong \coprod_{r=0}^{n-2} (\mathbb{Z}/p^{n-1-r}\mathbb{Z})^{(\varphi(p^r))}, \quad i \text{ odd, } 3 \leq i \leq p-2,$$

while for  $e_1 V_n$  the term with  $r=0$  must be omitted. This readily yields the known formula for  $|D^-(\mathbb{Z}G_n)|$ .

On the other hand,  $V_n^+ = \bigoplus_{i \text{ even}} e_i V_n$ . These even eigenspaces  $\{e_i V_n\}$  were studied by Ullom [78], who showed that  $e_0 V_n = 0$ . Further, for irregular  $p$  satisfying some mild hypothesis (see below) known to hold for  $p < 125,000$ ,  $e_i V_n \cong e_i(P_n/Q_n)$ , where  $P_n/Q_n$  is a ray class group. Specifically,

$$\begin{aligned} P_n &= \text{group of principal } R_n\text{-ideals of } K_n \text{ prime to } p, \\ Q_n &= \text{subgroup of all } \{R_n a : a \in K_n, v_n(a-1) \geq v_n(1 - \omega_1)\}, \end{aligned}$$

where  $v_n$  is the  $p$ -adic exponential valuation of  $K_n$ . (The isomorphism  $e_i V_n \cong e_i(P_n/Q_n)$  for odd  $i$  was pointed out in Ullom [77], and follows from Reiner-Ullom [74b].) For even  $i$ , Ullom [78] computed the annihilator of the  $\Lambda$ -module  $e_i(P_n/Q_n)$ , which leads to the following result:

**(50.62) Theorem (Ullom [78]).** *Let  $G_n$  be cyclic of order  $p^n$ ,  $n \geq 2$ , where  $p$  is an odd prime which is either regular or properly irregular. If  $n \geq 3$ , assume that for each  $i$ , the Iwasawa invariant  $\lambda_i$  is 0 or 1. Let  $\delta(p)$  be as in (50.56). Then*

- (i)  $e_0 V_n = e_0 D(\mathbb{Z}G_n) = 0$ .
- (ii) For even  $i$ ,  $2 \leq i \leq p-3$ ,

$$e_i V_n = 0 \text{ if } p \nmid B_i, \quad \text{and} \quad e_i V_n \cong \mathbb{Z}/p^{n-1}\mathbb{Z} \text{ if } p \mid B_i.$$

Therefore

$$e_i D(\mathbb{Z}G_n) = 0 \text{ if } p \nmid B_i, \quad \text{and} \quad e_i D(\mathbb{Z}G_n) \cong \coprod_{j=1}^{n-1} \mathbb{Z}/p^j\mathbb{Z} \text{ if } p \mid B_i.$$

(iii)  $\bigoplus_{i \text{ even}} e_i V_n$  is isomorphic to the direct sum of  $\delta(p)$  copies of  $\mathbb{Z}/p^{n-1}\mathbb{Z}$ .  
Therefore

$$D^+(\mathbb{Z}G) \cong \text{direct sum of } \delta(p) \text{ copies of } \coprod_{j=1}^{n-1} \mathbb{Z}/p^j\mathbb{Z},$$

and

$$|D^+(\mathbb{Z}G_n)| = p^m, \quad \text{where } m = \delta(p)n(n-1)/2.$$

**Remarks.** (i) The above theorem includes Theorems 50.56 and 50.60 as special cases. Theorem 50.61 is a consequence of the work in Ullom [77].

(ii) Oliver [83c] has completely determined the structure of  $D^-(\mathbb{Z}G_n)$  as abelian group.

## §50G. Twisted Group Rings and Crossed-Product Orders

The study of integral group rings often leads to problems involving twisted group rings; see (28.4) and §§50C,D for example. These are, in turn, special cases of the more general concept of a crossed-product order, already encountered in Volume I, p. 268, Example (b), as well as in (28.12). Before stating Wilson's Theorem 50.64, which is the main result of this subsection, we recall some definitions and fix the notation.

We assume throughout that  $R, S$  are Dedekind domains with quotient fields  $K, L$ , respectively, where  $L$  is a finite Galois extension of  $K$  with Galois group  $G = \text{Gal}(L/K)$ , and where  $S$  is the integral closure of  $R$  in  $L$ . The *twisted group algebra*  $L^\circ G$ , and the *twisted group ring*  $S^\circ G$ , are defined by

$$L^\circ G = \bigoplus_{\sigma \in G} Lu_\sigma, \quad S^\circ G = \bigoplus_{\sigma \in G} Su_\sigma, \quad \text{where } u_\sigma a = \sigma(a)u_\sigma, u_\sigma u_\tau = u_{\sigma\tau}$$

for all  $\sigma, \tau \in G$  and  $a \in S$ . Then  $S^\circ G$  is an  $R$ -order in the  $K$ -algebra  $L^\circ G$ , and by (28.3)  $L^\circ G \cong M_n(K)$ , where  $n = \dim_K L = |G|$ .

Let us generalize this construction by assuming instead that the  $S$ -basis elements  $\{u_\sigma : \sigma \in G\}$  multiply according to some factor set  $f: G \times G \rightarrow S^*$ . The *crossed-product algebra*  $(L^\circ G)_f$  and the *crossed-product order*  $(S^\circ G)_f$  are defined by setting

$$(50.63) \quad \begin{cases} (L^\circ G)_f = \bigoplus_{\sigma \in G} Lu_\sigma, & (S^\circ G)_f = \bigoplus_{\sigma \in G} Su_\sigma, \\ \text{where } u_\sigma a = \sigma(a)u_\sigma \quad \text{and} \quad u_\sigma u_\tau = f(\sigma, \tau)u_{\sigma\tau} & \text{for all } \sigma, \tau \in G, \quad a \in L. \end{cases}$$

The condition that  $f$  be a factor set is equivalent to the condition that multiplication of the elements  $\{u_\sigma\}$  be associative. As pointed out in (8.33i) (see also MO §29),  $(L^\circ G)_f$  is a central simple  $K$ -algebra, often denoted by  $(L/K, f)$ . Up to  $K$ -isomorphism, this algebra depends only on the class of  $f$  in the cohomology group  $H^2(G, L)$ . Of course, when  $f = 1$  we have the usual twisted group algebra  $L^\circ G$ .

The main result, due to S. M. J. Wilson [77b], is as follows:

**(50.64) Theorem.** *Let  $\Lambda = (S^\circ G)_f$  be the crossed-product order defined in (50.63), and assume that  $K$  is a global field. Then the kernel group  $D(\Lambda)$  is 0.*

We remark that if  $S$  is tamely ramified over  $R$ , then  $\Lambda$  is a hereditary  $R$ -order by Williamson's Theorem (see (28.12) or Exercise 50.10). In this case, we already know that  $D(\Lambda) = 0$  by (49.35).

Turning to the general case, the proof proceeds in a number of steps, which we now list:

- (i) Technical results on reduced norms; see (50.65), (50.66), and Exercise 50.11.
- (ii) Reduction of the problem to the local case.
- (iii) Preliminary result for the tamely ramified case; see (50.69).
- (iv) The case of wild ramification with cyclic ramification group; see (50.73).
- (v) Reduction to the cyclic case via local class field theory.

We begin with some results on reduced norms; as general references on this topic, see §7D and §45A, as well as *MO* §9.

**(50.65) Lemma.** *Let  $A = (L \circ G)_f$  as in (50.63), where  $G = \{\sigma_1, \dots, \sigma_n\}$ . There is a  $K$ -algebra monomorphism  $\varphi: A \rightarrow M_n(L)$ , given by*

$$\begin{aligned}\varphi(a) &= a^*, \quad \text{where } a^* = \text{diag}(\sigma_1^{-1}a, \dots, \sigma_n^{-1}a), \quad a \in L, \\ \varphi(u_\sigma) &= U(\sigma), \quad \text{where } U(\sigma) = [(\sigma\sigma_j)^{-1}f(\sigma, \sigma_j)\delta_{\sigma_i, \sigma\sigma_j}]_{1 \leq i, j \leq n},\end{aligned}$$

for  $\sigma \in G$ . Furthermore, for each  $x \in A$  we have

$$\text{nr}_{A/K}x = \det \varphi(x),$$

where  $\text{nr}_{A/K}$  is the reduced norm map from  $A$  to its center  $K$ .

*Proof.* (Compare with Exercises 28.2, 28.3) Let  $\mathbf{w} = (u_{\sigma_1}, \dots, u_{\sigma_n})$  be a row vector. It is easily verified that for  $a \in L$ ,  $\sigma, \tau \in G$ ,

$$a\mathbf{w} = \mathbf{w}a^*, \quad u_\sigma \mathbf{w} = \mathbf{w}U(\sigma).$$

This yields the formulas

$$U(\sigma)a^* = (\sigma(a))^*U(\sigma), \quad U(\sigma)U(\tau) = (f(\sigma, \tau))^*U(\sigma\tau),$$

so after extending  $\varphi$  by linearity, we obtain a  $K$ -algebra homomorphism  $\varphi: A \rightarrow M_n(L)$ . Further,  $\ker \varphi = 0$  since  $A$  is simple. It follows that the map

$$1 \otimes \varphi: L \otimes_K A \rightarrow M_n(L)$$

is an  $L$ -isomorphism. Therefore for  $x \in A$ ,

$$\text{red. char. pol.}_{A/K}x = \text{char. pol. of the matrix } \varphi(x).$$

This implies the desired formula for  $\text{nr}_{A/K}x$ .

**(50.66) Lemma.** *Let  $G = \text{Gal}(L/K)$ , and let  $H \leq G$ . Let  $L_0$  be the subfield of  $L$  fixed elementwise by  $H$ , so  $H = \text{Gal}(L/L_0)$ . Set*

$$A = (L \circ G)_f, \quad B = (L \circ H)_f,$$

viewing  $B$  as  $K$ -subalgebra of  $A$ . Then

$$\text{nr}_{A/K} b = N_{L_0/K}(\text{nr}_{B/L_0} b) \quad \text{for } b \in B,$$

where  $N_{L_0/K}$  is the usual norm from  $L_0$  to  $K$ .

*Proof.* We observe first that  $B$  is a central simple  $L_0$ -algebra. Now set

$$|G| = n, \quad |H| = m, \quad d = |G:H| = n/m = \dim_K L_0.$$

Let  $b \in B$  act by right multiplication on both  $A$  and  $B$ . By (7.34),

$$\begin{aligned} f(X) &= \text{char. pol.}_{B/L_0} b = \{\text{red. char. pol.}_{B/L_0} b\}^m, \\ g(X) &= \text{char. pol.}_{A/K} b = \{\text{red. char. pol.}_{A/K} b\}^n. \end{aligned}$$

Since  $A \cong B^{(d)}$  as right  $B$ -modules, we obtain

$$g(X) = \{\text{char. pol.}_{B/K} b\}^d = \{N_{L_0/K} f(X)\}^d,$$

the second equality by MO (9.12). Since  $n = md$ , we deduce that

$$\text{red. char. pol.}_{A/K} b = N_{L_0/K}(\text{red. char. pol.}_{B/L_0} b).$$

Comparing constant terms, the formula for  $\text{nr}_{A/K} b$  is now clear.

**(50.67) Corollary.** *There is a commutative diagram*

$$\begin{array}{ccc} K_1(B) & \xrightarrow{\theta} & K_1(A) \\ \text{nr} \downarrow & & \text{nr} \downarrow \\ L_0^\times & \xrightarrow{N_{L_0/K}} & K^\times, \end{array}$$

where  $\theta$  is the “change of rings” homomorphism arising from the inclusion  $B \rightarrow A$ .

Continuing with the proof of Wilson’s Theorem, let  $\Lambda = (S \circ G)_f$  and  $A = (L \circ G)_f$ , as in (50.63). From (26.2) we have  $\text{nr}_{A/K} \Lambda \subseteq R$ , and therefore  $\text{nr}_{A/K} \Lambda^\times \subseteq R^\times$  since  $\text{nr}$  is multiplicative. Let  $P$  range over the maximal ideals of  $R$ . For each  $P$ ,  $\Lambda_P$  is an  $R_P$ -order in the central simple  $K_P$ -algebra  $A_P$ . Using the formula for  $D(\Lambda)$  in Theorem 49.36, we see that in order to prove  $D(\Lambda) = 0$ , it suffices to show that  $\text{nr } \Lambda_P^\times = R_P^\times$  for each  $P$ .

Keep  $P$  fixed, and let us write

$$PS = (P_1 \cdots P_g)^e,$$

where the  $\{P_i\}$  are the distinct maximal ideals of  $S$  containing  $P$ . Since  $G = \text{Gal}(L/K)$  acts transitively on the  $\{P_i\}$ , they all have the same ramification index  $e$  in the extension  $L/K$ . Let

$L_i = P_i$ -adic completion of  $L$ ,  $S_i = P_i$ -adic completion of  $S$ , for  $1 \leq i \leq g$ ,

so  $S_i$  is the valuation ring of  $L_i$ . We have

$$L_P = K_P \otimes_K L \cong \coprod_{i=1}^g L_i, \quad S_P = R_P \otimes_R S \cong \coprod_{i=1}^g S_i.$$

The *decomposition group* of  $P_1$  (for the extension  $L/K$ ) is defined as

$$D = \{\sigma \in G : \sigma(P_1) = P_1\}$$

(see Volume I, page 599). In Step 3 of the proof of (46.24), we showed that the direct sum decomposition of  $S_P$  gives rise to an isomorphism of  $R_P$ -algebras:

$$\Lambda_P \cong M_g(\Gamma), \quad \text{where } \Gamma = (S_1 \circ D)_f = \bigoplus_{\sigma \in D} S_1 u_\sigma.$$

Here,  $f$  is viewed as a factor set  $f : D \times D \rightarrow S_1^\times$ , via the homomorphism  $S^\times \rightarrow S_1^\times$ . It follows that  $K_1(\Lambda_P) \cong K_1(\Gamma)$ . Further,  $\Gamma$  is an order in a central simple  $K_P$ -algebra, and

$$\text{nr } K_1(\Lambda_P) = \text{nr } K_1(\Gamma) = \text{nr } \Gamma^\times,$$

the latter equality holding since  $\Gamma^\times$  maps onto  $K_1(\Gamma)$ . Thus, in order to prove that  $\text{nr } \Lambda_P^\times = R_P^\times$ , it suffices to show that  $\text{nr } \Gamma^\times = R_P^\times$ . Note that  $D = \text{Gal}(L_1/K_P)$ .

*Changing notation for the rest of the proof*, we may assume that  $R$  is a complete d.v.r. with maximal ideal  $P$  and finite residue class field  $\bar{R} = R/P$  of characteristic  $p$ , and that  $L/K$  is a finite extension of local fields with Galois group  $G = \text{Gal}(L/K)$ . Let  $\Lambda = (S \circ G)_f$ ,  $A = (L \circ G)_f$  as in (50.63). We must show that in this situation,  $\text{nr}_{A/K} \Lambda^\times = R^\times$ .

Let us recall some definitions and facts from ramification theory, as described in any standard reference on algebraic number theory. Let  $G = \text{Gal}(L/K)$ , with  $K$  local, as above. Let  $S$  be the valuation ring of  $L$ ,  $\mathfrak{P}$  the maximal ideal of  $S$ , and let  $\bar{S} = S/\mathfrak{P}$  be its residue class field. Define the *inertia group*  $G_0$  and the *first ramification group*  $G_1$  by the formula

$$G_i = \{\sigma \in G : \sigma(x) \equiv x \pmod{\mathfrak{P}^{i+1}} \text{ for all } x \in S\}, \quad i = 0, 1.$$

Both  $G_0$  and  $G_1$  are normal subgroups of  $G$ . Let  $L_i$  be the subfield of  $L$  fixed by  $G_i$ , and let  $S_i$  be the valuation ring of  $L_i$ , and  $\mathfrak{P}_i$  the maximal ideal of  $S_i$ ,

for  $i = 0, 1$ . We have a diagram

$$\begin{array}{ccccccc}
 L & S & \mathfrak{P} = \pi S & & \bar{S} = S/\mathfrak{P} \\
 | & | & | & & | \\
 L_1 & S_1 & \mathfrak{P}_1 = \pi_1 S_1 & & \bar{S}_1 = S_1/\mathfrak{P}_1 \\
 | & | & | & & | \\
 L_0 & S_0 & \mathfrak{P}_0 = \pi_0 S_0 & & \bar{S}_0 = S_0/\mathfrak{P}_0 \\
 | & | & | & & | \\
 K & R & P & & \bar{R} = R/P.
 \end{array}$$

The following facts are well known:

- (i)  $L_0/K$  is unramified, and

$$G/G_0 \cong \text{Gal}(L_0/K) \cong \text{Gal}(\bar{S}/\bar{R}).$$

- (ii)  $L/L_0$  is completely ramified, so  $\bar{S} = \bar{S}_1 = \bar{S}_0$ .
- (iii)  $L_1/L_0$  is tamely ramified, and

$$G_0/G_1 \cong \text{Gal}(L_1/L_0) = \text{cyclic group of order } e', \text{ where } p \nmid e'.$$

- (iv)  $L/L_1$  is wildly ramified, and

$$G_1 = \text{Gal}(L/L_1) = p\text{-group}.$$

- (v) Using the Schur-Zassenhaus Theorem, it follows that  $G_0$  is a semidirect product

$$(50.68) \quad G_0 = G_1 \rtimes \langle \varphi \rangle \text{ for some cyclic group } \langle \varphi \rangle \text{ of order } e'.$$

We shall consider the  $R$ -order  $\Lambda = (S^\circ G)_f$  in the  $K$ -algebra  $A = (L^\circ G)_f$ , as in (50.63). For convenience of notation, we shall use the notation  $\text{nr}_{\Lambda/R}$  to denote the restriction to  $\Lambda$  of the reduced norm  $\text{nr}_{A/K}$ . Likewise, for  $i = 0, 1$ ,  $N_{S_i/R}$  will mean the restriction to  $S_i$  of the field norm  $N_{L_i/K}$ . Keeping this notation, we prove a preliminary result which essentially involves just tame ramification.

**(50.69) Proposition.** *Consider the crossed-product orders*

$$\Lambda_1 = (S^\circ G_1)_f \subseteq \Lambda_0 = (S^\circ G_0)_f \subseteq \Lambda = (S^\circ G)_f.$$

*Then the norm  $N_{S_1/R}$  induces a surjective homomorphism*

$$N_{S_1/R}: \frac{S_1^\circ}{\text{nr}_{\Lambda_1/S_1} \Lambda_1^\circ} \longrightarrow \frac{R^\circ}{\text{nr}_{\Lambda/R} \Lambda^\circ}.$$

*Proof.* By Lemma 50.66, we have

$$N_{S_1/R}(\text{nr}_{\Lambda_1/S_1} \Lambda_1^\circ) \subseteq \text{nr}_{\Lambda/R} \Lambda^\circ,$$

so the above map on quotients is well-defined. Likewise, there is a homomorphism

$$(50.70) \quad N_{S_1/S_0}: \frac{S_1^\circ}{\text{nr}_{\Lambda_1/S_1} \Lambda_1^\circ} \longrightarrow \frac{S_0^\circ}{\text{nr}_{\Lambda_0/S_0} \Lambda_0^\circ}.$$

Now  $N_{S_0/R}(S_0^\circ) = R^\circ$  because  $S_0/R$  is unramified. Hence, to establish the proposition, it suffices to prove that the map  $N_{S_1/S_0}$  in (50.70) is surjective.

The reduced norm  $\text{nr}_{\Lambda_0/S_0}$  maps  $\mathfrak{P}\Lambda_0$  into  $\mathfrak{P}_0$ , and induces a map  $\overline{\text{nr}}: \Lambda_0/\mathfrak{P}\Lambda_0 \rightarrow S_0/\mathfrak{P}_0$ . We may write

$$\bar{\Lambda}_0 = \Lambda_0/\mathfrak{P}\Lambda_0 = \left\{ \bigoplus_{\sigma \in G_0} S u_\sigma \right\} / \left\{ \bigoplus_{\sigma \in G_0} \mathfrak{P} u_\sigma \right\} = \bigoplus_{\sigma \in G_0} \bar{S} \bar{u}_\sigma,$$

where  $\bar{S} = S/\mathfrak{P}$ . Then  $G_0$  acts trivially on  $\bar{S}$ , and the structure of the  $\bar{S}$ -algebra  $\bar{\Lambda}_0$  is determined by the multiplication formula

$$\bar{u}_\sigma \bar{u}_\tau = \overline{f(\sigma, \tau)} \bar{u}_{\sigma\tau} \quad \text{for } \sigma, \tau \in G_0.$$

There is a commutative diagram

$$(50.71) \quad \begin{array}{ccc} \Lambda_0^\circ & \xrightarrow{\text{nr}_{\Lambda_0/S_0}} & S_0^\circ \\ \downarrow & & \downarrow \\ \bar{\Lambda}_0^\circ & \xrightarrow{\overline{\text{nr}}} & \bar{S}_0^\circ \cong \bar{S}^\circ, \end{array}$$

which we shall use in a moment.

Writing  $G_0 = G_1 \rtimes \langle \varphi \rangle$  as in (50.68), consider the  $\bar{S}$ -subalgebra  $\Phi$  of  $\bar{\Lambda}_0$  given by

$$\Phi = \bigoplus_{i=0}^{e'-1} \bar{S} \bar{u}_{\varphi^i}.$$

We may assume the factor set  $f$  chosen so that

$$u_{\varphi^i} = (u_\varphi)^i, \quad 0 \leq i \leq e' - 1; \quad (u_\varphi)^{e'} = \beta \in S^\circ,$$

where  $\varphi(\beta) = \beta$ . Consequently we obtain

$$\Phi \cong \bar{S}[X]/(X^{e'} - \bar{\beta}) \cong \coprod_j F_j,$$

with each  $F_j$  a finite field extension of  $\bar{S}$ . There is then a surjection

$$N: \Phi^{\cdot} \rightarrow \bar{S}^{\cdot}, \quad \text{where } N = \prod_j N_{F_j/\bar{S}}.$$

We note next that  $\bar{\Lambda}_0$  is a free  $\Phi$ -module of rank  $q$ , where  $q = |G_1|$ . It is easily verified that

$$\overline{\text{nr}} \ x = (Nx)^q \quad \text{for } x \in \Phi^{\cdot}.$$

Since the map  $\alpha \in \bar{S}^{\cdot} \rightarrow \alpha^q \in \bar{S}^{\cdot}$  is a surjection of  $\bar{S}^{\cdot}$  onto itself, and since  $N$  is surjective, it follows that  $\overline{\text{nr}} \ \bar{\Lambda}_0^{\cdot} = \bar{S}^{\cdot}$ . We may then conclude from (50.71) that

$$(50.72) \quad \text{nr}_{\Lambda_0/S_0} \Lambda_0^{\cdot} \equiv S_0^{\cdot} \pmod{(1 + \mathfrak{P})},$$

where this congruence (and the later ones as well) are to be read multiplicatively. Since  $\text{nr} \ \Lambda_0$  and  $S_0$  lie in  $L_0$ , and  $\mathfrak{P} \cap L_0 = \mathfrak{P}_0$ , the above congruence holds  $\pmod{(1 + \mathfrak{P}_0)}$ .

For any  $y \in \mathfrak{P}_0$  we have  $N_{S_1/S_0}(1 + y) = (1 + y)^{e'}$ ; since  $p \nmid e'$ , we conclude that  $N_{S_1/S_0}(1 + \mathfrak{P}_0) = 1 + \mathfrak{P}_0$ . Therefore

$$N_{S_1/S_0} S_1^{\cdot} \supseteq N_{S_1/S_0}(1 + \mathfrak{P}_1) \supseteq N_{S_1/S_0}(1 + \mathfrak{P}_0) = 1 + \mathfrak{P}_0.$$

This gives

$$(N_{S_1/S_0} S_1^{\cdot})(\text{nr}_{\Lambda_0/S_0} \Lambda_0^{\cdot}) \supseteq (1 + \mathfrak{P}_0)(\text{nr}_{\Lambda_0/S_0} \Lambda_0^{\cdot}) = S_0^{\cdot},$$

the last by virtue of (50.72). It follows that the map (50.70) is surjective, which completes the proof.

Our next step involves the wild ramification when  $G_1$  is assumed cyclic:

**(50.73) Proposition.** *Keeping the above notation, let  $G_1$  be a cyclic group of order  $q$ . Then*

$$\text{nr}_{\Lambda_1/S_1} \Lambda_1^{\cdot} = S_1^{\cdot}.$$

*Proof.* As in (50.71), there is a commutative diagram

$$\begin{array}{ccc} \Lambda_1^{\cdot} & \xrightarrow{\text{nr}_{\Lambda_1/S_1}} & S_1^{\cdot} \\ \downarrow & & \downarrow \\ \bar{\Lambda}_1^{\cdot} = (\Lambda_1/\mathfrak{P}\Lambda_1)^{\cdot} & \xrightarrow{\overline{\text{nr}}} & \bar{S}^{\cdot} \cong (S_1/\mathfrak{P}_1)^{\cdot}. \end{array}$$

Now  $q$  is a power of  $p$ , and viewing  $\bar{S}^{\cdot}$  as subgroup of  $\bar{\Lambda}_1^{\cdot}$  (which may require

a preliminary normalization of the factor set  $f$ ), we have  $\bar{\text{nr}} \alpha = \alpha^q$  for  $\alpha \in \bar{S}^\star$ . This shows that  $\bar{\text{nr}}$  is surjective, and therefore

$$\text{nr}_{\Lambda_1/S_1} \Lambda_1^\star \equiv S_1^\star (\text{mod } (1 + \mathfrak{P}_1))$$

(multiplicative congruence!). To complete the proof, we need only show that  $\text{nr} \Lambda_1^\star \supseteq 1 + \mathfrak{P}_1$ , where we write  $\text{nr}$  in place of  $\text{nr}_{\Lambda_1/S_1}$  for brevity.

Let  $G_1 = \langle \gamma : \gamma^q = 1 \rangle$ , and assume the factor set  $f$  chosen so that

$$u_{\gamma^i} = (u_\gamma)^i, \quad 0 \leq i \leq q-1; \quad (u_\gamma)^q = c \in S^\star,$$

where  $\gamma(c) = c$ , that is,  $c \in S_1^\star$ . Let  $\mathfrak{P} = \pi S$ ,  $\mathfrak{P}_1 = \pi_1 S_1$ ; since  $S/S_1$  is completely ramified, we may choose  $\pi_1 = N_{S/S_1} \pi$ . We now define filtrations of  $1 + \mathfrak{P}_1$  and  $\Lambda_1^\star$  by setting

$$W_i = 1 + \pi_1^i S_1, \quad X_i = 1 + \pi_1^i \Lambda_1, \quad i = 1, 2, \dots$$

Then

$$W_1 = 1 + \mathfrak{P}_1, \quad \text{and} \quad X_1 = 1 + \mathfrak{P}(S \circ G_1)_f \subseteq \Lambda_1^\star.$$

We intend to prove that  $\text{nr} X_1 \supseteq W_1$ , which will establish the proposition.

Given  $w \in W_1$ , we shall construct a sequence of elements  $x_1, x_2, \dots \in X_1$  such that for  $i \geq 1$ ,

$$(50.74) \quad \text{nr } x_i \equiv w \pmod{W_i} \quad \text{and} \quad x_{i+1} \equiv x_i \pmod{X_i}.$$

We shall then set  $x = \lim x_i \in X_1$ , and clearly  $\text{nr } x = w$ , as desired. To find the  $\{x_i\}$ , we choose  $x_1 = 1$ . Suppose now that  $i \geq 1$ , and that  $x_1, \dots, x_i$  have already been found satisfying (50.74). Let  $w_i = \text{nr } x_i$ , so  $w_i \equiv w \pmod{W_i}$ , and thus

$$w = w_i(1 + \pi_1^i cv) \quad \text{for some } v \in S_1,$$

where  $u_\gamma^q = c \in S_1^\star$  as above. Choose  $n \in \mathbb{Z}$  such that  $nq \equiv 1 \pmod{|S^\star|}$ , and set  $y_i = 1 + u_\gamma \pi^i v^n$ . By Exercise 50.11 we obtain

$$\text{nr } y_i = 1 - (-1)^q \pi_1^i cv^{nq} \equiv 1 + \pi_1^i cv \pmod{W_{i+1}}.$$

Choosing  $x_{i+1} = x_i y_i$ , we have

$$\text{nr } x_{i+1} = w_i \text{nr } y_i \equiv w \pmod{W_{i+1}},$$

which completes the proof.

Combining the two previous propositions, we show:

**(50.75) Corollary.** *Let  $\Lambda = (S \circ G)_f$ . Then  $\text{nr}_{\Lambda/R} \Lambda^\star = R^\star$  if  $G_1$  is cyclic.*

*Proof.* Let  $\Lambda_1 = (S \circ G_1)_f$ ; then by (50.66) and (50.73) we have

$$\text{nr}_{\Lambda/R} \Lambda^\cdot \supseteq N_{S_1/R}(\text{nr}_{\Lambda_1/S_1} \Lambda_1^\cdot) = N_{S_1/R} S_1^\cdot.$$

On the other hand,

$$R^\cdot = (N_{S_1/R} S_1^\cdot)(\text{nr}_{\Lambda/R} \Lambda^\cdot)$$

by (50.69). This shows that  $R^\cdot \subseteq \text{nr}_{\Lambda/R} \Lambda^\cdot$ , and therefore  $R^\cdot = \text{nr}_{\Lambda/R} \Lambda^\cdot$ , as desired.

In order to reduce the general case to that considered in Corollary 50.75, we use some facts from local class field theory which are available in most standard treatments of the subject (see, e.g., Cassels-Fröhlich [67], Serre [62], or Neukirch [69]).

**(50.76) Proposition.** *Let  $G = \text{Gal}(L/K)$ , where  $K, L$  are local fields. Then for each  $a \in R^\cdot$ , there exists a cyclic subgroup  $C \leq G$  such that  $a \in N_{S/R} \tilde{S}$ , where  $\tilde{S}$  is the subring of  $S$  fixed elementwise by  $C$ .*

*Proof.* Consider a tower of local fields  $K \subseteq F \subseteq L$ , with  $L/K$  a Galois extension. Set

$$G = \text{Gal}(L/K), \quad H = \text{Gal}(L/F), \quad G^{ab} = G/[G, G], \quad H^{ab} = H/[H, H].$$

Then there is a commutative diagram of abelian groups, with exact rows:

$$\begin{array}{ccccccc} 1 & \longrightarrow & N_{L/F} L^\cdot & \longrightarrow & F^\cdot & \xrightarrow{\alpha'} & H^{ab} \longrightarrow 1 \\ & & \downarrow & & N_{F/K} \downarrow & & \downarrow i_* \\ 1 & \longrightarrow & N_{L/K} L^\cdot & \longrightarrow & K^\cdot & \xrightarrow{\alpha} & G^{ab} \longrightarrow 1. \end{array}$$

Here,  $\alpha$  and  $\alpha'$  are the Artin homomorphisms, while  $i_*$  is induced by the inclusion  $i: H \rightarrow G$ . Since  $N_{L/K} L^\cdot = N_{F/K}(N_{L/F} L^\cdot)$ , an easy diagram-chase shows that for  $a \in K^\cdot$ ,

$$a \in N_{F/K} F^\cdot \Leftrightarrow \alpha(a) \in \text{im } i_*.$$

Now let  $a \in R^\cdot$ , and choose  $\sigma \in G$  so that  $\alpha(a)$  equals the image of  $\sigma$  in  $G^{ab}$ . We choose  $H = \langle \sigma \rangle \leq G$  in the above discussion, and  $F$  the subfield of  $L$  fixed by  $H$ , so  $H = \text{Gal}(L/F)$ . It follows that  $a = N_{F/K}(b)$  for some  $b \in F^\cdot$ . But then  $b$  lies in the valuation ring of  $F$ , since its norm is a unit of  $R$ . This completes the proof of the proposition.

We may now finish the proof of Wilson's Theorem 50.64. We are still treating the local case  $\Lambda = (S \circ G)_f$ , to which the proof has been reduced, and we need

to show that each  $a \in R^\circ$  lies in  $\text{nr}_{\Lambda/R}(\Lambda^\circ)$ . Choose  $C$  to be a cyclic subgroup of  $G$  as in (50.76), so that  $a \in N_{S/R}(\tilde{S}^\circ)$ , where  $\tilde{S}$  is the subring of  $S$  fixed by  $C$ . Let

$$\tilde{\Lambda} = (S^\circ C)_f,$$

a crossed-product order with center  $\tilde{S}$ . Then  $\text{nr}_{\tilde{\Lambda}/S}(\tilde{\Lambda}^\circ) = \tilde{S}^\circ$  by Corollary 50.75. However,

$$N_{S/R}(\text{nr}_{\tilde{\Lambda}/S}(\tilde{\Lambda}^\circ)) \subseteq \text{nr}_{\Lambda/R}\Lambda^\circ$$

by (50.66), so  $a \in \text{nr}_{\Lambda/R}(\Lambda^\circ)$  as required. This completes the proof of the theorem.

## §50. Exercises

1. Prove that  $D(ZG) = \text{Cl } ZG = 0$  for  $G$  an elementary abelian  $(2, 2)$ -group or a cyclic group of order 4.

[Hint: Use the fiber products

$$\begin{array}{ccc} ZG & \longrightarrow & ZH \\ \downarrow & & \downarrow \\ ZH & \longrightarrow & \bar{Z}H \end{array} \quad \text{and} \quad \begin{array}{ccc} ZG & \longrightarrow & Z[i] \\ \downarrow & & \downarrow \\ ZH & \longrightarrow & \bar{Z}H \end{array}$$

in the two cases, where  $|H| = 2$  and  $\bar{Z} = Z/2Z$ .]

2. Let  $f: A \rightarrow X$  and  $g: A \rightarrow Y$  be group homomorphisms, where  $X$  and  $Y$  are finite groups. Set

$$(f, g)A = \{(f(a), g(a)) \in X \times Y : a \in A\},$$

a subgroup of the direct product  $X \times Y$ . Prove that

$$|X \times Y : (f, g)A| = |X : f(A)| |Y : g(\ker f)|.$$

In particular, if  $f(A) = X$  and  $(f, g)A \trianglelefteq X \times Y$ , show that

$$\frac{X \times Y}{(f, g)A} \cong \frac{Y}{g(\ker f)}.$$

[Hint: The sequence

$$1 \rightarrow g(\ker f) \rightarrow (f, g)A \rightarrow f(A) \rightarrow 1$$

is exact.]

3. Let  $\Lambda \subseteq \Gamma$  be  $R$ -orders in a  $K$ -algebra  $A$ . Prove that

$$\Lambda \cap \Gamma^\circ = \Lambda^\circ.$$

[Hint: For  $x \in \Lambda \cap \Gamma^\circ$ , we have  $x^{-1} \in \Gamma$ , so  $x^{-1}$  is integral over  $R$ . Thus there is an equation

$$(x^{-1})^n + a_1(x^{-1})^{n-1} + \cdots + a_n = 0, \quad a_i \in R.$$

Multiplying by  $x^{n-1}$ , we deduce that  $x^{-1} \in R[x] \subseteq \Lambda$ , so  $x \in \Lambda^\circ$ .]

4. Keep the above notation, and assume that  $R$  has finite residue class fields. Show that  $\Gamma^\circ/\Lambda^\circ$  is finite.

[Hint: Choose  $a \in R$ ,  $a \neq 0$ , such that  $1 + a\Gamma \subseteq \Lambda \subseteq \Gamma$ , and set  $\bar{\Gamma} = \Gamma/a\Gamma$  (a finite ring). There is a homomorphism  $\Gamma^\circ \rightarrow \bar{\Gamma}^\circ$  whose kernel is  $(1 + a\Gamma) \cap \Gamma^\circ$ , which is  $(1 + a\Gamma)^\circ$  according to the preceding exercise. Hence  $\Gamma^\circ/(1 + a\Gamma)^\circ$  is embedded in the finite group  $\bar{\Gamma}^\circ$ , so  $(1 + a\Gamma)^\circ$  has finite index in  $\Gamma^\circ$ . The same then holds for  $\Lambda^\circ$ .]

5. Let  $D$  be an additive group with involution  $\tau$ , and suppose that  $2$  acts invertibly on  $D$ . Prove that (see p. 275)

$$D \cong D^+ \oplus D^-.$$

6. Let

$$0 \rightarrow A \xrightarrow{f} B \xrightarrow{g} C \rightarrow 0$$

be an exact sequence of additive groups with involution  $\tau$  which commutes with  $f$  and  $g$ . Assume that  $2$  acts invertibly on  $C$ . Prove that

$$0 \rightarrow A^- \rightarrow B^- \rightarrow C^- \rightarrow 0$$

is exact.

[Hint: Let  $c \in C^-$ , so  $\tau(c) = -c$ . Choose  $b \in B$  with  $g(b) = c/2$ . Then

$$g(b - \tau b) = c,$$

so  $g(B^-) = C^-$ .]

7. Let  $\Lambda = \mathbb{Z}G$ , where  $G$  is an abelian  $p$ -group,  $p$  odd. Prove that

$$\Lambda^\circ = (\Lambda^\circ)^+ \times G, \text{ where } (\Lambda^\circ)^+ = \{u \in \Lambda^\circ : \tau(u) = u\},$$

with  $\tau$  the canonical involution on  $\Lambda$  (see §50E).

[Hint (Fröhlich): Let  $\Gamma$  be the maximal order in  $QG$ . Then  $\Gamma^\circ = (\Gamma^\circ)^+ \times T$ , where  $T$  is the odd part of the torsion subgroup of  $\Gamma^\circ$ . For  $u \in \Lambda^\circ$ , write  $u = xy$  with  $x \in (\Gamma^\circ)^+$ ,  $y \in T$ . Then  $u^m = x^m$  for some odd  $m$ , so  $u^m \in (\Lambda^\circ)^+$ . Therefore  $(\Lambda^\circ)^+ \times G$  has odd index in  $\Lambda^\circ$ , and hence  $G = \Lambda^\circ \cap T$ . But for any  $x \in \Lambda^\circ$ ,  $x^2 = (x\tau(x))(x/\tau(x)) \in (\Lambda^\circ)^+ \times G$ . Hence  $\Lambda^\circ = (\Lambda^\circ)^+ \times G$ .]

8. Let  $R = \mathbb{Z}[\omega]$ ,  $K = \mathbb{Q}(\omega)$ , where  $\omega$  is a primitive  $p^m$ -th root of 1,  $m \geq 1$ , and  $p$  is prime. Let  $P = (1 - \omega)R$ , the unique prime ideal of  $R$  containing  $p$ . Show that

$$pR = P^{\varphi(p^m)} \quad \text{and} \quad \mathfrak{D}(R/\mathbb{Z}) = P^t, \quad \text{where } t = m\varphi(p^m) - p^{m-1}.$$

Here,  $\mathfrak{D}(R/\mathbb{Z})$  denotes the different of  $R$  relative to  $\mathbb{Z}$  (see §4B).

[Hint: The prime  $p$  ramifies completely in  $K$ , so  $pR = P^{\varphi(p^m)}$ . By §4B, the absolute norm of  $\mathfrak{D}(R/\mathbb{Z})$  is the discriminant of  $R$  relative to  $\mathbb{Z}$ . But  $N_{K/\mathbb{Q}}P = p$ , and therefore

$$\mathfrak{D}(R/\mathbb{Z}) = P^t, \text{ where } t \text{ is such that } d(R/\mathbb{Z}) = \pm p^t.$$

The discriminant  $d(R/\mathbb{Z})$  is well known (see CR (21.12), for example), and the exponent  $t$  is precisely  $m\varphi(p^m) - p^{m-1}$ .]

9. In the above, let  $p$  be odd, and set  $K_0 = \mathbb{Q}(\omega + \bar{\omega})$ ,  $R_0 = \text{alg. int. } \{K_0\}$ . Prove that

$$d(R/\mathbb{Z})/d(R_0/\mathbb{Z}) = p^{f(s)}\mathbb{Z}, \text{ where } f(s) = \frac{1}{2}\{sp^s - (s+1)p^{s-1} + 1\}.$$

[Hint: Put  $P_0 = P \cap R_0$ , so  $P_0R = P^2$  and  $P_0$  is tamely ramified in  $K/K_0$ . By Exercises 4.11–4.12, we obtain  $\mathfrak{D}(R/R_0) = PR$ . Therefore

$$\mathfrak{D}(R/\mathbb{Z}) = \mathfrak{D}(R/R_0)\mathfrak{D}(R_0/\mathbb{Z}) = P\mathfrak{D}(R_0/\mathbb{Z}).$$

Applying  $N_{K/\mathbb{Q}}$  to both sides, we have

$$d(R/\mathbb{Z}) = p\{d(R_0/\mathbb{Z})\}^2.$$

10. Prove that if  $S$  is tamely ramified over  $R$ , then the crossed-product order  $(S \circ G)_f$ , defined as in (50.63), is hereditary.

[Hint: Imitate the proof of (28.7) after normalizing the factor set so that  $u_1 = 1$ . The result is due to Williamson [63] and Harada [64].]

11. Let  $G = \text{Gal}(L/K)$  be a cyclic group of order  $n$ , with generator  $\sigma$ , and let  $A = (L \circ G)_f$  be a crossed-product algebra as in (50.63). Let  $f$  be the factor set arising from the relations

$$u_{\sigma^i} = u_{\sigma}^i, \quad 0 \leq i \leq n-1, \quad u_{\sigma}^n = r, r \in L.$$

Show that  $r \in K^\times$ , and that

$$\text{nr}_{A/K}(a + u_{\sigma}b) = N_{L/K}(a) - (-1)^n(N_{L/K}(b))r \quad \text{for } a, b \in L.$$

[Hint: Since  $u_{\sigma}$  commutes with  $r$ , it follows that  $r \in K^\times$ . Next, the map  $\varphi: A \rightarrow M_n(L)$  given in (50.65) carries  $a + u_{\sigma}b$  onto the  $n \times n$  matrix

$$\begin{bmatrix} a & b & 0 & \cdots & 0 & 0 \\ 0 & \sigma a & \sigma b & \cdots & 0 & 0 \\ 0 & 0 & \sigma^2 a & \cdots & 0 & 0 \\ & & & \cdots & & \\ & & & & \sigma^{n-2} a & \sigma^{n-2} b \\ r\sigma^{n-1} b & 0 & 0 & \cdots & 0 & \sigma^{n-1} a \end{bmatrix},$$

whose determinant is easily computed.]

12. Let  $K \leq H \trianglelefteq G$  be finite groups, with  $K \trianglelefteq G$ , and let  $\chi: H \rightarrow \mathbb{C}^*$  be a linear character trivial on  $K$ . Assume that  $\text{ind}_{H,K}^G \chi$  is an irreducible complex character of  $G$ , and let  $\varphi$  be the projection of  $CG$  onto the corresponding simple component. Prove that for the  $\mathbb{Z}$ -order  $\varphi(\mathbb{Z}G)$ , the kernel group  $D(\varphi(\mathbb{Z}G))$  is trivial.

[Hint (Wilson [77b]): Let  $\bar{G} = G/K$ ,  $\bar{H} = H/K$ . Then  $\varphi(\mathbb{Z}G)$  can be expressed as a crossed-product order  $(R \circ \bar{G})_f$ , where  $R = \mathbb{Z}[\eta]$  with  $\eta$  an  $|\bar{H}|$ -th root of 1, and where  $f$  is the image (under  $\chi$ ) of the factor set giving the extension  $1 \rightarrow \bar{H} \rightarrow \bar{G} \rightarrow G/H \rightarrow 1$ . Since  $\text{ind}_{H,K}^G \chi$  is irreducible, the Mackey criterion shows that  $\bar{G}$  acts faithfully on  $\bar{H}$ , and hence also on  $R$ . Now use Wilson's Theorem 50.64. See Wilson [77b] for further results of this nature.]

## §51. JACOBINSKI'S CANCELLATION THEOREM AND THE EICHLER CONDITION

Throughout this section, let  $\Lambda$  be an  $R$ -order in a f.d. separable  $K$ -algebra  $A$ , where  $R$  is a Dedekind domain whose quotient field  $K$  is a global field. We assume always that  $R \neq K$ , to avoid trivialities. A left  $\Lambda$ -lattice  $X$  is called *locally free* (of rank  $n$ ) if  $X_P \cong \Lambda_P^{(n)}$  as left  $\Lambda_P$ -modules, for each maximal ideal  $P$  of  $R$ . (The subscript  $P$  denotes  $P$ -adic completion.) If  $X, Y$  are locally free  $\Lambda$ -lattices of the same rank, we call  $X$  *stably isomorphic* to  $Y$  if

$$X \oplus \Lambda^{(k)} \cong Y \oplus \Lambda^{(k)} \quad \text{for some } k \geq 0.$$

We say that the order  $\Lambda$  has *locally free cancellation* if

$$(51.1) \quad X \text{ stably isomorphic to } Y \Leftrightarrow X \cong Y,$$

that is, we can “cancel” the summands  $\Lambda^{(k)}$ . In many applications, it is of the utmost importance to know whether  $\Lambda$  has locally free cancellation.

One of the main results of this section is the Jacobinski Cancellation Theorem 51.24, which guarantees that every  $R$ -order  $\Lambda$  in  $A$  has locally free cancellation, provided that  $A$  satisfies the Eichler condition<sup>†</sup> relative to  $R$ . Examples due to Eichler and Swan show that the Eichler condition is a *sufficient* condition for locally free cancellation, but is not a *necessary* condition.

By (49.3), each locally free  $\Lambda$ -lattice  $X$  of rank  $n$  can be written as

$$X \cong \Lambda^{(n-1)} \oplus X_0,$$

with  $X_0$  a locally free  $\Lambda$ -lattice of rank 1. Further, by §31B,  $X_0$  is isomorphic to a locally free left ideal of  $\Lambda$ . It follows at once that  $\Lambda$  has locally free cancellation if and only if (51.1) holds for locally free ideals  $X$  and  $Y$ .

By definition, the *locally free class group*  $\text{Cl}\Lambda$  is the finite abelian group whose elements are stable isomorphism classes  $[X]$  of locally free ideals  $X$  of

<sup>†</sup>See Definition 45.4, as well as §51A.

$\Lambda$  (that is, ideals in the *principal genus*  $g(\Lambda)$ ). Then  $\Lambda$  has locally free cancellation if and only if for  $X, Y \in g(\Lambda)$ ,

$$[X] = [Y] \Leftrightarrow X \cong Y.$$

The proof of Jacobinski's Theorem depends on a deep result concerning strong approximation for the kernel of the reduced norm map. This result was established by Eichler [38] when  $K$  is an algebraic number field, and by Swan [80] for  $K$  a (global) function field. The Eichler condition is a sufficient condition for the validity of this Eichler-Swan Theorem, which is proved in §51B.

### §51A. The Eichler Condition

In this subsection, we recall Definition 45.4 of the Eichler condition, and give examples where the condition holds true or fails. If  $K$  is an algebraic number field, the condition is the same as Eichler's original formulation, as generalized by Swan (see Swan-Evans [70] or MO(34.3)). On the other hand, if  $K$  is a (global) function field, the present version of the Eichler condition is a *weaker* restriction than that given in the above-cited references. As we shall see for  $K$  any global field, the Eichler condition defined below is a *sufficient* condition for the validity of the Eichler-Swan Theorem 51.13, concerning strong approximation for the kernel of the reduced norm.

Let  $P$  range over the primes of the global field  $K$ . Those primes  $P$  which come from maximal ideals of  $R$  are called " $R$ -primes" of  $K$ , while all others are "non- $R$  primes". If  $A$  is a central simple  $K$ -algebra, we say that  $A$  satisfies the *Eichler condition relative to  $R$* , and write  $A = \text{Eichler}/R$ , except when the  $P$ -adic completion  $A_P$  is a noncommutative skewfield for every non- $R$  prime  $P$  of  $K$ . Extending this definition to the case where  $A$  is a f.d. separable  $K$ -algebra with Wedderburn components  $\{A_i\}$ , we write

$$A = \text{Eichler}/R \Leftrightarrow A_i = \text{Eichler}/R_i \quad \text{for each } i,$$

where  $R_i$  is the integral closure of  $R$  in the center of  $A_i$ .

As observed in (45.5), if  $R = \text{alg. int. } \{K\}$  with  $K$  a number field, the only central simple  $K$ -algebras  $A$  which fail to be  $\text{Eichler}/R$  are the *totally definite quaternion algebras*. (By definition, these are algebras  $A$  such that every infinite prime  $P$  of  $K$  is a real prime, and such that  $A_P \cong \text{real quaternions}$  for every infinite prime  $P$  of  $K$ .)

**Examples.** (i) The algebra  $\mathbb{Q} \oplus \mathbb{Q}i \oplus \mathbb{Q}j \oplus \mathbb{Q}k$  of rational quaternions is a totally definite quaternion algebra.

(ii) More generally, let  $K$  be a totally real number field, so we may write  $K = \mathbb{Q}(\alpha)$ , where

$$\min. \text{pol.}_0(\alpha) = \prod_{i=1}^n (x - \alpha_i), \quad \text{with each } \alpha_i \in R.$$

Then  $K$  has  $n$  real primes  $P_1, \dots, P_n$ , and the isomorphism  $K_{P_t} \cong \mathbb{R}$  is given by  $\alpha \mapsto \alpha_t$ ,  $1 \leq t \leq n$ . Now set

$$A = K \oplus Ki \oplus Kj \oplus Kk, \quad \text{where } i^2 = c, \quad j^2 = d, \quad k = ij = -ji,$$

and where  $c, d$  are totally negative elements of  $K$  (that is,  $c < 0$  and  $d < 0$  in each  $K_{P_t}$ ,  $1 \leq t \leq n$ ). Then  $A$  is a totally definite quaternion algebra with center  $K$ .

Next, we list some cases where the Eichler condition obviously holds true:

**(51.2) Proposition.** *Let  $A$  be a f.d. separable  $K$ -algebra. Then  $A = \text{Eichler}/R$  in each of the following cases:*

- (i)  $A$  is commutative.
- (ii)  $A \cong M_n(D)$  where  $n > 1$  and  $D$  is a  $K$ -algebra.
- (iii)  $K$  is an algebraic number field with at least one complex prime.
- (iv)  $K$  is an algebraic number field, and  $A$  is a central simple  $K$ -algebra for which  $\dim_K A \neq 4$ .

Now consider the group algebra  $A = KG$  of a finite group  $G$  over an algebraic number field  $K$ , and let  $R = \text{alg. int. } \{K\}$ . Then  $A \neq \text{Eichler}/R$  if and only if  $A$  has a simple component  $B$  which is a totally definite quaternion algebra. Suppose this is the case, and let  $P$  be a real prime of the center of  $B$ . Then

$$B_P \cong \mathbb{H} = \text{skewfield of real quaternions},$$

and there is a homomorphism  $\varphi: G \rightarrow \mathbb{H}^\times$  given by composition of maps

$$G \rightarrow KG = A \rightarrow B \rightarrow B_P \cong \mathbb{H}.$$

Thus,  $G$  must have a homomorphic image  $\bar{G}$  in  $\mathbb{H}^\times$ , whose elements span  $\mathbb{H}$  over  $\mathbb{R}$ .

The finite subgroups of  $\mathbb{H}^\times$  are well known (see, e.g., Benson-Grove [71], Coxeter [40], or Vignéras [80, Ch. I, Th. 3.7]). To describe these subgroups, we use the notation  $\langle p, q, r \rangle$  to denote the group

$$\langle x, y, z, u: x^p = y^q = z^r = xyz = u, u^2 = 1 \rangle.$$

Then the finite subgroups of  $\mathbb{H}^\times$  are as follows:

- (1)  $C_n$  = cyclic group of order  $n \geq 1$ .
- (2)  $Q_n$  = generalized quaternion group of order  $4n = \langle 2, 2, n \rangle$ , where  $n \geq 1$ .
- (3)  $\tilde{T}$  = binary tetrahedral group of order  $24 = \langle 2, 3, 3 \rangle$ .
- (4)  $\tilde{O}$  = binary octahedral group of order  $48 = \langle 2, 3, 4 \rangle$ .
- (5)  $\tilde{I}$  = binary icosahedral group of order  $120 = \langle 2, 3, 5 \rangle$ .

Now  $C_n(n \geq 1)$  and  $Q_1$  are abelian groups, and thus cannot span  $H$  over  $R$ . Consequently we obtain:

**(51.3) Theorem.** *Let  $A = KG$ , where  $G$  is a finite group, and  $K$  is an algebraic number field with  $R = \text{alg. int. } \{K\}$ . Then  $A = \text{Eichler}/R$  if  $G$  has no homomorphic image of any of the following types:*

$$Q_n(n \geq 2), \tilde{T}, \tilde{O}, \tilde{I}.$$

In particular,  $A = \text{Eichler}/R$  if  $|G|$  is odd.

### §51B. The Eichler-Swan Theorem

The main result of this subsection is the Eichler-Swan Theorem, which states that when  $A = \text{Eichler}/R$ , then the Strong Approximation Theorem 51.13 holds true for the kernel of the reduced norm map. This result is due originally to Eichler [38] when  $K$  is an algebraic number field (see also Kneser [65]). For the case where  $K$  is a function field, the version given below is due to Swan [80], and represents a strengthening of his earlier results for this case.

The proof of the Eichler-Swan Theorem is somewhat complicated. Our treatment here is based on Swan's article [80], and is mostly self-contained, except for relying on some results concerning central simple algebras, proved in detail in MO.

For the convenience of the reader, we begin with a brief review of the topology on the adèle ring  $\hat{A}$  and the idèle group  $J(A)$ , where  $A$  is a  $K$ -algebra.

**Additive Structure.** Let  $K$  be a global field, and let  $P$  range over the maximal ideals of  $R$ . In our discussion, the archimedean primes of  $K$  will play a secondary role. For each  $P$ , the  $P$ -adic completion  $K_P$  is a complete metric space relative to the  $P$ -adic absolute value  $\varphi_P$  defined as in §4C. As basis for the neighborhoods of 0 in  $K_P$ , we may choose the open sets  $\{P^n R_P : n \geq 0\}$ . Then  $K_P$  is a locally compact topological space, and  $R_P$  is compact.

Now let  $V$  be any f.d.  $K$ -space, and let  $V_P = K_P \otimes_K V$  be its  $P$ -adic completion. Choose a  $K$ -basis  $\{v_i\}$  of  $V$ , which we view as  $K_P$ -basis for  $V_P$ . We may then define a metric on  $V_P$  by the formula

$$\|\sum_i a_i v_i\| = \max_i \{\varphi_P(a_i)\}, \quad \text{where } a_i \in K_P.$$

This makes  $V_P$  into a locally compact metric space, whose topology does not depend on the choice of  $K$ -basis of  $V$ . Let  $M$  be any full  $R$ -lattice in  $V$ ; the open sets  $\{P^n M_P : n \geq 0\}$  form a basis for the neighborhoods of 0 in  $V_P$ , and  $M_P$  is a compact subspace of  $V_P$ .

Let  $\hat{A}$  be the *adèle ring* of  $A$ , defined as in (42.5). Thus,

$$\hat{A} = \{(\alpha_P) \in \prod_p A_P : \alpha_P \in \Lambda_P \text{ a.e.}\},$$

where  $P$  ranges over all maximal ideals of  $R$ , and where  $\Lambda$  is any  $R$ -order in  $A$ . Note that  $\hat{A}$  is independent of the choice of  $\Lambda$ , since if  $\Gamma$  is another  $R$ -order in  $A$ , then  $\Lambda_P = \Gamma_P$  a.e. We now topologize  $\hat{A}$  by choosing, as basis for the neighborhoods of 0, all open sets  $U$  of the form

$$(51.4) \quad U = \prod_{P \in S} N_P(0) \times \prod_{P \notin S} \Lambda_P,$$

where  $S$  ranges over all finite sets of primes of  $R$ , and each  $N_P(0)$  ranges over all neighborhoods of 0 in  $A_P$ .

Each  $a \in A$  determines a principal adèle  $(a) \in \hat{A}$ , whose  $P$ -th component is  $a$  for each  $P$ . We shall identify  $A$  with the ring of principal adèles. It follows at once from the S.A.T. (4.8) that  $A$  is dense in  $\hat{A}$ , that is, given any  $x \in \hat{A}$  and any open set  $U$  as above, there exists a principal adèle  $a$  such that  $x - a \in U$ .

**Multiplicative Structure.** Let  $\hat{A}$  be the adèle ring of  $A$ , as above. It is easily seen that the group of units of the ring  $\hat{A}$  is precisely the *idèle group*  $J(A)$  of  $A$  relative to  $R$ , defined by

$$J(A) = \left\{ (\alpha_P) \in \prod_P A_P^\times : \alpha_P \in \Lambda_P^\times \text{ a.e.} \right\}.$$

This group depends on  $A$  and  $R$ , but not on  $\Lambda$ .

For each  $R$ -prime  $P$  of  $K$ , we topologize  $K_P^\times$  via the topology induced from the  $P$ -adic valuation on  $K_P$ . As basis for neighborhoods of an element  $x \in K_P^\times$ , we take the open sets  $\{(x + P^m R_P) \cap K_P^\times : m \geq 0\}$ . Thus for  $x, y \in K_P^\times$ ,  $y$  is near  $x$  if  $y - x \in P^m R_P$  for large  $m$ , or equivalently, if  $y \in x(1 + P^n R_P)$  for large  $n$ . Then  $K_P^\times$  is a locally compact topological group, and  $R_P^\times$  is a compact subgroup.

It is tempting to try topologizing  $J(A)$  by means of the adèle topology of  $\hat{A}$ . However,  $J(A)$  is *not* a topological group in this induced topology coming from  $\hat{A}$ , since the map  $\alpha \rightarrow \alpha^{-1}$ ,  $\alpha \in J(A)$ , is not continuous. For example, take the simplest case where  $R = \mathbb{Z}$  and  $A = \mathbb{Q}$ . For  $n \geq 1$ , let

$$\alpha_n = (1, \dots, 1, (p_n)^n, 1, \dots) \in J(A),$$

where  $p_n$  is the  $n$ -th rational prime. In the adèle topology,  $\lim_{n \rightarrow \infty} \alpha_n$  is the principal idèle 1. On the other hand,

$$\alpha_n^{-1} = (1, \dots, 1, (p_n)^{-n}, 1, \dots) \in J(A).$$

Given any neighborhood  $1 + U$ , with  $U$  as in (51.2), we have  $\alpha_n^{-1} \notin 1 + U$  for all sufficiently large  $n$ , and therefore  $\lim_{n \rightarrow \infty} \alpha_n^{-1} \neq 1$  in the topology on  $J(A)$  induced by the adèle topology on  $\hat{A}$ .

We therefore follow the standard procedure in algebraic number theory (see e.g. Cassels-Fröhlich [67] or Weiss [63]). To begin with, we topologize

$A_P^\circ$  by choosing, as basis for the neighborhoods of 1 in  $A_P^\circ$ , all open sets  $\{1 + P^n\Lambda_P : n \geq 1\}$ . Then  $A_P^\circ$  is locally compact, and  $\Lambda_P^\circ$  is compact. Now topologize the idèle group  $J(A)$  by choosing as basis for the open neighborhoods of  $1 \in J(A)$ , all open sets

$$(51.5) \quad W = \prod_{P \in S} N_P(1) \times \prod_{P \notin S} \Lambda_P^\circ,$$

with  $S$  ranging over all finite sets of  $R$ -primes  $P$  of  $K$ , and where each  $N_P(1)$  ranges over all open neighborhoods of 1 in  $A_P^\circ$ . Relative to this *idèle topology*,  $J(A)$  is a topological group, and the maps

$$\alpha \rightarrow \alpha^{-1}, \quad \alpha \in J(A), \quad \text{and} \quad (\alpha, \beta) \rightarrow \alpha\beta, \quad \alpha, \beta \in J(A),$$

are both continuous. Note that in the counterexample given above,  $\lim \alpha_n$  does not exist in the idèle topology.

We remark that the group  $A^\circ$  of principal idèles is *not* dense in  $J(A)$ , even in the simple case where  $R = \mathbb{Z}$  and  $A = \mathbb{Q}$ . For example, let  $x \in \mathbb{Z}_2$  ( $= 2$ -adic integers), and consider the idèle  $\alpha = (x, 1, 1, \dots) \in J(A)$ . Suppose we wish to choose  $a \in A^\circ$  close to  $\alpha$  in the idèle topology. Then  $ax$  is near 1 in  $\mathbb{Z}_2$ , while  $a \in \mathbb{Z}_p^\circ$  for  $p = 3, 5, 7, 11, \dots$ . This forces the equality  $a = \pm 2^m$  for some  $m \in \mathbb{Z}$ , and then we cannot make  $ax$  close to 1 in  $\mathbb{Z}_2$ .

**Reduced Norms.** Let  $A$  be a f.d. separable  $K$ -algebra with center  $C$ , and let

$$\mathfrak{O} = \text{integer closure of } R \text{ in } C.$$

The reduced norm map  $\text{nr}: A^\circ \rightarrow C^\circ$  extends to a map  $\text{nr}: J(A) \rightarrow J(C)$  of idèle groups, and this latter homomorphism is continuous (see, e.g., MO Exercise 33.2). We now define

$$(51.6) \quad J_0(A) = \{\alpha \in J(A) : \text{nr } \alpha = 1\}.$$

Thus, an idèle  $\alpha = (\alpha_P) \in J_0(A)$  if and only if  $\text{nr}_{A_P/C_P} \alpha_P = 1$  for each  $P$ . Then  $J_0(A)$  is a closed normal subgroup of  $J(A)$ , and acquires a topology induced from the idèle topology of  $J(A)$ . We now prove:

**(51.7) Lemma.** *The topology on  $J_0(A)$  induced from the idèle topology of  $J(A)$  agrees with that induced from the adèle topology of  $\hat{A}$ .*

*Proof.* Let  $\alpha_0 \in J_0(A)$ , and suppose  $\alpha \in J_0(A)$  is such that  $\alpha - \alpha_0$  is near 0 in  $\hat{A}$ . Then

$$\alpha^{-1}\alpha_0 - 1 = \alpha^{-1}(\alpha_0 - \alpha),$$

so once we show that the map  $\alpha \rightarrow \alpha^{-1}$ ,  $\alpha \in J_0(A)$ , is continuous in the adèle topology, it will follow that  $\alpha^{-1}\alpha_0$  is near 1 in  $J_0(A)$ , as desired.

In order to prove that the inverse map  $\alpha \rightarrow \alpha^{-1}$ ,  $\alpha \in J_0$  is continuous (in the adèle topology), we must show the following:

Given an element  $\alpha \in J_0(A)$  and a neighborhood  $U$  as in (51.4), there exists a neighborhood  $U'$  such that

$$(51.8) \quad \beta \in J_0(A) \cap (\alpha + U') \Rightarrow \beta^{-1} \in \alpha^{-1} + U.$$

Let  $\Lambda$  be an  $R$ -order in  $A$ . To begin with, we work with a single  $R$ -prime  $P$ . Let  $\xi \in A_P^\times$  be such that  $\text{nr } \xi = 1$ . Then

$$\text{red. char. pol.}_{A_P/K_P} \xi = X^n + a_1 X^{n-1} + \cdots + a_{n-1} X + (-1)^n \in K_P[X],$$

where  $n$  is independent of  $\xi$ . The coefficients  $\{a_i\}$  are continuous functions of  $\xi$  in the  $P$ -adic topology of  $A_P$  (see MO Exercise 33.2, for example). We may write

$$\xi^{-1} = (-1)^{n-1} \{ \xi^{n-1} + a_1 \xi^{n-2} + \cdots + a_{n-1} \} = f(\xi) \in K_P[\xi].$$

Then  $f(\xi)$  is a continuous function of  $\xi$  in the  $P$ -adic topology.

Keeping the above notation, suppose that  $\xi \in \Lambda_P$  and  $\text{nr } \xi = 1$ . Then the coefficients  $\{a_i\}$  lie in  $R_P$ , so  $\xi^{-1} \in R_P[\xi] \subseteq \Lambda_P$ , and therefore  $\xi \in \Lambda_P^\times$ .

Now let  $\alpha \in J_0(A)$  be given, as well as a neighborhood  $U$ . We may enlarge the finite set  $S$  used to define  $U$ , so as to include all  $R$ -primes  $P$  for which  $\alpha_P \notin \Lambda_P$ . We shall choose

$$U' = \prod_{P \in S} N'_P(0) \times \prod_{P \notin S} \Lambda_P,$$

with each  $N'_P(0)$  a neighborhood of 0 in  $A_P$ , to be determined later. For each  $\beta = (\beta_P) \in J_0(A) \cap (\alpha + U')$ , we then have  $\alpha_P, \beta_P \in \Lambda_P$  for  $P \notin S$ , and so  $\alpha_P^{-1}, \beta_P^{-1} \in \Lambda_P^\times$ , which implies that  $\beta_P^{-1} - \alpha_P^{-1} \in \Lambda_P$  for  $P \notin S$ .

On the other hand, for each of the finitely many primes  $P \in S$ , we may choose a neighborhood  $N'_P(0)$  in  $A_P$ , such that if  $\beta_P - \alpha_P \in N'_P(0)$ , then  $\beta_P^{-1} - \alpha_P^{-1} \in N_P(0)$ . Thus (51.8) holds for  $U'$  as above, which establishes the lemma.

Before starting the proof of the S.A.T. for the kernel of the reduced norm, let us record several facts from algebraic number theory, available in most standard texts on the subject. Let  $K$  be a global field as always. For each finite prime  $P$  of  $K$ , we normalize the  $P$ -adic absolute value  $\varphi_P$  by setting

$$\varphi_P(a) = (\text{card } R/P)^{-v_P(a)}, \quad a \in K^\times, \quad \text{and} \quad \varphi_P(0) = 0,$$

where  $v_P(a)$  is the smallest integer  $m$  such that  $a \in P^m R_P$ . For an infinite prime

$P$  of  $K$ , and  $a \in K$ , set

$$\varphi_P(a) = \begin{cases} |a_P| \in R, & P \text{ real}, \\ |a_P|^2 \in R, & P \text{ complex}. \end{cases}$$

These  $P$ -adic absolute values are related by:

**(51.9) Product Formula.** *For  $a \in K^\times$ ,  $\varphi_P(a) = 1$  a.e., and*

$$\prod_P \varphi_P(a) = 1,$$

where the product extends over all primes (finite and infinite) of  $K$ .

Next we quote without proof.

**(51.10) Very Strong Approximation Theorem (V.S.A.T.).** *Let  $P_1, \dots, P_n$  be distinct primes of  $K$  (finite or infinite), and let  $P_0$  be any other prime of  $K$ . Given elements  $\{a_i \in K_{P_i} : 1 \leq i \leq n\}$  and given any  $\varepsilon > 0$ , there exists an element  $a \in K$  such that*

$$\varphi_{P_i}(a - a_i) < \varepsilon \quad \text{for } 1 \leq i \leq n, \quad \text{and} \quad \varphi_P(a) \leq 1 \quad \text{for } P \neq P_0, P_1, \dots, P_n.$$

**(51.11) Corollary.** *Let  $R = \text{alg. int. } \{K\}$ , and let  $P_0$  be an infinite prime. Given an element  $a_i \in R_{P_i}$  for each finite prime among  $\{P_1, \dots, P_n\}$ , and given  $\varepsilon > 0$ , there exists an element  $a \in R$  for which*

$$\begin{aligned} \varphi_{P_i}(a - a_i) &< \varepsilon \quad \text{for } 1 \leq i \leq n, \quad \text{and} \quad \varphi_P(a) < 1 \quad \text{for each infinite prime} \\ &\cdot P \notin \{P_0, \dots, P_n\}. \end{aligned}$$

**Newton Polygons.** We shall need to use Newton polygons to compute the valuations of the roots of an algebraic equation over a complete local field  $F$ . Let  $F$  be a  $P$ -adic field with a non-archimedean exponential valuation  $v$ ; thus

$$v(a + b) \geq \text{Min}(v(a), v(b)) \quad \text{for } a, b \in F,$$

with equality whenever  $v(a) \neq v(b)$ . Given a polynomial

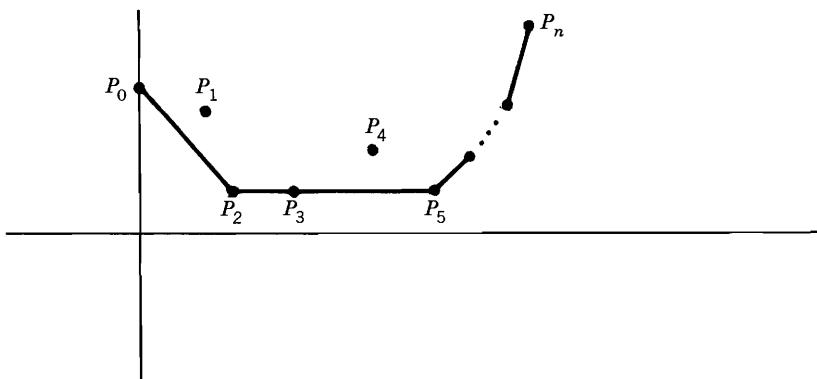
$$g(x) = a_0 x^n + a_1 x^{n-1} + \cdots + a_n \in F[x], \quad a_0 \neq 0,$$

not necessarily irreducible, we plot the points

$$P_0 = (0, v(a_0)), \quad P_1 = (1, v(a_1)), \dots, P_n = (n, v(a_n))$$

in Euclidean 2-space. The *Newton polygon* of  $g(x)$  is formed by connecting some

of these points so as to obtain a polygonal path which is concave upwards, and such that each  $P_i$  is either on or above this polygonal path. A picture helps:



**(51.12) Theorem.** Let  $\alpha_1, \dots, \alpha_n$  be the zeros of  $g(x)$  in some algebraic closure  $\tilde{F}$  of the  $P$ -adic field  $F$ , and let the valuation  $v$  be extended from  $F$  to  $\tilde{F}$ . Then the values  $\{v(\alpha_1), \dots, v(\alpha_n)\}$  coincide with the slopes of the sides of the Newton polygon of  $g(x)$ . Further, if  $P_iP_j$  is one of the sides, these are precisely  $j-i$   $\alpha$ 's for which  $v(\alpha) = \text{slope of } P_iP_j$ .

*Proof.* It is well known that  $v$  extends uniquely from  $F$  to  $\tilde{F}$  (see, e.g., MO(12.10) or Weiss [63]). Arrange the zeros  $\{\alpha_i\}$  so that

$$v(\alpha_1) = \dots = v(\alpha_m) < v(\alpha_{m+1}) = \dots = v(\alpha_l) < v(\alpha_{l+1}) \leq \dots \leq v(\alpha_n).$$

Taking  $a_0 = 1$  without loss of generality, so  $P_0 = (0, 0)$ , we may write

$$g(x) = (x - \alpha_1) \cdots (x - \alpha_m)(x - \alpha_{m+1}) \cdots (x - \alpha_n).$$

Expressing the coefficients  $\{a_i\}$  of  $g(x)$  as symmetric polynomials in the  $\alpha$ 's, it follows that

$$v(a_1) \geq v(\alpha_1), \quad v(a_2) \geq 2v(\alpha_1), \dots, v(a_m) = mv(\alpha_1),$$

$$v(a_{m+1}) \geq mv(\alpha_1) + v(\alpha_{m+1}) > (m+1)v(\alpha_1), \dots, v(a_n) = \sum_{i=1}^n v(\alpha_i).$$

It follows at once that  $P_0P_m$  is the first piece of the Newton polygon, and its slope is  $v(\alpha_1)$ . Now repeat the argument for  $h(x) = (x - \alpha_{m+1}) \cdots (x - \alpha_n)$ .

Having completed the preliminary work, we are now ready to state one of the major results of this section, due to Eichler when  $K$  is a number field, and to Swan when  $K$  is a function field.

**(51.13) Strong Approximation Theorem for the Kernel of the Reduced Norm (Eichler-Swan).** Let  $A$  be a f.d. separable  $K$ -algebra satisfying the Eichler condition relative to  $R$ , and let  $C$  denote the center of  $A$ . Write  $\text{nr}$  for the reduced norm map  $\text{nr}_{A/C}: A^\times \rightarrow C^\times$ , and also for the map on idèles  $J(A) \rightarrow J(C)$ . Set

$$u_0(A) = \{x \in A^\times : \text{nr } x = 1\}, \quad J_0(A) = \{\alpha \in J(A) : \text{nr } \alpha = 1\}.$$

Then  $u_0(A)$  is dense in  $J_0(A)$ , where we view  $u_0(A)$  as a group of principal idèles.

**Remarks.** (i) There is a more general formulation which involves archimedean primes as well (see Kneser [65]), but the formulation given above is adequate for our later applications.

(ii) It clearly suffices to establish the result when  $A$  is a central simple  $K$ -algebra.

Until further notice, we now assume that  $A$  is a central simple  $K$ -algebra, with  $K$  a global field as always in this section. For each prime  $P$  of  $K$ , we know that  $A_P$  is a central simple  $K_P$ -algebra, and we may write

$$A_P \cong M_{\kappa_P}(D_P), \quad \text{where } \dim_{K_P} D_P = m_P^2,$$

and  $D_P$  is a skewfield with center  $K_P$  and index  $m_P$ . We call  $\kappa_P$  the *local capacity* of  $A$  at  $P$ , and  $m_P$  the *local index*. By MO(25.7), we have  $m_P = 1$  a.e. Let us write

$$\dim_K A = n^2, \quad \text{so } n = m_P \kappa_P \quad \text{for each } P.$$

We wish to find elements of  $A$  with given reduced norm, and this will be accomplished by means of the following:

**(51.14) Lemma.** Let  $A$  be a central simple  $K$ -algebra of dimension  $n^2$ , and let

$$f(x) = x^n + a_1 x^{n-1} + \cdots + a_n \in K[x]$$

be a separable irreducible polynomial. Suppose that for each prime  $P$  of the global field  $K$ , the degree of each irreducible factor of  $f(x)$  in  $K_P[x]$  is a multiple of the local index  $m_P$ . Then there exists an element  $a \in A$  such that

$$\text{red. char. pol.}_{A/K} a = f(x).$$

For this element  $a \in A$ , we have

$$f(a) = 0 \quad \text{and} \quad \text{nr}_{A/K} a = (-1)^n a_n.$$

*Proof.* Let  $L$  be the field  $K(\alpha)$ , where  $f(\alpha) = 0$ . For each prime  $P$  of  $K$ , let  $P_1, \dots, P_r$  be the inequivalent valuations of  $L$  extending  $P$ . Then (see MO

§5C) we have

$$f(x) = \prod_{i=1}^r g_i(x) \quad \text{in } K_P[x],$$

a product of  $r$  distinct irreducible factors in  $K_P[x]$ . Furthermore,

$$L_{P_i} = K_P(\alpha_i), \quad \text{where } g_i(\alpha_i) = 0, \quad \text{for } 1 \leq i \leq r.$$

From the hypothesis of the lemma it follows that  $m_P$  divides  $\dim_{K_P} L_{P_i}$  for each  $P$  and each  $i$ . Therefore  $L$  is a splitting field for  $A$  over  $K$  locally at each prime of  $L$ , by MO(31.10). Hence by the Hasse-Brauer-Noether-Albert Theorem,  $L$  is a global splitting field:

$$L \otimes_K A \cong M_n(L).$$

(See MO(32.11) and (32.15).) But  $\dim_K L = n$ , and so  $L$  is embeddable in  $A$  as a maximal subfield (see MO(28.10)). Viewing  $\alpha$  as an element of  $A$ , we see at once that

$$\min. \text{ pol}_K \alpha = f(x) = \text{red. char. pol}_{A/K} \alpha,$$

by (7.34). The rest of the lemma is now clear.

In applying the above lemma, it will be necessary to start with a polynomial with constant term  $(-1)^n$ . As a preliminary step in choosing a suitable such polynomial, we prove:

**(51.15) Lemma.** *Let  $P_0$  be a non-R prime of  $K$ , either finite or infinite, and let  $\{P_1, \dots, P_k\}$  be any set of finite primes of  $K$  distinct from  $P_0$ . Given a polynomial*

$$f(x) = x^n + a_1 x^{n-1} + \cdots + a_{n-1} x + (-1)^n \in K_{P_0}[x],$$

*and given a positive integer  $m < n$  dividing  $n$ , subject to the restrictions that  $m = 1$  if  $K_{P_0} = C$ , and  $m = 1$  or  $2$  if  $K_{P_0} = R$ , then there exists an element  $d \in R$  such that*

- (i) *The degree of each irreducible factor of*

$$f(x) + dx^m$$

*in  $K_{P_0}[x]$  is a multiple of  $m$ , and*

- (ii)  *$v_{P_i}(d)$  is arbitrarily large for  $1 \leq i \leq k$ .*

*Proof.* Suppose first that  $P_0$  is archimedean. If  $m = 1$ , choose  $d = 0$ . If  $m = 2$ , then necessarily  $K_{P_0} = R$ ; in this case, choose  $d$  to be a large positive integer satisfying (ii), and such that  $f(x) + dx^m$  has no real zeros. Clearly (i) holds for this choice of  $d$ , and the result is now established for archimedean primes.

For the rest of the proof, assume  $P_0$  non-archimedean, and let  $v$  be its exponential valuation, normalized so that its value group is  $\mathbb{Z}$ . By hypothesis,  $P_0$  is a non- $R$  prime of  $K$ . If there is a non- $R$  prime  $P' \notin \{P_0, \dots, P_k\}$ , we can use the V.S.A.T. 51.10 to choose an element  $b \in R$  for which

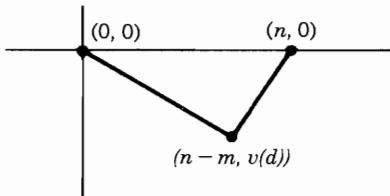
$$(51.16) \quad v(b) < 0, \quad \text{and} \quad v_{P_i}(b) > 0 \quad \text{for } 1 \leq i \leq k.$$

On the other hand, suppose each  $P \notin \{P_0, \dots, P_k\}$  is an  $R$ -prime of  $K$ . Again using (51.10), we can find  $b \in R$  such that  $v_{P_i}(b) > 0$  for  $1 \leq i \leq k$ . But then  $v(b) < 0$  by the Product Formula 51.9, so again we have an element  $b \in R$  satisfying (51.16).

Now choose  $r/s \in K$  with  $r, s \in R$ , such that  $v(r/s) = 1$ . Put  $c = rs^{m-1} \in R$ , so now  $v(c) = 1 + mv(s)$ , which is relatively prime to  $m$ . Finally, we choose  $d = cb^{qm}$ , with  $q$  a large positive integer to be specified later. Then

$$v(d) = v(c) + qmv(b) \equiv 1 \pmod{m}.$$

For  $1 \leq i \leq k$ , we can make  $v_{P_i}(d)$  as large as desired by choosing  $q$  sufficiently large. Further, since  $v(b) < 0$ , we can choose  $q$  so large that the Newton polygon of  $f(x) + dx^m$  over  $K_{P_0}$  takes the form shown:



The sides have slopes

$$v(d)/(n - m) \quad \text{and} \quad -v(d)/m.$$

When these fractions are reduced to lowest terms, the new denominators will be divisible by  $m$ . (In fact, the second fraction is already in lowest terms.)

It remains for us to verify (i) in this case. Let  $h(x)$  be an irreducible factor of  $f(x) + dx^m$  in  $K_{P_0}[x]$  of degree  $l$ ; we must show that  $m|l$ . Set  $L = K_{P_0}(\alpha)$ , where  $h(\alpha) = 0$ . Then  $\dim_{K_{P_0}} L = l$ , and  $v(\alpha)$  is one of the two slopes listed above. If  $e = e(L/K_{P_0})$  is the ramification index of  $v$  in the extension  $L/K_{P_0}$ , then  $v(\alpha) = a/e$  for some  $a \in \mathbb{Z}$ . It follows that  $m|e$ . But  $e|l$  by (4.10), since  $v$  extends uniquely from  $K_{P_0}$  to  $L$ . Together, these show that  $m|l$ , which completes the proof of the lemma.

We come now to the first place in the proof of the S.A.T. 51.13 where the Eichler condition appears. Let  $A$  be a central simple  $K$ -algebra of dimension  $n^2$ , satisfying Eichler/ $R$ . Then there exists a non- $R$  prime  $P_0$  of  $K$  for which  $A_{P_0}$  is not a noncommutative skewfield. This means that

$$\text{either } m_{P_0} = n = 1, \quad \text{or else } 1 \leq m_{P_0} < n,$$

where  $m_{P_0}$  is the local index of  $A$  at  $P_0$ . Using this fact, we are ready to prove one of the key lemmas needed for (51.13):

**(51.17) Proposition.** *Let  $\Lambda$  be an  $R$ -order in a central simple  $K$ -algebra  $A$  of dimension  $n^2$ , and assume  $A = \text{Eichler}/R$ . Then there exists a nonzero ideal  $r$  of  $R$  with the following property:*

*For each*

$$f(x) = x^n + a_1 x^{n-1} + \cdots + (-1)^n \in R[x],$$

*and for each pair of nonzero ideals  $a, b$  of  $R$  with  $b + ra = R$ , there exists an element  $\xi \in \Lambda^\times$  such that*

$$(51.18) \quad nr_{A/K}\xi = 1, \quad f(\xi) \equiv 0 \pmod{b\Lambda}, \quad \text{and} \quad \xi \equiv 1 \pmod{a\Lambda}.$$

*Proof.* Step 1. We begin by specifying the ideal  $r$ . For each maximal  $R$ -order  $\Gamma$  in  $A$  and each  $y \in A^\times$ , the conjugate  $y\Gamma y^{-1}$  is again a maximal order in  $A$ . We show that there are only a finite number of conjugacy classes of maximal orders in  $A$ . Let  $\Gamma'$  be any maximal order in  $A$ ; then

$$\Gamma' = (\Gamma'\Gamma) \cdot \Gamma \cdot (\Gamma'\Gamma)^{-1}$$

by MO(22.21). But the number of isomorphism classes of right  $\Gamma$ -ideals in  $A$  is finite, by the Jordan-Zassenhaus Theorem; let  $\{L_i : 1 \leq i \leq g\}$  be a full set of representatives of these isomorphism classes. Then we may write  $\Gamma'\Gamma = zL_i$  for some  $z \in A^\times$  and some  $i$ , and consequently

$$\Gamma' = zL_i\Gamma L_i^{-1}z^{-1}.$$

Thus, there are at most  $g$  conjugacy classes of maximal  $R$ -orders in  $A$ ; let  $\Gamma_1, \dots, \Gamma_h$  represent these classes, and choose a nonzero element  $r \in R$  such that  $r\Gamma_i \subseteq \Lambda$  for each  $i$ . Finally, choose the ideal  $r$  of  $R$  so that  $r$  is divisible by every prime ideal factor of  $rR$ , and also by each  $R$ -prime  $P$  for which  $m_P > 1$  (remember that  $m_P = 1$  a.e.).

Step 2. The proposition is trivially true for  $n = 1$  (just choose  $\xi = 1$ ), so let  $n > 1$  hereafter. Since  $A = \text{Eichler}/R$ , there exists a non- $R$  prime  $P_0$  of  $K$  for which  $1 \leq m_{P_0} < n$ . Choose  $P_0$  to be archimedean if possible (this can only happen when  $K$  is a number field). Further, when  $P_0$  is chosen archimedean, assume  $m_{P_0}$  is as large as possible, subject always to the condition that  $m_{P_0}$  is a proper divisor of  $n$ .

We now define

$$S_2 = \{P : P = \text{finite non-}R \text{ prime}, P \neq P_0, m_p > 1\} \cup \{P : P = R\text{-prime}, P | ra\}.$$

Without loss of generality, we may assume  $S_2 \neq \emptyset$ . For each  $P \in S_2$ , we choose

a separable irreducible polynomial

$$g^P(x) = x^n + \cdots + (-1)^n \in R_P[x],$$

such that  $g^P(x)$  is near  $(x - 1)^n$  coefficientwise in the  $P$ -adic topology. It is not hard to prove that such a choice is always possible; see, e.g., MO, bottom of page 299.

*Step 3.* We treat first the case  $n > 2$ . We are given a polynomial  $f(x) = x^n + \cdots + (-1)^n \in R[x]$ , and a pair of ideals  $a, b$  of  $R$ . Since  $P_0$  is a non- $R$  prime, it follows from the V.S.A.T. 51.10 that we can find a polynomial

$$g(x) = x^n + \cdots + (-1)^n \in R[x]$$

such that (coefficientwise)

$$\begin{cases} g(x) \text{ is near } g^P(x) \text{ for each } P \in S_2, \text{ and} \\ g(x) \text{ is near } f(x) \text{ at each } R\text{-prime dividing } b. \end{cases}$$

Note that since  $b + ra = R$  by hypothesis, no  $R$ -prime divisor of  $b$  lies in the set  $S_2$ .

Since  $m_{P_0}$  is a proper divisor of  $n$ , we can apply Lemma 51.15 with  $m = m_{P_0}$  to find an element  $d \in R$  such that

$$h(x) = g(x) + dx^m$$

satisfies the conditions:

- (i) The degree of each irreducible factor of  $h(x)$  in  $K_{P_0}[x]$  is a multiple of  $m$ , and
- (ii)  $h(x)$  is coefficientwise close to  $g(x)$  at each  $P \in S_2$  and also at each  $R$ -prime dividing  $b$ .

We intend to apply Lemma 51.14 to the polynomial  $h(x) \in R[x]$  constructed above, and begin by checking that  $h(x)$  satisfies the hypotheses of that lemma. First of all,  $h(x)$  is near  $g^P(x)$  at each  $P \in S_2$ ; since  $g^P(x)$  is separable and irreducible over  $K_P$ , so is  $h(x)$  (see MO(33.8)). In particular,  $h(x)$  must be separable irreducible over  $K$ . It remains to verify

(\*) *For every prime  $P$  of  $K$ , the degree of each irreducible factor of  $h(x)$  over  $K_P$  is divisible by  $m_P$ .*

This surely holds whenever  $m_P = 1$ . Next,  $S_2$  contains every finite prime  $P$  (except possibly  $P_0$ ) for which  $m_P > 1$ ; for each such  $P$ ,  $h(x)$  is irreducible over  $K_P$ , so (\*) is valid. Further, (\*) holds at  $P_0$  itself, by (51.15).

We must still check (\*) at the infinite primes of  $K$ , if there are any. If  $m_P = 1$

for each infinite prime  $P$ ,  $(*)$  is trivially true. If  $m_P = 2$  for some real prime  $P$  of  $K$ , then by the choice of  $P_0$  we must have  $m_{P_0} = 2$ , so  $m = 2$  in the above discussion. The first part of the proof of (51.15) then shows that the element  $d$  occurring there may be chosen so that  $h(x)$  has no linear factors in  $K_P[x]$  for each real prime  $P$ . After modifying our originally chosen  $d$  in this way, condition  $(*)$  now holds for every prime of  $K$ .

We may thus apply Lemma 51.14 to  $h(x)$ , and conclude that  $A$  contains an element  $\xi$  for which

$$h(\xi) = 0 \quad \text{and} \quad \text{nr } \xi = 1,$$

where  $\text{nr}$  means  $\text{nr}_{A/K}$ . It remains for us to check that the congruences in (51.18) hold true. Since  $a + b = R$ , we have  $a + b = 1$  for some  $a \in a$ ,  $b \in b$ , and therefore  $Ra + b = R$ . It therefore suffices to prove the proposition for the case where  $a = Ra$  is principal.

Each  $R$ -prime  $P$  dividing  $ra$  also divides  $ra$ , and so  $P \in S_2$  (here,  $r$  is as in Step 1). At each such  $P$ ,  $h(x)$  is near  $g(x)$ , and  $g(x)$  is near  $(x - 1)^n$ , so we may write

$$h(x) = (x - 1)^n + (ra)^n \bar{h}(x) \quad \text{for some } \bar{h}(x) \in R[x], \quad \deg \bar{h}(x) < n.$$

Now set  $\xi = 1 + ra\xi'$  with  $\xi' \in A$ . Since  $h(\xi) = 0$ , we have

$$(\xi')^n + \bar{h}(1 + ra\xi') = 0.$$

This shows that  $\xi'$  is integral over  $R$ , so by (26.9) it follows that  $\xi'$  lies in some maximal  $R$ -order in  $A$ . Replacing  $\xi$  and  $\xi'$  by  $y\xi y^{-1}$  and  $y\xi' y^{-1}$ , respectively, with  $y \in A^\times$ , we may now assume that  $\xi' \in \Gamma_i$  for one of the maximal orders  $\Gamma_i$  defined in Step 1. Then  $r\xi' \in \Lambda$  from the choice of  $r$ , and consequently  $\xi \equiv 1 \pmod{a\Lambda}$ . Further, this congruence implies that  $\xi \in \Lambda$ , and then necessarily  $\xi \in \Lambda^\times$  because  $\text{nr } \xi = 1$ .

Finally,  $h(x)$  is near  $f(x)$  at each  $R$ -prime dividing  $b$ . Since  $h(\xi) = 0$ , it follows that  $f(\xi) \equiv 0 \pmod{b\Lambda}$ . This shows that (51.18) holds, and completes the proof for the case  $n > 2$ .

*Step 4.* We finally consider the case where  $n = 2$ , so now  $P_0$  is a non- $R$  prime for which  $m_{P_0} = 1$ . In addition to the set  $S_2$  of finite primes defined in Step 2, we also introduce the set

$$S_1 = \{P: P = \text{real prime}, P \neq P_0, m_P = 2\},$$

which may possibly be empty. As in Step 2, for each  $P \in S_2$  we again choose a separable irreducible polynomial

$$g^P(x) = x^2 + a^{(P)}x + 1 \in R_P[x],$$

with  $a^{(P)}$  close to  $-2$  in the  $P$ -adic topology. Furthermore, for each  $P \in S_1$  (if

any), choose  $g^P(x)$  as above, where now  $a^{(P)} = 2 - \varepsilon$  for some small positive number  $\varepsilon$ . Since  $P_0 \notin S_1 \cup S_2$  and  $P_0$  is a non- $R$  prime, we can use the V.S.A.T. 51.10 to find a polynomial

$$g(x) = x^2 + cx + 1 \in R[x],$$

such that

$$\begin{cases} g(x) \text{ is near } g^P(x) \text{ for each } P \in S_1 \cup S_2, \text{ and} \\ g(x) \text{ is near } f(x) \text{ for each } R\text{-prime dividing } b. \end{cases}$$

It is easily checked that  $g(x)$  is irreducible (and separable) over  $K_P$  for each prime  $P$  of  $K$  for which  $m_P = 2$ . We can therefore apply Lemma 51.14 to the polynomial  $g(x)$  directly, obtaining an element  $\xi \in A$  for which  $g(\xi) = 0$  and  $\text{nr } \xi = 1$ . The rest of the argument is identical with that given in the latter half of Step 3. This completes the proof of the proposition.

Continuing with our proof of (51.13), let  $A$  be a central simple  $K$ -algebra. For each prime  $P$  of  $K$ , let

$$(51.19) \quad u_0(A_P) = \{x \in A_P : \text{nr}_{A_P/K_P} x = 1\}, \quad \text{and} \quad u_0(A) = \{x \in A : \text{nr}_{A/K} x = 1\}.$$

We wish to prove that  $u_0(A)$  is dense in  $J_0(A)$  (see (51.6)) whenever  $A = \text{Eichler}/R$ . As a preliminary step, independent of the Eichler condition, we prove:

**(51.20) Lemma.** *For any finite set  $S$  of primes of  $K$ ,  $u_0(A)$  is dense in  $\prod_{P \in S} u_0(A_P)$ .*

*Proof.* Let  $x = (x_P : P \in S)$ , with  $x_P \in u_0(A_P)$  for each  $P \in S$ , so  $\text{nr } x_P = 1$ . By (7.49) and the remarks following it, we know that  $x_P \in [A_P^\circ, A_P^\circ]$ . We may therefore write

$$x_P = \prod_{i=1}^m [b_{iP}, c_{iP}], \quad \text{with } b_{iP}, c_{iP} \in A_P^\circ, \quad \forall P \in S,$$

where we may assume  $m$  independent of  $P$ . For each  $i$ , choose elements  $b_i, c_i \in A$  close to  $b_{iP}, c_{iP}$  (respectively) at all  $P \in S$ . This can be done by virtue of the Weak Approximation Theorem in algebraic number theory (or else apply the V.S.A.T. 51.10). Since  $b_i$  is close to  $b_{iP}$ , and  $b_{iP} \in A_P^\circ$ , it follows that  $b_i \in A^\circ$  for each  $i$ ; likewise, each  $c_i \in A^\circ$ . Now set

$$y = \prod_{i=1}^m [b_i, c_i] \in u_0(A),$$

and clearly  $y$  is close to  $x$ . This completes the proof.

We are now ready to prove the S.A.T. 51.13 for the kernel  $J_0(A)$  of the reduced norm map on idèles. As we shall see, most of the difficulties have already

been overcome in our preliminary lemmas. For the proof, it suffices to restrict attention to the case where  $A$  is a central simple  $K$ -algebra of dimension  $n^2$ . We may assume that  $n > 1$ , since  $J_0(A) = 1$  when  $n = 1$ . Let  $\Lambda$  be an  $R$ -order in  $A$ .

*Step 1.* According to Lemma 51.7, as a basis for the neighborhoods of an element  $x \in J_0(A)$ , we may choose all open sets

$$x(J_0(A) \cap W), \quad \text{where } W = \prod_{P \in S} N_P(1) \times \prod_{P \notin S} \Lambda_P$$

(see (51.5)). Equivalently, we may choose all open sets

$$(x + U) \cap J_0(A), \quad \text{where } U = \prod_{P \in S} N_P(0) \times \prod_{P \notin S} \Lambda_P$$

(see (51.4)). Here,  $P$  ranges over maximal ideals of  $R$ , and  $S$  over all finite sets of such  $R$ -primes  $P$ . We shall continue using the notation given in (51.6) and (51.19).

We wish to prove that  $u_0(A)$  is dense in  $J_0(A)$  when  $A = \text{Eichler}/R$ . This means that for each finite set  $S$  of  $R$ -primes of  $K$ , and each choice of elements  $x_P \in u_0(A_P)$ ,  $P \in S$ , there exists an element  $a \in u_0(A)$  such that

$$a \text{ is near } x_P \text{ for each } P \in S, \quad \text{and} \quad a \in \Lambda_Q \text{ for each } R\text{-prime } Q \notin S.$$

*Step 2.* Assume hereafter that  $A$  satisfies the Eichler condition relative to  $R$ , and that  $A$  is a central simple  $K$ -algebra of dimension  $n^2$ , where  $n > 1$ . Let  $H$  denote the closure of  $u_0(A)$  in  $J_0(A)$ . For each  $R$ -prime  $P$ , we may view  $u_0(A_P)$  as a subgroup of  $J_0(A)$ , by identifying  $u_0(A_P)$  with

$$1 \times \cdots \times 1 \times u_0(A_P) \times 1 \times \cdots.$$

Let  $r$  be the nonzero ideal of  $R$  defined in Proposition 51.17, and set

$$(51.21) \quad \tilde{S} = \{P : P = R\text{-prime of } K, P \nmid r, m_P = 1\}.$$

Then almost every  $R$ -prime belongs to  $\tilde{S}$ , since  $m_P = 1$  a.e. The aim of this step is to prove that  $u_0(A_P) \leq H$  for each  $P \in \tilde{S}$ , where  $H$  is the closure of  $u_0(A)$  in  $J_0(A)$ .

For this purpose, introduce the group

$$H^* = \{\alpha = (a_P) \in H : a_P = 1 \text{ a.e.}\} \leq H.$$

We claim that  $H^* \trianglelefteq J_0(A)$ . Given  $\alpha = (a_P) \in H^*$  and  $\beta = (b_P) \in J_0(A)$ , we must show that  $\beta\alpha\beta^{-1} \in H^*$ . The  $P$ -component of  $\beta\alpha\beta^{-1}$ , denoted by  $(\beta\alpha\beta^{-1})_P$ , equals 1 for almost all  $P$ , and thus we are reduced to proving that  $\beta\alpha\beta^{-1} \in H$ . Let  $S$  be the finite set of  $R$ -primes  $P$  for which  $a_P \neq 1$ . By (51.20) we may choose a sequence  $\{c_1, c_2, \dots\}$  of elements of  $u_0(A)$  such that  $\lim_{i \rightarrow \infty} c_i = b_P$  in  $A_P$  at each

$P \in S$ . Then

$$(c_i \alpha c_i^{-1})_P = (\beta \alpha \beta^{-1})_P = 1 \text{ for } P \notin S,$$

$$(c_i \alpha c_i^{-1})_P \text{ is near } (\beta \alpha \beta^{-1})_P \text{ for } P \in S.$$

Consequently we have

$$\lim_{i \rightarrow \infty} c_i \alpha c_i^{-1} = \beta \alpha \beta^{-1} \text{ in } J_0(A).$$

But  $c_i \alpha c_i^{-1} \in H^*$  for each  $i$ , and  $H$  is closed in  $J_0(A)$ , so it follows that  $\beta \alpha \beta^{-1} \in H$ , as desired. We have thus proved that  $H^* \trianglelefteq J_0(A)$ .

Now fix a prime  $P \in \tilde{S}$ , and let us show that  $u_0(A_P) \leq H^*$ . Since  $m_P = 1$ , we have  $A_P \cong M_n(K_P)$ , and  $\text{nr}_{A_P/K_P}$  is just the usual determinant map. Therefore  $u_0(A_P) = SL_n(K_P)$ , and

$$H^* \cap u_0(A_P) \trianglelefteq SL_n(K_P).$$

However, any *proper* normal subgroup of  $SL_n(K_P)$  must consist only of scalar matrices (see, e.g., Artin [57]). We shall show that this cannot occur when  $P \in \tilde{S}$ , so we may then conclude that  $u_0(A_P) \leq H^* \leq H$ , as desired.

Keeping  $P \in \tilde{S}$  fixed, choose a polynomial

$$f(x) = x^n + \cdots + (-1)^n \in R[x]$$

such that  $f(x)$  has no linear factors in  $R_P[x]$ . This is always possible since  $R/P$  is finite (and  $n > 1$ ); see MO, Exercise 34.1. We shall find an element  $\xi \in H \cap SL_n(K_P) = H^* \cap SL_n(K_P)$  such that  $f(\xi) = 0$ . Then  $\xi$  cannot be a scalar matrix since  $f(x)$  has no linear factors over  $K_P$ . This implies that  $H^* \cap SL_n(K_P)$  cannot consist entirely of scalar matrices, so the intersection coincides with  $SL_n(K_P)$ , and thus  $u_0(A_P) = SL_n(K_P) \leq H^*$ .

In order to find this element  $\xi$ , we make use of Proposition 51.17, whose proof required the Eichler condition. Let  $\{P_1, P_2, \dots\}$  be the set of all  $R$ -primes of  $K$  different from  $P$ . For each  $m \geq 1$ , let

$$\alpha_m = (P_1 P_2 \cdots P_m)^m.$$

(If there are only finitely many  $\{P_i\}$ , let  $\alpha_m$  be the  $m$ -th power of their product.) For each  $m \geq 1$  we have  $P^m + \alpha_m = R$ , so by (51.17) there exists an element  $\xi_m \in u_0(A) \cap \Lambda$  such that

$$f(\xi_m) \equiv 0 \pmod{P^m \Lambda}, \quad \text{and} \quad \xi_m \equiv 1 \pmod{\alpha_m \Lambda}.$$

Of course each  $\xi_m \in \Lambda^\circ$ , by the proof of (51.7). Therefore  $\lim_{m \rightarrow \infty} \xi_m = 1$  in  $\Lambda_Q$  for each  $R$ -prime  $Q \neq P$ . On the other hand, we may view each  $\xi_m$  as an element of the compact group  $\Lambda_P^\circ$ , and we can then find a subsequence  $\{\xi_{m'}\}$  such that

$\lim \xi_{m'}$  exists in  $\Lambda_P^*$ . Now let  $\xi = \lim \xi_{m'} \in H$ ; then  $\xi_Q = 1$  for  $Q \neq P$ , while  $\xi_P \in u_0(A_P)$ . Since  $f(\xi_P) = 0$  in  $A_P$ , we now have an element  $\xi = \xi_P \in H \cap SL_n(K_P)$  for which  $f(\xi) = 0$ , as desired. This completes the proof that  $u_0(A_P) \leq H$  for all  $P \in \tilde{S}$ .

*Step 3.* We have defined  $H$  as the closure of  $u_0(A)$  in  $J_0(A)$ , and are trying to prove that  $H = J_0(A)$ . We shall use the fact that the set  $\tilde{S}$ , defined above, contains all but a finite number of  $R$ -primes of  $K$ . Consider first an element  $\alpha \in J_0(A)$  of the form

$$\alpha = 1 \times \cdots \times 1 \times \prod_{P \in \tilde{S}} a_P, \quad \text{with } a_P \in u_0(A_P) \text{ for } P \in \tilde{S}.$$

For each finite subset  $T$  of  $\tilde{S}$ , by Step 2 we can find an element  $h(T) \in H$  with

$$h(T)_Q = \begin{cases} a_Q, & Q \in T, \\ 1, & Q = R\text{-prime}, \quad Q \notin T. \end{cases}$$

Since  $\alpha = \lim_T h(T)$  and  $H$  is closed, we conclude that  $\alpha \in H$ , as desired.

Now let  $\beta = (b_P) \in J_0(A)$  be arbitrary. By (51.20), there exists a sequence  $\{c_1, c_2, \dots\}$  of elements of  $u_0(A) \leq H^*$ , with  $c_i$  approaching  $b_P$  at each of the finitely many  $R$ -primes  $P \notin \tilde{S}$ . Let  $\delta_i = (d_P)$ , where

$$d_Q = \begin{cases} 1, & Q \notin \tilde{S}, \\ c_i^{-1} b_Q, & Q \in \tilde{S}. \end{cases}$$

Then  $\beta = \lim_{i \rightarrow \infty} c_i \delta_i$ . But  $\delta_i \in H$  by the preceding discussion, and also each  $c_i \in H$ , so also  $\beta \in H$ . This proves that  $J_0(A) = H$ , and establishes Theorem 51.13.

We conclude this subsection with the first important application of the Eichler-Swan Theorem. We shall use it to prove Theorem 45.6, which plays a vital role in the calculation of  $K_1$  of a maximal order, and which we restate for convenience:

**(51.22) Theorem.** *Let  $\Lambda$  be a maximal  $R$ -order in a central simple  $K$ -algebra  $A$ , where  $K$  is a global field. Assume that  $A = \text{Eichler}/R$ . Then*

$$\text{nr}_{A/K} \Lambda^* = R^* \cap K^+,$$

where (as in (45.1))

$$K^+ = \{a \in K^* : a_P > 0 \text{ at each real prime } P \text{ of } K \text{ ramified in } A\}.$$

*Proof.* For each maximal ideal  $P$  of  $R$ ,  $A_P$  is a central simple  $K_P$ -algebra. We shall use the notation  $\text{nr}$  to indicate either  $\text{nr}_{A/K}$  or  $\text{nr}_{A_P/K_P}$ , depending on the context. The inclusion  $\text{nr} \Lambda^* \subseteq R^* \cap K^+$  is obvious from (26.2) and (7.48), and holds whether or not  $A = \text{Eichler}/R$ .

Now assume that  $A = \text{Eichler}/R$ , and let  $a \in R^\circ \cap K^+$ ; we must prove that  $a \in \text{nr } \Lambda^\circ$ . By (7.48) we have  $a = \text{nr } x$  for some  $x \in A^\circ$ . On the other hand, for each  $P$  we may view  $a$  as an element of  $R_P^\circ$ , and then by (45.8),  $a = \text{nr } y_P$  for some  $y_P \in \Lambda_P^\circ$ . Therefore the idèle  $\beta = (y_P)x^{-1}$  lies in  $J_0(A)$ , that is,  $\text{nr } \beta = 1$ .

Let  $S$  be some finite set of primes of  $R$ , chosen so that

$$y_P x^{-1} \in \Lambda_P^\circ \quad \text{for all } P \notin S.$$

By (51.13) we may choose  $z \in u_0(A)$  such that

$$z \text{ is near } y_P x^{-1} \text{ for } P \in S, \quad \text{and} \quad z \in \Lambda_P^\circ \text{ for } P \notin S.$$

Then

$$\text{nr } zx = (\text{nr } z)(\text{nr } x) = a,$$

and we need only show that  $zx \in \Lambda^\circ$ , or equivalently, that  $zx \in \Lambda_P^\circ$  for each  $R$ -prime  $P$ . For  $P \notin S$ , both  $z$  and  $x$  are in  $\Lambda_P^\circ$ , whence so is  $zx$ . On the other hand, for  $P \in S$  we know that  $zx$  is near  $y_P$  in  $A_P^\circ$ ; but  $y_P \in \Lambda_P^\circ$ , and  $\Lambda_P^\circ$  is an open subgroup of  $A_P^\circ$ , so it follows that  $zx \in \Lambda_P^\circ$ , as desired. This completes the proof of the theorem.

**(51.23) Corollary.** *Let  $\Lambda$  be a maximal  $R$ -order in a central simple  $K$ -algebra  $A$ , where  $K$  is a global field. Then for  $n \geq 2$ ,*

$$\text{nr } GL_n(\Lambda) = R^\circ \cap K^+,$$

whether  $A = \text{Eichler}/R$  or not.

*Proof.* For  $n > 1$ ,  $M_n(A) = \text{Eichler}/R$ . The result now follows from (51.22). (Compare the proof of (45.7).)

Swan [80, pages 188–189] gives an example in which  $A$  is a totally definite quaternion algebra over its center  $K = \mathbb{Q}(\sqrt{3})$ , so  $A \neq \text{Eichler}/R$ , where  $R = \text{alg. int. } \{K\}$ . He shows that Theorem 51.22 is *not* valid in this case, so the Eichler condition cannot be omitted, generally speaking. This example also gives an instance of a maximal order  $\Lambda$  for which

$$\text{nr } \Lambda^\circ < \text{nr } GL_2(\Lambda) = \text{nr } K_1(\Lambda).$$

### §51C. Locally Free Cancellation

Keeping the notation of the earlier subsections, let  $\Lambda$  be an  $R$ -order in a f.d. separable  $K$ -algebra  $A$ , where  $R$  is a Dedekind domain whose quotient field  $K$  is a global field,  $K \neq R$ . We shall apply the Eichler-Swan Theorem 51.13 to prove the important result:

**(51.24) Jacobinski Cancellation Theorem.** *If  $A$  satisfies the Eichler condition relative to  $R$ , then every  $R$ -order  $\Lambda$  in  $A$  has locally free cancellation.*

The theorem was first proved by Jacobinski [68b] for the case where  $K$  is a number field. We shall follow Fröhlich's [75] approach to the proof, for  $K$  any global field, and begin with some easy remarks which are independent of the Eichler condition.

**(51.25) Lemma.** *The  $R$ -order  $\Lambda$  has locally free cancellation if and only if*

$$J_0(A) \subseteq \alpha^{-1}U(\Lambda)\alpha \cdot A^\circ \quad \text{for all } \alpha \in J(A),$$

where

$$U(\Lambda) = \prod_p \Lambda_p^\circ = \text{group of unit idèles}, \quad A^\circ = \text{principal idèles}.$$

*Proof.* By (49.22), there is an isomorphism

$$\mathrm{Cl}\Lambda \cong J(A)/J_0(A)A^\circ U(\Lambda),$$

and the elements of the locally free class group  $\mathrm{Cl}\Lambda$  are stable isomorphism classes  $[\Lambda\alpha]$ ,  $\alpha \in J(A)$ . For  $\alpha, \beta \in J(A)$ , we saw in (49.6) that

$$\Lambda\alpha \cong \Lambda\beta \Leftrightarrow \beta \in U(\Lambda)\alpha A^\circ.$$

From the discussion at the beginning of §51, we show that  $\Lambda$  has locally free cancellation if and only if for  $\alpha, \beta \in J(A)$ ,  $[\Lambda\alpha] = [\Lambda\beta]$  implies  $\Lambda\alpha \cong \Lambda\beta$ . Thus,  $\Lambda$  has locally free cancellation if and only if for every  $\alpha \in J(A)$ ,

$$\beta \in J_0(A)A^\circ U(\Lambda)\alpha \Rightarrow \beta \in U(\Lambda)\alpha A^\circ,$$

or equivalently,

$$J_0(A)A^\circ U(\Lambda)\alpha \subseteq U(\Lambda)\alpha A^\circ.$$

Since  $J_0(A)$  contains the commutator subgroup of  $J(A)$ , the factors on the left-hand side can be arranged in any order, so the above condition can be rewritten as

$$U(\Lambda)\alpha J_0(A)A^\circ \subseteq U(\Lambda)\alpha A^\circ,$$

or equivalently,

$$\alpha J_0(A) \subseteq U(\Lambda)\alpha A^\circ, \quad \text{that is, } J_0(A) \subseteq \alpha^{-1}U(\Lambda)\alpha A^\circ.$$

This completes the proof of the lemma.

(51.26) **Corollary** (Fröhlich [75]). *Whether or not  $A = \text{Eichler}/R$ , we have:*

- (i) *Let  $\Lambda \subset \Gamma$  be  $R$ -orders in  $A$ . If  $\Lambda$  has locally free cancellation, then so does  $\Gamma$ .*
- (ii) *Let  $\Lambda, \Gamma$  be  $R$ -orders in f.d. separable  $K$ -algebras  $A, B$ , respectively. Let  $\varphi: A \rightarrow B$  be a surjection of  $K$ -algebras such that  $\varphi(\Lambda) \subseteq \Gamma$ . If  $\Lambda$  has locally free cancellation, then so does  $\Gamma$ .*

We are now ready to prove the Jacobinski Cancellation Theorem. Assume now that  $A = \text{Eichler}/R$ ; then  $u_0(A)$  is dense in  $J_0(A)$ , by the Eichler-Swan Theorem 51.13. For each  $\alpha \in J(A)$ ,  $\alpha^{-1}U(\Lambda)\alpha$  is an open subgroup of  $J(A)$ , by the discussion in §51B. It follows that

$$J_0(A) \subseteq \alpha^{-1}U(\Lambda)\alpha \cdot u_0(A) \subseteq \alpha^{-1}U(\Lambda)\alpha \cdot A^*$$

for each  $\alpha \in J(A)$ . Thus  $\Lambda$  has locally free cancellation by Lemma 51.25, and the proof is finished.

It is worthwhile to give some consequences of the Cancellation Theorem, and we begin with a definition:

(51.27) **Definition.** Let  $M$  be a left  $\Lambda$ -lattice, where  $\Lambda$  is an  $R$ -order in a f.d. separable  $K$ -algebra  $A$ . Put

$$\Gamma = \text{End}_\Lambda M, \quad \text{and} \quad B = \text{End}_A KM,$$

so  $\Gamma$  is an  $R$ -order in the f.d. separable  $K$ -algebra  $B$ . Call  $M$  an *Eichler lattice* if  $B = \text{Eichler}/R$ .

Generalizing (51.24), we prove:

(51.28) **Theorem (Jacobinski).** *Let  $M$  be an Eichler lattice over the  $R$ -order  $\Lambda$ , and let  $X$  be a left  $\Lambda$ -lattice such that  $X|M^{(k)}$  for some  $k$ . Then for any  $\Lambda$ -lattice  $L$ ,*

$$L \oplus X \cong M \oplus X \Leftrightarrow L \cong M.$$

*Proof.* If  $L \oplus X \cong M \oplus X$ , then  $L_P \oplus X_P \cong M_P \oplus X_P$  for each maximal ideal  $P$  of  $R$ . Therefore  $L_P \cong M_P$  by (6.15), which proves that  $L$  is necessarily in the genus of  $M$ . Increasing  $X$  if need be, we have

$$(51.29) \quad L \oplus M^{(k)} \cong M \oplus M^{(k)}$$

for some  $k$ . Furthermore,  $L|M^{(2)}$  by (31.7). Now use the Morita correspondence (6.3) between summands of  $\{M^{(n)}: n \geq 1\}$  and projective left  $\Gamma$ -modules, where  $\Gamma$  is as in (51.27). Let  $L$  correspond to the locally free left ideal  $W$  of  $\Gamma$ . The

$\Lambda$ -isomorphism (51.29) then yields an isomorphism of  $\Gamma$ -lattices

$$W \oplus \Gamma^{(k)} \cong \Gamma \oplus \Gamma^{(k)}.$$

Since  $B = K\Gamma = \text{Eichler}/R$  by hypothesis, we may apply (51.24) to conclude that  $W \cong \Gamma$ . Therefore  $L \cong M$ , as desired.

**(51.30) Corollary.** *Let  $N$  be a locally free left ideal of  $\Lambda$ , where  $\Lambda$  is an  $R$ -order in a f.d. separable  $K$ -algebra  $A$ . Then*

$$N \oplus \Lambda^{(k)} \cong \Lambda \oplus \Lambda^{(k)} \quad \text{for some } k \geq 1 \Rightarrow N \oplus \Lambda \cong \Lambda^{(2)},$$

whether or not  $A = \text{Eichler}/R$ .

*Proof.* We have

$$\text{End}_A K(N \oplus \Lambda) \cong \text{End}_A A^{(2)} \cong M_2(A^o),$$

and  $M_2(A^o) = \text{Eichler}/R$  by (51.2). Thus  $N \oplus \Lambda$  is an Eichler  $\Lambda$ -lattice. The hypotheses imply that

$$(N \oplus \Lambda) \oplus \Lambda^{(k-1)} \cong \Lambda^{(2)} \oplus \Lambda^{(k-1)},$$

and we may apply (51.28) since  $\Lambda^{(k-1)}|(N \oplus \Lambda)^{(k-1)}$ . This gives  $N \oplus \Lambda \cong \Lambda^{(2)}$ , as desired.

**(51.31) Remarks.** (i) The result is a special case of the Bass Cancellation Theorem 41.20.

(ii) Let  $L$  and  $M$  be  $\Lambda$ -lattices in the same genus. It may well happen, even when  $A = \text{Eichler}/R$ , that  $L \oplus X \cong M \oplus X$  for some  $\Lambda$ -lattice  $X$ , but  $L \not\cong M$ . For example, if  $M = \Lambda$  then from  $L \oplus X \cong \Lambda \oplus X$  for some  $X$  we can only conclude that  $[L]$  lies in the kernel group  $D(\Lambda)$  defined in §49B. Even when  $A$  is a commutative algebra, this kernel group need not be trivial.

We return next to the question, considered in (31.34), of finding a uniform upper bound on the number  $|g(M)|$  of isomorphism classes in the genus  $g(M)$  of a  $\Lambda$ -lattice  $M$ . (Caution: this notation differs from that of §31.) The approach here, due to Jacobinski [68b], gives an easily computed bound.

**(51.32) Theorem.** *Let  $\Lambda$  be an  $R$ -order in  $A$ . There exists a positive constant  $n_0 = n_0(\Lambda)$  such that*

$$|g(M)| \leq n_0 \text{ for every Eichler lattice } M.$$

*Proof.* We may assume that  $M$  is a faithful  $\Lambda$ -lattice, as in the proof of (31.32). Setting  $\Gamma = \text{End}_\Lambda M$ ,  $B = \text{End}_A KM$ , it follows that  $A$  and  $B$  have the same center

*C.* Let  $\mathfrak{O}$  be the integral closure of  $R$  in  $C$ . Choose a maximal order  $\Lambda'$  in  $A$ , and a nonzero  $r \in R$  with  $r\Lambda' \subseteq \Lambda \subseteq \Lambda'$ . Then  $\Gamma' = \text{End}_{\Lambda'} \Lambda' M$  is a maximal order in  $B$  containing  $\Gamma$  (see MO Exercise 21.1), where  $\Lambda' M$  is computed inside  $KM$ . It is easily checked that  $r\Gamma' \subseteq \Gamma$ .

Now  $\Gamma = \text{Eichler}/R$  by hypothesis, so (51.28) yields

$$|g(M)| = |g(\Gamma)| = |\text{Cl}\Gamma| = |\text{Cl}\Gamma'| |D(\Gamma)|.$$

The factor  $|\text{Cl}\Gamma'|$  is independent of the choice of  $M$ , by (49.32). Further, (49.40) gives

$$D(\Gamma) \cong \frac{\prod_{P \in S} \mathfrak{O}_P^\times}{\mathfrak{O}^+ \prod_{P \in S} \text{nr} \Gamma_P^\times},$$

where  $S$  consists of all maximal ideals  $P$  of  $R$  containing  $r$ . Since the set  $S$  is finite, it suffices to show that for each  $P \in S$ , there is a uniform upper bound on the index  $|\mathfrak{O}_P^\times : \text{nr} \Gamma_P^\times|$ . Note that  $\mathfrak{O}_P^\times = \text{nr}(\Gamma_P^\times)$ , and that  $S$  is independent of  $M$ .

Fixing  $P \in S$ , choose  $t > 0$  so that  $P^t \subseteq rR_P$ . Then we have

$$1 + P^t \Gamma_P^\times \subseteq \Gamma_P^\times \subseteq (\Gamma_P^\times)^*,$$

and therefore

$$|\mathfrak{O}_P^\times : \text{nr} \Gamma_P^\times| \leq |\mathfrak{O}_P^\times : \text{nr}(1 + P^t \Gamma_P^\times)|.$$

The maximal order  $\Lambda'_P$  can be expressed as

$$\Lambda'_P \cong \coprod_i M_{n_i}(\Delta_i),$$

with each  $\Delta_i$  a noncommutative d.v.r. (see (26.23)). Since  $\Gamma'_P = \text{End}_{\Lambda'_P}(\Lambda'_P M_P)$ , it follows readily that

$$\Gamma'_P \cong \coprod_i M_{m_i}(\Delta_i)$$

for some integers  $\{m_i\}$  which depend on  $\Lambda'_P M_P$  (and hence on  $M$ ). But then

$$\text{nr}(1 + P^t \Gamma'_P) = \text{nr}(1 + P^t \Lambda'_P),$$

and therefore

$$|\mathfrak{O}_P^\times : \text{nr}(1 + P^t \Gamma'_P)| = |\mathfrak{O}_P^\times : \text{nr}(1 + P^t \Lambda'_P)|,$$

with the right-hand side independent of  $M$ . This completes the proof.

Returning to the question of locally free cancellation, let  $G$  be a finite group. By Jacobinski's Cancellation Theorem,  $ZG$  has locally free cancellation unless  $G$  has a quotient  $Q_n (n \geq 2)$ ,  $\tilde{T}$ ,  $\tilde{O}$ , or  $\tilde{I}$  (see (51.3)). Even in these cases, however, it may happen that  $ZG$  has locally free cancellation. For example, Martinet [71] proved that  $ZQ_2$  has the cancellation property. This question was investigated thoroughly by Swan [83], who also calculated the number of isomorphism classes in each stable class for various cases. We state without proof some of his main results.

- (1) Let  $G$  be a binary polyhedral group. Then  $ZG$  has locally free cancellation if and only if  $G$  is one of the seven groups

$$Q_2, Q_3, Q_4, Q_5, \tilde{T}, \tilde{O}, \tilde{I}.$$

- (2) Cancellation fails for  $Q_2 \times C_2$ , where  $C_2$  is cyclic of order 2, but holds for  $Q_2 \times H$  if  $|H|$  is odd.
- (3) Let  $\Lambda'$  be a maximal order in  $QG$ , where  $G$  is a binary polyhedral group. Then  $\Lambda'$  has locally free cancellation if and only if  $G$  is one of the 11 groups

$$Q_2, Q_3, Q_4, Q_5, Q_6, Q_7, Q_9, Q_{15}, \tilde{T}, \tilde{O}, \tilde{I}.$$

(This result is a key step in proving (1).)

- (4) For  $G = Q_6$ , the generalized quaternion group of order 24, there are 16 isomorphism classes of locally free left ideals of  $ZG$ , and eight stable isomorphism classes. Of these stable classes, four of them consist of a single isomorphism class, and the other four have three isomorphism classes each.
- (5) The set of isomorphism classes of locally free left ideals in  $ZG$  has no natural group structure, generally speaking.

We conclude this section by stating without proof a number of results related to our previous theorems. As always,  $\Lambda$  denotes an  $R$ -order in a f.d. separable  $K$ -algebra  $A$ , where  $K$  is a global field.

**(51.33) Theorem (Jacobinski [68a]).** *Let  $M$  and  $N$  be  $\Lambda$ -lattices in the same genus. Then there is a finite extension  $K'$  of  $K$  such that*

$$R' \otimes_R M \cong R' \otimes_R N \quad \text{as } (R' \otimes_R \Lambda)\text{-lattices,}$$

where  $R'$  is the integral closure of  $R$  in  $K'$ .

Jacobinski also extended his Cancellation Theorem 51.24, giving necessary and sufficient conditions under which

$$M \oplus X \cong N \oplus X \Rightarrow M \cong N,$$

where  $M, N$ , and  $X$  are arbitrary  $\Lambda$ -lattices (and necessarily  $M, N$  lie in the same genus). His proof, and other related proofs in the literature, makes use of the following important generalization of Theorem 51.22:

**(51.34) Eichler's Theorem on Units.** *Let  $\Lambda$  be a maximal  $R$ -order in a central simple  $K$ -algebra  $A$ , where  $A = \text{Eichler}/R$ . Let  $\mathfrak{f}$  be a full two-sided ideal of  $\Lambda$ , and let  $x \in \Lambda$  be such that*

$$\text{nr}_{A/K}x \equiv a \pmod{\mathfrak{f} \cap R} \quad \text{for some } a \in R^\times \cap K^+.$$

*Then there exists a unit  $u \in \Lambda^\times$  such that*

$$x \equiv u \pmod{\mathfrak{f}}.$$

(For a proof, see Swan [80].)

## §51. Exercises

1. Show that the group  $J_0(A)$  defined in (51.6) is the closure of  $[J(A), J(A)]$ , whether or not  $A = \text{Eichler}/R$ . [Hint: Use (51.20).]

2. Let  $g(x) \in F[x]$  be irreducible, where  $F$  is a  $P$ -adic field. Show that the Newton polygon of  $g(x)$  consists of a single straight line segment.

3. Use Newton polygons to deduce Eisenstein's Irreducibility Criterion.

4. Let  $M$  and  $N$  be  $\Lambda$ -lattices in the same genus, where  $\Lambda$  is an  $R$ -order. Show that  $M^{(k)} \cong N^{(k)}$  for some positive integer  $k$ . Conversely, such an isomorphism implies that  $M, N$  are in the same genus. The result is due to Jacobinski [68b] and Roiter [66].

[Hint: Passing over to the order  $\Gamma = \text{End}_\Lambda M$ , it suffices to prove the result for locally free left  $\Gamma$ -modules. Now use (51.30) together with the finiteness of  $\text{Cl}(\Gamma)$ .]

5. Let  $M$  be a  $\Lambda$ -lattice. Show that there is only a finite number of isomorphism classes of indecomposable lattices  $X$  such that  $X \mid M^{(k)}$  for some  $k$ .

[Hint: It suffices to treat the case  $M = \Lambda$ . Now imitate the proof of Jones's Theorem 33.2.]

6. Let  $A$  be a central simple  $K$ -algebra,  $\dim_K A = n^2$ , and let  $\Lambda$  be a maximal  $R$ -order in  $A$ . Given a left ideal  $M$  of  $\Lambda$  of finite index, its reduced norm  $\text{nr } M$  is the ideal of  $R$  defined as follows: for each prime  $P$  of  $R$ , write  $M_P = \Lambda_P a_P$  with  $a_P \in \Lambda_P$ , and set

$$\text{nr } M_P = R_P \text{nr } a_P.$$

Then  $\text{nr } M$  is the unique ideal such that  $(\text{nr } M)_P = \text{nr } M_P$  for each  $P$ . Prove

(i)  $(\text{nr } M)^n = \text{ord}_R \Lambda / M$ , where  $\text{ord}_R$  is the  $R$ -order ideal defined as in §4D.

(ii) Let  $\alpha = (a_P) \in J(A)$ , with the  $\{a_P\}$  as above. Show that  $\text{nr } M$  is the ideal of  $R$  which corresponds to the idèle  $\text{nr } \alpha \in J(K)$  under the isomorphism  $J(K)/U(R) \cong \text{ideal group of } R$ .

- (iii) Using (49.17), show that if  $\text{nr } M = Rx$  for some  $x \in K^+$ , then  $[M] = 0$  in  $\text{Cl } \Lambda$ .
- (iv) If  $A = \text{Eichler}/R$ , deduce that if  $\text{nr } M = Rx$  with  $x \in K^+$ , then  $M$  is a principal ideal  $\Lambda m$  for some  $m \in A^+$ .

For further discussion of reduced norms of ideals, see MO §24, §34, and §35.

## §52. THE HOM DESCRIPTION OF THE CLASS GROUP

The idèle-theoretic formulas for the locally free class group  $\text{Cl } RG$  and the kernel group  $D(RG)$ , obtained in §49, are sometimes inconvenient for certain types of calculations arising from algebraic number theory. In these calculations, certain arithmetic invariants appear, associated with complex irreducible characters of  $G$ . Furthermore, the functorial properties of  $\text{Cl } RG$  and  $D(RG)$ , concerning their behavior under change of group or change of ground ring, can be described more readily in terms of the “Hom” version of  $\text{Cl } RG$  and  $D(RG)$ , which involves the ring  $\text{ch } G$  of virtual complex characters of  $G$ . This version was first introduced by Fröhlich [76], and then elaborated in a number of later articles. For a more detailed discussion of this topic, and especially for its applications to algebraic number theory, we refer the reader to the fundamental works of Fröhlich [83], [84]. In this section, we present the rudiments of the theory, which will suffice for our later applications.

Throughout this section,  $G$  denotes a finite group, and  $R$  a Dedekind domain whose quotient field  $K$  is an algebraic number field. As usual,  $\text{Irr } G$  denotes the set of irreducible complex characters of  $G$ , and  $\text{ch } G$  the ring of virtual characters of  $G$ , that is, the set of  $\mathbb{Z}$ -linear combinations of the characters  $\zeta \in \text{Irr } G$ . We begin with a brief review of some standard facts.

**Conjugate Characters.** Let  $E$  be a splitting field for  $G$  over  $K$ , chosen so that  $E$  is a finite Galois extension of  $K$ , with Galois group  $\Omega = \text{Gal}(E/K)$ . Let  $S$  be the integral closure of  $R$  in  $E$ . Since  $E$  is a splitting field for  $G$ , the group algebra  $EG$  is a direct sum of full matrix algebras over  $E$ , and every  $\zeta \in \text{Irr } G$  is afforded by an  $E$ -representation  $x \in G \rightarrow T(x) \in GL_n(E)$ . Let  $\omega \in \Omega$ ; applying  $\omega$  to the entries of  $T(x)$ , we obtain a *conjugate* representation  $T^\omega$  of  $G$ , affording a *conjugate character*  $\zeta^\omega$  of  $G$ . (See §7B.) Clearly,

$$(52.1) \quad \zeta^\omega(x) = (\zeta(x))^\omega, \quad x \in G, \quad \omega \in \Omega.$$

The Galois group  $\Omega$  acts on the set  $\text{Irr } G$ , and then  $\text{ch } G$  can be viewed as a right  $\Omega$ -module.

Keeping the above notation, let  $y \in KG$  and let  $\zeta \in \text{Irr } G$ . We define

$$\det_\zeta y = \det T(y), \quad y \in KG,$$

where  $T$  is a representation affording  $\zeta$ . (The notation here is slightly different from that used in §13B.) Note that  $\det_\zeta$  depends only on the character  $\zeta$ ,

and not on the choice of the representation  $T$  affording  $\zeta$ . Then

$$T(yz) = T(y)T(z) \quad \text{for } y, z \in KG,$$

and consequently

$$(52.2) \quad \det_\zeta(yz) = \det_\zeta(y) \cdot \det_\zeta(z) \quad \text{for } y, z \in KG.$$

Furthermore, from (52.1) we obtain

$$(52.3) \quad \det_{\zeta^\omega} y = (\det_\zeta y)^\omega \quad \text{for } y \in KG, \quad \omega \in \Omega, \quad \zeta \in \text{Irr } G.$$

It is clear that

$$\det_\zeta y \in E^* \quad \text{for } y \in (KG)^*.$$

Furthermore, for each maximal ideal  $P$  of  $S$ , the representation  $T$  may be chosen so that the matrices  $\{T(x) : x \in G\}$  have entries in  $S_P$  (see (16.14)). It follows that for  $y \in (RG)^*$  we have  $\det_\zeta y \in (S_P)^*$  for each  $P$ , and therefore

$$(52.4) \quad \det_\zeta y \in S^* \quad \text{for } y \in (RG)^*.$$

Finally, for  $\zeta, \eta \in \text{Irr } G$  we have

$$(52.5) \quad \det_{\zeta+\eta}(y) = \det_\zeta(y) \cdot \det_\eta(y) \quad \text{for } y \in (KG)^*.$$

It follows that  $\det_\zeta(y) \in E^*$  is well-defined for all virtual characters  $\zeta \in \text{ch } G$ , and all  $y \in (KG)^*$ .

**Schur Index.** The following results will be established in §74, and some of them have already been proved in §7B. First, there is a bijection between the set of orbits of  $\text{Irr } G$  under the action of  $\Omega$ , and the set of simple components of the group algebra  $KG$ . Given  $\zeta \in \text{Irr } G$ , let  $\{\zeta_1, \dots, \zeta_t\}$  be its distinct conjugates under the action of  $\Omega$ , where  $\zeta_1 = \zeta$ . Let  $B_\zeta$  be the simple component of  $KG$  corresponding to the orbit  $\{\zeta_1, \dots, \zeta_t\}$ . Then the center of  $B_\zeta$  is isomorphic to the field  $K(\zeta)$  obtained by adjoining to  $K$  all of the character values  $\{\zeta(x) : x \in G\}$ .

Furthermore,  $K(\zeta)$  is a Galois extension of  $K$ , and  $\dim_K K(\zeta)$  coincides with the number  $t$  of distinct conjugates of  $\zeta$ . The Galois group  $\text{Gal}(K(\zeta)/K)$  permutes the characters  $\{\zeta_1, \dots, \zeta_t\}$  transitively, and we have

$$K(\zeta) = \text{subfield of } E \text{ fixed by } \{\omega \in \Omega : \zeta^\omega = \zeta\}.$$

**The Det Homomorphism.** As above, let  $E$  be a splitting field for  $G$  over  $K$ , and let  $\Omega = \text{Gal}(E/K)$ . We have already seen that

$$\det_\zeta y \in E^* \quad \text{for } \zeta \in \text{ch } G \quad \text{and} \quad y \in (KG)^*.$$

The  $\text{Det}$  homomorphism assigns to each  $y \in (KG)^\circ$  the function

$$\xi \rightarrow \det_\xi y, \quad \xi \in \text{ch } G.$$

Denoting this function by  $\text{Det } y$ , we thus have (by definition)

$$(52.6) \quad (\text{Det } y)(\xi) = \det_\xi y \quad \text{for } y \in (KG)^\circ, \quad \xi \in \text{ch } G.$$

Let us view  $E^\circ$  and  $\text{ch } G$  as right  $\Omega$ -modules, and consider the set  $\text{Hom}_\Omega(\text{ch } G, E^\circ)$ . We make this into an abelian multiplicative group by defining

$$(fg)\xi = f(\xi)g(\xi) \quad \text{for } f, g \in \text{Hom}_\Omega, \quad \text{and} \quad \xi \in \text{ch } G.$$

It follows at once from (52.3) and (52.5) that  $\text{Det } y \in \text{Hom}_\Omega(\text{ch } G, E^\circ)$  for each  $y \in (KG)^\circ$ . Furthermore, the map  $y \rightarrow \text{Det } y$ ,  $y \in (KG)^\circ$ , is a homomorphism, since for  $\xi \in \text{ch } G$ ,  $y, z \in (KG)^\circ$ ,

$$(\text{Det } yz)(\xi) = \det_\xi(yz) = \det_\xi(y) \cdot \det_\xi(z) = (\text{Det } y)(\xi) \cdot (\text{Det } z)(\xi).$$

Thus we obtain a homomorphism

$$(52.7) \quad \text{Det}: (KG)^\circ \rightarrow \text{Hom}_\Omega(\text{ch } G, E^\circ),$$

carrying  $y \in (KG)^\circ$  onto  $\text{Det } y \in \text{Hom}_\Omega$ .

In the above discussion, we may replace  $K$  by some larger field on which  $\Omega$  is assumed to act trivially. For example, let  $P$  be a prime of  $K$ , and let  $K_P$  be the  $P$ -adic completion of  $K$ . Set

$$E_P = K_P \otimes_K E \cong \prod_{\mathfrak{P}} E_{\mathfrak{P}},$$

where  $\mathfrak{P}$  ranges over the primes of  $E$  above  $P$ , and  $E_{\mathfrak{P}}$  denotes the  $\mathfrak{P}$ -adic completion of  $E$ . Let  $\omega \in \Omega$  act as  $1 \otimes \omega$  on  $E_P$ . Let  $\xi \in \text{Irr } G$  be a character afforded by the  $E$ -representation  $T$  of  $G$  of degree  $n$ . Extending  $T$  linearly to a representation of  $K_P G$ , we obtain a ring homomorphism

$$K_P G \rightarrow M_n(K_P \otimes_K E) = M_n(E_P).$$

This yields a homomorphism of groups:

$$T: (K_P G)^\circ \rightarrow GL_n(E_P) \xrightarrow{\det} E_P^\circ.$$

Just as above, we then obtain a homomorphism

$$\text{Det}: (K_P G)^\circ \rightarrow \text{Hom}_\Omega(\text{ch } G, E_P^\circ).$$

As in (52.4), we note that

$$(52.8) \quad \text{Det}: (R_P G)^* \rightarrow \text{Hom}_\Omega(\text{ch } G, S_P)$$

for each maximal ideal  $P$  of  $R$ .

We show next that  $\text{Det}$  is closely related to the reduced norm map. It is this relation, in fact, which allows us to recast our previous formulas for  $\text{Cl } RG$  and  $D(RG)$  in terms of these  $\text{Hom}$  groups.

**(52.9) Proposition.** *Let  $A = KG$ , and let  $\text{nr}$  be the reduced norm map  $\text{nr}_{A/C}$  from  $A$  to its center  $C$ . Then there is an isomorphism*

$$f: C^* \cong \text{Hom}_\Omega(\text{ch } G, E^*)$$

such that the diagram

$$(52.10) \quad \begin{array}{ccc} A^* & \searrow \text{Det} & \\ \text{nr} \downarrow & & \\ C^* & \xrightarrow{f} & \text{Hom}_\Omega(\text{ch } G, E^*) \end{array}$$

is commutative.

*Proof.* In order to get an intuitive feeling for the result, we consider first the special case where  $E = K$ , so now  $\text{Irr } G = \text{Irr } KG = \{\zeta_1, \dots, \zeta_r\}$ , say. Then  $C^*$  is a direct product of  $r$  copies of  $K^*$ . On the other hand, the  $\{\zeta_i\}$  form a free  $\mathbb{Z}$ -basis of  $\text{ch } G$ , and thus

$$\text{Hom}(\text{ch } G, K^*) \cong \prod_{i=1}^r \text{Hom}(\mathbb{Z}, K^*) \cong \prod_{i=1}^r K^*.$$

The desired isomorphism  $f$  can then be given as follows: let  $C = \coprod_i C_i$ , and let  $c = \prod c_i$ ,  $c_i \in C_i$ . Then define  $f_c$  by

$$f_c(\sum a_i \zeta_i) = \prod c_i^{a_i}, \quad a_i \in \mathbb{Z}.$$

To verify that  $f \circ \text{nr} = \text{Det}$ , it suffices to work with simple components. Let  $A_i$  be a simple component of  $A$  with center  $C_i$ , and character  $\zeta_i$  afforded by a representation  $T_i$ . By definition of the reduced norm, we have

$$\text{nr } y = \det T_i(y) = \det_{\zeta_i} y = (\text{Det } y)(\zeta_i) \quad \text{for } y \in A_i^*.$$

If  $c_i = \text{nr } y$ , then  $f_c(\zeta_i) = c_i$ ; therefore  $(f \circ \text{nr})y = \text{Det } y$ , as desired.

Turning to the general case, let  $\Omega = \text{Gal}(E/K)$ , where  $E$  is a splitting field for  $G$ . Let  $\{\zeta_1, \dots, \zeta_k\}$  be a full set of representatives of the orbits of  $\text{Irr } G$  under the

action of  $\Omega$ , and identify each field  $K(\zeta_i)$  with a subfield of  $E$ . We may then write

$$C = \prod_{i=1}^k C_i, \quad \text{where } C_i = K(\zeta_i).$$

If  $\zeta \in \text{Irr } G$  is conjugate to  $\zeta_i$ , say  $\zeta = \zeta_i^\omega$  for some  $\omega \in \Omega$ , then  $\omega$  induces an automorphism  $K(\zeta) \cong K(\zeta)$ . We now define a map  $f: C \rightarrow \text{Hom}_\Omega(\text{ch } G, E)$  as follows: given  $c = \prod c_i \in K(\zeta_i)$ , let  $f_c$  be the function

$$f_c = \prod f_{c_i}, \quad \text{where } \begin{cases} f_{c_i}(\zeta_i^\omega) = c_i^\omega, & \omega \in \Omega, \\ f_{c_i}(\zeta) = 1 & \text{if } \zeta \neq \Omega\text{-conjugate of } \zeta_i. \end{cases}$$

This defines  $f_c(\zeta)$  for  $\zeta \in \text{Irr } G$ , and we extend  $f_c$  to a map on  $\text{ch } G$  by setting

$$f_c \left( \sum \zeta a_\zeta \right) = \prod \zeta f_c(\zeta)^{a_\zeta}, \quad a_\zeta \in \mathbb{Z}.$$

It is trivial to verify that the map  $f: c \rightarrow f_c$  is multiplicative, and that each  $f_c$  is an  $\Omega$ -homomorphism.

Let us verify that  $f$  is an isomorphism. Suppose first that  $f_c = 1$ , so  $f_c(\zeta) = 1$  for each  $\zeta \in \text{Irr } G$ ; taking  $\zeta = \zeta_i$  we obtain  $c_i = 1$  for each  $i$ , so  $c = 1$ . Secondly, given any  $g \in \text{Hom}_\Omega(\text{ch } G, E)$ , let  $u_i = g(\zeta_i) \in E$ ,  $1 \leq i \leq k$ . If  $\omega \in \Omega$  fixes  $\zeta_i$  then it also fixes  $u_i$ , and therefore  $u_i \in K(\zeta_i)$ . Choosing  $c = \prod_i u_i$ , we obtain  $f_c = g$ , so  $f$  is surjective. This proves that  $f$  is an isomorphism, as desired.

To prove that diagram (52.10) is commutative, it again suffices to work with a simple component  $A_i$  of  $A$  with center  $C_i$ . Let  $A_i$  correspond to the  $\Omega$ -orbit of  $\zeta_i$  in  $\text{Irr } G$ , and let  $a \in A_i$ . Define  $c = \text{nr}_{A/C} a = \text{nr}_{A_i/C_i} a \in C_i$ . By definition of the isomorphism  $f$ , we have

$$f_c(\zeta_i^\omega) = c^\omega \quad \text{for } \omega \in \Omega.$$

On the other hand, let  $T_i$  be the  $E$ -representation of  $G$  affording  $\zeta_i$ . Then

$$\text{nr}_{A_i/C_i} a = \det T_i(a) = \det_{\zeta_i}(a)$$

by definition of the reduced norm map. For  $\omega \in \Omega$ , we obtain

$$(\text{Det } a)(\zeta_i^\omega) = \det_{\zeta_i^\omega}(a) = (\det_{\zeta_i}(a))^\omega = c^\omega = f_c(\zeta_i^\omega),$$

that is,  $\text{Det}$  and  $f \circ \text{nr}$  agree on  $a \in A_i$ . This completes the proof of the proposition.

The reader will easily verify that the above discussion is independent of the choice of  $E$ , as long as  $E/K$  is Galois and  $E$  is a splitting field for  $G$ . To avoid a choice for  $E$ , we may instead use the algebraic closure  $K^e$  of  $K$  as a splitting field for  $G$ . Of course,  $\text{Gal}(K^e/K)$  is infinite, and it is conceptually somewhat simpler to work with finite Galois extensions.

Now let  $R = \text{alg. int. } \{K\}$ , and set

$$\Lambda = RG \subset \Lambda' \subset KG = A, \quad \Lambda' = \text{maximal } R\text{-order in } A.$$

As in §31B and §49A, we introduce the idèle group

$$J^*(A) = \{(\alpha_p) \in \prod A_p^\times : \alpha_p \in \Lambda_p^\times \text{ a.e.}\},$$

where  $P$  ranges over all primes of  $K$ , finite and infinite both. (For infinite  $P$ , define  $R_P = K_P$ ,  $\Lambda_P = A_P$ , etc.) Analogously, there are idèle groups  $J^*(C)$  and  $J^*(E)$ , where  $C$  is the center of  $A$ , and  $E$  is as above. Define

$$U^*(\Lambda) = \prod_p \Lambda_p^\times = \text{group of unit idèles in } J^*(A),$$

$$\tilde{J}(A) = \{\alpha \in J^*(A) : \text{nr}_{A/C} \alpha = 1\}.$$

As shown in (49.23) and (49.24), we may express  $\text{Cl } \Lambda$  in terms of these idèle groups, by the formulas

$$\text{Cl } \Lambda \cong \frac{J^*(A)}{\tilde{J}(A) A^\times U^*(\Lambda)} \cong \frac{J^*(C)}{C^\times \text{nr } U^*(\Lambda)},$$

where  $A^\times$  and  $C^\times$  are groups of principal idèles. The second of these isomorphisms arises by applying  $\text{nr}_{A/C}$  to the first formula.

From these isomorphisms and the preceding discussion, we deduce Fröhlich's [76] formula:

**(52.11) Hom Formula for Class Groups.** *There is an isomorphism*

$$\text{Cl } RG \cong \frac{\text{Hom}_\Omega(\text{ch } G, J^*(E))}{\text{Hom}_\Omega(\text{ch } G, E^\times) \cdot \text{Det } U^*(RG)}.$$

*Proof.* The isomorphism  $C^\times \cong \text{Hom}_\Omega(\text{ch } G, E^\times)$  extends readily to an isomorphism

$$J^*(C) \cong \text{Hom}_\Omega(\text{ch } G, J^*(E)).$$

In this isomorphism,  $\text{nr } U^*(\Lambda)$  maps onto  $\text{Det } U^*(\Lambda)$  because of the commutative diagram (52.10). We note also that

$$\text{Det } U^*(\Lambda) \subseteq \text{Hom}_\Omega(\text{ch } G, U^*(S))$$

by (52.8), where (as above)  $S$  is the integral closure of  $R$  in  $E$ .

If we want to avoid the use of infinite primes of  $K$ , then in the formula for  $\text{Cl } \Lambda$  we must replace  $C^\times$  by  $C^+$ , and must then describe the image of  $C^+$  in

$\text{Hom}_\Omega(\text{ch } G, E^*)$ . We shall return to this question later. For the moment, however, we make explicit the connection between locally free ideals of  $\Lambda$  and functions from  $\text{ch } G$  to  $J^*(E)$ .

**(52.12) Corollary.** *Let  $M = \Lambda\alpha$  be a locally free left  $\Lambda$ -ideal, where  $\alpha = (\alpha_p) \in J^*(A)$ . In the isomorphism (52.11), the class of  $M$  in  $\text{Cl } \Lambda$  corresponds to the class of the representative function  $f \in \text{Hom}_\Omega(\text{ch } G, J^*(E))$ , defined by the formula*

$$f(\zeta) = (f_P(\zeta)) \in J^*(E), \quad \text{for } \zeta \in \text{Irr } G,$$

where

$$f_P(\zeta) = \det_\zeta \alpha_p \in E_P \quad \text{for each prime } P \text{ of } K.$$

*Proof.* This is immediate from (52.10).

Before discussing the functorial properties of (52.11), we give some examples of representative functions of locally free ideals.

### (52.13) Example: Swan Modules

Let  $G$  be a group of order  $n$ , and define  $\sigma = \sum_{x \in G} x \in \mathbb{Z}G$ . For each  $r \in \mathbb{Z}$  relatively prime to  $n$ , define the *Swan module*

$$\langle r, \sigma \rangle = r\mathbb{Z}G + \sigma\mathbb{Z}G,$$

a locally free left ideal of  $\mathbb{Z}G$  (see §53). Let  $e = \sigma/n$ , a central idempotent of  $\mathbb{Q}G$ , and define  $u = 1 - e + re \in \mathbb{Q}G$ . As shown in §53, we have

$$\langle r, \sigma \rangle \cong \mathbb{Z}G\beta, \quad \text{where } \beta = (\beta_p), \quad \text{with } \beta_p = \begin{cases} 1, & p \nmid n, \\ u, & p \mid n, \end{cases}$$

and where we now take  $\beta_\infty = 1$ .

If  $p \nmid n$  or  $p = \infty$ , we have  $\beta_p = 1$ , and thus  $f_p(\zeta) = 1$  for all  $\zeta \in \text{Irr } G$ , where  $f$  represents  $\langle r, \sigma \rangle$ . If  $p \mid n$ , then  $f_p(\zeta) = \det_\zeta u$  for each  $\zeta$ . But  $u \rightarrow r$  in the trivial representation of  $G$ , while  $u \rightarrow 1$  in all nontrivial irreducible representations of  $G$ . Therefore if  $p \mid n$  we have

$$f_p(\zeta) = \begin{cases} r, & \zeta = 1, \\ 1, & \zeta \in \text{Irr } G, \quad \zeta \neq 1. \end{cases}$$

### (52.14) Example: Integers in Tamely Ramified Extensions

Let  $K$  be a finite Galois extension of  $\mathbb{Q}$  with Galois group  $G$ , and let  $R = \text{alg. int. } \{K\}$ . We may view  $K$  as a left  $\mathbb{Q}G$ -module by defining

$$\left( \sum_{\sigma \in G} a_\sigma \sigma \right) x = \sum a_\sigma \sigma(x) \quad \text{for } x \in K, \quad a_\sigma \in \mathbb{Q}.$$

The Normal Basis Theorem (MO, Exercise 29.14) asserts that  $K$  has a normal basis over  $\mathbb{Q}$ , that is, there exists an  $x \in K$  such that  $\{\sigma(x) : \sigma \in G\}$  is a  $\mathbb{Q}$ -basis of  $K$ . This is equivalent to the assertion that  $K$  is free (of rank 1) as  $\mathbb{Q}G$ -module.

The corresponding problem for rings of integers is considerably harder (and thus more interesting). Clearly  $R$  is a  $\mathbb{Z}G$ -module, and we say that  $R$  has a *normal integral basis* if  $R \cong \mathbb{Z}G$  or equivalently,  $R = \bigoplus_{\sigma \in G} \mathbb{Z}\sigma(x)$  for some  $x \in R$ . By Exercise 4.15, if  $R$  is tamely ramified over  $\mathbb{Z}$ , then  $R$  is projective as  $\mathbb{Z}G$ -module. (In this case,  $R$  is locally free as left  $\mathbb{Z}G$ -module, by Swan's Theorem 32.11.) Conversely, if  $R$  is  $\mathbb{Z}G$ -projective, then  $R$  is tamely ramified over  $\mathbb{Z}$ . Thus, in trying to decide whether  $R$  has a normal integral basis, we need only consider the tamely ramified case (see Exercises 4.13, 4.15, and Volume I, page 595, for discussion of tame ramification). It is customary to say that " $K$  is tamely ramified over  $\mathbb{Q}$ ," rather than refer to the rings of integers involved.

Supposing now that  $K/\mathbb{Q}$  is tamely ramified, the  $\mathbb{Z}G$ -module  $R$  is locally free, and thus determines a class  $[R]$  in the locally free class group  $\text{Cl } \mathbb{Z}G$ . Denote this class by  $U_K$  hereafter. Fröhlich [76] used the formula for  $\text{Cl } \mathbb{Z}G$  to prove the deep result that  $U_K \in D(\mathbb{Z}G)$ . Taylor [80] proved that  $U_K$  has order 1 or 2, and the latter possibility cannot occur unless the Galois group  $G$  has an irreducible symplectic<sup>†</sup> character; if no such character exists, then necessarily  $U_K = 0$  and  $R$  is  $\mathbb{Z}G$ -free. We remark also that Taylor and Chase have shown that  $\tau U_K = U_K$  in  $D(\mathbb{Z}G)$ , where  $\tau$  is the automorphism of  $D(\mathbb{Z}G)$  induced by the map  $x \mapsto x^{-1}$ ,  $x \in G$  (see §50E). For a systematic treatment of these matters, see Fröhlich [83].

We now state Fröhlich's formula for the function  $f \in \text{Hom}_{\Omega}(\text{ch } G, J^*(E))$  which represents the class  $U_K \in \text{Cl } \mathbb{Z}G$ . The formula involves the use of resolvents, which we define as follows. For each  $a \in K$ , form the sum

$$\sum_{\sigma \in G} \sigma(a)\sigma^{-1} \in KG.$$

Let  $\zeta$  be an irreducible complex character of  $G$ , afforded by a representation  $T$  in some splitting field  $E$  containing  $K$ . We define the *resolvent*

$$(a|\zeta) = \det T \left( \sum_{\sigma \in G} \sigma(a)\sigma^{-1} \right) = \det_{\zeta} \left( \sum_{\sigma} \sigma(a)\sigma^{-1} \right).$$

If  $K = \mathbb{Q}G \cdot a$ , then  $(a|\zeta) \in E$  for each  $\zeta \in \text{Irr } G$ . In the same manner, for each rational prime  $p$  (or for  $p = \infty$ ), we may define a resolvent  $(b|\zeta)$  for  $b \in K_p$ , where  $K_p = \mathbb{Q}_p \otimes_{\mathbb{Q}} K$  and  $G = \text{Gal}(K/\mathbb{Q})$  acts trivially on  $\mathbb{Q}_p$ .

Still assuming that  $K/\mathbb{Q}$  is tamely ramified, choose  $a \in K$  such that  $K = \mathbb{Q}G \cdot a$ . Further, for each  $p$  choose  $b_p \in R_p$  such that  $R_p = \mathbb{Z}_p G \cdot b_p$ . Then the class of  $[R]$  in  $\text{Cl } \mathbb{Z}G$  is represented by the function  $f \in \text{Hom}_{\Omega}(\text{ch } G, J^*(E))$  defined by

$$f = (f_p), \quad \text{where } f_p(\zeta) = (b_p|\zeta) \cdot (a|\zeta)^{-1}, \quad \zeta \in \text{Irr } G.$$

<sup>†</sup>Defined below.

It is this formula which lies at the heart of the above-mentioned theorems concerning  $U_K$ . See Fröhlich [83] for details.

The idèle groups occurring in (52.11) involve both finite and infinite primes. One of the main reasons for using infinite primes stems from the fact that in problems concerning the existence of normal integral bases, the irreducible symplectic characters of  $G$  play a key role (see (52.14)). We may define such characters as follows, anticipating the discussion in §73. Let  $B$  be a simple component of the group algebra  $RG$ , affording the real character  $\eta$ . There are three possibilities:

- (i)  $B \cong M_n(\mathbb{R})$ . Then  $C \otimes_{\mathbb{R}} B \cong M_n(C)$ , and  $\eta$  is an absolutely irreducible character of  $G$  realizable in  $\mathbb{R}$ .
- (ii)  $B \cong M_n(\mathbb{C})$ . Then  $C \otimes_{\mathbb{R}} B \cong M_n(C) \oplus M_n(C)$ , and  $\eta = \zeta + \bar{\zeta}$  for some  $\zeta \in \text{Irr } G$  which is distinct from its complex conjugate  $\bar{\zeta}$ , that is,  $\zeta$  is not real-valued.
- (iii)  $B \cong M_n(\mathbb{H})$ , where  $\mathbb{H}$  is the skewfield of real quaternions, of index 2. Then  $C \otimes_{\mathbb{R}} B \cong M_{2n}(\mathbb{C})$ , and  $\eta = 2\zeta$  for some real-valued  $\zeta \in \text{Irr } G$ . The character  $\zeta$  cannot be realized in  $\mathbb{R}$ , but  $2\zeta$  can be realized in  $\mathbb{R}$ . We call  $\zeta$  an *irreducible symplectic character* of  $G$ .

We shall use the above in singling out a subgroup  $\text{Hom}_{\Omega}^+$  of  $\text{Hom}_{\Omega}$ . As before, let  $\Omega = \text{Gal}(E/K)$  where  $E$  is a splitting field for  $G$ . Let us define

$$(52.15) \quad \begin{cases} \text{Hom}_{\Omega}^+(\text{ch } G, J^*(E)) \\ = \{f = (f_P) \in \text{Hom}_{\Omega}(\text{ch } G, J^*(E)) : f_P(\zeta) > 0 \text{ for every irreducible} \\ \text{symplectic character } \zeta \text{ of } G \text{ and every infinite prime } P \text{ of} \\ E \text{ extending a real prime of } K\}. \end{cases}$$

We claim that

$$\text{Det } U^*(\Lambda') = \text{Hom}_{\Omega}^+(\text{ch } G, U^*(S)),$$

where  $\Lambda'$  is a maximal order in  $KG$  containing  $RG$ , and where  $S = \text{alg. int. } \{E\}$ . It suffices to check the formula

$$\text{Det } A_{P_0} = \text{Hom}_{\Omega}^+(\text{ch } G, E_{P_0})$$

for every infinite prime  $P_0$  of  $K$ . This is clear from (52.10) when  $P_0$  is complex. On the other hand, for  $P_0$  real it suffices to verify the formula for every simple component  $B$  of  $A_{P_0}$ , and again the result follows from the diagram

$$\begin{array}{ccc} B^* & & \\ \downarrow \text{nr} & \searrow \text{Det} & \\ (\text{center of } B)^* & \xrightarrow{f} & \text{Hom}_{\Omega}(\text{ch } G, E_{P_0}). \end{array}$$

We leave the details to the reader.

We may now obtain Fröhlich's Hom description of the kernel group  $D(\Lambda)$ , where  $\Lambda = RG$ .

**(52.16) Theorem.** *In terms of the above notation, we have*

$$D(\Lambda) \cong \frac{\text{Hom}_{\Omega}^{+}(\text{ch } G, U^*(S))}{\text{Hom}_{\Omega}^{+}(\text{ch } G, S^*) \cdot \text{Det } U^*(\Lambda)}.$$

*Proof.* Let  $\text{Hom}$  denote  $\text{Hom}_{\Omega}$ , and use (52.11) for both  $\text{Cl } \Lambda$  and  $\text{Cl } \Lambda'$ . Since  $\text{Det } U^*(\Lambda') = \text{Hom}^{+}(\text{ch } G, U^*(S))$ , we obtain

$$\begin{aligned} D(\Lambda) &\cong \frac{\text{Hom}(\text{ch } G, E^*) \cdot \text{Hom}^{+}(\text{ch } G, U^*(S))}{\text{Hom}(\text{ch } G, E^*) \cdot \text{Det } U^*(\Lambda)} \\ &\cong \frac{\text{Hom}^{+}(\text{ch } G, U^*(S))}{\text{Det } U^*(\Lambda) \{ \text{Hom}(\text{ch } G, E^*) \cap \text{Hom}^{+}(\text{ch } G, U^*(S)) \}}. \end{aligned}$$

Since the intersection in the denominator above is  $\text{Hom}^{+}(\text{ch } G, S^*)$ , the theorem is established.

Let us now reformulate the above results on  $\text{Cl } RG$  and  $D(RG)$  in terms of the idèle groups  $J(E)$ ,  $U(S)$ , etc., which involve only the finite primes (that is, the maximal ideals of  $R$ ); see (49.17) and (49.36). As in the discussion and proof of (49.23), we obtain the formulas

$$(52.17) \quad \text{Cl } \Lambda \cong \frac{\text{Hom}_{\Omega}(\text{ch } G, J(E))}{\text{Hom}_{\Omega}^{+}(\text{ch } G, E^*) \cdot \text{Det } U(\Lambda)},$$

$$(52.18) \quad D(\Lambda) \cong \frac{\text{Hom}_{\Omega}(\text{ch } G, U(S))}{\text{Det } U(\Lambda) \cdot \text{Hom}_{\Omega}^{+}(\text{ch } G, S^*)}.$$

Further, the Hom version of (49.40) holds true. Let  $S(\Lambda) = \{P = \text{maximal ideal of } R: \Lambda_P \neq \text{maximal } R_P\text{-order}\}$ . Then

$$(52.19) \quad D(\Lambda) \cong \frac{\text{Hom}_{\Omega}(\text{ch } G, \prod_{P \in S(\Lambda)} S_P^*)}{\left\{ \prod_{P \in S(\Lambda)} \text{Det } \Lambda_P^* \right\} \cdot \text{Hom}_{\Omega}^{+}(\text{ch } G, S^*)}.$$

In particular, if  $G$  is a  $p$ -group ( $p = \text{prime}$ ), then

$$(52.20) \quad D(\Lambda) \cong \frac{\text{Hom}_{\Omega}(\text{ch } G, S_p^*)}{\text{Det}(R_p G) \cdot \text{Hom}_{\Omega}^{+}(\text{ch } G, S^*)}.$$

We now discuss some functorial properties of the Hom formulas for class groups.

**(52.21) Change of Group (Induction).** An inclusion of groups  $H \leq G$  extends to an inclusion  $RH \subseteq RG$ , yielding a “change of rings” map  $RG \otimes_{RH} \text{Hom}(ch H, \cdot) : \text{Cl } RH \rightarrow \text{Cl } RG$ . This carries a locally free  $RH$ -module  $RH\alpha$  (where  $\alpha \in J^*(KH)$  is an idèle) onto the locally free  $RG$ -module  $RG\alpha$ .

On the other hand, restriction of operators from  $G$  to  $H$  gives a map  $\text{ch } G \rightarrow \text{ch } H$ , which induces a map  $\text{Hom}(\text{ch } H, \cdot) \rightarrow \text{Hom}(\text{ch } G, \cdot)$ . Then we obtain a commutative diagram

$$\begin{array}{ccc} \text{Cl } RH & \longrightarrow & \text{Hom}_{\Omega}(\text{ch } H, J^*(E))/\cdots \\ \downarrow & & \downarrow \\ \text{Cl } RG & \longrightarrow & \text{Hom}_{\Omega}(\text{ch } G, J^*(E))/\cdots, \end{array}$$

where the horizontal arrows are the isomorphisms given in (52.11).

(We remark that a corresponding result holds whenever there is a homomorphism  $H \rightarrow G$  of groups. Indeed, it holds more generally for homomorphisms  $\Lambda \rightarrow \Lambda'$  of  $R$ -orders.)

To prove commutativity, it suffices to verify (after passing to  $P$ -adic completions and changing notation) that the following diagram commutes:

$$\begin{array}{ccc} (KH)^{\cdot} & \xrightarrow{\text{Det}} & \text{Hom}(\text{ch } H, E^{\cdot}) \\ \downarrow & & \downarrow \\ (KG)^{\cdot} & \xrightarrow{\text{Det}} & \text{Hom}(\text{ch } G, E^{\cdot}). \end{array}$$

This is a trivial computation, left to the reader.

**(52.22) Change of Groups (Restriction).** For  $H \leq G$ , each  $RG$ -module  $M$  may be viewed as  $RH$ -module  $M_H$ , by restriction of operators. Since  $RG|_H$  is  $RH$ -free of rank  $|G:H|$ , we obtain a homomorphism  $\text{res}_H^G : K_0(RG) \rightarrow K_0(RH)$ . This commutes with  $P$ -adic completion, and hence induces a map  $\text{res}_H^G : \text{Cl } RG \rightarrow \text{Cl } RH$  (see §49C).

Next we observe that the induction homomorphism  $\text{ind}_H^G : \text{ch } H \rightarrow \text{ch } G$  gives rise to a map  $\text{Hom}(\text{ch } G, \cdot) \rightarrow \text{Hom}(\text{ch } H, \cdot)$ . We claim that the diagram

$$\begin{array}{ccc} \text{Cl } RG & \longrightarrow & \text{Hom}_{\Omega}(\text{ch } G, J^*(E))/\cdots \\ \text{res} \downarrow & & \downarrow \\ \text{Cl } RH & \longrightarrow & \text{Hom}_{\Omega}(\text{ch } H, J^*(E))/\cdots \end{array}$$

commutes, where the horizontal arrows are the isomorphisms (52.11). (Note that this property is peculiar to group rings, and need not hold for arbitrary orders.)

By (49.16), in order to prove the above claim, it suffices to verify (after completing and changing notation) that the following diagram commutes:

$$\begin{array}{ccc} K_1(KG) & \xrightarrow{\text{Det}} & \text{Hom}(\text{ch } G, E^\cdot) \\ \text{res} \downarrow & & \downarrow \\ K_1(KH) & \xrightarrow{\text{Det}} & \text{Hom}(\text{ch } H, E^\cdot). \end{array}$$

For this, we need only prove that

$$(52.23) \quad \det_{\mu^G}(x) = \det_\mu(\text{res } x) \quad \text{for } x \in (KG)^\cdot \quad \text{and} \quad \mu \in \text{Irr } H.$$

Let  $G = \bigcup_{i=1}^n g_i H$ , where  $n = |G:H|$ . Then  $x \in (KG)^\cdot$  corresponds to the element  $[KG, x_i]$ , where  $x_i$  is left multiplication on the right  $KG$ -module  $KG$ . Let  $xg_i = g_j h_{ij}$ ,  $h_{ij} \in KH$ . Then  $\text{res } x \in GL_n(KH)$  is the matrix given by

$$\text{res } x = [g_j^{-1} x g_i]_{1 \leq i,j \leq n}$$

with the understanding that when  $g_j^{-1} x g_i$  is expressed as a linear combination of group elements, we omit all terms outside of  $H$ . Now let  $M$  be an  $E$ -representation of  $H$  affording  $\mu$ . Then  $\mu^G$  is afforded by  $M^G$ , where

$$M^G(x) = [\dot{M}(g_j^{-1} x g_i)]_{1 \leq i,j \leq n},$$

and  $\dot{M}$  vanishes outside  $H$ . Therefore for  $x \in (KG)^\cdot$ ,

$$\begin{aligned} \det_{\mu^G}(x) &= \det M^G(x) = \text{determinant of the matrix obtained by} \\ &\quad \text{applying } M \text{ to each entry of } \text{res } x \\ &= \det_\mu(\text{res } x). \end{aligned}$$

This completes the proof. The reader should compare this calculation with that given in the proof of (13.15). Indeed, for  $x \in G$  (viewed as element of  $(KG)^\cdot$ ), we have

$$\det_{\mu^G}(\text{res } x) = \{\varepsilon_{G \rightarrow H}^{\mu(1)}(x)\} \{\det_\mu V_H^G(x)\},$$

where the right-hand expression is in  $\pm H/H'$ . Our formula (52.23) is thus a generalization of formula (13.15i). (See also the proof of (46.18).)

**(52.24) Change of Ground Ring (Extension).** Let  $K'$  be a finite extension of  $K$  and  $R'$  the integral closure of  $R$  in  $K'$ . The inclusion  $RG \subset R'G$  gives a homomorphism

$$R' \otimes_R * : \text{Cl } RG \rightarrow \text{Cl } R'G.$$

Choose the splitting field  $E$  so that  $E$  is a Galois extension of  $K'$ , and let  $\Omega' = \text{Gal}(E/K')$ . It is easily verified that the following diagram commutes:

$$\begin{array}{ccc} \text{Cl } RG & \longrightarrow & \text{Hom}_{\Omega'}(\text{ch } G, J^*(E))/\cdots \\ \downarrow & & \downarrow \\ \text{Cl } R'G & \longrightarrow & \text{Hom}_{\Omega'}(\text{ch } G, J^*(E))/\cdots, \end{array}$$

where the horizontal arrows are the isomorphisms (52.11), and the map on Hom's is the canonical injection.

**(52.25) Change of Ground Ring (Restriction).** Keep the above notation. Since  $R'$  is  $R$ -projective,  $R'G$  is projective as  $RG$ -module, so the restriction map gives a homomorphism  $K_0(R'G) \rightarrow K_0(RG)$ . This commutes with completions, and induces a map  $\text{Cl } R'G \rightarrow \text{Cl } RG$ , by identifying these class groups with subgroups of  $K_0$  as in (49.15). For  $M$  a locally free ideal of  $R'G$ , the element of  $K_0(R'G)$  corresponding to  $[M] \in \text{Cl } R'G$  is  $[M] - [R'G]$ ; its image in  $K_0(RG)$  is then  $[M]_{RG} - [R'G]_{RG}$ . In terms of Hom's the restriction map  $\text{Cl } R'G \rightarrow \text{Cl } RG$  corresponds to a “norm” map from  $\text{Hom}_{\Omega'}$  to  $\text{Hom}_{\Omega}$ . There is a commutative diagram

$$\begin{array}{ccc} \text{Cl } R'G & \longrightarrow & \text{Hom}_{\Omega'}(\text{ch } G, J^*(E))/\cdots \\ \downarrow & & \downarrow \mathcal{N} \\ \text{Cl } RG & \longrightarrow & \text{Hom}_{\Omega}(\text{ch } G, J^*(E))/\cdots, \end{array}$$

with the horizontal arrows the isomorphisms (52.11). Let  $f \in \text{Hom}_{\Omega'}$  be a representative function of  $[M] \in \text{Cl } R'G$ , and define

$$\mathcal{N}f = \prod_{\sigma \in \Omega'/\Omega} \sigma f \sigma^{-1}.$$

The class  $[M] \in \text{Cl } R'G$  maps onto the class  $[N] + [R'G]_{RG} \in \text{Cl } RG$ , where  $N$  is the locally free  $RG$ -module with representative function  $\mathcal{N}f$ . For details and proof, see Fröhlich [76].

We briefly mention determinantal congruences, which follow from the Hom description of the class group. As usual, let  $E/K$  be a Galois extension with Galois group  $\Omega$ , and let  $S = \text{alg. int. } \{E\}$ ,  $R = \text{alg. int. } \{K\}$ . Let  $E$  be a splitting field for  $G$ . Given a rational prime  $p$ , let  $P$  be a maximal ideal of  $R$ , and  $P'$  of  $S$ , both containing  $p$ . Let  $\bar{S} = S/P'$ ,  $\bar{Z} = Z/p\mathbb{Z}$ .

Given a  $S$ -representation  $T$  of  $G$ , we may form the  $\bar{S}$ -representation  $\bar{T}$  of  $G$ , by reduction  $(\text{mod } P')$ . By (16.16), the composition factors of  $T$  depend only on the character  $\tau$  of  $G$  afforded by  $T$ . The map  $T \rightarrow \bar{T}$  gives the Brauer decomposition map

$$d: G_0(EG) \rightarrow G_0(\bar{S}G)$$

(see (16.20)), and  $G_0(EG) \cong \text{ch } G$ . By (17.15),

$$\ker d = \{\zeta \in \text{ch } G : \zeta(x) = 0 \text{ for each } p\text{-regular } x \in G\}.$$

We now prove:

**(52.26) Theorem on Determinantal Congruences.** *Let  $pS = \prod_{i=1}^m P_i^{e_i}$ . Then for  $a \in (S_p G)^*$  and  $\xi \in \ker d$ , we have*

$$\det_\xi a \equiv 1 \left( \bmod \prod_{i=1}^m P_i \right).$$

*Proof.* It suffices to verify the result after passing to  $P_i$ -adic completions, so changing notation, we now assume  $S$  is a complete d.v.r. with maximal ideal  $P'$ . Given  $a \in (SG)^*$  and  $\xi = \varphi - \psi \in \ker d$ , where  $\varphi, \psi$  are ordinary characters of  $G$ , we must show that

$$\det_\varphi a \equiv \det_\psi a \pmod{P'}, \quad \text{since } \det_\xi = \det_\varphi / \det_\psi.$$

If  $T$  affords  $\varphi$  and  $U$  affords  $\psi$ , the above congruence becomes

$$\det T(a) \equiv \det U(a) \pmod{P'},$$

that is,

$$(*) \quad \det \bar{T}(\bar{a}) = \det \bar{U}(\bar{a}) \text{ in } \bar{S}.$$

But  $\bar{T} = \bar{U}$  in  $G_0(\bar{S}G)$  because  $\xi \in \ker d$ , so  $(*)$  clearly holds.

## §52 Exercises

1. Let  $\zeta \in \text{Irr } G$  and  $x \in KG$ . Prove that  $\det_\zeta x \in K(\zeta)$ .

[Hint: See proof of (52.9).]

2. Let  $M$  be a locally free left ideal of  $RG$ , and  $\check{M}$  its contragredient (see §50E). If  $f \in \text{Hom}(\text{ch } G, J^*(E))$  is the representative function of  $[M]$  (see (52.12)), show that  $[\check{M}]$  has representative function  $\check{f}$ , where

$$\check{f}(\zeta) = f(\bar{\zeta})^{-1}, \quad \zeta \in \text{ch } G,$$

with  $\bar{\zeta}$  defined by  $\bar{\zeta}(x) = \zeta(x^{-1})$ ,  $x \in G$  (so  $\bar{\zeta} = \text{complex conjugate of } \zeta$  if  $K$  is a number field).

3. View  $\text{Cl } RG$  as a  $(\text{ch } KG)$ -module, as in (49.47), and let  $M, f$  be as above. For  $\zeta \in \text{ch } KG$ , let  $g$  be the representative function of the class  $\xi[M] \in \text{Cl } RG$ . Prove that

$$g(\zeta) = f(\bar{\zeta}\zeta), \quad \zeta \in \text{ch } G,$$

where  $\bar{\zeta}$  is the complex conjugate of  $\zeta$  (see Ullom [81]).

## §53. THE SWAN SUBGROUP OF THE CLASS GROUP

### §53A. The Swan Subgroup

Let  $G$  be a group of order  $n$ , and set

$$\sigma = \sigma_G = \sum_{x \in G} x \in \mathbb{Z}G,$$

so  $e = \sigma/n$  is a central idempotent in the group algebra  $\mathbb{Q}G$ . For each integer  $r$  relatively prime to  $n$ , let us define a *Swan module*

$$\langle r, \sigma \rangle = \mathbb{Z}Gr + \mathbb{Z}G\sigma = \mathbb{Z}Gr + \mathbb{Z}\sigma,$$

a two-sided ideal of  $\mathbb{Z}G$ . If  $p$  is any prime divisor of  $n$ , then  $\langle r, \sigma \rangle_p = \mathbb{Z}_p G$ , so by §31A  $\langle r, \sigma \rangle$  is locally free as left ideal of  $\mathbb{Z}G$ , and determines a class  $[r, \sigma] \in \mathrm{Cl} \mathbb{Z}G$ . As we shall see in a moment, the set of all classes  $[r, \sigma]$  with  $(r, n) = 1$  forms a subgroup  $T(G)$  of  $\mathrm{Cl} \mathbb{Z}G$ , called the *Swan subgroup* of  $\mathrm{Cl} \mathbb{Z}G$ . In fact,  $T(G)$  is a subgroup of the kernel group  $D(\mathbb{Z}G)$ .

Consider the fiber product .

$$(53.1) \quad \begin{array}{ccc} \mathbb{Z}G & \xrightarrow{f} & \mathbb{Z}G/\mathbb{Z}\sigma = \Gamma \\ \varepsilon \downarrow & & \downarrow \\ \mathbb{Z} & \longrightarrow & \bar{\mathbb{Z}} = \mathbb{Z}/n\mathbb{Z}, \end{array}$$

where  $\varepsilon$  is the augmentation map. This gives rise to an exact sequence

$$(53.2) \quad \mathbb{Z}^{\cdot} \times K_1(\Gamma) \xrightarrow{h} \bar{\mathbb{Z}}^{\cdot} \xrightarrow{\partial} D(\mathbb{Z}G) \rightarrow D(\Gamma) \rightarrow 0,$$

by (49.39). We claim that

$$(53.3) \quad \partial(\bar{r}) = [r, \sigma] \in D(\mathbb{Z}G).$$

In fact, the final part of the proof of (49.27) shows that

$$\partial(\bar{r}) = [M], \quad \text{where } M = \{(z, \gamma) \in \mathbb{Z} \oplus \Gamma : \bar{z} = \bar{r}\bar{\gamma} \text{ in } \bar{\mathbb{Z}}\}.$$

On the other hand,  $\mathbb{Z}G \cong \{(z, \gamma) : \bar{z} = \bar{\gamma} \text{ in } \bar{\mathbb{Z}}\}$ . There is an embedding  $M \rightarrow \mathbb{Z}G$ , given by  $(z, \gamma) \in M \mapsto (z, r\gamma) \in \mathbb{Z}G$ . But  $r \in \mathbb{Z}G$  corresponds to  $(r, r) \in \mathbb{Z} \oplus \Gamma$ , and  $\sigma \in \mathbb{Z}G$  to  $(n, 0) \in \mathbb{Z} \oplus \Gamma$ . Therefore the image of  $M$  in  $\mathbb{Z}G$  is precisely  $\langle r, \sigma \rangle$ , which proves (53.3). This shows that  $T(G)$  is a subgroup of  $D(\mathbb{Z}G)$ , and the sequence

$$(53.4) \quad \mathbb{Z}^{\cdot} \times K_1(\Gamma) \xrightarrow{h} \bar{\mathbb{Z}}^{\cdot} \xrightarrow{\partial} T(G) \rightarrow 0$$

is exact. Further, if  $\mathbb{Q}G$  satisfies the Eichler condition (or, more generally, if  $\mathbb{Z}G$

has locally free cancellation), then as in (49.39) the above sequence simplifies to an exact sequence

$$(53.5) \quad \mathbb{Z}^\cdot \times \Gamma^\cdot \xrightarrow{h} \bar{\mathbb{Z}}^\cdot \xrightarrow{\partial} T(G) \rightarrow 0.$$

Since  $h$  is a homomorphism, it follows from the group structure of  $\text{Cl } \mathbb{Z}G$  that

$$\langle r, \sigma \rangle \oplus \langle s, \sigma \rangle \cong \mathbb{Z}G \oplus \langle rs, \sigma \rangle \quad \text{for } (rs, n) = 1.$$

(One can also prove this result, due to Swan, by giving an explicit isomorphism.) Furthermore,  $\langle r, \sigma \rangle = \langle -r, \sigma \rangle$ , while by (42.11),

$$\langle r, \sigma \rangle \cong \langle s, \sigma \rangle \Leftrightarrow \bar{s} = \bar{\gamma}\bar{r} \text{ in } \bar{\mathbb{Z}} \quad \text{for some } \gamma \in \Gamma^\cdot.$$

We remark finally that by Exercise 53.2,

$$\langle r, \sigma \rangle \oplus \mathbb{Z} \cong \mathbb{Z}G \oplus \mathbb{Z}.$$

From (53.4) we obtain:

**(53.6) Proposition.** (i)  $T(G)$  is a homomorphic image of  $\bar{\mathbb{Z}}^\cdot / \{\pm 1\}$ , and therefore  $|T(G)|$  divides  $\varphi(n)/2$  if  $n > 2$ .

(ii) If  $G$  is a  $p$ -group, then  $T(G)$  is cyclic.

(iii)  $T(G) = 0$  if  $G$  is cyclic or dihedral.

*Proof.* Part (i) is clear from (53.4), since  $\bar{\mathbb{Z}}^\cdot$  has order  $\varphi(n)$ . Next, if  $n$  is a prime power  $p^k$ , then  $\bar{\mathbb{Z}}^\cdot$  is cyclic for odd  $p$ , while for  $p = 2$  and  $k > 1$ ,  $\bar{\mathbb{Z}} \cong \{\pm 1\} \times$  (cyclic group of order  $\varphi(n)/2$ ), which gives (ii).

To prove (iii), first let  $G = \langle x : x^n = 1 \rangle$ , and let  $(r, n) = 1$ . Then the element  $u = (x^r - 1)/(x - 1) \in \Gamma$  depends only on the class of  $r \pmod{n}$ , and  $u \in \Gamma^\cdot$  since  $u^{-1} = (x - 1)/(x^r - 1)$  in  $\Gamma$ . The element  $u \in \Gamma^\cdot$  maps onto  $\bar{r} \in \bar{\mathbb{Z}}^\cdot$ , so  $h$  is surjective. Thus  $T(G) = 0$  by (53.5). For the dihedral case, see Exercise 53.3 or Theorem 53.19.

The locally free left ideal  $\langle r, \sigma \rangle$  of  $\mathbb{Z}G$  may be expressed as  $\langle r, \sigma \rangle = \mathbb{Z}G\alpha$  for some idèle  $\alpha = (\alpha_p) \in J(\mathbb{Q}G)$ . If  $p \nmid r$ , then  $\langle r, \sigma \rangle_p = \mathbb{Z}_p G$ , and we may take  $\alpha_p = 1$ . On the other hand, if  $p \mid r$  then  $p \nmid n$ , and so  $\mathbb{Z}_p G = \mathbb{Z}_p \oplus \Gamma_p$ . Viewing elements of  $\mathbb{Z}_p G$  as ordered pairs from  $\mathbb{Z}_p \oplus \Gamma_p$ , we have  $r = (r, r)$ ,  $\sigma = (n, 0)$ . Thus  $\langle r, \sigma \rangle_p$  is the ideal generated by  $(r, r)$  and  $(n, 0)$ , that is,  $(1, r)(\mathbb{Z}_p \oplus \Gamma_p)$ . This yields

$$(53.7) \quad \langle r, \sigma \rangle = \mathbb{Z}G\alpha, \quad \text{where } \alpha = (\alpha_p), \quad \text{and} \quad \alpha_p = \begin{cases} (1, 1), & p \nmid r \\ (1, r), & p \mid r, \end{cases}$$

with  $(1, 1)$  and  $(1, r)$  viewed as elements of  $\mathbb{Z}_p \oplus \Gamma_p$ .

Another version of the above is also useful. Let  $e = \sigma/n$  as above, and put

$$(53.8) \quad u = (1 - e) + re = \text{central unit in } \mathbb{Q}G.$$

Then

$$\langle r, \sigma \rangle \cong \frac{u}{r} \langle r, \sigma \rangle = \left\langle u, \frac{u\sigma}{r} \right\rangle = \langle u, \sigma \rangle,$$

the last because  $u\sigma = r\sigma$ . We may write  $\langle u, \sigma \rangle = \mathbb{Z}G \cdot \beta$  for some idèle  $\beta = (\beta_p)$ . If  $p \nmid n$ , then  $e \in \langle u, \sigma \rangle$  and  $\langle u, \sigma \rangle_p = \langle u, e \rangle = \mathbb{Z}_p G$ , so  $\beta_p = 1$ . If  $p \mid n$  then  $\sigma = (u/r)\sigma \in u\mathbb{Z}_p G$ , so  $\langle u, \sigma \rangle = u \cdot \mathbb{Z}_p G$ . Thus

$$(53.9) \quad \langle r, \sigma \rangle = \langle u, \sigma \rangle = \mathbb{Z}G\beta, \quad \text{where } \beta_p = \begin{cases} 1 & \text{if } p \nmid n, \\ u & \text{if } p \mid n, \end{cases}$$

with  $u$  as in (53.8) (compare (52.13)).

We now prove:

**(53.10) Proposition.** *A surjection  $\varphi: G \rightarrow \bar{G}$  induces a surjection  $T(G) \rightarrow T(\bar{G})$ .*

*Proof.* We have already seen in (49.38) that  $\varphi$  induces a map  $D(\mathbb{Z}G) \rightarrow D(\mathbb{Z}\bar{G})$ . Now let  $r \in \mathbb{Z}$  be relatively prime to  $|\bar{G}|$ , and we may assume that also  $(r, n) = 1$ . Write

$$\mathbb{Q}G \cong \mathbb{Q} \oplus B, \quad \mathbb{Q}\bar{G} \cong \mathbb{Q} \oplus \bar{B}.$$

Then  $\varphi$  induces  $\mathbb{Q} \rightarrow \mathbb{Q}$ ,  $B \rightarrow \bar{B}$ , and  $\varphi$  carries the idèle  $\alpha$  associated with  $\langle r, \sigma \rangle$  onto the idèle  $\bar{\alpha}$  associated with  $\langle r, \sigma_{\bar{G}} \rangle$ , by (53.7). Thus  $\varphi[r, \sigma] = [r, \sigma_{\bar{G}}]$ , which proves the proposition.

**(53.11) Theorem (Ullom [76]).** *If  $H$  is a subgroup of  $G$ , then the restriction map  $\text{res}_H^G$  takes  $T(G)$  onto  $T(H)$ , and indeed  $\text{res}[r, \sigma_G] = [r, \sigma_H]$ .*

*Proof.* The easiest proof uses the Hom description of the class group. By (52.13), the class  $[r, \sigma] \in T(G)$  is represented by the function

$$f \in \text{Hom}_{\Omega}(\text{ch } G, J(E)), \quad \text{where } f_p(\zeta) = \det_{\zeta}(\beta_p) \quad \text{for } \zeta \in \text{Irr } G.$$

Thus for  $\zeta \in \text{Irr } G$ , we have from (53.9)

$$f_p(\zeta) = 1 \text{ if } p \nmid n; \quad f_p(\zeta) = 1 \text{ if } p \mid n \text{ and } \zeta \neq 1; \quad f_p(1_G) = r \text{ if } p \mid n.$$

We observe next that  $\text{res}_H^G: \text{Cl } \mathbb{Z}G \rightarrow \text{Cl } \mathbb{Z}H$  arises from the induction map  $\text{ind}_H^G: \text{ch } H \rightarrow \text{ch } G$ . If  $g = \text{res}_H^G f$ , then by (52.22)

$$g(\zeta) = f(\text{ind}_H^G \zeta) \quad \text{for } \zeta \in \text{ch } H.$$

But by Frobenius reciprocity, for  $\zeta \in \text{Irr } H$  we have

$$(1_G, \text{ind}_H^G \zeta)_G = (1_H, \zeta)_H,$$

and therefore

$$g(\zeta) = 1 \text{ for } \zeta \neq 1_H, \quad g(1_H) = f(1_G).$$

Let  $g'$  be the function in  $\text{Hom}_\Omega(\text{ch } H, J(E))$  which represents  $[r, \sigma_H]$ , so for  $\zeta \in \text{Irr } H$ ,

$$g'(\zeta) = 1 \text{ for } \zeta \neq 1_H, \quad g'_p(1_H) = \begin{cases} 1, & p \nmid |H|, \\ r, & p \mid |H|. \end{cases}$$

Thus  $g$  and  $g'$  agree, except at the primes  $q$  which divide  $|G|$  but not  $|H|$ . For such  $q$  (if any) we have

$$g_q(1_H) = r, \quad g'_q(1_H) = 1.$$

However, we may write  $Z_q H = Z_q \oplus \Delta$ , with  $\Delta$  a maximal order in  $\mathbb{Q}H/\mathbb{Q}\sigma_H$ . Choose  $\xi = (r, 1) \in (Z_q H)^\times$ , so  $\xi$  may be viewed as a unit idèle concentrated at position  $q$ . Then for  $\zeta \in \text{Irr } H$ ,

$$\text{Det}_\zeta \xi = \begin{cases} 1, & \zeta \neq 1, \\ r, & \zeta = 1. \end{cases}$$

This shows that  $g = g' \cdot \text{Det } \xi$ , so  $g$  and  $g'$  represent the same element in  $\text{Cl } ZH$ , by (52.16). Therefore  $\text{res}[r, \sigma_G] = [r, \sigma_H]$ , as desired.

As an easy consequence of the above, we deduce:

**(53.12) Theorem (Ullom [76]).** *The Artin exponent  $A(G)$  of  $G$  annihilates the Swan subgroup  $T(G)$  of  $\text{Cl } ZG$ . Therefore  $|G|T(G) = 0$ .*

*Proof.* From the definition of the Artin exponent (see §76), we may write

$$A(G) = \sum_i \text{ind}_{C_i}^G x_i \text{ in } \text{ch } \mathbb{Q}G,$$

where the  $\{C_i\}$  are cyclic subgroups of  $G$ , and  $x_i \in \text{ch } \mathbb{Q}C_i$ . By (49.47),  $\text{Cl } ZG$  is a Frobenius module over the Frobenius functor  $\text{ch } \mathbb{Q}G$ . For  $t \in T(G)$  we obtain

$$A(G)t = \sum_i t \text{ind}_{C_i}^G x_i = \sum_i \text{ind}_{C_i}^G (\text{res}_{C_i}^G t \cdot x_i),$$

using a Frobenius identity. But  $T(C_i) = 0$  by (53.6), and  $\text{res}_{C_i}^G t \in T(C_i)$  by (53.11),

so  $A(G)t = 0$ , as desired. The second assertion of the theorem holds because  $A(G)$  divides  $|G|$ .

**(53.13) Corollary.** *The restriction map  $T(G) \rightarrow \prod_p T(G_p)$  is surjective, where  $\{G_p\}$  ranges over a set of Sylow subgroups of  $G$ .*

*Proof.* For each  $p$ ,  $T(G_p)$  is a  $p$ -group, and  $\text{res}: T(G) \rightarrow T(G_p)$  is surjective, by (53.11) and (53.12). Now use the Chinese Remainder Theorem.

**(53.14) Theorem (Ullom [76]).** *Let  $G$  be an elementary abelian  $p$ -group of order  $p^{s+1}$ , where  $p$  is an odd prime and  $s \geq 0$ . Then  $T(G)$  is cyclic of order  $p^s$ , and is generated by the class  $[1 + p, \sigma]$ .*

*Proof.* Let  $K = \mathbb{Q}(\omega)$ ,  $R = \mathbb{Z}[\omega]$ , where  $\omega$  is a primitive  $p$ -th root of 1. Then

$$\mathbb{Q}G \cong \mathbb{Q} \oplus K^{(m)}, \quad \text{where } m = (p^{s+1} - 1)/(p - 1).$$

Then  $\Gamma = \mathbb{Z}G/\mathbb{Z}\sigma$  is an order in  $K^{(m)}$ , and hence is contained in the unique maximal order  $R^{(m)}$ . Since  $\bar{\mathbb{Z}}^\cdot \cong C_{p-1} \times \langle 1 + p \rangle$ , a product of cyclic groups of orders  $p - 1$  and  $p^s$ , respectively, the exact sequence (53.5) becomes

$$\mathbb{Z}^\cdot \times \Gamma^\cdot \xrightarrow{h} C_{p-1} \times \langle 1 + p \rangle \xrightarrow{\partial} T(G) \rightarrow 0.$$

Since  $T(G)$  is a  $p$ -group by (53.12), it suffices to show that  $h(\Gamma^\cdot) \leq C_{p-1}$ , for then  $T(G)$  is generated by  $\partial(1 + p)$ , that is, by  $[1 + p, \sigma]$ .

Let us view  $\Gamma$  as a subring of  $R^{(m)}$ ; each  $u \in \Gamma^\cdot$  is of the form  $u = (u_1, \dots, u_m)$ ,  $u_i \in R^\cdot$ , and we must show that  $h(u) \in C_{p-1}$ , that is,  $h(u)$  has order dividing  $p - 1$ . For  $a = 1, \dots, p - 1$ , let  $\varphi_a \in \text{Aut } G$  be defined by  $\varphi_a(g) = g^a$ ,  $g \in G$ . Then  $\varphi_a$  induces a ring automorphism of  $\mathbb{Q}G$ , carrying each simple component  $K$  of  $\mathbb{Q}G$  onto itself via the automorphism  $\omega \mapsto \omega^a$ . Therefore

$$\prod_{a=1}^{p-1} \varphi_a(u_i) = N_{K/\mathbb{Q}} u_i = +1,$$

since the norm  $N(u_i) = \pm 1$ , and  $N(u_i) > 0$  because  $p$  is odd. Consequently  $\prod_a \varphi_a(u) = 1$  in  $\Gamma^\cdot$ . But for each  $a, u$  and  $\varphi_a(u)$  have the same image  $\bar{u} \in \bar{\mathbb{Z}}^\cdot$ . Thus  $\bar{u}^{p-1} = 1$  in  $\bar{\mathbb{Z}}^\cdot$ , so  $h(u) \in C_{p-1}$ , and the proof is completed.

The case  $p = 2$  is even easier:

**(53.15) Theorem.** *For  $G$  elementary abelian of order  $2^{s+1}$ , where  $s \geq 1$ ,  $T(G)$  is cyclic of order  $2^{s-1}$ , generated by  $[5, \sigma]$ .*

*Proof.* Let  $n = 2^{s+1}$ , so  $\bar{\mathbb{Z}}^\cdot \cong \{\pm 1\} \times \langle 5 \rangle$ , a product of cyclic groups of orders 2,  $2^{s-1}$ , respectively. We may assume  $s \geq 2$ , the case  $s = 1$  being trivial. Then

$$5^{2^{s-2}} \equiv 1 + 2^s \pmod{n}.$$

Set  $r = 1 + 2^s$ , so

$$[5, \sigma]^{2^{s-2}} = [r, \sigma],$$

and we need only show that  $[r, \sigma] \neq 0$  in  $D(\mathbb{Z}G)$ .

Write  $G = \langle y \rangle \times H$ , where  $y^2 = 1$  and  $H = C_2^{(s)}$ . There is a fiber product

$$\begin{array}{ccc} \mathbb{Z}G & \xrightarrow{f} & \mathbb{Z}H \\ g \downarrow & & \downarrow \\ \mathbb{Z}H & \longrightarrow & kH, k = \mathbb{Z}/2\mathbb{Z}, \quad . \end{array}$$

where  $f(y) = 1$ ,  $g(y) = -1$ . This yields an exact Mayer-Vietoris sequence

$$(\mathbb{Z}H)^{\cdot} \times (\mathbb{Z}H)^{\cdot} \xrightarrow{\psi} (kH)^{\cdot} \xrightarrow{\delta} D(\mathbb{Z}G) \rightarrow D(\mathbb{Z}H) \oplus D(\mathbb{Z}H) \rightarrow 0.$$

By Exercise 53.1, we have (noting that  $1 + \sigma_H \in (kH)^{\cdot}$ )

$$\delta(1 + \sigma_H) = [\mathbb{Z}G\gamma], \quad \text{where } \gamma = (\gamma_p), \quad \text{and} \quad \gamma_p = \begin{cases} (1, 1), & p \text{ odd}, \\ (1 + \sigma_H, 1), & p = 2. \end{cases}$$

Now let  $u = 1 - e + re = 1 + \sigma/2$  as in (53.8). Then

$$\langle r, \sigma \rangle \cong \langle u, \sigma \rangle = \mathbb{Z}G\beta, \quad \text{where } \beta_p = \begin{cases} (1, 1), & p \text{ odd} \\ u, & p = 2. \end{cases}$$

But viewing  $u$  as element of  $\mathbb{Q}G$ , we have  $f(u) = 1 + \sigma_H$ ,  $g(u) = 1$ . It follows that

$$\delta(1 + \sigma_H) = [r, \sigma] \text{ in } D(\mathbb{Z}G).$$

To show that  $[r, \sigma] \neq 0$ , it therefore suffices to prove that  $1 + \sigma_H \notin \text{im } \psi$ . But every unit of  $\mathbb{Z}H$  is a torsion unit, and hence has the form  $\pm h$ ,  $h \in H$ , by Higman's Theorem. Since  $\psi(\pm h)$  cannot equal  $1 + \sigma_H$  in  $kH$ , it follows that  $[r, \sigma] \neq 0$ , and establishes the theorem.

In the same vein, we have:

**(53.16) Theorem.** *Let  $G = C_2^{(l)} \times C_4^{(m)}$ , where  $l + m \geq 2$ . Then  $T(G)$  is cyclic of order  $2^{l+2m-2}$ , with generator  $[5, \sigma]$ .*

*Proof.* The preceding argument carries over to this case. Write  $G = \langle y \rangle \times H$

where  $y^4 = 1$ , and use the fiber product

$$\begin{array}{ccc} \mathbb{Z}G & \longrightarrow & \mathbb{Z}G_0 \\ \downarrow & & \downarrow \\ RH & \longrightarrow & kG_0, \end{array}$$

where  $G_0 = \langle y^2 \rangle \times H$ ,  $R = \mathbb{Z}[i]$ , and  $k = \mathbb{Z}/2\mathbb{Z}$ .

The situation for quaternion groups is as follows:

**(53.17) Theorem.** *Let  $G$  be the generalized quaternion group of order  $2^{n+2}$ , where  $n \geq 1$ . Then  $T(G) = D(\mathbb{Z}G)$  is of order 2, with generator  $[3, \sigma]$ .*

*Proof.* We treat only the case  $n = 1$ , and use the notation and proof of (50.36). As shown there,  $D(\mathbb{Z}G)$  has order 2, and its nontrivial element may be taken as  $[\mathbb{Z}G\xi]$ , where  $\xi = (\xi_p)$  is the idèle with  $\xi_p = 1$  for  $p$  odd, and

$$\xi_2 = (i + j + k, 1) \in \Gamma_2^\circ \times \Delta_2^\circ.$$

(As first component, we could have used any element of  $\Gamma_2^\circ$  with reduced norm  $3(\text{mod } 8)$ .) On the other hand,  $[3, \sigma] = [5, \sigma] = [\mathbb{Z}G\beta]$ , where  $\beta = (\beta_p)$ , with  $\beta_p = 1$  for  $p$  odd, and

$$\beta_2 = 1 + 4(\sigma/8) = 1 + (\sigma/2) = (1, 1 + \sigma_H) \in \Gamma_2^\circ \times \Delta_2^\circ.$$

Then  $\xi_2\beta_2^{-1} = (i + j + k, (2 + x + y + xy)^{-1}) \in (\mathbb{Z}_2G)^\circ$ , so  $\mathbb{Z}G\xi = \mathbb{Z}G\beta$ . This completes the proof.

For  $G$  a dihedral 2-group, we already know from (50.31) that  $D(\mathbb{Z}G)$  is trivial, whence so is  $T(G)$ . On the other hand, we have:

**(53.18) Theorem. (Endo).** *Let  $G$  be the semidihedral group of order  $2^{n+2}$ ,  $n \geq 2$ , defined by*

$$SD_n = \langle a, b : a^{2^{n+1}} = 1, b^2 = 1, bab^{-1} = a^{2^n - 1} \rangle.$$

*Then  $D(\mathbb{Z}G) = T(G) = \text{group of order 2}$ .*

*Proof.* As in §50D, one shows that  $|D(\mathbb{Z}G)| \leq 2$ . However, the quaternion group of order 8 is a subgroup of  $SD_n$ . Thus  $T(G) \neq 1$  by (53.11) and (53.17). (For details, see Taylor [84].)

Turning to metacyclic groups, we use the results of §50C to prove the following theorem due to Ullom [76]:

**(53.19) Theorem.** *Consider the metacyclic group  $G$  of order  $pq$ , given by*

$$G = \langle x, y : x^p = 1, y^q = 1, yxy^{-1} = x^k \rangle,$$

where  $p$  is an odd prime,  $q$  is any divisor of  $p - 1$ , and  $k$  is a primitive  $q$ -th root of  $1 \pmod{p}$ . Then  $T(G)$  is cyclic of order  $q' = q/(q, 2)$ .

*Proof.* Let  $H = \langle y : y^q = 1 \rangle$  and  $R = \mathbb{Z}[\omega]$ , where  $\omega$  is a primitive  $p$ -th root of 1 over  $\mathbb{Q}$ . As in Step 1 of the proof of Theorem 50.25, where we calculated  $D(\mathbb{Z}G)$ , there is a fiber product

$$\begin{array}{ccc} \mathbb{Z}G & \longrightarrow & \mathbb{Z}H \\ \downarrow & & \downarrow \\ R \circ H & \longrightarrow & \bar{\mathbb{Z}}H, \end{array}$$

where  $\bar{\mathbb{Z}} = \mathbb{Z}/p\mathbb{Z}$ . This gives rise to an exact sequence

$$(R \circ H)^* \xrightarrow{h} (\bar{\mathbb{Z}}H)^* \xrightarrow{\delta} D(\mathbb{Z}G) \xrightarrow{f} D(\mathbb{Z}H),$$

using the fact that  $D(R \circ H) = 0$  by (49.35), since  $R \circ H$  is hereditary.

Since  $f(T(G)) \subseteq T(H)$  by (53.11), and  $T(H) = 0$  by (53.6), we conclude that  $T(G) \subseteq \ker f$ . We shall show below that  $\delta$  maps  $\text{cok } h$  into  $T(G)$ . It will then follow that  $T(G) \cong \text{cok } h$ . Now Step 3 of the proof of (50.25) shows that there is an isomorphism

$$\theta : \text{cok } h \cong \bar{\mathbb{Z}}^*/\{z^{q'} : z \in \bar{\mathbb{Z}}^*\},$$

given by the determinant map. For each  $r \in \mathbb{Z}$  prime to  $p$ , we shall find an element  $\xi \in (\bar{\mathbb{Z}}H)^*$  representing  $\theta^{-1}(r) \in \text{cok } h$ , and such that  $\delta(\xi) \in T(G)$ . Once this is done, we deduce that  $T(G) \cong \text{cok } h \cong$  cyclic group of order  $q'$ , as desired.

Given  $r \in \mathbb{Z}$  prime to  $p$ , we may assume that  $r \equiv 1 \pmod{q}$ . Writing  $r - 1 = qm$ , we choose

$$\xi = 1 + m\sigma_H \in \bar{\mathbb{Z}}H.$$

Since  $\mathbb{Z}$  contains the  $q$ -th roots of 1, it follows that

$$\bar{\mathbb{Z}}H \cong \bar{\mathbb{Z}} \oplus \cdots \oplus \bar{\mathbb{Z}} \quad (q \text{ copies}),$$

and that

$$\xi = (1 + mq, 1, \dots, 1) = (r, 1, \dots, 1).$$

Thus  $\xi \in (\bar{\mathbb{Z}}H)^*$ , and  $\theta(\xi) = r$ .

We now show that  $\delta(\xi) = [r, \sigma] \in T(G)$ . As in (53.8), let  $u = 1 - e + re = 1 + m\sigma/p$ , where  $e = \sigma/pq$ . Then  $u \rightarrow 1 + m\sigma_H \in \mathbb{Z}H$ , and  $u \rightarrow 1$  in  $R \circ H$ , so after identifying  $\mathbb{Q}G$  with  $\mathbb{Q}H \oplus \mathbb{Q}(R \circ H)$ , we may write  $u = (\xi, 1)$ . Note that  $u$  is a

unit in the completions of  $ZH \oplus R \circ H$  at both  $p$  and  $q$ . By Exercise 53.1, we have

$$\delta(\xi) = ZG\gamma, \quad \text{where } \gamma = (\gamma_P), \quad \text{with } \gamma_P = \begin{cases} 1, & P \neq p, \\ (\xi, 1), & P = p, \end{cases}$$

$P$  denoting a variable rational prime. On the other hand,  $\langle r, \sigma \rangle \cong \langle u, \sigma \rangle = ZG\beta$ , where  $\beta = (\beta_P)$  and

$$\beta_P = \begin{cases} 1, & P \neq p, q, \\ u, & P = p \text{ or } P \mid q. \end{cases}$$

Then  $\beta_P = \gamma_P$  if  $P \nmid q$ , while  $\beta_P \gamma_P^{-1} = u \in (Z_P G)^*$  if  $P \mid q$ . Thus  $ZG\beta = ZG\gamma$ , so  $\delta[\xi] = [r, \sigma] \in T(G)$  as claimed, and the proof is finished.

As is evident from the results proved so far in this subsection, there seems to be a close connection between the Artin exponent  $A(G)$  and the Swan subgroup  $T(G)$ , especially when  $G$  is a  $p$ -group. Ullom conjectured that in fact if  $G$  is a noncyclic  $p$ -group, with  $p$  odd, then  $T(G)$  is a cyclic group of order equal to  $A(G)$ . In §54 we shall give M. Taylor's proof of this conjecture, as well as the corresponding result for  $p = 2$ .

For results on  $T(G)$  with  $G$  the symmetric or alternating group, see Endo-Miyata [76].

### §53B. Rings of Integers in Tame Extensions

Let  $K \subseteq L$  be algebraic number fields, with rings of integers  $R \subseteq S$ , and suppose that  $L/K$  is a Galois extension with Galois group  $G$ . We view  $L$  as  $KG$ -module, and  $S$  as  $RG$ -module, as in Example 52.14. As shown there, if  $L/K$  is tamely ramified then  $S$  is projective as  $RG$ -module, and determines a class  $[S] \in \text{Cl } RG$ . Via the restriction homomorphism  $\text{Cl } RG \rightarrow \text{Cl } ZG$ , we may consider  $[S]$  as element of  $\text{Cl } ZG$ . In this subsection, we give the readily accessible proof that  $[S]$  is self-dual in  $\text{Cl } ZG$ . The result is due to Taylor [78c] in a special case, and to Chase [85] for the general case. The proof is a nice application of Swan modules  $\langle r, \sigma \rangle$ , and we follow the treatment in Taylor [84].

Let  $\check{S}$  be the contragredient of the  $RG$ -module  $S$  (see §10D), so

$$\check{S} = \text{Hom}_{RG}(S, RG) \cong \text{Hom}_R(S, R).$$

Each element of  $\text{Hom}_K(L, K)$  is given by  $x \in L \mapsto T_{L/K}(ax) \in K$ , for some  $a \in L$ , where  $T_{L/K}$  is the trace map. It follows that we may identify  $\check{S}$  with the *inverse different* (see §4B)

$$\mathfrak{D}^{-1}(S/R) = \{a \in L : T_{L/K}(aS) \subseteq R\}.$$

Assuming hereafter that  $L/K$  is tamely ramified, both  $S$  and  $\mathfrak{D}^{-1}(S/R) \cong \check{S}$  are

$RG$ -projective, and so (using the restriction map from  $\text{Cl } RG$  to  $\text{Cl } ZG$ ) they determine elements of  $\text{Cl } ZG$ . The main result is:

**(53.20) Theorem (Taylor, Chase).** *For  $L/K$  tamely ramified,*

$$[S] = [\check{S}] = [\mathfrak{D}^{-1}(S/R)] \text{ in } \text{Cl } ZG.$$

To begin the proof, consider the torsion  $RG$ -module

$$T = \frac{\mathfrak{D}^{-1}(S/R)}{S},$$

of homological dimension 1 over  $RG$ . Identifying  $\text{Cl } RG$  with the kernel of the homomorphism  $K_0(RG) \rightarrow K_0(KG)$  (see (49.11iv)), we have a surjection  $K_0(\mathcal{T}) \rightarrow \text{Cl } RG$ , where  $\mathcal{T}$  is the category of all  $R$ -torsion f.g.  $RG$ -modules of finite homological dimension. Then the image of  $T$  in  $\text{Cl } RG$  is  $[\mathfrak{D}^{-1}(S/R)] - [S]$ , and we must show this equals zero in  $\text{Cl } ZG$ .

Let  $P$  range over the maximal ideals of  $R$ . Then  $T = \bigoplus T_P$ , a finite direct sum of  $P$ -adic completions, and

$$T_P = \frac{\mathfrak{D}^{-1}(S_P/R_P)}{S_P}.$$

It suffices to show that each  $T_P$  has zero image in  $\text{Cl } ZG$ . Keep  $P$  fixed, and let us use the notation following (50.67). Thus

$$PS = (P_1 \cdots P_g)^e, \quad \text{and } p/e \text{ (since } L/K \text{ is tame),}$$

where  $p = \text{characteristic of } R/P$ . By Exercise 4.11, we have

$$\mathfrak{D}(S_P/R_P) = (P_1 \cdots P_g)^{e-1},$$

so now

$$T_P = (P_1 \cdots P_g)^{-(e-1)} S_P / S_P \cong \coprod_{i=1}^g P_i^{-(e-1)} S_i / S_i,$$

where  $S_i$  is the  $P_i$ -adic completion of  $S$ . Let  $D$  be the decomposition group of  $P_1$ , so  $D = \{\sigma \in G : \sigma P_1 = P_1\} \cong \text{Gal}(L_1/K_P)$ , where  $L_i$  is the  $P_i$ -adic completion of  $L$ . Since  $G$  acts transitively on the  $\{P_i\}$ , it is easily seen that

$$T_P \cong R_P G \otimes_{R_P D} (P_1^{-(e-1)} S_1 / S_1).$$

It thus suffices to prove that  $P_1^{-(e-1)} S_1 / S_1$  has zero image in  $\text{Cl } ZD$ .

Replacing  $G$  by  $D$  and then changing notation, we assume hereafter that  $g = 1$  and  $PS = P_1^e$ . Let  $T_1 = P_1^{-(e-1)} / S_1$ ; we must show that in the composite

map  $K_0(\mathcal{T}) \rightarrow \text{Cl } RG \rightarrow \text{Cl } ZG$ , the image of  $T_1$  in  $\text{Cl } ZG$  is zero. As in the discussion on pages 295, 296, let

$$G_0 = \{\sigma \in G : \sigma(x) \equiv x \pmod{P_1} \text{ for all } x \in S\}$$

be the inertia group of  $P_1$  in the extension  $L/K$ . Let  $L_0$  be the subfield of  $L$  fixed by  $G_0$ ; then  $L_0/K$  is unramified, while  $L/L_0$  is tamely ramified with ramification index  $e = |G_0|$ . Furthermore,  $G_0$  is a cyclic group, and  $S/P_1 \cong S_0/PS_0$ . Therefore

$$\frac{S}{PS + S_0} \cong \frac{P_1 + S_0}{PS + S_0} \cong \frac{P_1}{PS} \cong \frac{P_1^{-(e-1)}}{S} = T_1,$$

where these are  $RG$ -isomorphisms. In computing  $S/(PS + S_0)$  we may first localize at  $P$ , and then assume that  $S_P \cong R_P G$  since  $L/K$  is tamely ramified at  $P$ . We thus obtain

$$T_1 \cong \frac{RG}{P \cdot RG + RG\sigma_0}, \quad \text{where } \sigma_0 = \sum_{x \in G_0} x,$$

since  $RG\sigma_0$  is the  $G_0$ -trivial submodule of  $RG$ . It follows that

$$T_1 \cong RG \otimes_{RG_0} W, \quad \text{where } W = RG_0/(P \cdot RG_0 + R\sigma_0) \cong \bar{R}G_0/\bar{R}\sigma_0,$$

and where  $\bar{R} = R/P$ . Since  $\bar{R} \cong \mathbb{Z}^{(f)}$ , where  $\bar{\mathbb{Z}} = \mathbb{Z}/p\mathbb{Z}$  and  $f = \dim_{\mathbb{Z}} \bar{R}$ , we conclude that

$$W \cong \{\mathbb{Z}G_0/\langle p, \sigma_0 \rangle\}^{(f)} \text{ as } \mathbb{Z}G_0\text{-modules.}$$

Here,  $\langle p, \sigma_0 \rangle$  is a Swan submodule of  $\mathbb{Z}G_0$ , noting that  $(p, |G_0|) = 1$ . But  $\langle p, \sigma_0 \rangle$  is  $\mathbb{Z}G_0$ -free since  $G_0$  is cyclic, so the image of  $W$  in  $\text{Cl } ZG_0$  is zero, and therefore  $T_1$  has zero image in  $\text{Cl } ZG$ . This completes the proof.

For generalizations of the above theorem to the case where  $L/K$  is an arbitrary Galois extension, not necessarily tame, see Cassou-Noguès and Queyrut [82], and Desrochers [84].

### §53C. Generalized Swan Subgroups

We describe here some results of Oliver [78], showing that for a finite group  $G$ , the kernel group  $D(ZG)$  can be generated by certain “generalized” Swan subgroups. These were first defined by Matchett [76] as follows: let  $H \trianglelefteq G$  and set  $h = |H|$ , and

$$\sigma_H = \sum_{x \in H} x, \quad e = h^{-1}\sigma_H.$$

Starting with the fiber product

$$\begin{array}{ccc} \mathbb{Z}H & \longrightarrow & \mathbb{Z}H/\mathbb{Z}\sigma_H \\ \downarrow & & \downarrow \\ \mathbb{Z} & \longrightarrow & \bar{\mathbb{Z}}, \end{array}$$

where  $\bar{\mathbb{Z}} = \mathbb{Z}/h\mathbb{Z}$ , we apply the induction map  $\mathbb{Z}G \otimes_{\mathbb{Z}H} \cdot$  to obtain a new fiber product

$$\begin{array}{ccc} \mathbb{Z}G & \longrightarrow & \mathbb{Z}G/\mathbb{Z}G\sigma_H \\ \downarrow & & \downarrow \\ \mathbb{Z}(G/H) & \longrightarrow & \bar{\mathbb{Z}}(G/H). \end{array}$$

This gives rise to the exact Mayer-Vietoris sequence

$$K_1(\bar{\mathbb{Z}}(G/H)) \xrightarrow{\partial} D(\mathbb{Z}G) \rightarrow D(\mathbb{Z}G/\mathbb{Z}G\sigma_H) \oplus D(\mathbb{Z}(G/H)) \rightarrow 0,$$

and we define

$$T_H(G) = \text{image of } \partial \text{ in } D(\mathbb{Z}G) = \text{generalized Swan subgroup.}$$

We now state without proof some functorial properties of  $T_H(G)$ , proved by Matchett [76], which generalize (53.10) and (53.11):

- (1) Let  $G \rightarrow \bar{G}$  be a surjection of groups, and let  $N \trianglelefteq G$  map onto  $\bar{N} \trianglelefteq \bar{G}$ . Then there is a surjection  $T_N(G) \rightarrow T_{\bar{N}}(\bar{G})$ .
- (2) Let  $N \trianglelefteq G$ , and suppose that  $G = HN$  for some subgroup  $H$  of  $G$ . Then the restriction map  $\text{res}_H^G$  carries  $T_N(G)$  onto  $T_{N \cap H}(H)$ .

Oliver extended the definition of  $T_H(G)$  to the case where  $H$  is an arbitrary subgroup of  $G$ , not necessarily normal. Let  $N = N_G(H)$ , so by the above  $T_H(N)$  is a well defined subgroup of  $D(\mathbb{Z}N)$ . Extending the previous definition, we set

$$T_H(G) = \text{ind}_N^G T_H(N),$$

so  $T_H(G)$  is the image of the composite map

$$K_1(\bar{\mathbb{Z}}(N/H)) \rightarrow D(\mathbb{Z}N) \xrightarrow{\text{ind}_N^G} D(\mathbb{Z}G).$$

Then we have<sup>†</sup>:

**(53.21) Oliver's Theorem.** *For any finite group  $G$ , we have*

$$D(\mathbb{Z}G) = \sum_{H \leq G} T_H(G).$$

<sup>†</sup>Wilson's Theorem 50.64 plays a key role in the proof of (53.21).

In fact, it suffices to let  $H$  range over all subgroups of  $G$  of prime power order.

Oliver also gave an example showing that the analogous result fails, when  $\mathbb{Z}$  is replaced by a ring of algebraic integers. For details, and for the proof of the above theorem, see Oliver [78].

### §53. Exercises

1. Consider a fiber product of rings

$$\begin{array}{ccc} \Lambda & \longrightarrow & \Lambda' \\ \downarrow & & f \downarrow \\ \Lambda'' & \longrightarrow & \bar{\Lambda} \end{array}$$

where  $\Lambda, \Lambda'$ , and  $\Lambda''$  are  $\mathbb{Z}$ -orders, and  $\bar{\Lambda}$  is  $\mathbb{Z}$ -torsion. Given  $a \in \bar{\Lambda}$ , define

$$M = \{(x, y) \in \Lambda' \oplus \Lambda'': \bar{y} = \bar{x}a \text{ in } \bar{\Lambda}\}.$$

Show that  $M = \Lambda\alpha$ , where  $\alpha = (\alpha_p)$  is the idèle whose components are given by

$$\alpha_p = \begin{cases} (1, 1) \in \Lambda'_p \oplus \Lambda''_p & \text{if } \bar{\Lambda}_p = 0, \\ (u_p, 1) \in \Lambda'_p \oplus \Lambda''_p & \text{if } \bar{\Lambda}_p \neq 0, \end{cases}$$

where in the second case,  $u_p$  is an element of  $\Lambda'_p$  such that  $f(u_p) = a$  in  $\bar{\Lambda}_p$ . Note that in the Mayer-Vietoris sequence

$$\bar{\Lambda} \xrightarrow{\delta} D(\Lambda) \rightarrow D(\Lambda') \oplus D(\Lambda''),$$

we have for  $a \in \bar{\Lambda}$ ,

$$\delta(a) = [M] = [\Lambda\alpha] \in D(\Lambda).$$

2. Let  $(r, n) = 1$ , where  $|G| = n$ . Prove that

$$\langle r, \alpha \rangle \oplus \mathbb{Z} \cong \mathbb{Z}G \oplus \mathbb{Z}.$$

[Hint: There are exact sequences

$$0 \rightarrow \mathbb{Z}G \xrightarrow{r} \langle r, \sigma \rangle \rightarrow \mathbb{Z}/r\mathbb{Z} \rightarrow 0, 0 \rightarrow \mathbb{Z} \xrightarrow{r} \mathbb{Z} \rightarrow \mathbb{Z}/r\mathbb{Z} \rightarrow 0.$$

Now use Roiter's Lemma 31.8.]

3. Show that  $T(G) = 0$  for a dihedral group  $G$ .

[Hint (Oliver): Let  $G = \langle a, b : a^n = b^2 = 1, bab^{-1} = a^{-1} \rangle$ , and let  $2k + 1$  be relatively prime to  $n$ . Define

$$u_k = 1 + a + \cdots + a^k + b + ab + \cdots + a^{k-1}b \in \mathbb{Z}G/(\sigma).$$

Then  $u_k$  depends only on the class of  $k(\text{mod } n)$ , and under the map  $\mathbb{Z}G/(\sigma) \rightarrow \mathbb{Z}/2n\mathbb{Z}$ , the image of  $u_k$  is  $2k+1$ . It suffices to show that  $u_k$  is a unit in  $\mathbb{Z}G/(\sigma)$ . But

$$(1 + a^{2k}b + a^{2k+1})u_k = u_{k+(2k+1)},$$

$$(1 + a^{2k}b + a^{2k+1} + a^{4k}b + a^{4k+1})u_k = u_{k+2(2k+1)},$$

and so on, so  $u_k$  is a unit. (Also see (53.19)).]

## §54. $p$ -ADIC LOGARITHMS AND TAYLOR'S THEOREM

This section is devoted to the proof of a theorem of M. Taylor [80] which asserts that for a finite  $p$ -group  $G$ , the Swan subgroup  $T(G)$  of the class group  $\text{Cl } \mathbb{Z}G$  is cyclic of order equal to the Artin exponent  $A(G)$  (or  $A(G)/2$  if  $p=2$  with some exceptions). The method used involves a modified version of the  $p$ -adic logarithm, which is crucial not only to the determination of the Swan subgroup, but is also a key tool in problems in algebraic number theory connected with the existence of normal integral bases. For this latter application, we refer the reader to Fröhlich [83], as well as the articles by Taylor listed in the bibliography therein.

We begin with a review of the  $p$ -adic logarithm and  $p$ -adic exponential function. Until further notice, let  $K$  be a  $p$ -adic field (= finite extension of  $\mathbb{Q}_p$ ) with valuation ring  $R$ , and let  $P$  be the maximal ideal of  $R$ . Let  $v$  denote the exponential valuation on  $K$ , *normalized* so that  $v(p)=1$ , and thus the smallest positive value of  $v$  on  $K$  is  $1/e$ , where  $e$  is the ramification index of  $K$  over  $\mathbb{Q}_p$ . Consider the series

$$(54.1) \quad \log(1+x) = \sum_{n=1}^{\infty} (-1)^{n-1}x^n/n, \quad \text{and} \quad \exp x = \sum_{n=0}^{\infty} x^n/n!,$$

for  $x \in R$ . Since  $v$  is non-archimedean, a series  $\sum a_n$  converges if and only if  $\lim_{n \rightarrow \infty} v(a_n) = \infty$ . The following is a well-known result:

**(54.2) Proposition.** (i) *The series for  $\log(1+x)$  converges to an element of  $K$  for all  $x \in P$ . If  $v(x) \geq 1$ , then  $\log(1+x) \in pR$ .*

(ii) *The series for  $\exp x$  converges to an element of  $1+P$  whenever  $v(x) > 1/(p-1)$ . For  $p$  odd, if  $v(x) \geq 1$  then  $\exp x \in 1+pR$ .*

(iii) *For  $p$  odd, we have*

$$\exp(\log(1+x)) = 1+x, \quad \log(\exp x) = x \quad \text{for } v(x) \geq 1.$$

*Proof.* (i) If  $p^k \parallel n$ , then  $v(n) = k \leq (\log n)/(\log p)$ . For  $x \in R$ , this gives

$$v(x^n/n) = nv(x) - v(n) \geq nv(x) - (\log n)/(\log p).$$

Thus the series for  $\log(1+x)$  converges for  $v(x) > 0$ , that is, for  $x \in P$ . If  $v(x) \geq 1$  then  $v(x^n/n!) \geq 1$  for  $n \geq 1$ , so  $\log(1+x) \in pR$ .

(ii) For  $n > 0$  we have  $v(x^n/n!) = nv(x) - v(n!)$ . But

$$v(n!) = \left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \cdots \leq \frac{n}{p} + \frac{n}{p^2} + \cdots < \frac{n}{p-1},$$

where brackets is the “greatest integer” function. Thus

$$v(x^n/n!) > n \left( v(x) - \frac{1}{p-1} \right) \text{ for } n > 0.$$

This shows that  $\exp x$  converges for  $v(x) > 1/(p-1)$ , and that  $\exp x \in 1 + P$ . For odd  $p$ ,  $v(x) \geq 1$  implies that  $v(x^n/n!) \geq 1$  for  $n > 0$ , so  $\exp x \in 1 + pR$ .

Assertion (iii) follows from the usual manipulations with series.

**(54.3) Remarks.** (i) For  $x, y \in P$ ,

$$\log(1+x)(1+y) = \log(1+x) + \log(1+y).$$

(ii) If  $x, y \in R$  are such that  $v(x) > 1/(p-1)$  and  $v(y) > 1/(p-1)$ , then

$$\exp(x+y) = (\exp x)(\exp y).$$

(iii) For  $p = 2$ , the equalities in (54.2.iii) hold whenever  $v(x) \geq 2$ .

(iv) Let  $\omega \in R$  be a  $p^m$ -th root of 1, where  $m > 0$ . Then  $1 - \omega \in P$ , so  $\log \omega = \log(1 + (\omega - 1))$  converges. But then

$$0 = \log \omega^{p^m} = p^m \log \omega,$$

so  $\log \omega = 0$ . Note that  $\omega \neq \exp(\log \omega)$ .

(v) Let  $x \in 1 + P$  be such that  $\log x = 0$ . We claim that  $x$  must be a  $p$ -power root of 1. Choose  $m$  large enough that  $x^{p^m} \in 1 + p^2R$ . Then  $\log x^{p^m} = p^m \log x = 0$ , and

$$x^{p^m} = \exp(\log x^{p^m}) = 1,$$

so  $x$  is a  $p^m$ -th root of 1.

(vi) For odd  $p$ ,  $1 + pR$  contains no nontrivial  $p$ -power root of 1, since for such a root  $x$  we would have  $x = \exp \log x = 1$ . Likewise,  $1 + 4R$  contains no nontrivial 2-power root of 1.

From now on, let  $\Lambda$  be an  $R$ -order in a f.d.  $K$ -algebra  $A$ , and let  $J = \text{rad } \Lambda$ .

By (5.22) we have

$$J^l \subseteq P\Lambda \subseteq J \quad \text{for some } l > 0.$$

It follows readily from the proof of (54.2) that  $\log(1+x)$  converges to an element of  $A$  for all  $x \in J$ , and that

$$\log(1+x) \in p\Lambda \quad \text{for } x \in p\Lambda.$$

Likewise, for  $p$  odd,  $\exp x$  converges to an element of  $1 + p\Lambda$  for all  $x \in p\Lambda$ ; for  $p = 2$ ,  $\exp x$  converges to an element of  $1 + J$  if  $x \in pJ$ , and to an element of  $1 + p\Lambda$  if  $x \in p^2\Lambda$ . Again,  $\log$  and  $\exp$  are inverse functions when the convergence conditions are satisfied.

If  $A$  is noncommutative, formulas such as  $\log uv = \log u + \log v$  may break down because  $u$  and  $v$  need not commute. To overcome this difficulty, we introduce the quotient space

$$\bar{A} = A \left/ \sum_{x,y \in A} K(xy - yx) \right..$$

Generally speaking,  $\bar{A}$  is a  $K$ -space but not a ring. There is a canonical surjection  $A \rightarrow \bar{A}$  of  $K$ -spaces, but this need not be a ring homomorphism.

Assume hereafter that  $A = KG$ ,  $\Lambda = RG$ , where  $G$  is a finite group, and set

$$\bar{A} = KG \left/ \sum_{x,y \in G} K(xy - yx) \right., \quad \bar{\Lambda} = RG \left/ \sum_{x,y \in G} R(xy - yx) \right..$$

As we have seen in (32.3),  $\bar{\Lambda}$  is isomorphic to the free  $R$ -module spanned by symbols  $\{\mathfrak{C}_x\}$ , one for each conjugacy class in  $G$ . We may thus view  $\bar{\Lambda}$  as embedded in  $\bar{A}$ . Let  $y \in A \rightarrow \bar{y} \in \bar{A}$ ; then for each  $\zeta \in \text{ch } G$ , the value  $\zeta(y)$  depends only on  $\bar{y}$ , and we may write  $\zeta(\bar{y})$  instead of  $\zeta(y)$  if we wish.

We now introduce Taylor's modified version of the  $p$ -adic logarithm for group rings  $RG$ , where  $R$  is a  $p$ -adic ring and  $G$  is a  $p$ -group. For this purpose, we impose the extra hypothesis that  $K/\mathbb{Q}_p$  is unramified, so  $pR$  is the maximal ideal of  $R$ , and  $K/\mathbb{Q}_p$  is a Galois extension. The Galois group  $\text{Gal}(K/\mathbb{Q}_p)$  is cyclic, and is generated by the *Frobenius automorphism*  $F$  (see Volume I, p. 95, or proof of (45.15)). This automorphism is characterized by the property

$$F(\alpha) \equiv \alpha^p \pmod{pR} \quad \text{for all } \alpha \in R.$$

In the special case where  $K = \mathbb{Q}_p$ , we have  $F = 1$ , and the above congruence is the familiar Fermat Theorem;

$$a^p \equiv a \pmod{p\mathbb{Z}_p} \quad \text{for all } a \in \mathbb{Z}_p.$$

Let us now define a  $\mathbb{Q}_p$ -linear endomorphism  $\theta$  of  $KG$ , by the formula

$$\theta\left(\sum_{x \in G} \alpha_x x\right) = \sum_{x \in G} F(\alpha_x) x^p.$$

Note that  $\theta$  is *not* a ring homomorphism, and  $\theta$  is *not*  $K$ -linear if  $f \neq 1$ .

Now let

$$J = \text{rad } RG = I(RG) + pRG,$$

where  $I$  = augmentation ideal. Then  $1 + J$  is a multiplicative subgroup of  $(RG)^*$ . We define a modified logarithmic map

$$L_0: 1 + J \rightarrow KG$$

by the formula

$$(54.4) \quad L_0(1 - y) = -p \sum_{n=1}^{\infty} \frac{y^n}{n} + \sum_{n=1}^{\infty} \frac{\theta(y^n)}{n}, \quad y \in J.$$

Since  $y^l \in pRG$  for some  $l > 0$ , it is easily verified that the above series converge to elements of  $KG$ . Let  $\bar{L}_0(1 - y)$  denote the image of  $L_0(1 - y)$  in  $\overline{KG}$ , and set

$$L(1 - y) = \bar{L}_0(1 - y) \in \overline{KG}.$$

We intend to prove that  $L$  gives a homomorphism:

$$L(uv) = L(u) + L(v) \quad \text{for } u, v \in 1 + J.$$

At first glance this seems obvious, since by passing from  $A$  to  $\bar{A}$ , we have removed the obstacle arising from noncommutativity. However, this heuristic argument breaks down because  $\bar{A}$  is not a factor *ring* of  $A$ , but just a quotient space.

We now prove the following result of Taylor [78c]:

**(54.5) Theorem.** *Let  $R$  be an unramified extension of  $\mathbb{Z}_p$ , with Frobenius automorphism  $F$ . Let  $G$  be a  $p$ -group, and set  $J = \text{rad } RG$ . Let  $\theta$  be the  $\mathbb{Z}_p$ -linear endomorphism of  $RG$  defined by*

$$\theta\left(\sum_{x \in G} \alpha_x x\right) = \sum_{x \in G} F(\alpha_x) x^p.$$

*For each  $y \in J$ , let*

$$L(1 - y) = \bar{L}_0(1 - y), \quad \text{where } L_0(1 - y) = -p \sum_{n=1}^{\infty} \frac{y^n}{n} + \sum_{n=1}^{\infty} \frac{\theta(y^n)}{n},$$

and where  $\bar{L}_0$  denotes the image of  $L_0$  in  $\overline{KG} = KG/\sum_{x,y \in G} K(xy - yx)$ . Then for  $u, v \in 1 + J$  we have  $L(u), L(v) \in p\overline{RG}$ , and

$$L(uv) = L(u) + L(v).$$

*Proof.* Step 1. Let  $E \supset K$  be a splitting field for  $G$ , and identify the character ring  $\text{ch } G$  with the ring  $\text{ch } EG$  of virtual characters of  $G$  afforded by  $EG$ -modules. Let  $\psi$  be the  $p$ -th Adams operator on  $\text{ch } G$ , defined by

$$(\psi(\zeta))x = \zeta(x^p) \quad \text{for } x \in G, \quad \zeta \in \text{Irr } G$$

(see §12B). Then by (12.10),  $\psi$  is an endomorphism of the ring  $\text{ch } G$ .

Let  $\mathbf{T}$  be an  $E$ -representation of  $G$ , affording the character  $\tau$ . Let  $S$  be the valuation ring of  $E$ , with maximal ideal  $P'$ . We may assume  $\mathbf{T}$  chosen so that the matrices  $\{\mathbf{T}(x) : x \in G\}$  have entries in  $S$ . By definition,

$$\det_{\tau} y = \det \mathbf{T}(y), \quad y \in KG,$$

and  $\det_{\tau} y$  is independent of the choice of  $\mathbf{T}$  affording the given character  $\tau$ . If  $\tau'$  is another character of  $G$ , then (by definition)

$$\det_{\tau-\tau'}(y) = (\det_{\tau} y) / (\det_{\tau'} y) \quad \text{for } y \in (KG)^*.$$

Suppose now that  $x \in J$ , so  $1 - x \in (RG)^*$ . Then  $\mathbf{T}(1 - x) = \mathbf{I} - \mathbf{T}(x)$ . Since  $x^l \in pRG$  for some  $l > 0$ , it follows that  $\mathbf{T}(x)^l$  has entries in  $pS$ , and therefore

$$\det_{\tau}(1 - x) = \det(\mathbf{I} - \mathbf{T}(x)) \equiv 1 \pmod{P'}$$

It follows from (54.2) that the series for  $\log \det_{\tau}(1 - x)$  converges to an element of  $E$ . Indeed, this holds for each  $\tau \in \text{ch } G$ .

We now extend the Frobenius automorphism  $F$  of  $K/\mathbb{Q}_p$  to a ring automorphism  $x \rightarrow x^F$  of  $KG$ . Note that  $F$  is an automorphism of  $RG$  which carries  $J$  onto itself. It follows from the above discussion that for  $x \in J$ , the series for  $\log \det_{\tau}(1 - x^F)$  converges in  $E$ , for each virtual character  $\tau \in \text{ch } G$ .

Step 2. Keep the above notation. We shall show, for each  $\zeta \in \text{ch } G$  and  $x \in J$ , that

$$(54.6) \quad \zeta(L_0(1 - x)) = \log \{\det_{p\zeta}(1 - x) \cdot \det_{-\psi(\zeta)}(1 - x^F)\}.$$

Here,  $\psi(\zeta)$  is the  $p$ -th Adams operator  $\psi$  applied to  $\zeta$ , while  $p\zeta$  is  $\zeta + \cdots + \zeta$  ( $p$  copies).

To begin with, both sides of (54.6) are additive in  $\zeta$ , by virtue of (54.3i). It therefore suffices to consider the case where  $\zeta \in \text{Irr } G$ . Let  $\mathbf{T}: G \rightarrow GL_d(S)$  be a representation affording the character  $\zeta$ , and extend  $\mathbf{T}$  to a  $K$ -algebra homomorphism

$$\mathbf{T}: KG \rightarrow M_d(E)$$

by linearity. For  $x \in J$ , the eigenvalues  $\{a_j\}$  of  $\mathbf{T}(x)$  lie in the valuation ring of some finite extension of  $E$ , and each  $v(a_j) > 0$  since  $x \in J$ . We have

$$\text{char. pol. } \mathbf{T}(x) = \det(\lambda \mathbf{I}_d - \mathbf{T}(x)) = \prod_{j=1}^d (\lambda - a_j),$$

where  $\lambda$  is an indeterminate. Therefore

$$\det_\zeta(1-x) = \det \mathbf{T}(1-x) = \det(\mathbf{I} - \mathbf{T}(x)) = \prod_{j=1}^d (1-a_j).$$

We may then take  $p$ -adic logs of both sides, obtaining

$$\log \det_\zeta(1-x) = - \sum_{j=1}^d \sum_{n=1}^\infty \frac{a_j^n}{n} = - \sum_{n=1}^\infty \frac{1}{n} \left( \sum_j a_j^n \right).$$

Since  $\mathbf{T}(x^n)$  has eigenvalues  $\{a_j^n\}$ , we have

$$\sum_{j=1}^d a_j^n = \text{trace } \mathbf{T}(x^n) = \zeta(x^n),$$

by definition of the character  $\zeta$  afforded by  $\mathbf{T}$ . Thus for  $x \in J$ ,

$$(54.7) \quad \log \det_\zeta(1-x) = - \sum_{n=1}^\infty \zeta(x^n)/n = \zeta \left( - \sum_{n=1}^\infty x^n/n \right).$$

We shall use this formula twice, once with  $\zeta$  replaced by  $p\zeta$ , the second time with  $-\psi(\zeta)$  in place of  $\zeta$ . We obtain

$$\begin{aligned} \log \det_{p\zeta}(1-x) &= p\zeta(-\sum x^n/n) = \zeta(-p \sum x^n/n), \\ \log \det_{-\psi(\zeta)}(1-x^F) &= \psi(\zeta) \{ \sum F(x^n)/n \} = \zeta(\sum \theta(x^n)/n), \end{aligned}$$

the last equality holding because of the definitions of  $\psi(\zeta)$  and  $\theta$ . But then (54.6) follows, by adding the above two formulas.

*Step 3.* Now let  $u, v \in 1 + J$ . For any  $\zeta \in \text{ch } G$  we have

$$\det_\zeta(uv) = (\det_\zeta u)(\det_\zeta v),$$

and therefore

$$\log \det_\zeta(uv) = \log \det_\zeta u + \log \det_\zeta v.$$

Since  $(uv)^F = u^F v^F$ , it follows from (54.6) that

$$\zeta(L_0(uv)) = \zeta(L_0(u)) + \zeta(L_0(v)).$$

But for  $x \in KG$ , the value  $\zeta(x)$  depends only on the image  $\bar{x} \in \overline{KG}$ , since  $\zeta$  is a class function. Thus

$$\zeta(L(uv)) = \zeta(L(u)) + \zeta(L(v)) \quad \text{for all } \zeta \in \text{Irr } G.$$

However, the irreducible characters of  $G$  form a basis for the ring of class functions on  $G$ , and so we conclude that

$$L(uv) = L(u) + L(v) \quad \text{for } u, v \in 1 + J,$$

as desired.

*Step 4.* Now let  $u = 1 - y$ , where  $y \in J$ . It remains for us to verify that  $L(1 - y) \in p\overline{RG}$ , where

$$\overline{RG} = RG \left/ \sum_{x, z \in G} R(xz - zx) \right..$$

By definition,  $L(1 - y)$  is the image in  $\overline{KG}$  of

$$-p \sum_{n=1}^{\infty} \frac{y^n}{n} + \sum_{n=1}^{\infty} \frac{\theta(y^n)}{n},$$

which is an element of  $KG$ . We remark that  $K \otimes_R \overline{RG} \cong \overline{KG}$ , since  $\overline{RG}$  is  $R$ -free (see (32.3)). Since  $py^n/n \in p\overline{RG}$  whenever  $p \nmid n$ , we may ignore the terms in the first series for which  $p \nmid n$ . Thus, we must show

$$\sum_{n=1}^{\infty} \frac{\theta(y^n) - y^{pn}}{n} \in p\overline{RG},$$

after taking the image of the left-hand side in  $\overline{RG}$ . Let  $p^{m-1} \parallel n$ , and write  $n = p^{m-1}n_0$ , where  $p \nmid n_0$ . Setting  $x = y^{n_0}$ , we have  $y^n = x^{p^{m-1}}$ , so we need only prove

$$(54.8) \quad \theta(x^{p^{m-1}}) - x^{p^m} \in p^m \overline{RG} \quad \text{for } x \in J, \quad m \geq 1,$$

where again the left side must be viewed as element of  $\overline{RG}$ . We shall establish the above relation by grouping terms in  $x^{p^m}$  and  $\theta(x^{p^{m-1}})$  so that their difference has the desired congruence property in  $\overline{RG}$ .

Let us write  $x = \sum a_i g_i$ ,  $a_i \in R$ ,  $g_i \in G$ . Then for  $m \geq 1$ ,

$$x^{p^m} = \sum a_{j_1} \cdots a_{j_{p^m}} g_{j_1} \cdots g_{j_{p^m}},$$

where  $\{j_1, \dots, j_{p^m}\}$  ranges over all permutations of  $\{1, \dots, p^m\}$ . In this expansion of  $x^{p^m}$ , let us consider the subsum  $\xi$  of all terms in which  $\{j_1, \dots, j_{p^m}\}$  is a cyclic

permutation of some fixed  $p^m$ -tuple  $\{i_1, \dots, i_{p^m}\}$ . Then

$$\prod g_{j_\mu} \text{ is conjugate to } \prod g_{i_\mu} \text{ in } G,$$

so all of the terms in the subsum  $\xi$  have the same image in  $\overline{RG}$ . Now let  $H$  be a cyclic group of order  $p^m$ , which permutes  $p^m$ -tuples cyclically, and suppose there are precisely  $p^t$  elements of  $H$  which fix the  $p^m$ -tuple  $\{i_1, \dots, i_{p^m}\}$ . Then there are precisely  $p^{m-t}$  distinct cyclic arrangements of this  $p^m$ -tuple, and we may write

$$a_{i_1} \cdots a_{i_{p^m}} g_{i_1} \cdots g_{i_{p^m}} = \alpha^{p^t} g^{p^t},$$

where

$$(54.9) \quad \alpha = a_{i_1} \cdots a_{i_{p^{m-t}}}, \quad g = g_{i_1} \cdots g_{i_{p^{m-t}}}.$$

It follows that in  $\overline{RG}$ ,

$$\bar{\xi} = p^{m-t} \alpha^{p^t} \bar{g}^{p^t},$$

since conjugate elements of  $G$  have the same image in  $\overline{RG}$ .

Now consider the assertion (54.8) which we are trying to establish. For any subsum  $\xi$  of  $x^{p^m}$  such that  $t = 0$ , we already know that  $\bar{\xi} \in p^m \overline{RG}$ , by the above formula for  $\bar{\xi}$ . On the other hand, we show that for every subsum  $\xi$  such that  $t \geq 1$ , there is a corresponding subsum  $\theta(\xi')$  in  $\theta(x^{p^{m-1}})$  such that  $\overline{\theta(\xi')} - \bar{\xi} \in p^m \overline{RG}$ . Indeed, let  $\xi'$  be the subsum of  $x^{p^{m-1}}$  consisting of all terms

$$a_{j_1} \cdots a_{j_{p^{m-1}}} g_{j_1} \cdots g_{j_{p^{m-1}}}$$

for which  $\{j_1, \dots, j_{p^{m-1}}\}$  is a cyclic permutation of  $\{i_1, \dots, i_{p^{m-1}}\}$ . There are now  $p^{t-1}$  elements of the cyclic group  $\bar{H}$  of order  $p^{m-1}$  which stabilize  $\{i_1, \dots, i_{p^{m-1}}\}$ , and thus there are  $p^{(m-1)-(t-1)}$  distinct cyclic arrangements of this  $p^{m-1}$ -tuple. We may thus write  $\xi'$  as a sum of terms

$$\xi' = \alpha^{p^{t-1}} g^{p^{t-1}} + \cdots,$$

where the dots indicate conjugates of  $g^{p^{t-1}}$ , and where  $\alpha, g$  are as in (54.9). Then

$$\theta(\xi') = F(\alpha^{p^{t-1}}) g^{p^t} + \cdots, \quad \text{and} \quad \overline{\theta(\xi')} = p^{m-t} F(\alpha^{p^{t-1}}) \bar{g}^{p^t}.$$

Since  $F(\alpha) \equiv \alpha^p \pmod{pR}$ , we obtain readily (by induction on  $t$ )

$$F(\alpha^{p^{t-1}}) \equiv \alpha^{p^t} \pmod{p^t R}.$$

Therefore

$$\overline{\theta(\xi')} \equiv p^{m-t} \alpha^{p^t} \bar{g}^{p^t} = \bar{\xi} \pmod{p^m \overline{RG}},$$

so  $\overline{\theta(\zeta') - \zeta} \in p^m \overline{RG}$ . This completes the proof of (54.8), and establishes Theorem 54.5.

Before giving some easy consequences of the above theorem, we introduce some notation. For  $\zeta \in \text{ch } G$ , we write

$$(54.10) \quad \zeta \equiv 0 \pmod{p^k} \quad \text{if and only if } \zeta(x) \equiv 0 \pmod{p^k} \quad \text{for all } x \in G.$$

Then we have

**(54.11) Corollary.** *Let  $k \geq 0$  and suppose  $\zeta \in \text{ch } G$  satisfies  $\zeta \equiv 0 \pmod{p^k}$ . Then*

$$\zeta(x^{p^m}) \equiv \psi(\zeta)(x^{p^{m-1}}) \pmod{p^{m+k}} \quad \text{for } x \in Z_p G \quad \text{and} \quad m \geq 1.$$

*Proof.* In Step 4 of the preceding proof, we showed that

$$\theta(x^{p^{m-1}}) - x^{p^m} \in p^m \overline{RG}$$

for each  $x \in RG$ , where the left-hand side is viewed as element of  $\overline{RG}$ . (The hypothesis  $x \in J$  was not used in proving (54.8). If  $\zeta$  is afforded by an  $S$ -representation of  $G$  (as in the preceding proof), we conclude that

$$\zeta(\theta(x^{p^{m-1}})) - \zeta(x^{p^m}) \in p^m \zeta(\overline{RG}) \subseteq p^{m+k} S.$$

Now choose  $R = Z_p$ , so  $F = 1$  and thus

$$\zeta(\theta(x^{p^{m-1}})) = \psi(\zeta)(x^{p^{m-1}}) \quad \text{for } x \in Z_p G.$$

This completes the proof.

The next consequence of Theorem 54.5 will be vital in proving Taylor's Theorem about the Swan subgroup.

**(54.12) Corollary.** *Let  $\zeta \in \text{ch } G$  be such that  $\zeta \equiv 0 \pmod{p^k}$  for some  $k > 0$ . Then for each  $z \in (Z_p G)^\circ$ , there exists a  $p$ -power root of unity  $\mu(z) \in Q_p(\zeta)$  such that*

$$(54.13) \quad (\det_{p\zeta} z)(\det_{-\psi(\zeta)} z) \equiv \mu(z) \pmod{p^{k+1}}.$$

*Proof.* Denote by  $w$  the left-hand side of (54.13). We have  $(Z_p G)^\circ = Z_p^\circ(1 + J)$ , where  $J = \text{rad } Z_p G$ . For  $z \in Z_p^\circ$  we obtain  $w = z^{pd} z^{-d}$ , where  $d = \zeta(1)$ . Since  $z^{p-1} \equiv 1 \pmod{p}$  and  $p^k | d$ , it follows that  $w \equiv 1 \pmod{p^{k+1}}$ , and in this case we may choose  $\mu(z) = 1$ .

It remains to treat the case where  $z \in 1 + J$ . Let  $K_0 = Q_p(\zeta)$ ,  $R_0 = \text{d.v.r. in } K_0$ , and  $P_0 = \text{maximal ideal of } R_0$ . Since  $z \in 1 + J$ , it is clear from Exercise 52.1 that  $w \equiv 1 \pmod{P_0}$ . We must show that  $w \equiv \mu(z) \pmod{p^{k+1}}$  with  $\mu(z)$  a  $p$ -power root of 1 in  $K_0$ . Taking  $R = Z_p$  and  $f = 1$  in (54.6), we have  $\log w =$

$\zeta(L(z))$ , where  $L(z)$  is the logarithm defined in (54.5). But  $L(z) \in \overline{p\mathbb{Z}_p G}$ , and the values  $\{\zeta(g) : g \in G\}$  are multiples of  $p^k$  by hypothesis. It follows as in the preceding proof that  $\zeta(L(z)) \equiv 0 \pmod{p^{k+1}}$ . Thus we have

$$w \equiv 1 \pmod{P_0}, \quad \log w \equiv 0 \pmod{p^{k+1} R_0}.$$

We shall deduce from this that  $w \equiv \mu(z) \pmod{p^{k+1}}$  for some  $\mu(z)$ .

It is easily seen that for  $p$  odd

$$(54.14) \quad \log(1 + p^n y) \equiv p^n y \pmod{p^{n+1}} \quad \text{for } n \geq 1 \quad \text{and} \quad y \in R_0,$$

while for  $p = 2$  the above holds for all  $n \geq 1$ .

Since  $\log w \equiv 0 \pmod{p^{k+1}}$  and  $k \geq 1$ , we may use (54.14) repeatedly to find elements  $\{x_i : i = k+1, k+2, \dots\}$  of  $R_0$  such that for  $i \geq k+1$ ,

$$x_i \equiv w \pmod{p^{k+1}}, \quad \log x_i \equiv 0 \pmod{p^i}, \quad \text{and} \quad \lim_{i \rightarrow \infty} x_i = x' \text{ exists.}$$

Then  $\log x' = 0$  and  $x' \equiv w \pmod{p^{k+1}}$ , so  $x' \in 1 + P_0$ . By (54.3v),  $x'$  is a  $p$ -power root of 1, and so we need only choose  $\mu(z) = x'$ . This completes the proof.

Before embarking on the proof of Taylor's Theorem, let us tabulate the Artin exponent  $A(G)$  and the order  $|T(G)|$  of the Swan subgroup  $T(G)$ , for  $G$  a  $p$ -group.

$G = p$ -group of order $p^m$	$A(G)$	$ T(G) $
Cyclic	1	1
Noncyclic, $p$ odd	$p^{m-1}$	$p^{m-1}$
Generalized quaternion group of order $2^m$ , $m \geq 3$	2	2
Dihedral group of order $2^m$ , $m \geq 2$	2	1
Semidihedral group of order $2^m$ , $m \geq 4$	4	2
All other noncyclic 2-groups of order $2^m$	$2^{m-1}$	$2^{m-2}$

For  $G$  cyclic,  $A(G) = 1$  by definition, while  $T(G)$  is trivial by (53.6). In general, by (53.6) and (53.12),  $T(G)$  is a cyclic  $p$ -group whose order divides  $\varphi(p^m)/2$ ; thus  $|T(G)|$  divides  $p^{m-1}$  for  $p$  odd, and divides  $2^{m-2}$  for  $p = 2$ .

By (53.17) and (53.18),  $|T(G)| = 2$  for  $G$  a generalized quaternion 2-group or semidihedral 2-group, while  $D(\mathbb{Z}G)$  and  $T(G)$  are trivial for a dihedral 2-group by (50.31) (see also Exercise 53.3). Thus, it remains for us to prove:

**(54.15) Taylor's Theorem.** *Let  $G$  be a noncyclic  $p$ -group of order  $p^m$ . If  $p = 2$ , assume that  $G$  is not generalized quaternion, dihedral, or semidihedral. Then the order of the Swan subgroup  $T(G)$  of the locally free class group  $\mathrm{Cl}\mathbb{Z}G$  is given by*

$$|T(G)| = p^{m-1}, \quad p \text{ odd}; \quad |T(G)| = 2^{m-2}, \quad p = 2.$$

*Proof.* Let  $E = \mathbb{Q}(\omega)$ , where  $\omega = p^m$ -th root of 1, so  $E$  is a splitting field for  $G$ . Let  $\Omega = \text{Gal}(E/\mathbb{Q})$ , and  $S = \text{alg. int. } \{E\}$ . Let  $\Lambda = ZG$ , so by (52.20) we have (writing  $\text{Hom}$  in place of  $\text{Hom}_\Omega$ , for brevity)

$$(54.16) \quad D(\Lambda) \cong \frac{\text{Hom}(\text{ch } G, S_p)}{\text{Hom}^+(\text{ch } G, S) \cdot \text{Det } \Lambda_p}.$$

The Swan subgroup  $T(G)$  of  $D(\Lambda)$  consists of the classes  $[r, \sigma]$ , where  $p \nmid r$ . The class  $[r, \sigma]$  is represented by the function  $f \in \text{Hom}(\text{ch } G, S_p)$  such that

$$f(\zeta) = \begin{cases} r, & \text{if } \zeta = 1 \\ 1, & \text{if } \zeta \in \text{Irr } G, \quad \zeta \neq 1 \end{cases}$$

(see (52.13)). By (53.4) and (53.5),  $T(G)$  is a factor group of  $\bar{Z}/(\pm 1)$ , where  $\bar{Z} = Z/p^m Z$ .

We begin with the case where  $p$  is odd, so now  $|G| = p^m$ ,  $m \geq 2$ , and  $G$  is noncyclic. The element  $1 + p$  has order  $p^{m-1}$  in  $Z/(\pm 1)$ , so we shall consider the class  $[1 + p, \sigma] \in T(G)$ , and then take its representative function  $f \in \text{Hom}(\text{ch } G, S_p)$ . We shall then find a homomorphic image of the right-hand side of (54.16), such that  $f$  maps onto an element  $\bar{f}$  of order  $p^{m-1}$  in this image. It will then follow that  $|T(G)| \geq p^{m-1}$ , and consequently  $|T(G)| = p^{m-1}$ , as desired.

To construct the homomorphic image, we need some additional notation. For  $\zeta \in \text{ch } G$ , we write (as above)

$$\zeta \equiv 0 \pmod{p^k} \quad \text{if } \zeta(g) \equiv 0 \pmod{p^k} \quad \text{for each } g \in G.$$

Let  $\psi$  be the  $p$ -th Adams operator on  $\text{ch } G$ , and let  $\text{ch}^{(k)}(G)$  be the additive subgroup of  $\text{ch } G$  defined by

$$\text{ch}^{(k)}G = \{p\zeta - \psi(\zeta) : \zeta \in \text{ch } G, \zeta \equiv 0 \pmod{p^k}\}.$$

Now let

$$V_k = \{f \in \text{Hom}_\Omega(\text{ch } G, S_p) : \text{For each } \xi = p\zeta - \psi(\zeta) \in \text{ch}^{(k)}(G), f(\xi) \equiv \mu_\xi \pmod{p^{k+1}} \text{ with } \mu_\xi \text{ some } p\text{-power root of 1 in } \mathbb{Q}_p(\zeta)\}$$

Then Corollary 54.12 can be restated as follows:

$\text{Det } \Lambda_p$  is a subgroup of  $V_k$  for  $k > 0$ .

We observe next that inclusion  $\text{ch}^{(k)}G \subset \text{ch } G$  defines a restriction homomorphism

$$\text{res}: \text{Hom}(\text{ch } G, S_p) \rightarrow \text{Hom}(\text{ch}^{(k)}G, S_p).$$

By (54.16),  $\text{res}$  induces a surjective homomorphism

$$D(\Lambda) \rightarrow \frac{\text{res Hom}(\text{ch } G, S_p^\cdot)}{\text{res} \{ \text{Hom}^+(\text{ch } G, S^\cdot) \cdot V_k \}}, \quad k > 0,$$

using the fact that  $\text{Det } \Lambda_p^\cdot \leq V_k$ . We shall combine this surjection with another map, to be defined below. Given any  $\zeta \in \text{ch } G$  such that  $\zeta \equiv 0 \pmod{p^k}$ , where  $k > 0$ , let  $K = \mathbb{Q}(\zeta) \subseteq E$ ,  $R = \text{alg. int. } \{K\} \subseteq S$ , and let  $\hat{R} = R_p$ . Define a homomorphism

$$\frac{\text{res Hom}(\text{ch } G, \hat{S}^\cdot)}{\text{res} \{ \text{Hom}^+(\text{ch } G, S^\cdot) \cdot V_k \}} \xrightarrow{\theta} \frac{\hat{R}^\cdot}{R^\cdot(1 + p^{k+1}\hat{R})}$$

as follows: for each  $f \in \text{Hom}(\text{ch } G, \hat{S}^\cdot)$ , let

$$\theta(\text{res } f) = \text{residue class of } f(p\zeta - \psi(\zeta)).$$

Note that  $f(p\zeta - \psi(\zeta)) \in \hat{R}^\cdot$  since  $f(p\zeta - \psi(\zeta))$  is invariant under  $\text{Gal}(E/K)$ . Further,  $\hat{R}^\cdot \cap S^\cdot = R^\cdot$ , and  $R^\cdot$  contains each  $p$ -power root of unity in  $\hat{R}$ . It follows readily that  $\theta$  is well-defined.

In particular, we construct the map  $\theta$  corresponding to the regular character  $\rho$  of  $G$ ; we have  $\rho(1) = p^m$  and  $\rho \equiv 0 \pmod{p^m}$ . In this case we have  $K = \mathbb{Q}(\rho) = \mathbb{Q}$ ,  $R = \mathbb{Z}$ ,  $\hat{R} = \mathbb{Z}_p$ . Thus we obtain homomorphisms

$$D(\Lambda) \rightarrow \frac{\text{Hom}(\text{ch } G, \hat{S}^\cdot)}{\text{Hom}^+(\text{ch } G, S^\cdot) \cdot \text{Det } \Lambda_p^\cdot} \xrightarrow{\theta \circ \text{res}} \frac{\mathbb{Z}_p^\cdot}{(\pm 1)(1 + p^{m+1}\mathbb{Z}_p)} = W,$$

say, where for each  $f \in \text{Hom}(\text{ch } G, \hat{S}^\cdot)$ ,

$$\theta(\text{res } f) = \text{image of } f(p\rho - \psi(\rho)) \text{ in } W.$$

We wish to calculate the image of  $f$ , where  $f$  is the representative function of the class  $[1 + p, \sigma] \in T(G)$ , given by

$$f(\zeta) = \begin{cases} 1 + p, & \zeta = 1 \\ 1, & \zeta \in \text{Irr } G, \quad \zeta \neq 1. \end{cases}$$

We have

$$f(p\rho - \psi(\rho)) = f(\rho)^p / f(\psi(\rho)),$$

and we must calculate the multiplicities of the trivial character 1 in  $\rho$  and  $\psi(\rho)$ . Clearly,

$$(\rho, 1) = |G|^{-1} \sum_{x \in G} \rho(x) = 1, \quad (\psi(\rho), 1) = |G|^{-1} \sum_{x \in G} \rho(x^p).$$

Since  $G$  is a noncyclic  $p$ -group,  $p$  odd, Kulakoff's Theorem tells us that

$$\text{card} \{x \in G : x^p = 1\} \equiv 1 \pmod{p^2}$$

(see Huppert [67, p. 314] or Zassenhaus [49, p. 123]). It follows that  $f(p\rho - \psi(\rho)) = (1 + p)^{pq}$  for some integer  $q$  prime to  $p$ . Since  $(1 + p)^p$  has order  $p^{m-1}$  in  $W$ , the above remarks prove that the class  $[1 + p, \sigma]$  has order  $p^{m-1}$  in  $D(\Lambda)$ , and is a generator of the cyclic group  $T(G)$ .

Consider finally the case where  $p = 2$ , and let  $G$  be a noncyclic 2-group of order  $2^m$ , with  $G$  not generalized quaternion, dihedral, or semidihedral. In this case, a theorem of Thompson, Feit, and Alperin (see Isaacs [76, p. 52]) states that

$$\text{card} \{x \in G : x^2 = 1\} \equiv 0 \pmod{4}.$$

We now show that the class  $[5, \sigma] \in T(G)$  has order  $2^{m-2}$ , and thus generates the cyclic group  $T(G)$ . Let  $f$  be the representative function of this class; as above, define the map  $\theta$  by using the regular representation of  $G$ . Then

$$f(2\rho - \psi(\rho)) = 5^{2q}, \quad \text{where } q \text{ is odd.}$$

In this case,

$$W = \mathbb{Z}_2 / (\pm 1)(1 + 2^{m+1}\mathbb{Z}_2),$$

and clearly  $5^{2q}$  has order  $2^{m-2}$  in  $W$ . This shows that  $[5, \sigma]$  has order  $2^{m-2}$ , and completes the proof of Taylor's Theorem.

We conclude by stating, without proof, some results due to Oliver [83b], which provide a deeper understanding of Taylor's Theorem. Let  $G$  be a  $p$ -group, where  $p$  is odd, and let  $\Delta$  be a cyclic group of order  $p - 1$ . If  $G$  is cyclic, then  $\Delta$  embeds uniquely into  $\text{Aut } G$ , and thus  $\Delta$  acts on the finite  $p$ -group  $D(ZG)$ . This action gives rise to a decomposition of  $D(ZG)$  into eigenspaces  $\{{}^i D(ZG)\}$ ; see the discussion following (50.61).

Now let  $G$  be an arbitrary  $p$ -group,  $p$  odd. The center of  $QG$  is a direct sum of cyclotomic field extensions  $F_i$  of  $\mathbb{Q}$ , and  $\Delta$  embeds uniquely into each  $\text{Gal}(F_i/\mathbb{Q})$ , thereby giving an action of  $\Delta$  on the center of  $QG$ . Oliver proved that one can define an action of  $\Delta$  on  $D(ZG)$ , giving rise to eigenspaces  $\{{}^i D(ZG)\}$ , with  ${}^0 D(ZG)$  the  $\Delta$ -trivial submodule of  $D(ZG)$ . His main results are as follows:

- (1) If  $p$  is a regular odd prime, then  $D^+(ZG) \cong {}^0 D(ZG)$ .
- (2) The Swan subgroup  $T(G)$  is a subgroup of  ${}^0 D(ZG)$ .
- (3) Define the *Artin cokernel* (see §76) of  $G$  to be the ring

$$(\text{ch } QG) \left/ \sum_{C \leq G} \text{ind}_C^G \text{ch } QC \right.,$$

where  $C$  ranges over all cyclic subgroups of  $G$ . This is a commutative ring

(with identity element), whose characteristic is the Artin exponent  $A(G)$  of  $G$ . There is an isomorphism

$${}^0D(\mathbb{Z}G) \cong \text{Artin cokernel of } G.$$

This isomorphism carries  $T(G)$  onto the group  $\mathbb{Z} \cdot 1$ , where 1 is the identity element of the Artin cokernel. Consequently  $T(G)$  is cyclic, of order  $A(G)$ .

- (4) For an arbitrary finite group  $H$ , let

$$\Omega H \cong \coprod_i M_{n_i}(D_i), \quad D_i = \text{skewfield}, \quad d_i = \dim_{\mathbb{Q}} D_i.$$

Let  $C$  range over a full set of nonconjugate cyclic subgroups of  $H$ . Then

$$(\text{order of Artin cokernel of } H)^2 = \left( \prod_C \frac{\varphi(|C|)|N_H(C):C|}{|C|} \right) \left( \prod_i d_i \right),$$

where  $\varphi$  = Euler  $\varphi$ -function. For another version of this formula, due to Solomon [74], see (76.24).

For  $G$  an arbitrary  $p$ -group,  $p$  odd, the isomorphism in (3) then yields an explicit formula for the order of  ${}^0D(\mathbb{Z}G)$ .

## §54. Exercises

1. Keeping the notation of (54.12), assume that both  $\zeta$  and  $\psi(\zeta)$  are characters of  $G$  (not just virtual characters). Show that in (54.13),  $\mu(z)$  is necessarily equal to 1.

[Hint (Taylor [78a]): Use Newton's identities and (54.11).]

## §55. PICARD GROUPS

### §55A. Basic Properties

The Picard group of an order  $\Lambda$ , denoted by  $\text{Pic } \Lambda$ , is in a rough sense the two-sided analogue of the locally free class group  $\text{Cl } \Lambda$ . The elements of  $\text{Pic } \Lambda$  are bimodule isomorphism classes ( $M$ ) of suitably restricted  $(\Lambda, \Lambda)$ -bimodules  $M$ . We shall see that  $\text{Pic } \Lambda$  and  $\text{Cl } \Lambda$  are closely related. Generally speaking,  $\text{Pic } \Lambda$  is considerably harder to calculate than  $\text{Cl } \Lambda$ , and furthermore  $\text{Pic } \Lambda$  is not necessarily an abelian group. Many of the results given in the beginning of this section are due to Fröhlich [73] (see also Bass [68]).

We begin with a brief review of some definitions from §35 on invertible ideals, which in turn depend heavily on the Morita theory given in §3D. Throughout this section, let  $R$  denote a commutative ring (with 1). Let  $\Lambda, \Delta$  denote  $R$ -algebras, so there are homomorphisms  $R \rightarrow c(\Lambda), R \rightarrow c(\Delta)$ , where  $c(\Lambda)$  denotes the center of  $\Lambda$ . Let  $M = {}_\Lambda M_\Delta$  be a  $(\Lambda, \Delta)$ -bimodule; we assume always

that  $R$  centralizes  $M$ , that is,

$$rm = mr \text{ for all } r \in R, m \in M.$$

(This really means that  $(r1_{\Lambda})m = m(r1_{\Lambda})$  for all  $r, m$ .) There is no loss of generality in making these restrictions, since we can always choose  $R = \mathbb{Z}$  if need be. We assume once and for all that all maps occurring hereafter are  $R$ -homomorphisms.

A bimodule  ${}_{\Lambda}M_{\Delta}$  is *invertible* if  $M$  gives a Morita equivalence between the rings  $\Lambda$  and  $\Delta$ . By (3.54), this occurs if and only if  ${}_{\Lambda}M$  is a progenerator<sup>†</sup> for the category of left  $\Lambda$ -modules, and  $\Delta \cong (\text{End}_{\Lambda} M)^0$ . Equivalently, there must exist a bimodule  ${}_{\Delta}N_{\Lambda}$  and bimodule surjections

$$(55.1) \quad M \otimes_{\Delta} N \rightarrow \Lambda, \quad N \otimes_{\Lambda} M \rightarrow \Delta,$$

such that the diagrams

$$(55.2) \quad \begin{array}{ccc} M \otimes_{\Delta} N \otimes_{\Lambda} M & \longrightarrow & \Lambda \otimes_{\Lambda} M \\ \downarrow & & \downarrow \\ M \otimes_{\Delta} \Delta & \longrightarrow & M, \end{array} \quad \begin{array}{ccc} N \otimes_{\Lambda} M \otimes_{\Delta} N & \longrightarrow & \Delta \otimes_{\Delta} N \\ \downarrow & & \downarrow \\ N \otimes_{\Lambda} \Lambda & \longrightarrow & N \end{array}$$

commute. In this case, the maps in (55.1) are isomorphisms. We call  $N$  the *inverse* of  $M$ . The bimodule isomorphism class  $(N)$  of  $N$  is uniquely determined by  $M$ , and in fact  $N \cong M^{-1}$ , where

$$(55.3) \quad M^{-1} = \text{Hom}_{\Lambda}({}_{\Lambda}M_{\Delta}, {}_{\Lambda}\Lambda_{\Lambda}) \cong \text{Hom}_{\Delta}({}_{\Lambda}M_{\Delta}, {}_{\Delta}\Delta_{\Delta}).$$

Of course,  $M^{-1}$  gives a Morita equivalence between  $\Delta$  and  $\Lambda$ . We note also that

$$(55.4) \quad \Lambda = \text{Hom}_{\Delta}(M, M), \quad \Delta \cong \text{Hom}_{\Lambda}(M, M),$$

where now  $\Delta$  and  $\text{Hom}_{\Delta}(M, M)$  are viewed as rings of *right* operators on  $M$ .

We remark that by (35.4), invertibility is a “local” property, that is,  $M$  is invertible if and only if for each maximal ideal  $P$  of  $R$ , the localization  $M_P$  is an invertible  $(\Lambda_P, \Delta_P)$ -bimodule. (If  $R$  is a domain, the subscript  $P$  could equally well be interpreted to mean “ $P$ -adic completion.”)

In the above discussion, we are going to choose  $\Delta = \Lambda$ , and then consider invertible  $(\Lambda, \Lambda)$ -bimodules  ${}_{\Lambda}M_{\Lambda}$ . Unless otherwise stated, we do *not* assume that  $\Lambda$  centralizes  $M$ . Thus,  $\lambda m = m\lambda$  need not hold true for all  $\lambda \in \Lambda, m \in M$ . By the above,  ${}_{\Lambda}M_{\Lambda}$  is invertible if and only if  ${}_{\Lambda}M$  is a progenerator for the category of left  $\Lambda$ -modules, and every left  $\Lambda$ -endomorphism of  $M$  is given by a right multiplication by an element of  $\Lambda$ .

**(55.5) Definition.** Let  $\Lambda$  be an  $R$ -algebra, where  $R$  is a commutative ring. Let  $(M)$  denote the bimodule isomorphism class of the bimodule  ${}_{\Lambda}M_{\Lambda}$ , where we

<sup>†</sup>This means that  $M$  is a f.g. projective  $\Lambda$ -module, such that  $\Lambda$  is a direct summand of  $M^{(k)}$  for some  $k$ .

assume that  $R$  centralizes  $M$ . The *Picard group* of  $\Lambda$  relative to  $R$ , denoted by  $\text{Pic}_R\Lambda$ , is the multiplicative group consisting of all classes  $(M)$  of invertible bimodules. Multiplication is defined by

$$(M)(M') = (M \otimes_{\Lambda} M').$$

The identity element is the class  $(\Lambda)$ , and inverses are given by

$$(M)^{-1} = (M^{-1}), \quad \text{since } (M)(M^{-1}) = (M^{-1})(M) = (\Lambda).$$

*Beware:*  $\text{Pic}_R\Lambda$  need not be a commutative group!

We have already seen in §35 that when  $\Lambda = R$  is a Dedekind domain, then the elements of  $\text{Pic}_R\Lambda$  are precisely the classes of invertible fractional  $R$ -ideals in the quotient field of  $K$ ; but each fractional  $R$ -ideal is necessarily invertible, so in this case  $\text{Pic}_R\Lambda \cong \text{Cl } R$ , the usual ideal class group of  $R$ .

**(55.6) Definition.** Let  $\Lambda$  be an arbitrary ring, and let  $C = c(\Lambda)$  be its center. We define  $\text{Picent } \Lambda = \text{Pic}_C\Lambda$ , so  $\text{Picent } \Lambda$  is the subgroup of  $\text{Pic}_{\mathbb{Z}}\Lambda$  consisting of all isomorphism classes of invertible bimodules  ${}_{\Lambda}M_{\Lambda}$  centralized by  $C$ . (Note: “Picent” is pronounced “pick-sent.”) We shall see below that when  $\Lambda$  is an order in a semisimple algebra  $A$  over a field,  $\text{Picent } \Lambda$  is precisely the group of invertible two-sided  $\Lambda$ -ideals in  $A$ , modulo the subgroup of principal ideals generated by units in  $c(A)$ . Thus  $\text{Picent } \Lambda$  is a natural object of investigation. If  $R$  is a commutative ring, then  $\text{Picent } R$  is the group of classes of invertible  $(R, R)$ -bimodules centralized by  $R$ .

We proceed to derive a number of formal properties of Picard groups, and begin with an easy result.

**(55.7) Lemma.** *Let  $\Lambda, \Delta$  be  $R$ -algebras, and let  ${}_{\Lambda}M_{\Delta}$  be an invertible bimodule centralized by  $R$ . Then  $M$  determines an  $R$ -isomorphism  $\varphi: c(\Lambda) \cong c(\Delta)$ , defined thus: for each  $c \in c(\Lambda)$ ,  $\varphi(c)$  is the unique element of  $c(\Delta)$  such that*

$$(55.8) \quad c \cdot m = m \cdot \varphi(c) \quad \text{for all } m \in M.$$

Taking  $R = \mathbb{Z}$ , it follows that Morita equivalent rings have isomorphic centers.

*Proof.* Since  $M$  is invertible, elements of  $\Lambda$  and  $\Delta$  are completely determined by their action on  $M$ , by (55.4). For  $c \in c(\Lambda)$ , the map  $m \mapsto cm$  is a left  $\Lambda$ -endomorphism of  $M$ , so there is a unique  $\varphi(c) \in \Delta$  for which (55.8) holds true. For  $m \in M$  and  $x \in \Delta$ , we have

$$m(\varphi(c)x) = (cm)x = (mx)\varphi(c) = m(x\varphi(c)),$$

so  $\varphi(c)$  commutes with each  $x \in \Delta$ , and thus lies in  $c(\Delta)$ . It is easily checked that  $\varphi$  gives the desired  $R$ -isomorphism  $c(\Lambda) \cong c(\Delta)$ .

We use this result to prove the Morita equivalent rings have isomorphic Picard groups.

**(55.9) Theorem.** (i) *If the  $R$ -algebras  $\Lambda, \Delta$  are Morita equivalent over  $R$ , then  $\text{Pic}_R \Lambda \cong \text{Pic}_R \Delta$ .*

(ii) *If the rings  $\Lambda, \Lambda'$  are Morita equivalent, then  $\text{Picent } \Lambda \cong \text{Picent } \Lambda'$ .*

*Proof.* (i) Let  ${}_A M_\Delta$  be an invertible bimodule centralized by  $R$ . The reader will easily check that the map

$$(X) \rightarrow (M^{-1} \otimes_A X \otimes_\Delta M), \quad (X) \in \text{Pic}_R \Lambda,$$

gives an isomorphism  $\text{Pic}_R \Lambda \cong \text{Pic}_R \Delta$ . This isomorphism may depend on the choice of  $M$ .

(ii) Now let  ${}_A N_{\Lambda'}$  be an invertible bimodule, and as in (55.7), let  $N$  determine the isomorphism  $\varphi: C \cong C'$  of centers. Thus

$$c \cdot n = n \cdot \varphi(c) \quad \text{for all } c \in C = c(\Lambda) \quad \text{and all } n \in N.$$

For  $(X) \in \text{Picent } \Lambda$  we have  $cx = xc$  for all  $c \in C$ ,  $x \in X$ . We must show that  $(N^{-1} \otimes_A X \otimes_\Delta N) \in \text{Picent } \Lambda'$ . But each  $c' \in C'$  is of the form  $c' = \varphi(c)$  for some  $c \in C$ , and

$$(n' \otimes x \otimes n)\varphi(c) = n' \otimes x \otimes cn = n'c \otimes x \otimes n = \varphi(c)(n' \otimes x \otimes n),$$

so  $c'$  centralizes  $N^{-1} \otimes X \otimes N$ , as desired. This completes the proof. For further results of this nature, see Exercises 55.1–55.3.

Now let  $\text{Aut}_R \Lambda$  denote the group of all  $R$ -automorphisms of the  $R$ -algebra  $\Lambda$ , and let  $\text{In } \Lambda$  be the subgroup consisting of all inner automorphisms  $\{i_u; u \in \Lambda^\times\}$ , where  $i_u(x) = uxu^{-1}$ ,  $x \in \Lambda$ . Then  $\text{In } \Lambda \trianglelefteq \text{Aut}_R \Lambda$ , and we define

$$\text{Out}_R \Lambda = \text{Aut}_R \Lambda / \text{In } \Lambda = \text{outer automorphism group of } \Lambda \text{ over } R.$$

We shall see that  $\text{Out}_R \Lambda$  maps injectively into  $\text{Pic}_R \Lambda$ . To begin with, let  ${}_A M_\Delta$  be any bimodule, and let  $f \in \text{Aut } \Lambda$ ,  $g \in \text{Aut } \Delta$ . Let  ${}_f M_g$  be the  $(\Lambda, \Delta)$ -bimodule having the same elements as  $M$ , but with the actions of  $\Lambda$  and  $\Delta$  “twisted” by  $f$  and  $g$ , respectively:

$$\lambda \circ m \circ \delta (\text{in } {}_f M_g) = f(\lambda)m g(\delta) (\text{in } M)$$

for all  $\lambda \in \Lambda$ ,  $\delta \in \Delta$ ,  $m \in M$ . It is clear that

$${}_{f'}({}_f M_g)_{g'} \cong {}_{f'f} M_{gg'} \text{ as bimodules.}$$

The reader will easily verify the following:

**(55.10) Proposition.** Let  $\Lambda$  be an  $R$ -algebra, viewed as  $(\Lambda, \Lambda)$ -bimodule. For each  $f, g \in \text{Aut}_R \Lambda$  there is a  $(\Lambda, \Lambda)$ -bimodule  ${}_f\Lambda_g$  centralized by  $R$ . There are bimodule isomorphisms

$$\begin{aligned} {}_f\Lambda_g &\cong {}_{hf}\Lambda_{hg} \cong {}_1\Lambda_{f^{-1}g} \cong {}_{g^{-1}f}\Lambda_1, & {}_{f'}({}_f\Lambda_g)_{g'} &\cong {}_{f'f}\Lambda_{gg'}, \\ {}_f\Lambda_g \otimes {}_{f'}\Lambda_{g'} &\cong {}_f\Lambda_{g'f^{-1}g'}, & {}_1\Lambda_g \otimes {}_1\Lambda_{g'} &\cong {}_1\Lambda_{gg'}, \\ {}_1\Lambda_f \otimes {}_f\Lambda_1 &\cong \Lambda \cong {}_f\Lambda_1 \otimes {}_1\Lambda_f, \end{aligned}$$

where  $\otimes$  means  $\otimes_\Lambda$ .

Using these, we obtain:

**(55.11) Theorem.** Given an  $R$ -algebra  $\Lambda$ , there is an exact sequence of groups

$$1 \rightarrow \text{In } \Lambda \rightarrow \text{Aut}_R \Lambda \xrightarrow{\omega_0} \text{Pic}_R \Lambda,$$

where  $\omega_0(f) = ({}_1\Lambda_f)$  for  $f \in \text{Aut}_R \Lambda$ . Thus  $\omega$  induces a monomorphism

$$\omega: \text{Out}_R \Lambda \rightarrow \text{Pic}_R \Lambda.$$

*Proof.* Each  $f \in \text{Aut}_R \Lambda$  gives rise to a  $(\Lambda, \Lambda)$ -bimodule  ${}_1\Lambda_f$  centralized by  $R$ . By (55.10),  ${}_f\Lambda_1$  is an inverse for  ${}_1\Lambda_f$ , and  $\omega_0$  is a homomorphism. We must show that  $\ker \omega_0 = \text{In } \Lambda$ . We have  $\omega_0(f) = 1$  if and only if there exists a bimodule isomorphism  $\theta: \Lambda \cong {}_1\Lambda_f$ , that is, there exists a bijection  $\theta: \Lambda \rightarrow \Lambda$  such that

$$(*) \quad \theta(axb) = a \cdot \theta(x) \cdot f(b) \quad \text{for all } a, b, x \in \Lambda.$$

For  $f = i_u$ , where  $i_u(x) = uxu^{-1}$ , choose  $\theta$  so that  $\theta(x) = xu^{-1}$ . This proves that  $\ker \omega_0 \supseteq \text{In } \Lambda$ .

Conversely, let  $\theta: \Lambda \rightarrow \Lambda$  be a bijection satisfying (\*), and choose  $u = \theta(1)$ . Then  $\Lambda = \theta(\Lambda) = \theta(\Lambda \cdot 1) = \Lambda u$ , and likewise  $\Lambda = u\Lambda$ , so  $u \in \Lambda^\circ$ . Taking  $x = b = 1$  in (\*), we obtain  $\theta(a) = au$  for  $a \in \Lambda$ . Now set  $a = x = 1$  in (\*), so we have  $bu = uf(b)$  for all  $b \in \Lambda$ , and thus  $f$  is the inner automorphism  $i_{u^{-1}}$ . This completes the proof.

In considering the one-sided module structure of invertible bimodules, we shall repeatedly use the following elementary result:

**(55.12) Theorem.** Let  $(X), (Y) \in \text{Pic}_R \Lambda$ . Then  ${}_A X \cong {}_A Y$  if and only if  $(Y) \in (X) \cdot \text{im } \omega$ , that is,  $Y \cong {}_1 X_f$  as bimodules for some  $f \in \text{Aut}_R \Lambda$ .

*Proof.* For  $f \in \text{Aut}_R \Lambda$ , there is a bimodule isomorphism

$${}_1 X_f \cong X \otimes {}_1 \Lambda_f.$$

Thus  $(Y) \in (X) : \text{im } \omega$  if and only if  $Y \cong {}_1 X_f$  for some  $f$ . Clearly  ${}_{\Lambda} X \cong {}_{\Lambda} Y$  whenever such an isomorphism exists.

Conversely, a left  $\Lambda$ -isomorphism  $h: X \cong Y$  induces a ring isomorphism

$$h^*: \text{End}_{\Lambda} Y \cong \text{End}_{\Lambda} X, \quad \text{given by } h^*(\varphi) = h^{-1} \varphi h.$$

Since  ${}_{\Lambda} X_{\Lambda}$  is invertible, each element of  $\text{End}_{\Lambda} X$  is a right multiplication  $a_r$  for some  $a \in \Lambda$ , and  $\varphi \in \text{End}_{\Lambda} Y$  is some  $b_r$ . Thus each  $b \in \Lambda$  determines a unique  $f(b) \in \Lambda$  such that  $h^{-1} b_r h = (f(b))_r$  on  $X$ , that is,

$$(hx)b = h(xf(b)) \quad \text{for all } x \in X, \quad b \in \Lambda.$$

It follows easily that  $f \in \text{Aut}_R \Lambda$ , and that  $h: {}_1 X_f \rightarrow Y$  is a bimodule isomorphism.

Before studying  $\text{Picent } \Lambda$  in more detail, we briefly consider the relation between  $\text{Picent } \Lambda$  and  $\text{Pic}_R \Lambda$ , where  $\Lambda$  is an  $R$ -algebra with center  $C$ . By (55.7), each invertible  ${}_{\Lambda} M_{\Lambda}$  centralized by  $R$  determines an  $R$ -automorphism  $\Phi_M$  of  $C$ , according to the formula

$$\Phi_M(c) \cdot m = m \cdot c \quad \text{for all } m \in M, \quad c \in C.$$

Clearly  $\Phi_M$  depends only on the bimodule isomorphism class of  $M$ , and  $\Phi_M = \text{id}_C$  if and only if  $(M) \in \text{Picent } \Lambda$ . In the special case where  $M = {}_1 \Lambda_f$  with  $f \in \text{Aut}_R \Lambda$ , we have (for  $c \in C$ )

$$f(c)m = mf(c) = m \cdot c,$$

where  $m \cdot c$  is computed inside  ${}_1 \Lambda_f$ . Thus for  $M = {}_1 \Lambda_f$ ,  $\Phi_M$  is the restriction of  $f$  to  $C$ . From these remarks, we obtain:

**(55.13) Theorem.** *For any  $R$ -algebra  $\Lambda$  with center  $C$ , there is an exact sequence*

$$1 \rightarrow \text{Picent } \Lambda \rightarrow \text{Pic}_R \Lambda \xrightarrow{\Phi} \text{Aut}_R C.$$

*If  $\Lambda$  is commutative, the sequence is split exact.*

*Proof.* Let  $(M), (N) \in \text{Pic}_R \Lambda$ , and set  $f = \Phi_M$ ,  $g = \Phi_N$ . Then for each  $c \in C$  we have

$$f(c)m = mc, \quad g(c)n = nc \quad \text{for all } m \in M, \quad n \in N.$$

Therefore

$$(m \otimes n)c = m \otimes nc = mg(c) \otimes n = f(g(c))(m \otimes n),$$

which shows that  $\Phi_{M \otimes N} = \Phi_M \circ \Phi_N$ , that is,  $\Phi$  is a homomorphism. Our earlier remarks show that  $\ker \Phi = \text{Picent } \Lambda$ .

Now suppose  $\Lambda = C$ , and define  $\omega_0$  as in (55.11), so  $\omega_0(f) = {}_1\Lambda_f \in \text{Pic}_R \Lambda$  for  $f \in \text{Aut}_R \Lambda$ . By the above remarks,  $\Phi_{\omega_0(f)} = f$ , so  $\Phi \circ \omega_0 = \text{identity map}$  on  $\text{Aut}_R C$ . This completes the proof.

**(55.14) Remarks.** (i) When  $A = \coprod_{i=1}^t A_i$  is a semisimple algebra over a field  $K$ , we can describe the map

$$\Phi_A: \text{Pic}_K A \rightarrow \text{Aut}_K c(A)$$

explicitly, as follows. Suppose that the simple component  $A_i$  has skewfield part  $D_i$  and center  $K_i$ , so  $c(A) = \coprod K_i$ , and each  $f \in \text{Aut}_K c(A)$  must permute the  $\{K_i\}$ . Thus  $f$  is completely determined by some permutation  $\pi$  of the set  $\{1, \dots, t\}$ , together with a collection of  $K$ -isomorphisms  $f_i: K_i \cong K_{\pi(i)}$ ,  $1 \leq i \leq t$ , where  $f_i = f|_{K_i}$ . Now  $\text{Picent } A = 1$  by (55.15), so  $\Phi_A$  is injective. Each  $(X) \in \text{Pic}_K A$  yields a Morita equivalence of  $A$  with itself. Using this fact, Fröhlich [73] showed that the image of  $\Phi_A$  consists precisely of those elements  $f \in \text{Aut}_K c(A)$  such that for each  $i$ ,  $1 \leq i \leq t$ , the isomorphism  $f_i: K_i \cong K_{\pi(i)}$  can be extended to an isomorphism  $D_i \cong D_{\pi(i)}$ .

For a further discussion of these matters, we refer the reader to the work of Janusz [76].

(ii) Let  $R$  be a Dedekind domain with quotient field  $K$ , and let  $\Lambda$  be a maximal  $R$ -order in a f.d. separable  $K$ -algebra  $A$ . Keeping the above notation, we note first that there is a ring isomorphism

$$\text{Aut}_R c(\Lambda) \cong \text{Aut}_K c(A),$$

given by extending each  $R$ -automorphism  $f$  of  $c(\Lambda)$  to a  $K$ -automorphism  $f'$  of  $c(A)$ . It follows readily that  $f \in \text{im } \Phi$  if and only if  $f' \in \text{im } \Phi_A$ , where  $\Phi: \text{Pic}_R \Lambda \rightarrow \text{Aut}_R c(\Lambda)$ . Thus, the calculation of  $\text{im } \Phi$  reduces to the situation discussed in the previous remark.

(iii) If  $A$  is a central simple  $K_1$ -algebra, and  $\dim_K K_1 < \infty$ , we may view  $A$  as  $K$ -algebra. There is an exact sequence

$$1 \rightarrow \text{Picent } A \rightarrow \text{Pic}_K A \xrightarrow{\Phi_A} \text{Aut}_K K_1,$$

and  $\text{im } \Phi_A$  consists precisely of those  $K$ -automorphisms of  $K_1$  which can be extended to  $K$ -automorphisms of  $A$ . (In this connection, see Janusz [76]).

We now prove the fundamental result:

**(55.15) Theorem.** *For any f.d. semisimple  $K$ -algebra  $A$  we have*

$$\text{Picent } A = 1.$$

*Proof.* By Exercise 55.4 it suffices to treat the case where  $A$  is a central simple

$K$ -algebra. By the discussion preceding (35.4), for each  $(X) \in \text{Picent } A$  we have  $X \cong A$  as left  $A$ -modules. Therefore  $X \cong {}_1A_f$  (as bimodules) for some  $f \in \text{Aut}_K A$ , by (55.12). But  $f$  is an inner automorphism of  $A$  by the Skolem-Noether Theorem 3.62, so  $({}_1A_f) = 1$  in  $\text{Picent } A$  by (55.11). Thus  $(X) = 1$  as desired. Another proof can be given by using Exercise 55.3, since  $A$  is an Azumaya  $K$ -algebra, and  $\text{Pic}_K K = 1$ .

If  $\Lambda$  is a commutative ring, we may identify the set of  $(\Lambda, \Lambda)$ -bimodules centralized by  $\Lambda$  with the set of one-sided  $\Lambda$ -modules. In our present notation, Theorem 35.5 can now be stated as follows:

**(55.16) Theorem.** *Let  $\Lambda$  be a commutative  $R$ -algebra,  $f.g./R$  as module, where  $R$  is a commutative noetherian ring. Then any f.g.  $\Lambda$ -module  $M$  (centralized by  $\Lambda$ ) is invertible if and only if  $M_P \cong \Lambda_P$  for each maximal ideal  $P$  of  $R$ .*

In particular, if  $R$  is a local ring, then

$$\text{Picent } \Lambda = 1.$$

**Remarks.** (i) The proof of (35.5) shows that  $\text{Picent } \Lambda = 1$  for any commutative ring  $\Lambda$  such that  $\Lambda/\text{rad } \Lambda$  is a direct sum of fields.

(ii) If  $\Lambda$  is commutative and  $R$  is semilocal, then again we obtain  $\text{Picent } \Lambda = 1$ .

### §55B. Picard Groups of Orders

We shall specialize the preceding discussion to the case where  $\Lambda$  is an  $R$ -order in a f.d.  $K$ -algebra  $A$ , with  $K$  the quotient field of an integral domain  $R$ . We begin by explaining the connection between invertible ideals and invertible modules. If  $M$  and  $N$  are two-sided  $\Lambda$ -submodules of  $A$  such that  $MN = NM = \Lambda$ , we call  $M$  an *invertible*  $\Lambda$ -ideal in  $A$ , and  $N$  its *inverse*. In this case, the maps

$$M \otimes_{\Lambda} N \rightarrow MN = \Lambda, \quad N \otimes_{\Lambda} M \rightarrow NM = \Lambda$$

are both surjective, so  $M$  and  $N$  are invertible bimodules, and  $N = M^{-1}$ . Further,  $c(\Lambda)$  centralizes  $M$ , so  $(M) \in \text{Picent } \Lambda$ .

Let  $I(\Lambda)$  denote the multiplicative group of invertible  $\Lambda$ -ideals in  $A$ , with multiplication performed within  $A$ . If  $C = c(\Lambda)$ , then clearly  $c(A) = KC$ . We now show:

**(55.17) Theorem.** *There is an exact sequence of groups*

$$1 \rightarrow C^\cdot \rightarrow (KC)^\cdot \xrightarrow{\rho} I(\Lambda) \xrightarrow{\sigma} \text{Picent } \Lambda \xrightarrow{\tau} \text{Picent } A,$$

where  $\rho(u) = \Lambda u$ ,  $\sigma(M) = (M)$ , and  $\tau(X) = (KX)$ .

*Proof.* Exactness at  $(KC)^\cdot$  is clear, and  $\sigma\rho = 1$ . If  $\sigma(M) = 1$  then there is a

bimodule isomorphism  $\theta: \Lambda \cong M$ . Letting  $c = \theta(1)$ , we obtain  $M = \Lambda c$ . Then  $KM = K\Lambda \cdot c$  implies that  $c \in A^\times$ . Further, from  $\theta(1)a = \theta(a) = a\theta(1)$  for all  $a \in A$ , we deduce that  $c \in (KC)^\times$ . Thus  $M = \rho(c)$ , as desired.

Finally, let  $(X) \in \text{Picent } \Lambda$  be such that  $\tau(X) = 1$ . Since  $X$  is  $\Lambda$ -projective, the map  $X \rightarrow KX$  is injective, and there is a bimodule isomorphism  $f: KX \cong A$ . Set  $M = f(X)$ , so  $M$  is a  $\Lambda$ -ideal in  $A$  which is invertible as  $(\Lambda, \Lambda)$ -bimodule. Then

$$M^{-1} = \text{Hom}_\Lambda(\Lambda M, \Lambda \Lambda) \cong \text{Hom}_\Lambda(M_\Lambda, \Lambda_\Lambda).$$

Tensoring with  $K$  and identifying the new Hom's with  $A$ , we may then identify  $M^{-1}$  with a two-sided  $\Lambda$ -ideal in  $A$ . From (55.1) we deduce that  $MM^{-1} = M^{-1}M = \Lambda$ , so  $M$  is an invertible ideal. Then  $(X) = (M) \in \text{im } \sigma$ , as desired, and the proof is complete.

Combining the above with Theorem 55.15, we obtain:

**(55.18) Corollary.** *If  $\Lambda$  is an R-order in a f.d. semisimple K-algebra  $A$ , then*

$$\text{Picent } \Lambda \cong I(\Lambda)/\{\Lambda u; u \in (KC)^\times\}.$$

This justifies our earlier remark that  $\text{Picent } \Lambda$ , rather than  $\text{Pic}_R \Lambda$ , should be our primary concern. It may be viewed as a natural generalization of the usual ideal class group occurring in algebraic number theory. Furthermore, we have:

**(55.19) Theorem.** *Let  $\Lambda$  be an R-order in a f.d. semisimple K-algebra  $A$ , where  $K$  is a number field. Then  $\text{Pic } \Lambda$  and  $\text{Picent } \Lambda$  are finite groups.*

*Proof.* By the Jordan-Zassenhaus Theorem, there are only finitely many isomorphism classes of left  $\Lambda$ -ideals in  $A$ . It follows that the number of bimodule isomorphism classes of two-sided  $\Lambda$ -ideals is also finite, so  $\text{Picent } \Lambda$  is finite by (55.18). Finally, by (55.13) and (55.14ii),  $\text{Pic}(\Lambda)/\text{Picent } \Lambda$  embeds in the finite group  $\text{Aut}_\Omega c(A)$ .

Returning to the general case, let us define

$$(55.20) \quad N(\Lambda) = \text{normalizer of } \Lambda \text{ in } A = \{x \in A^\times : x\Lambda x^{-1} = \Lambda\}.$$

The normalizer arises naturally from the following:

**(55.21) Lemma.** *Let  $\Lambda$  be an R-order in a f.d. separable K-algebra  $A$ , and let  $x \in A^\times$ . Then*

- (i)  $\Lambda x$  is a  $(\Lambda, \Lambda)$ -bimodule if and only if  $x \in N(\Lambda)$ .
- (ii) For  $x \in N(\Lambda)$ ,  $\Lambda x$  is an invertible bimodule, with inverse  $\Lambda x^{-1}$ .
- (iii)  $x \in N(\Lambda)$  if and only if  $\Lambda x \subseteq x\Lambda$ .

*Proof.* For  $x \in A^\times$ , we have

$$\Lambda x \text{ is a bimodule} \Leftrightarrow x\Lambda \subseteq \Lambda x \Leftrightarrow x \in N(\Lambda),$$

the latter by Exercise 55.6. The rest of the lemma is now obvious.

Before stating the next result, which will be needed for the calculation of  $\mathrm{Picent}\Lambda$  in various cases, we introduce some additional notation: let  $C = c(\Lambda)$ , and put

$$\mathrm{Autcent}\Lambda = \mathrm{Aut}_C\Lambda, \quad \mathrm{Outcent}\Lambda = \mathrm{Out}_C\Lambda = \mathrm{Aut}_C(\Lambda)/\mathrm{In}(\Lambda).$$

By (55.11), there is a monomorphism

$$\omega: \mathrm{Outcent}\Lambda \rightarrow \mathrm{Picent}\Lambda, \quad \text{given by } \omega(f) = ({}_1\Lambda_f) \text{ for } f \in \mathrm{Autcent}\Lambda.$$

Then we have:

**(55.22) Theorem.** *Let  $\Lambda$  be an  $R$ -order in a f.d. semisimple  $K$ -algebra  $A$ .*

(i) *There is an isomorphism*

$$\rho: N(\Lambda)/\Lambda^\times(KC) \cong \mathrm{Outcent}\Lambda = \mathrm{Autcent}(\Lambda)/\mathrm{In}(\Lambda),$$

*induced by the map  $\rho(x) = i_x$  for  $x \in N(\Lambda)$ , where  $i_x$  is the automorphism of  $\Lambda$  given by  $\lambda \mapsto x\lambda x^{-1}$ ,  $\lambda \in \Lambda$ .*

(ii) *There is a commutative diagram*

$$\begin{array}{ccc} N(\Lambda)/\Lambda^\times(KC) & \xrightarrow{\rho} & \mathrm{Outcent}\Lambda \\ \searrow \omega' & & \downarrow \omega \\ & & \mathrm{Picent}\Lambda, \end{array}$$

*where  $\omega'(x) = (\Lambda x)$  for  $x \in N(\Lambda)$ . The maps  $\omega$  and  $\omega'$  are monomorphisms.*

(iii) *We have*

$$\omega(\mathrm{Outcent}\Lambda) = \{(X) \in \mathrm{Picent}\Lambda : {}_A X \cong {}_A \Lambda\}.$$

*Proof.* Each  $f \in \mathrm{Aut}_C\Lambda$  extends to an  $\tilde{f} \in \mathrm{Aut}_{KC}A$ . By the Skolem-Noether Theorem 3.62,  $\tilde{f} = i_x$  for some  $x \in A^\times$ , so  $\rho$  is surjective. The rest of the proof is an easy exercise for the reader.

**(55.23) Corollary.** *Let  $R$  be a d.v.r., and let  $\Lambda$  be a maximal  $R$ -order in a separable  $K$ -algebra  $A$ . Then the maps  $\rho, \omega, \omega'$  above are isomorphisms. In particular, if  $\Lambda \cong M_n(R)$  for some  $R$ , then  $N(\Lambda) \cong \Lambda^\times K$ .*

*Proof.* Given  $(X) \in \text{Picent } \Lambda$ , we may assume by (55.18) that  $X$  is a two-sided  $\Lambda$ -ideal in  $A$  such that  $KX = A$ . Then  ${}_A X \cong {}_A \Lambda$  by Exercise 26.11, so  $(X) \in \text{im } \omega$  by (55.20iii). Thus  $\omega$  gives an isomorphism  $\text{Outcent } \Lambda \cong \text{Picent } \Lambda$  in this case.

Finally, for  $\Lambda = M_n(R)$  we have  $\text{Picent } \Lambda \cong \text{Picent } R = 1$ , so  $N(\Lambda) = \Lambda^* K^*$  as claimed.

In the above proof, the hypothesis that  $\Lambda$  be a maximal order was used only to guarantee that for  $(X) \in \text{Picent } \Lambda$ , the  $(\Lambda, \Lambda)$ -bimodule  $X$  is free as left  $\Lambda$ -module. This property also holds when  $\Lambda$  is a group ring  $RG$  of a finite group  $G$  over a d.v.r.  $R$  of characteristic 0. If  $(X) \in \text{Picent } \Lambda$ , then  $KX \cong KG$  as bimodules, and  ${}_A X$  is a projective  $RG$ -module. By Swan's Theorem 32.1, it follows that  ${}_A X \cong {}_A \Lambda$ . We thus obtain the important result, basic in the calculation of Picard groups of group rings:

$$\text{Picent } RG \cong N(RG)/(RG)^*(KC)^*,$$

where  $N(RG)$  is the normalizer of  $RG$  in  $KG$ , and  $KC$  is the center of  $KG$ .

We shall return to this result in (55.30), but for the moment let us continue with our discussion of maximal orders.

**(55.24) Theorem.** *Let  $R$  be a complete d.v.r., and let  $\Lambda$  be a maximal  $R$ -order in a central simple  $K$ -algebra  $A$  with skewfield part  $D$ . Let  $e = e(D/K)$  be the ramification index of  $D$  over  $K$ , and  $d(\Lambda/R)$  the discriminant. Then*

$$\text{Picent } \Lambda \cong \mathbb{Z}/e\mathbb{Z},$$

and  $\text{Picent } \Lambda = 1$  if  $d(\Lambda/R) = R$ .

*Proof.* Let  $\pi$  be a prime element of  $R$ , and  $\pi_D$  a prime element of  $\Delta$ , where  $\Delta$  is the maximal  $R$ -order in  $D$  (see (26.22)). Then by (26.23),

$$\pi\Delta = (\pi_D\Delta)^e, \quad \text{rad } \Lambda = \pi_D\Lambda,$$

and every two-sided  $\Lambda$ -ideal in  $A$  is a power of  $\text{rad } \Lambda$ . Since  $\text{Picent } \Lambda \cong I(\Lambda)/\{\pi^k\Lambda : k \in \mathbb{Z}\}$ , we obtain  $\text{Picent } \Lambda \cong \mathbb{Z}/e\mathbb{Z}$ . Finally, if  $e > 1$  then  $\pi^{e-1}R$  divides  $d(\Lambda/R)$ , as follows from an easy generalization of Exercise 4.11 (see MO §25). This yields the last assertion in the theorem, and completes the proof.

In order to extend the above to the global case, we must investigate the connection between local and global Picard groups. The key result, valid for nonmaximal orders as well, is the following:

**(55.25) Theorem (Fröhlich [73]).** *Let  $\Lambda$  be any  $R$ -order in a separable  $K$ -algebra  $A$ , where  $R$  is a Dedekind domain with quotient field  $K$ , and let  $C = c(\Lambda)$ . For each maximal ideal  $P$  of  $R$ , let  $\Lambda_P$  denote the  $P$ -adic completion of  $\Lambda$ . Then*

$\text{Picent } \Lambda_P = 1$  a.e., and there is an exact sequence

$$1 \rightarrow \text{Picent } C \xrightarrow{\tau} \text{Picent } \Lambda \xrightarrow{\tau'} \prod_P \text{Picent } \Lambda_P \rightarrow 1.$$

The map  $\tau$  is given by  $\tau(L) = (L \otimes_C \Lambda)$  for  $(L) \in \text{Picent } C$ .

*Proof.* For almost all  $P$ ,  $\Lambda_P$  is a maximal  $R_P$ -order in a direct sum of full matrix algebras over fields. For such  $P$ ,  $\Lambda_P$  is a direct sum of matrix rings over d.v.r.'s, so  $\text{Picent } \Lambda_P = 1$  by (55.9) (or (55.22)).

Now let us make each left  $C$ -module  $L$  into a bimodule centralized by  $C$ . Then  $L \otimes_C \Lambda$  is naturally a  $(\Lambda, \Lambda)$ -bimodule centralized by  $C$ . As usual, let  $I(C)$  denote the group of invertible  $C$ -ideals in  $KC$ . Then for each  $L \in I(C)$ , there is a  $(\Lambda, \Lambda)$ -isomorphism

$$L \otimes_C \Lambda \cong L\Lambda \text{ (computed inside } A).$$

If  $L' = L^{-1}$ , then  $(L\Lambda)(L'\Lambda) = LL'\Lambda = \Lambda$ , so for each  $L \in I(C)$  we have  $L\Lambda \in I(\Lambda)$ . It is now clear that  $\tau$  is a homomorphism, and we must prove  $\tau$  injective.

For any bimodule  ${}_A M_\Lambda$ , let us define

$$M^\Lambda = \{m \in M : \lambda m = m\lambda \text{ for all } \lambda \in \Lambda\}.$$

Then  $M^\Lambda$  is a  $C$ -module, determined up to isomorphism by the class  $(M)$ . Clearly

$$(M \oplus N)^\Lambda = M^\Lambda \oplus N^\Lambda, \quad \text{and} \quad \Lambda^\Lambda = C.$$

We observe next that for  $(L) \in \text{Picent } C$ , we have

$$(L \otimes_C \Lambda)^\Lambda = L \otimes_C C \cong L \text{ as } C\text{-modules.}$$

(The formula is obvious when  $L = C$ , and hence also for every projective  $C$ -module  $L$ .) But now suppose that  $\tau(L) = 1$ ; then  $L \otimes_C \Lambda \cong \Lambda$ , so

$$L \cong (L \otimes_C \Lambda)^\Lambda \cong \Lambda^\Lambda \cong C,$$

which completes the proof that  $\tau$  is a monomorphism.

We show next that  $\tau'$  is surjective, where  $\tau'(X) = \prod_P (X_P)$  for each  $(X) \in \text{Picent } \Lambda$ . To begin with,  $c(\Lambda_P) = C_P$  so  $(X_P) \in \text{Picent } \Lambda_P$  for each  $P$ . Suppose now that for each  $P$ , we are given an element  $X(P) \in I(\Lambda_P)$ , and we wish to find an  $(X) \in \text{Picent } \Lambda$  for which  $\tau'(X) = \prod X(P)$ . Since  $\text{Picent } \Lambda_P = 1$  a.e., we may assume that  $X(P) = \Lambda_P$  a.e. We now set

$$X = A \cap \left( \bigcap_P X(P) \right),$$

a two-sided  $\Lambda$ -ideal of  $A$  such that  $X_P = X(P)$  for all  $P$ . For each  $P$ , let  $Y(P) =$

$X(P)^{-1}$ , and define  $Y$  analogously. Then  $XY = YX = \Lambda$ , since these equalities hold at each  $P$ . Thus  $X \in I(\Lambda)$ , and  $(X) \in \text{Picent } \Lambda$  as desired.

It remains to verify that  $\ker \tau' \leq \text{im } \tau$ , the reverse inclusion being obvious. Let  $X \in I(\Lambda)$  be such that  $\tau'(X) = 1$ , that is,  $(X_P) = 1$  in  $\text{Picent } \Lambda_P$  for each  $P$ . By (55.18), for each  $P$  there exists a unit  $c_P \in c(A_P)$  such that  $X_P = \Lambda_P c_P$ . Further, since  $X_P = \Lambda_P$  a.e., we may choose  $c_P = 1$  a.e. Now set

$$L = KC \cap \left( \bigcap_P C_P c_P \right), \quad L' = KC \cap \left( \bigcap_P C_P c_P^{-1} \right).$$

Then  $L$  and  $L'$  are  $C$ -lattices in  $KC$ , with  $L_P = C_P c_P$ ,  $L'_P = C_P c_P^{-1}$  for each  $P$ . Then  $LL' = C$  since  $L_P L'_P = C_P$  for each  $P$ . It follows that  $(L) \in \text{Picent } C$ , and  $X = L\Lambda$  since  $X_P = L_P \Lambda_P$  for each  $P$ . Thus  $(X) \in \text{im } \tau$ , as claimed, and the theorem is proved.

Before going on, let us show that when  $\Lambda$  is a commutative order, the group  $\text{Picent } \Lambda$  can be described in more familiar terms:

**(55.26) Theorem.** *Let  $\Lambda$  be an  $R$ -order in a f.d. separable commutative  $K$ -algebra  $A$ . There is a canonical isomorphism of groups*

$$\theta: \text{Picent } \Lambda \cong \text{Cl } \Lambda,$$

where  $\text{Cl } \Lambda$  is the locally free class group, defined as in §49.

*Proof.* This is *not* an immediate consequence of (55.16), because the group structures of  $\text{Picent } \Lambda$  and  $\text{Cl } \Lambda$  are different. By (55.18),  $\text{Picent } \Lambda$  consists of isomorphism classes  $(X)$  of locally free  $\Lambda$ -ideals  $X$  in  $A$ . For  $(X), (Y) \in \text{Picent } \Lambda$  we have  $(X) \cdot (Y) = (XY)$ , since  $X \otimes_{\Lambda} Y \cong XY$  (computed inside  $A$ ); note that  $\text{Picent } \Lambda$  is a *multiplicative* group.

On the other hand,  $\text{Cl } \Lambda$  is the *additive* group whose elements are stable isomorphism classes  $[M]$  of locally free  $\Lambda$ -ideals  $M$  in  $A$ . Given  $[M], [M'] \in \text{Cl } \Lambda$ , we have  $[M] + [M'] = [M'']$ , where  $M \oplus M' \cong \Lambda \oplus M''$ . Since  $\Lambda$  is commutative, (49.29) shows that  $\Lambda$  has locally free cancellation, so stable isomorphism coincides with isomorphism. Thus the map  $\theta: \text{Picent } \Lambda \rightarrow \text{Cl } \Lambda$ , given by  $\theta(X) = [X]$ , is a bijection. We must verify that  $\theta$  is a homomorphism of groups.

For each  $(X) \in \text{Picent } \Lambda$ , we may write  $X = \Lambda\alpha$  for some idèle  $\alpha \in J(A)$ , by §49A. For  $\alpha, \beta \in J(A)$ , we have  $\Lambda\alpha \cdot \Lambda\beta = \Lambda\alpha\beta$  since  $\Lambda$  is commutative. On the other hand, (49.8) gives

$$[\Lambda\alpha] + [\Lambda\beta] = [\Lambda\alpha\beta] \quad \text{in } \text{Cl } \Lambda.$$

It follows that  $\theta$  is an isomorphism of groups, as claimed. (See also (55.32) below.)

In particular, we have  $\text{Picent } R \cong \text{Cl } R$ , as already observed in the discussion following (55.5). More generally, let  $C = c(\Lambda)$  be the center of an  $R$ -order  $\Lambda$ , as

in (55.25). Then

$$\text{Picent } C \cong \text{Cl } C$$

by (55.26).

By (55.25), the calculation of  $\text{Picent } \Lambda$  reduces to the following problems:

(i) Determine  $\text{Picent } C$ , that is, the class group  $\text{Cl } C$ . We have studied this question in detail in §§49 and 50.

(ii) Determine  $\text{Picent } \Lambda_P$  for each  $P$ . For  $\Lambda$  an integral group ring  $RG$ , the remarks following (55.23) show that

$$\text{Picent } \Lambda_P \cong \text{Outcent } \Lambda_P \cong N(\Lambda_P)/\Lambda_P^*(K_P C),$$

where  $N(\Lambda_P)$  is the normalizer of  $\Lambda_P$  in  $K_P G$ .

(iii) Find the structure of  $\text{Picent } \Lambda$  as an extension of  $\prod_P \text{Picent } \Lambda_P$  by  $\text{Picent } C$ . Relatively little is known in this direction.

Combining our earlier results, we have:

**(55.27) Theorem (Fröhlich [73]).** *Let  $R$  be a Dedekind domain with quotient field  $K$ , and let  $\Lambda$  be a maximal  $R$ -order in the central simple  $K$ -algebra  $A$ . For each maximal ideal  $P$  of  $R$  dividing the discriminant  $d(\Lambda/R)$ , let  $e_P$  be the ramification index of the skewfield part of  $A_P$  over  $K_P$ . Then there is an exact sequence of abelian groups*

$$1 \rightarrow \text{Cl } R \rightarrow \text{Picent } \Lambda \rightarrow \coprod_{P|d(\Lambda/R)} \mathbb{Z}/e_P \mathbb{Z} \rightarrow 0.$$

If  $K$  is a global field, then for each  $P$ ,  $e_P$  equals the local index  $m_P$  of  $A$  at  $P$ .

*Proof.* In this case  $c(\Lambda) = R$ , and  $\text{Picent } R \cong \text{Cl } R$ . The group  $I(\Lambda)$  is abelian by (26.14), so  $\text{Picent } \Lambda$  is also abelian. The remaining assertions now follow from (55.24) and (26.22iv).

### §55C. Locally Free Picard Groups

Throughout this section, let  $\Lambda$  be an  $R$ -order in a f.d. separable  $K$ -algebra  $A$ , where  $R$  is a Dedekind domain with quotient field  $K$ . Here we shall define the locally free Picard group  $LFP(\Lambda)$  as a certain subgroup of  $\text{Picent } \Lambda$ , and shall derive its main properties. For  $R = \text{alg. int. } \{K\}$  and  $G$  a finite group, we have  $LFP(RG) = \text{Picent } RG$ . Generally speaking,  $LFP$  is easier to calculate than  $\text{Picent}$ . The results in this section are due to Fröhlich [73] and Fröhlich-Reiner-Ullom [74].

**(55.28) Definition.** A  $\Lambda$ -lattice  $M$  is *locally free of rank  $n$*  if  $M_P \cong \Lambda_P^{(n)}$  as  $\Lambda_P$ -

modules, for each maximal ideal  $P$  of  $R$  (equivalently,  $M$  is in the genus of  $\Lambda^{(n)}$ ). Let  $\text{LF}_n(\Lambda)$  denote the set of isomorphism classes of such  $M$ 's.

Now let  ${}_A M_\Delta$  be an invertible bimodule, where  $\Lambda$  and  $\Delta$  are  $R$ -orders in  $A$ . We claim that  $M \in \text{LF}_1(\Lambda)$  if and only if  $M \in \text{LF}_1(\Delta)$ . Passing to  $P$ -adic completions and changing notation briefly, we must show that  ${}_A M \cong \Lambda$  implies  $M_\Delta \cong \Delta$  (and conversely). Suppose that  $M = \Lambda m \cong \Lambda$  for some  $m \in M$ . Since  $M$  is invertible, we obtain

$$\Delta \cong \text{End}_A M \cong \text{End}_\Lambda \Lambda \cong \Lambda^\circ,$$

and thus  $M = m\Delta \cong \Delta$ . Thus, for invertible bimodules the property of being locally free does not depend on whether we use the left or right structure. It also follows readily from the above that if  $M$  is invertible and  $M \in \text{LF}_n(\Lambda)$ , then necessarily  $n = 1$ .

Suppose next that  $M, M'$  are invertible  $(\Lambda, \Lambda)$ -bimodules in  $\text{LF}_1(\Lambda)$ . Then also  $M^{-1}$  and  $M \otimes_\Lambda M'$  lie in  $\text{LF}_1(\Lambda)$ . We may therefore define the *locally free Picard group*  $\text{LFP}(\Lambda)$  as the subgroup of  $\text{Picent } \Lambda$  consisting of all classes of invertible bimodules  ${}_A M_\Lambda$  centralized by  $c(\Lambda)$ , such that  ${}_A M \in \text{LF}_1(\Lambda)$  (or equivalently,  $M_\Lambda \in \text{LF}_1(\Lambda)$ ).

By (55.18), each class  $(M) \in \text{Picent } \Lambda$  can be represented by an invertible two-sided  $\Lambda$ -ideal  $M$  in  $A$ . Let us show at once that any two-sided  $\Lambda$ -ideal  $X$  in  $A$ , such that  ${}_A X \in \text{LF}_1(\Lambda)$ , is necessarily invertible. To prove this, it suffices by (35.4) to check that  $X_P$  is invertible for each  $P$ . Passing to  $P$ -adic completions and changing notation for the moment,  $X$  is a  $(\Lambda, \Lambda)$ -bimodule such that  ${}_A X \cong {}_A \Lambda$ . It follows that  $X$  is invertible, by (55.21). We thus obtain:

**(55.29) Proposition.** *The locally free Picard group  $\text{LFP}(\Lambda)$  consists of all bimodule isomorphism classes  $(M)$  of two-sided  $\Lambda$ -ideals  $M$  in  $A$ , which are locally free as one-sided ideals. If  $M'$  is another such ideal, then<sup>†</sup>  $(M) = (M')$  if and only if  $M' = Mc$  for some  $c \in (KC)$ , where  $C = c(\Lambda)$ .*

If  $R$  is a d.v.r., then for any  $R$ -order  $\Lambda$ ,  $\text{LF}_1(\Lambda)$  consists of all free  $\Lambda$ -modules of rank 1. Hence in this case

$$\begin{aligned} \text{LFP}(\Lambda) &= \{(X) \in \text{Picent } \Lambda : {}_A X \cong {}_A \Lambda\} \\ &= \{({}_A \Lambda_f) : f \in \text{Autcent } \Lambda\} = \text{Outcent } \Lambda, \end{aligned}$$

by (55.22).

Returning to the situation where  $R$  is arbitrary, consider the map  $\tau : \text{Picent } C \rightarrow \text{Picent } \Lambda$  defined in (55.25). Since

$$\text{Picent } C \cong \text{Cl } C \cong \text{LFP}(C)$$

<sup>†</sup>This follows from (55.17).

by (55.26), it is clear that the image of  $\tau$  lies in  $\text{LFP}(\Lambda)$ . In view of the preceding remarks, (55.25) now gives:

**(55.30) Theorem.** *Let  $\Lambda$  be an  $R$ -order (with center  $C$ ) in a f.d. separable  $K$ -algebra  $A$ . There is an exact sequence of groups*

$$1 \rightarrow \text{Cl } C \rightarrow \text{LFP}(\Lambda) \rightarrow \coprod_P \text{Outcent } \Lambda_P \rightarrow 1,$$

with  $\text{Outcent } \Lambda_P = 1$  a.e. We have

$$\text{Outcent } \Lambda_P \cong N(\Lambda_P)/\Lambda_P(K_P C) \quad \text{for each } P,$$

where

$$N(\Lambda_P) = \text{normalizer of } \Lambda_P = \{a \in A_P : a\Lambda_P a^{-1} = \Lambda_P\}.$$

The remarks in §55B show at once that for each finite group  $G$  and  $R = \text{alg. int. } \{K\}$ ,

$$(55.31) \quad \text{LFP}(RG) \cong \text{Picent } RG, \quad \text{and} \quad \text{Picent } R_P G \cong \text{Outcent } R_P G$$

for each  $P$ . Thus, (55.30) gives us a method of calculating Picent for integral group rings.

Generalizing the results in (55.26), we now establish the connection between  $\text{LFP}(\Lambda)$  and the locally free class group  $\text{Cl } \Lambda$ , for an arbitrary  $R$ -order  $\Lambda$ . We begin with a theorem due to Fröhlich-Reiner-Ullom [74]:

**(55.32) Theorem.** *Let  $\Lambda$  be an  $R$ -order in an f.d. separable  $K$ -algebra  $A$ . There is a homomorphism of groups*

$$\theta : \text{LFP}(\Lambda) \rightarrow \text{Cl } \Lambda,$$

given by  $\theta(X) = [X]$  for each  $(X) \in \text{LFP}(\Lambda)$ .

*Proof.* Let  $(X), (Y) \in \text{LFP}(\Lambda)$ ; without loss of generality, we may assume that  $X$  is a two-sided ideal of  $\Lambda$  such that  ${}_X\Lambda \in \text{LF}_1(\Lambda)$ . There is then an exact sequence of  $(\Lambda, \Lambda)$ -bimodules

$$0 \rightarrow X \rightarrow \Lambda \rightarrow T \rightarrow 0,$$

with  $T$  an  $R$ -torsion bimodule. Since  $Y \in \text{LF}_1(\Lambda)$ , the functor  $* \otimes_{\Lambda} Y$  preserves exactness, and we obtain another exact sequence of bimodules:

$$0 \rightarrow X \otimes Y \rightarrow Y \rightarrow T \otimes Y \rightarrow 0,$$

where  $\otimes$  means  $\otimes_{\Lambda}$ . But  $T \otimes Y$  is direct sum of its  $P$ -primary components,

where  $P$  ranges over the maximal ideals of  $R$ . Since  $Y_P \cong \Lambda_P$  as left  $\Lambda_P$ -modules for each  $P$ , it follows that  $T \otimes Y \cong T$  as left  $\Lambda$ -modules. Schanuel's Lemma thus gives a left  $\Lambda$ -isomorphism

$$X \oplus Y \cong \Lambda \oplus (X \otimes Y).$$

In view of the definition of addition in  $\text{Cl } \Lambda$ , we obtain

$$[X] + [Y] = [X \otimes_{\Lambda} Y] \quad \text{in } \text{Cl } \Lambda.$$

Thus  $\theta$  is a homomorphism, as claimed.

Keeping the above notation, let  $X$  be a two-sided  $\Lambda$ -ideal in  $A$ , such that  ${}_A X \in \text{LF}_1(\Lambda)$ . Then for each  $P$ , we may write  $X_P = \Lambda_P x_P$ , and by (55.21) the element  $x_P$  must lie in the normalizer

$$N(\Lambda_P) = \{y \in A_P^{\times} : y\Lambda_P y^{-1} = \Lambda_P\}.$$

Further,  $x_P \in \Lambda_P^{\times}$  a.e., so  $x = (x_P)$  lies in the idèle group  $J(A)$ . We have  $X = \Lambda x$ , where the latter is defined as in (49.5), namely,

$$\Lambda x = A \cap \left\{ \bigcap_P \Lambda_P x_P \right\}.$$

The above discussion suggests that we introduce the *idèle normalizer* of  $\Lambda$ , defined by

$$(55.33) \quad JN(\Lambda) = \{(x_P) \in J(A) : x_P \in N(\Lambda_P) \text{ for each } P\}.$$

Then each class of  $\text{LFP}(\Lambda)$  is of the form  $(\Lambda x)$  for some  $x \in JN(\Lambda)$ . The homomorphism  $\theta$ , defined above, carries  $(\Lambda x)$  onto  $[\Lambda x] \in \text{Cl } \Lambda$ . We note further that for  $x, y \in JN(\Lambda)$  we have

$$\Lambda x \otimes_{\Lambda} \Lambda y \cong \Lambda x \cdot \Lambda y = \Lambda xy,$$

since  $\Lambda x = x\Lambda$  (check  $P$ -adic completions!). Further,  $\Lambda x \cong \Lambda y$  if and only if  $\Lambda x = \Lambda y \cdot c$  for some  $c \in (KC)^{\times}$ , that is,  $x \in U(\Lambda)y(KC)^{\times}$ . It follows that there is a surjective homomorphism  $JN(\Lambda) \rightarrow \text{LFP}(\Lambda)$ , given by  $x \mapsto (\Lambda x)$ , with kernel  $U(\Lambda)(KC)^{\times}$ . This gives

$$(55.34) \quad \text{LFP}(\Lambda) \cong JN(\Lambda)/U(\Lambda)(KC)^{\times}.$$

We now return to the homomorphism  $\theta: \text{LFP}(\Lambda) \rightarrow \text{Cl } \Lambda$  defined in (55.32), and we shall describe its kernel and cokernel under some simplifying hypotheses.

**(55.35) Theorem.** *Let  $\Lambda$  be an  $R$ -order in a f.d. separable  $K$ -algebra  $A$ , where*

$K$  is a global field. Assume that  $\Lambda$  has locally free cancellation. Then there is an exact sequence of groups

$$1 \rightarrow \text{Outcent } \Lambda \xrightarrow{\omega} \text{LFP}(\Lambda) \xrightarrow{\theta} \text{Cl } \Lambda \rightarrow \text{cok } \theta \rightarrow 1,$$

where (using the notation in (49.22))

$$\text{cok } \theta \cong J(A)/J_0(A)A^+JN(\Lambda).$$

*Proof.* Let  $(X) \in \text{LFP}(\Lambda)$  be such that  $\theta(X) = 0$ , that is,  $[X] = [\Lambda]$  in  $\text{Cl } \Lambda$ . Then  $X \cong \Lambda$  as left  $\Lambda$ -modules, since  $\Lambda$  has locally free cancellation by hypothesis. Therefore  $(X) \in \text{im } \omega$  by (55.22iii). Since  $\theta\omega = 0$ , it follows that  $\ker \theta = \text{im } \omega$ .

We next use the formula (49.22)

$$\text{Cl } \Lambda \cong J(A)/J_0(A)A^+U(\Lambda),$$

where  $U(\Lambda)$  is the group of unit idèles, and  $J_0(A) = \{\alpha \in J(A); \text{nr } \alpha = 1\}$ . The image of  $\text{LFP}(\Lambda)$  in this group consists of the classes containing elements of the idele normalizer  $JN(\Lambda)$ , defined by (55.33). Since  $JN(\Lambda) \supseteq U(\Lambda)$ , we obtain the desired formula for  $\text{cok } \theta$ .

**Remarks.** (i) If  $\Lambda$  is a commutative order, it has locally free cancellation by the discussion in (49.29). Further, in this case  $\text{Outcent } \Lambda = 1$  and  $JN(A) = J(A)$ , so (55.35) implies that  $\theta$  is an isomorphism. We have already proved this in (55.26), without the restrictive hypothesis that  $K$  be a global field.

(ii) The formula for  $\text{cok } \theta$ , in terms of idèles, is valid whether or not  $\Lambda$  has locally free cancellation. Further, taking reduced norms, we obtain

$$\text{cok } \theta \cong J(KC)/(KC)^+ \cdot \text{nr } JN(\Lambda).$$

For an ideal-theoretic version of this formula, see Fröhlich-Reiner-Ullom [74, Theorem 5.13].

We now compute  $\text{cok } \theta$  for the case where  $\Lambda$  is a maximal order, again keeping the hypotheses of (55.35). It suffices to treat the case where  $A$  is simple, and we begin by fixing the notation. Let  $A$  be a central simple  $K$ -algebra, where  $K$  is a global field, and set  $\dim_K A = n^2$ . Let  $\Lambda$  be a maximal  $R$ -order in  $A$ , so by (49.32) there is an isomorphism

$$\text{Cl } \Lambda \cong \text{Cl}_A R = I(R)/P_A(R).$$

The isomorphism may be described thus: each element of  $\text{Cl } \Lambda$  is of the form  $\Lambda\alpha$ , with  $\alpha = (\alpha_p) \in J(A)$ . Then  $\Lambda\alpha$  is a left  $\Lambda$ -ideal in  $A$ , whose reduced norm

$\text{nr}(\Lambda\alpha)$  is an  $R$ -ideal in  $K$ . For each maximal ideal  $P$  of  $R$ , we have

$$(\text{nr } \Lambda\alpha)_P = \text{nr } \Lambda_P \alpha_P = R_P \text{nr } \alpha_P$$

(see MO(24.11)). Viewing  $\text{nr } \alpha$  as element of the idèle group  $J(K)$ , we obtain

$$\text{nr } \Lambda\alpha = R \text{nr } \alpha = K \cap \left\{ \bigcap_P R_P \text{nr } \alpha_P \right\}.$$

The isomorphism  $\text{Cl } \Lambda \cong \text{Cl}_A R$  carries  $[\Lambda\alpha]$  onto the class of  $R \text{nr } \alpha$  in  $\text{Cl}_A R$ .

We now define a homomorphism

$$t_n: \text{Cl } R \rightarrow \text{Cl}_A R, \quad \text{by } t_n(a) = (a^n)$$

for each  $R$ -ideal  $a$  in  $K$ . In order for the map to be well-defined, we must have  $Ra^n \in P_A(R)$  for each  $a \in K$ . If no infinite prime of  $K$  ramifies in  $A$ , then  $P_A(R) = P(R)$ . On the other hand, if some infinite prime of  $K$  does ramify in  $A$ , then  $n$  must be even. In either case, we conclude that  $Ra^n \in P_A(R)$ , so  $t_n$  is a well-defined homomorphism.

Before stating our results, we need one more definition, already encountered in (45.14). For each prime  $P$  of  $K$ , we may write

$$A_P \cong M_{\kappa_P}(\Omega(P)), \quad \dim_{K_P} \Omega(P) = m_P^2, m_P \kappa_P = n,$$

where  $\Omega(P)$  is a skewfield with center  $K_P$  and index  $m_P$ . We call  $m_P$  the *local index* of  $A$  at  $P$ , and  $\kappa_P$  the *local capacity*. We now prove:

**(55.36) Theorem.** *Let  $\Lambda$  be a maximal  $R$ -order in a central simple  $K$ -algebra  $A$ , where  $K$  is a global field and  $A$  is not a totally definite quaternion algebra. Keeping the above notation, there is an exact sequence of groups*

$$(55.37) \quad 1 \rightarrow \ker t_n \rightarrow \ker \theta \rightarrow \prod_P \mathbb{Z}/m_P \mathbb{Z} \rightarrow \text{cok } t_n \rightarrow \text{cok } \theta \rightarrow 1,$$

where  $\theta: \text{LFP}(\Lambda) \rightarrow \text{Cl } \Lambda$  is as in (55.32).

Further, let  $V$  be the subgroup of the class group  $\text{Cl}_A R$  generated by all  $\{P^{\kappa_P}: m_P > 1\}$ . Then

$$(55.38) \quad \text{cok } \theta \cong \frac{\text{Cl}_A R}{t_n(\text{Cl } R) \cdot V}.$$

*Proof.* By the proof of (55.24), we know that  $\text{Picent } \Lambda_P \cong \mathbb{Z}/m_P \mathbb{Z}$  (see also (55.27)), and that  $\text{Picent } \Lambda_P$  is generated by the class  $(\text{rad } \Lambda_P)$ . Further, the proof of (55.24) shows that  $\text{Picent } \Lambda = \text{LFP}(\Lambda)$ , since each invertible  $(\Lambda, \Lambda)$ -bimodule must be locally free. We claim next that there is a commutative diagram with

exact rows:

$$\begin{array}{ccccccc} 1 & \longrightarrow & \text{Cl } R & \longrightarrow & \text{LFP}(\Lambda) & \longrightarrow & \prod_P \mathbb{Z}/m_p \mathbb{Z} \longrightarrow 1 \\ & & t_n \downarrow & & \theta \downarrow & & \downarrow \\ 1 & \longrightarrow & \text{Cl}_A R & \longrightarrow & \text{Cl } \Lambda & \longrightarrow & 1 \end{array}$$

The top row is given by (55.27), and  $\sigma$  is the inverse of the isomorphism  $\text{Cl } \Lambda \cong \text{Cl}_A R$  coming from the reduced norm map. To check commutativity, let  $\alpha$  be an ideal of  $R$ . Its image in  $\text{LFP}(\Lambda)$  is then  $(\Lambda\alpha)$ , which maps to  $[\Lambda\alpha] \in \text{Cl } \Lambda$ . Then

$$\sigma^{-1}[\Lambda\alpha] = (\text{nr } \Lambda\alpha) = (\alpha^n) = t_n(\alpha),$$

so the left-hand square commutes. The exact sequence (55.37) now comes from the Snake Lemma.

It remains to check the formula for  $\text{cok } \theta$ , and for this we must compute the image of  $\prod_P \mathbb{Z}/m_p \mathbb{Z}$  in  $\text{cok } t_n$ . Now  $\mathbb{Z}/m_p \mathbb{Z} \cong \text{Picent } \Lambda_p$ , and  $\text{Picent } \Lambda_p$  is a cyclic group of order  $m_p$  with generator  $(\text{rad } \Lambda_p)$ . Since  $\text{nr}(\text{rad } \Lambda_p) = P^{\kappa_p}$  (see MO(25.11)), the image of  $\mathbb{Z}/m_p \mathbb{Z}$  in  $\text{cok } t_n$  is the group generated by the class of  $P^{\kappa_p}$ . This gives formula (55.38) at once.

It should be remarked that in formula (55.38), we may replace  $V$  by the group  $\tilde{V}$  generated by all  $\{P^{\kappa_p} : P \text{ arbitrary}\}$ . For if  $P$  is such that  $m_p = 1$ , then necessarily  $\kappa_p = n$ , and so  $P^{\kappa_p} \in \text{im } t_n$ .

We have seen in (55.9) that Morita equivalent rings have isomorphic Picard groups. On the other hand, if  $\Lambda$  is an  $R$ -order and  $\Gamma = M_n(\Lambda)$ , then by §49 we have  $\text{Cl } \Lambda \cong \text{Cl } \Gamma$ . It is of interest to combine these facts with the sequence in (55.35) relating Picard groups and class groups. The results below are due to Fröhlich-Reiner-Ullom [74]:

**(55.39) Theorem.** *Let  $\Lambda$  be an  $R$ -order in a f.d. separable  $K$ -algebra  $A$ , where  $K$  is a global field, and where  $\Lambda$  has locally free cancellation. Let  $n \geq 1$  and set  $E = M_n(R)$ , and*

$$\Gamma = E \otimes_R \Lambda \cong M_n(\Lambda).$$

*Then  $\Gamma$  also has locally free cancellation, and we have:*

- (i) *There is a commutative diagram with exact rows*

$$\begin{array}{ccccccc} 1 & \longrightarrow & \text{Outcent } \Lambda & \xrightarrow{\omega} & \text{LFP}(\Lambda) & \xrightarrow{\theta} & \text{Cl } \Lambda \\ & & \alpha \downarrow & & \beta \downarrow & & \gamma \downarrow \\ 1 & \longrightarrow & \text{Outcent } \Gamma & \xrightarrow{\omega'} & \text{LFP}(\Gamma) & \xrightarrow{\theta'} & \text{Cl } \Gamma, \end{array}$$

where  $\alpha(f) = 1 \otimes f$  for  $f \in \text{Outcent } \Lambda$ , and where  $\beta$  and  $\gamma$  are given by the “change of rings” functor  $E \otimes_R *$ . The map  $\beta$  is an isomorphism.

(ii) For the above map  $\gamma: \text{Cl } \Lambda \rightarrow \text{Cl } \Gamma$ , we have

$$\ker \gamma \cong (\text{Cl } \Lambda)_n, \quad \text{cok } \gamma \cong (\text{Cl } \Lambda)/(n \cdot \text{Cl } \Lambda),$$

where

$$(\text{Cl } \Lambda)_n = \{\xi \in \text{Cl } \Lambda : n\xi = 0\}, \quad n \cdot \text{Cl } \Lambda = \{n\xi : \xi \in \text{Cl } \Lambda\}.$$

(iii) There is an exact sequence of groups

$$1 \rightarrow \text{Outcent } \Lambda \xrightarrow{\alpha} \text{Outcent } \Gamma \xrightarrow{\mu} (\text{Cl } \Lambda)_n \rightarrow \text{cok } \theta \rightarrow \text{cok } \theta'$$

$$\rightarrow (\text{Cl } \Lambda)/(n \cdot \text{Cl } \Lambda) \rightarrow 0.$$

*Proof.* It will be convenient to identify  $\text{Cl } \Lambda$  with a subgroup of  $SK_0(\Lambda)$  as in (49.15). Thus

$$\text{Cl } \Lambda = \{[\Lambda] - [M] : M \in g(\Lambda)\}.$$

The Morita equivalence  $\Lambda \sim \Gamma$  gives an isomorphism  $\varphi: \text{Cl } \Lambda \cong \text{Cl } \Gamma$ , which we may describe as follows. Let  $L = R^{(n)} \otimes_R \Lambda$ , a  $(\Gamma, \Delta)$ -bimodule giving a Morita equivalence between the orders  $\Lambda$  and  $\Gamma$ . To each left  $\Lambda$ -module  $X$  there corresponds a left  $\Gamma$ -module  $L \otimes_{\Lambda} X$ , and this correspondence is bijective on isomorphism classes. There is an isomorphism  $\varphi: K_0(\Lambda) \cong K_0(\Gamma)$ , given by  $[X] \mapsto [L \otimes_{\Lambda} X]$  for  $X \in \mathcal{P}(\Lambda)$ . Then  $\varphi$  induces an isomorphism  $\text{Cl } \Lambda \cong \text{Cl } \Gamma$ , again denoted by  $\varphi$ , and we have (for  $M \in g(\Lambda)$ )

$$\begin{aligned} \varphi([\Lambda] - [M]) &= [L \otimes_{\Lambda} \Lambda] - [L \otimes_{\Lambda} M] \\ &= [L \otimes_{\Lambda} \Lambda^{(n)}] - [L \otimes_{\Lambda} (\Lambda^{(n-1)} \oplus M)]. \end{aligned}$$

Since  $\Gamma \cong L^{(n)} \cong L \otimes_{\Lambda} \Lambda^{(n)}$  as left  $\Gamma$ -modules, we obtain

$$\varphi([\Lambda] - [M]) = [\Gamma] - [L \otimes_{\Lambda} (\Lambda^{(n-1)} \oplus M)] \in \text{Cl } \Gamma.$$

The above formula exhibits  $\varphi([\Lambda] - [M])$  as a difference of locally free left ideals of  $\Gamma$ . It follows readily from the above that if  $\Lambda$  has locally free cancellation, then so does  $\Gamma$ . (The converse may be false, however! See (51.2) and (51.24).)

We now write  $\Gamma = E \otimes_R \Lambda$ ; if  $C = \text{center of } \Lambda$ , then  $1 \otimes C = \text{center of } \Gamma$ . By Exercise 55.1, there is an isomorphism  $\text{Pic}_R \Lambda \cong \text{Pic}_R \Gamma$ , given by  $(X) \mapsto (E \otimes_R X)$  for  $(X) \in \text{Pic}_R \Lambda$ . This induces an isomorphism  $\text{Picent } \Lambda \cong \text{Picent } \Gamma$ , which commutes with taking  $P$ -adic completion for  $P$  a maximal ideal of  $R$ . It follows that there is an isomorphism  $\beta: \text{LFP}(\Lambda) \cong \text{LFP}(\Gamma)$ , induced by the functor  $\Gamma \otimes_{\Lambda} *$ , or equivalently, by  $E \otimes_R *$ . The remaining assertions in (i) above are obvious from (55.35).

Now let  $\varphi: \text{Cl } \Lambda \cong \text{Cl } \Gamma$  be as above, and let  $\gamma: \text{Cl } \Lambda \rightarrow \text{Cl } \Gamma$  be the map given by  $\Gamma \otimes_{\Lambda} *$ . Then  $\gamma = n\varphi$  by Exercise 55.2, and the assertions in (ii) are clear. It remains to establish the exactness of the sequence in (iii). For this purpose, consider the commutative diagram with exact rows:

$$\begin{array}{ccccccc} 1 & \longrightarrow & \text{LFP}(\Lambda) & \xrightarrow{\beta} & \text{LFP}(\Gamma) & \longrightarrow & 1 \\ & & \downarrow \theta & & \downarrow \theta' & & \\ 0 & \longrightarrow & \ker \gamma & \longrightarrow & \text{Cl } \Lambda & \longrightarrow & \text{Cl } \Gamma \end{array}$$

The Snake Lemma gives

$$1 \rightarrow \ker \theta \rightarrow \ker \theta' \rightarrow \ker \gamma \rightarrow \text{cok } \theta \xrightarrow{\gamma_*} \text{cok } \theta',$$

where  $\gamma$  induces  $\gamma_*$ . Then

$$\text{cok } \gamma_* = \frac{(\text{Cl } \Gamma)/\text{im } \theta'}{\gamma_* \{(\text{Cl } \Lambda)/\text{im } \theta\}} \cong \frac{\text{Cl } \Gamma}{\gamma(\text{Cl } \Lambda)} = \text{cok } \gamma,$$

which completes the proof of (iii) and the theorem.

As an immediate consequence of the above theorem, we see that the group  $\text{Outcent } \Gamma/\text{im}(\text{Outcent } \Lambda)$  has exponent  $n$ . Thus we obtain:

**(55.40) Corollary.** *Keep the notation and hypotheses of (55.39), so  $\Gamma = M_n(\Lambda)$ . Then*

(i) *For each  $f \in \text{Autcent } \Gamma$ , we have  $f^n = (1 \otimes g)\eta$  for some  $g \in \text{Autcent } \Lambda$  and some inner automorphism  $\eta$  of  $\Gamma$ .*

(ii) *For  $\Lambda$  a commutative  $R$ -order, we have*

$$\text{Outcent } M_n(\Lambda) \cong (\text{Cl } \Lambda)_n.$$

*Hence for each  $f \in \text{Autcent } M_n(\Lambda)$ ,  $f^n$  is an inner automorphism of  $M_n(\Lambda)$ .*

*Proof.* Assertion (i) is clear. For (ii), use (55.39 iii) together with the facts that  $\text{Outcent } \Lambda = 0$  and that  $\theta$  is an isomorphism.

As a special case of (55.40ii), we obtain

$$\text{Out}_R M_n(R) \cong (\text{Cl } R)_n,$$

a result due originally to Rosenberg-Zelinsky [61].

## §55D. Radical Reduction

The results in this section are all due to Fröhlich [73]. Let  $\Lambda$  be an  $R$ -algebra, where  $R$  is a commutative ring, and let  $J = \text{rad } \Lambda$ . Our aim here is to compare  $\text{Pic}_R \Lambda$  with  $\text{Pic}_R \Lambda/J^m$ , for  $m \geq 1$ . We assume throughout that  $\Lambda$  is a semilocal ring, that is,  $\Lambda/J$  is a semisimple artinian ring. (This is surely the case if  $\Lambda$  is a f.d. algebra over a field, or an algebra over a d.v.r., finitely generated as module; see §5.) By Exercises 55.7 and 55.8, for each  $(X) \in \text{Pic}_R \Lambda$ ,  $X/J^m X$  is an invertible bimodule over  $\Lambda/J^m$ , so “reduction mod  $J^m$ ” gives a homomorphism

$$\rho: \text{Pic}_R \Lambda \rightarrow \text{Pic}_R \Lambda/J^m.$$

To determine  $\ker \rho$ , we use two facts repeatedly: first, for  $m \geq 1$ , the map  $\Lambda^\cdot \rightarrow (\Lambda/J^m)^\cdot$  is surjective, by (50.7); second, by Nakayama’s Lemma, any homomorphism which is an isomorphism mod  $J^m$  is itself an isomorphism.

For each  $f \in \text{Aut}_R \Lambda$ ,  $f(J^m) = J^m$  for  $m \geq 1$ , so  $f$  induces  $\bar{f} \in \text{Aut}_R \Lambda/J^m$ . Let us define a relative automorphism group

$$\text{Aut}_R(\Lambda, J^m) = \{f \in \text{Aut}_R \Lambda : \bar{f} = 1 \text{ on } \Lambda/J^m\}.$$

As in (55.11), there is a homomorphism

$$\omega: \text{Aut}_R(\Lambda, J^m) \rightarrow \text{Pic}_R \Lambda, \quad \text{given by } \omega(f) = ({}_1 \Lambda_f),$$

and  $\ker \omega = (\text{In } \Lambda) \cap \text{Aut}_R(\Lambda, J^m)$ . We now prove:

**(55.41) Theorem (Fröhlich).** *Let  $\Lambda$  be a semilocal  $R$ -algebra, and let  $J = \text{rad } \Lambda$ . For  $m \geq 1$ , there is an exact sequence of groups*

$$\text{Aut}_R(\Lambda, J^m) \xrightarrow{\omega} \text{Pic}_R \Lambda \xrightarrow{\rho} \text{Pic}_R \Lambda/J^m.$$

Further, if  $m \geq 2$  and  $J^{m+1} = 0$ , the sequence

$$H^1(\Lambda/J^2, J^m) \rightarrow \text{Pic}_R \Lambda \rightarrow \text{Pic}_R \Lambda/J^m$$

is exact.

*Proof.* It is obvious that  $\rho \omega = 1$ . Now let  $(X) \in \text{Pic}_R \Lambda$  be such that  $\rho(X) = 1$ , so there is a bimodule isomorphism  $\varphi: \bar{X} \cong \bar{\Lambda}$ , where bars indicate reduction mod  $J^m$ . We may lift  $\varphi$  to a left  $\Lambda$ -homomorphism  $f: X \rightarrow \Lambda$ ; since  $f(\text{mod } J^m) = \varphi$ ,  $f$  is an isomorphism  $X \cong \Lambda$ . By (55.11) we conclude that  $X \cong {}_1 \Lambda_g$  as bimodules, for some  $g \in \text{Aut}_R \Lambda$ . Then  ${}_1 \bar{\Lambda}_{\bar{g}} \cong \bar{\Lambda}$  as  $\bar{\Lambda}$ -bimodules, so by (55.11)  $\bar{g}$  is an inner automorphism of  $\bar{\Lambda}$ . Hence there exists  $u \in \Lambda^\cdot$  such that  $\bar{g} = (i_u)^{-1}$ . But then in  $\text{Pic}_R \Lambda$  we have

$$(X) = ({}_1 \Lambda_g) = ({}_1 \Lambda_{i_u g}) = \omega(i_u g)$$

and  $i_u g \in \text{Aut}_R(\Lambda, J^m)$ . This proves the exactness of the first sequence.

Now let  $m \geq 2$  and assume that  $J^{m+1} = 0$ . By definition (see Volume I, p. 541), the cohomology group  $H^1$  is given by

$$H^1(\Lambda/J^2, J^m) = \text{Der}_R(\Lambda/J^2, J^m)/\text{inner derivations}.$$

The numerator is the  $R$ -module consisting of all derivations  $d: \Lambda/J^2 \rightarrow J^m$ , that is, all  $R$ -linear maps  $d$  such that

$$d(x, y) = xdy + (dx)y \quad \text{for } x, y \in \Lambda/J^2.$$

The inner derivations are those given by  $d(x) = xb - bx$ ,  $x \in \Lambda/J^2$ , for some  $b \in J^m$ . But  $J^{m+1} = 0$ , so for each  $d \in \text{Der}_R(\Lambda, J^m)$  we have  $d(J^2) = 0$ , and thus

$$\text{Der}_R(\Lambda, J^m) = \text{Der}_R(\Lambda/J^2, J^m)$$

in this case.

We note next that there is an  $R$ -isomorphism

$$\text{Der}_R(\Lambda/J^2, J^m) \cong \text{Aut}_R(\Lambda, J^m),$$

in which the derivation  $d$  corresponds to the automorphism  $f$ , where

$$f(\lambda) = \lambda + d\lambda \quad \text{for } \lambda \in \Lambda.$$

(It is easily checked that  $f$  is an automorphism if and only if  $d$  is a derivation.) Further, if  $d$  is an inner derivation, say  $d\lambda = \lambda b - b\lambda$  for all  $\lambda \in \Lambda$ , then

$$f(\lambda) = \lambda + \lambda b - b\lambda = (1 + b)^{-1}\lambda(1 + b) \quad \text{for } \lambda \in \Lambda,$$

so  $f$  is inner. It follows that there is a homomorphism from  $H^1(\Lambda/J, J^m)$  into  $\text{Pic}_R \Lambda$ , whose image is precisely  $\ker \rho$ . This completes the proof.

**(55.42) Corollary.** *Keep the above notation and hypotheses, and suppose that  $c(\Lambda) \rightarrow c(\Lambda/J)$  is surjective. Then so is*

$$\text{Autcent } \Lambda \rightarrow \text{Picent } \Lambda.$$

*Proof.* We choose  $R = C$  in the preceding, where  $C = c(\Lambda)$ . Since  $C \rightarrow c(\Lambda/J)$  is surjective,  $\text{Pic}_R \Lambda/J = \text{Picent } \Lambda/J = 1$  because  $\Lambda/J$  is semisimple. The result is now clear since  $\text{Aut}_C(\Lambda, J)$  is a subgroup of  $\text{Autcent } \Lambda$ .

**(55.43) Corollary.** *Let  $\Lambda$  be a finite ring. Then*

- (i)  $\text{Pic } \Lambda$  is finite.
- (ii) Let  $J = \text{rad } \Lambda$ , and let  $\rho: \text{Pic } \Lambda \rightarrow \text{Pic } \Lambda/J^2$  be the map defined in (55.41), given by reduction mod  $J^2$ . If  $\Lambda$  is  $p$ -torsion for some prime  $p$ , then  $\ker \rho$  is a finite  $p$ -group.

*Proof.* By (55.13), there is an exact sequence

$$1 \rightarrow \text{Picent } \Lambda/J \rightarrow \text{Pic } \Lambda/J \rightarrow \text{Aut } c(\Lambda/J).$$

But  $\text{Picent } \Lambda/J = 1$  since  $\Lambda/J$  is a semisimple artinian ring. Therefore  $\text{Pic } \Lambda/J$  is finite.

Taking  $R = \mathbb{Z}$  in (55.41), we obtain an exact sequence

$$\text{Aut}(\Lambda, J) \rightarrow \text{Pic } \Lambda \rightarrow \text{Pic } \Lambda/J.$$

It follows that  $\text{Pic } \Lambda$  is finite, as claimed.

Now assume that  $\Lambda$  is  $p$ -torsion, so  $p^k \Lambda = 0$  for some  $k > 0$ . For  $n \geq 2$ , let

$$L_n = \ker \left\{ \text{Pic} \frac{\Lambda}{J^n} \rightarrow \text{Pic} \frac{\Lambda}{J^{n-1}} \right\}.$$

so  $L_2 = \{1\}$ , and  $L_n = \ker \rho$  for large  $n$ . To show that  $L_n$  is a  $p$ -group, use induction on  $n$ . Let  $n > 2$ , and suppose that  $L_{n-1}$  is a  $p$ -group. There is a commutative diagram

$$\begin{array}{ccc} \text{Pic} \frac{\Lambda}{J^n} & \xrightarrow{\mu} & \text{Pic} \frac{\Lambda}{J^{n-1}} \\ & \searrow & \downarrow \\ & & \text{Pic} \frac{\Lambda}{J^2} \end{array}$$

so  $\mu: L_n \rightarrow L_{n-1}$ . We now apply the second part of (55.41), with  $\Lambda$  replaced by  $\Lambda/J^n$ ,  $J$  replaced by  $J/J^n = \text{rad } \Lambda/J^n$ , and  $J^m$  replaced by  $J^{n-1}/J^n$ . We obtain an exact sequence

$$H^1 \left( \frac{\Lambda}{J^2}, \frac{J^{n-1}}{J^n} \right) \rightarrow \text{Pic} \frac{\Lambda}{J^n} \xrightarrow{\mu} \text{Pic} \frac{\Lambda}{J^{n-1}}.$$

Therefore  $\ker(L_n \rightarrow L_{n-1}) \leq \text{im } H^1$ ; but  $\Lambda/J^2$  is  $p$ -torsion, whence so is  $\text{im}(H^1)$ , which shows that  $L_n$  is a  $p$ -group. This completes the proof.

For the remainder of this section, let  $R$  be a d.v.r. with maximal ideal  $P = \pi R$ , and quotient field  $K$ . Let  $\Lambda$  be an  $R$ -order in a f.d. separable  $K$ -algebra  $A$ , and let  $C = c(\Lambda)$  be the center of  $\Lambda$ . We wish to study the behavior of  $\text{Picent } \Lambda$  under reduction mod  $P^m$  for sufficiently large  $m$ . For  $m \geq 1$ , there is a homomorphism

$$\text{Picent } \Lambda \rightarrow \text{Pic}_R \Lambda/P^m, \quad \text{given by } (X) \rightarrow (X/P^m X).$$

We intend to prove that this map is injective for large  $m$ . Some notation is

required in order to state the result. For  $(X) \in \text{Picent } \Lambda$  and  $m \geq 1$ , define

$$\begin{aligned} T^m(X) &= \{x \in X : xa - ax \in P^m X \text{ for all } a \in \Lambda\}, \\ X^\Lambda &= \{x \in X : xa = ax \text{ for all } a \in \Lambda\}. \end{aligned}$$

Then  $X^\Lambda$  is a  $C$ -submodule of  $T^m(X)$ . Note that  $\Lambda^\Lambda = C$ , and  $C \subseteq T^m(\Lambda)$ .

The main result is as follows:

**(55.44) Theorem.** *Let  $(X) \in \text{Picent } \Lambda$ . Then*

$$(55.45) \quad T^n(X) \subseteq X^\Lambda + PX$$

for all sufficiently large  $n$ . For each such  $n$ , the homomorphism

$$\text{Picent } \Lambda \rightarrow \text{Pic}_R \Lambda / P^n \Lambda$$

is injective.

*Proof.* Step 1. Since  $A$  is a f.d. separable  $K$ -algebra, there is a nonzero ideal  $i(\Lambda)$  of  $R$  with the property that

$$i(\Lambda) \cdot H^1(\Lambda, X) = 0$$

for each  $(\Lambda, \Lambda)$ -bimodule  $X$ . Here,  $H^1$  is a cohomology group, defined as in (25.9). The largest ideal  $i(\Lambda)$  with this property is called the *Higman ideal* of  $\Lambda$ ; see Volume I, §29A, or CR (75.11). It follows that there exists an integer  $e \geq 0$  such that

$$\pi^e H^1(\Lambda, X) = 0 \quad \text{for all } X.$$

Let us show that

$$(55.46) \quad T^{m+e}(X) \subseteq X + P^m X \quad \text{for } m \geq 1,$$

which will imply (55.45) for all  $n \geq e + 1$ . Fix  $x \in T^{m+e}(X)$ ; then for each  $a \in \Lambda$ , we may write

$$xa - ax = \pi^{m+e} d(a), \quad \text{where } d(a) \in X.$$

This equation uniquely determines  $d(a)$ , since  $X$  is  $R$ -torsionfree. It is easily checked that the map  $d: \Lambda \rightarrow X$  is a derivation (see (25.7)), and thus determines a cohomology class in  $H^1(\Lambda, X)$ . Then  $\pi^e d$  is an inner derivation, so there exists an element  $y \in X$  such that

$$\pi^e d(a) = ya - ay \quad \text{for all } a \in \Lambda.$$

Therefore

$$xa - ax = \pi^m(ya - ay) \quad \text{for all } a \in \Lambda,$$

which proves that  $x - \pi^m y \in X^\Lambda$ . This establishes (55.46), as well as (55.45) for  $n \geq e + 1$ .

*Step 2.* Now let  $n \geq 1$  be such that (55.45) holds, and let  $(X) \in \text{Picent } \Lambda$ . We write

$$X_n = X/P^n X, \quad \Lambda_n = \Lambda/P^n \Lambda, \quad R_n = R/P^n.$$

We must show that if  $(X_n) = 1$  in  $\text{Pic}_R \Lambda_n$ , then  $(X) = 1$  in  $\text{Picent } \Lambda$ . Without loss of generality, we may assume that  $X$  is an invertible two-sided  $\Lambda$ -ideal in  $A$ , and that  $KX = A$ .

Since  $(X_n) = 1$  in  $\text{Pic}_R \Lambda_n$ , there is a bimodule isomorphism  $\theta: X_n \cong \Lambda_n$  which commutes with the action of  $R$ . It follows that  $\theta$  maps  $\pi X_n$  isomorphically onto  $\pi \Lambda_n$ , and also that  $\theta$  gives an isomorphism

$$T^n(X)/P^n X \cong T^n(\Lambda)/P^n \Lambda.$$

Now consider the commutative diagram with exact rows

$$\begin{array}{ccccccc} 0 & \longrightarrow & \frac{\pi X}{\pi^n X} & \longrightarrow & \frac{T^n(X) + PX}{P^n X} & \longrightarrow & 0 \\ & & \downarrow \theta_1 & & \downarrow \theta_2 & & \downarrow \theta_3 \\ 0 & \longrightarrow & \frac{\pi \Lambda}{\pi^n \Lambda} & \longrightarrow & \frac{T^n(\Lambda) + P\Lambda}{P^n \Lambda} & \longrightarrow & 0 \end{array}$$

Then  $\theta_1$  and  $\theta_2$  are isomorphisms, whence so is  $\theta_3$ .

By (55.45) we have (since  $X^\Lambda \subseteq T^n(X)$ )

$$T^n(X) + PX = X^\Lambda + PX = (X \cap KC) + PX,$$

and therefore

$$\{T^n(X) + PX\}/PX \cong X^\Lambda/(X^\Lambda \cap PX).$$

But  $X^\Lambda = X \cap KC$ , which is an  $R$ -pure  $C$ -submodule of  $X$ , and therefore  $X^\Lambda \cap PX = P \cdot X^\Lambda$ . Thus  $\theta_3$  gives an isomorphism (of  $C$ -modules)

$$X^\Lambda/PX^\Lambda \cong \Lambda^\Lambda/P\Lambda^\Lambda = C/PC.$$

It follows from (30.11) that  $X^\Lambda$  is projective as  $C$ -module, and then  $X^\Lambda \cong C$  by (6.6).

*Step 3.* There is a  $(\Lambda, \Lambda)$ -bimodule homomorphism

$$\psi: X^\Lambda \otimes_C \Lambda \rightarrow X, \quad \text{given by } x \otimes a \mapsto xa \quad \text{for } x \in X^\Lambda, \quad a \in \Lambda.$$

We shall show that  $\psi$  is a surjection. Since  $X^\Lambda \otimes_C \Lambda$  and  $X$  are  $R$ -lattices of the same  $R$ -rank, it will then follow that  $\psi$  is an isomorphism. This will imply  $X = C \otimes_C \Lambda \cong \Lambda$  as bimodules, i.e.,  $(X) = 1$  in  $\text{Picent } \Lambda$ , as desired.

To prove  $\psi$  surjective, we note first that there is a bimodule isomorphism

$$(X_n)^\Lambda \otimes_{c(\Lambda_n)} \Lambda_n \cong X_n,$$

since  $X_n \cong \Lambda_n$  as bimodules. Further, we have

$$(X_n)^\Lambda = T^n(X)/P^n X.$$

Consequently we obtain

$$X = T^n(X)\Lambda + P^n X,$$

so also (by (55.45))

$$X = T^n(X)\Lambda + PX = X^\Lambda \cdot \Lambda + PX.$$

Nakayama's Lemma then gives  $X = X^\Lambda \cdot \Lambda$ , so  $\psi$  is surjective, and the theorem is proved.

Combining the above with Theorem 55.41 and its corollaries, we deduce:

**(55.57) Corollary (Fröhlich [73]).** *Let  $\Lambda$  be as in (55.44), and suppose that  $R/P$  is a finite field. Then  $\text{Picent } \Lambda$  is a finite group, and so is<sup>†</sup>  $N(\Lambda)/\Lambda^*(KC)^*$ .*

*Proof.* For sufficiently large  $n$ ,  $\text{Picent } \Lambda$  maps injectively into  $\text{Pic}_R \Lambda / P^n \Lambda$ , which is finite by (55.43i). Further,  $N(\Lambda)/\Lambda^*(KC)^*$  is isomorphic to  $\text{Outcent } \Lambda$  by (55.22), and  $\text{Outcent } \Lambda$  maps injectively into  $\text{Picent } \Lambda$ .

## §55E. Picard Groups of Group Rings

Throughout this section, let  $R$  be a Dedekind domain with quotient field  $K$ , and let  $G$  be a finite group such that  $\text{char } K \nmid |G|$ . Set  $\Lambda = RG$ ,  $A = KG$ , so  $\Lambda$  is an  $R$ -order in the f.d. separable  $K$ -algebra  $A$ . Let  $C = c(\Lambda)$ .

We begin with an easy result:

**(55.48) Proposition.** *Let  $R$  be a d.v.r. with residue class field  $k = R/P$ . If  $\text{char } k \nmid |G|$ , then  $\text{Picent } RG = 1$ .*

<sup>†</sup>We use the notation of (55.30).

*Proof.* The hypothesis implies that  $|G| \in R^\times$ , so  $\Lambda$  is a separable  $R$ -algebra (see Exercise 55.3), and is therefore a central separable  $C$ -algebra. Thus  $\text{Picent } \Lambda \cong \text{Picent } C$ , and  $\text{Picent } C = 1$  by (55.16).

For another proof, let  $\tilde{\Lambda}$  be the  $P$ -adic completion of  $\Lambda$ . Then  $\tilde{\Lambda}$  is a maximal order in a direct sum of full matrix algebras over fields (see (74.11)), so  $\text{Picent } \tilde{\Lambda} = 1$ . Now use Exercise 55.11.

Somewhat more difficult is the following result of Fröhlich [73].

**(55.49) Theorem.** *Let  $R$  be a d.v.r. with finite residue class field  $k = R/P$ , and let  $G$  be a  $p$ -group, where  $p$  is prime. Then  $\text{Picent } RG$  is also a finite  $p$ -group.*

*Proof.* If  $\text{char } k \neq p$ , then  $\text{Picent } RG = 1$  by (55.48). Hence we may assume from now on that  $\text{char } k = p$ . By Exercise 55.9, there is a homomorphism

$$\rho: \text{Picent } \Lambda \rightarrow \text{Pic}_R \Lambda/J^2,$$

where  $J = \text{rad } \Lambda$ , and  $\ker \rho$  is a finite  $p$ -group. By (55.31),  $\text{Picent } \Lambda \cong \text{Outcent } \Lambda$ , so it suffices to show that  $\rho(\text{Outcent } \Lambda) = 1$ . Equivalently, we must prove that for each  $f \in \text{Autcent } \Lambda$ , its image  $f' \in \text{Aut}_R \Lambda/J^2$  is trivial.

Let  $G^{ab} = G/[G, G]$ ,  $G^p = \{x^p : x \in G\}$ ,  $H = G/[G, G]G^p$ , and set

$$\Lambda = RG, \quad J = \text{rad } \Lambda; \quad \tilde{\Lambda} = RG^{ab}, \quad \tilde{J} = \text{rad } \tilde{\Lambda}.$$

The surjection  $G \rightarrow G^{ab}$  induces a ring surjection  $\Lambda \rightarrow \tilde{\Lambda}$ , and we claim that this gives rise to an isomorphism of rings  $\Lambda/J^2 \cong \tilde{\Lambda}/\tilde{J}^2$ . Indeed, we have  $J = P\Lambda + I$ , where  $I$  is the augmentation ideal of  $RG$ . Then  $J^2 = (P^2, PI, I^2)$ , and we find readily that

$$\Lambda/J^2 \cong (R/P^2) \oplus \left( \bigoplus_{y \in H - \{1\}} ky \right),$$

$$\text{so } \Lambda/J^2 \cong \tilde{\Lambda}/\tilde{J}^2.$$

Next, the kernel of the surjection  $\Lambda \rightarrow \tilde{\Lambda}$  is the ideal generated by all  $\{xy - yx : x, y \in \Lambda\}$ , which is mapped onto itself by each  $f \in \text{Autcent } \Lambda$ . Thus  $f$  induces an automorphism  $\tilde{f}$  of  $\tilde{\Lambda}$ . But  $f$  preserves class sums in  $\Lambda$ , so for each conjugacy class  $\mathfrak{C}$  of  $G$ ,  $f$  fixes  $\sum_{x \in \mathfrak{C}} x$ . This class sum has image  $|\mathfrak{C}| \bar{x}$  in  $\tilde{\Lambda}$ , and since  $\text{char } k \nmid |G|$  by hypothesis, also  $\text{char } k \nmid |\mathfrak{C}|$ . Therefore  $\tilde{f}$  fixes each  $\bar{x} \in G^{ab}$  so  $\tilde{f} = 1$ .

Now consider the commutative diagram

$$\begin{array}{ccc} \Lambda & \longrightarrow & \tilde{\Lambda} \\ \downarrow & & \downarrow \\ \Lambda/J^2 & \cong & \tilde{\Lambda}/\tilde{J}^2. \end{array}$$

Since each  $f \in \text{Aut}_{\text{cent}} \Lambda$  induces the identity automorphism of  $\tilde{\Lambda}$ , it follows that the image of  $f$  in  $\text{Aut}_R \Lambda/J^2$  is also 1. This completes the proof of the theorem.

**(55.50) Corollary.** *Let  $G$  be a  $p$ -group, and let  $R$  be an arbitrary Dedekind domain. Let  $P$  range over all maximal ideals of  $R$ . Then*

$$\prod_P \text{Picent } R_P G$$

is a finite  $p$ -group.

Next we show:

**(55.51) Theorem (Fröhlich).** *Let  $\Lambda = \mathbb{Z}G$ , where  $G$  is a  $p$ -group, with  $p$  prime. Let  $C = \text{center of } \Lambda$ , and let  $D(C)$  be the kernel group (see (49.33)). Then  $D(C)$  is a finite  $p$ -group.*

*Proof.* Let  $\mathfrak{O}$  be a maximal  $\mathbb{Z}$ -order in  $\mathbb{Q} \otimes_{\mathbb{Z}} C$ . Then  $C_q = \mathfrak{O}_q$  for each rational prime  $q \neq p$ . As in the proof of (50.18), we deduce that

$$D(C) \cong \mathfrak{O}_p^\times / \mathfrak{O}^\times C_p^\times.$$

The rest of the proof is parallel to that of (50.18), and we omit the details.

We shall next give an example of the calculation of  $\text{Picent } \mathbb{Z}G$  to illustrate the methods developed in the previous subsections. Following Fröhlich [73] and Fröhlich-Reiner-Ullom [74], we consider the case where  $G$  is a dihedral group of order  $2p$ , with  $p$  an odd prime. To fix the notation, let

$$G = \langle x, y : x^p = 1, y^2 = 1, yxy^{-1} = x^{-1} \rangle.$$

Let  $\omega$  be a primitive  $p$ -th root of 1 over  $\mathbb{Q}$ , and set

$$R = \mathbb{Z}[\omega], \quad K = \mathbb{Q}(\omega); \quad S = \mathbb{Z}[\omega + \bar{\omega}], \quad L = \mathbb{Q}(\omega + \bar{\omega}),$$

where for  $\alpha \in K$ ,  $\bar{\alpha}$  denotes its complex conjugate. As in the proof of (50.25) (see also (34.43) and the discussion following it), there is a fiber product

$$(55.52) \quad \begin{array}{ccc} \Lambda = \mathbb{Z}G & \longrightarrow & R \circ H = \Gamma \\ \downarrow & & \downarrow g_2 \\ \mathbb{Z}H & \xrightarrow{g_1} & \bar{\mathbb{Z}}H. \end{array}$$

where  $H = \langle y : y^2 = 1 \rangle$ ,  $\mathbb{Z} = \mathbb{Z}/p\mathbb{Z}$ , and  $\Gamma = R \oplus Ry$  is a twisted group ring in which  $y^2 = 1$  and  $y\alpha = \bar{\alpha}y$  for all  $\alpha \in R$ . We have seen that

$$(55.53) \quad A = \mathbb{Q}G \cong \mathbb{Q}H \oplus B, \quad \text{where } B = \mathbb{Q} \otimes_{\mathbb{Z}} \Gamma = K \circ H \cong M_2(L).$$

The isomorphism  $B \cong M_2(L)$  may be given by

$$\alpha \in K \rightarrow \begin{pmatrix} \alpha & 0 \\ 0 & \bar{\alpha} \end{pmatrix}, \quad y \rightarrow \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

Then  $\Gamma$  is a hereditary  $Z$ -order in the central simple  $L$ -algebra  $B$ , and its center is  $S$  (viewed as a set of scalar matrices). Since  $R$  is unramified over  $S$  except at the unique prime ideal of  $S$  containing  $p$ , it follows that the 2-adic completion  $\Gamma_2$  is a maximal order in  $B_2$ , and is isomorphic to the ring of all  $2 \times 2$  matrices over  $S_2$ . On the other hand, the  $p$ -adic completion  $\Gamma_p$  is a hereditary order in  $M_2(L_p)$ .

We have  $S = \text{alg. int. } \{L\}$ ; let  $\text{Cl } S$  be its ideal class group, written multiplicatively, and define a homomorphism

$$t: \text{Cl } S \rightarrow \text{Cl } S \text{ by } t(\alpha) = (\alpha^2)$$

for each  $S$ -ideal  $\alpha$  in  $L$ . Clearly,

$$\ker t = (\text{Cl } S)_2 = \{x \in \text{Cl } S : x^2 = 1\}, \quad \text{cok } t = (\text{Cl } S)/(\text{Cl } S)^2.$$

We observe next that by (55.53) the algebra  $A$  satisfies the Eichler condition relative to  $Z$  (see (51.2)), and therefore the order  $\Lambda$  has locally free cancellation by the Jacobinski Cancellation Theorem 51.24. Thus by (55.35) there is a well-defined homomorphism  $\theta: \text{LFP}(\Lambda) \rightarrow \text{Cl } \Lambda$ , whose kernel is isomorphic to  $\text{Outcent } \Lambda$ .

Our main result is as follows:

**(55.54) Theorem.** *Let  $\Lambda = ZG$ , where  $G$  is a dihedral group of order  $2p$ , and keep the above notation. Then*

- (i)  $\text{Outcent } \Lambda \cong \ker \theta \cong (\text{Cl } S)_2 \times (\text{cyclic group of order } (p-1)/2)$ .
- (ii)  $\text{cok } \theta \cong \text{cok } t \cong (\text{Cl } S)/(\text{Cl } S)^2$ .
- (iii)  $\text{Cl } \Lambda \cong \text{Cl } S$  and

$$\text{Picent } \Lambda = \text{LFP}(\Lambda) \cong (\text{Cl } S) \times (\text{cyclic group of order } (p-1)/2).$$

*Proof. Step 1.* Since  $\Lambda = ZG$ , every projective  $ZG$ -lattice is locally free. Thus  $\text{Picent } \Lambda = \text{LFP}(\Lambda)$ . Likewise,  $\text{Picent } \Lambda_q \cong \text{Outcent } \Lambda_q$  for each rational prime  $q$ , and

$$\text{Outcent } \Lambda_q \cong N(\Lambda_q)/\Lambda_q^*(K_q C)^*.$$

By (55.30), there is an exact sequence

$$1 \rightarrow \text{Cl } C \xrightarrow{\tau} \text{LFP}(\Lambda) \rightarrow \coprod_q \text{Outcent } \Lambda_q \rightarrow 1.$$

In Step 3 we shall prove that  $\text{Outcent } \Lambda_q = 1$  for each  $q$ , so  $\tau: \text{Cl } C \cong \text{LFP}(\Lambda)$ . We take this for granted for the time being.

Now let  $\Gamma'$  be a maximal  $\mathbb{Z}$ -order in  $B$  containing  $\Gamma$ , and set  $\Lambda' \cong \mathbb{Z} \oplus \mathbb{Z} \oplus \Gamma'$ , a maximal order in  $A$  containing  $\Lambda$ . Then  $\text{Cl } \Lambda \cong \text{Cl } \Lambda'$  by (50.25), while  $\text{Cl } \Gamma \cong \text{Cl } \Gamma'$  by (49.35) since  $\Gamma$  is hereditary. Further,  $\text{Cl } \Gamma' \cong \text{Cl } S$  by (49.32). Let  $C' = \mathbb{Z} \oplus \mathbb{Z} \oplus S$  be the center of  $\Lambda'$ . Composition of maps gives a homomorphism

$$\text{Cl } S \cong \text{Cl } C' \rightarrow \text{LFP}(\Lambda') \rightarrow \text{Cl } \Lambda' \cong \text{Cl } S,$$

which is precisely the map  $t$  defined above (see the proof of (55.36)). We thus obtain a commutative diagram

$$\begin{array}{ccc} \text{Cl } C & \xrightarrow{\varphi} & \text{Cl } S \\ \tau \downarrow & & t \downarrow \\ \text{LFP}(\Lambda) & \xrightarrow{\theta} & \text{Cl } \Lambda \cong \text{Cl } S. \end{array}$$

Since  $\varphi$  is the composite of the surjection  $\text{Cl } C \rightarrow \text{Cl } C'$  and the isomorphism  $\text{Cl } C' \cong \text{Cl } S$ , it follows that  $\varphi$  is surjective. Taking for granted that  $\tau$  is an isomorphism, we obtain

$$\ker \theta \cong \ker t\varphi, \quad \text{cok } \theta \cong \text{cok } t\varphi.$$

However, there is an exact sequence

$$1 \rightarrow \ker \varphi \rightarrow \ker t\varphi \rightarrow \ker t \rightarrow \text{cok } \varphi \rightarrow \text{cok } t\varphi \rightarrow \text{cok } t \rightarrow 1.$$

Since  $\text{cok } \varphi = 1$ , we deduce that  $\text{cok } \theta \cong \text{cok } t$  (so (ii) is proved), and also the sequence

$$(55.55) \quad 1 \rightarrow \ker \varphi \rightarrow \ker \theta \rightarrow \ker t \rightarrow 1$$

is exact,

*Step 2.* From the diagram (55.52) we obtain a new fiber product

$$\begin{array}{ccc} C & \longrightarrow & S \\ \downarrow & & \downarrow g_2 \\ \mathbb{Z}H & \longrightarrow & \mathbb{Z}H, \\ & & g_1 \end{array}$$

where now  $g_2: S \rightarrow S/(\omega - \bar{\omega})^2 \cong \bar{\mathbb{Z}} \subset \mathbb{Z}H$ . This gives a Mayer-Vietoris sequence

$$(\mathbb{Z}H)^* \times S^* \xrightarrow{h} (\mathbb{Z}H)^* \rightarrow \text{Cl } C \xrightarrow{\varphi} \text{Cl } S \oplus \text{Cl } \mathbb{Z}H \rightarrow 0,$$

and  $\text{Cl } \mathbf{Z}H = 0$  by Exercise 49.1, so this  $\varphi$  agrees with our earlier  $\varphi$ . We have  $(\bar{\mathbf{Z}}H)^\circ = \bar{\mathbf{Z}}^\circ \times \bar{\mathbf{Z}}^\circ$  and  $h(S^\circ) = \bar{\mathbf{Z}}^\circ$ , since for  $n \in \mathbf{Z}$  prime to  $p$ , the element  $(\omega^n - \omega^{-n})/(\omega - \omega^{-1})$  lies in  $S^\circ$  and has image  $2\bar{n}$  in  $\bar{\mathbf{Z}}^\circ$ . Further,  $(\mathbf{Z}H)^\circ = \{\pm 1, \pm y\}$ . It follows readily that  $\text{cok } h$  is cyclic of order  $(p-1)/2$ . Furthermore, since  $g_2(S^\circ) = (g_2(S))^\circ$ , Exercise 49.5 shows that the surjection  $\varphi: \text{Cl } C \rightarrow \text{Cl } S$  is split. Therefore

$$\text{Cl } C \cong \text{Cl } S \oplus \ker \varphi, \quad \ker \varphi = \text{cyclic group of order } (p-1)/2.$$

*Step 3.* We now verify that  $\tau: \text{Cl } C \cong \text{LFP}(\Lambda)$ , or equivalently, that  $\text{Outcent } \Lambda_q = 1$  for each rational prime  $q$ . For  $q \neq 2$  or  $p$ ,  $\Lambda_q$  is a maximal order in  $A_{q_p}$  so  $\text{Outcent } \Lambda_q = 1$  by (55.24). For  $q = 2$ , we have

$$\Lambda_2 \cong \mathbf{Z}_2 H \oplus \Gamma_2,$$

and  $\text{Picent } \Lambda_2 = \text{Picent } \mathbf{Z}_2 H \times \text{Picent } \Gamma_2 = \text{Cl } \mathbf{Z}_2 H = 1$ , using the fact that  $\Gamma_2$  is a maximal order in  $A_2$ .

It remains to verify that  $\text{Outcent } \Lambda_p = 1$ , that is, if  $x \in A_p^\circ$  is such that  $x\Lambda_p x^{-1} = \Lambda_p$ , then  $x \in \Lambda_p(K_p C)^\circ$  (see (55.22)). Replacing  $x$  by  $ax$  with  $a \in R_p$ , and changing notation, we may assume that  $x \in \Lambda_p \cap A_p^\circ$ . Taking  $p$ -adic completions in the fiber product (55.52), we obtain a new fiber product

$$\begin{array}{ccc} \Lambda_p & \longrightarrow & \Gamma_p \\ \downarrow & & \downarrow g_2 \\ \mathbf{Z}_p H & \xrightarrow{g_1} & \bar{\mathbf{Z}}H, \end{array}$$

in which  $g_2$  is the map  $\Gamma_p \rightarrow \Gamma_p/\text{rad } \Gamma_p$ . We have

$$\Lambda_p = \{(y_1, y_2) \in \mathbf{Z}_p H \oplus \Gamma_p: g_1(y_1) = g_2(y_2) \text{ in } \bar{\mathbf{Z}}H\}.$$

Write  $x = (x_1, x_2) \in \Lambda_p \cap A_p^\circ$ . Then  $x(y_1, y_2)x^{-1} \in \Lambda_p$  for each  $(y_1, y_2) \in \Lambda_p$ , which implies that for each  $y_2 \in \Gamma_p$ , we have

$$(55.56) \quad x_2 y_2 x_2^{-1} \in \Gamma_p \quad \text{and} \quad x_2 y_2 x_2^{-1} \equiv y_2 \pmod{\text{rad } \Gamma_p}.$$

Let  $\pi$  denote a prime element of  $S_p$ . Since  $\Gamma_p$  is a hereditary order in  $M_2(S_p)$ , and  $\Gamma_p$  is not a maximal order, it follows from (26.28) that we may write

$$\Gamma_p = \begin{pmatrix} S_p & \pi S_p \\ S_p & S_p \end{pmatrix} = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix}: a, b, c, d \in S_p, b \in \pi S_p \right\}.$$

There are precisely two maximal orders containing  $\Gamma_p$ , namely,

$$\Omega = \begin{pmatrix} S_p & S_p \\ S_p & S_p \end{pmatrix} \quad \text{and} \quad \Omega' = z\Omega z^{-1}, \quad \text{where } z = \begin{pmatrix} \pi & 0 \\ 0 & 1 \end{pmatrix}.$$

Conjugation by  $x_2$  must either fix both  $\Omega$  and  $\Omega'$ , or else must interchange them. If  $x_2\Omega x_2^{-1} = \Omega$ , then  $x_2 \in \Omega^* L_p^*$  by (55.23). An easy calculation shows that for  $x_2 \in \Omega'$ , the first condition in (55.56) implies that  $x_2 \in \Gamma_p^*$ . In this case there exists an  $x' = (x'_1, x_2) \in \Lambda_p^*$  such that conjugation by  $x'$  and  $x$  coincide, and thus  $x \in \Lambda_p^*(K_p C)$  as desired. On the other hand, if  $x_2\Omega x_2^{-1} = \Omega'$ , then  $x'_2 = z^{-1}x_2$  conjugates  $\Omega$  into itself. Then  $z^{-1}x_2 \in \Omega^* L_p^*$ , and it is easily checked that the second condition in (55.56) cannot hold.

We have now proved all of the assertions of the theorem, except that the sequence (55.55) is split. We leave this as an exercise for the reader.

We conclude the discussion of Picard groups with a brief guide to the literature.

(1) Endo-Miyata-Sekiguchi [82] studied Picent  $\mathbb{Z}G$  for the cases:

(a)  $G$  = metacyclic group  $C_n \rtimes C_q$ , where  $(q, n) = 1$  and where  $C_q$  acts faithfully on each Sylow subgroup of  $C_n$ .

(b)  $G$  = dihedral group of order  $2n$ , with  $n$  arbitrary.

In both cases, they showed that  $\text{Outcent } \mathbb{Z}_p G = 1$  for all primes  $p$ , and thus

$$\text{Picent } \mathbb{Z}G = \text{LFP}(\mathbb{Z}G) \cong \text{Cl}(\text{center of } \mathbb{Z}G).$$

They obtained formulas for the orders of Picent  $\mathbb{Z}G$  and Outcent  $\mathbb{Z}G$ , in terms of the orders of various locally free class groups. See their Theorem 4.8 for case (a), and their Theorem 5.6 for case (b).

(2) Let  $G$  be a finite group, and let  $f \in \text{Aut } G$ . We say that  $f$  is *class-preserving* if for each  $x \in G$ ,  $f(x)$  is  $G$ -conjugate to  $x$ . Let  $\text{Aut}_c G$  be the group of all class-preserving automorphisms  $f$  of  $G$ , and  $\text{In}(G)$  its subgroup consisting of all inner automorphisms of  $G$ . Define

$$\text{Out}_c G = (\text{Aut}_c G)/\text{In } G.$$

Then we have:

**(55.57) Theorem (Endo-Miyata-Sekiguchi [82]).** *Let  $G$  be a nilpotent group of order  $n$ . Then both of the homomorphisms*

$$\text{Out}_c G \rightarrow \text{Outcent } \mathbb{Z}G, \quad \text{Out}_c G \rightarrow \prod_{p|n} \text{Outcent } \mathbb{Z}_p G,$$

*are injective.*

For each prime  $p$ , there exists a  $p$ -group  $G$  for which  $\text{Out}_c G$  is non-abelian (see Sah [68]). For each such  $G$ , it follows that the groups

$$(55.58) \quad \text{Outcent } \mathbb{Z}G, \quad \text{Picent } \mathbb{Z}G (= \text{LFP}(\mathbb{Z}G)), \quad \text{Outcent } \mathbb{Z}_p G$$

are non-abelian.

Similar results were obtained by Keating [79]. Given a prime  $p$ , Keating constructed a sequence of  $p$ -groups  $\{G_n : n \geq 1\}$  such that  $|G_n| = p^{6n}$  and  $G_n$  is nilpotent of class 2. He showed that (in the above notation)  $\text{Out}_c G$  contains a subgroup isomorphic to  $(\mathbb{Z}/p^n\mathbb{Z})^{(4)}$ , which then embeds in all of the groups listed in (55.58).

(3) Sekiguchi [83] showed that  $\text{Outcent } \mathbb{Z}_p G = 1$  for all metacyclic  $p$ -groups  $G$ , where  $p$  is any odd prime.

(4) Fröhlich [73] showed that for  $G$  the quaternion group of order 8,  $\text{Picent } \mathbb{Z}G$  has order 2, and  $\text{Outcent } \mathbb{Z}G$  is trivial.

## §55. Exercises

1. Let  $E = M_n(R)$ , where  $R$  is a commutative ring and  $n \geq 1$ . Given an  $R$ -algebra  $\Lambda$ , let  $\Gamma = E \otimes_R \Lambda \cong M_n(\Lambda)$ . Show that the isomorphism  $\text{Pic}_R \Lambda \cong \text{Pic}_R \Gamma$  given in (55.9) can also be described by the map

$$(X) \rightarrow (E \otimes_R X) \quad \text{for } (X) \in \text{Pic}_R \Lambda.$$

[Hint: Let  $L = R^{(n)} \otimes_R \Lambda$ , viewed as invertible  $(\Gamma, \Lambda)$ -bimodule. Set  $L^{-1} = \text{Hom}_\Lambda(L, \Lambda)$ . Then  $L$  gives an isomorphism

$$\text{Pic}_R \Lambda \cong \text{Pic}_R \Gamma, \quad \text{with } (X) \rightarrow (L \otimes_\Lambda X \otimes_\Lambda L^{-1}) \quad \text{for } (X) \in \text{Pic}_R \Lambda.$$

However, there are two-sided  $\Gamma$ -isomorphisms

$$L \otimes_\Lambda X \otimes_\Lambda L^{-1} \cong \text{Hom}_\Lambda(L, L \otimes_\Lambda X) \cong \text{Hom}_\Lambda(\Lambda^{(n)}, X^{(n)}) \cong E \otimes_R X.]$$

2. Keeping the above notation, let  $[Y] \in K_0(\Lambda)$ . Show that

$$[E \otimes_R Y] = n[L \otimes_\Lambda Y] \text{ in } K_0(\Gamma).$$

[Hint:  $L \otimes_\Lambda Y \cong R^{(n)} \otimes_R Y$  as left  $\Gamma$ -modules. Since  $E$  is isomorphic to a direct sum of  $n$  copies of the left  $E$ -module  $R^{(n)}$ , we obtain

$$[E \otimes_R Y] = n[R^{(n)} \otimes_R Y] = n[L \otimes_\Lambda Y],$$

as desired.]

3. Let  $R$  be a commutative ring, and let  $E$  be an  $R$ -algebra. Call  $E$  an *Azumaya  $R$ -algebra* ( $=$  *central separable  $R$ -algebra*) if  $c(E) = R$  and  $E$  is projective as left  $(E \otimes_R E^0)$ -module. (This generalizes the concept of separable algebras over fields in §7A; see DeMeyer-Ingraham [71].) Show that for every  $R$ -algebra  $\Lambda$  and every  $R$ -Azumaya algebra  $E$ , there is an isomorphism

$$\text{Pic}_R \Lambda \cong \text{Pic}_R (\Lambda \otimes_R E), \quad \text{given by } (X) \rightarrow (X \otimes_R E).$$

[Hint: See DeMeyer-Ingraham [71], or MO Exercise 37.4.]

4. Let  $\Lambda = \coprod_{i=1}^t \Lambda_i$  be a direct sum of rings. Prove that

$$\text{Picent } \Lambda \cong \prod_{i=1}^t \text{Picent } \Lambda_i.$$

[Hint: Let  $e_1, \dots, e_t$  be central idempotents in  $\Lambda$  such that  $\Lambda_i = \Lambda e_i$ . For each  $(X) \in \text{Picent } \Lambda$  we have  $e_i X = X e_i$ , so  $(e_i X) \in \text{Picent } \Lambda_i$ . The desired isomorphism is given by  $(X) \mapsto \prod (e_i X)$ .]

5. Let  $M, N$  be full  $R$ -lattices in a f.d.  $K$ -space  $V$ , where  $R$  is a Dedekind domain with quotient field  $K$ . Define the *generalized  $R$ -order ideal*  $\text{ord } M//N$  by the formula

$$\text{ord } M//N = (\text{ord } M/(M \cap N))(\text{ord } N/(M \cap N))^{-1},$$

where  $\text{ord } M/(M \cap N)$  is the usual  $R$ -order ideal (see §4D). Show that if  $L$  is another full  $R$ -lattice in  $V$ , then

$$(\text{ord } L//M)(\text{ord } M//N) = \text{ord } L//N.$$

6. Let  $M$  be a full  $R$ -lattice in a f.d. separable  $K$ -algebra  $A$ , where  $R, K$  are as above, and let  $x \in A^\times$ . Prove that

$$\text{ord } M//Mx = \text{ord } M//xM.$$

Deduce that if  $Mx \subseteq xM$ , then  $Mx = xM$ .

[Hint: By Exercise 5, it suffices to treat the case where  $Mx \subseteq M$  and  $xM \subseteq M$ . By (4.20a),

$$\text{ord } M/Mx = R \cdot N_{A/K}(x),$$

where  $N_{A/K}(x)$  denotes the norm, computed by letting  $x$  act as right multiplication on  $A$ . But the right and left norms coincide since  $A$  is separable, as is clear by passing to a splitting field, and using the fact that a matrix and its transpose have the same characteristic polynomial.]

7. Let  $\Lambda$  be a semilocal ring, that is,  $\bar{\Lambda} = \Lambda/J$  is semisimple artinian, where  $J = \text{rad } \Lambda$ . Show that for each invertible bimodule  ${}_A M_\Lambda$  we have  $J' M = M J^r$  for  $r \geq 0$ .

[Hint (Fröhlich): Put  $\bar{M} = M/JM$ , a  $(\bar{\Lambda}, \Lambda)$ -bimodule, and set  $E = \text{End}_{\bar{\Lambda}} \bar{M}$ . Then  $E$  is semisimple artinian, and may be viewed as a ring of right operators on  $\bar{M}$ . For  $a \in \Lambda$ , let  $a_r$  denote right multiplication on  $M$  or  $\bar{M}$ . The map  $a \mapsto a_r$  (on  $\bar{M}$ ) gives a ring homomorphism  $\varphi: A \rightarrow E$ , and  $\varphi$  is surjective since every  $\bar{\Lambda}$ -endomorphism of  $\bar{M}$  lifts to a  $\Lambda$ -endomorphism of  $M$ , and hence is some  $a_r$ . It follows that  $\varphi(J) \subseteq \text{rad } E = 0$ , so  $MJ \subseteq JM$ . Therefore  $MJ = JM$  by symmetry.]

8. Keeping the above notation, show that  $M/J'rM$  is an invertible bimodule over the ring  $\Lambda/J^r$  for  $r \geq 1$ .

[Hint: If  $\Lambda' = \Lambda/J^r$ , where  $r \geq 1$ , then  $\Lambda' \otimes_A M \cong M/J'rM$ , while  $M \otimes_A \Lambda' \cong M/MJ^r = M/J'rM$  by the preceding exercise.]

9. Let  $R$  be a d.v.r. with quotient field  $K$ , maximal ideal  $P$ , and finite residue class field

$k = R/P$  of characteristic  $p$ . Let  $\Lambda$  be an  $R$ -order in a f.d. separable  $K$ -algebra  $A$ , and let  $J = \text{rad } \Lambda$ . Show that

$$\ker(\text{Picent } \Lambda \rightarrow \text{Pic}_R \Lambda/J^2)$$

is a finite  $p$ -group.

[Hint (Fröhlich): Choose  $n$  so large that  $P^n \Lambda \subseteq J^2$  and  $\text{Picent } \Lambda \rightarrow \text{Pic}_R \Lambda_n$  is injective, where  $\Lambda_n = \Lambda \otimes_R k_n$ , and  $k_n = R/P^n$ . Then

$$\frac{\Lambda}{J^2} \cong \frac{\Lambda}{J^2} \otimes_R k_n \cong \frac{\Lambda_n}{J_n^2}.$$

Consider the commutative diagram:

$$\begin{array}{ccc} \text{Picent } \Lambda & \longrightarrow & \text{Pic}_R \Lambda_n \\ f \downarrow & & \searrow g \\ \text{Pic}_R \frac{\Lambda}{J^2} & \longrightarrow & \text{Pic}_R \frac{\Lambda_n}{J_n^2} \end{array}$$

Then  $\ker g$  is a  $p$ -group, and  $\ker f \leq \ker g$ .]

10. Keeping the above notation, show that  $\text{Pic}_R \Lambda \rightarrow \text{Pic}_R \Lambda/P^n \Lambda$  is injective for sufficiently large  $n$ .

[Hint: Use (55.44).]

11. Let  $\Lambda$  be as above, but do not assume  $R/P$  finite. Let  $\hat{\Lambda}$  be the  $P$ -adic completion of  $\Lambda$ . Prove that  $\text{Picent } \Lambda \cong \text{Picent } \hat{\Lambda}$ .

[Hint: Use (55.18).]

12. Prove that if  $G$  is a finite nilpotent group, then so are both  $\text{LFP}(ZG)$  and  $\text{Outcent } ZG$ .

[Hint (Endo-Miyata-Sekiguchi [82]): Use (55.50) and the fact that the map  $\tau$  in (55.25) carries  $\text{Picent } C$  into the center of  $\text{Picent } ZG$ .]

## The Theory of Blocks

Block theory is a refinement of the modular representation theory of a finite group  $G$  with respect to a  $p$ -modular system  $(K, R, k)$ . It begins with a division of the categories of  $KG$ -modules,  $RG$ -modules, and  $kG$ -modules into smaller categories, called  $p$ -blocks, which arise from a decomposition of  $RG$  as a direct sum of indecomposable two-sided ideals.

Most of the main results are due to R. Brauer. His work proved vital for the solution of certain problems in the classification of finite simple groups and for the calculations of character tables of the sporadic simple groups, and has inspired an extensive literature.

The foundations of the theory were reworked by Brauer himself, and later by Green, who introduced new methods based on his work on vertices and sources of indecomposable modules, the Green Correspondence, and his definition of defect groups of primitive idempotents in  $G$ -algebras. Block theory is now part of what is called local representation theory, which is an analysis of the deep connections which exist between modules and characters in  $p$ -blocks, and the  $p$ -local subgroup structure of  $G$ .

The chapter begins with a section describing the distribution of  $RG$ -modules,  $kG$ -modules, and  $KG$ -modules in  $p$ -blocks using several methods: block idempotents, linkage of P.I.M.'s, and central characters. The defect of a  $p$ -block is defined, and various results involving the coefficients of block idempotents, central characters, and the defect are derived, using the theory of Brauer characters from §18.

In §57, Green's elementary and self-contained approach to defect groups of primitive idempotents in  $G$ -algebras is developed. This is applied to reinterpret Brauer's important concept of the defect group of a  $p$ -block, and to establish a link between defect groups and vertices of indecomposable modules. These ideas lead to Green's theorem, which expresses defect groups as Sylow intersections.

The next two sections contain Alperin and Broué's investigation of the Brauer map, leading to their proof of Brauer's First Main Theorem, and Nagao's proof of Brauer's Second Main Theorem, using the theory of vertices of indecomposable modules. Brauer defined an important connection between  $p$ -blocks of  $G$  and  $p$ -blocks of certain subgroups of  $G$ , which is now called the Brauer Correspondence. It is useful to understand this correspondence from several points of

view, including central characters, the Brauer map, and vertices of indecomposable modules. Fortunately, there is an efficient way to make these connections, due to Okuyama, which we present in §58.

In §60, applications of the Second Main Theorem to character theory are obtained, such as the sectional orthogonality theorem. The section also includes a nice application to permutation groups of prime degree.

Section 61 contains some refinements of the Brauer Correspondence, including the theory of covering blocks for the case of a normal subgroup, the Third Main Theorem on the principal block, and the Extended First Main Theorem, which in a sense reduces the study of  $p$ -blocks of  $G$  to blocks of defect zero of certain subquotient groups.

The first really decisive applications of block theory to character theory were obtained by Brauer ([41], [42a], [42b]). Dade [66] extended this work to obtain a complete description of the ordinary and Brauer characters in blocks with cyclic defect groups. This is one of the high points in block theory so far. We present in §62 some of the main results on the modular representations in such a block, following Michler [76]. In §62E, Morita's result on the periodic behavior of composition factors of P.I.M.'s in a uniserial block is applied to obtain a periodic projective resolution of the trivial  $RG$ -module, in a finite group with a cyclic Sylow  $p$ -subgroup. The Brauer tree is defined, and illustrated in the special case of groups with cyclic self-centralizing Sylow  $p$ -subgroups which are T. I. sets, using the character theory of these groups, from §20.

The last section contains two applications of block theory to group theory. These are the Brauer-Suzuki Theorem on the nonsimplicity of groups with a quaternion Sylow 2-subgroup of order 8, and Glauberman's  $Z^*$ -Theorem, which has been applied to the classification of finite simple groups. Our account is based on the lectures of Dade [71].

## §56. INTRODUCTION TO BLOCK THEORY

### §56A. Background and Notation for Block Theory

Throughout this chapter,  $G$  denotes a finite group and  $p$  a rational prime number. A  $p$ -modular system  $(K, R, k)$  consists of a d.v.r.  $R$  with quotient field  $K$ , maximal ideal  $\mathfrak{p} = \pi R$ , and residue class field  $k = R/\mathfrak{p}$  of characteristic  $p$ . One example to keep in mind is that where  $K$  is an algebraic number field and  $R$  is the valuation ring of some discrete valuation on  $K$ . As another example, we may choose  $K$  to be the completion of an algebraic number field with respect to a non-archimedean valuation, and  $R$  the valuation ring of  $K$  (see §4C).

In order to keep the chapter reasonably self-contained, we shall review in this subsection some of the concepts related to a  $p$ -modular system, especially those connected with lifting idempotents. Other results from earlier chapters will be recalled later, when needed.

As in §17A, a field is called *sufficiently large* relative to  $G$  if it contains the  $m$ -th roots of unity, where  $m$  is the exponent of  $G$ . Such a field is a splitting

field for  $G$  and all of its subgroups, by Theorem 17.1. We have seen in §17B that if  $(K, R, k)$  is a  $p$ -modular system with  $\text{char } K = 0$  and  $K$  sufficiently large, then also  $k$  is sufficiently large, and Brauer characters of  $kG$ -modules can be defined. We shall use these characters later in this chapter.

The centers of the group algebras  $KG$ ,  $RG$ , and  $kG$ , associated with a  $p$ -modular system, will be of particular importance in block theory. We denote these centers by

$$c(KG), \quad c(RG), \quad c(kG),$$

respectively. By (3.37a), each of these centers has a basis over  $K$ ,  $R$ ,  $k$ , respectively, consisting of the class sums

$$C_i = \sum_{x \in \mathfrak{C}_i} x,$$

where  $\{\mathfrak{C}_i\}$  are the conjugacy classes in  $G$ .

Throughout this chapter, let bars denote “reduction mod  $\mathfrak{p}$ .” Thus, for  $a \in RG$  let  $\bar{a} \in kG$  denote its image under the canonical surjection  $RG \rightarrow kG$ . Likewise, for each  $RG$ -module  $M$  we put  $\bar{M} = M/\mathfrak{p}M$ , and let  $m \mapsto \bar{m}$  under the map  $M \rightarrow \bar{M}$ . Using this notation, we have at once an important connection between the centers of the above group algebras:

**(56.1) Lemma.** *There is a surjective homomorphism  $c(RG) \rightarrow c(kG)$ , given by*

$$\sum a_i C_i \rightarrow \sum \bar{a}_i C_i, \quad a_i \in R.$$

Let us now review some facts about idempotents, starting with a  $p$ -modular system  $(K, R, k)$  and an  $R$ -order  $A$ . (By definition,  $A$  is an  $R$ -algebra with a finite  $R$ -basis.) We shall be particularly interested in the cases where

$$A = RG \quad \text{or} \quad A = c(RG),$$

but for the moment we do not make this assumption. Let  $\text{rad } A$  denote the Jacobson radical of  $A$  (see §5A), and set  $\bar{A} = A/\mathfrak{p}A$ , a f.d.  $k$ -algebra. We then have (see (5.22) and (5.29)):

**(56.2) Proposition.** *Let  $A$  be an  $R$ -order. Then*

$$\mathfrak{p}A \leq \text{rad } A, \quad A/\text{rad } A \cong \bar{A}/\text{rad } \bar{A}.$$

*Further,  $A/\text{rad } A$  is a semisimple artinian ring, and*

$$\text{rad } M = (\text{rad } A)M$$

*for all f.g. left  $A$ -modules  $M$ .*

An *idempotent*  $e \in A$  is a nonzero element such that  $e^2 = e$ . Two idempotents  $e$  and  $e'$  are *orthogonal* if  $ee' = e'e = 0$ . An idempotent  $e$  is *primitive* if it cannot be expressed as a sum of two orthogonal idempotents, or equivalently, if and only if the left ideal  $Ae$  is indecomposable. By (3.19) and (6.4), this is equivalent to the assertion that the ring  $eAe$  has no idempotents except  $e$ . These definitions and remarks apply also to f.d. algebras over  $K$  or  $k$ .

We wish to describe the connection between idempotents in  $A$  and those in  $\bar{A}$ , under either of two restrictive hypotheses, each of which provides a satisfactory basis for the development of much of block theory.

**(56.3) Definition.** A  $p$ -modular system  $(K, R, k)$  is *admissible* (for block theory, relative to  $A$ ) if either

(a)  $R$  is complete in the  $p$ -adic topology, or

(b)  $\text{char } K = 0$ , and the  $K$ -algebra  $K \otimes_R A$  is a split semisimple  $K$ -algebra (that is, a direct sum of full matrix algebras over  $K$ ). In case  $A = RG$ , we say that  $(K, R, k)$  is *admissible for  $G$* .

Before imposing this hypothesis, we recall from §6B that the *K-S-A Theorem* (“Krull-Schmidt-Azumaya”) states that (under certain hypotheses) f.g.  $A$ -modules have unique decompositions into indecomposable summands (unique up to isomorphism). As usual, an  *$A$ -lattice* means a left  $A$ -module which is f.g. and projective over  $R$  (and hence  $R$ -free with a finite basis, since  $R$  is a d.v.r.).

**(56.4) Proposition.** Let  $(K, R, k)$  be an admissible  $p$ -modular system for the  $R$ -order  $A$ . Then we have:

- (i) Each idempotent  $\alpha \in \bar{A}$  can be lifted to  $A$ , that is,  $\alpha = \bar{a}$  for some idempotent  $a \in A$ .
- (ii) Each idempotent in  $A/\text{rad } A$  can be lifted to  $A$ .
- (iii) An idempotent  $e \in A$  is primitive if and only if  $eAe$  is a local ring.
- (iv) An idempotent  $e \in A$  is primitive if and only if  $\bar{e}$  is primitive in  $\bar{A}$ .
- (v) There is a decomposition

$$1 = e_1 + \cdots + e_m$$

into primitive orthogonal idempotents  $e_i \in A$ . Such a decomposition gives a corresponding decomposition

$$\bar{1} = \bar{e}_1 + \cdots + \bar{e}_m$$

in  $\bar{A}$ . Conversely, every such decomposition of  $\bar{1} \in \bar{A}$  lifts to a decomposition of  $1 \in A$ .

- (vi) The K-S-A Theorem holds for  $A$ -lattices.

*Sketch of Proof.* All of the above assertions have been proved explicitly in §§5, 6, when  $R$  is complete in the  $p$ -adic topology. We shall recall some of the main points, and also discuss the case where  $\text{char } K = 0$  and  $KA$  is split semisimple.

(i) For  $R$  complete, the result holds by (6.7). In the second case, use Exercise 6.16.

(ii) By (56.2), there is a surjection

$$\bar{A} \rightarrow \bar{A}/\text{rad } \bar{A} \cong A/\text{rad } A.$$

Since  $\bar{A}$  is artinian, every idempotent of  $\bar{A}/\text{rad } \bar{A}$  lifts to  $\bar{A}$ , by (6.7). We then use (i) to lift to  $A$ .

(iii) We have already noted that  $e$  is primitive if and only if  $eAe$  contains no idempotents other than  $e$ , while  $eAe$  is local if and only if  $eAe/\text{rad } eAe$  is a division ring (see §5C). Thus, if  $eAe$  is local,  $e$  is clearly primitive. Now let  $e$  be primitive. In case hypothesis (56.3a) holds,  $eAe$  is a local ring by (6.10). In case (b),  $eAe$  is an order in the  $K$ -algebra  $eKae$  and  $eKae$  is also a split semisimple  $K$ -algebra, by standard results in §3. Thus we can apply parts (i) and (ii) to  $eAe$ , and conclude that idempotents can be lifted from  $eAe/\text{rad } eAe$  to  $eAe$ . Since we have assumed that  $e$  is primitive, so that  $eAe$  has no nontrivial idempotents, the same holds for  $eAe/\text{rad } eAe$ . It follows that  $eAe$  is a local ring, as required.

(iv) The homomorphism

$$eAe \rightarrow \overline{eAe} = eAe/\mathfrak{p} eAe$$

is surjective, and by (56.2) we have

$$eAe/\text{rad } eAe \cong \overline{eAe}/\text{rad } \overline{eAe}$$

Thus  $eAe$  is local if and only if  $\overline{eAe}$  is local, and the result follows from (iii).

(v) The existence of a decomposition of 1 follows from the fact that  $A$  is a noetherian ring. The remaining remarks follow from (iv) (see the proof of (6.7)).

(vi) The result is (6.12) when  $R$  is complete, while under hypothesis (b) it is a special case of Heller's Theorem 30.18.

**(56.5) Proposition.** *Let  $A$  be a commutative  $R$ -order.*

(i) *The primitive idempotents in  $A$  form a finite set  $\{c_1, \dots, c_n\}$  and satisfy the conditions*

$$1 = c_1 + \cdots + c_n, \quad c_i c_j = 0 \quad \text{for } i \neq j.$$

(ii) If  $(K, R, k)$  is admissible for  $A$ , the natural map  $A \rightarrow \bar{A}$  induces a bijection of primitive idempotents.

**Remark.** Both conditions also hold for commutative algebras over  $K$  or  $k$ .

*Proof.* Let  $1 = c_1 + \cdots + c_n$  be a decomposition of  $1$  as a sum of primitive orthogonal idempotents; then

$$A = Ac_1 \oplus \cdots \oplus Ac_n$$

is a decomposition of  $A$  into indecomposable ideals. For an arbitrary primitive idempotent  $e \in A$  we have an orthogonal decomposition

$$e = ec_1 + \cdots + ec_n,$$

so  $e = ec_i$  for some  $i$ , and  $ec_j = 0$  for  $j \neq i$ . But  $c_i$  is primitive, and  $c_i = c_i e + c_i(1 - e)$ , so  $c_i = c_i e = e$ , which proves (i). Assertion (ii) follows from (56.4).

Now let  $A$  be an arbitrary  $R$ -order, and assume  $(K, R, k)$  admissible for  $A$ . Then  $A/\text{rad } A$  is artinian, and every idempotent in  $A/\text{rad } A$  lifts to  $A$ . Thus, by definition,  $A$  is a *semiperfect* ring (see §6C), and every f.g.  $A$ -module has a projective cover, by (6.25). By virtue of the isomorphism

$$A/\text{rad } A \cong \bar{A}/\text{rad } \bar{A},$$

the simple  $A$ -modules can be identified with the simple  $\bar{A}$ -modules.

Let  $\mathcal{P}(A)$  and  $\mathcal{P}(\bar{A})$  denote the categories of f.g. projective modules over  $A$  and  $\bar{A}$ , respectively. The indecomposable modules in  $\mathcal{P}(A)$  and  $\mathcal{P}(\bar{A})$  are called *principal indecomposable modules* (notation: P.I.M.), or also *indecomposable projective modules*. Up to isomorphism, each P.I.M.  $P \in \mathcal{P}(A)$  has the form  $P = Ae$ , with  $e$  a primitive idempotent in  $A$ , and conversely each such  $Ae$  is a P.I.M. A corresponding statement holds for P.I.M.'s in  $\mathcal{P}(\bar{A})$ . Further, for each P.I.M.  $P \in \mathcal{P}(A)$ , we have shown in (6.22) that  $\bar{P}/\text{rad } \bar{P}$  is a simple module, and  $P$  is its projective cover. Moreover,  $\bar{P}$  is a P.I.M. in  $\mathcal{P}(\bar{A})$ , and  $\bar{P}/\text{rad } \bar{P} \cong P/\text{rad } P$ , so  $\bar{P}$  is a projective  $\bar{A}$ -cover of the simple module  $P/\text{rad } P$ .

Now let  $A = RG$ , where  $(K, R, k)$  is admissible for  $G$ . The above remarks show that there is an isomorphism of projective class groups

$$K_0(RG) \cong K_0(kG),$$

where  $K_0(A)$  denotes the Grothendieck group of the category  $\mathcal{P}(A)$ , as in (16.5). By (16.7) we have

$$K_0(RG) = \bigoplus_{i=1}^r \mathbb{Z}[P_i], \quad \text{and} \quad K_0(kG) = \bigoplus_{i=1}^r \mathbb{Z}[U_i],$$

where the  $\{P_i\}$  are a basic set of P.I.M.'s in  $\mathcal{P}(RG)$ , the  $\{U_i\}$  are a corresponding set in  $\mathcal{P}(kG)$ , and the notation is such that  $\bar{P}_i = U_i$ ,  $1 \leq i \leq r$ . For more details, see (18.1) and (18.2).

### §56B. Definition of $p$ -Blocks for a Finite Group G

Let  $G$  be a finite group, and let  $(K, R, k)$  be an arbitrary  $p$ -modular system. By (56.5), the central primitive idempotents in  $RG$  form a finite set  $\{b_1, \dots, b_t\}$ , and satisfy the conditions

$$(56.6) \quad 1 = b_1 + \cdots + b_t, \quad b_i b_j = 0, \quad i \neq j, \quad \text{and} \\ RG = RGb_1 \oplus \cdots \oplus RGb_t.$$

It is evident that for each  $i$ ,  $1 \leq i \leq t$ ,  $RGb_i$  is an indecomposable two-sided ideal with identity element  $b_i$ , and the decomposition (56.6) is the unique expression of  $RG$  as a direct sum of indecomposable two-sided ideals.

The central primitive idempotents in  $RG$  are called the *block idempotents* of  $RG$ , and the indecomposable two-sided ideals  $B_i = RGb_i$ , for  $1 \leq i \leq t$ , are called the *block ideals* of  $RG$ .

A  $p$ -block  $B_i^R$  of  $RG$ -modules is the category of all f.g. left  $B_i$ -modules, for some block ideal  $B_i = RGb_i$ ,  $1 \leq i \leq t$ . Since  $B_i$  is a two-sided ideal in  $RG$  with identity element  $b_i$ , the objects of the  $p$ -block  $B_i^R$  are precisely the f.g. left  $RG$ -modules  $M$  such that  $b_i M = M$ .

Let  $M$  be an arbitrary f.g.  $RG$ -module; then

$$M = b_1 M \oplus \cdots \oplus b_t M$$

by (56.6), and the summand  $b_i M$  is an  $RG$ -module belonging to the  $p$ -block  $B_i^R$ . In particular, each f.g. indecomposable  $RG$ -module  $M$  belongs to a unique  $p$ -block  $B_i^R$ , namely, the  $p$ -block  $B_i^R$  such that  $b_i M \neq 0$ .

The preceding discussion applies equally well to  $kG$ . Denoting the *block idempotents* of  $kG$  by  $\{\beta_1, \dots, \beta_u\}$ , we now have

$$kG = kG\beta_1 \oplus \cdots \oplus kG\beta_u,$$

the unique decomposition of  $kG$  into indecomposable two-sided ideals, called the *block ideals* of  $kG$ . Each block idempotent  $\beta_i$  defines a  $p$ -block  $B_i^k$  of  $kG$ -modules, consisting of all f.g. left  $kG$ -modules  $V$  such that  $\beta_i V = V$ , or equivalently, the category of all f.g. left  $kG\beta_i$ -modules.

The most important applications of block theory occur in the case where the blocks of  $kG$ -modules correspond bijectively to the blocks of  $RG$ -modules. This need not hold for an arbitrary  $p$ -modular system, but there is such a bijection whenever  $\{K, R, k\}$  is admissible for  $G$ , by (56.1) and (56.5ii). It should be pointed out that if hypothesis (56.3b) holds for  $KG$ , then  $KG$  is a direct sum of full matrix algebras over  $K$ , and so its center  $c(KG)$  is a direct sum of copies

of  $K$ , and is also a split semisimple  $K$ -algebra. Thus, if  $(K, R, k)$  is admissible for  $G$ , then it is admissible for both  $RG$  and  $c(RG)$ , in the sense of Definition 56.3.

**(56.7) Proposition.** *Let the  $p$ -modular system  $(K, R, k)$  be admissible for  $G$ . Then reduction mod  $\mathfrak{p}$  defines a surjection  $c(RG) \rightarrow c(kG)$ , which, in turn, sets up a bijection*

$$b_i \rightarrow \bar{b}_i = \beta_i, \quad 1 \leq i \leq t,$$

*between the set of all block idempotents  $\{b_1, \dots, b_t\}$  of  $RG$  and the corresponding set  $\{\beta_1, \dots, \beta_t\}$  in  $kG$ .*

This is clear from the preceding remarks. We now introduce a simpler notation.

**(56.8) Definition.** Let  $(K, R, k)$  be an admissible  $p$ -modular system for  $G$ , and let  $\{b_1, \dots, b_t\}$  be the block idempotents of  $RG$ . Each  $b_i$  defines a  $p$ -block  $B_i$  of  $G$ , consisting of all f.g.  $RG$ -modules,  $KG$ -modules, and  $kG$ -modules on which  $b_i$  acts as the identity, together with their trace functions and Brauer characters. (Here,  $b_i$  acts on  $kG$ -modules via the homomorphism  $b_i \rightarrow \bar{b}_i = \beta_i$ , and on  $KG$ -modules via the inclusion  $b_i \in RG \subseteq KG$ .) We use the notation

$$M \in B_i, \quad \zeta \in B_i, \quad \psi \in B_i, \quad \text{etc.,}$$

to indicate that a module  $M$ , a  $K$ -character  $\zeta$ , or a Brauer character  $\psi$  of a  $kG$ -module belong to the block  $B_i$ .

**Remarks.** (i) It is clear that a  $p$ -modular system  $(K, R, k)$ , with  $\text{char } K = 0$  and  $K$  sufficiently large relative to  $G$ , is admissible for an arbitrary subgroup  $H$  of  $G$ , so the  $p$ -blocks of  $H$  are defined by the block idempotents in  $RH$ , using (56.8). Of course, a main problem is the relation between  $p$ -blocks of  $G$  and  $p$ -blocks of subgroups of  $G$ .

(ii) By a previous remark, each indecomposable  $RG$ -module belongs to a unique  $p$ -block. In particular, each P.I.M.  $P \in \mathcal{P}(RG)$  belongs to a unique  $p$ -block. If  $P = RGe$  for some primitive idempotent  $e$ , then  $P \in B_i$  implies that  $b_i P = P$ , and hence  $P \leq B_i$ , where  $B_i$  is the block ideal  $RGB_i$ . It follows that each block ideal  $B_i$  is a direct sum of P.I.M.'s belonging to the block  $B_i$ .

**(56.9) Examples.** Let  $(K, R, k)$  be a  $p$ -modular system with  $\text{char } K = 0$  and  $K$  sufficiently large relative to  $G$ . Proofs of the results below are left as exercises.

(i) If  $G$  is a  $p'$ -group, then  $|G|^{-1} \in R$ , so by (9.21ii) the central primitive idempotents in  $KG$  all belong to  $RG$ , and hence are the block idempotents. In this case,  $RG$  is a maximal order in  $KG$ , by (27.1), and the block ideals in  $RG$  are maximal orders in the Wedderburn components of  $KG$ . If  $P$  is a P.I.M. in  $RG$ , then  $KP$  is a simple  $KG$ -module, and  $\bar{P}$  is a simple  $kG$ -module. Two

P.I.M.'s in  $RG$  belong to the same  $p$ -block if and only if they are isomorphic. Evidently, in this situation,  $p$ -blocks have little to contribute to the representation theory of  $G$ .

(ii) Now assume that  $G$  is a  $p$ -group. In this case,  $RG$  is a local ring by (5.25), so 1 is the only block idempotent, and there is only one  $p$ -block.

### §56C. A Criterion for P.I.M.'s to Belong to the Same $p$ -Block

Let  $G$  be a finite group, and  $(K, R, k)$  an arbitrary  $p$ -modular system. We shall investigate the distribution of P.I.M.'s of  $kG$  and  $RG$  into blocks. One of the earliest results of block theory is the following criterion, due to Brauer-Nesbitt ([37], §6), for two P.I.M.'s in  $\mathcal{P}(kG)$  to be summands of the same block ideal in  $kG$ .

**(56.10) Definition.** Two P.I.M.'s  $U$  and  $U'$  in  $\mathcal{P}(kG)$  are said to be *linked* if and only if there is a sequence of P.I.M.'s  $\{U_1, \dots, U_m\}$  in  $\mathcal{P}(kG)$  such that  $U_1 = U$ ,  $U_m = U'$ , and for each  $i$ ,  $1 \leq i \leq m - 1$ ,  $U_i$  and  $U_{i+1}$  have a composition factor in common.

The relation of linkage clearly is an equivalence relation on the set of all P.I.M.'s in  $\mathcal{P}(kG)$ , while the simpler condition of relating two P.I.M.'s if they have a composition factor in common is not. The concept of linkage, incidentally, has proved useful in other categories of modules (see Humphreys-Jantzen [78] and Donkin [80] for the theory of blocks of rational  $G$ -modules, for a semisimple algebraic group  $G$ ).

The main result about linkage classes holds for P.I.M.'s in  $kG$ , for an arbitrary field  $k$  of characteristic  $p > 0$ . We recall that, by (56.5), the central primitive idempotents in  $kG$  form a finite set  $\{\beta_1, \dots, \beta_u\}$ . Moreover, we have

$$(56.11) \quad kG = kG\beta_1 \oplus \cdots \oplus kG\beta_u,$$

and this is the unique decomposition of  $kG$  as a direct sum of indecomposable two-sided ideals, called *block ideals*, as in §56B.

We now have the following result (see CR §55 for the corresponding theorem for artinian rings).

**(56.12) Theorem.** *Each block ideal in  $kG$  is the direct sum of all indecomposable projective left ideals belonging to one linkage class (see (56.10)). Thus two P.I.M.'s are linked if and only if they are isomorphic to direct summands of a single block ideal in  $kG$ . In particular, no two distinct block ideals of  $kG$  have a composition factor in common.*

The proof is based on the following important method for identifying composition factors.

**(56.13) Lemma.** *Let  $A$  be a left artinian ring, let  $Ae$  be a P.I.M. generated by*

a primitive idempotent  $e$ , and let  $F$  be the simple module  $Ae/(\text{rad } A)e$ . A f.g. left  $A$ -module  $M$  has a composition factor isomorphic to  $F$  if and only if  $eM \neq 0$ .

*Proof.* (See Exercise 3.10 for the case of a semisimple ring  $A$ .) From §3A,  $M$  has a composition series

$$M = M_0 > M_1 > \cdots > M_s > 0.$$

Since  $e$  is idempotent, it follows that  $eM \neq 0$  if and only if  $e(M_i/M_{i+1}) \neq 0$  for some  $i$ ,  $1 \leq i \leq s$ .

We now prove that  $e(M_i/M_{i+1}) \neq 0$  if and only if  $F \cong M_i/M_{i+1}$ . To show this, let  $W$  be the simple module  $M_i/M_{i+1}$ , and suppose  $eW \neq 0$ . Then  $ew \neq 0$  for some  $w \in W$ , and hence  $W = Aew$ , since  $W$  is a simple module. Then the obvious homomorphism  $Ae \rightarrow Aew$  defines an isomorphism  $F \cong W$ , since  $\text{rad } Ae$  is the unique maximal submodule of  $Ae$ . Conversely, if  $Ae/\text{rad } Ae \cong W$ , there is a nonzero homomorphism  $f: Ae \rightarrow W$ . Then  $f(e) \neq 0$  since  $f(Ae) = Af(e)$ , and  $f(e) \in eW$ , completing the proof.

*Proof of (56.12).* Each indecomposable projective left ideal in  $kG$  is generated by a primitive idempotent (see §56A). Let  $\{B_1, \dots, B_v\}$  be left ideals in  $kG$ , each of which is the sum of all indecomposable projective left ideals belonging to a single linkage class. We first prove that  $B_i B_j = 0$  if  $i \neq j$ . Otherwise, there exist indecomposable projective left ideals  $kGe$  and  $kGf$ , belonging to different linkage classes, such that  $(kGe)(kGf) \neq 0$ , which is impossible by Lemma 56.13. It follows that the ideals  $\{B_i\}_{1 \leq i \leq v}$  are two-sided ideals, and that  $kG = B_1 \oplus \cdots \oplus B_v$ . Since the decomposition (56.11) is the unique expression of  $kG$  as a direct sum of indecomposable two-sided ideals, each ideal  $B_i$  is a direct sum of certain of the block ideals  $\{kG\beta_i\}$ .

We now prove that the decompositions are the same. By the definition of the ideals  $\{B_i\}$ , it is sufficient to prove that if  $e$  and  $e'$  are primitive idempotents of  $kG$  such that  $kGe$  and  $kGe'$  have a common composition factor, and if  $kGe \leq kG\beta_j$ , then also  $kGe' \leq kG\beta_j$ . But if  $kGe' \leq kG\beta_l$ , with  $l \neq j$ , then  $\beta_l$  acts as 1 on every composition factor of  $kGe'$ , and as 0 on every composition factor of  $kGe$ . This contradicts the hypothesis that  $kGe$  and  $kGe'$  have a common composition factor, and completes the proof that each  $B_i$  is a block ideal.

**(56.14) Corollary.** Let  $G$  be a finite group, and let  $(K, R, k)$  be an admissible  $p$ -modular system for  $G$ . Then the following conditions concerning two P.I.M.'s  $P$  and  $P'$  in  $\mathcal{P}(RG)$  are equivalent:

- (i)  $P$  and  $P'$  belong to the same  $p$ -block of  $G$ .
- (ii)  $\bar{P}$  and  $\bar{P}'$  belong to the same  $p$ -block of  $G$ .
- (iii)  $\bar{P}$  and  $\bar{P}'$  belong to the same linkage class of left  $kG$ -modules (according to Definition 56.10).

*Proof.* Let  $\{b_1, \dots, b_t\}$  be the block idempotents of  $c(RG)$ . By (56.8),  $\{\bar{b}_i\}$  are

the block idempotents of  $c(RG)$ , and it follows that (i) and (ii) are equivalent. Since  $\bar{P}$  and  $\bar{P}'$  are P.I.M.'s in  $\mathcal{P}(kG)$  by the discussion at the end of §56A, (ii) and (iii) are also equivalent, by Theorem 56.12.

### §56D. Central Characters and Blocks of $KG$ -Modules.

In §56B, the  $p$ -blocks of  $G$  were defined in terms of the block idempotents of  $RG$  (and  $kG$ ). For applications to character theory, it is essential to know the distribution of simple  $KG$ -modules, and their characters, among the  $p$ -blocks. A solution to this problem, in principle, is provided by the connection between  $p$ -blocks and representations of the centers of  $RG$  and  $kG$ .

**(56.15) Definition.** Let  $A$  be f.d. algebra over a field  $k$ . A *central character* of  $A$  is a surjective homomorphism of  $k$ -algebras

$$\varphi: c(A) \rightarrow k'$$

from the center of  $A$  to a finite extension field  $k'$  of  $k$ . Two central characters

$$\varphi: c(A) \rightarrow k', \quad \psi: c(A) \rightarrow k''$$

are said to be *equivalent* if there is a  $k$ -isomorphism of fields  $\sigma: k' \rightarrow k''$  such that the diagram

$$\begin{array}{ccc} c(A) & \xrightarrow{\varphi} & k' \\ & \downarrow \cdot & \downarrow \sigma \\ & \xrightarrow{\psi} & k'' \end{array}$$

commutes.

Evidently, equivalence of central characters is an equivalence relation.

**(56.16) Proposition.** Let  $G$  be a finite group, and  $k$  a field. Let  $\{\beta_1, \dots, \beta_u\}$  be the block idempotents in  $c(kG)$ .

(i) For each block idempotent  $\beta_i$ , let

$$m_i = c(kG)/(\text{rad } c(kG) + c(kG)(1 - \beta_i)), \quad \text{and} \quad k_i = c(kG)/m_i.$$

Then  $m_i$  is a maximal ideal in  $c(kG)$ ,  $k_i$  is a finite extension field of  $k$ , and the natural map

$$\psi_i: c(kG) \rightarrow c(kG)/m_i = k_i$$

is a central character of  $kG$  with the property that

$$\psi_i(\beta_i) = 1 \quad \text{and} \quad \psi_i(\beta_j) = 0 \quad \text{if } i \neq j.$$

(ii) Every central character  $\psi: c(kG) \rightarrow k'$  is equivalent to exactly one of the central characters  $\psi_i$  defined in (i).

*Proof.* (i) For each  $i$ ,  $\beta_i$  is a primitive idempotent in the commutative  $K$ -algebra  $c(kG)$ , and  $\text{rad } c(kG)\beta_i$  is the unique maximal submodule of  $c(kG)\beta_i$ , by (6.9). It follows that  $\mathfrak{m}_i$  is a maximal ideal in  $c(kG)$ . Then  $k_i = c(kG)/\mathfrak{m}_i$  is a finite extension field of  $k$ , and the natural map  $\psi_i: c(kG) \rightarrow k_i$  has the required properties.

(ii) Let  $\psi: c(kG) \rightarrow k'$  be any central character. Then  $\mathfrak{m} = \ker \psi$  is a maximal ideal in  $c(kG)$ , and  $k' \cong c(kG)/\mathfrak{m}$ . Now

$$c(kG) = c(kG)\beta_1 \oplus \cdots \oplus c(kG)\beta_u$$

is the unique decomposition of  $c(kG)$  as a direct sum of indecomposable ideals. For some  $i$ ,  $\beta_i \notin \mathfrak{m}$ , so  $c(kG)\beta_i + \mathfrak{m} = c(kG)$ , and hence

$$c(kG)/\mathfrak{m} \cong c(kG)\beta_i/(c(kG)\beta_i \cap \mathfrak{m})$$

by an isomorphism theorem. Then  $c(kG)\beta_i \cap \mathfrak{m}$  coincides with the unique maximal submodule  $\text{rad } c(kG)\beta_i$  of  $c(kG)\beta_i$ . A similar argument shows that  $c(kG)(1 - \beta_i) \leq \mathfrak{m}$ , and it follows that  $\mathfrak{m} = \mathfrak{m}_i$ . Since  $k' \cong c(kG)/\mathfrak{m}$ , it follows that there exists an isomorphism of  $k$ -algebras  $\sigma: k' \rightarrow k_i$  such that  $\sigma \circ \psi = \psi_i$ , completing the proof.

Let  $R$  be a d.v.r. with maximal ideal  $\mathfrak{p}$  and residue class field  $k = R/\mathfrak{p}$ . By (56.2) we have

$$c(RG)/\text{rad } c(RG) \cong c(kG)/\text{rad } c(kG).$$

Then the simple  $c(RG)$ -modules can be identified with the simple  $c(kG)$ -modules, and these correspond to the central characters of  $kG$ . Thus we are led to:

**(56.17) Definition.** Let  $R$  be a d.v.r. with residue class field  $k = R/\mathfrak{p}$ . A *central character*  $\lambda$  of  $RG$  is a surjective homomorphism of  $R$ -algebras  $\lambda: c(RG) \rightarrow k'$ , where  $k'$  is a finite extension field of  $k$ , and  $k'$  is viewed as an  $R$ -algebra via the natural map from  $R$  to  $k$ . Equivalence of central characters of  $RG$  is defined as in (56.15).

**(56.18) Proposition.** Let  $v: c(RG) \rightarrow c(kG)$  be the natural surjection (see (56.1)).

(i) For each central character  $\psi$  of  $RG$ ,  $\ker \psi \geq \ker v$ , and there exists a unique central character  $\xi$  of  $kG$  such that

$$\psi = \xi \circ v.$$

(ii) The correspondence defined in (i) is a bijection, preserving the relation of equivalence, from the set of central characters of  $RG$  to the set of central characters of  $kG$ .

*Proof.* Let  $\psi$  be a central character of  $RG$ . Then  $\ker \psi$  is a maximal ideal of  $c(RG)$ , so  $\ker \psi \supseteq \text{rad } c(kG) \supset pc(kG) = \ker \nu$ , by (56.2) and therefore the first statement follows. The proof of the second statement is left as an exercise for the reader.

**Remark.** The equivalence classes of central characters of  $RG$  do not correspond bijectively with the block idempotents of  $RG$  as in (56.16) unless some additional hypotheses are satisfied, such as the completeness of  $R$ . The reason is that  $\text{rad } c(RG)b_i$  is not necessarily maximal in  $c(RG)b_i$ , for a block idempotent  $b_i$ , so the ideals  $m_i$  defined as in (56.16) are not necessarily maximal in  $c(RG)$ . This difficulty does not arise if  $(K, R, k)$  is a  $p$ -modular system which is admissible for  $G$ , since, in that case,  $c(RG)$  is a semiperfect ring. Thus we have

**(56.19) Proposition.** *Let  $(K, R, k)$  be a  $p$ -modular system which is admissible for  $G$ . Then the following sets are in bijective correspondence, defined by (56.16) and (56.18):*

- (i) *The  $p$ -blocks  $\{B_i\}$  of  $G$ ;*
- (ii) *The equivalence classes of central characters of  $RG$ ;*
- (iii) *The equivalence classes of central characters of  $kG$ .*

A central character  $\psi$  of  $RG$  (and its equivalence class) corresponds to a  $p$ -block  $B_i$  if and only if  $\psi(b_i) = 1$  and  $\psi(b_j) = 0$ ,  $j \neq i$ , where  $\{b_i\}$  are the block idempotents in  $RG$ . A similar statement applies to central characters of  $kG$ .

A sharper statement holds when  $k$  is a splitting field for  $G$ , that is,  $kG/\text{rad } kG$  is a split semisimple  $k$ -algebra.

**(56.20) Proposition.** *Let  $(K, R, k)$  be a  $p$ -modular system such that  $\text{char } K = 0$  and  $K$  is sufficiently large relative to  $G$ . Then  $(K, R, k)$  is admissible for  $G$ , and the following statements hold.*

- (i) *Each central character  $\psi_i$  of  $kG$  (as in (56.16i)) gives a homomorphism of  $k$ -algebras  $\psi_i: c(kG) \rightarrow k$ ; in other words, the fields  $\{k_i\}$  all coincide with  $k$ .*
- (ii) *Let  $\psi: c(kG) \rightarrow k'$  be an arbitrary central character of  $kG$ . Then  $k' = k$ , and  $\psi$  coincides with exactly one of the central characters  $\psi_i$ .*
- (iii) *Let  $\mathbf{F}$  be an irreducible  $k$ -representation of  $G$ . Then for each  $a \in c(kG)$ ,*

$$\mathbf{F}(a) = \psi(a)\mathbf{I} \quad \text{with } \psi(a) \in k,$$

and the map  $a \mapsto \psi(a)$  is a central character of  $kG$ .

- (iv) *Two irreducible  $k$ -representations  $\mathbf{F}$  and  $\mathbf{F}'$  of  $G$  belong to the same  $p$ -block if and only if the central characters  $\psi$  and  $\psi'$  corresponding to them, as in part (iii), coincide.*

*Proof.* We begin with part (iii). Since  $K$  is sufficiently large,  $k$  is a splitting

field for  $G$  by (17.2), and the commuting algebra of the set of matrices  $\{F(x) : x \in G\}$  is  $k \cdot \mathbf{I}$ . Thus if  $a \in c(kG)$ ,  $F(a) = \psi(a)\mathbf{I}$  with  $\psi(a) \in k$ , and (iii) is proved. Each central character  $\psi$  defined as in part (iii) is equivalent to one of the central characters  $\psi_i$ , by (56.16ii), and, in this case, we clearly have  $k_i = k$  and  $\psi = \psi_i$ —equivalence becomes equality.

Now let  $\psi_j$  be an arbitrary central character associated with a block idempotent  $\beta_j$  of  $kG$ . Then  $\psi_j$  is the central character corresponding, as in (iii), to any irreducible  $k$ -representation  $\mathbf{F}$  belonging to the block  $B_j$ , by the first part of the proof, and it follows that  $k_j = k$ . The rest of the proof is immediate from these remarks.

We are now in a position to discuss the  $p$ -blocks of  $KG$ -modules, for a  $p$ -modular system  $(K, R, k)$  such that  $\text{char } K = 0$ , and  $K$  is sufficiently large relative to  $G$ . The  $p$ -modular system is admissible for  $G$ , and the natural map  $RG \rightarrow kG$  defines a bijection

$$b_i \leftrightarrow \bar{b}_i, \quad 1 \leq i \leq t$$

from the block idempotents of  $RG$  to those of  $kG$ , by (56.7).

We wish to reorganize the character table data for  $K$ -characters and Brauer characters of  $kG$ -modules, summarized in (9.25) and (18.18), in terms of the  $p$ -blocks of  $G$ . We begin by discussing the principles on which this organization is based.

Each irreducible  $K$ -character  $\zeta \in \text{Irr } G$  defines a central character  $\omega: c(KG) \rightarrow K$ , as follows: let  $Z$  be a simple  $KG$ -module affording the character  $\zeta$ , and let  $\mathbf{Z}$  be an irreducible matrix representation of  $KG$  afforded by  $Z$ . Then

$$\mathbf{Z}(C_i) = \omega(C_i)\mathbf{I}$$

and (see §9D)  $\omega$  is a central character of  $KG$ , such that

$$(56.21) \quad \omega(C_i) = |\mathfrak{C}_i| \zeta(x_i)/\zeta(1), \quad \text{where } x \in \mathfrak{C}_i,$$

and  $C_i$  is the class sum associated with the class  $\mathfrak{C}_i$ . By (9.31) we have  $\omega(C_i) \in \text{alg. int. } \{K\}$  for each  $i$ , and hence  $\omega(C_i) \in R$ . We now define

$$(56.22) \quad \bar{\omega}: c(kG) \rightarrow k \quad \text{by } \bar{\omega}(C_i) = \overline{\omega(C_i)} \text{ for each } i.$$

If the multiplication of class sums is given by

$$C_i C_j = \sum c_{ijk} C_k, \quad c_{ijk} \in \mathbb{Z},$$

then by (9.30) we obtain

$$\omega(C_i) \omega(C_j) = \sum c_{ijk} \omega(C_k), \quad \text{and} \quad \bar{\omega}(C_i) \bar{\omega}(C_j) = \sum \bar{c}_{ijk} \bar{\omega}(C_k).$$

It follows that  $\bar{\omega}: c(kG) \rightarrow k$  is a central character of  $kG$ .

Now let  $B_i$  be the  $p$ -block defined by the block idempotent  $b_i$ . Then  $Z \in B_i$  if and only if  $b_i$  acts as 1 on  $Z$ , or equivalently,

$$\omega(b_i) = 1, \quad \omega(b_j) = 0 \quad \text{for } j \neq i.$$

Therefore  $Z \in B_i$  if and only if  $\bar{\omega} = \psi_i$ , where  $\psi_i$  is the central character of  $c(kG)$  associated with  $b_i$  as in (56.19). We have thus proved:

**(56.23) Proposition.** *Let  $Z$  and  $Z'$  be simple  $KG$ -modules, and  $\omega, \omega'$  the corresponding central characters of  $KG$ . Then  $Z$  and  $Z'$  belong to the same  $p$ -block if and only if  $\bar{\omega} = \bar{\omega}'$ , where  $\{\bar{\omega}, \bar{\omega}'\}$  are the central characters of  $kG$  defined in (56.22).*

**(56.24) Corollary** (Brauer-Nesbitt [41]). *Two irreducible  $K$ -characters  $\{\zeta, \zeta'\}$  of  $G$  belong to the same  $p$ -block if and only if*

$$|\mathfrak{C}| \zeta(x)/\zeta(1) \equiv |\mathfrak{C}| \zeta'(x)/\zeta'(1) \pmod{p}$$

for each conjugacy class  $\mathfrak{C}$ , and each  $x \in \mathfrak{C}$ .

The preceding result gives the distribution of the irreducible characters into  $p$ -blocks for any finite group  $G$  whose character table is known.

Another description of the  $p$ -blocks of  $K$ -characters is easily obtained as follows. Let  $\text{Irr } G = \{\zeta^1, \dots, \zeta^s\}$ , and for each  $i$ , let  $e_i$  be the central primitive idempotent in  $KG$  defined by  $\zeta^i$ . Thus (see (9.21))

$$e_i = \zeta^i(1)|G|^{-1} \sum_{x \in G} \zeta^i(x^{-1})x.$$

Because of the factor  $|G|^{-1}$ , the idempotents  $e_i$  usually do not belong to  $RG$ . On the other hand, each block idempotent  $b \in c(RG)$  belongs to  $c(kG)$ , and hence can be expressed uniquely as a sum of the central idempotents  $\{e_i\}_{1 \leq i \leq s}$ . Therefore we obtain

**(56.25) Proposition.** *Let  $B$  be a  $p$ -block of  $G$ , defined by the block idempotent  $b \in RG$ . Then, letting  $e_i$  be the central idempotent associated with  $\zeta^i \in \text{Irr } G$ ,*

$$b = \sum_{\zeta^i \in B} e_i$$

is the expression of  $b$  as a sum of central primitive idempotents in  $KG$ .

**(56.26) Organization of  $p$ -Blocks of Characters.** The distribution among the  $p$ -blocks of simple  $KG$ -modules and  $kG$ -modules, and their characters and Brauer characters, of course leads to information about the decomposition matrix and the Cartan matrix (see §18). Keeping  $(K, R, k)$  as in the preceding two results, let us number the simple  $KG$ -modules and their characters

$$\{Z_1, \dots, Z_s\}, \quad \{\zeta^1, \dots, \zeta^s\}$$

so that the first  $x_1$  of them belong to the block  $B_1$ , the next  $x_2$  to  $B_2$ , etc. As in (9.25), we let  $\zeta^1 = 1_G$  be the principal (or trivial) character, and call the  $p$ -block  $B_1$  containing  $1_G$  the *principal p-block of G*. We also number the simple  $kG$ -modules  $\{F_1, \dots, F_r\}$  and their Brauer characters  $\{\varphi^1, \dots, \varphi^r\}$  in a similar manner. Finally the P.I.M.'s  $\{U_1, \dots, U_r\}$  of  $kG$  and their Brauer characters  $\{\eta^1, \dots, \eta^r\}$  are arranged so that  $F_i = U_i/\text{rad } U_i$ ,  $1 \leq i \leq r$ . For each block idempotent  $b \in RG$ , we know that  $\bar{b}$  is a block idempotent in  $kG$ , and clearly  $\bar{b}U_i \neq 0$  if and only if  $\bar{b}F_i \neq 0$ . Thus the P.I.M.'s  $\{U_i\}$  are distributed among the blocks in the same way as the  $\{F_i\}$ .

If  $M_i$  is a full  $RG$ -lattice in  $Z_i$ , and  $Z_i \in B$ , then the block idempotent  $b$  of  $B$  acts as the identity on  $M_i$ . Then  $\bar{b} = id$  on  $\bar{M}_i$ , and it follows that all the composition factors of  $M_i$  belong to  $B$ . Let

$$d: G_0(kG) \rightarrow G_0(kG)$$

be the *decomposition map* (see (16.20)), so by (16.19) we have

$$d[Z_i] = \sum_{j=1}^r d_{ij}[F_j], \quad 1 \leq i \leq s,$$

where  $\mathbf{D} = (d_{ij})$  is the *decomposition matrix*. By the way we have ordered the modules, the decomposition matrix has the form

$$(56.27) \quad \mathbf{D} = \begin{bmatrix} \mathbf{D}_1^{x_1 \times y_1} & & \mathbf{0} \\ & \ddots & \\ \mathbf{0} & & \mathbf{D}_t^{x_t \times y_t} \end{bmatrix}$$

with zeros except for the diagonal blocks  $\{\mathbf{D}_i\}_{1 \leq i \leq t}$ , where each diagonal block describes the decomposition map for  $K$ -characters belonging to a given block.

The *Cartan map* (see (18.4))

$$c: K_0(kG) \rightarrow G_0(kG)$$

is defined by the  $r \times r$  *Cartan matrix*  $\mathbf{C} = (c_{ij})$ , where

$$c[U_i] = \sum_{j=1}^r c_{ij}[F_j], \quad 1 \leq i \leq r.$$

Then because of the arrangement of the P.I.M.'s  $\{U_i\}$  and the simple modules  $\{F_j\}$  according to blocks, the Cartan matrix also has a block decomposition

$$(56.28) \quad \mathbf{C} = \begin{bmatrix} \mathbf{C}_1^{y_1 \times y_1} & & \\ & \ddots & \\ & & \mathbf{C}_t^{y_t \times y_t} \end{bmatrix}$$

with zeros except for the diagonal blocks  $\{\mathbf{C}_i\}$ . Each diagonal block describes the action of the Cartan map on the P.I.M.'s belonging to a given block. Using the basic result (18.10) that  $\mathbf{C} = {}^t \mathbf{D} \mathbf{D}$ , we obtain

$$\mathbf{C}_i = {}^t \mathbf{D}_i \mathbf{D}_i, \quad 1 \leq i \leq t.$$

### §56E. The Defect of a Block

We continue the investigation of  $p$ -blocks of characters in  $\text{Irr } G$ . As in §56D,  $(K, R, k)$  denotes a  $p$ -modular system, such that  $\text{char } K = 0$  and  $K$  is sufficiently large relative to  $G$ . We shall define a nonnegative integer associated with each block, called its *defect*. This concept was introduced by Brauer-Nesbitt [41]; it relates the degrees of the characters in a  $p$ -block to properties of the block idempotents in  $RG$  and  $kG$ . In §57, we shall define a  $p$ -subgroup of  $G$  associated to each  $p$ -block, called the *defect group* of the block, whose order is  $p^d$ , where  $d$  is the defect.

We shall follow the organization of modules, characters, etc. in terms of the  $p$ -blocks  $\{\mathbf{B}_1, \dots, \mathbf{B}_t\}$ , defined by the block idempotents  $\{b_1, \dots, b_t\}$ , as described in (56.26). Since  $(K, R, k)$  is an admissible  $p$ -modular system,  $\{\bar{b}_1, \dots, \bar{b}_t\}$  are the block idempotents in  $kG$ , by (56.8).

We shall often use the  $p$ -adic valuation  $v_p$ , defined on the rational field  $\mathbb{Q}$  (see §4). Thus, for  $a \in \mathbb{Z}$ ,  $v_p(a)$  is the exponent to which  $p$  appears in the prime factorization of  $a$ , and we have  $v_p(a/b) = v_p(a) - v_p(b)$ , for  $a, b \in \mathbb{Z}$ ,  $b \neq 0$ .

Let us set

$$z_i = \zeta^i(1) = \dim_K Z_i, \quad f_j = \varphi^j(1) = \dim_k F_j, \quad u_j = \eta^j(1) = \dim_K U_j,$$

where  $1 \leq i \leq s$ ,  $1 \leq j \leq r$ . We also put

$$|G| = g, \quad e = v_p(g), \quad G_{p'} = \{\text{all } p\text{-regular elements of } G\}.$$

**(56.30) Definition.** The *defect*  $d_j$  of the  $p$ -block  $\mathbf{B}_j$  is the integer defined by the formula

$$d_j = e - \min \{v_p(z_i) : Z_i \in \mathbf{B}_j\}.$$

Since  $z_i \mid g$  for each  $i$  by (9.32), it follows that the defect of a block is always a nonnegative integer. A restatement of the definition is:

$$p^{e-d_j} \mid z_i \text{ for all } Z_i \in \mathbf{B}_j \quad \text{but} \quad p^{e-d_j+1} \nmid z_i \text{ for some } Z_i \in \mathbf{B}_j.$$

In the extreme case of defect zero, we have:

**(56.31) Proposition.** Let  $\mathbf{B}_j$  be a  $p$ -block of defect zero. Then  $\mathbf{B}_j$  contains exactly one simple  $KG$ -module  $Z$ , exactly one simple  $kG$ -module  $F$ , and exactly one P.I.M.  $U$ . The contributions  $\mathbf{D}_j$  and  $\mathbf{C}_j$  to the decomposition matrix and the Cartan

matrix, respectively, are given by

$$\mathbf{D}_j = (1), \quad \mathbf{C}_j = (1).$$

Moreover,  $\zeta(x) = 0$  for all  $p$ -irregular  $x \in G$ , where  $\zeta$  is the character afforded by  $Z$ .

*Proof.* Let  $Z$  be a simple  $KG$ -module belonging to  $B_j$ , and let the primitive idempotent associated with  $Z$  be

$$e = \zeta(1)|G|^{-1} \sum_{x \in G} \zeta(x^{-1})x,$$

as in (9.21). Since  $B_j$  has defect zero, it follows that  $e \in RG$ , and hence  $Z$  is the only simple module in  $B_j$ , by (56.25). The rest of the proof follows from (18.28). We recall the argument, and give a new proof of a crucial step. There exists an indecomposable projective  $RG$ -module  $P_i$ , with  $K$ -character  $\tau_i$ , such that  $Z$  is a direct summand of  $K \otimes_R P_i$ . Then  $eP_i \neq 0$ , and hence  $eP_i = P_i$ . Thus  $\tau_i = a\zeta$  for some positive integer  $a$ , and it follows that  $\zeta$  vanishes on  $p$ -irregular elements, by (18.26). Then  $\zeta = \sum b_j \tau_j$  for some integers  $b_j$ , by (18.26), and it follows that  $a = 1$ , and  $\tau_i = \zeta$ . Then  $eRG = P_i \oplus \cdots \oplus P_i$ , and hence  $ekG = \bar{P}_i \oplus \cdots \oplus \bar{P}_i$ , where  $e$  is a block idempotent in  $kG$  and  $\bar{P}_i$  is an indecomposable projective  $kG$ -module. Since the block ideal  $ekG$  contains only one P.I.M., it follows that the block  $B_j$  contains only one simple  $kG$ -module  $F_i = \bar{P}_i/\text{rad } \bar{P}_i$ . Now consider the decomposition map, applied to  $[Z] = [K \otimes P_i]$ . Since  $\tau_i = \zeta$ , and  $\tau_i = \sum_{l=1}^s d_{il} \zeta^l$  by (18.26), we obtain  $d_{ii} = 1$  if  $\zeta = \zeta^i$  and  $d_{mi} = 0$  if  $m \neq i$ . Since the block  $B_j$  contains only one simple  $kG$ -module, it follows that  $\mathbf{D}_j = (1)$ , and hence  $\bar{P}_i$  is a simple  $kG$ -module, completing the proof. (This discussion gives a more conceptual version of the proof of CR (86.3), which used the orthogonality relations for the coefficients of the matrix representation affording  $\zeta$ .)

At the other extreme, the principal block  $B_1$  contains the trivial character  $1_G$ , and hence has defect  $e = |G|_p$ . Of course, there may be other blocks of defect  $e$ . A criterion for irreducible characters to belong to the principal block is easily derived from (56.23) (see the Exercises).

Returning to the general discussion, we next characterize the defect in terms of the degrees of the simple  $kG$ -modules.

**(56.32) Proposition.** *The defect  $d_j$  of the  $p$ -block  $B_j$  satisfies the equation*

$$d_j = e - \min \{v_p(f_i) : F_i \in B_j\}.$$

*Proof.* By (18.17), the  $s \times r$  matrix  $\bar{\mathbf{D}}$  has rank  $r$ . It follows that for each block  $B_j$ , the  $x_j \times y_j$  matrix  $\bar{\mathbf{D}}_j$  has rank  $y_j$ . On the other hand, we have

$$\zeta^i|_{G_{p'}} = \sum_{l=1}^r d_{il} \varphi^l, \quad 1 \leq i \leq s,$$

by (18.19). Upon evaluating both sides at 1 for the characters belonging to  $B_j$ , we obtain

$$\begin{bmatrix} z_{j_1} \\ \vdots \\ z_{j_{x_j}} \end{bmatrix} = \mathbf{D}_j \begin{bmatrix} f_{j_1} \\ \vdots \\ f_{j_{y_j}} \end{bmatrix}$$

where  $\{z_{j_1}, \dots, z_{j_{x_j}}\}$  and  $\{f_{j_1}, \dots, f_{j_{y_j}}\}$  are the degrees of the characters  $\zeta^i \in B_j$  and  $\varphi^i \in B_j$ , respectively. Since  $\mathbf{D}_j$  has rank  $y_j$ , it follows that

$$v_p(G.C.D.(z_{j_1}, \dots, z_{j_{x_j}})) = v_p(G.C.D.(f_{j_1}, \dots, f_{j_{y_j}})).$$

Then by (56.30),

$$e - d_j = \min \{v_p(z_i) : Z_i \in B_j\} = \min \{v_p(f_i) : F_i \in B_j\},$$

completing the proof.

Restating the preceding results, we have:

**(56.33) Corollary.** *The defect  $d_j$  of  $B_j$  is characterized as follows:*

$$\begin{aligned} d_j &= \text{smallest integer } (\geq 0) \text{ such that } p^{e-d_j} | z_i \text{ for all } Z_i \in B_j \\ &= \text{smallest integer } (\geq 0) \text{ such that } p^{e-d_j} | f_i \text{ for all } F_i \in B_j. \end{aligned}$$

We next find connections between the defect  $d_j$  of  $B_j$  and the coefficients of the block idempotent  $b_j \in c(RG)$ . We shall write

$$(56.34) \quad b_j = \sum_{m=1}^s a_{jm} C_m, \quad \text{where } a_{jm} \in R;$$

then  $\bar{b}_j = \sum_{m=1}^s \bar{a}_{jm} C_m$  is the corresponding block idempotent in  $c(kG)$ , by (56.5). For each block  $B_j$ , there is a central character  $\psi_j : c(kG) \rightarrow k$ , characterized by the conditions (see (56.16))

$$\psi_j(\bar{b}_j) = 1, \quad \psi_j(\bar{b}_l) = 0, \quad l \neq j.$$

Moreover, each simple  $KG$ -module  $Z$  is associated with a central character  $\omega$ , defined by (56.21), and we have

$$\bar{\omega} = \psi_j \Leftrightarrow Z \in B_j,$$

by (56.23).

We also require the character table data, as summarized in (18.18) and §18C. In particular, the conjugacy classes are arranged so that  $\mathfrak{C}_1, \dots, \mathfrak{C}_r$  are the  $p'$ -classes. The value of a character  $\zeta^i$  on an element of the class  $\mathfrak{C}_j$  is given by

$\zeta_j^i$ , while  $\zeta_{j*}^i$  denotes  $\zeta^i(x^{-1})$ ,  $x \in \mathfrak{C}_j$ . Similar notations are used for the Brauer characters  $\varphi^i$  and  $\eta^i$ ,  $1 \leq i \leq r$ .

**(56.35) Proposition.** *The coefficients of the block idempotent  $b_j = \sum a_{jm} C_m$  in  $c(RG)$  are given by*

$$a_{jm} = g^{-1} \sum_{Z_i \in \mathfrak{B}_j} z_i \zeta_{m*}^i$$

while for  $p$ -regular classes  $\mathfrak{C}_m$ , we also have

$$a_{jm} = g^{-1} \sum_{F_l \in \mathfrak{B}_j} u_l \varphi_{m*}^l.$$

*Proof.* The first formula is immediate from (56.25). Using the first formula, we have, for a  $p$ -regular class  $\mathfrak{C}_m$ ,

$$\begin{aligned} a_{jm} &= g^{-1} \sum_{Z_i \in \mathfrak{B}_j} z_i \zeta_{m*}^i = g^{-1} \sum_{Z_i \in \mathfrak{B}_j} z_i \left( \sum_{F_l \in \mathfrak{B}_j} d_{il} \varphi_{m*}^l \right) \\ &= g^{-1} \sum_{F_l \in \mathfrak{B}_j} \left( \sum_{Z_i \in \mathfrak{B}_j} d_{il} z_i \right) \varphi_{m*}^l \\ &= g^{-1} \sum_{F_l \in \mathfrak{B}_j} u_l \varphi_{m*}^l \end{aligned}$$

since

$$(\eta_j^i) = \mathbf{C}(\varphi_j^i) = {}^t \mathbf{DD}(\varphi_j^i) = {}^t \mathbf{D}(\zeta_j^i)$$

by (18.21) and (18.10). This completes the proof.

**(56.36) Definition.** The defect  $\delta_i$  of the conjugacy class  $\mathfrak{C}_i$  of  $G$  is the nonnegative integer

$$\delta_i = e - v_p(h_i) \quad \text{where } h_i = |\mathfrak{C}_i|.$$

If  $x \in \mathfrak{C}_i$ , then  $h_i = |G:C_G(x)|$ , and thus  $\delta_i = v_p|C_G(x)|$ ,  $x \in \mathfrak{C}_i$ .

The next result includes Osima's theorem that the block idempotents in  $c(RG)$  are supported on the  $p$ -regular classes, and relates the coefficients of the block idempotents in  $c(kG)$  to the class defects  $\delta_j$ .

**(56.37) Proposition.** *Let  $b_j = \sum a_{jm} C_m$  be a block idempotent in  $RG$  belonging to a block  $\mathfrak{B}_j$  of defect  $d_j$ . The coefficients satisfy the conditions:*

- (i)  $a_{jm} = 0$  for each  $p$ -irregular class  $\mathfrak{C}_m$ , and
- (ii)  $\bar{a}_{jm} = 0$  for each  $p$ -regular class  $\mathfrak{C}_m$  such that  $\delta_m > d_j$ .

The proof of the first part is based on a lemma:

**(56.38) Lemma.** *For all  $p$ -irregular  $x \in G$  and  $p$ -regular  $y \in G$  we have*

$$\sum_{Z_i \in B_j} \zeta^i(x) \zeta^i(y) = 0.$$

*Proof.* Let  $\mathbf{Z} = (\zeta_j^i)^{s \times r}$  be the matrix of character values of the  $\zeta^i \in \text{Irr } G$  on the  $p$ -regular classes. Since  $x$  is  $p$ -irregular, we have

$$(\zeta^1(x), \dots, \zeta^s(x)) \mathbf{Z} = 0$$

by the second orthogonality relation (9.26). The same formula holds with  $\mathbf{D}$  in place of  $\mathbf{Z}$ , since  $\mathbf{Z} = \mathbf{D}\Phi$  and  $\Phi$  is invertible. Using the distribution of the characters  $\zeta^i$  into blocks, together with the resulting decomposition (56.27) of the decomposition matrix  $\mathbf{D}$ , it follows that for each  $l$  such that  $\varphi^l \in B_j$ , we have

$$\sum_{Z_l \in B_j} \zeta^i(x) d_{il} = 0$$

Therefore, after multiplying by  $\varphi^l(y)$  and summing on  $l$ , we obtain the desired formula, since

$$\zeta^i(y) = \sum_{F_l \in B_j} d_{il} \varphi^l(y).$$

*Proof of (56.37).* (i) This result follows at once by setting  $y = 1$  in (56.38), and applying the first formula for the coefficients  $a_{jm}$  in (56.35).

(ii) Assume  $\delta_m > d_j$ , let  $Z_i \in B_j$ , and let  $\omega^i$  be the central character of  $KG$  corresponding to  $Z_i$ , as in (56.21). Then

$$\omega^i(C_m) = h_m \zeta_m^i / z_i \in R,$$

and it follows that  $\zeta_m^i \in p$ , because

$$v_p(z_i/h_m) = v_p(z_i) - v_p(h_m) \geq (e - d_j) - (e - \delta_m) = \delta_m - d_j > 0.$$

Since  $\bar{\mathbf{D}}_j$  has rank  $y_j$  (as we noted in the proof of (56.32)), and  $\mathbf{Z} = \mathbf{D}\Phi$ , it follows that  $\varphi_m^i \in p$  for all  $F_i \in B_j$ . But  $v_p(u_i/g) \geq 0$  by Exercise 18.5, so  $u_i/g \in R$ , and hence (using (56.35)),

$$a_{jm} = g^{-1} \sum_{F_l \in B_j} u_l \varphi_{m*}^l \in p,$$

completing the proof.

**Remark.** We can now give a more useful version of the congruence criterion (56.24). Namely,  $\zeta$  and  $\zeta'$  belong to the same  $p$ -block if and only if the condition (56.24) holds for all  $p$ -regular  $x$ . The proof, based on (56.37i), is left as an exercise.

In the course of the proof of (56.37), we used the important fact that

$$(56.39) \quad v_p(u_i) \geq v_p(g) = e \quad \text{for each P.I.M. } U_i, \quad 1 \leq i \leq r,$$

by Exercise 18.5. The next result shows that this inequality cannot be improved, for P.I.M.'s belonging to a given block.

**(56.40) Corollary.** *Each p-block  $B_j$  contains a P.I.M.  $U_i$  such that*

$$v_p(u_i) = e.$$

*Proof.* Suppose  $v_p(u_i) > e$  for all P.I.M.'s  $U_i \in B_j$ . Then  $v_p(u_i/g) > 0$  for each  $U_i \in B_j$ , and we obtain  $\bar{b}_j = 0$  by (56.37ii) and (56.35), contrary to the fact that  $\bar{b}_j$  is a block idempotent in  $c(kG)$ .

The main result of this subsection is the following theorem, which asserts that the defect of a block is equal to the defect of certain conjugacy classes. These classes are determined from the coefficients of the corresponding block idempotent in  $kG$ .

**(56.41) Theorem.** *Let  $B_j$  be a block of defect  $d_j$ , with block idempotent  $b_j = \sum a_{jm} C_m$ . Let  $\psi_j$  be the corresponding central character of  $kG$ . Then the following statements hold.*

- (i)  $\psi_j(\bar{b}_j) = \sum_{1 \leq m \leq r, \delta_m = d_j} \bar{a}_{jm} \psi_j(C_m) = 1$ ;
- (ii)  $\bar{b}_j = \sum_{1 \leq m \leq r, \delta_m \leq d_j} \bar{a}_{jm} C_m$ ; and
- (iii)  $\psi_j(\bar{a}_{jm} C_m) \neq 0$  for some p-regular class  $C_m$  of defect  $d_j$ .

*Proof.* This result follows easily from the preceding discussion, as soon as we establish one further point, namely: for each class  $C_m$  of defect  $\delta_m$ ,

$$(56.42) \quad \psi_j(C_m) = 0 \quad \text{whenever } \delta_m < d_j.$$

To prove this, choose  $Z_i \in B_j$  such that  $v_p(z_i) = e - d_j$ . Then  $\bar{\omega}^i = \psi_j$ , and we have

$$\omega^i(C_m) = h_m \zeta_m^i / z_i.$$

Moreover,

$$v_p(h_m/z_i) = v_p(h_m) - v_p(z_i) = (e - \delta_m) - (e - d_j) = d_j - \delta_m > 0,$$

so  $\omega^i(C_m) \in \mathbb{P}$ . Thus  $\psi_j(C_m) = 0$ , as required.

The rest of the proof is left as an exercise for the reader.

**(56.43) Corollary.** *A simple KG-module  $Z_i$  belongs to a p-block of defect d if and only if the following conditions are satisfied:*

- (i)  $\omega_i(C_m) \in \mathfrak{p}$  whenever  $\delta_m < d$ ,  $1 \leq m \leq r$ ; and
- (ii)  $\omega_i(C_l) \notin \mathfrak{p}$  for some  $p$ -regular class  $\mathfrak{C}_l$  of defect  $d$ .

### §56. Exercises

All the exercises are stated with reference to a  $p$ -modular system  $(K, R, k)$  such that  $\text{char } K = 0$  and  $K$  is sufficiently large relative to  $G$ .

1. Prove that  $c(kG)/\text{rad } c(kG)$  is a split semisimple  $k$ -algebra.

[Hint: Use (56.20).]

2. Let  $G$  be a direct product,  $G = G_1 \times G_2$ . Prove that  $c(kG) \cong c(kG_1) \otimes c(kG_2)$ , and that every central character of  $kG$  can be expressed as a product  $\psi = \psi_1 \otimes \psi_2$ , where  $\psi_1$  and  $\psi_2$  are central characters of  $kG_1$  and  $kG_2$ , respectively.

[Hint: Use Exercise 1 and (10.38).]

3. Prove that if  $\beta_1$  is a block idempotent of  $kG_1$  and  $\beta_2$  is a block idempotent of  $kG_2$ , then  $\beta_1 \otimes \beta_2$  is a block idempotent of  $k(G_1 \times G_2) \cong kG_1 \otimes kG_2$ .

[Hint: Use (56.19).]

4. Prove the assertion of Exercise 3 for block idempotents of  $RG$ .

5. Let  $\{\zeta_{11}, \dots, \zeta_{1m_1}\}$  and  $\{\zeta_{21}, \dots, \zeta_{2m_2}\}$  be  $p$ -blocks of  $K$ -characters of  $G_1$  and  $G_2$ , respectively. Prove that  $\{\zeta_{1i} \cdot \zeta_{2j}; 1 \leq i \leq m_1, 1 \leq j \leq m_2\}$  is a  $p$ -block of  $K$ -characters of  $G_1 \times G_2$ .

[Hint: Use (56.25) together with the preceding exercises].

6. Determine the  $p$ -blocks of  $K$ -characters, and their defects, for a finite abelian group  $G$ .

[Hint: Use the examples at the end of §56B, and the preceding exercises.]

7. Let  $\omega: c(KG) \rightarrow K$  be a central character of  $KG$  associated with an irreducible  $K$ -character  $\zeta$  (see (56.21)). Prove that  $\zeta$  belongs to the principal block if and only if  $\omega(C) \equiv |\mathfrak{C}|(\text{mod } p)$  for each class sum  $C = \sum_{x \in \mathfrak{C}} x$ . Use this to determine the  $K$ -characters belonging to the principal  $p$ -block in the symmetric groups  $S_3, S_4, S_5$  for  $p = 2, 3, 5$ , using their character tables (see Volume I, p. 220).

- 
8. Prove that if a  $p$ -block of  $kG$ -modules contains a P.I.M. which is a simple  $kG$ -module, then the block has defect zero.

[Hint: Use (56.32) and (56.39).]

9. Let  $\zeta$  be an irreducible  $K$ -character of  $G$  such that  $\zeta(x) = 0$  for all  $p$ -irregular  $x \in G$ . Prove that  $\zeta$  belongs to a  $p$ -block of defect zero.

10. Fill in the details of the following alternative proof of (56.31). Let  $Z$  be a simple  $KG$ -module in  $B_j$ , and let  $e$  be the primitive central idempotent in  $KG$  associated with

$Z$ . Then  $e \in RG$ , since  $B_j$  has defect zero. We may write

$$KG = \bigoplus M_{n_i}(K), \Gamma = \bigoplus \Gamma_i, \Gamma_i \cong M_{n_i}(R),$$

with  $\Gamma$  a maximal  $R$ -order in  $KG$ . By (27.8),  $\bigoplus (n_i/n_i)\Gamma_i$  is the largest  $\Gamma$ -ideal in  $RG$ . If  $Z$  is a simple  $M_{n_i}(K)$ -module, then  $n_i = \zeta(1)$ , and we deduce that  $\Gamma_i \subseteq RG$ . Therefore  $\Gamma_i = RG \cdot e$ , so the  $R$ -block ideal  $B_j \cong M_{n_i}(R)$ . It follows that

$$Z \cong K^{(n_i)}, \quad P \cong R^{(n_i)}, \quad \bar{P} \cong k^{(n_i)} \cong F_i \cong U_i,$$

where  $P$  is the unique P.I.M. belonging to  $B_j$ . The remaining assertions of (56.31) are now clear, with the last statement following as in Step 1 of the proof of (32.16).

## §57. THE DEFECT GROUP OF A $p$ -BLOCK

### §57A. $G$ -Algebras, the Trace Map, and Defect Groups

Throughout this section,  $G$  denotes a finite group,  $p$  a fixed prime number, and  $R$  a commutative ring satisfying either of the following hypotheses:

- (a)  $R$  is a field of characteristic  $p$ ; or
- (b)  $R$  is a d.v.r. with quotient field  $K$  and maximal ideal  $\mathfrak{p}$  containing  $p$ , such that  $R$  is complete in the  $\mathfrak{p}$ -adic topology.

We recall the notations, defined for subsets  $X, Y$  of  $G$ :

$$\begin{aligned} {}^aX &= aXa^{-1} = X^{a^{-1}} \quad \text{for } X \subseteq G, \quad a \in G \\ X &= {}_H Y \quad \text{if } X = {}^aY \quad \text{for } a \in H \leq G; \end{aligned}$$

and

$$X \leq_H Y \quad \text{if } X \subseteq {}^aY \quad \text{for } a \in H \leq G.$$

We shall call a family of representatives of the left cosets  $G/H = \{xH : x \in G\}$  a *cross section* of  $G/H$ , and a set of representatives of the double cosets  $\{HxL : x \in G\}$  a *cross section* of  $H \backslash G / L$ , for  $H, L \leq G$ .

**(57.1) Definition.** A  $G$ -algebra  $A$  is an  $R$ -algebra with a finite  $R$ -basis, upon which  $G$  acts as a group of  $R$ -algebra automorphisms. Thus for each  $x \in G, a \in A$ , there is defined an element  $xa \in A$  (or  $x \cdot a \in A$ ) such that the map  $a \in A \rightarrow xa \in A$  is an automorphism of  $A$  as  $R$ -module, and we have

$$x(ya) = (xy)a \quad \text{and} \quad x(ab) = (xa)(xb)$$

for all  $x, y \in G$  and  $a, b \in A$ . For an arbitrary subgroup  $H \leq G$ ,  $A_H$  denotes the  $R$ -subalgebra of  $A$  consisting of fixed elements under the  $H$ -action; thus

$$A_H = \{a \in A : ha = a \text{ for all } h \in H\}.$$

Note that

$$D \leq H \Rightarrow A_H \subseteq A_D$$

for all subgroups  $D$  and  $H$  of  $G$ .

**(57.2) Definition.** Let  $A$  be a  $G$ -algebra, and let  $H, D$  be subgroups of  $G$  such that  $D \leq H$ . The *trace map* (defined by the pair of subgroups  $D$  and  $H$ ) is the  $R$ -endomorphism of  $A$

$$T_{H/D}: A \rightarrow A$$

defined by

$$T_{H/D}(a) = \sum_{h \in H/D} ha, \quad a \in A,$$

where the notation  $h \in H/D$  means that the sum is taken over a cross section of the left cosets  $H/D$ . We shall use the notation  $A_{H/D}$  for the image of  $A_D$  under the trace map  $T_{H/D}$ ; thus

$$A_{H/D} = T_{H/D}(A_D).$$

The following properties of the trace map follow immediately from the definitions, and are left as exercises for the reader.

**(57.3) Proposition.** For  $D \leq H \leq L \leq G$ , the following statements hold:

- (i)  $T_{H/D} A_D \subseteq A_H$ , and for  $a \in A_D$ ,  $T_{H/D} a$  is independent of the choice of the cross section of  $H/D$ ;
- (ii)  $T_{L/H} \circ T_{H/D} = T_{L/D}$  (transitivity);
- (iii) For all  $a \in A_D$  and  $b \in A_H$  we have

$$T_{H/D}(ba) = b(T_{H/D}a), \quad \text{and} \quad T_{H/D}(ab) = (T_{H/D}(a))b.$$

- (iv)  $A_{H/D} = T_{H/D}(A_D)$  is a two-sided ideal in  $A_H$ ;
- (v) For all  $x \in G$  and  $a \in A_D$ ,

$$x \cdot A_H = A_{x_H}, \quad \text{and} \quad x \cdot T_{H/D}(a) = T_{x_H/x_D}(xa).$$

**(57.4) Remarks.** The preceding ideas will be applied to assign subgroups of  $G$  to primitive idempotents in  $G$ -algebras. The following examples of  $G$ -algebras are particularly important.

- (i)  $E = \text{End}_R M$ , for a left  $RG$ -lattice  $M$ , with the  $G$ -action given by

$$x \cdot f = xf x^{-1}, \quad \text{for } x \in G, f \in E;$$

and

$$(ii) \quad A = RG, \text{ with } x \cdot a = xax^{-1}, \text{ for } x \in G, a \in A.$$

In the first example, we have  $E_G = \text{End}_{RG} M$ , and the trace map  $T_{G/H}$  carries  $\text{End}_{RH}(M_H)$  to  $\text{End}_{RG} M$ . If  $M$  is an indecomposable  $RG$ -lattice, then 1 is the unique idempotent in  $E_G$ ; in §19, the trace map was used to assign a conjugacy class of  $p$ -subgroups of  $G$  to  $M$  (the vertices of  $M$ ). In the second example, we have  $A_G = c(RG)$ , and the primitive idempotents in  $A_G$  are the block idempotents of  $RG$  discussed in the preceding section. In this situation, following Green [63], we shall assign a conjugacy class of  $p$ -subgroups to a given block idempotent in  $A_G$ , called the *defect groups* of the block. We recover, in this way, previous definitions of defect groups of block idempotents, due to Brauer [56] and Osima [55] (see CR §87). The point of the present approach is that it gives useful connections between the theory of vertices and sources, from §19, and defect groups of  $p$ -blocks.

Returning to the general situation, we begin with the analogues of the Mackey theorems (see §10B) for trace maps.

**(57.5) Proposition.** *Let  $A$  be a  $G$ -algebra,  $L$  a subgroup of  $G$ , and  $D, H$  subgroups of  $L$ . Then*

$$(i) \quad T_{L/H} a = \sum T_{D/D \cap {}^x H}(xa), \text{ for all } a \in A_H, \text{ where the sum is taken over a cross section } \{x\} \text{ of the } (D, H)\text{-double cosets in } L. \text{ Moreover, we have}$$

$$(ii) \quad T_{L/H}(a)T_{L/D}(b) = \sum T_{L/D \cap {}^x H}((x \cdot a)b), \text{ for all } a \in A_H, b \in A_D, \text{ where the sum is taken over the same cross section of } D \setminus L/H \text{ as in part (i).}$$

*Proof.* (i) Let  $L = \dot{\cup} DxH$ , and consider a fixed double coset  $DxH$ . By the proof of Mackey's Subgroup Theorem 10.13, we have

$$D = \dot{\bigcup}_j s_j(D \cap {}^x H) \quad \text{and} \quad DxH = \bigcup_j s_j xH,$$

for a cross section  $\{s_j\}$  of  $D/(D \cap {}^x H)$ . By (57.3v), we have  $xa \in A_{{}^x H} \subseteq A_{D \cap {}^x H}$  for all  $a \in A_H$ , and hence

$$(57.6) \quad T_{D/D \cap {}^x H}(x \cdot a) = \sum_j s_j(xa) = \sum_j (s_j x)a.$$

By the preceding remarks, the elements  $\{s_j x\}$ , taken over representatives of the different  $(D, H)$ -double cosets in  $L$ , form a cross section of left cosets  $L/H$ . Upon adding the expressions (57.6) over the given cross section of  $D \setminus L/H$ , we obtain (i).

$$(ii) \quad \text{Let } a \in A_H, b \in A_D. \text{ Then}$$

$$\begin{aligned}
T_{L/H}(a)T_{L/D}(b) &= T_{L/D}(T_{L/H}(a)b) \quad (\text{by (57.3iii)}) \\
&= T_{L/D}\left(\sum_{DxH} (T_{D/D \cap xH}(xa))b\right) \quad (\text{by part (i)}) \\
&= T_{L/D}\left(\sum_{DxH} T_{D/D \cap xH}((x \cdot a)b)\right) \quad (\text{by (57.3iii)}) \\
&= \sum_{DxH} T_{L/D \cap xH}((x \cdot a)b) \quad (\text{by (57.3ii)}),
\end{aligned}$$

completing the proof.

**(57.7) Corollary.** *Let  $L, D$ , and  $H$  be as in (57.5). Then*

$$A_{L/H}A_{L/D} \subseteq \sum_x A_{L,D \cap xH},$$

where the sum is taken over a cross section of the  $(D, H)$  double cosets in  $L$ .

**(57.8) Rosenberg's Lemma.** *Let  $A$  be an  $R$ -algebra with a finite basis, over a commutative ring  $R$  satisfying either of the conditions (a) or (b) stated at the beginning of §57A. Let  $e$  be a primitive idempotent in  $A$ , and suppose that*

$$e \in I + I',$$

for two-sided ideals  $I$  and  $I'$  in  $A$ . Then either  $e \in I$  or  $e \in I'$ .

*Proof.* Since  $e$  is a primitive idempotent,  $eAe$  is an indecomposable left ideal, and we have  $(\text{End}_A Ae)^\circ \cong eAe$  by (3.19). Then  $eAe$  is a local ring with identity element  $e$ , by (6.10), which applies because of the hypotheses on  $R$ . Moreover,

$$e \in eIe + eI'e,$$

and  $eIe$  and  $eI'e$  are two-sided ideals of  $eAe$ . If both  $eIe$  and  $eI'e$  are properly contained in  $eAe$ , then both are contained in  $\text{rad } eAe$ , and hence  $e \in \text{rad } eAe$ , which is impossible. Thus we may assume  $eIe = eAe$ ; and obtain  $e \in eAe = eIe \subseteq I$ , as required. (See Rosenberg [61].)

The first main result of this subsection is the following theorem.

**(57.9) Theorem. (Green [63]).** *Let  $A$  be a  $G$ -algebra,  $H$  a subgroup of  $G$ , and let  $e$  be a primitive idempotent in  $A_H$ . There exists a  $p$ -subgroup  $D \leq H$  such that*

- (i)  $e \in A_{H/D}$ , and having the further property that
- (ii)  $D \leq_H D'$  for any other subgroup  $D' \leq H$  such that  $e \in A_{H/D'}$ .

*Proof.* Since  $A_H = A_{H/H}$  and  $e \in A_H$ , the family of subgroups  $\{D\}$  such that  $D \leq H$  and  $e \in A_{H/D}$  is nonempty, and contains a minimal subgroup  $D_0$ . Let  $D'$  be another subgroup of  $H$  such that  $e \in A_{H/D'}$ . Then  $e = e^2 \in A_{H/D'} \cdot A_{H/D_0}$ , and we obtain

$$e \in \sum_{D_0 \times D' \leq H} A_{H/(D_0 \cap {}^{x_D} D')}$$

by (57.7). For each  $x \in H$ ,  $A_{H/(D_0 \cap {}^{x_D} D')}$  is a two-sided ideal in  $A_H$ , by (57.3iv), and  $e$  is contained in their sum. By Rosenberg's Lemma 57.8, we have  $e \in A_{H/(D_0 \cap {}^{x_D} D')}$  for some  $x \in H$ . By the minimality of  $D_0$ , it follows that  $D_0 \leq_H D'$ .

Now let  $S$  be a Sylow  $p$ -subgroup of  $H$ ; then the index  $m = |H:S|$  is prime to  $p$ , and hence is a unit in  $R$ . Moreover,  $A_H \subseteq A_S$ , and, for all  $a \in A_H$ , we have

$$T_{H/S}a = ma, \quad \text{and} \quad T_{H/S}(m^{-1}a) = a,$$

since  $m$  is a unit in  $R$ . In particular,

$$e \in T_{H/S}(A_S) = A_{H/S},$$

so  $D_0 \leq_H S$ , by the first part of the proof. Thus  $D_0$  is a  $p$ -subgroup of  $H$ , and the proof is completed.

Note that

$$e \in A_{H/D} \Rightarrow e \in A_{H/x_D} \quad \text{for all } x \in H,$$

by (57.3v), since  $xe = e$ .

**(57.10) Definition.** Let  $H \leq G$ , and let  $e$  be a primitive idempotent in  $A_H$ . By Theorem 57.9, there exists a  $p$ -subgroup  $D \leq H$ , which is the unique minimal subgroup up to  $H$ -conjugacy, such that

$$e \in A_{H/D} = T_{H/D}(A_D).$$

The group  $D$  and its  $H$ -conjugates are called *defect groups of the primitive idempotent  $e$* .

For the rest of the subsection, let  $A$  be the  $G$ -algebra  $RG$ , with  $G$ -action given by conjugation (see (57.4)). We shall examine the connection between the coefficients of a primitive idempotent  $e \in A_G$  as a linear combination of class sums, and the defect groups of  $e$ . Among other things, this will show that the different definitions of defect groups (by Brauer and Osima (see CR §87), and Green (57.10)) coincide.

**(57.11) Definition.** Let  $H \leq G$ . An  $H$ -conjugacy class  $\Omega \subseteq G$  is an orbit of the

$H$ -action on  $G$  by conjugation:

$$h \cdot x = hxh^{-1}, \quad h \in H, \quad x \in G.$$

The  $H$ -class sums in  $RG$  are the elements

$$L = \sum_{x \in \Omega} x,$$

where  $\{\Omega\}$  are the  $H$ -conjugacy classes in  $G$ . A *class defect group* of an  $H$ -conjugacy class  $\Omega$  is a Sylow  $p$ -subgroup  $D$  of the centralizer  $C_H(x)$ , for some  $x \in \Omega$ .

**Remarks.** (i) The class defect groups of an  $H$ -conjugacy class  $\Omega$  form a single conjugacy class of  $p$ -subgroups of  $H$ , by the Sylow theorem. Moreover, if  $D$  is a class defect group of an  $H$ -conjugacy class  $\Omega$ , then we have

$$(57.12) \quad D' \leq_H D \Leftrightarrow D' \text{ is a } p\text{-subgroup of } C_H(x) \text{ for some } x \in \Omega$$

(ii) In case  $H = G$ , the  $H$ -conjugacy classes are the usual conjugacy classes in  $G$ . If  $D$  is a class defect group of a conjugacy class  $\mathfrak{C}$  in  $G$ , then clearly

$$(57.13) \quad |D| = p^\delta, \quad \text{where } \delta \text{ is the defect of } \mathfrak{C}, \text{ defined in (56.36).}$$

**(57.14) Proposition.** Let  $A$  be the  $G$ -algebra  $RG$ . For each subgroup  $H \leq G$ ,  $A_H$  has an  $R$ -basis consisting of the  $H$ -class sums  $\{L\}$ , defined in (57.11). If  $D \leq H \leq G$ , then<sup>†</sup>

$$A_{H/D} \equiv \sum_{D_i \leq_H D} RL_i \pmod{pA_H}$$

where the sum is taken over all  $H$ -class sums  $\{L_i\}$  whose class defect groups  $\{D_i\}$  satisfy the condition that  $D_i \leq_H D$ .

*Proof.* The first statement is similar to (3.37a), and its proof is left to the reader. For the second statement, we note that  $A_D$  has a basis consisting of  $D$ -class sums  $\{X\}$ , and  $A_{H/D} = T_{H/D}(A_D)$ . A  $D$ -class sum can be expressed in the form

$$X = \sum_{d \in D/C_D(x)} d \cdot x,$$

where  $x$  is a representative of the corresponding  $D$ -class. Then

$$\begin{aligned} (57.15) \quad T_{H/D} X &= \sum_{h \in H/D} h \cdot X = \sum_{h \in H/C_D(x)} h \cdot x \\ &= |C_H(x); C_D(x)| \sum_{h \in H/C_H(x)} h \cdot x = |C_H(x); C_D(x)| L \end{aligned}$$

<sup>†</sup>We follow the convention that  $p = 0$  in case  $R$  is a field of characteristic  $p$ .

where  $L$  is the  $H$ -class sum associated with the  $H$ -class  $\mathfrak{L}$  containing  $x$ . For a given element  $x$ , put  $m = |C_H(x):C_D(x)|$ . Then  $T_{H/D}X \in \mathfrak{p}A_H$  if  $p|m$ , by (57.15). If  $p \nmid m$ , then  $m$  is a unit in  $R$ , and we have

$$L = T_{H/D}(m^{-1}X) \in A_{H/D}$$

by (57.15). Recalling that  $m = |C_H(x):C_D(x)|$ , we have

$$\begin{aligned} p \nmid m &\Leftrightarrow C_D(x) \text{ contains a Sylow } p\text{-subgroup of } C_H(x) \\ &\Leftrightarrow D \text{ contains a class defect group of the } H\text{-class } \mathfrak{L} \ni x. \end{aligned}$$

The elements  $\{T_{H/D}(X)\}$  in (57.15) span the  $R$ -module  $A_{H/D}$ , so the second statement of the proposition follows from the preceding discussion.

Now let  $(K, R, k)$  be a  $p$ -modular system which is admissible for  $G$  (see (56.3)). The results proved earlier in §57A apply to both  $G$ -algebras

$$A = RG \quad \text{and} \quad \bar{A} = \bar{R}G = kG.$$

This is clear in case  $R$  is complete. If  $R$  is not complete, the other hypotheses of (56.3) imply that  $eAe$  is a local ring for any primitive idempotent  $e$ , so that Rosenberg's Lemma 57.8 holds in this case, along with the rest of the theory of defect groups. As an immediate consequence of (57.14), we then have:

**(57.16) Corollary.** *Keep the notation of the preceding paragraph, and let  $D \leq G$ . Then for  $a \in A$ ,*

$$a \in A_{G/D} \Leftrightarrow \bar{a} \in \bar{A}_{G/D}.$$

We now obtain:

**(57.17) Theorem.** *Let  $(K, R, k)$  be a  $p$ -modular system which is admissible for  $G$ . Let  $A = RG$ ,  $\bar{A} = kG$ ,  $A_G = c(RG)$ ,  $\bar{A}_G = c(kG)$ . Let  $D$  be a fixed  $p$ -subgroup of  $G$ . Then the following statements hold:*

- (i)  $D$  is a defect group of a block idempotent  $b \in A_G$  if and only if  $D$  is a defect group of the block idempotent  $\bar{b} \in \bar{A}_G$ .
- (ii)  $D$  is a defect group of  $b$  if and only if

$$b \equiv \sum_{D_i = G^D} a_i C_i + \sum_{D_j < G^D} a_j C_j \pmod{\mathfrak{p}}$$

where (in the first sum) at least one coefficient  $a_i \not\equiv 0 \pmod{\mathfrak{p}}$ . Here each  $C_i$  is a class sum, and  $D_i$  is a class defect group of the class associated with  $C_i$ .

(iii)  $D$  is a defect group of  $\bar{b}$  if and only if

$$\bar{b} = \sum_{D_i =_G D} \alpha_i C_i + \sum_{D_j <_G D} \alpha_j C_j$$

with at least one coefficient (in the first sum)  $\alpha_i \neq 0$  in  $k$ , and the rest of the notation is as in part (ii).

(iv) If  $D$  is a defect group of  $b$ , then  $D$  is a class defect group of some conjugacy class in  $G$ .

*Proof.* (i) By (56.5), the map  $b \rightarrow \bar{b}$  is a bijection of block idempotents in  $A$  and  $\bar{A}$ , respectively. The result then follows from Corollary 57.16 and Definition 57.10.

(ii) Let  $D$  be a defect group of  $b$ . Then  $b$  has the required expression as a linear combination of class sums, by (57.14) and (57.10), except that possibly all the coefficients in the first sum are in  $p$ . But if this occurs, then by (57.14),

$$b \in \sum_{D_j <_G D} A_{G/D_j},$$

and the  $\{A_{G/D_j}\}$  are two-sided ideals in  $A_G$  by (57.3iv). Then  $b \in A_{G/D_j}$  for some  $D_j <_G D$  by Rosenberg's Lemma, contradicting the assumption that  $D$  is a defect group of  $b$ . Conversely, if  $b$  has an expression as in (ii), it follows immediately from (57.14) and (57.10) that  $D$  is a defect group of  $b$ .

Part (iii) follows from part (i), together with (57.14) and the argument used in part (ii).

Finally, (iv) follows from either part (ii) or (iii).

**(57.18) Definition.** Let  $(K, R, k)$  be admissible for  $G$ , and let  $B$  be a  $p$ -block of  $G$  defined by a block idempotent  $b \in RG$ . A defect group of the block  $B$  is any defect group of the block idempotent  $b \in A_G$ , where  $A = c(RG)$ . (Compare with the definition in CR, p. 623.)

By (57.9), the defect groups of a  $p$ -block of  $G$  form a single conjugacy class of  $p$ -subgroups of  $G$ . By (57.17), they coincide with the defect groups of the block idempotents  $\bar{b} \in \bar{A}_G = c(kG)$ . They are related to the defect of the block as follows.

**(57.19) Corollary.** Let  $(K, R, k)$  be a  $p$ -modular system such that  $\text{char } K = 0$ , and  $K$  is sufficiently large relative to  $G$ . Let  $B$  be a  $p$ -block of  $G$  of defect  $d$  (see (56.30)), and let  $D$  be a defect group of  $B$ , as in (57.18). Then  $|D| = p^d$ .

The result follows at once from Theorems 57.17 and 56.41.

**(57.20) Corollary.** *Keep the hypothesis of Corollary 57.19. Then the defect groups of the principal  $p$ -block  $B_1$  are the Sylow  $p$ -subgroups of  $G$ .*

The proof is left as an exercise.

### §57B. Defect Groups as Vertices

Defect groups of blocks can be interpreted as vertices of the indecomposable block ideals in  $RG$ , under the two-sided action of  $G \times G$  on  $RG$  (see §19). We shall obtain this result, and other related facts, in this subsection, after a review of the theory of vertices of indecomposable  $RG$ -lattices from the point of view of  $G$ -algebras. This approach, incidentally, is independent of most of §19, and requires only Gaschütz's criterion (19.2) for relative projectivity.

We shall continue to use the definitions and notation introduced in §57A. We recall (see §19B) that an  $RG$ -lattice is a f.g. left  $RG$ -module, which is  $R$ -projective; we use the notation:

$$\text{Ind } RH = \text{set of all indecomposable } RH\text{-lattices.}$$

Let  $M$  be an  $RG$ -lattice, and let  $E = \text{End}_R M$ , viewed as a  $G$ -algebra as in (57.4). The  $G$ -action on  $E$  is given by

$$x \cdot f = xfx^{-1} \quad \text{for } x \in G, \quad f \in E.$$

Then

$$(x \cdot f)m = xf(x^{-1}m) \quad \text{for all } m \in M, \quad x \in G, \quad f \in E.$$

As in §57A, we set

$$E_H = \{f \in E : af = f \text{ for all } a \in H\}.$$

Then  $E_H$  is an  $R$ -subalgebra of  $E$ , for each subgroup  $H \leq G$ , and, in particular, we have

$$E_G = \text{End}_{RG} M.$$

We also require the trace map

$$T_{H/D} : E_D \rightarrow E_H, \quad \text{for } D \leq H \leq G,$$

defined in (57.2), and use the notation

$$E_{H/D} = T_{H/D} E_D$$

for the image of the trace map.

From §19, we recall that a *vertex* of an indecomposable  $RG$ -lattice  $M$  is a subgroup  $D \leq G$  such that  $M$  is  $(G, D)$ -projective, and  $D \leq_G D'$  for any

other subgroup  $D'$  such that  $M$  is  $(G, D')$ -projective. We also recall (see (19.2)) that  $M$  is  $(G, D)$ -projective if and only if

$$T_{G/D}f = \text{id}_M \quad \text{for some } f \in E_D.$$

**(57.21) Proposition.** *Let  $M \in \text{Ind } RG$ , and let  $E = \text{End}_R M$  be the  $G$ -algebra defined above. Then  $\text{id}_M$  is a primitive idempotent in  $E_G$ . Moreover, a subgroup  $D \leq G$  is a defect group of  $\text{id}_M$ , in the sense of (57.11), if and only if  $D$  is a vertex of  $M$ .*

*Proof.* It is immediate, by (6.4), that  $\text{id}_M$  is primitive in  $E_G = \text{End}_{RG} M$ . We next observe that  $\text{id}_M \in E_{G/D}$  for a subgroup  $D \leq G$  if and only if  $M$  is  $(G, D)$ -projective, by the remarks preceding the statement of the proposition. Thus, in this case, the definitions of vertex and defect group coincide, and the proof is completed.

We next apply these ideas to block ideals in  $RG$ , and begin by noting that  $RG$  is an  $R(G \times G)$ -lattice, where the action of  $G \times G$  on  $RG$  is given by

$$(x, y) \cdot a = xay^{-1}, \quad a \in RG, \quad x, y \in G.$$

Let  $G_0$  be the diagonal subgroup of  $G \times G$ , and  $\Delta: G \rightarrow G_0$  the isomorphism given by

$$\Delta(x) = (x, x), \quad x \in G.$$

**(57.22) Proposition.** *Let  $b$  be a block idempotent in the  $G$ -algebra  $A = RG$ . A subgroup  $D \leq G$  is a defect group of  $b \in A_G$ , in the sense of (57.10), if and only if  $\Delta D$  is a vertex of the indecomposable  $R(G \times G)$ -lattice  $Ab = RGb$ .*

*Proof.* It is easily checked that there is an isomorphism of  $R(G \times G)$ -lattices

$$RG \cong \text{ind}_{G_0}^{G \times G} 1_{G_0},$$

where  $1_{G_0}$  denotes the trivial  $RG_0$ -module (see (19.17)). A block ideal  $RGb$  is an indecomposable direct summand of the  $R(G \times G)$ -lattice  $RG$ , and hence is  $(G \times G, G_0)$ -projective by (19.2v), using the isomorphism above.

It follows that a vertex of  $RGb$  is a subgroup of  $G_0$ , and hence has the form  $\Delta D$ , for some subgroup  $D \leq G$ . We shall prove that  $D$  is a defect group of the primitive idempotent  $b \in A_G$ , where  $A = RG$ .

Let  $E = \text{End}_R RGb$ , viewed as a  $(G \times G)$ -algebra with the action of  $(x, y) \in G \times G$  on  $f \in E$  given by

$$(x, y)f(a) = xf(x^{-1}ay)y^{-1} \quad \text{for } a \in A.$$

Let  $a_l$  denote left multiplication by  $a \in A$  on  $RGb$ ; then  $a_l \in E$  for all  $a \in A$ , and  $b_l$  acts as the identity on  $RGb$ . Let  $H, L \leq G$ ; then we have

$$(57.23) \quad b_l \in E_{G \times G/H \times L} \Leftrightarrow \Delta D \leq_{G \times G} H \times L,$$

since  $\Delta D$  is a vertex of  $RGb$ . Using the formula for  $(x, y) \cdot f$ ,  $f \in E$ , we obtain

$$(57.24) \quad (x, y) \cdot a_l = (x \cdot a)_l \quad \text{for all } a \in A, \quad x, y \in G,$$

where  $x \cdot a = xax^{-1}$ . We also note that for  $a \in A$ ,  $a_l$  commutes with the right multiplications on  $RGb$  by elements of  $G$ ; conversely, any element of  $E$  which commutes with all the right multiplications by elements of  $G$  has the form  $a_l$  for some  $a \in Ab$ .

We can now prove easily that

$$(57.25) \quad (A_H)_l = E_{H \times G} \quad \text{and} \quad (A_{G/D'})_l = E_{G \times G/D' \times G}$$

for all subgroups  $D', H \leq G$ . For the first statement, let  $(x, y) \in H \times G$ . Then  $(x, y)a_l = (x \cdot a)_l = a_l$  for  $a \in A_H$ , by (57.24). Thus  $(A_H)_l \subseteq E_{H \times G}$ . Conversely, let  $f \in E_{H \times G}$ . Then  $f = a_l$  for some  $a \in Ab$  by a previous remark, and it follows that  $a \in A_H$  by (57.24), since  $Ab$  acts faithfully on  $Ab$  by left multiplication. The second statement in (57.25) follows easily from the first. Indeed,  $(A_{D'})_l = E_{D' \times G}$  by the first part, so

$$E_{G \times G/D' \times G} = T_{G \times G/D' \times G}(A_{D'})_l.$$

If  $a \in A_{D'}$ , then we have

$$\begin{aligned} T_{G \times G/D' \times G}(a_l) &= \sum_{g \in G/D'} (g, 1) \cdot a_l \\ &= \sum_{g \in G/D'} (g \cdot a)_l \quad (\text{by (57.24)}) \\ &= (T_{G/D'} a)_l \end{aligned}$$

by the definition of the trace maps. Thus we have proved (57.25).

Now let  $D' \leq G$ . Then

$$\begin{aligned} b \in A_{G/D'} &\Leftrightarrow b_l \in (A_{G/D'})_l \Leftrightarrow b_l \in E_{G \times G, D' \times G} \quad (\text{by (57.25)}) \\ &\Leftrightarrow \Delta D \leq_{G \times G} D' \times G \quad (\text{by (57.23)}) \\ &\Leftrightarrow D \leq_G D'. \end{aligned}$$

Therefore  $D$  is a defect group of  $b$  in  $A_G$  in the sense of Definition 57.10, completing the proof.

We conclude this subsection with a connection between defect groups and vertices of indecomposable modules in a block.

**(57.26) Proposition.** *Let  $A$  be the  $G$ -algebra  $RG$ , let  $D \leq H \leq G$ , and let  $e$  be an idempotent in  $A_{H/D}$ . Let  $M$  be a f.g. left  $RG$ -module such that  $eM \neq 0$ . Then  $eM$  is an  $(H, D)$ -projective  $RH$ -module.*

*Proof.* Since  $e \in A_H$ ,  $x \cdot e = xex^{-1} = e$  for all  $x \in H$ , and hence  $eM$  is an  $RH$ -submodule of  $M_H$ . The further restriction that  $e \in A_{H/D}$  means that

$$T_{H/D}a = \sum_{x \in H/D} x \cdot a = e \quad \text{for some } a \in A_D.$$

The operation  $a \rightarrow x \cdot a$ ,  $x \in H$ , is an  $R$ -algebra automorphism. Consequently,

$$e = eee = \sum_{x \in H/D} e(x \cdot a)e = \sum_{x \in H/D} x \cdot (eae).$$

Thus

$$T_{H/D}(eae) = e.$$

The left multiplication  $(eae)_l$  lies in  $\text{End}_{RD}eM$ , and we have

$$\sum_{x \in H/D} x(eae)_l x^{-1} = e_l = \text{id} \quad (\text{on } eM).$$

Thus  $eM$  is  $(H, D)$ -projective by (19.2), and the proof is complete.

**(57.27) Corollary.** *Let  $M$  be an indecomposable  $RG$ -lattice such that  $bM = M$  for a block idempotent  $b \in RG$ , and let  $D$  be a defect group of  $b$ . Then  $M$  is  $(G, D)$ -projective, so  $D' \leq_G D$  for any vertex  $D'$  of  $M$ .*

*Proof.* Since  $D$  is a defect group of  $b$ , we have  $b \in A_{G/D}$ , where  $A$  is the  $G$ -algebra  $RG$ . Then  $M$  is  $(G, D)$ -projective by (57.26), and the result follows.

Later (see (59.10)) we shall prove Hamernik's Theorem that every  $p$ -block of  $G$  with defect group  $D$  contains an indecomposable  $RG$ -lattice with vertex  $D$ . This result, together with (57.27), characterizes defect groups in terms of vertices of modules.

### §57C. Defect Groups as Sylow Intersections

This subsection is devoted to a proof of Green's Theorem (Green [62a, 63]) that a defect group of a  $p$ -block can be expressed as the intersection of two Sylow  $p$ -subgroups of  $G$ . The proof uses the preceding discussion, and some additional properties of vertices proved in §19.

Besides the notation introduced earlier in the section, we write  $M|N$  to indicate that an  $RH$ -module  $M$  is isomorphic to a direct summand of  $N$ , and

$$\text{vtx } M, \quad \text{for } M \in \text{Ind } RH$$

to denote the set of vertices of the indecomposable  $RH$ -lattice  $M$ . Then  $\text{vtx } M$  is an  $H$ -conjugacy class of  $p$ -subgroups of  $H$ .

**(57.28) Proposition.** Let  $M \in \text{Ind } RG$ , let  $D \in \text{vtx } M$ , and let  $D \leq H \leq G$ . Then there exists  $U \in \text{Ind } RH$  such that

$$U|M_H \quad \text{and} \quad D \in \text{vtx } U.$$

This result is an immediate consequence of Theorem 19.15, since  $D \leq H$  implies that  $M$  is  $(G, H)$ -projective, by (19.5vii).

**(57.29) Proposition.** Let  $M = R$ , on which  $G$  acts trivially. Then any Sylow  $p$ -subgroup of  $G$  is a vertex of  $M$ .

*Proof.* Let  $D$  be a vertex of  $M$ , and  $S$  a Sylow  $p$ -subgroup of  $G$ . Then  $D \leq_G S$  by (19.13i) (or by (57.21) and (57.10)). Now let  $E = \text{End}_R M$ , viewed as a  $G$ -algebra as in §57B. Then  $\text{id}_M \in T_{G/D} E_D$ , and  $E_D = R \cdot \text{id}_M$  since  $M = R$ . It follows that

$$\text{id}_M \in |G:D|R \cdot \text{id}_M.$$

If  $D <_G S$  then  $|G:D| \in p$  so  $\text{id}_M \in p \text{id}_M$ , which is impossible. Therefore  $D =_G S$ , as required.

The first statement of the next result is a consequence of the Green Indecomposability Theorem (see (19.25)). We shall give a new elementary proof, due to M. Cabanes.

**(57.30) Proposition.** Let  $G$  be a  $p$ -group, and let  $M$  be a transitive permutation module over  $RG$ , that is,  $M$  has an  $R$ -basis  $X$  which is a transitive  $G$ -set. Let  $H = \text{Stab}_G x_0$ , for some  $x_0 \in X$ . Then  $M \in \text{Ind } RG$ , and  $H \in \text{vtx } M$ .

*Proof.* We have  $M \cong (1_H)^G$ , as  $RG$ -module. In case  $R$  is a d.v.r. with residue field  $k$ , it suffices to prove that  $k \otimes_R M$  is an indecomposable  $kG$ -module, and we have  $k \otimes_R M \cong (1_H)^G$  as  $kG$ -modules. Thus, in case  $R$  is either a field of characteristic  $p$  or a d.v.r. with residue field  $k$  of characteristic  $p$ , it is sufficient to prove that  $(1_H)^G$  is indecomposable, in case  $1_H$  is the trivial  $kH$ -module for a field  $k$  of characteristic  $p$ . Since  $\text{inv}_G M \neq 0$  for any  $kG$ -module  $M$ , for a finite  $p$ -group  $G$  (see (5.24)), the indecomposability of  $(1_H)^G$  will follow if we can prove that

$$\dim_k \text{inv}_G (1_H)^G = 1.$$

But this follows at once from Frobenius reciprocity (10.21), since

$$\text{inv}_G (1_H)^G \cong \text{Hom}_{kG}(1_G, (1_H)^G) \cong \text{Hom}_{kH}(1_{kH}, 1_{kH}) \cong k.$$

Thus  $M \in \text{Ind } RG$ , and the first statement is proved.

For the second statement, we begin with the fact that  $M$  is  $(G, H)$ -projective by (19.2v), since  $M \cong (1_H)^G$ . Then  $D \leq_G H$  for any  $D \in \text{vtx } M$ . Conversely,  $1_H|M_H$

by (19.3a). By (57.29),  $H \in \text{vtx } 1_H$ , and so  $H \leq_G D$  by (19.14i). This completes the proof.

The main result can now be stated as follows:

**(57.31) Theorem.** *Let  $D$  be a defect group of a block idempotent  $b \in RG$ . Let  $S$  be a Sylow  $p$ -subgroup of  $G$  containing  $D$ . Then there exists an element  $z \in C_G(D)$  such that*

$$D = S \cap {}^zS.$$

*Proof.* The idea of the proof is straightforward. Since  $D \leq S$ , we have  $\Delta D \leq S \times S$  in  $G \times G$ . We then decompose  $(RG)_{S \times S}$  as a direct sum of indecomposable  $R(S \times S)$ -lattices, and determine their vertices. Since  $(RGb)_{S \times S} | (RG)_{S \times S}$ , the K-S-A Theorem implies that  $(RGb)_{S \times S}$  is isomorphic to a direct sum of a subset of the indecomposable summands of  $(RG)_{S \times S}$ . Since  $\Delta D$  is a vertex of the indecomposable  $R(G \times G)$ -lattice  $RGb$  by (57.22), it follows that  $\Delta D$  is a vertex of one of the  $(S \times S)$ -summands of  $RG$ , which will turn out to have the required form. Now we shall fill in the details.

Let

$$G = \bigcup_{i=1}^m Sx_iS,$$

where  $\{Sx_iS\}$  are the  $(S, S)$ -double cosets in  $G$ . Then clearly

$$RG = \bigoplus_{i=1}^m R(Sx_iS),$$

where  $R(Sx_iS)$  is the  $R$ -submodule of  $RG$  with an  $R$ -basis consisting of the elements of  $Sx_iS$ . Each summand  $R(Sx_iS)$  is a submodule of  $(RG)_{S \times S}$  under the two-sided action of  $S$ . The key result is:

**(57.32) Lemma.** *Let  $M = R(SxS)$  be the  $R(S \times S)$ -sublattice of  $(RG)_{S \times S}$  defined by an  $(S, S)$ -double coset  $SxS$ , for some  $x \in G$ . Then  $M \in \text{Ind } R(S \times S)$ , and*

$${}^{(x, 1)}(\Delta(S \cap {}^{x^{-1}}S)) \in \text{vtx } M,$$

(where  ${}^{(x, 1)}(\Delta X)$  denotes the conjugate of  $\Delta X$  by  $(x, 1)$  in  $G \times G$ , for a subset  $X \subseteq G$ ).

*Proof of (57.32).* The  $p$ -group  $S \times S$  acts transitively on the double coset  $SxS$ . Therefore  $M$  is a transitive permutation module over  $R(S \times S)$ , and, by (57.30),  $M$  is indecomposable, with vertex  $\text{Stab}_{S \times S} x$ . Thus we need only check that

$$\text{Stab}_{S \times S} x = {}^{(x, 1)}(\Delta(S \cap {}^{x^{-1}}S)).$$

Let  $h \in S \cap {}^{x^{-1}}S$ ; then  ${}^{(x, 1)}(h, h) = ({}^x h, h)$ , and

$$({}^x h, h) \cdot x = x h x^{-1} x h^{-1} = x,$$

so  ${}^{(x,1)}(\Delta(S \cap {}^{x^{-1}}S)) \leq \text{Stab}_{S \times S}x$ . For the reverse inclusion, let  $(u,v) \in S \times S$ , and assume that  $(u,v)x = uxv^{-1} = x$ . Then  $v = x^{-1}ux \in S \cap {}^{x^{-1}}S$  and  $(u,v) = {}^{(x,1)}(v,v)$ , as required.

*Proof of (57.31).* By the K-S-A Theorem, it follows that  $(RGb)_{S \times S}$  is a direct sum of indecomposable  $R(S \times S)$ -lattices, each of which is isomorphic to  $R(Sx_iS)$  for some  $i$ ,  $1 \leq i \leq m$ . Since  $\Delta D \leq S \times S$  and  $\Delta D$  is a vertex of  $RGb$  by (57.22), it follows that

$$\Delta D = {}_{(S \times S)}^{(x,1)}(\Delta(S \cap {}^{x^{-1}}S)),$$

for some  $x \in G$ , by (57.28) and (57.32). Then for some element  $(g,h) \in S \times S$ , we have

$$\Delta D = {}^{(g,h)(x,1)}\Delta(S \cap {}^{x^{-1}}S)$$

and

$$(g,h)(x,1) = (gxh^{-1}, 1)(h, h).$$

It follows that

$$\Delta D = {}^{(z,1)}\Delta(S \cap {}^{z^{-1}}S), \quad \text{for } z = gxh^{-1}.$$

Then  $u \in D$  if and only if there exists  $v \in S \cap {}^{z^{-1}}S$  such that

$$(u, u) = ({}^z v, v).$$

We obtain  $D = S \cap {}^{z^{-1}}S$  by comparing the second components, and  $z \in C_G(D)$  by comparing the first. This completes the proof.

Some applications are given in the Exercises. Refinements of Theorem 57.31 have been obtained by Green [63], Lam [76], and Robinson [83]. A different proof was given by Thompson [67a]. Robinson also found criteria for a given  $p$ -subgroup of  $G$  to be a defect group of some  $p$ -block. Humphreys [71] applied the theorem above to determine the  $p$ -blocks in finite Chevalley groups over fields of characteristic  $p$ .

## §57. Exercises

The assumptions about the underlying  $p$ -modular system  $(K, R, k)$  in the Exercises for §56 remains in force. In addition, it may be assumed that  $R$  is complete in the  $p$ -adic topology, and that  $k$  is a perfect field, in exercises involving Green's Theorem on Zeros of Characters 19.27.

- Let  $B$  be a block ideal in  $kG$ . Prove that  $B$  is a simple  $k$ -algebra if and only if the defect group of the corresponding block idempotent is  $\{1\}$ .

[Hint: Use (57.27) for one implication and Exercise 56.8 for the other. Also see Exercise 56.10.]

2. Let  $\zeta$  be an irreducible  $K$ -character of  $G$  belonging to a  $p$ -block with defect group  $D$ . Let  $x \in G$  be an element whose  $p$ -part is not conjugate to an element of  $D$ . Prove that  $\zeta(x) = 0$ .

[Hint: Use (57.26) and Green's Theorem on Zeros of Characters 19.27.]

3. A *trivial source module* is an indecomposable  $RG$ -lattice  $M$  such that  $M|(1_H)^G$  for some subgroup  $H \leq G$ , where  $1_H$  denotes the  $RG$ -lattice  $R$  with trivial  $H$ -action. Prove the following statements (see also §81).

- (i) Let  $D$  be a vertex of a trivial source module  $M$ . Prove that  $M|(1_D)^G$  (so that  $M$  does indeed have a trivial source in the sense of Definition 19.11).

[Hint: Since  $M|(1_H)^G$ , we may assume that  $D \leq H$ , by the basic property of vertices (19.8). Then show that  $1_H|(1_D)^H$ , and hence  $(1_H)^G|((1_D)^H)^G$ .]

- (ii) Let  $M$  be a trivial source module with vertex  $D$ . Prove that  $1_D|M_D$  (where  $M_D = \text{res}_D^G M$ ).

[Hint: By part (i),  $1_D$  is a source of  $M$ . Since  $M$  is  $(G, D)$ -projective,  $M_D$  has an indecomposable summand having a vertex and source in common with  $M$ , by (19.15).]

- (iii) Let  $M$  be a trivial source module with vertex  $D$ , such that  $M|(1_H)^G$  for some subgroup  $H \leq G$ . Prove that  $M_H$  has an indecomposable summand  $U$  with vertex  $D'$  such that  $H \cap D \leq_H D'$ .

[Hint: By part (ii),  $1_D|M_D$ , so  $1_{D \cap H}|M_{D \cap H}$ . Then  $M_H$  has an indecomposable summand  $U$  such that  $1_{D \cap H}|U_{D \cap H}$ . Since  $D \cap H$  is a vertex of  $1_{D \cap H}$  (by (57.29)), we have  $D \cap H \leq_H D'$  (by (19.14)).]

4. Prove that block ideals in  $RG$  are trivial source modules (as  $R(G \times G)$ -modules). (The same result holds for block ideals in  $kG$ .)

[Hint: Use the fact that

$$RG \cong (1_{\Delta G})^{G \times G}$$

as  $R(G \times G)$ -lattices, where  $\Delta G$  denotes the diagonal subgroup of  $G \times G$ .]

5. Let  $B$  be a block ideal in  $RG$ . Prove that  $B$  is an absolutely indecomposable  $R(G \times G)$ -lattice.

[Hint: Let  $B = bRG$ , for a block idempotent  $b$ . Let  $E = \text{End}_{R(G \times G)} B$ , and  $E = \tilde{E}/\text{rad } E$ . Show that  $E \cong c(RG)b$ , by (57.25), and that  $\tilde{E} \cong k$  by the results in §56D. Then apply (30.29).]

6. (Alperin [67]; Green [63]). Let  $D$  be a defect group of a  $p$ -block of  $G$ . Prove that  $D$  is a *tame intersection* of Sylow  $p$ -subgroups of  $G$ , i.e., there exist Sylow  $p$ -subgroups  $P, Q$  of  $G$  such that  $D = P \cap Q$  and  $N_P(D)$  and  $N_Q(D)$  are both Sylow  $p$ -subgroups of  $N_G(D)$ .

[Hint: Let  $A$  be a Sylow  $p$ -subgroup of  $N_G(D)$ . Then  $A \geq D$ . Choose a Sylow  $p$ -subgroup  $P$  of  $G$  such that  $P \geq A$ . Then  $A = P \cap N_G(D) = N_P(D)$ . By Theorem 57.31, there exists  $z \in C_G(D)$  such that  $D = P \cap Q$  with  $Q = {}^zP$ . Then  ${}^zA = {}^zP \cap N_G(D) = Q \cap N_G(D) = N_Q(D)$ , and the result follows.]

## §58. THE BRAUER CORRESPONDENCE

The main subject of this section is the connection between  $p$ -blocks of  $G$  and  $p$ -blocks of subgroups of  $G$ . The first connection is given by the Brauer map  $\sigma$  relative to a  $p$ -subgroup  $D$  of  $G$ . This defines a homomorphism of  $k$ -algebras  $\sigma: c(kG) \rightarrow c(kN_G(D))$ , which is used to prove Brauer's First Main Theorem 58.6. To some extent, at least, this theorem reduces the study of blocks with a given defect group  $D$  to a situation in which  $D$  is a normal subgroup. Further group-theoretic reductions are presented in §61. A general connection between blocks of  $G$  and blocks of subgroups of  $G$ , called the Brauer Correspondence, is defined in §58C. The Brauer Correspondence can be interpreted in terms of central characters, in some cases through the Brauer map with respect to a  $p$ -subgroup  $D$ , and through the Green Correspondence of indecomposable modules (Theorem 58.22). All these approaches are discussed, and the connections between them are worked out.

### §58A. The Brauer Map

In this section  $G$  denotes a finite group,  $p$  a prime number, and  $R$  is either a field of characteristic  $p$ , or a complete d.v.r. with maximal ideal  $\mathfrak{p}$  containing  $p$ , as in §57A. We first recall some of the basic properties of  $G$ -algebras, trace maps, and defect groups from the preceding section.

Let  $A$  be the  $G$ -algebra  $RG$  on which  $G$  acts by conjugation. For  $H \leq G$ , set

$$A_H = \{a \in A : x \cdot a = a \text{ for all } x \in H\}$$

where  $x \cdot a = xax^{-1}$ . Then  $A_G$  is the center  $c(RG)$  of  $RG$ . For  $D' \leq H$ , we defined a trace map

$$T_{H/D'}: A_{D'} \rightarrow A_H, \quad \text{given by } T_{H/D'}(a) = \sum_{x \in H/D'} x \cdot a, \quad a \in A_{D'}.$$

We put

$$A_{H/D'} = T_{H/D'}(A_{D'}) = \text{the image of the trace map.}$$

Then  $A_{H/D'}$  is a two-sided ideal in  $A_H$ , by (57.3). A *block idempotent*  $b$  in  $A$  is a primitive idempotent in  $A_G$ . A subgroup  $D'$  is called a *defect group* of a block idempotent  $b \in A_G$  provided that

$$b \in A_{G/D'}, \quad \text{and} \quad b \in A_{G/D''} \Rightarrow D' \leq_G D''.$$

The defect groups of a block idempotent form a  $G$ -conjugacy class of  $p$ -subgroups of  $G$ .

**(58.1) Definition.** Let  $D$  be a  $p$ -subgroup of  $G$ . The *Brauer map*  $\sigma (= \sigma_D)$  relative

to  $D$  is the  $R$ -linear map  $RG \rightarrow RC_G(D)$  defined on elements  $x \in G$  by

$$\sigma(x) = \begin{cases} x, & \text{if } x \in C_G(D) \\ 0, & \text{otherwise,} \end{cases}$$

and extended by linearity to all of  $RG$ .

The Brauer map has many interesting and subtle properties, which are used to relate  $p$ -blocks of  $G$  to  $p$ -blocks of subgroups of  $G$ . Following Alperin and Broué [79], we summarize some of the basic facts about the Brauer map in the next lemma. In our notation, we take  $\mathfrak{p} = 0$  if  $R$  is a field of characteristic  $p$ .

**(58.2) Lemma.** *Let  $D \leq H \leq G$ , for a  $p$ -subgroup  $D$  of  $G$ , and let  $\sigma$  be the Brauer map relative to  $D$ . Then the following statements hold.*

- (i)  $\sigma(A) \subseteq RC_G(D)$ .
- (ii) If  $D \leq H \leq N_G(D)$ , then  $\sigma(A_H) \subseteq c(RH)$ .
- (iii) If  $L$  is an  $H$ -class sum whose class defect group<sup>†</sup> contains no  $H$ -conjugate of  $D$ , then  $\sigma L = 0$ .
- (iv) For any  $D' \leq H$  such that  $D \not\leq_H D'$ , we have  $\sigma(A_{H/D'}) \equiv 0 \pmod{\mathfrak{p}A}$ .
- (v) We have  $A_D = RC_G(D) + \sum_{D' < D} A_{D/D'}$ , and the map  $\sigma: A_D \rightarrow RC_G(D)$  is a homomorphism mod  $\mathfrak{p}$ , in the sense that for  $a, a' \in A_D$ ,

$$\sigma(aa') \equiv \sigma(a)\sigma(a') \pmod{\mathfrak{p}A}.$$

- (vi) For  $a \in A_D$ ,

$$\sigma(T_{G/D}a) \equiv T_{N_G(D)/D}(\sigma a) \pmod{\mathfrak{p}A}.$$

*Proof.* Part (i) is clear. For (ii), from  $H \leq N_G(D)$  we obtain  $C_G(D) \trianglelefteq H$ , and therefore

$$(58.3) \quad \sigma(y \cdot a) = y \cdot \sigma(a) \text{ for all } a \in A, y \in H.$$

If  $a \in A_G$ , then  $y \cdot \sigma(a) = \sigma(a)$  for all  $y \in H$ , and (ii) holds.

(iii) Let  $\mathfrak{L}$  be the  $H$ -conjugacy class defining  $L$ . If  $\sigma L \neq 0$ , then  $\mathfrak{L} \cap C_G(D) \neq 0$ , and  $D$  is contained in some class defect group of  $\mathfrak{L}$ , completing the proof of (iii).

- (iv) By (57.14) we have

$$A_{H/D'} \equiv \sum R L_i \pmod{\mathfrak{p}A}$$

where the  $\{L_i\}$  are  $H$ -class sums whose defect groups satisfy  $D_i \leq_H D'$ . If  $D \not\leq_H D'$ , then  $D \not\leq_H D_i$  for each  $i$ , and the result follows from (iii).

<sup>†</sup>See (57.11).

(v) By (57.14) again,  $A_D$  has an  $R$ -basis consisting of the  $D$ -class sums

$$L = \sum_{u \in D/C_D(x)} u \cdot x = T_{D/C_D(x)} x, \quad \text{for } x \in G.$$

Such a class sum is in  $RC_G(D)$  if  $x \in C_G(D)$ , while if  $x \notin C_G(D)$ , then  $C_D(x) < D$  and

$$L \in A_{D/C_D(x)} \subseteq A_{D/D'} \quad \text{for } D' = C_D(x) < D.$$

This proves the first assertion in (v). For the second, write

$$A_D = RC_G(D) + X, \quad \text{where } X = \sum_{D' < D} A_{D/D'}.$$

Then  $X$  is a two-sided ideal in  $A_D$ , by (57.3). Moreover,  $\sigma(X) \subseteq \mathfrak{p}A$ , by part (iv). It now follows easily that  $\sigma$  is a homomorphism mod  $\mathfrak{p}$ , for let  $a, a' \in A_D$ , and write

$$a \equiv u(\text{mod } X), \quad a' \equiv u'(\text{mod } X), \quad \text{with } u, u' \in RC_G(D).$$

Then  $aa' \equiv uu'(\text{mod } X)$ , and hence

$$\sigma(aa') \equiv \sigma(uu') = \sigma(u)\sigma(u') \equiv \sigma(a)\sigma(a')(\text{mod } \mathfrak{p}A),$$

as required.

(vi) By (57.5), we have

$$T_{G/D}a = \sum_x T_{N_G(D)/N_G(D) \cap {}^x D}(x \cdot a), \quad \text{for all } a \in A_D,$$

where the sum is taken over a cross section of the  $(N_G(D), D)$ -double cosets in  $G$ . Now apply  $\sigma$  to both sides of this formula. For each double coset  $N_G(D)x D$ , we have

$$D \leq_{N_G(D)} (N_G(D) \cap {}^x D) \Leftrightarrow N_G(D) \cap {}^x D = D \quad \text{and} \quad x \in N_G(D).$$

Therefore

$$\sigma(T_{G/D}a) \equiv \sigma(T_{N_G(D)/D}a) \pmod{\mathfrak{p}A}$$

by part (iii) and (57.14). Finally,

$$\sigma(T_{N_G(D)/D}a) = T_{N_G(D)/D}\sigma a$$

by (58.3). This completes the proof of the lemma.

Several parts of the lemma come into sharp focus in the next result.

**(58.4) Proposition.** *Let  $k$  be a field of characteristic  $p$ , and let  $A$  be the  $G$ -algebra*

$kG$ . The Brauer map  $\sigma: A_G \rightarrow kC_G(D)$  (relative to  $D$ ) defines a  $k$ -algebra homomorphism from  $A_G$  into  $c(kN_G(D))$ , whose kernel is precisely

$$\mathfrak{A} = \sum_{D' \leq G, D \not\leq_G D'} A_{G/D'}.$$

Moreover,  $\sigma$  defines a surjection of  $k$ -algebras

$$A_{G/D} \rightarrow T_{N_G(D)/D}(kC_G(D))$$

whose kernel contains no block idempotents of  $G$  with defect group  $D$ .

*Proof.* Since  $A_G \subseteq A_D$ ,  $\sigma$  defines a  $k$ -algebra homomorphism by (58.2v), using  $R = k$ . Further,  $\sigma(A_G) \subseteq c(kN_G(D))$  by (58.2ii), using  $H = N_G(D)$ . By (58.2iv) we have

$$A_{G/D'} \subseteq \ker \sigma \quad \text{for all } D' \leq G \quad \text{with } D \not\leq_G D'.$$

Therefore  $\mathfrak{A} \subseteq \ker \sigma$ . To prove that  $\mathfrak{A} = \ker \sigma$ , we use the fact that  $A_G$  has a  $k$ -basis consisting of  $G$ -class sums

$$C = \sum_{y \in \mathfrak{C}} y = T_{G/C_G(x)^x} \quad \text{for } x \in \mathfrak{C}$$

By (58.2iv),  $C \in \ker \sigma$  unless  $D \leq C_G(x)$  for some  $x \in \mathfrak{C}$ . In that case,  $\mathfrak{C} \cap C_G(D) \neq \emptyset$ , and

$$\sigma C = C' = \sum_{y \in \mathfrak{C} \cap C_G(D)} y \neq 0.$$

Since the  $G$ -conjugacy classes, and their nonempty intersections with  $C_G(D)$  are disjoint, it follows that

$$a \in \ker \sigma \Leftrightarrow a \in \mathfrak{A} \quad \text{for all } a \in A_G,$$

and the first statement is proved.

The final statement in the proposition follows at once from (58.2vi) and the first part of the proof. In particular, no block idempotent with defect group  $D$  is in  $\mathfrak{A}$ , by Rosenberg's Lemma 57.8 and the fact that  $A_{G/D'}$  is a two-sided ideal in  $A_G$  for all  $D' < G$ . This completes the proof.

## §58B. Brauer's First Main Theorem

We carry over the notation from §58A. The main result of this subsection establishes a bijection from the set of  $p$ -blocks of  $G$  with a given defect group  $D$  to the set of  $p$ -blocks of  $N_G(D)$  with defect group  $D$ . Thus, it is natural to begin with some properties of block idempotents and defect groups in finite groups having a normal  $p$ -subgroup.

**(58.5) Proposition.** *Let  $G$  be a finite group with a normal  $p$ -subgroup  $D$ , and let  $A$  be the  $G$ -algebra  $RG$ , as in §58A. Then the following statements hold:*

(i) *For every block idempotent  $b \in A_G$ , we have*

$$b \in RC_G(D) \cap A_G + \mathfrak{p}A_G.$$

(ii)  *$D$  is contained in the defect groups of all block idempotents in  $A_G$ .*

*Proof.* (i) By Lemma 58.2v, we have

$$A_G \subseteq RC_G(D) + \sum_{D' < D} A_{G/D'}.$$

It is sufficient to prove that  $A_{G/D'} \subseteq \text{rad } A_G$  for all subgroups  $D' < D$ , since in that case we have  $b \equiv b_1 \pmod{(\text{rad } A_G)}$  for some  $b_1 \in RC_G(D)$ . Then  $b \equiv b^m \pmod{(\text{rad } A_G)^m}$  for every positive integer  $m$ , so we obtain  $b \in RC_G(D) + \mathfrak{p}A_G$  since  $(\text{rad } A_G)^m \subseteq \mathfrak{p}A_G$  for some  $m$ . For a given subgroup  $D' < D$ , we have

$$A_{G/D'} = T_{G/D}(T_{D/D'} A_{D'})$$

by transitivity of the trace map, so  $A_{G/D'} \subseteq \text{rad } A_G$  if we can prove that  $T_{D/D'}(A_{D'}) \subseteq \text{rad } A$  for  $D' < D$ . Let  $\tau: RG \rightarrow R(G/D)$  be the natural surjection; then

$$T_{D/D'} a = \sum_{x \in D/D'} x \cdot a \equiv |D:D'| a \pmod{\ker \tau}.$$

But  $|D:D'| \in \mathfrak{p}$  for  $D' < D$ , while  $\ker \tau \subseteq \text{rad } A$  by (5.26). Since  $\mathfrak{p}A \subseteq \text{rad } A$  by (56.2), we obtain

$$A_{G/D'} \subseteq A_G \cap \text{rad } A \subseteq \text{rad } A_G,$$

as required.

(ii) Let  $b$  be a block idempotent in  $A_G$ . From part (i), it follows that

$$b \equiv \sum \alpha_i L_i \pmod{\mathfrak{p}A_G}, \quad \text{with } \alpha_i \in R,$$

where the  $\{L_i\}$  are  $G$ -class sums whose class defect groups  $D_i$  contain  $D$ . On the other hand, if  $D'$  is a defect group of  $b$ , then  $D_i = {}_G D'$  for the class defect group  $D_i$  of some class sum  $L_i$  whose coefficient  $\alpha_i \notin \mathfrak{p}$ , by Theorem 57.17. Since  $D$  is a normal subgroup, we obtain  $D \leq D'$ , completing the proof.

Returning to the general situation, we shall establish the first of several basic results of Brauer ([56], [59]), which are called the First, Second, and Third Main Theorems. Brauer first proved the theorem below in case the coefficient ring  $R$  is a splitting field of characteristic  $p$  (Brauer [56]; see also CR §87).

The approach to follow is based on Alperin-Broué [79].

**(58.6) Brauer's First Main Theorem.** *Let  $G$  be a finite group,  $D$  a  $p$ -subgroup*

of  $G$ , and set  $H = N_G(D)$ . Let  $\sigma: c(RG) \rightarrow c(RH)$  denote the Brauer map with respect to  $D$ . For each block idempotent  $b \in c(RG)$  with defect group  $D$ , there exists a unique block idempotent  $b' \in c(RH)$  with defect group  $D$  such that

$$(58.7) \quad \sigma b \equiv b' \pmod{pc(RG)}.$$

The mapping (58.7) defines a bijection from the set of block idempotents in  $c(RG)$  with defect group  $D$  to the set of block idempotents in  $c(RH)$  with defect group  $D$ .

*Proof.* First assume the coefficient ring is a field  $k$  of characteristic  $p$ . Let  $A$  denote the  $G$ -algebra  $kG$ , and  $A'$  the  $H$ -algebra  $kH$ , so  $A_G = c(kG)$  and  $A'_H = c(kH)$ . By (58.4) and (58.2ii), the Brauer map  $\sigma$  relative to  $D$  defines a surjection of  $k$ -algebras

$$\sigma: A_{G/D} \rightarrow T_{H/D}(kC_G(D)) \subseteq A'_H.$$

By (57.10) and (58.5), the set of block idempotents  $b \in A_G$  with defect group  $D$  coincides with the set of all primitive idempotents in  $A_{G/D}$ . Moreover, none of them is contained in the kernel of  $\sigma$  (by the last statement of (58.4)). By a general result on commutative f.d.  $k$ -algebras (see Exercise 2),  $\sigma$  defines a bijection from the set of all primitive idempotents in  $A_{G/D}$  to the set of all primitive idempotents in  $T_{H/D}(kC_G(D))$ . To complete the proof in this case, it remains to show (i) that each primitive idempotent in  $A'_H$  with defect group  $D$  belongs to  $T_{H/D}(kC_G(D))$ , and (ii) that for each primitive idempotent  $b \in A_{G/D}$  with defect group  $D$ ,  $\sigma(b) = b'$  is a primitive idempotent in  $A'_H$  with defect group  $D$ .

For the first statement, let  $b^*$  be a primitive idempotent in  $A'_H$  with defect group  $D$ . Since  $D \trianglelefteq H$ , we have  $b^* \in kC_G(D) \cap A'_H$  by (58.5i). Therefore  $\sigma b^* = b^*$ . Since  $b^*$  has defect group  $D$ , we obtain  $b^* = T_{H/D}a$  for some  $a \in A'$ , and hence

$$b^* = \sigma b^* = \sigma T_{H/D}a = T_{H/D}\sigma a \in T_{H/D}(kC_G(D)),$$

using (58.3), and that fact that  $D \trianglelefteq H$ .

To prove (ii), we begin with the fact that  $\sigma(b) = b'$  is primitive in  $T_{H/D}(kC_G(D)) \subseteq A'_{H/D}$ , and have to prove that  $b'$  is primitive in  $A'_H$ , with defect group  $D$ . By (58.5ii),  $b'$  will have defect group  $D$  if we can prove it is primitive in  $A'_H$ . Suppose it is not; then  $b' = \sum_{i=1}^m b''_i$  with  $m > 1$ , for some block idempotents  $\{b''_i\}$  in  $A'_H$ . Since  $b''_i \notin T_{H/D}(kC_G(D))$ , its defect group properly contains  $D$ , by part (i), for  $1 \leq i \leq m$ . On the other hand,  $b''_i = b''_i b' \in A'_{H/D}$  for each  $i$ , since  $A'_{H/D}$  is a two-sided ideal in  $A'_H$ . This is a contradiction, and establishes that  $b'$  is primitive in  $A'_H$ , completing the proof of the theorem in case  $R$  is a field.

Now let  $R$  be a complete d.v.r. with quotient field  $K$ , and residue field  $k = R/\mathfrak{p}$  of characteristic  $p$ . Then  $(K, R, k)$  is a  $p$ -modular system which is admissible for  $G$  (see (56.3)). By (57.16), it follows that the map  $a \rightarrow \bar{a}$  from  $RG$  to  $kG$  defines a bijection from the block idempotents in  $RG$  with defect group  $D$ , to those in  $kG$  with defect group  $D$ . The same statement holds for block idempotents in

$RH$  and  $kH$ . Moreover, the Brauer map, relative to  $D$ , from  $kG$  to  $kC_G(D)$  is clearly the map defined by

$$\bar{a} \rightarrow \overline{\sigma(a)}, \quad \text{for } a \in RG,$$

where  $\sigma$  is the Brauer map, relative to  $D$ , on  $RG$ . From these remarks and the first part of the proof, it follows that there exists a bijection satisfying (58.7) from the set of block idempotents in  $RG$  with defect group  $D$  to those in  $RH$  with defect group  $D$ , completing the proof of the theorem.

An important extension of the First Main Theorem is given in §61B.

### §58C. The Brauer Correspondence

Brauer's First Main Theorem 58.6 establishes a connection between  $p$ -blocks of  $G$  with a given defect group  $D$ , and  $p$ -blocks of  $N_G(D)$  with defect group  $D$ . Using the theory of central characters, Brauer defined a more general connection, called the Brauer correspondence, between  $p$ -blocks of  $G$  and  $p$ -blocks of certain subgroups of  $G$ . The bijection described in (58.6) turns out to be a special case of the Brauer correspondence (see Exercise 4).

Throughout this subsection,  $(K, R, k)$  denotes a  $p$ -modular system which is admissible for  $G$  (see (56.3)).

From §56D we recall that a central character of  $RG$  is a homomorphism of  $R$ -algebras

$$\lambda: c(RG) \rightarrow k'$$

where  $k'$  is a finite extension field of  $k$ . The central characters of  $RG$  are in bijective correspondence with the central characters of  $kG$ . There is also a bijection between  $p$ -blocks of  $G$  and equivalence classes of central characters of  $RG$ . A central character  $\lambda$  of  $RG$  corresponds to a  $p$ -block  $B$  of  $G$  if and only if

$$\lambda(b) = 1 \quad \text{and} \quad \lambda(b') = 0 \quad \text{for all } b' \neq b,$$

where  $b$  is the block idempotent of  $B$ , and  $\{b'\}$  are the block idempotents of blocks  $B' \neq B$ .

By (56.20), the central characters of  $RG$  themselves are in bijective correspondence with the  $p$ -blocks of  $G$ , in case  $k$  is a splitting field for  $G$ . In this situation, distinct central characters are inequivalent.

**(58.8) Definition.** Let  $(K, R, k)$  be a  $p$ -modular system which is admissible for  $G$ . Let  $H$  be a subgroup of  $G$ , and  $\psi'$  a central character of  $RH$  associated with the  $p$ -block  $B'$  of  $H$ . Then  $\psi'$  determines an  $R$ -linear map  $(\psi')^G: c(RG) \rightarrow R$  as follows.\* Let  $C = \sum_{x \in G} x$  be a class sum in  $c(RG)$ . Put

\*The map  $(\psi')^G$  has nothing to do with induction of characters of modules.

$$C' = \sum_{x \in \mathfrak{C} \cap H} x \in c(RH),$$

if  $\mathfrak{C} \cap H \neq \emptyset$ , and put  $C' = 0$  otherwise. The class sums  $C$  form an  $R$ -basis for  $c(RG)$ , so we may define an  $R$ -linear map  $(\psi')^G$  by setting

$$(\psi')^G(C) = \begin{cases} \psi'(C') & \text{if } \mathfrak{C} \cap H \neq \emptyset \\ 0 & \text{if } \mathfrak{C} \cap H = \emptyset. \end{cases}$$

If the  $R$ -linear map  $(\psi')^G$  is a central character of  $RG$ , the  $p$ -block of  $G$  associated with  $(\psi')^G$  will be denoted by  $(B')^G$ , and we shall say that the *Brauer correspondence* is defined for the block  $B'$ . Then  $(B')^G$  is the *Brauer correspondent* of  $B'$ .

It is easily verified that if  $\psi'$  and  $\psi''$  are central characters of  $RH$ , and if  $(\psi')^G$  and  $(\psi'')^G$  are central characters of  $RG$ , then  $\psi'$  and  $\psi''$  are equivalent in the sense of (56.15) if and only if  $(\psi')^G$  and  $(\psi'')^G$  are equivalent. Thus the Brauer correspondence  $B' \rightarrow (B')^G$ , when it is defined, is independent of the choice of representatives of equivalence classes of central characters.

The purpose of this subsection is to give other useful interpretations of the Brauer correspondence, and conditions under which it is defined, following Brauer [59], Alperin [77], Okuyama [78], and Alperin-Burry [80].

As a start, we show that in some cases the Brauer correspondence can be defined in terms of the Brauer map  $\sigma$ , occurring in §58A.

**(58.9) Theorem.** *Let  $(K, R, k)$  be a  $p$ -modular system such that  $\text{char } K = 0$  and  $K$  is sufficiently large relative to  $G$ . Let  $D$  be a  $p$ -subgroup of  $G$ , and let  $H$  be a subgroup such that*

$$DC_G(D) \leq H \leq N_G(D).$$

*Then the Brauer correspondence  $B' \rightarrow (B')^G$  is defined for all  $p$ -blocks  $B'$  of  $H$ . If  $\psi'$  is a central character of  $RH$ , then the central character  $(\psi')^G$  of  $RG$  is given by*

$$(\psi')^G = \psi' \circ \sigma$$

*where  $\sigma : c(RG) \rightarrow c(RH) \cap RC_G(D)$  is the Brauer map relative to  $D$  (see (58.1)).*

*Proof.* Let  $\psi'$  be an arbitrary central character of  $RH$ . By Lemma 58.2, the Brauer map  $\sigma : c(RG) \rightarrow c(RH) \cap RC_G(D)$  is a homomorphism mod  $p$ . Since  $pRH \subseteq \ker \psi'$ , the map  $\psi' \circ \sigma$  is a central character of  $RG$ , and we have only to prove that  $\psi' \circ \sigma = (\psi')^G$ . Let  $C = \sum_{x \in \mathfrak{C}} x$  be a class sum in  $RG$ , and suppose that  $\mathfrak{C} \cap H \neq \emptyset$ . Then

$$C' = \sum_{x \in \mathfrak{C} \cap H} x = \sum_i C'_i + \sum_j C''_j$$

where the  $\{C'_i\}$  are class sums in  $c(RH)$  supported by classes in  $\mathfrak{C} \cap C_G(D)$ , while

the  $\{C''_j\}$  are class sums in  $c(RH)$  supported by  $H$ -conjugacy classes  $\mathfrak{C}_j''$  such that  $\mathfrak{C}_j'' \cap C_G(D) = \emptyset$ . We have

$$(\psi')^G(C) = \psi'(C') = \sum_i \psi'(C'_i) + \sum_j \psi'(C''_j).$$

Since

$$(\psi' \circ \sigma)(C) = \sum_i \psi'(C'_i),$$

it is sufficient to prove that

$$\psi'(C''_j) = 0 \quad \text{for each } j.$$

Let  $D'$  be a defect group of the  $p$ -block of  $H$  associated with  $\psi'$ . By Theorems 57.17 and 56.42,  $\psi'$  vanishes on all  $H$ -class sums in  $c(RH)$  whose class defect groups do not contain an  $H$ -conjugate of  $D'$ . We also have  $D \leq D'$  by (58.5), since  $D \trianglelefteq H$ . For each of the  $H$ -classes  $\mathfrak{C}$  such that  $\mathfrak{C} \cap C_G(D) = \emptyset$ , the class defect groups do not contain  $D$ , and hence contain no  $H$ -conjugate of  $D'$ . Thus  $\psi'(C'_j) = 0$  for each  $j$ , as required.

**(58.10) Corollary.** *Keep the hypothesis of (58.9). If  $B'_1$  is the principal block of  $H$ , then  $(B'_1)^G = B_1$ , where  $B_1$  is the principal block of  $G$ .*

*Proof.* Let  $\psi'_1$  be the central character of  $RH$  associated with  $B'_1$ . By (56.24) we have

$$\psi'_1(C') = |\mathfrak{C}'|$$

for each  $H$ -class sum  $C'$  supported on  $\mathfrak{C}'$ . By (58.9) we have

$$(\psi'_1)^G(C) = (\psi'_1 \circ \sigma)(C) = |\mathfrak{C} \cap C_G(D)|$$

for each  $G$ -class sum  $C$  supported on  $\mathfrak{C}$ . However,

$$|\mathfrak{C}| \equiv |\mathfrak{C} \cap C_G(D)| \pmod{p}$$

since  $D$  is a  $p$ -group, by consideration of the orbits of the action of  $D$  on  $\mathfrak{C}$ . Thus

$$(\psi'_1)^G(C) = |\mathfrak{C}|$$

and  $(\psi'_1)^G$  corresponds to the principal block of  $G$ , by (56.24) again.

**(58.11) Corollary.** *Keep the notation of (58.9). Let  $b$  be a block idempotent of  $RG$ , associated with the  $p$ -block  $B$ . Then either  $\sigma b \equiv 0 \pmod{\mathfrak{p}RH}$  or*

$$\sigma b \equiv \sum b'_i \pmod{\mathfrak{p}RH}$$

where the sum is taken over block idempotents  $\{b'_i\}$  of  $RH$  associated with  $p$ -blocks  $\{B'_i\}$  of  $H$  such that  $(B'_i)^G = B$  for each  $i$ . We have  $\sigma b \equiv 0 \pmod{pRH}$  if and only if there is no  $p$ -block  $B'$  of  $H$  such that  $(B')^G = B$ .

*Proof.* Let  $\sigma: c(kG) \rightarrow c(kH)$  be the Brauer map defined on the center of  $kG$ . Then

$$\sigma(\bar{a}) = \overline{\sigma(a)} \quad \text{for all } a \in c(RG)$$

(see the proof of (58.6)). Since  $\sigma$  is a homomorphism of  $k$ -algebras,  $\sigma(\bar{b})$  is either zero or a sum of block idempotents in  $kH$ . If the image is zero, then  $\sigma(b) \in pRH$ , and for all central characters  $\psi'$  of  $RH$  we have  $\psi'(\sigma(b)) = 0$ . This clearly occurs if and only if there is no  $p$ -block  $B'$  of  $H$  such that  $(B')^G = B$ .

Now assume  $\sigma(\bar{b}) \neq 0$ , and let  $\sigma(\bar{b}) = \sum \beta'_i$ , where  $\{\beta'_i\}$  are block idempotents of  $kH$ . Then there exist block idempotents  $\{b'_i\}$  in  $RH$  such that  $\bar{b}'_i = \beta'_i$  for each  $i$ , and

$$\sigma b \equiv \sum b'_i \pmod{pRH}.$$

Let  $\{\psi'_i\}$  be the central characters of  $RH$  associated with the block idempotents  $\{b'_i\}$  in the blocks  $\{B'_i\}$  of  $RH$ . Then we have  $(B'_i)^G = B$  for each  $i$  by the definition of the Brauer correspondence, since  $(\psi'_i)^G(b) = 1$  for each  $i$ . Finally, let  $b'$  be a block idempotent of  $RH$  associated with the central character  $\psi'$ , and assume that  $(\psi')^G = \psi$ , where  $\psi$  is a central character of  $RG$  such that  $\psi(b) = 1$ . Then

$$\psi'((\sigma b)b') = (\psi')^G(b)\psi'(b') \neq 0,$$

and hence  $(\sigma b)b' \neq 0$ . This shows that  $b' = b_i$  for some  $i$ , completing the proof.

Suppose now that  $(K, R, k)$  is a  $p$ -modular system, with  $R$  a complete d.v.r. For an arbitrary subgroup  $H$  of  $G$ , we wish to investigate whether the Brauer correspondence is defined for blocks of  $H$ . This will be accomplished by obtaining another criterion (see (58.15)) for each central character  $\psi'$  of  $RH$  to yield a central character  $(\psi')^G$  of  $G$ .

As in §57B, we view  $RG$  as an  $R(G \times G)$ -lattice, with the action of  $G \times G$  given by

$$(x, y)a = xay^{-1}, \quad \text{for } x, y \in G, \quad a \in RG.$$

For  $T$  any subset of  $G$ , let  $RT$  denote the  $R$ -sublattice of  $RG$  spanned by the elements of  $T$ . Further, let  $\Delta: H \rightarrow H \times H$  be the diagonal map. Given an  $R(G \times G)$ -lattice  $M$ , its restriction  $M_{H \times H}$  is an  $R(H \times H)$ -lattice. Each block idempotent  $b' \in c(RH)$  determines a block ideal  $B' = RHb'$  and a  $p$ -block  $B'$  of  $H$ .

As usual, we shall use the notation  $M|N$ , for  $A$ -modules  $M$  and  $N$ , to mean that  $M$  is isomorphic to a direct summand of  $N$ .

**(58.12) Lemma.** *Let  $B'$  be a block ideal of  $RH$ .*

(i) We have

$$B' \mid R(HyH) \quad \text{and} \quad R(HyH) \mid (RG)_{H \times H}$$

for some  $(H, H)$  double coset  $HyH$  in  $G$ .

(ii) For each  $y \in G$ ,

$$\text{Stab}_{H \times H} y = {}^{(y, 1)}(\Delta(H \cap {}^{y^{-1}}H)).$$

Setting  $X = \text{Stab}_{H \times H} y$ , the  $R(H \times H)$ -module  $R(HyH)$  is  $(H \times H, X)$ -projective.

*Proof.* Let  $G = \bigcup_{i=1}^n Hy_iH$ ; then we clearly have

$$(RG)_{H \times H} = \bigoplus_{i=1}^m R(Hy_iH).$$

Since  $R$  is complete and  $B'$  is an indecomposable  $R(H \times H)$ -lattice, it follows from the K-S-A Theorem that for some  $i$ ,  $1 \leq i \leq m$ ,  $B' \mid R(Hy_iH)$ . Each  $R(H \times H)$ -lattice of the form  $R(HyH)$  is a transitive permutation module, with an  $R$ -basis consisting of the transitive  $H \times H$ -set  $HyH$ . Then  $R(HyH) \simeq \text{ind}_X^{H \times H} 1_X$  where  $1_X$  is the trivial  $RX$  module and  $X = \text{Stab}_{H \times H} y$ . By (19.2v),  $R(HyH)$  is  $(H \times H, X)$ -projective. Finally,  $\text{Stab}_{H \times H} y = {}^{(y, 1)}(\Delta(H \cap {}^{y^{-1}}H))$  by the proof of (57.32), completing the proof.

**(58.13) Lemma.** Let  $B'$  be a block ideal in  $RH$ , defined by the block idempotent  $b'$ . Then there exist isomorphisms of  $R$ -algebras

$$\alpha: c(RG) \rightarrow E = \text{End}_{R(G \times G)} RG$$

and

$$\alpha: c(B') \rightarrow E' = \text{End}_{R(H \times H)} B',$$

given by

$$\alpha(a) = a_l \quad \text{and} \quad \alpha'(a') = (a')_l$$

where  $a_l$  and  $(a')_l$  denote left multiplication by  $a$  and  $a'$  on  $RG$  and  $B'$ , respectively.

*Proof.* It is clear that the map  $\alpha$  is an injective homomorphism of  $R$ -algebras. If  $f \in E$ , then  $f = a_l$  for some  $a \in RG$ , since the left regular module  $RG$  has the double centralizer property. Since  $f$  also commutes with the left multiplications, it follows that  $a \in c(RG)$ . Since  $B'$  is an  $R$ -algebra with identity element  $b'$ , the same argument shows that  $\alpha'$  is an isomorphism.

**(58.14) Corollary.** Keep the notation of (58.13). Then

$$E' = \text{End}_{R(H \times H)} B'$$

is a f.g. commutative local  $R$ -algebra, and  $E'/\text{rad } E'$  is a finite extension field of  $k = R/\mathfrak{p}$ .

*Proof.* Since  $B'$  is an indecomposable  $R(H \times H)$ -lattice,  $E'$  is a local ring by (6.10). Moreover,  $E'$  is commutative by (58.13), and  $\text{p}E' \subset \text{rad } E'$  by (56.2). Thus  $E'/\text{rad } E'$  is a f.d.  $k$ -algebra, and the result follows.

Keep the notation of (58.13). The following definitions will be used in the next three results. Since  $B'|_{(RG)_{H \times H}}$  by (58.12), there exists an injection

$$i: B' \rightarrow (RG)_{H \times H}$$

and a projection

$$j: (RG)_{H \times H} \rightarrow B'$$

both of which are  $R(H \times H)$ -homomorphisms. Using these maps we define an  $R$ -linear map

$$\theta: E \rightarrow E' \quad \text{by } \theta(f) = jfi, \quad f \in E.$$

Let  $\lambda$  be the natural homomorphism of  $R$ -algebras

$$\lambda: E' \rightarrow k' = E'/\text{rad } E'$$

given in (58.14), where  $k'$  is a finite extension field of  $k$ . The key result is:

**(58.15) Proposition.** (Okuyama [78]). *Let  $H \leq G$ , and let  $B'$  be a  $p$ -block of  $H$ . Then the Brauer correspondent  $(B')^G$  of  $B'$  is defined (see (58.8)) if and only if the  $R$ -linear map*

$$\lambda\theta: E \rightarrow E' \rightarrow k' = E'/\text{rad } E'$$

*is a homomorphism of  $R$ -algebras.*

*Proof.* For each element  $a = \sum_{x \in G} c_x x \in RG$ , let

$$a_H = \sum_{x \in H} c_x x, \quad \text{and} \quad a_{G-H} = \sum_{x \notin H} c_x x.$$

Then  $a = a_H + a_{G-H}$ , and  $a_H \in c(RH)$  whenever  $a \in c(RG)$ . For each  $a \in c(RG)$ , let  $\tau(a) = a_H b'$ , where  $b'$  is the block idempotent in  $RH$  associated with  $B'$ , and set  $B' = RHb'$ . Then  $\tau(a) \in c(B')$ , and we shall prove that the diagram

$$\begin{array}{ccc}
 c(RG) & \xrightarrow{\tau} & c(B') \\
 \alpha \downarrow & & \downarrow \alpha' \\
 E & \xrightarrow{\theta} & E'
 \end{array}
 \tag{58.16}$$

is commutative, where  $\alpha$  and  $\alpha'$  are the isomorphisms defined in (58.13), and  $\theta f = jfi$ , as above, for  $f \in E$ . Let  $a \in c(RG)$ ; then

$$\alpha'(\tau(a)) = (a_H b')_l \quad \text{and} \quad \theta\alpha(a) = ja_l i.$$

Applying these maps to  $t \in B'$ , we have

$$(a_H b')_l t = a_H t \quad \text{and} \quad (ja_l i)(t) = j(at),$$

so it is sufficient to check that  $a_H t = j(at)$ , for all  $t \in B'$ . We have  $at = a_H t + a_{G-H} t$ , and it is easily checked that  $j(a_H t) = a_H t$  while  $j(a_{G-H} t) = 0$ , using the fact that  $RG$  is a free right  $RH$ -module with a basis given by a cross section of  $G/H$ . This proves the commutativity of (58.16).

Now let

$$\psi' : c(RH) \rightarrow c(B')/\text{rad } c(B') = k'$$

be the central character associated with the block  $B'$ . By Definition 58.8, the map  $(\psi')^G$  is given by

$$(\psi')^G(a) = \psi'(a_H b') = a_H b' + \text{rad } c(B'), \quad \text{for } a \in c(kG),$$

and is a central character if and only if this map is a homomorphism of  $R$ -algebras. Since the diagram (58.16) is commutative, this condition is clearly equivalent to the statement that the map

$$\lambda\theta : E \rightarrow k'$$

is a homomorphism of  $R$ -algebras. This completes the proof.

Following Okuyama, we now obtain several module-theoretic interpretations of the Brauer Correspondence. Among other things, these transfer questions about the behavior of defect groups under the Brauer Correspondence to problems about vertices of indecomposable lattices (see also Alperin-Burry [80].)

**(58.17) Proposition.** *Let  $H \leq G$ , and let  $B'$  be a  $p$ -block of  $H$  for which a Brauer correspondent  $(B')^G$  is defined. Then*

$$B' | B_{H \times H},$$

where  $B'$  and  $B$  are the block ideals associated with  $B'$  and  $(B')^G$ , respectively.

*Proof.* We have  $RG = B \oplus I$  for some two-sided ideal  $I$ . Let  $f \in E = \text{End}_{R(G \times G)} RG$  be the projection on  $B$ . Then  $f|_B = \text{id}_B$  and  $f|_I = 0$ . By (58.15),  $\lambda\theta$  is a homomorphism of  $R$ -algebras, so  $\lambda\theta f = 1$  in  $k'$ , since  $f$  is an idempotent in  $E$ . Then  $\theta f = jfi$  is a unit in  $E'$ , because  $E'$  is a local ring. Then the maps

$$fi : B' \rightarrow B \quad \text{and} \quad jf.B \rightarrow B'$$

are  $R(H \times H)$ -homomorphisms, and

$$(jf)(fi) = jf^2i = jfi = \theta f \in E'.$$

Thus  $(jf)(fi)$  is a unit in  $E'$ , so  $B'|B_{H \times H}$ , completing the proof.

**(58.18) Corollary.** *Keep the notation of (58.17), and let  $D'$  be a defect group of the block  $B'$ . Then  $D' \leq_G D$ , where  $D$  is a defect group of  $(B')^G$ .*

*Proof.* The result follows at once from (58.17) and a basic property of vertices (Theorem 19.14), using the interpretation of defect groups as vertices (see (57.22)).

**(58.19) Theorem.** *Let  $H \leq G$ , and let  $B'$  be a  $p$ -block of  $H$  whose corresponding block ideal  $B'$  occurs with multiplicity one in the decomposition of  $(RG)_{H \times H}$  into indecomposable  $R(H \times H)$ -lattices. Then  $(B')^G$  is defined.*

*Proof.* Let  $(RG)_{H \times H} = B' \oplus U$  for some  $R(H \times H)$ -lattice  $U$ . Then for any  $R(H \times H)$ -endomorphisms  $g: B' \rightarrow U$  and  $h: U \rightarrow B'$ , their composition  $hg$  lies in  $\text{rad } E'$ . Otherwise,  $hg$  is an automorphism of  $B'$  since  $E'$  is a local ring, and it follows that  $B'|U$  by (2.3), contradicting the assumption that  $B'$  occurs with multiplicity one in  $(RG)_{H \times H}$ .

We shall prove that the criterion of (58.15) is satisfied, namely that the map  $\lambda\theta: E \rightarrow E'/\text{rad } E'$  is a homomorphism of  $R$ -algebras. The map  $\lambda\theta$  is  $R$ -linear, and we need only check that it is multiplicative. Let  $f_1, f_2 \in E$ ; then we can write

$$f_i = f'_i + f''_i, \quad i = 1, 2,$$

where  $f'_i: RG \rightarrow B'$  and  $f''_i: RG \rightarrow U$  are the  $R(H \times H)$ -endomorphisms of  $RG$  arising from the decomposition  $(RG)_{H \times H} = B' \oplus U$ . Then

$$\theta f_i = j f_i = j f'_i + j f''_i, \quad \text{for } i = 1, 2,$$

and  $j f''_i \in \text{rad } E'$  for  $i = 1, 2$ , since it is the composite of  $R(H \times H)$ -maps from  $B' \rightarrow U$  and  $U \rightarrow B'$ . By the same reasoning, we have

$$\theta(f_1 f_2) \equiv j f'_1 f'_2 i \pmod{\text{rad } E'}$$

and it follows that

$$\theta(f_1 f_2) \equiv (\theta f_1)(\theta f_2) \pmod{\text{rad } E'}.$$

Then  $\lambda\theta$  preserves multiplication, since  $\lambda$  is the natural map from  $E' \rightarrow E'/\text{rad } E'$ , and the result follows.

The preceding discussion yields some useful general conditions for the Brauer correspondence to be defined.

**(58.20) Theorem.** (Brauer [59]). *Let  $D$  be a  $p$ -subgroup of  $G$ , and  $H$  a subgroup such that  $H \geq DC_G(D)$ . Let  $B'$  be a  $p$ -block of  $H$  with defect group  $D'$ . Then the block ideal  $B'$  of  $B'$  occurs with multiplicity one in  $(RG)_{H \times H}$ , and therefore  $(B')^G$  is defined, provided that  $D' \geq D$ .*

*Proof.* By (58.19), it is sufficient to prove that  $B'$  occurs with multiplicity one in  $(RG)_{H \times H}$ . By (57.22),  $\Delta D' \leq H \times H$  is a vertex of the indecomposable  $R(H \times H)$ -lattice  $B'$ . The multiplicity of  $B'$  in  $(RG)_{H \times H}$  is the sum of the multiplicities of  $B'$  in the submodules  $\{R(HyH) : y \in G\}$ , by (58.12i) and the first step of the proof of (58.12). If  $B' \mid R(HyH)$  for some  $y \in G$ , then  $R(HyH)$  is  $(H \times H, Y)$ -projective, where

$$Y = {}^{(y, 1)}\Delta(H \cap {}^{y^{-1}}H)$$

by (58.12), and hence  $\Delta D' \leq_{H \times H} Y$ , since  $\Delta D'$  is a vertex of  $B'$ . An easy computation shows that if  $\Delta D' \leq_{H \times H} Y$ , then  $y \in HC_G(D')H$ , and hence  $y \in H$ , since  $C_G(D') \leq H$  by hypothesis. It follows that  $B' \mid RH$  and  $B' \nmid R(HyH)$  if  $y \notin H$ , completing the proof that  $B'$  occurs with multiplicity one in  $(RG)_{H \times H}$ .

The next result extends part of the Theorem 58.9 to block theory with respect to an arbitrary  $p$ -modular system which is admissible for  $G$ , and gives a straightforward module theoretic description of the Brauer Correspondence.

**(58.21) Theorem** (Alperin [77]). *Let  $D$  be a  $p$ -subgroup of  $G$ , and  $H$  a subgroup satisfying the condition*

$$DC_G(D) \leq H \leq N_G(D).$$

*Then the following statements hold.*

- (i) *The Brauer correspondence  $B' \rightarrow (B')^G$  is defined for all  $p$ -blocks  $B'$  of  $H$ .*
- (ii) *Let  $B'$  be a block ideal in  $RH$ , and  $B$  a block ideal in  $RG$ , associated with the blocks  $B'$  of  $H$  and  $B$  of  $G$ , respectively. Then we have*

$$(B')^G = B \Leftrightarrow B' \mid B_{H \times H}.$$

*Proof.* (i) Let  $B'$  be an arbitrary block of  $H$ , with defect group  $D' \leq H$ . Then  $D \leq D'$  by (58.5) since  $D \trianglelefteq H$ . It follows that  $C_G(D') \leq C_G(D) \leq H$ , using the hypothesis of the Theorem. Then  $D'C_G(D') \leq H$ , and we can apply Brauer's Theorem 58.20 to conclude that  $(B')^G$  is defined.

(ii) First assume that  $B' \mid B_{H \times H}$ . Then  $(B')^G$  is defined, by part (i), and  $B'$  occurs with multiplicity one in  $(RG)_{H \times H}$ . It follows that  $B = (B')^G$ , by (58.17). Conversely,  $B' \mid B_{H \times H}$  if  $B = (B')^G$  by (58.17), completing the proof.

The next theorem gives an interpretation of the Brauer correspondence in terms of vertices of indecomposable lattices (see also the Nagao Decomposition Theorem 59.4 and its consequences, in case  $H \leq N_G(D)$ ).

**(58.22) Theorem.** (Alperin). Let  $D$  be a  $p$ -subgroup of  $G$ , let  $H \leq G$ , and assume that  $DC_G(D) \leq H$ . Let  $N \in \text{Ind } RH$ ,  $M \in \text{Ind } RG$ , and assume further that  $N|M_H$  and  $D \in \text{vtx } N$ . Let  $M$  belong to the  $p$ -block  $B$  of  $G$ . Then  $N$  belongs to a  $p$ -block  $B'$  of  $H$  such that  $(B')^G = B$ .

*Proof.* (See Alperin-Burry [80]). Step 1. We have

$$RG = RH \oplus (\bigoplus_{y \notin H} R(HyH)).$$

Our first assertion is that if  $U|R(HyH)$ , for  $U \in \text{Ind } R(H \times H)$  and  $y \notin H$ , then  $\Delta D \not\leq_{H \times H} \text{vtx } U$ . We begin with the fact that for each  $y \in G$ ,

$$HyH \cong \text{ind}_Y^{H \times H}$$

where

$$Y = \text{Stab}_{H \times H} y = {}^{(y, 1)} \Delta (H \cap {}^{y^{-1}} H)$$

(from §57C). Then  $\Delta D \leq_{H \times H} \text{vtx } U$  and  $U|R(HyH)$  imply that  $\Delta D \leq_{H \times H} Y$ . An easy computation then shows that  $y \in H$  since  $C_G(D) \leq H$ , completing the proof of Step 1.

Step 2. Let  $e$  be the sum of the block idempotents in  $RH$  from blocks corresponding to  $B$  (in the Brauer correspondence) so  $e = 0$  if there are none. In any case,

$$B = eB \oplus (1 - e)B \text{ as } R(H \times H)\text{-modules,}$$

where  $B$  is the block ideal in  $RG$  associated with the given block  $B$ . Since

$$RG = RH + \sum_{y \notin H} R(HyH),$$

we have

$$(1 - e)B|(1 - e)RH \oplus (1 - e) \sum_{y \notin H} R(HyH).$$

By (58.17),  $(1 - e)RH$  is a direct sum of block ideals which are not isomorphic to direct summands of the restriction  $B_{H \times H}$ , or for which the Brauer correspondence is not defined. The vertices of the latter set of block ideals do not contain  $\Delta D$  by (58.20) and (57.22). Therefore  $(1 - e)B$  has no indecomposable  $R(H \times H)$ -summand whose vertex contains  $\Delta D$ , by Step 1.

Step 3. Suppose the theorem is false. Then  $(1 - e)_N = \text{id}_N$ , where  $N$  is the  $RH$ -lattice in the statement of the theorem. We next construct the  $RH$ -lattice  $(1 - e)B \otimes_R N$ , on which  $H$  acts according to the rule

$$h((1 - e)a \otimes n) = (1 - e)hah^{-1} \otimes hn.$$

We shall now prove, under the assumption of Step 3, that  $N|(1-e)B \otimes_R N$  as  $RH$ -lattices. Since  $N|M_H$  by hypothesis, there exists an injection  $i: N \rightarrow M_H$  and a projection  $j: M_H \rightarrow N$ . Define a homomorphism of  $RH$ -modules

$$\varphi: N \rightarrow (1-e)B \otimes_R N$$

by setting

$$\varphi(n) = (1-e)b \otimes n,$$

where  $b$  is the block idempotent in  $B$ . Then define another homomorphism of  $RH$ -modules

$$\psi: (1-e)B \otimes_R N \rightarrow N,$$

where

$$\psi((1-e)a \otimes n) = j((1-e)a \cdot i(n)), \quad \text{for } a \in B.$$

To check that  $\psi$  is an  $RH$ -map, we have

$$\begin{aligned} \psi(h((1-e)a \otimes n)) &= \psi((1-e)hah^{-1} \otimes hn) = j((1-e)hah^{-1} \cdot i(hn)) \\ &= j((1-e)hai(n)) = h(j((1-e)ai(n))) \end{aligned}$$

as required. Using the assumption that  $(1-e)_N = \text{id}_N$ , we obtain

$$\begin{aligned} \psi\varphi(n) &= \psi((1-e)b \otimes n) = j((1-e)bi(n)) \\ &= j((1-e)i(n)) = ji((1-e)n) = jin = n, \end{aligned}$$

proving the assertion of Step 3.

*Step 4.* The two  $H$ -actions on  $B$ , given by

$$h \cdot a = hah^{-1} \quad \text{and} \quad h \cdot a = \Delta(h) \cdot a, \quad a \in B, \quad h \in H,$$

clearly coincide. It follows that  $(1-e)B$  contains no indecomposable  $RH$ -summands whose vertices contain  $D$ , by Step 2. Thus  $(1-e)B$  is a direct sum of  $(H, D_i)$ -projective lattices, for subgroups  $\{D_i\}$  such that  $D \not\leq_H D_i$  for each  $i$ . It follows that the  $RH$ -lattice  $(1-e)B \otimes_R N$  has the same property (see Exercise 6). In particular, no indecomposable  $RH$ -summand of  $(1-e)B \otimes_R N$  has vertex  $D$ , contradicting Step 3, where it was shown that  $N|(1-e)B \otimes_R N$ . Thus we have proved that  $eN = N$ , and hence  $N$  belongs to a block  $B'$  of  $H$  such that  $(B')^G = B$ , as required.

## §58. Exercises

In Exercise 1,  $R$  denotes either a field of characteristic  $p$ , or a complete d.v.r. whose residue field has characteristic  $p$ .

1. Let  $D \trianglelefteq G$ , and let  $b$  be a block idempotent in  $RG$  with defect group  $D$ . Prove that

$$b \equiv \sum \beta_j L_j \pmod{pA_G}, \quad \beta_j \in R,$$

where the  $L_j$  are  $G$ -class sums whose class defect groups satisfy  $D_j = D$  for each  $j$ .

[Hint: See the proof of (58.5).]

2. Let  $k$  be a field, and let  $\varphi: A \rightarrow A'$  be a surjection of f.d. commutative  $k$ -algebras. Prove that  $\varphi$  defines a bijection from the set of all primitive idempotents of  $A$  not contained in the kernel of  $\varphi$  to the set of all primitive idempotents of  $A'$ .

[Hint: An idempotent  $e \in A$  is primitive if and only if  $eA (= eAe)$  is a local  $k$ -algebra. Then show, using the assumption that  $\varphi$  is surjective, that if  $e$  is primitive in  $A$ , then either  $\varphi(e) = 0$  or  $\varphi(e)$  is primitive in  $A'$ . To check that  $\varphi$  defines a bijection, see (56.5).]

In Exercise 3–5,  $(K, R, k)$  denotes a  $p$ -modular system satisfying the conditions stated in the Exercises of §56.

3. Prove the transitivity of the Brauer Correspondence. More precisely, let  $H'' \leq H' \leq G$ , and let  $B''$  be a  $p$ -block of  $H''$  such that  $(B'')^{H'}$  and  $((B'')^{H'})^G$  are defined. Prove that  $((B'')^G)$  is defined, and coincides with the block  $((B'')^{H'})^G$ . (See (58.8).)

4. Let  $D$  be a  $p$ -subgroup of  $G$ , and let  $H = N_G(D)$ . Prove that the Brauer correspondence is defined for each  $p$ -block of  $H$  with defect group  $D$ , and coincides with the bijection of  $p$ -blocks with defect group  $D$  described by the First Main Theorem 58.6.

[Hint: Use (58.7) and (58.11).]

5. Prove that the First Main Theorem 58.6 establishes a bijection from the set of  $p$ -blocks of  $G$  with defect group  $D$  to the set of all  $p$ -blocks of  $H = N_G(D)$  of defect  $d$ , where  $|D| = p^d$ .

6. Let  $H \leq G$ , and let  $R$  be a commutative ring. Let  $N$  be an arbitrary  $RG$ -lattice, and let  $M$  be a  $(G, H)$ -projective  $RG$ -lattice. Prove that the inner tensor product  $M \otimes_R N$  is  $(G, H)$ -projective.

[Hint: Apply (19.2iii) to the endomorphism  $\gamma \otimes 1$  of  $M \otimes N$ , where  $\gamma \in \text{End}_{RH}(M)$  and satisfies (19.2iii).]

## §59. APPLICATIONS OF BLOCKS TO CHARACTER THEORY

Let  $M$  be an indecomposable  $RG$ -lattice, and let  $H$  be a subgroup of  $G$ . The distribution of indecomposable summands of the restriction  $M_H$  among the blocks of  $H$  was examined in §58C (Theorem 58.22). This section begins with another result in this direction, called the Nagao Decomposition, which is proved using the Brauer homomorphism. The result leads to Nagao's proof of Brauer's Second Main Theorem. Most of the applications of block theory to characters, and applications to finite group theory (see §63) involve Brauer's

Second Main Theorem in some way. Other proofs of the theorem were given by Brauer [59], Iizuka [61], and Dade [65].

### §59A. The Nagao Decomposition

In this subsection,  $D$  denotes a  $p$ -subgroup of a finite group  $G$ , and  $H$  a subgroup satisfying

$$(59.1) \quad D \cdot C_G(D) \leq H \leq N_G(D)$$

We let  $(K, R, k)$  be a  $p$ -modular system with  $\text{char } K = 0$  and  $K$  sufficiently large relative to  $G$ ; then  $(K, R, k)$  is admissible for  $G$  and its subgroups. We let

$$\sigma: c(RG) \rightarrow c(RH)$$

denote the Brauer map (58.1) relative to  $D$ . The main result of the subsection is a theorem of Nagao [63] on a decomposition of the restriction  $M_H$  of an arbitrary  $RG$ -lattice  $M$  belonging to a given  $p$ -block  $B$  of  $G$ , in terms of the effect of the Brauer map on the block idempotent in  $B$ . As an application, we obtain a connection between the Green Correspondence of indecomposable lattices (20.8) and the Brauer Correspondence of blocks (§58C). In §59B, we give Nagao's proof of Brauer's Second Main Theorem, which is in application of the Nagao decomposition to character theory.

We shall use the theory of  $G$ -algebras from §57 (also summarized at the beginning of §58A). In particular,  $A$  denotes the  $G$ -algebra  $RG$ . Define

$$A_H = \{a \in A : xa = a \text{ for all } x \in H\},$$

and

$$A_{H/D'} = T_{H/D'}(A_{D'}), \quad \text{for } D' \leq H.$$

We recall that  $A_{H/D'}$  is a two-sided ideal in  $A_H$ , for each subgroup  $D' \leq H$ .

By (57.14), we have

$$(59.2) \quad A_{H/D'} \equiv \sum RL_i (\text{mod } \mathfrak{p} A_H),$$

where the sum is taken over  $H$ -class sums  $\{L_i\}$  in  $A_H$  whose class defect groups  $\{D'_i\}$  satisfy the condition that  $D'_i \leq_H D'$ .

**(59.3) Lemma.** *Let  $\mathfrak{L}$  be an  $H$ -conjugacy class in  $G$ , and assume that  $\mathfrak{L} \not\leq C_G(D)$ . Then the  $H$ -class sum  $L = \sum_{y \in \mathfrak{L}} y$  belongs to  $A_{H/D'}$  for some  $p$ -subgroup  $D' \leq H$  such that  $D \not\leq D'$ .*

*Proof.* Let  $x \in \mathfrak{L} - C_G(D)$ , and let  $D'$  be a Sylow  $p$ -subgroup of  $C_H(x)$ . Then  $D'$  is a class defect group of the  $H$ -class  $\mathfrak{L}$  containing  $x$ , and we have  $L \in A_{H/D'}$  by (59.2). Moreover,  $D \not\leq D'$  since  $x \notin C_G(D)$ , and the proof is completed.

**(59.4) Nagao Decomposition Theorem.** Let  $b$  be a block idempotent in  $RG$ , and let  $M$  be an  $RG$ -lattice such that  $bM = M$ . Then  $b = b_1 + b_2$ , where  $b_1$  and  $b_2$  are either orthogonal idempotents in  $A_H$ , or one of them is zero, and the resulting decomposition

$$M_H = b_1 M \oplus b_2 M$$

of  $M_H$  into  $RH$ -lattices has the following properties:

- (i)  $b_1 M \equiv \sigma(b)M \pmod{pM}$ , and  $b_1 M$  is either zero or a direct sum of indecomposable  $RH$ -lattices belonging to the blocks  $\{B'_i\}$  of  $H$  such that  $(B'_i)^G = B$ .
- (ii)  $b_2 M$  is either zero or a direct sum of indecomposable  $RH$ -lattices whose vertices do not contain  $D$ .

*Proof.* By (58.11), it follows that either  $\sigma b \equiv 0 \pmod{pA_H}$  or  $\sigma b \equiv b' \pmod{pA_H}$ , where

$$b' = \sum_i b'_i,$$

and the  $\{b'_i\}$  are all the block idempotents in  $c(RH)$  belonging to blocks  $\{B'_i\}$  of  $H$  such that  $(B'_i)^G = B$ . Set  $b' = 0$  if  $\sigma b \equiv 0 \pmod{pA_H}$ ; then we have

$$\sigma b \equiv b' \pmod{pA_H}$$

in either case.

Now let  $\mathfrak{C}$  be a conjugacy class in  $G$ , and let  $C = \sum_{x \in \mathfrak{C}} x$  be the class sum supported by  $\mathfrak{C}$ . We may write

$$C = C' + C''$$

where  $C' = \sum_{x \in \mathfrak{C} \cap C(D)} x$  if  $\mathfrak{C} \cap C(D) \neq \emptyset$  and  $C' = 0$  otherwise; then  $C'' = C - C' \in A_H$ , and  $C''$  is supported by  $H$ -class sums containing elements  $x \notin C_G(D)$ . Then  $\sigma C = C'$  by (58.1), and by Lemma 59.3,

$$C'' = C - \sigma C \in \sum_{D'} A_{H/D'},$$

where the sum is taken over  $p$ -subgroups  $D' \leq H$  such that  $D \not\leq D'$ . Since  $b$  is an  $R$ -linear combination of  $G$ -class sums, the preceding remarks imply, by linearity, that

$$(59.5) \quad b - \sigma b \in \sum_{D'} A_{H/D'}$$

where the sum is taken over subgroups  $D' \leq H$  such that  $D \not\leq D'$ , as above.

Now set

$$b_1 = bb', \quad b_2 = b(b - b');$$

then

$$b = b_1 + b_2,$$

and  $b_1$  and  $b_2$  are either orthogonal idempotents or one of them is zero.

Then

$$M = bM = b_1M \oplus b_2M.$$

Moreover,

$$b - \sigma b \equiv b - b' \pmod{\mathfrak{p}A_H},$$

so

$$b_1M = b'M \quad \text{and} \quad b_1M \equiv \sigma(b)M \pmod{\mathfrak{p}M},$$

using the assumption that  $M = bM$ . This completes the proof of (i), since  $b'$  is a sum of block idempotents in  $c(RH)$  with the required properties, by the first part of the proof.

For the proof of (ii), we have

$$b_2 = b(b - b') \equiv b(b - \sigma b) \pmod{\mathfrak{p}A_H}.$$

Then  $b_2 \in \sum_{D \not\leq D'} A_{H/D'} + \mathfrak{p}A_H$  by (59.5), since  $A_{H/D'}$  is a two-sided ideal in  $A_H$  for each subgroup  $D' \leq H$ . Then either  $b_2 = 0$  and there is nothing further to be proved, or  $b_2 = \sum b_j''$ , where  $\{b_j''\}$  are primitive orthogonal idempotents in  $A_H$ . Then, for each  $j$ ,

$$b_j'' = b_2 b_j'' \in \sum_{D \not\leq D'} A_{H/D'} + \mathfrak{p}A_H,$$

again using the fact that  $A_{H/D'}$  is a two-sided ideal for each  $D'$ . By Rosenberg's Lemma (57.8), we obtain

$$b_j'' \in A_{H/D'}$$

for some  $p$ -subgroup  $D' \leq H$  such that  $D \not\leq D'$ . Then  $b_j''M$  is  $(H, D')$ -projective by (57.26), and hence  $b_j''M$  is a direct sum of indecomposable  $RH$ -lattices whose vertices do not contain  $D$ , since they are  $H$ -conjugate to subgroups of  $D'$  and  $D \trianglelefteq H$ . Finally,  $b_2M = \bigoplus_j b_j''M$ , and the proof of part (ii) is complete.

**(59.6) Corollary.** *Let  $M$  be an indecomposable RG-lattice belonging to a block  $B$  of  $G$ , and let  $N$  be an indecomposable RH-lattice such that  $N|M_H$ . Then at least one of the following possibilities occurs.*

(i)  *$N$  belongs to a block  $B'$  of  $H$  with defect group  $D'$  such that*

$$(B')^G = B \quad \text{and} \quad C_G(D') \leq H.$$

(ii)  *$D$  is not contained in any vertex of  $N$ .*

*Proof.* By Theorem 59.4 and the K-S-A Theorem, either  $N|b_1M$  or  $N|b_2M$ . In the first case, part (i) of (59.4) applies, and hence  $N$  belongs to a block  $B'$  of  $H$  such that  $(B')^G = B$ . Since  $H$  satisfies (59.1), we have  $D \trianglelefteq H$ , so  $D \leq D'$  by (58.5), and consequently  $C_G(D') \leq C_G(D) \leq H$ , again using (59.1). If  $N|b_2M$ , then (ii) holds, by part (ii) of (59.4).

**(59.7) Corollary** (Green [78a]). (i) Let  $M \in \text{Ind } RG$ ,  $N \in \text{Ind } RH$ , and assume  $N|M_H$  and  $D \leq D''$  for some vertex  $D''$  of  $N$ . If  $N$  belongs to the  $p$ -block  $B'$  of  $H$ , then  $(B')^G$  is defined, and  $M \in (B')^G$ .

(ii) Let  $N \in \text{Ind } RH$ , and assume  $D \leq D''$  for some vertex  $D''$  of  $N$ . If  $N$  belongs to the block  $B'$  of  $H$ , then  $\text{ind}_H^G N$  contains a summand  $M \in \text{Ind } RG$  such that  $M \in (B')^G$ .

Part (i) follows from Corollary (59.6). Part (ii) follows from part (i), using the fact that there exists  $M \in \text{Ind } RG$  such that

$$M|\text{ind}_H^G N \quad \text{and} \quad N|M_H,$$

by the K-S-A Theorem.

The next result gives a connection between the Brauer Correspondence and the Green Correspondence (20.8) (see also (58.22).) We first restate (20.8), for convenient reference.

**(59.8) Green Correspondence.** Let  $H = N_G(D)$ , for a  $p$ -subgroup  $D \leq G$ . There exists a bijection from the set of isomorphism classes of indecomposable  $RG$ -lattices  $M$  with vertex  $=_G D$ , to the set of isomorphism classes of indecomposable  $RH$ -lattices  $N$  with vertex  $D$ . Two lattices  $M \in \text{Ind } RG$  and  $N \in \text{Ind } RH$  correspond to each other if and only if either of the following conditions hold:

$$\text{ind}_H^G N = M \oplus X \quad \text{or} \quad M_H = N \oplus Y,$$

where the “error” term  $X$  is a direct sum of indecomposable  $RG$ -lattices whose vertices are conjugate to proper subgroups of  $D$ , and the “error” term  $Y$  has a similar property.

We now have

**(59.9) Theorem.** Let  $H = N_G(D)$ , and let  $M \in \text{Ind } RG$  and  $N \in \text{Ind } RH$  both have vertex  $D$ . Assume that  $M \leftrightarrow N$  in the Green Correspondence (59.8). Then  $M$  and  $N$  belong to blocks  $B$  of  $G$  and  $B'$  of  $H$ , respectively, which are Brauer correspondents:  $B = (B')^G$ .

*Proof.* Assume  $M \in B$ , for a  $p$ -block  $B$  of  $G$ . Then  $N|M_H$  by (59.8), and  $N$  has vertex  $D$ . If  $N \in B'$ , for a block  $B'$  of  $H$ , then  $(B')^G = B$  by (59.7i), since  $N$  has vertex  $D$ .

We conclude this subsection with a characterization of the defect group of a block in terms of the vertices of indecomposable lattices belonging to the block. By (57.27), we have  $D' \leq_G D$ , for  $M \in B$ , where  $M$  is an indecomposable  $RG$ -lattice with vertex  $D'$ , and  $B$  is a block of  $G$  with defect group  $D$ .

**(59.10) Theorem (Hamernik).** *Let  $B$  be a block of  $G$  with defect group  $D$ . Then there exists an indecomposable  $RG$ -lattice  $M$  such that  $M \in B$  and  $D \in \text{vtx } M$ .*

*Proof (Alperin-Burry [80]).* Let  $H = N_G(D)$ . By Brauer's First Main Theorem (58.6) and Theorem (58.9), it follows that  $B = (B')^G$  for a  $p$ -block  $B'$  of  $H$  with defect group  $D$ . Let  $b'$  be the block idempotent in  $B'$ . Since the kernel of the natural map  $\tau: RH \rightarrow R(H/D)$  is contained in  $\text{rad } RH$  (by (5.26)),  $\tau(b') \neq 0$ , and there exists an indecomposable projective  $R(H/D)$ -module  $N$  such that  $\tau(b') \neq 0$ . Then  $N$  can be viewed as an  $RH$ -module, and  $N \in B'$  since  $b'N \neq 0$ . We first prove that  $D \in \text{vtx } N$ . Since  $N \in \mathcal{P}(R(H/D))$ , it follows that  $N$  is  $(H, D)$ -projective, by Gaschütz's criterion (19.2). Therefore  $D' \leq_H D$ , for any vertex  $D'$  of  $N$ . On the other hand,  $D$  acts trivially on  $N$ , so  $N_D$  is a direct sum of indecomposable  $RD$ -lattices all having vertex  $D$ , by (57.34). It follows that  $N$  also has vertex  $D$ , by (57.28).

Now let  $M \in \text{Ind } RG$  correspond to  $N$  by (59.8). Then  $D \in \text{vtx } M$ , and  $M \in (B')^G = B$  by Theorem (59.9). This completes the proof.

## §59B. Brauer's Second Main Theorem

In this subsection, we apply the Nagao Decomposition (59.4) to character theory. As in §59A, we let  $(K, R, k)$  denote a  $p$ -modular system such that  $\text{char } K = 0$  and  $K$  is sufficiently large relative to  $G$ . We also assume that  $R$  is complete in the  $p$ -adic topology, with a perfect residue field  $k$ . Then  $(K, R, k)$  is admissible for  $G$  and its subgroups, and the hypotheses of Green's theorem on zeros of characters (19.27) are satisfied.

Our objective is a theorem of Brauer [59] (see (59.14) and (59.17)) which gives the character values  $\zeta^i(x)$ , for  $\zeta^i \in \text{Irr } G$  and  $x \in G$ , in terms of the values  $\{\chi^j(x)\}$ , for certain irreducible characters  $\{\chi^j\}$  of the centralizer  $C_G(u)$ , where  $u$  is the  $p$ -part of  $x$ . The crucial point is that the characters  $\{\chi^j\}$  are taken only from those blocks of  $C_G(u)$  which are Brauer correspondents of the block of  $G$  containing  $\zeta^i$ . Most of the applications of block theory to finite groups, including those discussed later in this chapter, involve this theorem in some way.

We first recall (19.27).

**(59.11) Green's Theorem on Zeros of Characters.** *Let  $D$  be a  $p$ -subgroup of  $G$ , let  $D \leq H \leq G$ , and let  $M$  be an  $(H, D)$ -projective  $RH$ -lattice. Then for every element  $x \in H$  whose  $p$ -part is not  $H$ -conjugate to an element of  $D$ , we have*

$$\text{Tr}(x, M) = 0.$$

*In other words, the  $K$ -character of  $H$  afforded by  $K \otimes_R M$  vanishes at  $x$ .*

Using (59.11), we next obtain the character-theoretic version of the Nagao Decomposition.

**(59.12) Theorem (Nagao).** *Let  $b$  be a block idempotent in  $RG$ , and let  $M$  be an  $RG$ -lattice such that  $bM = M$ . For  $x \in G$ , let  $u$  be the  $p$ -part of  $x$ , and set  $D = \langle u \rangle$  and  $H = C_G(u) = C_G(D)$ , so that the pair of subgroups  $\{D, H\}$  satisfies (59.1). Let*

$$M_H = b_1 M \oplus b_2 M$$

*be the Nagao Decomposition (59.4) of the restriction of  $M$  to  $H$ . Then*

$$\mathrm{Tr}(x, M) = \mathrm{Tr}(x, b_1 M).$$

*In other words, if  $\chi$  and  $\chi_1$  are the  $K$ -characters of  $G$  and  $H$  afforded by  $K \otimes_R M$  and  $K \otimes_R b_1 M$  respectively, then*

$$\chi(x) = \chi_1(x).$$

*Proof.* Since  $x \in H$  and  $b_1 M$  and  $b_2 M$  are  $RH$ -sublattices of  $M_H$ , we have

$$\mathrm{Tr}(x, M) = \mathrm{Tr}(x, b_1 M) + \mathrm{Tr}(x, b_2 M),$$

so it is sufficient to prove that  $\mathrm{Tr}(x, b_2 M) = 0$ . Let  $N$  be an indecomposable  $RH$ -lattice such that  $N|b_2 M$ , and let  $D'$  be a vertex of  $N$ . Then  $N$  is  $(H, D')$ -projective, and  $D \not\leq D'$  by Theorem 59.4ii. Since  $D = \langle u \rangle$  and  $H = C_G(u)$ , it follows that  $u$  is not  $H$ -conjugate to an element of  $D'$ . Since  $u$  is the  $p$ -part of  $x$ , we can apply (59.11) to obtain  $\mathrm{Tr}(x, N) = 0$ . But  $N$  is an arbitrary  $RH$ -component of  $b_2 M$ , so we obtain  $\mathrm{Tr}(x, b_2 M) = 0$ , as required.

We next introduce some notation needed for the statement of Brauer's Theorem. Let  $\zeta \in \mathrm{Irr} G$ , and let  $H \leq G$ . Then we have

$$(59.13) \quad \zeta|_H = \sum_{B'} (\zeta|_H)_{B'},$$

where the sum is taken over the  $p$ -blocks  $B'$  of  $H$ , and  $(\zeta|_H)_{B'}$  is the contribution to  $\zeta|_H$  from irreducible characters of  $H$  belonging to the block  $B'$ .

**(59.14) Brauer's Second Main Theorem (First Form).** *Let  $x \in G$ , and set  $H = C_G(u)$ , where  $u$  is the  $p$ -part of  $x$ . Let  $\zeta$  be an irreducible  $K$ -character of  $G$  belonging to a  $p$ -block  $B$  of  $G$ , and let  $B'$  range over the  $p$ -blocks of  $H$ . Then*

$$\zeta_H(x) = \sum_{B'} (\zeta_H)_{B'}(x),$$

*where the sum extends over all  $B'$  for which  $(B')^G = B$ . Further,*

$$(\zeta_H)_{B'}(x) = 0 \quad \text{whenever } (B')^G \neq B.$$

*Proof.* Let  $M$  be an  $RG$ -lattice such that  $K \otimes_R M$  affords  $\zeta$ . Then  $bM = M$ , where  $b$  is the block idempotent in  $B$ . Let

$$M_H = b_1 M \oplus b_2 M$$

be the Nagao Decomposition (59.4) of  $M_H$ . By Theorem 59.12,

$$\mathrm{Tr}(x, M) = \mathrm{Tr}(x, b_1 M).$$

By Theorem 59.4,  $b_1 M$  is either zero or a direct sum of indecomposable  $RH$ -lattices belonging to the blocks  $\{B'\}$  of  $H$  such that  $(B')^G = B$ . Upon tensoring these with  $K$  and computing the characters, we obtain

$$\zeta|_H(x) = \sum_{(B')^G = B} (\zeta|_H)_{B'}(x).$$

It remains to show that  $(\zeta|_H)_{B'}(x) = 0$  if  $B'$  is not a Brauer correspondent of  $B$ . For such a block, it follows from the Nagao Decomposition (59.4) that  $(\zeta|_H)_{B'}$  is afforded by an  $RH$ -summand of  $b_2 M$ . By the proof of Theorem 59.12, we obtain  $(\zeta|_H)_{B'}(x) = 0$  for all such blocks  $B'$  for which  $(B')^G \neq B$ , completing the proof.

The next result is Brauer's original version of the Second Main Theorem, and requires some preliminary discussion. Let  $u$  be a fixed  $p$ -element in  $G$ , and let  $H = C_G(u)$ . Let

$$\mathrm{Irr} G = \{\zeta^1, \dots, \zeta^s\}, \quad \mathrm{Irr} H = \{\chi^1, \dots, \chi^{s'}\},$$

$\{\xi^1, \dots, \xi^{r'}\}$  = the irreducible Brauer characters of  $H$ .

**(59.15) Proposition.** *Keeping the above notation, there exist uniquely determined algebraic integers  $\{d_{ij}^u\}$  in  $K$ , depending on  $\zeta^i$ ,  $\xi^j$ , and  $u$  as above, such that*

$$\zeta^i(xu) = \sum_{j=1}^{r'} d_{ij}^u \xi^j(x)$$

for all  $p'$ -elements  $x \in H$ .

*Proof.* For each  $i$ , the restriction  $\zeta^i|_H$  is a  $\mathbb{Z}$ -linear combination of the characters  $\chi^j \in \mathrm{Irr} H$ , so we have

$$\zeta^i|_H = \sum_{j=1}^{s'} q_{ij} \chi^j, \quad q_{ij} \in \mathbb{Z}, \quad 1 \leq i \leq s.$$

The decomposition map for the group  $H$  yields formulas

$$\chi^j = \sum_{l=1}^{r'} d'_{jl} \xi^l \quad \text{on } H_{p'},$$

where  $(d'_{jl})^{s' \times r'}$  is the decomposition matrix for  $H$ . Now let  $x \in H$  be a  $p'$ -element, and let  $\mathbf{T}_j$  be a matrix representation affording  $\chi^j$ ,  $1 \leq j \leq s'$ . Since  $u$  belongs to the center of  $H$ , we have, by (9.31),

$$\mathbf{T}_j(u) = \varepsilon_j \mathbf{I}, \quad \text{where } \varepsilon_j = \chi^j(u)/\chi^j(1) \in \text{alg. int. } K.$$

Then

$$\mathbf{T}_j(xu) = \varepsilon_j \mathbf{T}_j(x)$$

and hence  $\chi^j(xu) = \varepsilon_j \chi^j(x)$ . Upon setting

$$d_{il}^u = \sum_{j=1}^{s'} q_{ij} \varepsilon_j d'_{jl}, \quad \text{for } 1 \leq i \leq s, \quad 1 \leq l \leq r',$$

and substituting in the preceding formulas, we obtain the desired result. The uniqueness of the elements  $\{d_{il}^u\}$  follows from the linear independence of the Brauer characters  $\{\xi^j\}$  (see (17.9)).

Note that in case  $u = 1$ , the algebraic integers  $d_{ij}^1$  are all in  $\mathbb{Z}$ , and are simply the usual decomposition numbers for the group  $G$ .

**(59.16) Definition.** The algebraic integers  $\{d_{ij}^u\}$  defined by (59.15) for each  $p$ -element  $u \in G$  are called the *generalized decomposition numbers* of  $G$ .

We can now state:

**(59.17) Brauer's Second Main Theorem (Second Form).** Let  $\zeta^i \in \text{Irr } G$  be a character of  $G$  belonging to a  $p$ -block  $B$ . Let  $u$  be a  $p$ -element of  $G$ , and set  $H = C_G(u)$ . Then the generalized decomposition number  $d_{ij}^u = 0$  unless the irreducible Brauer character  $\xi^j$  of  $H$  belongs to a  $p$ -block  $B'$  of  $H$  such that  $(B')^G = B$ .

*Proof.* By Theorem (59.14), we have

$$\zeta^i(xu) = \sum_j q_{ij} \chi^j(xu)$$

for each  $p$ -element  $x \in H$ , where the sum is taken over all irreducible  $K$ -characters  $\{\chi^j\}$  of  $H$  belonging to  $p$ -blocks  $\{B'_l\}$  of  $H$  such that  $(B'_l)^G = B$ . The preceding formulas, combined with the definition of the generalized decomposition numbers, yield the formula

$$\zeta^i(xu) = \sum_l d_{ij}^u \xi^j(x), \quad \text{for } x \in H_{p'},$$

where the sum is taken over irreducible Brauer characters  $\{\xi^j\}$  of  $H$ , belonging to  $p$ -blocks  $B'_l$  such that  $(B'_l)^G = B$ . Since the Brauer characters  $\{\xi^j\}$  are linearly independent on  $H_{p'}$ , it follows that  $d_{ij}^u = 0$  for all Brauer characters  $\xi^j$  belonging to  $p$ -blocks  $B'$  of  $H$  such that  $(B')^G \neq B$ , completing the proof.

### §59. Exercise

1. (*Alperin*). Use (58.22) to obtain the following strengthened version of (59.9). Let  $D$  be a  $p$ -subgroup of  $G$ , and let  $H$  be a subgroup such that  $H \geq N_G(D)$ . Let  $M \in \text{Ind } RG$ ,  $N \in \text{Ind } RH$ , and assume that both  $M$  and  $N$  have vertex  $D$ . Let  $M$  belong to the  $p$ -block  $B$  of  $G$ , and  $N$  to the  $p$ -block  $B'$  of  $H$ . Prove that if  $M \leftrightarrow N$  according to the Green Correspondence, then  $B = (B')^G$ .

## §60. *p*-SECTIONS AND CHARACTERS IN BLOCKS

### §60A. Block Orthogonality and *p*-Sections

We continue the study of characters in blocks, begun in §59A, with some orthogonality relations involving blocks of characters and  $p$ -sections. These results, which are due to Brauer, often provide a practical method for distributing the irreducible characters into  $p$ -blocks, using information about the character table, in cases where it would be difficult to test the congruence relations (56.24). Some applications are given in §§60B and C.

As in §59A, we fix a  $p$ -modular system  $(K, R, k)$  such that  $\text{char } K = 0$ ,  $K$  is sufficiently large relative to  $G$ ,  $R$  is a complete d.v.r. with maximal ideal  $\mathfrak{p}$  and quotient field  $K$ , and  $k = R/\mathfrak{p}$ , a perfect field of characteristic  $p$ .

We set

$$\text{Irr } G = \{\zeta^1 = 1_G, \dots, \zeta^s\}$$

and  $\{B_1, \dots, B_t\}$  the  $p$ -blocks of  $G$ , defined by block idempotents  $\{b_1, \dots, b_t\}$  in  $RG$ , with  $B_1$  the principal block, containing  $\zeta^1$ .

**(60.1) Definition.** Let  $U$  denote the set of all  $p$ -elements in  $G$ . Each element  $u \in U$  defines a  $p$ -section  $X = X(u)$ , consisting of all elements  $x \in G$  whose  $p$ -part is conjugate to  $u$ .

An equivalence relation may be defined on  $G$ , putting  $x$  equivalent to  $y$  if and only if the  $p$ -parts of  $x$  and  $y$  are conjugate in  $G$ . The  $p$ -sections are clearly the equivalence classes in  $G$  for this equivalence relation. It is also clear that each  $p$ -section is a union of conjugacy classes. One  $p$ -section has already been used extensively, namely the set  $G_p$ , consisting of all  $p'$ -elements of  $G$ .

The first result will be called the theorem on *p*-section orthogonality.

**(60.2) Theorem (Brauer).** Let  $B_j$  be a  $p$ -block of  $G$ . Then

$$\sum_{\zeta^i \in B_j} \zeta^i(x) \zeta^i(y^{-1}) = 0, \quad \text{for } x, y \in G,$$

unless  $x$  and  $y$  belong to the same  $p$ -section.

*Proof.* (Green [62a]). We shall apply Green's Theorem on Zeros of Characters 59.11. Let  $b_j \in RG$  be the block idempotent associated with  $B_j$ , and let  $D_j$  be a defect group of  $B_j$ . By Proposition 57.22,  $\Delta D_j = \{(d, d) : d \in D_j\}$  is a vertex of the indecomposable  $R(G \times G)$ -lattice  $RGb_j \subseteq RG$ , under the usual action of  $G \times G$  on  $RG$ . Then  $RGb_j$  is  $(G \times G, \Delta D_j)$ -projective. Now let  $x, y \in G$ , and let  $u, v$  be the  $p$ -parts of  $x$  and  $y$ , respectively. Then the  $p$ -part of  $(x, y) \in G \times G$  is  $(u, v)$ . If  $x$  and  $y$  belong to different  $p$ -sections, then  $u \neq_G v$ , and hence  $(u, v)$  is not conjugate in  $G \times G$  to an element of  $\Delta D_j$ . Thus we obtain

$$\mathrm{Tr}((x, y), RGb_j) = 0,$$

by Theorem 59.11.

The proof is completed as follows. Since  $KGb_j = K \otimes_R RGb_j$ , we have

$$\mathrm{Tr}((x, y), RGb_j) = \mathrm{Tr}((x, y), KGb_j) = 0.$$

Moreover,

$$KGb_j = \sum_{\zeta^i \in B_j} KGe_i,$$

where  $e_i$  is the central primitive idempotent in  $KG$  corresponding to  $\zeta^i$  (see (56.25)). The two-sided ideals  $KGe_i$  are stable under the action of  $(x, y) \in G \times G$ , so it is sufficient to prove that for each irreducible character  $\zeta^i$ , and  $(x, y) \in G \times G$ ,

$$\mathrm{Tr}((x, y), KGe_i) = \zeta^i(x)\zeta^i(y^{-1}).$$

This is a nice problem in character theory, and is left to the reader. This completes the proof of the theorem.

**Remarks.** The preceding result includes Lemma 56.38 as a special case. The proofs we have given for the two results are quite different. The proof of (56.38) is based on calculations with Brauer characters and depends on the invertibility of the Brauer character table matrix  $\Phi$ , while the proof of (60.2) uses the theory of relatively projective modules and Green's Theorem on Zeros of Characters.

Brauer's Theorem is closely related to the Second Orthogonality Theorem 9.26. By Theorem 9.26, any two distinct columns of the character table matrix  $Z$  in (9.25) are orthogonal. Brauer's theorem asserts that the parts of two distinct columns arising from characters in a single  $p$ -block are orthogonal, provided the columns are defined by conjugacy classes belonging to different  $p$ -sections.

We turn now to another connection between blocks of characters and  $p$ -sections, based on Brauer's Second Main Theorem. We first introduce some notation. Let

$$\alpha = \sum_{i=1}^s a_i \zeta^i, \quad a_i \in K,$$

be an arbitrary class function in  $\text{cf}_K G$ . For each block  $B_j$ , define

$$\alpha_{B_j} = \sum_{\zeta^i \in B_j} a_i \zeta^i.$$

We then have:

**(60.3) Theorem.** *Let  $\alpha \in \text{cf}_K G$ , and suppose that  $\alpha$  vanishes on a given  $p$ -section  $X$ . Then  $\alpha_{B_j}$  vanishes on  $X$ , for each  $p$ -block  $B_j$ ,  $1 \leq j \leq t$ . In other words, if a class function vanishes on a  $p$ -section, then it vanishes block by block.*

*Proof* (Feit [82]). Let  $\alpha = \sum_{i=1}^s a_i \zeta^i$ , for  $a_i \in K$ , and let  $u$  be a  $p$ -element in the  $p$ -section  $X$ . Set  $H = C_G(u)$ . Then by assumption,  $\alpha(su) = 0$  for all  $s \in H_{p'}$ . Using Proposition 59.15, we obtain

$$\alpha(su) = \sum_{j=1}^{r'} \left( \sum_{i=1}^s a_i d_{ij}^u \right) \xi^j(s) = 0, \quad \text{for all } s \in H_{p'},$$

where  $\{\xi^1, \dots, \xi^{r'}\}$  are the irreducible Brauer characters of  $H$ , and the  $\{d_{ij}^u\}$  are the generalized decomposition numbers. Since the irreducible Brauer characters of  $H$  are linearly independent on  $H_{p'}$  (see (17.9)), it follows that

$$(60.4) \quad \sum_{i=1}^s a_i d_{ij}^u = 0 \quad \text{for } j = 1, \dots, r'.$$

Now let  $B$  be a fixed  $p$ -block of  $G$ . By the second form of Brauer's Second Main Theorem 59.17, we know that  $d_{ij}^u \neq 0$  for  $\zeta^i \in B$  only if  $\xi^j$  belongs to a block  $B'$  of  $H$  such that  $(B')^G = B$ . It follows easily from this result and (60.4) that

$$\sum_{\zeta^i \in B} a_i d_{ij}^u = 0 \quad \text{for } j = 1, \dots, r'.$$

Upon substituting back in the formula for  $\alpha(su)$ , we obtain

$$\alpha(su) = \sum_{j=1}^{r'} \left( \sum_{\zeta^i \in B} a_i d_{ij}^u \right) \xi^j(s) = 0$$

for all  $s \in H_{p'}$  and hence

$$\alpha_B(su) = 0 \quad \text{for all } s \in H_{p'}.$$

Since every element in the given  $p$ -section  $X$  is conjugate to  $su$  for some  $s \in H_{p'}$ , we have shown that  $\alpha_B$  vanishes on  $X$ , for each block  $B$ , as required.

## §60B. Determination of the Principal Block Using Block Orthogonality

We shall apply the results on block orthogonality (§60A) to determine the principal block in certain types of finite groups. In the rest of this subsection we assume:

**(60.5) Hypothesis.** *G is a finite group with a cyclic Sylow p-subgroup D satisfying the conditions*

- (i)  $C_G(D) = D$  (*D is self-centralizing*)
- (ii)  $D^*$  is a T.I. set with normalizer  $H = N_G(D)$ , where  $D^* = D - \{1\}$  (see (14.16)).

Examples of groups satisfying (60.5) were given in §20B; they include the infinite family of finite simple groups  $\{PSL_2(\mathbb{F}_p) : p \geq 5\}$ .

The characters of finite groups satisfying (60.5) were determined in §20B, and we begin by recalling some concepts and results from §14C and §20B.

**(60.6) Proposition.** *Let G be a finite group satisfying (60.5). Then the following statements hold.*

- (i) *For all  $x \in D^*$ ,  $C_G(x) = D$  (so D is an SA-subgroup<sup>†</sup>).*
- (ii) *The normalizer  $H = N_G(D)$  is a Frobenius group with Frobenius kernel D.*
- (iii)  *$H \cong D \rtimes A$ , where A is an abelian group whose order divides  $p - 1$ .*

*Proof.* (i) Let  $z \in C_G(x)$  for  $x \in D^*$ , and assume for the moment that  $z \notin D$ . We first observe that  $H/D = N_G(D)/C_G(D)$ , and is isomorphic to a subgroup of  $\text{Aut } D$ . The only automorphisms  $\alpha \neq 1$  of a cyclic  $p$ -group  $D$  having nontrivial fixed points are those of order divisible by  $p$ , and these do not arise from elements of  $H$  since  $D$  is a Sylow  $p$ -subgroup of  $G$ . Thus we may assume  $z \notin H$ . In that case,  ${}^zD \neq D$  and  $x \in D \cap {}^zD$ , contradicting the assumption that  $D^*$  is a T.I. set. The statement (ii) follows from (i), by (14.17i). The factorization of  $H$  given in (iii) follows from (ii), while the properties of  $A$  are clear, since  $A \cong N_G(D)/C_G(D)$  by (60.5), and  $N_G(D)/C_G(D)$  is isomorphic to a subgroup of the automorphism group of the cyclic group  $D$ .

We shall determine the structure of the principal block in groups  $G$  satisfying (60.5). In case  $|D| = p$ , the results are due to Brauer [41], and, in the general case, to Thompson [67b]. These ideas led to Dade's definitive work on the structure of blocks with cyclic defect groups (see Dade [66], Feit [82, VII], and §62).

The results we need from §20B are as follows. Let  $H = DA$  as in (60.6iii), and put

$$m = |D| = p^d, \quad e = |H/D| = |A|, \quad \text{and } n = (m - 1)/e.$$

We shall assume, in the rest of the subsection, that  $n \geq 2$ . By (14.17), the set  $D^*$  is the union of exactly  $n$  special classes in  $H$ .

<sup>†</sup>See Volume I, p. 354.

The characters are taken in a field  $K$  such that  $\text{char } K = 0$  and  $K$  is sufficiently large relative to  $G$ . When appropriate we also assume that  $K$  is part of a  $p$ -modular system  $(K, R, k)$ .

Since  $H$  is a Frobenius group with Frobenius kernel  $D$ ,  $H$  has exactly  $e$  distinct irreducible nonlinear characters  $\{\psi_1, \dots, \psi_n\}$ , all of degree  $e$ , which are induced from nontrivial linear characters of  $D$ . By (14.17iv), a  $\mathbb{Z}$ -basis for the virtual characters of  $H$  vanishing off the special classes is given by

$$\lambda_i = \psi_i - \psi_n, \quad 1 \leq i \leq n-1,$$

together with any one additional character of the form

$$(1_D)^H - \psi_i, \quad 1 \leq i \leq n.$$

By (20.20) we have

$$\text{Irr } G = \{1_G, \zeta_1, \dots, \zeta_n; \theta_1, \dots, \theta_f; \chi_1, \dots, \chi_h\}.$$

There exists a sign  $\varepsilon = \pm 1$  and multiplicities  $a$  and  $c_l \neq 0$ ,  $1 \leq l \leq f$ , such that

$$(\lambda_i)^G = (\psi_i - \psi_n)^G = \varepsilon(\zeta_i - \zeta_n), \quad 1 \leq i \leq n-1$$

and

$$\Gamma_i = ((1_D)^H - \psi_i)^G = 1_G - \varepsilon\zeta_i + a \sum_{j=1}^n \zeta_j + \sum_{l=1}^f c_l \theta_l, \quad 1 \leq i \leq n.$$

The constants  $\varepsilon, a$ , and  $\{c_l\}$  are independent of  $i$ ,  $1 \leq i \leq n$ , and satisfy the conditions:

$$\begin{aligned} e &= a^2(n-1) + (a-\varepsilon)^2 + \sum_{l=1}^f c_l^2, \\ a &= 0, \text{ or } \varepsilon, \quad |c_l| = 1, \quad 1 \leq l \leq f, \quad \text{and} \quad f = e-1. \end{aligned}$$

The characters  $\{\zeta_1, \dots, \zeta_n\}$  are called *exceptional characters* (relative to  $D$ ), and the characters  $\{\theta_1, \dots, \theta_f; \chi_1, \dots, \chi_h\}$  are called *nonexceptional*, and are arranged so that the first  $f$  characters  $\{\theta_j\}$  appear with nonzero multiplicity in the virtual characters  $\Gamma_i$ ,  $1 \leq i \leq n$ , while the remaining ones  $\{\chi_j\}$  have the property that  $(\chi_j, \Gamma_i) = 0$  for all  $j$ ,  $1 \leq j \leq h$ , and  $i$ ,  $1 \leq i \leq n$ . We then have (see (20.20)).

**(60.7) Theorem.** *Let  $n = (m-1)/e \geq 2$ . Then the following statements hold.*

(i) *The exceptional characters  $\{\zeta_i\}$  have the same degree, which is prime to  $p$ . The nonexceptional characters  $\{\theta_j: 1 \leq j \leq f\}$  have degrees satisfying  $\theta_j(1) \equiv \pm 1 \pmod{p}$ , while the degrees of the remaining characters  $\{\chi_j\}$  are all divisible by  $|D|$ .*

(ii) Up to sign, the values of the  $\{\zeta_i\}$  agree with the values of the  $\{\psi_i\}$  on the special classes. More precisely, we have

$$\zeta_i|_{D^*} = \varepsilon \psi_i|_{D^*}, \quad 1 \leq i \leq n.$$

The values of the nonexceptional characters  $\{\theta_j\}$  on the elements of  $D^*$  are all  $\pm 1$ , while the nonexceptional characters  $\{\chi_j\}$  vanish on  $D^*$ .

(iii) The exceptional characters agree on the elements of  $G_{p'}$ :

$$\zeta_i(x) = \zeta_j(x), \quad \text{for all } x \in G_{p'}, \quad 1 \leq i, j \leq n.$$

The values of the characters  $\{\theta_j\}$  and  $\{\zeta_i\}$  are related as follows:

$$\delta \zeta_1(x) = 1 + \sum_{i=1}^f \delta_i \theta_i(x) \quad \text{for all } x \in G_{p'},$$

where  $\{\delta, \delta_1, \dots, \delta_f\}$  are all  $\pm 1$ , and are independent of  $x \in G_{p'}$ .

Here is the main result of this subsection.

**(60.8) Theorem.** Let  $G$  be a finite group satisfying (60.5). Then the following statements hold.

(i) The principal block  $B_1$  of  $G$  consists of the irreducible characters  $\{1_G, \zeta_1, \dots, \zeta_n; \theta_1, \dots, \theta_f\}$  (in the notation of (60.7)). These are precisely the irreducible characters of  $G$  whose degrees are prime to  $p$ .

(ii) The decomposition numbers for irreducible characters in  $B_1$  are all either 0 or 1.

(iii) Each nonprincipal block of  $G$  has defect zero, and contains a single nonexceptional irreducible character  $\chi_j$ , for  $1 \leq j \leq h$ .

Assuming the truth of part (i), the rest of the theorem is a consequence of earlier results. In fact, (ii) follows from Theorem 20.20v, while (iii) is a consequence of (60.7i) and (56.32). Before giving the proof of part (i), we establish some preliminary results.

**(60.9) Lemma.** Let  $D$  be a cyclic Sylow  $p$ -subgroup of  $G$ , satisfying (60.5). Then the subgroup  $H = N_G(D)$  has only one  $p$ -block.

*Proof.* Let  $(K, R, k)$  be a  $p$ -modular system, with  $\text{char } K = 0$  and  $K$  sufficiently large. Let  $B$  be an arbitrary  $p$ -block of  $H$ , and  $b$  the corresponding block idempotent in  $c(RH)$ . Since  $D$  is a normal  $p$ -subgroup of  $H$ , we have  $b \in RC_H(D) \pmod{p}$  by (58.5), and hence

$$b \in RD \pmod{p},$$

(because of the hypothesis (60.5)). Then  $b \equiv 1 \pmod{p}$  since  $RD$  is an indecomposable  $R$ -algebra and contains only one idempotent. The central character  $\omega$  of  $RH$  associated with the trivial character of  $H$  therefore satisfies

$$\bar{\omega}(b) = \bar{\omega}(1) = 1,$$

and it follows that  $B$  is the principal block, by (56.19).

Another way of looking at it is to note that, for  $b$  as above, the Brauer map  $\sigma: c(RH) \rightarrow c(RD) = RD$  satisfies the condition  $\sigma(b) \equiv b \pmod{p}$ . Since  $b$  belongs to the principal block of  $RD$ , the preceding formula shows that  $b$  also belongs to the principal block of  $RH$ , by (58.11) and (58.10).

**(60.10) Lemma.** *Let  $D^*$  and  $D^{*G}$  denote the union of special classes in  $H$  and  $G$ , respectively, associated with  $D^* = D - \{1\}$ . Then  $D^*$  and  $D^{*G}$  are the complements, in  $H$  and  $G$  respectively, of the  $p$ -sections  $H_{p'}$  and  $G_{p'}$ .*

The proof is immediate from the definitions. The point of (60.10) is that the virtual characters (of  $H$  or  $G$ ) vanishing off the special classes coincide with the virtual characters vanishing on certain  $p$ -sections.

**(60.11) Lemma.** *Let  $G$  be a finite group satisfying (60.5), and let  $\xi$  be a class function on  $G$  vanishing off  $D^{*G}$ . Then  $\xi = \xi_{B_1}$ , that is,  $\xi$  is a linear combination of irreducible characters in the principal block.*

*Proof.* Since  $\xi$  vanishes off  $D^{*G}$ , it vanishes on the  $p$ -section  $G_{p'}$ , by (60.10). By (59.13) we have

$$\xi = \sum \xi_{B_i},$$

and each  $\xi_{B_i}$  vanishes off  $D^{*G}$  by (60.3). Let  $B_i$  be a nonprincipal  $p$ -block of  $G$ , and suppose  $\xi_{B_i}(x) \neq 0$  for  $x \in D^*$ . Then by the first version of Brauer's Second Main Theorem 59.14, we have

$$\xi_{B_i}(x) = \sum_{(B'_j)^G = B_i} (\xi|_H)_{B'_j}(x) \neq 0$$

where the sum is taken over blocks  $\{B'_j\}$  of  $H$  which correspond to  $B_i$ . But this is impossible by Lemma 60.9, since  $H$  has only one block, and that block is the Brauer correspondent of the principal block of  $G$ . Thus  $\xi_{B_i} = 0$  if  $B_i$  is not the principal block, as required.

**(60.12) Corollary.** *Let  $\zeta \in \text{Irr } G$ , and assume  $(\zeta, \psi^G) \neq 0$  for some class function  $\psi$  on  $H$  vanishing off  $D^*$ . Then  $\zeta \in B_1$ .*

*Proof.* If  $\psi$  vanishes off  $D^*$ , then  $\psi^G$  vanishes off  $D^{*G}$ . Then  $\zeta \in B_1$  for any irreducible character  $\zeta$  satisfying  $(\zeta, \psi^G) \neq 0$ , by the preceding result.

*Proof of Theorem 60.8.* First consider the characters  $\{1, \zeta_1, \dots, \zeta_n, \theta_1, \dots, \theta_f\}$ . These all occur with nonzero multiplicities in the virtual characters  $\Gamma_i^G$  or  $\lambda_i^G = (\psi_i - \psi_n)^G$  for some  $i$ , and hence belong to the principal block by the preceding corollary, using the fact that  $\Gamma_i^G$  and  $(\psi_i - \psi_n)^G$  vanish off  $D^{*G}$ . The remaining irreducible characters  $\{\chi_j\}$  all have the property that  $\chi_j(1) \equiv 0 \pmod{|D|}$  by (60.7i). Since  $|D| = |G|_p$ , each character  $\chi_j$  belongs to a block of defect zero, and is not in  $B_1$ . This completes the proof.

### §60C. Applications to the Classification of Transitive Permutation Groups of Degree $p$

The study of transitive permutation groups on a set  $\Omega$  of  $p$  elements, for a prime  $p$ , has a long history. We shall present a few theorems on the subject, which make use of the results obtained in §60B. For historical remarks and additional results, see Brauer [43] and Feit [82, VIII]. In what follows, it is assumed that a *permutation group*  $G$  on a set  $\Omega$  acts faithfully, so no element  $g \neq 1$  fixes all elements of  $\Omega$ .

**(60.13) Proposition.** *Let  $G$  be a transitive permutation group on a set  $\Omega$ , with  $|\Omega| = p$  for some odd prime  $p$ , and let  $D$  be a Sylow  $p$ -subgroup of  $G$ . Then  $|D| = p$ ,  $C_G(D) = D$ , and  $D^*$  is a T.I. set.*

*Proof.* Let  $H$  be the stabilizer of a point in  $\Omega$ . Then  $G/H \cong \Omega$  as  $G$ -sets, so  $|G:H| = p$ . On the other hand,  $H$  is a faithful permutation group on a set of  $p-1$  elements, so  $|H|$  divides  $(p-1)!$ . Thus if  $D$  is a Sylow  $p$ -subgroup, we have  $|D| = p$ . Now identify  $G$  with a subgroup of the symmetric group  $S_p$  on  $p$  letters. Then  $D$  is generated by a  $p$ -cycle, and an easy calculation shows that  $C_G(D) = D$ . The last statement is clear since  $|D| = p$ .

**Remark.** By the preceding result, any group  $G$  satisfying the hypothesis of (60.13) also satisfies (60.5), so the results of §60B can be applied to the characters of  $G$ .

**(60.14) Proposition.** *Let  $G$  be a transitive permutation group on a set  $\Omega$  of  $p$  elements, for a prime  $p$ , and assume that  $|N_G(D)| = 2p$ . Then either  $D \trianglelefteq G$  or the action of  $G$  on  $\Omega$  is 2-transitive.*

**Remark.** The conclusion of (60.14) holds without the assumption that  $|N_G(D)| = 2p$  (Burnside). We prove here only the special case, as an introduction to our main theorem (60.17) in which the same hypothesis is used.

*Proof of (60.14).* We may assume  $p > 3$ . From §60B, we have

$$\text{Irr } G = \{1, \zeta_1, \dots, \zeta_n, \theta; \chi_1, \dots, \chi_h\},$$

where there is only one nonexceptional character  $\theta$ , since  $e = 2$  in this case. Let

$\psi$  be the permutation character arising from the action of  $G$  on  $\Omega$ . Then  $\psi(1) = p$ , and it is sufficient to prove that  $\psi = 1_G + \chi$  for some nontrivial  $\chi \in \text{Irr } G$  (by Exercise 10.3) or that  $D \trianglelefteq G$ . From the information about degrees of characters, summarized in (60.7), none of the characters,  $\zeta_i$ ,  $1 \leq i \leq h$ , can occur in  $\psi$ . Since  $\theta(1) \equiv \pm 1 \pmod{p}$ ,  $(\theta, \psi) > 0$  implies that either  $\psi = 1 + \theta$ , or  $\theta(1) = 1$ . As we shall see, the latter case occurs only if  $D \trianglelefteq G$ . Since  $e = 2$ , we have  $\zeta_i(1) \equiv \pm 2 \pmod{p}$ , from the discussion in Volume I, p. 488. We next prove:

**(60.15) Lemma.** *Keep the hypotheses of (60.14). Then the irreducible characters  $\{\zeta_1, \dots, \zeta_n\}$  are algebraic conjugates of one another (see Exercise 9.14).*

*Proof.* Since  $|D| = p$ , the nontrivial characters  $\{\lambda_i\}$  of  $D$  are algebraically conjugate. It follows that the induced characters  $\psi_i = \lambda_i^H$  are also algebraically conjugate, by the formula for induced characters. By (60.7ii) we have

$$\zeta_i|_{D^*} = \varepsilon \psi_i|_{D^*} \quad \text{for } 1 \leq i \leq n, \quad \text{and} \quad \varepsilon = \pm 1.$$

If  $\sigma$  is a field automorphism such that  $\sigma\psi_i = \psi_j$ , then the preceding formula implies that  $\sigma\zeta_i = \zeta_j$  (since the exceptional characters  $\{\zeta_i\}$  take constant values on the  $p'$ -classes, by (60.7iii)).

Let us return to the proof of (60.14). If  $(\psi, \zeta_i) > 0$  for some  $i$ , then  $(\psi, \sigma\zeta_i) > 0$  for all field automorphisms  $\sigma$ , since  $\psi$  is rational valued. Then  $(\psi, \sum_{i=1}^n \zeta_i) > 0$ . Since  $n = \frac{1}{2}(p-1)$  and  $\zeta_i(1) \equiv \pm 2 \pmod{p}$ , this is impossible unless  $\zeta_i(1) = 2$  for all  $i$ . By (60.7iii), we have

$$\delta\zeta_1(1) = 1 + \delta'\theta(1) \quad \text{where} \quad \delta, \delta' = \pm 1.$$

Thus  $\zeta_1(1) = 2$  only if  $\theta(1) = 1$ . In that case,  $\theta(x) = 1$  for all  $x \in D$  by (14.19iv), and hence  $G$  has a proper normal subgroup containing  $D$ . The proof is completed by the following lemma.

**(60.16) Lemma.** *Keep the hypothesis of (60.14). Then either  $G$  is simple or  $D \trianglelefteq G$ .*

*Proof.* We first prove that if  $N$  is a proper normal subgroup, then  $N \geq D$ . To see this, we first note that all  $N$ -orbits  $N\alpha$ ,  $\alpha \in \Omega$ , have the same size since  $g(N\alpha) = (gNg^{-1})g\alpha = N(g\alpha)$  and  $G$  acts transitively. Since  $|\Omega| = p$ ,  $N$  is either transitive on  $\Omega$  or  $N \leq G_\alpha = \text{Stab}_G \alpha$  for some  $\alpha \in \Omega$ . In the latter case we obtain  $N \leq \bigcap_{\alpha \in \Omega} G_\alpha$ , contrary to the assumption that  $G$  acts faithfully on  $\Omega$ . Thus  $N$  acts transitively, and it follows that  $G = G_\alpha N$  for  $\alpha \in \Omega$ . Then  $p \nmid |G_\alpha|$  since  $G_\alpha$  cannot contain a  $p$ -cycle, so  $p \mid N$ , and  $D \leq N$ , proving the first assertion.

Now let  $N$  be a minimal proper normal subgroup. Then  $D \leq N$  by the previous discussion, and we shall prove that  $G = N \cdot N_G(D)$  by what is called the *Frattini argument*, as follows. Let  $g \in G$ . Then  ${}^g D \leq N$  since  $N \leq G$ , so  ${}^g D = {}^x D$  for some  $x \in N$  since  $D$  is a Sylow subgroup of  $N$ . Thus  $x^{-1}g \in N_G(D)$ , as required.

We then note that the centralizer and normalizer of  $D$  in  $N$  both coincide with  $D$ , since  $G \neq N$  and  $|N_G(D):D| = 2$ . Then  $N$  has a normal  $p$ -complement  $L$  by Burnside's Theorem 13.20. By the minimality of  $N$ , we obtain  $L = 1$ ,  $N = D$ , and  $D \trianglelefteq G$ , completing the proof.

Before stating the main result of this subsection, we recall some properties of multiply transitive permutation groups.

Let  $G$  be a permutation group on a finite set  $\Omega$ . For  $\alpha \in \Omega$ , we set  $G_\alpha = \text{Stab}_G \alpha$ , and

$$G_{\{\alpha_1, \dots, \alpha_k\}} = G_{\alpha_1} \cap \dots \cap G_{\alpha_k} \quad \text{for } \alpha_i \in \Omega, \quad 1 \leq i \leq k.$$

The group  $G$  is called  *$k$ -transitive* on  $\Omega$  for some integer  $k \geq 1$  if  $G$  acts transitively on the ordered  $k$ -tuples of distinct elements from  $\Omega$ , and *sharply  $k$ -transitive* if it is  $k$ -transitive and  $G_{\{\alpha_1, \dots, \alpha_k\}} = 1$  for one (and hence every)  $k$ -tuple  $(\alpha_1, \dots, \alpha_k)$  from  $\Omega$ . Note that each sharply 2-transitive permutation group is a Frobenius group, by (14.3).

Our main result is:

**(60.17) Theorem (Ito [60]).** *Let  $G$  be a nonsolvable 2-transitive permutation group on a set  $\Omega$  of  $p$  elements for some prime  $p$ . Let  $D$  be a Sylow  $p$ -subgroup, and assume that  $|N_G(D)| = 2p$ . Then  $p = 1 + 2^l$  for some integer  $l$ , and  $G$  is sharply 3-transitive on  $\Omega$ .*

**Remarks.** The simple sharply 3-transitive groups were classified by Zassenhaus [36] (see also Huppert–Blackburn [82]). Using Zassenhaus's result combined with Ito's Theorem 60.17, it follows that if  $G$  is a simple group satisfying the hypotheses of (60.17), then  $G \cong SL_2(\mathbb{F}_{2^l})$  for some  $l > 1$ . Using the classification of finite simple groups, all nonsolvable 2-transitive permutation groups are known, including of course those of prime degree (see Feit [80]).

We are now ready to begin the proof of Ito's Theorem 60.17. As in the case of (60.14), we may assume that  $p > 3$ .

*Step 1.* We first prove that  $G$  is simple. If not, then  $D \trianglelefteq G$  by 60.16, and it follows that  $G$  is solvable, contrary to assumption.

*Step 2.* We next set up an application of character theory. By Theorem 60.8, the principal block<sup>†</sup> of  $G$  is given by

$$\mathbf{B}_1 = \{1_G, \zeta_1, \dots, \zeta_n, \theta\},$$

noting as before that there is only one nonexceptional character  $\theta$  since  $e = 2$ .

<sup>†</sup>The theory of blocks is not required for the proof of Ito's Theorem beyond the organization it provides for the characters of  $G$ .

Letting  $\psi$  denote the permutation character on  $\Omega$ , we have

$$\psi = 1 + \theta, \quad \theta(1) = p - 1,$$

using the proof of (60.14).

*Step 3.* We shall derive some additional properties of the characters  $\{\zeta_i\}$  and  $\theta$ . From (60.13), we know that  $G_\alpha$  consists of  $p$ -regular elements. Therefore, by (60.7iii), we have

$$\zeta_i|_{G_\alpha} = \zeta_j|_{G_\alpha} \quad \text{for all } i, j, 1 \leq i, j \leq n,$$

and for some constants  $\delta, \delta' = \pm 1$ , which are independent of  $x \in G_{p'}$ ,

$$\delta \zeta_1|_{G_\alpha} = 1_{G_\alpha} + \delta' \theta|_{G_\alpha}.$$

Since  $\theta(1) = p - 1$ , we have  $\delta' \neq 1$ , otherwise  $p|\zeta_1(1)$  which is impossible. Therefore  $\delta' = -1$ , so

$$\delta \zeta_1(1) = 2 - p < 0,$$

hence  $\delta = -1$ , and

$$\zeta_1(1) = \cdots = \zeta_n(1) = p - 2.$$

*Step 4.* We shall prove that  $\zeta_i|_{G_\alpha}$  is irreducible, for  $1 \leq i \leq n$ . Suppose not, and let

$$\zeta_i|_{G_\alpha} = a_1 \xi_1 + \cdots + a_r \xi_r, \quad \xi_i \in \text{Irr } G_\alpha,$$

with  $r > 0, a_i > 0$  for all  $i$ , and  $\xi_i \neq \xi_j$  if  $i \neq j$ . Since  $\deg \zeta_i = p - 2$  by Step 3, we may assume  $\deg \xi_1 < \frac{1}{2}(p - 2)$ . Then  $a_1 = (\zeta_i|_{G_\alpha}, \xi_1)_G = (\zeta_i, \xi_1^G)$  by reciprocity, and  $\xi_1 \neq 1_{G_\alpha}$  since  $(1_{G_\alpha}, \psi) = 0$  and  $(\zeta_i, \psi) = 0$  by Step 2. By Step 3, we have  $\theta|_{G_\alpha} = 1_{G_\alpha} + \zeta_i|_{G_\alpha}$ , and hence

$$a_1 = (\zeta_i|_{G_\alpha}, \xi_1) = (\theta|_{G_\alpha}, \xi_1),$$

using the fact that  $(1_{G_\alpha}, \xi_1) = 0$ . We also have  $a_1 = (\zeta_i|_{G_\alpha}, \xi_1) = (\zeta_j|_{G_\alpha}, \xi_1)$  using Step 3. Therefore

$$\begin{aligned} \xi_1^G(1) &\geq a_1(\theta(1) + \sum_{i=1}^n \zeta_i(1)) = a_1(p - 1 + \frac{1}{2}(p - 1)(p - 2)) \\ &\geq \frac{1}{2}a_1(p - 1)(p). \end{aligned}$$

On the other hand,

$$\xi_1^G(1) = p\xi_1(1) \leq \frac{1}{2}p(p - 2),$$

which is a contradiction. We have proved that  $\zeta_i|_{G_\alpha}$  is irreducible, as required.

*Step 5.* We have proved that

$$\theta|_G = 1 + \zeta_i|_{G_\alpha}, \quad \text{for } 1 \leq i \leq n,$$

and  $\zeta_i|_{G_\alpha}$  is irreducible. Since  $\theta|_{G_\alpha}$  is the permutation character of  $G_\alpha$  on  $\Omega - \{\alpha\}$ , it follows that  $\theta|_{G_\alpha}$  is 2-transitive on  $\Omega - \{\alpha\}$  and hence  $G$  is 3-transitive on  $\Omega$ . From this fact we also know that  $p(p-1)(p-2)||G|$ .

*Step 6.* We next prove that  $G$  is sharply 3-transitive, that is,  $G_{\alpha\beta\gamma} = 1$  for  $\alpha, \beta, \gamma$  distinct in  $\Omega$ . For this purpose we apply Exercise 60.2, using the fact that  $G$  is 3-transitive by Step 5. Let  $x \in G_{\alpha\beta\gamma}$ . We shall prove that  $x \in \ker \psi$ , where  $\psi$  is the permutation character of  $G$  on  $\Omega$ . We can then conclude that  $x = 1$ , since  $G$  is simple, by Step 1. Let  $\theta_a$  be the antisymmetric part of  $\theta^2$ . By Exercise 2,

$$\theta_a = \frac{1}{2}\theta(\theta - 1) - \beta.$$

In particular,  $\theta_a(1) = \frac{1}{2}(p-1)(p-2)$ , so  $p \nmid \theta_a(1)$ , and for some  $\xi \in \text{Irr } G$ , we have

$$(\xi, \theta_a) \neq 0 \quad \text{and} \quad p \nmid \xi(1).$$

Then by Theorem 60.8i,  $\xi$  belongs to the principal block  $B_1$  of  $G$ , and  $\xi \neq 1_G$ ,  $\theta$  by Exercise 2ii. Then  $\xi = \zeta_j$  for some  $j$ . By Lemma 60.15, it follows that  $(\sum_{j=1}^n \zeta_j, \theta_a) > 0$ , since  $\theta_a$  is a rational character. By Step 3,  $\zeta_j(1) = p-2$  for each  $j$ , and by comparing degrees, we obtain

$$\theta_a = \sum_{j=1}^n \zeta_j, \quad n = \frac{1}{2}(p-1).$$

Now let  $x \in G_{\alpha\beta\gamma}$ . Then  $\psi(x) \geq 3$ . Since  $x \in G_\alpha$ ,  $x \in G_{\beta'}$ ,

$$\theta_a(x) = \sum \zeta_j(x) = \frac{1}{2}(p-1)(\theta(x) - 1) = \frac{1}{2}\theta(x)(\theta(x) - 1)) - \beta(x),$$

using Step 3. Then

$$\beta(x) = \frac{1}{2}(\theta(x) - 1)(\theta(x) - (p-1)) \geq 0$$

and  $\theta(x) \geq 2$  since  $x \in G_\alpha$ . Therefore  $\theta(x) \geq p-1$ ,  $\psi(x) = p$ , and  $x \in \ker \psi = \{1\}$ , completing the proof.

*Step 7.* By Step 6, we have  $|G| = p(p-1)(p-2)$  and  $|G_\alpha| = (p-1)(p-2)$ . It remains to prove that  $p-1 = 2^k$  for some  $k$ . Since  $G_{\alpha\beta\gamma} = 1$ , no element of  $G_\alpha$  fixes more than one element of  $\Omega - \{\alpha\}$ . Therefore, by Corollary 14.3,  $G_\alpha$  is a Frobenius group, with Frobenius kernel  $N$  and complement  $H$ , and we have  $\Omega - \{\alpha\} \cong G_\alpha/H$

as  $G_\alpha$ -sets. Then  $|H| = p - 2$ ,  $|N| = p - 1$ , and  $C_{G_\alpha}(x) \leq N$  for all  $x \in N$ , by (14.4). Since  $|N| = p - 1$  is even,  $N$  contains an involution  $v$ , and we have

$$|G_\alpha : C_{G_\alpha}(v)| \geq |G : N| = p - 2.$$

It follows that the conjugacy class of  $v$  coincides with  $N - \{1\}$ . Therefore  $N$  is an elementary abelian 2-group, and  $p - 1 = 2^k$ , as required. This completes the proof of the theorem.

## §60. Exercises

1. Let  $G$  be a 2-transitive permutation group on a set  $\Omega$ , and let  $\psi = 1_G + \theta$  be the permutation character. Then

$$\psi^2 = \psi \vee \psi + \psi \wedge \psi.$$

Since  $\psi = (1_{G_\alpha})^G$ , we can compute  $\psi \vee \psi$  and  $\psi \wedge \psi$  using Theorem 12.17. Prove that

$$\psi \vee \psi = \psi + \mu_+, \quad \psi \wedge \psi = \mu_-,$$

where  $\mu_+$  and  $\mu_-$  are defined as follows. Since  $\psi$  is 2-transitive,  $G = G_\alpha \cup G_\alpha y G_\alpha$ . Then from §12C,  $y^2 \in G_\alpha \cap {}^y G_\alpha$ . Let  $N = \langle y, G_\alpha \cap {}^y G_\alpha \rangle$ . Then  $\mu_+ = (1_N)^G$  while  $\mu_- = (\varepsilon_N)^G$ , where  $\varepsilon_N$  is the extension to  $N$  of the unique nontrivial character of  $N/G_\alpha \cap {}^y G_\alpha$ .

2. Keep the notation of Exercise 1, and assume that  $G$  is 3-transitive on  $\Omega$ . Let  $\psi_s = \psi \vee \psi$  and  $\psi_a = \psi \wedge \psi$ .

- (i) Prove that for all  $x \in G$ ,

$$\theta_a = \frac{1}{2}\theta(\theta(x) - 1) - \beta(x),$$

where  $\beta(x)$  is the number of transpositions in the cycle decomposition of  $x$  on  $\Omega$ , and  $\theta_a$  is the antisymmetric part of  $\theta^2$ .

[Hint: Let  $\{v_\alpha : \alpha \in \Omega\}$  be a basis of the  $CG$ -module affording  $\psi$ , and let  $v_0 = \sum_{\alpha \in \Omega} v_\alpha$ . Then  $V = W \oplus \langle v_0 \rangle$ , where  $W$  affords  $\theta$  and  $v_0$  affords  $1_G$ . Moreover,  $V \wedge V = W \wedge W \oplus (W \wedge \langle v_0 \rangle)$ , and  $W \wedge \langle v_0 \rangle$  affords  $\theta$ . Thus it is sufficient to prove that

$$\psi_a(x) = \frac{1}{2}\psi(x)(\psi(x) - 1) - \beta(x), \quad \text{for } x \in G.$$

This is shown as follows. We have

$$V \wedge V = \bigoplus V_{\alpha\beta}, \quad \text{where } V_{\alpha\beta} = \langle v_\alpha \otimes v_\beta - v_\beta \otimes v_\alpha \rangle, \quad \alpha \neq \beta.$$

Since  $G$  is 2-transitive,  $G$  acts transitively on the subspaces  $\{V_{\alpha\beta}\}$ . Each transposition  $(\alpha\beta) \in G$  acts as  $-1$  on  $V_{\alpha\beta}$  and as  $+1$  on all other  $V_{\gamma\delta}$ 's. Since  $\psi(x)$  is the number of fixed points of  $x$  on  $\Omega$ , the formula for  $\psi_a(x)$  is easily verified.]

- (ii) Let  $\theta_a = \theta \wedge \theta$ , as in part (i). Prove that  $(\theta_a, 1_G) = (\theta_a, \theta) = 0$ .

[Hint: Since  $G$  is 3-transitive on  $\Omega$ ,  $G$  is 2-transitive on  $\Omega - \{\alpha\}$ . Therefore  $(\theta|_{G_\alpha}, \theta|_{G_\alpha}) = (\theta^2|_{G_\alpha}, 1_{G_\alpha}) = 2$ , and hence  $(\theta^2, \psi)_G = 2$ . Then show that  $\theta \vee \theta$  is the permutation character  $\tau$  of  $G$  on the set of unordered pairs  $\{\alpha, \beta\}_{\alpha \neq \beta}$ , and that  $(\tau, \psi) = (\tau|_{G_\alpha}, 1_{G_\alpha})_{G_\alpha} = 2$ . Since  $\theta^2 = \theta_s + \theta_\alpha$ , the result follows.]

## §61. REFINEMENTS OF THE BRAUER CORRESPONDENCE

### §61A. Blocks and Normal Subgroups

In this subsection,  $R$  denotes either a field of characteristic  $p$ , or a d.v.r. with maximal ideal  $\mathfrak{p}$  such that  $R$  is complete in the  $\mathfrak{p}$ -adic topology and the residue field  $R/\mathfrak{p}$  has characteristic  $p$ . We shall study the connections between  $p$ -blocks of  $G$  and  $p$ -blocks of a normal subgroup  $H$  of  $G$ , and their defect groups. Some results in this direction were obtained earlier, for the special case of a normal  $p$ -subgroup (see (58.5)). Our discussion is based on the work of Brauer [59], Alperin-Burry [80], and Alperin-Broué [79], and uses many of the ideas introduced in §58C for the module-theoretic approach to the Brauer correspondence.

We first introduce some notation, which will be used throughout this subsection. We always let  $H$  denote a normal subgroup of  $G$ . Then  $G$  acts by conjugation on the set of block idempotents of  $RH$ . For each block idempotent  $b' \in c(RH)$ , we set

$$\text{Stab}_G b' = \{g \in G : {}^g b' = b'\},$$

where  ${}^g b = gbg^{-1}$  as usual. Since  $b'$  is the unique central idempotent in its block ideal  $B'$ , we also have

$$\text{Stab}_G b' = \{g \in G : {}^g B' = B'\} = \text{Stab}_G B'.$$

For each block ideal  $B'$  in  $RH$ , we let  $R(GB'G)$  denote the two-sided ideal in  $RG$  generated by  $B'$ . Then  $R(GB'G)$  consists of all  $R$ -linear combinations of the elements  $\{xay : x, y \in G, a \in B'\}$ .

We recall the left action of  $R(G \times G)$  on  $RG$ , given by  $(x, y)a = xay^{-1}$ , for  $(x, y) \in G \times G$  and  $a \in RG$ . A left  $R(G \times G)$ -module  $M$  defines a left  $R(H \times H)$ -module by restriction of scalars, as well as a left  $RH$ -module, by restriction of scalars from  $RG$  to  $RH$ . We denote these restrictions by

$$M_{H \times H} \quad \text{and} \quad M_{H \times 1},$$

respectively.

We shall find it useful to consider certain subgroups of  $G \times G$  which are related to the stabilizers of the block ideals  $\{B'\}$  of  $RH$ , and are defined by

$$T = T(B') = (H \times H)\Delta(\text{Stab}_G B'),$$

where  $\Delta: G \rightarrow G \times G$  is the diagonal map. For each block ideal  $B'$  of  $RH$ , and  $T = T(B')$ , we have  $T \cdot B' \subseteq B'$ ; we then let  $\tilde{B}'$  denote the block ideal  $B'$  viewed as an  $RT$ -module.

**(61.1) Definition.** Let  $B$  be a block ideal of  $RG$ , and  $B'$  a block ideal of  $RH$ . We shall say that  $B$  covers  $B'$  whenever  $B'|_{B_{H \times H}}$ . In this case, we also say that  $B$  covers  $B'$ , where  $B$  and  $B'$  are the corresponding blocks of  $G$  and  $H$ , respectively.

In the statement and proof of the theorem below, the defect groups of block idempotents will also be called the defect groups of the corresponding block ideals.

Note that if the Brauer correspondent  $(B')^G$  is defined for a  $p$ -block  $B'$  of  $H$ , then the block  $B = (B')^G$  covers  $B'$ , by (58.17). Later (see (61.4)) we shall obtain a criterion for one block to cover another, in terms of modules in the blocks.

Our aim is to prove:

**(61.2) Theorem** (Alperin-Burry [80]).

(i) *Each block ideal  $B$  of  $RG$  covers exactly one  $G$ -conjugacy class of block ideals of  $RH$ .*

(ii) *Let  $B$  cover  $B'$ , and let  $D$  be a defect group of  $B$ . Then  $D \cap H = {}_G D'$ , for some defect group  $D'$  of  $B'$ . Moreover,  $D \leq {}_G \text{Stab}_G B'$ .*

(iii) *Let  $B'$  be a block ideal of  $RH$  which is covered by some block ideal of  $RG$ . Then there is a block ideal  $B_0$  of  $RG$  such that  $B_0$  covers  $B'$ , whose defect group  $D_0$  is the unique maximal element among the defect groups of all block ideals covering  $B'$ , with respect to the order relation  $\leq_G$ .*

(iv) *Let  $D'$  be a defect group of  $B'$ , and assume that  $H \geq C_G(D')$ . Then  $(B')^G$  is defined, and is the unique block of  $G$  covering  $B'$ .*

We begin with some preliminary results.

**(61.3) Lemma.** *Let  $B'$  be a block ideal in  $RH$  with block idempotent  $b'$ . Let  $T = T(B')$  be the subgroup of  $G \times G$  defined by  $T = (H \times H)\Delta(\text{Stab}_G B')$ , and  $\tilde{B}'$  the extension of  $B'$  to  $T$ , as described above.*

(i) *We have*

$$R(GB'G) = \sum_{x \in G} {}^x(b')RG.$$

(ii) *The left  $RH$ -module  $RG_{H \times 1}$  can be expressed uniquely as a direct sum of modules belonging to the different blocks of  $H$ . In this decomposition, the submodule  $R(GB'G)_{H \times 1}$  coincides with the direct summand associated with the conjugates of the block  $B'$ .*

(iii) *There exists a direct decomposition*

$$R(GB'G)_{H \times H} = \bigoplus (x, y)B' \text{ (as } R(H \times H)\text{-modules),}$$

where the sum is taken over a cross-section of  $(G \times G)/T$ .

(iv) There is an isomorphism of  $R(G \times G)$ -modules

$$R(GB'G) \cong \text{ind}_T^{G \times G} \tilde{B}'.$$

(v) A block ideal  $B$  of  $RG$  covers  $B'$  if and only if  $B|R(GB'G)$  (as  $R(G \times G)$ -modules).

*Proof.* (i) For all  $x, y \in G$ , we have

$$xB'y = (xB'x^{-1})xy \subseteq {}^x(b')RG.$$

The formula (i) now follows, since  $R(GB'G)$  is generated as  $R$ -module by the elements  $xay$ , for  $x, y \in G$  and  $a \in B'$ . The statement (ii) is an immediate consequence of (i).

(iii) It is easily checked that  $(u, v)B' = B'$  for all  $(u, v) \in T(B')$ . It follows that the sum  $\sum (x, y)B'$ , taken over a cross-section of  $(G \times G)/T(B')$ , is a submodule of  $RG_{H \times H}$ . Further discussion is needed in order to prove that the sum is direct. We have

$$T(B') \leq (H \times H)\Delta G \leq G \times G.$$

A cross-section for the first inclusion can be chosen from  $\Delta G$ , and for the second from  $G \times 1$ . Products of elements of these cross-sections form a cross-section of  $(G \times G)/T(B')$ . Notice that  $(x, x)B' = xB'x^{-1} \subseteq RH$  for all  $x \in G$ ; while  $(y, 1)B' \subseteq R(G - H)$  if  $y \notin H$ , that is  $(y, 1)a$  is supported outside  $H$  for all  $a \in B'$ . For an arbitrary element  $(x, yx)$  of the resulting cross-section, we have  $(x, yx)B' \subseteq RH$  only if  $y = 1$ , and the block ideals  $(x, x)B' = xB'x^{-1}$  are all different as  $\{(x, x)\}$  ranges over a cross-section of  $(H \times H)\Delta G/T(B')$ . Using these remarks, it is easily verified that

$$(x, z)B \cap \sum_{(x', z') \neq (x, z)} (x', z')B' = 0$$

for arbitrary elements  $\{(x, z), (x', z'), \dots\}$  of the cross-section, and (iii) is proved. Part (iv) follows at once from part (iii) and the Imprimitivity Theorem 10.5.

(v) First suppose  $B|R(GB'G)$ . Using part (iii) and the K-S-A Theorem, it follows that  $(x, y)B'|B_{H \times H}$  for some  $(x, y) \in G \times G$ . Then  $B'|((x, y)^{-1}B_{H \times H})$ , and hence  $B'|B_{H \times H}$ , using the fact that  $(x, y)^{-1}B = B$  for all  $(x, y) \in G \times G$ . This proves the implication one way.

Conversely, suppose  $B'|B$ , and let  $b$  be the block idempotent in  $B$ . Then

$$b \in \sum R(GB''G),$$

where the summands are two-sided ideals in  $RG$  defined by the block ideals  $\{B''\}$  of  $RH$ . By Rosenberg's Lemma 57.8, we obtain  $b \in R(GB''G)$  for some block ideal  $B''$ . It is then easily checked that  $B|R(GB''G)$ . Since  $B'|B$  and  $B|R(GB''G)$ , we obtain  $B' \mid R(GB''G)_{H \times H}$ . By parts (i) and (ii) of the Lemma and the K-S-A Theorem, it follows that  $B'$  and  $B''$  are conjugate block ideals. Then  $R(GB'G) = R(GB''G)$  by a second application of part (i), and we obtain  $B|R(GB'G)$ , completing the proof.

Before continuing with the proof of the main result, we obtain the following corollary of (61.3), which provides a useful criterion for one block to cover another in terms of modules in the blocks.

**(61.4) Corollary.** *A block  $B$  of  $G$  covers a block  $B'$  of  $H$  if and only if there exists a left  $RG$ -module  $M$  in  $B$  whose restriction  $M_H$  has a nonzero direct summand belonging to the block  $B'$ .*

*Proof.* Let  $B$  and  $B'$  be defined by block idempotents  $b \in RG$  and  $b' \in RH$  respectively. If  $B$  covers  $B'$ , then clearly  $b'(bRG) \neq 0$ , and it follows that  $(bRG)_H$  has an indecomposable direct summand  $N$  such that  $b'N \neq 0$ . Conversely, let  $M$  be a left  $RG$ -module in  $B$  such that  $M_H$  has a nonzero direct summand belonging to  $B'$ . Letting  $B = bRG$ , we have  $b'B \neq 0$ . By the second part of the proof of (61.3v),  $B|R(GB''G)$  for some block ideal  $B''$  of  $RH$ , and hence  $b'R(GB''G) \neq 0$ . By part (i) of (61.3), it follows that the blocks  $B'$  and  $B''$  are conjugate. Then  $R(GB''G) = R(GB'G)$ , and  $B|R(GB'G)$ . By (61.3v), it follows that  $B$  covers  $B'$ , completing the proof of the corollary.

*Proof of Theorem 61.2.* (i) By the proof of (61.3v),  $B|R(GB'G)$  for some block ideal  $B'$  of  $RH$ , and hence  $B$  covers at least one block ideal of  $RH$ . If  $B$  covers another block ideal  $B''$  of  $RH$ , then  $B|R(GB''G)$  by (61.3v) again, and it follows that  $B'$  and  $B''$  are conjugate, by (61.3i) and (61.3ii). This completes the proof of part (i).

(ii) The proof of this part of the theorem is based on the interpretation of defect groups in terms of vertices and sources, and, in particular, the fact that block ideals are trivial source modules (see Exercise 57.3). We begin with the assumption that  $B$  covers  $B'$ , so  $B' \mid B_{H \times H}$ . If  $D$  and  $D'$  are defect groups of  $B$  and  $B'$ , then by (57.22),  $\Delta D$  and  $\Delta D'$  are vertices of  $B$  and  $B'$ , as indecomposable modules over  $R(G \times G)$  and  $R(H \times H)$ , respectively. Since  $B' \mid B_{H \times H}$ , we have  $\Delta D' \leq_{G \times G} \Delta D$  by (19.14i), and hence  $D' \leq_G D \cap H$ , using the fact that  $H \trianglelefteq G$ .

For the reverse inclusion, we begin with the fact that  $B|R(GB'G)$  by (61.3v). Moreover, the indecomposable components of  $R(GB'G)_{H \times H}$  all have the form  $(x, y)B'$  for some  $(x, y) \in G \times G$ , by (61.3iii). Since  $B$  is a trivial source module (see Exercise 57.4) we can apply Exercise 57.3 to deduce that  $B_{H \times H}$  has a component  $U$  such that  $(H \times H) \cap \Delta D \leq_{H \times H} \text{vtx } U$ , since  $\Delta D$  is a vertex of  $B$ . By the K-S-A Theorem, we have  $U \cong (x, y)B'$ , so a vertex of  $U$  is given by  $(x, y)\Delta D'(x, y)^{-1}$  for some  $(x, y) \in G \times G$ , since  $\Delta D'$  is a vertex of  $B'$ . It follows that  $H \cap D \leq_G D'$ , completing the proof of the first statement of part (ii).

For the second statement,

$$B \mid \text{ind}_T^{G \times G} \tilde{B}'$$

by (61.3iv), so a vertex  $\Delta D$  of  $B$  satisfies the condition that

$$\Delta D \leq_{G \times G} T.$$

Using the definition of  $T$ , we obtain

$$D \leq_G H \cdot \text{Stab}_G B' = \text{Stab}_G B',$$

completing the proof of part (ii).

(iii) By (61.3iii)–(61.3v), the block ideals covering  $B'$  are precisely the indecomposable components of  $\text{ind}_T^{G \times G} \tilde{B}'$ , where  $T$  and  $\tilde{B}'$  are defined as in (61.3). Then, for each block  $B$  covering  $B'$ , we have

$$\text{vtx } B \leq_{G \times G} \text{vtx } \tilde{B}',$$

by (19.14), and by (19.16) there is one block  $B_0$  covering  $B'$  such that  $\text{vtx } B_0 =_{G \times G} \text{vtx } \tilde{B}'$ . Upon converting these statements into the language of defect groups using (57.22), part (iii) follows.

(iv) We have  $H \geq D' C_G(D')$ . By Theorem 58.20,  $B'$  occurs with multiplicity one in  $RG_{H \times H}$ . It follows that  $(B')^G$  is defined, and is the unique block of  $G$  covering  $B'$ . This completes the proof of the theorem.

We obtain next some additional information about the defect groups of blocks  $B_0$  of  $G$  satisfying part (iii) of Theorem 61.2. For this purpose, we assume that  $R$  is part of a  $p$ -modular system  $(K, R, k)$  such that  $\text{char } K = 0$ ,  $K$  is sufficiently large relative to  $G$ ,  $R$  is complete in the  $p$ -adic topology, and  $k = R/p$  is a perfect field of characteristic  $p$ . Under these conditions, we know that for an arbitrary subgroup  $G_0 \leq G$ , the block ideals  $\{B_0\}$  of  $RG_0$  are absolutely indecomposable  $R(G_0 \times G_0)$ -lattices, by Exercise 57.5.

**(61.5) Theorem.** *Let  $H \leq G$ , let  $B'$  be a block ideal of  $RH$ , and let  $B_0$  be a block ideal of  $RG$  such that  $B_0$  covers  $B'$ , and  $B_0$  satisfies part (iii) of Theorem 61.2. Let  $D_0$  be a defect group of  $B_0$ . Then*

$$|D_0 : D_0 \cap H| = |\text{Stab}_G B' : H|_p.$$

We first require:

**(61.6) Lemma** (Cline [73]). *Let  $M$  be an  $RG$ -lattice such that  $M_H$  is an absolutely indecomposable  $RH$ -lattice. Let  $D$  be a vertex of  $M$ . Then  $DH/H$  is a Sylow  $p$ -subgroup of  $G/H$ .*

*Proof.* Let  $S$  be a Sylow  $p$ -subgroup of  $G$ . Then  $M_{SH}$  is indecomposable, and  $M_{SH}|(M_{SH})^G$  by (19.2.iv) since the index  $|G: SH|$  is prime to  $p$ . It follows that if  $D' \in \text{vtx } M_{SH}$ , then  $D' = {}_G D$ , so it suffices to show that if  $D' \leq S$ , then  $D'H = SH$ .

Since  $|SH: D'H|$  is a power of  $p$  and  $M_{D'H}$  is absolutely indecomposable, the induced module  $(M_{D'H})^{SH}$  is indecomposable, by Green's Theorem (see Corollary (19.23)). Moreover,  $M_{SH}$  is  $D'H$ -projective, since  $D'$  is a vertex of  $M_{SH}$  and  $D'H \geq D'$ . Then  $M_{SH}|(M_{D'H})^{SH}$  by (19.2) again. It follows that

$$M_{SH} \cong (M_{D'H})^{SH},$$

and we obtain  $SH = D'H$  by comparing  $R$ -ranks. This completes the proof of the lemma.

*Proof of Theorem 61.5.* Let  $B_0$  satisfy part (iii) of (61.2), and let  $D_0$  be a defect group of  $B_0$  such that  $D_0 \leq \text{Stab}_G B'$ , by (61.2ii). Let

$$T = (H \times H)\Delta(\text{Stab}_G B')$$

and let  $\tilde{B}'$  be the block ideal  $B'$  viewed as an  $RT$ -lattice, as in the proof of (61.2iii). Then  $\tilde{B}'_{H \times H} \cong B'$ , and is an absolutely indecomposable  $R(H \times H)$ -lattice, by the remarks preceding the theorem. We can now apply Lemma 61.6, with  $\tilde{B}'$  in place of  $M$ ,  $T$  in place of  $G$ ,  $H \times H$  in place of  $H$ , and  $\Delta D_0$  the vertex of  $\tilde{B}'$ , by the proof of (61.2iii). By the lemma, we obtain

$$|\Delta D_0 : \Delta D_0 \cap (H \times H)| = |T : H \times H|_p,$$

using the isomorphism  $DH/H \cong D/D \cap H$ . It then follows at once that

$$|D_0 : D_0 \cap H| = |\text{Stab}_G B' : H|_p,$$

completing the proof.

## §61B. An Extension of Brauer's First Main Theorem

In this subsection,  $(K, R, k)$  denotes a  $p$ -modular system with  $K$  sufficiently large relative to  $G$ ,  $\text{char } K = 0$ , and  $R$  complete in the  $p$ -adic topology. Brauer's First Main Theorem 58.6 establishes a bijection between the set of blocks of  $G$  with a given defect group  $D$  and the set of blocks of  $N_G(D)$  with defect group  $D$ . The first part of the theorem below makes the same statement, with  $N_G(D)$  replaced by an arbitrary subgroup  $G_0 \geq N_G(D)$ . The proof uses Brauer's Theorem 58.20, which is based on the module-theoretic approach to the Brauer Correspondence. The rest of the theorem relates blocks of  $N_G(D)$  with defect group  $D$  to blocks of  $DC_G(D)$  with defect group  $D$ , using the results of §61A, and then to blocks of  $DC_G(D)/D$  of defect zero. The parts of the theorem, taken together, reduce the study of blocks of  $G$  with defect group  $D$ , at least to some extent, to the study of blocks of defect  $D$  of the subgroups  $DC_G(D)/D$ , and ultimately,

to blocks of defect zero of the quotient group  $DC_G(D)/D$ . Note that  $N_G(D)$  acts by conjugacy not only on the blocks of its normal subgroup  $D$ , but also, in a well-defined manner, on the block idempotents of  $R(DC_G(D)/D)$ , using the natural map

$$\tau: R(DC_G(D)) \rightarrow R(DC_G(D)/D)$$

(see (5.26)), since  $\ker \tau$  is invariant under conjugation by elements of  $N_G(D)$ .

**(61.7) Extended First Main Theorem.** *Let  $G$  be a finite group, and let  $D$  be a  $p$ -subgroup of  $G$ .*

(i) *Let  $G_0$  be an arbitrary subgroup of  $G$  containing  $N_G(D)$ . Then the Brauer correspondence defines a bijection from the set of blocks of  $G$  with defect group  $D$  to the set of blocks of  $G_0$  with defect group  $D$ .*

(ii) *Each block of  $N_G(D)$  with defect group  $D$  covers a unique conjugacy class of blocks of  $DC_G(D)$ , each of which has defect group  $D$ .*

(iii) *Let  $\tau: R(DC_G(D)) \rightarrow R(DC_G(D)/D)$  be the natural map. Then  $\tau$  defines a bijection, preserving conjugacy with respect to  $N_G(D)$ , from the set of blocks of  $DC_G(D)$  with defect group  $D$  to the set of blocks of  $DC_G(D)/D$  of defect zero.*

*Proof.* (i) Since  $G_0 \geq N_G(D)$ , we have  $N_G(D) = N_{G_0}(D)$ . The correspondence of blocks given in Brauer's First Main Theorem 58.6 coincides with the Brauer Correspondence, by Exercise 58.4. Thus the Brauer correspondence defines bijections from the set of blocks of  $N_G(D)$  with defect group  $D$ , with the set of blocks of  $G_0$  with defect group  $D$ , and the set of blocks of  $G$  with defect group  $D$ . Now let  $B'$  be a fixed block of  $N_G(D)$  with defect group  $D$ . Then  $B_0 = (B')^{G_0}$  is a block of  $G_0$  with defect group  $D$ . Since  $G_0 \geq N_G(D) \geq DC_G(D)$ , the Brauer Correspondence is defined for blocks of  $G_0$  with defect group  $D$ , by Theorem 58.20. In particular,  $B_0^G = ((B')^{G_0})^G$  is defined, and it is clear that  $((B')^{G_0})^G = (B')^G$  (see Exercise 58.3). Since  $(B')^G$  also has defect group  $D$  by Theorem 58.6, it follows that  $B_0 = (B')^{G_0} \rightarrow B_0^G = (B')^G$  is the required bijection from blocks of  $G_0$  with defect group  $D$  to those of  $G$  with defect group  $D$ .

(ii) Since  $DC_G(D) \trianglelefteq N_G(D)$ , each block  $B'$  of  $N_G(D)$  with defect group  $D$  covers a unique conjugacy class of blocks of  $DC_G(D)$ , by Theorem 61.2i. If  $B''$  is a block of  $DC_G(D)$  covered by the block  $B'$  of  $N_G(D)$  with defect group  $D$ , then a defect group  $D''$  of  $B''$  is conjugate, in  $N_G(D)$ , to  $D \cap DC_G(D) = D$ , by (61.2ii). Since  $D$  is a normal  $p$ -subgroup of  $DC_G(D)$ , the defect group of every block of  $DC_G(D)$  contains  $D$  by (58.5) and hence  $D$  is the defect group of  $B''$ , completing the proof of part (ii).

(iii) Let  $A = R(DC_G(D))$ ,  $\tilde{A} = R(DC_G(D)/D)$ , and let  $\tau: A \rightarrow \tilde{A}$  be the natural map. As we remarked earlier,  $x(\ker \tau)x^{-1} \subseteq \ker \tau$  for all  $x \in N_G(D)$ , so the action of  $N_G(D)$  on  $\tilde{A}$  is given by

$${}^x\tau(a) = \tau({}^xa) \quad \text{for all } a \in A, \quad x \in N_G(D).$$

We have  $\tau(c(A)) \subseteq c(\tilde{A})$ , but the map  $\tau: c(A) \rightarrow c(\tilde{A})$  is not necessarily surjective, so it is not immediate that  $\tau(b)$  is a block idempotent in  $c(\tilde{A})$ , for a block idempotent  $b$  in  $A$ . Nevertheless, we shall prove that this is always the case, following an argument due to Landrock [83]. We first note that since  $\ker \tau \subseteq \text{rad } A$ , we have  $A/\text{rad } A \cong \tilde{A}/\text{rad } \tilde{A}$  by (5.6), so  $\tau$  defines a bijection from the simple  $A$ -modules to the simple  $\tilde{A}$ -modules.

Now let

$$(61.8) \quad \tau(b) = \tilde{b}_1 + \cdots + \tilde{b}_r,$$

for a given block idempotent  $b \in A$ , and block idempotents  $\{\tilde{b}_i; 1 \leq i \leq r\}$  in  $\tilde{A}$ ; we shall prove that  $r = 1$ . Consider a projective indecomposable  $A$ -module  $U_i$  belonging to the block ideal  $B$  in  $A$  defined by  $b$ , and assume  $U_i$  is not simple. Then all the homomorphic images of  $U_i$  are indecomposable, and it follows that we have a short exact sequence

$$(61.9) \quad 0 \rightarrow M_1 \rightarrow U \rightarrow M_2 \rightarrow 0$$

with  $U$  an indecomposable homomorphic image of  $U_i$ , and  $M_1$  and  $M_2$  simple modules, all belonging to the block  $B$ . If, for each such sequence,  $\tilde{M}_1$  and  $\tilde{M}_2$  belong to the same block of  $\tilde{A}$ , then all simple composition factors of  $\tau(b)\tilde{A}$  belong to a single block, by the theory of linkage (see §56C), and it follows that  $\tau(b)$  is a block idempotent of  $\tilde{A}$ , as required. So let us assume that  $r > 1$  in (61.8). Then there exists a short exact sequence (61.9) with the property than  $\tilde{M}_1$  and  $\tilde{M}_2$  belong to different blocks of  $\tilde{A}$ , and  $U$  is indecomposable. Let us consider the endomorphism  $\varphi = \varphi_a$  of  $U$  defined by

$$\varphi(u) = (1 - a)u, \quad \text{for } a \in Z(D),$$

where  $Z(D)$  is the center of  $D$ . Since  $A = R(DC_G(D))$ ,  $a \in c(A)$ , and  $\varphi \in \text{End}_A U$ . Moreover,  $\varphi$  is nilpotent mod  $A$ , since  $a$  is a  $p$ -element. Since  $\mathfrak{p}A \subseteq \text{rad } A$ ,  $\varphi$  annihilates  $M_1$ . If  $\ker \varphi = M_1$ , then  $M_2 \cong \text{im } \varphi$ , and  $M_2$  is isomorphic to a submodule of  $U$ , which is impossible since  $\tilde{M}_1$  and  $\tilde{M}_2$  belong to different blocks of  $\tilde{A}$ . It follows that  $\varphi$  annihilates  $U$ , so  $Z(D)$  acts trivially on  $U$ . Since  $D$  is a  $p$ -group, we can repeat the argument, and show that  $D$  acts trivially on  $U$ . Then  $U$  can be viewed as an indecomposable  $\tilde{A}$ -module with composition factors belonging to different blocks of  $\tilde{A}$ . This is a contradiction, and we have proved that  $r = 1$  in (61.8).

We next prove that the map  $b \rightarrow \tau(b)$  is surjective, between the set of block idempotents of  $A$  and the block idempotents of  $\tilde{A}$ . Let  $\tilde{b}$  be an arbitrary block idempotent in  $\tilde{A}$ ; then there exists a idempotent  $e \in A$  such that  $\tau(e) = \tilde{b}$ , by (6.7). Then there exists a block idempotent  $b \in A$  such that  $\tau(be) \neq 0$ , and hence  $\tau(b)\tilde{b} \neq 0$ . Then  $\tau(b) = \tilde{b}$ , by the first part of the proof, and  $\tau$  is surjective on the block idempotents. It is then clear that  $\tau$  defines a bijection between the block idempotents of  $A$  and those of  $\tilde{A}$ .

Now let us view  $A$  as an  $G_1$ -algebra, and  $\tilde{A}$  as a  $\tilde{G}_1$ -algebra, where  $G_1 =$

$DC_G(D)$  and  $\tilde{G}_1 = DC_G(D)/D$ . Then, from §57A and the properties of the trace map, we obtain

$$b \in A_{G_1/D} \Leftrightarrow \tau(b) \in \tilde{A}_{\tilde{G}_1/1}$$

for all block idempotents  $b \in A$ . Using (57.10) together with what has been proved earlier, we conclude that  $\tau$  defines a bijection from the block idempotents of  $A$  with defect group  $D$  to the block idempotents of  $\tilde{A}$  with defect group 1. By (57.19), this is the conclusion of part (iii), and completes the proof of the theorem.

Our first application of the Extended First Main Theorem is:

**(61.10) Corollary.** *Let  $B$  be a block of  $G$  with defect group  $D$ . There exists a unique  $N_G(D)$ -conjugacy class of blocks  $\{B'\}$  of  $DC_G(D)$  with the properties:*

- (i)  $(B')^G = B$ , and
- (ii) the defect group of  $B'$  is  $D$ , for each block  $\{B'\}$  in the conjugacy class.

*Proof.* By Theorem 61.7,  $B = \tilde{B}^G$ , for a unique block  $\tilde{B}$  of  $N_G(D)$  with defect group  $D$ . Since  $N_G(D) \geq DC_G(D)$ , a block  $\tilde{B}$  of  $N_G(D)$  covers a block  $B'$  of  $DC_G(D)$  if and only if  $(B')^{N_G(D)} = \tilde{B}$ , by Alperin's Theorem 58.21 and Definition 61.1. The statement of the corollary now follows from (61.7ii).

We now have:

**(61.11) Theorem.** *Let  $D$  be a  $p$ -subgroup of  $G$ , and let  $B'$  be a block of the subgroup  $DC_G(D)$  with defect group  $D$ . Then  $B'$  contains exactly one simple  $kG$ -module, and exactly one irreducible  $K$ -character  $\zeta$  such that  $D \leq \ker \zeta$ .*

*Proof.* The irreducible  $K$ -characters in  $B'$  having  $D$  in their kernels correspond to the irreducible  $K$ -characters of  $DC_G(D)/D$  in the block  $B'_0$  of  $DC_G(D)/D$  corresponding to  $B'$  under the natural map  $\tau: R(DC_G(D)) \rightarrow R(DC_G(D)/D)$ , as in (61.7iii). Since  $B'_0$  has defect zero by (61.7iii), there is exactly one such irreducible character, by (56.31). Now let  $F$  be a simple  $k(DC_G(D))$ -module belonging to the block  $B'$ . Since  $D$  is a normal  $p$ -subgroup of  $DC_G(D)$ ,  $D$  acts trivially on  $F$  by Clifford's Theorem, and hence  $F$  is a simple  $k(DC_G(D)/D)$ -module belonging to the block  $B'_0$ . Then  $F$  is uniquely determined, by (56.31) again, completing the proof.

**(61.12) Definition.** The unique irreducible  $K$ -character  $\zeta$  in a block  $B'$  of  $DC_G(D)$  with defect group  $D$ , such that  $D \leq \ker \zeta$ , is called the *canonical character* of  $B'$ .

A consequence of the preceding results is that a block  $B$  of  $G$  with defect group  $D$  is determined by a conjugacy class, with respect to  $N_G(D)$ , of blocks  $B'$  of  $DC_G(D)$  with defect group  $D$  such that  $(B')^G = B$ . By (61.11), these blocks are in bijective correspondence with  $N_G(D)$ -conjugacy classes of irreducible  $K$ -characters of  $DC_G(D)$  containing  $D$  in their kernels.

We shall use these ideas to define an important numerical invariant of a  $p$ -block  $B$  of  $G$ , with defect group  $D$ . By (61.10), there exists a unique conjugacy class of blocks  $\{B'\}$  of  $DC_G(D)$ , all with defect group  $D$ , such that  $(B')^G = B$  for each block  $B'$  in the conjugacy class. Let  $b'$  be a block idempotent in  $R(DC_G(D))$  such that  $b'$  defines a block  $B'$  with these properties. Then  $\bar{b}'$  is the corresponding block idempotent in  $k(DC_G(D))$ , and we have:

**(61.13) Proposition.** *Let  $b'$  be a block idempotent in  $R(DC_G(D))$ , and let  $\bar{b}'$  be the corresponding block idempotent in  $k(DC_G(D))$ . Then*

$$\text{Stab}_{N_G(D)} b' = \text{Stab}_{N_G(D)} \bar{b}'.$$

The proof is immediate, by (56.5), since  $N_G(D)$  permutes the block idempotents of  $R(DC_G(D))$  and  $k(DC_G(D))$ .

**(61.14) Definition.** Let  $D$  be a  $p$ -subgroup of  $G$ , and let  $B$  be a block of  $G$  with defect group  $D$ . The *inertial index*  $e$  of  $B$  is defined by the formula

$$e = |\text{Stab}_{N_G(D)} b' : DC_G(D)|,$$

where  $b'$  is a block idempotent in  $R(DC_G(D))$  associated with any block  $B'$  with defect group  $D$  such that  $(B')^G = B$ .

By (61.10) and (61.13), the inertial index is an invariant of the block  $B$ , and can be defined in terms of block idempotents in either  $R(DC_G(D))$  or  $k(DC_G(D))$  which correspond to  $B$  under the Brauer Correspondence.

The following basic result is due to Brauer [67]. The proof is an immediate consequence of the results on covering blocks of normal subgroups (§61A).

**(61.15) Theorem.** *Let  $(K, R, k)$  be a  $p$ -modular system with  $\text{char } K = 0$ ,  $K$  sufficiently large relative to  $G$ ,  $R$  complete in the  $p$ -adic topology, and  $k = R/p$  a perfect field of characteristic  $p$ . Let  $B$  be an arbitrary  $p$ -block of  $G$  with inertial index  $e$ . Then  $e \not\equiv 0 \pmod{p}$ .*

*Proof.* Let  $D$  be a defect group of  $B$ , and let  $\tilde{B}$  be the unique block of  $N_G(D)$  with defect group  $D$  such that  $(\tilde{B})^G = B$  (see (58.6)). Then  $\tilde{B}$  covers a unique conjugacy class of blocks  $\{\tilde{B}'\}$  (with defect group  $D$ ), of  $DC_G(D)$ . Since  $N_G(D) \geq C_G(D)$ , the block  $\tilde{B}$  is the unique block of  $N_G(D)$  covering  $B'$ , and hence  $\tilde{B}$  plays the role of the block  $B_1$  in (61.2iii). Since  $D$  is the defect group of  $\tilde{B}$  and  $D \cap DC_G(D) = D$  is also a defect group of  $B'$  by (61.2ii), we obtain

$$1 = |D : D \cap DC_G(D)| = |\text{Stab}_{N_G(D)} B' : DC_G(D)|_p.$$

by Theorem 61.5. This proves that the inertial index of  $B$  is prime to  $p$ , as required.

### §61C. Brauer's Third Main Theorem

In order to apply Brauer's Second Main Theorem 59.14, it is necessary to know, at least in certain cases, which  $p$ -blocks of a subgroup  $H \leq G$  are Brauer correspondents of a given  $p$ -block of  $G$ . This is a difficult problem in general, but has a simple answer for the important case of the principal block of  $G$ . The result is Brauer's Third Main Theorem 61.16, which is proved in this subsection.

We assume throughout the subsection that  $(K, R, k)$  denotes a  $p$ -modular system such that  $\text{char } K = 0$  and  $K$  is sufficiently large relative to  $G$ .

For an arbitrary subgroup  $H \leq G$ ,  $B_1(H)$  denotes the principal block of  $H$ . By (57.20), the Sylow  $p$ -subgroups of  $H$  are the defect groups of  $B_1(H)$ .

In the discussion to follow, we shall make frequent use of the results of §§61B, C and the properties of the Brauer Correspondence from §58, such as the transitivity (Exercise 58.3).

**(61.16) Brauer's Third Main Theorem.** *Let  $B$  be a block of a subgroup  $H \leq G$  with defect group  $D$ , and assume that  $H \geq DC_G(D)$ . Then  $B^G$  is defined, and we have*

$$B^G = B_1(G) \Leftrightarrow B = B_1(H).$$

Our presentation follows Alperin [86]. We first require a preliminary result, which contains the crucial ideas, and is a special case of the main theorem.

**(61.17) Proposition.** *The conclusions of (61.16) hold in case  $H = DC_G(D)$ .*

*Proof.* We are given a block  $B$  of  $DC_G(D)$  with defect group  $D$ . Then  $B^G$  is defined, by (58.9), and  $B^G = B_1(G)$  if  $B = B_1(H)$ , by (58.10). We now have to prove that  $B^G = B_1(G)$  only if  $B = B_1(H)$ .

We begin with the special case in which  $D$  is a Sylow  $p$ -subgroup of  $G$ . Then  $D$  is a defect group of  $B_1(G)$ , and  $B_1(G)$  is the Brauer correspondent of a unique block of  $N_G(D)$  with defect group  $D$  by Brauer's First Main Theorem 58.6. Since  $B_1(N_G(D))^G = B_1(G)$  by (58.10), this unique block of  $N_G(D)$  is  $B_1(N_G(D))$ . By Theorem 61.7ii,  $B_1(N_G(D))$  covers a unique conjugacy class of blocks of  $DC_G(D)$  with defect group  $D$ . But it is immediate from (61.4) that  $B_1(N_G(D))$  covers  $B_1(H)$ , and  $B_1(H)$  has defect group  $D$  by (57.20). Clearly  $B_1(H)$  is fixed under conjugation by elements of  $N_G(D)$ , and is therefore the unique block of  $H$  with defect group  $D$  corresponding to  $B_1(G)$  by the Brauer correspondence (see (61.10)). This completes the proof for the case of a Sylow  $p$ -subgroup of  $G$ .

We now use induction on the index of  $D$  in a Sylow  $p$ -subgroup to establish the general case. Specifically, we assume that if  $D' > D$ , and  $B'$  is a block of  $D'C_G(D')$  with defect group  $D'$ , and  $(B')^G = B_1(G)$ , then  $B' = B_1(D'C_G(D'))$ .

For our given block  $B$  of  $DC_G(D)$  with defect group  $D$ , let us assume that  $B^G = B_1(G)$  and  $B \neq B_1(DC_G(D))$ , and derive a contradiction. The Brauer correspondent  $B^{N_G(D)}$  is defined, and has a defect group  $D' \geq D$  by (58.5). We may assume that  $D' > D$ , for if we have equality, then  $(B^{N_G(D)})^G = B_1(G)$ , and it follows that  $D$  is a defect group of  $B_1(G)$  by Brauer's first main theorem. Then  $D$  is a

Sylow  $p$ -subgroup of  $G$ , and we have  $B = B_1(DC_G(D))$  by the first part of the proof. So we may assume that  $D' > D$ . By Corollary 61.10, there exists a block  $B'$  of  $D'C_{N_G(D)}(D')$  with defect group  $D'$  such that  $(B')^{N_G(D)} = B^{N_G(D)}$ . This requires also the observation that  $D'C_{N_G(D)}(D') = D'C_G(D')$  since  $D' > D$ , and so  $C_G(D') \leq N_G(D)$ . We then have

$$(B')^G = ((B')^{N_G(D)})^G = (B^{N_G(D)})^G = (B_1)^G,$$

using transitivity of the Brauer correspondence. By the induction hypothesis, we obtain  $B' = B_1(D'C_G(D'))$ . Then  $(B')^{N_G(D)} = B_1(N_G(D))$  by (58.10), and hence  $B^{N_G(D)} = B_1(N_G(D))$ . But  $B_1(N_G(D))$  covers only the principal block of  $DC_G(D)$  by (61.4), and we have  $B = B_1(DC_G(D))$ ; contrary to assumption. This completes the proof.

*Proof of Theorem 61.16.* First assume that  $B = B_1(H)$ . Then  $B^G = B_1(G)$  by (58.10), in case we have  $H \leq N_G(D)$ . In the general case, we assume only that  $H \geq DC_G(D)$ , and have to use deeper properties of the Brauer correspondence, from §58C. Since  $B$  has defect group  $D$  by assumption,  $B^G$  is defined, by (58.20). Let  $M$  be the ring  $R$ , with trivial  $G$ -action; so  $M$  affords the trivial  $R$ -representation  $1_G$ . Then  $M$  belongs to  $B_1(G)$ , and the restriction  $M_H$  is indecomposable and clearly belongs to  $B_1(H)$ . Moreover, a defect group  $D$  of  $B_1(H)$  is a Sylow  $p$ -subgroup of  $H$ , and hence is a vertex of  $M_H$ , by (57.29). It follows that  $B_1(H)^G = B_1(G)$ , by Theorem 58.22, completing the proof of one implication.

Now let  $B$  be a block of  $H$  with defect group  $D$ , and assume that  $H \geq DC_G(D)$  and  $B^G = B_1(G)$ . By Theorem 58.6, there is a unique block  $\tilde{B}$  of  $N_H(D)$  with defect group  $D$  such that  $\tilde{B}^H = B$ . Then  $\tilde{B}$  covers a unique conjugacy class of blocks  $\{B'\}$  of  $DC_H(D)$  such that  $(B')^{N_H(D)} = \tilde{B}$  and  $B'$  has defect group  $D$ , by (61.10). We also note that  $DC_H(D) = DC_G(D)$  since  $H \geq C_G(D)$ . Combining these results, we obtain

$$(B')^G = ((B')^{N_H(D)})^H = ((\tilde{B})^H)^G = B^G = B_1(G),$$

by transitivity of the Brauer Correspondence. Then  $B' = B_1(DC_G(D))$  by (61.17), and hence  $B = (B')^H = B_1(H)$  by the first part of the proof. This completes the proof of the Third Main Theorem.

An interesting generalization of the Third Main Theorem was obtained by Okuyama [81]. His proof (which includes a new proof of the Third Main Theorem itself) is entirely independent of the preceding discussion, and is based instead on calculations with characters, using (58.8) to define the Brauer Correspondence.

## §62. BLOCKS WITH CYCLIC DEFECT GROUPS

The main result gives the numbers of simple and indecomposable  $kG$ -modules belonging to a  $p$ -block of  $G$  with a cyclic defect group in terms of the inertial

index of the block. The proof follows Michler [76], and draws together ideas from homological algebra, uniserial algebras, the Green Correspondence, Clifford Theory from §§11 and 19, and many other results discussed earlier in this chapter. The information about the modules in such a block provides a basis for a new construction of a periodic projective resolution of the trivial  $RG$ -module (see also Michler [75]). Dade's comprehensive results on the  $K$ -characters belonging to a cyclic block are not given in full generality, but are illustrated in §62E for the special case of a group with a cyclic self-centralizing Sylow  $p$ -subgroup which is a T.I. set. A combinatorial description of the relations between P.I.M.'s and simple  $kG$ -modules in a cyclic block, called the Brauer tree, is also given in this case. A complete and definitive account of blocks with cyclic defect groups, including Brauer's work on blocks of defect one, Dade's work [66] on cyclic blocks, with many extensions and improvements, was given by Feit [82]. It remains a challenging problem to obtain equally strong results for other types of blocks (see, for example, Broué-Puig [80]).

### §62A. Preliminary Results from Homological Algebra

In §§62A and 62B, we shall collect some elementary facts from homological algebra concerning indecomposable modules for group algebras and their connection with the Green correspondence. These will be applied in §62D on modules in blocks with cyclic defect groups, and some of them will also reappear in §§78 and 81 on Auslander-Reiten sequences and the Green ring.

In the first part of our discussion,  $G$  denotes a finite group, and  $R$  an arbitrary commutative ring. We recall some facts about the relative trace map,  $G$ -algebras, and relative projectivity, from §§19, 20, and 57.

Let  $M$  and  $N$  be f.g. left  $RG$ -modules, and let us set

$$(M, N) = \text{Hom}_R(M, N).$$

Then  $G$  acts on  $(M, N)$  according to the rule

$$x\varphi = x\varphi x^{-1}, \quad \text{for } x \in G, \quad \varphi \in (M, N).$$

For an arbitrary subgroup  $H \leq G$ , we set

$$(M, N)_H = \{\varphi \in (M, N) : x\varphi = \varphi \quad \text{for all } x \in H\}.$$

Then  $(M, N)_H$  is simply the set of  $RH$ -homomorphisms from  $M$  to  $N$ :

$$(M, N)_H = \text{Hom}_{RH}(M, N).$$

Following the terminology introduced in §57, we define the *relative trace map*

$$T_{G/H} : (M, N)_H \rightarrow (M, N)_G,$$

for  $H \leq G$ , by the formula

$$T_{G/H}\varphi = \sum_{x \in G/H} x\varphi,$$

where the sum is taken over a cross section of the set of left cosets  $G/H$ . The map  $T_{G/H}: (M, N)_H \rightarrow (M, N)_G$  is independent of the choice of a cross section. We next set

$$(M, N)_{G/H} = \text{im } T_{G/H} = T_{G/H}(M, N)_H,$$

and obtain easily:

**(62.1) Lemma.** *Let  $H \leq G$ , and let  $L, M$  and  $N$  be left  $RG$ -modules.*

- (i) *Let  $\psi \in (L, M)_G$  and  $\varphi \in (M, N)_G$ . Then  $\varphi\psi \in (L, N)_G$ . Moreover,  $\varphi\psi \in (L, N)_{G/H}$  if either  $\psi \in (L, M)_{G/H}$  or  $\varphi \in (M, N)_{G/H}$ .*
- (ii)  *$(M, M)_{G/H}$  is an ideal in  $(M, M)_G$ .*
- (iii) *A left  $RG$ -module  $M$  is  $(G, H)$ -projective if and only if  $\text{id}_M \in (M, M)_{G/H}$ .*

Parts (i) and (ii) are similar to the results in (57.3), and are left as exercises. Part (iii) is a restatement of part of Theorem 19.2.

Now let  $k$  be a field. We let  $\mathcal{P}(kG)$  denote the category of f.g. projective  $kG$ -modules, and note that a  $kG$ -module  $M$  belongs to  $\mathcal{P}(kG)$  if and only if  $M$  is  $(G, 1)$ -projective, since the coefficient ring is a field (see §19A).

**(62.2) Definitions.** Let  $M$  and  $N$  be f.g. left  $kG$ -modules. A map  $\varphi \in (M, N)_G$  is called *projective* provided that  $\varphi \in (M, N)_{G/1}$ . A *projective presentation*  $(P, \pi)$  of a  $kG$ -module  $N$  is a surjective homomorphism  $\pi: P \rightarrow N$  for some  $P \in \mathcal{P}(kG)$ . A left  $kG$ -module is called a *core* if and only if  $M$  has no nonzero projective direct summands.

From the preceding remarks, it is clear that a  $kG$ -module  $M$  is projective if and only if  $\text{id}_M$  is a projective map. The idea of a core is related to the following construction. Let  $M$  be an arbitrary f.g.  $kG$ -module. Then  $M$  can be expressed as a direct sum of indecomposable  $kG$ -modules. If we discard the projective ones, we are left with a module, called the *core* of  $M$ , which is uniquely determined, up to isomorphism, by the K-S-A Theorem. Thus a module is isomorphic to its core if it has the property stated in the last part of (62.2) (see also §78A).

We now have:

**(62.3) Proposition.** *Let  $L$  and  $M$  be  $kG$ -modules, and let  $\pi: P \rightarrow M$  be a projective presentation of  $M$ . A map  $\lambda \in (L, M)_G$  is projective if and only if there exists a map  $\mu \in (L, P)_G$  such that  $\lambda = \pi\mu$ .*

*Proof.* The condition means that for some  $h \in (L, P)_G$ , the diagram

$$\begin{array}{ccccc} & & L & & \\ & \swarrow \mu & \downarrow \lambda & & \\ P & \xrightarrow{\quad} & M \rightarrow 0 & & \\ & \pi & & & \end{array}$$

commutes. If  $\mu$  exists, then we have

$$\lambda = \pi(\text{id}_P)\mu,$$

where  $\text{id}_P$  is projective since  $P$  is a projective module. Then  $\lambda$  is a projective map, by (62.1).

Conversely, let  $\lambda$  be a projective map; then  $\lambda = T_{G/1}\lambda_0$  for some  $\lambda_0 \in (L, M)_G$ , by Definition 62.2. Since  $M$  is a projective  $k$ -module, there exists a map  $j \in (M, P)$  such that  $\pi j = \text{id}_M$ . Set

$$\mu = T_{G/1}(j\lambda_0).$$

Then  $\mu \in (L, P)_G$ , and we have

$$\pi\mu = \pi T_{G/1}(j\lambda_0) = T_{G/1}(\pi j\lambda_0) = T_{G/1}(\lambda_0) = \lambda,$$

using the basic properties of the trace map. This completes the proof.

Thus a map  $\lambda \in (L, M)_G$  is projective if and only if  $\lambda$  factors through a projective module. Let  $M^*$  denote the contragredient  $kG$ -module, for a f.g. left  $kG$ -module  $M$ . The correspondence  $M \rightarrow M^*$  is a contravariant functor from the category of f.g.  $kG$ -modules to itself, by §10D. Moreover, a f.g.  $kG$ -module is projective if and only if it is injective, by (19.2). Using these remarks, we obtain easily the following dual version of the preceding result.

**(62.4) Proposition.** *Let  $\pi': M \rightarrow Q$  be an injective embedding of a f.g. left  $kG$ -module  $M$  (that is,  $Q$  is injective and  $\ker \pi' = 0$ ). Let  $\lambda' \in (M, L)_G$ , for some f.g.  $kG$ -module  $L$ . Then  $\lambda'$  is a projective map if and only if there exists  $\mu' \in (Q, L)_G$  such that  $\lambda' = \mu'\pi'$ .*

**(62.5) Proposition.** *Let  $M$  be a core, and let  $\eta: M \rightarrow N$  be a surjective homomorphism of  $kG$ -modules. Then  $\eta$  is not projective unless  $\eta = 0$ .*

*Proof.* Let  $\pi: P \rightarrow N$  be a projective cover of  $N$  (see §6C). If  $\eta$  is projective, there exists a map  $\mu \in (M, P)_G$  such that  $\eta = \pi\mu$ , by (62.3). Since  $\eta$  is surjective, we have  $\text{im } \mu = P$  by the definition of projective covers, from §6C. Then the extension  $\mu: M \rightarrow P$  splits, since  $P$  is projective. This contradicts the assumption that  $M$  is a core, unless  $\eta = 0$ .

The dual version is:

**(62.6) Corollary.** *Let  $M$  be a core, and let  $\eta':M \rightarrow N$  be a homomorphism of  $kG$ -modules such that  $\ker \eta' = 0$ . Then  $\eta'$  is not projective unless  $\eta' = 0$ .*

**(62.7) Proposition.** *Let  $M$  and  $N$  be f.g.  $kG$ -modules. Then  $(M, N)_{G/1} = 0$  if either of the following statements hold:*

- (i)  *$M$  is a core and  $N$  is simple.*
- (ii)  *$M$  is simple and  $N$  is a core.*

*Proof.* Let  $\eta \in (M, N)_{G/1}$ , and assume  $\eta \neq 0$ . Then, in case (i),  $\eta$  is surjective, and is a projective map by (62.2). This contradicts (62.5). In case (ii), we contradict (62.6) unless  $(M, N)_{G/1} = 0$ .

**(62.8) Corollary.** *Let  $M$  be simple and nonprojective. Then  $(M, M)_{G/1} = 0$ .*

## §62B. Functorial Properties of the Green Correspondence

In this subsection, we extend the Green correspondence from indecomposable lattices, as in §20A, to maps in the category of  $RG$ -lattices. These results, which are due to Feit [69] and Green [72], are interesting in themselves, and have important applications to modules in blocks with cyclic defect groups (see §§62D, E).

Throughout the discussion,  $G$  denotes a finite group, and  $R$  denotes either a field of characteristic  $p > 0$  or a d.v.r. whose residue field  $R/p$  has characteristic  $p > 0$ , and with the property that  $R$  is complete in the  $p$ -adic topology. Then the K-S-A Theorem holds, in the category of  $RH$ -lattices, for an arbitrary subgroup  $H \leq G$ .

We first proceed to extend some of the concepts introduced in §62A to a more general situation. Let  $\mathcal{Z} = \{Z_i\}$  be a family of subgroup of  $G$ . Let  $M, N$  be  $RG$ -lattices, and let

$$(M, N)_{G, \mathcal{Z}} = \sum_{Z_i \in \mathcal{Z}} T_{G/Z_i}(M, N)_{Z_i},$$

where  $T_{G/Z_i}$  is the relative trace map defined in §62A. In particular, we have  $(M, M)_{G, \mathcal{Z}} = (M, N)_{G/Z}$  as in §62A, in case  $\mathcal{Z}$  contains only the subgroup  $Z$ .

We shall call a map  $\mu \in (M, N)_G$  a  $(G, \mathcal{Z})$ -projective map in case  $\mu \in (M, N)_{G, \mathcal{Z}}$ . An  $RG$ -lattice  $M$  is called  $(G, \mathcal{Z})$ -projective if and only if the identity map  $\text{id}_M$  is  $(G, \mathcal{Z})$ -projective (see (62.1 iii)). It is easily shown, using Rosenberg's Lemma 57.8, that this concept of a  $(G, \mathcal{Z})$ -projective  $RG$ -lattice agrees with Definition 20.1 (see Exercise 1). An  $RG$ -lattice  $M$  is called a  $(G, \mathcal{Z})$ -core (see (62.2)) provided that  $M$  contains no nonzero  $(G, \mathcal{Z})$ -projective direct summands. It follows from the K-S-A Theorem that each  $RG$ -lattice  $M$  has a decomposition

$$(62.9) \quad M = f_{\mathcal{Z}}M \oplus M;$$

where  $f_{\mathcal{X}}M$  is a  $(G, \mathcal{X})$ -core and  $M'$  is  $(G, \mathcal{X})$ -projective, and that the  $RG$ -lattices  $f_{\mathcal{X}}M$  and  $M'$  are uniquely determined up to isomorphism.

We now apply these ideas to the Green correspondence. As in §20A,  $(G, H, D)$  denotes an admissible triple, consisting of a  $p$ -subgroup  $D \leq G$ , and  $H \leq G$  such that  $H \geq N_G(D)$ . We then let  $\mathcal{X}$  and  $\mathcal{Y}$  denote the families of subgroups.

$$\begin{aligned}\mathcal{X} &= \{{}^x D \cap H : x \in G - H\} \\ \mathcal{Y} &= \{{}^x D \cap H : x \in G - H\}.\end{aligned}$$

We note that  $\mathcal{X} \leq_H \mathcal{Y}$ , in the sense that for every subgroup  $X \in \mathcal{X}$ , there exists a subgroup  $Y \in \mathcal{Y}$  such that  $X \leq_H Y$ . We shall use the notation  $A \leq_H \mathcal{X}$ , for  $A \leq G$ , to indicate that  $A \leq_H X$  for some subgroup  $X \in \mathcal{X}$ .

Our first result is simply a reinterpretation of the Green correspondence 20.6 in terms of the concepts introduced in this subsection.

**(62.10) Proposition.** *Let  $M$  be an indecomposable  $RG$ -lattice whose vertex  $D^*$  satisfies the conditions*

$$D^* \leq D \quad \text{and} \quad D^* \not\leq_G \mathcal{X}.$$

Let

$$M_H = f_{\mathcal{Y}}M_H \oplus M'_H$$

be the decomposition (62.9) of the restriction  $M_H$  of  $M$  to  $RH$ , where  $f_{\mathcal{Y}}M_H$  is an  $(H, \mathcal{Y})$ -core and  $M'_H$  is  $(H, \mathcal{Y})$ -projective. Then  $f_{\mathcal{Y}}M_H$  is an indecomposable  $RH$ -lattice with vertex  $D^*$ , and is isomorphic to the Green correspondent of  $M$  in the category of  $RH$ -lattices.

The proof is an immediate consequence of (20.6), and is left to the reader.

To simplify notation we set

$$(62.11) \quad fM = f_{\mathcal{Y}}M_H,$$

for an arbitrary  $RG$ -lattice  $M$ ; then  $fM$  is a uniquely determined  $RH$ -lattice having no nonzero  $(H, \mathcal{Y})$ -projective direct summands. Moreover, we have:

**(62.12) Proposition.** *Let  $M$  be a  $(G, D)$ -projective  $RG$ -lattice, and let  $fM$  be the  $RH$ -lattice defined by (62.11). Then  $fM$  is  $(H, D)$ -projective.*

*Proof.* Since  $M$  is  $(G, D)$ -projective, we have  $M|L^G$  for some  $RD$ -lattice  $L$ , by (19.2v). Then  $M_H|(L^G)_H$ , and hence  $M_H$  is  $(H, D)$ -projective, because  $(L^G)_H$  is a direct sum of  $RH$ -lattices each of which is  $(H, D)$ -projective by Mackey's Theorem 19.6 and (19.2v) together with (19.5 viii). The result follows, since  $fM|M_H$ .

The main result of this subsection is the following theorem of Green [72].

**(62.13) Theorem.** Let  $M$  and  $N$  be  $(G, D)$ -projective  $RG$ -lattices, and let  $fM$  and  $fN$  be the  $(H, D)$ -projective  $RH$ -lattices defined by (62.11). Then there exists an isomorphism of  $R$ -modules

$$(M, N)_G / (M, N)_{G, \mathcal{X}} \cong (fM, fN)_H / (fM, fN)_{H, \mathcal{X}}.$$

The proof is based on a series of lemmas.

**(62.14) Lemma.** Let  $U, V, W$  be  $RH$ -lattices, and let  $\alpha \in (U, V)_H$ ,  $\beta \in (V, W)_H$ . Then  $\beta\alpha \in (U, W)_{H, \mathcal{X}}$  if one of the maps is  $(H, D)$ -projective and the other is  $(H, \mathcal{Y})$ -projective.

*Proof.* Let us first assume that, for some subgroup  $Y \in \mathcal{Y}$ ,

$$\alpha = T_{H/D}\xi \quad \text{and} \quad \gamma = T_{H/Y}\eta,$$

where  $\xi \in (U, V)_D$  and  $\eta \in (V, W)_Y$ . Then

$$\gamma\alpha = (T_{H/Y}\eta)(T_{H/D}\xi) = \sum_z T_{H/D \cap {}^z Y}(z\eta \cdot \xi),$$

where  $z\eta \in (V, W)_{zY}$ , and the sum is taken over a cross section of the double cosets  $D \backslash H / Y$ , by the proof of (57.5). For each  $z$  in the cross section, we have

$$D \cap {}^z Y \leq D \quad \text{and} \quad D \cap {}^z Y \leq_H Y,$$

for  $Y \in \mathcal{Y}$ . This implies that  $D \cap {}^z Y \leq_H \mathcal{X}$  for each  $z$ , and hence  $\gamma\alpha$  is  $(H, \mathcal{X})$ -projective. Since an arbitrary  $(H, \mathcal{Y})$ -projective map  $\beta \in (V, W)_{H, \mathcal{Y}}$  can be expressed as a sum  $\beta = \sum \beta_i$ , with  $\beta_i \in (V, W)_{H/Y_i}$  for some subgroups  $Y_i \in \mathcal{Y}$ , the preceding calculation shows that  $\beta\alpha \in (U, W)_{H, \mathcal{X}}$ , as required. A similar argument applies if the assumptions concerning  $\alpha$  and  $\beta$  are reversed.

Now let  $M$  be a  $(G, D)$ -projective  $RG$ -lattice, and let

$$M_H = fM \oplus M',$$

with  $fM$  as in (62.11), and  $M'$   $(H, \mathcal{Y})$ -projective. Associated with this decomposition there are injection and projection maps

$$M_H \xrightarrow[i]{p} fM, \quad \text{and} \quad M_H \xleftarrow[i']{p'} M',$$

with  $pi = \text{id}_{fM}$ ,  $p'i' = \text{id}_{M'}$ . Setting  $\varepsilon = ip$ ,  $\varepsilon' = ip'$ , it follows that  $\varepsilon$  and  $\varepsilon'$  are orthogonal idempotents in  $(M_H, M_H)_H$ , whose sum is  $\text{id}_{M_H}$ . We shall write  $i_M$ ,  $p_M$ , etc., to indicate that these maps are associated with a given module  $M$ .

It is now easy to prove:

**(62.15) Lemma.** *Let  $M$  and  $N$  be  $(G, D)$ -projective  $RG$ -lattices, and keep the preceding notation. There is an isomorphism of  $R$ -modules*

$$\mu: (M_H, N_H)_{H/D}/(M_H, N_H)_{H,\mathcal{X}} \cong (fM, fN)_{H/D}/(fM, fN)_{H,\mathcal{X}},$$

with inverse  $v$ , where the maps are defined by

$$\begin{aligned}\mu[\lambda] &= [p_N \lambda i_M], \lambda \in (M_H, N_H)_{H/D}, \\ v[\alpha] &= [i_N \alpha p_M], \alpha \in (fM, fN)_{H/D}.\end{aligned}$$

Here, the brackets indicate elements of the factor modules given above.

*Proof.* First of all, it is clear that

$$(M_H, N_H)_{H,\mathcal{X}} \leq (M_H, N_H)_{H/D} \quad \text{and} \quad (fM, fN)_{H,\mathcal{X}} \leq (fM, fN)_{H/D},$$

since each subgroup in  $\mathcal{X}$  lies in  $D$ . Now let  $\lambda \in (M_H, N_H)_{H/D}$ . Then  $\lambda \in (M_H, N_H)_{H,\mathcal{Y}}$  since  $\mathcal{X} \leq_H \mathcal{Y}$ , and it follows that  $p_M \lambda i_M \in (fM, fN)_{H,\mathcal{X}}$  by Lemma 62.14, since the other factors are  $(H, D)$ -projective maps. For example,  $i_M: fM \rightarrow M_H$  is  $(H, D)$ -projective since both  $M_H$  and  $fM$  are  $(H, D)$ -projective  $RH$ -modules, by (62.12) (see also Exercise 2). We have now proved that the map  $\mu$ , given above, is a well-defined  $R$ -homomorphism. Similarly, the same is true for  $v$ .

Now let  $\lambda \in (M_H, N_H)_{H/D}$ . Then we have

$$\lambda = (\varepsilon_N + \varepsilon'_N)\lambda(\varepsilon_M + \varepsilon'_M) = \varepsilon_N \lambda \varepsilon_M + \varepsilon'_N \lambda \varepsilon_M + \varepsilon_N \lambda \varepsilon'_M + \varepsilon'_N \lambda \varepsilon'_M,$$

and it follows that

$$v\mu[\lambda] = [i_N p_N \lambda i_M p_M] = [\varepsilon_N \lambda \varepsilon_M] = [\lambda],$$

since the other terms  $\varepsilon'_N \lambda \varepsilon_M, \varepsilon_N \lambda \varepsilon'_M, \varepsilon'_N \lambda \varepsilon'_M$  belong to  $(M_H, N_H)_{H,\mathcal{X}}$ , by Lemma 62.14 again. On the other hand, for  $\alpha \in (fM, fN)_{H/D}$ , we have

$$\mu v[\alpha] = [p_N i_N \alpha p_M i_M] = [\alpha],$$

since  $p_M i_M = \text{id}_{fM}$ , and similarly for  $N$ . This completes the proof.

Using (62.15), to complete the proof of Green's Theorem we need only establish:

**(62.16) Lemma.** *Keep the preceding notation. There exists an isomorphism of  $R$ -modules*

$$(M_H, N_H)_{H/D}/(M_H, N_H)_{H,\mathcal{X}} \cong (M, N)_{G/D}/(M, N)_{G,\mathcal{X}}.$$

*Proof.* The modules  $M, N$  and  $M_H, N_H$  are  $(G, D)$ -projective and  $(H, D)$ -

projective, respectively. By the proof of (62.12) and Exercise 2, we have  $(M, N)_G = (M, N)_{G/D}$ , and  $(M_H, N_H)_H = (M_H, N_H)_{H/D}$ . It follows that

$$\begin{aligned}\beta \in (M_H, N_H)_{H/D} &\Rightarrow T_{G/H}\beta \in (M, N)_{G/D}, \\ \alpha \in (M, N)_{G/D} &\Rightarrow R_{G/H}\alpha \in (M_H, N_H)_{H/D},\end{aligned}$$

where  $T_{G/H}$  is the relative trace map, and  $R_{G/H}$  the inclusion map.

We next observe that, from the proof of (57.5i), we have for all  $\xi \in (M_D, N_D)_D$ :

$$R_{G/H}T_{G/D}\xi = \sum T_{H/H \cap {}^x D}R_{{}^x D/H \cap {}^x D}{}^x \cdot \xi,$$

where the sum is taken over a cross section of  $H \setminus G/D$ . Using this formula, we obtain

$$(62.17) \quad R_{G/H}T_{G/H}\beta \equiv \beta \pmod{(M_H, N_H)_{H,\mathcal{Y}}}$$

for all  $\beta \in (M_H, N_H)_{H/D}$ . This follows since  $\beta = T_{H/D}\xi$  for some  $\xi \in (M_D, N_D)_D$ , so we have

$$\begin{aligned}R_{G/H}T_{G/H}\beta &= R_{G/H}T_{G/D}\xi = T_{H/D}\xi + \sum_{x \notin H} T_{H/H \cap {}^x D}R_{{}^x D/H \cap {}^x D}{}^x \cdot \xi \\ &\equiv \beta \pmod{(M_H, N_H)_{H,\mathcal{Y}}},\end{aligned}$$

since the subgroups  $H \cap {}^x D$  belong to  $\mathcal{Y}$  for all  $x \in G - H$ . The same argument shows that

$$(62.18) \quad R_{G/H}(M, N)_{G/D} \leq (M_H, N_H)_{H/D} + (M_H, N_H)_{H,\mathcal{Y}}.$$

We next prove that

$$(62.19) \quad R_{G/H}(M, N)_{G,\mathcal{X}} \leq (M_H, N_H)_{H,\mathcal{Y}}.$$

Let  $X \in \mathcal{X}$ ; then for  $\eta \in (M_X, N_X)_X$ , we have

$$R_{G/H}T_{G/X}\eta = \sum_z T_{H/H \cap {}^z X}R_{{}^z X/H \cap {}^z X}{}^z \eta,$$

where the sum is taken over a cross section of  $H \setminus G/X$ . Moreover,  $X = {}^x D \cap D$  for some  $x \in G - H$ , so

$$H \cap {}^z X = H \cap {}^{zx} D \cap {}^z D \leq Y$$

for some subgroup  $Y \in \mathcal{Y}$ , since for each  $z$ , either  $zx \in G - H$  or  $z \in G - H$ . This proves (62.19).

Now let

$$Q = (M_H, N_H)_{H/D} \cap (M_H, N_H)_{H,\mathcal{Y}},$$

and note that  $(M_H, N_H)_{H,\mathcal{X}} \leq Q$ . Consider the diagram of  $R$ -modules and  $R$ -homomorphisms

$$(62.20) \quad \begin{array}{ccc} \frac{(M_H, N_H)_{H/D}}{(M_H, N_H)_{H,\mathcal{X}}} & \xrightarrow{t} & \frac{(M, N)_{G/D}}{(M, N)_{G,\mathcal{X}}} \\ q \downarrow & & r \downarrow \\ \frac{(M_H, N_H)_{H/D}}{Q} & \xleftarrow{s} & \frac{(M_H, N_H)_{H/D} + (M_H, N_H)_{H,\mathcal{Y}}}{(M_H, N_H)_{H,\mathcal{Y}}} \end{array}$$

The map  $q$  is surjective, and  $s$  is the natural isomorphism. Further,  $t$  is a well-defined surjection defined by  $T_{G/H}$ , since

$$T_{G/H}(M_H, N_H)_{H,\mathcal{X}} \leq (M, N)_{G,\mathcal{X}}.$$

The map  $r$  is given by  $R_{G/H}$ , using (62.18) and (62.19).

We now show that the diagram (62.20) commutes, that is,  $q = srt$ . Let  $x \in (M_H, N_H)_{H/D}$ , and let  $\bar{x}$  be its class in the quotient module. Then

$$(rt)\bar{x} = \text{class of } R_{G/H}T_{G/H}x = x + (M_H, N_H)_{H,\mathcal{Y}}$$

by (62.17). Then  $(srt)\bar{x} = x + Q = q\bar{x}$ , as required.

By (62.20) we have

$$\ker t \leq \ker q = Q/(M_H, N_H)_{H,\mathcal{X}}.$$

But  $\ker q = 0$ , since each  $\lambda \in Q = (M_H, N_H)_{H/D} \cap (M_H, N_H)_{H,\mathcal{Y}}$  can be factored as a product of an  $(H, D)$ -projective map and an  $(H, \mathcal{Y})$ -projective map, and hence is  $(H, \mathcal{X})$ -projective by (62.14). Thus  $t$  is an isomorphism, and the lemma is proved.

This completes the proof of Theorem 62.13.

### §62C. Uniserial Algebras and Blocks of Finite Representation Type

In this subsection,  $k$  denotes a field of characteristic  $p > 0$ . A f.d.  $k$ -algebra  $A$  is called a  $k$ -algebra of *finite representation type* if the number of isomorphism classes of indecomposable left  $A$ -modules is finite. We shall first obtain sufficient condition for a block ideal in  $kG$  to be of finite representation type, in terms of the defect group of the block. As we shall see, this result includes D. Higman's criterion for the group algebra  $kG$  itself to be of finite representation type (see CR 64.1). The rest of the subsection will be devoted to the study of a particularly important family of algebras of finite representation type, called uniserial algebras. While not all block ideals of finite representation type are uniserial, uniserial blocks play a crucial role in our analysis of blocks with cyclic defect groups in §62D, E.

**(62.21) Theorem.** Let  $B$  be a block ideal in  $kG$ , and let  $D$  be a defect group of the corresponding block. Then  $B$  is of finite representation type if and only if  $D$  is cyclic.

*Proof.* Let us assume  $D = \langle x \rangle$  is a cyclic group of order  $d$  with generator  $x$ ; then  $kD$  has exactly  $d$  isomorphism classes of indecomposable modules, by linear algebra. If  $D$  is the defect group of the block  $B$ , then every  $B$ -module is  $(G, D)$ -projective, by (57.27). Let  $\{T_j : 1 \leq j \leq d\}$  be a basic set of indecomposable  $kD$ -modules. By the K-S-A Theorem, the number of isomorphism classes of indecomposable  $kG$ -modules  $M$  such that  $M|T_j^G$ , for  $1 \leq j \leq d$ , is finite. If  $M$  is an indecomposable  $kG$ -module belonging to the block  $B$ , then it follows from the K-S-A Theorem that  $M|T_j^G$  for some  $j$ ,  $1 \leq j \leq d$ , since  $M$  is  $(G, D)$ -projective. Therefore  $B$  has finite representation type. For the converse, see Benson [84a].

The preceding result implies that if  $G$  has a cyclic Sylow  $p$ -subgroup, then  $kG$  is of finite representation type, for an arbitrary field  $k$  of characteristic  $p$ . Higman's Theorem (CR(64.1)) also asserts that if the Sylow  $p$ -subgroups of  $G$  are not cyclic, then  $kG$  has indecomposable modules of arbitrarily large dimension over  $k$ . The corresponding result for block ideals holds, but the proof is more complicated and will not be given here.

Let  $A$  be an arbitrary f.d.  $k$ -algebra. We recall from §56A that a *principal indecomposable module* (P.I.M.), or *projective indecomposable module*, is an indecomposable direct summand of  $A$ . Each (left) P.I.M. has the form  $Ae$ , with  $e$  a primitive idempotent in  $A$ .

**(62.22) Definition.** Let  $A$  be a f.d.  $k$ -algebra. A f.g. left  $A$ -module  $M$  is called a *uniserial module* if  $M$  has a unique composition series. (Every submodule and factor module of  $M$  is then also uniserial.) We shall call  $A$  a *uniserial  $k$ -algebra* if every left or right P.I.M. is a uniserial module.

We first make some simple observations. Let  $N = \text{rad } A$ , and let  $M$  be a f.g. left  $A$ -module. *The radical series*

$$M \supset N M \supset N^2 M \supset \dots$$

is a chain of submodules such that each quotient  $N^i M / N^{i+1} M$  is annihilated by  $N$ , and hence is a semisimple  $A$ -module. It follows that

(62.23)  $M$  is uniserial  $\Leftrightarrow N^i M / N^{i+1} M$  is simple, for  $i = 0, 1, 2, \dots$

For each f.g. left  $A$ -module  $M$ , the  $k$ -dual  $M^* = \text{Hom}_k(M, k)$  is a f.g. right  $A$ -module, with the module operation defined by

$$(fa)(m) = f(am), \quad \text{for } f \in M^*, \quad a \in A, \quad m \in M.$$

It is easily checked that  $M \rightarrow M^*$  is a contravariant functor from the category

of f.g. left  $A$ -modules to the category of f.g. right  $A$ -modules (see §9A). A f.g. left  $A$ -module  $M$  is uniserial if and only if the right module  $M^*$  is uniserial (see Exercise 4). It also follows that a f.g. left  $A$ -module  $M$  is projective if and only if its  $k$ -dual  $M^*$  is a f.g. injective right module. Thus we have at once:

**(62.24) Proposition.** *A f.d.  $k$ -algebra  $A$  is uniserial if and only if every indecomposable projective or injective left  $A$ -module is uniserial.*

The next result, due to Nakayama [40], is proved by using the theory of projective covers and injective hulls (see §6D).

**(62.25) Theorem.** *Let  $A$  be f.d. uniserial  $k$ -algebra. Then  $A$  has finite representation type. Moreover, every f.g. indecomposable left  $A$ -module  $M$  is uniserial, and is a homomorphic image of an indecomposable projective module.*

*Proof* (Feit [82]). It is clearly sufficient to prove that every f.g. left  $A$ -module  $M$  is a direct sum of uniserial modules, since every uniserial module is a homomorphic image of an indecomposable projective module (Exercise 5.) We shall use induction on  $\dim_k M$ . The result is clearly true if  $M$  is a simple module, so let us assume  $M$  is not simple. Let  $T$  be a maximal uniserial submodule of  $M$ , and let  $U$  be a submodule which is maximal with respect to the property  $U \cap T = 0$ . We may assume  $0 < \dim_k T < \dim_k M$ .

We prove first that  $M/U$  has a simple socle. Let  $U_0 \supseteq U$ , and assume that  $U_0/U$  is a simple submodule of  $M/U$ . Then  $U_0 \cap T \neq 0$  by the maximality of  $U$ , and we have  $N(U_0 \cap T) = 0$  where  $N = \text{rad } A$ , since  $N(U_0 \cap T) \subseteq U \cap T = 0$ . Since  $T$  is uniserial,  $U_0 \cap T$  coincides with  $\text{soc } T$ , and hence  $U_0 = U + (U_0 \cap T)$  is uniquely determined. It follows that  $\text{soc } M/U = U_0/U$ , and is a simple module.

The injective hull of  $M/U$  also has a simple socle, and is indecomposable and hence uniserial, by (62.24), since  $A$  is uniserial. Since  $M/U$  is isomorphic to a submodule of its injective hull,  $M/U$  is uniserial, so  $F = (M/U)/\text{rad}(M/U)$  is a simple module. Let  $P$  be the projective cover of  $F$ ; then  $P$  is a P.I.M., hence uniserial, and there exists a commutative diagram

$$\begin{array}{ccccc} & & P & & \\ & g \swarrow & \downarrow f & & \\ M & \xrightarrow{h} & M/U & \longrightarrow & 0 \end{array}$$

with  $f$  surjective, and  $\ker h = U$ , using the facts that  $P$  is projective and  $M/U$  is uniserial (see Exercise 5).

The next step is to observe that  $g(P)$  is a uniserial submodule of  $M$ , and  $M = g(P) + U$  since  $f$  is surjective. Then  $M/U \cong g(P)/(g(P) \cap U)$ , so  $\dim_k g(P) \geq \dim_k T$  since  $T \cap U = 0$ . Moreover,  $\dim_k g(P) = \dim_k T$ , since  $T$  is a uniserial submodule of maximal dimension. It then follows that  $g(P) \cap U = 0$ , again by consideration of  $\dim_k M/U$ . Therefore  $M = g(P) \oplus U$ , and  $U$  is a direct sum of

uniserial modules by the induction hypothesis. This completes the proof of the theorem.

As in the case of group algebras, an arbitrary f.d.  $k$ -algebra  $A$  can be expressed as a direct sum

$$A = A_1 \oplus \cdots \oplus A_m$$

of indecomposable two-sided ideals, called *blocks* or *block ideals*. These are generated by primitive idempotents in the center of  $A$ , called *block idempotents* (see §56 or CR §55). Next, let  $U = Ae$  be a P.I.M., where  $e$  is a primitive idempotent in  $A$ . The *multiplicity* of  $U$  in  $A$  is, by definition, the number of summands isomorphic to  $U$  which occur in the decomposition of the left regular module  ${}_AA$  into a direct sum of P.I.M.'s. Note that the P.I.M.'s are distributed into blocks, and each P.I.M. is contained in some block of  $A$ .

**(62.26) Theorem (Morita [51]).** *Let  $A$  be a f.d.  $k$ -algebra, and let  $N = \text{rad } A$ . Then the following are equivalent:*

- (i)  $N = cA = Ac$  for some element  $c \in A$ .
- (ii)  $A$  is a uniserial algebra, and has the further property that for each block of  $A$ , all the P.I.M.'s in that block occur with the same multiplicity in  $A$ .

*Proof.* Assume (i), and let us first prove that  $A$  is uniserial. We have  $N^i = Ac^i = c^iA$  for  $i = 1, 2, \dots$ . Let  $Ae$  be an indecomposable projective left ideal in  $A$ , generated by a primitive idempotent  $e$ , and let  $L$  be a nonzero left ideal contained in  $Ae$ . We shall prove that  $L = N^i e$  for some  $i$ . Suppose  $L \subseteq N^i e$  and  $L \not\subseteq N^{i+1} e$ . Let  $a \in L$  be an element such that  $a \notin N^{i+1} e$ . Since  $N^i e = c^i Ae$ , we have

$$a = c^i a_0, \quad \text{where } a_0 \in Ae, \quad a_0 \notin Ne.$$

Then  $Aa_0 \not\subseteq Ne$ , and since  $Ne$  is the unique maximal submodule of  $Ae$ , we obtain  $Aa_0 = Ae$ . Then

$$L \supseteq Aa \supseteq Ac^i a_0 = N^i a_0 = N^i Ae = N^i e,$$

and hence  $L = N^i e$ . This proves that  $Ae$  is uniserial. The same argument shows that  $eA$  is uniserial, so we have proved that  $A$  is uniserial, and must still establish the remaining assertion in (ii).

Let us write

$$A = \bigoplus_i \bigoplus_{j=1}^{f(i)} Ae_{ij},$$

where the  $\{e_{ij}\}$  are primitive idempotents, numbered so that

$$(62.27) \quad Ae_{ij} \cong Ae_{i'j'} \Leftrightarrow e_{ij}A \cong e_{i'j'}A \Leftrightarrow i = i'.$$

Then  $f(i)$  is the multiplicity of  $Ae_{ij}$  as a direct summand of  $_AA$ , for each  $i, j$ .

The P.I.M.'s  $\{Ae_{ij}\}$  have the following properties, which hold because  $A$  is uniserial and (by hypothesis)  $N^j = c^j A = Ac^j$  for each  $j \geq 1$ .

**(62.28) Lemma.** *We have<sup>†</sup> for  $j \geq 1$ ,*

- (i)  $Ac^j e_{ki} \cong Ac^j e_{k1}$ ,  $1 \leq i \leq f(k)$ .
- (ii)  $Ae_{ki}c^j \cong Ae_{k1}c^j$ ,  $1 \leq i \leq f(k)$ .
- (iii)  $Ac^j e_{k1} \not\cong Ac^j e_{l1}$  if  $k \neq l$ .
- (iv)  $Ae_{k1}c^j \not\cong Ae_{l1}c^j$  if  $k \neq l$ .
- (v)  $Ac^j e_{ki}$  and  $Ae_{ki}c^j$  are indecomposable left ideals.

*Sketch of proof.* Since  $Ae_{ki} \cong Ae_{k1}$ , the terms of their radical series  $\{N^j e_{ki}\}$  and  $\{N^j e_{k1}\}$  are isomorphic, and the terms of their socle series  $Ae_{ki} \cap r(N^j)$  and  $Ae_{k1} \cap r(N^j)$  are also isomorphic. The first two statements of (62.28) follow from these remarks, since  $N^j = c^j A = Ac^j$ . For the proof of (iii), assume that  $Ac^j e_{k1} \cong Ac^j e_{l1}$ . Then  $N^j e_{k1} \cong N^j e_{l1}$ . Moreover,  $N^j e_{k1}/N^{j+1} e_{k1} \cong N^j e_{l1}/N^{j+1} e_{l1} \cong Ae/Ne$  for some primitive idempotent  $e$ , since  $A$  is uniserial. Consequently there exist elements  $a \in eN^j e_{k1}$  and  $b \in eN^j e_{l1}$  such that  $a, b \notin N^{j+1}$  and

$$eN^j = aA = bA = ae_{k1}A = be_{l1}A.$$

Then there exist surjective homomorphisms

$$e_{k1}A \rightarrow eN^j \quad \text{and} \quad e_{l1}A \rightarrow eN^j,$$

and it follows that  $k = l$  by (62.27). The other statements are easily proved, and are left as exercises.

Continuing with the proof of Theorem 62.26, we now have

$$N^j = \bigoplus_{k=1}^d \bigoplus_{i=1}^{f(k)} Ac^j e_{ki} = \bigoplus_{l=1}^d \bigoplus_{i'=1}^{f(l)} Ae_{li'}c^j, \quad \text{for } j \geq 1.$$

Since the summands are indecomposable, the K-S-A Theorem and (62.28) imply that there exists a permutation  $\pi$  of  $\{1, 2, \dots, d\}$  such that

$$Ac^j e_{ki} \cong Ae_{\pi(k)i'}c^j \quad \text{and} \quad f(k) = f(\pi(k)),$$

where we omit the terms which are zero. We also have

$$N^j e_{k1}/N^{j+1} e_{k1} \cong Ae_{\pi(k), 1}/Ne_{\pi(k), 1} \quad \text{if } Ac^j e_{k1} \neq 0.$$

Since the block ideals of  $A$  are the sums of linkage classes of P.I.M.'s (see §56 or CR §55), it follows that the multiplicities  $f(k)$  are the same for the P.I.M.'s  $\{Ae_{ki}\}$  belonging to a given block ideal. Thus (i) implies (ii), as asserted in the theorem.

<sup>†</sup>These formulas hold for all  $j \geq 1$  for which the corresponding left ideals are different from zero.

Conversely, let us assume (ii) and prove (i). We put

$$Ne_{k1}/N^2e_{k1} \cong Ae_{\varphi(k)1}/Ne_{\varphi(k)1}.$$

As before,  $k \neq l$  implies  $\varphi(k) \neq \varphi(l)$ , and since  $Ae_{k1}$  and  $Ae_{\varphi(k)}$  are contained in the same block, we have  $f(k) = f(\varphi(k))$ . It follows that for all  $k$  and  $i$ , there exists  $c_{ki} \in e_{\varphi(k)i}Ne_{ki}$ , with  $c_{ki} \notin N^2$  and such that

$$Ac_{ki} \cong Ne_{ki} \quad \text{and} \quad c_{ki}A = e_{\varphi(k)i}N,$$

since  $A$  is uniserial. We then put  $c = \sum_{k,i} c_{ki}$ , and obtain

$$Ac = \sum Ac_{ki},$$

and therefore  $N = Ac$  by the preceding remarks. A similar argument shows that  $N = cA$ , and the proof of the theorem is completed.

The next result shows that the composition factors of the P.I.M.'s in a given block of a uniserial symmetric algebra occur in a periodic manner. This will be applied in §62E to obtain a periodic projective resolution of the trivial  $RG$ -module, in case  $G$  has a cyclic Sylow  $p$ -subgroup.

**(62.29) Theorem (Morita [51]).** *Let  $A$  be a f.d.  $k$ -algebra which is uniserial and symmetric (see §9A), and let  $N = \text{rad } A$ . Let  $\{U_1, \dots, U_m\}$  be a basic set of P.I.M.'s belonging to an arbitrary block of  $A$ , and let  $\{F_1, \dots, F_m\}$  be the corresponding simple modules, so that  $F_i = U_i/\text{rad } U_i$ ,  $1 \leq i \leq m$ . Then the composition lengths of any two of the modules  $\{U_i\}$  are equal. Moreover, for a suitable ordering of  $\{1, \dots, m\}$  the composition factors of the  $U_i$  occur as follows:*

$$\begin{aligned} U_1 &: F_1, F_2, \dots, F_m, F_1, \dots, F_m, \dots, F_1, \dots, F_m, F_1 \\ U_2 &: F_2, F_3, \dots, F_1, F_2, \dots, F_1, \dots, F_2, \dots, F_1, F_2 \\ &\dots \\ U_m &: F_m, F_1, \dots, F_{m-1}, F_m, \dots, F_{m-1}, \dots, F_m, \dots, F_{m-1}, F_m, \end{aligned}$$

where, for example,  $F_1, F_2, \dots, F_m, \dots, F_1, \dots, F_m, F_1$  are the factors of the radical series  $U_1 \supset N U_1 \supset N^2 U_1 \supset \dots$  of  $U_1$ .

The proof uses some facts about symmetric algebras from §9A. We first prove:

**(62.30) Lemma.** *Let  $A$  satisfy the hypotheses of Theorem 62.29. Let  $N = \text{rad } A$ , and let  $e$  and  $f$  be primitive idempotents such that*

$$Ne/N^2e \cong Af/Nf.$$

*Then we have*

$$Ne \cong Af/\text{soc } Af.$$

*Proof.* Since  $A$  is uniserial, we have

$$Ne = Ab \quad \text{and} \quad fN = bA$$

for some element  $b \in fNe$  such that  $b \notin N^2$  (see the last part of the proof of Theorem 62.26). Then the map  $af \rightarrow afb$  (for  $a \in A$ ) is a surjective homomorphism from  $Af$  to  $Ab = Ne$ , and hence defines an isomorphism

$$Af/(Af \cap l(b)) \cong Ne,$$

where<sup>†</sup>  $l(b) = \{x \in A : xb = 0\}$ . We then have

$$Af \cap l(b) = Af \cap l(N),$$

since  $l(N) \subseteq l(b)$ , and  $x \in Af \cap l(b)$  implies  $xN = xfN = xbA = 0$ . Moreover,  $l(N) = r(N)$  by (9.9) since  $A$  is a symmetric algebra, and we obtain

$$Af \cap l(N) = Af \cap r(N) = \text{soc } Af,$$

completing the proof.

*Proof of Theorem 62.29.* Since the number of isomorphism classes of simple  $A$ -modules is finite, it is clear that there exists a sequence of nonisomorphic P.I.M.'s  $\{U_1, \dots, U_m\}$  such that

$$\begin{aligned} NU_1/N^2U_1 &\cong U_2/NU_2, \\ NU_2/N^2U_2 &\cong U_3/NU_3, \dots, \quad NU_m/N^2U_m \cong U_1/NU_1, \end{aligned}$$

for some integer  $m \geq 1$ , with the understanding that in case  $m = 1$ , we have  $NU_1/N^2U_1 \cong U_1/NU_1$ . Then  $U_i/NU_i \cong \text{soc } U_i$  for  $1 \leq i \leq m$  by (9.12), since  $A$  is a symmetric algebra. It follows by Lemma 62.30 that the composition factors of  $\{U_1, \dots, U_m\}$  occur as asserted in (62.29). Then no simple module other than  $\{F_1, \dots, F_m\}$  can occur as a composition factor of  $\{U_1, \dots, U_m\}$  and hence  $\{U_1, \dots, U_m\}$  is a basic set of P.I.M.'s belonging to a block ideal of  $A$  (see §56C or CR §55). Upon splitting off this block ideal, we can repeat the argument with the remaining P.I.M.'s, and the theorem follows.

**(62.31) Corollary.** *Let  $A$  be a f.d.  $k$ -algebra which is uniserial, symmetric, and indecomposable as a two-sided ideal. Assume that its radical  $N$  has the property that  $N = Ac = cA$  for some element  $c \in N$ , and let  $N^q = 0$ ,  $N^{q-1} \neq 0$ . Then the composition length of each indecomposable projective left  $A$ -module is  $q$ .*

*Proof.* For each left P.I.M.  $Ae$ , with  $e^2 = e$ , we have  $N^j e = Ac^j e$ . The result

<sup>†</sup> $l(\ )$  denotes left annihilator, and  $r(\ )$  right annihilator.

follows from the preceding theorem and the formula for  $N^j$  in the proof of Theorem 62.26.

The last result in this subsection is another useful criterion, due to Michler [76], for a  $k$ -algebra to be uniserial.

**(62.32) Theorem.** *Let  $A$  be a f.d.  $k$ -algebra of finite representation type. Assume that  $k$  is a splitting field for  $A$ , and that  $A$  has exactly one simple module, up to isomorphism. Then  $A$  is a uniserial  $k$ -algebra.*

*Proof.* The hypothesis implies that  $A$  has exactly one P.I.M.  $U$ , up to isomorphism. Since  $A$  is a direct sum of  $n$  copies of  $U$ ,  $U$  is a generator of the category  $\mathcal{M}_A$ , by (3.49iii). Let  $U = Ae$ , with  $e$  an idempotent. Then

$$A \cong M_n(B), \quad \text{where } B \cong (\text{End}_A U)^\circ \cong (eAe)^\circ,$$

and  $B$  is of finite representation type, by Morita's Theorem 3.54.

Let  $J = \text{rad } B$ . Then  $B$  is a local  $k$ -algebra, by (6.10). Letting  $a \rightarrow \bar{a}$  denote the natural map from  $A$  to  $A/\text{rad } A$ , we have

$$(\bar{e}\bar{A}\bar{e})^\circ \cong \text{End}_{\bar{A}} \bar{A}\bar{e} \cong k$$

since  $\bar{A}\bar{e}$  is a simple  $\bar{A}$ -module and  $k$  is a splitting field. Since  $\text{rad } eAe = e(\text{rad } A)e$  by (5.13), we obtain

$$B/J \cong (\bar{e}\bar{A}\bar{e})^\circ \cong k,$$

and hence  $B = k \oplus J$  (where we identify  $k$  with  $k \cdot 1$ ).

Since  $B$  has finite representation type,  $B/J^2$  has the same property, and is a commutative  $k$ -algebra. We shall prove that  $\dim_k(J/J^2) = 1$  (see Lemma 62.33 below). Assuming this fact for the moment, let  $c \in J, c \notin J^2$ . Then  $Bc + J^2 = J$ , and hence  $J = Bc$  by Nakayama's Lemma 5.7. Similarly  $J = cB$ . Using the isomorphism  $A \cong M_n(B)$  and the identification of  $B$  with the subring  $e_{11}Be_{11}$ , where  $e_{11}$  is a matrix unit, we have  $\text{rad } A = M_n(J)$ , by (5.14). Since  $J = cB = Bc$ , it follows that  $\text{rad } A = Ac = cA$ . Then  $A$  is uniserial, by Theorem 62.26, completing the proof. It remains to prove:

**(62.33) Lemma.** *Let  $B = k + J$ , where  $J = \text{rad } B$ , and assume that  $B$  has finite representation type. Then  $\dim_k(J/J^2) = 1$ .*

The proof is a simple modification of CR 64.3. We shall prove that if  $\dim_k J/J^2 > 1$ , then  $B/J^2$  has indecomposable modules of arbitrarily large dimension over  $k$ , contradicting the assumption that  $B$  is of finite representation type.

We have  $B/J^2 = (k \oplus J)/J^2$ . Let  $u_1, \dots, u_m$  be a  $k$ -basis of  $J/J^2$ , and suppose that  $m > 1$ . Let  $d$  be a positive integer, and let  $M$  be the  $k$ -space with basis

$$x_0, x_1, \dots, x_d, y_1, \dots, y_d.$$

To make  $M$  into a  $(B/J^2)$ -module, set

$$\begin{aligned} u_j x_i &= 0 \text{ for all } i \text{ and } j, \quad u_j y_i = 0 \text{ for } j > 2 \text{ and all } i, \\ u_1 y_i &= x_i, \quad \text{and} \quad u_2 y_i = x_{i-1}, \quad 1 \leq i \leq d. \end{aligned}$$

It is easily checked that  $M$  is a  $(B/J^2)$ -module, and we shall prove it is indecomposable. We have  $M = X \oplus Y$ , where  $X$  and  $Y$  are generated by the basis elements  $\{x_i\}$  and  $\{y_j\}$ , respectively. Let  $\pi$  be the projection  $M \rightarrow Y$ . Note that the maps defined by  $u_1$  and  $u_2$  are injective from  $Y$  to  $X$ , and map  $X$  to 0. Suppose  $M = M_1 \oplus M_2$ , for nonzero  $(B/J^2)$ -submodules  $M_1$  and  $M_2$ , and let

$$\dim_k \pi M_1 = m_1, \quad \dim_k \pi M_2 = m_2.$$

We have  $u_1 M_1 \subseteq M_1$  and  $u_1 M_1 = u_1 \pi M_1$  so  $\dim u_1 M = m_1$ . We also note that  $u_2 M_1$  contains a vector not in  $u_1 M_1$ , and it follows that  $\dim_k M_1 \geq 2m_1 + 1$ ,  $\dim_k M_2 \geq 2m_2 + 1$ . Since  $\pi M = \pi M_1 + \pi M_2$ , we have  $m_1 + m_2 \geq d$ , and hence  $\dim_k M \geq 2(m_1 + m_2) + 2 > 2d + 1$ , which is impossible. Thus  $M$  is indecomposable, and the lemma is proved.

## §62D. Modular Representations in Blocks with Cyclic Defect Groups

In this subsection,  $G$  denotes a finite group, and  $k$  a perfect field of characteristic  $p > 0$ , which is sufficiently large relative to  $G$ . We shall prove a theorem which gives the number of simple and indecomposable  $kG$ -modules in a  $p$ -block of  $G$  with a cyclic defect group  $D \neq 1$ , in terms of the inertial index of the block (see (61.14)). One also has information about the number of ordinary characters in such a block, as well as a way of constructing the indecomposable modules themselves (see Dade [66], Janusz [69], and Feit [82]). Our proof, which is due to Michler [76], focuses on the use of the Green correspondence to transfer information about indecomposable modules in blocks of subgroups to blocks of  $G$  itself. The main result is as follows:

**(62.34) Theorem.** *Let  $B$  be a block of  $kG$ -modules with a cyclic defect group  $D \neq 1$ , and let  $e$  denote the inertial index of  $B$  (see (61.14)). Then the following statements hold.*

- (i)  $e|p - 1$ .
- (ii)  $B$  contains exactly  $e$  isomorphism classes of simple  $kG$ -modules.
- (iii)  $B$  is of finite representation type, and contains exactly  $e|D|$  isomorphism classes of indecomposable  $kG$ -modules.

The proof will occupy the entire subsection. We remark incidentally, that blocks having a trivial defect group are simply blocks of defect zero, and the corresponding theorem has already been established (see Exercise 57.1).

We begin with a proof of part (i) of the main theorem.

**(62.35) Proposition.** *The inertial index  $e$  of  $B$  divides  $p - 1$ .*

*Proof.* Since  $D$  is cyclic,  $DC_G(D) = C_G(D)$ . By (61.14), we have

$$e = |\text{Stab}_{N_G(D)} b' : C_G(D)|,$$

where  $b'$  is a block idempotent in  $kC_G(D)$  belonging to a block  $B'$  of  $C_G(D)$  with defect group  $D$ , such that  $(B')^G = B$ . By (61.15), we have  $e \not\equiv 0 \pmod{p}$ . On the other hand,  $e$  divides the order of the quotient group  $N_G(D)/C_G(D)$ , which is isomorphic to a subgroup of the automorphism group of the cyclic group  $D$ . If  $D$  has order  $d$ , its automorphism group has order  $p^{d-1}(p-1)$ . The result follows by combining these observations.

**(62.36) Definition.** A block  $B$  of  $kG$ -modules is called *uniserial* if the corresponding block ideal  $B$  is a uniserial  $k$ -algebra (see (62.22)).

We note that a uniserial block ideal  $B$  has finite representation type, and that every indecomposable  $B$ -module is a homomorphic image of a P.I.M. (see (62.25)).

Some properties of uniserial block ideals are given in §62C. While blocks with cyclic defect groups are not necessarily uniserial, the consideration of uniserial blocks is essential for the proof of the main theorem.

We continue the proof of Theorem 62.1 by considering the important and interesting case of a normal cyclic defect group, and establish a stronger result in this situation. Incidentally, Step 2 of the proof is a nice application of the general version of Clifford theory from §11C.

**(62.37) Proposition.** *Let  $B$  be a block of  $kG$ -modules with a cyclic defect group  $D$  such that  $D \trianglelefteq G$ . Then  $B$  is a uniserial block, and satisfies parts (i)–(iii) of Theorem 62.34.*

*Proof. Step 1.* We show first that  $B$  is uniserial, by proving that  $\text{rad } B$  satisfies the hypothesis of (62.26), where  $B$  is the block ideal in  $kG$  associated with  $B$ . Let  $I$  denote the augmentation ideal of the group algebra  $kD$  (see (5.24)). If  $D = \langle x \rangle$ , then clearly  $I = (x - 1)kD$ . We shall prove

$$(62.38) \quad \text{rad } B = (x - 1)B = B(x - 1).$$

Since  $D \trianglelefteq G$ , we have  $gIg^{-1} = I$  for all  $g \in G$ , and it follows that  $IB = BI$ . Then  $IB$  is a nilpotent two-sided ideal in  $B$ , since  $I$  is the radical of  $kD$  by (5.24). Then  $IB \subseteq \text{rad } B$ , and we shall prove equality by showing that  $B/IB$  is a semisimple algebra. Let  $\tau: kG \rightarrow k(G/D)$  be the natural map. Then  $\ker \tau = IkG$  by the proof of (5.26). It is then easily checked that

$$IB = B \cap \ker \tau,$$

using the fact that  $B = b(kG)$  for a block idempotent  $b$ .

Now let  $M$  be an arbitrary f.g.  $B/IB$ -module. Then  $M$  can be viewed as a  $B$ -module on which  $D$  acts trivially. Since  $D$  is the defect group of  $B$ ,  $M$  is  $(G, D)$ -projective by (57.27), and we have by (19.2)

$$\sum_{g \in G/D} g\gamma g^{-1} = \text{id}_M$$

for some  $\gamma \in \text{End}_{kD} M$ . Since  $D$  acts trivially on  $M$ , the action of  $g \in G$  on  $M$  is given by

$$gm = \tau(g)m, \quad \text{for all } m \in M,$$

and the preceding formula becomes

$$\sum_{\tau(g) \in G/D} \tau(g)\gamma\tau(g)^{-1} = \text{id}_M$$

where the sum is taken over the factor group  $G/D$ . This proves that  $M$  is a projective  $k(G/D)$ -module. Therefore every f.g.  $(B/IB)$ -module is projective, and hence  $B/IB$  is a semisimple algebra. This completes the proof of (62.38), and it follows by (62.26) that  $B$  is a uniserial block.

*Step 2.* We have already proved in (62.35) that  $e \mid p - 1$ . We next show, using the Clifford theory in §11C, that the number of isomorphism classes of simple modules in  $B$  is equal to  $e$ . We begin with the observation that  $C_G(D) \trianglelefteq G$  since  $D \trianglelefteq G$ . By Theorem 61.7ii, the block ideal  $B$  covers a unique conjugacy class of block ideals  $\{B'\}$  in  $kC_G(D)$ , each of which has defect group  $D$ . Moreover, each block ideal  $B'$  of  $kC_G(D)$  with defect group  $D$  has exactly one simple module, by (61.11).

Now let  $F$  be a simple  $B$ -module. By Clifford's Theorem 11.1, the restriction  $F_{C_G(D)}$  is a semisimple  $kC_G(D)$ -module, and we have

$$F_{C_G(D)} = \bigoplus {}^x L,$$

where the sum is taken over the  $G$ -conjugates  $\{{}^x L : x \in G\}$  of a simple summand  $L$  of  $F_{C_G(D)}$ , and distinct conjugates occur with the same multiplicity.

Let  $b$  be the block idempotent in  $B$ , and  $b'$  the block idempotent in  $B'$ , for a representative  $B'$  of the conjugacy class of block ideals  $C_G(D)$  covered by  $B$ . Then by Theorem (61.2) and Corollary (61.4) we may assume that  $L$  belongs to the block  $B'$ , and  ${}^x b' \cdot {}^x L \neq 0$ . Then  ${}^x b' \cdot {}^x L \neq 0$  for each  $x \in G$ , proving that  ${}^x L$  belongs to the conjugate block  ${}^x B'$  for each  $x \in G$ . Since  $B'$  has, up to isomorphism, only the one simple module  $L$ , it follows that

$${}^x L \simeq L \Leftrightarrow {}^x b' = b'.$$

Thus we have  $\text{Stab}_G L = \text{Stab}_G b'$ . Letting  $T$  denote this stabilizer, we have  $C_G(D) \trianglelefteq T$ , and the quotient group  $T/C_G(D)$  is a subgroup of the automorphism group of  $D$ . Since  $D$  is cyclic of order  $p^d$ , its automorphism group is abelian of

order  $p^{d-1}(p-1)$ , and contains a cyclic subgroup of order  $p-1$ . Since  $T$  is the stabilizer of  $b'$ , the order of  $T/C_G(D)$  is the inertial index  $e$  of the block  $B$ , by (61.14), and hence divides  $p-1$ . It follows that  $T/C_G(D)$  is a cyclic group of order dividing  $p-1$ .

We are now ready to apply Clifford theory. We first observe that the simple  $B$ -modules  $F$  are precisely the composition factors of the induced module  $L^G$ , where  $L$  is the unique simple  $B'$ -module in a block ideal  $B'$  of defect group  $D$  covered by  $B$ . This follows since  $L|F_{C_G(D)}$  for every simple  $B$ -module  $F$ , by the preceding discussion, so  $\text{Hom}_{kG}(L^G, F) \neq 0$  by Frobenius reciprocity (11.13). Thus every simple  $B$ -module  $F$  occurs as a composition factor of  $L^G$ . Moreover, every composition factor of  $L^G$  is a  $B$ -module, since  $B$  is the unique block ideal covering  $B'$ , by (61.2iv).

It follows at once from (11.16) and (11.17) that the number of isomorphism classes of composition factors of  $L^G$  is equal to the number of isomorphism classes of simple submodules of  $L^T$ , where  $T = \text{Stab}_G L$ , and that there is a lattice isomorphism, preserving module homomorphisms, from the lattice of left ideals of  $E = \text{End}_{kG}(L^T)$  to the lattice of  $kG$ -modules of  $L^G$ . We shall prove that  $E \cong k(T/C_G(D))$ , and that  $E$  is a split semisimple  $k$ -algebra. By the proof of (11.20),  $E$  is isomorphic to a twisted group algebra  $k(T/C_G(D))_\alpha$  of the cyclic group  $T/C_G(D)$ , of order dividing  $p-1$ , over the sufficiently large field  $k$  of characteristic  $p$ . Although the results (11.45) and (11.46) were proved for algebraically closed fields of characteristic zero, they apply equally well in this situation, and show that the factor set  $\alpha$  can be taken to be the trivial factor set. Thus  $E$  is a split semisimple group algebra with exactly  $e = |T/C_G(D)|$  simple modules. Moreover  $L^T$  is semisimple by (11.17), and it follows that  $L^T$ , and hence  $L^G$  have exactly  $e$  nonisomorphic composition factors. This completes the proof of Step 2.

*Step 3.* It remains to prove that the number of indecomposable  $B$ -modules is  $|D|e$ . By Steps 1 and 2,  $B$  is a uniserial block ideal, with exactly  $e$  simple modules. From (62.25), each indecomposable  $B$ -module is a homomorphic image of an indecomposable projective module. There are  $e$  isomorphism classes of indecomposable projective  $B$ -modules, and each one has composition length  $|D|$  by (62.31), since  $\text{rad } B = (x-1)B = B(x-1)$  by Step 1. It follows that the number of indecomposable  $B$ -modules is exactly  $|D|e$ , as required.

The preceding result (62.37) applies to the block of  $N_G(D)$ , with defect group  $D$ , corresponding via (58.6) to the given block  $B$  in Theorem 62.34. The next task is to transfer this information from  $N_G(D)$  to  $G$ . This is not straightforward, however, for the following reason. Suppose we have information about simple and indecomposable modules in a block of  $N_G(D)$  with defect group  $D$ , corresponding to  $B$  as in (58.6). The indecomposable modules will have vertices contained in  $D$ , by (57.27), but the Green Correspondence (20.6) applies only to those indecomposable modules in  $B$  whose vertices are not in the family  $\{{}^x D \cap D : x \in G - N_G(D)\}$  (see (20.5)), and does not apply to all indecomposable nonprojective modules in  $B$ , in general.

To resolve this difficulty, we shall apply the Green Correspondence to a certain

subgroup  $H \geq N_G(D)$ . The right choice is

$$H = N_G(Y),$$

where  $Y$  is the unique minimal subgroup of  $D$  of order  $p$ . Then

$$N_G(D) \leq H,$$

since  $Y$  is a characteristic subgroup of  $D$ ; hence  $(G, H, D)$  is an admissible triple of groups for the Green Correspondence (see (20.4)). For the rest of this subsection, we keep to this choice of  $Y$  and  $H$ .

Before applying the Green Correspondence, let us describe the families of subgroups  $\{\mathcal{X}, \mathcal{Y}, \mathcal{A}\}$  in (20.4). We have

$$(62.39) \quad \mathcal{X} = \{{}^x D \cap D : x \in G - H\} = \{1\},$$

since  ${}^x D \cap D \neq 1$  implies  $Y \leq {}^x D \cap D$  and hence  $x \in H = N_G(Y)$ . We next have

$$(62.40) \quad \mathcal{Y} = \{{}^x D \cap H : x \in G - H\};$$

then  $\mathcal{Y}$  contains no nontrivial  $H$ -conjugates of subgroups of  $D$ . Finally,

$$(62.41) \quad \mathcal{A} = \{D^* \leq D : D^* \not\leq {}_G \mathcal{X}\} = \{D^* \leq D : D^* \neq 1\}$$

by (62.39). We next recall that the Green Correspondence 20.6 defines a bijection between isomorphism classes of indecomposable  $kG$ -modules and indecomposable  $kH$ -modules, with vertices in  $\mathcal{A}$ . Corresponding modules  $M \in \text{Ind } kG$  and  $N \in \text{Ind } kH$  have the same vertex, and we shall write

$$f(M) = N \quad \text{and} \quad g(N) = M.$$

By (20.6) we have

$$M_H = f(M) \oplus O(\mathcal{Y}) \quad \text{and} \quad N^G = g(N) \oplus O(\mathcal{X}),$$

where  $O(\mathcal{Y})$  denotes an  $(H, \mathcal{Y})$ -projective  $kH$ -module, and  $O(\mathcal{X})$  a  $(G, \mathcal{X})$ -projective  $kG$ -module (see (20.1)). By (20.3), it follows that an  $(H, \mathcal{Y})$ -projective  $kH$ -module is a direct sum of indecomposable modules whose vertices are  $H$ -conjugate to subgroups of groups belonging to  $\mathcal{Y}$ .

The critical question is whether the Green Correspondence is compatible with the distribution of modules in blocks. Fortunately, we have:

**(62.42) Proposition.** *Let  $B$  be a block of  $kG$ -modules with cyclic defect group  $D$ , and let  $H = N_G(Y)$ , where  $Y$  is the subgroup of  $D$  of order  $p$ . Then:*

- (i) *There exists a unique block  $B'$  of  $kH$ -modules with defect group  $D$ , such that  $(B')^G = B$ .*

(ii) *The Green Correspondence defines a bijection between the sets of indecomposable nonprojective modules in the blocks  $B$  and  $B'$ .*

(iii) *Let  $M \in B$  and  $N \in B'$  be indecomposable non-projective modules such that  $f(M) = N$  and  $g(N) = M$ , as in part (ii). Then we have*

$$M_H = N \oplus N^* \quad \text{and} \quad N^G = M \oplus M^*,$$

where  $N^*$  is a direct sum of projective  $kH$ -modules and of modules belonging to  $H$ -blocks different from  $B'$ , while  $M^*$  is a projective  $kG$ -module.

*Proof (Alperin).* The first statement follows from the Extended First Main Theorem 61.7i, since  $H \geq N_G(D)$ .

We next consider an indecomposable nonprojective  $kH$ -module  $N$  in the block  $B'$  defined in part (i). Then  $\text{vtx } N \neq 1$ , so  $N$  corresponds by (20.6) to a  $kG$ -module  $M$  with the same vertex. Thus  $M$  is indecomposable and not projective, and we must prove that  $M$  is in  $B$ . Let  $D' \in \text{vtx } N$ ; then  $N \mid M_H$  and we may assume that  $D' \leq D$ , by (57.27). Then

$$H = N_G(Y) \geq C_G(Y) \geq C_G(D')$$

since  $D' \neq 1$  and  $Y \leq D'$ . It follows that  $M \in B$  by (58.22), since  $B = (B')^G$ .

Now let  $M$  be an indecomposable nonprojective  $kG$ -module in the block  $B$ ; then  $\text{vtx } M \neq 1$ , and  $\text{vtx } M \leq_G D$  by (57.27), so  $M$  corresponds to an indecomposable nonprojective  $kH$ -module  $N$  with the same vertex  $D' \leq D$ . Then  $C_G(D') \leq H$ , so  $N$  belongs to a block  $B''$  of  $H$  such that  $(B'')^G = B$ , and we have to prove that  $B'' = B'$ . If  $D''$  is a defect group of  $B''$ , then  $D''$  contains a vertex of  $N$ , so we may assume that  $D'' \geq Y$ . We also have  $D'' \leq_G D$  by Corollary 58.18, so  $D''$  is cyclic, and hence  $N_G(D'') \leq N_G(Y) = H$ . Then Theorem 61.7i applies to  $B''$ , and shows that  $(B'')^G = B$  also has defect group  $D''$ . It follows that  $D'' = _G D$  and hence  $B'' = B'$  by Theorem 61.7i again.

For the proof of part (iii), we have  $N^G = M \oplus M^*$  with  $M^*$  projective, by (62.39), since  $\mathcal{X} = \{1\}$ . On the other hand, if  $M_H = N \oplus N^*$ , then each indecomposable nonprojective summand of  $N^*$  has a vertex which is  $H$ -conjugate to no subgroup of  $D$ , and hence does not belong to the block  $B'$  by (57.27). This completes the proof.

We next prove that the numbers of simple modules in the blocks  $B$  and  $B'$  are the same, where  $B'$  is the  $H$ -block defined in (62.42). In fact, we shall prove somewhat more, and will apply the additional information in §62E. The discussion is based on the results in §§62A, B.

Let  $\{S_1, \dots, S_d\}$  be a basic set of simple modules in  $B'$ , and let  $\{T_1, \dots, T_d\}$  be a set of P.I.M's in  $B'$ , such that  $T_i/N'T_i \cong S_i$ ,  $1 \leq i \leq d$ , where  $N'$  is the radical of the block ideal  $B'$ . Let us assume that  $B'$  is a uniserial block. If  $(N')^m = 0$ ,  $(N')^{m-1} \neq 0$ , then

$$T_i \supset N'T_i \supset \cdots \supset (N')^{m-1}T_i \supset 0$$

is the unique composition series of each module  $T_i$ , by (62.29), since  $B'$  is a symmetric algebra. Now set

$$(62.43) \quad T_{ij} = T_i/(N')^j T_i, \quad 1 \leq i \leq d, \quad 1 \leq j \leq m.$$

Then the modules  $\{T_{ij}\}$  are a basic set of indecomposable modules in  $B'$ .

Let  $\{V_1, \dots, V_{d'}\}$  be a basic set of simple modules in  $B = (B')^G$ , and set  $I = \{1, \dots, d\}$ ,  $J = \{1, \dots, d'\}$ . The modules  $\{S_i; i \in I\}$  and  $\{V_j; j \in J\}$  are  $(H, D)$ - or  $(G, D)$ -projective, respectively, since  $D$  is a defect group of both blocks  $B'$  and  $B$ . On the other hand, none of the modules  $\{S_i\}$  or  $\{V_j\}$  is projective, since both blocks  $B$  and  $B'$  have positive defect (see Exercise 56.8).

In the statement and proof of the next result, we shall use the notation

$$(M, Q)_H, \quad (M, Q)_{H/1}, \quad \text{etc.},$$

from §62A, for a pair of  $kH$ -modules  $M$  and  $Q$ , and a corresponding notation for  $kG$ -modules.

**(62.44) Proposition.** *Keep the preceding notation, and assume that  $B'$  is a uniserial block of  $H$ . Then the following statements hold:*

(i) *The Green correspondents  $\{fV_j; j \in J\}$  and  $\{gS_i; i \in I\}$ , of the simple modules  $\{V_j\}$  in  $B$  and  $\{S_i\}$  in  $B'$ , are nonprojective indecomposable modules in  $B'$  and  $B$  respectively.*

(ii) *There exist  $k$ -isomorphisms*

$$(S_i, fV_j)_H \cong (gS_i, V_j)_G \quad \text{and} \quad (fV_j, S_i)_H \cong (V_j, gS_i)_G$$

for all  $i \in I$ ,  $j \in J$ .

(iii) *There exists a map  $h: J \rightarrow I$  such that*

$$h(j) = i \Leftrightarrow (fV_j, S_i)_H \neq 0, \quad \text{for } i \in I, \quad j \in J.$$

Moreover,  $h$  is a bijection, so  $d = d'$ .

(iv)  *$(fV_j, S_i)_H \cong k$  or  $0$ , according as  $h(j) = i$  or  $h(j) \neq i$ .*

*Proof.* The first statement follows from (62.42), since the modules  $\{S_i\}$  and  $\{V_j\}$  are nonprojective simple modules.

(ii) We first apply Theorem 62.13 to the  $(G, D)$ -projective modules  $gS_i$  and  $V_j$ , using the fact that, in this case, the family of subgroups  $\mathcal{X}$  contains only the trivial subgroup, so  $(gS_i, V_j)_{G, \mathcal{X}} = (gS_i, V_j)_{G/1}$ . We have, by (62.13),

$$\begin{aligned} (gS_i, V_j)_G / (gS_i, V_j)_{G/1} &\cong (fgS_i, fV_j)_H / (fgS_i, fV_j)_{H/1} \\ &\cong (S_i, fV_j)_H / (S_i, fV_j)_{H/1}, \end{aligned}$$

since  $fgS_i \cong S_i$  for each  $i \in I$ . We can then apply Proposition 62.7 to obtain

$$(gS_i, V_j)_{G/1} = 0 \quad \text{and} \quad (S_i, fV_j)_{H/1} = 0, \quad \text{for } i \in I, \quad j \in J,$$

since  $S_i$  and  $V_j$  are simple modules, and  $gS_i$  and  $fV_j$  are indecomposable nonprojective modules. It follows that  $(S_i, fV_j)_H \cong (gS_i, V_j)_G$ . Similarly  $(fV_j, S_i)_H \cong (V_j, gS_i)_G$ , for  $i \in I$ ,  $J \in J$ , and (ii) is proved.

(iii) and (iv). Let  $j \in J$ . Then  $fV_j \cong T_{h(j), v(j)}$  for a unique indecomposable module  $T_{h(j), v(j)}$  defined above. This defines maps  $h: J \rightarrow I$  and  $v: J \rightarrow [1, m]$ . Since  $T_{h(j), v(j)}$  is uniserial with top composition factor  $S_{h(j)}$ , we have

$$(fV_j, S_i)_H = \begin{cases} k & \text{if } i = h(j), \\ 0 & \text{if } i \neq h(j). \end{cases}$$

Now let  $i \in I$ , and let  $S$  be a minimal submodule of  $gS_i$ . Then  $S \in B$ , so  $S \cong V_j$  for some  $j$ , and it follows that  $(V_j, gS_i)_G \neq 0$ . Then  $(fV_j, S_i)_H \neq 0$  by part (ii) and we obtain  $h(j) = i$ , proving that  $h$  is surjective. Next suppose  $j, j' \in J$  and  $h(j) = h(j') = i$ . Then  $fV_j \cong T_{i, v}$  and  $fV_{j'} \cong T_{i, v'}$  for some choices of  $v$  and  $v'$ . Thus there exists a  $kH$ -surjection  $\theta: T_{i, v} \rightarrow T_{i, v'}$  by definition of the modules  $\{T_{ij}\}$ , and the map  $\theta$  is not projective by (62.5). It follows that  $(fV_j, fV_{j'})_H / (fV_j, fV_{j'})_{H/1} \neq 0$ , and since  $fV_j$  and  $fV_{j'}$  are  $(H, D)$ -projective, we obtain  $(V_j, V_{j'})_G / (V_j, V_{j'})_{G/1} \neq 0$  by (62.13). Therefore  $(V_j, V_{j'})_G \neq 0$ , and we have  $j = j'$ . This completes the proof.

The next result is the stepping stone to the proof of the main theorem.

**(62.45) Proposition.** *Keep the preceding notation, and assume that  $B'$  is a uniserial block of  $H$  with defect group  $D$ . If  $B'$  contains exactly  $e$  simple modules and  $e|D|$  indecomposable modules, then the same is true for  $B$ .*

*Proof.* Then Green Correspondence defines a bijection between the isomorphism classes of nonprojective indecomposable modules in the blocks  $B$  and  $B'$ , by (62.42). On the other hand, by (62.44) the blocks  $B$  and  $B'$  also contain the same number of simple modules, and hence the same number of indecomposable projective modules. This completes the proof.

*Proof of Theorem 62.34.* We shall use induction on  $|G|$ . Thus we shall consider a block  $B$  of  $G$  with cyclic defect group  $D$ , and assume that for  $|G_0| < |G|$ , the result holds for blocks of  $kG_0$  with cyclic defect group.

*Step 1.* We first prove the theorem when  $|D| = p$ . In this case,  $Y = D$ , and  $H = N_G(Y) = N_G(D)$ . If  $B'$  is the  $H$ -block defined in (62.42i), then  $B'$  has the same inertial index as  $B$  by Definition 61.14. Since the defect group  $D$  of  $B'$  is normal in  $H$ , we may apply (62.37) to deduce that  $B'$  is a uniserial block, with exactly  $e$  simple modules and  $e|D|$  indecomposable modules. Then  $B$  also contains exactly  $e$  simple modules and  $e|D|$  indecomposable modules, completing the proof of Step 1.

*Step 2.* We may now assume that  $|D| > p$ , and let  $Y$  be the subgroup of  $D$  of order  $p$ . In this step, we shall assume that  $G = C_G(Y)$ , and prove the theorem for  $G$ . In addition, we shall prove that  $B$  is uniserial and has exactly one simple module and  $|D|$  indecomposable modules.

We first compute the inertial index, using the definition (61.14). Let  $B'$  be a block of  $C_G(D)$  with defect group  $D$  such that  $(B')^G = B$ . Then the inertial index of  $B$  is given by

$$e = |\text{Stab}_{N_G(D)} b' : C_G(D)|,$$

where  $b'$  is the block idempotent of  $B'$  in  $kC_G(D)$ . Since  $e \not\equiv 0 \pmod{p}$  by (62.35) and  $G = C_G(Y)$ , it follows that  $\text{Stab}_{N_G(D)} b' : C_G(D)$  is a  $p'$ -group of automorphisms of  $D$  which acts trivially on the subgroup  $Y$  of order  $p$ . It is not difficult to prove that the order of such a group is 1, and hence  $e = 1$  (see Gorenstein [68; Th. 2.7, p. 178]).

We next require a lemma which will permit us to use the induction hypothesis. We note that since  $G = C_G(Y)$ ,  $Y$  is a normal subgroup of each of the groups  $G$ ,  $N_G(D)$ ,  $C_G(D)$ , and of course of  $D$ .

**(62.46) Lemma.** *Assume  $G = C_G(Y)$ , as in Step 2. Let  $N = N_G(D)$ ,  $C = C_G(D)$  and set  $\bar{G} = G/Y$ ,  $\bar{N} = N/Y$ ,  $\bar{C} = C/Y$ , and  $\bar{D} = D/Y$ . Let  $B_1$  be the unique block of  $N$  with defect group  $D$  such that  $(B_1)^G = B$ , and let  $B_1$  and  $B$  denote the block ideals of  $B_1$  and  $B$ , with block idempotents  $b_1$  and  $b$ , respectively. Let  $\tau: kG \rightarrow k\bar{G}$  denote the natural homomorphism. Then:*

- (i)  $\tau(b)$  and  $\tau(b_1)$  are block idempotents in  $k\bar{G}$  and  $k\bar{N}$ , respectively, and both have defect group  $\bar{D}$ .
- (ii) The block ideals  $k\bar{G}\tau(b)$  and  $k\bar{N}\tau(b_1)$  are related by the Brauer correspondence, and both blocks have inertial index equal to 1.

*Proof.* The first statement follows from the proof of part (iii) of Theorem 61.7, noting that in this case  $Y$  is contained in the center of both  $G$  and  $N$ .

For the proof of part (ii), we have  $(B_1)^G = B$ , so  $B_1 | B_{N \times N}$  by (58.17), and hence  $bb_1 = b_1$ . Then  $\tau(b)\tau(b_1) = \tau(b_1)$ , and it follows that  $\tau(B_1) | \tau(B)_{\bar{N} \times \bar{N}}$ , since  $\tau(b)$  and  $\tau(b_1)$  are block idempotents by part (i). It is easily checked that  $\bar{N} \geq C_G(\bar{D})$ , so the Brauer correspondence is defined for the block  $\tau(B_1)$ , by (58.20). Since  $\tau(B_1) | \tau(B)_{\bar{N} \times \bar{N}}$ , its Brauer correspondent is  $\tau(B)$ . Finally, since both  $B$  and  $B_1$  have inertial index 1, by the first part of the proof of Step 2, and since  $\bar{N} = N_G(\bar{D})$ , it is easily verified that the blocks  $\tau(B)$  and  $\tau(B_1)$  also have inertial index 1, completing the proof of the lemma.

To complete the proof of Step 2, let  $\bar{B}$  be the block of  $\bar{G}$  defined by  $\tau(b)$ . Since  $\bar{B}$  has inertial index 1 by the preceding lemma, it follows that  $\bar{B}$  contains exactly one simple module and  $|\bar{D}|$  indecomposable modules, up to isomorphism. We have  $\ker \tau = IkG$ , where  $I$  is the augmentation ideal of the group algebra  $kY$ . As in the

proof of (62.37), we have  $\ker \tau \cap B = IB \subseteq \text{rad } B$ , and  $\bar{B} \cong B/IB$ . From these remarks, it follows that  $B$  contains a unique simple module, and hence  $B$  is a uniserial block, by (62.32). Then  $B$  contains a unique indecomposable projective module  $U$ , and the number of indecomposable modules in  $B$  is the composition length of  $U$ . By CR(89.8), the Cartan matrix of the block  $B$  is  $(|D|)$  and this proves that the composition length of  $U$  is  $|D|$ , since  $U$  is uniserial. This completes the proof of Step 2.

*Step 3.* This time we shall assume that  $G = N_G(Y)$ , and will prove that  $B$  is a uniserial block, containing exactly  $e$  simple modules and  $e|D|$  indecomposable modules, where  $e$  is the inertial index.

In this case,  $C_G(Y) \trianglelefteq G$ , so  $B$  covers a unique conjugacy class of blocks of  $C_G(Y)$ , all with defect group  $D$ . This follows from Theorem 61.2, using the fact that  $D \leq C_G(Y)$  to calculate the defect groups. By Step 2, each of these blocks is uniserial, and contains exactly one simple module and  $|D|$  indecomposable modules.

Our first objective is to prove that  $B$  is a uniserial block. Let  $B_0$  be a uniserial block of  $C_G(Y)$  with defect group  $D_1$  covered by  $B_1$  and let  $T_0 = \text{Stab}_G b_0$ , where  $b_0$  is the block idempotent of  $B_0$ . Then  $C_G(Y) \trianglelefteq T_0$ , and we have

$$(62.47) \quad |T_0 : C_G(Y)| \not\equiv 0 \pmod{p}$$

by (61.5). Moreover,  $B_0$  is covered by a unique block  $\tilde{B}_0$  of  $T_0$ . Letting  $B_0$  and  $\tilde{B}_0$  denote the block ideals of  $B_0$  and  $\tilde{B}_0$ , respectively, we have

$$(62.48) \quad \text{rad } \tilde{B}_0 = \tilde{B}_0(\text{rad } B_0) = (\text{rad } B_0)\tilde{B}_0$$

by Exercise 6, because of (62.47). Since  $B_0$  is uniserial, we have  $\text{rad } B_0 = uB_0 = B_0u$  for some element  $u \in B_0$  by (62.26), and hence the same is true for  $\tilde{B}_0$  because of (62.48). It follows that  $\tilde{B}_0$  is also a uniserial block, by (62.26).

Since  $B_0$  is a uniserial block containing a unique simple module,  $T_0 = \text{Stab}_G b_0$  coincides with the stabilizer of each indecomposable module in  $B_0$ . This follows easily from the fact that the isomorphism class of an indecomposable module in  $B_0$  is determined by its composition length. Then  $U^G = \text{ind}_{T_0}^G U$  is an indecomposable module in  $B$  for each indecomposable module  $U$  in  $\tilde{B}_0$ , by (19.20). Moreover,  $U$  is uniserial, and  $F^G$  is a simple module for each composition factor  $F$  of  $U$ . It follows that  $U^G$  is also uniserial, since induction is an exact functor.

We can now complete the proof that  $B$  is a uniserial block. Each indecomposable module  $M$  in  $B$  is  $(G, D)$ -projective, and hence  $(G, C_G(Y))$ -projective, since  $C_G(Y) \geq D$ . Then  $M \mid V^G$  for some indecomposable module  $V$  in  $B_0$ , and it follows easily from (19.20) that in fact  $M \cong U^G$  for some indecomposable module  $U$  in  $\tilde{B}_0$ . Then  $M$  is uniserial by the preceding discussion, and we have proved that  $B$  is uniserial.

It remains to count the simple and indecomposable modules in  $B$ . Let  $\bar{G} = G/Y$ , and let  $\tau: kG \rightarrow k\bar{G}$  be the natural map. Then  $\tau(b)$  defines a block  $\bar{B}$  of  $k\bar{G}$ ,

where  $b$  is the block idempotent in  $B$ . It is easily verified, using the proof of (61.7iii), that  $\bar{B}$  has defect group  $\bar{D}$  and the same inertial index as  $B$ . By the induction hypothesis, it follows that the number of simple modules in  $\bar{B}$  is  $e$ , and hence the same is true for  $B$ , since  $\ker \tau$  is contained in  $\text{rad } kG$ . Moreover, the number of indecomposable modules in  $\bar{B}$  is  $e|D/Y|$  by the induction hypothesis, and it is not difficult to check that the number of indecomposable modules in  $B$  is  $e|D| = e|D/Y||Y|$  using the fact that  $B$  is a uniserial block. This completes the proof of Step 3.

*Step 4.* We are in a position to complete the proof of the main Theorem 62.34. Let  $Y$  be the subgroup of  $D$  of order  $p$ . Then  $N_G(Y) \geq N_G(D)$ , so the Brauer correspondence assigns to  $B$  a unique block  $B'$  of  $N_G(Y)$  with defect group  $D$ , by (61.7i). Moreover, it is readily verified that  $B$  and  $B'$  have the same inertial index. We may apply Step 3 to  $B'$  and conclude that  $B'$  is a uniserial block containing  $e$  simple modules and  $e|D|$  indecomposable modules. Then  $B$  contains  $e$  simple modules and  $e|D|$  indecomposable modules by (62.45), completing the proof.

## §62E. Periodic Projective Resolutions in Blocks with Cyclic Defect Groups

Let  $G$  be a finite group, and  $(K, R, k)$  a  $p$ -modular system such that  $\text{char } K = 0$ ,  $K$  is sufficiently large relative to  $G$ , and  $k$  is a perfect field of characteristic  $p$ . Let  $B$  be a  $p$ -block of  $G$  with a cyclic defect group  $D$ . In §62D, some definitive information was obtained concerning the simple and indecomposable  $kG$ -modules belonging to  $B$ . The question arises, what can be said about the  $KG$ -modules and  $RG$ -modules belonging to  $B$ ? In case  $B$  is the principal block, and  $D$  is a cyclic self-centralizing Sylow  $p$ -subgroup such that  $D^*$  is a T.I. set, the  $K$ -characters belonging to  $B$  were described in §60B, using the results in §20B. These results (of Thompson [67b]) were extended to determine the  $K$ -characters belonging to an arbitrary block with cyclic defect group by Dade [66]. A complete and up-to-date account of Dade's results, with additions and improvements, was given by Feit [82, Chapter VII].

In this subsection, we shall describe some properties of  $RG$ -modules belonging to  $B$ . In particular, we shall prove that the presence of a cyclic Sylow  $p$ -subgroup manifests itself in the existence of a periodic projective resolution (see (8.1)) of the trivial  $RG$ -module. The result, which is due to Green [74], and a closely related theorem of Alperin–Janusz [73] were first proved using Dade's results on the  $K$ -characters in  $B$ . We shall give a new proof of a somewhat less precise result, using the results on  $kG$ -modules in  $B$  from §62D, combined with Morita's work on uniserial blocks, from §62C (see also Michler [75]). We shall also show the connection between these results and the  $KG$ -modules in  $B$ , in the special situation considered in §60B.

We begin with a few remarks about the Heller operator  $\Omega$  in the category of f.g.  $kG$ -modules. A fuller discussion of this topic, with proofs of some facts stated below, will be found in §78. Let  $M$  be a core (see (62.2)). We define  $\Omega M$  to be the kernel of a surjective homomorphism  $\pi: P \rightarrow M$ , where  $P$  is a projective cover of

$M$  (see §6B). Thus we have a short exact sequence (ses)

$$0 \rightarrow \Omega M \rightarrow P \rightarrow M \rightarrow 0.$$

By Schanuel's Lemma 2.24 and the properties of projective covers, it follows easily that the isomorphism class of  $\Omega M$  is uniquely determined by the isomorphism class of  $M$  (see §78A). The resulting operation  $(M) \rightarrow (\Omega M)$  in the set of isomorphism classes  $(M)$  of f.g.  $kG$ -modules is called the *Heller operator*. The same definition and remarks apply to  $RG$ -lattices, since  $RG$  is a semiperfect ring (see §18A). The main property of  $\Omega$  we require is contained in the following result, which is proved for  $kG$ -modules in §78A.

**(62.49) Proposition.** *Let  $M$  be a f.g.  $kG$ -module, or an  $RG$ -lattice. If  $M$  is indecomposable and nonprojective, so is  $\Omega M$ .*

The proof for  $RG$ -lattices is left as an exercise.

The next result uses reduction mod  $p$ ,  $M \rightarrow \bar{M} = M/pM$ , from the category of  $RG$ -lattices to the category of f.g.  $kG$ -modules (see §16C).

**(62.50) Proposition.** *Let*

$$0 \rightarrow U \rightarrow Q \rightarrow V \rightarrow 0$$

*be a ses of f.g.  $kG$ -modules, with  $Q$  projective, and suppose there exists an  $RG$ -lattice  $M$  such that  $\bar{M} \cong V$ . Then there exists a commutative diagram, with exact rows, and  $P$  projective,*

$$\begin{array}{ccccccc} 0 & \longrightarrow & N & \longrightarrow & P & \longrightarrow & M & \longrightarrow 0 \\ \downarrow & & \downarrow & & \downarrow & & \downarrow & \\ 0 & \longrightarrow & U & \longrightarrow & Q & \longrightarrow & V & \longrightarrow 0 \end{array},$$

*where each vertical map is reduction mod  $p$ .*

The proof is left as an exercise.

Now let  $B$  be a  $p$ -block of  $G$  with a cyclic defect group  $D \neq 1$ . Our first objective is to construct some short exact sequences involving the indecomposable projective  $kG$ -modules in  $B$ . This will involve the connection between modules in  $B$  and modules in a corresponding block  $B'$  of the subgroup  $H = N_G(Y)$ , where  $Y$  is subgroup of  $D$  of order  $p$ . We shall make frequent use of results from §§62C and 62D, especially Proposition 62.44 and the remarks preceding it, and the proof of Theorem 62.34.

Since  $H \geq N_G(D)$ , there is a unique  $p$ -block  $B'$  of  $H$  with defect group  $D$  such that  $(B')^G = B$ . By Step 3 of the proof of Theorem 62.34,  $B'$  is a uniserial block, and both blocks  $B$  and  $B'$  contain exactly  $e$  isomorphism classes of simple modules, where  $e$  is the inertial index of  $B$ .

Let  $\{S_1, \dots, S_e\}$  be a basic set of simple modules in  $B'$ , and let  $T_i$  be a projective cover of  $S_i$ , for  $1 \leq i \leq e$ . Then the modules  $\{T_i\}$  all have the same composition length  $q$  by (62.29), since the block ideal  $B'$  is a symmetric uniserial algebra. Letting  $N' = \text{rad } B'$ , each of the modules  $T_i$  has a unique composition series

$$T_i \supset N'T_i \supset (N')^2 T_i \supset \cdots \supset (N')^q T_i = 0,$$

and the modules

$$T_{ij} = T_i / (N')^j T_i, \quad 1 \leq i \leq e, \quad 1 \leq j \leq q,$$

form a basic set of indecomposable modules in  $B'$ . Since the number of indecomposable modules in  $B'$  is  $e|D|$  by Theorem 62.34, we have  $q = |D| = p^d$  for some positive integer  $d$ , and it follows that

$$q \equiv 1 \pmod{e},$$

since  $e|p - 1$  by (62.34i).

The periodic behavior of the modules in  $B$  and  $B'$  is best explained if we index a set of modules  $\{S_i, T_i, T_{ij}\}$  so that  $i$  is any integer, and  $S_i, T_i, T_{ij}$  have their previous interpretations for  $1 \leq i \leq e$  and satisfy

$$S_i \cong S_{i+e}, T_i \cong T_{i+e}, T_{ij} \cong T_{i+e,j},$$

for  $1 \leq j \leq q$  and all  $i \in \mathbb{Z}$ . In this terminology, we have:

**(62.51) Proposition.** *There exists an ordering of  $\{1, 2, \dots, e\}$  such that the following statements hold.*

(i) *For each  $i \in \mathbb{Z}$ , the modules in a composition series of  $T_i$  are indecomposable, and are isomorphic, respectively, to the sequence of modules:*

$$T_{i,q}, T_{i+1,q-1}, T_{i+2,q-2}, \dots, T_{i+q-1,1} \cong T_{i,1}.$$

(ii)  *$T_{ij} \in \mathcal{P}(kH)$  if and only if  $j = q$ .*

(iii)  *$T_{i1} \cong S_i$  for all  $i \in \mathbb{Z}$ .*

(iv) *For each  $i \in \mathbb{Z}$  and  $j < q$  there exists a ses of  $kH$ -modules*

$$0 \rightarrow T_{i+j,q-j} \rightarrow T_{iq} \rightarrow T_{ij} \rightarrow 0.$$

(v) *For each  $j < q$  we have*

$$\Omega T_{ij} \cong T_{i+j,q-j}.$$

(vi)  *$\Omega^2 S_i \cong S_{i+1}$  for all  $i \in \mathbb{Z}$ .*

*Proof.* (i) We order  $\{1, 2, \dots, e\}$  as in Morita's Theorem 62.29. Then (i) follows at once from (62.29) and the description of the modules  $\{T_{ij}\}$ , together with the fact that  $q \equiv 1 \pmod{e}$ . Statements (ii)–(iv) follow from part (i), while (v) follows from (iv) and the definition of the Heller operator  $\Omega$ . For (vi) we have

$$\Omega^2 S_i \cong \Omega^2(T_{i,1}) \cong \Omega(T_{i+1,q-1}) \cong T_{i+q,1} \cong S_{i+1}$$

using (v) and the fact that  $q \equiv 1 \pmod{e}$ , so that

$$T_{i+q,1} \cong T_{i+1,1} \cong S_{i+1}$$

by (iii). This completes the proof.

The next result carries this information over to modules in  $\mathbf{B}$ , using the Green Correspondence and Proposition 62.44.

**(62.52) Theorem.** *Keep the notation of Proposition 62.51. Then there exists a basic set of simple  $kG$ -modules  $\{V_1, \dots, V_e\}$  in  $\mathbf{B}$  which can be ordered so that the following statements hold.*

(i) *Let  $\{fV_j\}$  and  $\{gS_i\}$  denote the Green correspondents of the modules  $\{V_j\}$  and  $\{S_i\}$ , respectively. We have*

$$(fV_j, S_i)_H \cong (V_j, gS_i)_G \cong k \text{ or } 0,$$

according as  $i = j$  or  $i \neq j$ .

(ii) *There exists a permutation  $\delta$  of  $\{1, 2, \dots, e\}$  such that*

$$(S_i, fV_j)_H \cong (gS_i, V_j)_G \cong k \text{ or } 0,$$

according as  $\delta(i) = j$  or  $\delta(i) \neq j$ .

(iii) *For each  $i$ ,  $1 \leq i \leq e$ , let  $U_i$  denote a projective cover of the simple  $KG$ -module  $V_i$ , and, as in the case of modules in the block  $\mathbf{B}'$ , extend the definition of  $U_i$  and  $V_i$  so that  $i$  is taken in  $\mathbb{Z}$ , and  $U_i \cong U_{i+e}$ ,  $V_i \cong V_{i+e}$ , and also  $\delta(i+e) = \delta(i)$  for  $i \in \mathbb{Z}$ . Then there exist ses's of  $kG$ -modules*

$$F_{2i}: 0 \rightarrow \Omega gS_i \rightarrow U_{\delta(i)} \rightarrow gS_i \rightarrow 0$$

and

$$F_{2i+1}: 0 \rightarrow gS_{i+1} \rightarrow U_{i+1} \rightarrow \Omega gS_i \rightarrow 0$$

for all  $i \in \mathbb{Z}$ .

*Proof.* We have already noted that  $\mathbf{B}$  contains exactly  $e$  isomorphism classes of simple modules. We order them in such a way that the bijection  $h$  described in (62.44) is the identity. Then part (i) of the theorem follows from (62.44ii–iv).

Using the fact that  $(S_i, fV_j)_H \cong (gS_i, V_j)_G$  for all  $i$  and  $j$ , by (62.44ii), we can then essentially repeat the proof of (62.44) to prove the existence of a permutation  $\delta$  of  $\{1, 2, \dots, e\}$  satisfying part (ii) of the theorem.

By parts (i) and (ii), we have

$$(62.53) \quad \text{soc } gS_i \cong V_i \quad \text{and} \quad gS_i/\text{rad } gS_i \cong V_{\delta(i)} \quad \text{for } 1 \leq i \leq e.$$

From the second of these isomorphisms, and the fact that  $U_{\delta(i)}$  is a projective cover of  $V_{\delta(i)}$ , it follows that there exists a surjection  $U_{\delta(i)} \rightarrow gS_i$ , and consequently  $U_{\delta(i)}$  is a projective cover of  $gS_i$ . Then we have a ses of  $kG$ -modules

$$F_{2i}: 0 \rightarrow \Omega gS_i \rightarrow U_{\delta(i)} \rightarrow gS_i \rightarrow 0$$

for all  $i \in \mathbb{Z}$ , using the definition of the Heller operator  $\Omega$ .

To obtain the exact sequences  $F_{2i+1}$ , we start from the facts that  $\text{soc } gS_{i+1} \cong V_{i+1}$  by (62.53), and that  $U_{i+1}$  is an injective hull of  $V_{i+1}$ . Consequently there exists a ses, for each  $i \in \mathbb{Z}$ ,

$$(62.54) \quad 0 \rightarrow gS_{i+1} \rightarrow U_{i+1} \rightarrow W_{i+1} \rightarrow 0,$$

where  $W_{i+1}$  is some  $kG$ -module.

On the other hand, we have

$$(62.55) \quad \Omega gT_{ij} \cong g\Omega T_{ij}, \quad i \in \mathbb{Z}, \quad j < q,$$

for each nonprojective indecomposable module  $T_{ij}$  in  $B'$  (see Exercise 7). This implies that

$$\Omega(\Omega gS_i) \cong g\Omega^2 S_i \cong gS_{i+1}$$

by (62.51vi), and hence there exists a ses

$$0 \rightarrow gS_{i+1} \rightarrow U \rightarrow \Omega gS_i \rightarrow 0,$$

with  $U$  projective. By a version of Schanuel's Lemma, we obtain  $W_{i+1} \cong \Omega gS_i$ , and we can take (62.54) as the exact sequence  $F_{2i+1}$ , for all  $i \in \mathbb{Z}$ . This completes the proof of the theorem.

Before stating the main result on  $RG$ -modules, we recall that a *projective resolution* of a module  $M$  over a ring  $A$  is an exact sequence

$$\cdots \rightarrow P_2 \rightarrow P_1 \rightarrow M \rightarrow 0$$

with  $P_i$  projective, for all  $i \geq 1$ .

**(62.56) Theorem.** *Let  $G$  have a cyclic Sylow  $p$ -subgroup  $D$ , and let  $e$  be the inertial*

index of the principal  $p$ -block  $B_1$ . Then there exists a family of  $RG$ -lattices  $\{X_i : i \geq 0\}$ , and an ordering of indecomposable projective  $RG$ -modules  $\{P_1, \dots, P_e\}$  in  $B_1$ , such that the following statements hold.

- (i) Extend the definition of the modules  $\{P_i\}$  so that  $i \in \mathbb{Z}$  and  $P_{i+e} \cong P_i$  for all  $i \in \mathbb{Z}$ . Then there exist ses's of  $RG$ -lattices

$$E_i : 0 \rightarrow X_{2i+1} \rightarrow P_{\delta(i)} \rightarrow X_{2i} \rightarrow 0$$

and

$$E_{2i+1} : 0 \rightarrow X_{2i+2} \rightarrow P_{i+1} \rightarrow X_{2i+1} \rightarrow 0$$

for all  $i \in \mathbb{Z}_+$ , with  $X_0$  the trivial  $RG$ -lattice, and  $\delta$  as in (62.52ii).

- (ii) The ses's  $\{E_i : i \in \mathbb{Z}_+\}$  provide a projective resolution of the trivial  $RG$ -lattice  $X_0$ , which is periodic of period  $2e$ :

$$\cdots \rightarrow P_{\delta(0)} \rightarrow P_0 \rightarrow P_{\delta(e-1)} \rightarrow P_{e-1} \rightarrow \cdots \rightarrow P_{\delta(1)} \rightarrow P_1 \rightarrow P_{\delta(0)} \rightarrow X_0 \rightarrow 0.$$

*Proof.* We shall apply Theorem 62.52 to the principal block. By (62.52iii), there exist ses's of  $kG$ -modules in  $B_1$ :

$$F_{2i} : 0 \rightarrow Y_{2i+1} \rightarrow U_{\delta(i)} \rightarrow Y_{2i} \rightarrow 0$$

and

$$F_{2i+1} : 0 \rightarrow Y_{2i+2} \rightarrow U_{i+1} \rightarrow Y_{2i+1} \rightarrow 0,$$

where  $Y_{2i} \cong gS_i$  and  $Y_{2i+1} \cong \Omega gS_i$ , for all  $i \in \mathbb{Z}$ . The  $p$ -block of  $H$  corresponding to  $B_1$  is the principal block  $B'_1$  of  $H$ , which contains the trivial  $H$ -module, denoted by  $S_0$ . Then  $Y_0 \cong gS_0$  is the trivial  $kG$ -module, by the properties of the Green Correspondence.

We start the proof of the theorem with the observation that if  $X_0$  denotes the trivial  $RG$ -lattice, then we have  $\bar{X}_0 \cong Y_0$ , where  $\bar{X}_0 = X_0/\mathfrak{p}X_0$ . We may assume the indecomposable projective  $RG$ -lattices in  $B_1$  are ordered in such a way that  $\bar{P}_i \cong U_i$ , for all  $i \in \mathbb{Z}$  (see §18A). By (62.50), we can lift the ses  $F_0$  to a ses of  $RG$ -lattices

$$E_0 : 0 \rightarrow X_1 \rightarrow P_{\delta(0)} \rightarrow X_0 \rightarrow 0,$$

such that  $\bar{X}_0 = Y_0$  and  $\bar{X}_1 \cong Y_1$ . By (62.50) again, starting from  $\bar{X}_1 \cong Y_1$ , we can lift the ses  $F_1$  to a ses of  $RG$ -lattices

$$E_1 : 0 \rightarrow X_2 \rightarrow P_1 \rightarrow X_1 \rightarrow 0,$$

such that  $\bar{X}_2 \cong Y_2$ . Continuing by induction, we can define  $RG$ -lattices  $\{X_i\}$  and ses  $\{E_i\}$  for all  $i \in \mathbb{Z}_+$ , such that part (i) of Theorem 62.56 holds. Part (ii) is an immediate consequence of part (i), finishing the proof.

**(62.57) Remarks and Examples. The Brauer Tree.** Let us interpret some of the preceding results in the special case, considered in §§20 and 60, of a finite group  $G$  with a cyclic self-centralizing Sylow  $p$ -subgroup  $D$  such that  $D^*$  is a T.I. set. Let

$$|D| = p^d, e = |N_G(D):D|, \quad \text{and} \quad n = (p^d - 1)/e,$$

and assume  $n \geq 2$ . By (60.9), the group  $N_G(D)$  has only one  $p$ -block, and it follows that  $e$  is the inertial index of the principal  $p$ -block  $B_1$  of  $G$  (see (61.14)). By Theorem 60.8, there are exactly  $e + (p^d - 1)/e$  irreducible  $K$ -characters in  $B_1$ , namely,

$$\{\theta_0 = 1_G, \theta_1, \dots, \theta_{e-1}, \zeta_1, \dots, \zeta_n\}$$

(see (60.7)). By Theorem 62.34, there are exactly  $e$  characters  $\{\tau_1, \dots, \tau_e\}$  afforded by the indecomposable projective  $RG$ -lattices in  $B_1$ . We require one more crucial piece of information relating the characters  $\{\tau_i\}$  and the irreducible characters in  $B_1$ .

**(62.58) Proposition.** *Let  $\tau$  be a  $K$ -character afforded by an indecomposable projective  $RG$ -lattice belonging to  $B_1$ . Then we have either*

$$\tau = \sum_{i=1}^n \zeta_i + \theta_j, \quad \text{for some } j, 0 \leq j \leq e-1$$

or

$$\tau = \theta_i + \theta_j, \quad \text{with } 0 \leq i < j \leq e-1.$$

*Proof.* We shall take full advantage of what has already been proved in §20B. In particular, we know that if  $(\tau, \zeta_i) > 0$  for an exceptional character  $\zeta_i$ , then  $\sum \zeta_i$  is a summand of  $\tau$ . We also recall that the decomposition numbers of the irreducible characters in  $B_1$  are either 0 or 1, so that  $(\tau, \zeta) = 0$  or 1 for all irreducible characters  $\zeta$  in  $B_1$ .

Suppose  $\sum \zeta_i$  is a summand of  $\tau$ . Then  $\tau$  contains at least one of the characters  $\theta_j$ ,  $0 \leq j \leq e-1$ , since  $\tau$  vanishes on  $D^*$ , while  $\sum \zeta_i$  does not, by Theorem 20.20. Assume  $\sum \zeta_i + \theta_j + \theta_l$  is a summand of  $\tau$ . Then  $h(\sum \zeta_i + \theta_j + \theta_l) \leq 1$  by (20.16). We may assume that

$$\Gamma_1 = (1_D - \xi)^G = -\varepsilon \zeta_1 + \sum c_j \theta_j, \quad \text{where } c_0 \theta_0 = 1_G.$$

Then

$$\begin{aligned} 1 &\geq h(\sum \zeta_i + \theta_j + \theta_l) \geq |(\sum \zeta_i + \theta_j + \theta_l, 1_D - \xi)_D| \\ &= |(\sum \zeta_i + \theta_j + \theta_l, \Gamma_1)_G| = |-\varepsilon + c_j + c_l|. \end{aligned}$$

Since  $\varepsilon$ ,  $c_j$ , and  $c_l$  are all  $\neq 1$ , some partial sum  $-\varepsilon + c_j$ ,  $-\varepsilon + c_l$  or  $c_j + c_l$  is  $\pm 2$ , and this contradicts (20.16), since the characters  $\sum \zeta + \theta_j$ ,  $\sum \zeta + \theta_l$ , and  $\theta_j + \theta_l$  are

also summands of  $\tau$ . A similar argument shows that if  $\sum \zeta_i$  is not a summand of  $\tau$ , then  $\tau$  is a sum of exactly two of the remaining characters  $\{\theta_i\}$ . This completes the proof.

Using Proposition 62.58, the decomposition numbers of the block  $B_1$ , which are the multiplicities of the irreducible  $K$ -characters in the indecomposable projective characters  $\tau$  by (18.26), can be described by a graph, as follows. There are  $e+1$  vertices of the graph, labeled by the irreducible characters  $\{\theta_0, \theta_1, \dots, \theta_{e-1}\}$  and  $\theta_{exc} = \sum \zeta_i$ . Two vertices are joined by an edge if and only if the corresponding characters are summands of some indecomposable projective character  $\tau$ . Since the graph contains exactly  $e+1$  vertices and  $e$  edges, it contains no closed paths, and is a tree, called the *Brauer tree* of the block  $B_1$ .

From Dade's results [66] (see also Feit [82, Chapter VII]), it follows that the same remarks apply to an arbitrary block with a cyclic defect group, in any finite group  $G$ . Green proved [74] that the periodic projective resolution described in Theorem 62.56 is closely related to the Brauer tree, and describes a "walk" around the Brauer tree.

## §62. Exercises

In Exercises 1 and 2,  $R$  denotes a field of characteristic  $p$ , or a complete d.v.r. whose residue field has characteristic  $p$ .

- Let  $\mathcal{L}$  be a family of subgroups of  $G$ . An  $RG$ -lattice  $M$  is called  $(G, \mathcal{L})$ -projective (see (20.1)) if and only if  $M = \bigoplus M_i$ , for a set of  $RG$ -lattices  $\{M_i\}$  such that, for each  $i$ ,  $M_i$  is  $(G, Z_i)$ -projective for some subgroup  $Z_i \in \mathcal{L}$ . Prove that  $M$  is  $(G, \mathcal{L})$ -projective if and only if  $\text{id}_M$  is  $(G, \mathcal{L})$ -projective (see §62B).

[Hint: Using (62.1), reduce to the case of an indecomposable  $RG$ -lattice  $M$ . In that case,  $\text{id}_M$  is a primitive idempotent. If  $(M, M)_G = \sum (M, M)_{G/Z_i}$ , then  $\text{id}_M \in (M, M)_{G/Z_i}$  for some subgroup  $Z_i$ , by Rosenberg's Lemma 57.8 and (62.1).]

- Let  $M_1, M_2$  be  $(H, D)$ -projective  $RH$ -lattices, for  $D \leq H$ . Prove that  $(M_1, M_2)_H = (M_1, M_2)_{H/D}$ .
- Let  $k$  be a field of characteristic  $p$ , and let  $G$  be a finite group having a cyclic Sylow  $p$ -subgroup. Apply Theorem 62.21 to prove that  $kG$  has finite representation type (see Higman's Theorem (CR (64.1))).
- Let  $A$  be a f.d.  $k$ -algebra, for a field  $k$ . Prove that a f.g. left  $A$ -module  $M$  is uniserial (see (62.22)) if and only if the  $k$ -dual  $M^*$  is a f.g. uniserial right  $A$ -module.
- Let  $M$  be a f.g. uniserial left  $A$ -module, for a f.d. algebra  $A$  over a field  $k$ . Prove that  $M$  is a homomorphic image of a P.I.M.

[Hint: Let  $P$  be a P.I.M. such that  $P/\text{rad } P \cong M/\text{rad } M$ , and deduce that  $P$  is a projective cover of  $M$  (see Theorem 6.23).]

- Let  $H \trianglelefteq G$ , and assume  $|G:H| \not\equiv 0 \pmod{p}$  for a prime  $p$ . Let  $k$  be a field of characteristic  $p$ . Prove that  $\text{rad } kG = (\text{rad } kH)kG = kG(\text{rad } kH)$ .

[Hint (Feit): Since  $H \trianglelefteq G$ ,  $x(\text{rad } kH)x^{-1} \subseteq \text{rad } kH$  for all  $x \in G$ , so  $(\text{rad } kH)kG = kG(\text{rad } kH)$  is a nilpotent two-sided ideal in  $kG$ . Then show that each left  $kG$ -module is  $(G, H)$ -projective, since  $|G:H| \neq 0$  in  $k$ . It follows that each ses

$$0 \rightarrow M' \rightarrow M \rightarrow kG/(\text{rad } kH)kG \rightarrow 0$$

of f.g.  $kG$ -modules splits when restricted to  $kH$ , and hence is a split ses of  $kG$ -modules. Thus  $kG/(\text{rad } kH)kG$  is a semisimple  $kG$ -module, and  $\text{rad } kG \subseteq (\text{rad } kH)kG$ , completing the proof.]

7. (Green [74]). Prove that the Heller operator  $\Omega$  commutes with the Green Correspondence. More precisely, let  $H \geq N_G(D)$ , and let  $g$  be the Green Correspondence from indecomposable nonprojective  $(H, D)$ -projective  $kH$ -modules  $L$  to nonprojective indecomposable  $(G, D)$ -projective  $kG$ -modules  $g(L)$ . Prove that in this situation,

$$\Omega gL \cong g(\Omega L).$$

(The result is needed (in (62.55)) only in case  $\mathcal{X} = \{1\}$ , and can be proved using Schanuel's Lemma.)

8. Determine the Brauer tree of the principal  $p$ -block of  $PSL_2(\mathbb{F}_p)$  (see (62.57)).

## §63. APPLICATIONS TO GROUP THEORY

### §63A. The Kernel of the Principal Block

In this subsection,  $G$  denotes a finite group,  $p$  a prime number, and  $(K, R, k)$  a  $p$ -modular system such that  $\text{char } K = 0$  and  $K$  is sufficiently large relative to  $G$ . The  $K$ -kernel of a  $p$ -block  $B$  of  $G$  is the intersection of the kernels of the irreducible  $K$ -characters belonging to  $B$ . Similarly, the  $k$ -kernel of  $B$  is the intersection of the kernels of the irreducible  $k$ -representations of  $G$  belonging to  $B$ . We shall prove two results of Brauer [64] on the kernel of the principal block.

**(63.1) Theorem.** *The  $K$ -kernel of the principal  $p$ -block  $B_1$  of  $G$  is the maximal normal  $p'$ -subgroup  $O_{p'}(G)$  of  $G$ .*

*Proof.* Let

$$f = |O_{p'}(G)|^{-1} \sum_{x \in O_{p'}(G)} x.$$

Then  $f$  is an idempotent in the center  $c(RG)$  of  $RG$ , since  $O_{p'}(G)$  is a normal  $p'$ -subgroup of  $G$ ;  $Kf$  affords the trivial representation of  $O_{p'}(G)$ . We have

$$f = \sum_{i \in I} b_i,$$

for certain block idempotents  $b_i \in c(RG)$ , and each block idempotent  $b_i$  can be

expressed as a sum

$$b_i = \sum_{\zeta^j \in B_i} e_j,$$

where  $\{e_j\}$  is the set of central primitive idempotents in  $KG$  associated with characters  $\zeta^j$  belonging to the block  $B_i$  defined by  $b_i$ . The central primitive idempotents  $e_j$  which occur as summands of  $f$  are characterized by the condition  $fe_j = e_j$ . In particular, we have  $fe_1 = e_1$ , where  $e_1 = |G|^{-1} \sum_{g \in G} g$  is the central primitive idempotent associated with the trivial  $K$ -character  $1_G$  of  $G$ . It follows that the block idempotent  $b_1$  associated with the principal block  $B_1$  of  $G$  is a summand of  $f$ . Consequently,  $fe_j = e_j$  for all irreducible characters  $\zeta^j$  belonging to  $B_1$ , and it follows that

$$O_{p'}(G) \leq \bigcap_{\zeta^j \in B_1} \ker \zeta^j.$$

For the reverse inclusion, let  $N$  denote the  $K$ -kernel of  $B_1$ . If  $N \not\leq O_{p'}(G)$ , then  $p \mid |N|$ , and hence  $N$  contains a  $p$ -element  $u \neq 1$ . Then by the  $p$ -section orthogonality theorem (60.2), we have

$$0 = \sum_{\zeta^j \in B_1} \zeta^j(u) \zeta^j(1) = \sum_{\zeta^j \in B_1} (\zeta^j(1))^2,$$

which is impossible. Therefore  $N \leq O_{p'}(G)$  and the theorem is proved.

**(63.2) Theorem.** *The  $k$ -kernel of the principal  $p$ -block  $B_1$  is  $O_{p',p}(G)$ , which is the maximal normal subgroup  $L$  containing  $O_{p'}(G)$  such that the quotient  $L/O_{p'}(G)$  is a  $p$ -group.*

*Proof.* Let  $Q$  be the  $k$ -kernel of  $B_1$ , and let  $F_j$  be a simple  $kG$ -module belonging to  $B_1$ . Then there exists a simple  $KG$ -module  $Z_i$  belonging to  $B_1$  such that  $F_j$  occurs as a composition factor of  $\bar{M}_i$ , where  $M_i$  is a full  $RG$ -lattice in  $Z_i$ , since the decomposition map is surjective (see Corollary 18.14). If  $x \in O_{p'}(G)$ , then  $x$  acts trivially on  $Z_i$  by Theorem 63.1, and hence  $x$  acts trivially on  $F_j$ . This proves that  $O_{p'}(G) \leq Q$ .

Now let  $s$  be a  $p'$ -element in  $Q$ . Then  $\varphi^j(s) = \varphi^j(1)$  for all irreducible Brauer characters  $\varphi^j \in B_1$ . For each irreducible  $K$ -character  $\zeta^i \in B_1$ , we have

$$\zeta^i = \sum_{\varphi^j \in B_1} d_{ij} \varphi^j \text{ on } G_{p'},$$

where  $(d_{ij})$  is the decomposition matrix (see (56.27)). It follows that

$$\zeta^i(s) = \sum_{\varphi^j \in B_1} d_{ij} \varphi^j(s) = \sum_{\varphi^j \in B_1} d_{ij} \varphi^j(1) = \zeta^i(1).$$

Thus  $s$  belongs to the  $K$ -kernel of  $B_1$ , which is  $O_{p'}(G)$  by (63.1). At this point, we have proved that  $Q/O_{p'}(G)$  is a  $p$ -group.

On the other hand,  $O_{p'}(G)$  acts trivially on each simple  $kG$ -module  $F_j$  belonging to  $B_1$ , by the first part of the proof, so  $F_j$  is a simple  $k(G/O_{p'}(G))$ -module. By Clifford's Theorem (see (17.16)), any normal  $p$ -subgroup of  $G/O_{p'}(G)$  acts trivially on  $F_j$ , and it follows that  $O_{p',p}(G) \leq Q$ . This completes the proof.

**(63.3) Corollary.** *The group  $G$  has a normal  $p$ -complement (see §13C) if and only if the Brauer character  $\varphi^1$  afforded by the trivial  $kG$ -module is the only irreducible Brauer character belonging to the principal block.*

*Proof.* We clearly have

$$O_{p',p}(G) = G \Leftrightarrow G \text{ has a normal } p\text{-complement.}$$

But the condition  $O_{p',p}(G) = G$  is also equivalent to the statement that  $\varphi^1$  is the only irreducible Brauer character belonging to  $B_1$ , by (63.2). This completes the proof.

### §63B. The Brauer-Suzuki Theorem on Quaternion Sylow 2-Groups

A generalized quaternion 2-group  $S$  has a presentation

$$S = \langle x, y : x^{2^n} = 1, y^2 = x^{2^{n-1}}, x^y = x^{-1} \rangle.$$

The quaternion group  $Q$  is the generalized quaternion group of order 8. In §14E, we proved that the generalized quaternion groups of order  $\geq 16$  cannot occur as Sylow 2-subgroups of finite simple groups. In this subsection we shall prove the corresponding result for Sylow 2-subgroups of order 8:

**(63.4) Theorem.** (Brauer-Suzuki [59]). *Let  $G$  be a finite group whose Sylow 2-subgroups are quaternion groups of order 8, and let  $t$  be the unique involution in a Sylow 2-subgroup of  $G$ . Then  $G$  contains a proper normal subgroup  $N$  such that  $t \in N$ .*

This theorem completes the line of investigation begun in §14E, and will be applied in §63C to prove the important  $Z^*$ -theorem of Glauberman. A new approach is needed in order to prove Theorem 63.4, however, since the first two steps of the proof of Theorem 14.23 are not valid in case the Sylow groups are quaternion of order 8. Our method this time will be to investigate the  $K$ -characters in the principal 2-block of  $G$ , following the lectures of Dade [71].

We begin with some general remarks based on our previous discussion of  $p$ -sections and orthogonality (§60A). As in §60A, we fix a  $p$ -modular system  $(K, R, k)$  such that  $\text{char } K = 0$ ,  $K$  is sufficiently large relative to  $G$ , and  $R$  is a complete d.v.r. with maximal ideal  $\mathfrak{p}$  such that  $R/\mathfrak{p}$  is a perfect field of characteristic  $p$ .

Let  $T$  be a set of  $p$ -elements in  $G$  such that  $T = T^{-1}$ . The union of  $p$ -sections  $X(T)$  is defined by

$$X(T) = \{x \in G, x_p \in {}_G T\},$$

where  $x_p$  denotes the  $p$ -part of  $x$ , and  $u \in_G T$  means that  $u^g \in T$  for some  $g \in G$ . Then  $X(T)$  is a union of conjugacy classes,  $X(T) = X(T)^{-1}$ , and  $X(T)$  is also a union of  $p$ -sections (see §60A).

It will be useful to introduce some notation. We define sets of class functions:

$$\begin{aligned} \text{cf}(G, X(T)) &= \{\alpha \in \text{cf}_K(G) : \alpha(x) = 0 \text{ for all } x \in G - X(T)\}, \\ \text{cf}(G, X(T); B_j) &= \{\alpha_{B_j} : \alpha \in \text{cf}(G, X(T))\}, \end{aligned}$$

where  $\alpha_{B_j}$  is the contribution to  $\alpha$  from irreducible characters in the  $p$ -block  $B_j$ :

$$\alpha_{B_j} = \sum_{\zeta^i \in B_j} (\alpha, \zeta^i) \zeta^i, \quad \text{for } \alpha \in \text{cf}_K G.$$

As an immediate consequence of Theorem 60.3 and the above remarks, we have:

**(63.5) Proposition.** *Keep the preceding notation. Then*

$$\text{cf}(G, X(T)) = \bigoplus_j \text{cf}(G, X(T); B_j),$$

where the sum is taken over the  $p$ -blocks of  $G$ , and the summands are orthogonal with respect to the usual scalar product of class functions.

Now let  $S$  be a T.I. set in  $G$  with the property that  $x \in S$  if and only if  $x_p \in S$ , where  $x_p$  is the  $p$ -part of  $x$  (see (14.16)). Let  $T$  be the set of  $p$ -elements in  $S$ , and assume that  $T = T^{-1}$ . Let  $H = N_G(S)$ ; then  $S$  is the  $p$ -section in  $H$  defined by  $T$ , and the  $p$ -section  $X(T)$  in  $G$  defined by  $T$  is the set of all conjugates of elements of  $S$ :

$$X(T) = \{x^g : x \in S, g \in G\}.$$

We shall denote  $X(T)$  by  $S^G$ , in view of the preceding remark.

**(63.6) Theorem.** *Keep the preceding assumptions and notation. Then the induction map defines a surjective isometry*

$$\text{ind}_H^G : \text{cf}(H, S; B'_1) \rightarrow \text{cf}(G, S^G; B_1),$$

where  $B'_1$  and  $B_1$  denote the principal  $p$ -blocks of  $H$  and  $G$ , respectively. The inverse map is given by

$$\mu \mapsto \mu_S, \quad \text{for } \mu \in \text{cf}(G, S^G, B_1),$$

where  $\mu_S$  is the class function on  $H$  which coincides with  $\mu$  on  $S$  and vanishes on  $H - S$ .

*Proof.* Using Steps 2 and 3 of the proof of Frobenius's Theorem 14.2, it follows that

$$\text{ind}_H^G : \text{cf}(H, S) \rightarrow \text{cf}(G, S^G)$$

is an isometry, where  $S$  is the T.I. set described above and  $H = N_G(S)$ . The same arguments show that

$$(\psi^G)_S = \psi \quad \text{and} \quad (\mu_S)^G = \mu$$

for all  $\psi \in \text{cf}(H, S)$  and  $\mu \in \text{cf}(G, S^G)$ , where  $\psi^G = \text{ind}_H^G \psi$ , and  $\mu_S$  is defined as in the statement of the theorem. Therefore the induction map from  $\text{cf}(H, S)$  to  $\text{cf}(G, S^G)$  is surjective, and the inverse map is  $\mu \mapsto \mu_S$ .

In order to make a connection between the induction map and the principal blocks of  $H$  and  $G$ , we shall use Brauer's Second Main Theorem, and therefore we consider centralizers of the  $p$ -elements contained in  $S$ .

Let  $u \in T$ ; then  $C_G(u) \leq H$  since  $S$  is a T.I. set, and we set

$$X(u) = \{x \in C_G(u) : x_p \in \{u, u^{-1}\}\}.$$

Then  $X(u)$  is a  $p$ -section in  $H$  for each  $u \in T$ , and we have

$$S = \bigcup_{u \in T} X(u)$$

(note that  $X(u) = X(u^{-1})$  and that  $X(u)$  is a union of conjugacy classes in  $C_G(u)$ ).

Let  $\mu$  be a class function on any subgroup containing  $H$ , and let  $u \in T$ . We let  $\mu_{X(u)}$  denote the class function on  $C_G(u)$  which coincides with  $\mu$  on  $X(u)$  and vanishes outside  $X(u)$ . Then by (63.5), applied to  $C_G(u)$ , we have

$$(63.7) \quad \mu_{X(u)} = \sum_{\tilde{\mathcal{B}}_i} (\mu_{X(u)})_{\tilde{\mathcal{B}}_i}$$

where  $\{\tilde{\mathcal{B}}_i\}$  are the blocks of  $C_G(u)$ .

In particular, if  $\mu \in \text{cf}(G, S^G, \mathcal{B}_1)$ , then (63.7) becomes

$$(63.8) \quad \mu_{X(u)} = (\mu_{X(u)})_{\tilde{\mathcal{B}}_1}, \quad (\mu_{X(u)})_{\tilde{\mathcal{B}}_i} = 0 \quad \text{if } \tilde{\mathcal{B}}_i \neq \tilde{\mathcal{B}}_1,$$

where  $\tilde{\mathcal{B}}_1$  is the principal block of  $C_G(u)$ , by Brauer's Second and Third Main Theorems (see (59.14) and (61.16)).

On the other hand, if  $\psi$  is a class function on a subgroup containing  $H$ , we have

$$\psi_S = \sum (\psi_S)_{\mathcal{B}'_j}$$

by (63.5) again, since  $S$  is a  $p$ -section in  $H$ , and the sum is taken over the blocks of  $H$ . Another application of the Second Main Theorem yields

$$((\psi_S)_{\mathcal{B}'_j})_{X(u)} = \sum_{(\mathcal{B}_i)^H = \mathcal{B}'_j} (\psi_{X(u)})_{\mathcal{B}_i},$$

where the sum is taken over the blocks of  $C_G(u)$ .

Now let  $\mu \in \text{cf}(G, S^G; B_1)$ . Noting that  $S = \bigcup_{u \in T} X(u)$ , and that

$$\tilde{B}_i^G = B_1 \Leftrightarrow \tilde{B}_i^H = B'_1 \Leftrightarrow \tilde{B}_i = \tilde{B}_1 \text{ (by (61.16))},$$

we obtain

$$\mu_S = \sum_{u \in T} (\mu_S)_{X(u)} = \sum_{u \in T} ((\mu_S)_{X(u)})_{B_1} = (\mu_S)_{B'_1},$$

by (63.8) and the preceding remarks. Thus we have proved that the map  $\mu \rightarrow \mu_S$  carries  $\text{cf}(G, S^G; B_1)$  into  $\text{cf}(H, S; B'_1)$ .

In order to finish the proof, we have to show that  $\psi^G \in \text{cf}(G, S^G; B_1)$  for all  $\psi \in \text{cf}(H, S; B'_1)$ . We have  $\psi^G = \sum_i (\psi^G)_{B_i}$  and  $(\psi^G)_{B_i} \in \text{cf}(G, S^G; B_i)$  for all  $p$ -blocks  $B_i$  of  $G$ , by (63.5). We shall prove that

$$(63.9) \quad (((\psi^G)_{B_i})_S)_{B'_1} = 0 \quad \text{if } B_i \neq B_1.$$

This will imply that

$$((\psi^G)_{B_1})_S = (\psi^G)_S,$$

and hence  $\psi^G = (\psi^G)_{B_1} \in \text{cf}(G, S^G; B_1)$  since  $\mu \rightarrow \mu_S$  is the inverse of the induction map. In order to prove (63.9), let  $\mu \in \text{cf}(G, S^G; B_i)$ , for  $i \neq 1$ . Then for each  $u \in T$ , we have, as in (63.8),

$$\mu_{X(u)} = \sum_j (\mu_{X(u)})_{B_j}$$

where the sum is taken over blocks  $\tilde{B}_j$  of  $C_G(u)$  such that  $(\tilde{B}_j)^G = B_i$ . Then  $(\mu_{X(u)})_{B_1} = 0$ , by (61.16), where  $\tilde{B}_1$  is the principal block of  $C_G(u)$ . Since  $u$  is arbitrary in  $T$ , and  $\mu_S = \sum_{u \in T} (\mu_S)_{X(u)}$ , we obtain  $(\mu_S)_{B'_1} = 0$ , completing the proof of (63.9), and also the proof of Theorem 63.6.

The preceding result gives a method for finding the irreducible characters in the principal block of  $G$  which do not vanish on  $S^G$ . In particular, this construction works in the following situation.

**(63.10) Definition.** Keep the assumptions and notation from Theorem 63.6. Let  $\{\psi_1, \dots, \psi_h\}$  be the set of irreducible  $K$ -characters of  $B'_1$  which do not vanish on  $S$ ; these characters  $\{\psi_i\}$  are said to be *coherent* in case there exist irreducible  $K$ -characters of  $G$   $\{\zeta_1, \dots, \zeta_h\}$  and signs  $\varepsilon_i = \pm 1$ ,  $1 \leq i \leq h$ , with the property that whenever  $a_1\psi_1 + \dots + a_h\psi_h \in \text{cf}(H, S; B'_1)$ , for  $a_i \in K$ , we have

$$(a_1\psi_1 + \dots + a_h\psi_h)^G = a_1\varepsilon_1\zeta_1 + \dots + a_h\varepsilon_h\zeta_h.$$

**(63.11) Theorem.** Let  $\{\psi_1, \dots, \psi_h\}$  be coherent, according to (63.10). Then  $\{\zeta_1, \dots, \zeta_h\}$  are precisely the irreducible characters in the principal block  $B_1$  of  $G$

which do not vanish on  $S^G$ . Moreover, we have

$$\zeta_i|_S = \varepsilon_i \psi_i|_S, \quad \text{for } 1 \leq i \leq h.$$

*Proof.* We shall use the notation  $\xi_X$  for the function which is equal to  $\xi$  on  $X$ , and vanishes off  $X$ , and  $\xi|_X$  for the restriction of  $\xi$  to  $X$ , for  $\xi \in \text{cf}(G)$ , and  $X \subseteq G$ . We shall also need the result that, for a union of  $p$ -sections  $X \subseteq G$  and an irreducible character  $\zeta$  belonging to a block  $B$ , we have

$$(63.12) \quad \zeta_X \in \text{cf}(G, X; B),$$

which is easily proved using  $p$ -section orthogonality (60.2) and (60.3).

To begin the proof, let  $\zeta$  be an irreducible character in  $B_1$  which does not vanish on  $S^G$ . Then  $\zeta_{S^G}$  is a nonzero element of  $\text{cf}(G, S^G; B_1)$ , and hence, by Theorem 63.6,  $(\zeta_{S^G}, \psi^G) \neq 0$  for some  $\psi \in \text{cf}(H, S; B'_1)$ . Since the characters  $\{\psi_i\}$  are coherent, we have  $\psi = \sum a_i \psi_i$  for some coefficients  $a_i \in K$ , and  $\psi^G = \prod a_i \varepsilon_i \zeta_i \in \text{cf}(G, S^G; B_1)$ . Then

$$(\zeta_{S^G}, \psi^G) = (\zeta, \sum a_i \varepsilon_i \zeta_i) \neq 0,$$

and  $\zeta = \zeta_i$  for some  $i$ ,  $1 \leq i \leq h$ .

It remains to prove that  $\zeta_i \in B_1$  and  $\zeta_i|_{S^G} \neq 0$ , etc. for  $1 \leq i \leq h$ . By (63.12),  $(\psi_i)_S \in \text{cf}(H, S; B'_1)$ , for  $1 \leq i \leq h$ . Then  $((\psi_i)_S, \psi)_H \neq 0$  for some  $\psi = \sum a_j \psi_j$  in  $\text{cf}(H, S; B'_1)$  and we have

$$a_i = (\psi_i, \psi)_H = ((\psi_i)_S, \psi)_H \neq 0.$$

Then  $\psi^G = \sum a_i \varepsilon_i \zeta_i \in \text{cf}(G, S^G; B_1)$  by (63.6), and  $\zeta_i$  appears with nonzero multiplicity in  $\psi^G$ , so  $\zeta_i \in B_1$ .

For all  $\psi \in \text{cf}(H, S; B'_1)$ , we have

$$(\zeta_i, \psi^G) = ((\varepsilon_i \psi_i)_S, \psi) \quad \text{for } 1 \leq i \leq h,$$

by the preceding discussion. It follows that

$$(63.13) \quad ((\zeta_i)_S, \psi)_H = (\zeta_i|_H, \psi) = (\zeta_i, \psi^G) = ((\varepsilon_i \psi_i)_S, \psi)$$

for all  $\psi \in \text{cf}(H, S; B'_1)$ . We have  $(\varepsilon_i \psi_i)_S \in \text{cf}(H, S; B'_1)$  and  $(\zeta_i)_S \in \text{cf}(G, S^G; B_1)$  by (63.12), and hence  $(\zeta_i)_S = ((\zeta_i)_S^G \in \text{cf}(H, S; B'_1)$ , by Theorem 63.6. Then  $(\zeta_i)_S = (\varepsilon_i \psi_i)_S$  by (63.13), since the scalar product  $(\ , \ )_H$  is nondegenerate when restricted to  $\text{cf}(H, S; B_1)$  (see (63.5)). This completes the proof of the theorem.

We are now ready to begin the proof of the Brauer-Suzuki Theorem 63.4. Let  $G$  be a counterexample of minimal order, and let  $Q$  be a fixed Sylow 2-subgroup of  $G$ . Using the preceding results, we shall first study the characters in the principal

2-blocks of certain subgroups of  $G$ , and use this information to derive a contradiction involving characters in the principal 2-block of  $G$ .

Throughout the discussion, we are concerned only with the prime  $p = 2$ , and therefore consider characters, modules, etc., with reference to a fixed 2-modular system  $(K, R, k)$  satisfying the assumptions made earlier in the section. We begin with a series of lemmas, starting from properties of the subgroup  $Q$ .

**(63.14) Lemma.** *All elements of order 4 in  $Q$  are conjugate in  $G$ .*

*Proof.* Let  $x, y$  have order 4 in  $Q$ . We may assume that  $\langle x \rangle \neq \langle y \rangle$  since  $x =_Q x^{-1}$ . Suppose  $x \neq {}_G y$ ; then  $\langle x \rangle \neq {}_G \langle y \rangle$ . We shall apply the transfer homomorphism

$$V_{\langle y \rangle}^G : G/G' \rightarrow \langle y \rangle$$

(see (13.10)), and will prove that  $xG' \notin \ker V_{\langle y \rangle}^G$ , using a computation similar to the proof of Burnside's Transfer Theorem 13.20. We first consider the orbits of  $\langle x \rangle$  acting on  $G/\langle y \rangle$ . Let  $z_i \langle y \rangle$  be a representative of an  $\langle x \rangle$ -orbit of cardinality  $d_i$ ; then  $\{x^j z_i, 0 \leq j \leq d_i - 1\}$  are representatives of the cosets of  $G/\langle y \rangle$  corresponding to the orbit, and we have

$$xx^j z_i = x^{j+1} z_i, \quad 0 \leq j \leq d_i - 1 \quad \text{and} \quad xx^{d_i-1} z_i = z_i y_i, \quad \text{for } y_i \in \langle y \rangle.$$

Then

$$V_{\langle y \rangle}^G xG' = \prod y_i = \prod z_i^{-1} x^{d_i} z_i,$$

where the product is taken over the  $\langle x \rangle$ -orbits, of cardinalities  $\{d_i\}$ . If some  $d_i$  is odd, then  $\langle (x^{d_i})^{z_i} \rangle = \langle x^{z_i} \rangle \subseteq \langle y \rangle$  since  $d_i$  is the least power of  $x^{z_i}$  contained in  $\langle y \rangle$ . This implies that  $x =_G y$ , contrary to assumption. If  $d_i$  is even, then  $(x^{d_i})^{z_i} = x^{d_i}$  (since  $4|d_i \Rightarrow x^{d_i} = 1$ , while if  $2|d_i$  (but not 4), then  $(x^{d_i})^{z_i} = y^2 = x^2 = x^{d_i}$ ). Therefore

$$V_{\langle y \rangle}^G xG' = x^{|G/\langle y \rangle|} \neq 1$$

since  $|G/\langle y \rangle| = 2q$  with  $q$  odd, and  $x^{2q} \neq 1$ . On the other hand,  $V_{\langle y \rangle}^G x^2 G' = x^{2|G/\langle y \rangle|} = 1$ . It follows that  $G$  contains a proper normal subgroup  $N$  such that  $t = x^2 \in N$ , where  $t$  is the involution in  $Q$ . This contradicts the assumption that  $G$  is a minimal counterexample, and completes the proof.

**(63.15) Corollary.** *All elements of order 4 in  $Q$  are conjugate in  $C_G(t)$ , where  $t$  is the unique involution in  $Q$ .*

*Proof.* Let  $x, y \in Q$  be elements of order 4. Then  $x^g = y$  for some  $g \in G$ , by (63.14). Then  $x^2 = y^2 = t$ , and it follows that  $g \in C_G(t)$ .

Now we fix some notation for the rest of the proof. We set

$$H = C_G(t) \quad \text{and} \quad L = N_G(\langle x \rangle),$$

where  $t$  is the involution in  $Q$  and  $x$  is a fixed element of order 4 in  $Q$ . We clearly have  $L \leq H$ .

**(63.16) Lemma.** *We have*

$$L = QO_2(L) \quad \text{and} \quad O_2(L) \leq C_G(x).$$

*Proof.* Since  $\langle x \rangle \leq Q$ ,  $Q$  is also a Sylow 2-subgroup of  $L$ . The map  $x \rightarrow x^{-1}$  is the only nontrivial automorphism of  $\langle x \rangle$ , so any element of  $Q - \langle x \rangle$  inverts  $x$ . It follows that  $L = QC_G(x)$ , and that  $\langle x \rangle = Q \cap C_G(x)$  is a cyclic Sylow 2-subgroup of  $C_G(x)$ . Then  $C_G(x) = \langle x \rangle O_2(C_G(x))$  by (13.22). Moreover,  $O_2(C_G(x))$  is characteristic in  $C_G(x)$  and hence normal in  $L$ , so  $L = QO_2(C_G(x))$  and  $O_2(C_G(x)) = O_2(L)$ . This completes the proof.

By (63.1), the characters in the principal block  $B_1(L)$  contains  $O_2(L)$  in their kernels, and are consequently the irreducible characters of  $Q$ , lifted to  $L$ , by (63.16). We expect a factorization  $G = HO_2(G)$ , and hence, using (63.1), we hope to construct characters in the principal block of  $G$  from those in  $B_1(H)$ , and, in turn, from the known characters in  $B_1(L)$ . We now begin to put this plan into action.

The character table of  $Q$  is as follows:

	1	$t$	$x$	$y$	$xy$
1	1	1	1	1	1
$\lambda_1$	1	1	1	-1	-1
$\lambda_2$	1	1	-1	1	-1
$\lambda_3$	1	1	-1	-1	1
$\theta$	2	-2	0	0	0

where  $y$  is an element of order 4 such that  $\langle y \rangle \neq \langle x \rangle$ .

Each irreducible character  $\lambda$  of  $Q$  can be extended to an irreducible character  $\tilde{\lambda}$  of  $L$  having  $O_2(L)$  in its kernel, by (63.16). As an immediate consequence of (63.1) and (63.16), we have:

**(63.17) Lemma.**  $B_1(L) = \{\tilde{1}, \tilde{\lambda}_1, \tilde{\lambda}_2, \tilde{\lambda}_3, \tilde{\theta}\}$ .

We next begin to investigate  $B_1(H)$ , using (63.6), and the sets

$$\sqrt{x} = \{l \in L : x \in \langle l \rangle\}$$

and

$$\sqrt{x^H} = \{l^h : l \in \sqrt{x}, h \in H\}.$$

**(63.18) Lemma.** (i)  $\sqrt{x}$  is a T.I. set in  $L$  with the property that  $l \in \sqrt{x} \Leftrightarrow l_2 \in \sqrt{x}$ .

$$(ii) \quad \sqrt{x} = xO_{2'}(L) \cup x^{-1}O_{2'}(L).$$

$$(iii) \quad \text{cf}(L, \sqrt{x}, B_1(L)) = \langle \tilde{\lambda} + \tilde{\lambda}_1 - \tilde{\lambda}_2 - \tilde{\lambda}_3 \rangle.$$

(iv) The virtual character

$$\varphi = (\tilde{\lambda} + \tilde{\lambda}_1 - \tilde{\lambda}_2 - \tilde{\lambda}_3)^H$$

generates  $\text{cf}(H, \sqrt{x^H}, B_1(H))$ .

(v)  $(\varphi, \varphi)_H = 4$ , so  $\varphi = 1 + a_1\psi_1 + a_2\psi_2 + a_3\psi_3$  for some irreducible characters  $\psi_i \in B_1(H)$  and signs  $a_i = \pm 1$ . Moreover,  $\{\tilde{\lambda}, \tilde{\lambda}_1, \tilde{\lambda}_2, \tilde{\lambda}_3\}$  are coherent (see (63.10)) with  $\varepsilon_1 = a_1$ ,  $\varepsilon_2 = -a_2$ ,  $\varepsilon_3 = -a_3$ .

(vi) The irreducible characters in  $B_1(H)$  which do not vanish on  $(\sqrt{x})^H$  are precisely  $\{1, \psi_1, \psi_2, \psi_3\}$ .

(vii) We have  $a_1\psi_1 = a_2\psi_2 = a_3\psi_3 = 1$  on  $\sqrt{x}$  and also on  $(\sqrt{x})^H$ .

The proof is left as an exercise, using (63.6) and (63.11). Note that (iii) follows from (63.17). The fact that  $(\varphi, \varphi)_H = 4$  follows by Steps 2 and 3 of Theorem 14.2, since  $\tilde{\lambda} + \tilde{\lambda}_1 + \tilde{\lambda}_2 - \tilde{\lambda}_3$  vanishes off the T.I. set  $\sqrt{x}$ . Part (v) follows from (63.6), and the coherence condition (63.10) is easily verified. For the proof of (vii) we have

$$a_1\psi_1(x) = \tilde{\lambda}_1(x) = 1,$$

$$a_2\psi_2(x) = -\varepsilon_2\psi_2(x) = -\tilde{\lambda}_2(x) = 1,$$

$$a_3\psi_3(x) = -\varepsilon_3\psi_3(x) = -\tilde{\lambda}_3(x) = 1,$$

using the character table of  $Q$ .

In order to construct the remaining irreducible characters in  $B_1(H)$ , we make a deeper study of  $\text{ch } H$ , using the Brauer Criterion 15.15, and the fact that for all irreducible characters  $\psi$  of  $H$ , we have

$$\text{either } \psi(th) = \psi(h) \text{ for all } h \in H, \text{ or } \psi(th) = -\psi(h) \text{ for all } h \in H,$$

since  $\langle t \rangle$  is contained in  $Z(H)$ . We also note that

$$\langle t \rangle H_{2'} = H_{2'} \cup tH_{2'},$$

where  $H_{2'}$  is the set of all elements of odd order belonging to  $H$ . Since  $t \in Z(H)$ ,

$\langle t \rangle H_2$  is the 2-section in  $H$  consisting of all elements whose 2-part is either 1 or  $t$ .

We now define two sets of virtual characters:

$$X_+ = \{\xi \in \text{ch } H : \xi \in \text{cf}(H, \langle t \rangle H_2; \mathbb{B}_1(H)) \text{ and } \xi(th) = \xi(h) \text{ for all } h \in H\},$$

$$X_- = \{\xi \in \text{ch } H : \xi \in \text{cf}(H, \langle t \rangle H_2; \mathbb{B}_1(H)) \text{ and } \xi(th) = -\xi(h) \text{ for all } h \in H\},$$

Both  $X_+$  and  $X_-$  are  $\mathbb{Z}$ -submodules of  $\text{ch } H$ . We next define a map  $\xi \rightarrow \xi^*$ , for  $\xi \in X_+ \cup X_-$ , where  $\xi^* \in \text{cf } H$  is given by

$$\xi^*(h) = \begin{cases} \xi(h) & \text{if } h \in H_2, \\ -\xi(h) & \text{if } h \in tH_2, \\ 0 & \text{otherwise.} \end{cases}$$

(63.19) Lemma. *The map  $\xi \rightarrow \xi^*$  has the properties*

$$(X_+)^* \subseteq X_-, \quad (2X_-)^* \subseteq X_+,$$

and is an isometry with respect to the scalar product of class functions on  $H$ .

*Proof.* Let  $\xi \in X_+ \cup 2X_-$ . We first prove that  $\xi^* \in \text{ch } H$ , using Brauer's Criterion 15.15. We must show that  $\xi^*|_E \in \text{ch } E$ , for all elementary subgroups  $E \leq H$ . By (63.15),  $\{1, t, x\}$  are representatives of all conjugacy classes of 2-elements in  $H$ , so it is sufficient to consider elementary subgroups  $E$  of the following types:

$$E = T, \quad \langle t \rangle \times T, \quad \langle x \rangle \times T, \quad \text{and} \quad Q \times T$$

where  $T$  is any subgroup of odd order.

Case 1.  $E = T$ . Then  $\xi^* = \xi$ .

Case 2.  $E = \langle t \rangle \times T$ . Since  $\xi \in X_+ \cup 2X_-$ , we have  $\xi|_E = \lambda \otimes \mu$ , where  $\lambda$  is a linear character of  $\langle t \rangle$  and  $\mu$  is a virtual character of  $T$ . Then  $\xi^*|_E = \lambda' \otimes \mu$ , where  $\lambda'$  is the other linear character of  $T$ .

Case 3.  $E = \langle x \rangle \times T$ . If  $\xi \in X_+ \cup X_-$ , then  $\xi$  vanishes on elements of order 4, so  $\xi|_E = \lambda^{(x)} \otimes \tau$  where  $\lambda$  is a linear character of  $\langle t \rangle$  and  $\tau \in \text{ch } T$ . Then  $\xi^*|_E = (\lambda')^{(x)} \otimes \tau \in \text{ch } E$ , where  $\lambda'$  is defined as in Case 2.

Case 4.  $E = Q \times T$ . Assume first that  $\xi \in X_-$ . Then  $\xi|_E = \theta \otimes \tau$  for some  $\tau \in \text{ch } T$ , since all characters of  $Q$  different from  $\theta$  have  $t$  in their kernel. Then if  $\xi \in 2X_-$ ,  $\xi|_E = 2\theta \otimes \tau$  and  $\xi^*|_E = (1 + \lambda_1 + \lambda_2 + \lambda_3) \otimes \tau$  (since  $2\theta$  has degree 4, and a character of  $Q$  vanishing on  $Q - \langle t \rangle$  is a multiple of the regular character of  $Q/\langle t \rangle$ ). If  $\xi \in X_+$ , then  $\xi|_E = (1 + \lambda_1 + \lambda_2 + \lambda_3) \otimes \tau$  for  $\tau \in \text{ch } T$ , and  $\xi^*|_E = 2\theta \otimes \tau$ . This completes the proof that  $\xi^* \in \text{ch } H$  for all  $\xi \in X_+ \cup 2X_-$ .

We have, for  $\xi_1, \xi_2 \in X_+ \cup 2X_-$

$$(\xi_1^*, \xi_2^*) = |H|^{-1} \sum_{h \in H} \xi_1^*(h) \xi_2^*(h^{-1}) = |H|^{-1} \sum_{h \in H} \xi_1(h) \xi_2(h^{-1})$$

by the definition of  $\xi^*$ .

At this point, we have  $\xi^* \in \text{cf}(H, \langle t \rangle H_2)$  for all  $\xi \in X_+ \cup 2X_-$ , and have to prove it is supported on  $B_1(H)$ . Let  $\psi \in \text{Irr } H$ , and assume  $(\psi, \xi^*) \neq 0$ , for  $\xi \in X_+ \cup 2X_-$ . Then

$$(\psi, \xi^*) = (\psi, (\xi)_{H_2}) - (\xi)_{tH_2} \neq 0.$$

Since both  $(\xi)_{H_2}$  and  $(\xi)_{tH_2}$  are in  $\text{cf}(H, \langle t \rangle H_2; B_1(H))$  by (63.12), we have  $\xi^* \in X_+ \cup X_-$ . The statements that  $(X_+)^* \subseteq X_-$  and  $(2X_-)^* \subseteq X_+$  are clear from what has been shown, and the lemma is proved.

**(63.20) Lemma.** *The irreducible characters in  $B_1(H)$  whose kernels contain  $t$  are precisely  $\{1, \psi_1, \psi_2, \psi_3\}$ .*

*Proof.* By (63.18vii), we have

$$a_i \psi_i(x) = 1 \quad \text{for } i = 1, 2, 3.$$

If  $t \notin \ker \psi_i$ , then  $\psi_i|_{\langle x \rangle} = c_1 \eta_1 + c_2 \eta_2$ , with  $c_i \in \mathbb{Z}$ , where  $\eta_1, \eta_2$  are the characters of  $\langle x \rangle$  not having  $t$  in their kernels, and it follows that  $\psi_i(x)$  is a multiple of  $\sqrt{-1}$ , which is impossible. Thus the characters  $1, \psi_1, \psi_2, \psi_3$  all have  $t$  in their kernels, and they all belong to  $B_1(H)$  by (63.18v).

Now let  $\psi$  be an irreducible character in  $B_1(H)$  such that  $t \in \ker \psi$ , and suppose that  $\psi \notin \{1, \psi_1, \psi_2, \psi_3\}$ . By (63.18vi),  $\psi$  vanishes on  $\sqrt{x^n} = H - \langle t \rangle H_2$ . It follows that  $\psi \in X_+$ , and hence  $\psi^* \in X_-$  by (63.19). Then  $(\psi^*, \psi^*) = (\psi, \psi) = 1$  and  $\psi^*(1) = \psi(1)$ , so  $\psi^* \in \text{Irr } H$ . The corresponding central idempotents  $\varepsilon$  and  $\varepsilon^* \in c(KH)$  satisfy

$$\varepsilon + \varepsilon^* = \psi(1)|H|^{-1} \sum_{h \in H} (\psi(h^{-1}) + \psi^*(h^{-1}))h = \psi(1)|H|^{-1} \sum_{h \in H_2} 2\psi(h^{-1})h,$$

by the definition of  $\psi^*$ . Since  $\psi$  vanishes on  $Q - \langle t \rangle$  and  $t \in \ker \psi$ , we have  $4|\deg \psi|$  (since  $\psi|_Q$  is a multiple of the regular character of  $Q/\langle t \rangle$ ). Then we obtain  $\varepsilon + \varepsilon^* \in RH$ , and hence  $\varepsilon + \varepsilon^* = b_1$ , where  $b_1$  is the block idempotent in  $B_1(H)$  (see (56.25)); but this is clearly impossible, since  $b_1$  must also have as a summand the central idempotent associated with the trivial representation.

**(63.21) Corollary.**  $X_+ = \{c_0 1 + c_1 a_1 \psi_1 + c_2 a_2 \psi_2 + c_3 a_3 \psi_3 : \sum c_i = 0, c_i \in \mathbb{Z}\}$ .

*Proof.* By (63.20) and the definition of  $X_+$ , any virtual character  $\xi \in X_+$  is a  $\mathbb{Z}$ -linear combination of  $\{1, a_1 \psi_1, a_2 \psi_2, a_3 \psi_3\}$ . Moreover, since  $\xi$  vanishes off  $\langle t \rangle H_2$ , we have  $\xi(x) = 0$ , and hence  $\sum c_i = 0$  by (63.18vii).

**(63.22) Lemma.**  $B_1(H)$  contains exactly three irreducible characters  $\psi_4, \psi_5, \psi_6$  whose kernels do not contain  $t$ , and  $X_- = Z\psi_4 + Z\psi_5 + Z\psi_6$ .

*Proof.* If  $\psi$  is an irreducible character in  $B_1(H)$  whose kernel does not contain  $t$ , then  $\psi \notin \{1, \psi_1, \psi_2, \psi_3\}$  by (63.20); therefore  $\psi$  vanishes on  $(\sqrt{x})^H$  by (63.18vi), and hence  $\psi \in X_-$ . By (63.19),  $X_+$  and  $X_-$  have the same  $Z$ -rank, and the  $Z$ -rank of  $X_+$  is 3 by (63.21). The lemma follows from these remarks.

**(63.23) Lemma.** There exist integers  $a_4, a_5, a_6 = \pm 1$  such that (after renumbering) we have

$$\begin{aligned} 2a_4\psi_4^* &= 1 + a_1\psi_1 - a_2\psi_2 - a_3\psi_3, \\ 2a_5\psi_5^* &= 1 - a_1\psi_1 + a_2\psi_2 - a_3\psi_3, \\ 2a_6\psi_6^* &= 1 - a_1\psi_1 - a_2\psi_2 + a_3\psi_3. \end{aligned}$$

*Proof.* We first observe that  $\{2\psi_4, 2\psi_5, 2\psi_6\}$  form a  $Z$ -basis for  $2X_-$ , by (63.22). We also have

$$(2\psi_i^*, 2\psi_j^*)_H = 4\delta_{ij},$$

using (63.19); since  $(2X_-)^* \subseteq X_+$ , we obtain

$$2\psi_4^* = c_01 + c_1a_1\psi_1 + c_2a_2\psi_2 + c_3a_3\psi_3, \quad \sum c_i = 0,$$

by (63.21). It is then easily checked that we can choose  $a_4 = \pm 1$  so that the first formula in (63.23) holds. The others are proved similarly.

By the argument used in the proof of (63.18i), it follows that  $\sqrt{t} = \{g \in H : t \in \langle g \rangle\}$  is a T.I. set in  $H$ , satisfying the condition that  $g \in \langle t \rangle$  if and only if  $g_2 \in \langle t \rangle$  (so we can apply (63.6)).

**(63.24) Lemma.** Let  $\text{ch}(H, \sqrt{t}; B_1(H))$  denote the set of virtual characters of  $H$  which belong to  $\{\text{cf}(H, \sqrt{t}; B_1(H))\}$ . Then

$$\begin{aligned} &\{1 + a_1\psi_1 + a_2\psi_2 + a_3\psi_3, a_2\psi_2 + a_3\psi_3 + a_4\psi_4, \\ &a_1\psi_1 + a_3\psi_3 + a_5\psi_5, a_1\psi_1 + a_2\psi_2 + a_6\psi_6\} \end{aligned}$$

form a  $Z$ -basis of  $\text{ch}(H, \sqrt{t}; B_1(H))$ .

*Proof.* Since  $\sqrt{x} \subset \sqrt{t}$  and  $H - \sqrt{t} = H_2$ , it is straightforward to verify that the virtual characters listed above belong to  $\text{ch}(H, \sqrt{t}; B_1(H))$ , using the preceding results. For example,  $1 + a_1\psi_1 + a_2\psi_2 + a_3\psi_3$  vanishes on  $H - \sqrt{x}^H \supset H_2$ , by (63.18v). Using (63.23) we obtain

$$\begin{aligned} (1 + a_1\psi_1 - a_2\psi_2 - a_3\psi_3)_{H_2} &= 2a_4\psi_4^*|_{H_2} = 2a_4\psi_4|_{H_2} \\ &= -2(a_2\psi_2 + a_3\psi_3)|_{H_2}. \end{aligned}$$

Thus  $a_2\psi_2 + a_3\psi_3 + a_4\psi_4 \in \text{ch}(H, \sqrt{t}; B_1(H))$ , and similarly for the others. These virtual characters span a  $\mathbb{Z}$ -submodule  $T$  of  $\text{ch}(H, \sqrt{t}; B_1(H))$  of rank 4. Since  $\{\psi_4, \psi_5, \psi_6\}$  are linearly independent on  $H_2$ , by (63.22), the map  $\xi \rightarrow \xi|_{H_2}$ , (for  $\xi$  a virtual character supported on  $B_1(H)$ ) has an image of  $\mathbb{Z}$ -rank  $\geq 3$ , and contains  $\text{ch}(H, \sqrt{t}; B_1(H))$  in its kernel. Since the number of irreducible characters in  $B_1(H)$  is 7, the rank of  $\text{ch}(H, \sqrt{t}; B_1(H))$  is  $\leq 4$ . It is easily checked that  $\text{ch}(H, \sqrt{t}; B_1(H))/T$  is torsion-free, and hence  $\text{ch}(H, \sqrt{t}; B_1(H)) = T$  because both sides have the same  $\mathbb{Z}$ -rank. This completes the proof.

We are ready to obtain some precise information about the irreducible characters belonging to the principal block  $B_1(G)$ .

**(63.25) Lemma.** *The characters  $\{1, \psi_1, \dots, \psi_6\}$  in  $B_1(H)$  are coherent (see (63.10)). In fact, there exist irreducible characters  $\{1, \zeta_1, \dots, \zeta_6\}$  in  $B_1(G)$ , and signs  $\varepsilon_i = \pm 1$ , such that*

$$\begin{aligned} (1 + a_1\psi_1 + a_2\psi_2 + a_3\psi_3)^G &= 1 + \varepsilon_1\zeta_1 + \varepsilon_2\zeta_2 + \varepsilon_3\zeta_3, \\ (a_2\psi_2 + a_3\psi_3 + a_4\psi_4)^G &= \varepsilon_2\zeta_2 + \varepsilon_3\zeta_3 + \varepsilon_4\zeta_4, \\ (a_1\psi_1 + a_3\psi_3 + a_5\psi_5)^G &= \varepsilon_1\zeta_1 + \varepsilon_3\zeta_3 + \varepsilon_5\zeta_5, \\ (a_1\psi_1 + a_2\psi_2 + a_6\psi_6)^G &= \varepsilon_1\zeta_1 + \varepsilon_2\zeta_2 + \varepsilon_6\zeta_6. \end{aligned}$$

*Proof.* This result follows easily from (63.24) and the Isometry Theorem 63.6. For example, let

$$\theta_1 = (1 + a_1\psi_1 + a_2\psi_2 + a_3\psi_3)^G.$$

Then  $(\theta_1, \theta_1) = 4$  by (63.6), and  $(\theta_1, 1_G) = 1$ . Therefore there exist irreducible characters  $\{\zeta_1, \zeta_2, \zeta_3\}$  in  $B_1(G)$  such that the first statement of the lemma holds, for suitably chosen  $\varepsilon_i = \pm 1$ . Using (63.6) again, we conclude that  $\theta_2 = (a_2\psi_2 + a_3\psi_3 + a_4\psi_4)^G$  has norm 3 and that  $(\theta_1, \theta_2) = 2$ . This yields another irreducible character  $\zeta_4 \in B_1(G)$  such that the first two relations hold. Continuing in this way, we construct characters in  $B_1(G)$  satisfying the assertions of the lemma. To verify that  $\{1, \psi_1, \dots, \psi_6\}$  are coherent, we use what has already been shown, and the explicit  $\mathbb{Z}$ -basis of  $\text{ch}(H, \sqrt{t}; B_1(H))$  given in (63.24). This completes the proof.

**(63.26) Corollary.** *We have*

$$\varepsilon_i\zeta_i|_{\sqrt{t}} = a_i\psi_i|_{\sqrt{t}} \text{ for } 1 \leq i \leq 6.$$

This follows from (63.11), since coherence has been established in (63.25). In the notation of (63.11), we have for each  $i$ ,  $1 \leq i \leq 6$ ,

$$a_i\psi_i \rightarrow \varepsilon'_i a_i \zeta_i \quad \text{with } \varepsilon'_i a_i = \varepsilon_i.$$

Thus

$$\zeta_i|_{\sqrt{t}} = \varepsilon'_i \psi_i|_{\sqrt{t}} \Rightarrow \varepsilon_i \zeta_i|_{\sqrt{t}} = \varepsilon_i \varepsilon'_i \psi_i|_{\sqrt{t}} = a_i \psi_i|_{\sqrt{t}},$$

as required.

*Proof of the Brauer-Suzuki Theorem 63.4.* Let  $\mathfrak{C}$  be the conjugacy class in  $G$  containing  $t$ , and let  $C = \sum_{x \in \mathfrak{C}} x$  be the corresponding class sum. We first prove that

$$(63.27) \quad \mathfrak{C}^2 \cap \sqrt{t} = \emptyset.$$

Otherwise, there exist  $u, v \in \mathfrak{C}$  with  $t \in \langle uv \rangle$ . It is easily checked that  $\langle u, v \rangle$  is a dihedral group, with  $\langle uv \rangle$  a cyclic subgroup of index 2. Since  $t \in \langle uv \rangle$ ,  $4 \mid \langle u, v \rangle$  and  $\langle u, v \rangle$  contains a Klein 4-group, which is impossible because the Sylow 2-subgroup of  $G$  is a quaternion group.

Let  $\theta = a_2 \psi_2 + a_3 \psi_3 + a_4 \psi_4$ . Then  $\theta^G \in \text{cf}(G, \sqrt{t^G}; B_1(G))$  and hence  $\theta^G(C^2) = 0$  by (63.27). Since  $\theta^G = \varepsilon_2 \zeta_2 + \varepsilon_3 \zeta_3 + \varepsilon_4 \zeta_4$  by (63.25), we obtain

$$\varepsilon_2 \zeta_2(C^2) + \varepsilon_3 \zeta_3(C^2) + \varepsilon_4 \zeta_4(C^2) = 0,$$

and hence, using the central characters  $\omega_i$  associated with the  $\zeta_i$ ,

$$\begin{aligned} 0 &= \varepsilon_2 \zeta_2(1) \zeta_2(C^2)/\zeta_2(1) + \varepsilon_3 \zeta_3(1) \zeta_3(C^2)/\zeta_3(1) + \varepsilon_4 \zeta_4(1) \zeta_4(C^2)/\zeta_4(1) \\ &= \varepsilon_2 \zeta_2(1) \zeta_2(C)^2/\zeta_2(1)^2 + \varepsilon_3 \zeta_3(1) \zeta_3(C)^2/\zeta_3(1)^2 + \varepsilon_4 \zeta_4(1) \zeta_4(C)^2/\zeta_4(1)^2 \\ &= |\mathfrak{C}|^2 (\varepsilon_2 \zeta_2(t)^2/\zeta_2(1) + \varepsilon_3 \zeta_3(t)^2/\zeta_3(1) + \varepsilon_4 \zeta_4(t)^2/\zeta_4(1)). \end{aligned}$$

Now  $1 + a_1 \psi_1 + a_2 \psi_2 + a_3 \psi_3 = (1 + \lambda_1 - \lambda_2 - \lambda_3)^H$  vanishes on  $t$  by (63.18iv), so

$$\begin{aligned} 2a_4 \psi_4(t) &= -2a_4 \psi_4^*(t) = -(1 + a_1 \psi_1 - a_2 \psi_2 - a_3 \psi_3)(t) \\ &= 2a_2 \psi_2(t) + 2a_3 \psi_3(t), \end{aligned}$$

using (63.23). Since  $\varepsilon_i \zeta_i|_{\sqrt{t}} = a_i \psi_i|_{\sqrt{t}}$  by (63.26), we obtain

$$(\varepsilon_2 \zeta_2 + \varepsilon_3 \zeta_3 - \varepsilon_4 \zeta_4)(t) = 0.$$

Moreover  $\varepsilon_2 \zeta_2(1) + \varepsilon_3 \zeta_3(1) + \varepsilon_4 \zeta_4(1) = 0$  since  $\theta^G$  vanishes off  $\sqrt{t^G}$ . Combining the preceding results, we have

$$\frac{\varepsilon_2 \zeta_2(t)^2}{\varepsilon_2 \zeta_2(1)} + \frac{\varepsilon_3 \zeta_3(t)^2}{\varepsilon_3 \zeta_3(1)} - \frac{(\varepsilon_2 \zeta_2(t) + \varepsilon_3 \zeta_3(t))^2}{\varepsilon_2 \zeta_2(1) + \varepsilon_3 \zeta_3(1)} = 0,$$

and hence

$$\varepsilon_2 \zeta_2(t) \varepsilon_3 \zeta_3(1) - \varepsilon_3 \zeta_3(1) \varepsilon_2 \zeta_2(t) = 0.$$

Therefore

$$\zeta_2(t)\zeta_3(1) - \zeta_3(1)\zeta_2(t) = 0.$$

Similarly we obtain

$$\zeta_3(t)\zeta_1(1) - \zeta_3(1)\zeta_1(t) = 0.$$

It follows that, for some constant  $d$ , we have

$$\zeta_i(t) = d\zeta_i(1), \quad i = 1, 2, 3.$$

Since

$$1 + \varepsilon_1\zeta_1 + \varepsilon_2\zeta_2 + \varepsilon_3\zeta_3 = (1 + a_1\psi_1 + a_2\psi_2 + a_3\psi_3)^G = (1 + \lambda_1 - \lambda_2 - \lambda_3)^G$$

vanishes outside  $(\sqrt{x})^G$ , and hence at 1 and  $t$ , we have

$$1 + \varepsilon_1\zeta_1(1) + \varepsilon_2\zeta_2(1) + \varepsilon_3\zeta_3(1) = 0$$

and

$$1 + d(\varepsilon_1\zeta_1(1) + \varepsilon_2\zeta_2(1) + \varepsilon_3\zeta_3(1)) = 0.$$

Therefore  $d = 1$ , so  $t \in \ker \zeta_1$ , and  $N = \ker \zeta_1$  is a normal subgroup of  $G$  containing  $t$ . Moreover,  $N \neq G$  since  $\zeta_1 \neq 1_G$ . This proves that  $G$  is not a counterexample, and we have reached a contradiction; finishing the proof.

### §63C. Glauberman's $Z^*$ -Theorem

The Brauer-Suzuki Theorem (§14E and §63B) states that a finite group  $G$ , whose Sylow 2-subgroups are quaternion or generalized quaternion groups, has a proper normal subgroup containing the unique involution in a given Sylow 2-subgroup. Glauberman [66] proved a far-reaching generalization of the Brauer-Suzuki Theorem, called the  $Z^*$ -theorem, which has played a crucial part in the proofs of a number of results related to the classification of the finite simple groups.

In this subsection we shall give a proof of the  $Z^*$ -theorem, based on the lectures of Dade [71]. The main step is another application of blocks of characters to produce proper normal subgroups.

Let  $G$  be a finite group. We let  $Z^*(G)$  denote the unique normal subgroup containing  $O_{2^*}(G)$  such that  $Z^*(G)/O_{2^*}(G) = Z(G/O_{2^*}(G))$ , the center of  $G/O_{2^*}(G)$ .

**(63.28) Glauberman's  $Z^*$ -Theorem.** *Let  $t$  be an involution in a finite group  $G$ , such that some Sylow 2-subgroup  $S$  of  $G$  contains  $t$  but no other conjugates of  $t$ ; in other words  $\mathfrak{C} \cap S = \{t\}$  where  $\mathfrak{C}$  is the conjugacy class containing  $t$ . Then  $t \in Z^*(G)$ .*

The Brauer-Suzuki Theorem is a special case of the  $Z^*$ -theorem, and is used in an essential way in the first part of the proof of the  $Z^*$ -theorem. The rest of the subsection is devoted to a proof of the  $Z^*$ -theorem. As in §63B, we fix a 2-modular system  $(K, R, k)$  such that  $\text{char } K = 0$  and  $K$  is sufficiently large relative to  $G$ .

To begin the proof, let  $G$  be a minimal counterexample to the  $Z^*$ -theorem, and let  $S$  be a Sylow 2-subgroup of  $G$ . If  $t$  is the given involution in  $S$ , then  $S$  contains another involution  $u \neq t$ . Otherwise,  $S$  contains a unique involution, and it is not difficult to prove that in this case  $S$  is either cyclic or generalized quaternion. The first possibility is ruled out by Burnside's Transfer Theorem 13.22, and the second by the Brauer-Suzuki Theorem (14.23 and 63.4).

*Step 1.* Let  $h, g \in G$ , and assume that  $\langle t^h, t^g \rangle$  is a 2-group. Then  $t^h = t^g$ . Moreover for arbitrary  $g \in G$ ,  $\langle t, u^g \rangle$  is dihedral of order  $4q$ , for  $q$  an odd number, where  $u$  is in involution in  $S$  different from  $t$ . The first statement holds since  $t^h \neq t^g$  implies that  $\langle t^h, t^g \rangle$  is contained in a conjugate of  $S$ , which contradicts the hypothesis of the  $Z^*$ -theorem. For the second statement, we have  $t \neq u$  in  $S$ , so  $t \neq {}_G u$  and  $u^g \neq t$ . Then  $\langle t, u^g \rangle$  is a dihedral group of order  $2^a q$ , for  $q$  odd. If  $a = 1$ , then  $t = {}_G u^g$ , contrary to assumption. If  $a > 2$ , then a Sylow 2-group of  $\langle t, u^g \rangle$  is dihedral of order  $2^a$ , and does not have  $t$  in the center. We then reach a contradiction, as in the proof of the first statement.

*Step 2.* We shall prove that there exists no proper normal subgroup  $N \trianglelefteq G$  such that  $t \in N$ . First of all, since  $G$  is a minimal counterexample, we have  $O_2(G) = 1$ . Now suppose that  $t \in N$  for some subgroup  $N \trianglelefteq G$ . Then  $O_2(N)$  is a characteristic subgroup of  $N$ , and  $O_2(N) \leq O_2(G) = 1$ . Therefore  $S \cap N$  is a Sylow 2-subgroup of  $N$ , and  $S \cap N$  contains  $t$  and no other  $N$ -conjugate of  $t$ . By the minimality of  $G$ , and the fact that  $O_2(N) = 1$ , we obtain  $t \in Z^*(N) = Z(N)$ . Then  $t$  belongs to a Sylow 2-group of  $Z(N)$ . If  $g \in G$ , then  $t$  and  $t^g$  commute since both are in  $Z(N)$ , so  $\langle t, t^g \rangle$  is a 2-group, and  $t = t^g$  by Step 1. Since  $g \in G$  is arbitrary, we obtain  $t \in Z(G)$ , which is impossible.

*Step 3.* Now let  $H$  be any proper subgroup of  $G$  containing  $t$ . We claim that  $t \in Z^*(H)$ , and begin by checking that  $H$  satisfies the hypotheses of the  $Z^*$ -theorem. Let  $T$  be a Sylow 2-group of  $H$  containing  $t$ . If  $t$  and  $t^h$  belong to  $T$ , for some  $h \in H$ , then  $\langle t, t^h \rangle$  is a 2-group, and  $t = t^h$  by Step 1. Thus we can apply the  $Z^*$ -theorem to  $H$ , in view of the minimality of  $G$ , and obtain  $t \in Z^*(H)$ .

*Step 4.* Let  $t, u$  be distinct involutions in  $S$ , and let  $\zeta$  be an irreducible character in the principal block  $B_1(G)$ . We shall prove that  $\zeta(t(u^g)) = \zeta(tu)$  for all  $g \in G$ .

First assume that  $\langle t, u^g \rangle$  is abelian. We may assume that  $S < G$ , so  $t \in Z^*(S)$  by Step 3. Then  $t \in Z(S)$ , and  $\langle t, u \rangle$  is abelian. Then  $t$  and  $t^g$  both belong to  $C_G(u^g)$ . By Sylow's Theorem, there exists  $h \in C_G(u^g)$  such that  $t$  and  $t^{gh}$  belong to the same Sylow 2-subgroup of  $C_G(u^g)$ . Then  $\langle t, t^{gh} \rangle$  is a 2-group, and  $t = t^{gh}$  by Step 1. Moreover,  $tu^g = t^{gh}u^g = (tu)^{gh}$  since  $h \in C_G(u^g)$ . It follows that  $\zeta(tu^g) = \zeta(tu)$  for all  $g \in G$  and  $\zeta \in \text{Irr } G$ .

A delicate situation occurs when  $\langle t, u^g \rangle$  is not abelian. In this case,  $\langle t, u^g \rangle$  is dihedral of order  $4q$ , with  $q$  odd, by Step 1. Moreover  $\langle tu^g \rangle$  is cyclic of index 2 in  $\langle t, u^g \rangle$ , and hence contains an involution  $v \in Z\langle t, u^g \rangle$ .

We prove next that  $H = C_G(v) < G$ . Otherwise,  $v \in Z(G)$ , and it is easily checked that  $G/\langle v \rangle$  satisfies the hypotheses of the  $Z^*$ -theorem. Then  $t\langle v \rangle \in Z^*(G/\langle v \rangle)$  by minimality of  $G$ . If  $N \trianglelefteq G$  is the inverse image of  $O_2(G/\langle v \rangle)$ , then  $N/\langle v \rangle$  has odd order and  $N = N_1\langle v \rangle$  for  $N_1 = O_2(N)$  (by a special case of the Schur-Zassenhaus Theorem 8.35). Then  $N_1 = 1$  since  $O_2(G) = 1$ , and hence  $t\langle v \rangle \in Z(G/\langle v \rangle)$ . This means that  $\langle t, v \rangle \trianglelefteq G$ , and hence  $\langle t, v \rangle = G$  by Step 2. Thus  $t \in Z(G)$  and we have reached a contradiction.

Since  $H = C_G(v) < G$  and  $t \in H$ , we have  $t \in Z^*(H)$  by Step 3. We also have  $tu^g \in H$  and  $u^g \in H$ . The image of  $\langle t, u^g \rangle$  in  $H/O_2(H)$  is dihedral, and  $tO_2(H) \in Z(H/O_2(H))$ . Then  $(tu^g)^2 \in O_2(H)$ , and the image of  $\langle t, u^g \rangle$  in  $H/O_2(H)$  is a Klein 4-group.

Now let  $\zeta \in B_1(G)$ . We have, for  $x \in O_2(H)$ ,

$$\begin{aligned}\zeta(vx) &= \sum_{\zeta_j \in B_1(H)} a_j \zeta_j(vx) \\ &= \sum a_j \zeta_j(v) = \zeta(v),\end{aligned}$$

using (63.1) and Brauer's Second and Third Main Theorems 59.14 and 61.16.

Now  $tu^g \equiv v \pmod{O_2(H)}$ , since  $(tu^g)^2 \in O_2(H)$  and  $\langle tu^g \rangle = \langle v \rangle \langle (tu^g)^2 \rangle$ . Then  $\zeta(tu^g) = \zeta(v)$  for  $\zeta \in B_1(G)$ . The Sylow 2-subgroup of  $\langle t, u^g \rangle$  containing  $t$  is just  $\langle t, v \rangle$ , so  $tv$  is an involution commuting with  $t$ , and  $tv = (u^g)^z$  for some  $z \in \langle t, u^g \rangle$ . Then  $\langle t, u^{gz} \rangle$  is abelian, and  $v = t^2v = tu^{gz}$  so

$$\zeta(v) = \zeta(tu^{gz}) = \zeta(tu)$$

by the proof of the first part of this step. Combining our results, we obtain  $\zeta(tu^g) = \zeta(v) = \zeta(tu)$ , as required.

*Step 5.* Let  $t, u$  be distinct involutions in  $S$ , and let  $\mathfrak{C}_t$ ,  $\mathfrak{C}_u$ , and  $C_t, C_u$  be the conjugacy classes and class sums defined by them. For all  $\zeta \in B_1(G)$  we have

$$\zeta(C_t C_u)/\zeta(1) = (\zeta(C_t)/\zeta(1)(\zeta(C_u)/\zeta(1)))$$

so

$$\zeta(1)\zeta(C_t C_u) = \zeta(C_t)\zeta(C_u).$$

Now

$$C_t C_u = \sum t^g u^h = \sum (tu^{hg^{-1}})^g$$

so, using Step 4, we obtain

$$\zeta(1)|\mathfrak{C}_t||\mathfrak{C}_u|\zeta(tu) = |\mathfrak{C}_t||\mathfrak{C}_u|\zeta(t)\zeta(u).$$

On the other hand,  $t \in Z(S)$  by the hypothesis of the  $Z^*$ -theorem, so  $tu$  is an involution in  $S$  different from  $t$ , and we have

$$\zeta(1)\zeta(u) = \zeta(t)\zeta(tu)$$

by the argument used above. Then

$$\zeta(t)^2 \zeta(u) = \zeta(1)\zeta(t)\zeta(tu) = \zeta(1)^2 \zeta(u).$$

If  $\zeta(u) \neq 0$ , then  $\zeta(t) = \pm \zeta(1)$  and  $t \cdot \ker \zeta \in Z(G/\ker \zeta)$ . Let  $N$  be the intersection of the kernels of characters  $\zeta \in B_1(G)$  such that  $\zeta(u) \neq 0$  for some involution  $u$  in  $S - \{t\}$ . Then  $tN \in Z(G/N)$ .

In order to prove that  $Z^*$ -theorem, it is sufficient to prove that  $N$  contains no involutions, since that implies that  $N = 1$  and  $t \in Z(G)$ , in view of the fact that  $O_{2'}(G) = 1$ . In fact, it suffices to show that  $N$  contains no involutions belonging to  $S$ . First assume that  $N$  contains an involution  $u \neq t$ , with  $u \in S$ . By the  $p$ -Section Orthogonality Theorem 60.2, we obtain

$$\begin{aligned} 0 &= \sum_{\zeta \in B_1(G)} \zeta(u)\zeta(1) = \sum_{\zeta \in B_1(G), \zeta(u) \neq 0} \zeta(u)\zeta(1) \\ &= \sum_{\zeta \in B_1(G), \zeta(u) \neq 0} \zeta(1)^2 \end{aligned}$$

by the definition of  $N$ . This is a contradiction, since the trivial character  $\zeta^1 \in B_1(G)$  and  $\zeta^1(u) \neq 0$ .

Now suppose  $t \in N$ . Then  $N = G$  by Step 2, and hence  $N$  contains an involution  $u \in S$  such that  $u \neq t$ , since  $S$  has that property. But we have just shown that this is impossible. Therefore  $N$  contains no involutions, so  $N \leq O_{2'}(G) = 1$ , and therefore  $t \in Z(G)$ , completing the proof.

# The Representation Theory of Finite Groups of Lie Type

The finite groups of Lie type include the classical matrix groups over finite fields: the general linear groups  $GL_n(\mathbb{F}_q)$ , the unimodular groups  $SL_n(\mathbb{F}_q)$ , the orthogonal groups  $SO_n(\mathbb{F}_q)$ , and the symplectic groups  $Sp_{2n}(\mathbb{F}_q)$ . Their structure was worked out by Dickson [01]. His work inspired a series of books and articles containing extensions, improvements, and new proofs, by Artin, Dieudonné, and others. These culminated in Chevalley's paper [55], which provided a uniform construction, and general methods for analyzing the structure, of families of groups associated with each type of semisimple Lie algebra over  $\mathbb{C}$ . The Chevalley groups include the classical groups, and analogues of the exceptional simple Lie groups. As a result of the classification of finite simple groups, it is now known that the simple groups of Lie type (the Chevalley groups and twisted types of Chevalley groups), together with the alternating groups  $A_n$ ,  $n \geq 5$ , and 26 sporadic groups, comprise all non-abelian finite simple groups. Thus the finite groups of Lie type occupy a special place in finite group theory.

The finite dimensional representations of the semisimple Lie algebras and Lie groups were determined by H. Weyl [25], [26]. His classification was based on the theory of weights, and showed the importance for representation theory of certain finite groups generated by reflections in the dual space of a Cartan subalgebra of the given Lie algebra (now called Weyl groups).

The representation theory of finite groups of Lie type was slow to yield, however, but is now in a state of rapid development. A major advance was achieved by Deligne-Lusztig [76], who proved, using powerful new methods, a series of conjectures of Macdonald. These were based on the construction of the characters of  $GL_n(\mathbb{F}_q)$  by Green [55],  $Sp_4(\mathbb{F}_q)$  by Srinivasan [68], and of  $G_2(\mathbb{F}_q)$  by Chang-Ree [74], together with Harish-Chandra's approach to the representation theory of semisimple Lie groups, called the philosophy of cusp forms. Introductions to the Deligne-Lusztig theory have been given by Srinivasan [79] and Carter [85].

According to Harish-Chandra's principles, the representation theory, over the field  $\mathbb{C}$ , of the finite groups of Lie type involves the solution of two main problems: the construction of the cuspidal modules, and the decomposition, using the theory of Hecke algebras (§11), of induced modules from proper

parabolic subgroups arising from cuspidal modules of their Levi subgroups.

This chapter contains an account of Harish-Chandra's organization of the representation theory, and several applications of Hecke algebras to the solution of the decomposition problem.

The first two sections contain a detailed introduction to root systems, finite groups generated by reflections, Coxeter groups, and finite groups with  $BN$ -pairs. In particular, the deep connections between finite groups with  $BN$ -pairs and their Weyl groups are established. While this material is available in several standard references, we have included it for the benefit of readers coming to the subject for the first time, without previous knowledge of Chevalley groups.

The next section contains some general principles for analyzing representations of finite groups on the rational homology of complexes arising from posets with finite group actions. These are applied to the combinatorial building and the Coxeter poset of a finite group with a  $BN$ -pair,  $G$ , and its Weyl group  $W$ , to obtain a homological interpretation of the sign representation of  $W$ , and the Steinberg representation of  $G$ , using only the background from the previous two sections.

In §§67 and 68, the permutation representation  $(1_B)^G$  is decomposed, using its Hecke algebra  $\mathcal{H}$ . The connection between the representations of  $\mathcal{H}$  and the representations of  $W$  is used to obtain a parametrization of the irreducible characters in  $(1_B)^G$  by characters of  $W$ , and a method for proving that the degrees of these characters are given by polynomials with rational coefficients, called generic degrees.

The next two sections are devoted to the Levi decompositions of parabolic subgroups of finite groups with split  $BN$ -pairs satisfying the commutator relations, and their application to Harish-Chandra's philosophy of cusp forms.

A duality operation in the ring of virtual characters  $\text{ch } G$  is discussed in §71, and used in §72 to prove that the set of projective characters  $\text{Pch } G$  forms a principal ideal in  $\text{ch } G$ , generated by the Steinberg character. The last section also contains a classification of the simple  $kG$ -modules, in the natural characteristic, based on the representation theory of modular Hecke algebras (which are not semisimple algebras).

## §64. ROOT SYSTEMS AND FINITE REFLECTION GROUPS

### §64A. Finite Groups Generated by Reflections. Root Systems

Throughout this section, let  $V$  denote a f.d. vector space over the real field  $\mathbb{R}$ , and assume  $V$  is equipped with a symmetric, positive definite bilinear form taking values  $(\xi, \eta) \in \mathbb{R}$ , for  $\xi, \eta \in V$ . We call  $V$  a *real euclidean space*, and refer to the bilinear form  $(\xi, \eta)$  as an *inner product* on  $V$ . The form is of course nondegenerate. The *group of orthogonal transformations* on  $V$  is defined by

$$O(V) = \{s \in \text{End}_{\mathbb{R}} V : (s\xi, s\eta) = (\xi, \eta) \quad \text{for all } \xi, \eta \in V\}.$$

For a subspace  $U$  of  $V$ , we set

$$U^\perp = \{\xi \in V : (\xi, \eta) = 0 \text{ for all } \eta \in U\},$$

and call  $U^\perp$  the *orthogonal complement* of  $U$ .

For a set of elements  $\{s_i\}$  of  $O(V)$ , let  $\langle s_1, s_2, \dots \rangle$  denote the subgroup of  $O(V)$  that they generate. We shall also use the notation  $\langle \alpha, \beta, \dots \rangle$  for the subspace of  $V$  generated by the vectors  $\alpha, \beta, \dots$  of  $V$ .

**(64.1) Definition.** A *reflection* is a linear map  $s: V \rightarrow V$  such that  $s \in O(V)$ ,  $s \neq 1$ , and  $s$  fixes every vector in some hyperplane in  $V$ .

**(64.2) Proposition.** (i) Let  $H$  be a hyperplane in  $V$ . There exists a unique reflection  $s \in O(V)$  that leaves fixed the elements of  $H$ . Then  $s^2 = 1$ , and  $s$  is specified by the formula

$$s\xi = \xi - \frac{2(\xi, \alpha)}{(\alpha, \alpha)}\alpha \quad \text{for all } \xi \in V,$$

where  $\alpha$  is an arbitrary nonzero vector in  $H^\perp$ . Note that  $s\alpha = -\alpha$ .

(ii) Let  $\alpha$  be a given nonzero vector in  $V$ , and let  $s_\alpha$  be the reflection in the hyperplane  $H = \langle \alpha \rangle^\perp$ . Then for all  $g \in O(V)$ ,

$$gs_\alpha g^{-1} = s_{g\alpha}.$$

*Proof.* (i) Let  $H^\perp = \langle \alpha \rangle$ , so  $H = \langle \alpha \rangle^\perp$ , and let  $s$  be any reflection fixing each element of  $H$ . Then  $s\alpha \in H^\perp$  since  $s \in O(V)$ , and it follows that  $s\alpha = -\alpha$ , using the fact that  $s \neq 1$ . From the equality

$$V = H \oplus \langle \alpha \rangle,$$

we have  $s^2 = 1$ . Now let  $\xi \in V$  be expressed as

$$\xi = \eta + t\alpha, \quad \eta \in H, \quad t \in \mathbb{R}.$$

Then  $t = (\xi, \alpha)/(\alpha, \alpha)$ , and

$$s\xi = \eta - t\alpha = \xi - 2t\alpha.$$

This proves the formula for  $s$ , and establishes the uniqueness of  $s$ . It is also clear that the formula for  $s$  does indeed define a reflection fixing the elements of the hyperplane  $\langle \alpha \rangle^\perp$ .

(ii) Clearly  $gs_\alpha g^{-1} \in O(V)$  has order 2, and fixes the elements of the hyperplane  $\langle g\alpha \rangle^\perp$ . Therefore  $gs_\alpha g^{-1} = s_{g\alpha}$  by part (i).

**(64.3) Definition.** A group generated by reflections (abbreviated as g.g.r.) is a subgroup of  $O(V)$  generated by reflections.

We shall be mainly interested in finite g.g.r.'s. Their structure and classification will be obtained by using combinatorial properties of finite sets of vectors in  $V$ , called root systems, which are permuted by the elements of the g.g.r. (These root systems first arose in the classification of semisimple Lie algebras over  $\mathbb{C}$ ; see Bourbaki [68] for a historical account.) Our approach follows, to some extent, Steinberg [67] and Chevalley [56–58]. From the point of view of abstract group theory, we are studying certain finite groups generated by involutions.\*

**(64.4) Definitions.** A root system  $\Delta$  in  $V$  is a finite set of vectors  $\{\alpha, \beta, \dots\}$  satisfying the conditions (i)–(iii) below.

(i)  $0 \notin \Delta$ , and the vectors in  $\Delta$  span  $V$ .

(ii) (Reduced condition) If  $\alpha \in \Delta$ , then  $-\alpha \in \Delta$ ; further, if  $c \in \mathbb{R}$  is such that  $c\alpha \in \Delta$ , then  $c = \pm 1$ .

(iii) For each  $\alpha \in \Delta$ , we have  $s_\alpha \Delta = \Delta$ , where  $s_\alpha$  is the reflection fixing the hyperplane  $\langle \alpha \rangle^\perp$ .

A crystallographic root system is a root system  $\Delta$  satisfying the additional condition:

(iv) (Crystallographic condition) For all pairs of roots  $\alpha, \beta \in \Delta$ , we have  $2(\alpha, \beta)/(\beta, \beta) \in \mathbb{Z}$ .

The g.g.r.  $W = W(\Delta)$  generated by the reflections  $\{s_\alpha : \alpha \in \Delta\}$  is called the g.g.r. associated with the root system  $\Delta$ .

**Remarks.** (i) It can be proved (see (64.11)) that a crystallographic root system can be embedded in a full  $\mathbb{Z}$ -lattice in  $V$ . The g.g.r.'s associated with crystallographic root systems are sometimes called *Weyl groups*, and can be identified with the Weyl groups of semisimple Lie algebras over  $\mathbb{C}$  with respect to Cartan subalgebras (see Humphreys [72]).

(ii) Let  $\Delta$  be a root system in  $V$ . Since  $W$  permutes the elements of  $\Delta$ , and  $\Delta$  contains a basis of  $V$ , it follows that the g.g.r.  $W(\Delta)$  is a finite group.

Conversely, let  $W$  be a finite g.g.r., and let  $\Delta$  be the set of unit vectors orthogonal to the hyperplanes fixed by reflections in  $W$ . By (64.2ii), it follows that  $W$  permutes the elements of  $\Delta$ . Letting  $\langle \Delta \rangle$  denote the subspace of  $V$  generated by  $\Delta$ , we have  $V = \langle \Delta \rangle \oplus \langle \Delta \rangle^\perp$ . The elements of  $W$  leave the subspaces  $\langle \Delta \rangle$  and  $\langle \Delta \rangle^\perp$  invariant, and act trivially on  $\langle \Delta \rangle^\perp$ ; hence  $W$  acts faithfully on  $\langle \Delta \rangle$ . It is then clear that  $\Delta$  is a root system in  $\langle \Delta \rangle$  whose Weyl group is isomorphic to  $W$ ; thus every finite g.g.r. is associated with a root system.

**Examples.** We shall consider some examples of root systems in vector spaces  $V$

\*Recall that an involution in a group is an element of order 2.

of dimensions 1 or 2, with the standard euclidean inner product. These examples include cases where not all the roots have the same length.

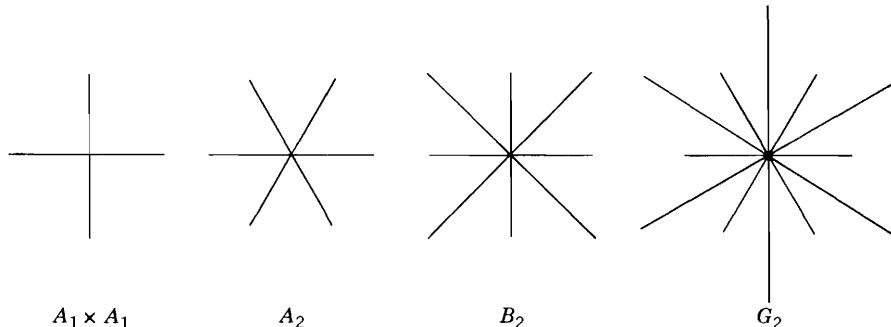
If  $\dim V = 1$ , the only possibility for a root system is a pair of opposing vectors  $\{\pm \alpha\}$ , associated with the g.g.r.  $\langle s_\alpha \rangle$  of order 2.

Root systems in the plane are associated with dihedral groups. An arbitrary finite dihedral group  $D_m$  of order  $2m$  is isomorphic to the symmetry group of a regular  $m$ -sided polygon in the plane. It is generated by a rotation  $r$  of order  $m$  and a reflection  $s$ , so that

$$D_m = \langle r, s : r^m = 1, s^2 = 1, srs^{-1} = r^{-1} \rangle.$$

There are exactly  $m$  reflections in  $D_m$ , and  $D_m$  is generated by the reflections it contains. The unit vectors orthogonal to the hyperplanes fixed by the reflections in  $D_m$  form a root system in the plane whose g.g.r. is  $D_m$ , by the preceding remark.

The two-dimensional crystallographic root systems are given as follows. The



notations  $A_1 \times A_1$ ,  $A_2$ , etc. are taken from Cartan's classification of crystallographic root systems. The g.g.r.'s associated with these root systems are dihedral, of orders 4, 6, 8, and 12, respectively. This observation, together with the preceding paragraph, shows that the dihedral groups of orders 8 and 12 are each associated with two root systems, one of which is crystallographic, and one of which is not. The point is that to satisfy the crystallographic condition, the lengths of the roots cannot be chosen arbitrarily.

Here is a sketch of the proof that the root systems of type  $A_1 \times A_1$ ,  $A_2$ ,  $B_2$ , and  $G_2$  are the only crystallographic root systems in two dimensions. Let  $\Delta$  be a crystallographic root system, and let  $\alpha, \beta$  be linearly independent roots in  $\Delta$ . If  $\theta$  denotes the angle between  $\alpha$  and  $\beta$ , then

$$\frac{4(\alpha, \beta)(\beta, \alpha)}{(\alpha, \alpha)(\beta, \beta)} = 4 \cos^2 \theta < 4.$$

The crystallographic condition then implies that

$$2(\alpha, \beta)/(\beta, \beta) \in \{0, \pm 1, \pm 2, \pm 3\},$$

from which one readily obtains the above classification.

In case  $V$  has dimension  $n$ , the symmetric groups  $S_{n+1}$  and the hyperoctahedral groups  $H_n$  are g.g.r.'s associated with crystallographic root systems in  $V$  (see Exercises 64.1, 64.2).

Returning to the general discussion, we shall begin to study an arbitrary finite g.g.r.  $W$  associated with a root system  $\Delta$  in  $V$ , in terms of order relations on  $V$  and  $\Delta$ . Every nonzero vector  $\xi \in V$  defines a partition of  $V$ :

$$V = V_-(\xi) \dot{\cup} H_\xi \dot{\cup} V_+(\xi),$$

where  $H_\xi$  is the hyperplane  $\langle \xi \rangle^\perp$ , and

$$V_+(\xi) = \{ \lambda \in V : (\lambda, \xi) > 0 \}, \quad V_-(\xi) = \{ \lambda \in V : (\lambda, \xi) < 0 \}.$$

Since  $\Delta$  is a finite set, there exist vectors  $\xi$  such that  $(\xi, \alpha) \neq 0$  for all  $\alpha \in \Delta$ . Let us fix such an element  $\xi$ . We then have a partition of  $\Delta$  into positive roots  $\Delta_+$  and negative roots  $\Delta_-$ , defined by

$$\Delta_+ = \Delta \cap V_+(\xi), \quad \Delta_- = \Delta \cap V_-(\xi).$$

We have:

**(64.5) Lemma.** *Let  $\xi \in V$  be such that  $(\xi, \alpha) \neq 0$  for each  $\alpha \in \Delta$ . Suppose that  $\sum c_\alpha \alpha = 0$  for some set of positive roots  $\alpha \in \Delta_+$ , with nonnegative real coefficients  $\{c_\alpha\}$ . Then each  $c_\alpha = 0$ .*

*Proof.* From  $\sum c_\alpha \alpha = 0$ , we obtain  $\sum c_\alpha (\alpha, \xi) = 0$ . Since  $(\alpha, \xi) > 0$  for each  $\alpha$ , it follows that each  $c_\alpha = 0$ .

Given a finite set of vectors  $\{\alpha_i\}$ , by their *positive span* we mean the collection of all vectors of the form  $\sum c_i \alpha_i$  with coefficients  $c_i \geq 0$ , and not all  $c_i = 0$ . For example,  $\Delta_+$  is precisely the set of roots in  $\Delta$  that belong to the positive span of  $\Delta_+$ . We now establish:

**(64.6) Theorem.** *Let  $\Pi$  be a subset of  $\Delta_+$  such that  $\Delta_+$  is the set of all roots contained in the positive span of  $\Pi$ , and let  $\Pi$  be minimal with this property. Then the following statements hold:*

- (i)  *$\Pi$  is a basis of  $V$ .*
- (ii) *Every root in  $\Delta$  can be expressed in the form  $\pm(\sum a_i \alpha_i)$ , with  $\alpha_i \in \Pi$ , and nonnegative real coefficients  $\{a_i\}$ .*
- (iii) *For all pairs of distinct roots  $\alpha_i, \alpha_j$  in  $\Pi$  we have*

$$(\alpha_i, \alpha_j) \leq 0.$$

*Proof.* We begin with the proof of (ii). As we observed in the remark preceding

the statement,  $\Delta_+$  is the positive span of  $\Delta_+$ , so that minimal subsets  $\Pi \subseteq \Delta_+$  having this property do exist. For such a subset  $\Pi$ , (ii) clearly holds, by the definition of positive span, since  $\Delta = \Delta_+ \cup \Delta_-$ .

We next prove (iii), and will use (iii) to prove that  $\Pi$  is a linearly independent set. Let

$$\Pi = \{\alpha_i, \dots, \alpha_n\}, \quad a_{ij} = 2(\alpha_i, \alpha_j)/(\alpha_j, \alpha_j), \quad s_i = s_{\alpha_i},$$

for  $\alpha_i \in \Pi$ . Then, for all  $i$  and  $j$ ,

$$s_i(\alpha_j) = \alpha_j - a_{ji}\alpha_i,$$

and either  $s_i\alpha_j \in \Delta_+$  or  $-s_i\alpha_j \in \Delta_+$ . Thus one of  $\alpha_j - a_{ji}\alpha_i$ ,  $-\alpha_j + a_{ji}\alpha_i$  lies in  $\Delta_+$ . Then (iii) will follow from:

**(64.7) Lemma.** *For all pairs of distinct roots  $\alpha_i, \alpha_j \in \Pi$ , it is impossible to have  $c_i\alpha_i - c_j\alpha_j \in \Delta_+$ , with both  $c_i, c_j > 0$ .*

*Proof of Lemma.* Suppose, to the contrary, that  $c_i\alpha_i - c_j\alpha_j \in \Delta_+$  with  $c_i, c_j > 0$ . Then

$$c_i\alpha_i - c_j\alpha_j = \sum_k a_k \alpha_k,$$

where  $a_k \geq 0$  for each  $k$ . If  $c_i \leq a_i$ , then

$$\sum_{k \neq i,j} a_k \alpha_k + (a_i - c_i)\alpha_i + (a_j + c_j)\alpha_j = 0,$$

with all coefficients nonnegative, and  $a_j + c_j > 0$ , contrary to Lemma 64.5. On the other hand, if  $c_i > a_i$ , then

$$(c_i - a_i)\alpha_i = c_j\alpha_j + \sum_{k \neq i} a_k \alpha_k,$$

which allows us to express  $\alpha_i$  as a positive linear combination of other roots in  $\Pi$ , contrary to the minimality of  $\Pi$ . This completes the proof of Lemma 64.7, and part (iii) of the theorem.

In order to prove (i), it is sufficient to show that  $\Pi$  is a linearly independent set, since we already know that  $\Delta_+$  spans  $V$ , and hence so does  $\Pi$ . Using part (iii), it is enough to prove:

**(64.8) Lemma.** *Let  $\{\alpha_1, \dots, \alpha_m\}$  be a set of positive roots such that  $(\alpha_i, \alpha_j) \leq 0$  for all  $i \neq j$ . Then  $\{\alpha_1, \dots, \alpha_m\}$  is a linearly independent set.*

*Proof.* Suppose, to the contrary, that  $\{\alpha_1, \dots, \alpha_m\}$  are linearly dependent. By

Lemma 64.5, a relation of linear dependence must have the form

$$\sum_{i \in I} a_i \alpha_i = \sum_{j \in J} b_j \alpha_j \neq 0, \quad \text{where all } a_i, b_j > 0,$$

for two nonempty disjoint subsets  $I, J$  of the index set  $\{1, \dots, m\}$ . Putting  $\rho = \sum a_i \alpha_i = \sum b_j \alpha_j$ , we have  $(\rho, \rho) > 0$  by the positivity of the inner product, while on the other hand

$$(\rho, \rho) = \sum a_i b_j (\alpha_i, \alpha_j) \leq 0.$$

This contradiction proves the lemma, and completes the proof of the theorem.

**(64.9) Definition.** A set of roots  $\Pi$  satisfying conditions (i)–(iii) of Theorem 64.6 is called a *fundamental system* (or a *simple system*), and the roots  $\alpha_i \in \Pi$  are called *fundamental roots* (or *simple roots*). The reflections  $\{s_{\alpha_i} : \alpha_i \in \Pi\}$  are called *fundamental reflections* (relative to  $\Pi$ ).

**(64.10) Corollary.** Every positive set of roots  $\Delta_+$ , as defined above, contains a unique fundamental system  $\Pi$ . Conversely, each fundamental system  $\Pi$  is contained in a unique positive set of roots  $\Delta_+ = V_+(\xi) \cap \Delta$ , for some nonzero vector  $\xi$ .

*Proof.* For the first statement, it follows from the theorem that  $\Pi$  is characterized as the set of those elements of  $\Delta_+$  that cannot be expressed as positive linear combinations of two or more elements of  $\Delta_+$ . Conversely, if  $\Pi$  is a fundamental system, then  $\Pi$  is a basis of  $V$ , and since  $V$  can be identified with its dual space using the inner product, there certainly exist nonzero vectors  $\xi$  in  $V$  such that  $\Pi \subset V_+(\xi)$ . For any such  $\xi$ , it follows from the definition of  $\Pi$  that  $\Delta_+ = V_+(\xi) \cap \Delta$  is the set of roots which are positive linear combinations of the elements of  $\Pi$ . Thus  $\Delta_+$  is independent of the choice of  $\xi$ , and is unique.

**(64.11) Remark.** Let  $\Delta$  be a crystallographic root system, and let  $\Pi$  be a fundamental system. An analysis of the proof of Theorem 64.6 shows that all the roots in  $\Delta$  are  $\mathbb{Z}$ -linear combinations of the fundamental roots, and hence  $\Delta$  spans a  $\mathbb{Z}$ -lattice on which the Weyl group acts. (This fact explains the term “crystallographic root system”.)

**(64.12) Definition.** Let  $\Pi$  be a fundamental system in an arbitrary root system  $\Delta$ , and let  $\Delta_+$  be the positive system determined by  $\Pi$  (see (64.10)). Let  $\alpha \in \Delta_+$ , and define the *height* of  $\alpha$  (notation:  $\text{ht } \alpha$ ), by

$$\text{ht } \alpha = \sum a_i \quad \text{if} \quad \alpha = \sum a_i \alpha_i, \quad \alpha_i \in \Pi.$$

Note that since all the coefficients  $a_i$  are nonnegative,  $\text{ht } \alpha > 0$  for each  $\alpha \in \Delta_+$ .

The next result is the key to the structure of the Weyl group  $W$  of the root system  $\Delta$ .

**(64.13) Main Lemma.** *Let  $\Pi$  be a fundamental system and  $\Delta_+$  the positive system containing  $\Pi$ . Let  $\alpha \in \Pi$ , and let  $\beta \in \Delta_+$  be a positive root such that  $\beta \neq \alpha$ . Then  $s_\alpha \beta \in \Delta_+$ . Thus each fundamental reflection  $s_\alpha$ ,  $\alpha \in \Pi$ , permutes the positive roots different from  $\alpha$ .*

*Proof.* Let  $\Pi = \{\alpha, \alpha_2, \dots, \alpha_n\}$ ; then  $\beta \in \Delta_+$  can be expressed as  $\beta = c_1\alpha + \sum_{j=2}^n c_j\alpha_j$ , with each  $c_j \geq 0$ ,  $1 \leq j \leq n$ . Since  $\beta \neq \alpha$ , the reduced property (64.4ii) of  $\Delta$  implies that at least one of  $c_2, \dots, c_n$  is nonzero, say  $c_2$ . Then  $s_\alpha \beta = \beta + c\alpha$  for some  $c \in \mathbb{R}$ , so the coefficient of the fundamental root  $\alpha_2$  in  $s_\alpha \beta$  is  $c_2$ . Since  $c_2 > 0$ , it follows from the definition of a fundamental system that  $s_\alpha \beta$  must lie in  $\Delta_+$ , as required.

**(64.14) Theorem.** *Let  $\Pi = \{\alpha_1, \dots, \alpha_n\}$  be a fundamental system in  $\Delta$ . Then the g.g.r.  $W = W(\Delta)$  is generated by the fundamental reflections  $\{s_{\alpha_i} : \alpha_i \in \Pi\}$ . Moreover, every root  $\alpha$  is in the  $W$ -orbit of some fundamental root.*

*Proof.* Let  $W_0$  be the subgroup of  $W$  generated by the fundamental reflections  $\{s_{\alpha_i} : \alpha_i \in \Pi\}$ , and let  $\Delta_+$  be the positive system containing  $\Pi$ , as in (64.10).

*Step 1.* Let  $\alpha \in \Delta_+$ , and suppose that  $\alpha \notin \Pi$ . We assert that  $(\alpha, \alpha_i) > 0$  for some  $\alpha_i \in \Pi$ . Assume, to the contrary, that  $(\alpha, \alpha_i) \leq 0$  for all  $\alpha_i \in \Pi$ . Then  $\Pi \cup \{\alpha\}$  is a linearly independent set by (64.8), contradicting the fact that  $\Pi$  is a basis of  $V$ .

*Step 2.* We assert that every positive root  $\alpha \in \Delta_+$  of minimal height is in  $\Pi$ . For if  $\alpha \notin \Pi$ , then  $(\alpha, \alpha_i) > 0$  for some  $\alpha_i \in \Pi$ , by Step 1. Then  $s_{\alpha_i}\alpha \in \Delta_+$  by the Main Lemma 64.13, and  $s_{\alpha_i}\alpha = \alpha - [2(\alpha, \alpha_i)/(\alpha_i, \alpha_i)]\alpha_i$ . Since  $(\alpha, \alpha_i) > 0$ , it follows that  $ht s_{\alpha_i}\alpha < ht \alpha$ , which is impossible. This completes the proof of this step.

*Step 3.* We now prove that every positive root  $\alpha$  is in the  $W_0$ -orbit of some element of  $\Pi$ , by using induction on  $ht \alpha$ . The result is true for positive roots of minimal height by Step 2. Now let  $\alpha \in \Delta_+$ ,  $\alpha \notin \Pi$ . By the proof of Step 2, there exists  $\alpha_i \in \Pi$  such that  $s_{\alpha_i}\alpha \in \Delta_+$  and  $ht s_{\alpha_i}\alpha < ht \alpha$ , so we can apply induction to conclude that  $w \cdot s_{\alpha_i}\alpha \in \Pi$  for some  $w \in W_0$ , completing the proof of the assertion.

*Step 4.* We now prove that every root is in the  $W_0$ -orbit of some element of  $\Pi$ . By Step 3, it is sufficient to consider a root  $\beta \in \Delta_-$ . Then  $-\beta \in \Delta_+$ , and  $-\beta = w\alpha_i$  for some  $w \in W_0$  and some  $\alpha_i \in \Pi$ , by Step 3. We then have  $\beta = ws_{\alpha_i}\alpha_i$ , and  $ws_{\alpha_i}\alpha_i \in W_0$ , as required.

At this point we have proved the second statement of the theorem. To prove the first, namely that  $W_0 = W$ , it is enough to show that  $s_\alpha \in W_0$  for each root  $\alpha$ . By Steps 1–4, there exist  $\alpha_i \in \Pi$  and  $w \in W_0$  such that  $\alpha = w \cdot \alpha_i$ . Then  $s_\alpha = ws_{\alpha_i}w^{-1}$  by (64.2), and  $ws_{\alpha_i}w^{-1} \in W_0$ , completing the proof of the theorem.

Our next objective, to be completed in §64B, is to obtain a presentation of an arbitrary finite g.g.r.  $W$ , using a set of fundamental reflections  $\{s_{\alpha_i} \in \Pi\}$  as

generators (see Definition 1.23). The determination of the relations satisfied by the reflections  $\{s_{\alpha_i} : \alpha_i \in \Pi\}$  is based on the following analysis of the lengths of words in  $W$  in terms of properties of  $\Delta$ . Note, in particular, that for each  $n$  the symmetric group  $S_n$  is a finite g.g.r. (see Exercise 64.1). Thus, as a special case of the discussion below, we will obtain a presentation of  $S_n$  in terms of generators and relations. In interpreting some of the preliminary results below, the reader will find it useful to keep the example of  $S_n$  in mind.

**(64.15) Definitions.** Let  $\Delta$  be a root system, with a given set  $\Delta_+$  of positive roots and a fundamental system  $\Pi \subseteq \Delta_+$ . For each  $w \in W$ , we define its *length*  $l(w)$  as the minimal number of factors needed in expressing  $w$  as a product of fundamental reflections, as in Theorem 64.14. An expression

$$w = s_{\alpha_1} \cdots s_{\alpha_k}, \quad \alpha_i \in \Pi, \quad 1 \leq i \leq k,$$

is called *reduced* if  $l(w) = k$ . For each  $w \in W$ , we also define two subsets  $\Delta_w^+$  and  $\Delta_w^-$  of  $\Delta$  by

$$\Delta_w^\pm = \{\alpha \in \Delta_+ : w\alpha \in \Delta_\pm\},$$

and finally set

$$N(w) = |\Delta_w^-|, \quad w \in W.$$

The remarkable fact that  $l(w) = N(w)$ , along with other facts that are basic in determining a presentation of  $W$ , are contained in the next result, the parts of which are so closely related that it is best to discuss them as a package. The theme is to relate properties of  $W$  as an abstract group to geometric and combinatorial properties of  $\Delta$ .

First we need a remark on notation. As usual, we let  $\Pi = \{\alpha_1, \dots, \alpha_n\}$  be a fundamental system in  $\Delta$ ; let  $\Delta_+$  be the positive system containing  $\Pi$ , and let  $S = \{s_1, \dots, s_n\}$  be the set of fundamental reflections, where  $s_i$  is an abbreviation for  $s_{\alpha_i}$ . Each  $w \in W$  is expressible as a product of the  $\{s_i\}$ , and we shall write

$$w = s(1)s(2)\cdots s(m),$$

where repetitions may occur, and where  $s(i)$  is a fundamental reflection corresponding to the fundamental root  $\alpha(i) \in \Pi$ . We are now ready to establish:

**(64.16) Theorem.** *Let  $\Pi$ ,  $\Delta_+$  and  $S$  be as above. Then we have:*

- (i) *For each  $w \in W$  and each  $s_i \in S$ ,*

$$|\Delta_{ws_i}^-| = |\Delta_w^-| \pm 1,$$

*the sign depending on whether  $w\alpha_i \in \Delta_+$  or  $\Delta_-$ .*

(ii) (*Cancellation Law*). Let  $w = s(1) \cdots s(m)$ , with  $s(i) \in S$ , and suppose that  $m > N(w)$ . Then there exist integers  $i, j$  (not necessarily distinct), with  $1 \leq i \leq j \leq m - 1$ , such that

(a) if  $i < j$ , then

$$\alpha(i) = s(i+1) \cdots s(j) \alpha(j+1) \quad \text{and} \quad s(i+1) \cdots s(j+1) = s(i) \cdots s(j),$$

or

(b) if  $i = j$ , the above equations are interpreted as

$$\alpha(i) = \alpha(i+1) \quad \text{and} \quad s(i+1) = s(i).$$

In either case, we have

$$w = s(1) \cdots \hat{s}(i) \cdots \hat{s}(j+1) \cdots s(m),$$

where the notation indicates that the  $i$ -th and  $(j+1)$ -st factors have been deleted from the expression for  $w$ .

(iii) For each  $w \in W$ , we have  $l(w) = N(w)$ .

(iv) (*Exchange Condition*). Suppose that

$$l(s(1) \cdots s(m)) = m \quad \text{and} \quad l(s(0)s(1) \cdots s(m)) < m + 1,$$

where each  $s(i) \in S$ . Then for some  $j$ ,  $0 \leq j \leq m - 1$ , we have

$$s(0)s(1) \cdots s(j) = s(1)s(2) \cdots s(j+1).$$

(v) If  $w \in W$  is such that  $w(\Delta_+) = \Delta_+$ , then  $w = 1$ .

(vi) There exists a unique element  $w_0 \in W$  of maximal length. This element has the properties:  $l(w_0) \geq l(w)$  for all  $w \in W$ , and

$$l(w_0) = |\Delta_+|, \quad w_0 \Delta_+ = \Delta_-, \quad w_0^2 = 1.$$

(vii) An element  $w \in W$  has a reduced expression ending with a given  $s_i \in S$  if and only if  $w\alpha_i < 0$ , where  $s_i$  is the reflection associated with the fundamental root  $\alpha_i$ .

*Proof.* We shall use the Main Lemma 64.13 constantly.

(i) First assume that  $w\alpha_i \in \Delta_+$ . We shall prove that  $\Delta_{ws_i}^- = \{\alpha_i\} \dot{\cup} s_i(\Delta_w^-)$  (disjoint union), where as above

$$\Delta_w^- = \{\alpha \in \Delta_+ : w\alpha \in \Delta_-\}.$$

Now  $s_i\alpha_i = -\alpha_i$ , so from the hypothesis  $w\alpha_i \in \Delta_+$  we deduce that  $\alpha_i \in \Delta_{ws_i}^-$ . Further,

$\alpha_i \notin \Delta_w^-$ , and also  $\alpha_i \notin s_i(\Delta_w^-)$ , since otherwise  $-\alpha_i = s_i\alpha_i \in \Delta_w^-$  (using  $s_i^2 = 1$ ), which is contrary to the fact that  $\Delta_w^-$  consists of positive roots. By the Main Lemma,  $s_i\Delta_w^-$  consists of positive roots, and  $s_i\Delta_w^- \subset \Delta_{ws_i}^-$ , so  $\Delta_{ws_i}^-$  contains the disjoint sets  $\{\alpha_i\}$  and  $s_i\Delta_w^-$ . Now let  $\beta \in \Delta_{ws_i}^-$ , and suppose  $\beta \neq \alpha_i$ . Then  $ws_i\beta \in \Delta_-$ , and  $s_i\beta \in \Delta_+$  by the Main Lemma, so  $s_i\beta \in \Delta_w^-$ . Then  $\beta \in s_i\Delta_w^-$  since  $s_i^2 = 1$ , and the result is proved.

On the other hand, if  $w\alpha_i \in \Delta_-$ , we have  $ws_i(\alpha_i) \in \Delta_+$ , and we can apply the first statement to get

$$\Delta_w^- = \Delta_{ws_i s_i}^- = \{\alpha_i\} \dot{\cup} s_i(\Delta_{ws_i}^-).$$

Thus  $|\Delta_w^-| - 1 = |\Delta_{ws_i}^-|$ , and the result follows.

(ii) Suppose next that  $w = s(1) \cdots s(m)$  where  $N(w) < m$ . Then by part (i) we have  $s(1) \cdots s(j)\alpha(j+1) \in \Delta_-$  for some  $j \leq m-1$ . Also, since  $\alpha(j+1) \in \Delta_+$ , there exists  $i \leq j$  such that  $\alpha(j) = \alpha(j+1)$  if  $i = j$ , while if  $i < j$  then

$$\alpha(j+1) \in \Delta_+, \quad s(j)\alpha(j+1) \in \Delta_+, \quad \dots, \quad s(i+1) \cdots s(j)\alpha(j+1) \in \Delta_+,$$

and

$$s(i) \cdots s(j)\alpha(j+1) \in \Delta_-.$$

By the Main Lemma, it follows that, in the case  $i < j$ ,

$$s(i+1) \cdots s(j)\alpha(j+1) = \alpha(i);$$

hence, by (64.2ii),

$$s(i) = s(i+1) \cdots s(j)s(j+1)s(j) \cdots s(i+1).$$

Unwinding this expression (using  $s(i)^2 = 1$ ), we obtain

$$s(i) \cdots s(j) = s(i+1) \cdots s(j+1).$$

The last statement in the cancellation law (whether  $i < j$  or not) follows by substituting what has been obtained so far in the original expression for  $w$ , again using the fact that  $s(k)^2 = 1$  for each  $k$ .

(iii) Let  $w = s(1) \cdots s(m)$ ,  $s(i) \in S$ ,  $1 \leq i \leq m$ , and assume that  $l(w) = m$ . By part (ii) we have  $N(w) \geq m$ , since otherwise the expression could be shortened. On the other hand,  $N(w) \leq m$  by part (i), and the equality is proved.

(iv) The Exchange Condition follows directly from the Cancellation Law, using the equality of  $l(w)$  and  $N(w)$ . Indeed, applying (ii) to  $w = s(0) \cdots s(m)$ , we have either  $s(0) = s(1)$  or else the case  $i < j$  occurs, because  $l(s(1) \cdots s(m)) = m$ . Then  $s(i+1) \cdots s(j+1) = s(i) \cdots s(j)$ , and we must have  $i = 0$ , again because  $s(1) \cdots s(m)$  is reduced.

(y) If  $w \neq 1$ , then  $l(w) > 0$ , whence  $N(w) > 0$  by (iii); then  $w(\Delta_+) \neq \Delta_+$  by the definition of  $N(w)$ , completing the argument.

(iv) Let  $w_0$  be an element of maximal length. By (i) and the equality of  $N(w)$  and  $l(w)$ , it follows that  $w_0(\alpha_i) \in \Delta_-$  for each  $\alpha_i \in \Pi$ . Thus  $w_0\Delta_+ = \Delta_-$ . If  $w'_0$  is another element of maximal length, then also  $w'_0\Delta_+ = \Delta_-$ , and  $w_0^{-1}w'_0\Delta_+ = \Delta_+$ , so  $w'_0 = w_0$  by (v). Similarly  $w_0^2 = 1$ .

(vii) follows from (i) and the equality of  $N(w)$  and  $l(w)$ .

**Remark.** All these amazing facts raise the question as to what extent the discussion depends on the choice of a particular fundamental system. This question is settled in Exercise 3, where it is shown that any two fundamental systems are conjugate by an element of  $W$ .

## §64B. Coxeter Groups

An *involution* in a group is an element of order 2. We shall be concerned with finite groups  $W$  having a set  $S$  of generators, such that each  $s_i \in S$  is an involution.

**(64.17) Definition.** A *finite Coxeter group*  $W$  is a finite group  $W$  with a presentation

$$W = \langle s_1, \dots, s_n : (s_i s_j)^{m_{ij}} = 1 \text{ for all } i, j \rangle,$$

where the  $\{m_{ij}\}$  are positive integers such that

$$m_{ii} = 1, \quad m_{ij} > 1 \quad \text{if } i \neq j, \quad \text{and} \quad m_{ji} = m_{ij} \quad \text{for all } i, j.$$

We set  $S = \{s_1, \dots, s_n\}$ , a set of involutory generators of  $W$ , and call the pair  $(W, S)$  a *finite Coxeter system*.

Our aim is to prove that every finite g.g.r., defined as in §64A, is a Coxeter group. This result was first proved by Coxeter [34], using an ingenious topological argument, which has been reformulated in purely group-theoretic terms by Benson–Grove [71]. We shall give a proof based on the Exchange Condition (64.16iv), which has the advantage of also giving presentations for Hecke algebras of certain permutation representations of finite groups with  $BN$ -pairs. These results, which are due to Matsumoto [64], also appear in Bourbaki [68], where Coxeter systems are studied without assuming any finiteness conditions.

**(64.18) Definition.** Let  $W$  be a group with a finite set  $S = \{s_1, \dots, s_n\}$  of involutory generators, so every element of  $W$  is a product of elements of  $S$ . For  $w \in W$ , the *length*  $l(w)$  of  $w$  is defined as the least number of factors needed to express  $w$  as a product of elements of  $S$ . An expression

$$w = s(1) \cdots s(m), \quad \text{with } s(i) \in S, \quad 1 \leq i \leq m,$$

(with repetitions  $s(i) = s(j)$  allowed, in general) is said to be *reduced* if  $l(w) = m$ . The set of generators  $S$  satisfies the *exchange condition* if whenever

$$l(s(1) \cdots s(m)) = m, \quad l(s(0)s(1) \cdots s(m)) < m + 1,$$

there exists an integer  $k$  such that

$$s(1) \cdots s(k) = s(0) \cdots s(k - 1).$$

**(64.19) Lemma.** *Let  $D$  be a finite group generated by a pair of involutions  $r, s$ . Then no two distinct reduced expressions in  $r$  and  $s$  are equal in  $D$ , except for the cases:*

$$(rs)^k = (sr)^k \text{ if } rs \text{ is of even order } 2k,$$

$$(rs)^k r = (sr)^k s \text{ if } rs \text{ is of odd order } 2k + 1.$$

The proof is left as an exercise. The reader will note that only expressions with alternating factors  $r$  and  $s$  can be in reduced form, and that such a group  $D$  is easily shown to be isomorphic to a dihedral group, so previous information about the generation of dihedral groups can be applied.

The next result is the theorem of Matsumoto mentioned earlier. Its statement involves the concept of a *monoid*  $M$ , which is simply a set with an associative multiplication  $(m, m') \rightarrow mm'$ ,  $m, m' \in M$ , with the additional property that  $M$  has an identity element  $e$ , satisfying  $me = em = m$  for all  $m \in M$ . The monoids with which we shall be concerned are either groups or the multiplicative structures of rings.

**(64.20) Theorem (Matsumoto [64]).** *Let  $W$  be a finite group generated by a set of involutions  $S = \{s_1, \dots, s_n\}$  satisfying the exchange condition. For each pair  $(i, j)$ ,  $i \neq j$ , let  $m_{ij}$  be the order of  $s_i s_j$ . Then we have, for all  $i \neq j$ ,*

$$(64.21) \quad \begin{cases} (s_i s_j)^{k_{ij}} = (s_j s_i)^{k_{ij}} & \text{if } m_{ij} = 2k_{ij}, \\ (s_i s_j)^{k_{ij}} s_i = (s_j s_i)^{k_{ij}} s_j & \text{if } m_{ij} = 2k_{ij} + 1. \end{cases}$$

Let  $M$  be a monoid with identity  $e$ , and suppose  $\{m_1, \dots, m_n\}$  are elements of  $M$  satisfying the relations (64.21). Then there exists a well-defined map  $f: W \rightarrow M$  such that  $f(1) = e$ ,  $f(s_i) = m_i$ ,  $1 \leq i \leq n$ , and if  $s_{i_1} \cdots s_{i_l}$  is an arbitrary reduced expression in  $W$ , then  $f(s_{i_1} \cdots s_{i_l}) = m_{i_1} \cdots m_{i_l}$ .

*Proof.* To avoid multiple subscripts, we shall use the notation

$$s_{i(1)} \cdots s_{i(l)}, \quad \text{where each } s_{i(k)} \in S,$$

to denote products of elements of  $S$ , with repetitions allowed, and  $m_{i(1)} \cdots m_{i(l)}$  for the corresponding product of elements of  $M$ . We may view 1 as the product of the

empty subset of  $S$ . It is then natural to define a map  $f:W \rightarrow M$  by setting

$$f(1) = e, \quad f(s_i) = m_i, \quad f(s_{i(1)} \cdots s_{i(l)}) = m_{i(1)} \cdots m_{i(l)}$$

for each  $i$ ,  $1 \leq i \leq n$ , and for each reduced product  $s_{i(1)} \cdots s_{i(l)}$  of elements of  $S$ . We have to prove that  $f$  is well defined, that is, if two reduced expressions represent the same element of  $W$ :

$$(64.22) \quad s_{i(1)} \cdots s_{i(l)} = s_{j(1)} \cdots s_{j(l)}, \quad \text{with each } s \in S,$$

then

$$m_{i(1)} \cdots m_{i(l)} = m_{j(1)} \cdots m_{j(l)}.$$

(Note that the expressions in (64.22) must have the same number of factors, since they are reduced.)

We use induction on  $l$ , noting that the desired result is trivially true for  $l = 0, 1$ . Therefore we may take  $l > 1$ , and assume the result holds for shorter expressions. From (64.22) we obtain

$$s_{j(1)} s_{i(1)} \cdots s_{i(l)} = s_{j(2)} \cdots s_{j(l)},$$

and therefore the left-hand side has length  $< l + 1$ . By the exchange condition, there exists an integer  $k$ , with  $1 \leq k \leq l$ , such that

$$(64.23) \quad s_{j(1)} s_{i(1)} \cdots s_{i(k-1)} = s_{i(1)} \cdots s_{i(k)}.$$

Substituting back in the expression (64.22), we obtain

$$(64.24) \quad s_{j(1)} \cdots s_{j(l)} = s_{i(1)} \cdots s_{i(l)} = s_{j(1)} s_{i(1)} \cdots \hat{s}_{i(k)} \cdots s_{i(l)},$$

with the factor  $s_{i(k)}$  deleted from the last expression. Cancelling  $s_{j(1)}$  we obtain

$$s_{j(2)} \cdots s_{j(l)} = s_{i(1)} \cdots \hat{s}_{i(k)} \cdots s_{i(l)},$$

and the expression on the left is reduced, so both are reduced. By induction we have

$$m_{j(2)} \cdots m_{j(l)} = m_{i(1)} \cdots \hat{m}_{i(k)} \cdots m_{i(l)},$$

and hence

$$m_{j(1)} \cdots m_{j(l)} = m_{j(1)} m_{i(1)} \cdots \hat{m}_{i(k)} \cdots m_{i(l)}.$$

In the case  $k < l$ , we also have by induction, from (64.23), since both factors are

reduced,

$$m_{j(1)} m_{i(1)} \cdots m_{i(k-1)} = m_{i(1)} \cdots m_{i(k)},$$

and can substitute this in the expression above to obtain  $m_{i(1)} \cdots m_{i(l)} = m_{j(1)} \cdots m_{j(l)}$ , proving the result in this case. In the case  $k = l$ , the previous inductive argument yields

$$m_{j(1)} \cdots m_{j(l)} = m_{j(1)} m_{i(1)} \cdots m_{i(l-1)}.$$

In the case  $k = l$ , formula (64.24) becomes

$$(64.25) \quad s_{j(1)} s_{i(1)} \cdots s_{i(l-1)} = s_{i(1)} \cdots s_{i(l)},$$

and it suffices to deduce from this that

$$m_{j(1)} m_{i(1)} \cdots m_{i(l-1)} = m_{i(1)} \cdots m_{i(l)}.$$

Now repeat the argument, using formula (64.25) instead of (64.22), with  $i(1), \dots, i(l)$  playing the role of the  $j$ 's in the original discussion. The previous argument now establishes the result, except for what corresponds to the exceptional case (64.25), which now requires us to prove that if

$$s_{i(1)} s_{j(1)} s_{i(1)} \cdots s_{i(l-2)} = s_{j(1)} s_{i(1)} \cdots s_{i(l-1)},$$

then necessarily

$$m_{i(1)} m_{j(1)} m_{i(1)} \cdots m_{i(l-2)} = m_{j(1)} m_{i(1)} \cdots m_{i(l-1)}.$$

Continuing in this way, we either obtain the result at some stage, or arrive at a final exceptional case, which is to prove that the equality of two reduced expressions involving only the factors  $s_{i(1)}$  and  $s_{j(1)}$ , namely

$$s_{i(1)} s_{j(1)} s_{i(1)} \cdots = s_{j(1)} s_{i(1)} s_{j(1)} \cdots$$

implies that

$$m_{i(1)} m_{j(1)} m_{i(1)} \cdots = m_{j(1)} m_{i(1)} m_{j(1)} \cdots.$$

By Lemma 64.19, applied to the group  $\langle s_{i(1)}, s_{j(1)} \rangle$ , the only equality of two reduced expressions involving  $s_{i(1)}$  and  $s_{j(1)}$  is one of the formulas (64.21), and we have assumed in the hypothesis of the theorem that these relations also hold for  $\{m_1, \dots, m_n\}$ . This completes the proof.

**(64.26) Theorem.** *Let  $W = W(\Delta)$  be a finite g.g.r. associated with a root system  $\Delta$ , and let  $S = \{s_1, \dots, s_n\}$  be a set of fundamental reflections defined by some fundamental system  $\Pi \subseteq \Delta$  (see Definition 64.9). Then  $(W, S)$  is a Coxeter system.*

*Proof.* By (64.16iv), the set of generators  $S$  satisfies the exchange condition. According to Definition 1.23, we have to prove that if  $G$  is any group containing elements  $\{g_1, \dots, g_n\}$  such that  $g_i^2 = 1$ ,  $(g_i g_j)^{m_{ij}} = 1$  for  $i \neq j$ , where  $m_{ij}$  = order of  $s_i s_j$ , then there exists a homomorphism  $f: W \rightarrow G$  such that  $f(s_i) = g_i$ ,  $1 \leq i \leq n$ . By Matsumoto's Theorem 64.20, there exists a map  $f: W \rightarrow G$  such that  $f(1) = e$ , where  $e$  is the identity element in  $G$ ,  $f(s_i) = g_i$ ,  $1 \leq i \leq n$ , and  $f(s_{i(1)} \cdots s_{i(l)}) = g_{i(1)} \cdots g_{i(l)}$  for all reduced expressions  $s_{i(1)} \cdots s_{i(l)}$ . We shall prove that  $f$  is a homomorphism, and for this it is sufficient to prove that for all  $w \in W$ , and  $s_i \in S$ , we have

$$f(s_i w) = f(s_i) f(w).$$

Let  $w = s_{i(1)} \cdots s_{i(k)}$ ,  $s_{i(j)} \in S$ , be a reduced expression, so  $l(w) = k$ . If  $s_i s_{i(1)} \cdots s_{i(k)}$  is a reduced expression, then the result is immediate by the properties of the map  $f$ . So we may assume that  $l(s_i w) < l(w)$ . Put  $w' = s_i w$ ; then  $l(s_i w') > l(w')$  by our assumption; hence by the first case we have  $f(s_i w') = f(s_i) f(w')$ . Since both  $s_i$  and  $f(s_i)$  are involutions, we have  $s_i w' = w$ , and  $f(s_i) f(s_i w') = f(w')$ , which is the desired result, and completes the proof of the theorem.

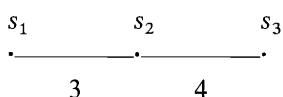
We shall next establish a converse to Theorem 64.26, asserting that every finite Coxeter group can be identified with a g.g.r. acting on some Euclidean space. We also include some remarks on the classification of finite Coxeter groups.

The first step is to define the concept of an indecomposable Coxeter system. The natural definition of indecomposability for a root system  $\Delta$  and the associated g.g.r.  $W(\Delta)$  is that  $\Delta$  cannot be decomposed as a union of two mutually orthogonal subroot systems. Noting that for two roots  $\alpha, \beta \in \Delta$ ,  $(\alpha, \beta) = 0$  if and only if the reflections  $s_\alpha$  and  $s_\beta$  commute, we are led to the following definition:

**(64.27) Definition.** Let  $(W, S)$  be a finite Coxeter system. The *Coxeter graph* associated with  $(W, S)$  consists of a set of vertices, edges, and positive integers associated with edges, as follows. We identify the vertices with the elements of  $S$ , and join two vertices by an edge if and only if the corresponding elements  $s, s'$  of  $S$  do not commute; in this case, we label the edge by the positive integer  $m$ , where  $m$  is the order of  $ss'$  in  $W$ . The Coxeter system is called *indecomposable* if and only if the Coxeter graph is connected.

Note that the condition for  $s$  and  $s'$  to be joined by an edge in the Coxeter graph is equivalent to the statement that  $m > 2$ , where  $m$  is the order of  $ss'$ , since two involutions in a group commute if and only if their product has order 2.

We also remark that the presentation (64.17) of a finite Coxeter system  $(W, S)$  can be read from the Coxeter graph; for example,



is the Coxeter graph of the Coxeter group

$$\langle s_1, s_2, s_3 : s_1^2 = s_2^2 = s_3^2 = (s_1 s_2)^3 = (s_2 s_3)^4 = (s_1 s_3)^2 = 1 \rangle.$$

In (64.30) we shall see that every finite Coxeter group is isomorphic to a direct product of indecomposable ones.

The classification of Coxeter groups is reduced to the classification of root systems by the next result, which asserts that every finite Coxeter group is isomorphic to a g.g.r. This means, by Theorem 64.26, that the families of finite Coxeter groups and finite g.g.r.'s can be identified with one another.

**(64.28) Theorem.** *Let  $(W, S)$  be a finite Coxeter system, with generators  $S = \{s_1, \dots, s_n\}$ . Let  $V$  be a vector space of dimension  $n$  over  $\mathbb{R}$ , and let  $\{e_1, \dots, e_n\}$  be a basis of  $V$ . Define a bilinear form  $B: V \times V \rightarrow \mathbb{R}$  by setting*

$$B(e_i, e_j) = -\cos \pi/m_{ij}, \quad 1 \leq i, j \leq n,$$

where  $m_{ij}$  is the order of  $s_i s_j$  in  $W$ . For each  $s_i \in S$ , define a linear transformation  $T(s_i)$  on  $V$  by setting

$$T(s_i)e_j = e_j - 2B(e_j, e_i)e_i, \quad 1 \leq j \leq n.$$

Then the following statements hold:

- (i) The map  $T: S \rightarrow \text{End } V$  can be extended to a faithful representation  $T: W \rightarrow GL(V)$ .
- (ii) The bilinear form  $B$  is symmetric, positive definite, and invariant with respect to  $T(w)$  for all  $w \in W$ .
- (iii) The group  $T(W)$  is a finite g.g.r., and  $\{T(s_1), \dots, T(s_n)\}$  can be identified with a set of fundamental reflections in  $T(W)$ .
- (iv) If  $(W, S)$  is an indecomposable Coxeter system, then the representation  $T$  is absolutely irreducible.

*Proof.* (See Bourbaki [68, Chapter V], and Deodhar [82]). We have  $m_{ii} = 1$ , and  $m_{ij} \geq 2$  for  $i \neq j$ , since  $s_i^2 = 1$  and since we may assume the elements of  $S$  are distinct. It follows that  $B(e_i, e_i) = 1$ ,  $1 \leq i \leq n$ , and that the restriction of  $B$  to the subspace  $\langle e_i, e_i \rangle$  is nondegenerate, for all  $i \neq j$ ,  $1 \leq i, j \leq n$ . Then we have

$$V = \langle e_i \rangle \oplus \langle e_i \rangle^\perp \quad \text{for } 1 \leq i \leq n,$$

and

$$V = \langle e_i, e_j \rangle \oplus \langle e_i, e_j \rangle^\perp \quad \text{for } i \neq j, \quad 1 \leq i, j \leq n.$$

(The notation  $\langle v, w, \dots \rangle$  denotes the subspace of  $V$  generated by  $v, w$ , etc., and  $\perp$

denotes orthogonality with respect to the form  $B$ .) Using the definition of  $T(s_i)$  and the first decomposition of  $V$ , we see that  $T(s_i)^2 = 1$ ,  $1 \leq i \leq n$ . The second implies that  $T(s_i)T(s_j)$  acts trivially on  $\langle e_i, e_j \rangle^\perp$  if  $i \neq j$ , and leaves  $\langle e_i, e_j \rangle$  invariant. An easy computation shows that  $(T(s_i)T(s_j))^{m_{ij}} = 1$  on  $\langle e_i, e_j \rangle$ . It follows from the universal property of the defining relations of  $W$  that  $T$  can be extended to a representation  $T: W \rightarrow GL(V)$ .

A computation shows that

$$B(T(s_i)e_j, T(s_i)e_k) = B(e_j, e_k), \quad 1 \leq i, j, k \leq n,$$

and hence the form  $B$  is invariant with respect to  $T(w)$  for all  $w \in W$ . It is also clear that  $B$  is symmetric.

Label the vertices of the Coxeter graph of  $(W, S)$  by the integers  $\{1, \dots, n\}$ , in such a way that  $\{1, \dots, n_1\}, \{n_1 + 1, \dots, n_1 + n_2\}$ , etc., correspond to the connected components of the graph. Let  $V_1, \dots, V_k$  be the subspaces of  $V$  spanned by  $\{e_1, \dots, e_{n_1}\}, \{e_{n_1+1}, \dots, e_{n_1+n_2}\}$ , etc., and let  $S_1, S_2, \dots, S_k$  be the corresponding subsets of  $S$ . Note that the order of  $s_i s_j$  in  $W$  is 2 if and only if  $B(e_i, e_j) = 0$ . It follows from the definition of the Coxeter graph that  $V_i \subset V_j^\perp$  for all  $i \neq j$ , and hence

$$V = V_1 \oplus \cdots \oplus V_k.$$

Moreover, we have

$$T(s_i)V_j \subseteq V_j, \quad 1 \leq i \leq n, \quad 1 \leq j \leq k.$$

We now prove that each subspace  $V_i$  is an absolutely simple  $RW$ -module, with the  $W$ -action defined by the restriction of the representation  $T$  to  $V_i$ .

Consider a linear map  $X: V \rightarrow V$  that commutes with all the  $\{T(w): w \in W\}$ . For each  $i$ ,  $1 \leq i \leq n$ , the decomposition  $V = \langle e_i \rangle \oplus \langle e_i \rangle^\perp$  implies that  $\langle e_i \rangle$  is the  $(-1)$ -eigenspace for  $T(s_i)$ , and  $\langle e_i \rangle^\perp$  is the  $(+1)$ -eigenspace for  $T(s_i)$ . It follows that  $X$  leaves the subspaces  $\langle e_i \rangle$  and  $\langle e_i \rangle^\perp$  invariant for each  $i$ , and hence there exist elements  $\lambda_i \in R$  such that

$$Xe_i = \lambda_i e_i, \quad 1 \leq i \leq n.$$

Now suppose  $s_i s_j$  has order  $> 2$ , so that  $i$  and  $j$  belong to the same connected component of the Coxeter graph. Then  $B(e_i, e_j) \neq 0$ , and we have

$$T(s_i)e_j = e_j + a_{ji}e_i, \quad \text{where } a_{ji} \neq 0.$$

Since  $X$  and  $T(s_i)$  commute, we have  $XT(s_i)e_j = \lambda_j T(s_i)e_j$ , and  $X(e_j + a_{ji}e_i) = \lambda_j e_j + a_{ji}\lambda_i e_i$ . It follows that  $\lambda_i = \lambda_j$ , since  $a_{ji} \neq 0$ . Thus  $X$  acts as a scalar multiplication on each of the subspaces  $V_i$ ,  $1 \leq i \leq k$ , and by (3.43) and CR Exercise 27.1, it follows that each submodule  $V_i$  is absolutely simple. This proves part (iv).

Now consider one of the absolutely simple modules  $V_i$  for a fixed  $i$ , where  $1 \leq i \leq k$ , and let  $B_i$  be the restriction of  $B$  to  $V_i$ . Since  $W$  is a finite group, there exists a  $T(W)$ -invariant positive definite symmetric bilinear form  $B'_i$  on  $V_i$ , which can be constructed using the averaging process (see CR Exercise 10.6). Then  $B'_i$  identifies  $V_i$  with its dual, and we have

$$B_i(u, v) = B'_i(u, Xv), \quad u, v \in V_i,$$

for some  $X \in \text{End}_R V_i$ . Since both  $B_i$  and  $B'_i$  are  $T(W)$ -invariant, it follows that  $XT(w) = T(w)X$  for all  $w \in W$ . Because  $V_i$  is absolutely simple,  $X = \lambda \cdot 1$  for some  $\lambda \in R$ , and we have  $B_i = \lambda B'_i$ ; further,  $\lambda > 0$  since  $B(e_i, e_i) = 1$  for each  $i$ . It follows that  $B_i$  is positive definite on each space  $V_i$ , and hence  $B$  is positive definite on  $V$ , completing the proof of (ii).

At this point we can identify  $T(W)$  with a finite g.g.r. acting on  $V$ , with the inner product given by  $B$ . Then the vectors  $\{e_1, \dots, e_n\}$  and their images  $\{T(w)e_i : w \in W, 1 \leq i \leq n\}$  form a root system  $\Delta$  associated with  $T(W)$ . We now prove, following Deodhar [82], that  $\{e_1, \dots, e_n\}$  is a fundamental system in  $\Delta$ ; this will imply that  $\{T(s_1), \dots, T(s_n)\}$  is a set of fundamental reflections in  $T(W)$ , by definition of the  $\{T(s_i)\}$ .

By Definition 64.9, it suffices to prove that if  $l(ws_i) \geq l(w)$ , then  $T(w)e_i = \sum a_j e_j$ , with each  $a_j \geq 0$ . We use induction on  $l(w)$ , and note that the result is clearly true if  $l(w) = 0$  or 1, so we may assume  $l(w) \geq 1$ . Since  $W$  is a finite Coxeter group, the map  $\varepsilon: S \rightarrow \pm 1$  defined by  $\varepsilon(s_j) = -1$ ,  $1 \leq j \leq n$ , preserves the defining relations (64.17), and can be extended to a homomorphism  $\varepsilon: W \rightarrow \pm 1$ . It follows that  $\varepsilon(w) = (-1)^{l(w)}$ , and from this an easy argument shows that  $l(ws_j) = l(w) \pm 1$  for all  $s_j \in S$ . Since  $l(w) \geq 1$ , there exists  $s_j \in S$  such that  $s_j \neq s_i$  and  $l(ws_j) = l(w) - 1$ . Let  $W_{ij} = \langle s_i, s_j \rangle$ . From what has been said, it follows that we can write

$$w = xy, \quad \text{where } y \in W_{ij},$$

with  $l(w) = l(x) + l(y)$ , and where  $x$  is an element of minimal length in the coset  $wW_{ij}$ . We then deduce that

$$l(x) < l(w), \quad l(ys_i) > l(y) \quad \text{and} \quad l(xs_i) > l(x), \quad l(xs_j) > l(x).$$

The reader will easily verify that if  $y \in W_{ij}$ , and  $l(ys_i) > l(y)$ , then

$$T(y)e_i = ae_i + be_j, \quad \text{with } a, b \geq 0.$$

Taking this for granted, we then have

$$T(w)e_i = T(x)T(y)e_i = aT(x)e_i + bT(x)e_j,$$

and by induction, we obtain  $T(w)e_i = \sum a_j e_j$ , with each  $a_j \geq 0$ , as required. This completes the proof that  $\{e_1, \dots, e_n\}$  is a fundamental system in  $\Delta$ , and part (iii) of the theorem is established.

It remains to prove that the representation  $T$  is faithful. Let  $\Pi = \{e_1, \dots, e_n\}$ , and let  $\Delta_+$  be the set of positive roots containing  $\Pi$ . By (64.16),  $l(w) = N(w) = |\Delta_w^-|$ , for  $w \in W$ , where  $\Delta_w^- = \{\alpha \in \Delta_+ : T(w)\alpha \in \Delta_-\}$ . It follows that if  $T(w)$  acts trivially on  $V$ , then  $l(w) = 0$  and  $w = 1$ . Thus  $\ker T = 1$ , and  $T$  is a faithful representation. This completes the proof of the theorem.

**(64.29) Definition.** Let  $(W, S)$  be an indecomposable Coxeter system. The absolutely irreducible representation  $T$  defined in (64.28) is called the *reflection representation of  $W$* .

**(64.30) Proposition.** Let  $(W, S)$  be a finite Coxeter system, and let  $S_1, \dots, S_k$  be the subsets of  $S$  associated with the connected components of the Coxeter graph of  $W$ . Let  $W_i = \langle S_i \rangle$ ,  $1 \leq i \leq k$ . Then  $(W_i, S_i)$  is a finite Coxeter system for each  $i$ , and we have

$$W = W_1 \times \cdots \times W_k \quad (\text{direct product}).$$

The proof is left as an exercise for the reader.

The classification of indecomposable Coxeter systems is given in Bourbaki [68]. By Theorem 64.28, the problem comes down to the classification of root systems associated with indecomposable g.g.r.'s. A list of the Coxeter graphs of indecomposable g.g.r.'s whose root systems satisfy the crystallographic condition

$$A_n, \quad n \geq 1 \quad \bullet - \bullet - \bullet - \cdots - \bullet - \bullet$$

$$B_n - C_n, \quad n \geq 2 \quad \bullet - \bullet - \bullet - \cdots - \bullet - \bullet \quad 4$$

$$D_n, \quad n \geq 4 \quad \bullet - \bullet - \bullet - \cdots - \bullet - \bullet \quad \bullet - \bullet$$

$$E_6 \quad \bullet - \bullet - \bullet - \bullet - \bullet - \bullet$$

$$E_7 \quad \bullet - \bullet - \bullet - \bullet - \bullet - \bullet - \bullet$$

$$E_8 \quad \bullet - \bullet$$

$$F_4 \quad \bullet - \bullet - \bullet - \bullet \quad 4$$

$$G_2 \quad \bullet - \bullet \quad 6$$

is given above, using the notation of E. Cartan. In the list, unlabeled edges are assigned the integer 3. The classification of the corresponding root systems can be found in Bourbaki [68], or in any book on Lie algebras, and will not be repeated here. There is, up to a change of scale, a unique root system of each type, except in the case of  $B_n$ ,  $C_n$ , where there are two. The first step in the classification, which asserts that the Coxeter graph of an indecomposable Coxeter system is a tree, is given in Exercise 4. The classification of root systems of types  $A_n$ ,  $D_n$ ,  $E_n$  is sketched in §77.

### §64C. Parabolic Subgroups of Finite Coxeter Groups

In this subsection,  $(W, S)$  denotes an arbitrary finite Coxeter system (see (64.17)). By Theorem 64.28, there exists a root system  $\Delta$  in a Euclidean space such that  $W$  can be identified with the g.g.r. associated with  $\Delta$ , and  $S$  with a set of fundamental reflections. Thus the results of (64.16) can be applied to the pair  $(W, S)$ . In particular, we recall the following results for the convenience of the reader; these are the only ones required for most of this subsection.

**(64.31) Cancellation Law.** *Let*

$$w = s_{i(1)} \cdots s_{i(m)} \in W, \quad \text{where each } s_{i(j)} \in S,$$

*and assume that we have  $l(w) < m$ . Then there exist integers  $j \leq k$  such that*

$$w = s_{i(1)} \cdots \hat{s}_{i(j)} \cdots \hat{s}_{i(k+1)} \cdots s_{i(m)}.$$

**(64.32) Exchange Condition.** *Let*

$$l(s_{i(1)} \cdots s_{i(m)}) = m \quad \text{and} \quad l(s_{i(0)} s_{i(1)} \cdots s_{i(m)}) < m + 1.$$

*Then for some  $j$ ,  $0 \leq j \leq m - 1$ ,*

$$s_{i(0)} \cdots s_{i(j)} = s_{i(1)} \cdots s_{i(j+1)}.$$

As a first application of these results, we have

**(64.33) Lemma.** *Let*

$$s_{i(1)} \cdots s_{i(m)} = s_{j(1)} \cdots s_{j(m)}, \quad \text{with each } s \in S,$$

*be two reduced expressions of length  $m$ . Then*

$$\{i(1), \dots, i(m)\} = \{j(1), \dots, j(m)\};$$

*in other words, the subsets of  $S$  supporting the two expressions coincide.*

*Proof.* We use induction on  $m$ . The result is clear if  $m = 1$ , and so we assume  $m > 1$ . From the hypothesis we have

$$s_{i(2)} \cdots s_{i(m)} = s_{i(1)} s_{j(1)} \cdots s_{j(m)}.$$

It follows that  $l(s_{j(1)} \cdots s_{j(m)}) = m$ , and  $l(s_{i(1)} s_{j(1)} \cdots s_{j(m)}) < m + 1$ , so by (64.32) we have (for some  $k$ )

$$s_{i(2)} \cdots s_{i(m)} = s_{i(1)} s_{j(1)} \cdots s_{j(m)} = s_{j(1)} \cdots \hat{s}_{j(k)} \cdots s_{j(m)}.$$

By the induction hypothesis, we obtain

$$\{i(2), \dots, i(m)\} \subseteq \{j(1), \dots, j(m)\}.$$

We also have, from the above formula,

$$s_{i(1)} = s_{j(1)} \cdots \hat{s}_{j(k)} \cdots s_{j(m)} s_{j(m)} \cdots s_{j(1)}$$

The right-hand side has length 1, and therefore, by successive applications of the Cancellation Law 64.31, it follows that  $i(1) \in \{j(1), \dots, j(m)\}$ , and we have shown that

$$\{i(1), \dots, i(m)\} \subseteq \{j(1), \dots, j(m)\}.$$

The reverse inclusion is proved similarly, and the result follows.

The next result, which is an easy application of the preceding lemma, introduces an important family of subgroups of  $W$ .

**(64.34) Proposition.** *Let  $J$  be an arbitrary subset of the fundamental reflections  $S = \{s_1, \dots, s_n\}$ , and let  $W_J$  denote the subgroup  $\langle J \rangle$  of  $W$  generated by the involutions in  $J$ . Then for each  $w \in W_J$ , all reduced expressions for  $w$  have all their factors in  $J$ .*

*Proof.* Let  $w$  be an arbitrary element of  $W_J$ . Then  $w$  has at least one reduced expression with all factors in  $J$ , by successive applications of the cancellation law. The fact that all reduced expressions for  $w$  have the same property follows at once from (64.33), completing the proof.

**(64.35) Definition.** Let  $(W, S)$  be a finite Coxeter system. The subgroups  $\{W_J\}_{J \subseteq S}$ , and their conjugates, are called *parabolic subgroups* of  $W$ . For a fixed set of generators  $S$ , the subgroups of the form  $\{W_J\}_{J \subseteq S}$  are called *standard parabolic subgroups*.

**(64.36) Proposition.** *Let  $W$  be a finite g.g.r. associated with a root system  $\Delta$ , let  $\Pi$  be a set of fundamental roots, and let  $S$  be the set of fundamental reflections. Let*

$J \subseteq S$ , and let  $\Pi_J$  be the corresponding subset of  $\Pi$ . Set  $\Delta_J = \Delta \cap \langle \Pi_J \rangle$ . ( $\langle \Pi_J \rangle$  is the subspace of the underlying vector space  $V$  generated by  $\Pi_J$ .) Then  $\Delta_J$  is a root system in  $\langle \Pi_J \rangle$  with fundamental system  $\Pi_J$ , and  $W_J$  is the g.g.r. associated with  $\Delta_J$ .

*Proof.* By (64.26), the pair  $(W, S)$  is a Coxeter system. It is easily checked that  $\Delta_J$  satisfies the axioms (64.4) for a root system. Since  $\Delta_J$  is contained in the subspace of  $V$  generated by the linearly independent set  $\Pi_J$ , it is clear from (64.9) that  $\Pi_J$  is a fundamental system in  $\Delta_J$ . Finally, by Theorem 64.14, the g.g.r. associated with  $\Delta_J$  is generated by the reflections corresponding to the roots in  $\Pi_J$ , and it follows that this g.g.r. coincides with  $W_J$ , completing the proof.

The preceding result shows that the parabolic subgroups of  $W$  are themselves g.g.r.'s associated with subroot systems of  $\Delta$ . As shown in the exercises, however, there exist, in general, subroot systems of  $\Delta$  whose g.g.r.'s are not parabolic subgroups of  $W$ . Their study is a subtle business and is needed for the determination of the conjugacy classes in a Weyl group (Carter [72a]).

**(64.37) Proposition.** *Let  $(W, S)$  be a finite Coxeter system. Then the following statements hold:*

- (i) *For  $J \subseteq S$ , the length  $l(w)$  of an element of  $W_J$  is the same whether  $w$  is viewed as an element of  $W$ , or of the subgroup  $W_J$  with the set of involutory generators  $J$ , as in (64.34).*
- (ii) *For each  $J \subseteq S$ , the pair  $(W_J, J)$  is a Coxeter system.*
- (iii) *The map  $J \rightarrow W_J$ ,  $J \subseteq S$ , is a bijection from the family of all subsets of  $S$  to a family of subgroups of  $W$ .*
- (iv) *For all  $I, J \subseteq S$ ,  $W_I \cap W_J = W_{I \cap J}$ .*
- (v)  *$S$  is a minimal set of generators of  $W$ .*

The proofs are all easy consequences of the preceding results, and are left as exercises.

By (64.37iv), the intersection of two standard parabolic subgroups  $W_I$  and  $W_J$  is a parabolic subgroup  $W_{I \cap J}$ . The last result in this section is that the intersection of any two parabolic subgroups is parabolic (that is, a conjugate of subgroup of the form  $W_I$ ,  $I \subseteq S$ .) This is a somewhat surprising result, especially in view of Exercise 5, which shows that the intersection of two g.g.r.'s is not necessarily a g.g.r. We first require a preliminary result.

**(64.38) Proposition.** *Let  $I, J \subseteq S$ . Every double coset  $W_I w W_J \in W_I \backslash W / W_J$  contains a unique element  $x$  of minimal length. This element has the further property that each element in  $W_I x W_J$  has an expression  $uxv$ , with  $u \in W_I$ ,  $v \in W_J$ , and*

$$l(uxv) = l(u) + l(x) + l(v).$$

*Proof.* Let  $x \in W_I w W_J$  be an element of minimal length  $m$  in the double coset, and let  $uxv$  be another element in the double coset, with  $u \in W_I$ ,  $v \in W_J$ . We shall prove that if  $l(uxv) = m$ , then  $uxv = x$ . If, for reduced expressions for  $u$ ,  $x$ ,  $v$ , the resulting expression for  $uxv$  is also reduced, then  $l(uxv) = m$  implies  $u = v = 1$ , since  $l(x) = m$  by assumption. If the expression obtained for  $uxv$  is not reduced, then by the Cancellation Law we have  $uxv = u_1 x_1 v_1$ , with  $u_1, x_1, v_1$  obtained from  $u, x, v$ , respectively, by cancelling factors; further,  $u_1 \in W_I$  and  $v_1 \in W_J$ , since by (64.34) any reduced expression for  $u$  has all its factors in  $I$ , and similarly those of  $v$  lie in  $J$ . Then  $x_1 \in W_I x W_J$ , and if  $x_1 \neq x$ , then  $x_1$  is an element of the double coset of shorter length than  $x$ , contrary to the choice of  $x$ . So we have  $uxv = u_1 xv_1$ , and continuing the cancellation process if necessary, we obtain a reduced expression for  $uxv$  of the form  $u' xv'$ , with  $u'$  and  $v'$  reduced. Since  $l(u' xv') = m$ , we have  $u' = v' = 1$ , which proves the uniqueness of  $x$ . For the second statement, let  $uxv \in W_I x W_J$ , with  $u \in W_I$  and  $v \in W_J$ . By the above argument, we can obtain a reduced expression for  $uxv$  of the form  $u_1 xv_1$ , with  $u_1$  a reduced expression in  $W_I$  and  $v_1$  a reduced expression in  $W_J$ . Then  $l(uxv) = l(u_1 xv_1) = l(u_1) + l(x) + l(v_1)$ , completing the proof.

**(64.39) Definition.** We call an element  $x$  of minimal length in a double coset  $W_I w W_J$ , as in (64.38), a *distinguished double coset representative* (d.d.c.r.). Let  $D_{IJ}$  denote the set of d.d.c.r.'s for all double cosets in  $W_I \backslash W / W_J$ .

Note, in particular, that for each  $I \subseteq S$ ,  $D_{I\emptyset}$  is a set of coset representatives for right cosets  $W_I w$ , and each element in  $D_{I\emptyset}$  is characterized as the unique element of minimal length in its coset. If  $x \in D_{I\emptyset}$ , and  $u \in W_I$  then  $l(ux) = l(u) + l(x)$  by (64.38). Similar statements can be made, of course, for  $D_{\emptyset J}$ , where  $J \subseteq S$ . It is easily shown that  $D_{IJ} = D_{I\emptyset} \cap D_{\emptyset J}$ .

**(64.40) Theorem** (Kilmoyer [69]; Solomon [76]). *The intersection of any two parabolic subgroups of  $W$  is a parabolic subgroup. More precisely, any intersection of conjugates of  $W_I$  and  $W_J$  is a conjugate of  $W_I \cap {}^x W_J$  for some  $x \in D_{IJ}$ , and we have*

$$W_I \cap {}^x W_J = W_K, \quad \text{if } x \in D_{IJ},$$

where  $K = I \cap {}^x J$ .

*Proof.* First note that for  $y, z \in W$ , the subgroup  ${}^y W_I \cap {}^z W_J$  is conjugate to  $W_I \cap {}^w W_J$ , where  $w = y^{-1}z$ . Further, if  $x \in D_{IJ}$  is the d.d.c.r. in  $W_I w W_J$ , we may write  $w = uxv$  with  $u \in W_I$ ,  $v \in W_J$ ; then  $W_I \cap {}^w W_J = {}^u(W_I \cap {}^x W_J)$ .

Now let  $x \in D_{IJ}$ , and let  $K = I \cap {}^x J$ . We clearly have  $W_K \subseteq W_I \cap {}^x W_J$ , so it is sufficient to prove that if  $w \in W_I \cap {}^x W_J$ , then  $w \in W_K$ . The result is obvious if  $l(w) = 0$ , so we assume  $l(w) > 0$ , and assume, as an induction hypothesis, that the result holds for shorter elements of  $W_I \cap {}^x W_J$ . Because  $w \in W_I$  and  $w \neq 1$ , we have  $l(sw) < l(w)$  for some  $s \in I$ . We also have  $w = xv x^{-1}$ , for  $v \in W_J$ , so  $wx = xv$ . Then  $x \in D_{IJ}$  implies  $x \in D_{I\emptyset}$ , and

$$l(sxv) = l(sw) + l(x) < l(w) + l(x) = l(wx) = l(xv).$$

Now let

$$x = s_{i(1)} \cdots s_{i(p)}, \quad \text{and} \quad v = s_{i(p+1)} \cdots s_{i(p+q)},$$

be reduced expressions. By (64.34),  $\{s_{i(p+1)}, \dots, s_{i(p+q)}\} \subseteq J$ . As  $x \in D_{\emptyset J}$ , it follows that

$$xv = s_{i(1)} \cdots s_{i(p)} s_{i(p+1)} \cdots s_{i(p+q)}$$

is a reduced expression, and so  $l(sxv) < l(xv)$  implies that

$$sxv = s_{i(1)} \cdots \hat{s}_{i(j)} \cdots s_{i(p+q)},$$

by the Exchange Condition. If  $j \leq p$ , then we may cancel  $v$  from both sides, and obtain

$$sx = s_{i(1)} \cdots \hat{s}_{i(j)} \cdots s_{i(p)} \in W_I x W_J,$$

and  $l(sx) < l(x)$ , which is impossible. Therefore  $j \geq p+1$ , and we have  $x^{-1}sx \in W_J$  (remembering that  $x = s_{i(1)} \cdots s_{i(p)}$ ). We obtain

$$1 + l(x) = l(sx) = l(xx^{-1}sx) = l(x) + l(x^{-1}sx),$$

because  $x^{-1}sx \in W_J$  and  $x \in D_{\emptyset J}$ . Thus  $l(x^{-1}sx) = 1$ , and  $x^{-1}sx \in S \cap W_J = J$ . Then  $s \in I \cap {}^x J = K$ , and

$$w = s(sw), \quad l(sw) < l(w),$$

so  $sw \in W_I \cap {}^x W_J$ . By the induction hypothesis  $sw \in W_K$ , and hence  $w \in W_K$ , as required.

**(64.41) Corollary.** *Let  $W$  be a finite g.g.r. associated with a root system  $\Delta$ , let  $\Pi$  be a set of fundamental roots, and  $S$  the set of fundamental reflections, as in (64.36). Let  $\Pi_I, \Pi_J$  be the subsets of  $\Pi$  corresponding to subsets  $I, J \subseteq S$ . Then for  $x \in D_{IJ}$ ,*

$$\Pi_I \cap x\Pi_J = \Pi_K, \quad \text{and} \quad \Delta_I \cap x\Delta_J = \Delta_K,$$

where  $K = I \cap {}^x J$  as in (64.40).

*Proof.* Let  $\alpha \in \Pi_K$ ; then  $s_\alpha \in K \subseteq I \cap {}^x J$ , and it follows that  $\alpha \in \Pi_I$ , and  $x^{-1}s_\alpha x = s_{x^{-1}\alpha} \in J$ , so  $x^{-1}\alpha \in \Pi_J$  since  $x^{-1}\alpha > 0$  for  $x \in D_{IJ}$ . Conversely,  $\alpha \in \Pi_I \cap x\Pi_J$  implies  $\alpha = x\beta$ , for  $\beta \in \Pi_J$ , so  $s_\alpha = xs_\beta x^{-1} \in W_I \cap {}^x W_J = W_K$  by (64.40). Then  $s_\alpha \in K$  since  $l(s_\alpha) = 1$ , and the only elements in  $W_K$  of length 1 are the elements of  $K$ , by (64.37i). For the second statement, we have  $\Delta_K = W_K \Pi_K$  by (64.14) applied to  $W_K$ . Then

$$W_K \Pi_K \subseteq W_I \Pi_I \cap {}^x W_J x \Pi_J \subseteq \Delta_I \cap x \Delta_J.$$

Conversely, if  $\gamma \in \Delta_I \cap x\Delta_J$ , then  $s_\gamma \in W_I \cap {}^xW_J = W_K$  by (64.40). But  $s_\gamma \in W_K$  implies  $\gamma \in \Delta_K$ , since  $W_K$  is the g.g.r. of  $\Delta_K$  by (64.36), and the proof is completed.

## §64. Exercises

1. Let  $n$  be a positive integer, and let  $\{e_1, \dots, e_{n+1}\}$  be an orthonormal basis of  $\mathbb{R}^{n+1}$ , with respect to the usual inner product. Let  $\Delta$  be the set of all vectors  $\alpha = e_i - e_j$ ,  $i \neq j$ ,  $1 \leq i, j \leq n+1$ , and let  $V$  denote the hyperplane in  $\mathbb{R}^{n+1}$  consisting of all vectors  $\sum a_i e_i$  with  $\sum a_i = 0$ .

(i) Prove that  $\Delta$  is a root system in  $V$ , satisfying the crystallographic condition, whose associated g.g.r.  $W(\Delta)$  is isomorphic to the symmetric group  $S_{n+1}$ . Show that the reflections  $\{s_\alpha : \alpha \in \Delta\}$  in  $\mathbb{R}^{n+1}$  permute the basis vectors  $\{e_i\}$ , so their restrictions to  $V$  generate  $W(\Delta)$  and define the isomorphism  $W(\Delta) \cong S_{n+1}$ .

(ii) Show that the set of roots  $\{e_i - e_j : i < j\}$  is a positive set of roots in  $V$  containing the fundamental system  $\Pi = \{\alpha_1, \dots, \alpha_n\}$ , where  $\alpha_i = e_i - e_{i+1}$ ,  $1 \leq i \leq n$ .

(iii) Let  $S = \{s_{\alpha_1}, \dots, s_{\alpha_n}\}$ . Verify that  $(W(\Delta), S)$  is an indecomposable Coxeter system whose Coxeter graph is of type  $A_n$ .

(iv) Let  $J \subseteq S$ , and let  $W_J$  be the corresponding standard parabolic subgroup of  $W(\Delta)$ . Prove that  $W_J$  is isomorphic to a subgroup of the symmetric group  $S_{n+1}$  of the form  $S_{n_1} \times \dots \times S_{n_r}$ , for some partition  $\{n_1, \dots, n_r\}$  of  $n+1$  (see also the definition of Young subgroups in §75A.)

2. Let  $\{e_1, \dots, e_n\}$  be an orthonormal basis of  $\mathbb{R}^n$ , as in Exercise 1, and let  $\Delta$  denote the set of vectors  $\{\pm e_i, \pm e_i \pm e_j, i \neq j, 1 \leq i, j \leq n\}$ .

(i) Prove that  $\Delta$  is a root system in  $\mathbb{R}^n$ , satisfying the crystallographic condition whose associated g.g.r. is isomorphic to the *hyperoctahedral group*  $H_n$ . (The group  $H_n$  is defined as the wreath product  $Z_2 \wr S_n$  (see §13A), and is isomorphic to the symmetry group of the  $n$ -dimensional cube.)

(ii) Prove that  $\Pi = \{e_1 - e_2, \dots, e_{n-1} - e_n, e_n\}$  is a fundamental system of roots in  $\Delta$ , and that the associated Coxeter system in  $W(\Delta)$  is indecomposable, of type  $B_n - C_n$ .

3. Let  $\Delta$  be a root system, and let  $\Delta_{+,1}$  and  $\Delta_{+,2}$  be two positive sets of roots in  $\Delta$ . Prove that there exists  $w \in W(\Delta)$  such that  $w\Delta_{+,1} = \Delta_{+,2}$ .

[Hint (Steinberg): Let  $n = |\Delta_{+,1} \cap -\Delta_{+,2}|$ . If  $n = 0$ , then  $\Delta_{+,1} = \Delta_{+,2}$ . Let  $n > 0$ . Then prove that  $|\Pi_1 \cap -\Delta_{+,2}| > 0$ , where  $\Pi_1$  is the fundamental system of roots contained in  $\Delta_{+,1}$ . Let  $\alpha \in \Pi_1 \cap -\Delta_{+,2}$ , and show that  $|s_\alpha \Delta_{+,1} \cap -\Delta_{+,2}| = n-1$ , so  $|\Delta_{+,1} \cap -s_\alpha \Delta_{+,2}| = n-1$  and an induction hypothesis can be applied.]

4. Let  $(W, S)$  be an indecomposable Coxeter system, with  $W$  a finite group. Prove that the Coxeter graph associated with  $(W, S)$  is a tree.

[Hint (Bourbaki [68]): We have to prove that the Coxeter graph contains no closed paths of length  $> 1$ . Suppose, to the contrary, that a closed path does exist. Let  $V$  be the vector space affording the reflection representation, with basis  $\{e_1, \dots, e_m\}$  and bilinear form  $B$  (see (64.28)). By reindexing, we may assume that  $e_1, \dots, e_m$  correspond to the ordered set of reflections which define a closed path in the Coxeter graph. Let  $e = e_1 + \dots + e_m$ . Then  $e \neq 0$ , and  $B(e, e) = m + 2\sum_{i < j} B(e_i, e_j)$ . Since  $B(e_i, e_{i+1}) =$

$-\cos(\pi/m_{i,i+1}) \leq -\cos(\pi/3) = -1/2$ , for  $1 \leq i \leq m-1$  and similarly for  $B(e_m, e_1)$ , we obtain  $B(e, e) \leq 0$ , contradicting the fact that  $B$  is positive definite (by (64.28)).]

5. Let  $\Delta$  be a root system of type  $B_2$ , consisting of the roots  $\{\pm e_i, \pm e_i \pm e_j, 1 \leq i, j \leq 2\}$  in the notation of Exercise 2. Let  $\alpha_1 = e_1 - e_2$ ,  $\alpha_2 = e_2$ ,  $s_i = s_{\alpha_i}$ ,  $i = 1, 2$ . Then  $\{s_1, s_2\}$  is a set of fundamental reflections in  $W(\Delta)$ . Verify that the subgroups  $W_1 = \langle s_1, s_2s_1s_2 \rangle$  and  $W_2 = \langle s_2, s_1s_2s_1 \rangle$  are both g.g.r.'s and that neither is a parabolic subgroup. Show that  $W_1 \cap W_2$  is not a g.g.r.

6. Let  $\Delta$  be a root system, and let  $W$  denote the g.g.r. associated with  $\Delta$ . Let  $S$  be a set of fundamental reflections in  $W$ , defined by a set of positive roots  $\Delta_+ \subset \Delta$ , and let  $J \subseteq S$ . Prove that  $\Delta_w^- \subseteq \Delta_J$  for each  $w \in W_J$  (see §64C).

## §65. FINITE GROUPS WITH BN-PAIRS

### §65A. The Bruhat Decomposition

We begin with an axiomatic approach to finite groups of Lie type due to J. Tits [62]. The axioms capture the essential features of Chevalley's analysis in [55] of the structure of what are now called Chevalley groups. They are also part of the foundations of the theory of buildings, and lead to a geometrical classification of the finite Chevalley groups (Tits [74]). In this subsection we give the axioms for *BN*-pairs, and we derive some of their consequences. These include a double coset decomposition of a group with a *BN*-pair (called the Bruhat decomposition); its role in the study of groups of Lie type is analogous to that of the root space decomposition of a semisimple Lie algebra over  $\mathbb{C}$  relative to a Cartan subalgebra. (For the construction of Chevalley groups from semisimple Lie algebras, see Chevalley [55], Steinberg [67], or Carter [72b].)

**(65.1) Definitions.** A *finite group with a BN-pair\** is a finite group  $G$  containing a pair of subgroups  $B, N$  satisfying the following axioms:

(i)  $G = \langle B, N \rangle$ .

(ii)  $B \cap N \trianglelefteq N$ .

(iii) Let  $W = N/(B \cap N)$ , and for each  $w \in W$  choose a coset representative  $\dot{w} \in N$ . Then  $W$  is generated by a set  $S = \{s_1, \dots, s_n\}$  of involutions such that

$$(65.2) \quad \dot{s}_i B \dot{w} \subseteq B \dot{w} B \cup B \dot{s}_i w B$$

and

$$(65.3) \quad \dot{s}_i B \dot{s}_i \neq B$$

for each  $w \in W$  and each  $s_i \in S$ .

\*Also called a *Tits system*; see Bourbaki [68].

For a group  $G$  satisfying the axioms, we will usually denote  $B \cap N$  by  $T$ , and call the group  $W = N/T$  the *Weyl group* associated with the *BN-pair*. The generators  $S$  of  $W$  will be called the *distinguished generators* of  $W$ , and the cardinality  $|S|$  is called the *rank* of the *BN-pair*. (We shall see later that both  $S$  and the rank are uniquely determined.) The subgroup  $B$  is called a *Borel subgroup* of  $G$ .

We proceed to derive consequences of the axioms. It may be useful for a reader who is unfamiliar with these things to read §65A in parallel with §65B, where an important family of examples of *BN-pairs* is constructed.

Our first remark concerning a group with a *BN-pair* is that, since  $T \leq B$ , subsets of  $G$  of the form  $wB$ ,  $BwB$ ,  ${}^wB$ , etc. are independent of the choice of the coset representative  $w$ , and can thus be written unambiguously as

$$wB, BwB, {}^wB, \text{ for } w \in W.$$

We also note that since  $W$  has a set of involutory generators  $S$ , we can define the *length*  $l(w)$  of elements  $w \in W$  as in (64.18), as well as the concept of *reduced expression* for elements of  $W$ . We now have:

**(65.4) Theorem (Bruhat Decomposition).** *Let  $G$  be a finite group with a BN-pair. Then*

$$G = \bigcup_{w \in W} BwB.$$

*In particular, the map  $w \rightarrow BwB$  gives a bijection:  $W \leftrightarrow B \backslash G/B$ .*

*Proof.* Let  $X = \bigcup_w BwB$ , a subset of  $G$  containing both  $B$  and  $N$ . To prove the first statement in the theorem, we need only show that  $X$  is a *subgroup* of  $G$ . For this, it suffices to check that  $bX = X$  for all  $b \in B$  (which is obvious), and that\*  $zX = X$  for all  $z \in W$ . Since the elements of  $S$  generate  $W$ , we need only verify that  $s_i X = X$  for each  $s_i \in S$ . However, this is an immediate consequence of (65.2).

For the second part of the theorem, we must show that if  $w \neq w'$  in  $W$ , then  $BwB \neq Bw'B$ . Let  $m = l(w')$ , the length of  $w'$  as a product of involutions in  $S$ , as in (64.18). We use induction on  $m$ , noting that when  $m = 0$  we have  $w' = 1$ ; clearly  $BwB \neq B$ , since otherwise  $w \in B \cap N$ , so  $w = 1$ . We may thus assume that  $w \neq w'$ , and that

$$l(w) \geq l(w') = m > 0.$$

Then for some  $s_i \in S$  we have  $l(s_i w') \leq m - 1$ , so  $l(w) \neq l(s_i w')$ , and therefore  $w \neq s_i w'$ . We also have  $s_i w \neq s_i w'$ , so by the induction hypothesis, both  $Bs_i w B$  and

\*For  $z \in W$ ,  $zX$  means  $\dot{z}X$ , where  $\dot{z} \in N$  is a coset representative of  $z$ . Since  $X$  is a union of double cosets of the form  $BwB$ , our earlier remarks show that  $zX$  depends only on  $z$ , and not on the choice of the coset representative  $\dot{z}$ .

$BwB$  are distinct from  $Bs_iw'B$ . By (65.2) this implies that

$$(Bs_iB)(BwB) \cap Bs_iw'B = \emptyset.$$

On the other hand,  $Bs_iw'B \subseteq (Bs_iB)(Bw'B)$ , so it follows that  $BwB \neq Bw'B$ , as required.

Throughout the rest of §65A, we assume that  $G$  is a group with a  $BN$ -pair, with Weyl group  $W$  and set of distinguished generators  $S$  of  $W$ . The next two results describe, to some extent, the multiplication of double cosets.

**(65.5) Proposition.** *If  $w \in W$  and  $s_i \in S$  are such that  $l(s_iw) \geq l(w)$ , then  $s_iBw \subseteq Bs_iwB$ .*

*Proof.* We use induction on  $l(w)$ , noting that the result is clear if  $l(w) = 0$ . We may therefore assume  $l(w) > 0$ , and find  $s_j \in S$  such that  $w = w's_j$ , with  $l(w') \leq l(w) - 1$ . Suppose the result is false in this situation; then by (65.2) we have  $s_iBw \cap BwB \neq \emptyset$ , so  $s_iBw' \cap BwBs_j \neq \emptyset$ . Since  $l(s_iw) \geq l(w)$  and  $s_iw = s_iw's_j$ , we also have  $l(s_iw') \geq l(w')$ , since otherwise  $l(s_iw) \leq l(s_iw') + 1 < l(w') + 1 \leq l(w)$ . Then, by the induction hypothesis,  $s_iBw' \subseteq Bs_iw'B$ , so

$$Bs_iw'B \cap BwBs_j \neq \emptyset$$

by the previous discussion. Now

$$wBs_j \subseteq Bws_jB \cup BwB$$

by (65.2), so  $Bs_iw'B$  is either  $Bws_jB$  or  $BwB$ . Then  $s_iw' = ws_j$  or  $s_iw' = w$  by (65.4). These are both easily seen to be impossible, and the result follows. Note that the first equality implies  $s_i = 1$ , which is ruled out by (65.3); this is the first use of that axiom.

We now have the complementary statement:

**(65.6) Proposition.** *If  $l(s_iw) \leq l(w)$ , where  $s_i \in S$  and  $w \in W$ , then  $s_iBw \cap BwB \neq \emptyset$ .*

*Proof.* By (65.2) we have  $s_iBs_i \subseteq B \cup Bs_iB$ , and  $s_iBs_i \cap Bs_iB \neq \emptyset$  by (65.3). Then  $s_iB \cap Bs_iBs_i \neq \emptyset$ , and hence

$$s_iBw \cap Bs_iBs_iw \neq \emptyset.$$

Since  $l(s_i s_i w) = l(w) \geq l(s_i w)$ , we have

$$Bs_iBs_iw \subseteq BwB$$

by (65.5); hence  $s_iBw \cap BwB \neq \emptyset$ , as required.

**(65.7) Corollary.** *Let  $w \in W$  and  $s_i \in S$ . Then*

- (i)  $l(s_i w) \neq l(w)$ .
- (ii)  $l(s_i w) = l(w) \pm 1$ .
- (iii)  $l(s_i w) < l(w) \Rightarrow s_i B \subseteq B w B w^{-1} B$ .

The proofs of (i) and (ii) are left as exercises, using (65.5) and (65.6). For (iii), we have  $s_i B w \cap B w B \neq \emptyset$ , and the result follows.

These apparently innocuous results are surprisingly powerful, as is shown by the next result, which will imply that the Weyl group of a finite group with a BN-pair is always a Coxeter group.

**(65.8) Proposition.** *The set of distinguished generators  $S$  of  $W$  satisfies the Exchange Condition (see (64.32)), namely: if the elements  $s_{i(0)}, \dots, s_{i(m)} \in S$  are such that*

$$l(s_{i(1)} \cdots s_{i(m)}) = m \quad \text{and} \quad l(s_{i(0)} s_{i(1)} \cdots s_{i(m)}) < m + 1,$$

then for some  $k$ ,  $1 \leq k \leq m$ , we have

$$s_{i(1)} \cdots s_{i(k)} = s_{i(0)} \cdots s_{i(k-1)}.$$

*Proof.* Let  $w \in W$ , and let  $w' = s_{j(1)} \cdots s_{j(p)}$  be a product of involutions from  $S$ . By repeated use of (65.2), we obtain

$$w B w' \subseteq \cup B w s_{j(q_1)} \cdots s_{j(q_t)} B,$$

where the union is taken over all subsequences of  $[1, p]$ ,

$$1 \leq q_1 < q_2 < \cdots < q_t \leq p.$$

Now let  $w = s_{i(1)} \cdots s_{i(m)}$ , so  $l(w) = m$  and  $l(s_{i(0)} w) < m + 1$  by hypothesis. Then by (65.7iii) and the preceding remark, we have

$$s_{i(0)} B \subseteq B w B w^{-1} B \subseteq \cup B w s_{i(p_1)} \cdots s_{i(p_k)} B,$$

where

$$m \geq p_1 > p_2 > \cdots > p_k \geq 1.$$

This implies, by (65.4), that

$$s_{i(0)} = w s_{i(p_1)} \cdots s_{i(p_k)}$$

for some subsequence  $\{p_i\}$  as above. Since  $l(s_{i(0)}) = 1$  and  $l(ws_i) = l(w) \pm 1$  by

(65.7ii), then necessarily  $k = m - 1$ , and so

$$s_{i(0)} = ws_{i(m)} \cdots \hat{s}_{i(j)} \cdots s_{i(1)}$$

with one factor omitted. This is the Exchange Condition.

As an immediate application we have the important result:

**(65.9) Theorem.** *Let  $W$  be the Weyl group of a finite group with a BN-pair, and let  $S$  be the set of distinguished generators of  $W$ , as in (65.1). Then  $(W, S)$  is a Coxeter system (see (64.17)).*

The proof is a direct application of (65.8) and the proof of (64.26).

### §65B. Examples of BN-Pairs

With some exceptions in low ranks, finite groups with BN-pairs tend to occur in infinite families  $\{G(\mathbb{F}_q)\}$ , parametrized by finite fields  $\mathbb{F}_q$ , with all the groups in the family having the same Weyl group. In this subsection, we shall construct such a family, namely the general linear groups  $\{GL_{n+1}(\mathbb{F}_q)\}$  for a fixed positive integer  $n$ , consisting of all invertible  $(n+1) \times (n+1)$ -matrices with entries in a finite field  $\mathbb{F}_q$ .

In this case, it is no more difficult to consider the groups

$$G = GL_{n+1}(K), \quad n \geq 1,$$

where  $K$  is an arbitrary field (of course,  $G$  may now be infinite). We define subgroups of  $G$  as follows:

$B$  = group of upper triangular matrices  $= \{(a_{ij}) \in G : a_{ij} = 0 \text{ if } i > j\}$ ,

$N$  = group of monomial matrices in  $G$ ,

$T$  = group of diagonal matrices in  $G$ ,

where a *monomial matrix* is an element  $g \in G$  such that each row and each column of  $g$  contains exactly one nonzero entry. Clearly  $T = B \cap N$ . We now prove, following Bourbaki [68]:

**(65.10) Theorem.** *The subgroups  $B$  and  $N$  defined above form a BN-pair in  $G = GL_{n+1}(K)$  of rank  $n$ , whose Weyl group  $W$  is isomorphic to the symmetric group  $S_{n+1}$ .*

*Proof.* Let  $\{e_1, \dots, e_{n+1}\}$  be a basis for the vector space  $K^{n+1}$  on which  $G$  acts. From elementary linear algebra, we know that  $G$  is generated by the diagonal matrices together with the elementary matrices

$$E_{ij}(c) = I + c e_{ij}, \quad i \neq j, \quad c \in K,$$

where  $\mathbf{e}_{ij}$  is a matrix with 1 in the  $(i, j)$  position and zeros elsewhere. Another elementary fact is that rows or columns of a matrix  $g \in G$  can be interchanged by left or right multiplication by permutation matrices; these belong to the subgroup  $N$ . The subgroup  $B$  contains all matrices  $\{\mathbf{E}_{ij}(c) : i < j, c \in K\}$ . Consider an arbitrary elementary matrix  $\mathbf{E}_{ij}(c)$ , for  $i \neq j$ . A moment's thought shows that there exist permutation matrices  $\mathbf{P}, \mathbf{Q} \in N$  such that  $\mathbf{P}\mathbf{E}_{ij}(c)\mathbf{Q} \in B$ . For example, the operations

$$\begin{pmatrix} 1 & 0 \\ c & 1 \end{pmatrix} \rightarrow \begin{pmatrix} c & 1 \\ 1 & 0 \end{pmatrix} \rightarrow \begin{pmatrix} 1 & c \\ 0 & 1 \end{pmatrix}$$

can be achieved by interchanging rows and columns, and hence by multiplication by elements of  $N$ . It follows from these remarks that  $G = \langle B, N \rangle$ , and (65.1i) is proved.

We have already noted that  $B \cap N = T$ . Let  $\langle v, w, \dots \rangle$  denote the subspace of  $K^{n+1}$  generated by vectors  $v, w, \dots$ . Each matrix  $n \in N$  permutes the lines (= one-dimensional subspaces)  $\langle e_1 \rangle, \dots, \langle e_{n+1} \rangle$ . It follows that there exists a homomorphism from  $N$  to the symmetric group  $S_{n+1}$  whose kernel is the diagonal subgroup  $T$ . Thus (65.1ii) is proved, and we have  $N/(B \cap N) \cong S_{n+1}$ , where  $N/(B \cap N)$  will turn out to be the Weyl group, once we have verified the other axioms.

By Exercise 64.1, the transpositions  $\{\tau_i = (i, i+1), 1 \leq i \leq n\}$  generate  $S_{n+1}$ . For each  $i$ , let  $\dot{s}_i \in N$  be the element that interchanges the basis vectors  $\{e_i, e_{i+1}\}$  and leaves the others fixed. The homomorphism  $N \rightarrow S_{n+1}$  maps  $\dot{s}_i$  onto  $\tau_i$ , for  $1 \leq i \leq n$ ; hence  $W = N/(B \cap N)$  is generated by the images  $s_i \in W$  of the elements  $\dot{s}_i$ ,  $1 \leq i \leq n$ , and so

$$N/(B \cap N) = \langle s_1, \dots, s_n \rangle, \quad s_i^2 = 1, \quad 1 \leq i \leq n.$$

We clearly have

$$\dot{s}_i B \dot{s}_i \neq B, \quad 1 \leq i \leq n,$$

and (65.3) holds.

It remains to prove (65.2), namely that

$$\dot{s}_i B \dot{w} \subseteq B \dot{w} B \cup B \dot{s}_i \dot{w} B$$

for each  $s_i$  and each  $w \in N/(B \cap N)$  (where, as usual,  $\dot{w}$  denotes a coset representative in  $N$  of the element  $w \in N/(B \cap N)$ ). It is clearly sufficient to prove

$$(65.11) \quad \dot{s}_i B \subseteq BB' \cup B \dot{s}_i B'$$

where  $B' = \dot{w} B \dot{w}^{-1}$ .

For each  $i$ ,  $1 \leq i \leq n$ , let  $G_i$  be the subgroup of  $G$  leaving invariant the two-dimensional subspace  $\langle e_i, e_{i+1} \rangle$  and fixing the other basis vectors. Then

$G_i \cong GL_2(K)$  and  $s_i \in G_i$ . Moreover, we have

$$(65.12) \quad G_i B = B G_i,$$

which is easily verified since both sides are characterized as the set of all elements  $g \in G$  such that  $ge_j \in \langle e_1, \dots, e_j \rangle$ , if  $j \neq i$ , and  $ge_i \in \langle e_1, \dots, e_{i+1} \rangle$ .

By (65.12),  $s_i B \subseteq B G_i$ , and hence (65.11) will follow once we prove that

$$G_i \subseteq BB' \cup B s_i B'.$$

For this, in turn, it suffices to show that

$$G_i \subseteq (B \cap G_i)(B' \cap G_i) \cup (B \cap G_i)s_i(B' \cap G_i).$$

If we identify  $G_i$  with  $GL_2(K)$ , then  $B \cap G_i$  is identified with the subgroup  $B_2$  of upper triangular matrices in  $GL_2(K)$ . Let  $B_2^-$  denote the group of lower triangular matrices in  $GL_2(K)$ .

Now consider  $B' \cap G_i = \dot{w}B\dot{w}^{-1} \cap G_i$ . We assert that this group is identified with either  $B_2$  or  $B_2^-$ ; the first case occurs when  $\dot{w}B\dot{w}^{-1} \cap G_i$  carries  $\langle e_i \rangle$  onto itself, while the second case occurs when  $\dot{w}B\dot{w}^{-1} \cap G_i$  carries  $\langle e_{i+1} \rangle$  to itself. To verify this assertion, we observe that the subgroup  $\dot{w}^{-1}G_i\dot{w}$  stabilizes the subspace  $\dot{w}^{-1}\langle e_i, e_{i+1} \rangle$  and fixes the lines  $\langle \dot{w}^{-1}e_k \rangle$ ,  $k \neq i, i+1$ . Then  $\dot{w}^{-1}\langle e_i \rangle = \langle e_k \rangle$ ,  $\dot{w}^{-1}\langle e_{i+1} \rangle = \langle e_l \rangle$  for some  $k \neq l$ ,  $1 \leq k, l \leq n+1$ , and  $B \cap \dot{w}^{-1}G_i\dot{w}$  fixes either  $\langle e_k \rangle$  or  $\langle e_l \rangle$  by the definition of  $B$ . This means that  $\dot{w}B\dot{w}^{-1} \cap G_i$  stabilizes either  $\langle e_i \rangle$  or  $\langle e_{i+1} \rangle$ , proving our assertion.

In order to complete the proof, it is therefore sufficient to prove the two statements:

$$GL_2(K) = B_2 \cup B_2 s B_2, \quad \text{and} \quad GL_2(K) = B_2 B_2^- \cup B_2 s B_2^-,$$

where  $s = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ . The first is easily shown as follows. If  $g \in GL_2(K)$  and  $g \notin B_2$ , then

$$g = \begin{pmatrix} a & b \\ c & d \end{pmatrix}, \quad \text{where } c \neq 0.$$

Then  $E_{12}(t) \in B_2$  for all  $t \in K$ , and

$$E_{12}(-ac^{-1})g = \begin{pmatrix} 0 & * \\ * & * \end{pmatrix}.$$

It follows that

$$s E_{12}(-ac^{-1})g \in B,$$

and  $g \in B_2 s B_2$ , as required.

For the second statement, we note that  $s^2 = 1$  and  $sB_2s = B_2^-$ . Using the first statement, we have

$$GL_2(K) = GL_2(K)\dot{s} = B_2\dot{s} \cup B_2\dot{s}B_2\dot{s} \subseteq B_2\dot{s} \cup B_2B_2^-.$$

This proves the second statement, and completes the proof of the theorem.

**Remarks.** We leave it to the reader to check that the preceding argument, followed step by step, also produces a BN-pair in the *unimodular group*

$$SL_{n+1}(K) = \{g \in GL_{n+1}(K) : \det g = 1\},$$

where now the subgroups  $B$ ,  $N$ , and  $T$  are the intersections with  $SL_{n+1}(K)$  of the corresponding groups for  $GL_{n+1}(K)$ . Since the center  $Z(SL_{n+1}(K))$  consists of the scalar matrices  $\{\xi \cdot \mathbf{I}; \xi \in K, \xi^{n+1} = 1\}$ , we see that  $Z(SL_{n+1}(K)) \leq T$ . It follows that the *projective unimodular group*

$$PSL_{n+1}(K) = SL_{n+1}(K)/Z(SL_{n+1}(K))$$

also has a BN-pair, in which the subgroups  $B$ ,  $N$ , and  $T$  are the images in  $PSL_{n+1}(K)$  of the corresponding groups in  $SL_{n+1}(K)$ , under the natural map  $SL_{n+1}(K) \rightarrow PSL_{n+1}(K)$ .

The other classical groups over finite fields—the orthogonal, symplectic, and unitary groups—also have BN-pairs.\* These are examples of Chevalley groups. The Chevalley groups can all be constructed by a uniform procedure. The general method used for their construction also produces a BN-pair in each case (see Chevalley [55], Steinberg [67], or Carter [72b]).

The finite Chevalley groups can also be obtained from the groups of  $\mathbb{F}_q$ -rational points on connected reductive affine algebraic groups defined over finite fields  $\mathbb{F}_q$  (see Steinberg [67], [68], Borel–Tits [65]).

### §65C. Parabolic Subgroups of Finite Groups with BN-Pairs

Throughout this subsection,  $G$  denotes a finite group with a BN-pair. We let  $W$  denote the Weyl group of  $G$ , and  $S$  the set of distinguished generators in  $W$ . By (65.9), the pair  $(W, S)$  is a finite Coxeter system, so we may apply the results of §§ 64B, C to  $(W, S)$ . As in §65A, we use the notation  $\dot{w}$  to denote a coset representative in  $N$  of an element  $w \in W$ .

**(65.13) Theorem (Tits [62]).** *Let  $J \subseteq S$ , let  $W_J$  be the parabolic subgroup of  $W$  associated with  $J$ , as in (64.35), and set  $P_J = BW_JB$ . Then  $P_J$  is a subgroup of  $G$  containing  $B$ , and moreover, every subgroup containing  $B$  coincides with some  $P_J$ .*

\*For an elementary construction of BN-pairs in the other classical groups, along the lines of the preceding discussion, see Bourbaki [68, Ex. 20, p. 53].

*Proof.* In order to prove that  $P_J$  is a subgroup, it is sufficient to check that  $gP_J = P_J$  for each  $g \in P_J$ . This is clearly true if  $g \in B$ , so it is enough to verify that  $wP_J = P_J$  for each  $w \in W_J$ . Since  $W_J$  is generated by  $J$ , we only have to prove that  $sP_J = P_J$  for  $s \in J$ , and this is immediate by (65.2).

To show that the  $\{P_J\}$  are the only subgroups containing  $B$ , we first prove:

**(65.14) Lemma.** Let  $w = s_{i(1)}, \dots, s_{i(m)}$  be a reduced product of elements of  $S$ , and let  $J = \{s_{i(1)}, \dots, s_{i(m)}\}$ . Then

$$\langle B, \dot{w} \rangle = \langle B, \dot{w}B\dot{w}^{-1} \rangle = P_J.$$

*Proof.* We clearly have  $\langle B, \dot{w}B\dot{w}^{-1} \rangle \leq \langle B, \dot{w} \rangle \leq P_J$ . Since  $l(s_{i(1)}w) < l(w)$ , we obtain

$$s_{i(1)}B \subseteq \langle B, \dot{w}B\dot{w}^{-1} \rangle$$

by (65.7iii). Continuing, we have  $l(s_{i(2)}s_{i(1)}w) < l(s_{i(1)}w)$ , so

$$s_{i(2)}B \subseteq \langle B, \dot{s}_{i(1)}\dot{w}B\dot{w}^{-1}\dot{s}_{i(1)}^{-1} \rangle \subseteq \langle B, \dot{w}B\dot{w}^{-1} \rangle,$$

by the first step. We obtain finally  $P_J \subseteq \langle B, \dot{w}B\dot{w}^{-1} \rangle$ , completing the proof of the lemma.

We can now finish the proof of the theorem. Any subgroup  $Q$  containing  $B$  is a union of  $(B, B)$ -double cosets, so by (65.4) we have

$$Q = \cup B\dot{w}B, \quad \dot{w} \in N \cap Q.$$

Then  $Q = \langle B, \dot{w} : \dot{w} \in N \cap Q \rangle$ . By Lemma 65.14, each subgroup  $\langle B, \dot{w} \rangle = P_J$  for some  $J$  and each  $P_J$  is contained in  $Q$  (for  $\dot{w} \in N \cap Q$ ). Letting

$$I = \bigcup_{P_J \subseteq Q} J,$$

we have  $P_I \subseteq Q$  and  $Q \subseteq P_I$ , completing the proof of (65.13).

**(65.15) Definition.** The subgroups of  $G$  containing a fixed Borel subgroup  $B$  of  $G$  are called *standard parabolic subgroups* of  $G$ ; the set of all *parabolic subgroups* of  $G$  consists of a set of standard parabolic subgroups, and their  $G$ -conjugates. In particular,  $B$  is the *standard Borel subgroup*.

By (65.13), the standard parabolic subgroups  $P \geq B$  are the subgroups  $\{P_I\}_{I \subseteq S}$ . Each standard parabolic subgroup  $P_I$  has a  $BN$ -pair with Borel subgroup  $B$  and Weyl group  $W_I$ .

We next have:

**(65.16) Proposition.** Let  $w \in W$ . Then  $w$  belongs to the set of distinguished

generators  $S$  of  $W$  if and only if  $w \neq 1$  and

$$B \cup BwB$$

is a subgroup of  $G$ .

The proof is an easy application of Lemma 65.14, and is left to the reader. Note that this result proves the uniqueness of the set of distinguished generators  $S$ . The next result will imply that  $S$  is a minimal set of generators (see also (64.37v)).

**(65.17) Proposition.** *Let  $I, J \subseteq S$ . Then*

$$(i) \quad I \subseteq J \Leftrightarrow P_I \leq P_J.$$

$$(ii) \quad P_I \cap P_J = P_{I \cap J}.$$

(iii) *The map  $I \rightarrow P_I$  gives a bijection from the subsets of  $S$  onto the set of standard parabolic subgroups.*

*Proof.* (i) Suppose  $P_I \leq P_J$ , and let  $s \in I$ . Then  $BsB = BwB$  for some  $w \in W_J$ ; hence  $s \in W_J$  and  $s \in J$  by (64.34). The reverse implication is clear, and (i) is proved.

(ii) By (65.13),  $P_I \cap P_J = P_K$  for some  $K \subseteq S$ . Then  $K \subseteq I \cap J$  by part (i). On the other hand,  $P_{I \cap J} \subseteq P_K$ , so  $I \cap J \subseteq K$ , also by (i).

(iii) The map  $I \rightarrow P_I$  is surjective, by (65.13). It is also injective, since  $P_I = P_J$  implies  $I = J$ , by part (i), completing the proof.

**(65.18) Corollary.** *The set  $S$  is a minimal set of generators of  $W$ .*

**(65.19) Theorem.** *Each parabolic subgroup  $P$  is its own normalizer in  $G$ , that is,  $N_G(P) = P$ . More generally, if  $P$  and  $Q$  are parabolic subgroups such that  $P \cap Q$  is parabolic, then*

$$gPg^{-1} \leq Q \Leftrightarrow P \leq Q \text{ and } g \in Q.$$

*Proof.* For the first statement, we may assume  $P = P_I$  for some  $I \subseteq S$ . Then  $N_G(P_I)$  contains  $B$ , so  $N_G(P_I) = P_J$  for  $J \supseteq I$ , by (65.13) and (65.17). Now let  $s \in J$ ; then  $sBs^{-1} \leq P_I$ , since  $B \leq P_I$ . Therefore

$$\langle B, sBs^{-1} \rangle \leq P_I,$$

so  $s \in I$ , by (65.14) and (65.17), proving the first statement.

To prove the second part, suppose that  $P \cap Q$  is parabolic. We may then assume that  $P = P_I$ ,  $Q = P_J$  for some  $I, J \subseteq S$ , by definition and by (65.13). It is obvious that if  $P_I \leq P_J$  and  $g \in P_J$ , then  $gP_Ig^{-1} \leq P_J$ . Conversely, let  $gP_Ig^{-1} \leq P_J$  where  $I, J \subseteq S$ , and  $g \in G$ . By (65.4),  $g \in BwB$  for some  $w \in W$ , and since  $B \leq P_I \cap P_J$ , we have  $wBw^{-1} \leq P_J$ ; hence  $\langle B, wBw^{-1} \rangle \leq P_J$ , and  $g \in BwB \leq P_J$ , by (65.14). We now have  $gP_Ig^{-1} \leq P_J$ , and  $g \in P_J$ , so  $P_I \leq P_J$ , completing the proof.

**(65.20) Corollary.** *Each parabolic subgroup of  $G$  is conjugate to a unique standard parabolic subgroup  $P_I$ , for some  $I \subseteq S$ .*

The last result in this section shows a further connection between parabolic subgroups of  $G$  and parabolic subgroups of  $W$ .

**(65.21) Theorem.** *Let  $I, J \subseteq S$ . There exists a bijection of double cosets*

$$W_I \backslash W / W_J \leftrightarrow P_I \backslash G / P_J$$

given by

$$W_I w W_J \leftrightarrow BW_I w W_J B = P_I w P_J.$$

*Proof.* Since  $P_I = BW_I B$  and  $P_J = BW_J B$ , we have

$$(65.22) \quad BW_I w W_J B \subseteq P_I w P_J.$$

We now prove the reverse inclusion. Let  $w'$  range over all the elements of  $W_I$ , and  $w''$  over  $W_J$ . Since

$$P_I = \bigcup_{w'} Bw' B \quad \text{and} \quad P_J = \bigcup_{w''} Bw'' B,$$

we need only establish that

$$Bw' Bw Bw'' B \subseteq Bw' ww'' B.$$

This is immediate by repeated use of (65.2). We have thus established the equality of the two expressions in (65.22). The existence of the bijection now follows from the uniqueness part of the Bruhat decomposition (65.4), completing the proof.

## §66. HOMOLOGY REPRESENTATIONS OF FINITE GROUPS WITH BN-PAIRS

This section contains a striking illustration of the close connection between the representation theory of a finite group of Lie type  $G$  and the representations of the Weyl group  $W$  of  $G$ . The connection arises in this case through the comparison of the posets of proper parabolic subgroups of  $W$  and  $G$ , respectively, and the representations of  $W$  and  $G$  on their rational homology. The section contains a general introduction to representations of finite groups on the homology of simplicial complexes, followed by a discussion of the particular representations obtained in the case of  $W$  and  $G$ .

### §66A. Homology Representations of Finite Groups

In this subsection, we present an introduction to representations of finite groups arising from their actions on posets and finite simplicial complexes. This work

extends the theory of permutation representations afforded by group actions on sets, already discussed in §1B and §10. Our approach follows Curtis-Lehrer [81], which in turn is based partly on ideas from Quillen [78], Lusztig [74], Bredon [72], and Curtis [80b]. For further discussion of assumed results from algebraic topology, see Hilton-Wylie [60], Eilenberg-Steenrod [52], and Godement [64].

The contents of this subsection, concentrating on the Lefschetz character and the endomorphism algebra of a homology representation, are applied in §66B to give a geometric interpretation of the sign representation of a finite g.g.r., and in §66C to the Steinberg representation of a finite group with a *BN*-pair.

We begin with some definitions. An (abstract) *simplicial complex*  $\Sigma$  consists of a set of points  $\{x, y, \dots\}$ , called *vertices*, together with certain finite, non-empty sets of vertices  $\{\sigma\}$  called *simplices*, satisfying the axioms that

- (i) each singleton set  $\{x\}$  is a simplex, and
- (ii) each non-empty subset  $\sigma'$  of a simplex  $\sigma$  is also a simplex.

We shall restrict our attention mainly to *finite* simplicial complexes, that is, complexes  $\Sigma$  whose vertex set is finite.

An *r-simplex* of  $\Sigma$  is a simplex  $\sigma = \{x_0, x_1, \dots, x_r\}$  consisting of  $r + 1$  vertices. A *simplicial map*  $f: \Sigma \rightarrow \Sigma'$  of simplicial complexes is a map  $f$  from the vertices of  $\Sigma$  to those of  $\Sigma'$ , such that if  $\{x_0, x_1, \dots, x_r\}$  is an *r*-simplex in  $\Sigma$ , then  $\{f(x_0), f(x_1), \dots, f(x_r)\}$  are the vertices (possibly with repetitions) of a simplex in  $\Sigma'$ . The finite simplicial complexes form a category, in which morphisms are simplicial maps.

Now let  $G$  be a finite group; a simplicial complex  $\Sigma$  is called a *G-complex*, and  $G$  is said to *act* on  $\Sigma$ , if the vertices of  $\Sigma$  form a *G-set* (see (1.18)), and if the action of  $G$  carries simplices onto simplices.

The representation theory of *G*-complexes will turn out to be equivalent to the conceptually simpler theory of *G*-posets. A *poset*  $(X, \leq)$  is a partially ordered set with a reflexive, antisymmetric, transitive relation  $\leq$ . A *G-poset* is a poset  $(X, \leq)$ , with  $X$  a *G-set* such that the *G*-action preserves the order relation: if  $x \leq y$ , then  $gx \leq gy$ , for  $x, y \in X$  and  $g \in G$ .

Each *G*-poset  $X$  defines a *G*-complex  $\Sigma(X)$ , whose vertices are the elements of  $X$ , and whose simplices are *chains* in  $X$  (i.e., finite totally ordered subsets of  $X$ ).

The finite *G*-complexes form a category, in which the objects are *G*-complexes, and the morphisms are simplicial maps preserving the *G*-action. The *G*-posets also form a category in the obvious way, namely, the morphisms are *G*-maps preserving the partial order structure. Then the rule, which assigns to each *G*-poset  $X$  the corresponding complex  $\Sigma(X)$ , is a functor from one category to the other.

Clearly, *G*-posets are abundant in group theory; any family of subgroups of a group  $G$ , closed under conjugation, is a *G*-poset, with the order relation given by inclusion and the *G*-action by conjugation. Our object is to assign a *Q*-representation of  $G$  to each such *G*-poset, and to investigate some of its properties. In particular, we need to discuss the poset structure of *G*-orbits, which is more subtle than the study of *G*-orbits in *G*-sets, and which can best be understood by introducing some geometrical concepts.

To each simplicial complex  $\Sigma$  we may associate an *underlying topological space*, or *geometric realization*, denoted by  $|\Sigma|$ . This geometric realization  $|\Sigma|$  is defined to be the set of all real-valued functions  $p$ , defined on the vertex set of  $\Sigma$ , and satisfying the three conditions:

$$\begin{cases} p(x) \geq 0 \text{ for all vertices } x \text{ of } \Sigma, \\ \sum_x p(x) = 1, \\ \text{supp } p \text{ is a simplex of } \Sigma, \end{cases}$$

where the *support* of  $p$  is defined by

$$\text{supp } p = \{x : p(x) \neq 0\}.$$

For each  $n$ -simplex  $\sigma$  of  $\Sigma$ , denote by  $|\sigma|$  the subset of  $|\Sigma|$  defined by

$$|\sigma| = \{p \in |\Sigma| : \text{supp } p \subseteq \sigma\}.$$

We now proceed to topologize  $|\sigma|$ , by making its points correspond to those inside a standard  $n$ -simplex in  $\mathbb{R}^n$ . Specifically, let  $e_1, \dots, e_n$  be an orthonormal basis for  $\mathbb{R}^n$ , and consider the standard  $n$ -simplex in  $\mathbb{R}^n$  with vertices 0 and the endpoints of the vectors  $e_1, \dots, e_n$ . Each point  $p \in |\sigma|$  determines a point in this standard  $n$ -simplex, namely, the endpoint of the vector  $\sum_{i=1}^n p(x_i)e_i$ , where  $\sigma = \{x_0, x_1, \dots, x_n\}$ . In view of the condition  $\sum_{i=0}^n p(x_i) = 1$ , the correspondence between the points of  $|\sigma|$  and those of the standard  $n$ -simplex in  $\mathbb{R}^n$ , is a bijection. We then topologize  $|\sigma|$  by using this bijection, and the natural topology in  $\mathbb{R}^n$ . Finally, we topologize the geometrical realization  $\Sigma \rightarrow |\Sigma|$  by choosing, as the family of open sets, those subsets  $U$  of  $|\Sigma|$  such that  $U \cap |\sigma|$  is open in  $|\sigma|$  for every simplex  $\sigma$  of  $\Sigma$ .

It will be convenient to write each point  $p \in |\Sigma|$  as a formal sum  $p = \sum_x p(x)x$ , in which  $x$  ranges over the vertex set of  $\Sigma$ . The correspondence, which carries the simplicial complex  $\Sigma$  onto its geometric realization  $|\Sigma|$ , is a functor from the category of simplicial complexes and simplicial maps to the category of topological spaces and continuous maps. A simplicial map  $f : \Sigma \rightarrow \Sigma'$  yields a continuous map  $|f| : |\Sigma| \rightarrow |\Sigma'|$ , defined by

$$p \in |\Sigma| \rightarrow |f|p = \sum p(x)f(x) \in |\Sigma'|.$$

Thus we have a composite functor

$$X \rightarrow \Sigma(X) \rightarrow |\Sigma(X)|,$$

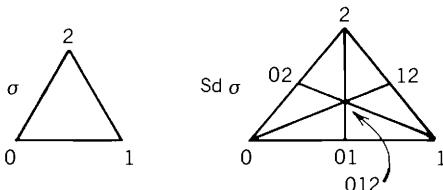
which carries the finite  $G$ -poset  $X$  onto the geometrical realization  $|\Sigma(X)|$  of the finite simplicial complex  $\Sigma(X)$ . Here,  $G$  is as usual some finite group.

A useful construction is the *barycentric subdivision*  $Sd\Sigma$  of a simplicial complex  $\Sigma$ . This is the poset whose elements are the simplices  $\sigma$  of  $\Sigma$ , and the order

relation is inclusion of simplices:  $\sigma' \leq \sigma$  if  $\sigma' \subseteq \sigma$ . It is clear that if  $\Sigma$  is a  $G$ -complex, then  $Sd \Sigma$  is a  $G$ -poset, with the same  $G$ -action. The following result explains our previous remark that the representation theory of a finite group  $G$  on  $G$ -complexes is equivalent to its representation theory on  $G$ -posets.

**(66.1) Proposition.** *Let  $\Sigma$  be a  $G$ -complex, and  $X = Sd \Sigma$  be the  $G$ -poset defined above. Then there is a  $G$ -equivariant\* homeomorphism between the underlying topological spaces of  $\Sigma$  and of the  $G$ -complex  $\Sigma(Sd \Sigma)$  associated with the  $G$ -poset  $Sd \Sigma$ .*

*Sketch of Proof.* It is sufficient to consider the case of a simplex  $\sigma$ , and the argument in this case can easily be derived from the following example. Here  $\sigma$



has vertices 0, 1, 2, 1-simplices 01, 12, 02, and 2-simplex 012. Then  $\Sigma(Sd \Sigma)$  has vertices corresponding to the simplices of  $\sigma$ , 1-simplices (0, 01), (1, 01), (1, 12), (2, 12), etc., and 2-simplices (0, 01, 012), (1, 01, 012), etc. One then defines a canonical homeomorphism from  $|Sd \sigma|$  to  $|\sigma|$ , using barycentric coordinates in the corresponding simplices in Euclidean space, and that preserves a group action if one is present. (For further details, see Eilenberg–Steenrod [52].)

The preceding result allows us to concentrate on  $G$ -posets rather than  $G$ -complexes. For a  $G$ -poset  $X$ , the *barycentric subdivision*  $Sd X$  is the  $G$ -poset whose elements are the chains in  $X$ , and the order relation is inclusion of one chain in another, with the same  $G$ -action. It is also useful to introduce the notation  $|X|$  for the underlying topological space of the simplicial complex  $\Sigma(X)$ . Then by (66.1) and the identifications we have made, there exists a  $G$ -equivariant homeomorphism

$$(66.2) \quad |X| \simeq |Sd X|.$$

Another  $G$ -poset related to a given  $G$ -poset  $X$  is the *opposite poset*  $X^\circ$ , consisting of the same elements as  $X$ , with the order reversed. We clearly have  $\Sigma X = \Sigma X^\circ$ ,  $Sd X = Sd X^\circ$ , and there is a  $G$ -equivariant homeomorphism  $|X| \simeq |X^\circ|$ .

We are now in a position to give geometric interpretations of fixed points and orbits in  $G$ -posets.

**(66.3) Proposition.** *Let  $X$  be a  $G$ -poset, for a group  $G$ , and let  $g \in G$ . Then  $g$  fixes a simplex  $\sigma$  in  $Sd X$  if and only if  $g$  fixes all the vertices of  $\sigma$ . Moreover, there exists a*

\*A  $G$ -equivariant map between two sets with  $G$ -actions is a map preserving the  $G$ -action.

homeomorphism  $|X^g| \simeq |X|^g$ , where  $X^g$  denotes the subposet of  $X$  consisting of elements fixed by  $g$ , and  $|X|^g$  is the fixed point set of  $g$  in the topological space  $|X|$ .

*Proof.* Recall that  $g \in G$  preserves the order relation in  $X$ , by definition. The first statement is clear, since  $g$  fixes a chain in  $X$  if and only if it fixes the elements of the chain. For the second part, we show that each element  $p \in |X|^g$  is in the geometric realization of a unique simplex fixed by  $g$ , which is then a simplex in  $\Sigma(X^g)$ , by the first remark. The simplex in  $\Sigma(X^g)$ , whose existence is claimed, is the unique minimal simplex  $\sigma$  with  $p$  in the interior of  $|\sigma|$ . Since  $g$  fixes  $p$ , and  $g$  is a simplicial map, it follows that  $g$  maps the simplex  $\sigma$  to itself, as required. It is then straightforward to construct a homeomorphism  $|X^g| \simeq |X|^g$ .

We now come to an important concept, similar to one introduced by Bredon [72] for  $G$ -complexes, that allows us to construct orbit posets.

**(66.4) Definition.** Let  $X$  be a  $G$ -poset. Then  $X$  is said to be *regular* (with respect to the  $G$ -action) if for all  $x, y \in X$ , and  $g \in G$ , the relations  $x \leq y$  and  $gx \leq y$  imply that  $gx = x$ .

The reader should check that, even in the simplest cases, a  $G$ -poset may fail to be regular. Nevertheless, we have:

**(66.5) Proposition.** Let  $X$  be an arbitrary  $G$ -poset. Then the second barycentric subdivision  $Sd^2 X$  is a regular  $G$ -poset.\*

*Proof.* The elements in  $Sd X$  are chains, denoted by  $(x) = (x_0 < x_1 < \dots < x_m)$ , and the elements of  $Sd^2 X$  are chains of chains  $\{(Y^0) \subset (Y^1) \subset \dots \subset (Y^n)\}$ , where  $(Y^i)$  is a chain  $(y_{i0}^i < \dots < y_{id_i}^i)$ , and the order relation is inclusion. Note that  $\text{card}(Y^0) < \text{card}(Y^1) < \dots < \text{card}(Y^n)$ . It follows that if an element  $g \in G$  carries one subchain  $(Y^{i_0}) \subset \dots \subset (Y^{i_m})$  to another  $(Y^{j_0}) \subset \dots \subset (Y^{j_m})$ , then we have  $\text{card}(Y^{i_0}) = \text{card}(Y^{j_0}), \dots, \text{card}(Y^{i_m}) = \text{card}(Y^{j_m})$ , since the action of  $g$  preserves cardinality of subsets of  $(Y^n)$ . Therefore  $(Y^{i_0}) = (Y^{j_0}), \dots, (Y^{i_m}) = (Y^{j_m})$ , since the element  $(Y^0) \subset \dots \subset (Y^n)$  of  $Sd^2 X$  has a unique element  $(Y^i)$  of a given cardinality. This completes the proof.

For a  $G$ -poset  $X$ , it follows from (66.2) that the structure of the underlying topological space  $|X|$  and the action of  $G$  on this space are unchanged (up to homeomorphism) when  $X$  is replaced by  $Sd^2 X$ . Since  $Sd^2 X$  is a regular  $G$ -poset by the preceding result, it therefore suffices for us to consider regular  $G$ -posets in what follows.

For a regular  $G$ -poset  $X$ , we now define the *orbit poset*

$$\bar{X} = G \setminus X$$

as the poset whose elements are  $G$ -orbits  $\bar{x} = Gx$  of elements  $x$  of  $X$ , with the order

\*As an exercise, the reader can check that if  $X$  is a finite  $G$ -poset, then  $Sd X$  is regular.

relation  $\bar{x} \leq \bar{y}$  provided that  $x_0 \leq y_0$  for some  $x_0 \in \bar{x}$  and  $y_0 \in \bar{y}$ . The proof that  $\bar{x} \leq \bar{y}$  is a well-defined order relation is left to the reader.

It is entirely possible for the opposite poset  $X^\circ$  to be regular, while  $X$  is not regular (this occurs, for example, in the case of the Coxeter poset defined in (66.25)). It is clear that if either  $X$  or  $X^\circ$  is regular, then the orbit poset  $\bar{X}$  is well defined.

**(66.6) Proposition.** *Let  $X$  be a regular G-poset. Then  $\text{Sd } X$  is regular, and the map*

$$\psi: \overline{x_0 < x_1 < \dots < x_m} \mapsto \bar{x}_0 < \bar{x}_1 < \dots < \bar{x}_m, \quad x_i \in X,$$

*defines an isomorphism of posets  $\overline{\text{Sd } X} \cong \text{Sd } \bar{X}$ .*

*Proof.* We show first that  $\text{Sd } X$  is regular. For suppose that  $(x), (y)$  are chains in  $X$ , with  $(x) \leq (y)$ ,  $g(x) \leq (y)$  in  $\text{Sd } X$ , for some  $g \in G$ . Then we obtain  $(x) = g(x)$ , as desired, by applying the regularity condition to the maximal element of  $(y)$ . The map  $\psi$  defined above is clearly a map of posets, and is surjective. Now suppose we have two chains

$$y_0 < y_1 < \dots < y_m \quad \text{and} \quad y'_0 < y'_1 < \dots < y'_m,$$

where  $\bar{y}_i = \bar{y}'_i$  for  $0 \leq i \leq m$ . Then for each  $i$ , we may write  $y'_i = g_i y_i$  with  $g_i \in G$ . Therefore  $g_i y_i = y'_i \leq y'_m = g_m y_m$ , so  $g_m^{-1} g_i y_i \leq y_m$ . Since  $y_i \leq y_m$ , we deduce that  $g_m^{-1} g_i y_i = y_i$ , by regularity. It follows that

$$g_m(y_0 < \dots < y_m) = y'_0 < \dots < y'_m,$$

completing the proof.

**(66.7) Corollary.** *Let  $\bar{x}_0 < \dots < \bar{x}_m$  be a chain in the orbit poset  $\bar{X}$ . Then the set of all chains  $y_0 < \dots < y_m$  in  $X$  lying over  $\bar{x}_0 < \dots < \bar{x}_m$  (in the sense that  $y_i \in \bar{x}_i$ ,  $0 \leq i \leq m$ ), is a single  $G$ -orbit in  $\text{Sd } X$ .*

**(66.8) Proposition.** *Let  $X$  be a finite regular G-poset. Then  $|\bar{X}|$  is homeomorphic to the topological orbit space  $G \backslash |X|$  of  $G$ -orbits on  $|X|$ .*

*Proof.* We first recall that if a discrete group  $G$  acts on a topological space  $Z$ , then the topology in the orbit space  $\bar{Z}$  is defined by letting  $U \subseteq \bar{Z}$  be open in  $\bar{Z}$  whenever  $\pi^{-1}U$  is open in  $Z$ , where  $\pi: Z \rightarrow \bar{Z}$  is the natural map. This construction has the universal property that if  $f: Z \rightarrow W$  is a continuous map from  $Z$  to a topological space  $W$ , which is constant on  $G$ -orbits, then there exists a continuous map  $\bar{f}: \bar{Z} \rightarrow W$  making the following diagram commutative:

$$\begin{array}{ccc} Z & \xrightarrow{f} & W \\ \pi \searrow & \nearrow \bar{f} & \\ \bar{Z} & & \end{array}$$

In our case,  $x \in X \rightarrow \bar{x} \in \bar{X}$  is a map of posets, so the composite functor  $X \rightarrow \Sigma(X) \rightarrow |\Sigma(X)| = |X|$  defines a continuous map  $\varphi: |X| \rightarrow |\bar{X}|$ , given by

$$\varphi(\sum p(x)x) = \sum p(x)\bar{x}, \quad \text{for } p \in |X|.$$

Since the action of  $G$  on  $|X|$  is defined by

$$|g|(\sum p(x)x) = \sum p(x)gx, \quad g \in G,$$

it follows that  $\varphi$  is constant on  $G$ -orbits in  $|X|$ , and hence defines a continuous map  $\bar{\varphi}: G \setminus |X| \rightarrow |\bar{X}|$ , given by

$$\bar{\varphi}(\overline{\sum p(x)x}) = \sum p(x)\bar{x}.$$

Then  $\bar{\varphi}$  is surjective, and since  $G \setminus |X|$  is a compact Hausdorff space,  $\bar{\varphi}$  will be a homeomorphism if it is injective. Now let  $\varphi(p') = \varphi(p'')$ , for  $p', p'' \in |X|$ ; we shall prove that  $p'$  and  $p''$  lie in the same  $G$ -orbit. We may assume  $p' = \sum p'(x)x$ ,  $p'' = \sum p''(y)y$ , where the supports of  $p'$  and  $p''$  are strictly increasing chains in  $X$  lying over the chain in  $\bar{X}$  supporting  $\varphi(p') = \varphi(p'')$ . By (66.7), we have  $\text{supp } p' = g \text{ supp } p''$  for some  $g \in G$ , and it follows that  $p' = g \cdot p''$ , since  $\varphi(p') = \varphi(p'')$  implies  $p'(x) = p''(y)$  if  $\bar{x} = \bar{y}$ . Thus  $\bar{\varphi}$  is injective, and the result follows.

**(66.9) Definition.** Let  $X$  and  $Y$  be  $G$ -posets. Their *cartesian product*  $X \times Y$  is the  $G$ -poset on the cartesian product of the sets  $X$  and  $Y$ , with the order relation

$$(x, y) \leq (x', y') \quad \text{if and only if } x \leq x' \quad \text{and} \quad y \leq y', \quad \text{for } x, x' \in X \quad \text{and} \quad y, y' \in Y.$$

The  $G$ -action on  $X \times Y$  is diagonal action:

$$g(x, y) = (gx, gy), \quad \text{for all } x \in X, y \in Y, g \in G.$$

We quote without proof (see Eilenberg–Steenrod [52, II, §8]):

**(66.10) Proposition.** *Let  $X$  and  $Y$  be  $G$ -posets. There exists a  $G$ -equivariant homeomorphism*

$$|X \times Y| \simeq |X| \times |Y|.$$

With these topological preliminaries out of the way, we now turn to homology representations. We first recall that a *chain complex*  $C$  over a field  $K$  is a graded vector space

$$C = \bigoplus_{r=0}^{\infty} C_r,$$

with the  $\{C_r\}$  subspaces of  $C$ , together with a *boundary homomorphism*  $\partial: C \rightarrow C$ ,

which is a  $K$ -endomorphism such that

$$\partial C_r \subseteq C_{r-1} \quad \text{for } r \geq 1, \quad \partial C_0 = 0, \quad \text{and} \quad \partial^2 = 0.$$

Then  $\text{im } \partial \subseteq \ker \partial$ , and the quotient

$$H_*(C) = \ker \partial / \text{im } \partial = \bigoplus_{r=0}^{\infty} H_r(C)$$

is the *homology group* of  $C$ . Clearly  $H_*(C)$  is also a graded vector space, with

$$H_r(C) = (\ker \partial|_{C_r}) / (\text{im } \partial|_{C_{r+1}}) \quad \text{for } r \geq 0.$$

A finite group  $G$  is said to act on a chain complex  $C$  if each subspace  $C_r$  is a f.d.  $KG$ -module and if  $\partial$  commutes with the action of  $G$ . We refer to  $C$  as a *chain complex with  $G$ -action* in this case, and then the homology spaces  $\{H_r(C)\}$  are  $KG$ -modules, affording what we shall call *homology representations* of  $G$ .

Now let  $X$  be a  $G$ -poset, and  $K$  a field. We shall define a chain complex  $C(X)$  with  $G$ -action, as follows. For  $r \geq 0$ , the subspace  $C_r(X)$  of  $r$ -chains has a  $K$ -basis  $\{c_\sigma\}$ , indexed by  $r$ -simplices  $\sigma = (x_0 < x_1 < \dots < x_r)$  in  $\Sigma(X)$ . The action of  $G$  is given by its permutation action on the  $r$ -chains:

$$gc_\sigma = c_{g\sigma}, \quad \text{for } \sigma \text{ as above, and } g \in G.$$

The boundary homomorphism  $\partial: C_r(X) \rightarrow C_{r-1}(X)$  is given by

$$\partial c_\sigma = \sum_{i=0}^r (-1)^i c_{\sigma_i}$$

where if  $\sigma = (x_0 < \dots < x_r)$ , then  $\sigma_i = (x_0 < \dots < \hat{x}_i < \dots < x_r)$  is the  $i$ -th face of  $\sigma$ , for  $0 \leq i \leq r$ ; as usual,  $\hat{x}_i$  denotes the omission of  $x_i$ . The vector space  $C_r(X)$  is called the *vector space of  $r$ -chains*, where an  $r$ -chain is a formal linear combination of  $r$ -simplices with coefficients in  $K$ . It is easily verified that  $\partial^2 = 0$ , so that  $C(X)$  is indeed a chain complex with  $G$ -action, and the resulting homology representation

$$H_*(X) = \bigoplus_{r=0}^{\infty} H_r(X),$$

where  $H_r(X)$  means  $H_r(C(X))$ , is called the *homology representation* associated with the  $G$ -poset  $X$ .

The preceding discussion shows that the homology modules  $\{H_r(X)\}$  associated with a  $G$ -poset  $X$  are the same as the  $KG$ -modules arising from the homology of the simplicial complex  $\Sigma X$ , over the field  $K$ . These homology modules, in turn, coincide with the singular homology modules of the underlying topological space  $|X|$ , with the  $G$ -action defined as above. In particular, these

remarks imply, by (66.5) and (66.1), that a  $G$ -poset  $X$  and its barycentric subdivision  $\text{Sd } X$  afford the same homology representations, so there is no loss of generality in restricting our discussion to homology representations associated with regular  $G$ -posets (see (66.4)).

We now seek to define the character of a homology representation  $H_*(X)$ , whose properties should generalize those of the permutation character associated with a  $G$ -set. (For example, we recall that the value of a permutation character on  $g \in G$  is the number of fixed points of  $g$  (see Exercise 10.2).) This new type of character, the Lefschetz character, is defined as follows:

**(66.11) Definition.** Let  $X$  be a  $G$ -poset. The *Lefschetz character* of the homology representation  $H_*(X)$  is the map  $\Lambda: G \rightarrow K$  defined by

$$\Lambda(g) = \sum_{r \geq 0} (-1)^r \text{Tr}(g, H_r(X)).$$

The *degree*  $\Lambda(1)$  of the Lefschetz character is called the *Euler characteristic* of  $X$ , and is denoted by  $\chi(X)$ .

Here we assume, as usual, that  $X$  and  $G$  are finite, so that the homology spaces  $\{H_r(X), r \geq 0\}$  are f.d./ $K$ , and are 0 for all sufficiently large  $r$ , so  $\Lambda$  is well defined. We note that if  $K$  is a field of characteristic zero, then the Lefschetz character is a virtual  $K$ -character of  $G$ , by Vol. I, p. 208. In this case, the homology representation over  $K$  is obtained by extension of the base field from the homology representation with coefficients in the rational field  $\mathbb{Q}$ , and the Euler characteristic coincides with the alternating sum

$$\sum_{r=0}^{\infty} (-1)^r \dim H_r(X).$$

This is the usual Euler characteristic  $\chi(|X|)$  of the underlying topological space  $|X|$ .

The computation of the Lefschetz character is transferred to the chain modules  $C_r(X)$  by means of the next result.

**(66.12) Hopf Trace Formula.** Let  $C = \bigoplus_{r \geq 0} C_r$  be a chain complex over a field  $K$ , with boundary map  $\partial$ , such that each subspace  $C_r$  is f.d./ $K$ , and  $C_r = 0$  for all sufficiently large  $r$ . Let  $f: C \rightarrow C$  be a graded chain map of degree zero, that is, a  $K$ -endomorphism  $f: C \rightarrow C$  such that  $f(C_r) \subseteq C_r$  for each  $r \geq 0$ , and  $f\partial = \partial f$ . Then  $f$  induces a  $K$ -endomorphism  $f_*$  of  $H_*(C)$  such that  $f_*(H_r(C)) \subseteq H_r(C)$  for all  $r$ , and we have

$$\sum_{r=0}^{\infty} (-1)^r \text{Tr}(f, C_r) = \sum_{r=0}^{\infty} (-1)^r \text{Tr}(f_*, H_r(C)).$$

*Proof.* For each  $r \geq 0$ , let  $\partial_r$  denote  $\partial|_{C_r}$ . Now keep  $r$  fixed, and set

$$Z_r = \ker \partial_r, \quad B_r = \text{im } \partial_{r+1},$$

so

$$B_r \leq Z_r \leq C_r$$

since  $\partial^2 = 0$ . Both  $B_r$  and  $Z_r$  are  $f$ -stable, since  $f$  commutes with  $\partial$ . Therefore

$$\text{Tr}(f, C_r) = \text{Tr}(f, C_r/Z_r) + \text{Tr}(f, Z_r/B_r) + \text{Tr}(f, B_r).$$

The surjection  $\partial_r: C_r \rightarrow B_{r-1}$  has kernel  $Z_r$ , so we have  $C_r/Z_r \cong B_{r-1}$  as  $f$ -modules. Therefore

$$\text{Tr}(f, C_r/Z_r) = \text{Tr}(f, B_{r-1}).$$

Since  $Z_r/B_r = H_r(C)$ , we obtain

$$\text{Tr}(f, C_r) = \text{Tr}(f, H_r(C)) + \text{Tr}(f, B_{r-1}) + \text{Tr}(f, B_r).$$

Substituting this expression for  $\text{Tr}(f, C_r)$  into the alternating sum  $\sum (-1)^r \text{Tr}(f, C_r)$ , we easily obtain the desired formula.

**(66.13) Corollary.** *Let  $K$  be a field of characteristic zero. Then the Euler characteristic  $\chi(X)$  of a  $G$ -poset  $X$  is given by*

$$\chi(X) = \sum_{r=0}^{\infty} (-1)^r \dim C_r(X),$$

where  $C_r(X)$  is the vector space of  $r$ -chains, for  $r \geq 0$ .

We now have:

**(66.14) Proposition.** *Let  $X$  be a  $G$ -poset, and  $\Lambda$  the Lefschetz character of the homology representation  $H_*(X)$  of  $G$ . Then we have*

$$\Lambda(g) = \chi(X^g) = \chi(|X|^g), \quad \text{for each } g \in G.$$

In other words, the value of the Lefschetz character at  $g \in G$  is the Euler characteristic of the fixed point set  $|X|^g$ ,

*Proof.* Let  $g \in G$ . Since the action of  $g$  commutes with the boundary map  $\partial$ , we have

$$\Lambda(g) = \sum (-1)^r \text{Tr}(g, C_r(X))$$

by the Hopf trace formula. On each vector space  $C_r(X)$ ,  $g$  acts as a permutation of the basis elements, so by Exercise 10.2,  $\text{Tr}(g, C_r(X))$  is the number of  $r$ -chains  $\sigma = (x_0 < \dots < x_r)$  fixed by  $g$ . By (66.3), the  $r$ -chains fixed by  $g$  are the  $r$ -chains of the fixed point poset  $X^g$ , and so we have

$$\Lambda(g) = \chi(X^g)$$

by Corollary 66.13. Finally,  $\chi(X^g) = \chi(|X|^g)$  by the second part of (66.3), since  $|X^g|$  is homeomorphic to  $|X|^g$ .

Note how the preceding result extends, in a profound way, the result of Exercise 10.2 for permutation characters. The value of a permutation character counts the number of fixed points; the value of the Lefschetz character “counts” the fixed point set on the underlying topological space, provided we use the Euler characteristic instead of cardinality.

In our introduction to homology representations, the last main topic is an interpretation of the endomorphism algebra  $\text{End}_{KG} H_*(X)$ , for a field  $K$  of characteristic zero and a  $G$ -poset  $X$ . We first require an analogue of Maschke’s Theorem for chain complexes (see (3.14)).

**(66.15) Proposition.** *Let  $G$  be a finite group, and let  $(C, \partial)$  be a chain complex over a field  $K$  with  $G$ -action, where  $|G| \neq 0$  in  $K$ . As usual, let  $\text{inv}_G C = \{x \in C : gx = x, g \in G\}$ . Then  $(\text{inv}_G C, \partial)$  is also a chain complex, and there is an isomorphism of graded vector spaces:*

$$\text{inv}_G H_*(C) \cong H_*(\text{inv}_G C).$$

*Proof.* Since  $\partial$  commutes with the action of  $G$ ,  $\text{inv}_G C$  is stable under the action of  $\partial$ . Therefore  $\text{inv}_G C$  is a chain complex, with graded components  $\text{inv}_G C_r$ ,  $r \geq 0$ , and with boundary map given by the restriction of  $\partial$  to  $\text{inv}_G C$ . Let  $Z = \ker \partial$ ,  $B = \text{im } \partial$  in  $C$ ; then the  $G$ -action on  $H_*(C) = Z/B$  is given by

$$g(z + B) = gz + B, \quad z \in Z, \quad g \in G.$$

Clearly  $z + B \in \text{inv}_G H_*(C)$  if and only if  $gz \equiv z \pmod{B}$  for all  $g \in G$ . It follows that there is an injective  $K$ -homomorphism

$$\varphi : H_*(\text{inv}_G C) \rightarrow \text{inv}_G H_*(C),$$

given by

$$\varphi(z + \partial(\text{inv}_G C)) = z + B, \quad z \in \text{inv}_G Z.$$

To check this, we need only verify that

$$B \cap \text{inv}_G Z \subseteq \partial(\text{inv}_G C).$$

Let  $z$  be an element of this intersection; since  $B = \partial C$ , we may write  $z = \partial c$  for some  $c \in C$ . But then

$$z = |G|^{-1} \sum_{g \in G} gz = \partial(|G|^{-1} \sum_{g \in G} gc) \in \partial(\text{inv}_G C),$$

since  $\partial$  commutes with the action of  $G$ .

It remains to prove  $\varphi$  surjective, and for this we must show that if  $z \in Z$  satisfies

$$gz \equiv z \pmod{B} \quad \text{for all } g \in G,$$

then  $z + b \in \text{inv}_G Z$  for some  $b \in B$ . We may write

$$gz = z + b_g \quad \text{with } b_g \in B, \quad \text{for all } g \in G.$$

Then we have

$$|G|^{-1} \sum_{g \in G} gz = z + |G|^{-1} \sum_{g \in G} b_g \in z + B.$$

Choosing  $b = |G|^{-1} \sum b_g \in B$ , we obtain  $z + b \in \text{inv}_G Z$ , completing the proof.

This result can be applied to  $G$ -posets, and yields:

**(66.16) Proposition.** *Let  $X$  be a regular  $G$ -poset, and let  $C(X)$  be the chain complex of  $X$  over a field  $K$  of characteristic zero. Then there is an isomorphism of chain complexes.*

$$\text{inv}_G C \cong C(\bar{X}),$$

where  $C(\bar{X})$  is the chain complex over  $K$  associated with the orbit poset  $\bar{X} = G \setminus X$ . Further, there is an isomorphism of graded vector spaces:

$$\text{inv}_G H_*(X) \cong H_*(\bar{X}).$$

*Proof.* We first define a  $K$ -linear map  $\varphi: C(X) \rightarrow C(\bar{X})$  with the properties that  $\varphi$  commutes with the boundary maps in the two chain complexes, and  $\varphi(ga) = \varphi(a)$  for all  $g \in G, a \in C(X)$ . The map  $\varphi$  is defined on a basis of  $C(X)$ , and sends  $c_\sigma$  to  $c_{\bar{\sigma}}$ , where  $\sigma = (x_0 < \dots < x_r)$  is an  $r$ -simplex in  $\Sigma(X)$ , and  $\bar{\sigma} = (\bar{x}_0 < \dots < \bar{x}_r)$  is the corresponding  $r$ -simplex in  $\Sigma(\bar{X})$ . We leave it to the reader to check that  $\varphi$  has the desired properties.

Now consider  $\text{inv}_G C(X) = \bigoplus_{r \geq 0} \text{inv}_G C_r(X)$ . For fixed  $r \geq 0$ ,  $G$  acts as a permutation group on the basis  $\{c_\sigma\}$  of the vector space of  $r$ -chains  $C_r(X)$ . Therefore  $\text{inv}_G C_r(X)$  has a basis consisting of elements  $\sum_{\sigma \in \bar{\sigma}} c_\sigma$ , where  $\{\bar{\sigma}\}$  ranges over the  $G$ -orbits of  $r$ -simplices in  $\Sigma X$  (see Exercise 10.2ii). Letting  $\varphi_1$  be the restriction of  $\varphi$ , it follows that the map  $\varphi_1: \text{inv}_G C(X) \rightarrow C(\bar{X})$  is an isomorphism, since  $\varphi$  is bijective on corresponding bases of  $C_r(X)$  and  $C_r(\bar{X})$ .

by Proposition 66.6. Since  $\varphi_1$  commutes with the boundary maps in  $C(X)$  and  $C(\bar{X})$ , respectively, the first part of the proposition is established. The second part follows immediately from (66.15), completing the proof.

We also require the connection between the homology  $H_*(X \times Y)$  of the cartesian product  $X \times Y$  of two  $G$ -posets  $X$  and  $Y$ , and the homology of the factors  $H_*(X)$  and  $H_*(Y)$ . Suppose first that  $M = \bigoplus_{r \geq 0} M_r$  and  $N = \bigoplus_{s \geq 0} N_s$  are two graded vector spaces over  $K$ , such that the subspaces  $\{M_r\}$  and  $\{N_s\}$  are  $KG$ -modules, for a finite group  $G$ . Then  $M \otimes N$  has a natural structure as a graded  $KG$ -module, given by

$$M \otimes N = \bigoplus_{t \geq 0} (M \otimes N)_t,$$

where for each  $t$ ,

$$(M \otimes N)_t = \bigoplus_{r+s=t} M_r \otimes N_s,$$

and where each submodule  $M_r \otimes N_s$  is the inner tensor product of  $KG$ -modules (Definition 10.15). We then have:

**(66.17) Proposition.** *Let  $X$  and  $Y$  be  $G$ -posets, and  $X \times Y$  their cartesian product (as in (66.9)). Let  $K$  be an arbitrary field. There is an isomorphism of graded  $KG$ -modules*

$$H_*(X \times Y) \cong H_*(X) \otimes H_*(Y),$$

such that for each  $r \geq 0$ ,

$$H_r(X \times Y) \cong \bigoplus_{j=0}^r H_j(X) \otimes H_{r-j}(Y)$$

as  $KG$ -modules.

The proof depends on the Eilenberg-Zilber theorem and the theory of acyclic models, and is given in Godement ([64]).

We now come to the main result of this subsection, which we will apply in §66C to homology representations of finite groups with  $BN$ -pairs.

**(66.18) Theorem.** *Let  $H_*(X)$  be a homology representation of a finite group  $G$  over the field of rational numbers  $\mathbb{Q}$ , associated with a regular  $G$ -poset  $X$ . Then  $X \times X$  is a regular  $G$ -poset, and there is an isomorphism of graded vector spaces over  $\mathbb{Q}$ :*

$$H_*(G \setminus (X \times X)) \cong \text{End}_{\mathbb{Q}G} H_*(X),$$

where  $G \setminus (X \times X)$  is the orbit poset of the regular  $G$ -poset  $X \times X$ . The isomorphism is such that for each  $r \geq 0$ ,

$$H_r(G \setminus (X \times X)) \cong \bigoplus_{j=0}^r \text{Hom}_{\mathbb{Q}G}(H_j(X), H_{r-j}(X)).$$

*Proof.* We first remark that by (10.27), any f.d.  $\mathbb{Q}G$ -module  $M$  is isomorphic to its contragredient module  $M^*$ , since the character afforded by  $M$  is real-valued. Upon identifying  $M$  with  $M^*$ , we then have

$$M \otimes_{\mathbb{Q}} N = \text{Hom}_{\mathbb{Q}}(M, N)$$

for each  $\mathbb{Q}G$ -module  $N$ , and there is an isomorphism of vector spaces:

$$\text{inv}_G M \otimes_{\mathbb{Q}} N \cong \text{Hom}_{\mathbb{Q}G}(M, N),$$

by (10.30) and (10.31ii).

Now consider the homology representation  $H_*(X)$ . It follows at once from the definitions that  $X \times X$  is regular. We have, by (66.17),

$$H_r(X \times X) \cong \bigoplus_{j=0}^r H_j(X) \otimes H_{r-j}(X) \quad \text{for } r \geq 0.$$

Since  $X \times X$  is regular, we have

$$H_*(G \setminus (X \times X)) \cong \text{inv}_G H_*(X \times X),$$

so for each  $r \geq 0$ , we obtain from (66.16)

$$H_r(G \setminus (X \times X)) \cong \text{inv}_G H_r(X \times X) \cong \bigoplus \text{inv}_G(H_j(X) \otimes H_{r-j}(X)).$$

Finally, by the remark at the beginning of the discussion, there is an isomorphism of vector spaces over  $\mathbb{Q}$ :

$$\text{inv}_G H_j(X) \otimes H_{r-j}(X) \cong \text{Hom}_{\mathbb{Q}G}(H_j(X), H_{r-j}(X))$$

for  $0 \leq j \leq r$ , completing the proof.

The preceding theorem is the first step toward the study, from the geometrical point of view, of the  $\mathbb{Q}G$ -endomorphism algebra of a homology representation, and is already quite powerful, as we shall see later in the section. The theory is still incomplete, however. What is needed is a better geometrical understanding of the multiplication in  $\text{End}_{\mathbb{Q}G} H_*(X)$ . For example, in the case of a permutation representation, there is an explicit description of the multiplication in the endomorphism algebra in terms of the intersection numbers  $\{\mu_{ijk}\}$  of the Hecke

algebra, as in (11.34). A generalization of this description is still missing in the case of homology representations.

### §66B. The Coxeter Poset of a Finite g.g.r.

Let  $\Delta$  be a root system in an  $n$ -dimensional euclidean space  $V$ , and let  $W = W(\Delta)$  be the finite g.g.r. associated with  $\Delta$ , as in §64A. Since  $W \leq O(V)$ ,  $W$  acts on the unit sphere  $S^{n-1}$  in  $V$ . In this subsection, we shall prove that  $S^{n-1}$  is the geometric realization  $|\Gamma|$  of a  $W$ -poset  $\Gamma$ , called the *Coxeter poset* of  $W$ , and will determine the homology representation of  $W$  on  $\Gamma$ . By §64B, every finite Coxeter group is isomorphic to a g.g.r., so the discussion applies to an arbitrary finite Coxeter group.

Following Steinberg [67], we begin with the determination of a fundamental domain for the action of  $W$  on  $V$ . As in §64A, we let  $\Delta_{\pm}$  denote the sets of positive (resp. negative) roots associated with a fundamental system  $\Pi$  (see (64.10)).

**(66.19) Definition.** Let  $\Pi$  be a fundamental system in  $\Delta$ . The (closed) *chamber*  $D$  in  $V$  associated with  $\Pi$  is the set

$$D = \{\xi \in V : (\xi, \alpha) \geq 0 \text{ for all } \alpha \in \Pi\}.$$

The *faces* of the chamber  $D$  are the subsets  $D_I$ ,  $I \subset \Pi$ , defined by

$$D_I = \{\xi \in D : (\xi, \alpha) = 0 \text{ for all } \alpha \in I\}.$$

The chamber  $D$  is a closed convex cone with vertex at 0, and will turn out to be a fundamental domain for the action of  $W$  on  $V$ .

**(66.20) Lemma.** Every  $\xi \in V$  is in the  $W$ -orbit of some  $\xi' \in D$ .

*Proof.* We introduce a partial order  $\leq$  on  $V$ , with  $\delta \leq \delta'$  if either  $\delta = \delta'$  or  $\delta' - \delta$  is in the positive span of  $\Pi$ . The  $W$ -conjugates  $\xi'$  of  $\xi$  form a finite set, since  $|W| < \infty$ , so we can choose one which is maximal in the partial ordering. Now let  $\alpha \in \Pi$ . Then  $s_{\alpha}\xi'$  is a  $W$ -conjugate of  $\xi$ , and

$$s_{\alpha}\xi' = \xi' - 2(\xi', \alpha)(\alpha, \alpha)^{-1}\alpha,$$

so  $(\xi', \alpha) \geq 0$ , since otherwise  $s_{\alpha}\xi' > \xi'$ , contrary to the selection of  $\xi'$ . Thus  $\xi' \in D$ , and the lemma is proved.

**(66.21) Lemma.** Let  $\xi, \eta \in D$ ,  $w \in W$ , and assume  $w\xi = \eta$ . Then: (i)  $w$  is a product of fundamental reflections  $\{s_{\alpha}\}$  such that  $s_{\alpha}\xi = \xi$ , and (ii)  $\xi = \eta$ .

*Proof.* We first recall (see (64.15) and (64.16)) that  $N(w) = \text{card } \{\alpha \in \Delta_+ : w\alpha \in \Delta_-\}$ , and that  $N(w) = l(w)$ . We prove (66.21) using induction on  $N(w)$ , the result being trivial for  $N(w) = 0$ . Now assume that  $N(w) > 0$ , and choose

$\alpha \in \Pi$  such that  $w\alpha \in \Delta_-$ . Since  $\eta \in D$ , we obtain

$$0 \geq (\eta, w\alpha) = (w\xi, w\alpha) \geq 0,$$

whence  $(\xi, \alpha) = 0$ , and  $s_\alpha \xi = \xi$ . Then  $ws_\alpha \xi = \eta$  and  $N(ws_\alpha) < N(w)$  by (64.16). We can therefore apply the induction hypothesis to  $ws_\alpha$  to obtain (i). Statement (ii) follows from (i).

In stating the next result, the symbol  $I$  will denote a proper subset of  $\Pi$ , and will also denote the corresponding subset of the fundamental reflections, so that  $W_I$  is the parabolic subgroup of  $W$  defined by this set of reflections (see §64C).

**(66.22) Theorem.** (i)  *$D$  is a fundamental domain for the action of  $W$  on  $V$ , in the sense that every element of  $V$  is in the  $W$ -orbit of a unique element of  $D$ .*

(ii) *Let  $I$  be a subset of  $\Pi$ , and  $D_I$  the corresponding face of  $D$ , as in (66.19). Then the following three subgroups of  $W$  coincide:*

- (a)  $\{w \in W : wD_I = D_I\}$ , the stabilizer of the set  $D_I$ ,
- (b)  $\{w \in W : w\xi = \xi, \forall \xi \in D_I\}$ , the point-stabilizer of  $D_I$ , and
- (c)  $W_I = \langle s_\alpha : \alpha \in I \rangle$ , the parabolic subgroup of  $W$  corresponding to  $I$ .

*Proof.* (i) By (66.20), each element of  $V$  is conjugate to some element of  $D$ , and this element is unique by Lemma 66.21ii.

(ii) By Lemma 66.21, the point and set stabilizers of  $D_I$  coincide, and are contained in the parabolic subgroup  $W_I$ , by (66.21i). Conversely, it is clear that any element of  $W_I$  fixes every vector in  $D_I$ , and the theorem is proved.

**(66.23) Corollary.** (i) *Let  $\Pi$  be a fundamental system in  $\Delta$ , and  $D$  the chamber associated with  $\Pi$ . For each  $w \in W$ ,  $wD$  is the chamber associated with the fundamental system  $w\Pi$ , and  $V$  is the union of the chambers  $\{wD\}$ . The interiors  $\{\text{int}(wD)\}_{w \in W}$  of the chambers  $\{wD\}$  form a partition of the open set*

$$V - \bigcup_{\alpha \in \Delta} H_\alpha,$$

where for  $\alpha \in \Delta$ ,  $H_\alpha$  is the hyperplane  $\langle \alpha \rangle^\perp$ .

(ii) *The faces of the chamber  $wD$ ,  $w \in W$ , are the translates  $\{wD_I\}$  of the faces  $\{D_I, I \subset \Pi\}$ , of  $D$ . Their stabilizers are the parabolic subgroups  $wW_Iw^{-1}$ ,  $I \subset \Pi$ .*

**(66.24) Corollary.** *The map  $wD_I \rightarrow wW_I$ ,  $w \in W$ ,  $I \subset \Pi$ , is a bijection from the set of faces of the chambers  $\{wD\}_{w \in W}$  to the set of left cosets of the parabolic subgroup  $W_I$ . Moreover,*

$$wD_I \subseteq w'D_{I'} \Leftrightarrow wW_I \supseteq w'W_{I'}, \quad \text{for } w, w' \in W \quad \text{and } I, I' \subset \Pi.$$

Both (66.23) and (66.24) follow from the preceding discussion, especially Lemma 66.21, and their proofs are left as exercises. The following definition is suggested by these results.

**(66.25) Definition.** Let  $(W, S)$  be a finite Coxeter system, with  $|S| \geq 2$ . The *Coxeter poset*  $\Gamma$  is the  $W$ -poset consisting of all left cosets

$$\{wW_I : w \in W, I \subset S\},$$

ordered by inclusion. The action of  $W$  on  $\Gamma$  is given by left translation: for  $x \in W$ ,

$$wW_I \rightarrow xwW_I \quad \text{for all } w \in W, I \subset S.$$

It is easily checked that  $\Gamma$  satisfied the definition of a  $W$ -poset, from §66A. The restriction  $|S| \geq 2$  excludes the trivial case  $|W| = 2$ .

The results so far obtained give a geometric interpretation of the parabolic subgroups of  $W$ . They lead us, in turn, to the homology representation of  $W$  on  $H_*(\Gamma)$ . In particular, for  $n = |S|$ ,  $H_{n-1}(\Gamma)$  affords the sign representation of  $W$ , defined below.

**(66.26) Definition.** Let  $(W, S)$  be finite Coxeter system. The *sign representation*  $\varepsilon$  of  $W$  is the representation  $\varepsilon: W \rightarrow \mathbb{Q}$  of degree 1, defined uniquely by

$$\varepsilon(s) = -1 \quad \text{for all } s \in S.$$

It is clear from Definition 64.17 that the map  $\varepsilon$ , given above, preserves the defining relations of  $W$ , and does indeed extend to a linear representation  $\varepsilon: W \rightarrow \mathbb{Q}$ . In case  $(W, S)$  is realized as a finite g.g.r. associated with a root system in a Euclidean space, then we clearly have

$$(66.27) \quad \varepsilon(w) = \det w \quad \text{for all } w \in W,$$

since the determinant of a reflection is  $-1$ .

We now have:

**(66.28) Theorem.** Let  $\Delta$  be a root system in  $V$ , and  $(W, S)$  the Coxeter system associated with  $\Delta$ , where  $W = W(\Delta)$ , and  $S$  is the set of reflections associated with a fundamental system  $\Pi \subseteq \Delta$ . Let  $n = |S| = \dim V$ , and assume  $n \geq 2$ . Then the following statements hold:

- (i) The group  $W$  acts on the unit sphere\*  $S^{n-1}$  in  $V$ , and there is a  $W$ -equivariant homeomorphism

$$|\Gamma| \simeq S^{n-1},$$

\*The sphere  $S^{n-1}$  is the set of vectors  $\xi \in V$  such that  $\|\xi\| = (\xi, \xi)^{1/2} = 1$ .

where  $|\Gamma|$  is the underlying topological space of the Coxeter poset  $\Gamma$  associated with the Coxeter system  $(W, S)$ .

(ii) The homology representation of  $W$  on  $H_*(\Gamma)$ , over the rational field  $\mathbb{Q}$ , is given as follows:  $H_i(\Gamma) = 0$  except in dimensions  $0$  and  $n - 1$ . Moreover  $H_0(\Gamma)$  affords the trivial representation  $1_W$ , while  $H_{n-1}(\Gamma)$  affords the sign representation  $\varepsilon$ .

*Proof.* Since  $W$  is a group of orthogonal transformations,  $W$  clearly acts on the sphere  $S^{n-1}$ . We now give an outline of the proof that  $|\Gamma| \simeq S^{n-1}$ , leaving some points to be verified by the reader. (A more detailed discussion is given in Bourbaki [68, Ch. 5].) Let  $D$  be the chamber in  $V$  defined by  $\Pi$ , as in (66.19). It is easily verified, using the fact that  $\Pi$  is a basis of  $V$ , that the hyperplanes  $\{H_\alpha = \langle \alpha \rangle^\perp : \alpha \in \Pi\}$  are the *walls* of  $D$ , in the sense that  $H_\alpha \cap D$  is contained in the boundary of  $D$ , and generates the vector space  $H_\alpha$ . The same argument shows that each face  $D_I = D \cap H_{\alpha_{i_1}} \cap \dots \cap H_{\alpha_{i_g}}$ , where  $I = \{\alpha_{i_1}, \dots, \alpha_{i_g}\} \subset \Pi$ , generates a subspace of  $V$  of dimension  $n - |I|$ . Using the discussion in §66A, it is then readily shown that the intersection  $D \cap S^{n-1}$  is homeomorphic to the underlying topological space of an (abstract)  $(n - 1)$ -simplex  $\sigma$ . The vertices of  $\sigma$  correspond to the intersections  $D_I \cap S^{n-1}$ , for  $|I| = n - 1$ ,  $I \subset \Pi$ , since for such  $I$ , each face  $D_I$  is a half-line and intersects  $S^{n-1}$  in a point. These points support a spherical simplex homeomorphic to  $|\sigma|$ . The  $k$ -dimensional faces of  $\sigma$ ,  $0 \leq k \leq n - 1$ , are realized by the intersections  $D_K \cap S^{n-1}$ , with  $|K| = n - k - 1$ ,  $K \subseteq \Pi$ .

By (66.23),  $S^{n-1}$  is the union of the intersections  $\{wD \cap S^{n-1}\}_{w \in W}$ , and their interiors partition the set  $S^{n-1} - \bigcup_{\alpha \in \Delta} H_\alpha$ . By the first paragraph, each such intersection is homeomorphic to  $|\sigma|$ . These intersections  $\{wD \cap S^{n-1}\}_{w \in W}$ , and their faces  $\{wD_I \cap S^{n-1}\}_{w \in W}$ , where  $I \subset \Pi$ , form a  $W$ -poset under inclusion, with  $W$ -action given by left translation. By (66.24), this poset is isomorphic, as a  $W$ -poset, to the opposite poset  $\Gamma^\circ$  of the Coxeter poset. By (66.24), the simplicial complex  $\Sigma(\Gamma)$  is  $W$ -isomorphic to the barycentric subdivision of the simplicial complex whose geometric realization is  $S^{n-1}$ . Then by (66.1), there is a  $W$ -equivariant homeomorphism  $|\Gamma| \simeq S^{n-1}$ , completing the proof of part (i).

(ii) Since  $|\Gamma| \simeq S^{n-1}$  by part (i), we have

$$H_i(\Gamma) = 0, \quad i \neq 0, n - 1, \quad H_0(\Gamma) \cong H_{n-1}(\Gamma) \cong \mathbb{Q},$$

by the standard result on the homology of the  $(n - 1)$ -sphere  $S^{n-1}$  (Eilenberg-Steenrod [52, Theorem I.16.6]). We leave it to the reader to prove that  $H_0(\Gamma)$  affords the trivial representation of  $W$ .

We now prove, using the Lefschetz character and Proposition 66.14, that  $H_{n-1}(\Gamma)$  affords the sign representation. From what has been shown so far, the Lefschetz character  $\Lambda$  of  $H_*(\Gamma)$  is given by

$$\Lambda = 1_W + (-1)^{n-1} \operatorname{Tr}(\cdot, H_{n-1}(\Gamma)).$$

Now let  $s$  be an arbitrary reflection in  $W$ . Then the fixed point set  $|\Gamma|^s \simeq (S^{n-1})^s$  is

homeomorphic to an  $(n - 2)$ -sphere, whose Euler characteristic is  $1 + (-1)^{n-2}$ . By (66.14), we have

$$\Lambda(s) = 1 + (-1)^{n-2},$$

and comparing this formula with the general expression for  $\Lambda$ , we obtain

$$\mathrm{Tr}(s, H_{n-1}(\Gamma)) = -1,$$

which completes the proof that  $H_{n-1}(\Gamma)$  affords the sign representation.

**(66.29) Corollary** (Solomon [66]). *Let  $\varepsilon$  be the sign character of a finite Coxeter group  $W$ . Then*

$$\varepsilon = \sum_{J \subseteq S} (-1)^{|J|} (1_{W_J})^W.$$

*Proof.* We apply the Hopf Trace Formula (66.12) to the homology representation  $H_*(\Gamma)$ . From the proof of Theorem 66.28, the homology of  $\Gamma$  can be computed from a chain complex  $C = \bigoplus_{r \geq 0} C_r$ , where the vector space  $C_r$  of  $r$ -chains has a basis corresponding to the elements of  $\Gamma$ ,

$$\{wW_I, |I| = n - r - 1\}.$$

The group  $W$  acts as a permutation group on the basis of  $C_r$ . Thus we have, for each  $r \geq 0$ ,

$$\mathrm{Tr}(x, C_r) = \sum_{|I|=n-r-1} (1_{W_I})^W(x), \quad \text{for all } x \in W,$$

since  $(1_{W_I})^W(x)$  counts the number of cosets  $\{wW_I\}_{w \in W}$  fixed by  $x$ , by Exercise 10.2i. By the Hopf Trace Formula and by part (ii) of the preceding theorem, the Lefschetz character  $\Lambda$  of  $H_*(\Gamma)$  is given by

$$\begin{aligned} \Lambda(x) &= 1 + (-1)^{n-1} \varepsilon(x) = \sum_{r=0}^{n-1} (-1)^r \mathrm{Tr}(x, C_r) \\ &= \sum_{J \subseteq S} (-1)^{n-|J|-1} (1_{W_J})^W(x) \quad \text{for } x \in W. \end{aligned}$$

Upon solving for  $\varepsilon$ , we obtain Solomon's formula.

While the formula (66.29) can perhaps best be understood in terms of the preceding argument, it is also possible to give a short direct proof of it, independent of the theory of homology representations (see Exercise 66.2).

### §66C. The Combinatorial Building and the Steinberg Representation of a Finite Group with a BN-Pair

Throughout this subsection,  $G$  denotes a finite group with a BN-pair of rank  $n$ , and  $W$  the Weyl group of  $G$ , with  $(W, S)$  the Coxeter system in  $W$ , as in (65.9). We shall construct an absolutely irreducible  $\mathbb{Q}$ -representation  $\text{St}_G$  of  $G$ , called the *Steinberg representation*, which plays a special role in the representation theory of  $G$ . In case  $n = 1$ , the Bruhat decomposition implies that the permutation representation of  $G$  on the cosets  $G/B$  of a Borel subgroup is 2-transitive, by Exercise 10.3, and in this case  $\text{St}_G$  is defined as the unique nontrivial irreducible component of this permutation representation (see Exercise 10.3ii, and example (ii) in Vol. I, §18, p. 443, for the groups  $SL_2(q)$ ). In case  $n > 1$ , there is no straightforward construction of  $\text{St}_G$  by the methods of Volume I, and it is for this reason that we have introduced homology representations in this section. We shall exhibit  $\text{St}_G$  as a homology representation on a  $G$ -poset with vanishing homology except in two dimensions, in much the same way as the sign representation of  $W$  was realized on the homology of  $\Gamma$  in the preceding section.

**(66.30) Definition (Tits [74]).** The *combinatorial building*  $\Delta$  of a finite group  $G$  with a BN-pair of rank  $n > 1$  is the  $G$ -poset of all proper parabolic subgroups of  $G$  (see (65.15)), ordered by inclusion, with the  $G$ -action given by conjugation:

$$P \rightarrow {}^g P = gPg^{-1}, \quad \text{for } g \in G, \quad P \in \Delta.$$

Our aim is to calculate the homology  $H_*(\Delta)$  over the rational field  $\mathbb{Q}$ , and the nature of the homology representations it affords. The main result is due to Solomon and Tits (Solomon [69]), and was also proved by Garland [73], using the determination of the homotopy type of the underlying topological space  $|\Delta|$ . We shall give a new proof, due to Curtis-Lehrer [82], based on a comparison of the endomorphism algebras of  $H_*(\Delta)$  and  $H_*(\Gamma)$ , using Theorem 66.18, where  $\Gamma$  is the Coxeter poset of  $W$  (see (66.25)). The key to this approach is the following result, which shows that although  $\Delta$  and  $\Gamma$  are posets on which different groups act, certain orbit posets associated with them have the same structure.

**(66.31) Lemma.** *Let  $G$  be a finite group with a BN-pair of rank  $n > 1$ , and let  $W$  be the Weyl group of  $G$ . Then the Coxeter poset  $\Gamma$  of  $W$  and the combinatorial building  $\Delta$  of  $G$  have the property that\*  $\Gamma^\circ$  and  $\Delta^\circ$  are regular  $W$ - and  $G$ -posets, respectively. Moreover, there is an isomorphism of posets*

$$W \setminus (\Gamma \times \Gamma) \cong G \setminus (\Delta \times \Delta).$$

*Proof.* To prove that  $\Gamma^\circ$  is regular, we have to show that if  $xW_I \leq yW_J$  and  $xW_I \leq zW_J$ , for  $x, y, z \in W$ , then  $yW_J = zW_J$ . This is clear, however, since the cosets  $yW_J$  and  $zW_J$  both contain  $xW_I$ , and so have a nonempty intersection. The proof

\* $\Gamma^\circ$  Denotes the opposite poset of  $\Gamma$  (see §66A).

that  $\Delta^\circ$  is regular is less trivial: we have to show that if  $P$  and  $Q$  are parabolic subgroups such that  $P \leq Q$  and  $P \leq {}^g Q$ , where  $g \in G$ , then  $Q = {}^g Q$ . This is precisely what was established in Theorem 65.19, in somewhat greater generality.

It follows that the opposite posets of  $\Gamma \times \Gamma$  and  $\Delta \times \Delta$  are both regular, so the orbit posets  $W \backslash (\Gamma \times \Gamma)$  and  $G \backslash (\Delta \times \Delta)$  are both defined (see (66.18)). We shall prove that both posets are isomorphic to the poset of triples

$$\Omega = \{(I, J, w), \quad I, J \subset S, \quad w \in D_{IJ}\},$$

where  $D_{IJ}$  is a set of d.d.c.r.'s (see (64.39)). The order relation in  $\Omega$  is given by

$$(I, J, w) \leq (I', J', w')$$

if and only if

$$I \subseteq I', \quad J \subseteq J' \quad \text{and} \quad W_I w W_J \subseteq W_{I'} w' W_{J'}.$$

First consider an orbit  $\mathcal{O}$  in  $G \backslash (\Delta \times \Delta)$ ; then  $\mathcal{O}$  contains a representative of the form  $(P_I, {}^g P_J)$  with  $I, J \subset S$  and  $g \in G$ . By (65.21),  $g \in P_I w P_J$  for some  $w \in D_{IJ}$ , whence  $\mathcal{O}$  contains  $(P_I, {}^w P_J)$ . We let  $\mathcal{O}$  correspond to the triple  $(I, J, w) \in \Omega$ . Now suppose another orbit  $\mathcal{O}' \in G \backslash (\Delta \times \Delta)$  contains a representative  $(P_{I'}, {}^{w'} P_{J'})$ , with  $w' \in D_{I'J'}$ . We shall prove that

$$(66.32) \quad \mathcal{O} \leq \mathcal{O}' \Leftrightarrow I \subseteq I', \quad J \subseteq J' \quad \text{and} \quad W_I w W_J \subseteq W_{I'} w' W_{J'}.$$

The proof is simply a workout with the properties of parabolic subgroups established in §65C. We have, for some  $g \in G$ ,

$$\mathcal{O} \leq \mathcal{O}' \Leftrightarrow {}^g(P_I, {}^w P_J) \leq (P_{I'}, {}^{w'} P_{J'}) \Leftrightarrow {}^g P_I \leq P_{I'} \quad \text{and} \quad {}^g({}^w P_J) \leq {}^{w'} P_{J'}.$$

By (65.19) and (65.17), these conditions are equivalent to:

$$I \subseteq I', \quad J \subseteq J' \quad \text{and} \quad P_I w P_J \subseteq P_{I'} w' P_{J'}.$$

By (65.21), the last condition is equivalent to  $W_I w W_J \subseteq W_{I'} w' W_{J'}$ , which proves statement (66.32). It shows, in particular, that each orbit corresponds to a unique element of  $\Omega$ , and that the posets  $G \backslash (\Delta \times \Delta)$  and  $\Omega$  are isomorphic.

The proof that  $W \backslash (\Gamma \times \Gamma) \cong \Omega$  is easier, and is left as an exercise for the reader.

We now have:

**(66.33) Theorem (Solomon–Tits).** *Let  $\Delta$  be the combinatorial building of a finite group with a BN-pair of rank  $n \geq 2$ , and let  $H_*(\Delta) = \bigoplus_{r \geq 0} H_r(\Delta)$  denote the rational homology of  $\Delta$ . Then  $H_r(\Delta) = 0$  except in dimensions  $r = 0$  and  $r = n - 1$ . In these dimensions,  $H_0(\Delta)$  affords the trivial representation, while  $H_{n-1}(\Delta)$  affords an absolutely irreducible nontrivial representation.*

*Proof.* By Lemma 66.31 and two applications of Theorem 66.18, there exist isomorphisms of graded vector spaces over  $\mathbb{Q}$ :

$$\mathrm{End}_{\mathbb{Q}W} H_*(\Gamma) \cong H_*(W \setminus (\Gamma \times \Gamma)) \cong H_*(G \setminus (\Delta \times \Delta)) \cong \mathrm{End}_{\mathbb{Q}G} H_*(\Delta).$$

By Theorem 66.28, we have an isomorphism of vector spaces

$$\mathrm{End}_{\mathbb{Q}W} H_0(\Gamma) \cong \mathrm{End}_{\mathbb{Q}W} H_{n-1}(\Gamma) \cong \mathbb{Q},$$

and

$$\mathrm{Hom}_{\mathbb{Q}W}(H_i(\Gamma), H_j(\Gamma)) = 0 \quad \text{if } i + j \neq 0, 2(n - 1).$$

Upon carrying these results over to  $\mathrm{End}_{\mathbb{Q}G} H_*(\Delta)$ , and checking that  $H_0(\Delta)$  affords the trivial representation, we obtain the result. Note that the isomorphism  $\mathrm{End}_{\mathbb{Q}G} H_{n-1}(\Delta) \cong \mathbb{Q}$  implies, by (3.43), that the representation of  $G$  on  $H_{n-1}(\Delta)$  is absolutely irreducible.

**(66.34) Definition.** Let  $G$  be a finite group with a BN-pair of rank  $n$ . If  $n > 1$ , the *Steinberg representation*  $\mathrm{St}_G$  is the nontrivial absolutely irreducible  $\mathbb{Q}$ -representation of  $G$  afforded by the rational homology group  $H_{n-1}(\Delta)$ , where  $\Delta$  is the combinatorial building of  $G$ .

If  $n = 1$ ,  $\mathrm{St}_G$  is the unique nontrivial irreducible component of the permutation representation of  $G$  afforded by the  $G$ -set  $G/B$ .

The character of  $G$  afforded by the Steinberg representation will also be denoted by  $\mathrm{St}_G$ .

Corresponding to Solomon's formula (66.29) for the sign representation of  $W$ , we have the following formula for the character  $\mathrm{St}_G$  (see Curtis [66]).

**(66.35) Theorem.** *The character  $\mathrm{St}_G$  of the Steinberg representation of a finite group with a BN-pair is given by*

$$\mathrm{St}_G = \sum_{J \subseteq S} (-1)^{|J|} (1_{P_J})^G.$$

*Proof.* As in the proof of (66.29), it can be shown (see Exercise 3) that the homology  $H_*(\Delta)$  can be derived from a chain complex  $C = \bigoplus_{r \geq 0} C_r$ , in which the vector space of  $r$ -chains  $C_r$  has a basis indexed by the parabolic groups of the form  ${}^g P_I$ , with  $|I| = n - r - 1$ . Since  $N_G(P_I) = P_I$  for all  $I \subset R$  by (65.19), it follows that for  $g \in G$ ,

$$\mathrm{Tr}(g, C_r) = \sum_{|I|=n-r-1} (1_{P_I})^G(g).$$

The formula for  $\mathrm{St}_G$  now follows by the Hopf Trace Formula, exactly as in the proof of (66.29).

**Remarks.** A more elementary approach to the formula for the character  $\text{St}_G$ , independent of the theory of homology representations, was given by Curtis [66], and will be presented in §67 as part of the discussion of the Hecke algebra  $\mathcal{H}(G, B)$ . This approach gives the character  $\text{St}_G$ , but not the module which affords the character. For another construction of the module affording  $\text{St}_G$ , see Steinberg [56], [57].

For the group  $G$  of  $\mathbb{F}_q$ -rational points on a connected reductive affine algebraic group defined over a finite field  $\mathbb{F}_q$ , the values of the Steinberg character on arbitrary elements of  $G$  have been computed using the Lefschetz character of the homology representation  $H_*(\Delta)$ , together with Proposition 66.14 (see Curtis-Lehrer-Tits [80]). In §71, we shall give a different approach to the problem of calculating the values of  $\text{St}_G$ , due to Alvis.

## §66. Exercises

- (Steinberg) Let  $\mathcal{H} = \{H_1, \dots, H_t\}$  be a finite set of distinct hyperplanes in a real Euclidean space  $V$ , each containing the origin (see §64A). Let  $\mathcal{C}$  denote the set of equivalence classes  $\{c\}$  defined by the equivalence relation on  $V$  which puts  $v \sim v'$ , for  $v, v' \in V$ , provided that, for each hyperplane  $H_i \in \mathcal{H}$ , either  $v$  and  $v'$  both belong to  $H_i$ , or both lie on the same side of  $H_i$  (in the sense that  $\langle v, \alpha_i \rangle$  and  $\langle v', \alpha_i \rangle$  are both nonzero and of the same sign, where  $\langle \alpha_i \rangle^\perp = H_i$ ). For each element  $c \in \mathcal{C}$ , let  $\dim c$  be the dimension of the subspace of  $V$  generated by the elements of  $c$ . Let  $N_i$  denote the number of equivalence classes  $c \in \mathcal{C}$  of dimension  $i$ , for  $i \geq 0$ . Prove that

$$\sum_{i \geq 0} (-1)^i N_i = (-1)^{\dim V}.$$

[Hint: Use induction on the number of hyperplanes. The proof of the induction step goes as follows. Let  $\mathcal{H}$  be a set consisting of  $t$  hyperplanes, and let  $\mathcal{H}'$  be a set containing  $\mathcal{H}$  and one additional hyperplane  $H$ . Let  $\mathcal{C}$  and  $\mathcal{C}'$  be the sets of equivalence classes defined by  $\mathcal{H}$  and  $\mathcal{H}'$ , respectively. Prove that each element  $c \in \mathcal{C}$  of dimension  $i$ , whose interior is divided into two parts by  $H$ , yields two elements of  $\mathcal{C}'$  of dimension  $i$  and one element  $c \cap H \in \mathcal{C}'$  of dimension  $i - 1$ .]

- Prove Solomon's formula (66.29) using the preceding exercise.

[Hint: Let  $W = W(\Phi)$ , for a root system  $\Phi$  in a real Euclidean space  $V$ . Let  $\mathcal{H}$  be the set of hyperplanes  $\langle \alpha \rangle^\perp$ , for roots  $\alpha \in \Phi$ , and let  $\mathcal{C}$  be the set of equivalence classes defined by  $\mathcal{H}$ , as in Exercise 1. Let  $w \in W$ , and let  $U = \{v \in V : wv = v\}$ . Using (66.22), prove that  $U$  is the union of all elements  $c \in \mathcal{C}$  that are fixed by  $w$ . Apply Exercise 1 to  $U$ , and obtain  $\sum (-1)^i N_i = (-1)^{\dim U}$ . Using (66.22) again, prove that

$$N_i = \sum_{J, n-|J|=i} (1_{w_J})^W(w), \quad (n = \dim V)$$

for each  $i$ , and hence

$$\sum_J (-1)^{n-|J|} (1_{w_J})^W(w) = (-1)^{\dim U}.$$

On the other hand,

$$\det w = (-1)^{n - \dim U},$$

by standard properties of orthogonal transformations.]

3. Let  $G$  be a finite group with a  $BN$ -pair, of rank greater than one. Define a simplicial complex  $\Delta'$  as follows: the vertices of  $\Delta'$  are the maximal parabolic subgroups of  $G$ , and a set of maximal parabolic subgroups defines a simplex in  $\Delta'$  if and only if their intersection is parabolic. Prove the following statements. (i) The  $r$ -simplices of  $\Delta'$  form a  $G$ -set that is isomorphic to the  $G$ -set consisting of all parabolic subgroups  ${}^g P_I$ ,  $|I| = n - r - 1$ . (ii)  $Sd(\Delta') \cong \Sigma(\Delta)$ , where  $\Delta$  is the combinatorial building of  $G$ , and  $\Sigma(\Delta)$  is the simplicial complex associated with  $\Delta$  as in §66A. (For this interpretation of  $\Delta$ , see Tits [74].)

## §67. THE HECKE ALGEBRA $\mathcal{H}(G, B)$ AND THE DECOMPOSITION OF $(1_B)^G$

In this section, we continue to explore the connections between the representations of a finite group of Lie type  $G$  and the representations of the Weyl group  $W$  of  $G$ . This time we consider the decomposition of the permutation representation of  $G$  on the cosets of a Borel subgroup  $B$ , through the study of the Hecke algebra  $\mathcal{H}(G, B, 1_B)$ , denoted here by  $\mathcal{H}$ . It is shown that  $\mathcal{H}$  has a presentation as a C-algebra with generators and relation that are the exact counterparts of the defining relations of  $W$  given by the Coxeter system  $(W, S)$ . This fact is of crucial importance for the construction of representations of  $\mathcal{H}$  and the corresponding representations of  $G$  (see §11D). In particular, the representations of  $\mathcal{H}$  are calculated for the case of a  $BN$ -pair of rank 2, and applied to the incidence algebra of a generalized polygon, a proof of the Feit–Higman theorem on generalized polygons, and a construction of the reflection representation of the Hecke algebra  $\mathcal{H}$ .

### §67A. The Structure of the Hecke Algebra $\mathcal{H}(G, B)$

Throughout this section,  $G$  denotes a finite group with a  $BN$ -pair,  $W$  the Weyl group of  $G$ , and  $S$  the set of distinguished generators of  $W$ . Let

$$G = \bigcup_{w \in W} BwB$$

be the Bruhat decomposition of  $G$  with respect to a Borel subgroup  $B$  (see (65.4)). We recall that the pair  $(W, S)$  is a Coxeter system (see (65.9) and (64.17)). Thus the group  $W$  has a presentation

$$W = \langle s_1, \dots, s_n : (s_i s_j)^{m_{ij}} = 1 \quad \text{for all } i, j \rangle,$$

where  $S = \{s_1, \dots, s_n\}$ , and the  $\{m_{ij}\}$  are positive integers such that  $m_{ii} = 1$  and  $m_{ij} = m_{ji}$  for all  $i, j$ . This means that in order to construct representations

$T: W \rightarrow GL(M)$  on a vector space  $M$ , it is sufficient to find elements  $\{T_i\}_{1 \leq i \leq n}$  in  $GL(M)$  satisfying the defining relations of  $W$ :

$$T_i^2 = 1, (T_i T_j)^{m_{ij}} = 1 \quad \text{for all } i, j.$$

Then the map  $s_i \mapsto T_i$ ,  $1 \leq i \leq n$ , can be extended to a representation  $T$ .

Our aim is to prove that the Hecke algebra  $\mathcal{H}(G, B) = \mathcal{H}(G, B, 1_B)$  has a presentation, as an algebra, similar to the presentation of the group  $W$ . Using this presentation, representations of  $\mathcal{H}(G, B)$  can be constructed, and used to decompose the permutation representation  $(1_B)^G$ , by the methods of §11D.

We shall denote the Hecke algebra  $\mathcal{H}(G, B)$  by  $\mathcal{H}$ . Recall that  $\mathcal{H}$  is a semisimple subalgebra of the complex group algebra  $\mathbb{C}G$ , defined as

$$\mathcal{H} = e\mathbb{C}Ge,$$

where  $e = |B|^{-1} \sum_{b \in B} b$  is the idempotent in  $\mathbb{C}B$  such that the left ideal  $\mathbb{C}Ge$  affords the permutation representation  $(1_B)^G$ . The algebra  $\mathcal{H}$  is isomorphic to the opposite algebra of the centralizer ring  $\text{End}_{\mathbb{C}G}\mathbb{C}Ge$ . Thus the representations and characters of  $\mathcal{H}$  are closely related to the characters  $\zeta \in \text{Irr } G$  for which  $(\zeta, (1_B)^G) \neq 0$  (see Theorem 11.25).

The first step in analyzing the structure of  $\mathcal{H}$  is to examine the *standard basis* of  $\mathcal{H}$ , consisting of the elements

$$a_D = |B|^{-1} \sum_{x \in D} x, \quad D \in B \backslash G/B \quad (\text{see (11.34)}).$$

Since there is a bijective map  $w \leftrightarrow BwB$  from  $W$  to the double cosets  $B \backslash G/B$ , we shall label the standard basis elements by the elements of  $W$ , and denote them by  $\{a_w\}_{w \in W}$ . Their multiplication will be derived from the results in §65A.

For each  $w \in W$ , we define its *index*

$$\text{ind } w = |B : {}^w B \cap B|,$$

using our convention from §65A that  ${}^w B$  stands for  ${}^{\dot{w}} B$ , where  $\dot{w}$  is a coset representative in  $N$  corresponding to an element  $w \in N/T$ . In particular, the *index parameters* of  $G$  are defined to be the numbers

$$(67.1) \quad q_i = \text{ind } s_i, \quad 1 \leq i \leq n,$$

where  $S = \{s_1, \dots, s_n\}$  is the set of distinguished generators of  $W$ .

As in §§64 and 65, let  $l(w)$  denote the length function on the Coxeter group  $W$ . We now have:

**(67.2) Theorem (Iwahori [64]).** *The multiplication of the standard basis elements  $\{a_w = |B|^{-1} \sum_{x \in BwB} x, w \in W\}$  of  $\mathcal{H}$  satisfies*

$$a_s a_w = a_{s.w} \quad \text{if} \quad l(s_i w) > l(w),$$

and

$$a_{s_i}a_w = q_i a_{s_i w} + (q_i - 1)a_w \quad \text{if } l(s_i w) < l(w),$$

for all  $s_i \in S$  and  $w \in W$ , where the  $\{q_i\}$  are the index parameters given in (67.1).

*Proof.* Multiplication in  $\mathcal{H}$  is given by

$$a_u a_v = \sum_{w \in W} \mu_{uvw} a_w \quad \text{for } u, v \in W,$$

where the  $\mu$ 's are structure constants satisfying

$$\mu_{uvw} = |B|^{-1} |BuB \cap w(BvB)^{-1}|,$$

by (11.34).

In case  $l(s_i w) > l(w)$ , we have  $s_i B w \subseteq B s_i w B$  by (65.5), so the product  $a_{s_i} a_w$  is supported on the double coset  $B s_i w B$ . We therefore have

$$a_{s_i} a_w = \mu a_{s_i w},$$

where  $\mu$  is the structure constant

$$\mu = |B|^{-1} |Bs_i B \cap s_i w B w^{-1} B| = |B|^{-1} |s_i B s_i B \cap w B w^{-1} B|.$$

Since  $s_i B s_i \subset B \cup B s_i B$  by (65.2), and  $B \subseteq w B w^{-1} B$ , the first statement of the theorem (that  $\mu = 1$ ) will follow once we prove that

$$Bs_i B \cap w B w^{-1} B = \emptyset \quad \text{if } l(s_i w) > l(w).$$

Suppose this is false, and let

$$w = s_{j(1)} \cdots s_{j(p)}, \quad s_{j(k)} \in S, \quad 1 \leq k \leq p.$$

By the first formula in the proof of (65.8), we have

$$Bs_i B = BwyB,$$

where  $y$  is a product of some factors of  $w^{-1}$ , so  $l(y) \leq l(w)$ . By (65.4) we have

$$s_i = wy, \quad \text{and} \quad w^{-1}s_i = y.$$

Thus if  $l(w) = p$ , so  $s_{j(1)} \cdots s_{j(p)}$  is a reduced product, then  $l(w^{-1}s_i) = l(s_i w) \leq p$ , contrary to assumption. Thus  $\mu = 1$ , proving the first formula.

We next establish

$$(67.3) \quad a_{s_i}^2 = q_i a_1 + (q_i - 1)a_{s_i} \quad \text{for all } s_i \in S.$$

Since

$$(Bs_iB)(Bs_iB) \subseteq B \cup Bs_iB,$$

we have

$$a_{s_i}^2 = \eta a_1 + \lambda a_{s_i}, \quad \eta, \lambda \in \mathbb{C},$$

where the structure constant  $\eta$  satisfies

$$\eta = |B|^{-1} |Bs_iB \cap Bs_iB| = \text{ind } s_i = q_i.$$

By Exercise 11.19, the map  $\text{ind}: \mathcal{H} \rightarrow \mathbb{C}$  is a homomorphism of algebras. Upon applying  $\text{ind}$  to the formula for  $(a_{s_i})^2$ , we obtain

$$q_i^2 = q_i + \lambda q_i,$$

since  $\eta = q_i$  and  $\text{ind } a_1 = 1$ . It follows that  $\lambda = q_i - 1$ , proving (67.3).

Finally, let  $l(s_i w) < l(w)$ , and put  $w' = s_i w$ . Then  $l(s_i w') > l(w')$ , and by the first part of the proof we have

$$a_w = a_{s_i} a_{w'}.$$

Then

$$a_{s_i} a_w = a_{s_i}^2 a_{w'} = q_i a_{w'} + (q_i - 1) a_{s_i} a_{w'} = q_i a_{s_i w} + (q_i - 1) a_{w'},$$

completing the proof of the theorem.

**(67.4). Corollary.** *The Hecke algebra  $\mathcal{H}$  is generated by elements  $\{1 = a_1, a_{s_1}, \dots, a_{s_n}\}$ , where  $S = \{s_1, \dots, s_n\}$ . These generators satisfy the quadratic relations*

$$a_{s_i}^2 = q_i 1 + (q_i - 1) a_{s_i}, \quad 1 \leq i \leq n,$$

and the homogeneous relations

$$(a_{s_i} a_{s_j})^{k_{ij}} = (a_{s_j} a_{s_i})^{k_{ij}} \quad \text{if } m_{ij} = 2k_{ij}, \\ (a_{s_i} a_{s_j})^{k_{ij}} a_{s_i} = (a_{s_j} a_{s_i})^{k_{ij}} a_{s_j} \quad \text{if } m_{ij} = 2k_{ij} + 1,$$

where  $m_{ij}$  is the order of  $s_i s_j$  in  $W$ .

**(67.5) Corollary.** *If  $s_i$  is conjugate to  $s_j$  in  $W$ , then  $q_i = q_j$ .*

The proofs of both corollaries are left as exercises.

**(67.6) Theorem (Iwahori, Matsumoto).** *The generators and relations given in (67.4) define a presentation of the Hecke algebra  $\mathcal{H}$ .*

*Proof.* We have to prove that if  $A$  is an associative  $C$ -algebra containing elements  $\{a_1, \dots, a_n\}$  satisfying the relations in (67.4), then there exists a homomorphism of algebras  $f: \mathcal{H} \rightarrow A$  such that  $f(a_{s_i}) = a_i$ ,  $1 \leq i \leq n$ . By Matsumoto's Theorem 64.20, there exists a map  $f': W \rightarrow A$  such that  $f'(s_i) = a_i$ ,  $1 \leq i \leq n$ , and such that

$$f'(s_{i(1)} \cdots s_{i(m)}) = a_{i(1)} \cdots a_{i(m)}$$

for every reduced product  $s_{i(1)} \cdots s_{i(m)}$  of elements of  $S$ . Since the elements  $\{a_w\}_{w \in W}$  form a basis for  $\mathcal{H}$ , there exists a linear map  $f: \mathcal{H} \rightarrow A$  such that  $f(a_w) = f'(w)$ , for  $w \in W$ . It is then sufficient to prove that

$$(67.7) \quad f(a_{s_i} a_w) = f(a_{s_i}) f(a_w)$$

for all  $s_i \in S$  and  $w \in W$ . We now imitate the last part of the proof of Theorem 64.26. First assume  $l(s_i w) > l(w)$ . Then a reduced expression for  $s_i w$  is obtained from a reduced expression for  $w$  by left multiplication by  $s_i$ , and the result (67.7) follows by the definition of  $f$ , since  $a_{s_i} a_w = a_{s_i w}$  by (67.2). Next assume  $l(s_i w) < l(w)$ , and let  $w' = s_i w$ . Then  $l(s_i w') > l(w')$ , and by the first part of the proof, we have

$$f(a_w) = f(a_{s_i} a_{w'}) = f(a_{s_i}) f(a_{w'}),$$

since  $a_{s_i} a_{w'} = a_w$  by (67.2). By assumption, the elements  $f(a_{s_i})$  also satisfy the quadratic relations in (67.4), whence

$$\begin{aligned} f(a_{s_i}) f(a_w) &= f(a_{s_i})^2 f(a_{w'}) \\ &= q_i f(a_{w'}) + (q_i - 1) f(a_{s_i}) f(a_{w'}) \\ &= q_i f(a_{s_i w}) + (q_i - 1) f(a_w) \end{aligned}$$

by the first part of the proof again, since  $l(s_i w') > l(w')$  and  $w' = s_i w$ . On the other hand,

$$a_{s_i} a_w = q_i a_{s_i w} + (q_i - 1) a_w$$

by (67.2). We then obtain (67.7), in this case, by applying  $f$  to the last relation and comparing with the previous formula. This completes the proof.

**Remark.** The quadratic relations

$$a_{s_i}^2 = q_i a_1 + (q_i - 1) a_{s_i}, \quad 1 \leq i \leq n,$$

can also be expressed in the form

$$(a_{s_i} - q_i)(a_{s_i} + 1) = 0, \quad 1 \leq i \leq n.$$

Thus in order to construct representations of the Hecke algebra  $\mathcal{H}$ , it is sufficient

to map the generators to matrices  $T_i$ ,

$$a_{s_i} \rightarrow T_i, \quad 1 \leq i \leq n,$$

such that each matrix  $T_i$  has eigenvalues either  $q_i$  or  $-1$ , and such that these matrices satisfy the homogeneous relations. The simplest examples are the one-dimensional representations of  $\mathcal{H}$ , one of which is the *index homomorphism*

$$\text{ind}: \mathcal{H} \rightarrow \mathbb{C}$$

defined by

$$\text{ind } a_{s_i} = q_i, \quad 1 \leq i \leq n.$$

Another one-dimensional representation is the *sign representation*

$$\text{sgn}: \mathcal{H} \rightarrow \mathbb{C}$$

defined by

$$\text{sgn } a_{s_i} = -1, \quad 1 \leq i \leq n.$$

By Exercise 11.19, the index homomorphism corresponds to the trivial representation  $1_G$ , according to (11.25). We shall show in the next subsection that  $\text{sgn}$  corresponds to the Steinberg representation, defined in (66.34).

## §67B. The Sign Representation of $\mathcal{H}$ and the Steinberg Representation of $G$

As in the previous subsection,  $G$  denotes a finite group with a  $BN$ -pair, with Borel subgroup  $B$  and Weyl group  $W$ . We shall construct the character of the representation of  $G$  corresponding to the sign representation of the Hecke algebra  $\mathcal{H} = \mathcal{H}(G, B, 1_G)$ , defined in §67A. It will turn out to be the character of the Steinberg representation  $\text{St}_G$ , for which a construction was given in §66C using homology representations. The discussion to follow, which establishes further properties of  $\text{St}_G$ , is independent of homology representations, except that we require Solomon's formula (66.29) for the sign representation of  $W$  (see also Exercise 66.2).

**(67.8) Lemma.** *Let  $G$  be a transitive permutation group on each of the two finite sets  $X$  and  $Y$ , and let  $H$  and  $K$  be stabilizers of a point in  $X$  and  $Y$ , respectively. Let  $\psi$  and  $\theta$  be the permutation characters of  $G$  defined by the permutation representations on  $X$  and  $Y$ , respectively. Then*

$$(\psi, \theta) = |H \backslash G/K|.$$

*Proof.* By Proposition 1.20, there are isomorphisms of  $G$ -sets  $X \cong G/H$  and  $Y \cong G/K$ , and we have  $\psi = (1_H)^G$ ,  $\theta = (1_K)^G$ . The number of double cosets

$|H \backslash G/K|$  is the number of  $H$ -orbits in  $G/K$ . Thus

$$|H \backslash G/K| = (1_H, (1_K)^G|_H)_H = ((1_H)^G, (1_K)^G)_G = (\psi, \theta)_G,$$

by Frobenius reciprocity (10.9), completing the proof. (The result is also a consequence of the intertwining number theorem (10.24). Another proof is outlined in Exercise 10.2.)

The next result shows how to use the lemma to construct certain virtual characters of  $G$  from virtual characters of  $W$ , using information about double cosets of parabolic subgroups (see (65.21)). As in §65C, we denote standard parabolic subgroups of  $W$  by  $\{W_J\}_{J \subseteq S}$ , and the corresponding parabolic subgroups of  $G$  by  $\{P_J\}_{J \subseteq S}$ .

**(67.9) Proposition.** *The correspondence*

$$\xi = \sum_{J \subseteq S} n_J (1_{W_J})^W \rightarrow \hat{\xi} = \sum_{J \subseteq S} n_J (1_{P_J})^G, \quad \text{where each } n_J \in \mathbb{Z},$$

defines a mapping of virtual characters of  $W$  to virtual characters of  $G$  that preserves scalar products. Thus

$$(\xi, \eta)_W = (\hat{\xi}, \hat{\eta})_G$$

for two virtual characters  $\xi, \eta \in \text{ch } CW$  of the above form. In particular,

$$\xi \in \text{Irr } W \Rightarrow \pm \hat{\xi} \in \text{Irr } G.$$

*Proof.* By (65.21), there is a bijection

$$W_I \backslash W / W_J \leftrightarrow P_I \backslash G / P_J \quad \text{for all } I, J \subseteq S.$$

Moreover, by Lemma 67.8, we have

$$(\xi, \xi')_W = \sum_{I, J \subseteq S} n_I n'_J ((1_{W_I})^W, (1_{W_J})^W) = \sum_{I, J \subseteq S} n_I n'_J |W_I \backslash W / W_J|,$$

while

$$(\hat{\xi}, \hat{\xi}')_G = \sum_{I, J \subseteq S} n_I n'_J |P_I \backslash G / P_J|,$$

for virtual characters  $\xi, \xi'$  as above. In particular,

$$\xi = \xi' \Leftrightarrow (\xi - \xi', \xi - \xi')_W = 0 \Leftrightarrow (\hat{\xi} - \hat{\xi}', \hat{\xi} - \hat{\xi}')_G = 0 \Leftrightarrow \hat{\xi} = \hat{\xi}'.$$

It follows that  $\xi \rightarrow \hat{\xi}$  is a bijection for virtual characters of the above form, and preserves scalar products. This completes the proof.

**Remark.** If  $G = GL_{n+1}(\mathbb{F}_q)$ , then by §65B, we have  $W \cong S_{n+1}$ . In this case, a result of Frobenius (see §75B) asserts that every irreducible character of  $W$  is a  $\mathbb{Z}$ -linear combination of the characters  $(1_{W_J})^W$ ,  $J \subseteq S$ . Thus (67.9) provides the basis for an explicit construction, due to Steinberg [51], of all characters  $\zeta \in \text{Irr } G$  such that  $(\zeta, (1_B)^G) > 0$ . On the other hand, for a Weyl group of type  $B_2$  (the dihedral group of order 8), only the trivial character and the sign character can be expressed in this way. Nevertheless, the preceding result always produces at least one nontrivial irreducible character of  $G$ .

**(67.10) Theorem.** Let  $G$  be a finite group with a BN-pair, and Coxeter system  $(W, S)$ , and let  $\text{St}_G$  be the virtual character defined by

$$\text{St}_G = \sum_{J \subseteq S} (-1)^{|J|} (1_{P_J})^G.$$

Then the following statements hold:

$$(i) \quad \text{St}_G \in \text{Irr } G, \text{ and } \deg \text{St}_G = |B : B \cap {}^{w_0}B|,$$

where  $w_0$  is the unique element of maximal length in  $W$  (see (64.16vi)).

(ii)  $\text{St}_G$  satisfies the conditions  $(\text{St}_G, (1_B)^G) = 1$ , and  $(\text{St}_G, (1_{P_J})^G) = 0$  for all  $J \neq \emptyset$ . Moreover,  $\text{St}_G$  is characterized by these multiplicities: If  $\zeta \in \text{Irr } G$  satisfies  $(\zeta, (1_B)^G) = 1$  and  $(\zeta, (1_{P_J})^G) = 0$  for all  $J \neq \emptyset$ , then  $\zeta = \text{St}_G$ .

(iii) The restriction  $\text{St}_G|_{\mathcal{H}}$  of  $\text{St}_G$  to the Hecke algebra  $\mathcal{H} = \mathcal{H}(G, B, 1_B)$  is the sign character  $\text{sgn}$  of  $\mathcal{H}$ , given by  $\text{sgn}(a_{s_i}) = -1$  for all  $s_i \in S$ .

*Proof.* (i) By (66.29) (see also Exercise 66.2), the sign character of  $W$  is given by the formula

$$\varepsilon = \sum_{J \subseteq S} (-1)^{|J|} (1_{W_J})^W.$$

By Proposition 67.9, it follows that  $\text{St}_G$ , as defined above, is a virtual character such that  $\pm \text{St}_G \in \text{Irr } G$ . We now calculate the degree  $\text{St}_G(1)$ , and show, in particular, that  $\text{St}_G(1) > 0$ , which implies that  $\text{St}_G \in \text{Irr } G$ . We use the formula

$$\text{St}_G(1) = \sum_{J \subseteq S} (-1)^{|J|} |G : P_J|,$$

and begin by showing that for each  $J \subseteq S$ , the index  $|G : P_J|$  is given by

$$(67.11) \quad |G : P_J| \doteq \sum_{x \in D_{\emptyset \cup J}} |B : B \cap {}^x B|,$$

where  $D_{\emptyset \cup J}$  is a set of distinguished double coset representatives (see (64.39)). It follows from (65.21) that

$$G = \bigcup_{x \in D_{\emptyset \cup J}} BxP_J.$$

By a familiar computation (see Volume I, p. 238), we then have

$$|BxP_J/P_J| = |B:B \cap {}^x P_J|, \quad x \in D_{\emptyset J}.$$

To obtain (67.11), it thus suffices to show that

$$B \cap {}^x P_J = B \cap {}^x B \quad \text{for all } x \in D_{\emptyset J}.$$

We have

$$P_J = \bigcup_{w \in W_J} BwB,$$

so (67.11) will follow if we can prove that

$$xBwBx^{-1} \cap B = \emptyset, \quad \text{for } w \in W_J, w \neq 1,$$

or equivalently, that

$$xBwB \cap Bx = \emptyset, \quad x \in D_{\emptyset J}, \quad w \in W_J, \quad w \neq 1.$$

By (64.38) we have  $l(xw) = l(x) + l(w)$  for all  $w \in W_J$  and for  $x \in D_{\emptyset J}$ , whence  $xBw \subset BxwB$ . Consequently,  $xBwB \cap Bx = \emptyset$  for  $w \in W_J, w \neq 1$ , by the uniqueness part of the Bruhat decomposition (65.4), completing the proof of (67.11).

Substituting (67.11) in the formula for  $\text{St}_G(1)$ , we obtain

$$\text{St}_G(1) = \sum_{J \subseteq S} (-1)^{|J|} \sum_{x \in D_{\emptyset J}} |B:B \cap {}^x B|.$$

By (64.38), it follows that an element  $x \in W$  belongs to  $D_{\emptyset J}$ , for  $J \subseteq S$ , if and only if  $l(xs_J) > l(x) \forall j \in J$ . Thus  $|B:B \cap {}^x B|$  appears in the formula for  $\text{St}_G(1)$  exactly  $\sum_{J \subseteq R(x)} (-1)^{|J|}$  times, where  $R(x) = \{s \in S : l(xs) \geq l(x)\}$ . Moreover,  $\sum_{J \subseteq R(x)} (-1)^{|J|} = 0$  for all  $x \in W$  such that  $R(x) \neq \emptyset$ . We also have  $R(x) = \emptyset$  for the unique element  $x = w_0$  of maximal length in  $W$  (see (64.16vi)). For this element  $w_0$ , the contribution to  $\text{St}_G(1)$  is  $|B:B \cap {}^{w_0} B|$ , and part (i) is proved.

(ii) The sign character  $\varepsilon$  of  $W$  has degree 1, whence  $(\varepsilon, 1_{\{\cdot\}}^W) = 1$  since  $1_{\{\cdot\}}^W$  is the regular character of  $W$ . We also have  $(\varepsilon, 1_{W_J}^W) = 0$  for  $J \neq \emptyset$ , by Frobenius reciprocity, since  $(\varepsilon|_{W_J}, 1_{W_J})_{W_J} = 0$  if  $J \neq \emptyset$ . We then apply the isometry of virtual characters given in Proposition 67.9 to obtain

$$(\text{St}_G, (1_B)^G) = 1, \quad (\text{St}_G, (1_{P_J})^G) = 0, \quad J \neq \emptyset,$$

since  $\text{St}_G$  corresponds to  $\varepsilon$  under the map defined in (67.9).

Now consider an arbitrary irreducible character  $\zeta$  of  $G$  satisfying the conditions

$$(\zeta, (1_B)^G) = 1, \quad (\zeta, (1_{P_J})^G) = 0, \quad J \neq \emptyset.$$

By the definition of  $\text{St}_G$  in part (i), we have

$$(\zeta, \text{St}_G) = \left( \zeta, \sum_{J \subseteq S} (-1)^{|J|} (1_{P_J})^G \right) = 1.$$

Therefore  $\zeta = \text{St}_G$ , completing the proof of part (ii).

(iii) By (11.25), the restriction  $\text{St}_G|_{\mathcal{H}}$  of  $\text{St}_G$  to the Hecke algebra  $\mathcal{H}$  is an irreducible character of degree  $(\text{St}_G, (1_B)^G) = 1$ . In order to prove that  $\text{St}_G|_{\mathcal{H}}$  is the sign character of  $\mathcal{H}$ , it is sufficient to show that

$$\text{St}_G(a_{s_i}) = -1 \quad \text{for all } s_i \in S.$$

By part (ii), we have  $(\text{St}_G, (1_B)^G) = 1$  and  $(\text{St}_G, (1_{P_{\{s_i\}}})^G) = 0$  for all  $s_i \in S$ . Then, by (11.21), we obtain

$$\text{St}_G(e_B) = 1 \quad \text{and} \quad \text{St}_G(e_{P_{\{s_i\}}}) = 0, \quad s_i \in S,$$

where  $e_B$  and  $e_{P_{\{s_i\}}}$  are the idempotents affording the trivial representations of  $B$  and  $P_{\{s_i\}}$ , respectively. Moreover,

$$P_{\{s_i\}} = B \cup Bs_iB.$$

Thus from  $\text{St}_G(e_{P_{\{s_i\}}}) = 0$  we have  $\text{St}_G(\sum_{x \in P_{\{s_i\}}} x) = 0$ , whence

$$\text{St}_G \left( \sum_{b \in B} b + \sum_{x \in Bs_iB} x \right) = 0.$$

Now

$$e_B = |B|^{-1} \sum_{b \in B} b, \quad a_{s_i} = |B|^{-1} \sum_{x \in Bs_iB} x, \quad s_i \in S,$$

so the preceding formula becomes

$$\text{St}_G(e_B) + \text{St}_G(a_{s_i}) = 0 \quad \text{for all } s_i \in S.$$

Therefore  $\text{St}_G(a_{s_i}) = -1$  for all  $s_i \in S$ , completing the proof.

As an example, we shall calculate the degrees of the Steinberg representations of the finite general linear groups, discussed in §65B. The result is as follows:

**(67.12) Proposition.** *Let  $\mathbb{F}_q$  be a finite field of  $q$  elements, where  $q$  is a power of the prime  $p$ , and let  $G = GL_{n+1}(\mathbb{F}_q)$ . Then the degree of the Steinberg character of  $G$  is given by*

$$\text{St}_G 1 = q^{n(n+1)/2} = |G|_p.$$

*Proof:* It is sufficient to prove the first equality, since the second is a standard exercise in elementary group theory. By (67.10), we have

$$\text{St}_G(1) = |B : B \cap {}^{w_0}B|,$$

where  $w_0$  is the element of maximal length in the Weyl group. Thus  $\text{St}_G(1) = \text{ind } a_{w_0}$ , where  $a_{w_0}$  is the standard basis element corresponding to  $w_0$  in the Hecke algebra  $\mathcal{H} = \mathcal{H}(G, B, 1_B)$ . By (65.10), the Weyl group of  $G$  is isomorphic to the symmetric group  $S_{n+1}$ , which is a g.g.r. associated with a root system  $\Delta$  of type  $A_n$ , by Exercise 64.1. Then  $l(w_0) = |\Delta_+| = n(n+1)/2$  by (64.16vi) and Exercise 64.1. Now let

$$w_0 = s_{i(1)} \cdots s_{i(m)}, \quad s_{i(j)} \in S,$$

be a reduced expression for  $w_0$ , where  $m = l(w_0) = n(n+1)/2$ . Using (67.2) repeatedly, we obtain

$$a_{w_0} = a_{s_{i(1)}} \cdots a_{s_{i(m)}}.$$

Then, since  $\text{ind}: \mathcal{H} \rightarrow \mathbb{C}$  is a homomorphism of algebras, we have

$$\text{ind } a_{w_0} = \text{ind } a_{s_{i(1)}} \cdots \text{ind } a_{s_{i(m)}} = q_{i(1)} \cdots q_{i(m)},$$

where the  $\{q_{i(j)}\}$  are the index parameters (67.1). It remains to compute the index parameters  $q_i = \text{ind } s_i = |B : {}^{s_i}B \cap B|$ ,  $s_i \in S$ . Using the coset representatives  $\{\dot{s}_i\}$  defined in the proof of (65.10), it is easily checked that  $\text{ind } s_i = |\mathcal{F}_q| = q$  for all  $s_i \in S$ . Therefore

$$\text{St}_G 1 = \text{ind } a_{w_0} = q^{n(n+1)/2},$$

as required.

**(67.13) Remark.** The fact that  $\text{St}_G(1) = |G|_p$  has many consequences, some of which we list here. By (18.28),  $\text{St}_G$  is an irreducible character of defect zero, and vanishes on the  $p$ -irregular elements of  $G$ . If  $(K, R, k)$  is a  $p$ -modular system, for  $K$  sufficiently large, then  $\text{St}_G$  is the  $K$ -character afforded by  $KM$ , for some indecomposable projective  $RG$ -module  $M$ . Moreover,  $\bar{M}$  is a simple projective  $kG$ -module.

We shall see later (in (69.9)) that  $\text{St}_G(1) = |G|_p$  for all finite groups  $G$  with split  $BN$ -pairs of characteristic  $p$ , and hence for all finite Chevalley groups.

### §67C. Representations of the Hecke Algebra $\mathcal{H}$ for a $BN$ -Pair of Rank 2

We begin with the determination, by Kilmoyer-Solomon [73], of the irreducible representations of the Hecke algebra  $\mathcal{H}(G, B, 1_B)$  for a finite group  $G$  with a  $BN$ -pair of rank 2. Using their results together with (11.32iii), we shall then indicate

how to calculate explicitly the degrees of all characters  $\zeta \in \text{Irr } G$  such that  $(\zeta, (1_B)^G) \neq 0$ ; these degrees will be expressed in terms of the index parameters (67.1).

In §67D, we give a second application of the Kilmoyer–Solomon results, namely, their proof of the Feit–Higman theorem [64] on generalized polygons. This result, in turn, is a crucial first step in the classification by Tits (see [74; p. 220]) of finite simple groups with  $BN$ -pairs of rank  $\geq 3$ .

As another application of these results, in §67E we shall give Kilmoyer's construction of the reflection representation of a finite group with a  $BN$ -pair (see Kilmoyer [69] and Curtis–Iwahori–Kilmoyer [71]).

Our first main objective is to prove the following theorem on the representations of certain algebras  $A$  whose presentation is analogous to that of Hecke algebras of  $BN$ -pairs of rank 2.

**(67.14) Theorem.** *Let  $m$  be a positive integer. Let  $A$  be a semisimple algebra over  $C$  of dimension  $2m$ , generated by two elements  $\{a_r, a_s\}$ , which satisfy the following relations:*

(a) (Quadratic relations)

$$a_r^2 = q_r 1 + (q_r - 1)a_r, \quad a_s^2 = q_s 1 + (q_s - 1)a_s,$$

for some positive real numbers  $q_r$  and  $q_s$  (called index parameters), and

(b) (Homogeneous relations)

$$\begin{aligned} (a_r a_s)^k &= (a_s a_r)^k && \text{if } m = 2k, \\ (a_r a_s)^k a_r &= (a_s a_r)^k a_s && \text{if } m = 2k + 1. \end{aligned}$$

Then we have:

*Case 1. If  $m = 2k$  is even, there are precisely 4 representations of  $A$  of degree 1, namely:*

$$\begin{cases} \text{index representation of } A, \text{ given by } \text{ind } a_r = q_r, \text{ ind } a_s = q_s; \\ \text{sign representation of } A, \text{ given by } \text{sgn } a_r = \text{sgn } a_s = -1; \\ a_r \rightarrow q_r, \quad a_s \rightarrow -1; \\ a_r \rightarrow -1, \quad a_s \rightarrow q_s. \end{cases}$$

All other irreducible representations of  $A$  have degree 2, and are given as follows. Set

$$\rho = \sqrt{q_r q_s}, \quad \theta_j = 2\pi j/m, \quad 1 \leq j \leq m,$$

and let  $\{c_j\}, \{d_j\}$  be complex numbers such that

$$c_j d_j = q_r + q_s + 2\rho \cos \theta_j \quad 1 \leq j \leq m.$$

For  $1 \leq j \leq k$ , where  $k = m/2$ , put

$$T_j(a_r) = \begin{pmatrix} -1 & c_j \\ 0 & q_r \end{pmatrix}, \quad T_j(a_s) = \begin{pmatrix} q_s & 0 \\ d_j & -1 \end{pmatrix}.$$

Then  $\{T_1, \dots, T_{k-1}\}$  are a full set of inequivalent irreducible two-dimensional representations of  $A$ .

*Case 2.* If  $m = 2k + 1$  is odd, we assume that  $q_r = q_s$ . Then there are precisely two representations of  $A$  of degree 1, namely, the representations  $\text{ind}$  and  $\text{sgn}$  defined above. Further, we define  $\rho$ ,  $\theta_j$ , and  $T_j$  as above. Then all other irreducible representations of  $A$  have degree 2, and are given (up to equivalence) by  $T_1, \dots, T_k$ .

**Remarks.** (i) Up to equivalence, the representation  $T_j$  does not depend on the choice of  $c_j$  and  $d_j$ , provided their product  $c_j d_j$  is equal to  $q_r + q_s + 2\rho \cos \theta_j$ .

(ii) In the special case  $q_r = q_s = 1$ , the algebra  $A$  is just the group algebra of a dihedral group  $D_m$  of order  $2m$ , with generators  $a_r$  and  $a_s$ , and the representations of  $A$  defined above are the irreducible complex representations of  $D_m$  (see (7.39) and (10.11)).

(iii) By Theorem 67.6, the Hecke algebra  $\mathcal{H} = \mathcal{H}(G, B, 1_B)$  of a finite group with a  $BN$ -pair of rank 2 has a presentation as in Theorem 67.14, with  $\{a_r, a_s\}$  the standard basis elements of  $\mathcal{H}$  corresponding to the distinguished generators  $\{r, s\}$  of the Weyl group  $W$  of  $G$ . In this case, the dimension of  $\mathcal{H}$  is  $2m$ , where  $m$  is the order of  $rs$  in  $W$ . The index parameters  $q_r$  and  $q_s$  in (67.14) coincide with the index parameters of  $G$  defined in (67.1), and satisfy the condition that  $q_r = q_s$  if  $m$  is odd, by (67.5). The Hecke algebra  $\mathcal{H}$  is semisimple, by the remark following Definition 11.22.

*Proof.* We first note that the algebra  $A$  has a presentation with the generators  $a_r$  and  $a_s$ , and relations (a) and (b). This observation holds since any algebra with two generators, satisfying the relations (a) and (b), is easily shown to have dimension  $\leq 2m$ , so the assumption that  $\dim A = 2m$  implies that  $A$  is the universal such algebra. We now discuss the cases separately.

*Case 1 ( $m = 2k$ ).* It is easily verified that the four displayed maps, defined on the generators of  $A$ , preserve the defining relations, and therefore give well-defined one-dimensional representations of  $A$ . Further, in any one-dimensional representation  $\varphi: A \rightarrow \mathbb{C}$ , the quadratic relations impose restrictions on the images  $\varphi(a_r)$ ,  $\varphi(a_s)$ , from which it follows readily that there are no other one-dimensional representations besides those defined previously.

For the discussion of the two-dimensional representations, we simplify the notation by omitting (for the moment) the subscript  $j$  from the symbols  $c_j$ ,  $d_j$ , and  $\theta_j$ , where  $1 \leq j \leq k$ . Let  $\mathbf{R}$ ,  $\mathbf{S}$  be the matrices given by

$$a_r \rightarrow \mathbf{R} = \begin{pmatrix} -1 & c \\ 0 & q_r \end{pmatrix}, \quad a_s \rightarrow \mathbf{S} = \begin{pmatrix} q_s & 0 \\ d & -1 \end{pmatrix}.$$

Since  $\mathbf{R}$  has eigenvalues  $\{-1, q_r\}$  and  $\mathbf{S}$  has eigenvalues  $\{-1, q_s\}$ , the quadratic relations are clearly satisfied by the matrices  $\mathbf{R}$  and  $\mathbf{S}$ . For the homogeneous relations, we first consider

$$\mathbf{RS} = \begin{pmatrix} -q_s + cd & -c \\ qr & -q_r \end{pmatrix} \quad \text{and} \quad \mathbf{SR} = \begin{pmatrix} -q_s & q_s c \\ -d & cd - q_r \end{pmatrix},$$

which both have the same characteristic polynomial

$$\begin{aligned} t^2 + (q_r + q_s - cd)t + qrq_s &= t^2 - 2\rho(\cos \theta)t + \rho^2 \\ &= (t - \rho e^{i\theta})(t - \rho e^{-i\theta}). \end{aligned}$$

Since  $0 < \theta < \pi$ , the eigenvalues  $\{\rho e^{\pm i\theta}\}$  of  $\mathbf{RS}$  and  $\mathbf{SR}$  are distinct, and there exists an invertible  $2 \times 2$  matrix  $\mathbf{P}$  such that

$$\mathbf{PRSP}^{-1} = \begin{pmatrix} \rho e^{i\theta} & 0 \\ 0 & \rho e^{-i\theta} \end{pmatrix} \quad (\text{and similarly for } \mathbf{SR})$$

Let  $\mathbf{R}' = \mathbf{PRP}^{-1}$ ,  $\mathbf{S}' = \mathbf{PSP}^{-1}$ , and  $\mathbf{D} = \mathbf{R}'\mathbf{S}' = \text{diag}(\rho e^{i\theta}, \rho e^{-i\theta})$ . Since  $m = 2k$  is even, we have  $e^{ik\theta} = e^{i\pi j} = e^{-ik\theta}$ , so that  $(\mathbf{R}'\mathbf{S}')^k = (\mathbf{S}'\mathbf{R}')^k = \pm \rho^k \mathbf{I}$ , and the homogeneous relation holds. The representation defined by the matrices  $\mathbf{R}$  and  $\mathbf{S}$  is irreducible, since  $A$  is semisimple, and the only matrices commuting with  $\mathbf{R}$  and  $\mathbf{S}$  are scalar multiples of  $\mathbf{I}$ . We also note that  $\text{Tr } \mathbf{RS} = 2\rho \cos \theta$ , so the characters of the representations  $\{T_1, \dots, T_{k-1}\}$  are distinct. The sum of the squares of the dimensions of the irreducible representation obtained so far is  $2m$ , and hence they form a basic set, by the results of §3 on split semisimple algebras.

*Case 2* ( $m = 2k + 1$ ). In this case we let  $q = q_r = q_s$ , and continue with the discussion of the matrices  $\mathbf{R}$  and  $\mathbf{S}$  defined in Case 1. Let

$$\mathbf{R}' = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}.$$

Then  $\det \mathbf{R}' = \det \mathbf{R} = -q$ ,  $\rho = q$ , and we have

$$\mathbf{S}' = (\mathbf{R}')^{-1} \mathbf{D} = \begin{pmatrix} -\delta e^{i\theta} & \beta e^{-i\theta} \\ \gamma e^{i\theta} & -\alpha e^{-i\theta} \end{pmatrix}.$$

Since  $\text{Tr } \mathbf{R} = \text{Tr } \mathbf{S} = q - 1$ , we have

$$\alpha + \delta = q - 1, \quad \alpha e^{-i\theta} + \delta e^{i\theta} = -(q - 1),$$

and it follows that  $\delta = -e^{-i\theta}\alpha$ . Then

$$\mathbf{S}' = \begin{pmatrix} \alpha & \beta e^{-i\theta} \\ \gamma e^{i\theta} & \delta \end{pmatrix}.$$

Using the fact that  $e^{(2k+1)i\theta} = 1$ , a direct computation shows that

$$\mathbf{D}^k \mathbf{R}' \mathbf{D}^{-k} = \mathbf{S}'.$$

Since  $\mathbf{D} = \mathbf{R}' \mathbf{S}'$ , this implies that

$$(\mathbf{R}' \mathbf{S}')^k \mathbf{R}' = \mathbf{S}' (\mathbf{R}' \mathbf{S}')^k,$$

proving the homogeneous relation. The rest of the proof is the same as in Case 1.

The next result can be used to calculate explicitly the degrees of the irreducible characters in  $(1_B)^G$ , for a finite group  $G$  with a  $BN$ -pair of rank 2 (using also the proof of (67.24) below).

**(67.15) Corollary.** *Let  $\mathcal{H}$  be the Hecke algebra  $\mathcal{H}(G, B, 1_B)$  of a finite group  $G$  with a  $BN$ -pair of rank 2. Let  $\varphi$  be the character of any of the irreducible representations of  $\mathcal{H}$  constructed in (67.14). Then  $\varphi$  is the restriction to  $\mathcal{H}$  of a unique irreducible character  $\zeta$  of  $G$  such that  $(\zeta, (1_B)^G) > 0$ . The degree of  $\zeta$  is given by*

$$\deg \zeta = (\deg \varphi) |G:B| / \sum_{w \in W} (\text{ind } a_w)^{-1} \varphi(a_w) \varphi(a_{w^{-1}}),$$

where the  $\{a_w\}$  are the standard basis elements of  $\mathcal{H}$ . The set of characters  $\{\zeta\}$  of  $G$  obtained in this way coincides with the set

$$\{\zeta \in \text{Irr } G : (\zeta, (1_B)^G) > 0\}.$$

The proof that  $\mathcal{H}$  satisfies the hypotheses of (67.14) was given in §67A, and explained in the remark following the statement of the theorem. The other statements follow from §11A (see (11.25) and (11.32)).

## §67D. The Feit-Higman Theorem on Generalized Polygons

The results of §67C apply not only to  $BN$ -pairs, but to other situations as well. In particular, certain finite geometries lead to algebras satisfying the hypotheses of (67.14), and the character theory of these algebras can be used to classify the geometries. As we mentioned in the introduction to §67C, we shall give such an application here to the theorem of Feit-Higman [64] on generalized polygons, following the simplified version of their proof by Kilmoyer-Solomon [73]. The proof will use the orthogonality relations derived in §9 for the irreducible characters of a split semisimple algebra, which in this case is neither a group algebra nor a Hecke algebra. The incidence algebras defined below are examples of algebras defined by combinatorial association schemes, also called coherent configurations (see Dembowski ([68, §7.1]), D.G. Higman [75], [76], and MacWilliams-Sloane [77]).

We define an *incidence structure*  $(P, L, F)$  to be a triple consisting of a set  $P$  of elements called *points*, a set  $L$  of elements called *lines*, and a subset  $F \subseteq P \times L$  of pairs  $(p, l)$  called *flags*. A point  $p$  is on a line  $l$ , or is *incident* to  $l$ , if  $(p, l)$  is a flag.

We assume throughout that  $P$  and  $L$  are finite sets, and that there are  $s + 1$  points on every line and  $t + 1$  lines incident to every point. If  $x = (p, l)$  and  $y = (q, m)$  are distinct flags, we write  $x \cap y = p$  if  $p = q$  and  $x \cap y = l$  if  $l = m$ . For each  $x \in F$ , define subsets  $S(x), T(x)$  of  $F$  by

$$S(x) = \{y \in F : x \cap y \in L\}, \quad T(x) = \{z \in F : x \cap z \in P\}.$$

Let  $V$  be the vector space over  $\mathbb{C}$  with the elements of  $F$  as basis, and define endomorphisms  $\sigma, \tau$  of  $V$  by

$$\sigma(x) = \sum_{y \in S(x)} y, \quad \tau(x) = \sum_{z \in T(x)} z.$$

Let  $A$  be the algebra of endomorphisms of  $V$  generated by  $\sigma$  and  $\tau$ ; we shall call  $A$  the *incidence algebra* associated with  $(P, L, F)$ .

**(67.16) Lemma.** *The endomorphisms  $\sigma$  and  $\tau$  satisfy*

$$\sigma^2 = s \cdot 1 + (s - 1)\sigma \quad \text{and} \quad \tau^2 = t \cdot 1 + (t - 1)\tau.$$

*Proof.* Let  $x = (p, l) \in F$ , and let  $p, p_1, \dots, p_s$  be the points on  $l$ . Then  $S(x)$  consists of the flags  $\{(p_1, l), \dots, (p_s, l)\}$ . For any one of the flags  $y = (p_i, l)$ ,  $p_i \neq p$ ,  $S(y)$  consists of the flags  $(p, l)$  and the flags  $(p_j, l)$  for  $j \neq i$ . Thus

$$\sigma(x) = \sum_i (p_i, l)$$

and

$$\sigma^2(x) = \sum_i \left[ (p, l) + \sum_{j \neq i} (p_j, l) \right] = s \cdot x + (s - 1)\sigma x.$$

The proof for  $\tau$  is similar.

Let  $(P, L, F)$  be an incidence structure, and let  $a, b \in P \cup L$ . A *chain* of length  $h$  from  $a$  to  $b$  is a sequence

$$a_0 = a, a_1, \dots, a_h = b$$

of elements from  $P \cup L$  such that  $a_i$  and  $a_{i+1}$  are incident, for  $0 \leq i \leq h - 1$ . The least integer  $h$  (if one exists) for which there is a chain of length  $h$  from  $a$  to  $b$  is called the distance  $\rho(a, b)$  from  $a$  to  $b$ .

**(67.17) Definition.** A *generalized  $m$ -gon* is an incidence structure  $(P, L, F)$  for which the following conditions hold:

- (i)  $\rho(a, b) \leq m$  for all  $a, b \in P \cup L$ .
- (ii) If  $\rho(a, b) = h < m$ , then there is only one chain of length  $h$  from  $a$  to  $b$ .
- (iii) For each  $a \in P \cup L$ , there exists an element  $b \in P \cup L$  such that  $\rho(a, b) = m$ .

Note that the vertices and edges of an ordinary  $m$ -gon satisfy (i)–(iii), with  $s = t = 1$ . Examples of generalized  $m$ -gons arising from finite groups with  $BN$ -pairs of rank 2 are described in Exercise 67.2.

We now work out the structure of the incidence algebra  $A$  associated with a generalized  $m$ -gon, and begin with some additional definitions. Two flags  $x, y$  are called *adjacent* if either  $x \cap y \in P$  or  $x \cap y \in L$ . A *gallery* of length  $h$  from  $x$  to  $y$  is a sequence

$$x_0 = x, x_1, \dots, x_h = y$$

of flags such that  $\{x_i, x_{i+1}\}$  are adjacent, for  $0 \leq i \leq h - 1$ . The *distance*  $d(x, y)$  between two flags is the least integer  $h$  for which there exists a gallery of length  $h$  from one to the other. A gallery from  $x$  to  $y$  is *minimal* if its length is  $d(x, y)$ ; in this case,  $x_{i-1} \cap x_i \in P$  implies  $x_i \cap x_{i+1} \in L$ , for each  $i$ . The following lemma follows easily from the axioms, and its proof is left as an exercise.

**(67.18) Lemma.** *Let  $(P, L, F)$  be a generalized  $m$ -gon, and let  $x, y \in F$ . Then:*

- (i)  $d(x, y) \leq m$ .
- (ii) If  $d(x, y) < m$ , there exists a unique minimal gallery from  $x$  to  $y$ .
- (iii) If  $d(x, y) = m$ , there exist exactly two minimal galleries  $x_0, \dots, x_m$  from  $x$  to  $y$ , where  $x_0 = x$  and  $x_m = y$ . For one of these minimal galleries,  $x_{m-1} \cap y \in P$ , while for the other we have  $x_{m-1} \cap y \in L$ .
- (iv) For each integer  $j > 0$ , let  $S_j(x)$  be the set of all flags  $y \in F$  such that  $d(x, y) = j$ , and such that if  $x_0, x_1, \dots, x_j$  is a minimal gallery from  $x$  to  $y$  then  $x_{j-1} \cap y \in L$ . Similarly,  $T_j(x)$  is the set of flags  $y$  for which  $d(x, y) = j$  and  $x_{j-1} \cap y \in P$ , for a minimal gallery  $\{x_0, \dots, x_j\}$  from  $x$  to  $y$ . Then we have:

$$S(x) = S_1(x), \quad T(x) = T_1(x),$$

$$S_j(x) \cap T_j(x) = \emptyset, \quad 1 \leq j \leq m - 1,$$

and

$$S_m(x) = T_m(x).$$

Now let  $1 \leq j \leq m$ . Then

- (v)  $y \in S_j(x) \Leftrightarrow$  there exists a unique  $z \in T_{j-1}(x)$  such that  $y \in S(z)$ .
- (vi)  $y \in T_j(x) \Leftrightarrow$  there exists a unique  $z \in S_{j-1}(x)$  such that  $y \in T(z)$ .
- (vii) If  $m$  is odd, then  $s = t$ .

We are now ready to prove:

**(67.19) Theorem.** *Let  $A$  be the incidence algebra associated with a generalized  $m$ -gon  $(P, L, F)$ . Then  $A$  is a semisimple algebra of dimension  $2m$ , and has a presentation as a  $\mathbb{C}$ -algebra with generators  $\{\sigma, \tau\}$ , and defining relations:*

$$\sigma^2 = s \cdot 1 + (s - 1)\sigma, \quad \tau^2 = t \cdot 1 + (t - 1)\tau$$

and

$$\begin{cases} (\sigma\tau)^k = (\tau\sigma)^k & \text{if } m = 2k \text{ is even,} \\ (\sigma\tau)^k\sigma = (\tau\sigma)^k\tau & \text{if } m = 2k + 1 \text{ is odd.} \end{cases}$$

*Proof.* We first prove that  $A$  is semisimple. The matrices of the generators  $\sigma$  and  $\tau$  with respect to the basis  $F$  are clearly real symmetric matrices. It follows that the algebra  $A$ , viewed as a matrix algebra, is closed under the operations of taking transposes  $\mathbf{X} \rightarrow {}^t\mathbf{X}$  and complex conjugates  $\mathbf{X} \rightarrow \bar{\mathbf{X}}$ , where  $\bar{\mathbf{X}} = (\bar{x}_{ij})$  if  $\mathbf{X} = (x_{ij})$ . The radical  $\text{rad } A$  of the matrix algebra  $A$  is also closed under these operations. Now let  $\mathbf{X} \in \text{rad } A$ , so also  $\bar{\mathbf{X}} {}^t\mathbf{X} \in \text{rad } A$ . The diagonal entries of  $\bar{\mathbf{X}} {}^t\mathbf{X}$  are the squares of the norms of the rows of  $\mathbf{X}$ , in the usual metric. It follows that if  $\mathbf{X} \neq 0$ , then  $\text{Tr } \mathbf{X} {}^t\mathbf{X} \neq 0$ , which is impossible if the matrix  $\mathbf{X} {}^t\mathbf{X}$  is nilpotent. Since  $\text{rad } A$  consists of nilpotent matrices, we have  $\text{rad } A = 0$ , proving that  $A$  is semisimple.

Next define endomorphisms  $\sigma_j$  and  $\tau_j$  of  $V$  by

$$\sigma_j x = \sum_{y \in S_j(x)} y, \quad \tau_j x = \sum_{y \in T_j(x)} y.$$

By (67.18v), we have, for  $x \in F$ ,

$$\sigma\tau_{j-1}x = \sum_{z \in T_{j-1}(x)} \sigma z = \sum_{z \in T_{j-1}(x)} \sum_{y \in S(z)} y = \sum_{y \in S_j(x)} y = \sigma_j x,$$

proving that  $\sigma\tau_{j-1} = \sigma_j$ . Similarly  $\tau\sigma_{j-1} = \tau_j$ . Since  $\sigma_1 = \sigma$  and  $\tau_1 = \tau$ , we have

$$\sigma_{2j-1} = (\sigma\tau)^{j-1}\sigma, \quad \sigma_{2j} = (\sigma\tau)^j, \quad \tau_{2j-1} = (\tau\sigma)^{j-1}\tau, \quad \tau_{2j} = (\tau\sigma)^j.$$

In particular, we have  $S_m(x) = T_m(x)$  by (67.18iv), so that  $\sigma_m = \tau_m$ , and the homogeneous relations in (67.19) hold. The quadratic relations were proved in (67.16).

It follows that  $A$  is generated as a vector space by the elements

$$(67.20) \quad 1, \sigma_1, \dots, \sigma_{m-1}, \tau_1, \dots, \tau_{m-1}, \quad \sigma_m = \tau_m,$$

so  $\dim A \leq 2m$ . On the other hand, the sets  $S_i(x) \cap S_j(x)$ ,  $T_i(x) \cap T_j(x)$ , and  $S_i(x) \cap T_j(x)$  are empty if  $i \neq j$ , and by (67.16)  $F$  is the disjoint union of the sets

$$S_0(x) = T_0(x) = \{x\}, \quad S_1(x), \dots, S_{m-1}(x), \quad T_1(x), \dots, T_{m-1}(x), \quad S_m(x) = T_m(x).$$

Thus the elements in (67.20) form a basis for  $A$ , and  $\dim A = 2m$ . The proof that  $A$  has the required presentation is the same as the first paragraph of the proof of (67.14), and we are finished.

We shall call the elements (67.20) the *standard basis* of  $A$ , and denote them by  $\{\beta_0, \beta_1, \dots, \beta_{2m-1}\}$ , with  $\beta_0 = 1$ . We next describe a dual basis to the standard basis with respect to a suitable bilinear form.

**(67.21) Proposition.** (i) *The incidence algebra  $A$  has a representation of degree 1, called  $\text{ind}$ , defined by*

$$\text{ind } \sigma = s, \quad \text{ind } \tau = t.$$

(ii) *The bilinear form  $B: A \times A \rightarrow \mathbb{C}$ , whose value at  $(a, a')$  is the coefficient of  $\beta_0$  in the expression of the product  $aa'$  in terms of the standard basis, is nondegenerate, associative, and symmetric (see §9A).*

(iii) *Let  $a \rightarrow \hat{a}$  be the transpose map in  $A$ . Then*

$$\hat{\sigma} = \tau, \quad \hat{\tau} = \sigma,$$

*and  $a \rightarrow \hat{a}$  is an antiautomorphism of  $A$ .*

(iv) *The dual basis of the standard basis, with respect to the bilinear form defined in part (ii), is*

$$\{\hat{\beta}_0 = 1, (\text{ind } \beta_1)^{-1} \hat{\beta}_1, \dots, (\text{ind } \beta_{2m-1})^{-1} \hat{\beta}_{2m-1}\}.$$

The proof follows easily from the definition of  $A$  and Theorem 67.19, and is left as an exercise for the reader. For two irreducible characters  $\mu, \mu'$  in  $\text{Irr } A$ , let us set

$$(67.22) \quad \langle \mu, \mu' \rangle = \sum_{i=0}^{2m-1} (\text{ind } \xi_i)^{-1} \mu(\xi_i) \mu'(\hat{\xi}_i).$$

Then we have, by Propositions (67.21) and (9.19):

**(67.23) Corollary.** *Let  $\mu, \mu'$  be distinct irreducible characters of  $A$ . Then  $\langle \mu, \mu' \rangle = 0$ .*

The main results of this subsection are the following three theorems, due to Feit-Higman [64].

**(67.24) Feit-Higman Theorem.** *Let  $(P, L, F)$  be a generalized  $m$ -gon, with  $s+1$  points on each line, and  $t+1$  lines through each point. Then either  $s=t=1$  and  $(P, L, F)$  is an ordinary polygon, or else  $m \in \{2, 3, 4, 6, 8, 12\}$ . If  $s > 1$  and  $t > 1$ , then  $m \in \{2, 3, 4, 6, 8\}$ . Moreover,  $st$  is a square if  $m=6$ , while  $2st$  is a square if  $m=8$ .*

**(67.25) Theorem.** *Let  $G$  be a finite group with a BN-pair of rank 2, whose Weyl group is a dihedral group of order  $2m$ . Then  $m \in \{2, 3, 4, 6, 8\}$ .*

**(67.26) Theorem.** *The Weyl group of a finite group with a BN-pair is a direct product of a number (possibly zero) of dihedral groups of order 16 and the Weyl group of a semisimple Lie algebra over  $\mathbb{C}$ .*

Before proving (67.24) and (67.25), we note that Theorem (67.26) follows from (67.25), using the fact that the Weyl group of a finite group with a BN-pair is a Coxeter group (by Theorem 65.9).

We now begin the proof of Theorem 67.24. The idea is to compute explicitly the characters of the incidence algebra  $A$  of a generalized  $m$ -gon, using Theorem 67.14. Some details are omitted and can be found in Kilmoyer-Solomon [73]. We first note that  $A$  satisfies the hypothesis of Theorem 67.14, with  $\{\sigma, \tau\}$  in place of the generators  $a_r$  and  $a_s$ , and  $s$  and  $t$  instead of the index parameters  $q_r$  and  $q_s$ . By (67.14), the irreducible representations of  $A$  of degree 2 are given as follows. Let

$$\rho = \sqrt{st}, \quad \theta_j = 2\pi j/m, \quad 1 \leq j \leq m,$$

and let  $\{c_j, d_j\}$  be complex numbers such that

$$c_j d_j = s + t + 2\rho \cos \theta_j, \quad 1 \leq j \leq m.$$

For  $1 \leq j \leq k$ , put

$$\mathbf{T}_j(\sigma) = \begin{pmatrix} -1 & c_j \\ 0 & s \end{pmatrix}, \quad \mathbf{T}_j(\tau) = \begin{pmatrix} t & 0 \\ d_j & -1 \end{pmatrix}.$$

Then the  $\{\mathbf{T}_j\}$  define a complete set of irreducible representations of  $A$  of degree 2, by (67.14). For each  $j$ , let  $\mu_j$  be the character of  $\mathbf{T}_j$ . Then it is readily shown, using the proof of (67.14), that

$$\mu_j(\sigma_{2i}) = \mu_j(\tau_{2i}) = 2\rho^i \cos i\theta_j, \quad 1 \leq i \leq k,$$

and that

$$\mu_j(\sigma_{2i+1}) = \rho^{i-1} (\sin \theta_j)^{-1} (s(t-1) \sin i\theta_j + \rho(s-1) \sin (i+1)\theta_j),$$

while

$$\mu_j(\tau_{2i+1}) = \rho^{i-1} (\sin \theta_j)^{-1} (t(s-1) \sin i\theta_j + \rho(t-1) \sin (i+1)\theta_j).$$

We use these formulas to compute the scalar products  $\langle \mu_j, \mu_j \rangle$  of the characters

$\{\mu_J\}$ , defined in (67.22). The computation becomes, in case  $m = 2k$ ,

$$\begin{aligned}\langle \mu_j, \mu_j \rangle &= \sum_{i=0}^{k-1} [(\text{ind } \sigma_{2i})^{-1} \mu_j(\sigma_{2i})^2 + (\text{ind } \tau_{2i})^{-1} \mu_j(\tau_{2i})^2 \\ &\quad + (\text{ind } \sigma_{2i+1})^{-1} \mu_j(\sigma_{2i+1})^2 + (\text{ind } \tau_{2i+1})^{-1} \mu_j(\tau_{2i+1})^2],\end{aligned}$$

since  $\mu_j(a) = \mu_j(\bar{a})$  for all  $a \in A$ ; a similar formula holds in case  $m = 2k + 1$ . The sums are easily computed using the character values, converting the trigonometric functions to exponential form, and summing the geometric series which arise. The result is that

$$\langle \mu_j, \mu_j \rangle = 4k + \left[ \frac{(s-1)^2}{s} + \frac{(t-1)^2}{t} \right] \frac{k}{\sin^2 \theta_j} + \frac{(s-1)(t-1)}{\rho} \frac{2k \cos \theta_j}{\sin^2 \theta_j}$$

if  $m = 2k$ ,  $\theta_j = j\pi/k$ , and

$$\langle \mu_j, \mu_j \rangle = 4k + 2 + \frac{(s-1)^2}{s} \frac{2k+1}{1 - \cos \theta_j} \quad \text{if } m = 2k+1, \quad \theta_j = \frac{2j\pi}{2k+1}.$$

Now let  $\varphi_V$  be the character of  $A$  afforded by the representation of  $A$  on  $V$ , and write

$$\varphi_V = \sum_{\mu \in \text{Irr } A} n_\mu \mu$$

where  $n_\mu$  is the multiplicity of  $\mu$  in  $\varphi_V$ . If  $\beta$  is a standard basis element  $\neq 1$ , then the proof of (67.19) shows that for  $x \in F$ ,  $\beta x$  is a sum of flags different from  $x$ . Consequently  $\varphi_V(\beta) = 0$ . On the other hand,  $\varphi_V(1) = |F|$ . Thus  $\langle \mu, \varphi_V \rangle = |F|\mu(1)$ . The orthogonality relations (67.23) imply that

$$|F|\mu(1) = \langle \mu, \varphi_V \rangle = n_\mu \langle \mu, \mu \rangle,$$

and it follows that

$$\langle \mu, \mu \rangle \in \mathbb{Q} \quad \text{for all } \mu \in \text{Irr } A.$$

Now assume  $m = 2k$ . Then  $\theta_1 + \theta_{k-1} = \pi$ ,  $\cos \theta_1 = -\cos \theta_{k-1}$ , and  $\sin \theta_1 = \sin \theta_{k-1}$ . Using the formulas for  $\langle \mu_1, \mu_1 \rangle + \langle \mu_{k-1}, \mu_{k-1} \rangle$  given above, we obtain

$$\left[ \frac{(s-1)^2}{s} + \frac{(t-1)^2}{t} \right] \frac{k}{\sin^2 \theta_1} \in \mathbb{Q}.$$

If  $s = t = 1$ , then clearly  $(P, L, F)$  is an ordinary polygon. If either  $s > 1$  or  $t > 1$ , we conclude that

$$\sin^2 \theta_1 = \sin^2 \frac{\pi}{k} \in \mathbb{Q}.$$

Thus the field of  $k$ -th roots of 1 is at most quadratic over  $\mathbb{Q}$ , so  $k \in \{1, 2, 3, 4, 6\}$ , and  $m \in \{2, 4, 6, 8, 12\}$ . Since  $\langle \mu_j, \mu_j \rangle - \langle \mu_{k-j}, \mu_{k-j} \rangle \in \mathbb{Q}$  for  $1 \leq j \leq k-1$ , the preceding formulas show that

$$\left[ \frac{(s-1)(t-1)}{\rho} \right] \frac{2k \cos \theta_j}{\sin^2 \theta_j} \in \mathbb{Q}.$$

If both  $s > 1$  and  $t > 1$ , then we obtain  $\rho^{-1} \cos \theta_j \in \mathbb{Q}$  for  $1 \leq j \leq k-1$ , where  $\rho = \sqrt{st}$ . This excludes the case  $m = 12$ , and implies  $\rho \in \mathbb{Q}$  if  $m = 6$ , while  $\sqrt{2}\rho \in \mathbb{Q}$  if  $m = 8$ .

In case  $m = 2k+1$ , we have  $s = t$ , and if  $s > 1$ , the formulas for  $\langle \mu, \mu \rangle$  imply that  $\cos(2\pi/m) \in \mathbb{Q}$ . Thus the field of  $m$ -th roots of 1 is at most quadratic over  $\mathbb{Q}$ , and we obtain  $m = 3$ , completing the proof.

*Proof of Theorem 67.25.* Let  $G$  be a finite group with a  $BN$ -pair of rank 2, whose Weyl group is dihedral of order  $2m$ , with distinguished generators  $\{r, s\}$ . Let  $\mathcal{H}$  be the Hecke algebra  $\mathcal{H}(G, B, 1_B)$ . By (65.3) it is clear that both index parameters  $q_r$  and  $q_s$  are  $> 1$ . Since  $\mathcal{H}$  also has the structure of the algebra  $A$  in (67.14), (by Corollary 67.6), the results used in the proof of (67.24) can all be applied to characters of  $\mathcal{H}$ . In this case, the orthogonality relations and the fact that  $\langle \mu, \mu \rangle \in \mathbb{Q}$  for  $\mu \in \text{Irr } A$  follow from (11.32ii). Then Theorem 67.25 follows by exactly the same arguments used in the proof of (67.24).

**Remarks.** (i) The formulas for  $\langle \mu, \mu \rangle$  calculated in the proof of (67.24) are precisely the denominators in the formulas for degrees of characters in  $(1_B)^G$  given in (67.15).

(ii) Our approach to Theorems 67.24 and 67.25 has been to exploit the common structures of the incidence algebra  $A$  and the Hecke algebra  $\mathcal{H}$ .

### §67E. The Reflection Representation of the Hecke Algebra $\mathcal{H}$

We return to the study of a finite group  $G$  with a  $BN$ -pair of arbitrary rank. Let  $W$  be the Weyl group of  $G$ , and  $S = \{s_1, \dots, s_n\}$  the distinguished generators of  $W$ . The Hecke algebra  $\mathcal{H} = \mathcal{H}(G, B, 1_B)$  has a presentation with generators  $\{a_{s_1}, \dots, a_{s_n}\}$  and relations

$$a_{s_i}^2 = q_i 1 + (q_i - 1)a_{s_i}, \quad 1 \leq i \leq n, \quad q_i = \text{ind } a_{s_i},$$

and

$$\begin{cases} (a_{s_i} a_{s_j})^{k_{ij}} = (a_{s_j} a_{s_i})^{k_{ij}} & \text{if } m_{ij} = 2k_{ij}, \\ (a_{s_i} a_{s_j})^{k_{ij}} a_{s_i} = (a_{s_j} a_{s_i})^{k_{ij}} a_{s_j} & \text{if } m_{ij} = 2k_{ij} + 1, \end{cases}$$

where  $m_{ij}$  is the order of  $s_i s_j$ , as in §67A.

In the general case, it is a formidable task to construct irreducible representations of  $\mathcal{H}$ , other than the one-dimensional representations  $\text{ind}$  and  $\text{sgn}$  defined earlier. Nevertheless, the results of the preceding two subsections give some indications as to how to proceed. For a  $BN$ -pair of rank 2, it follows from the results of §§67C,D that the Hecke algebra  $\mathcal{H}$  and the group algebra of  $W$  are isomorphic as  $\mathbb{C}$ -algebras, even though no explicit isomorphism is given. In the next section, it will be proved that  $\mathcal{H} \cong CW$  in the general case (see (68.21)). These results suggest that irreducible representations of  $W$  can somehow be lifted to  $\mathcal{H}$ .

A particularly interesting representation of an indecomposable Coxeter group is the reflection representation, defined in §64B. In this section, we shall sketch Kilmoyer's construction of a corresponding irreducible representation of  $\mathcal{H}$ , called the *reflection representation* (see Curtis-Iwahori-Kilmoyer [71]). Besides its intrinsic interest, the method is a special case of a general construction of representations of Hecke algebras and Coxeter groups, by what are called  $W$ -graphs (see Kazhdan-Lusztig [79], Gyoja [84]).

By (64.28), the reflection representation of  $W$  is irreducible only if  $(W, S)$  is an indecomposable Coxeter system, so it is natural to make this assumption throughout this subsection. We shall need to use the fact that in this case the Coxeter graph of  $(W, S)$  is a tree, by Exercise 64.4.

Let  $V = \bigoplus_{i=1}^n Cv_i$  be an  $n$ -dimensional  $\mathbb{C}$ -space, where  $n = |S|$ . Let  $\{c_{ij}\}_{1 \leq i,j \leq n}$  be a set of complex numbers satisfying the conditions:

$$\begin{cases} c_{ii} = q_i + 1, \text{ where } q_i \text{ is the index parameter } \text{ind } a_{s_i}, \\ c_{ij} = c_{ji} = 0 \quad \text{if } m_{ij} = 2, \\ c_{ij}c_{ji} = q_i + q_j + 2\sqrt{q_i q_j} \cos \frac{2\pi}{m_{ij}}, \quad \text{if } m_{ij} > 2. \end{cases}$$

(Here  $\sqrt{\phantom{x}}$  is the positive square root, so that  $q_i q_j = q_i = q_j$  if  $m_{ij}$  is odd, by (67.5).) Note that in case  $n = 2$ ,  $c_{12}$  and  $c_{21}$  are defined in the same way as the parameters  $c_j$  and  $d_j$  in (67.14).

**(67.27) Lemma.** *There exists a nonzero symmetric bilinear form  $B$  on  $V$ , such that  $B(v_i, v_i) \neq 0$  for  $1 \leq i \leq n$ , and that satisfies the condition*

$$-c_{ij} = \frac{(q_i + 1)B(v_i, v_j)}{B(v_i, v_i)}, \quad 1 \leq i, j \leq n.$$

*Proof.* We prove the lemma by induction on the rank  $n$ . The result is clear if  $n = 1$ , so let  $n > 1$ . Since the Coxeter graph of  $(W, S)$  is a tree, it follows that there exists a subset  $J$  of  $S$ , with  $|J| = n - 1$ , such that  $(W_J, J)$  is an indecomposable Coxeter system. Thus if  $s_{i_0} \notin J$ , there is a unique  $s_{j_0} \in J$  such that  $m_{i_0 j_0} > 2$ . By the induction hypothesis, we may assume that  $B$  is defined on the subspace of  $V$

spanned by  $\{v_i\}_{i \neq i_0}$ . We then extend the definition of  $B$  to  $V$  by setting

$$\begin{cases} B(v_{i_0}, v_{j_0}) = B(v_{j_0}, v_{i_0}) = -B(v_{j_0}, v_{j_0})c_{j_0 i_0}(q_{j_0} + 1)^{-1}, \\ B(v_{i_0}, v_{i_0}) = -B(v_{i_0}, v_{j_0})(q_{i_0} + 1)c_{i_0 j_0}^{-1}, \\ B(v_{i_0}, v_j) = B(v_j, v_{i_0}) = 0 \quad \text{if } j \neq i_0, j_0. \end{cases}$$

It is easily checked that  $B$  satisfies the conditions of the lemma.

**(67.28) Lemma.** *For  $1 \leq i \neq j \leq n$ , let  $\langle v_i, v_j \rangle$  be the subspace of  $V$  generated by  $v_i$  and  $v_j$ . Then the restriction  $B|_{\langle v_i, v_j \rangle}$  is nondegenerate.*

*Proof.* The matrix of  $B_{\langle v_i, v_j \rangle}$  is

$$\mathbf{B}_{ij} = \begin{pmatrix} B(v_i, v_i) & B(v_i, v_j) \\ B(v_j, v_i) & B(v_j, v_j) \end{pmatrix},$$

and it suffices to prove that  $\det \mathbf{B}_{ij} \neq 0$ . Using (67.27), it is enough to show that

$$d = c_{ij}c_{ji} - (q_i + 1)(q_j + 1) \neq 0.$$

By the definition of  $\{c_{ij}\}$ , we have  $d \neq 0$  if  $m_{ij} = 2$ . Now suppose  $m_{ij} > 2$ . Then

$$d = 2\sqrt{q_i q_j} \cos \theta - q_i q_j - 1 = -(\sqrt{q_i q_j} - e^{\sqrt{-1}\theta})(\sqrt{q_i q_j} - e^{-\sqrt{-1}\theta}),$$

where  $\theta = 2\pi/m_{ij}$ . It follows that  $d \neq 0$ , since  $0 < \theta < \pi$  when  $m_{ij} > 2$ , so  $\sin \theta \neq 0$ , and hence  $e^{\pm\sqrt{-1}\theta}$  cannot equal the real number  $\sqrt{q_i q_j}$ .

**(67.29) Theorem.** *Assume that the Coxeter system  $(W, S)$  associated with  $G$  is indecomposable, and let  $\mathcal{H}$  be the Hecke algebra  $\mathcal{H}(G, B, 1_B)$ . There exists a representation  $T: \mathcal{H} \rightarrow \text{End}_C V$  such that*

$$T(a_{s_i})v = q_i v - \frac{(q_i + 1)B(v_i, v)}{B(v_i, v_i)}v_i \quad \text{for all } v \in V, \quad s_i \in S.$$

The representation  $T$  is irreducible, and the bilinear form  $B$  is nondegenerate on  $V$ .

*Proof.* For the first statement, it suffices to show that the map  $T$ , defined on the generators  $\{a_{s_i}\}$  of  $\mathcal{H}$  as in (67.29), preserves the defining relations of  $\mathcal{H}$ . For each  $i$ ,  $1 \leq i \leq n$ , we have  $V = \langle v_i \rangle \oplus \langle v_i \rangle^\perp$  since  $B(v_i, v_i) \neq 0$ , where  $\langle v_i \rangle^\perp = \{v \in V : B(v, v_i) = 0\}$ . Then  $T(a_{s_i})$ , as defined above, acts as scalar multiplication by  $q_i$  on  $\langle v_i \rangle^\perp$  and by  $-1$  on  $\langle v_i \rangle$ . It follows that

$$T(a_{s_i})^2 = q_i \cdot 1 + (q_i - 1)T(a_{s_i}), \quad 1 \leq i \leq n,$$

and the quadratic relations hold.

By Lemma 67.28, the restriction  $B|_{\langle v_i, v_j \rangle}$ ,  $i \neq j$ , is nondegenerate. Then

$$V = \langle v_i, v_j \rangle \oplus \langle v_i, v_j \rangle^\perp.$$

On  $\langle v_i, v_j \rangle^\perp$ ,  $T(a_{s_i})$  and  $T(a_{s_j})$  act as scalar multiplications by  $q_i$  and  $q_j$ , respectively. It follows that the homogeneous relations for  $T(a_{s_i})$  and  $T(a_{s_j})$  hold on  $\langle v_i, v_j \rangle^\perp$ , since  $q_i = q_j$  if  $m_{ij}$  is odd, by (67.5). On  $\langle v_i, v_j \rangle$ , the matrices of  $T(a_{s_i})$  and  $T(a_{s_j})$  are

$$\begin{pmatrix} -1 & c_{ij} \\ 0 & q_i \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} q_j & 0 \\ c_{ji} & -1 \end{pmatrix}$$

respectively, by the definition of  $B$  (see (67.27)). Then the homogeneous relations also hold on  $\langle v_i, v_j \rangle$  by the proof of (67.14). Thus  $T$  can be extended to define a representation of  $\mathcal{H}$ , by (67.6).

We shall prove that  $T$  is irreducible, and  $B$  nondegenerate, by induction on  $n$ . We may assume  $n > 1$ , and that the result holds for indecomposable Coxeter systems of rank  $< n$ . Choose a subset  $J \subset S$ ,  $|J| = n - 1$ , as in the proof of (67.27), and let  $V_J = \langle v_j : s_j \in J \rangle$ . By the induction hypothesis,  $B|_{V_J}$  is nondegenerate, so  $V = V_J \oplus V_J^\perp$ , and  $\dim_C V_J^\perp = 1$ .

Let  $\mathcal{H}_J$  be the subalgebra of  $\mathcal{H}$  generated by  $\{a_{s_j}\}_{s_j \in J}$ . By the induction hypothesis, the restriction of  $T$  to  $\mathcal{H}_J$  is irreducible on  $V_J$ , while  $V_J^\perp$  affords the representation  $\text{ind}$  of  $\mathcal{H}_J$ , by the first part of the proof. The simple  $\mathcal{H}_J$ -modules  $V_J$  and  $V_J^\perp$  are nonisomorphic, since their dimensions are different if  $n > 3$ , while  $V_J$  affords  $\text{sgn}$  in case  $n = 2$ .

Now consider  $V$  as a left  $\mathcal{H}$ -module. If  $V$  is not simple, then  $V = V' \oplus V''$  for some nontrivial submodules, since  $\mathcal{H}$  is semisimple. Then both  $V'$  and  $V''$  are  $\mathcal{H}_J$ -modules, and hence coincide with  $V_J$  and  $V_J^\perp$ , by what has been seen earlier. But  $V_J$  is clearly not an  $\mathcal{H}$ -submodule of  $V$ , by the properties of  $J$  and the definition of  $T$ . This completes the proof that  $T$  is irreducible.

Finally, we prove that  $B$  is nondegenerate on  $V$ . If not, then  $V^\perp \neq 0$ . If  $v$  is a nonzero vector in  $V^\perp$ , then by the definition of  $T$ ,

$$T(a_{s_i})v = q_i v, \quad 1 \leq i \leq n,$$

and  $\langle v \rangle$  is a proper  $\mathcal{H}$ -submodule of  $V$ . This contradicts the irreducibility of  $T$ , and finishes the proof.

**Remarks.** (i) The reader can easily verify that if we set all the parameters  $\{q_s\}$  equal to 1, in the definition of  $B$  and  $T$ , then  $T$  defines a representation of  $W$ , which is the reflection representation (64.28).

(ii) Let  $G$  be a finite group with a  $BN$ -pair, whose Weyl group  $(W, S)$  is indecomposable. Then there exists a unique character  $\zeta \in \text{Irr } G$  such that  $(\zeta, (1_B)^G) > 0$ , and  $\zeta|_{\mathcal{H}}$  is the character of  $T$ , by (11.25). This is called the *reflection*

*character* of  $G$ , and has a number of interesting properties. For example,

$$(\zeta, (1_{P_J})^G) = 1$$

for all maximal parabolic subgroups of  $G$ , and is the unique character in  $\text{Irr } G$  with this property. Its degree has been computed explicitly for each individual type of Coxeter group (Curtis-Iwahori-Kilmoyer [71]), and in case  $G$  is a Chevalley group, its values on regular  $p'$ -elements have been determined by Lusztig [79], for Weyl groups of type  $A_n$ ,  $D_n$ , and  $E_n$ ,  $n = 6, 7, 8$ .

(iii) The reflection representation of an indecomposable Coxeter group has the property that all its exterior powers are also irreducible. Corresponding irreducible representations of  $\mathcal{H}$  were constructed explicitly by Kilmoyer (see Curtis-Iwahori-Kilmoyer [71]).

## §67. Exercises

1. Let  $W = \langle s_1, s_2 : s_1^2 = s_2^2 = (s_1 s_2)^m = 1 \rangle$  be a dihedral group of order  $2m$ . Define an incidence structure whose set of points is the coset space  $W/\langle s_1 \rangle$ , and whose lines are the cosets  $W/\langle s_2 \rangle$ . A point  $x\langle s_1 \rangle$  and a line  $y\langle s_2 \rangle$  are defined to be incident if their intersection is nonempty. Prove that the incidence structure is an ordinary  $m$ -gon (see §67D).
2. (Feit-Higman [64]). Let  $G$  be a finite group with a BN-pair of rank 2, whose Weyl group  $W = \langle s_1, s_2 \rangle$  is dihedral of order  $2m$ . Let  $P_1 = B \cup Bs_1B$  and  $P_2 = B \cup Bs_2B$ , where  $B$  is the given Borel subgroup. Define an incidence structure  $(\mathcal{P}, \mathcal{L})$ , whose set of points  $\mathcal{P}$  is the coset space  $G/P_1$ , and whose set of lines  $\mathcal{L}$  is the set of cosets  $G/P_2$ , with incidence defined as in Exercise 1.

(i) Define a double-coset incidence structure  $\{\tilde{\mathcal{P}}, \tilde{\mathcal{L}}\}$ , whose set of points  $\tilde{\mathcal{P}}$  consists of the double cosets  $\{BgP_1 : g \in G\}$ , and whose lines are the double cosets  $\{BhP_2 : h \in G\}$ , with incidence defined as above. Prove that the double coset geometry is an ordinary  $m$ -gon.

[Hint: Use (65.21) and the preceding exercises.]

(ii) Prove that the coset geometry  $(\mathcal{P}, \mathcal{L})$  is a generalized  $m$ -gon.

[Hint: Prove that if  $X \in \mathcal{P} \cup \mathcal{L}$ , and if  $BX$  is incident to  $Z = BgP_1$  in the double-coset geometry, then  $Z = BY$ , for  $Y \in \mathcal{P} \cup \mathcal{L}$  and  $X \cap Y \neq \emptyset$ . In order to prove that  $\rho(x, y) \leq m$ , it may be assumed that  $Y = P_1$  or  $P_2$  since  $G$  acts transitively on the coset spaces  $G/P_1$  and  $G/P_2$ . Then use the preceding remarks to show that if  $Z_0 = BX, \dots, Z_h = BY$  is a chain of length  $\leq m$  in the double-coset geometry then  $Z_0 = BX, Z_1 = BX_1, \dots, Z_h = BX_h$  for a chain  $X_0 = X, \dots, X_h$  of length  $\leq m$  in the coset geometry. The same idea, along with properties of BN-pairs from §65, can be used to prove (ii) and (iii) of (67.17).]

(iii) Prove that there are  $|P_2 : B|$  points on each line, and  $|P_1 : B|$  lines through each point, in the generalized  $m$ -gon  $(\mathcal{P}, \mathcal{L})$ .

[Hint: The number of points on each line is the number of cosets  $gP_1$  intersecting a given coset  $g'P_2$ . Show that if it is nonempty, the intersection is given by  $gP_1 \cap g'P_2 = g''(P_1 \cap P_2) = g''B$ .]

## §68. GENERIC ALGEBRAS AND FINITE COXETER GROUPS

### §68A. Generic Algebras and the Deformation Theorem

In §67, we have shown that the Hecke algebra  $\mathcal{H} = \mathcal{H}(G, B, 1_B)$  of a finite group  $G$  with a  $BN$ -pair is closely related to the group algebra  $CW$  of the Weyl group of  $G$ . Following Tits (see Bourbaki [68, Ch. 4]), we shall make the connection more precise. This is done by introducing the generic algebra of the Coxeter system  $(W, S)$ , and using it to prove that in fact the algebras  $\mathcal{H}$  and  $CW$  are isomorphic. These methods are also applied to parametrize the characters in  $\text{Irr } \mathcal{H}$  in terms of the characters in  $\text{Irr } W$ . Thus we obtain, using §11D, a canonical parametrization of the characters  $\zeta \in \text{Irr } G$  such that  $(\zeta, (1_B)^G) \neq 0$  in terms of the characters of  $W$ .

**(68.1) Proposition.** *Let  $(W, S)$  be a finite Coxeter system (see §64B), and let  $S = \{s_1, \dots, s_n\}$ . Let  $R$  be any commutative  $\mathbb{Q}$ -algebra containing elements  $\{u_1, \dots, u_n\}$  such that  $u_i = u_j$  whenever\*  $s_i = {}_ws_j$ . Let  $A$  be a free  $R$ -module with a basis  $\{e_w : w \in W\}$  indexed by the elements  $w$  of  $W$ . Then there exists an  $R$ -algebra, whose underlying  $R$ -module is  $A$ , and whose multiplication is uniquely determined by the following formulas:*

$$e_{s_i} e_w = \begin{cases} e_{s_i w}, & \text{if } l(s_i w) > l(w), \\ u_i e_{s_i w} + (u_i - 1)e_w, & \text{if } l(s_i w) < l(w), \end{cases}$$

for all  $s_i \in S$ ,  $w \in W$ .

**Remark.** For motivation, see Theorem 67.2. That result, however, does not imply (68.1), since not every finite Coxeter group is the Weyl group of a finite group with a  $BN$ -pair (see the Feit–Higman Theorems 67.24–67.26).

*Proof.* (Bourbaki [68, Ch. 4. Ex. 23]). Let  $j$  be the  $R$ -automorphism of  $A$  defined by  $j(e_w) = e_w^{-1}$ ,  $w \in W$ , so  $j^2 = 1$ . For each  $i$ , let  $P_i$  be the  $R$ -endomorphism of  $A$  such that  $P_i e_w = e_{s_i} e_w$ , as in the statement of (68.1), and let  $Q_i = j P_i j$ ,  $1 \leq i \leq n$ . We first prove that

$$(68.2) \quad P_i Q_k = Q_k P_i, \quad \text{for } 1 \leq i, \quad k \leq n,$$

by letting both sides of (68.2) act on basis elements  $\{e_w\}_{w \in W}$ . An easy calculation shows that the result holds for  $l(w) = 0$ . Assuming  $l(w) > 0$ , we have to prove that

$$e_{s_i} j(e_{s_k} e_w^{-1}) = j e_{s_k} j(e_{s_i} e_w).$$

By (64.16), it follows that either  $l(s_i w s_k) = l(w)$  or  $l(s_i w s_k) = l(w) \pm 2$ . In the latter case, the result follows easily, since the possibilities for  $l(s_i w)$ ,  $l(w s_k)$ , etc. are uniquely determined. On the other hand, suppose that  $l(s_i w s_k) = l(w)$ . If

\*We write  $s = {}_ws'$  to indicate that  $s$  and  $s'$  are conjugate in  $W$ .

If  $l(s_i w) \neq l(ws_k)$ , then the possibilities again can be determined, and the result checked using the formulas for  $e_{s_i} \cdot e_w$ . Finally, if  $l(s_i ws_k) = l(w)$  and  $l(s_i w) = l(ws_k)$ , then it follows from the results in §64A that  $s_i w = ws_k$ , and hence  $s_i = ws_k$ . The result (68.2) thus holds in this case as well, using the hypothesis that  $u_i = u_k$  if  $s_i = ws_k$ .

We next prove that if  $s_{i_1} \cdots s_{i_l} = s_{j_1} \cdots s_{j_l}$  are two reduced products of elements of  $S$ , then

$$(68.3) \quad P_{i_1} \cdots P_{i_l} = P_{j_1} \cdots P_{j_l}.$$

Let both sides act on  $e_w$ ,  $w \in W$ , and use induction on  $l(w)$ . The result is clear if  $l(w) = 0$ , so we may assume  $l(w) > 0$ . Let  $w = w's_k$ ,  $s_k \in S$ , where  $l(w') < l(w)$ . Then

$$e_w = j e_{w^{-1}} = j P_k j e_{w'} = Q_k e_{w'},$$

and hence, by (68.2),

$$(P_{i_1} \cdots P_{i_l} - P_{j_1} \cdots P_{j_l})e_w = Q_k(P_{i_1} \cdots P_{i_l} - P_{j_1} \cdots P_{j_l})e_{w'} = 0,$$

using the induction hypothesis.

Next, define left multiplication by  $e_w$ , for  $w \in W$ , by the formula

$$(68.4) \quad e_w e_{w'} = P_{i_1} \cdots P_{i_l} e_{w'},$$

if  $w = s_{i_1} \cdots s_{i_l}$  is a reduced expression for  $w$ . Note that, by (68.3), this operation is well defined. Further, we have

$$(68.5) \quad e_w e_{s_i} = Q_i e_w, \quad \text{for all } w \in W, s_i \in S,$$

since if  $w = s_{i_1} \cdots s_{i_l}$  as above, then

$$e_w e_{s_i} = P_{i_1} \cdots P_{i_l} e_{s_i} = P_{i_1} \cdots P_{i_l} Q_i e_1 = Q_i e_w,$$

by (68.2).

An argument similar to the proof of (68.3) shows that

$$(68.6) \quad e_w e_{w''} = Q_{j_m} \cdots Q_{j_1} e_{w'}$$

if  $w'' = s_{j_1} \cdots s_{j_m}$  is a reduced product of factors from  $S$ . The proof, of course, uses (68.5) as a start.

The associative law

$$(e_w e_{w'}) e_{w''} = e_w (e_{w'} e_{w''}) \quad \text{for all } w, w', w'' \in W,$$

follows at once from (68.4) and (68.6), since the endomorphisms  $P_i$  and  $Q_k$  commute, by (68.2). The uniqueness of the multiplication is clear, and the proposition is proved.

**(68.7) Definition.** Let  $(W, S)$  be a finite Coxeter system, with  $S = \{s_1, \dots, s_n\}$  and let  $R$  be a commutative ring containing elements  $\{u_1, \dots, u_n\}$  such that  $u_i = u_j$  whenever  $s_i = w s_j$ . The  $R$ -algebra  $A$  defined in (68.1) is called the *generic algebra* of the Coxeter system  $(W, S)$  over the ring  $R$ , and its  $R$ -basis  $\{e_w : w \in W\}$  is the *standard basis* of  $A$ .

**(68.8) Proposition.** Let  $A$  be the generic algebra of a Coxeter system  $(W, S)$  over a commutative ring  $R$ , as in (68.7). Then  $A$  has a presentation as an  $R$ -algebra with generators  $\{e_{s_i} : s_i \in S\}$ , and relations as follows:

$$e_{s_i}^2 = u_i 1 + (u_i - 1)e_{s_i}, \quad 1 \leq i \leq n \text{ (quadratic relations)}$$

and, for  $1 \leq i, j \leq n$ , the homogeneous relations:

$$\begin{aligned} (e_{s_i} e_{s_j})^{k_{ij}} &= (e_{s_j} e_{s_i})^{k_{ij}} && \text{if } m_{ij} = 2k_{ij}, \\ (e_{s_i} e_{s_j})^{k_{ij}} e_{s_i} &= (e_{s_j} e_{s_i})^{k_{ij}} e_{s_j} && \text{if } m_{ij} = 2k_{ij} + 1, \end{aligned}$$

where  $e_1 = 1$ , and where  $m_{ij}$  is the order of  $s_i s_j$  in  $W$ .

The proof is exactly the same as that of Theorem 67.6, after checking that the defining relations hold in  $A$ , using the properties of the multiplication stated in Proposition 68.1.

**(68.9) Proposition.** For the generic algebra  $A$  of a Coxeter system  $(W, S)$  there exist two  $R$ -algebra homomorphisms from  $A$  to  $R$ , called IND and SGN, defined by:

$$\text{IND } e_{s_i} = u_i \quad \text{and} \quad \text{SGN } e_{s_i} = -1, \quad 1 \leq i \leq n.$$

This result follows at once from the presentation of  $A$  given in (68.8), since the proposed mappings preserve the defining relations.

Suppose for the moment that  $R$  is an arbitrary commutative ring, and that  $A = \bigoplus_{i=1}^n Ra_i$  is an  $R$ -free  $R$ -algebra. A *specialization* of  $R$  is a ring homomorphism  $f: R \rightarrow F$ , with  $F$  a field. Then  $F$  becomes an  $(F, R)$ -bimodule, with  $R$  acting from the right via  $f$ . As in §2B, the tensor product  $F \otimes_R A$  acquires the structure of an  $F$ -algebra, and we have

$$F \otimes_R A = \bigoplus_{i=1}^n F a'_i, \quad \text{where } a'_i = 1 \otimes a_i, \quad 1 \leq i \leq n.$$

Call  $F \otimes_R A$  the *specialized algebra*, and denote it by  $A_f$ . For  $1 \leq i, j \leq n$ , we have:

$$(68.10) \quad a_i a_j = \sum_k r_{ijk} a_k \Rightarrow a'_i a'_j = \sum_k f(r_{ijk}) a'_k,$$

where the  $r$ 's lie in  $R$ . It is sometimes convenient to view the specialized algebra

$F \otimes_R A$  as an  $R$ -algebra, using the  $R$ -action on  $F$  via  $f$ . Then the map  $f:R \rightarrow F$  can be extended to a homomorphism of  $R$ -algebras  $f:A \rightarrow A_f$ , such that  $f(a_i) = a'_i$ ,  $1 \leq i \leq n$ , for the bases of  $A$  and  $A_f$  described above.

We can now begin to make more precise the still somewhat vague connection between the Hecke algebra  $\mathcal{H}(G, B, 1_B)$  of a finite group  $G$  with a  $BN$ -pair, and the group algebra  $CW$  of the Weyl group  $W$  associated with the  $BN$ -pair.

**(68.11) Proposition.** *Let  $A$  be the generic algebra of a finite Coxeter system  $(W, S)$ , over a commutative ring  $R$ , as in (68.7).*

(i) *Assume that  $F$  is a field, and that  $f':R \rightarrow F$  is a specialization such that  $f'(u_i) = 1$ ,  $1 \leq i \leq n$ . Then  $A_{f'} \cong FW$  as  $F$ -algebras.*

(ii) *Assume that  $W$  is the Weyl group of a finite group  $G$  with a  $BN$ -pair, with index parameters  $\{q_i\}_{1 \leq i \leq n}$  (see §67A). Let  $f'':R \rightarrow C$  be a specialization such that  $f''(u_i) = q_i$ ,  $1 \leq i \leq n$ . Then  $A_{f''}$  is isomorphic to the Hecke algebra  $\mathcal{H}(G, B, 1_B)$ , as  $C$ -algebras.*

**Remark.** Specializations  $f'$  and  $f''$ , as in (68.11i, ii), need not exist for an arbitrary commutative ring  $R$ . A sufficient condition for them to exist is that  $R = \mathbb{Q}[u_1, \dots, u_n]$ , where the  $\{u_i\}$  are indeterminates over  $\mathbb{Q}$  such that  $u_i = u_j$  if  $s_i = w s_j$ .

*Proof.* (i) By (68.1) and (68.10), the specialized basis elements  $e'_w = f'(e_w)$ ,  $w \in W$ , multiply according to the rule  $e'_{s_i} e'_w = e'_{s_i w}$ , for all  $s_i \in S$  and  $w \in W$ , since both formulas in (68.1) give the same result when  $u_i \rightarrow 1$ . It is then clear that the map  $w \mapsto e'_w$  extends to an isomorphism  $FW \cong A_{f'}$ .

(ii) This time we have

$$e''_{s_i} e''_w = \begin{cases} e''_{s_i w}, & \text{if } l(s_i w) > l(w), \\ q_i e''_{s_i w} + (q_i - 1)e''_w, & \text{if } l(s_i w) < l(w), \end{cases}$$

for all  $s_i \in S$  and  $w \in W$ , where  $\{e''_w\}$  are the specialized basis elements. By Theorem 67.6, there exists a homomorphism of  $C$ -algebras  $\mathcal{H} \rightarrow A_{f''}$  such that  $a_{s_i} \mapsto e''_{s_i}$ ,  $1 \leq i \leq n$ . The homomorphism is clearly surjective, and  $\dim_C \mathcal{H} = \dim_C A_{f''}$ , so we have  $\mathcal{H} \cong A_{f''}$ , as required.

**(68.12) Corollary.** *Let  $(W, S)$  be a finite Coxeter system, and let  $R$  be a commutative integral domain containing elements  $\{u_i\}$  such that  $u_i = u_j$  if  $s_i = w s_j$  in  $S$ . Let  $K$  be the quotient field of  $R$ . Suppose there exists a specialization  $f':R \rightarrow \mathbb{Q}$  for which  $f'(u_i) = 1$  for each  $i$ . Then  $A^K = K \otimes_R A$  is a separable  $K$ -algebra.*

*Proof.* Let  $T$  be the trace form on  $A^K$  defined by

$$T(a, b) = T_{A/K}(ab).$$

By Exercise 7.6,  $A^K$  is separable if  $T$  is nondegenerate. For any specialization

$f:R \rightarrow F$  to a field  $F$ , we have  $T(e_x, e_y) \in R$  for all  $x, y \in W$ , by (68.1). It follows directly that

$$f(T(e_x, e_y)) = T_f(e'_x, e'_y) \quad \text{for all } x, y \in W,$$

where  $T$  and  $T_f$  are the trace forms on  $A^K$  and  $A_f$ , respectively, and  $\{e'_x : x \in W\}$  are the specialized basis elements in  $A_f$ . In particular, for the specialization  $f':R \rightarrow Q$  as in (68.12), we have  $A_{f'} \cong QW$  by (68.11), and  $T_{f'}$  is the trace form on  $QW$ . The bilinear form  $T_{f'}$  is nondegenerate on  $QW$  by the discussion of Example 9.2C, and hence  $T$  is nondegenerate on  $A^K$ , completing the proof.

Our aim is to compare the structures of the specialized algebras  $\{A_f\}$  of a generic algebra  $A$  as  $f$  varies over specializations for which the specialized algebras  $A_f$  are separable.

**(68.13) Definition.** Let  $B$  be a separable algebra over a field  $F$ . The *numerical invariants* of  $B$  are the dimensions of the simple  $B^{F^*}$ -modules, where  $F^*$  is an algebraic closure of  $F$ , and  $B^{F^*} = F^* \otimes_F B$ .

Clearly two separable algebras over  $F$  become isomorphic when the field is extended to  $F^*$  if and only if they have the same numerical invariants (see §7A).

We now give three lemmas leading to the proof of Tits's Deformation Theorem. Our approach follows Steinberg [67] (see also Bourbaki [68, p. 56, Ex. 26]).

**(68.14) Lemma.** Let  $B = \bigoplus_{i=1}^n Lb_i$  be a split semisimple algebra over an algebraically closed field  $L$ . Let

$$L' = L[t_1, \dots, t_n], \quad \tilde{L} = L(t_1, \dots, t_n),$$

where the  $\{t_i\}$  are indeterminates over  $L$ . Set

$$b = \sum_{i=1}^n t_i b_i \in B^{\tilde{L}}, \quad \text{where } B^{\tilde{L}} = \bigoplus \tilde{L}b_i.$$

We call  $b$  a “general element” of  $B$ ; its characteristic polynomial  $P(X) \in \tilde{L}[X]$  can be computed by letting  $b$  act on the basis elements  $\{b_i\}$ , so  $P(X) \in L'[X]$ . Let

$$P(X) = \prod P_i(X)^{p_i}$$

be the factorization of  $P(X)$  into prime powers in  $L'[X]$ . Then we have:

- (i) The multiplicities  $\{p_i\}$  are the numerical invariants of  $B$ .
- (ii)  $p_i = \deg P_i(X)$  for all  $i$ .
- (iii) Let  $-\varphi(t_1, \dots, t_n) \in L'$  be the coefficient of  $X^{p_i-1}$  in  $P_i(X)$ . Then the map

$$\sum \xi_j b_j \mapsto \varphi_i(\xi_1, \dots, \xi_n), \quad \text{where each } \xi_j \in L,$$

is an irreducible character of  $B$ , and all irreducible characters of  $B$  are obtained in this way.

(iv) Let  $P(X) = \prod Q_j(X)^{q_j}$  be another factorization of  $P(X)$ , with the  $\{Q_j(X)\}$  monic in  $L'[X]$ , and  $q_j = \deg Q_j(X)$ , for each  $j$ . Then the polynomials  $\{Q_j(X)\}$  are distinct, and coincide with the polynomials  $\{P_i(X)\}$ .

*Proof.* We leave it to the reader to check that the statements of the lemma are independent of the choice of the basis and the set of indeterminates used to define a general element. For the proof of (i)–(iii), we may assume that  $B = M_n(L)$  is a split simple  $L$ -algebra, with  $L$ -basis given by the  $n^2$  matrix units  $\{\mathbf{E}_{ij}\}$ . Denoting the indeterminates by  $\{t_{ij}\}$ , the general element  $b \in B$  is represented by the matrix

$$\mathbf{b} = \sum_{i,j=1}^n t_{ij} \mathbf{E}_{ij}.$$

The matrix  $\mathbf{b}$  is obtained from the action of  $b$  on an  $L$ -basis of a simple left  $B$ -module  $V$ . Therefore

$$\text{char. pol.}_{BL/L} b = (\text{char. pol. } \mathbf{b})^n,$$

and

$$\text{char. pol. } \mathbf{b} = \det(X\mathbf{I} - (t_{ij})) \in L'[X].$$

To complete the proof of (i) and (ii), we need only show that  $\text{char. pol. } \mathbf{b}$  is irreducible in  $L'[X]$ . Any proper factorization of this polynomial remains proper after specializing the indeterminates  $\{t_{ij}\}$ . In particular, a specialization of  $\text{char. pol. } \mathbf{b}$  is given by

$$\text{char. pol. } \begin{bmatrix} 0 & 0 & \cdots & 0 & t \\ 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 \\ \vdots & & & & \vdots \\ 0 & 0 & \cdots & 1 & 0 \end{bmatrix} = X^n - t,$$

with  $t$  an indeterminate. But  $X^n - t$  is irreducible by Eisenstein's criterion, so it follows that  $\text{char. pol. } \mathbf{b}$  must also be irreducible.

Next, suppose that

$$\text{char. pol. } \mathbf{b} = X^n - \psi(\{t_{ij}\}) X^{n-1} + \cdots + (-1)^n \det(t_{ij}).$$

Then a simple left  $B$ -module  $V$  affords a character  $\varphi$  of  $B$ , given by

$$\varphi: \sum \xi_{ij} \mathbf{E}_{ij} \rightarrow \text{trace of } \sum \xi_{ij} \mathbf{E}_{ij} = \psi(\{\xi_{ij}\}).$$

This implies (iii) at once.

(iv) Returning to the general situation, let

$$P(X) = \prod P_i(X)^{p_i} = \prod Q_j(X)^{q_j},$$

where the first factorization is as given above, and where  $q_j = \deg Q_j(X)$  for each  $j$ . But the  $\{P_i(X)\}$  are *distinct* irreducible polynomials, since they involve different indeterminates, and so  $P_i(X)$  occurs exactly  $p_i$  times as factor of  $P(X)$ . If now  $P_i(X)|Q_j(X)$  for some  $j$ , then  $\deg Q_j(X) \geq p_i$ . Hence if  $Q_j(X) \neq P_i(X)$ ,  $P_i(X)$  would occur more than  $p_i$  times in  $P(X)$ . Thus the  $\{Q_j\}$  are a permutation of the  $\{P_i\}$ , as claimed, and the lemma is proved.

The next two lemmas are standard results in commutative algebra.

**(68.15) Lemma.** *Let  $R$  be an integral domain with quotient field  $K$ , and let  $K^*$  be an algebraic closure of  $K$ , and  $R^*$  the integral closure of  $R$  in  $K^*$ . Then, for any set of indeterminates  $\{t_1, \dots, t_n\}$  over  $K^*$ ,  $R^*[t_1, \dots, t_n]$  is the integral closure of  $R[t_1, \dots, t_n]$  in  $K^*[t_1, \dots, t_n]$ .*

For a proof, see Bourbaki ([64, p. 19, Prop. 13]).

**(68.16) Lemma.** *Keep the above notation, and let  $f$  be a homomorphism of  $R$  into a field  $F$ . Then  $f$  can be extended to a homomorphism  $f^*: R^* \rightarrow F^*$ , where  $F^*$  is an algebraic closure of  $F$ .*

For a proof, see Atiyah–MacDonald ([69, Ex. 5.2]).

**(68.17) Deformation Theorem (Tits).** *Let  $R$  be an integral domain,  $K$  its field of quotients, and let  $f: R \rightarrow F$  be a homomorphism of  $R$  into a field  $F$ . Let  $A$  be an  $R$ -algebra with a finite basis over  $R$ , let  $A^K$  be the  $K$ -algebra  $K \otimes_R A$ , and  $A_f$  the specialized  $F$ -algebra  $F \otimes_R A$  (see the discussion following (68.9)). If both  $A^K$  and  $A_f$  are separable algebras, then they have the same numerical invariants.*

*Proof.* Let  $K^*$  and  $F^*$  be algebraic closures of  $K$  and  $F$ , respectively, and let  $R^*$  be the integral closure of  $R$  in  $K^*$ . Let  $n = \dim_K A^K$ , and let  $\{t_1, \dots, t_n\}$  and  $\{t'_1, \dots, t'_n\}$  be sets of indeterminates over  $K^*$  and  $F^*$ , respectively. Let

$$(68.18) \quad \begin{aligned} R' &= R[t_1, \dots, t_n], & R^{*\prime} &= R^*[t_1, \dots, t_n], & K^{*\prime} &= K^*[t_1, \dots, t_n], \\ F' &= F[t'_1, \dots, t'_n], & F^{*\prime} &= F^*[t'_1, \dots, t'_n]. \end{aligned}$$

Let  $A = \bigoplus_{i=1}^n Ra_i$ ; then we may identify  $\{a_1, \dots, a_n\}$  with a  $K^*$ -basis of  $A^K$ , and  $a = \sum_{i=1}^n t_i a_i$  with a general element of  $A^K$ . A general element of the specialized algebra  $A_f$  is  $a' = \sum_{i=1}^n t'_i a'_i$ , where  $a'_i = 1 \otimes a_i$ ,  $1 \leq i \leq n$ .

Let  $P(X) = \text{char. pol. } a$ , and  $P'(X) = \text{char. pol. } a'$ . Then  $P(X) \in R'[X]$  since the structure constants of  $A$  are in  $R$ , and  $P'(X) \in F'[X]$ . We may extend  $f$  to a homomorphism from  $R'[X]$  to  $F'[X]$ , also denoted by  $f$ , by setting  $f(t_i) = t'_i$ ,

$1 \leq i \leq n$ , and  $f(X) = X$ . By (68.10), it follows that

$$(68.19) \quad f(P(X)) = P'(X).$$

Now consider the factorization of  $P(X)$  described in Lemma 68.14. We have  $P(X) = \prod P_i(X)^{p_i}$ , where the factors  $P_i(X) \in K^{*'}[X]$ , for each  $i$ . Since  $P(X)$  is monic, its roots are integral over  $R'$ . The coefficients of the factors  $\{P_i(X)\}$ , which already belong to  $K^*$ , are symmetric functions of the roots of  $P(X)$ , and hence are also integral over  $R'$ . Thus  $P_i(X) \in R^{*'}[X]$  for each  $i$ , by Lemma 68.15.

We next extend  $f: R \rightarrow F$  to a homomorphism  $f^*: R^* \rightarrow F^*$ , by (68.16). Then  $f: R'[X] \rightarrow F'[X]$  extends to a homomorphism  $f^*: R^{*'}[X] \rightarrow F^{*'}[X]$ . Using (68.19), we obtain

$$f^*(P(X)) = P'(X) = \prod f^*(P_i(X))^{p_i},$$

where each polynomial  $f^*(P_i(X)) \in F^{*'}[X]$ . Since  $p_i = \deg P_i(X)$  for each  $i$ , we also have  $p_i = \deg f^*(P_i(X))$  for each  $i$ . The multiplicities  $\{p_i\}$  are the numerical invariants of  $A^K$  by (68.14i), and are also the numerical invariants of  $A_f$  by (68.14iv). This completes the proof.

**(68.20) Corollary.** *Keeping the notation of (68.17), assume that both  $A^K$  and  $A_f$  are separable algebras. Let  $R^*$  be the integral closure of  $R$  in  $K^*$ , and let  $f^*: R^* \rightarrow F^*$  be an extension of  $f$  (see Lemma 68.16). Let  $\mu \in \text{Irr } A^{K^*}$ . Then*

$$\mu(a_i) \in R^*, \quad 1 \leq i \leq n.$$

For each irreducible character  $\mu \in \text{Irr } A^{K^*}$ , define an  $F^*$ -linear map  $\mu_{f^*}: A_f^{F^*} \rightarrow F^*$ , by setting

$$\mu_{f^*}(a'_i) = f^*(\mu(a_i)), \quad \text{where} \quad a'_i = 1 \otimes a_i, \quad \text{for } 1 \leq i \leq n.$$

Then  $\mu_{f^*} \in \text{Irr } A_f^{F^*}$ , and the map  $\mu \mapsto \mu_{f^*}$  is a bijection from  $\text{Irr } A^{K^*}$  to  $\text{Irr } A_f^{F^*}$  (which depends on the choice of  $f^*$ ).

*Proof.* We shall use the notation from the proof of (68.17). Let  $\mu \in \text{Irr } A^{K^*}$ . By Lemma 68.14iii, we have

$$\mu(\sum \xi_i a_i) = \varphi_i(\xi_1, \dots, \xi_n) \quad \text{for all} \quad \sum \xi_i a_i \in A^{K^*}, \quad \xi_i \in K^*,$$

where  $-\varphi_i$  is a coefficient of some irreducible factor  $P_i(X)$  of  $P(X)$ . In the proof of (68.17), it was shown that each  $P_i(X) \in R^{*'}[X]$ . It follows that  $\varphi_i \in R^{*'}$ , and hence  $\mu(a_i) \in R^*$  for each  $i$ . From the proof of (68.17), we also know that  $f^*(P_i(X))$  is a monic irreducible factor of the characteristic polynomial  $P'(X)$  of the general element of  $A_f$ . Then  $-f^*(\varphi_i) \in F^{*'}$ , and is the coefficient of  $f^*(P_i(X))$  corresponding to  $-\varphi_i$ . Using (68.14iii) again, we deduce that

$$\sum \xi'_i a'_i \rightarrow f^* \varphi_i(\xi'_1, \dots, \xi'_n) \quad \text{for all} \quad \xi'_i \in F^*$$

is an irreducible character of  $A_f^*$ , which we shall denote by  $\mu_{f^*}$ . From its definition, we have

$$\mu_{f^*}(a'_i) = f^*(\mu(a_i)), \quad 1 \leq i \leq n.$$

The last statement follows from (68.14). This completes the proof.

We are now in a position to prove:

**(68.21) Theorem.** *Let  $G$  be a finite group with a BN-pair, and let  $(W, S)$  be the Weyl group of  $G$ . Let  $\mathcal{H}$  be the Hecke algebra  $\mathcal{H}(G, B, 1_B)$ . Then there exists an isomorphism of  $\mathbb{C}$ -algebras:*

$$\mathcal{H} \cong CW.$$

*Proof.* Let  $A$  be the generic ring of the Coxeter system  $(W, S)$  over the commutative integral domain  $R = \mathbb{Q}[u_1, \dots, u_n]$ , where  $S = \{s_1, \dots, s_n\}$ , and the  $\{u_i\}$  are indeterminates over  $\mathbb{Q}$  such that  $u_i = u_j$  if  $s_i = w s_j$ . Then, putting  $F = \mathbb{C}$  in (68.11i), the specializations  $f': R \rightarrow \mathbb{C}$  and  $f'': R \rightarrow \mathbb{C}$  in parts (i) and (ii) of (68.11) are defined, and we have

$$A_{f'} \cong CW \quad \text{and} \quad A_{f''} \cong \mathcal{H}$$

by (68.11). By Corollary 68.12,  $A^K$  is a separable  $K$ -algebra, where  $K$  is the quotient field of  $R$ . Both of the specialized algebras  $CW$  and  $\mathcal{H}$  are also separable. By the Deformation Theorem, the algebras  $\mathcal{H}$  and  $CW$  have the same numerical invariants, and hence are isomorphic, since  $\mathbb{C}$  is algebraically closed.

**Remarks.** (i) Keep the notation of (68.17). With suitable hypotheses on  $R$ , it is possible to define a decomposition map  $d$  from  $G_0(K^* \otimes_R A)$  to  $G_0(F^* \otimes_F A_f)$  and a Cartan map  $c$  from  $K_0(F^* \otimes_F A_f)$  to  $G_0(F^* \otimes_R A_f)$  so that  $\mathbf{C} = {}^t \mathbf{D} \mathbf{D}$ , where  $\mathbf{C}$  is the Cartan matrix and  $\mathbf{D}$  is the decomposition matrix. If  $A_f$  is separable, then  $\mathbf{C}$  is the identity matrix,  $\mathbf{D}$  is a permutation matrix, and (68.20) and (68.17) both follow as in the proof of (18.11). The elementary proof of (68.17) given above, however, applies to a more general situation.

(ii) It is possible to construct explicitly an isomorphism  $\mathcal{H} \cong CW$  (see Lusztig [81]).

## §68B. Parametrization of Characters in $(1_B)^G$

Finite groups of Lie type do not occur in isolation; they are members of infinite families with a fixed Weyl group, parametrized by finite fields  $\{\mathbb{F}_q\}$ . For example, the general linear groups  $\{GL_{n+1}(\mathbb{F}_q)\}$ , for fixed  $n$ , form such a family, all having the Weyl group  $S_{n+1}$ , by §65B. Our first task will be to axiomatize the concept of families of groups with BN-pairs.

The main objective of representation theory for such a family is to determine all the irreducible representations and characters at once, by some sort of generic method. This ambitious plan is now surprisingly near completion (see Carter [85]).

A significant step in this program is the parametrization of irreducible characters in  $(1_B)^G$  in terms of characters of the Weyl group. The existence and properties of this parametrization are the main objectives of this subsection.

**(68.22) Definition.** Let  $(W, S)$  be a finite Coxeter system. A *system  $\mathcal{S}$  of finite groups with BN-pairs of type  $(W, S)$*  consists of the following data:

- (i) An infinite set  $\mathbf{CP}$  of prime powers  $\{q\}$ , called *characteristic powers*.
- (ii) For each  $q \in \mathbf{CP}$ , there exists a finite group  $G(q) \in \mathcal{S}$  with a BN-pair, with Weyl group  $(W, S)$ .
- (iii) There exists a set of positive integers  $\{c_s\}_{s \in S}$  such that for each  $q \in \mathbf{CP}$ , the index parameters (see (67.1)) of  $G(q)$  are given by

$$|B(q):^s B(q) \cap B(q)| = q^{c_s}, \quad \text{for each } s \in S,$$

where  $B(q)$  is a standard Borel subgroup of  $G(q)$ .

**Remarks.** (i) By Corollary 67.5, it follows that  $c_s = c_{s'}$ , for  $s, s' \in S$ , if  $s = ws'$ .

(ii) Let  $\mathcal{S} = \{GL_{n+1}(\mathbb{F}_q)\}$ , for a fixed  $n$ , where  $\{\mathbb{F}_q\}$  ranges over all finite fields. Then  $\mathcal{S}$  is a system, as in (68.22), for which  $\mathbf{CP}$  is the set of all prime powers,  $c_s = 1$  for all  $s \in S$ , and for each  $q \in \mathbf{CP}$ ,

$$G(q) = GL_{n+1}(\mathbb{F}_q).$$

(iii) Twisted types of Chevalley groups give rise to systems for which not all the integers  $\{c_s\}$  in (68.22iii) are equal to 1 (see Carter [72b], Steinberg [67]).

Before we come to the main results, we require some additional properties of the index homomorphism  $\text{IND}: A \rightarrow R$  defined in (68.9). We let  $(W, S)$  be a fixed Coxeter system,  $S = \{s_1, \dots, s_n\}$ , and let  $R = \mathbb{Q}[u_1, \dots, u_n]$  be the polynomial ring over  $\mathbb{Q}$ , with indeterminates  $\{u_i\}$  such that  $u_i = u_j$  if  $s_i = ws_j$ . We also recall the definition of the generic algebra  $A$  of  $(W, S)$  over  $R$  (see (68.7)).

**(68.23) Lemma.** Let  $\mathcal{S} = \{G(q)\}$  be a system of finite groups with BN-pairs of type  $(W, S)$ , and let  $A$  be the generic algebra of the Coxeter system  $(W, S)$  over the ring  $R = \mathbb{Q}[u_1, \dots, u_n]$ . Let  $J \subseteq S$ , and let  $W_J$  be the parabolic subgroup of  $W$  corresponding to  $J$  (see §64C). Then the following statements hold:

- (i) Let  $X$  be a nonempty subset of  $W$  such that  $W_J X = X$ , and let  $e_X = \sum_{w \in X} e_w$ , where  $\{e_w\}$  is the standard basis of  $A$ . Then

$$e_{s_i} e_X = \text{IND}(e_{s_i}) e_X \quad \text{for all } s_i \in S.$$

(ii) Let  $\varepsilon_J = \sum_{w \in W_J} e_w$ . Then  $\text{IND } \varepsilon_J \neq 0$ , and

$$\varepsilon_J^2 = (\text{IND } \varepsilon_J) \varepsilon_J.$$

In particular,  $(\text{IND } \varepsilon_J)^{-1} \varepsilon_J$  is an idempotent in  $A^K$ , where  $K$  is the quotient field of  $R$ .

(iii) Let  $G(q) \in \mathcal{S}$ , let  $B = B(q)$  be a Borel subgroup of  $G(q)$ , and let  $P_J \geq B$  be the standard parabolic subgroup of  $G(q)$  corresponding to  $J$  (see §65C). Let  $f: R \rightarrow C$  be the specialization defined by  $f(u_i) = q^{c_i}$ ,  $1 \leq i \leq n$ , where  $\{q^{c_i}\}$  are the index parameters of  $G(q)$ , as in (68.22iii). Then

$$|P_J : B| = f(\text{IND } \varepsilon_J).$$

*Proof.* (i) For each  $s_i \in J$ , there is a partition

$$X = X_+(s_i) \cup X_-(s_i),$$

where

$$X_{\pm}(s_i) = \{w \in X : l(s_i w) \geqslant l(w)\}.$$

From the properties of the length function  $l(w)$ , we then have

$$s_i X_+(s_i) = X_-(s_i) \quad \text{and} \quad s_i X_-(s_i) = X_+(s_i).$$

Put

$$e_{X,+} = \sum_{w \in X_+(s_i)} e_w, \quad e_{X,-} = \sum_{w \in X_-(s_i)} e_w.$$

By (68.1), we then have

$$e_{s_i} e_{X,+} = e_{X,-}, \quad e_{s_i} e_{X,-} = u_i e_{X,+} + (u_i - 1) e_{X,-}.$$

Since  $e_X = e_{X,+} + e_{X,-}$ , we obtain

$$e_{s_i} e_X = u_i e_X,$$

which is part (i). Part (ii) is left as an exercise for the reader.

(iii) We have

$$P_J = \bigcup_{w \in W_J} BwB.$$

Then

$$|P_J : B| = \sum_{w \in W_J} |BwB| / |B| = \sum_{w \in W_J} |B : {}^w B \cap B| = \sum_{w \in W_J} \text{ind}_B w,$$

where  $w \in N$  is a coset representative corresponding to  $w \in N/T$ . By Exercise 11.19,

there is a homomorphism of  $\mathbb{C}$ -algebras  $\text{ind}: \mathcal{H}(G(q), B, 1_B) \rightarrow \mathbb{C}$  such that  $\text{ind } a_w = \text{ind}_B w$ , where  $a_w$  is the standard basis element of  $\mathcal{H}(G, B, 1_B)$  defined by the double coset  $BwB$ . If  $w = s_{(1)} \cdots s_{(k)}$  is a reduced expression for  $w$ , with each  $s_{i(j)} \in S$ , then we have

$$e_w = e_{s(1)} \cdots e_{s(k)} \quad \text{in } A \text{ (by (68.1))}$$

and

$$a_w = a_{s(1)} \cdots a_{s(k)} \quad \text{in } \mathcal{H}(G(q), B, 1_B) \text{ (by (67.2)).}$$

Moreover,  $\text{ind } a_{s(i)} = |B : {}^{s^i}B \cap B| = q^{c_i}$ , for  $1 \leq i \leq k$ . Therefore  $f(u_i) = \text{ind } a_{s(i)}$ ,  $1 \leq i \leq k$ , for the specialization  $f$  defined above, and we obtain

$$f(\text{IND } e_w) = \prod_i f(\text{IND } e_{s(i)}) = \prod_i \text{ind } a_{s(i)} = \text{ind } a_w.$$

Combining these facts, we obtain

$$f(\text{IND } \varepsilon_J) = \sum_{w \in W_J} f(\text{IND } e_w) = |P_J : B|$$

as required.

Keep the notation introduced earlier in this subsection. In addition, let

$K$  = the quotient field of  $R = \mathbb{Q}[u_1, \dots, u_n]$ ,

$K^*$  = an algebraic closure of  $K$ ,

$R^*$  = the integral closure of  $R$  in  $K^*$ ,

$f': R \rightarrow \mathbb{C}$  = the specialization such that  $f'(u_i) = 1$ ,  $1 \leq i \leq n$ ,

$f'': R \rightarrow \mathbb{C}$  = the specialization such that  $f''(u_i) = q^{c_i}$ ,  $1 \leq i \leq n$ ,

where  $\{q^{c_i}\}$  are the index parameters of the group  $G(q) \in \mathcal{S}$ ,

$(f')^*$ ,  $(f'')^*$  = extensions of  $f'$  and  $f''$  to homomorphisms from  $R^*$  to  $\mathbb{C}$  (see Lemma 68.16).

**(68.24) Theorem.** *Let  $G(q) \in \mathcal{S}$ . There exists a bijection  $\varphi \leftrightarrow \zeta_{\varphi, q}$  from  $\text{Irr } W$  to  $\{\zeta \in \text{Irr } G(q) : (\zeta, (1_B)^G) > 0\}$ . This bijection depends only on the choices of the extensions  $f'^*$  and  $f''^*$ , and has the following property. For each  $J \subseteq S$ , let  $W_J$  and  $P_J(q)$  be the corresponding parabolic subgroups of  $W$  and  $G(q)$ , respectively. Then*

$$(\zeta_{\varphi, q}, 1_{P_J(q)}^{G(q)}) = (\varphi, (1_{W_J})^W).$$

In particular,

$$(\zeta_{\varphi, q}, (1_{B(q)})^{G(q)}) = \deg \varphi, \quad \text{for all } \varphi \in \text{Irr } W.$$

*Proof.* By (68.11), we have  $A_{f'} \cong CW$  and  $A_{f''} \cong \mathcal{H}(G(q), B(q), 1)$ . By (68.20), there exist bijections, depending only on the choice of the extensions  $(f')^*$  and

$(f'')^*$ :

$$\text{Irr } A^{K^*} \leftrightarrow \text{Irr } A_{f'} \quad \text{and} \quad \text{Irr } A^{K^*} \leftrightarrow \text{Irr } A_{f''}.$$

Let  $\varphi \in \text{Irr } W$ , let  $\mu_\varphi \in \text{Irr } A^{K^*}$  correspond to  $\varphi$  in the first bijection, and let  $\mu_{\varphi,q} \in \text{Irr } A_{f''}$  correspond to  $\mu_\varphi$  in the second bijection.

By the proof of (68.11), the isomorphism  $A_{f''} \cong \mathcal{H}$  carries the basis elements  $\{e''_w : w \in W\}$  of  $A_{f''}$  to the standard basis elements  $\{a_w : w \in W\}$  of  $\mathcal{H}$ , where

$$a_w = |B(q)|^{-1} \sum_{x \in B(q)wB(q)} x, \quad \text{for each } w \in W,$$

as in §11D. By Theorem 11.25, there exists a unique character  $\zeta_{\varphi,q} \in \text{Irr } G(q)$  such that  $(\zeta_{\varphi,q}, 1_{B(q)}^{G(q)}) > 0$ , and whose restriction to  $\mathcal{H}$  is given by

$$(68.25) \quad \zeta_{\varphi,q}(a_w) = \mu_{\varphi,q}(e''_w), \quad \text{for all } w \in W.$$

The correspondence  $\varphi \leftrightarrow \zeta_{\varphi,q}$  is the bijection described in the statement of the theorem, and we now have to check the statement about multiplicities.

Let  $J \subseteq S$ , and let  $\varepsilon_J = \sum_{w \in W_J} e_w$ , as in (68.23ii). Then  $(\text{IND } \varepsilon_J)^{-1} \varepsilon_J$  is an idempotent in  $A^K$ , on which the irreducible characters  $\mu_\varphi$  of  $A^{K^*}$  take nonnegative integer values  $m(\varphi, J)$ . Therefore, for  $J \subseteq S$  and  $\varphi \in \text{Irr } W$ , we have

$$\mu_\varphi(\varepsilon_J) = m(\varphi, J) \text{IND } \varepsilon_J,$$

for some nonnegative integer  $m(\varphi, J)$ . Upon applying the specialization  $f''^*$  to this equation, and using (68.20) and (68.25), we obtain

$$\zeta_{\varphi,q} \left( \sum_{w \in W_J} a_w \right) = \mu_{\varphi,q}(\varepsilon_J) = m(\varphi, J) |P_J(q):B(q)|,$$

since  $f''(\text{IND } \varepsilon_J) = |P_J(q):B(q)|$  by (68.23iii). Since

$$\sum_{w \in W_J} a_w = |B(q)|^{-1} \sum_{g \in P_J(q)} g,$$

it follows that

$$\zeta_{\varphi,q}(|P_J(q)|^{-1} \sum_{g \in P_J(q)} g) = m(\varphi, J).$$

By (11.21), we then obtain

$$m(\varphi, J) = (\zeta_{\varphi,q}, (1_{P_J(q)})^{G(q)}).$$

A similar argument, which we leave to the reader, shows that also

$$m(\varphi, J) = (\varphi, (1_{W_J})^W),$$

and the theorem is proved.

**Remarks.** By Theorem 67.10iii, the Steinberg character  $\text{St}_G$  of any one of the groups  $G = G(q)$  in  $\mathcal{S}$  has the following multiplicities in the permutation characters  $(1_{P_J})^G$ ,  $J \subseteq S$ :

$$(\text{St}_G, (1_B)^G) = 1, \quad (\text{St}_G, (1_{P_J})^G) = 0, \quad J \neq \emptyset.$$

Since  $\text{St}_G$  is uniquely determined in  $\text{Irr } G$  by these multiplicities, and the sign character  $\varepsilon$  of  $W$  is determined by the corresponding multiplicities, it follows that

$$\text{St}_G = \zeta_{\varepsilon, q}$$

for any choices of the extended specializations  $(f')^*$  and  $(f'')^*$ . A similar result is true for all characters of  $W$ , apart from a few exceptions.

**(68.26) Theorem (Benson-Curtis [72]).** Let  $(W, S)$  be an indecomposable Coxeter system associated with a system  $\mathcal{S}$  of finite groups with BN-pairs. Then each character  $\varphi \in \text{Irr } W$  is uniquely determined by the multiplicities  $\{(\varphi, (1_{W_J})^W) : J \subseteq S\}$ , with the following exceptions:

- (a) the characters of degree 2, in case  $W$  is dihedral of order 12 or 16 (see the Feit-Higman Theorem 67.24);
- (b) the two characters of degree  $2^9 = 512$ , in case  $W$  is of type  $E_7$ ;
- (c) the four characters of degree  $2^{12} = 4096$ , in case  $W$  is of type  $E_8$ .

We omit the proof, which involves a lengthy case-by-case argument. The point of the theorem is that the correspondence  $\varphi \leftrightarrow \zeta_{\varphi, q}$  described in Theorem 68.24 is canonical, that is, independent of the choices of  $(f')^*$  and  $(f'')^*$ , with the exceptions noted above. For another application, see the exercises.

### §68C. Generic Degrees

Now that we have parametrized the characters in  $(1_B)^G$  for a group  $G = G(q)$  belonging to a system  $\mathcal{S}$ , we are in a position to consider the main problems of character theory, at least for components of  $(1_B)^G$ . Can we give the degrees, and possibly other character values, of the characters  $\{\zeta_{\varphi, q}\}$  for all the groups  $G(q) \in \mathcal{S}$ , by some uniform method? The main result of this subsection is that the degrees of these characters  $\{\zeta_{\varphi, q}\}$  can be expressed as polynomials in  $q$ . This result was predicted by Brauer, and is clearly a step in the right direction. We also include some other properties of the degrees; these results lead, through a case-by-case analysis, to the explicit calculation of the degrees for each family of finite groups with BN-pairs. For some results on other character values, see §70C.

We shall use the notation given in §68B (see (68.1), the statements of (68.23) and (68.24), and the remarks preceding (68.24)). For each character  $\varphi \in \text{Irr } W$ , we have

$$(68.27) \quad (f')^*(\mu_\varphi(e_w)) = \varphi(w), \quad w \in W,$$

where we have identified the specialized algebra  $A_{f'}$  with  $CW$ , using (68.11i).

The degree formula (11.32iii) motivates the following:

**(68.28) Definition.** Let  $\varphi \in \text{Irr } W$ . The generic degree (or formal degree) associated with  $\varphi$  is the element of  $K^*$  given by

$$d_\varphi = \frac{P(u) \deg \varphi}{\sum_{w \in W} (\text{IND } e_w)^{-1} \mu_\varphi(e_w) \mu_\varphi(e_{w^{-1}})},$$

where  $P(u) = \sum_{w \in W} \text{IND } e_w \in R$ .

Of course, it is not clear from the definition that  $d_\varphi$  is a well-defined element of  $K^*$ . This point, and the exact sense in which it is a generic degree, will be made precise in (68.30). We shall need to use the fact that a homomorphism  $f:R \rightarrow F$ , from a commutative integral domain  $R$  into a field  $F$ , can be extended canonically to the localization  $R_f$  of  $R$  at the prime ideal  $\ker f$  (see §4A). The ring  $R_f$ , which is a subring of the quotient field of  $K$ , is sometimes called the *specialization ring of f*. Given a map  $f:R \rightarrow F$ , its extension to  $R_f$  will also be denoted by  $f$ .

We also need to look more closely at the generic algebra  $A^{K^*}$ . Since  $A^K$  is separable by (68.12), the algebra  $A^{K^*}$  is a split semisimple  $K^*$ -algebra, having a  $K^*$ -basis that we may identify with the standard  $R$ -basis  $\{e_w : w \in W\}$  of  $A$ . By analogy with (11.30iii), it is natural to consider the bilinear form  $\beta: A^{K^*} \times A^{K^*} \rightarrow K^*$ , whose value  $\beta(e_w, e_{w'})$  is the coefficient of 1 ( $= e_1$ ) in the expression of the product  $e_w e_{w'}$  as a  $K^*$ -linear combination of the standard basis elements. We then have:

**(68.29) Lemma.** The bilinear form  $\beta: A^{K^*} \times A^{K^*} \rightarrow K^*$  is symmetric, associative, and nondegenerate. The elements

$$\{(\text{IND } e_w)^{-1} e_w\}_{w \in W} \quad \text{and} \quad \{e_{w^{-1}}\}_{w \in W}$$

are dual bases with respect to the form.

The form  $\beta$  is clearly associative. Its other properties follow from the formula

$$\beta(e_w, e_{w'}) = \begin{cases} 0 & \text{if } w^{-1} \neq w', \\ \text{IND } e_w, & \text{if } w^{-1} = w'. \end{cases}$$

This is easily proved by induction on  $l(w)$ , using the properties of multiplication of standard basis elements established in (68.1), and is left as an exercise for the reader.

With this result in hand, we can apply the orthogonality relations (9.17) to the characters  $\{\mu_\varphi\}_{\varphi \in \text{Irr } W}$  of the split semisimple  $K^*$ -algebra  $A^{K^*}$ .

**(68.30) Proposition.** Let  $\{d_\varphi\}$  be the generic degrees associated with the characters  $\varphi \in \text{Irr } W$ , for a finite Coxeter system  $(W, S)$ . Then the elements  $d_\varphi$  are well-defined elements of the quotient field of  $R^*$  in  $K^*$ . Moreover, the following statements hold.

- (i)  $(f')^*(d_\varphi) = \deg \varphi$  for all  $\varphi \in \text{Irr } W$ .
- (ii) The generic degrees are the unique solutions in  $K^*$  of the system of equations

$$\sum_{\varphi \in \text{Irr } W} d_\varphi \mu_\varphi(e_w) = \begin{cases} P(u), & w = 1 \\ 0, & w \neq 1. \end{cases}$$

- (iii) If  $(W, S)$  is the Coxeter system of a system  $\mathcal{S}$  of finite groups with BN-pairs, then

$$(f'')^*(d_\varphi) = \deg \zeta_{\varphi, q} \quad \text{for each } \varphi \in \text{Irr } W \text{ and } q \in \mathbf{CP},$$

where  $\zeta_{\varphi, q}$  is the character in  $(1_{B(q)})^{G(q)}$  associated with  $\varphi$ , as in (68.24).

*Proof.* We have  $\mu_\varphi(e_w) \in R^*$  for all  $w \in W$ , by (68.20). The next calculation shows that  $d_\varphi \in R_{f'}^*$ , and proves (i). We have

$$(f')^*(d_\varphi) = \frac{|W| \deg \varphi}{\sum_{w \in W} \varphi(w) \varphi(w^{-1})} = \deg \varphi, \quad \varphi \in \text{Irr } W,$$

by (68.27), (68.28), and the orthogonality relations for  $\text{Irr } W$ .

(ii) Using the dual bases of  $A^{K^*}$  given in (68.29), an easy calculation using Proposition 9.17 shows that the central primitive idempotent  $\varepsilon_\varphi$  in  $A^{K^*}$  corresponding to the character  $\mu_\varphi$  is given by

$$\varepsilon_\varphi = \frac{d_\varphi}{P(u)} \sum_{w \in W} (\text{IND } e_w)^{-1} \mu_\varphi(e_{w^{-1}}) e_w.$$

The relation  $\sum_{\varphi \in \text{Irr } W} \varepsilon_\varphi = 1$  implies the formula stated in (ii). The uniqueness of the elements  $\{d_\varphi\}$  as solutions of the equations in (ii) follows from the orthogonality relations (9.17) for  $\text{Irr } A^{K^*}$ .

(iii) As in the proof of (i), we shall show that  $d_\varphi$  belongs to the specialization ring  $R_{f''}^*$ , which will imply (iii). We first require the formula

$$\zeta_{\varphi, q}(a_w) = \mu_{\varphi, q}(e_w'') \quad \text{for all } w \in W$$

(see (68.25)). We then obtain

$$\begin{aligned} (f'')^*(d_\varphi) &= \frac{(f'')^*(P(u)) \deg \varphi}{\sum_{w \in W} f''(\text{IND } e_w)^{-1} (f'')^* \mu_\varphi(e_w) (f'')^* \mu_\varphi(e_{w^{-1}})} \\ &= \frac{|G(q):B(q)| (\zeta_{\varphi, q}, (1_{B(q)})^{G(q)})}{\sum_{w \in W} (\text{ind } a_w)^{-1} \zeta_{\varphi, q}(a_w) \zeta_{\varphi, q}(a_{w^{-1}})} = \deg \zeta_{\varphi, q}. \end{aligned}$$

The proof of the preceding formula uses (11.32iii), together with the facts that  $f''(\text{IND } e_w) = \text{ind } a_w$  and  $f''(P(u)) = |G(q):B(q)|$ , by (68.23). We have also applied (68.24) to obtain  $\deg \varphi = (\zeta_{\varphi,q}, (1_{B(q)})^{G(q)})$ . This completes the proof.

The next result is due to Benson–Curtis [72].

**(68.31) Theorem.** *Let  $\mathcal{S}$  be a system of finite groups with BN-pairs. Assume that the set of characteristic powers  $\mathbf{CP}$  contains almost all primes. Let  $\{c_1, \dots, c_n\}$  define the index parameters of the groups in  $\mathcal{S}$  (see (68.22)), and let  $\mathbb{Q}[u_1, \dots, u_n] \subseteq \mathbb{Q}[u]$ , where  $u_i = u^{c_i}$ ,  $1 \leq i \leq n$ , for some fixed indeterminate  $u$  over  $\mathbb{Q}$ . Then for each  $\varphi \in \text{Irr } W$ , the generic degree  $d_\varphi$  (see (68.28)) belongs to  $R = \mathbb{Q}[u]$ , and thus there exists a polynomial  $F_\varphi(u) \in \mathbb{Q}[u]$  such that  $d_\varphi = F_\varphi(u)$ .*

**Remarks.** Once the polynomials  $\{F_\varphi(u), \varphi \in \text{Irr } W\}$  have been determined, the degrees of the irreducible characters  $\zeta_{\varphi,q}$  in  $(1_{B(q)})^{G(q)}$  can be found by substitution:

$$\deg \zeta_{\varphi,q} = F_\varphi(q), \quad q \in \mathbf{CP}$$

(see (68.30ii)). For example, let  $\mathcal{S}$  be the system consisting of the groups  $\{GL_{n+1}(F_q)\}$ . Then the generic degree associated with the sign character  $\varepsilon$  of  $W$  is given by

$$F_\varepsilon(u) = u^{n(n+1)/2},$$

and for each prime power  $q$ ,  $F_\varepsilon(q) = \deg \text{St}_G$ , where  $\text{St}_G = \zeta_{\varepsilon,q}$  is the Steinberg character of  $GL_{n+1}(F_q)$ , by the example in §67B.

The assumption that  $\mathbf{CP}$  contains almost all primes is satisfied by all families of untwisted Chevalley groups, and for some families of twisted types of Chevalley groups such as the unitary groups. For the twisted Chevalley groups defined by Suzuki and Ree, however, all of the characteristic powers associated with the family are powers of 2. In the case of the family of type  ${}^2F_4$ , defined by Ree, the generic degrees defined above need not be polynomials (see Curtis–Iwahori–Kilmoyer [71, §9]).

The proof of (68.31) depends on the following result from analytic number theory:

**(68.32) Hilbert Irreducibility Theorem.** *Let  $F(u, X) \in \mathbb{Z}[u, X]$  be an irreducible polynomial in two variables, of positive degree in  $X$ . Then there exist infinitely many primes  $\{q\}$  such that  $F(q, X)$  is an irreducible polynomial in  $\mathbb{Z}[X]$ .*

For a proof, see Lang ([62, Ch. VIII]).

*Proof of (68.31).* Let  $K$  be the quotient field of  $R$ , and let  $\varphi$  be a fixed irreducible

character of  $W$ . We first prove that  $d_\varphi \in K$ . Let

$$c_\varphi = \text{L.C.M.} \left\{ \text{IND } e_w : w \in W \right\} \cdot \sum_{w \in W} (\text{IND } e_w)^{-1} \mu_\varphi(e_w) \mu_\varphi(e_{w^{-1}}).$$

Once we prove that  $c_\varphi \in K$ , then clearly also  $d_\varphi \in K$ , by definition 68.28. For each  $w \in W$ , we have  $\mu_\varphi(e_w) \in R^*$  by (68.20), and hence  $c_\varphi \in R^*$ . Then  $\min. \text{pol}_K c_\varphi \in R[X]$ , by Proposition 1.8, since  $R = \mathbb{Q}[u]$  is integrally closed in  $K$ . For a suitably chosen integer  $a$ , it follows that

$$F(u, X) = a \cdot \min. \text{pol}_K c_\varphi \in \mathbb{Z}[u, X],$$

and  $F(u, X)$  is irreducible, of positive degree in  $X$ . If  $F(u, X)$  has degree 1 in  $X$ , then  $c_\varphi \in K$ , and there is nothing further to prove. Now suppose the degree in  $X$  of  $F(u, X)$  is  $> 1$ . For each  $q \in \mathbf{CP}$ , let  $(f'')^*: R^* \rightarrow C$  extend the specialization  $f'': u \rightarrow q$ . By (68.30),  $(f'')^* d_\varphi = \deg \zeta_{\varphi, q} \in \mathbb{Z}$ , and hence  $(f'')^*(c_\varphi) \in \mathbb{Q}$ . Then

$$F(q, (f'')^*(c_\varphi)) = 0$$

for each  $q \in \mathbf{CP}$ , since  $F(u, c_\varphi) = 0$ . It follows that the polynomials  $\{F(q, X) : q \in \mathbf{CP}\}$  all have a rational zero, contradicting the Irreducibility Theorem 68.32. Thus  $c_\varphi \in K$ , as required.

The proof of the theorem is completed using the following elementary result, whose verification is left to the reader.

**(68.33) Lemma.** *Let  $h(u) \in \mathbb{Q}(u)$  be a rational function such that for infinitely many positive integers  $\{n_i\}$ , we have  $h(n_i) \in \mathbb{Z}$ . Then  $h(u) \in \mathbb{Q}[u]$ .*

The next result and Proposition 68.30ii have turned out to be of decisive importance for the calculation of the generic degrees. (See Carter [85] for tables of generic degrees for the exceptional Weyl groups of type  $E_6$ ,  $E_7$ ,  $E_8$ ,  $F_4$ , and  $G_2$ .) The same methods show that the generic degrees  $d_\varphi$  lie in  $\mathbb{Q}(u_1, \dots, u_n)$ , in the more general case where the  $\{u_i\}$  are indeterminates over  $\mathbb{Q}$  satisfying only the condition that  $u_i = u_j$  if  $s_i = w s_j$ .

**(68.34) Theorem.** *Keep the assumptions of (68.31). Then for each  $\varphi \in \text{Irr } W$ , the generic degree  $F_\varphi(u)$  divides the polynomial  $\text{IND } e_{w_0} \cdot P(u)$  in the polynomial ring  $\mathbb{Q}[u]$ , where  $w_0$  is the unique element of maximal length in  $W$  (see 64.16)).*

*Proof.* Let  $m(u) = \text{IND } e_{w_0} \in \mathbb{Q}[u]$ . It is clear that

$$m(u) = \text{L.C.M.} \text{ IND } e_w.$$

By Theorem 11.32iv, we have

$$F_\varphi(q) | m(q)P(q)$$

for all  $q \in \mathbf{CP}$ , since  $F_\varphi(q) = \deg \zeta_{\varphi,q}(\zeta_{\varphi,q}, (1_{B(q)})^{G(q)}) > 0$ , and  $P(q) = |G(q):B(q)|$ , by (68.23iii). From this, it follows easily that  $F_\varphi(u)|m(u)P(u)$  in  $\mathbb{Q}[u]$ , as required.

## §68 Exercises

- Keep the notation preceding the statement of Theorem 68.24. Let  $\varphi \in \text{Irr } W$ , for an indecomposable Coxeter system  $(W, S)$  associated with a system  $\mathcal{S}$  of finite groups with BN-pairs. Using Theorem 68.26, prove that, if  $\varphi$  is not one of the exceptions (a), (b), or (c) to (68.26), then the corresponding character  $\mu_\varphi \in \text{Irr}(K^* \otimes_R A)$  is rational, in the sense that  $\mu_\varphi(1 \otimes e_w) \in R$ , for each basis element  $1 \otimes e_w$  of  $K^* \otimes_R A$  (Benson-Curtis [72]).

[Hint. Let  $\sigma: K^* \rightarrow K^*$  be a field automorphism which acts as the identity on the subfield  $K$ . Then  $\sigma(R^*) = R^*$ , and  $\sigma$  permutes the irreducible characters of  $K^* \otimes_R A$ , in such a way that, for  $\varphi \in \text{Irr } W$ ,  $\sigma\mu_\varphi = \mu_{\varphi'}$  for some  $\varphi' \in \text{Irr } W$ , where  $\mu_\varphi(1 \otimes e_w) = \sigma(\mu_{\varphi'}(1 \otimes e_w))$  for all  $w \in W$  (see (68.20)). We have  $\mu_\varphi(\varepsilon_J) = (\text{IND } \varepsilon_J)m(\varphi, J)$  for each subset  $J \subseteq S$ , as in the proof of (68.24). Apply  $\sigma$ , and obtain  $\mu_{\varphi'}(\varepsilon_J) = (\text{IND } \varepsilon_J)m(\varphi', J)$ , since  $\text{IND } \varepsilon_J$  and  $m(\varphi, J)$  are both fixed by  $\sigma$ . By the proof of (68.24), it follows that  $(\varphi, (1_{W_J})^W) = (\varphi', (1_{W_J})^W)$  for all  $J \subseteq S$ . By (68.26), it follows that  $\varphi = \varphi'$ . Since this holds for each automorphism  $\sigma$  of  $K^*$  over  $K$ , it follows from (68.20) that  $\mu_\varphi(1 \otimes e_w) \in K \cap R^* = R$ , for all  $w \in W$ , as required.]

- Let  $G(q) \in \mathcal{S}$ . Apply the preceding exercise to prove that, for each nonexceptional (in the sense of (68.26)) character  $\varphi \in \text{Irr } W$ , the corresponding character  $\zeta_{\varphi,q}$  is rational-valued on  $G(q)$ .

[Hint: Apply (11.34).]

## §69. FINITE GROUPS WITH SPLIT BN-PAIRS

### §69A. The Levi Decomposition

Throughout this section,  $p$  denotes a fixed prime number. For a finite group  $H$ , we shall use the notation  $O_p(H)$  to denote the unique maximal normal  $p$ -subgroup of  $H$ .

**(69.1) Definition.** A finite group  $G$  is said to have a *split BN-pair of rank  $n$  and characteristic  $p$*  if the following conditions are satisfied:

- $G$  has a BN-pair of rank  $n$  (see §65A) such that

$$T = \bigcap_{x \in N} {}^x B,$$

where  $T = B \cap N$ .

- There exists a normal subgroup  $U \trianglelefteq B$  such that

$$B = U \rtimes T \text{ (semidirect product).}$$

(iii)  $U = O_p(B)$ , and  $T$  is an abelian  $p'$ -group.\*

**Remarks.** (a) In the special case where  $G$  has a split  $BN$ -pair of rank 0,  $G$  is simply a finite abelian  $p'$ -group, and we have  $G = B = N = T$ , and  $U = 1$ .

(b) The first condition, that  $T = \cap^x B$ , can always be achieved in a finite group with a  $BN$ -pair without altering the Borel subgroup  $B$  or the Weyl group  $W$  (see Bourbaki [68, Ex. 5, pp. 47]).

The next result summarizes the properties of finite groups with split  $BN$ -pairs, which we shall require throughout the rest of the chapter. We shall continue to use the conventions introduced in §65A for groups with  $BN$ -pairs. In particular, we let  $w \in N$  denote a coset representative of an element  $w$  in the Weyl group  $W = N/T$ . We shall also use the two-sided notation for conjugates:

$${}^a A = aAa^{-1}, \quad A^b = b^{-1}Ab,$$

and for subsets  $A$  normalized by  $T$ , we shall write

$${}^w A = {}^{\dot{w}} A, \quad A^w = A^{\dot{w}}, \quad \text{for all } w \in W.$$

Some additional notation is needed for finite groups with split  $BN$ -pairs, as follows. Let  $\{G, B, U, N, T\}$  be a finite group with a split  $BN$ -pair, as in (69.1). By (65.9), the Weyl group  $W$  of  $G$  is a finite Coxeter group. By (64.28), we may identify  $W$  with a finite g.g.r. in some euclidean space, associated with a root system  $\Delta$ . We may also assume that the set  $S$  of distinguished generators of  $W$  is a set of fundamental reflections defined by a fundamental set of roots  $\Pi$  in  $\Delta$ . Further, let  $\Delta_{\pm}$  be the positive and negative roots, respectively, determined by  $\Pi$ , as in §64A, and define  $\Delta_w^{\pm}$ ,  $w \in W$ , as in (64.15).

Let  $w_0$  be the unique element of maximal length in  $W$  (see (64.16)), and let  $U^- = U^{w_0}$ . For each  $w \in W$ , set

$$U_w^+ = U \cap U^w, \quad U_w^- = U \cap U^{w_0 w}.$$

Then  $U_w^+ = \{u \in U : {}^{\dot{w}} u \in U\}$ ,  $U_w^- = \{u \in U : {}^{\dot{w}} u \in U^-\}$ . Note in particular that  $U = U_{w_0}^-$ .

Now let  $\Pi = \{\alpha_1, \dots, \alpha_n\}$  and  $S = \{s_1, \dots, s_n\}$ , where  $s_i = s_{\alpha_i}$  for each  $i$ . We may then define subgroups  $\{U_{\alpha_i}\}$  by the formula

$$U_{\alpha_i} = U \cap U^{w_0 s_i}, \quad 1 \leq i \leq n.$$

In the next result, a root structure is introduced in  $G$ , consisting of subgroups  $\{U_{\alpha}\}$  on which the Weyl group of  $G$  acts in the same way that  $W$  acts on the roots in  $\Delta$ .

\* Recall that a  $p'$ -group is a finite group whose order is prime to  $p$ .

**(69.2) Proposition.** Let  $\{G, B, N, U, T\}$  be a finite group with a split BN-pair of rank  $n$  and characteristic  $p$ , and let  $(W, S)$  be the Coxeter system in the Weyl group  $W$  of  $G$ , as above. Then the following statements hold.

(i)  $U^- \cap B = 1$ .

(ii)  $U = U_w^- U_w^+$  and  $U_w^- \cap U_w^+ = 1$ , for all  $w \in W$ .

(iii) There exists a bijection  $\alpha \rightarrow U_\alpha$  from the root system  $\Delta$  to the set of conjugates  $\{{}^x U_{\alpha_i} : x \in N, \alpha_i \in \Pi\}$ , which extends the map  $\alpha_i \rightarrow U_{\alpha_i}, \alpha_i \in \Pi$ . For all  $w \in W$  and  $\alpha \in \Delta$ , we have

$${}^w U_\alpha = U_{w(\alpha)}.$$

(iv) For each  $w \in W$ , there exists an ordering  $\{\beta_1, \beta_2, \dots\}$  of the roots in  $\Delta_w^-$  such that

$$U_w^- = U_{\beta_1} U_{\beta_2} \cdots,$$

with uniqueness of expression. A similar statement holds for  $\Delta_w^+$  and  $U_w^+$ . In particular,  $U_w^\pm = \langle U_\alpha : \alpha \in \Delta_w^\pm \rangle$ .

(v) (Sharp form of the Bruhat decomposition.) Let  $\{\dot{w}\}_{w \in W}$  denote a fixed cross section of  $W = N/T$ . Then

$$BwB = BwU_w^- \quad \text{for each } w \in W.$$

Moreover,  $G = \dot{\bigcup}_{w \in W} BwU_w^-$ , and each element of  $G$  can be written uniquely in the form  $b\dot{w}u$ , with  $b \in B$ ,  $w \in W$ , and  $u \in U_w^-$ , for  $\dot{w}$  in the fixed cross section of  $N/T$ .

(vi) For each  $i$ ,  $U_{\alpha_i} T \cup U_{\alpha_i} T s_i U_{\alpha_i}$  is a subgroup of  $G$ .

We do not prove (69.2) here. We shall assume, in what follows, that all finite groups with split BN-pairs satisfy (69.2i)–(69.2vi), together with

**(69.2vii) (Commutator Formula)** Let  $\alpha, \beta$  be linearly independent roots. Then\*

$$(U_\alpha, U_\beta) \subseteq \prod U_{i\alpha + j\beta},$$

where the product is taken (in some order) over the set of all roots which can be expressed in the form  $i\alpha + j\beta$ ,  $i, j > 0$ .

**Remarks.** The statements (69.2i)–(69.2vii) are standard properties of Chevalley groups and twisted types of Chevalley groups (see Chevalley [55], Carter [72b], and Steinberg [67]). They also hold for the finite groups  $G(\mathbb{F}_q)$ , consisting of  $\mathbb{F}_q$ -rational points on a connected reductive affine algebraic group defined over

\* For subsets  $A, B$  of a group, we let  $(A, B)$  denote the set of all commutators  $(a, b) = aba^{-1}b^{-1}, a \in A, b \in B$ .

$\mathbb{F}_q$  (see Borel-Tits [65]). The statements (69.2i)–(69.2vi) can be proved in an elementary way from the axioms for split  $BN$ -pairs (see Richen [69]). The commutator formula (69.2vii) can also be proved from the axioms, with some exceptions in case  $p = 2$  that do not occur as Chevalley groups (see Fong-Seitz [73], [74]; Tinberg [80a]).

**Example.** In order to give the reader a better understanding of Proposition 69.2, we shall verify properties (i)–(vii) for the finite general linear groups, by methods that are typical of the proofs of these facts for Chevalley groups. Some details are omitted.

**(69.3) Proposition.** *Let  $\mathbb{F}_q$  be a finite field of characteristic  $p$ , and  $n$  a positive integer. The general linear group  $G = GL_{n+1}(\mathbb{F}_q)$  has a split  $BN$ -pair of rank  $n$  and characteristic  $p$ , and satisfies the conditions stated in Proposition 69.2.*

*Proof.* We keep the notation introduced in the proof of Theorem 65.10, where we showed that  $G$  has a  $BN$ -pair of rank  $n$ . In addition to the groups  $B$ ,  $N$ , and  $T$  defined previously, let

$$U = \text{group of upper unit triangular matrices} = \{(a_{ij}) \in B : a_{ii} = 1 \text{ for each } i\}$$

$$U^- = \text{group of lower unit triangular matrices.}$$

Since  $\text{char } \mathbb{F}_q = p$ ,  $U$  is a  $p$ -group,  $T$  is an abelian  $p'$ -group, and it is easily checked that  $B$  is a semidirect product  $B = U \rtimes T$ . Thus  $G$  satisfies (ii) and (iii) of (69.1).

As in the proof of (65.10), let  $\{e_1, \dots, e_{n+1}\}$  be a basis for the vector space on which  $G$  acts, and let  $\varphi: N \rightarrow S_{n+1}$  be the homomorphism defined by setting  $\varphi(x) = \sigma \in S_{n+1}$ , where

$$x \langle e_i \rangle = \langle e_{\sigma(i)} \rangle, \quad 1 \leq i \leq n+1.$$

The map  $\varphi$  identifies the Weyl group  $N/T$  of  $G$  with  $S_{n+1}$ , since  $\ker \varphi = T$ . For  $1 \leq i \leq n$ , let  $s_i$  be the element of  $N$  that interchanges  $e_i$  and  $e_{i+1}$  and fixes the other basis vectors. Then  $\varphi(s_i) = (i, i+1)$ , so  $\varphi$  identifies the distinguished generators  $\{s_i\}$  of  $N/T$  with the transpositions  $\{(i, i+1)\}$ .

Now consider the root system  $\Delta$  associated with  $S_{n+1}$ , defined in Exercise 64.1. Then  $\Delta$  consists of the vectors  $\{\varepsilon_i - \varepsilon_j : i \neq j, 1 \leq i, j \leq n+1\}$ , in a Euclidean space with an orthonormal basis given by  $\{\varepsilon_1, \dots, \varepsilon_{n+1}\}$ . The elements of  $S_{n+1}$  permute the basis vectors  $\{\varepsilon_i\}$ , and hence permute the roots. Let

$$\Pi = \{\alpha_1, \dots, \alpha_n\}, \quad \text{where } \alpha_i = \varepsilon_i - \varepsilon_{i+1}, \quad 1 \leq i \leq n.$$

By Exercise 64.1,  $\Pi$  is a fundamental system in  $\Delta$ , and the fundamental reflections  $\{s_{\alpha_i}\}_{1 \leq i \leq n}$  can be identified with the transpositions  $\{(i, i+1), 1 \leq i \leq n\}$  considered above. Let  $\Delta_{\pm}$  be the positive (resp. negative) roots in  $\Delta$  defined by the set  $\Pi$ .

We now carry over the root system  $\Delta$  to the finite group  $G$  as follows. For each root  $\alpha = \varepsilon_i - \varepsilon_j \in \Delta$ , let  $U_\alpha$  be the subgroup of  $G$  consisting of all elementary matrices

$$x_\alpha(t) = E_{ij}(t) = \mathbf{I} + t\mathbf{e}_{ij}, \quad t \in \mathbb{F}_q,$$

(see (40.22)). We clearly have

$$(69.4) \quad U = \langle U_\alpha : \alpha \in \Delta_+ \rangle \quad \text{and} \quad U^- = \langle U_\alpha : \alpha \in \Delta_- \rangle.$$

The subgroups  $\{U_\alpha\}_{\alpha \in \Delta}$  are normalized by  $T$  and permuted under conjugation by the elements of  $N$ . An easy calculation shows that if  $\varphi(x) = \sigma \in S_{n+1}$ , then

$${}^x U_\alpha = U_{\sigma\alpha} \quad \text{for all } x \in N.$$

Using the isomorphism  $N/T \cong S_{n+1}$ , we can rewrite this formula as

$$(69.5) \quad {}^w U_\alpha = U_{w\alpha}, \quad w \in W, \quad \alpha \in \Delta.$$

Let  $w_0$  be the element of maximal length in  $W$ . Then  $w_0\Delta_+ = \Delta_-$  by (64.16vi), and it follows that  $U^- = U^{w_0}$ , using (69.4) and (69.5). Since  $U \cap U^- = 1$ , we have

$$\bigcap_{x \in N} {}^x B \leq B \cap B^{w_0} = UT \cap U^- T = T,$$

proving (69.1i). We also have  $B \cap U^- = 1$ , and  $U_w^- \cap U_w^+ = 1$  since  ${}^w(U_w^- \cap U_w^+) \leq U^- \cap U = 1$ . Another application of (69.5) shows that  $U_{\alpha_i} = U \cap U^{w_0 s_i}$ ,  $1 \leq i \leq n$ , completing the proof of (69.2iii).

We leave it to the reader to check (69.2vi), as well as the formula

$$(69.6) \quad (U_\alpha U_\beta) = \begin{cases} 1 & \text{if } \alpha + \beta \notin \Delta \\ U_{\alpha+\beta} & \text{if } \alpha + \beta \in \Delta, \end{cases}$$

for all roots  $\alpha, \beta$  such that  $\beta \neq \pm \alpha$ . This implies (69.2vii).

The remaining parts of (69.2) are proved using (69.6), as follows. First consider the structure of  $U = U_{w_0}$ . Let  $m = |\Delta_+|$ , and let  $\{\beta_1, \dots, \beta_m\}$  be the positive roots arranged in order of increasing height (see (64.12)). Note that if  $i < j$ , then  $ht(\varepsilon_i - \varepsilon_j) = j - i$ . We claim now that

$$U = U_{\beta_1} \cdots U_{\beta_m}.$$

For each  $i \geq 0$ , let  $U_i$  denote the subgroup of  $U$  generated by all root subgroups  $\{U_\beta : \beta \in \Delta_+, ht \beta \geq i\}$ . Then  $U_i \trianglelefteq U$  for each  $i$ , by (69.6). It is now readily shown, using (69.6) and decreasing induction on  $i$ , that for each  $i \leq 0$  we have

$$U_i = U_{\beta_j} U_{\beta_{j+1}} \cdots U_{\beta_m}$$

where the notation is chosen so that  $\{\beta_j, \dots, \beta_m\}$  are the positive roots of height  $\geq i$ . Setting  $i = 0$ , we obtain the desired result.

A similar argument shows that for each  $w \in W$ , we have

$$(69.7) \quad U = U_w^- U_w^+,$$

where  $U_w^\pm = \langle U_\alpha : \alpha \in \Delta_w^\pm \rangle$  as in (69.2iv). The factorization (69.7) is proved by showing that

$$U_i = (U_i \cap U_w^-)(U_i \cap U_w^+)$$

using decreasing induction on  $i$ . From (69.7) and (69.5), we obtain the alternative description

$$U_w^- = U \cap U^{w_0 w}, \quad U_w^+ = U \cap U^w.$$

In particular, we have  $U_w^+ = U_{w_0 w}^-$ . The product formula

$$U_w^- = U_{\gamma_1} \cdots U_{\gamma_t},$$

for some ordering of the roots  $\gamma_i \in \Delta_w^-$ , is proved in the same way as for  $U$ . The uniqueness of expression in the factorization of  $U_w^-$  follows by induction on  $l(w)$ , since

$$(69.8) \quad U_{ws_i}^- = U_{\alpha_i}^{-s_i} U_w^- \quad \text{and} \quad U_{\alpha_i} \cap {}^{s_i} U_w^- = 1 \quad \text{if } l(ws_i) \geq l(w).$$

This result follows, in turn, from the formula  $\Delta_{ws_i}^- = \{\alpha_i\} \dot{\cup} s_i(\Delta_w^-)$  if  $l(ws_i) \geq l(w)$  (see the proof of (64.16i)), and the fact that  ${}^{s_i}(U_{\alpha_i} \cap {}^{s_i} U_w^-) \leq U_{-\alpha_i} \cap U_w^- \leq U^- \cap U = 1$ .

It remains to prove (69.2v). Since  $G$  has a  $BN$ -pair by (65.10), we have

$$G = \bigcup_{w \in W} B \dot{w} B.$$

Now let  $w \in W$ , and consider  $B \dot{w} B$ . Since  $B = TU$  and  $U = U_w^+ U_w^-$  by (69.7), we have

$$B \dot{w} B = B \dot{w} T U_w^+ U_w^- = B \dot{w} U_w^-$$

since  $\dot{w} T U_w^+ \dot{w}^{-1} \leq B$ . Now let

$$g = b \dot{w} u = b' \dot{w} u'$$

be two expressions of an element  $g \in B \dot{w} B$ , with  $b, b' \in B$  and  $u, u' \in U_w^-$ . Then

$$(b')^{-1} b = \dot{w} u' u^{-1} \dot{w}^{-1} \in B \cap U^- = 1$$

by (69.2i), and hence  $b = b'$ ,  $u = u'$ . This completes the proof of the proposition.

Returning to the general discussion, we have:

**(69.9) Proposition.** *Let  $G$  be a finite group with a split BN-pair of rank  $n$  and characteristic  $p$ . Then the following statements hold.*

- (i)  $|G| = |U||T|\sum_{w \in W} |U_w^-|$ , where  $W$  is the Weyl group of  $G$ .
- (ii)  $U$  is a Sylow  $p$ -subgroup of  $G$ .
- (iii)  $O_p(G) = 1$ .
- (iv)  $\text{St}_G(1) = |G|_p$ , where  $\text{St}_G$  is the Steinberg character of  $G$  (see §67B).

The proof is left as an exercise for the reader. Part (i) is an application of (69.2v), and implies part (ii), using the fact that  $|U_w^-|$  is a power of  $p$  for all  $w$ , and is 1 if and only if  $w = 1$ .

**Remark.** Part (iii) of (69.9) is the exact counterpart, in finite group theory, of the condition that an affine algebraic group  $G$  be *reductive*, namely  $R_u(G) = 1$ , where  $R_u(G)$  is the unipotent radical of  $G$  (see Carter [85]).

We are now ready to prove the main result of this section.\* The statement involves notation introduced earlier in this section and in §§64C and 65C. In particular, for  $J \subseteq S$ ,  $\Delta_J$  denotes the root system associated with the parabolic subgroup  $W_J$  of  $W$ .

**(69.10) Theorem.** *Let  $G$  be a finite group with a split BN-pair of characteristic  $p$ , let  $(W, S)$  be the Weyl group of  $G$ , with distinguished generators  $S$ , and let  $P_J$  be a standard parabolic subgroup of  $G$ , for some subset  $J$  of  $S$ . Define*

$$L_J = \langle T, U_\alpha : \alpha \in \Delta_J \rangle, \quad V_J = \langle U_\beta : \beta \in \Delta_+ - \Delta_{J,+} \rangle.$$

Then we have:

- (i)  $P_J = V_J \rtimes L_J$  (semidirect product).
- (ii)  $V_J = O_p(P_J)$ .
- (iii)  $P_J = N_G(V_J)$ .
- (iv)  $L_J$  is a finite group with a split BN-pair of characteristic  $p$ , with Borel subgroup  $B \cap L_J$ , and Weyl group  $W_J$ .

We first require some additional properties of root systems.

**(69.11) Lemma.** *For  $J \subset S$ , let  $w_J$  denote the element of maximal length in the Coxeter group  $W_J$ . Then we have:*

- (i)  $\Delta_{J,+} = \Delta_{w_J}^-, \Delta_+ - \Delta_{J,+} = \Delta_{w_J}^+ \quad \text{where } \Delta_{J,+} = \Delta_J \cap \Delta_+$ .

\*The reader will find it profitable to compare the proof given below, based on (69.2), with a proof of the theorem for Chevalley groups (see Carter [72b]).

(ii) Let  $\alpha \in \Delta_{w_J}^+$ ,  $\beta \in \Delta_J$ , and suppose that  $i\alpha + j\beta \in \Delta$ , where  $i, j > 0$ . Then  $i\alpha + j\beta \in \Delta_{w_J}^+$ .

*Proof.* (i) is easily proved from the definitions (see (64.15) and (64.36)) and is left as an exercise.

(ii) By part (i),  $\alpha \in \Delta_+ - \Delta_{J,+}$ . Since  $\beta \in \Delta_J$ , and  $i, j > 0$ , it follows that  $i\alpha + j\beta \in \Delta_+$  is a linear combination of fundamental roots, in which some fundamental root not in  $\Pi_J$  appears with a positive coefficient. Then  $i\alpha + j\beta \in \Delta_+$ , by (64.6), and moreover  $i\alpha + j\beta \in \Delta_+ - \Delta_{J,+}$ , completing the proof.

*Proof of Theorem 69.10.* First let  $J = \emptyset$ . Then  $L_J = T$ ,  $V_J = U$ , and (i), (ii), and (iv) hold by definition of a split BN-pair. We have  $N_G(U) \geq B$ , and must have equality; otherwise,  $N_G(U)$  contains  $s$  for some  $s \in S$ , by (65.13), which is impossible since  ${}^sU \neq U$  by (69.2). Thus (iii) holds, and the theorem is proved in this case.

Now assume  $J \neq \emptyset$ ; then  $V_J \leq U_{w_J}^+$  by (69.11i), and by (69.2iv) we have equality. Next, by (69.11ii) and the commutator formulas (69.2vii), it follows that  $L_J$  normalizes  $V_J$ . Using the Bruhat decomposition of  $P_J$  together with the facts that  $BwB = BwU_w^-$  and  $U = U_w^+U_w^-$ ,  $w \in W$  (by (69.2v) and (69.2ii)), we obtain

$$(69.12) \quad P_J = \bigcup_{w \in W_J} UT\dot{w}U_w^- = \dot{\cup} V_J U_{w_J}^- T\dot{w}U_w^-.$$

We now verify that the coset representatives  $\{\dot{w} : w \in W_J\}$  belong to  $L_J$ . By (69.2vi),  $U_{\alpha_i}T \cup U_{\alpha_i}T\dot{s}_iU_{\alpha_i}$  is a group, and hence contains  $U_{-\alpha_i} = {}^{s_i}U_{\alpha_i}$ . Moreover  $U_{-\alpha_i} \not\leq U_{\alpha_i}T$  by (69.2i), and it follows that

$$U_{-\alpha_i} \cap U_{\alpha_i}T\dot{s}_iU_{\alpha_i} \neq \emptyset.$$

Thus  $v = u't\dot{s}_i u''$  for some  $v \in U_{-\alpha_i}$ ,  $u', u'' \in U_{\alpha_i}$ ,  $t \in T$ . Solving for  $\dot{s}_i$ , we obtain

$$\dot{s}_i \in \langle U_{\alpha_i}, U_{-\alpha_i}, T \rangle.$$

Therefore  $\dot{s}_i \in L_J$  if  $s_i \in J$ , and since any element  $w \in W_J$  is a product of elements of  $J$ , we have shown that  $\dot{w} \in L_J$  for all  $w \in W_J$ . The subgroups  $U_w^-$ , for  $w \in W_J$ , also are contained in  $L_J$ , since  $U_w^- = \langle U_\alpha : \alpha \in \Delta_w^- \rangle$  by (69.2iv), and  $\Delta_w^- \subseteq \Delta_J$  if  $w \in W_J$  (see Exercise 64.6). Thus (69.12) implies that  $P_J \leq V_J L_J$ .

We next prove that  $L_J$  has a BN-pair with subgroups  $B'$ ,  $N'$ , where  $B' = U_{w_J}^- T$ ,  $N' = \langle T, \dot{w} : w \in W_J \rangle$ . The axioms are all easily verified except for showing that

$$s_i B' w \subseteq B' w B' \cup B' s_i w B', \quad s_i \in J, \quad w \in W_J.$$

This is proved as follows. Let  $w_J = w's_b$ ,  $w' \in W_J$ ,  $l(w') = l(w_J) - 1$ . Then  $\Delta_{w_J}^- = \{\alpha_i\} \dot{\cup} s_i(\Delta_{w'}^-)$ , and by the proof of (69.8) we have  $U_{w_J}^- = {}^{s_i}U_{w'}^- \cdot U_{\alpha_i}$  so

$$s_i B' w = T U_{w'}^- \dot{s}_i U_{\alpha_i} \dot{w} \subseteq B' \dot{s}_i U_{\alpha_i} \dot{w}.$$

If  $w^{-1}\alpha_i \in \Delta_+$ , then by (69.2iii),  $\dot{w}^{-1}U_{\alpha_i}\dot{w} = U_{w^{-1}(\alpha_i)} \subseteq B'$ , and

$$s_i B' w \subseteq B' s_i w B'$$

in this case. Now assume  $w^{-1}\alpha_i \in \Delta_-$ ; then we have

$$s_i B' w \subseteq B' U_{-\alpha_i} s_i \dot{w} \subseteq B' s_i w B' \cup B' s_i U_{\alpha_i} s_i w$$

since, as we noted above,  $U_{-\alpha_i}$  is contained in the group defined in (69.2vi). The second expression becomes

$$B' w w^{-1} s_i U_{\alpha_i} s_i w \subseteq B' w U_{w^{-1}s_i\alpha_i} \subseteq B' w B',$$

since  $w^{-1}s_i\alpha_i \in \Delta_+$ , in this case. This completes the proof that  $L_J$  has a BN-pair. An easy argument, again using (69.2), shows that  $L_J$  has a split BN-pair of characteristic  $p$ , with  $U_{w_J}^- = O_p(B')$ .

The sharp form of the Bruhat decomposition of  $L_J$  becomes

$$(69.13) \quad L_J = \bigcup_{w \in W_J} U_{w_J}^- T \dot{w} U_w^-.$$

Then (69.12) asserts that  $P_J = L_J V_J$ . Moreover,  $B \cap L_J = U_{w_J}^- T$  by (69.13) combined with the Bruhat decomposition in  $G$ , so that

$$L_J \cap V_J \leq (L_J \cap B) \cap V_J = U_{w_J}^- T \cap U_{w_J}^+ = 1$$

by (69.2ii), and (i) is proved.

We next prove (ii). Since  $V_J \leq U$  and  $P_J = L_J V_J$  by (i), we have  $V_J \leq O_p(P_J)$ . On the other hand,  $O_p(P_J) \leq U$ , since  $U$  is a Sylow  $p$ -subgroup of  $P_J$ , by (69.9ii). Let  $u \in O_p(P_J)$ ; then by (69.2ii), we have  $u = u' u''$ , with  $u' \in V_J$ ,  $u'' \in U_{w_J}^-$ . Then

$${}^{w_J} u \in O_p(P_J) \leq U, \quad \text{and} \quad {}^{w_J} u = {}^{w_J} u' {}^{w_J} u'' \in V_J \cdot {}^{w_J} U_{w_J}^-.$$

Since  ${}^{w_J} U_{w_J}^- \leq U^-$ , and  $U \cap U^- = 1$ , it follows that  $u'' = 1$  and  $u \in V_J$ , completing the proof of (ii).

(iii) By part (i), we have  $P_J \leq N_G(V_J)$ . If the inclusion were proper, then  $N_G(V_J) = P_J$ , for some  $J' \not\supseteq J$ , by (65.13) and (65.17). We would then have  ${}^{w_{J'}} V_J = V_J$ , which is impossible, since  $V_J$  contains  $U_\alpha$  for some  $\alpha \in \Delta_{w_J}^-$ , if  $J' \neq J$ , and  ${}^{w_{J'}} U_\alpha \leq U^-$ , by (69.2iii). Thus  $N_G(V_J) = P_J$ , and (iii) is proved. Since (iv) has already been proved, the theorem is established.

**(69.14) Definition.** Let  $G$  be as in Theorem 69.10, and let  $J \subseteq S$ . The semidirect product decomposition  $P_J = L_J V_J$  is called a *Levi decomposition* of  $P_J$ , and the subgroup  $L_J$  is called a *standard Levi factor* of  $P_J$ .

The Levi decomposition is of fundamental importance in the representation theory of  $G$ , since questions about representations and characters of  $G$  can often be reduced to the corresponding questions for Levi subgroups, which are themselves groups with  $BN$ -pairs of lower rank than  $G$ .

### §69B. Intersections of Parabolic Subgroups

Throughout this subsection, the following notation will be used.

$G$  = a finite group with a split  $BN$ -pair of characteristic  $p$

$B$  = a Borel subgroup of  $G$

$U = O_p(B)$

$W$  = the Weyl group of  $G$

$S = \{s_1, \dots, s_n\}$  = the distinguished generators of  $W$

$\Pi = \{\alpha_1, \dots, \alpha_n\}$  = a set of fundamental roots in the root system associated with  $W$ , such that  $s_i \leftrightarrow s_{\alpha_i}$ ,  $1 \leq i \leq n$ .

Let  $J_1, J_2 \subseteq S$ , and let  $P_{J_1}, P_{J_2}$  be the corresponding standard parabolic subgroups of  $G$ , as in §65C. In §§70, 71 we shall have to calculate  $(\varphi_1^G, \varphi_2^G)$ , for  $\varphi_1 \in \text{ch } CP_{J_1}$ ,  $\varphi_2 \in \text{ch } CP_{J_2}$ . In order to apply the Intertwining Number Theorem 10.24, we require information about the intersections  $P_{J_1} \cap {}^x P_{J_2}$ ,  $x \in G$ . In contrast to the situation for finite Coxeter groups (see (64.40)), the intersection  $P_{J_1} \cap {}^x P_{J_2}$  is not always a parabolic subgroup. In this subsection, we determine these intersections explicitly.

We shall make frequent use of the notation and results from §§69A, 64C, and 65C. In particular, for  $J \subseteq S$  we set:

$W_J = \langle J \rangle$ , a parabolic subgroup of  $W$

$\Delta_J, \Pi_J$  = the root system, and fundamental roots, associated with  $W_J$  (see (64.36))

$\Delta_{J,+} = \Delta_+ \cap \Delta_J$ , where  $\Delta_+$  is the set of positive roots containing  $\Pi$

$w_J$  = the unique element of maximal length in  $W_J$

$P_J = L_J V_J$  = the Levi decomposition of  $P_J$  (see (69.10)).

The following results were proved in the context of reductive algebraic groups defined over finite fields by Borel-Tits [65], Harish-Chandra [70], and Springer [75]. Their adaptations to finite groups with split  $BN$ -pairs were given by Curtis [75].

**(69.15) Proposition.** *Let  $J \subseteq S$ . For all subsets  $J' \subseteq J$ ,  $P_{J'} \cap L_J$  is a standard parabolic subgroup of  $L_J$  (containing the Borel subgroup  $B \cap L_J$  of  $L_J$ ). Moreover,*

$$O_p(P_{J'} \cap L_J) = V_{J'} \cap L_J,$$

and  $P_{J'} \cap L_J$  has a Levi decomposition

$$P_{J'} \cap L_J = L_{J'}(V_{J'} \cap L_J),$$

and  $V_{J'} = (V_{J'} \cap L_J)V_J$ . The map  $P_{J'} \rightarrow P_{J'} \cap L_J$  gives a bijection from the set of

standard parabolic subgroups  $\{P_{J'}\}_{J' \subseteq J}$  of  $G$  to the set of all standard parabolic subgroups of  $L_J$ .

*Proof.* By (69.10iv),  $B \cap L_J$  is a Borel subgroup of  $L_J$ . Now let  $J' \subseteq J$ . Then  $P_{J'} \geq B$ , and  $P_{J'} \cap L_J \geq B \cap L_J$ , so  $P_{J'} \cap L_J$  is a standard parabolic subgroup of  $L_J$ . By the definition in (69.10),  $L_{J'}$  is a standard Levi factor of  $P_{J'} \cap L_J$ . Since  $V_J \leq V_{J'}$ , the Levi decomposition  $P_{J'} = L_{J'}V_{J'}$  implies that  $V_{J'} = (V_{J'} \cap L_J)V_J$ . Then  $P_{J'} = L_{J'}V_{J'} = L_{J'}(V_{J'} \cap L_J)V_J$ . It is easily seen that  $V_{J'} \cap L_J = O_p(P_{J'} \cap L_J)$ , and hence  $L_{J'} \cap P_{J'} = L_{J'}(V_{J'} \cap L_J)$  is a Levi decomposition of  $L_J \cap P_{J'}$ .

Now let  $J', J'' \subseteq J$ , and suppose  $P_{J'} \cap L_J = P_{J''} \cap L_J$ . Then  $O_p(P_{J'} \cap L_J) = O_p(P_{J''} \cap L_J)$ , whence  $V_{J'} \cap L_J = V_{J''} \cap L_J$ . By what has been shown above, this implies that  $V_{J'} = V_{J''}$ , and we conclude that  $P_{J'} = P_{J''}$  by Theorem 69.10iii. Finally, if  $Q$  is a standard parabolic subgroup of  $L_J$ , then  $QV_J \geq (B \cap L_J)V_J = B$ , by the proof of (69.10). Then  $QV_J$  is a standard parabolic subgroup of  $G$  contained in  $P_J$ , and we clearly have  $QV_J \cap L_J = Q$ . Thus the correspondence  $P_{J'} \rightarrow P_{J'} \cap L_J$ , for  $J' \subseteq J$ , is a bijection, and the proof is complete.

For the remainder of §69B, let  $I, J \subseteq S$ , and let  $x \in D_{IJ}$  be a fixed distinguished double coset representative (see (64.39)). By (64.40) and (64.41) we have

$$W_I \cap {}^x W_J = W_K, \quad \text{where } K = I \cap {}^x J,$$

$$\Delta_I \cap x\Delta_J = \Delta_K, \quad \text{and} \quad \Pi_I \cap x\Pi_J = \Pi_K.$$

**(69.16) Theorem.** Let  $I, J \subseteq S$ , and let  $x \in D_{IJ}$ , as above. Then the following statements hold:

- (i)  $P_K = (P_I \cap {}^x P_J)V_I$ , where  $K = I \cap {}^x J$ .
- (ii)  $V_K = (P_I \cap {}^x V_J)V_I$  and  $L_K = L_I \cap {}^x L_J$ .
- (iii)  $P_I \cap {}^x V_J = (L_I \cap {}^x V_J)(V_I \cap {}^x V_J)$ .
- (iv)  $L_I \cap {}^x P_J$  is a standard parabolic subgroup of  $L_I$ ,

and

$$L_I \cap {}^x P_J = L_I \cap P_K, \quad O_p(L_I \cap {}^x P_J) = L_I \cap {}^x V_J.$$

- (v) We have a factorization

$$P_I \cap {}^x P_J = L_K(L_I \cap {}^x V_J)(V_I \cap {}^x L_J)(V_I \cap {}^x V_J),$$

with uniqueness of expression.

*Proof.* (i) The product on the right-hand side of (i) is a subgroup, because  $P_I$  normalizes  $V_I$  (see (69.10)). From the definitions of  $K, L_K$ , and  $V_K$ , we have

$$L_K \leq L_I \cap {}^x L_J \quad \text{and} \quad V_K \geq V_I,$$

so

$$P_K = \langle T, U_\alpha : \alpha \in \Delta_K \cup \Delta_+ \rangle \leq (P_I \cap {}^x P_J) V_I.$$

Conversely,  $P_I \cap {}^x P_J$  is a union of intersections of the form

$$ByB \cap {}^x(BzB), \quad \text{with } y \in W_I, \quad z \in W_J.$$

Since  $x \in D_{IJ}$ , we have

$$l(yx) = l(y) + l(x) \quad \text{and} \quad l(xz) = l(x) + l(z) \quad \text{for all } y \in W_I, \quad z \in W_J.$$

Also recall that if  $l(xy) = l(x) + l(y)$ , where  $x, y \in W$ , then

$$xBy \subseteq BxyB,$$

by (65.5). Thus if the above intersection  $ByB \cap {}^x(BzB) \neq \emptyset$ , we have  $ByBx \cap {}^x BzB \neq \emptyset$ , and hence

$$ByxB \cap BxzB \neq \emptyset.$$

By the uniqueness statement in (65.4), it follows that  $yx = xz$  in  $W$ , and therefore  $y = xzx^{-1} \in W_I \cap {}^x W_J = W_K$ . We have now shown that if  $ByB \cap {}^x(BzB) \neq \emptyset$ , then  $y \in W_K$ , and hence  $(P_I \cap {}^x P_J) V_I \leq P_K$ , completing the proof of (i).

(ii) By part (i), we have  $(P_I \cap {}^x V_J) V_I \leq P_K$ , and it is then clear that  $(P_I \cap {}^x V_J) V_I \leq O_p(P_K)$ . In order to prove the reverse inclusion, we start with the fact that by its definition in (69.10),  $V_K$  is generated by root subgroups  $\{U_\beta : \beta \in \Delta_+ - \Delta_{K,+}\}$ ; we shall prove that  $U_\beta \leq (P_I \cap {}^x V_J) V_I$  for each such root  $\beta$ . If  $\beta \notin \Delta_{I,+}$ , then  $U_\beta \leq V_I$  by the definition of  $V_I$ , and there is nothing further to prove in this case. We may thus assume that  $\beta \in \Delta_{I,+}$ , and  $\beta \notin \Delta_K$ . Since  $x \in D_{IJ}$ , we have  $l(s_i x) \geq l(x)$  for all  $s_i \in I$ , and hence  $x^{-1}(\alpha_i) \subseteq \Delta_+$  for all  $\alpha_i \in \Pi_I$ , by (64.16vii), and it follows that  $x^{-1}\beta \in \Delta_+$ . On the other hand,  $\beta \notin \Delta_K$  implies  $x^{-1}\beta \notin \Delta_J$ , since  $\Delta_K = \Delta_I \cap x\Delta_J$ , and we have  $x^{-1}\beta \in \Delta_+ - \Delta_{J,+}$ . Thus  $U_{x^{-1}\beta} \leq V_J$  by the definition of  $V_J$ , and since  $U_{x^{-1}\beta} = {}^{x^{-1}}U_\beta$  by (69.2), we obtain  $U_\beta \leq {}^x V_J \cap P_I$ , completing the proof of the first statement. The second is proved after (iv).

(iii) The right-hand side is certainly contained in the left, since  $P_I = L_I V_I$  by (69.10). For the reverse inclusion, we have

$$P_I \cap {}^x V_J \leq V_K,$$

by the first part of (ii). By (69.11i) and the definition of  $V_K$ , we have  $V_K = U_{w_K}^+$ , where  $w_K$  is the element of maximal length in  $W_K$ . By (69.2iv), it follows that  $V_K$  is the product of the root subgroups  $\{U_\beta : \beta \in \Delta_+ - \Delta_{K,+} = \Delta_{w_K}^+\}$ , taken in some order. By the proof of part (ii), these root subgroups satisfy the condition:

$$\text{either } U_\beta \leq V_I \quad \text{or} \quad U_\beta \leq P_I \cap {}^x V_J, \quad \text{for } \beta \notin \Delta_+ - \Delta_{I,+}.$$

We also have  $V_I \trianglelefteq V_K$ , since  $K \subseteq I$ , and  $V_I$  is normalized by  $P_I$ , which certainly contains  $V_K$ . Thus

$$(69.17) \quad (U_\beta, U_\gamma) \leq V_I, \quad \text{if} \quad U_\beta \leq V_I, \quad U_\gamma \leq V_K.$$

Now let  $g \in P_I \cap {}^x V_J$ . Since  $g \in V_K$ ,  $g$  is a product of elements belonging to the root subgroups  $\{U_\beta\}$  as above, and by rearranging the factors, using the commutator relation (69.17), we obtain

$$g = g'g'',$$

where  $g'$  is a product of elements of root subgroups  $U_\beta \leq P_I \cap {}^x V_J$ ,  $\beta \notin \Delta_+ - \Delta_{I,+}$ , and  $g'' \in V_I$ . Thus  $g'' \in V_I \cap {}^x V_J$ , since both  $g$  and  $g'$  belong to  ${}^x V_J$ , and  $g' \in L_I \cap {}^x V_J$  because the root subgroups  $\{U_\beta \leq P_I \cap {}^x V_J, \beta \in \Delta_{w_K}^+, \beta \notin \Delta_+ - \Delta_{I,+}\}$  all belong to  $L_I$ . Thus  $g \in (L_I \cap {}^x V_J)(V_I \cap {}^x V_J)$ , and (iii) is proved.

(iv) The proof of (ii) shows that  $x^{-1}(\Delta_{I,+}) \subseteq \Delta_+$ . By the remark following (69.13),  $B \cap L_I = U_{w_I}^- T$ , and  $\Delta_{w_I}^- = \Delta_{I,+}$  by (69.11i). It follows that

$$B \cap L_I \leq L_I \cap {}^x P_J,$$

and hence  $L_I \cap {}^x P_J$  is a standard parabolic subgroup of  $L_I$ , containing the Borel subgroup  $B \cap L_I$  (see (69.10iv)). Moreover,  $L_I \cap {}^x P_J \leq L_I \cap V_K$ , and by (69.15), we have  $O_p(L_I \cap P_K) = L_I \cap V_K$ . By parts (ii) and (iii), we obtain  $L_I \cap V_K = L_I \cap {}^x V_J$ . By (69.15) again, we have

$$L_I \cap P_K = L_K(L_I \cap V_K) = L_K(L_I \cap {}^x V_J) \leq L_I \cap {}^x P_J,$$

using the fact that  $\Delta_K = \Delta_I \cap x\Delta_J$ . Combining our results, we have shown that

$$L_I \cap {}^x P_J = L_I \cap P_K \quad \text{and} \quad O_p(L_I \cap {}^x P_J) = L_I \cap {}^x V_J,$$

completing the proof of (iv).

We are now in a position to prove the second statement of (ii). Since  $\Delta_K = \Delta_I \cap x\Delta_J$ , we have  $L_K \leq L_I \cap {}^x L_J$ , by the definition of the Levi subgroups in (69.10). Then

$$L_I \cap {}^x L_J \leq L_I \cap {}^x P_J = L_K(L_I \cap {}^x V_J)$$

by part (iv). Suppose  $l \in L_I \cap {}^x L_J$ , and write  $l = mu$ , with  $m \in L_K$ ,  $u \in L_I \cap {}^x V_J$ . Then  $m^{-1}l = u \in {}^x L_J \cap {}^x V_J = 1$ , so  $u = 1$ , and  $L_I \cap {}^x L_J \leq L_K$ , completing the proof.

(v) We first prove

$$(69.18) \quad P_I \cap {}^x P_J = L_K(P_I \cap {}^x V_J)(V_I \cap {}^x P_J).$$

Now  $P_I \cap {}^x P_J \leq P_K = L_K V_K$  by part (i), and  $V_K = (P_I \cap {}^x V_J)V_I$  by part (ii). Thus

each element  $g \in P_I \cap {}^x P_J$  can be expressed in the form

$$g = luv, \quad \text{with} \quad l \in L_K, \quad u \in P_I \cap {}^x V_J, \quad v \in V_I.$$

This formula implies that  $v \in V_I \cap {}^x P_J$ , and we have  $P_I \cap {}^x P_J \leq L_K (P_I \cap {}^x V_J) (V_I \cap {}^x P_J)$ . For the reverse inequality, it suffices by (i) to prove that  $L_K \leq P_I \cap {}^x P_J$ , and this is immediate by the second part of (ii). The factorization of  $P_I \cap {}^x P_J$  given in (v) follows from (69.18), using (iii). The uniqueness of expression follows by consideration of the Levi decompositions in  $P_I$  and  ${}^x P_J$ , and is left to the reader. This completes the proof of the theorem.

By (65.19), two standard parabolic subgroups  $P_I$  and  $P_J$  are never conjugate in  $G$  unless they coincide. On the other hand, their Levi subgroups may be conjugate even when  $I \neq J$ . To conclude this subsection, we give a criterion for this to occur, in terms of the results obtained in (69.16) on slicing up intersections of parabolic subgroups.

**(69.19) Theorem.** *Let  $I, J \subseteq S$ , and let  $x \in D_{IJ}$ , as in (69.16). Then the following statements are equivalent.*

- (i)  $P_K = P_I$ .
- (ii)  $P_I \cap {}^x V_J \leq V_I$ .
- (iii)  $L_I \leq {}^x L_J$ .

*Proof.* (i)  $\Rightarrow$  (iii). By (i) we have  $W_K = W_I$ , whence  $\Delta_K = \Delta_I$ . Since  $\Delta_K = \Delta_I \cap x\Delta_J$ , it follows that  $\Delta_I \leq x\Delta_J$ . Then  $L_I \leq {}^x L_J$ , by (69.2iii) and the definitions of the Levi subgroups in (69.10).

(iii)  $\Rightarrow$  (ii). From (iii) and (69.10) applied to  $P_J$ , we obtain  $L_I \cap {}^x V_J = 1$ . Then (ii) follows from (69.16iii).

(ii)  $\Rightarrow$  (i). By (69.16ii),  $P_I \cap {}^x V_J \leq V_I$  implies that  $V_K = V_I$ . Then  $P_I = P_K$  by (69.10iii), completing the proof.

## §69. Exercise

Describe the standard parabolics, and their Levi decompositions, for the split  $BN$ -pair in  $GL_{n+1}(\mathbb{F}_q)$  given in (69.3).

## §70. CUSPIDAL CHARACTERS

### §70A. Generalized Restriction and Induction

Each proper standard parabolic subgroup  $P_I$  in a finite group  $G$  of Lie type has a Levi subgroup  $L_I$ . This is also a finite group of Lie type, with a  $BN$ -pair whose rank is smaller than that of the given  $BN$ -pair in  $G$ . Thus it is natural

to seek as much information as possible on the relation between characters of  $L_I$  and  $G$ . The usual operations of induction and restriction, and their connections through the Mackey theorems (§§10B,C), require information concerning the double cosets  $L_I \backslash G / L_I$ . This involves the subgroup  $V_I = O_p(P_I)$ , where  $p$  is the characteristic, and depends in a complicated way on the structure of the group  $G$ . On the other hand, the double cosets  $P_I \backslash G / P_I$  are parametrized by elements of the Weyl group  $W$  of  $G$ , by (65.21), and are thus described by generic information, depending only on the family of groups of Lie type of type  $W$  to which  $G$  belongs.

For these reasons, it is useful to define generalized operations of restriction and induction, which suppress the influence of the  $p$ -subgroups  $V_I$ . These ideas were first used systematically by Green [55] in his determination of the characters of  $GL_n(\mathbb{F}_q)$ , and were applied by Harish-Chandra [70] to reductive groups over finite fields.

We begin with some elementary remarks about these generalized operations, suggested by the Levi decomposition of standard parabolic subgroups  $P_I = L_I \rtimes V_I$ , where  $V_I = O_p(P_I)$ , and where  $L_I$  is a standard Levi subgroup (see §69A). We shall use some notation from §§9, 10:

$\text{ch } H = \text{ch } CH$ , the ring of virtual C-characters of a finite group  $H$ ,

$\text{Irr } H =$  a basic set of irreducible C-characters of  $H$ ,

$\zeta \rightarrow \zeta_H = \text{res}_H^G \zeta$ , the operation of restriction from  $\text{ch } G$  to  $\text{ch } H$ , for a subgroup  $H \leq G$ ,

$\lambda \rightarrow \lambda^G = \text{ind}_H^G \lambda$ , the operation of induction from  $\text{ch } H$  to  $\text{ch } G$ .

For the moment, let  $G$  denote an arbitrary finite group,  $H$  a subgroup of  $G$ , and  $V$  a normal subgroup of  $H$ . In this situation, we can define an operation of *generalized restriction*  $r_{H/V}^G : \text{ch } G \rightarrow \text{ch } H/V$ , as follows. Let  $X$  be a  $CG$ -module, affording the character  $\xi$ . Then

$$\text{inv}_V X = \{x \in X : vx = x \quad \text{for all } v \in V\}$$

is a  $CH$ -submodule of  $\text{res}_H^G X$ , since  $V \trianglelefteq H$ , and is in fact a  $C(H/V)$ -module, since  $V$  acts trivially on  $\text{inv}_V X$ . We then define  $r_{H/V}^G \xi$  to be the C-character of  $H/V$  afforded by  $\text{inv}_V X$ , and extend by linearity to obtain a  $Z$ -homomorphism  $r_{H/V}^G : \text{ch } G \rightarrow \text{ch } H/V$ .

The operation of *generalized induction*  $i_{H/V}^G : \text{ch } H/V \rightarrow \text{ch } G$  is defined as the composite of the pullback operation  $\lambda \in \text{ch } H/V \rightarrow \tilde{\lambda} \in \text{ch } H$  (via the natural homomorphism  $H \rightarrow H/V$ ), and the induction map  $\text{ind}_H^G$ . Specifically, for  $\lambda \in \text{ch } H/V$ , define

$$i_{H/V}^G \lambda = \text{ind}_H^G \tilde{\lambda} = \tilde{\lambda}^G, \quad \text{where } \tilde{\lambda}(h) = \lambda(\bar{h}), \quad h \in H \rightarrow \bar{h} \in H/V.$$

The following properties of these operations are easily verified:

**(70.1) Proposition.** *Keep the preceding notation, so that  $V \trianglelefteq H \leq G$ . Then the following statements hold.*

(i) For each  $\xi \in \text{ch } G$ , let  $\xi_H = \text{res}_H^G \xi$  and write

$$\xi_H = \xi' + \xi'',$$

where  $\xi'$  is the contribution to  $\xi_H$  from characters  $\lambda \in \text{Irr } H$  whose kernels contain  $V$ , and  $\xi''$  is the contribution from the other characters in  $\text{Irr } H$ . Then  $\xi'$  can be viewed as a virtual character of  $H/V$ , and we have

$$r_{H/V}^G \xi = \xi'.$$

(ii) For all  $\xi \in \text{ch } G$ , we have

$$r_{H/V}^G \xi = \sum_{\lambda \in \text{Irr } H/V} (\xi, i_{H/V}^G \lambda) \lambda,$$

where  $i_{H/V}^G \lambda = \tilde{\lambda}^G$  for  $\lambda \in \text{ch } H/V$ .

(iii) The operations of generalized restriction and induction are adjoint operations with respect to the usual scalar products of characters of  $G$  and  $H/V$ , respectively:

$$(\xi, i_{H/V}^G \lambda)_G = (r_{H/V}^G \xi, \lambda)_{H/V}, \quad \text{for } \xi \in \text{ch } G, \quad \lambda \in \text{ch } H/V.$$

The proof is left as an exercise for the reader.

We next discuss these operations for virtual  $\mathbb{C}$ -characters of a finite group  $G$  with a split  $BN$ -pair of characteristic  $p$ . As usual, let  $W$  denote the Weyl group of  $G$ ,  $S$  the set of distinguished generators of  $W$ , and  $\{B, N\}$  the given  $BN$ -pair in  $G$ , with  $T = B \cap N$ . For each subset  $I \subseteq S$ ,  $P_I$  denotes the standard parabolic subgroup  $BW_I B$ . By (69.14),  $P_I$  has the Levi decomposition

$$(70.2) \quad P_I = L_I \ltimes V_I,$$

where  $V_I = O_p(P_I)$ , and  $L_I$  is the standard Levi factor of  $P_I$  generated by  $T$  and the root subgroups  $\{U_\alpha : \alpha \in \Delta_I\}$ . The parabolic subgroup  $W_I \leq W$  is the Weyl group of  $L_I$ , associated with the  $BN$ -pair  $\{B \cap L_I, N \cap L_I\}$ .

By the preceding discussion, for each  $I \subseteq S$  we have

$$V_I \trianglelefteq P_I \leq G, \quad P_I / V_I \cong L_I,$$

and we can define the operations of generalized restriction and induction from  $\text{ch } G$  to  $\text{ch } L_I$ , using the identification  $P_I / V_I \cong L_I$ .

By (65.20), two standard parabolic subgroups  $P_I$  and  $P_J$  ( $I, J \subseteq S$ ) are never conjugate in  $G$  unless  $I = J$ . On the other hand, standard Levi factors  $L_I$  and  $L_J$  may be conjugate by elements of  $N$  even though  $I \neq J$ ; when this occurs, it may happen that  $i_{P_I/V_I}^G \xi = i_{P_J/V_J}^G \eta$  for characters  $\xi, \eta$  of  $L_I$  and  $L_J$ , respectively. This phenomenon is not accounted for by the usual connection between conjugacy

and induction (see Lemma 10.12). One of the main results of this subsection is a general version of a theorem relating conjugacy of Levi subgroups to generalized induction (see (70.11)). In order to obtain this result, however, we have to consider a wider class of parabolic subgroups.

Throughout the rest of this subsection,  $\mathcal{P}$  denotes the family of all  $N$ -conjugates of the standard parabolic subgroups  $\{P_I : I \subseteq S\}$ . Each subgroup  $P \in \mathcal{P}$  has the form  $P = {}^n P_I$  for some  $n \in N$ , and some uniquely determined standard parabolic subgroup  $P_I$  (by (65.19)). Then  $P$  has a Levi decomposition arising from (70.2), and we have

$$(70.3) \quad P = L \ltimes V, \quad L = {}^n L_I, \quad V = {}^n V_I.$$

Moreover, the subgroups  $L$  and  $V$  depend only on the subgroup  $P \in \mathcal{P}$ , and are independent of the choice of  $n \in N$  such that  $P = {}^n P_I$ , by (65.19), since  $N \cap P_I \leq L_I$ . We shall call  $L$  a *standard Levi subgroup* of  $P$ , and sometimes denote  $L$  and  $V$  by  $L_P$  and  $V_P$ , respectively, noting that  $V_P = O_p(P)$ . We also let  $W_L$  denote the subgroup  $(N \cap P)/T \leq W$ ; then  $W_L$  is the Weyl group of the  $BN$ -pair  $({}^n B \cap L, N \cap L)$  in  $L$ .

Given  $L \leq P$  as in (70.3), similar considerations apply to the parabolic subgroups of  $L$ , using (69.15). The set of parabolic subgroups of  $L$  that plays the role of  $\mathcal{P}$  is given by

$$\mathcal{P}_L = \{Q \cap L : Q \in \mathcal{P} \text{ and } Q \leq P\}.$$

Each parabolic subgroup  $Q$ , such that  $Q \in \mathcal{P}$  and  $Q \leq P$  has a standard Levi decomposition

$$Q = L_Q V_Q, \text{ where } L_Q \leq L \text{ and } V_Q = O_p(Q).$$

By (69.15), the corresponding parabolic subgroup  $Q \cap L$  of  $L$  has the Levi decomposition

$$Q \cap L = L_Q (V_{Q \cap L}),$$

where  $V_{Q \cap L} = O_p(Q \cap L)$ , and  $L_Q$  is the standard Levi subgroup. Moreover, we have, by (69.15),

$$V_Q = V_{Q \cap L} \ltimes V_P,$$

where  $V_P = O_p(P)$ .

**(70.4) Definition.** Let  $P$  be a parabolic subgroup of  $G$  belonging to the family  $\mathcal{P}$ , and let  $P = L \ltimes V$  be its Levi decomposition, as in (70.3). The operation of generalized restriction  $T_{L,P}^G : \mathrm{ch} G \rightarrow \mathrm{ch} L$  is called *truncation*, and is defined by

$$T_{L,P}^G \xi(l) = |V|^{-1} \sum_{v \in V} \xi(lv), \quad \text{for } \xi \in \mathrm{ch} G, \quad l \in L.$$

The operation of *generalized induction*  $R_{L,P}^G : \text{ch } L \rightarrow \text{ch } G$  is defined by

$$R_{L,P}^G \lambda = \text{ind}_P^G \tilde{\lambda} = \tilde{\lambda}^G, \quad \text{for } \lambda \in \text{ch } L,$$

where  $\lambda \rightarrow \tilde{\lambda}$  is the pullback operation from  $\text{ch } L$  to  $\text{ch } P$ , given by

$$\tilde{\lambda}(lv) = \lambda(l) \quad \text{for all } l \in L, \quad v \in V.$$

**(70.5) Remarks.** Later in this subsection we shall prove that the operations  $T_{L,P}^G$  and  $R_{L,P}^G$  depend only on the Levi factor  $L$ , and not on the parabolic subgroups  $P \in \mathcal{P}$  (see (70.10)), justifying the simpler notation  $T_L^G$  and  $R_L^G$ , respectively.

The standard Borel subgroup  $B$  lies in  $\mathcal{P}$ , and has the Levi decomposition  $B = T \ltimes U$ , where  $U = O_p(B)$  and is a Sylow  $p$ -subgroup of  $G$  (by (69.9)). Then  $T$  is an abelian  $p'$ -group, and  $\text{Irr } T$  consists of linear characters. For each  $\lambda \in \text{Irr } T$ , the operation

$$\lambda \rightarrow R_{T,B}^G \lambda = \tilde{\lambda}^G$$

is a special case of the operation  $\theta \rightarrow R_T^G \theta$ , defined by Deligne-Lusztig for each maximal torus  $T$  and character  $\theta \in \text{Irr } T$  (see Deligne-Lusztig [76, Example 1.10]). Note in particular that  $R_{T,B}^G 1_T = (1_B)^G$ , whose decomposition is the main subject of §§67 and 68.

The next result summarizes the basic properties of truncation and generalized induction, including an easy form of the conjugacy result.

**(70.6) Proposition.** (i) Let  $P \in \mathcal{P}$ , and let  $L$  be the standard Levi subgroup of  $P$ . Let  $\xi \in \text{ch } G$  be a character afforded by a  $\mathbb{C}G$ -module  $X$ . Then

$$T_{L,P}^G \xi \text{ is the character of } L \text{ afforded by } \text{inv}_V X \quad \text{where } V = O_p(P), \text{ and}$$

$$T_{L,P}^G \xi = \sum_{\lambda \in \text{Irr } L} (\xi, R_{L,P}^G \lambda) \lambda.$$

(ii) (Adjointness.) For  $P, L$  as above, let  $\xi \in \text{ch } G$ ,  $\eta \in \text{ch } L$ . Then

$$(T_{L,P}^G \xi, \eta)_L = (\xi, R_{L,P}^G \eta)_G.$$

(iii) (Transitivity.) Let  $P \leq Q$ , for parabolic subgroups  $P$  and  $Q$  in  $\mathcal{P}$ , and let  $L, M$  be the standard Levi subgroups of  $P$  and  $Q$ , respectively. Then  $P \cap M$  is a parabolic subgroup of  $M$ ,  $L$  is a standard Levi subgroup of  $P \cap M$ , and we have

$$T_{L,P}^G = T_{L,M \cap P}^M \circ T_{M,Q}^G \quad \text{and} \quad R_{L,P}^G = R_{M,Q}^G \circ R_{L,M \cap P}^M.$$

(iv) (Weak conjugacy.) Let  $P_1, P_2, Q_1, Q_2 \in \mathcal{P}$ , and let  $L_1, L_2, M_1, M_2$  be their standard Levi subgroups. Assume  $P_1 \leq Q_1$ ,  $P_2 \leq Q_2$ ; then  $L_1$  and  $L_2$  are also standard Levi subgroups of  $M_1 \cap P_1$  and  $M_2 \cap P_2$ . Let  $w \in W$  be an element such that  $P_1 = {}^w P_2$ ,  $Q_1 = {}^w Q_2$ ,  $L_1 = {}^w L_2$ ,  $M_1 = {}^w M_2$ . Then  $M_1 \cap P_1 = {}^w(M_2 \cap P_2)$ ,

and we have

$$T_{L_1, M_1 \cap P_1}^{M_1} {}^w\xi = {}^w(T_{L_2, M_2 \cap P_2}^{M_2} \xi)$$

for all virtual characters  $\xi \in \text{ch } M_2$ .

*Proof.* (i) We clearly have

$$e_V X = \text{inv}_V X, \quad \text{where } e_V = |V|^{-1} \sum_{v \in V} v$$

and  $V = O_p(P)$ . If  $l \in L$ , then  $le_V = e_V l$  since  $L$  normalizes  $V$ . Consequently,

$$\xi(e_V l) = \text{Tr}(l, e_V X) = \text{Tr}(l, \text{inv}_V X),$$

since  $e_V$  is an idempotent projection from  $X$  to  $\text{inv}_V X$ . We also have  $T_{L, P}^G \xi(l) = \xi(e_V l)$  by Definition 70.4, completing the proof of the first statement. The second statement follows from (70.1). Part (ii) follows for characters  $\xi$  of  $G$  and  $\eta \in \text{Irr } L$  by the second statement in part (i), and extends to virtual characters by linearity.

For the proof of (iii), it is sufficient to derive either one of the transitivity formulas, since the other will follow by adjointness. By the preceding discussion, we have

$$V_P = (V_P \cap M) \ltimes V_Q, \quad \text{and} \quad M \cap P = L \ltimes (V_P \cap M),$$

where  $V_P = O_p(P)$  and  $V_Q = O_p(Q)$ . Transitivity of the truncation operation follows at once from these remarks and Definition 70.4.

(iv) The assumptions imply that  $O_p(M_1 \cap P_1) = {}^w O_p(M_2 \cap P_2)$ , and the result follows from Definition 70.4.

We next obtain a version of Mackey's Intertwining Number Theorem 10.24 for generalized induction. The result is proved first for standard parabolic subgroups, and then for parabolic subgroups in  $\mathcal{P}$ .

**(70.7) Proposition.** *Let  $I, J \subseteq S$ , and let  $D_{IJ}$  denote the distinguished cross section of  $W_I \backslash W / W_J$ . Let  $\lambda \in \text{ch } L_I$ ,  $\mu \in \text{ch } L_J$ . Then*

$$(R_{L_I, P_I}^G \lambda, R_{L_J, P_J}^G \mu) = \sum_{x \in D_{IJ}} (T_{L_I, P_K \cap L_I}^{L_I} \lambda, {}^x T_{L_{K'}, P_{K'} \cap L_J}^{L_J} \mu)_{L_K},$$

where for a fixed  $x \in D_{IJ}$ , the subsets  $K$  and  $K'$  of  $S$  are defined by

$$K = I \cap {}^x J, \quad K' = {}^{x^{-1}} K,$$

and we have  $L_K = {}^x L_{K'}$ .

*Proof.* The subset of  $N$  consisting of coset representatives  $\{\dot{x}: x \in D_{IJ}\}$  forms a cross section of  $P_I \backslash G / P_J$ . (To simplify notation in what follows, we shall often write  $x$  instead of  $\dot{x}$ , for  $x \in D_{IJ}$ .) By Theorem 10.24 and the definition,

$$(R_{L_I, P_I}^G \lambda, R_{L_J, P_J}^G \mu) = \sum_{x \in D_{IJ}} (\tilde{\lambda}|_{P_I \cap {}^x P_J}, {}^x \tilde{\mu}|_{P_I \cap {}^x P_J})_{P_J \cap {}^x P_J},$$

where  $\tilde{\lambda}$  and  $\tilde{\mu}$  denote the pullbacks of  $\lambda$  and  $\mu$  to  $P_I$  and  $P_J$ , respectively. We now calculate the scalar products on the right-hand side. Let  $x$  be a fixed element of  $D_{IJ}$ , and let

$$K = I \cap {}^x J \subseteq I, \quad K' = {}^{x^{-1}} K \subseteq J,$$

as in the statement above. Since  $K = {}^x K'$ ,  $\Delta_K = x \cdot \Delta_{K'}$ , it follows from the definition of the standard Levi subgroups  $L_K$  and  $L_{K'}$  that  $L_K = {}^x L_{K'}$  (see (69.10)). By Theorem 69.16v, there is a factorization

$$P_I \cap {}^x P_J = L_K (L_I \cap {}^x V_J) (V_I \cap {}^x L_J) (V_I \cap {}^x V_J),$$

with uniqueness of expression. Note that by §64C,  $x^{-1} \in D_{JI}$  and  $K' = J \cap {}^{x^{-1}} I$ , so that (69.16) can be applied to the terms  $L_I \cap {}^x V_J$ , and also to  $V_I \cap {}^x L_J = {}^{x^{-1}} (V_I \cap L_J)$ , in the factorization of  $P_I \cap {}^x P_J$ . This gives (for  $V_{IK} = O_p(P_K \cap L_I)$  etc.),

$$(70.8) \quad L_I \cap {}^x V_J = V_{IK} = L_I \cap V_K \quad \text{and} \quad V_I \cap {}^x L_J = {}^x V_{J,K'} = {}^x (L_J \cap V_{K'}),$$

by (69.16iv). We then obtain, for the scalar product corresponding to  $x \in D_{IJ}$ ,

$$\begin{aligned} & (\tilde{\lambda}|_{P_I \cap {}^x P_J}, {}^x \tilde{\mu}|_{P_I \cap {}^x P_J})_{P_J \cap {}^x P_J} \\ &= |P_I \cap {}^x P_J|^{-1} \sum_{l,v,y,z} \tilde{\lambda}(lv^x(y)z) \overline{{}^x \tilde{\mu}(lv^x(y)z)}, \end{aligned}$$

where  $l \in L_K$ ,  $v \in V_{IK}$ ,  $y \in V_{JK'}$ ,  $z \in V_I \cap {}^x V_J$ . In order to simplify this expression, we first note that since  $L_I$  normalizes  $V_I$  and  $L_J$  normalizes  $V_J$ , we have

$$(u, u') \in V_I \cap {}^x V_J$$

for all commutators  $(u, u') = uu'u^{-1}(u')^{-1}$ , with  $u \in V_{IK} = L_I \cap {}^x V_J$ ,  $u' \in {}^x V_{JK'} = V_I \cap {}^x L_J$  (by (70.8)). Then, for each element of  $P_I \cap {}^x P_J$  in factored form, as above, we have

$$lv^x(y)z \equiv lv \pmod{V_I} \quad \text{and} \quad lv^x(y)z \equiv l^x(y) \pmod{{}^x V_J}.$$

Therefore, by the definitions of  $\tilde{\lambda}$  and  $\tilde{\mu}$ , we obtain

$$\tilde{\lambda}(lv^x(y)z) = \lambda(lv) \quad \text{and} \quad {}^x \tilde{\mu}(lv^x(y)z) = {}^x \mu(l^x(y)).$$

By the uniqueness of factorization of elements of  $P_I \cap {}^x P_J$ , it follows that the

scalar product becomes

$$|L_K|^{-1} |V_{IK}|^{-1} |V_{JK'}|^{-1} \sum_{l,v,y} \lambda(lv) {}^x\mu(l{}^x(y)),$$

with  $l, v, y$  as above. Finally, using the definition of truncation (70.4), and the facts that  $V_{IK} = O_p(P_K \cap L_I)$  and  $V_{JK'} = O_p(P_{K'} \cap L_J)$  by (69.16iv), we have

$$|V_{IK}|^{-1} \sum_v \lambda(lv) = T_{L_K, P_K \cap L_I}^{L_I} \lambda(l)$$

and

$$|V_{JK'}|^{-1} \sum_y {}^x\mu(l{}^x(y)) = {}^x T_{L_{K'}, P_{K'} \cap L_J}^{L_J} \mu(l).$$

Then the scalar product corresponding to  $x \in D_{IJ}$  becomes

$$(T_{L_K, P_K \cap L_I}^{L_I} \lambda, {}^x T_{L_{K'}, P_{K'} \cap L_J}^{L_J} \mu)_{L_K},$$

since  ${}^x L_{K'} = L_K$ , and the proof is completed.

It is now straightforward to extend the preceding result to parabolic subgroups in the family  $\mathcal{P}$ .

**(70.9) Theorem.** *Let  $P$  and  $Q$  be parabolic subgroups in  $\mathcal{P}$ , with standard Levi subgroups  $L$  and  $M$ , respectively. Let  $W_L, W_M$  be the Weyl groups of  $L$  and  $M$ , and let  $D$  be an arbitrary cross section of  $W_L \backslash W / W_M$ . For each  $w \in D$ ,  $L \cap {}^w Q$  is a parabolic subgroup of  $L$ ,  ${}^{w^{-1}} P \cap M$  is a parabolic subgroup of  $M$ , and  $L \cap {}^w M$ ,  ${}^{w^{-1}} L \cap M$  are standard Levi subgroups of  $L \cap {}^w Q$  and  ${}^{w^{-1}} P \cap M$ , respectively. Let  $\xi \in \text{ch } L$  and  $\eta \in \text{ch } M$ . Then*

$$(R_{L,P}^G \xi, R_{M,Q}^G \eta) = \sum_{w \in D} (T_{L \cap {}^w M, L \cap {}^w Q}^L \xi, {}^w T_{w^{-1} L \cap M, w^{-1} P \cap M}^{M_{-1}} \eta)_{L \cap {}^w M}.$$

*Proof.* We may assume that for some elements  $r, s \in W$ , and some uniquely determined subsets  $I, J \subseteq S$ , we have

$$P = {}^r P_I, L = {}^r L_I, W_L = {}^r W_I, \quad \text{and} \quad Q = {}^s P_J, M = {}^s L_J, W_M = {}^s W_J.$$

Then

$$W = \bigcup_{w \in D} W_L w W_M = \bigcup_{w \in D} W_I r^{-1} w s W_J,$$

so  $r^{-1} D s$  is a cross section of  $W_I \backslash W / W_J$ . It follows that  $D$  is a cross section of  $P \backslash G / Q$ , by (65.21). By Theorem 10.24 we have

$$(R_{L,P}^G \xi, R_{M,Q}^G \eta)_G = \sum_{w \in D} (\tilde{\xi}|_{P \cap {}^w Q}, {}^w \tilde{\eta}|_{P \cap {}^w Q})_{P \cap {}^w Q},$$

where  $\tilde{\xi}$  and  $\tilde{\eta}$  denote the pullbacks of  $\xi$  and  $\eta$  to  $P$  and  $Q$ , respectively.

Now let  $w$  be a fixed element of  $D$ . Then

$$W_L w W_M = r W_I r^{-1} w s W_J s^{-1}.$$

Replacing  $s$  by  $ss_1$  for some  $s_1 \in W_J$ , and  $r$  by  $rr_1$  for some  $r_1 \in W_I$ , we may assume that the same conjugacy relations

$$P = {}^r P_I, \quad L = {}^r L_I, \quad Q = {}^s P_J, \quad M = {}^s L_J,$$

hold and that  $r^{-1} w s = z \in D_{IJ}$ . Then the scalar product corresponding to  $w$  becomes

$$(\tilde{\xi}|_{P \cap {}^w Q}, {}^w \tilde{\eta}|_{P \cap {}^w Q})_{P \cap {}^w Q} = ({}^{r^{-1}} \tilde{\xi}|_{P_I \cap {}^z P_J}, {}^z ({}^{s^{-1}} \tilde{\eta}|_{P_I \cap {}^z P_J}))_{P_I \cap {}^z P_J}$$

by the definition of conjugate characters. Since  $z = r^{-1} w s \in D_{IJ}$ , we may apply the proof of (70.7) to the right-hand side, to obtain

$$(T_{L_K, P_K \cap L_I}^{L_I} {}^{r^{-1}} \xi, {}^z T_{L_{K'}, P_{K'} \cap L_J}^{L_J} {}^{s^{-1}} \eta)_{L_K},$$

where  $K = I \cap {}^z J$ ,  $K' = {}^{z^{-1}} I \cap J$ , and

$$L_K = L_I \cap {}^z L_J = {}^{r^{-1}} (L \cap {}^w M), \quad L_{K'} = {}^{s^{-1}} ({}^{w^{-1}} L \cap M),$$

by (69.16ii). Applying the weak conjugacy formula for truncation (70.6iv), we obtain

$$T_{L_K, P_K \cap L_I}^{L_I} {}^{r^{-1}} \xi = {}^{r^{-1}} (T_{L \cap {}^w M, L \cap {}^w Q}^L \xi)$$

and

$${}^z T_{L_{K'}, P_{K'} \cap L_J}^{L_J} {}^{s^{-1}} \eta = {}^{r^{-1} w} T_{w^{-1} L \cap M, w^{-1} P \cap M}^M \eta.$$

Their scalar product on  $L_K$  becomes

$$\begin{aligned} & ({}^{r^{-1}} T_{L \cap {}^w M, L \cap {}^w Q}^L \xi, {}^{r^{-1} w} T_{w^{-1} L \cap M, w^{-1} P \cap M}^M \eta)_{L_K} \\ &= (T_{L \cap {}^w M, L \cap {}^w Q}^L \xi, {}^w T_{w^{-1} L \cap M, w^{-1} P \cap M}^M \eta)_{L \cap {}^w M}, \end{aligned}$$

since  $L_K = {}^{r^{-1}} (L \cap {}^w M)$ . This completes the proof of the theorem.

We now prove that the operations of truncation  $T_{L,P}^G$  and generalized induction  $R_{L,P}^G$  are independent of the parabolic subgroup  $P \in \mathcal{P}$  containing a given Levi subgroup  $L$ . This result, and the conjugacy result following from it, are basic for the analysis of cuspidal characters in §70B. For standard parabolic subgroups, the result is due to Curtis [80], Alvis [80], Kawanaka [82], and Deligne (see Lusztig-Spaltenstein [79]). The proof to follow is an elementary version of an argument due to Deligne.

**(70.10) Theorem** *Let  $P$  and  $Q$  be parabolic subgroups in  $\mathcal{P}$  having a common*

standard Levi subgroup  $L$ . Then

$$R_{L,P}^G \lambda = R_{L,Q}^G \lambda \quad \text{and} \quad T_{L,P}^G \xi = T_{L,Q}^G \xi$$

for all virtual characters  $\lambda \in \text{ch } L$  and  $\xi \in \text{ch } G$ , respectively.

*Proof.* The theorem clearly holds in case the Weyl group of  $G$  is trivial, that is, the rank of the  $BN$ -pair in  $G$  is zero. Thus we may assume  $L \neq G$ , and that the Theorem holds for groups of smaller  $BN$ -rank than  $G$ . By the adjointness property (70.6ii), it is sufficient to prove the theorem for the operation of generalized induction, and we may assume, from the induction hypothesis, that the theorem holds for  $L$  and parabolic subgroups in  $\mathcal{P}_L$ . Let  $\lambda \in \text{ch } L$ , and let  $D$  be a fixed cross section of  $W_L \backslash W / W_L$ . From three applications of Theorem 70.9, we have

$$\begin{aligned} (R_{L,P}^G \lambda, R_{L,P}^G \lambda) &= \sum_{w \in D} (T_{L \cap {}^w L, L \cap {}^w P}^L \lambda, {}^w T_{w^{-1} L \cap L, w^{-1} P \cap L'}^L \lambda)_{L \cap {}^w L}, \\ (R_{L,P}^G \lambda, R_{L,Q}^G \lambda) &= \sum_{w \in D} (T_{L \cap {}^w L, L \cap {}^w Q}^L \lambda, {}^w T_{w^{-1} L \cap L, w^{-1} Q \cap L'}^L \lambda)_{L \cap {}^w L}, \end{aligned}$$

and

$$(R_{L,Q}^G \lambda, R_{L,Q}^G \lambda) = \sum_{w \in D} (T_{L \cap {}^w L, L \cap {}^w Q}^L \lambda, {}^w T_{w^{-1} L \cap L, w^{-1} Q \cap L'}^L \lambda)_{L \cap {}^w L},$$

By the induction hypothesis, the three expressions on the right-hand side coincide. It follows that

$$(R_{L,P}^G \lambda - R_{L,Q}^G \lambda, R_{L,P}^G \lambda - R_{L,Q}^G \lambda) = 0,$$

and hence  $R_{L,P}^G \lambda = R_{L,Q}^G \lambda$ , as required.

As a corollary we obtain:

**(70.11) Strong Conjugacy Theorem.** *Let  $I, J \subseteq S$ , and assume that  $L_I = {}^x L_J$  for some  $x \in W$ , where  $L_I$  and  $L_J$  are the standard parabolic subgroups of  $P_I$  and  $P_J$ , respectively. Let  $\psi \in \text{ch } L_J$  and let  $\varphi = {}^x \psi \in \text{ch } L_I$ . Then*

$$R_{L_I, P_I}^G \varphi = R_{L_J, P_J}^G \psi.$$

*Proof.* Since  ${}^x P_J$  and  $P_I$  are in  $\mathcal{P}$  and both have the same standard parabolic subgroup  $L_I$ , we have

$$R_{L_I, P_I}^G \varphi = R_{L_I, {}^x P_J}^G \varphi$$

by Theorem 70.10. Since  $\varphi = {}^x \psi$  and  $L_I = {}^x L_J$ , we then obtain

$$R_{L_I, {}^x P_J}^G \varphi = R_{L_J, {}^x P_J}^G {}^x \psi = R_{L_J, P_J}^G \psi$$

by the usual conjugacy theorem for induced characters (10.12), since the pullback of  ${}^x\psi$  to  ${}^xP_J$  clearly coincides with the conjugate  ${}^x\tilde{\psi}$  of the pullback  $\tilde{\psi}$  of  $\psi$  to  $P_J$ . This completes the proof.

**Remark.** As an illustration of Theorem 70.11, let  $P_I$  and  $P_J$  be standard parabolic subgroups such that  $I \neq J$ , but  $L_I = {}^xL_J$  for some  $x \in W$ . Then  $P_I$  and  $P_J$  are not conjugate in  $G$ , by (65.19). Nevertheless, we have  $(1_{P_I})^G = (1_{P_J})^G$  by (70.11), since  $(1_{P_I})^G = R_{L_I, P_I}^G 1_{L_I}$  and  $(1_{P_J})^G = R_{L_J, P_J}^G 1_{L_J}$ . For a particular case of this phenomenon, see Exercise 10.4. This raises the interesting problem of classification of transitive permutation representations of a finite group  $G$ , and shows that it involves more than the question of conjugacy of subgroups stabilizing points.

## §70B. The Philosophy of Cusp Forms

Throughout this subsection,  $G$  denotes a finite group with a split  $BN$ -pair of characteristic  $p$ ,  $W$  the Weyl group of  $G$ , and  $S$  the set of distinguished generators of  $W$ . For each subset  $I \subseteq S$ ,  $P_I$  denotes the standard parabolic subgroup, and  $L_I$  the standard Levi subgroup, both associated with the parabolic subgroup  $W_I$  of  $W$ . As in §70A,  $\mathcal{P}$  denotes the family of all  $N$ -conjugates of the standard parabolic subgroups. For each parabolic subgroup  $P \in \mathcal{P}$  with standard Levi subgroup  $L$ , we let

$$T_L^G : \text{ch } G \rightarrow \text{ch } L \quad \text{and} \quad R_L^G : \text{ch } L \rightarrow \text{ch } G$$

denote the operations of truncation and generalized induction. Thus,  $T_L^G = T_{L,P}^G$  and  $R_L^G = R_{L,P}^G$  in the notation of Definition 70.4. The simplified notation is justified by (70.10), where we proved that

$$T_{L,P}^G = T_{L,Q}^G \quad \text{and} \quad R_{L,P}^G = R_{L,Q}^G$$

for any two parabolic subgroups  $P$  and  $Q$  in  $\mathcal{P}$  having the same standard Levi subgroup.

**(70.12) Definition.** A virtual character  $\zeta \in \text{ch } G$  is called *cuspidal* if  $T_{L_I}^G \zeta = 0$  for all Levi subgroups  $L_I$  of proper parabolic subgroups  $P_I$ ,  $I \subset S$ . A left  $CG$ -module  $M$  is called *cuspidal* if  $\text{inv}_{V_I} M = 0$  for all proper subsets  $I \subset S$ , where  $V_I = O_P(P_I)$ . In case  $G$  is an abelian  $p'$ -group (so that  $S = \emptyset$ ), all virtual characters  $\zeta \in \text{ch } G$  and all  $CG$ -modules are said to be cuspidal.

It follows from (70.6i) that a left  $CG$ -module  $M$  is cuspidal if and only if its character is cuspidal.

**(70.13) Proposition.** *For  $\zeta \in \text{ch } G$ , the following statements are equivalent:*

- (i)  $\zeta$  is cuspidal.

(ii) For all proper subsets  $I \subset S$  and elements  $x \in L_I$ ,

$$|V_I|^{-1} \sum_{v \in V_I} \zeta(xv) = 0,$$

where  $V_I = O_p(P_I)$ .

(iii)  $(\zeta, (1_{V_I})^G) = 0$  for all proper subsets  $I \subset S$ .

(iv)  $(\zeta, R_L^G \lambda) = 0$  for all standard Levi subgroups  $L$  of proper parabolic subgroups  $P \in \mathcal{P}$ ,  $P \neq G$ , and all virtual characters  $\lambda \in \text{ch } L$ .

The proof is immediate from the results of §70A, and is left as an exercise for the reader.

**Remarks.** The concept of cuspidal representations and characters is due to Harish-Chandra [70], who had already used the same concept in the representation theory of reductive Lie groups, and reductive algebraic groups over local fields. In the case of finite groups of Lie type, the significance of the concept is clear from Proposition 70.13. For such a group, we might hope to calculate  $\text{Irr } L_I$  for proper subsets  $I \subset S$ , and then to decompose the induced characters  $R_L^G \lambda$  for  $\lambda \in \text{Irr } L_I$ ,  $I \subset S$ . The cuspidal characters  $\zeta \in \text{Irr } G$ , if any exist, are precisely the characters of  $G$  that are missed by this procedure (see (70.13iv)). The main point of this subsection is that not only do cuspidal characters exist, but in a certain precise sense, they control the character theory of  $G$ . This is Harish-Chandra's philosophy of cusp forms.

Other expositions of Harish-Chandra's work have been given by Springer [75] and, in the present context, by Curtis [75].

**(70.14) Proposition.** Let  $\zeta \in \text{Irr } G$ . Then either  $\zeta$  is cuspidal, or else there exists a proper subset  $I \subset S$  and a cuspidal character  $\lambda \in \text{Irr } L_I$ , such that  $(\zeta, R_{L_I}^G \lambda) \neq 0$ .

*Proof.* If  $\zeta$  is not cuspidal, then  $S \neq \emptyset$  and  $T_{L_I}^G \zeta \neq 0$  for some proper subset  $I \subset S$ . Let  $I$  be a minimal subset of  $S$  such that  $T_{L_I}^G \zeta \neq 0$ . Then by (70.6i) we have

$$T_{L_I}^G \zeta = \sum_{\lambda \in \text{Irr } L_I} (\zeta, R_{L_I}^G \lambda) \lambda,$$

with at least one multiplicity  $(\zeta, R_{L_I}^G \lambda) \neq 0$ . Using the minimality of  $I$ , we shall prove that all characters  $\lambda \in \text{Irr } L_I$  such that  $(\zeta, R_{L_I}^G \lambda) \neq 0$  are cuspidal.

Let  $\lambda \in \text{Irr } L_I$  be such a character, and assume it fails to be cuspidal. Then for some proper subset  $K \subset I$  we have  $T_{L_K}^{L_I} \lambda \neq 0$ . By transitivity of truncation (see (70.6iii)), we obtain

$$T_{L_K}^G \zeta = T_{L_K}^{L_I} T_{L_I}^G \zeta = \sum_{\lambda \in \text{Irr } L_I} (\zeta, R_{L_I}^G \lambda) T_{L_K}^{L_I} \lambda \neq 0,$$

since the multiplicities are nonnegative and  $T_{L_K}^{L_I} \lambda \neq 0$  for at least one  $\lambda$  such that

$(\zeta, R_{L_I}^G \lambda) \neq 0$ . This contradicts the assumption that  $I$  is a minimal subset such that  $T_{L_I}^G \zeta \neq 0$ , and finishes the proof.

The main result of this subsection is the following version in two parts, A, B, of a theorem of Harish-Chandra [70], formulated as in Springer [75].

**(70.15A) Theorem.** *Let  $I, J \subseteq S$ , and let  $\varphi$  and  $\psi$  be irreducible cuspidal characters of  $L_I$  and  $L_J$ , respectively. Then we have:*

- (i)  $(R_{L_I}^G \varphi, R_{L_J}^G \psi) = 0$  unless there exists  $x \in W$  such that  $L_I = {}^x L_J$  and  $\varphi = {}^x \psi$ .
- (ii) In case  $(R_{L_I}^G \varphi, R_{L_J}^G \psi) \neq 0$ , we have  $R_{L_I}^G \varphi = R_{L_J}^G \psi$ .

Part B of Theorem 70.15 gives a formula for  $(R_{L_I}^G \varphi, R_{L_I}^G \varphi)$ , for  $\varphi$  cuspidal in  $\text{Irr } L_I$ , in terms of the Weyl group of  $G$ . We first require some definitions.

Let  $N_W(L_I) = \{w \in W : {}^w L_I = L_I\}$ , for a fixed subset  $I \subseteq S$ . Then  $W_I \trianglelefteq N_W(L_I)$ , and the factor group  $N_W(L_I)/W_I$  acts by conjugation on  $\text{Irr } L_I$ , according to the rule

$${}^{\bar{t}} \lambda = i\lambda, \quad \text{for } \bar{t} = iW_I \in N_W(L_I)/W_I.$$

For each  $\lambda \in \text{Irr } L_I$ , let  $S_\lambda$  denote the stabilizer in  $N_W(L_I)/W_I$  of  $\lambda$ , that is,

$$S_\lambda = \{\bar{t} \in N_W(L_I)/W_I : {}^{\bar{t}} \lambda = \lambda\}.$$

**(70.15B) Theorem.** *Let  $\varphi$  be an irreducible cuspidal character of  $L_I$ , for some  $I \subseteq S$ . Then*

$$(R_{L_I}^G \varphi, R_{L_I}^G \varphi) = |S_\varphi|,$$

where  $S_\varphi$  is the stabilizer of  $\varphi$  in  $N_W(L_I)/W_I$ .

*Proof of (70.15A).* By Proposition 70.7, we have

$$(R_{L_I}^G \varphi, R_{L_J}^G \psi) = \sum_{x \in D_{IJ}} (T_{L_K}^{L_I} \varphi, {}^x T_{L_K}^{L_J} \psi)_{L_K},$$

where for a fixed  $x \in D_{IJ}$ ,  $K = I \cap {}^x J$  and  $K' = {}^{x^{-1}} K$ . Since  $\varphi$  and  $\psi$  are cuspidal characters of  $L_I$  and  $L_J$ , respectively, at least one of the truncations  $T_{L_K}^{L_I} \varphi$  or  $T_{L_K}^{L_J} \psi$  is zero (in the summand corresponding to  $x \in D_{IJ}$ ), unless both  $K = I$  and  $K' = J$ . The latter is clearly equivalent to  $I = {}^x J$ , and this implies  $L_I = {}^x L_J$ , by (64.41) and the definition of the standard Levi subgroups  $L_I$  and  $L_J$  (see (69.10)). The intertwining number thus becomes

$$(70.16) \quad (R_{L_I}^G \varphi, R_{L_J}^G \psi) = \sum (\varphi, {}^x \psi)_{L_I},$$

where the sum is taken over all  $x \in D_{IJ}$  such that  $L_I = {}^x L_J$ . It follows that  $(R_{L_I}^G \varphi, R_{L_J}^G \psi) = 0$  unless  $L_I = {}^x L_J$  and  $\varphi = {}^x \psi$  for some  $x \in D_{IJ}$ , since both  $\varphi$  and  $\psi$

are irreducible characters. If these conditions hold, for some  $x \in D_{IJ}$ , then  $R_{L_I}^G \varphi = R_{L_J}^G \psi$  by the Strong Conjugacy Theorem 70.11, completing the proof of both parts of (70.15A).

*Proof of (70.15B).* Since  $\varphi$  is cuspidal and irreducible, we can apply the proof of (70.15A), in particular (70.16), to obtain

$$(R_{L_I}^G \varphi, R_{L_I}^G \varphi) = \sum (\varphi, {}^x \varphi)_{L_I},$$

where the sum is taken over all  $x \in D_{II}$  such that  ${}^x L_I = L_I$  and  ${}^x \varphi = \varphi$ . The elements  $x \in D_{II}$  with the property that  ${}^x L_I = L_I$  clearly form a cross section of  $N_W(L_I)/W_I$ , and those that also satisfy the condition  ${}^x \varphi = \varphi$  are in bijective correspondence with the elements of  $S_\varphi$ . Since the corresponding scalar products  $(\varphi, {}^x \varphi)$  are all 1, for  $x W_I \in S_\varphi$ , we obtain

$$(R_{L_I}^G \varphi, R_{L_I}^G \varphi) = |S_\varphi|,$$

as required.

**(70.17) Remarks.** (i) In view of Theorems 70.15A and B, the calculation of  $\text{Irr } G$ , for a finite group of Lie type  $G$ , is equivalent to the solution of the following problems:

**Problem I.** Find all irreducible cuspidal characters for each finite group of Lie type.

**Problem II. (The Decomposition Problem.)** For each subset  $I \subset S$ , and each irreducible cuspidal character  $\varphi$  of  $L_I$ , find the characters in  $\text{Irr } G$  which appear with positive multiplicity in  $R_{L_I}^G \varphi$ .

(ii) By Theorem 70.15B, it follows that

$$(R_{L_I}^G \varphi, R_{L_I}^G \varphi) \leq |W|$$

for each  $I \subseteq S$  and each cuspidal character  $\varphi \in \text{Irr } L_I$ . We also recall that, by Definition 70.12, the trivial character  $1_T$  (and all other irreducible characters of  $T$ ) are cuspidal characters of  $T = B \cap N$ . Then  $R_T^G 1_T = (1_B)^G$ , and

$$(R_T^G 1_T, R_T^G 1_T) = ((1_B)^G, (1_B)^G) = |B \setminus G/B| = |W|$$

by the Bruhat decomposition (65.4). Thus the decomposition problem for the permutation character  $(1_B)^G$ , discussed in §§67 and 68, is an extreme case of Problem II. It has been shown that the methods used to decompose  $(1_B)^G$ , suitably extended, also yield crucial information about multiplicities, generic degrees, etc., in the general case of Problem II (see Howlett-Lehrer [80], Lusztig [84, Chapter 8], Carter [85, Chapter 10]).

**(70.18) Examples.** Let  $G$  be the simple group  $PSL_2(\mathbb{F}_5)$  of order 60; then

$G \cong A_5 \cong SL_2(\mathbb{F}_4)$ . The characters of  $G$  were calculated in §14D. These characters can also be found using the philosophy of cusp forms, as follows. Let  $B$  be the Borel subgroup of  $PSL_2(\mathbb{F}_5)$ , and let  $B = U \rtimes T$ . Then  $|B| = 10$ ,  $|U| = 5$ , and  $|T| = 2$ . In this case  $B$  is the only proper standard parabolic subgroup, and  $U = O_p(B)$ . We have

$$(1_U)^B = 1_B + \varepsilon_B, \quad \text{and} \quad (1_U)^G = (1_B)^G + (\varepsilon_B)^G,$$

where  $\varepsilon_B$  is the pullback (to  $B$ ) of the nontrivial character of  $T$ . Since both  $1_B$  and  $\varepsilon_B$  are cuspidal characters of  $T$ , we obtain

$$((1_B)^G, (\varepsilon_B)^G) = 0 \quad \text{and} \quad ((1_B)^G, (1_B)^G) = ((\varepsilon_B)^G, (\varepsilon_B)^G) = 2.$$

Moreover,  $(1_B)^G = 1_G + St_G$ , where  $St_G$  is the Steinberg character of degree 5, and  $(\varepsilon_B)^G = \zeta_1 + \zeta_2$ , where  $\zeta_1$  and  $\zeta_2$  are irreducible characters of degree 3, as is easily shown using the facts that  $\deg(\varepsilon_B)^G = 6$  and that the degrees of its two components divide  $|G| = 60$ . Thus the solution of Problem II yields the irreducible components of  $(1_U)^G$ , of degrees 1, 5, 3, 3. Using the isomorphism  $G \cong SL_2(\mathbb{F}_4)$ , we also obtain an irreducible character of degree 4, the Steinberg character of  $G$  in its realization as a group of Lie type in characteristic 2. This character does not appear in  $(1_U)^G$ , and, by Proposition 70.13, is the unique cuspidal character of  $PSL_2(\mathbb{F}_5)$ . Adding the squares of the degrees of the characters obtained so far, we see that we have found all irreducible characters of  $G$ .

(ii) Let  $G$  be the simple group  $PSL_2(\mathbb{F}_p)$ , with  $p$  an odd prime and  $p \geq 5$ . Then  $G$  has a cyclic self-centralizing Sylow  $p$ -subgroup which is a T.I. set, so the characters of  $G$  can be determined by the methods of §20B. We have

$$\text{Irr } G = \{1, \zeta_1, \dots, \zeta_n, \theta_1, \dots, \theta_f, \chi_1, \dots, \chi_h\},$$

in the notation of §20B. The numbers  $n, f, h$  are given by

$$n = 2, \quad f = e - 1 = \frac{1}{2}(p - 3) \quad \text{and} \quad h = 1.$$

The following statements about  $\text{Irr } G$  are left as exercises for the reader. We have

$$\zeta_i(1) = \frac{1}{2}(p \pm 1), \quad \theta_j(1) = p \pm 1, \quad \text{and} \quad \chi_1(1) = p,$$

for  $i = 1, 2, j = 1, \dots, e - 1$ . Moreover,

$$\zeta_i(1) = \begin{cases} \frac{1}{2}(p + 1) & \text{if } p \equiv 1 \pmod{4}, \\ \frac{1}{2}(p - 1) & \text{if } p \equiv -1 \pmod{4}, \end{cases}$$

while both possibilities for  $\theta_j(1)$  usually occur. The group  $G$  has a split  $BN$ -pair of characteristic  $p$ , with Weyl group  $W$  of order 2, by §64B. We have  $\chi_1 = St_G$ , and the remaining characters either are cuspidal or are components

of  $(1_U)^G$ . Those of degree  $p - 1$  and  $\frac{1}{2}(p - 1)$  (if they occur) are cuspidal, while those of degree  $p + 1$  and  $\frac{1}{2}(p + 1)$  (if they occur) are components of  $(1_U)^G$  (along with  $1_G$  and  $\text{St}_G$ ).

### §70C. Formulas for Character Values

In addition to providing an organization of  $\text{Irr } G$  for a finite group of Lie type  $G$ , the methods of §§70A, B also yield explicit information about values of irreducible characters of  $G$ . We shall give illustrations of these ideas, after some preliminary remarks. Let us keep the notation introduced at the beginning of §70B.

**(70.19) Definition.** Two standard parabolic subgroups  $P_I, P_J$ , for  $I, J \subseteq S$ , are said to be *associated* (notation:  $P_I \sim P_J$ ) whenever their standard Levi subgroups  $L_I$  and  $L_J$  are conjugate by an element of  $N$ , that is,  $L_I = {}^x L_J$ , for some  $x \in W$ .

**(70.20) Proposition.** *The relation  $\sim$  extends to an equivalence relation on the family of all parabolic subgroups of  $G$ . Thus  $P \sim Q$  if and only if  $P = {}_G P_I, Q = {}_G P_J$ , and  $P_I \sim P_J$ . We also have, for  $I, J \subseteq S$ ,*

$$P_I \sim P_J \text{ if and only if } W_I = {}_W W_J.$$

The proof of the first statement is immediate, using the fact that by (65.20), each parabolic subgroup is  $G$ -conjugate to a unique standard parabolic subgroup. For the second statement, see Exercise 1.

The equivalence classes arising from the relation  $\sim$  are called *association classes*, and are denoted by  $\{\mathcal{A}_I : I \subseteq S\}$ . Then, for  $I \subseteq S$ ,

$$\mathcal{A}_I = \{P \leq G : P \text{ parabolic, and } P \sim P_I\}.$$

By Theorem 70.15A, we have a corresponding partition of the irreducible characters of  $G$ :

$$\text{Irr } G = \bigcup_{I \subseteq S} \mathcal{E}_I,$$

where

$$(70.21) \quad \mathcal{E}_I = \{\zeta \in \text{Irr } G : (\zeta, R_{L_I}^G \varphi) \neq 0 \text{ for } \varphi \text{ cuspidal in } \text{Irr } L_I\}.$$

We note that  $\mathcal{E}_I = \mathcal{E}_J$  if  $P_I \sim P_J$ , and  $\mathcal{E}_I \cap \mathcal{E}_J = \emptyset$  if  $P_I \not\sim P_J$ , for  $I, J \subseteq S$ . The characters in  $\mathcal{E}_S$  are the cuspidal characters of  $G$ , while at the other extreme, the characters in  $\mathcal{E}_{\emptyset}$  are the irreducible components of characters of the form

$$R_T^G \lambda = \text{ind}_B^G \tilde{\lambda},$$

where  $\lambda$  is a linear character of the standard torus  $T = B \cap N$ , and  $\tilde{\lambda}$  denotes its pullback (or lift) to  $B$ .

The characters in  $\mathcal{E}_S$  are sometimes called the *discrete series* of  $G$ , while those in  $\mathcal{E}_{\emptyset}$  are said to belong to the *principal series*, by analogy with the representation theory of semisimple Lie groups. In particular, the characters in  $(1_B)^G$  all belong to the principal series. For the construction of the characters in the discrete series  $\mathcal{E}_S$ , see Deligne-Lusztig [76], Srinivasan [79], and Carter [85].

The above considerations of course apply to the irreducible characters of standard Levi subgroups  $L_I$ , for  $I \subseteq S$ . Thus for  $J \subseteq I$ , we set

$$\mathcal{E}_J(L_I) = \{\lambda \in \text{Irr } L_I : (\lambda, R_{L_J}^{L_I} \mu)_{L_I} \neq 0, \text{ for } \mu \text{ cuspidal in } \text{Irr } L_J\}.$$

We clearly have

$$\mathcal{E}_{J_1}(L_I) = \mathcal{E}_{J_2}(L_I) \Rightarrow \mathcal{E}_{J_1}(G) = \mathcal{E}_{J_2}(G), \text{ for all } J_1, J_2 \subseteq I,$$

but the converse is not necessarily true (see Exercise 3).

The next result shows that generalized induction respects the distribution of irreducible characters into association classes  $\{\mathcal{E}_I\}$ .

**(70.22) Proposition.** *Let  $\zeta \in \text{Irr } G$ , and let  $\lambda \in \text{Irr } L_I$  for some subset  $I \subseteq S$ . Then  $(\zeta, R_{L_I}^G \lambda) = 0$  unless there exists a subset  $J \subseteq I$  such that*

$$\zeta \in \mathcal{E}_J(G) \quad \text{and} \quad \lambda \in \mathcal{E}_J(L_I).$$

*Proof.* We have  $\lambda \in \mathcal{E}_J(L_I)$  for some subset  $J \subseteq I$ , by (70.14). This means that for some cuspidal character  $\varphi \in \text{Irr } L_J$ , we have

$$R_{L_J}^{L_I} \varphi = (\lambda, R_{L_J}^{L_I} \varphi) \lambda + \sum_{\lambda' \in \text{Irr } L_I, \lambda' \neq \lambda} (\lambda', R_{L_J}^{L_I} \varphi) \lambda',$$

with the multiplicity  $(\lambda, R_{L_J}^{L_I} \varphi) \neq 0$ . By transitivity of generalized induction (70.6), it follows that

$$R_{L_J}^G \varphi = R_{L_I}^G R_{L_J}^{L_I} \varphi = (\lambda, R_{L_J}^{L_I} \varphi) R_{L_I}^G \lambda + \sum_{\lambda' \neq \lambda} (\lambda', R_{L_J}^{L_I} \varphi) R_{L_I}^G \lambda'.$$

Now let  $\zeta \in \text{Irr } G$ , and assume  $(\zeta, R_{L_I}^G \lambda) \neq 0$ . Since

$$(\lambda, R_{L_J}^{L_I} \varphi) > 0 \quad \text{and} \quad (\lambda', R_{L_J}^{L_I} \varphi) \geq 0 \text{ for } \lambda' \neq \lambda,$$

we obtain  $(\zeta, R_{L_I}^G \varphi) > 0$ . Thus  $\zeta \in \mathcal{E}_J(G)$ , as required.

We are now in a position to prove two reduction theorems, which express certain character values  $\zeta(x)$ , for  $\zeta \in \text{Irr } G$  and  $x \in G$ , in terms of the character values  $\lambda(x)$  of irreducible characters  $\lambda$  of smaller groups of Lie type containing  $C_G(x)$ .

**(70.23) Theorem (Curtis [75]).** *Let  $\zeta \in \mathcal{E}_J(G)$ , where  $J \subseteq S$ . Let  $x \in G$  be an element*

such that  $C_G(x) \leq L_I$  for some subset  $I \subseteq S$ . Then either  $\zeta(x) = 0$ , or else

$$\zeta(x) = \sum_{\lambda \in \mathcal{E}_{J'}(L_I)} (\zeta, R_{L_I}^G \lambda) \lambda(x),$$

where the sum is taken over subsets  $J' \subseteq I$  such that  $\mathcal{E}_{J'}(G) = \mathcal{E}_{J'}(G)$ .

*Proof.* By (70.1), we have

$$\zeta(x) = \zeta|_{P_I}(x) = T_{L_I}^G \zeta(x) + \zeta''(x),$$

where

$$T_{L_I}^G \zeta = \sum_{\lambda \in \text{Irr } L_I} (\zeta, R_{L_I}^G \lambda) \lambda,$$

and  $\zeta''$  is the contribution to the restriction  $\zeta|_{P_I}$  from irreducible characters of  $P_I$  whose kernels do not contain  $V_I = O_p(P_I)$ . Since  $C_G(x) \leq L_I$ , we have  $C_G(x) \cap V_I = 1$ , and hence  $\zeta''(x) = 0$  by the Feit-Thompson Lemma (Exercise 9.15). The result now follows from (70.22), since the multiplicities  $(\zeta, R_{L_I}^G \lambda)$  vanish unless  $\lambda \in \mathcal{E}_{J'}(L_I)$  and  $\mathcal{E}_{J'}(G) = \mathcal{E}_{J'}(G)$ , for  $J' \subseteq I$ .

**Remarks.** (i) The preceding result, and extensions of it to follow, are somewhat analogous to Brauer's Second Main Theorem 59.14. The organization of characters of  $G$  into  $p$ -blocks (as in Brauer's Theorem) is replaced, in this case, by the distribution of characters into series  $\{\mathcal{E}_J(G) : J \subseteq S\}$ , following (70.21). The Brauer correspondence, from blocks of  $C_G(x)$  to blocks of  $G$ , is replaced by generalized induction from Levi subgroups  $\{L_I : I \subseteq S\}$  to  $G$ .

(ii) Much stronger versions of (70.23) have been proved for irreducible characters of reductive algebraic groups defined over finite fields, using the Deligne-Lusztig theory (see Fong-Srinivasan [82]).

Our second reduction theorem shows that, in the case of principal series characters  $\zeta$  in  $(1_B)^G$ , the nonzero multiplicities appearing in the formula for  $\zeta(x)$  in (70.23) are independent of  $q$  if  $G = G(q)$  as in (68.22). This result has been extended to arbitrary principal series characters by McGovern [82], and to the general situation described in Theorem 70.22 by Howlett-Lehrer [83].

Before stating the result, we review the parametrization of irreducible characters in  $(1_B)^G$  in terms of characters in  $\text{Irr } W$ , from §68B. Throughout the rest of the subsection, we let  $\mathcal{S} = \{G(q)\}$  be a system of finite groups with BN-pairs of type  $(W, S)$ , with the following properties (see (68.22)):

- (i) The set of characteristic powers  $\{q\}$  contains almost all primes.
- (ii) For each characteristic powers  $q = p^a$  of a prime  $p$ , the group  $G(q) \in \mathcal{S}$  has a split BN-pair of characteristic  $p$ , with the fixed Weyl group  $W$  (see (69.1)).

By Theorem 68.24, for each group  $G(q) \in \mathcal{S}$  there exists a bijection  $\varphi \rightarrow \zeta_{\varphi, q}$  from the characters  $\varphi \in \text{Irr } W$  to the characters  $\zeta_{\varphi, q} \in \text{Irr } G(q)$ , such that  $\zeta_{\varphi, q}$  appears with positive multiplicity in  $(1_{B(q)})^{G(q)}$ .

Besides the parametrization  $\varphi \rightarrow \zeta_{\varphi,q}$ , we require the fact that the degrees of the characters  $\zeta_{\varphi,q}$  are given by polynomials in  $q$ . Because of assumption (i) above, we may apply Theorem 68.31 to obtain a polynomial  $F_\varphi(u) \in \mathbb{Q}[u]$  for each  $\varphi \in \text{Irr } W$ , such that the degree of the character  $\zeta_{\varphi,q}$  is given by

$$\deg \zeta_{\varphi,q} = F_\varphi(q) \text{ for all groups } G(q) \in \mathcal{S}.$$

These considerations also apply to the standard Levi subgroups  $\{L_I(q)\}$  of the groups  $G(q) \in \mathcal{S}$ , associated with a fixed subset  $I \subseteq S$  (see (69.14)). These form a system of groups with BN-pairs of type  $(W_I, I)$ , where  $W_I$  is the parabolic subgroup of  $W$  generated by the reflections in  $I$ . This system also satisfies the hypotheses (i) and (ii) above, so there is a bijection  $\psi \rightarrow \eta_{\psi,q}$  from the characters  $\psi \in \text{Irr } W_I$  to the characters  $\eta_{\psi,q}$  in  $\text{Irr } L_I(q)$  that appear with positive multiplicity in  $(1_{B_I(q)})^{L_I(q)}$ , where  $B_I(q) = B(q) \cap L_I(q)$ . For each group  $G(q) \in \mathcal{S}$ , we let  $T(q) = B(q) \cap N(q)$ , so  $(1_{B(q)})^{G(q)} = R_{T(q)}^{G(q)} 1$ .

**(70.24) Theorem (Curtis [75]).** *Let  $G(q) \in \mathcal{S}$ , and let  $x \in G(q)$  be an element such that  $C_{G(q)}(x) \leq L_I(q)$  for some  $I \subseteq S$ . Then for each  $\varphi \in \text{Irr } W$ ,*

$$\zeta_{\varphi,q}(x) = \sum_{\psi \in \text{Irr } W_I} (\zeta_{\varphi,q}, R_{L_I(q)}^{G(q)} \eta_{\psi,q}) \eta_{\psi,q}(x).$$

The multiplicities are independent of  $q$ , and are given by

$$(\zeta_{\varphi,q}, R_{L_I(q)}^{G(q)} \eta_{\psi,q})_{G(q)} = (\varphi, \psi^W)_W,$$

for all  $G(q) \in \mathcal{S}$ ,  $\varphi \in \text{Irr } W$ , and  $\psi \in \text{Irr } W_I$ .

To prove this, let us first establish several preliminary results.

**(70.25) Lemma.** *Let  $(\zeta_{\varphi,q}, R_{L_I(q)}^{G(q)} \eta) \neq 0$  for some character  $\eta \in \text{Irr } L_I(q)$ . Then  $(\eta, R_{T(q)}^{L_I(q)} 1) \neq 0$ , and  $\eta = \eta_{\psi,q}$  for some character  $\psi \in \text{Irr } W_I$ .*

*Proof.* By Theorem 70.22, we have  $(\eta, R_{T(q)}^{L_I(q)} \lambda) \neq 0$  for some linear character  $\lambda \in \text{Irr } T(q)$ . Then by transitivity of generalized induction, we have

$$(R_{T(q)}^{G(q)} 1, R_{T(q)}^{G(q)} \lambda) \neq 0,$$

and hence  $\lambda = 1$  by Theorem 70.15A. Since  $R_{T(q)}^{L_I(q)} 1 = (1_{B_I(q)})^{L_I(q)}$ , we have  $\eta = \eta_{\psi,q}$  for some character  $\psi \in \text{Irr } W_I$ , by the remarks preceding the theorem.

We next take up the calculation of the multiplicities, using some ideas of Scott [73]. Let  $\{c_1, \dots, c_n\}$  define the index parameters of the groups  $G(q) \in \mathcal{S}$  (see (68.22)). Let  $R = \mathbb{Q}[u_1, \dots, u_n]$ , where  $u_i = u^{c_i}$ ,  $1 \leq i \leq n$ , for some fixed indeterminate  $u$  over  $\mathbb{Q}$ , and let  $A$  be the generic algebra of the Coxeter system  $(W, S)$  over the ring  $R$  (see §68A).

For each group  $G(q) \in \mathcal{S}$ , the map  $u \rightarrow q$  defines a specialization of  $R$  such that the specialized algebra  $A_{(q)}$  is isomorphic to the Hecke algebra  $\mathcal{H}(G(q), B(q), 1_B)$ , by (68.11). The map  $u \rightarrow 1$  defines a specialization such that the specialized algebra  $A_{(1)} \cong CW$ .

Now let:

$K = \text{quotient field of } R$ ,

$K^* = \text{a splitting field of } A^K \text{ such that } \dim_K K^* < \infty$ ,

$R^* = \text{the integral closure of } R \text{ in } K^*$ ,

$\hat{R} = \text{the localization of } R^* \text{ at some fixed prime ideal } \mathfrak{q} \text{ containing either } u - 1, \text{ or } u - q \text{ for some } G(q) \in \mathcal{S}$ .

By (68.20), there is a bijection  $\text{Irr } W \leftrightarrow \text{Irr } A^{K^*}$ ; for each  $\varphi \in \text{Irr } W$ , we shall denote the corresponding irreducible character of  $A^{K^*}$  by  $\mu_\varphi$ .

**(70.26) Lemma.** *Let  $\mu_\varphi \in \text{Irr } A^{K^*}$  for an arbitrary character  $\varphi \in \text{Irr } W$ . Then there exists a primitive idempotent  $e \in A^{K^*}$  such that the minimal left ideal  $A^{K^*}e$  affords  $\mu_\varphi$ , and  $\mu_\varphi(ea) \in \hat{R}$  for all elements  $a \in A$ .*

*Proof.* The localization  $\hat{R}$  is a d.v.r. Therefore, letting  $V$  be a simple  $A^{K^*}$ -module affording  $\mu_\varphi$ , there is an  $A^{\hat{R}}$ -lattice  $V_0$  in  $V$  such that  $V_0^{K^*} \cong V$ . Then  $V_0$  is a free  $\hat{R}$ -module with a finite basis  $\{v_1, \dots, v_d\}$ . For each  $a \in A$ , left multiplication by  $a$  acting on the basis  $\{v_i\}$  is given by a matrix  $(\alpha_{ij}(a))$  with entries in  $\hat{R}$ . The Wedderburn component of  $A^{K^*}$  corresponding to  $\mu_\varphi$  is faithfully represented by its action on  $V$ . Let  $e$  be the primitive idempotent in  $A^{K^*}$  whose matrix with respect to the basis  $\{v_i\}$  is  $\text{diag}(1, 0, \dots, 0)$ . Then  $A^{K^*}e$  affords  $\mu_\varphi$ , and if  $a \in A$ , it follows that  $\mu_\varphi(ea) \in \hat{R}$ , since  $\mu_\varphi(ea) = \text{Tr}(ea, V) = \alpha_{11}(a)$ , where  $(\alpha_{ij}(a))$  is as above.

**(70.27) Lemma.** *Let  $e$  be an arbitrary primitive idempotent in  $A^{K^*}$  affording the character  $\mu_\varphi$ , for some  $\varphi \in \text{Irr } W$ . Then*

$$e = F_\varphi(u)P(u)^{-1} \sum_{w \in W} (\text{IND } e_w)^{-1} \mu_\varphi(ee_w^{-1})e_w,$$

where  $F_\varphi(u) \in \mathbb{Q}[u]$  is the generic degree corresponding to  $\varphi$ , and  $P(u) = \sum_{w \in W} \text{IND } e_w$ .

*Proof.* Let  $\rho: A^{K^*} \rightarrow K^*$  be the map defined by

$$\rho = \sum_{\varphi \in \text{Irr } W} F_\varphi(u) \mu_\varphi.$$

By (68.30ii), we have

$$\rho(e_w) = \begin{cases} 0 & \text{if } w \neq 1, \\ P(u) & \text{if } w = 1. \end{cases}$$

Using the bilinear form  $\beta:A^K \times A^K \rightarrow K$  defined in §68C, it follows that for  $w, w' \in W$ ,

$$e_w e_{w'} = c_1 e_1 + \sum_{x \neq 1} c_x e_x, \quad c_x \in K, \quad x \in W,$$

where  $c_1 = 0$  if  $ww' \neq 1$  and  $c_1 = \text{IND } e_w$  if  $ww' = 1$ . Combining this result with the preceding formula, we obtain

$$\rho(e_w e_{w'}) = \begin{cases} 0 & \text{if } ww' \neq 1 \\ P(u) \text{IND } e_w & \text{if } ww' = 1. \end{cases}$$

Now let  $e = \sum_{w \in W} \lambda_w e_w$ , with  $\lambda_w \in K^*$  for all  $w \in W$ . Applying  $\rho$  to both sides of the formula,

$$ee_{w_1^{-1}} = \sum \lambda_w e_w e_{w_1^{-1}}, \quad \text{for } w_1 \in W,$$

we obtain

$$F_\varphi(u) \mu_\varphi(ee_{w_1^{-1}}) = \lambda_{w_1} P(u) \text{IND } e_{w_1},$$

since  $\mu_{\varphi'}(ee_{w_1^{-1}}) = 0$  if  $\varphi' \neq \varphi$ . Thus the coefficients  $\{\lambda_w\}$  of  $e$  have the required form, and the lemma is proved.

Before stating the next result, we recall that  $\hat{R}$  denotes the localization of  $R^*$  at a prime ideal containing either  $u - 1$  or  $u - q$ , for some group  $G(q) \in \mathcal{S}$ . By Lemma 68.16 there exists an extension of the given specialization to  $R^*$ , and hence a further extension  $\hat{f}$  to the localization  $\hat{R}$ , that is,  $\hat{f}: \hat{R} \rightarrow C$ . The specialized algebra defined by  $\hat{f}$  will be denoted by  $\hat{A}$ . The map  $\hat{f}$  can be extended to a homomorphism of  $\hat{R}$ -algebras  $\hat{f}: A^{\hat{R}} \rightarrow \hat{A}$ , where the  $\hat{R}$ -algebra structure of  $\hat{A}$  is defined using the homomorphism  $\hat{f}: \hat{R} \rightarrow C$ .

**(70.28) Lemma.** *Keep the notation of the preceding paragraph. Let  $\varphi \in \text{Irr } W$ , and let  $\mu_\varphi$  be the corresponding character of  $A^{K^*}$ . Then there exists a primitive idempotent  $e$  in  $A^{K^*}$  affording  $\mu_\varphi$ , with the following properties:*

- (i)  $e \in A^{\hat{R}}$ ;
- (ii)  $\hat{f}(e) = \hat{e}$  is a primitive idempotent in the specialized algebra  $\hat{A}$ ;
- (iii)  $\hat{e}$  affords the specialized character  $\hat{\mu}_\varphi = \mu_{\varphi, \hat{f}}$  (see (68.20)).

*Proof.* (i) By Lemma 70.26, there exists a primitive idempotent  $e \in A^{K^*}$  affording  $\mu_\varphi$ , such that  $\mu_\varphi(ea) \in \hat{R}$  for all  $a \in A$ . By Lemma 70.27, we obtain  $e \in A^{\hat{R}}$ , since the elements  $P(u)$  and  $\{\text{IND } e_w : w \in W\}$  are clearly invertible in  $\hat{R}$ .

- (ii) Because  $e \in A^{\hat{R}}$  is primitive in  $A^{K^*}$ , we have

$$eAe \subseteq eA^{K^*}e \cap A^{\hat{R}} \subseteq K^*e \cap A^{\hat{R}} \subseteq \hat{R}e,$$

using the fact that  $\hat{R}$  is a d.v.r. It follows that

$$\hat{e}\hat{A}\hat{e} = \mathbf{C}\hat{e}$$

and hence  $\hat{e} = \hat{f}(e)$  is primitive in  $\hat{A}$ .

(iii) By (68.20), the specialized character  $\hat{\mu}_\varphi$  satisfies the condition

$$\hat{\mu}_\varphi(\hat{e}) = \hat{f}(\mu_\varphi(e)) = 1.$$

Thus  $\hat{A}\hat{e}$  is a minimal ideal in the semisimple algebra  $\hat{A}$ , and affords the character  $\hat{\mu}_\varphi$ .

*Proof of Theorem 70.24.* Since  $C_G(x) \leq L_I$  and  $\zeta_{\varphi,q} \in \mathcal{E}_{\mathcal{S}}(G(q))$ , we obtain

$$\zeta(x) = \sum_{\lambda \in \mathcal{E}_{\mathcal{S}}(L_I)} (\zeta_{\varphi,q}, R_{L_I(q)}^{G(q)} \lambda) \lambda(x)$$

by Theorem 70.23. By Lemma 70.25, the multiplicities  $(\zeta_{\varphi,q}, R_{L_I(q)}^{G(q)} \lambda)$  are 0 unless  $\lambda = \eta_{\psi,q}$  for some character  $\psi \in \text{Irr } W_I$ . It remains to calculate these multiplicities in terms of the characters of  $W$  and  $W_I$ .

Let  $A_I$  be the  $R$ -subalgebra of  $A$  generated by the elements  $\{e_w : w \in W_I\}$ . Then  $A_I$  is the generic algebra of the system of finite groups with  $BN$ -pairs of type  $W_I$ , consisting of the standard Levi subgroups  $\{L_I(q)\}$  of the groups  $G(q) \in \mathcal{S}$ . Let  $\psi \in \text{Irr } W_I$ ,  $\varphi \in \text{Irr } W$ , and let  $v_\psi$  and  $\mu_\varphi$  be the irreducible characters of  $A_I^{K^*}$  and  $A^{K^*}$  corresponding to  $\psi$  and  $\varphi$ , respectively. There exists a primitive idempotent  $e \in A_I^{K^*}$  affording  $v_\psi$  satisfying the conditions of Lemma 70.28, where  $\hat{R}$  is a d.v.r. chosen as in the discussion preceding the lemma. Then  $\mu_\varphi(e) = m$ , for some nonnegative integer  $m$ ; moreover,  $m$  is independent of the choice of the primitive idempotent  $e$  affording  $v_\psi$ , since all such idempotents are conjugate in  $A_I^{K^*}$ , by Exercise 6.15. We shall prove that

$$m = (\varphi, \psi^w)_W = (\zeta_{\varphi,q}, R_{L_I(q)}^{G(q)} \eta_{\psi,q})_{G(q)},$$

for all groups  $G(q) \in \mathcal{S}$ . The proof is based on Lemma 70.28.

First assume the homomorphism  $\hat{f}: \hat{R} \rightarrow \mathbf{C}$  extends the specialization  $u \rightarrow 1$ . Then the specialized algebras  $\hat{A}$  and  $\hat{A}_I$  are isomorphic to  $\mathbf{C}W$  and  $\mathbf{C}W_I$ , respectively, by (68.11). By Lemma 70.28, the idempotent  $\hat{e} = \hat{f}(e) \in \hat{A}_I$  corresponds to a primitive idempotent in  $\mathbf{C}W_I$  affording the character  $\psi$ , and

$$m = \hat{f}(\mu_\varphi(e)) = \hat{\mu}_\varphi(\hat{e}) = (\varphi, \psi^w)_W,$$

by Frobenius reciprocity.

Now let  $\hat{f}: \hat{R} \rightarrow \mathbf{C}$  extend a specialization  $u \rightarrow q$ , for some group  $G(q) \in \mathcal{S}$ . In this case, we have,

$$\hat{A} \cong H(G(q), B(q), 1) \quad \text{and} \quad \hat{A}_I \cong H(P_I(q), B(q), 1)$$

for the specialized algebras  $\hat{A}$  and  $\hat{A}_I$ . By Theorem 68.24, the specialized characters  $\hat{\mu}_\varphi$  and  $\hat{\nu}_\psi$  of  $\hat{A}$  and  $\hat{A}_I$ , respectively, correspond to the restrictions of  $\zeta_{\varphi,q}$  to  $\mathcal{H}(G(q), B(q), 1)$  and of  $\tilde{\eta}_{\psi,q}$  to  $\mathcal{H}(P_I(q), B(q), 1)$ , where  $\tilde{\eta}_{\psi,q}$  denotes the pullback of  $\eta_{\psi,q}$  to  $P_I(q)$ . Thus if  $e \in A_I^R$  is a primitive idempotent in  $A_I^{K^*}$  affording  $\nu_\psi$ , the specialized idempotent  $\hat{e} \in \hat{A}_I$  corresponds to a primitive idempotent in  $\mathcal{H}(P_I(q), B(q), 1)$  affording the restriction of  $\tilde{\eta}_{\psi,q}$ . By Lemma 11.23, this idempotent is primitive in  $CP_I(q)$ , and affords  $\tilde{\eta}_{\psi,q}$ . We then obtain

$$m = \hat{f}(\mu_\varphi(e)) = \hat{\mu}_\varphi(e) = (\zeta_{\varphi,q}|_{P_I(q)}, \tilde{\eta}_{\psi,q}) = (\zeta_{\varphi,q}, R_{L_I(q)}^{G(q)} \eta_{\psi,q}),$$

by Frobenius reciprocity, completing the proof of the Theorem.

## §70. Exercises

1. Let  $G$  be a finite group with a split  $BN$ -pair of characteristic  $p$ , and let  $(W, S)$  be the Coxeter system associated with  $G$ . Let  $I, J \subseteq S$ . Prove that  $L_I = {}^x L_J$ , for  $x \in W$ , if and only if  $W_I = {}^x W_J$ .
2. Keep the notation of Exercise 1. Prove the *Generalized Subgroup Theorem*: Let  $I, J \subseteq S$ , and let  $\lambda \in \text{ch } L_J$ . Then

$$T_{L_I}^G R_{L_J}^G \lambda = \sum_{x \in D_{IJ}} R_{L_K}^{L_I x} T_{L_K}^{L_J} \lambda,$$

where for each  $x \in D_{IJ}$ ,  $K = I \cap {}^x J = {}^x K'$ .

[Hint: Use (70.6ii) and (70.7)].

3. Let  $G = GL_4(\mathbb{F}_q)$ , with the usual  $BN$ -pair. Let  $\{s_1, s_2, s_3\}$  be the set of distinguished generators of the Weyl group. Let  $J_1 = \{s_1\}$ ,  $J_2 = \{s_2\}$ ,  $I = \{s_1, s_3\}$ . Prove that  $\mathcal{E}_{J_1}(G) = \mathcal{E}_{J_2}(G)$ , but  $\mathcal{E}_{J_1}(L_I) \neq \mathcal{E}_{J_2}(L_I)$  (see the remarks preceding (70.22)).
4. Let  $\varphi \in \text{Irr } W$ , and let  $\zeta_{\varphi,q}$  be the corresponding character in  $(1_{B(q)})^{G(q)}$ . Apply the reduction theorem (70.24) to prove that, for each  $t \in T(q)$  which is regular in the sense that  $C_{G(q)}(t) = T(q)$ , we have

$$\zeta_{\varphi,q}(t) = (\zeta_{\varphi,q}, (1_{B(q)})^{G(q)}) = \deg \varphi.$$

## §71. A DUALITY OPERATION IN $\text{ch } CG$

Let  $H$  be a finite group. A *duality operation* in  $\text{ch } CH$  is a  $\mathbb{Z}$ -automorphism of order 2 that preserves the inner product  $(\lambda, \mu)_H$ , for  $\lambda, \mu \in \text{ch } CH$ . Such an operation clearly permutes, up to sign, the irreducible  $\mathbb{C}$ -characters of  $H$ . A familiar example of a duality operation is the map  $\zeta \rightarrow \bar{\zeta}$ , for  $\zeta \in \text{ch } CH$ , given by complex conjugation. This map corresponds to the operation of forming the contragredient module of a given  $CH$ -module.

Now let  $G$  be a finite group with a split  $BN$ -pair of characteristic  $p$ . We shall

define another duality operation  $D_G : \text{ch } CG \rightarrow \text{ch } CG$  in this case, such that  $D_G 1_G = \text{St}_G$ , where  $\text{St}_G$  is the Steinberg character of  $G$ . This operation has a number of applications to both the ordinary and modular representation theory of  $G$ , which we shall discuss, along with other things, in this section and the next. The results in this section are due to Curtis [80a] and Alvis ([80], [82]) (see also the survey article (Curtis [82])). The main results were proved independently by Kawanaka [82], who also discussed  $D_G$  in the context of Fourier transforms of functions on the Lie algebra of  $G$ , and by Deligne–Lusztig ([82], [83]).

### §71A. Definition and Basic Properties of $D_G$

Throughout this section,  $G$  denotes a finite group with a split  $BN$ -pair of characteristic  $p$ , and  $(W, S)$  the pair consisting of the Weyl group  $W$  and the set  $S$  of distinguished generators of  $W$ . We shall follow the notation of §70, and also use most of its results. In particular,  $\text{ch } H$  denotes the set of all virtual  $\mathbb{C}$ -characters of a finite group  $H$ .

The general concept of a *duality operation* was defined above. We begin with a duality operation in  $\text{ch } W$ , given by the map

$$\mu \mapsto \mu\varepsilon, \quad \mu \in \text{ch } W,$$

where  $\varepsilon$  is the sign character of  $W$  (see (66.26)). This map is clearly a duality operation, and has traditionally been used to organize the character tables of finite Coxeter groups. This operation is related to the parabolic subgroups of  $W$  by the following result:

**(71.1) Proposition.** *Let  $(W, S)$  be a finite Coxeter system, and let  $\varepsilon$  be the sign representation of  $W$ . Then*

$$\mu\varepsilon = \sum_{J \subseteq S} (-1)^{|J|} (\mu|_{W_J})^W.$$

*Proof.* By Solomon's formula (66.29), we have

$$\varepsilon = \sum_{J \subseteq S} (-1)^{|J|} (1_{W_J})^W.$$

Multiplying by  $\mu$ , we obtain

$$\mu\varepsilon = \sum_{J \subseteq S} (-1)^{|J|} \mu \cdot (1_{W_J})^W.$$

The proof is completed by the observation that

$$\mu \cdot (1_{W_J})^W = (\mu|_{W_J})^W \quad \text{for all } J \subseteq S,$$

by (15.5).

We now define a duality operation in  $\text{ch } G$ , using a formula similar to (71.1). The operations of restriction and induction occurring in (71.1) are replaced by truncation and generalized induction (§70A).

**(71.2) Definition.** The *duality operation*  $D_G$  in  $\text{ch } G$  is the  $\mathbb{Z}$ -endomorphism given by

$$D_G \zeta = \sum_{J \subseteq S} (-1)^{|J|} R_{L_J}^G T_{L_J}^G \zeta, \quad \text{for } \zeta \in \text{ch } G.$$

**Remarks and Example.** By (66.34), we have

$$D_G 1_G = \text{St}_G.$$

Note that in this case the degrees of  $1_G$  and its dual  $D_G 1_G$  differ by  $|G|_p$ , since

$$\text{St}_G 1 = |B : B \cap {}^{w_0}B| = |B : T| = |U| = |G|_p,$$

by (67.10) and (69.9).

On the other hand, we have

$$D_G \zeta = (-1)^{|S|} \zeta$$

for all cuspidal characters  $\zeta$  of  $G$ , by (70.12).

These remarks show that the operation  $D_G$  is *not* given by multiplication by a linear character, as in (71.1); it is not even clear at this point whether (71.2) defines a duality operation. This fact will follow from the next two theorems.

The first is due to Curtis [80a], with a simplified proof based on §70. Another proof, in a geometrical context, has been given by Digne-Michel [82]. In order to state the result, we recall that for each  $J \subseteq S$ , the standard Levi subgroup  $L_J$  is a finite group with a split  $BN$ -pair, so  $D_{L_J} : \text{ch } L_J \rightarrow \text{ch } L_J$  is defined (by (71.2)).

**(71.3) Theorem.** Let  $\zeta \in \text{ch } G$  and  $I \subseteq S$ . Then

$$T_{L_I}^G D_G \zeta = D_{L_I} T_{L_I}^G \zeta.$$

In other words, truncation intertwines duality.

*Proof.* We must prove that

$$(71.4) \quad \sum_{J \subseteq S} (-1)^{|J|} T_{L_I}^G R_{L_J}^G T_{L_J}^G \zeta = \sum_{K \subseteq J} (-1)^{|K|} R_{L_K}^{L_I} T_{L_K}^{L_I} T_{L_I}^G \zeta,$$

for each  $\zeta \in \text{ch } G$ . We begin by applying the Generalized Subgroup Theorem (Exercise 70.2) to a typical term on the left side of (71.4). We obtain

$$T_{L_I}^G R_{L_J}^G T_{L_J}^G \zeta = \sum_{x \in D_{IJ}} R_{L_K}^{L_I} \dot{\times} (T_{L_K}^{L_I} T_{L_J}^G \zeta) = \sum_{x \in D_{IJ}} R_{L_K}^{L_I} \dot{\times} (T_{L_K}^G \zeta),$$

by transitivity of truncation (70.6iii), where

$$K = I \cap {}^x J = {}^x K'$$

as in the statement of the Generalized Subgroup Theorem. For  $x \in D_{IJ}$  and  $K, K'$  as above, we have  $L_K = {}^x L_{K'}$ , and the corresponding term in the sum becomes

$$R_{L_K}^{L_I} T_{L_K}^G \zeta,$$

by (70.10). Then the left side of (71.4) is given by

$$\sum_{K \subseteq I} \sum_{J \subseteq S} (-1)^{|J|} a_{IJK} R_{L_K}^{L_I} T_{L_K}^G \zeta,$$

where for  $I, J \subseteq S$  and  $K \subseteq I$ ,

$$a_{IJK} = \text{card} \{x \in D_{IJ} : I \cap {}^x J = K\}.$$

The identity (71.4) is an immediate consequence of these facts, and the following:

**(71.5) Lemma.** *For  $J \subseteq S$  and  $K \subseteq I$ , let  $a_{IJK}$  be defined as above. Then*

$$\sum_{J \subseteq S} (-1)^{|J|} a_{IJK} = (-1)^{|K|}.$$

We omit the proof, and refer the reader to Curtis [80a]. For a geometric interpretation of the lemma, see Howlett-Lehrer [82] and Digne-Michel [82]. This completes the proof of Theorem 71.3.

Since  $D_G 1_G = \text{St}_G$ , we obtain:

**(71.6) Corollary.** *For each subset  $I \subseteq S$ , we have*

$$T_{L_I}^G \text{St}_G = \text{St}_{L_I}.$$

We next state the following basic result:

**(71.7) Theorem.** (Alvis [80]). *The duality operation  $D_G$  is a self-adjoint isometry in  $\text{ch } G$  of order 2. Thus*

$$(D_G \zeta, \eta) = (\zeta, D_G \eta) \quad \text{and} \quad D_G^2 \zeta = \zeta,$$

for all  $\zeta, \eta \in \text{ch } G$ .

*Proof.* By (70.6i), we have

$$T_{L_J}^G \zeta = \sum_{\varphi \in \text{Irr } L_J} (\zeta, R_{L_J}^G \varphi) \varphi.$$

Using this fact, we obtain

$$\begin{aligned} (D_G \zeta, \eta) &= \sum_{J \subseteq S} (-1)^{|J|} (R_{L_J}^G T_{L_J}^G \zeta, \eta) \\ &= \sum_{J \subseteq S} (-1)^{|J|} \left( R_{L_J}^G \left\{ \sum_{\varphi \in \text{Irr } L_J} (\zeta, R_{L_J}^G \varphi) \varphi \right\}, \eta \right) \\ &= \sum_{J \subseteq S} (-1)^{|J|} \sum_{\varphi \in \text{Irr } L_J} (\zeta, R_{L_J}^G \varphi) (R_{L_J}^G \varphi, \eta) = (\zeta, D_G \eta), \end{aligned}$$

by symmetry.

We next prove that  $D_G^2$  is the identity map. Let  $\zeta \in \text{ch } G$ . Then

$$\begin{aligned} D_G^2 \zeta &= \sum_{J \subseteq S} (-1)^{|J|} R_{L_J}^G T_{L_J}^G D_G \zeta = \sum_{J \subseteq S} (-1)^{|J|} R_{L_J}^G D_{L_J} T_{L_J}^G \zeta \\ &= \sum_{J \subseteq S} (-1)^{|J|} \sum_{K \subseteq J} (-1)^{|K|} R_{L_J}^G R_{L_K}^{L_J} T_{L_K}^{L_J} T_{L_J}^G \zeta \\ &= \sum_{J \subseteq S} (-1)^{|J|} \sum_{K \subseteq J} (-1)^K R_{L_K}^G T_{L_K}^G \zeta \\ &= \sum_{K \subseteq S} (-1)^{|K|} \left( \sum_{J \supseteq K} (-1)^{|J|} \right) R_{L_K}^G T_{L_K}^G \zeta = (-1)^{2|S|} \zeta = \zeta. \end{aligned}$$

In this calculation, we have used (71.3) at the second step, (70.6iii) at the fourth, and the fact that  $\sum_{J \supseteq K} (-1)^{|J|} = 0$  if  $K \neq S$  in the last step.

From what has been shown, it is now easy to prove that  $D_G$  is an isometry. Let  $\zeta, \eta \in \text{ch } G$ . Then

$$(D_G \zeta, D_G \eta) = (\zeta, D_G^2 \eta) = (\zeta, \eta),$$

completing the proof.

**(71.8) Corollary.** *The map  $D_G$  is a duality operation, and permutes the irreducible characters of  $G$ , up to sign.*

*Proof.* Let  $\zeta \in \text{Irr } G$ . Then  $D_G \zeta \in \text{ch } G$  and  $(D_G \zeta, D_G \zeta) = (\zeta, \zeta) = 1$  by (71.7). It follows that  $\pm D_G \zeta \in \text{Irr } G$ , as required.

## §71B. The Effects of $D_G$ on Character Degrees

We keep the assumptions and notation of §71A. It will be necessary to extend the operations of truncation  $T_{L_J}^G$  and generalized induction  $R_{L_J}^G$ , for  $J \subseteq S$ , to the vector spaces  $\text{cf}(G)$  and  $\text{cf}(L_J)$  of complex-valued class functions on  $G$  and  $L_J$ . This is easily done by linearity, since  $\text{Irr } G$  is a  $\mathbb{C}$ -basis of  $\text{cf}(G)$ , by (9.23i).

The first result is a variation by Alvis [80] on a theorem of Springer [80].

**(71.9) Theorem.** *Let  $V$  denote the set of all  $p$ -elements in  $G$ , and  $\chi_V$  the characteristic function on  $V$  (that is, the function that is 1 on  $V$ , and 0 on the*

complement of  $V$ ). Then

$$D_G \rho_G = |G|_{p'} \chi_V,$$

where  $\rho_G$  is the regular character of  $G$ , and  $|G|_{p'}$  is the  $p'$ -part of the order of  $G$ .

Before starting the proof, we require a lemma. We recall (from §70A) that for a class function  $\xi$  on  $L_J$ ,  $J \subseteq S$ , the pullback  $\tilde{\xi}$  (or  $\xi\tilde{}$ ) is the class function on the parabolic subgroup  $P_J$  defined by  $\tilde{\xi}(lv) = \xi(l)$ ; here  $l \in L_J$  and  $v \in V_J$ , using the Levi decomposition  $P_J = L_J V_J$  (see (69.10)).

**(71.10) Lemma.** Let  $J \subseteq S$ . Then  $(T_{L_J}^G \chi_V)\tilde{=} \chi_V|_{P_J}$ .

*Proof.* Let  $P_J = L_J V_J$  be the Levi decomposition of  $P_J$ . Since  $V_J$  is a normal  $p$ -subgroup of  $P_J$ , it is easily verified that for an arbitrary element  $v \in V_J$ , an element  $g \in P_J$  is a  $p$ -element if and only if  $gv$  is a  $p$ -element. We have to prove that

$$(T_{L_J}^G \chi_V)\tilde{(}g\tilde{)} = \chi_V(g) \text{ for all } g \in P_J.$$

First suppose  $g$  is a  $p$ -element. Then  $\chi_V(g) = 1$ . Now write  $g = lv$ ,  $l \in L_J$ ,  $v \in V_J$ , obtaining

$$(T_{L_J}^G \chi_V)\tilde{(}g\tilde{)} = (T_{L_J}^G \chi_V)(l) = |V_J|^{-1} \sum_{v \in V_J} \chi_V(lv).$$

Since  $g$  is assumed to be a  $p$ -element, so also is  $l$ , as well as all the products  $lv$ ,  $v \in V_J$ , by the first step of the proof. It follows that  $(T_{L_J}^G \chi_V)\tilde{(}g\tilde{)} = 1$ , and the lemma is proved in this case. On the other hand if  $g$  is not a  $p$ -element, the same argument shows that both  $\chi_V(g)$  and  $(T_{L_J}^G \chi_V)\tilde{(}g\tilde{)}$  are zero, completing the proof.

*Proof of (71.9).* We note first that  $\text{St}_G(1) = |G|_p$  by (69.9), and hence  $\text{St}_G$  vanishes on  $p$ -irregular elements of  $G$  by (18.28) and (18.26ii), since  $\text{St}_G \in \text{Irr } G$ . We now have

$$\begin{aligned} |G|_{p'}^{-1} \rho_G &= \chi_V \cdot \text{St}_G \quad (\text{by direct verification}) \\ &= \sum_{J \subseteq S} (-1)^{|J|} \chi_V \cdot (1_{P_J})^G \quad (\text{since } \text{St}_G = D_G 1_G) \\ &= \sum_{J \subseteq S} (-1)^{|J|} (\chi_V|_{P_J})^G = \sum_{J \subseteq S} (-1)^{|J|} ((T_{L_J}^G \chi_V)\tilde{)}^G \quad (\text{by (15.5) and (71.10)}) \\ &= \sum_{J \subseteq S} (-1)^{|J|} R_{L_J}^G T_{L_J}^G \chi_V = D_G \chi_V. \end{aligned}$$

Now apply  $D_G$  to both sides, to obtain

$$|G|_{p'}^{-1} D_G \rho_G = D_G^2 \chi_V = \chi_V,$$

by (71.7), completing the proof.

We obtain several new results about irreducible characters of  $G$  as a consequence of (71.9). The last of these is related to a conjecture of MacDonald (see Springer [80] and Alvis [80], [82]).

**(71.11) Theorem (Alvis [80]).** *The following statements hold for all  $\zeta \in \text{Irr } G$ :*

- (i)  $\sum_{u \in V} \zeta(u) = |G|_p D_G \zeta(1).$
- (ii)  $(D_G \zeta)(1)_{p'} = \zeta(1)_{p'}.$
- (iii)  $\zeta(1)^{-1} \sum_{u \in V} \zeta(u)$  is, up to sign, a power of  $p$ .

*Proof.* (i) By the definition of  $\chi_V$  and (71.7), we obtain

$$\sum_{u \in V} \zeta(u) = |G|(\zeta, \chi_V)_G = |G|(D_G \zeta, D_G \chi_V)_G.$$

Since  $D_G \chi_V = |G|_p^{-1} \rho_G$  by (71.9), the expression becomes

$$\sum_{u \in V} \zeta(u) = |G|_p (D_G \zeta)(1),$$

using Exercise 9.2 and the fact that  $\pm D_G \zeta \in \text{Irr } G$ .

(ii) We first note that the set  $V$  of all  $p$ -elements is the union of conjugacy classes  $\{\mathfrak{C}'\}$  of  $p$ -elements. For each  $\mathfrak{C}'$ , let  $u_{\mathfrak{C}'}$  denote an element of  $\mathfrak{C}'$ . Then

$$\zeta(1)^{-1} \sum_{u \in V} \zeta(u) = \sum_{\mathfrak{C}'} \zeta(1)^{-1} |\mathfrak{C}'| \zeta(u_{\mathfrak{C}'}) \in \mathbb{Z},$$

since the left side is a rational number, by part (i), and the right side is an algebraic integer by (9.31). Thus

$$|G|_p D_G \zeta(1) \zeta(1)^{-1} \in \mathbb{Z}$$

by part (i). Since  $\pm D_G \zeta \in \text{Irr } G$ , we can replace  $\zeta$  by  $D_G \zeta$  in the above argument, to obtain

$$|G|_p (D_G^2 \zeta)(1) (D_G \zeta)(1)^{-1} = |G|_p \zeta(1) (D_G \zeta)(1)^{-1} \in \mathbb{Z},$$

using (71.7). Then (ii) follows by comparing these results.

(iii) is a direct consequence of (i) and (ii), and completes the proof of the theorem.

**(71.12) Corollary (Steinberg [68]).** *Let  $V$  denote the set of all  $p$ -elements in  $G$ . Then  $|V| = (|G|_p)^2$ .*

For the proof, simply apply (71.11i) with  $\zeta = 1_G$ , and use the fact that  $D_G 1_G = \text{St}_G$ .

The next result shows how  $D_G$  interacts with Harish-Chandra's "philosophy of cusp forms" (see §70B).

**(71.13) Proposition.** *Let  $J \subseteq S$ , and let  $\varphi$  be a cuspidal irreducible character of the standard Levi subgroup  $L_J$ . Then*

$$D_G(R_{L_J}^G \varphi) = (-1)^{|J|} R_{L_J}^G \varphi.$$

Moreover,

$$(\zeta, R_{L_J}^G \varphi) \neq 0 \Rightarrow (D_G \zeta, R_{L_J}^G \varphi) \neq 0 \text{ for all } \zeta \in \text{Irr } G.$$

Thus for  $\varphi$  as above,  $D_G$  permutes the irreducible components of  $R_{L_J}^G \varphi$ , up to sign.

*Proof..* Let  $\zeta \in \text{Irr } G$ . Then we have

$$\begin{aligned} (D_G R_{L_J}^G \varphi, \zeta)_G &= (R_{L_J}^G \varphi, D_G \zeta)_G = (\varphi, T_{L_J}^G D_G \zeta)_{L_J} \\ &= (\varphi, D_{L_J} T_{L_J}^G \zeta)_{L_J} = (D_{L_J} \varphi, T_{L_J}^G \zeta)_{L_J} = (-1)^{|J|} (\varphi, T_{L_J}^G \zeta)_{L_J} \\ &= (-1)^{|J|} (R_{L_J}^G \varphi, \zeta)_G, \end{aligned}$$

by (71.7), (70.6), (71.3), (71.7), and (70.6), respectively. We have also used the fact that  $D_{L_J} \varphi = (-1)^{|J|} \varphi$ , for cuspidal characters  $\varphi$  of  $L_J$ , by the remark following (71.2). This completes the proof.

The preceding result raises interesting questions as to the exact manner in which  $D_G$  permutes the characters in  $R_{L_J}^G \varphi$ , as in (71.13), and whether a sharpened version of Theorem 71.11ii on the comparison of  $\deg \zeta$  and  $\deg D_G \zeta$  is available in this context. We answer these questions here for the case of  $(1_B)^G$ . For arbitrary principal series characters, see McGovern [82], and for the general case, see Howlett-Lehrer [83].

We require the parametrization  $\varphi \rightarrow \zeta_{\varphi, q}$  of irreducible characters in  $(1_{B(q)})^{G(q)}$  by characters  $\varphi \in \text{Irr } W$ , for a system  $\mathcal{S} = \{G(q)\}$  of finite groups with BN-pairs of type  $(W, S)$  (see the summary following (70.23)).

**(71.14) Theorem** (Curtis [80a]). *Let  $\varepsilon$  denote the sign character of  $W$  (see (66.26)). Then we have*

$$D_G \zeta_{\varphi, q} = \zeta_{\varepsilon \varphi, q},$$

for all irreducible characters  $\{\zeta_{\varphi, q}\}$  in  $(1_{B(q)})^{G(q)}$  and all  $G(q) \in \mathcal{S}$ .

*Proof.* By (71.13) and (71.8), it is sufficient to show that for all  $\varphi \in \text{Irr } W$ , we have

$$(71.15) \quad (D_G \zeta_{\varphi, q}, \zeta_{\varepsilon \varphi, q}) = 1.$$

We first prove that for all characters  $\varphi, \varphi' \in \text{Irr } W$ , and  $J \subseteq S$ , the following

statement holds:

$$(71.16) \quad (R_{L_J}^G T_{L_J}^G \zeta_{\varphi, q}, \zeta_{\varphi', q})_{G(q)} = ((\varphi|_{W_J})^W, \varphi')_W.$$

To prove (71.16), apply (70.6) and (70.25) to obtain

$$T_{L_J}^G \zeta_{\varphi, q} = \sum_{\psi \in \text{Irr } W_J} (\zeta_{\varphi, q}, R_{L_J}^G \eta_{\psi, q}) \eta_{\psi, q},$$

where  $\{\eta_{\psi, q}\}$  are the irreducible characters in  $(1_{B_{J(q)}})^{L_J(q)}$  parametrized by the characters  $\psi \in \text{Irr } W_J$  as in §70C. It follows that the left side of (71.16) is given by

$$\sum_{\psi \in \text{Irr } W_J} (\zeta_{\varphi, q}, R_{L_J}^G \eta_{\psi, q}) (R_{L_J}^G \eta_{\psi, q}, \zeta_{\varphi', q}).$$

By Theorem 70.24, this expression equals

$$\sum_{\psi \in \text{Irr } W_J} (\varphi, \psi^W) (\psi^W, \varphi'),$$

which becomes

$$\left( \sum_{\psi \in \text{Irr } W_J} (\varphi, \psi^W) \psi^W, \varphi' \right) = \left( \left( \sum_{\psi \in \text{Irr } W_J} (\varphi|_{W_J}, \psi) \psi \right)^W, \varphi' \right),$$

using Frobenius reciprocity. Thus (71.16) follows. We now have

$$\begin{aligned} (D_G \zeta_{\varphi, q}, \zeta_{\varepsilon\varphi, q}) &= \sum_{J \subseteq S} (-1)^{|J|} ((\varphi|_{W_J})^W, \varepsilon\varphi) \\ &= \left( \sum_{J \subseteq S} (-1)^{|J|} \varphi|_{W_J}^W, \varepsilon\varphi \right) = (\varepsilon\varphi, \varepsilon\varphi) = 1, \end{aligned}$$

by (71.16) and (71.1), using the definition of  $D_G$ . This establishes (71.15) and the theorem.

Now let us assume that (68.31) applies to the system  $\mathcal{S}$ . Then for each  $\varphi \in \text{Irr } W$ , there exists a polynomial  $F_\varphi = F_\varphi(u)$  with rational coefficients, such that

$$\deg \zeta_{\varphi, q} = F_\varphi(q) \text{ for all } q.$$

We shall compare the generic degree polynomials  $F_\varphi$  and  $F_{\varepsilon\varphi}$ , for each  $\varphi \in \text{Irr } W$ . By Theorem 71.14, this information will describe  $\deg \zeta_{\varphi, q}$  and  $\deg D_{G(q)}(\zeta_{\varphi, q})$ , for each  $q$  (see (71.11ii)).

Let  $u$  be an indeterminate over  $\mathbb{Q}$ ,  $R = \mathbb{Q}[u]$ ,  $K = \mathbb{Q}(u)$ ,  $K^*$  an algebraic closure of  $K$ , and let  $A$  be the generic algebra of the Coxeter system  $(W, S)$  associated with  $\mathcal{S}$ . Then  $A$  is an algebra over the ring  $\mathbb{Q}[u_1, \dots, u_n]$ , where  $u_i = u^{c_i}$ , and the  $\{c_i\}$  are the index parameter of  $\mathcal{S}$  (see (68.22)).

Let  $J_K$  be the involutory automorphism of  $K$  that sends  $u$  to  $u^{-1}$ , and let  $J_{K^*}$  be some fixed extension of  $J_K$  to an involution of  $K^*$ . It is then readily shown that there exists an involution of rings  $J: A^K \rightarrow A^K$ , given by

$$J\left(\sum \xi_w e_w\right) = \sum J_K(\xi_w) \text{SGN}(e_w) J_K(\text{IND } e_w) e_w,$$

where SGN and IND are as defined in (68.9), and the coefficients  $\{\xi_w : w \in W\}$  are in  $K$ . To see this, we observe that  $J$  is a semilinear automorphism of the vector space  $A^K$ , preserving the defining relations of  $A$  given in (68.8).

It is also easily shown, using the discussion in Volume I, p. 152, that  $J$  defines a permutation  $\mu \rightarrow \mu^J$  of the irreducible characters  $\{\mu\}$  of  $A^{K^*}$ , given by

$$\mu^J(a) = J_{K^*}(\mu(J(a))), \quad \text{for } a \in A.$$

In particular, we have

$$\mu^J(e_w) = \text{SGN}(e_w) \text{IND}(e_w) \mu(e_w)$$

for each basis element  $e_w$ . Using these ideas, we shall prove:

**(71.17) Theorem (Green [70]).** *Let  $F_\varphi(u) \in \mathbb{Q}[u]$  be the generic degree polynomial associated with  $\varphi \in \text{Irr } W$ . Then we have*

$$F_{\varepsilon\varphi} = u^N F_\varphi(u^{-1}),$$

where  $N = \text{IND}(e_{w_0})$ , and  $w_0$  is the element of maximal length in  $W$ .

*Proof.* Since we are assuming (68.31), we have

$$F_\varphi(u) = \frac{P(u) \deg \varphi}{\sum_{w \in W} (\text{IND } e_w)^{-1} \mu_\varphi(e_w) \mu_\varphi(e_w^{-1})},$$

where  $\mu_\varphi$  is the irreducible character of  $A^{K^*}$  corresponding to  $\varphi$ . Clearly  $u^N J_K(P(u)) = u^N P(u^{-1}) = P(u)$ , since  $P(u) = \sum_{w \in W} \text{IND } e_w$ . By the remark preceding the theorem, the irreducible character of  $A^{K^*}$  corresponding to  $\varepsilon\varphi$  is  $(\mu_\varphi)^J$ , and hence  $F_{\varepsilon\varphi}$  is given by the same formula as  $F_\varphi$ , with  $\mu_\varphi$  replaced by  $\mu_\varphi^J$ . The proof now follows from a simple calculation, using the definition of  $(\mu_\varphi)^J$ .

### §71C. The Values of the Steinberg Character

In this subsection, we evaluate the Steinberg character  $\text{St}_G$  of a finite group with a split  $BN$ -pair of characteristic  $p$ . The method we follow was communicated to us by D. Alvis, and is based on the fact that truncation intertwines duality (see (71.3) and (71.6)). Using the theory of algebraic groups, Steinberg ([68], (15.5)) calculated  $\text{St}_G(x)$ ,  $x \in G$ , up to sign. Another approach to the calculation of  $\text{St}_G(x)$ , including the sign, is given in the context of homology

representations of reductive algebraic groups over finite fields, by Curtis-Lehrer-Tits [80] (see §66C).

The evaluation of irreducible characters of  $G$  depends, in general, on detailed information about conjugacy classes, which is available only in the context of algebraic groups (see Springer-Steinberg [70]). Nevertheless, the following result can be proved in the present context, and has applications to the  $p$ -modular representation theory of  $G$  and, in a sharpened form, to the character theory of reductive algebraic groups over finite fields (see Deligne-Lusztig [76]).

As usual in this section,  $G$  denotes a finite group with a split BN-pair of characteristic  $p$ ,  $W$  the Weyl group of  $G$ ,  $S$  the set of distinguished generators of  $G$ , and  $\text{St}_G$  the Steinberg character of  $G$ , given by the formula

$$(71.18) \quad \text{St}_G = \sum_{J \subseteq S} (-1)^{|J|} (1_{P_J})^G$$

(see (67.10)). For each  $J \subseteq S$ , we let  $P_J = L_J V_J$  be the Levi decomposition of the parabolic subgroup  $P_J$ , as in (69.10), with  $V_J = O_p(P_J)$ , and  $L_J$  a finite group with a split BN-pair of characteristic  $p$ , whose Weyl group is  $W_K$ .

We also recall that each element  $x \in G$  can be expressed uniquely as a commuting product  $x = su$  of a  $p'$ -element  $s$  and a  $p$ -element  $u$ . We denote the set of  $p'$ -elements in a group  $H$  by  $H_{p'}$ , and will sometimes write  $x = x_{p'} x_p$ , with  $x_{p'} = s$ ,  $x_p = u$ , as above.

**(71.19) Theorem.** *Let  $G$  be a finite group with a split BN-pair of characteristic  $p$ , and let  $\text{St}_G$  be the Steinberg character of  $G$ . Then*

$$\text{St}_G(1) = |G|_p, \quad \text{and} \quad \text{St}_G(x) = 0 \quad \text{if } x \notin G_{p'}.$$

For each  $s \in G_{p'}$ , let  $J$  be a subset of  $S$  such that  $s$  is conjugate to an element in  $L_J$ , but not to any element in  $L_K$ , for  $K \subset J$ . Then

$$\text{St}_G(s) = (-1)^{|J|} |C_G(s)|_p.$$

We begin the proof with a lemma that is a special case of the conjugacy part of the Schur-Zassenhaus Theorem (see §8C). Our self-contained proof is due to Alvis.

**(71.20) Lemma.** *Let  $p$  be a prime, and let the finite group  $H$  be a semidirect product  $H = V \rtimes L$ , where  $V$  is a  $p$ -subgroup. Then for all  $l \in L$  and  $v \in V$ , we have*

$$(lv)_{p'} =_V l_{p'},$$

that is, the  $p'$ -parts of  $lv$  and  $l$  are  $V$ -conjugate.

*Proof.* We may assume that  $L = \langle l \rangle$ . Suppose first that there exists a proper normal subgroup  $V_1 \triangleleft V$  such that  $lV_1l^{-1} = V_1$ . Then  $V_1 \triangleleft H$ , and we set  $H_1 = V_1 \rtimes L$ , and  $\bar{H} = H/V_1$ . Then  $\bar{H} = \bar{V} \rtimes \bar{L}$ , where  $\bar{H} = H/V_1$ ,  $\bar{V} = V/V_1$ ,

and  $\bar{L} = LV_1/V_1$ . As an induction hypothesis, assume the lemma holds for  $\bar{H}$  and  $H_1$ . Let  $h \rightarrow \bar{h}$  be the natural map from  $H$  to  $\bar{H}$ . Then clearly

$$(\bar{lv})_{p'} = \overline{(lv)_{p'}},$$

and it follows that

$$(lv)_{p'} =_V l_{p'} u \text{ for some } u \in V_1.$$

But then  $l_{p'} u = (l_{p'} u)_{p'}$  and  $l_{p'}$  are  $V_1$ -conjugate in  $H_1$ , and so  $(lv)_{p'}$  and  $l_{p'}$  are  $V$ -conjugate, as required.

It remains to check the minimal situation, in which  $l$  normalizes no proper normal subgroup of  $V$ . Then  $C_V(l) = V$  or 1. In the first case we have  $(lv)_{p'} = l_{p'}$ , and the result holds trivially. In the second case, where  $C_V(l) = 1$ , the map  $v_1 \rightarrow l^{-1}v_1^{-1}lv_1$  is a bijection of  $V$ , since  $V$  is finite. In particular,  $v = l^{-1}v_1^{-1}lv_1$  for some  $v_1 \in V$ , and hence  $lv =_V l$ . Then  $(lv)_{p'} =_V l_{p'}$ , and the proof is complete.

*Proof of (71.19).* By (69.9iv), we have  $\text{St}_G 1 = |G|_{p'}$ . Then  $\text{St}_G x = 0$  for all  $x \notin G_{p'}$ . This follows either from Gallagher's Theorem 15.19 (in the context of complex-valued characters of  $G$ ) or by (18.28) and (18.26), using Brauer theory.

Now consider an arbitrary  $p'$ -element  $s \in G$ . We shall calculate  $\text{St}_G s$  in a series of steps.

*Step 1.* First assume that  $s$  is not contained in any proper parabolic subgroup of  $G$ . Then  $sxP_J \neq xP_J$  for all  $x \in G$  and  $J \subset S$ , and hence  $(1_{P_J})^G(s) = 0$  for all  $J \subset S$ . By the alternating sum formula (71.18) for  $\text{St}_G$ , we obtain

$$\text{St}_G(s) = (-1)^{|S|} \quad (\text{if } s \notin P \text{ for all proper parabolic subgroups } P).$$

*Step 2.* Let  $s \in G_{p'}$  be an arbitrary  $p'$ -element, and let  $s$  be conjugate to an element in  $L_J$ , for some  $J \subseteq S$ , but not to an element in  $L_K$ , for  $K \subset J$ . Then

$$(71.21) \quad \text{St}_G s = (-1)^{|J|} |V_J \cap C_G(s)|.$$

We first apply (71.6), and obtain

$$(71.22) \quad \text{St}_{L_J}(s) = T_{L_J}^G \text{St}_G(s) = |V_J|^{-1} \sum_{v \in V_J} \text{St}_G(sv).$$

We now calculate both sides of (71.22) separately. Beginning with the left side, we note first that the standard parabolic subgroups of  $L_J$  all have the form  $L_J \cap P_K$ , for  $K \subseteq J$ , by (69.15), and that each such subgroup has the Levi decomposition

$$L_J \cap P_K = L_K(V_K \cap L_J),$$

also by (69.15). It follows that no conjugate of  $s$  is contained in a proper parabolic subgroup of  $L_J$ , since otherwise  $s$  is conjugate to an element of  $L_K$  for  $K \subset J$ , by Lemma 71.20, applied to the semidirect product  $L_K(V_K \cap L_J)$ . We conclude

that

$$\mathrm{St}_{L_J} s = (-1)^{|J|},$$

by Step 1 applied to the group  $L_J$ .

Now consider the right side of (71.22). If  $\mathrm{St}_G(sv) \neq 0$  for some  $v \in V_J$ , then  $sv \in G_{p'}$  and hence  $sv = {}_{V_J} s$  by (71.20). Then the right side of (71.22) becomes

$$|V_J|^{-1} m \cdot \mathrm{St}_G s,$$

where

$$m = \mathrm{card} \{sv \in sV_J : sv = {}_{V_J} s\}.$$

Now any  $V_J$ -conjugate of  $s$  can be written in the form

$$v_1 s v_1^{-1} = s(s^{-1} v_1 s v_1^{-1}),$$

where  $s^{-1} v_1 s v_1^{-1} \in V_J$  since  $s$  normalizes  $V_J$ . Thus  $m$  is the number of all  $V_J$ -conjugates of  $s$ , which equals

$$|V_J| |V_J \cap C_G(s)|^{-1}.$$

Upon substituting this information in (71.22), we obtain (71.21), as required.

*Step 3.* It is now sufficient to prove that for  $s$  as in Step 2, we have

$$(71.23) \quad |V_J \cap C_G(s)| = |C_G(s)|_p.$$

Since  $V_J$  is a  $p$ -group,  $|V_J \cap C_G(s)|$  clearly divides  $|C_G(s)|_p$ . On the other hand, since  $\mathrm{St}_G \in \mathrm{Irr} G$  by (67.10i), we have

$$(71.24) \quad \frac{|G : C_G(s)| \mathrm{St}_G s}{\mathrm{St}_G 1} = \frac{|G|_{p'}}{|C_G(s)|_{p'}} \cdot \frac{\mathrm{St}_G s}{|C_G(s)|_p}.$$

This is an algebraic integer, by (9.31). It also lies in  $\mathbb{Q}$  by (71.21), and hence is a rational integer. It follows that the  $p$ -part of (71.24) is also a rational integer, and hence  $|C_G(s)|_p$  divides  $\mathrm{St}_G s$ . This completes the proof of (71.23), and establishes the theorem.

## §72. MODULAR REPRESENTATIONS OF FINITE GROUPS OF LIE TYPE

### §72A. The Ballard-Lusztig Theorem on Characters of P.I.M.'s

Throughout this subsection,  $G$  denotes a finite group with a split  $BN$ -pair of characteristic  $p$ . We let  $W$  denote the Weyl group of  $G$ , and  $S$  the set of

distinguished generators of  $W$  (see §69A). The prime  $p$  is sometimes called the *natural characteristic* of  $G$ . Our aim is to present some aspects of the modular representation theory of  $G$ , with respect to a  $p$ -modular system  $(K, R, k)$ , such that  $\text{char } K = 0$  and  $K$  is sufficiently large relative to  $G$ . The first result is a remarkable theorem, proved by Ballard [76] and Lusztig [76] independently, which asserts that the  $K$ -characters afforded by P.I.M.'s in  $\mathcal{P}(RG)$  are all divisible by the Steinberg character  $\text{St}_G$ , in the ring  $\text{ch } G$  (see also Feit [76], for a related result). Our approach follows Broué [82], and is based on properties of the duality operation  $D_G$  established in §71.

We begin with some properties of the operations  $T_{L_I}^G$  and  $R_{L_I}^G$ , for  $I \subseteq S$ , similar to the identity (15.5), which states that  $\zeta \cdot \psi^G = (\zeta_H \cdot \psi)^G$  for all class functions  $\zeta \in \text{cf}_K G$ ,  $\psi \in \text{cf}_K H$ , where  $H \leq G$ . We first require the concept of  $p'$ -sections, which are the equivalence classes in  $G$  defined by the equivalence relation that puts  $x$  equivalent to  $x'$ , for  $x, x' \in G$ , if and only if their  $p'$ -parts are conjugate in  $G$ .

**(72.1) Lemma.** *Let  $\mu \in \text{cf}_K G$ , and suppose that  $\mu$  is constant on  $p'$ -sections. Let  $I \subseteq S$ , and let  $P_I = L_I V_I$  be the Levi decomposition of a standard parabolic subgroup  $P_I$  (see (69.10).) Then we have*

$$\mu(lv) = \mu(l) \quad \text{for all } l \in L_I, v \in V_I$$

*Proof.* By (71.20), we obtain

$$(lv)_{p'} = {}_G l_{p'} \quad \text{for all } l \in L_I, v \in V_I,$$

and the lemma follows.

**(72.2) Proposition.** *Let  $v \in \text{cf}_K G$ , and assume that  $v$  is constant on  $p'$ -sections. Then the following statements hold, for each subset  $I \subseteq S$ .*

$$(i) \quad T_{L_I}^G(\chi \cdot v) = (T_{L_I}^G \chi)(T_{L_I}^G v) \text{ for all } \chi \in \text{cf}_K G;$$

and

$$(ii) \quad R_{L_I}^G(\xi) \cdot v = R_{L_I}^G(\xi \cdot T_{L_I}^G v), \text{ for all } \xi \in \text{cf}_K L_I.$$

*Proof.* (i) We have

$$T_{L_I}^G v(l) = |V_I|^{-1} \sum_{v \in V_I} v(lv) \text{ for all } l \in L_I$$

by the definition of truncation (70.4). Using Lemma 72.1 it follows that  $T_{L_I}^G v = v$ , since  $v$  is constant on  $p'$ -sections. We then obtain

$$T_{L_I}^G(\chi \cdot v)(l) = |V_I|^{-1} \sum_{v \in V_I} \chi(lv)v(lv) = [|V_I|^{-1} \sum_{v \in V_I} \chi(lv)]v(l),$$

using (72.1). Since  $v = T_{L_I}^G v$  by the preceding remark, part (i) is proved.

For the proof of part (ii), we use the adjointness formula (70.6ii), extended to class functions. Then, for all  $\zeta \in \text{Irr } G$ , we have

$$(R_{L_I}^G(\xi \cdot T_{L_I}^G v), \zeta)_G = (\xi \cdot T_{L_I}^G v, T_{L_I}^G \zeta)_{L_I} = (\xi, T_{L_I}^G \bar{v} T_{L_I}^G \zeta)_{L_I}$$

where  $\bar{v}(x) = v(x^{-1})$  for  $x \in G$ . Since  $\bar{v}$  is also constant on  $p'$ -sections, we have

$$T_{L_I}^G \bar{v} \cdot T_{L_I}^G \zeta = T_{L_I}^G(\bar{v}\zeta)$$

by part (i). Applying the adjointness formula (70.6ii) again, we obtain

$$(R_{L_I}^G(\xi \cdot T_{L_I}^G v) - (R_{L_I}^G \xi) \cdot v, \zeta)_G = 0$$

for all  $\zeta \in \text{Irr } G$ , and part (ii) follows, since  $\text{Irr } G$  is a basis for  $\text{cf}_K G$ . This completes the proof.

We shall find it convenient to use the notation  $\text{cf}_K(G, G_{p'})$ , as in §63, to denote the set of class functions in  $\text{cf}_K G$  that vanish outside  $G_{p'}$ . We next define the *Brauer lift*  $\text{Br}_G$ , which is a  $K$ -homomorphism

$$\text{Br}_G : \text{cf}_K(G, G_{p'}) \rightarrow \text{cf}_K G$$

defined by

$$(72.3) \quad \text{Br}_G \varphi(x) = \varphi(s) \quad \text{for all } \varphi \in \text{cf}_K(G, G_{p'}),$$

where  $x \in G$ , and  $s$  is the  $p'$ -part of  $x$ . By Theorem 18.12,  $\text{Br}_G \varphi \in \text{ch } G$  whenever  $\varphi$  is a Brauer character, afforded by some  $kG$ -module. We also define a map  $\text{Br}_G^* : \text{cf}_K G \rightarrow \text{cf}_K(G, G_{p'})$  by setting

$$(72.4) \quad \text{Br}_G^* \mu(x) = \begin{cases} \sum_{u \in C_G(s)_p} \mu(su) & \text{if } x = s \in G_{p'}, \\ 0 & \text{if } x \notin G_{p'}, \end{cases}$$

where  $C_G(s)_p$  denotes the set of  $p$ -elements in the centralizer of  $s$ . As the notation suggests, we have:

**(72.5) Proposition.** *The maps  $\text{Br}_G$  and  $\text{Br}_G^*$  are transposes of each other with respect to the scalar product  $( , )_G$ .*

The proof is immediate from the definitions, and is omitted.

Now let  $D_G : \text{cf}_K G \rightarrow \text{cf}_K G$  be the duality operation, defined on  $\text{ch } G$  by (71.2), and extended by linearity to  $\text{cf}_K G$ . By (66.35), the Steinberg character of  $G$  is given by

$$\text{St}_G = D_G 1_G,$$

where  $1_G$  is the trivial character of  $G$ .

**(72.6) Theorem (Broué [82]).** Let  $\varphi \in \text{cf}_K(G, G_p)$  and  $\chi \in \text{cf}_K G$ . Then

$$(i) \quad \text{Br}_G \varphi = D_G(\text{St}_G \cdot \varphi)$$

and

$$(ii) \quad \text{Br}_G^* \chi = \text{St}_G \cdot D_G \chi.$$

*Proof.* (i) For each class function  $\varphi \in \text{cf}_K(G, G_p)$ ,  $\text{Br}_G \varphi$  is constant on  $p'$ -sections, by its definition (72.3). We also have

$$T_{L_I}^G \text{Br}_G \varphi = \text{Br}_G \varphi \text{ for all } I \subseteq S,$$

by the proof of (72.2i). It follows that

$$R_{L_I}^G T_{L_I}^G (\chi \cdot \text{Br}_G \varphi) = R_{L_I}^G ((T_{L_I}^G \chi) \cdot \text{Br}_G \varphi) = (R_{L_I}^G T_{L_I}^G \chi) \text{Br}_G \varphi$$

for all  $I \subseteq S$  and  $\chi \in \text{cf}_K G$ , by (72.2i) and (72.2ii). Since

$$D_G \chi = \sum_{I \subseteq S} (-1)^{|I|} R_{L_I}^G T_{L_I}^G \chi,$$

we obtain

$$D_G(\chi \cdot \text{Br}_G \varphi) = (D_G \chi) \text{Br}_G \varphi, \quad \text{for } \varphi \in \text{cf}_K(G, G_p) \quad \text{and} \quad \chi \in \text{cf}_K G.$$

Setting  $\chi = 1_G$ , the preceding formula becomes

$$D_G(\text{Br}_G \varphi) = \text{St}_G \text{Br}_G \varphi.$$

Now apply  $D_G$  to both sides of this equation. The result is that

$$\text{Br}_G \varphi = D_G^2 \text{Br}_G \varphi = D_G(\text{St}_G \text{Br}_G \varphi) = D_G(\text{St}_G \varphi)$$

since  $D_G^2 = \text{id}$  by (71.7), and  $\text{St}_G \text{Br}_G \varphi = \text{St}_G \cdot \varphi$  using the fact that  $\text{St}_G$  vanishes on  $p$ -irregular elements, by (71.19). This completes the proof of part (i).

(ii) First let  $\xi \in \text{cf}_K(G, G_p)$ . Then, for all  $\chi \in \text{cf}_K G$ ,

$$(\text{Br}_G^* \chi, \xi) = (\chi, \text{Br}_G \xi) = (\chi, D_G(\text{St}_G \cdot \xi)) = (D_G \chi, \text{St}_G \cdot \xi) = (D_G \chi \cdot \text{St}_G, \xi)$$

using part (i), (72.5), (71.7), and the fact that  $\text{St}_G$  is rational valued by (71.19). On the other hand,  $\text{Br}_G^* \chi$  and  $D_G \chi \cdot \text{St}_G$  both vanish on  $G - G_{p'}$ , by (72.4) and (71.19). It follows that

$$(\text{Br}_G^* \chi - D_G \chi \cdot \text{St}_G, \zeta) = 0 \text{ for all } \zeta \in \text{Irr } G,$$

and hence  $\text{Br}_G^* \chi = D_G \chi \cdot \text{St}_G$ , completing the proof.

Notice that part (i) of the preceding theorem gives an interesting interpretation

of the Brauer lift  $\text{Br}_G \varphi$ . We shall concentrate on an application of part (ii), which is based on some additional properties of the Cartan-Brauer triangle (18.5). Let  $\text{Bch } G$  denote the set of virtual Brauer characters; thus a class function  $\xi$  belongs to  $\text{Bch } G$  if and only if  $\xi$  is a  $\mathbb{Z}$ -linear combination of Brauer characters afforded by  $kG$ -modules. By (17.15), there is a commutative diagram

$$\begin{array}{ccc} G_0(KG) & \longrightarrow & \text{ch } G \\ d \downarrow & & \downarrow d' \\ G_0(kG) & \longrightarrow & \text{Bch } G \end{array}$$

where the horizontal maps are isomorphisms,  $d$  is the decomposition map, and  $d'$  is the restriction map  $\psi \rightarrow \psi|_{G_p}$ .

We denote by  $\text{Pch } G$  the  $\mathbb{Z}$ -module generated by the Brauer characters of the P.I.M.'s in  $\mathcal{P}(kG)$ . Then  $\text{Pch } G \subseteq \text{Bch } G$ , and there exists a commutative diagram

$$\begin{array}{ccc} K_0(kG) & \longrightarrow & \text{Pch } G \\ c \downarrow & & \downarrow c' \\ G_0(kG) & \longrightarrow & \text{Bch } G \end{array}$$

where  $c$  is the Cartan map (18.4),  $c'$  is the identity map, and the horizontal maps are isomorphisms.

There is also a commutative diagram

$$\begin{array}{ccc} K_0(kG) & \longrightarrow & \text{Pch } G \\ e \downarrow & & \downarrow e' \\ G_0(KG) & \longrightarrow & \text{ch } G \end{array}$$

where  $e$  is defined by (18.3), the horizontal maps are isomorphisms, and  $e'$  is defined as follows. Let  $\{P_1, \dots, P_r\}$  be a basic set of indecomposable projective  $RG$ -modules, and let  $\{\tau_1, \dots, \tau_r\}$  be the  $K$ -characters afforded by them.

Let  $U_i = \bar{P}_i$ , for  $1 \leq i \leq r$ . Then  $\{U_1, \dots, U_r\}$  is a basic set of P.I.M.'s in  $\mathcal{P}(kG)$ . Their Brauer characters  $\{\eta^i : 1 \leq i \leq r\}$  form a  $\mathbb{Z}$ -basis of  $\text{Pch } G$ , and we have  $\eta^i = \tau_i|_{G_p}$ , for  $1 \leq i \leq r$ . The map  $e'$  is defined on the basis of  $\text{Pch } G$  consisting of the Brauer characters  $\{\eta^i\}$  by the rule

$$(72.7) \quad e' \eta^i = \tau_i, \quad 1 \leq i \leq r.$$

Using (18.5) and the preceding remarks, we obtain a commutative diagram

$$(72.8) \quad \begin{array}{ccc} \text{ch } G & \xrightarrow{d'} & \text{Bch } G \\ e' \swarrow & & \searrow c' \\ \text{Pch } G & & \end{array}$$

which will also be called the *Cartan-Brauer triangle*.

For the rest of the discussion, it will be convenient to regard  $\text{Bch } G$  and  $\text{Pch } G$  as  $\mathbb{Z}$ -submodules of  $\text{cf}_K(G, G_p)$ . We then have:

**(72.9) Proposition.** *Let  $\eta \in \text{Pch } G$  and  $\chi \in \text{ch } G$ . Then*

$$(\eta, d' \chi)_G = (e' \nu, \chi)_G.$$

*Proof.* It is sufficient to consider the special case of a basis element  $\eta^i$  of  $\text{Pch } G$ , as in (72.7), and a basis element  $\zeta^i$  of  $\text{ch } G$ , where  $\zeta^i \in \text{Irr } G$ . Then

$$(\eta^i, d' \zeta^j) = \left( \eta^i, \sum_{l=1}^r d_{jl} \varphi^l \right) = d_{ji}$$

by (18.23i), while

$$(e' \eta^i, \zeta^j) = (\tau_i, \zeta^j) = d_{ji}$$

by (18.26i). This completes the proof.

We can now state the main result.

**(72.10) Theorem (Ballard [76], Lusztig [76]).** *For every virtual projective character  $\eta \in \text{Pch } G$ , we have*

$$\eta = \text{St}_G \cdot \mu \text{ for some } \mu \in \text{ch } G.$$

*In other words,  $\text{Pch } G$  is a principal ideal in  $\text{ch } G$  generated by  $\text{St}_G$ .*

*Proof.* By the definition of the maps  $d'$  and  $\text{Br}_G$ , we have

$$d' \text{Br}_G = \text{id} \quad \text{on } \text{Pch } G.$$

Taking transposes with respect to the scalar product  $(\ , \ )_G$ , and using (72.9) and (72.5), the preceding formula yields

$$\text{Br}_G^* e' = \text{id} \quad \text{on } \text{Pch } G.$$

This implies that the map  $\text{Br}_G^*$  defines a surjection

$$\text{Br}_G^*: \text{ch } G \rightarrow \text{Pch } G.$$

Now let  $\eta \in \text{Pch } G$ . Then

$$\eta = \text{Br}_G^* \chi = \text{St}_G \cdot D_G \chi$$

for some  $\chi \in \text{ch } G$ , by (72.6) and the fact that  $\text{Br}_G^*$  is surjective. Moreover,  $D_G \chi \in \text{ch } G$  whenever  $\chi \in \text{ch } G$ . This completes the proof.

**Remark.** By (67.10) and (69.9),  $\text{St}_G$  is an irreducible character of  $G$  whose degree is the  $p$ -part  $|G|_p$  of the order of  $G$ . By (56.31),  $\text{St}_G$  belongs to a  $p$ -block of  $G$  of defect zero, and is afforded by an  $RG$ -lattice  $P \in \mathcal{P}(RG)$  with the property that  $\bar{P} = P/\mathfrak{p}P$  is a P.I.M. in  $\mathcal{P}(kG)$ , and is also a simple  $kG$ -module. An explicit construction of a primitive idempotent  $e \in kG$  such that  $kGe \cong \bar{P}$  was given by Steinberg ([56], [57]).

## §72B. The Simple $kG$ -Modules

As in §72A,  $G$  denotes a finite group with a split  $BN$ -pair of characteristic  $p$ , and  $k$  a field of characteristic  $p$  that is sufficiently large relative to  $G$ . Our objective is to classify the simple  $kG$ -modules, in the natural characteristic  $p$ . We shall present a direct approach to the problem, based on the work of Richen [69] and Curtis [65], [70], and recent contributions involving modular Hecke algebras by Carter-Lusztig [76], Sawada [77], Tinberg [79], [80b], Green [78b], and Cabanes. For related results, see Norton [79]. In case  $G = G(\mathbb{F}_q)$  is the group of  $\mathbb{F}_q$ -rational points on a connected reductive affine algebraic group  $\mathbf{G}$ , the simple  $kG$ -modules can also be classified using the rational characters of a maximal torus of  $\mathbf{G}$  (see Borel [70] or Steinberg [67]).

In spite of these efforts, the problem of calculating the Brauer characters of the simple  $kG$ -modules, or even their degrees, remains unsolved at this time. A conjecture concerning the Brauer characters has been made by Lusztig [80].

We shall use the notation from §§65 and 69. In particular,  $B$  denotes a fixed Borel subgroup of  $G$ ,  $U = O_p(G)$ , and  $T = N \cap B$ . We assume that  $T = \bigcap_{n \in N} {}^n B$ , and that  $T$  is an abelian  $p'$ -group (see (69.1)). As usual,  $W$  denotes the Weyl group  $N/T$ , and  $S = \{s_1, \dots, s_l\}$  denotes the set of distinguished generators of  $W$ . Let  $\Delta$  be a root system associated with  $W$ , and  $\{U_\alpha : \alpha \in \Delta\}$  the corresponding root subgroups of  $G$  (see (69.2)), ordered so that  $U$  is generated by the root subgroups  $\{U_\alpha : \alpha \in \Delta_+\}$ , and the involutions  $s_i \in S$  are the fundamental reflections with respect to a set of fundamental roots  $\Pi = \{\alpha_1, \dots, \alpha_l\}$  in  $\Delta_+$ .

For each subset  $I \subseteq S$ ,  $W_I$  denotes the parabolic subgroup of  $W$  generated by the reflections belonging to  $I$ .

**(72.11) Lemma.** *Let  $L$  be a simple  $kB$ -module. Then  $\dim_k L = 1$ , and  $U$  acts trivially on  $L$ .*

*Proof.* Since  $U = O_p(B) \trianglelefteq B$ , the restriction  $L_U$  is a semisimple  $kU$ -module, by Clifford's Theorem 11.1. Then  $U$  acts trivially on  $L$  by (5.24), since  $U$  is a  $p$ -group and  $\text{char } k = p$ . It follows that  $L$  is a simple  $k(B/U)$ -module, and hence  $\dim L = 1$ , using the facts that  $B/U \cong T$  is an abelian  $p'$ -group, and  $k$  is sufficiently large. This completes the proof.

**(72.12) Corollary.** *Let  $M$  be a simple  $kG$ -module. Then  $\text{inv}_U M \neq 0$ , and there exists a surjection of  $kG$ -modules  $(1_U)^G \rightarrow M$ .*

*Proof.* Let  $L$  be a simple  $kB$ -submodule of  $M_B$ . Then  $U$  acts trivially on  $L$ ,

by (72.11), so  $\text{inv}_U M \neq 0$ . By the Frobenius Reciprocity Theorem 10.8, we obtain

$$\text{Hom}_{kG}((1_U)^G, M) \cong \text{Hom}_{kU}(1_U, M) \cong \text{inv}_U M \neq 0,$$

and the result follows, since  $M$  is a simple  $kG$ -module.

By (72.12), every simple  $kG$ -module occurs as a composition factor of  $(1_U)^G$ , so it is natural to classify them in terms of representation of  $\text{End}_{kG}(1_U)^G$ , as in §11D. We now introduce some of the notation and basic ideas needed to carry out this plan. Let  $k_U$  denote the field  $k$ , viewed as a  $kU$ -module on which  $U$  acts trivially. Throughout this subsection, we shall set

$$Y = kG \otimes_{kU} k_U, \quad \text{and} \quad E = (\text{End}_{kG} Y)^\circ \text{ (opposite ring)}.$$

We may identify  $Y$  with the induced module  $(1_U)^G$ , and note that  $Y$  is a cyclic  $kG$ -module, generated by  $1 \otimes 1$ . The  $k$ -algebra  $E$  is called the *modular Hecke algebra*, and is taken as a  $k$ -algebra of right operators on  $Y$ , so that  $Y$  is a  $(kG, E)$ -bimodule. In contrast to §11D, it is no longer true, in this case, that  $E$  is a semisimple  $k$ -algebra.

**(72.13) Proposition** (i) *A  $k$ -basis of the modular Hecke algebra  $E$  consists of the elements  $\{a_n : n \in N\}$ , whose action on  $Y$  is given by the formulas*

$$(1 \otimes 1)a_n = \sum_{u \in U/U \cap {}^n U} un \otimes 1, \quad (g \otimes 1)a_n = g((1 \otimes 1)a_n)$$

for all  $n \in N$  and  $g \in G$ , where, as usual,  $u \in U/U \cap {}^n U$  means that the sum is taken over a cross section of the left cosets  $U/U \cap {}^n U$ .

(ii) *Let  $M$  be an arbitrary f.g. left  $kG$ -module. Then  $\text{inv}_U M \neq 0$ , and there exists a left action of  $E$  on  $\text{inv}_U M$ , given by*

$$a_n m = \sum_{u \in U/U \cap {}^n U} unm, \quad m \in \text{inv}_U M,$$

for each basis element  $a_n$  of  $E$  defined in part (i).

*Proof.* (i) The additive structure of  $E$  is described by the Frobenius Reciprocity Theorem 10.8, which asserts that there is an isomorphism of  $k$ -spaces

$$(72.14) \quad \text{End}_{kG} Y \cong \text{Hom}_{kU}(k_U, Y).$$

The elements of  $N$  form a cross section of the double cosets  $U \backslash G / U$ , by the sharp form of the Bruhat decomposition (69.2v). This yields a direct decomposition.

$$\text{Hom}_{kU}(k_U, Y) \cong \bigoplus_{n \in N} \text{Hom}_{kU}(k_U, kUnU \bigotimes_{kU} k_U),$$

where the sum is taken over the cross section  $N$  of  $U \backslash G/U$ , and  $kUnU$  denotes the  $k$ -space generated by the elements of the double coset  $UnU$ . Each subspace  $\text{Hom}_{kU}(k_U, kUnU \otimes_{kU} k)$  is one-dimensional, and is generated by an element  $f_n$  such that

$$f_n(1) = \sum_{u \in U/U \cap {}^n U} un \otimes 1 \quad (\text{for each } n \in N).$$

The isomorphism (72.14) is described explicitly in the proof of the Adjointness Theorem 2.19 (see also the proof of (10.8).) Let  $a_n \in E$  be the element corresponding to  $f_n$  in (72.14). Then we have

$$(1 \otimes 1)a_n = \sum_{u \in U/U \cap {}^n U} un \otimes 1, \quad \text{for each } n \in N,$$

by the proof of (2.19). Since  $Y$  is a cyclic  $kG$ -module with generator  $1 \otimes 1$ , and each endomorphism  $a_n$  commutes with the action of  $kG$ , the maps  $\{a_n : n \in N\}$  are uniquely determined by their action on  $1 \otimes 1$ , completing the proof of part (i).

(ii) Since  $Y$  is a  $(kG, E)$ -bimodule, there exists a left action of  $E$  on  $\text{Hom}_{kG}(Y, M)$  given by composition:

$$a \cdot f = f \circ a \quad \text{for } a \in E \quad \text{and} \quad f \in \text{Hom}_{kG}(Y, M),$$

for any left  $kG$ -module  $M$ . Moreover, there exist isomorphisms of  $k$ -spaces

$$\text{Hom}_{kG}(Y, M) \cong \text{Hom}_{kU}(k_U, M_U) \cong \text{inv}_U M,$$

using (10.8). It follows that there exists also a left action of  $E$  on  $\text{inv}_U M$ , which is given by

$$a_n m = \sum_{u \in U/U \cap {}^n U} unm, \quad \text{for } m \in \text{inv}_U M \quad \text{and} \quad n \in N.$$

To verify the last statement, each element  $m \in \text{inv}_U M$  corresponds to a map  $f_m \in \text{Hom}_{kU}(k_U, M_U)$  such that  $f_m(1) = m$ . By the proof of (2.19), the map  $\varphi_m \in \text{Hom}_{kG}(Y, M)$  corresponding to  $f_m$  is given by

$$\varphi_m(g \otimes 1) = gm, \quad \text{for } g \in G.$$

Then  $a_n \varphi_m$  acts on  $1 \otimes 1$  according to the rule

$$\begin{aligned} a_n \varphi_m(1 \otimes 1) &= \varphi_m \circ a_n(1 \otimes 1) = \sum_{u \in U/U \cap {}^n U} \varphi_m(un \otimes 1) \\ &= \sum_{u \in U/U \cap {}^n U} unm. \end{aligned}$$

To finish the proof of (ii), we need only verify that  $\text{inv}_U M \neq 0$ , and this is part of (72.12).

We turn next to the multiplicative structure of the modular Hecke algebra  $E$ , after some preliminary discussion. We let  $\pi$  denote the natural map  $N \rightarrow N/T = W$ , and use it to define a length function on  $N$ , setting

$$l(n) = l(\pi(n)) = l(w) \quad \text{if } \pi(n) = w \in W,$$

where  $w \rightarrow l(w)$  is the usual length function on the Weyl group  $W$ . Note that  $l(n) = 0$  if and only if  $n \in T$ . In what follows, we shall often set  $U_i = U_{\alpha_i}$ , for  $\alpha_i \in \Pi$ , and  $U_i^* = U_i - \{1\}$ .

**(72.15) Lemma.** (*Structure equations in  $G$ .*) *Let  $n_i \in N$  be an element of length one, with  $\pi(n_i) = s_i \in S$ , for  $1 \leq i \leq l$ . Then there exist maps  $f_i: U_i^* \rightarrow U_i^*$ ,  $t_i: U_i^* \rightarrow T$ , and  $g_i: U_i^* \rightarrow U_i^*$ , which depend on the choice of  $n_i$ , and satisfy*

$$n_i u n_i = f_i(u) t_i(u) n_i g_i(u) \quad \text{for all } u \in U_i^*.$$

*Proof.* By (69.2vi),

$$G_i = U_i T \cup U_i T n_i U_i$$

is a subgroup of  $G$ , and clearly has a split  $BN$ -pair of rank 1. For each element  $u \in U_i^*$ , we have  $n_i u n_i \in U_i T n_i U_i$ , otherwise  $n_i u n_i \in U_i T$  by the Bruhat decomposition of  $G_i$ , and we contradict the fact that  $U^- \cap B = 1$  (see (69.2i)). It then follows easily, using the Bruhat decomposition in  $G_i$ , that the maps  $f_i$ ,  $t_i$ , and  $g_i$  exist, as stated in the lemma.

**(72.16) Proposition.** *The basis elements  $\{a_n : n \in N\}$  of the modular Hecke algebra  $E$  are multiplied as follows:*

$$a_t a_n = a_{tn} \quad \text{and} \quad a_n a_t = a_{nt} \quad \text{for all } n \in N, t \in T.$$

$$a_{n_i} a_n = a_{n_i n} \quad \text{if } l(n_i) = 1 \quad \text{and} \quad l(n_i n) \geq l(n)$$

$$a_{n_i} a_n = \sum_{u \in U_i^*} a_{t_i(u)} a_n \quad \text{if } l(n_i) = 1 \quad \text{and} \quad l(n_i n) < l(n)$$

where  $\{t_i(u) : u \in U_i^*\}$  are the elements of  $T$  determined by the structure equations (72.15) involving the element  $n_i \in N$ .

*Proof.* In this proof, and for the rest of this section it will be convenient to use the notation

$$(72.17) \quad \sigma(X) = \sum_{x \in X} x \quad \text{for } X \subseteq G,$$

where the sum is taken in the group algebra  $kG$ . We first observe that if  $n \in N$  and  $\pi(u) = w \in W$ , then  $U \cap {}^n U = U_w^{+,-1}$ , and hence  $U_w^{-1}$  is a cross section of

$U/U \cap {}^n U$ , by (69.2ii)). Accordingly we may write

$$(1 \otimes 1)a_n = \sigma(U_{w^{-1}})n \otimes 1$$

in the equation defining  $a_n$ , using the notation (72.17). In particular, we have

$$(1 \otimes 1)a_t = t \otimes 1 \quad \text{for } t \in T$$

since  $\pi(t) = 1$  and  $U_1^- = 1$ . Now let  $n \in N$  and  $\pi(n) = w$ . Then we obtain, for  $t \in T$ ,

$$\begin{aligned} (1 \otimes 1)a_t a_n &= (t \otimes 1)a_n = t((1 \otimes 1)a_n) = t\sigma(U_{w^{-1}})n \otimes 1 \\ &= \sigma(U_{w^{-1}})tn \otimes 1 = (1 \otimes 1)a_{tn}, \end{aligned}$$

using the preceding formulas, and the facts that  $a_n$  commutes with the action of  $kG$ ,  $\pi(tn) = \pi(n) = w$ , and  $t\sigma(U_{w^{-1}})t^{-1} = \sigma(U_{w^{-1}})$  since  $T$  normalizes  $U_{w^{-1}}$  (see §69A). As in the proof of (72.13i), it follows that

$$a_t a_n = a_{tn}$$

since  $Y$  is a cyclic  $kG$ -module. A similar argument proves that  $a_n a_t = a_{nt}$ .

Next we assume that  $l(n_i) = 1$  so  $\pi(n_i) = s_i \in S$ , and consider an element  $n \in N$  such that  $\pi(n) = w$  and  $l(s_i w) \geq l(w)$ . Then we obtain

$$\begin{aligned} (1 \otimes 1)a_{n_i} a_n &= (\sigma(U_i)n_i \otimes 1)a_n = \sigma(U_i)n_i \sigma(U_{w^{-1}})n \otimes 1 \\ &= \sigma(U_i)\sigma(s_i U_{w^{-1}})n_i n \otimes 1 = \sigma(U_{w^{-1}s_i})n_i n \otimes 1 \\ &= (1 \otimes 1)a_{n_i n}. \end{aligned}$$

Here we have used the fact that  $\sigma(U_i)\sigma(s_i U_{w^{-1}}) = \sigma(U_{w^{-1}s_i})$ , since  $U_{w^{-1}s_i} = U_{\alpha_i} s_i U_{w^{-1}}$  and  $U_{\alpha_i} \cap s_i U_{w^{-1}} = 1$  if  $l(s_i w) > l(w)$ , by (69.8). It follows that  $a_{n_i} a_n = a_{n_i n}$ , proving the second statement in (72.16).

For the proof of the third formula in (72.16), we first consider  $a_{n_i}^2$ . We have

$$\begin{aligned} (1 \otimes 1)a_{n_i}^2 &= \sigma(U_i)n_i \sigma(U_i)n_i \otimes 1 \\ &= \sigma(U_i)n_i^2 \otimes 1 + \sigma(U_i) \sum_{u \in U_i^*} f_i(u)t_i(u)n_i g_i(u) \otimes 1 \\ &= \sigma(U_i) \sum_{u \in U_i^*} t_i(u)n_i \otimes 1 = (1 \otimes 1) \sum_{u \in U_i^*} a_{t_i(u)n_i} \end{aligned}$$

using the structure equations (72.15) involving  $n_i$ , and the fact that  $\sigma(U_i)n_i^2 \otimes 1 = |U_i|(n_i^2 \otimes 1) = 0$  in  $k$ , since  $n_i^2 \in T$ . It follows that

$$a_{n_i}^2 = \sum_{u \in U_i^*} a_{t_i(u)n_i}$$

Now let  $l(n_i) = 1$  and assume that  $l(n_i n) < l(n)$ . Put  $n' = n_i n$ ; then  $n = n_i^{-1}n'$  and

$l(n_i^{-1}n') \geq l(n')$ . Consequently

$$a_n = a_{n_i^{-1}}a_{n'} = a_{n_i}a_t a_{n'} \quad \text{if } n_i^{-1} = n_i t, \quad t \in T,$$

using the preceding results. Multiplication by  $a_{n_i}$  yields

$$\begin{aligned} a_{n_i}a_n &= a_{n_i}^2 a_t a_{n'} = \sum_{u \in U_i^*} a_{t_i(u)} a_{n_i} a_t a_{n'} \\ &= \sum_{u \in U_i^*} a_{t_i(u)} a_{n_i^{-1}} a_{n'} = \sum_{u \in U_i^*} a_{t_i(u)} a_{n'}, \end{aligned}$$

completing the proof.

**(72.18) Corollary.** *Let  $X$  be a simple  $E$ -module. Then  $\dim_k X = 1$ .*

*Proof.* By (72.16), the subalgebra  $E_T$  of  $E$  generated by the elements  $\{a_t : t \in T\}$  is isomorphic to the group algebra  $kT$ , which is a commutative split semisimple  $k$ -algebra, by our assumptions on  $T$  and  $k$ . It follows that  $X|_{E_T}$  is a semisimple  $E_T$ -module, and the simple submodules are all one-dimensional. Moreover, if  $\langle x \rangle$  is a simple  $E_T$ -submodule of  $X|_{E_T}$  and  $n \in N$ , then  $a_n \langle x \rangle$  is another simple  $E_T$ -module or zero, since  $T \trianglelefteq N$  and

$$a_t a_n = a_{tn} = a_n a_{ntn^{-1}}$$

by (72.16). Now let  $\langle x_0 \rangle$  be a fixed simple  $E_T$ -submodule of  $X|_{E_T}$ , and let  $n \in N$  be an element of maximal length such that  $a_n x_0 \neq 0$ . Then  $\langle a_n x_0 \rangle$  is an  $E_T$ -submodule, and it follows from (72.16) that  $\langle a_n x_0 \rangle$  is an  $E$ -submodule of  $X$ . Since  $X$  is simple, we have  $X = \langle a_n x_0 \rangle$ . Therefore  $\dim_k X = 1$ , as required.

**(72.19) Proposition.** *Let  $M$  be an arbitrary f.g.  $kG$ -module, and let  $\langle m \rangle$  be a simple (and hence one-dimensional)  $E$ -submodule of  $\text{inv}_U M$ . Then we have*

$$kGm = kU^-m,$$

where  $U^- = {}^{w_0}U$  (see §69A).

*Proof.* By (72.13),  $\text{inv}_U M$  is a nonzero  $E$ -module, and its simple  $E$ -submodules are one-dimensional, by (72.18). By (72.13ii), the action of any element  $t \in T$  on  $\text{inv}_U M$  is the same as the action of the corresponding element  $a_t \in E$ . Therefore a simple  $E$ -submodule  $\langle m \rangle$  of  $\text{inv}_U M$  is a  $kB$ -submodule of  $M_B$ . The result that  $kGm = kU^-m$  will follow if we can prove that  $nm \in kU^-m$  for all  $n \in N$ , since

$$G = n_0 G = \bigcup_{n \in N} U^- n B \quad \text{where } \pi(n_0) = w_0,$$

by the Bruhat decomposition. We begin with an element  $n_i \in N$  of length 1. Then

$a_{n_i}m = \mu_i m$  for some  $\mu_i \in k$ . On the other hand, using (72.13) and (72.15), we obtain

$$\begin{aligned} a_{n_i}m &= \mu_i m = n_i m + \sum_{u \in U_i^*} u n_i m \\ &= n_i m + \sum_{u \in U_i^*} n_i^{-1}(n_i u n_i) m \\ &= n_i m + \sum_{u \in U_i^*} n_i^{-1} f_i(u) t_i(u) n_i g_i(u) m. \end{aligned}$$

From this it follows that  $n_i m \in kU_{-\alpha_i}m$ , since  ${}^{n_i}U_i = U_{-\alpha_i}$ . Now let  $n \in N$  be an element such that  $l(n) > 1$ , and write  $n = n' n_i$  for some elements  $n_i$  and  $n'$  with  $l(n_i) = 1$  and  $l(n') < l(n)$ . By the preceding argument, we have

$$nm = n' n_i m \in n' kU_{-\alpha_i} m,$$

and the result follows by induction on  $l(n)$ , since  $n' U_{-\alpha_i}(n')^{-1} \subseteq U^-$  from the results in §69A. This completes the proof.

We are ready to begin the classification of the simple  $kG$ -modules  $M$ . In the next result, we shall prove that  $\text{inv}_U M$  is a simple, and hence one-dimensional,  $E$ -module. In particular,  $\text{inv}_U M$  is a simple  $kB$ -submodule of  $M_B$ , and affords a linear representation  $\chi \in \text{Hom}(B, k^\times)$ , where  $k^\times$  is the multiplicative group of the field  $k$ . By analogy with the representation theory of semisimple algebraic groups or Chevalley groups (see Steinberg [67] or Borel [70]), we might expect the simple  $kG$ -modules  $M$  to be determined up to isomorphism by the homomorphism  $\chi \in \text{Hom}(B, k^\times)$  afforded by  $\text{inv}_U M$ . But this is not true, in general. For example, the group  $SL_2(\mathbb{F}_p)$  has a simple module of dimension  $p$  over an algebraically closed field of characteristic  $p$ , corresponding to the Steinberg character (see §67 or §18C). In this module, and in the trivial module, the subspaces of fixed points under the action of a Sylow  $p$ -subgroup  $U$  both afford the trivial representation of the Borel subgroup  $B$  containing  $U$ , but of course the modules are not isomorphic. The modules are distinguished, however, by the simple  $E$ -modules defined by the spaces of fixed elements under the action of  $U$ . We shall prove that this situation holds in the general case, by a method which still preserves some analogy with the algebraic group case. A different approach, based on the observation that the modular Hecke algebra  $E$  is a quasi-Frobenius algebra, has been given by Green, Sawada, and Tinberg (see the references at the beginning of §72B).

**(72.20) Theorem.** *Let  $M$  be a simple  $kG$ -module. Then  $\text{inv}_U M$  is a simple, and hence one-dimensional,  $E$ -module. Two simple  $kG$ -modules  $M_1$  and  $M_2$  are isomorphic if and only if there exists an isomorphism of  $E$ -modules:  $\text{inv}_U M_1 \cong \text{inv}_U M_2$ .*

*Proof.* Let  $M$  be a simple  $kG$ -module, and let  $\langle m \rangle$  be a simple  $E$ -submodule of  $\text{inv}_U M$ . Using the fact that  $M$  is simple, we have  $M = kU^- m$ , by (72.19). Since  $U$  is a  $p$ -group, we have  $kU^- = k \oplus \text{rad } kU^-$ , and  $\text{rad } kU^-$  is generated

by the elements  $\{u - 1 : u \in U\}$  (see (5.24)). Then  $M = km \oplus \text{rad } kU^-m$ , and in order to prove the first statement of the theorem, it is enough to show that  $\text{rad } kU^-m \cap \text{inv}_U M = 0$ .

Assume, to the contrary, that  $X = \text{rad } kU^-m \cap \text{inv}_U M \neq 0$ . We shall prove that  $X$  is an  $E$ -submodule of  $\text{inv}_U M$ . Since  $X$  is clearly stabilized by the action of  $T$ , and hence by the elements  $\{a_t : t \in T\}$ ,  $X$  is an  $E$ -module if we can prove that  $a_{n_i}X \subseteq X$  for all elements  $n_i \in N$  of length 1. From the action of  $a_{n_i}$  on  $\text{inv}_U M$ , this will follow from the result that  $\sigma(U_i)n_i \text{rad } kU^-m \subseteq \text{rad } kU^-m$ . Since  $M = km + \text{rad } kU^-m$ , it is enough to prove

$$(72.21) \quad \sigma(U_i)n_i(u - 1)m \in \text{rad } kU^-M, \quad \text{for all } u \in U^- \quad \text{and} \quad l(n_i) = 1.$$

We have  $\sigma(U_i)n_i m = a_{n_i}m = \mu_i m$  for some  $\mu_i \in k$ , since  $\langle m \rangle$  is an  $E$ -module. Then for  $u \in U^-$ ,

$$\sigma(U_i)n_i(u - 1)m = \sigma(U_i)n_i um - \mu_i m = n_i \sigma(U_{-\alpha_i})um - \mu_i m,$$

since  $n_i^{-1}U_i n_i = U_{-\alpha_i}$ . For each element  $u \in U^-$ , and  $u_i \in U_{-\alpha_i}$ , we have

$$u_i u = v_i u'_i \quad \text{where } v_i \in V_i, \quad u' \in U_{-\alpha_i},$$

and  $V_i$  is the subgroup of  $U^-$  generated by the root subgroups  $\{U_{-\alpha} : \alpha \in \Delta_+, \alpha \neq \alpha_i\}$ . Moreover, the map  $u_i \rightarrow u'_i$ , for fixed  $u \in U'$ , is a permutation of  $U_{-\alpha_i}$ . Both of these facts follow from the factorization, with uniqueness of expression,  $U^- = U_{-\alpha_i}V_i = V_iU_{-\alpha_i}$  (see §69A). Returning to our calculation of (72.21), we obtain

$$n_i \sigma(U_{-\alpha_i})um - \mu_i m = \sum_{u'_i \in U_{-\alpha_i}} n_i v_i u'_i m - \mu_i m,$$

where the  $\{v_i\}$  are some elements of  $V_i$ . Upon writing each  $v_i = 1 + (v_i - 1)$ , this expression becomes

$$\sigma U_i n_i m - \mu_i m + \sum_{v_i} n_i(v_i - 1)n_i^{-1}n_i u'_i m.$$

The first term is zero, while the second is in  $\text{rad } kU^-M$  since  $n_i V_i n_i^{-1} \leq U^-$ , by (69.2.iii). This completes the proof of (72.21), and shows that  $X$  is an  $E$ -submodule of  $\text{inv}_U M$ . Letting  $\langle m' \rangle$  be a simple  $E$ -submodule of  $X$ , it follows from (72.19) that  $M = kGm' = kU^-m' \subseteq \text{rad } kU^-M$ , which is impossible since  $\text{rad } kU^-$  is a nilpotent ideal in  $kU^-$ . Thus  $X$  must be zero. This completes the proof that  $\text{inv}_U M$  is a simple  $E$ -module.

Now let  $M_1$  and  $M_2$  be simple  $kG$ -modules. If  $M_1 \cong M_2$ , then it follows easily, using the first part of the proof, that there exists an isomorphism of  $E$ -modules  $\text{inv}_U M_1 \cong \text{inv}_U M_2$ . For the converse, we assume that  $\text{inv}_U M_1 \cong \text{inv}_U M_2$  as  $E$ -modules. Let  $\text{inv}_U M_1 = \langle m_1 \rangle$  and  $\text{inv}_U M_2 = \langle m_2 \rangle$ . Consider the direct sum  $M = M_1 \oplus M_2$ , and let  $\pi_i$ ,  $i = 1, 2$ , be the resulting projections of  $kG$ -modules. Let  $m = m_1 + m_2 \in M$ ; then  $\langle m \rangle$  is a simple  $E$ -submodule of  $\text{inv}_U M$

that is isomorphic to  $\langle m_1 \rangle$  and  $\langle m_2 \rangle$ . Then  $kGm = kU^-m$  by (12.19),  $\pi_i m = m_i$  for  $i = 1, 2$ , and the projections restrict to surjective  $kG$ -maps  $\pi_i: kGm \rightarrow M_i$ ,  $i = 1, 2$ , because  $M_1$  and  $M_2$  are simple modules. We shall prove that  $\pi_1: kGm \rightarrow M_1$  is an isomorphism. We have  $\ker \pi_1 \cap kGm \subseteq M_2 \cap kGm$ , and  $M_2 \cap kGm$  is either 0 or  $M_2$ . It follows that  $\pi_1: kGm \rightarrow M_1$  is an isomorphism if we can prove that  $m_2 \notin M_2 \cap kGm$ . Suppose, to the contrary, that  $m_2 \in M_2 \cap kGm$ ; then  $m_2 = \xi m + m'$  for  $\xi \in k$  and  $m' \in \text{rad } kU^-m$ . Upon applying  $\pi_1$  and  $\pi_2$  to this expression, we obtain

$$0 = \xi m_1 + \pi_1 m' \quad \text{and} \quad m_2 = \xi m_2 + \pi_2 m',$$

where  $\pi_1 m' \in \text{rad } kU^-M_1$  and  $\pi_2 m' \in \text{rad } kU^-M_2$ . It follows that  $\xi = 0$  and  $\xi = 1$ , which is impossible. Thus  $\ker \pi_1 \cap kGm = 0$ , and  $\pi_1: kGm \rightarrow M_1$  is an isomorphism. Similarly,  $\pi_2: kGm \rightarrow M_2$  is an isomorphism, and  $M_1 \cong M_2$  as required.

The next step is to construct a basic set of simple  $E$ -modules, and to prove that each of them occurs in  $\text{inv}_U M$  for some simple  $kG$ -module  $M$ . We require a few more items of notation and some preliminary remarks. For each  $i$ ,  $1 \leq i \leq l$ , we set

$$G'_i = \langle U_{\alpha_i}, U_{-\alpha_i} \rangle, \quad T_i = T \cap G'_i,$$

and note that each group  $G'_i$  is a subgroup of the group  $G_i = U_{\alpha_i} T \cup U_{\alpha_i} T n U_{\alpha_i}$ , discussed earlier, and is a finite group with a split  $BN$ -pair of rank 1. From the proof of (72.15), it is clear that we can choose in each group  $G'_i$  a fixed element  $n'_i$  of length 1, such that  $n'_i \in N \cap G'_i$  and  $\pi(n'_i) = s_i \in S$ . For each such element  $n'_i$ , we clearly have

$$(72.22) \quad (n'_i, T) \subseteq T_i,$$

where  $(n'_i, T)$  is the set of commutators  $\{(n'_i, t), t \in T\}$ . Moreover, the elements  $\{t'_i(u): u \in U_i^*\}$ , defined by the structure equations (72.15) involving  $n'_i$ , belong to the subgroup  $T_i$ , for each  $i$ .

We recall that  $E$  is generated by the commutative split semisimple algebra  $E_T = \sum_{t \in T} k a_t \cong kT$ , and the elements  $\{a_{n'_i}: 1 \leq i \leq l\}$ . We have

$$(72.23) \quad a_{n'_i}^2 = \sum_{u \in U_i^*} a_{t'_i(u)} a_{n'_i}$$

for each  $i$ , by (72.16). For any left  $kG$ -module  $M$ , the left action of  $E_T$  on  $\text{inv}_U M$  is the same as the action of  $kT$ , by (72.13), and we shall frequently use this identification.

**(72.24) Proposition.** *Let  $\chi$  be a linear  $k$ -representation of  $T$ , and assume that  $T_i \not\subseteq \ker \chi$  for some  $i$ ,  $1 \leq i \leq l$ . Then*

$$\sum_{u \in U_i^*} \chi(t'_i(u)) = 0.$$

*Proof.* Let us set  $Y_i = kG'_i \otimes_{kU_i} k_{U_i} \cong (1_{U_i})^{G'_i}$ , and let  $E'_i$  denote the modular Hecke algebra  $\text{End}_{kG'_i} Y_i$ , acting on  $\text{inv}_{U_i} Y_i$  from the left, so that  $kT_i$  acts in the same way as  $\sum_{t \in T_i} ka_t$ . For any linear character  $\psi$  of  $T_i$ , let  $e_\psi = |T_i|^{-1} \sum_{t \in T_i} \psi(t^{-1}) t \in kT_i$  be the corresponding idempotent. In  $\text{inv}_U Y_i$ , consider the nonzero elements

$$m_1 = e_\chi(1 \otimes 1), \quad m_2 = a_{n_i} e_{\hat{\chi}}(1 \otimes 1), \quad m_0 = m_1 + cm_2$$

where  $\hat{\chi}$  denotes the conjugate character  $s_\chi$ , and  $c \in k$  is an element to be determined later. The elements  $m_0$ ,  $m_1$ , and  $m_2$  all afford the linear representation  $\chi$  of  $T$ . Moreover, using (72.23) we obtain

$$a_{n_i} m_0 = a_{n_i} m_1 + z_\chi c m_2,$$

where  $z_\chi$  denotes the element  $\sum_{u \in U_i^*} \chi(t'_i(u))$ . Then  $a_{n_i} m_0$  and  $a_{n_i} m_1$  afford  $\hat{\chi}$ , assuming they are different from zero. In any case, it follows that if  $\chi \neq \hat{\chi}$  then  $z_\chi = 0$ , proving the result in this case. Now assume that  $\chi = \hat{\chi}$ , and suppose  $z_\chi \neq 0$ . Then, setting  $c = -z_\chi^{-1}$ , it is clear that  $\langle m_0 \rangle$  is a simple  $E'_i$ -submodule of  $\text{inv}_{U_i} Y_i$ , affording the linear character  $\chi$  of  $T$ , and such that  $a_{n_i} m_0 = 0$ . Let  $M = kG'_i m_0$ , and let  $\tilde{M}$  be the quotient of  $M$  by a maximal submodule not containing  $m_0$ . Then  $\tilde{M}$  is a simple  $kG'_i$ -module, and  $\langle \tilde{m}_0 \rangle \cong \langle m_0 \rangle$  as  $E'_i$ -modules, where  $\tilde{m}_0$  is the image of  $m_0$  in  $\tilde{M}$ . By the calculation used in the proof of (72.19), we obtain

$$n'_i \tilde{m}_0 \equiv z_\chi \tilde{m}_0 \pmod{\text{rad } kU_{-\alpha_i} \tilde{m}_0}.$$

Moreover,  $\langle n'_i \tilde{m}_0 \rangle$  is a line fixed by the Sylow group  $U_{-\alpha_i}$  in  $G'_i$ , and, by (72.20), it is the unique such line. We have  $\text{rad } kU_{-\alpha_i} \tilde{m}_0 \neq 0$ , otherwise  $\tilde{M} = \langle \tilde{m}_0 \rangle$  affords a nontrivial linear representation of  $G'_i$ , which is impossible since  $G'_i$  is generated by  $p$ -groups. Moreover,  $\text{rad } kU_{-\alpha_i} \tilde{m}_0$  is stable under the action of  $kU_{-\alpha_i}$ , and hence  $\langle n'_i \tilde{m}_0 \rangle \subseteq \text{rad } kU_{-\alpha_i} \tilde{m}_0$ . It follows that  $z_\chi \tilde{m}_0 \in \text{rad } kU_{-\alpha_i} \tilde{m}_0$  which is a contradiction if  $z_\chi \neq 0$ . This completes the proof.

**(72.25) Corollary.** *Let  $\langle m \rangle$  be a simple  $E$ -module, affording the linear representation  $\chi$  of  $E_T \cong kT$ . Then the eigenvalues of the generators  $\{a_{n_i}\}$  of  $E$  are given by:*

$$a_{n_i} m = \mu_i m, \quad \text{with} \quad \mu_i = 0 \quad \text{or} \quad -1,$$

and  $\mu_i = 0$  unless  $T_i \leq \ker \chi$ .

*Proof.* Suppose  $\mu_i \neq 0$ . Then

$$\mu_i^2 m = a_{n_i}^2 m = \sum_{u \in U_i^*} \hat{\chi}(a_{t'_i(u)}) \mu_i m$$

by (72.23), where  $\hat{\chi}$  corresponds to the conjugate character  $s_\chi$  as in the proof of (72.24). Then  $\hat{\chi}(a_t) = 1$  for all  $t \in T_i$ , by (72.24), and we obtain  $\mu_i = -1$ , as required.

**(72.26) Definition.** Let  $\langle m \rangle$  be a simple  $E$ -module, affording the linear representation  $\chi$  of  $E_T \cong kT$ . Then the data

$$(\chi, \mu_1, \dots, \mu_l),$$

where  $a_{n_i}m = \mu_i m$  for each  $i$ , is called the *weight* of  $\langle m \rangle$ .

By (72.18), every simple  $E$ -module is uniquely determined by its weight. We next prove that every simple  $E$ -module occurs in  $\text{inv}_U Y$ .

**(72.27) Theorem.** Let  $\chi$  be a linear representation of  $kT$ , and let  $\{\mu_1, \dots, \mu_l\}$  be elements of  $k$  satisfying the conditions of Corollary 72.25. Then  $\text{inv}_U Y$  contains a simple  $E$ -module of weight  $(\chi, \mu_1, \dots, \mu_l)$ .

*Proof.* Let  $I$  be the subset of  $S$  consisting of the generators  $s_i$  such that  $T_i \leq \ker \chi$  and  $\mu_i = 0$ . Using (72.22), it can be proved that there exists a set of coset representatives  $\{n_w \in N : \pi(n_w) = w \in W_I\}$ , for the parabolic subgroup  $W_I \leq W$ , with the property that for all  $w, w' \in W_I$ , we have

$$n_w n_{w'} n_{ww'}^{-1} \in \ker \chi.$$

Let  $n_0 \in N$  be a representative of the element  $w_0$  of maximal length in  $W$ . We then define

$$m = \sum_{w \in W_I} a_{n_w n_0} e_{n_w n_0}(\chi) (1 \otimes 1) \in \text{inv}_U Y,$$

where for each  $w \in W_I$ ,  $e_{n_w n_0}(\chi)$  is a primitive idempotent in  $kT$  affording the linear character  $t \mapsto \chi^{ww_0}$ , so  $\chi^{ww_0}(t^{ww_0}) = \chi(t)$ ,  $t \in T$ . Then  $m$  is a nonzero element of  $\text{inv}_U Y$  affording the linear character  $\chi$  of  $T$ . We shall prove that  $\langle m \rangle$  is a simple  $E$ -module with the required properties.

First consider a generator  $s_i \in S - I$ , and let  $w \in W_I$ . Then  $l(s_i w) > l(w)$ , and hence  $l(s_i w w_0) < l(w w_0)$ . Using (72.16), it follows that

$$a_{n_i} a_{n_w n_0} e_{n_w n_0}(\chi) (1 \otimes 1) = \sum_{u \in U_i^+} \chi(t'_i(u)) a_{n_w n_0} e_{n_w n_0}(\chi) (1 \otimes 1).$$

Therefore  $a_{n_i}m = \mu_i m$  where  $\mu_i = -1$  or  $0$  according as  $T_i \leq \ker \chi$  or  $T_i \not\leq \ker \chi$ , using (72.24) in the second case.

Now let  $s_i \in I$ , and choose a cross section  $\{\tilde{w}\}$  of the right cosets  $\langle s_i \rangle \backslash W_I$ , with the property that  $l(s_i \tilde{w}) > l(\tilde{w})$  for all  $\tilde{w}$ . Then we obtain

$$a_{n_i} a_{n_{\tilde{w}} n_0} e_{n_{\tilde{w}} n_0}(\chi) (1 \otimes 1) = -a_{n_{\tilde{w}} n_0} e_{n_{\tilde{w}} n_0}(\chi) (1 \otimes 1)$$

while

$$a_{n_i} a_{n_s, \tilde{w} n_0} e_{n_s, \tilde{w} n_0}(\chi) (1 \otimes 1) = a_{n_{\tilde{w}} n_0} e_{n_{\tilde{w}} n_0}(\chi) (1 \otimes 1),$$

because of (72.16) and the choice of the coset representatives  $\{n_w : w \in W_I\}$ . It follows that, in this case, we have  $a_{n_i}m = 0$ , completing the proof.

Combining our results, we have:

**(72.28) Theorem.** *There exists a bijection from the set of isomorphism classes ( $M$ ) of simple  $kG$ -modules, to the set of isomorphism classes ( $\langle m \rangle$ ) of simple  $E$ -modules. These, in turn, are parametrized by the set of all weights  $\{(\chi, \mu_1, \dots, \mu_l)\}$  where each  $\chi$  is a linear character of  $T$ , and the  $\{\mu_i\}$  are chosen arbitrarily from  $\{0, -1\}$ , subject to the condition that  $\mu_i \neq 0$  implies  $T_i \leq \ker \chi$ .*

*Proof.* The fact that the simple  $E$ -modules are parametrized by the set of weights is immediate, from (72.25) and (72.27). It is also clear that the correspondence  $M \rightarrow \text{inv}_U M$  defines an injective map from the set of isomorphism classes of simple  $kG$ -modules to the set of isomorphism classes of simple  $E$ -modules, by (72.20). It remains to prove that it is surjective. By (72.27), each simple  $E$ -module is isomorphic to a submodule  $\langle m \rangle$  of  $\text{inv}_U Y$ . Then the cyclic module  $kGm \leq Y$  clearly has a simple quotient  $M$  in which the image of  $m$  is different from zero. By (72.20), it follows that  $\text{inv}_U M \cong \langle m \rangle$  as  $E$ -modules. This completes the proof.

**(72.29) Corollary.** *The number of isomorphism classes of simple  $kG$ -modules is exactly  $\sum_{I \subseteq S} |T/T_I|$ , where, for each subset  $I \subseteq S$ ,  $T_I = \langle T_i : s_i \in I \rangle$ .*

*Proof.* Let  $(\chi, \mu_1, \dots, \mu_l)$  be a weight of a simple  $E$ -module, and set  $I = \{s_i \in S : \mu_i = -1\}$ . Then  $T_I \leq \ker \chi$ . Conversely, for each linear representation  $\chi$  of  $T$  such that  $T_I \leq \ker \chi$ , there exists one and only one simple  $E$ -module of weight  $(\chi, \mu_1, \dots, \mu_l)$ , where  $\mu_i = -1$  if and only if  $s_i \in I$ . Since  $T$  is an abelian  $p'$ -group, and  $k$  is sufficiently large, the number of linear representations  $\chi : T \rightarrow k^*$  such that  $T_I \leq \ker \chi$  is  $|T/T_I|$ , and the result follows.

**(72.30) Remark.** Let  $G$  be a universal Chevalley group over the finite field  $F_q$  of characteristic  $p$ , and let  $k$  be an extension field of  $F_q$ , which is sufficiently large relative to  $G$ . In this case, it is easily checked that

$$T = \prod_{i=1}^l T_i \quad (\text{direct product})$$

and

$$|T_i| = q - 1, \quad 1 \leq i \leq l,$$

where  $l$  is the rank of the  $BN$ -pair in  $G$  (see Steinberg [67]). It follows that

$$\sum_{I \subseteq S} |T/T_I| = \prod_{i=1}^l (|T_i| + 1) = q^l.$$

This gives another proof of the result, due to Steinberg [63], that the number of  $p'$ -classes in  $G$  (and hence the number of nonisomorphic simple  $kG$ -modules) is equal to  $g^l$ .

**(72.31) Remark.** Let  $P_I$  be a standard parabolic subgroup of  $G$ , having the Levi decomposition  $P_I = L_I V_I$  (see (69.10)), and let  $M$  be a simple  $kG$ -module. As in the characteristic zero theory, presented in §70, it is of interest to study the truncation of  $M$  at  $P_I$ , which is the  $kL_I$ -module  $\text{inv}_{V_I} M$ . In the natural characteristic, we have the following result, which is stated here without proof:

**(72.32) Theorem (Smith [82]).** *Then truncation  $\text{inv}_{V_I} M$  is a simple  $kL_I$ -module, for all subsets  $I \subseteq S$  and simple  $kG$ -modules  $M$ .*

## Rationality Questions

Let  $G$  be a finite group, and let  $K$  be a field. A  $KG$ -module  $M$  is *realizable* in a subfield  $F$  of  $K$  provided that there exists an  $FG$ -module  $M_0$  such that  $M = K \otimes_F M_0$ . When this occurs, we shall call  $M_0$  an  $F$ -form of  $M$ . The existence of an  $F$ -form means that  $M$  affords an  $F$ -rational matrix representation  $x \rightarrow \mathbf{M}(x)$ ,  $x \in G$ , with the property that all the entries of the matrices  $\{\mathbf{M}(x), x \in G\}$  lie in  $F$ . Thus the term “rationality questions” refers to problems connected with realizability.

There are, first of all, general principles that apply to all finite groups. These are first discussed in §73 for  $CG$ -modules, with reference to the real field  $\mathbb{R}$ . The results in this case are particularly elegant and explicit, and are due to Frobenius-Schur [06]. We have given an elementary self-contained approach, following Serre, which belongs in every course on basic character theory.

Rationality questions involving arbitrary fields are discussed in §74, from the point of view of central simple algebras. Here the main ideas, especially for number fields, are due to Schur. We have given a survey of the classical results of Schur, Brauer, Witt, and others, along with recent contributions by Benard-Schacher, Yamada, and Janusz.

A second approach to rationality questions is to investigate families of finite groups that behave exceptionally, either well or badly. The prototypes of good behavior are the symmetric groups, where the situation can be described quite simply: everything is rational. Section 75 contains a new approach to the representation theory of the symmetric groups due to James, which produces a basic set of simple modules over an arbitrary field. Strong results on the rationality properties of simple modules also hold for other types of Weyl groups and generic Hecke algebras associated with them, but that is another story (see Benson-Curtis [72] and Lusztig [81]).

The chapter also contains several induction theorems closely related to questions of rationality. These include Serre’s theorem on real-valued characters in §73B, Frobenius’ theorem on characters of the symmetric groups, Solomon’s generalization of the Artin Induction Theorem in §75B, and an introduction to the Artin exponent in §76.

### §73. UNITARY, ORTHOGONAL, AND SYMPLECTIC CG-MODULES

#### §73A. Rationality Questions over the Real Field R

We consider CG-modules  $M$ , where  $G$  is a finite group, and are interested in subfields  $K$  of  $\mathbb{C}$  such that  $M$  is *realizable* in  $K$ . This means that there exists an isomorphism of CG-modules

$$(73.1) \quad M \cong \mathbb{C} \otimes_K M_0$$

for some  $KG$ -module  $M_0$  (called a  $K$ -form of  $M$ ). A  $K$ -basis of  $M_0$  is then a  $\mathbb{C}$ -basis of  $M$ , and relative to this basis, the matrices  $\{\mathbf{M}(x): x \in G\}$  have entries in  $K$ . It is easily shown (see (7.15)) that a field  $K \subseteq \mathbb{C}$  is a splitting field for  $G$  if and only if every simple CG-module has a  $K$ -form.

In this subsection we consider the basic question as to which CG-modules admit R-forms, where R is the real field. A beautiful solution of this problem, which involves interesting and unexpected connections with the internal structure of the group  $G$ , was given by Frobenius-Schur [06]. Our account follows Serre [77], with some changes and additions.

We first recall that the contragredient module  $M^*$  of a CG-module  $M$  is the dual space  $M^* = \text{Hom}_{\mathbb{C}}(M, \mathbb{C})$ , on which  $G$  acts according to the rule

$$(x \cdot f)m = f(x^{-1}m), \quad \text{for all } f \in M^*, \quad m \in M, \quad x \in G.$$

If  $M$  affords the character  $\mu$  of  $G$ , then  $M^*$  affords the character  $\mu^*$  given by

$$(73.2) \quad \mu^*(x) = \mu(x^{-1}) = \overline{\mu(x)} \quad \text{for } x \in G,$$

where bar denotes complex conjugation (see §10D). We shall call  $\mu$  *real-valued* if  $\mu(x) \in \mathbb{R}$  for all  $x \in G$ , or equivalently, if  $\mu = \bar{\mu}$ . Clearly  $\mu$  is real-valued whenever  $M$  has an R-form.

We now have:

**(73.3) Theorem (Frobenius-Schur).** *Let  $M$  be a CG-module with character  $\mu$ . Then*

- (i)  $\mu$  is real-valued if and only if  $M$  admits a nondegenerate  $G$ -invariant bilinear form.
- (ii)  $M$  has an R-form if and only if  $M$  admits a nondegenerate symmetric  $G$ -invariant bilinear form (over  $\mathbb{C}$ ). In this case,  $M$  affords a representation in which each  $x \in G$  is represented by a real orthogonal matrix.

*Proof.* (i)  $\mu$  is real-valued if and only if  $M \cong M^*$ . The existence of a CG-isomorphism from  $M$  to  $M^*$  is easily shown to be equivalent to the existence of a  $G$ -invariant nondegenerate bilinear form on  $M$ , by the sort of argument used in §10D. We leave it as an exercise for the reader to check this assertion.

(ii) First assume  $M$  has an  $R$ -form  $M_0$ . The  $RG$ -module  $M_0$  admits a positive definite symmetric  $G$ -invariant bilinear form  $\langle m, n \rangle$ , obtained by the averaging process from the usual inner product  $(m, n)$  defined with respect to some  $R$ -basis of  $M_0$ . Specifically, define

$$\langle m, n \rangle = |G|^{-1} \sum_{x \in G} (xm, xn), \quad \text{for } m, n \in M_0.$$

Since  $M \cong C \otimes_R M_0$ , the form  $\langle m, n \rangle$  extends to a nondegenerate, symmetric,  $G$ -invariant bilinear form on  $M$ , proving one implication in part (ii).

Conversely, let  $M$  admit a symmetric nondegenerate  $G$ -invariant bilinear form  $B(m, n)$ . Let  $[m, n]$  be a nondegenerate  $G$ -invariant positive definite hermitian bilinear form on  $M$  (whose existence follows by the same argument used above: see CR Exercise (10.6)). Then there exists a map  $\varphi: M \rightarrow M$  such that

$$B(m, n) = \overline{[\varphi(m), n]} \quad \text{for all } m, n \in M.$$

The map  $\varphi$  is clearly bijective and semilinear, in the sense that

$$\varphi(zm) = \bar{z}\varphi(m) \quad \text{for all } z \in C, \quad m \in M.$$

Moreover,  $\varphi^2 \in GL(M)$ , and we have

$$[\varphi^2 m, n] = \overline{B(\varphi(m), n)} = \overline{B(n, \varphi(m))} = [\varphi n, \varphi m] \quad \text{for all } m, n \in M.$$

Since  $[m, n] = \overline{[n, m]}$ , we obtain

$$[m, \varphi^2 n] = \overline{[\varphi^2 n, m]} = \overline{[\varphi m, \varphi n]} = [\varphi n, \varphi m] = [\varphi^2 m, n],$$

using the previous computation. Thus  $\varphi^2$  is self-adjoint. Moreover,

$$[\varphi^2 m, m] = [\varphi m, \varphi m] > 0 \quad \text{for all } m \neq 0,$$

so  $\varphi^2$  is positive definite. A standard application of the spectral theorem for self-adjoint linear transformations shows that a positive definite self-adjoint map  $T$  has a unique positive definite self-adjoint square root  $U$  such that  $U^2 = T$  and  $U = p(T)$  for some polynomial  $p$  with real coefficients. Let  $v$  be the positive definite self-adjoint square root of  $\varphi^2$ , and put  $\sigma = \varphi v^{-1}$ . Since  $v = p(\varphi^2)$ ,  $v$  and  $\varphi$  commute, and we obtain

$$\sigma^2 = \varphi^2 v^{-2} = 1.$$

It follows that  $M = M_0 \oplus M_1$ , where  $M_0 = \{m \in M : \sigma m = m\}$  and  $M_1 = \{m \in M : \sigma m = -m\}$ . Since  $\sigma$  is semilinear,  $M_0$  and  $M_1$  are  $R$ -subspaces of  $M$  such that  $M_1 = iM_0$  (where  $i = \sqrt{-1}$ ). Thus  $M = M_0 \oplus iM_0$ . Since both  $B(m, n)$

and  $[m, n]$  are  $G$ -invariant, it follows that  $\varphi^2$  and  $v$  commute with the action of  $G$ , whence so does  $\sigma$ . Then  $M_0$  is clearly an  $R$ -form of  $M$ , and the theorem is proved.

**(73.4) Example.** Let  $Q = \langle a, b : a^4 = 1, b^2 = a^2, bab^{-1} = a^{-1} \rangle$  be the quaternion group of order 8. The  $C$ -characters of  $Q$  are all rational-valued, and in fact  $Q$  has the same character table as the dihedral group  $D_4$  (see Exercise 9.9). Let  $M$  be the unique simple two-dimensional  $CQ$ -module. Then its character is real-valued, but  $M$  does not admit an  $R$ -form. To see this, suppose to the contrary that  $M_0$  is an  $R$ -form of  $M$ . By Theorem 73.3, it follows that the matrices  $\{\mathbf{M}(x) : x \in G\}$  afforded by  $M$ , with respect to a suitable  $R$ -basis of  $M_0$ , are real orthogonal matrices. But it is easily shown that the finite subgroups of the orthogonal group on the plane are either cyclic or dihedral. Thus  $M$  does not have an  $R$ -form. (See also the example at the end of §74A.)

In the next part of the discussion, we make use of the theorem of Frobenius, which states that every f.d. division algebra over  $R$  is isomorphic to exactly one of the following:  $R$ ,  $C$ , or  $H$ , where  $H$  is the division algebra of real quaternions (for proof see [M0, Exercise 31.8]). Thus the simple  $RG$ -modules  $M$  can be put in three classes, according as  $\text{End}_{RG} M \cong R$ ,  $C$ , or  $H$ . (The same idea gives a classification of simple  $A$ -modules, for any f.g. semisimple  $R$ -algebra.)

We also require the following important construction, which we describe in a general form for later use (see also §10A).

**(73.5) Definition.** Let  $M$  be a f.g.  $KG$ -module, where  $G$  is a finite group, and  $K$  a field. For any subfield  $F \subset K$  such that  $\dim_F K < \infty$ , the natural embedding  $FG \subset KG$  defines the structure of a f.g.  $FG$ -module on  $M$ , called the  $FG$ -module obtained by *restriction of scalars*, and denoted by  $M|_{FG}$  (or simply  $M_{FG}$ ).

**(73.6) Lemma.** Let  $M$  be a  $KG$ -module affording a matrix representation  $x \rightarrow \mathbf{M}(x) = (m_{ij}(x))$ ,  $x \in G$ , with entries  $\{m_{ij}(x)\}$  in  $K$ . Then for any subfield  $F \subset K$  with  $\dim_F K < \infty$ ,  $M_{FG}$  affords a matrix representation  $x \rightarrow \rho_{K/F}(m_{ij}(x))$ , where  $\rho_{K/F}$  is the regular matrix representation of  $K$  over  $F$ .

*Proof.* Let  $\{u_1, \dots, u_d\}$  be a  $K$ -basis for  $M$ , and  $\{\xi_1, \dots, \xi_e\}$  an  $F$ -basis of  $K$ . Thus the set

$$\{\xi_i u_j : 1 \leq i \leq e, 1 \leq j \leq d\}$$

is an  $F$ -basis of  $M_{FG}$ . We have, for  $x \in G$ :

$$\begin{aligned} x(\xi_i u_j) &= \xi_i(x u_j) = \xi_i \sum_{k=1}^d (m_{kj}(x) u_k) \\ &= \sum_{k=1}^d (m_{kj}(x) \xi_i) u_k = \sum_{k=1}^d \sum_{l=1}^e \rho_{li}(m_{kj}(x)) \xi_l u_k, \end{aligned}$$

where  $\rho_{K/F}(a) = (\rho_{ij}(a))$ ,  $a \in K$ , is the regular matrix representation of  $K$  over  $F$  with respect to the basis  $\{\xi_1, \dots, \xi_e\}$ . This completes the proof.

**(73.7) Corollary.** *Keep the previous notation, and assume that  $K/F$  is a Galois extension with Galois group  $\mathfrak{G} = \text{Gal}(K/F)$ . Then for all  $x \in G$ ,*

$$\text{Tr}(x, M_{FG}) = \sum_{\sigma \in \mathfrak{G}} \sigma \text{Tr}(x, M).$$

*Proof.* By Lemma 73.6,

$$\begin{aligned} \text{Tr}(x, M_{FG}) &= \sum_{k=1}^d \text{Trace } \rho_{K/F}(m_{kk}(x)) \\ &= \sum_{\sigma \in \mathfrak{G}} \sigma \text{Tr}(x, M), \end{aligned}$$

as required, since by Galois theory, the trace of the regular representation of  $K/F$  is given by  $\sum_{\sigma \in \mathfrak{G}} \sigma$ .

Returning to the real and complex fields, we have:

**(73.8) Corollary.** *Let  $M$  be a f.g. CG-module with character  $\mu$ . Then the character afforded by the RG-module  $M|_{RG}$  obtained by restriction of scalars is given by*

$$x \rightarrow \text{Tr}(x, M|_{RG}) = \mu(x) + \overline{\mu(\bar{x})}, \quad x \in G,$$

where bar denotes complex conjugation.

This result follows at once from (73.7), since  $C/R$  is a Galois extension with Galois group  $\langle \sigma \rangle$ , where  $\sigma$  is complex conjugation.

**(73.9) Theorem.** *Let  $M$  be a simple CG-module, with character  $\mu$ , and let  $n = \dim_C M$ . Then exactly one of the following possibilities occurs:*

(i)  $\mu$  is not real-valued. Then the RG-module  $M_{RG}$ , obtained from  $M$  by restriction of scalars, is a simple RG-module of dimension  $2n$  over R, affording the character  $\mu + \bar{\mu}$ . In this case, the endomorphism algebra  $\text{End}_{RG} M_{RG}$  is isomorphic to C, and the corresponding Wedderburn component of RG is isomorphic to  $M_n(C)$ .

(ii)  $\mu$  is real-valued, and  $M$  has an R-form  $M_0$ . Then  $M_0$  is absolutely simple, with character  $\mu$ . Moreover,  $\text{End}_{RG} M_0 \cong R$ , and the Wedderburn component of RG corresponding to  $M_0$  is isomorphic to  $M_n(R)$ . In this case,  $M_{RG}$  is a direct sum of two copies of  $M_0$ .

(iii)  $\mu$  is real-valued, but  $M$  does not have an R-form. Then the RG-module  $M_{RG}$  obtained by restriction of scalars is a simple RG-module of dimension  $2n$ , whose

character is  $2\mu$ . The endomorphism algebra  $\text{End}_{RG} M_{RG}$  is isomorphic to  $H$ , and the corresponding Wedderburn component of  $RG$  is isomorphic to  $M_n(H)$ .

*Proof.* (i) By Corollary 73.8, we have  $\text{Tr}(x, M_{RG}) = \mu(x) + \bar{\mu}(x)$  for all  $x \in G$ . Then the character of  $C \otimes_R M_{RG}$  is  $\mu + \bar{\mu}$ , and hence  $C \otimes_R M_{RG} \cong M \oplus M^*$ , and  $M^* \not\cong M$  by (73.2), since  $\mu \neq \bar{\mu}$  because of the hypothesis that  $\mu$  is not real-valued. We next prove that  $M_{RG}$  is a simple  $RG$ -module. Suppose, to the contrary, that  $M_1$  is a proper submodule of  $M_{RG}$ . Then  $C \otimes_R M_1$  is isomorphic either to  $M$ ,  $M^*$ , or  $M \oplus M^*$ , and each of these possibilities is easily seen to be impossible. Thus  $M_{RG}$  is a simple  $RG$ -module. By Exercise 2.9, we have

$$\dim_R \text{End}_{RG} M_{RG} = \dim_C \text{End}_{CG} C \otimes M_{RG} = \dim_C \text{End}_{CG} (M \oplus M^*) = 2,$$

since  $M$  is simple and  $M \not\cong M^*$ . By Frobenius's theorem on real division algebras, we conclude that  $\text{End}_{RG} M_{RG} \cong C$ , and the rest follows from the Wedderburn theorems.

(ii) The  $R$ -form  $M_0$  is clearly a simple  $RG$ -module, with character  $\mu$ . Since  $C \otimes_R M_0 \cong M$ , we have  $\dim_R \text{End}_{RG} M_0 = \dim_C \text{End}_{CG} M = 1$  by the same reasoning as in the proof of (i). The rest of part (ii) follows from the Wedderburn theorems.

(iii) This is proved by an argument similar to the proof of (i), and is left as an exercise for the reader. This completes the proof of the theorem.

We shall now give some other ways of distinguishing between the possibilities described in the above theorem. The first is a kind of geometric characterization, in terms of the existence of  $G$ -invariant bilinear forms on  $M$ .

**(73.10) Theorem.** *Let  $M$  be a simple  $CG$ -module, affording the character  $\mu$ .*

(i) *If  $M$  does not admit a nonzero  $G$ -invariant bilinear form, then  $\mu$  is not real-valued, and  $M$  has no  $R$ -form. Call  $M$  unitary in this case.*

(ii) *If  $M$  admits a nonzero  $G$ -invariant bilinear form, then this form is unique up to scalar multiples. It is nondegenerate, and is either symmetric or skew-symmetric. If the form is symmetric, then  $\mu$  is real-valued, and  $M$  has an  $R$ -form. We call  $M$  orthogonal in this case (since  $M$  affords a real representation of  $G$  by orthogonal transformations).*

*If the form is skew-symmetric, then  $\mu$  is real-valued, but  $M$  has no  $R$ -form. We call  $M$  symplectic, since  $M$  affords a representation of  $G$  by symplectic transformations.\**

*Proof.* If  $M$  admits a nonzero  $G$ -invariant bilinear form  $B$ , then  $B$  defines a nonzero  $CG$ -homomorphism between  $M$  and  $M^*$ . This homomorphism is uniquely determined up to a scalar multiple by Schur's Lemma, since both  $M$  and  $M^*$  are simple  $CG$ -modules. It follows that  $B$  is nondegenerate and is uniquely

\*A symplectic transformation on a vector space over a field is a linear map preserving a nondegenerate skew-symmetric bilinear form on the vector space.

determined up to scalar multiples. Now write  $B = B_+ + B_-$ , with  $B_+$  symmetric and  $B_-$  skew-symmetric. It is clear that both  $B_+$  and  $B_-$  are also  $G$ -invariant, so by uniqueness we may assume that either  $B = B_+$  or  $B = B_-$ . In the first case, it follows that  $M$  has a real form, and hence is orthogonal, by Theorem 73.3ii. In case  $B = B_-$ , we conclude that  $\mu$  is real-valued by (73.3i), and that  $M$  does not admit a nondegenerate symmetric  $G$ -invariant bilinear form, because of the uniqueness of  $B$ . Then  $M$  is symplectic in this case. Finally,  $M$  is unitary if and only if neither of the above situations occur. This is equivalent to the assertions that  $\mu$  is not real-valued, and that  $M$  admits no nonzero  $G$ -invariant bilinear form. These remarks complete the proof of the theorem.

We remark that in case  $M$  is unitary,  $M$  does admit a positive definite  $G$ -invariant hermitian form (see the proof of Theorem 73.3).

We conclude this subsection with an important test of the type of a simple CG-module, as in (73.10), in terms of the character table of  $G$ . We first recall some concepts introduced in §12C. Let  $M$  be an arbitrary f.g. CG-module, with character  $\mu$ . Starting from the isomorphism of vector spaces over  $C$ ,

$$\text{Hom}_{CG}(M^*, M) \cong \text{inv}_G(M \otimes M),$$

we define the *intertwining number*

$$i(M^*, M) = \dim_C \text{inv}_G(M \otimes M).$$

We also introduce the *symmetric* and *antisymmetric intertwining numbers*, defined by

$$(73.11) \quad i_s(M^*, M) = \dim_C \text{inv}_G(M \vee M) \quad \text{and} \quad i_a(M^*, M) = \dim_C \text{inv}_G(M \wedge M),$$

where  $M \vee M$  and  $M \wedge M$  denote the CG-modules consisting of symmetric tensors and skewsymmetric tensors, respectively, in  $M \otimes M$ . Since we have

$$M \otimes M \cong (M \vee M) \oplus (M \wedge M)$$

as CG-modules, it follows that

$$i(M^*, M) = i_s(M^*, M) + i_a(M^*, M).$$

We now define the *Frobenius-Schur indicator*

$$(73.12) \quad c(M) = i_s(M^*, M) - i_a(M^*, M),$$

and note that  $c(M) \in \{0, \pm 1\}$  for a simple CG-module  $M$ .\*

\*We take this opportunity to correct the statement of (12.11). In the statement of (12.11ii), delete “ $c(M \otimes N) = c(M)c(N)$  and,” and in (12.11iii), replace “ring homomorphisms” by “ $Z$ -homomorphisms.”

The next result shows that the Frobenius-Schur indicator  $c(M)$  determines the type of a simple module  $M$ , and gives a method for calculating  $c(M)$  in terms of the character afforded by  $M$ . The invariant  $c(M)$  has proved to be so useful, in recent calculations of characters of finite simple groups, that there is good reason to regard the Frobenius-Schur indicators  $\{c(Z_i)\}$  of a basic set of simple CG-modules  $\{Z_i : 1 \leq i \leq s\}$ , as part of the character table data of an arbitrary finite group  $G$  (see (9.25)).

**(73.13) Theorem (Frobenius-Schur).** *Let  $M$  be a simple CG-module with character  $\mu$ . Then  $c(M) \in \{0, \pm 1\}$ , and is given by*

$$(73.14) \quad c(M) = |G|^{-1} \sum_{x \in G} \mu(x^2).$$

Moreover,  $M$  is orthogonal if  $c(M) = 1$ , symplectic if  $c(M) = -1$ , and unitary if  $c(M) = 0$  (see Theorem 73.10).

*Proof.* We first establish (73.14) for an arbitrary CG-module  $M$  affording the character  $\mu$ . Since  $x^{|G|} = 1$  for each  $x \in G$ , the minimal polynomial of the action of  $x$  on  $M$  has no repeated factors, and hence  $M$  has a basis  $\{m_1, \dots, m_d\}$  consisting of eigenvectors of  $x$ , with eigenvalues  $\{\xi_1, \dots, \xi_d\}$ , respectively, for a given  $x \in G$ . By (12.3), it follows easily that  $M \vee M$  has a basis consisting of the tensors  $\{m_i \otimes m_j + m_j \otimes m_i : 1 \leq i \leq j \leq d\}$  while  $M \wedge M$  has a basis consisting of the tensors  $\{m_i \otimes m_j - m_j \otimes m_i : 1 \leq i < j \leq d\}$ . It follows that we have

$$\left\{ \begin{array}{l} \mu(x) = \sum_{i=1}^d \xi_i, \quad \mu(x^2) = \sum_{i=1}^d \xi_i^2, \\ \mu_s(x) = \sum_{i \leq j} \xi_i \xi_j = \sum \xi_i^2 + \sum_{i < j} \xi_i \xi_j, \\ \mu_a(x) = \sum_{i < j} \xi_i \xi_j, \end{array} \right.$$

where  $\mu_s$  and  $\mu_a$  are the characters of  $G$  afforded by  $M \vee M$  and  $M \wedge M$ , respectively. Thus we obtain

$$(73.15) \quad \mu(x^2) = \mu_s(x) - \mu_a(x) \quad \text{for } x \in G.$$

On the other hand, by (73.11)

$$i_s(M^*, M) = (\mu_s, 1_G), \quad \text{and} \quad i_a(M^*, M) = (\mu_a, 1_G).$$

Therefore we obtain from (73.15)

$$c(M) = (\mu_s - \mu_a, 1_G) = |G|^{-1} \sum \mu(x^2),$$

which establishes formula (73.14).

For an arbitrary f.d. CG-module  $M$ , the dual  $(M \otimes M)^*$  of the inner tensor product  $M \otimes M$  is the vector space of bilinear forms on  $M$ , on which  $G$  acts diagonally. It follows that the duals of  $M \vee M$  and  $M \wedge M$  are the vector spaces of symmetric and skew-symmetric bilinear forms on  $M$ , with diagonal  $G$ -action. Moreover,

$$\dim_{\mathbb{C}} \text{inv}_G M = \dim_{\mathbb{C}} \text{inv}_G M^*$$

for any f.g. CG-module  $M$ .

Now let  $M$  be a simple CG-module. By (73.12), we have  $c(M) \in \{0, \pm 1\}$ , as noted earlier. It is clear that  $c(M) = 1$  if and only if  $i_s(M^*, M) = \dim_{\mathbb{C}} \text{inv}_G(M \vee M) = \dim_{\mathbb{C}} \text{inv}_G(M \vee M)^* = 1$ . This occurs if and only if  $M$  admits a nonzero  $G$ -invariant symmetric bilinear form, and hence  $M$  is orthogonal, by Theorem 73.10ii. A similar argument, again based on (73.10ii), shows that  $M$  is symplectic if and only if  $c(M) = -1$ . Finally,  $M$  admits no nonzero  $G$ -invariant bilinear form if and only if  $c(M) = 0$ , and in this case  $M$  is unitary, by (73.10i). This completes the proof.

For an interesting connection between the Frobenius-Schur indicators  $\{c(M)\}$  of the simple CG-modules, and the set of involutions in  $G$ , see the Exercises.

### §73B. Induction Theorems for Real-Valued Characters

Let  $M$  be a CG-module with character  $\mu$ . By Theorem 73.3,  $\mu$  is real-valued if and only if  $M$  admits a nondegenerate  $G$ -invariant bilinear form. If  $M$  is a simple module, then the character  $\mu$  is real-valued if and only if  $M$  is either orthogonal or symplectic; by Theorem 73.10. The characterization of real-valued virtual characters is more subtle, however, and suggests the study of the following  $\mathbb{Z}$ -submodules of the ring of virtual characters of  $G$ .

We shall denote by  $\text{ch } G$  the ring of virtual  $\mathbb{C}$ -characters of  $G$ ; then  $\text{ch } G$  is a free  $\mathbb{Z}$ -module with a basis consisting of the characters

$$\text{Irr } G = \{\zeta^1, \dots, \zeta^s\}$$

afforded by a basic set of simple CG-modules (see §9C).

**(73.16) Definition.** Let  $G$  be a finite group. We define two  $\mathbb{Z}$ -submodules of  $\text{ch } G$ ,

$$\text{ch}_O G \quad \text{and} \quad \text{ch}_S G,$$

as follows. The first,  $\text{ch}_O G$ , is the  $\mathbb{Z}$ -module generated by the characters of all CG-modules that admit symmetric nondegenerate  $G$ -invariant bilinear forms, while the second,  $\text{ch}_S G$ , is generated by the characters of all CG-modules that admit skew-symmetric nondegenerate  $G$ -invariant bilinear forms.

By Theorem 73.3i, both  $\text{ch}_O G$  and  $\text{ch}_S G$  consist of real-valued virtual characters. Further properties of  $\text{ch}_O G$  and  $\text{ch}_S G$  are contained in the next result, which is a nice application of the Frobenius-Schur theory from §73A.

Let  $\text{Irr } RG$  be the set of characters of  $G$  afforded by a basic set of simple  $RG$ -modules, and let  $\text{ch } RG$  be the subring of  $\text{ch } G$  spanned (over  $\mathbb{Z}$ ) by all characters in  $\text{Irr } RG$ . As usual,  $\text{Irr } G$  denotes the set of irreducible complex characters of  $G$ . For  $\mu \in \text{Irr } G$ , we call  $\mu$  *unitary*, *orthogonal*, or *symplectic*, according to the types of simple  $CG$ -modules given in (73.10).

**(73.17) Proposition.** (i) Let  $\zeta^i, \zeta^j, \zeta^k$  range over the orthogonal, unitary, and symplectic characters in  $\text{Irr } G$ , respectively. Then

$$\text{Irr } RG = \{\zeta^i\} \cup \{\zeta^j + \bar{\zeta}^j\} \cup \{2\zeta^k\},$$

and these form a  $\mathbb{Z}$ -basis for  $\text{ch } RG$ .

- (ii)  $\text{ch}_O G = \text{ch } RG$ , and is a subring of  $\text{ch } G$  containing  $1_G$ .
- (iii) We have

$$\text{ch}_O G \cdot \text{ch}_S G \subseteq \text{ch}_S G,$$

so  $\text{ch}_S G$  is a module over the ring  $\text{ch}_O G$ .

*Proof.* (i) The characters  $\{\zeta^i\}$ ,  $\{\zeta^i + \bar{\zeta}^i\}$ , and  $\{2\zeta^k\}$  are afforded by simple  $RG$ -modules, by Theorem 73.9, and are clearly linearly independent over  $\mathbb{Z}$ . It remains to prove that an arbitrary character  $\mu$ , afforded by an  $RG$ -module  $M$ , is a  $\mathbb{Z}$ -linear combination of the characters in the list. It is enough to consider the case of a simple  $RG$ -module  $M$ . Let  $\zeta$  be the irreducible complex character afforded by a simple  $CG$ -direct summand of  $C \otimes_R M$ . Then it is easily shown, using (73.9), that  $\mu = \zeta, \zeta + \bar{\zeta}$ , or  $2\zeta$ , according as  $\zeta$  is orthogonal, unitary, or symplectic; this completes the proof of part (i).

(ii) It is sufficient to prove that  $\text{ch}_O G = \text{ch } RG$ , since  $\text{ch } RG$  is clearly a subring of  $\text{ch } G$  containing  $1_G$ . First let  $\mu$  be the character of an  $RG$ -module  $M$ . Then  $\mu$  is also the character of the  $CG$ -module  $C \otimes_R M$ , which has an  $R$ -form, by construction. By Theorem 73.3ii,  $C \otimes_R M$  admits a nondegenerate symmetric  $G$ -invariant bilinear form, so  $\mu \in \text{ch}_O G$ , and we have proved that  $\text{ch } RG \subseteq \text{ch}_O G$ . For the reverse inclusion, let  $\lambda$  be a character afforded by a  $CG$ -module  $L$  that admits a symmetric nondegenerate  $G$ -invariant bilinear form. Then  $L$  has an  $R$ -form, by (73.3ii), and it follows that  $\lambda \in \text{ch } RG$ . Therefore  $\text{ch } RG = \text{ch}_O G$ , and (ii) is proved

(iii) Let  $\mu$  and  $\nu$  be characters afforded by  $CG$ -modules  $M$  and  $N$ , such that  $M$  admits a symmetric nondegenerate  $G$ -invariant bilinear form  $f$ , and  $N$  admits a skew-symmetric nondegenerate  $G$ -invariant bilinear form  $g$ . Then the inner tensor product  $M \otimes N$  admits a bilinear form  $f \otimes g$ , defined by

$$(f \otimes g)(m_1 \otimes n_1, m_2 \otimes n_2) = f(m_1, m_2)g(n_1, n_2).$$

It is easily checked that  $f \otimes g$  is nondegenerate,  $G$ -invariant, and skew-symmetric. The character afforded by  $M \otimes N$  is  $\mu\nu$ , and we have shown that  $\mu\nu \in \text{ch}_S G$ . This completes the proof that  $\text{ch}_O G \cdot \text{ch}_S G \subseteq \text{ch}_S G$ .

The main result of this subsection is an induction theorem for virtual characters in  $\text{ch}_O G$ , due to Serre [71]. This theorem, and a similar one for  $\text{ch}_S G$ , have arithmetical applications to Galois Gauss sums and Artin root numbers of real-valued characters (see Martinet [77], Serre [71], and Deligne [76]). Serre's proof uses the Borel-Serre theorem on supersolvable subgroups of compact Lie groups. We shall give a proof due to Ritter [82], based on the Witt-Berman Induction Theorem (see §21 or CR §42).

We require a preliminary definition. By Exercise 73.1, every irreducible complex character of a dihedral group  $D_m$  (of order  $2m$ ) is orthogonal. Thus, if  $G$  is an arbitrary group and  $\xi \in \text{Irr } G$ , it is natural to call  $\xi$  a *dihedral character* of  $G$  if  $\xi$  is the pullback of an irreducible complex character, of degree 2, of a dihedral homomorphic image of  $G$ . This means that  $\deg \xi = 2$ , and  $G/\ker \xi \cong D_m$  for some  $m$ . It is then clear that all dihedral characters of  $G$  are orthogonal.

We now prove:

**(73.18) Serre's Induction Theorem.** *Every virtual character in  $\text{ch}_O G$  is a  $\mathbb{Z}$ -linear combination of induced characters  $\{\text{ind}_H^G \psi\}$ , where  $H \leq G$  and  $\psi \in \text{Irr } RH$  is one of the following types:*

- (i)  $\psi$  is a linear character,  $\psi: H \rightarrow \{\pm 1\}$ ,
- (ii)  $\psi = \lambda + \bar{\lambda}$  for some linear character  $\lambda: H \rightarrow \mathbb{C}^\times$ ,
- (iii)  $\psi$  is a dihedral character.

*Proof.* We have  $\text{ch}_O G = \text{ch } RG$  by (73.17). The Witt-Berman Theorem 21.6, applied to  $\text{ch } RG$ , asserts that every virtual character in  $\text{ch } RG$  is a  $\mathbb{Z}$ -linear combination of induced characters of the form  $\text{ind}_H^G \mu$ , where  $H$  is an  $R$ -elementary subgroup of  $G$ , and  $\mu$  is a character afforded by a simple  $RH$ -module. By transitivity of induction, the theorem follows once we establish:

**(73.19) Lemma.** *Let  $H$  be an  $R$ -elementary group. Then the conclusion of Theorem 73.18 holds for  $H$ .*

*Proof.* Since  $\text{ch}_O H = \text{ch } RG$ , it is sufficient to prove that an arbitrary character  $\mu$  afforded by a simple  $RH$ -module  $M$  is induced from a character of a subgroup of type (i)–(iii), as in (73.18).

Let  $\Delta = \text{End}_{RH} M$ . The simple  $RH$ -module  $M$  is called  $\Delta$ -*primitive* if it is impossible to express  $M$  as a direct sum

$$M = M_1 \oplus \cdots \oplus M_t, \quad \text{with } t > 1,$$

where the  $M_i$  are nonzero  $\Delta$ -submodules of  $M$  that are permuted transitively by

the action of  $H$ . First assume that  $M$  is not  $\Delta$ -primitive. Then for a decomposition above, with  $t > 1$ , we have  $M \cong \text{ind}_{H_1}^H M_1$  by the Imprimitivity Theorem 10.5, where

$$H_1 = \text{Stab}_H M_1 = \{h \in H : hM_1 = M_1\}.$$

It is easily checked that  $M_1$  is a simple  $RH_1$ -module,  $H_1 < H$ , and  $H_1$  is an  $R$ -elementary group (since all subgroups of  $R$ -elementary groups are  $R$ -elementary).

Therefore, using induction on  $|H|$ , we may assume that  $M$  is a  $\Delta$ -primitive simple  $RH$ -module, on which  $H$  acts faithfully. The  $R$ -elementary group  $H$  can be expressed as a semidirect product

$$H = \langle x \rangle \rtimes D,$$

where  $\langle x \rangle$  is a cyclic  $p'$ -group,  $D$  is a  $p$ -group for some prime  $p$ , and where

$$uxu^{-1} = x^{\pm 1} \quad \text{for all } u \in D$$

(see §21A).

Let  $N$  be a maximal abelian normal subgroup of  $H$  containing  $\langle x \rangle$ . Then  $H/N$  is a  $p$ -group, and we have  $C_H(N) = N$ . Otherwise, there is a subgroup  $N_1 \trianglelefteq H$  such that  $N < N_1 \leq C_H(N)$  and  $|N_1:N| = p$ , so  $N_1$  is an abelian normal subgroup of  $H$ , contradicting the choice of  $N$ .

Let  $\{e_1, \dots, e_r\}$  be the set of primitive idempotents in the commutative group algebra  $RN$ . Then we have

$$M = \bigoplus_{i=1}^r e_i M.$$

Since  $N \trianglelefteq H$ , the idempotents  $\{e_i\}$  are permuted by inner automorphisms, and hence  $H$  permutes the subspaces  $\{e_i M : 1 \leq i \leq r\}$ . The  $H$ -action is clearly transitive, because  $M$  is a simple  $RH$ -module. We also have  $\Delta e_i M \subseteq e_i M$ , for each  $i$ , where  $\Delta = \text{End}_{RH} M$ . Since  $M$  is  $\Delta$ -primitive, we obtain  $M = e_i M$  for some  $i$ , and  $e_j M = 0$  if  $j \neq i$ .

Now let  $T: RH \rightarrow \text{End}_R M$  be the representation of the group algebra  $RH$  on  $M$ . Then we have  $T(RN) = T(RNe_i)$ , and  $T(RNe_i)$  is invariant under inner automorphisms by elements of  $T(H)$ , since  $M = e_i M$  and  $e_j M = 0$  if  $j \neq i$ . The Wedderburn component  $RNe_i$  of  $RN$  is a field, so its image  $T(RNe_i)$  is also a field, which we shall denote by  $F$ . Since  $T(N)$  is a subgroup of the multiplicative group of  $F$ ,  $T(N)$  is cyclic, and generates  $F$  over the field  $R$ . However, the representation  $T$  is faithful on  $H$  and thus it follows that  $N$  is cyclic, and that  $H/N$  is represented faithfully by a group of field automorphisms of  $F$  over  $R$ , using the fact that  $C_H(N) = N$ . This shows that  $|H/N| = 1$  or 2.

If  $|H/N| = 1$ , then  $H$  is cyclic, and it is easily checked that the character  $\mu$  of  $M$  satisfies either (i) or (ii) of (73.18).

Now assume that  $|H/N| = 2$ . Then  $H$  has a cyclic subgroup  $\langle y \rangle$  of index 2, so

the irreducible nonlinear characters of  $H$  are induced from linear characters of  $\langle y \rangle$ , and have degree 2. From §73A, we have either

- (a)  $\mathbb{C} \otimes_R M$  is a simple  $CH$ -module, or
- (b)  $\mathbb{C} \otimes_R M \cong V \oplus V^*$ , for a symplectic or unitary simple  $CH$ -module  $V$ .

In case (a),  $H$  is represented faithfully as a group of orthogonal transformations on a two-dimensional space over  $R$ , and hence is isomorphic to a dihedral group. Then  $\mu$  is a dihedral character in this case.

If (b) holds, then the character of  $V$  has the form  $\text{ind}_{\langle y \rangle}^H \tau$  for a linear character  $\tau$  of  $\langle y \rangle$ , and hence

$$\mu = \text{ind}_{\langle y \rangle}^H (\tau + \bar{\tau}).$$

This completes the proof of the lemma, and of the Serre Induction Theorem.

### §73. Exercises

1. Let  $D_m$  be the dihedral group of order  $2m$ . Prove that every simple  $\mathbb{C}D_m$ -module is orthogonal (see (7.310)).

[Hint: Let  $D_m = \langle a, b : a^m = (ab)^2 = b^2 = 1 \rangle$ . Use elementary linear algebra to construct the correct number of inequivalent nonlinear irreducible representations from  $D_m$  to  $O(V)$ , where  $O(V)$  is the orthogonal group on a two-dimensional real Euclidean space  $V$  (see also (7.39)). For another approach, use Exercise 5 below.]

2. Let  $Q_m$  denote the generalized quaternion group of order  $4m$  (see (1.24)). Prove that every simple two dimensional  $\mathbb{C}Q_m$ -module  $M$  is either symplectic or orthogonal, and is orthogonal if and only if  $M$  is the pullback of a simple  $\mathbb{C}\bar{Q}_m$ -module, for a dihedral quotient group  $\bar{Q}_m$  of  $Q_m$ .

[Hint: See (7.40).]

In Exercises 3–5,  $G$  denotes a finite group of order  $n$ .

3. Prove that if  $m$  is an integer such that  $\text{G.C.D. } (m, n) = 1$ , then for each  $y \in G$ , the equation  $x^m = y$  has a unique solution.

4. Let  $m$  be a positive integer, and let  $\theta_m(y)$  be the number of solutions of the equation  $x^m = y$ , for each  $y \in G$ . Prove that  $\theta_m$  is a class function on  $G$ , and that

$$\theta_m = \sum_{\zeta \in \text{Irr } G} c_m(\zeta) \zeta, \quad \text{with } c_m(\zeta) = n^{-1} \sum_{x \in G} \zeta(x^m).$$

[Hint: Use the orthogonality relations to show that

$$c_m(\zeta) = (\theta_m, \zeta) = n^{-1} \sum_{y \in G} \theta_m(y) \overline{\zeta(y)}, \quad \text{for } \zeta \in \text{Irr } G.$$

Each term in the sum can be expressed in the form

$$\theta_m(y)\overline{\zeta(y)} = \sum_{x \in G, x^m = y} \overline{\zeta(x^m)},$$

and it follows that

$$n^{-1} \sum_{x \in G} \overline{\zeta(x^m)} = n^{-1} \sum_{y \in G} \sum_{x^m = y} \overline{\zeta(x^m)} = c_m(\zeta).]$$

5. Keep the notation of Exercise 4. Note that  $c_2(\zeta) = c(M)$ , where  $c(M)$  is the Frobenius-Schur indicator of a simple CG-module  $M$  affording  $\zeta$ . Prove that if  $t$  is the number of involutions in  $G$ , then

$$t + 1 = \sum_{\zeta \in \text{Irr } G} c_2(\zeta) \zeta(1).$$

## §74. THE SCHUR INDEX

In this section we shall develop the general theory of the Schur index, giving its main properties in §74A, and then concentrating on the case of group algebras in §§74B,C. The Schur index  $m_Q(\zeta)$ , of an irreducible complex character  $\zeta$  of a finite group  $G$ , is the index of a certain skewfield associated to  $\zeta$ . This index gives significant information about fields in which  $\zeta$  can be realized. We shall treat the more general situation in which  $Q$  is replaced by an arbitrary ground field, not necessarily of characteristic 0. Our approach uses the theory of central simple algebras, rather than manipulations with characters and idempotents.

In §74A we derive a number of different characterizations of the Schur index, first for arbitrary algebras, and then specifically for group algebras. We apply these results in §74B, introducing the theory of Hasse invariants when needed. This in turn leads to a review of Brauer groups in §74C, which play a key role in the proofs of the Benard-Schacher Theorem and the Brauer-Witt Theorem.

For other treatments of Schur indices, and especially the theorems in §74A, B, see Feit [67], [83], and Isaacs [76]. It is a useful exercise, which we leave to the reader, to interpret the results of the preceding section in terms of Schur indices.

### §74A. General Theory

In this subsection we collect a number of results, mostly proved earlier in this book, that relate splitting fields for algebras, indices of skewfields, and irreducible characters of finite groups. We fix the following notation once and for all:  $A$  is a f.d.  $k$ -algebra with center  $c(A)$ , where  $k$  is a field. If  $D$  is a division algebra of finite dimension over its center  $K$ , then by (7.22)  $\dim_K D = m^2$  for some integer  $m$ , called the *index* of  $D$ . If  $A \cong M_r(D)$ , we also call  $m$  the *index* of  $A$ . A finite direct sum of full matrix algebras over a field  $K$  is called a *split semisimple*  $K$ -algebra.

In the proof of (3.60) (see also Exercise 49.1), we established the following easy result:

**(74.1) Lemma.** *Let  $A$  and  $B$  be any  $k$ -algebras. Then*

$$c(A \otimes_k B) = c(A) \otimes_k c(B).$$

*Proof.* (We do not require that  $A$  and  $B$  be f.d.  $k$ -algebras.) Denote  $\otimes_k$  by  $\otimes$  for brevity. Let  $x = \sum a_i \otimes b_i \in c(A \otimes B)$ , where each  $a_i \in A$ ,  $b_i \in B$ . We may assume that the  $\{b_i\}$  are linearly independent over  $k$ . Since  $x$  commutes with  $a \otimes 1$  for each  $a \in A$ , it follows that each  $a_i \in c(A)$ . We then rewrite  $x$  as  $x = \sum a'_j \otimes b'_j$ , with each  $a'_j \in c(A)$ ,  $b'_j \in B$ , where now the  $\{a'_j\}$  are linearly independent over  $k$ . Then each  $b'_j \in c(B)$ , since  $x$  commutes with  $1 \otimes b$  for each  $b \in B$ . Thus  $x \in c(A) \otimes c(B)$ , as desired.

We show next that under ground field extensions, simple algebras behave in the same way as their centers. To be explicit, we now prove:

**(74.2) Proposition.** *Let  $A$  be a f.d. simple  $k$ -algebra with center  $K$ , and let  $E$  be a finite separable field extension of  $k$ .*

(i) *There is a decomposition*

$$E \otimes_k K = \bigoplus_{i=1}^t (E \otimes_k K) \varepsilon_i,$$

*a direct sum of fields, where  $1 = \sum \varepsilon_i$  is the decomposition of 1 into central primitive idempotents in  $E \otimes_k K$ . Correspondingly,*

$$E \otimes_k A = \bigoplus_{i=1}^t A_i, \quad \text{where } A_i = (E \otimes_k A) \varepsilon_i.$$

*For each  $i$ ,  $A_i$  is a simple algebra with center  $(E \otimes_k K) \varepsilon_i$ .*

(ii) *If  $K/k$  is a Galois extension of degree  $t = \dim_k K$ , then*

$$K \otimes_k K \cong \bigoplus_{i=1}^t K \varepsilon_i,$$

*with each  $K \varepsilon_i$  a field. Correspondingly, viewing  $A$  as embedded in  $K \otimes_k A$ , we have*

$$K \otimes_k A \cong \bigoplus_{i=1}^t A \varepsilon_i,$$

*with each  $A \varepsilon_i \cong A$  as  $k$ -algebra. The Galois group  $\text{Gal}(K/k)$  acts transitively on the simple components  $\{A \varepsilon_i\}$  of  $K \otimes_k A$ , and  $c(A \varepsilon_i) = K \varepsilon_i$ .*

*Proof.* Since  $E/k$  is separable,  $E \otimes_k K$  is a direct sum of fields. The assertions in (i) then follow directly from (3.60) and (74.1). For (ii), we may write  $K \cong k[x]/(f(x))$ , with  $f(x)$  irreducible over  $k$ . Then  $f(x)$  splits into linear factors

in  $K[x]$ , so

$$K \otimes_k K \cong K[x]/(f(x)) \cong K \oplus \cdots \oplus K.$$

The remaining assertions in (ii) are then clear, since  $\text{Gal}(K/k)$  acts transitively on the zeros of  $f(x)$ .

As a consequence, we may describe the behavior of a simple module under ground field extension, in a special case needed for our later discussion. We show, keeping the notation of (74.2):

**(74.3) Corollary.** *Let  $A$  be a f.d. simple  $k$ -algebra, whose center  $K$  is a Galois extension of  $k$ . Let  $U$  be a simple left  $A$ -module. Then there is a  $(K \otimes_k A)$ -isomorphism*

$$K \otimes_k U \cong W_1 \oplus \cdots \oplus W_t,$$

where  $W_i$  is a simple left  $Ae_i$ -module.

*Proof.* We may write  $A \cong M_r(D)$  where  $D$  is a skewfield with center  $K$ . Then  $A \cong U^{(r)}$  as left  $A$ -modules. By (74.2ii),  $K \otimes_k A$  is a direct sum of  $t$  simple algebras  $Ae_i$ , and  $Ae_i \cong M_r(D)e_i$  for each  $i$ . Thus

$$K \otimes_k A \cong \bigoplus_{i=1}^t M_r(D)e_i \cong (W_1 \oplus \cdots \oplus W_t)^{(r)}$$

as left  $(K \otimes_k A)$ -modules. Since  $K \otimes_k A \cong (K \otimes_k U)^{(r)}$ , this gives the desired result.

Let us combine (74.2) with the results in §7B to obtain a more precise form of the basic Theorem 7.18. We again restrict our attention to simple modules over a simple algebra, since the general case eventually reduces to this special case. The fundamental result, which will be applied later to the case of group algebras, is as follows:

**(74.4) Theorem.** *Let  $A = M_r(D)$  be a f.d. simple  $k$ -algebra, where  $D$  is a skewfield with center\*  $K$  and index  $m$ . Let  $E$  be a finite Galois extension of  $k$  with Galois group  $\mathfrak{G}$ , and assume that  $E$  splits  $A$  over  $k$ , that is,  $E \otimes_k A$  is a split semisimple  $E$ -algebra. Then*

$$E \otimes_k K = \bigoplus_{i=1}^t Ee_i \quad \text{and} \quad E \otimes_k A = \bigoplus_{i=1}^t A_i, \quad \text{with } A_i = (E \otimes_k A)e_i,$$

where the  $\{e_i\}$  are orthogonal central primitive idempotents, and  $t = \dim_k K$ . For each  $i$ ,  $A_i$  is a simple algebra whose center  $Ee_i$  is isomorphic to  $E$ . Then we have:

\*We are not assuming here that  $K$  is a Galois extension of  $k$ .

(i)  $\mathfrak{G}$  acts transitively on the idempotents  $\{\varepsilon_1, \dots, \varepsilon_t\}$ , and on the simple components  $\{A_1, \dots, A_t\}$  of  $E \otimes_k A$ .

(ii) For each  $i$ ,  $1 \leq i \leq t$ , let  $V_i$  be a simple left  $A_i$ -module. Then  $\mathfrak{G}$  acts transitively on the set  $\{V_1, \dots, V_t\}$ , which is a full set of simple  $(E \otimes_k A)$ -modules. Let

$$\mathfrak{H} = \{\sigma \in \mathfrak{G} : \sigma V_1 \cong V_1\}.$$

Then  $K$  is isomorphic to the subfield of  $E$  fixed by  $\mathfrak{H}$ .

(iii) Let  $U$  be a simple left  $A$ -module. Then

$$E \otimes_k U \cong (V_1 \oplus \cdots \oplus V_t)^{(m)} \text{ as left } (E \otimes_k A)\text{-modules.}$$

*Proof.* Most of the above assertions were proved in (7.18) and (7.19), and we restate part of the argument for convenience. Let  $\otimes_k$  be written as  $\otimes$  for convenience. Since  $E \otimes A$  is split, it follows from (7.2) that  $K$  is separable over  $k$ , and also (by 74.2i) that  $E \otimes K$  is a direct sum of  $t$  copies of  $E$ . This gives  $t = \dim_k K$ , as claimed.

We now write

$$K = k(\alpha) \cong k[x]/(f(x)), \quad \text{where } f(x) = \min. \text{ pol. } \alpha.$$

Then  $E \otimes K \cong E[x]/(f(x))$ , so  $f(x)$  factors completely in  $E[x]$ ; thus

$$f(x) = \prod_{i=1}^t (x - \alpha_i), \quad \alpha_i \in E.$$

Consequently we may write

$$E \otimes K \cong \coprod_{i=1}^t E[x]/(x - \alpha_i) = \bigoplus_{i=1}^t E\varepsilon_i.$$

The Galois group  $\mathfrak{G} = \text{Gal}(E/k)$  acts transitively on the  $\{\alpha_i\}$ , and also on the  $\{\varepsilon_i\}$ . If  $\sigma \in \mathfrak{G}$  is such that  $\sigma(\alpha_1) = \alpha_i$ , then  $\sigma(\varepsilon_1) = \varepsilon_i$ . Thus for  $\sigma \in \mathfrak{G}$ ,

$$\sigma(\varepsilon_1) = \varepsilon_1 \Leftrightarrow \sigma(\alpha_1) = \alpha_1 \Leftrightarrow \sigma \text{ fixes the field } k(\alpha_1).$$

Letting  $\mathfrak{H} = \{\sigma \in \mathfrak{G} : \sigma V_1 \cong V_1\}$ , it follows that  $\sigma \in \mathfrak{H}$  if and only if  $\sigma$  fixes  $k(\alpha_1)$ . Therefore  $k(\alpha_1)$  is the subfield of  $E$  fixed by  $\mathfrak{H}$ . But  $K \cong k(\alpha_1)$ , so (ii) is proved.

Finally, we have

$$E \otimes A \cong \bigoplus_{i=1}^t M_l(E)\varepsilon_i.$$

for some  $l$ . Comparing  $E$ -dimensions of both sides, we obtain  $l = mr$ . Since

$A \cong U^{(r)}$  as left  $A$ -modules, we deduce that

$$(E \otimes U)^{(r)} \cong \bigoplus_{i=1}^t V_i^{(l)},$$

so  $E \otimes U \cong \bigoplus V_i^{(m)}$  as claimed. This completes the proof.

Now let  $G$  be a finite group, and let  $k$  be an arbitrary field, of characteristic  $\geq 0$ . The results below hold whether or not  $\text{char } k$  divides  $|G|$ , and are of significance even when  $\text{char } k = 0$ . Let  $E$  be a finite Galois extension of  $k$ , such that  $E$  is a splitting field for  $G$ . By Exercise 74.1, such fields  $E$  necessarily exist; see also §17A. For such a field  $E$ , the  $E$ -algebra  $EG/\text{rad } EG$  is a split semi-simple  $E$ -algebra, and each simple  $EG$ -module  $V$  is absolutely simple (that is,  $\text{End}_{EG} V \cong E$ ).

With the above notation, let  $V$  be a simple  $EG$ -module. We say that  $V$  is *realizable* in a subfield  $F$  of  $E$  if  $V \cong E \otimes_F V_0$  for some  $FG$ -module  $V_0$  (which is then necessarily simple). If  $V$  affords the matrix representation  $T$  of  $G$ , then  $V$  is realizable in  $F$  if and only if  $T$  is equivalent (over  $E$ ) to an  $F$ -representation of  $G$ . In this case,  $F$  must contain all of the character values  $\{\zeta(x) : x \in G\}$ , where  $\zeta$  is the character of  $G$  afforded by  $V$  (or  $V_0$ ).

Let us denote by  $k(\zeta)$  the field obtained by adjoining to  $k$  all of the character values  $\{\zeta(x) : x \in G\}$ . Since each  $\zeta(x)$  is a sum of roots of unity, it follows that  $k(\zeta)$  is a subfield of a cyclotomic extension of  $k$ , and therefore  $k(\zeta)$  is a Galois extension of  $k$ .

If  $U$  is a simple left  $kG$ -module, then  $(\text{rad } kG)U = 0$ . Since  $\text{rad } EG = E \otimes_k \text{rad } kG$  by the proof of (7.10), it follows that  $E \otimes_k U$  is a semisimple  $EG$ -module. By (7.9), each simple  $EG$ -module  $V$  is a summand of  $E \otimes_k U$  for some simple  $kG$ -module  $U$ , unique up to isomorphism. The preceding Theorem 74.4 plays a key role in studying the relationship between  $U$  and  $V$ , and in determining in which fields  $V$  is realizable. Our main result is as follows:

**(74.5) Theorem.** *Let  $G$  be a finite group,  $k$  any field, and let  $E$  be a splitting field for  $G$ , such that  $E$  is a finite Galois extension of  $k$ . Let  $\mathfrak{G} = \text{Gal}(E/k)$  be the Galois group of  $E$  over  $k$ . Then we have:*

(i) *For  $U$  a simple left  $kG$ -module, set*

$$(74.6) \quad D = \text{End}_{kG} U, \quad K = \text{center of } D, \quad m = \text{index of } D, \quad t = \dim_k K.$$

*Then there is an isomorphism of  $EG$ -modules*

$$(74.7) \quad E \otimes_k U \cong (V_1 \oplus \cdots \oplus V_t)^{(m)},$$

*where  $\{V_1, \dots, V_t\}$  are a set of nonisomorphic simple left  $EG$ -modules permuted transitively by  $\mathfrak{G}$*

(ii) *Let  $\zeta$  be an absolutely irreducible character of  $G$ , afforded by some*

(absolutely) simple left  $EG$ -module  $V$ . There is a simple  $kG$ -module  $U$ , unique up to isomorphism, such that  $\zeta$  occurs in the character  $\eta$  of  $G$  afforded by  $U$ . Then  $V$  is one of the  $\{V_i\}$  occurring in (74.7), say  $V = V_1$ , and we have

$$\eta = m(\zeta_1 + \cdots + \zeta_t), \quad K \cong k(\zeta_1) \cong \cdots \cong k(\zeta_t),$$

where  $V_i$  affords the character  $\zeta_i$  of  $G$ .

(iii) Suppose that the absolutely irreducible character  $\zeta$  of  $G$  is afforded by a simple  $FG$ -module, where  $F$  is a finite extension of  $k$ . Then  $F \supseteq k(\zeta)$ , and

$$\dim_{k(\zeta)} F \text{ is a multiple of } m.$$

Further, there exist such fields  $F$  for which  $\dim_{k(\zeta)} F = m$ .

*Proof.* The discussion preceding the statement of the theorem shows that there exist splitting fields  $E$  for  $G$  which are finite Galois over  $k$ . Further, by (7.10) we have

$$E \otimes_k (kG/\text{rad } kG) \cong EG/\text{rad } EG = \text{split semisimple } E\text{-algebra}.$$

Let us write

$$kG/\text{rad } kG = \bigoplus B_j,$$

where the  $\{B_j\}$  are f.d. simple  $k$ -algebras. Given a simple  $kG$ -module  $U$ , there is a unique  $j$  such that  $U$  is a simple faithful left  $B_j$ -module. For  $x \in kG$ , let  $x_l$  denote left multiplication on  $U$ , and set  $(kG)_l = \{x_l : x \in kG\}$ . Then  $U$  is also a simple faithful left  $(kG)_l$ -module. Therefore  $B_j \cong (kG)_l$  as  $k$ -algebras, and so

$$E \otimes_k B_j \cong (EG)_l = E \otimes_k (kG)_l$$

as algebras acting from the left on  $E \otimes_k U$ . By the above,  $E \otimes_k B_j$  is a split semisimple  $E$ -algebra.

Now set  $A = (kG)_l$  and  $D = \text{End}_{kG} U = \text{End}_A U$ . Then the assertions in (i) are merely a restatement of part of Theorem 74.4.

To prove (ii), let  $V$  afford the absolutely irreducible character  $\zeta$  of  $G$ . By (7.9),  $V$  is a summand of  $E \otimes_k U$  for some simple  $kG$ -module  $U$ . Decompose  $E \otimes_k U$  as in (74.7), with  $V = V_1$ . Let  $\zeta_i$  be the character of  $G$  afforded by  $V_i$ ,  $1 \leq i \leq t$ , and let  $U$  afford the character  $\eta$ . Then (74.7) gives

$$\eta = m(\zeta_1 + \cdots + \zeta_t),$$

where  $t = \dim_k K$  as in (74.6). The characters  $\{\zeta_1, \dots, \zeta_t\}$  are distinct by the Frobenius-Schur Theorem 3.41, and by (i),  $\mathfrak{G}$  permutes these characters transitively.

Now write

$$E \otimes_k A = \bigoplus_{i=1}^t A_i, \quad A_i = \text{simple } k\text{-algebra},$$

where  $V_i$  is a simple left  $A_i$ -module, and where  $A_i \cong M_{mr}(E)\varepsilon_i$  as in (74.4). Put  $\mathfrak{H} = \{\sigma \in \mathfrak{G} : \sigma(A_1) = A_1\}$ , so we have

$$\mathfrak{H} = \{\sigma \in \mathfrak{G} : \sigma(V_1) \cong V_1\} = \{\sigma \in \mathfrak{G} : \sigma(\zeta_1) = \zeta_1\}.$$

It follows that the subfield of  $E$  fixed by  $\mathfrak{H}$  is precisely  $k(\zeta_1)$ , so  $K \cong k(\zeta_1)$  by (74.4). This completes the proof of (ii).

Before starting the proof of (iii), we examine formula (74.7) more carefully, using the fact that  $K = k(\zeta_1) = \cdots = k(\zeta_t)$  is a Galois extension of  $k$ . By (74.3) we have

$$K \otimes_k U \cong W_1 \oplus \cdots \oplus W_t,$$

a sum of  $t$  nonisomorphic simple  $KG$ -modules  $\{W_i\}$  that are permuted transitively by  $\text{Gal}(K/k)$ . The proof of (74.3) shows also that  $W_i$  is a simple  $M_r(D)$ -module for some  $r$  (independent of  $i$ ), so  $\text{End}_{KG} W_i \cong D$ . Further,

$$E \otimes_k U \cong E \otimes_K (K \otimes_k U) \cong \bigoplus_{i=1}^t (E \otimes_K W_i).$$

By (74.7), we have

$$E \otimes_K W_i \cong V_i^{(m)}.$$

Thus, in the step from  $k$  to  $K$ , the simple  $kG$ -module  $U$  splits into  $t$  nonisomorphic simple  $KG$ -modules  $\{W_i\}$ . In the step from  $K$  to  $E$ , each  $W_i$  splits into  $m$  copies of the absolutely simple  $EG$ -module  $V_i$ .

We now prove (iii), so let  $F \supseteq k$  be a field in which the character  $\zeta$  is realizable. Obviously  $F \supseteq k(\zeta) = K$ , and there is an absolutely simple  $FG$ -module  $X$  affording the character  $\zeta$ , such that  $X$  is a summand of some  $F \otimes_K W_i$ , where the  $\{W_i\}$  are the simple  $KG$ -modules defined above. Since  $\text{End}_{KG} W_i = D$ , it follows from Exercise 74.2 that  $F$  splits  $D$  over  $K$ . Then

$$F \otimes_K D \cong M_m(F) \cong X^{(m)}.$$

View  $X$  as a left  $D$ -space, and count dimensions over  $D$ . This gives

$$\dim_K F = m \cdot \dim_D X,$$

so  $m$  divides  $\dim_K F$  as claimed.

On the other hand, we may choose  $F$  to be a maximal subfield of  $D$ . Then

by (7.22),  $\dim_K F = m$  and  $F$  splits  $D$  over  $K$ . The preceding argument can be reversed to show that  $\zeta$  is realizable in  $F$ . This completes the proof of the theorem.

In the above, we started with an absolutely irreducible character  $\zeta$  of  $G$ , afforded by some absolutely simple  $EG$ -module  $V$ . We showed that there exists a simple  $kG$ -module  $U$ , affording a character  $\eta$  of  $G$ , with

$$\eta = m(\zeta_1 + \cdots + \zeta_t), \quad E \otimes_k U \cong V_1^{(m)} \oplus \cdots \oplus V_t^{(m)},$$

where (say)  $V = V_1$  and  $\zeta = \zeta_1$ . The characters  $\{\zeta_i\}$  are distinct, and are a full set of algebraic conjugates of  $\zeta$  under the action of  $\text{Gal}(E/k)$ . The integer  $m$  is the index of the skewfield  $D$ , where  $D = \text{End}_{kG} U$ . The center  $K$  of  $D$  is isomorphic (over  $k$ ) to each field  $k(\zeta_i)$  obtained by adjoining the character values  $\{\zeta_i(x) : x \in G\}$  to  $k$ .

We call  $m$  the *Schur index* of  $\zeta$  relative to  $k$ , and write  $m = m_k(\zeta)$ . From the above theorem, we obtain at once:

**(74.8) Corollary.** *Let  $m = m_k(\zeta)$  be the Schur index of the absolutely irreducible character  $\zeta$  of  $G$ .*

- (i) *If  $\mu$  is a character of  $G$  afforded by some  $kG$ -module, then the multiplicity of  $\zeta$  in  $\mu$  is a multiple of  $m$ . For suitably chosen  $\mu$ , this multiplicity equals  $m$ .*
- (ii) *Let  $V$  be an absolutely simple  $EG$ -module affording the character  $\zeta$ . Then  $V^{(m)}$  is realizable in the field  $k(\zeta)$ , and  $m$  is the smallest positive integer with this property. Furthermore,*

$$m \text{ is a divisor of } \dim_E V.$$

*Proof.* The assertions are clear from Theorem 74.5. For the second statement in (ii), we note that by Theorem 74.5,  $V$  is a simple  $M_{mr}(E)$ -module for some integer  $r$ ; then  $\dim_E V = mr$ , which is a multiple of  $m$ .

For fields of characteristic  $p > 0$ , the theory becomes much simpler.

**(74.9) Theorem.** *Let  $\zeta$  be an absolutely irreducible character of  $G$  afforded by an  $EG$ -module  $V$ , and suppose that  $\text{char } E = p > 0$ . Then  $m_k(\zeta) = 1$ , and  $V$  is realizable in the field  $k(\zeta)$ .*

*Proof.* The proof of (7.11) shows that  $kG/\text{rad } kG$  is a direct sum of matrix algebras over fields. Thus all Schur indices are 1, and the remaining assertion of (74.9) follows from (74.8ii).

**(74.10) Remarks.** (i) Let  $E$  be a splitting field for  $G$  containing  $k$ , and let  $\zeta$  be an absolutely irreducible character of  $G$  (afforded by a simple  $EG$ -module). By (74.5iii), there exist fields  $F \supseteq K$ , with  $\dim_K F = m_k(\zeta)$ , such that  $\zeta$  is realizable in  $F$  (that is,  $\zeta$  is afforded by some simple  $FG$ -module). However, there is no

guarantee that  $F$  can be chosen as a subfield of  $E$ , and indeed there exist counterexamples to this supposition (Fein [74]).

(ii) Let  $k$  be an algebraic number field, and let  $M_r(D)$  be a simple component of  $kG$ , where  $D$  is a skewfield of index  $m$ . By (74.8),  $mr = \zeta(1)$  for some irreducible complex character  $\zeta$  of  $G$ . Since  $\zeta(1)$  divides  $|G|$ , we conclude that also  $mr$  divides  $|G|$ . Thus, each Schur index  $m_k(\zeta)$  is a divisor of  $|G|$ . We proved these results in another manner in (27.11), using Jacobinski's Conductor Formula (27.8).

(iii) Let  $\zeta \in \text{Irr } G$ , and let  $K$  be a field of characteristic 0. Then for any character  $\eta$  of  $G$  afforded by a  $KG$ -module,

$$(\zeta, \eta)_G \equiv 0 \pmod{m_K(\zeta)}.$$

Further,  $(\zeta, \eta)_G = m_K(\zeta)$  for suitably chosen  $\eta$ .

**Example.** Let  $G$  be a quaternion group of order 8. Then

$$\mathbb{Q}G \cong \mathbb{Q} \oplus \mathbb{Q} \oplus \mathbb{Q} \oplus \mathbb{Q} \oplus \mathbb{H},$$

where  $\mathbb{H}$  is the skewfield of rational quaternions, and is of index 2. There is a unique irreducible complex character  $\zeta$  of  $G$  of degree 2, afforded by a simple  $EG$ -module  $V$ , where  $E = \mathbb{Q}(i)$ . Then  $V^{(2)}$  is realizable in  $\mathbb{Q}$ , and indeed  $E \otimes_{\mathbb{Q}} \mathbb{H} \cong V^{(2)}$ , but  $V$  is not realizable in  $\mathbb{Q}$ . The character  $\zeta$  is rational-valued (necessarily!), and  $\mathbb{Q}(\zeta) = \mathbb{Q}$ . See also Exercise 73.2.

## §74B. Schur Indices for Group Algebras

We present here a number of general results on Schur indices and the structure of group algebras. For example, we study the group algebra  $\mathbb{Q}G$  of a  $p$ -group  $G$ ; we have already used the structure of  $\mathbb{Q}G$  in our proofs in §50B, for example. We also give some results on  $KG$  for  $K$  a  $p$ -adic field and  $G$  any  $p'$ -group.

We begin with:

**(74.11) Theorem.** *Let  $K$  be a finite extension of the  $p$ -adic field  $\mathbb{Q}_p$ , where  $p$  is any prime, and let  $G$  be a finite group whose order  $n$  is prime to  $p$ . Then*

$$KG \cong \coprod_{i=1}^t M_{n_i}(K_i),$$

where each  $K_i$  is a field, unramified over  $K$ .

*Proof.* Let  $A = KG$ ,  $\Lambda = RG$ , where  $R$  is the valuation ring of  $K$ . Let  $P$  be the prime ideal of  $R$ , and  $\bar{R} = R/P$  its residue class field of characteristic  $p$ . By hypothesis  $n \in R^\times$ , so by (27.1)  $\Lambda$  is a maximal  $R$ -order in  $A$ . Let us write

$$A = \bigoplus_{i=1}^t A_i, \quad A_i = \text{simple algebra with center } K_i, \quad \dim_{K_i} A_i = n_i^2.$$

The  $\Lambda = \bigoplus \Lambda_i$ , with  $\Lambda_i$  a maximal  $R_i$ -order in  $A_i$ , where  $R_i$  is the valuation ring of  $K_i$ .

Since  $\Lambda$  is maximal, the Jacobinski Conductor Formula (27.8) shows that  $\mathfrak{D}_i^{-1} = \Lambda_i$  for each  $i$  (since  $n/n_i \in R$ ), where  $\mathfrak{D}_i^{-1}$  is the inverse different of  $\Lambda_i$  relative to  $R_i$ , using reduced traces. Thus the different  $\mathfrak{D}(\Lambda_i/R) = \Lambda_i$ . But the proof of (27.13) shows that

$$\mathfrak{D}(\Lambda_i/R) = \mathfrak{D}(\Lambda_i/R_i)\mathfrak{D}(R_i/R).$$

Further, by MO (20.3),

$$\mathfrak{D}(\Lambda_i/R) = (\text{rad } \Lambda_i)^{m_i-1},$$

where  $m_i$  is the index of  $A_i$ . Also, by Exercise 4.11,  $(\text{rad } R_i)^{e_i-1}$  divides  $\mathfrak{D}(R_i/R)$ , where  $e_i$  is the ramification index of  $K_i$  over  $K$ . It follows that  $m_i = 1$  and  $e_i = 1$ , which proves the theorem.

It is of interest to give an alternative proof of the above theorem using character theory. As above, let  $K$  be a  $p$ -adic field and  $G$  a  $p'$ -group of order  $n$ . Let  $\zeta$  be an absolutely irreducible character of  $G$ , afforded by a representation in some extension field of  $K$ . Then there is a simple component  $A_i$  of  $KG$ , for which the simple  $A_i$ -module  $U$  affords a character  $\eta$  in which  $\zeta$  occurs. By (74.5), we have

$$K \subseteq K_i \cong K(\zeta) \subseteq K(\sqrt[n]{1}),$$

where  $K_i$  is the center of  $A_i$ . Since  $p \nmid n$ , it follows from §4H that  $K(\sqrt[n]{1})/K$  is unramified, and therefore also  $K_i/K$  is unramified.

It remains for us to show that the Schur index  $m_K(\zeta)$  equals 1. Since

$$(74.12) \quad m_{K(\zeta)}(\zeta) = m_K(\zeta)$$

by (74.5iii), we may replace  $K$  by  $K(\zeta)$ . Changing notation, we assume now that  $K = K(\zeta)$ , so the values  $\{\zeta(x) : x \in G\}$  lie in  $R$ . By the proof of (74.5) (see also (74.8ii)), we have  $\eta = m\zeta$ , where  $m = m_K(\zeta)$ , and so  $R$  contains all values of the character  $\eta$ .

Let bars denote reduction mod  $P$ , and let us show that  $\bar{\eta}$  is an irreducible character of  $G$ . Let  $M$  be any full  $RG$ -lattice in  $U$ , and set  $\bar{M} = M/PM$ , an  $\bar{R}G$ -module which affords the character  $\bar{\eta}$ . Since  $RG$  is semisimple,  $\bar{M}$  is a direct sum of simple modules. By (6.8), each direct sum decomposition of  $\bar{M}$  lifts to one of  $M$ . But  $M$  is indecomposable, since  $KM = U$  is a simple module. This shows that  $\bar{M}$  is simple, and hence  $\bar{\eta}$  is irreducible.

Finally,  $\bar{R}$  contains the character values  $\{\bar{\eta}(x) : x \in G\}$ , so by (74.9) we conclude that  $\bar{\eta}$  is absolutely irreducible, and  $\bar{M}$  is absolutely simple. On the other hand, from  $\eta = m\zeta$  we deduce  $\bar{\eta} = m\bar{\zeta}$ . It follows that  $m = 1$  (and  $\bar{\eta} = \bar{\zeta}$ ), so  $m_K(\zeta) = 1$  as desired. This completes the proof.

For yet another version of the proof, and for generalizations of the theorem, see Feit [82, Ch. IV, Th. 9.3 and its corollaries].

We now turn to some results on group algebras over global fields, and concentrate on the structure of  $\mathbb{Q}G$ , where  $G$  is a  $p$ -group. We intend to show that, for  $p$  odd,  $\mathbb{Q}G$  is a direct sum of matrix algebras over fields which are cyclotomic extensions of  $\mathbb{Q}$ . A somewhat more complicated result holds when  $p = 2$ , since quaternion skewfields may occur in this case. Our approach is as follows: We first establish Schilling's Theorem, which says that if  $G$  is nilpotent, then each simple component of  $\mathbb{Q}G$  has index 1 or 2. We then use some easy character theory to find the centers of these simple components. As we shall see, it suffices to prove the results when  $G$  is a  $p$ -group, and then use the fact that a nilpotent group is the direct product of its Sylow subgroups.

Our proof of Schilling's Theorem follows that given in MO (41.9), and as a preliminary step, we review some facts about indices of skewfields and Hasse invariants. Let  $D$  be a skewfield with center  $K$  and index  $m$ , where  $K$  is an algebraic number field. For each prime  $P$  of  $K$ , let  $m_P$  be the local index of  $D$  at  $P$  (see the discussion preceding (51.14)). Note that if  $P$  is an infinite prime of  $K$ , then  $m_P = 1$  if  $P$  is a complex prime, or if  $P$  is real and  $D_P$  is a matrix algebra over  $K_P$ . On the other hand,  $m_P = 2$  if  $P$  is real and  $D_P$  is a matrix algebra over the real quaternions.

The relation between the global index  $m$  of  $D$  and the local indices  $\{m_P\}$  is given by

$$(74.13) \quad m = \text{least common multiple of } \{m_P : P = \text{prime of } K\}.$$

(see MO (32.19).)

For each prime  $P$  of  $K$ , we associate with the skewfield  $D$  an element  $\text{inv}_P D \in \mathbb{Q}/\mathbb{Z}$ , called the *Hasse invariant* of  $D$  at  $P$ , defined by  $\text{inv}_P D = r_P/m_P$ , with  $r_P \in \mathbb{Z}$ ,  $(r_P, m_P) = 1$ . Explicitly, we write

$$D_P \cong M_\kappa(\Omega), \quad \Omega = \text{skewfield with center } K_P \text{ and index } m_P.$$

For  $P$  an infinite prime, choose  $r_P = 1$  always, so  $\text{inv}_P D = 1/m_P \in \mathbb{Q}/\mathbb{Z}$ , and thus  $\text{inv}_P D$  is 0 or  $1/2 \pmod{\mathbb{Z}}$ . On the other hand, let  $P$  be a finite prime of  $K$ , and let  $W = K_P(\omega)$  be the unique unramified extension of  $K_P$  of degree  $m_P$ , where  $\omega$  is a root of 1. We may find a prime element  $\pi \in \Omega$  such that  $\pi^{m_P}$  is a prime element of the valuation ring of  $K_P$ , and such that

$$\Omega = \bigoplus_{i=0}^{m_P-1} W\pi^i, \quad \text{where} \quad \pi\omega\pi^{-1} = \omega^{r_P}.$$

Here,  $r_P$  is an integer uniquely determined  $(\pmod{m_P})$ , and  $(r_P, m_P) = 1$  (see MO, §14).

The Hasse invariants  $\{\text{inv}_P D\}$  satisfy the condition

$$(74.14) \quad \sum_P r_P/m_P \in \mathbb{Z},$$

where  $P$  ranges over all primes of  $K$ , including the infinite primes. (Indeed, this is the only restriction in the Hasse invariants. Given any set of fractions  $r_p/m_p$  in lowest terms, whose sum is an integer, and such that  $m_p = 1$  for complex  $P$ ,  $m_p = 1$  or 2 for real  $P$ , there always exists a skewfield  $D$  with prescribed Hasse invariants  $\{r_p/m_p\}$ ; see MO (32.12).)

We now prove:

**(74.15) Schilling's Theorem.** *Let  $G$  be a group of order  $p^r$ , where  $p$  is prime and  $r \geq 0$ . Let  $K$  be any field of characteristic 0.*

- (i) *For  $p$  odd, each simple component of  $KG$  is a full matrix algebra over a field.*
- (ii) *For  $p = 2$ , each simple component of  $KG$  has the form  $M_k(D)$ , where  $D$  is either a field or a skewfield of index 2.*

*Proof.* We begin with the case where  $K = \mathbb{Q}$ , so let  $M_k(D)$  be a simple component of  $\mathbb{Q}G$ , where  $D$  is a skewfield with center  $E$ . For each prime  $P$  of  $E$ , let  $m_P$  be the local index of  $D$  at  $P$ , and  $r_P/m_P$  its Hasse invariant. By (74.5ii),  $E \subseteq K(\omega)$  where  $\omega$  is a primitive  $p^r$ -th root of 1. By §4H, there is thus a unique prime  $P_0$  of  $E$  dividing  $p$ .

Now suppose  $p$  is odd; then the index  $m$  of  $D$  is odd, by (74.10ii), since  $m|p^r$ . It follows at once that  $m_P$  is odd for every prime  $P$  of  $E$ , so in particular no infinite prime  $P$  of  $E$  can have local index 2. The sum in (74.14) thus consists of a single term  $r_{P_0}/m_{P_0}$ , where  $r_{P_0} \in \mathbb{Z}$  and  $(r_{P_0}, m_{P_0}) = 1$ . It follows that  $m_{P_0} = 1$ , and therefore  $m = 1$  by (74.13). Thus  $D = E$ , as claimed.

On the other hand, for  $p = 2$  there may be real primes  $P$  of  $E$  such that  $m_P = 2$ . It follows from (74.14) that  $r_{P_0}/m_{P_0} = \frac{1}{2}$  or 1, so  $m_{P_0} = 1$  or 2. Thus  $m = 1$  or 2 by (74.13), so either  $D = E$  or else  $D$  is a skewfield of index 2; in the latter case, there must exist at least one real prime  $P$  of  $E$  such that  $D_P$  is the skewfield of real quaternions.

Now let  $K$  be arbitrary, and let  $B_j$  range over the simple components of  $\mathbb{Q}G$ . Then  $KG = \bigoplus (K \otimes_{\mathbb{Q}} B_j)$ . If  $E_j$  denotes the center of  $B_j$ , then

$$K \otimes_{\mathbb{Q}} B_j = (K \otimes_{\mathbb{Q}} E_j) \otimes_{E_j} B_j.$$

We may write  $K \otimes_{\mathbb{Q}} E_j = \bigoplus F_{ij}$ , with each  $F_{ij}$  a finite field extension of  $K$ . Since the index of  $F_{ij} \otimes_{E_j} B_j$  divides the index of  $B_j$  (Exercise 74.4), the theorem is proved.

This theorem was rediscovered by Witt and Roquette, with different proofs. As an immediate corollary, we have:

**(74.16) Corollary.** *Let  $G$  be a finite nilpotent group of order  $n$ , and let  $K$  be a field of characteristic 0. For  $n$  odd, each simple component of  $KG$  is a full matrix algebra over a field. For  $n$  even, each simple component is a full matrix algebra over a field or over a skewfield of index 2.*

*Proof.* Let  $G_{p_1}, \dots, G_{p_t}$  be the Sylow subgroups of  $G$ . Then  $G = G_{p_1} \times \cdots \times G_{p_t}$ , and so

$$KG \cong KG_{p_1} \otimes_K \cdots \otimes_K KG_{p_t}.$$

The result is then clear from Schilling's Theorem.

We now strengthen the previous results, and begin with:

**(74.17) Theorem.** *Let  $G$  be a  $p$ -group, where  $p$  is an odd prime. Then*

$$QG \cong Q \oplus \prod_{i=1}^t M_{n_i}(K_i),$$

where for  $1 \leq i \leq t$ ,  $K_i$  is a cyclotomic extension  $Q(\omega_i)$ , with  $\omega_i$  a  $p$ -power root of 1, and  $\dim_Q K_i > 1$ .

*Proof.* The simple component  $Q$  of  $QG$  corresponds to the trivial representation of  $G$ . Now let  $B$  be any simple component of  $QG$ , so its center  $K$  has the form  $K = Q(\zeta)$ , where  $\zeta \in \text{Irr } G$ , and thus  $K$  is a subfield of a cyclotomic field. If  $\zeta$  is a linear character, the values  $\{\zeta(x) : x \in G\}$  are  $p$ -power roots of 1, and clearly  $Q(\zeta)$  is a cyclotomic field; note that  $\dim_Q Q(\zeta) > 1$  if  $\zeta \neq 1$ .

We use induction on  $|G|$  to show that for each  $\zeta \in \text{Irr } G$ ,  $Q(\zeta)$  is a cyclotomic field. The result is clear from the above remarks when  $|G| = p$ , since then each  $\zeta \in \text{Irr } G$  is a linear character. Now assume the result for proper subgroups of  $G$ , and let  $\zeta \in \text{Irr } G$  be nonlinear. By Blitchfeldt's Theorem 11.3 we may write  $\zeta = \text{ind}_S^G \lambda$  for some linear character  $\lambda$  on a proper subgroup  $S$  of  $G$ . We may therefore write  $\zeta = \text{ind}_H^G \theta$  for some  $\theta \in \text{Irr } H$ , where  $H$  is a normal subgroup of  $G$  of index  $p$ . Then  $Q(\theta) = Q(\omega)$  for  $\omega$  some  $p$ -power root of 1, by the induction hypothesis. Clearly  $Q(\zeta) \subseteq Q(\theta)$ , and we shall now show that either  $Q(\zeta) = Q(\omega)$  or  $Q(\zeta) = Q(\omega^p)$ .

Let us write  $G = \langle H, g \rangle$ , where  $g^p \in H$ . For each  $i$ ,  $0 \leq i \leq p-1$ , let  $\theta_i \in \text{Irr } H$  be the character conjugate to  $\theta$ , defined by

$$\theta_i(x) = \theta(g^{-i}xg^i), \quad x \in H.$$

Since  $\zeta = \text{ind}_H^G \theta$  is irreducible, it follows from (10.25) that the characters  $\{\theta_i : 0 \leq i \leq p-1\}$  are distinct, and  $\text{ind}_H^G \theta_i = \zeta$  for each  $i$ . By Frobenius Reciprocity, these are the only irreducible characters of  $H$  which induce to  $\zeta$ . Since  $H \trianglelefteq G$ ,  $\zeta$  vanishes on  $G - H$ , and furthermore,

$$\zeta(x) = \sum_{i=0}^{p-1} \theta_i(x) = \sum_{i=0}^{p-1} \theta(g^{-i}xg^i) \quad \text{for } x \in H.$$

We note also that  $Q(\theta) = Q(\theta_i)$  for each  $i$ . The discussion now splits into two cases.

*Case 1.* Suppose that the map  $\theta \rightarrow {}^g\theta$  is induced by an automorphism  $\sigma$  of the field  $\mathbb{Q}(\theta)$ , that is, for some  $\sigma \in \text{Gal}(\mathbb{Q}(\theta)/\mathbb{Q})$  we have

$$\theta(g^{-1}xg) = (\theta(x))^\sigma \quad \text{for all } x \in H.$$

Then for  $x \in H$ ,

$$\zeta(x) = \sum_{i=0}^{p-1} (\theta(x))^{\sigma^i} = T_{\mathbb{Q}(\theta)/F} \theta(x),$$

where  $F$  is the subfield of  $\mathbb{Q}(\theta)$  fixed by  $\sigma$ , and  $T$  denotes the trace map. Since  $\theta(g^{-p}xg^p) = \theta(x)$  for  $x \in H$ , we have  $\sigma^p = 1$  and  $\sigma \neq 1$ . But  $\text{Gal}(\mathbb{Q}(\theta)/\mathbb{Q})$  is a cyclic group of order  $p^{k-1}(p-1)$ , for some  $k \geq 1$ . In this case, we must therefore have  $k \geq 2$ , and  $F$  is the unique subfield of  $\mathbb{Q}(\theta)$  with  $\dim_F \mathbb{Q}(\theta) = p$ . Thus in this case we have  $\mathbb{Q}(\theta) = \mathbb{Q}(\omega)$ , and  $\mathbb{Q}(\zeta) = F = \mathbb{Q}(\omega^p)$ , where  $\omega$  is a primitive  $p^k$ -th root of 1, and  $k \geq 2$ .

*Case 2.* Let  $\Omega = \text{Gal}(\mathbb{Q}(\theta)/\mathbb{Q})$ , and suppose that  ${}^g\theta \neq \theta^\sigma$  for any  $\sigma \in \Omega$ . We shall show that for each  $\sigma \in \Omega$ ,

$$(*) \quad \zeta^\sigma = \zeta \Leftrightarrow \theta^\sigma = \theta.$$

Since  $\mathbb{Q}(\zeta) \subseteq \mathbb{Q}(\theta)$ , this will imply that  $\mathbb{Q}(\zeta) = \mathbb{Q}(\theta)$ , as desired. To prove  $(*)$ , note that if  $\sigma \in \Omega$  fixes  $\theta$ , it also fixes  $\zeta$ . Conversely, let  $\sigma \in \Omega$  be such that  $\zeta^\sigma = \zeta$ . Then

$$\zeta = \zeta^\sigma = \sum_{i=0}^{p-1} (\theta_i)^\sigma,$$

so  $\sigma$  must permute the  $p$  characters  $\{\theta_i : 0 \leq i \leq p-1\}$ . If  $\theta^\sigma \neq \theta$ , then  $\sigma$  permutes them cyclically, and therefore  ${}^g\theta = \theta^{\sigma^j}$  for some  $j$ , contrary to the hypotheses of Case 2. Thus  $\theta^\sigma = \theta$ , as claimed, which proves  $(*)$ .

We have now shown that in both cases  $\mathbb{Q}(\zeta)$  is a cyclotomic field. It remains to show that  $\mathbb{Q}(\zeta) \supseteq \mathbb{Q}$  if  $\zeta \neq 1$ . If  $\zeta$  is not the trivial character, we may (after changing notation) assume that  $\zeta$  is a faithful irreducible character of  $G$ , where  $G$  is a nontrivial  $p$ -group. Then the center of  $G$  contains an element  $x \neq 1$ , and we must have  $\zeta(x) = \omega \zeta(1)$ , where  $\omega$  is a  $p$ -power root of 1,  $\omega \neq 1$ . Thus  $\dim_{\mathbb{Q}} \mathbb{Q}(\zeta) > 1$ . This completes the proof of the theorem.

Turning to the case of 2-groups, the situation is somewhat more complicated:

**(74.18) Theorem.** *Let  $G$  be a 2-group, and let  $M_n(D)$  be a simple component of  $\mathbb{Q}G$ , where  $D$  is a skewfield with center  $K$  and index  $m$ . Then  $m = 1$  or  $2$ , and  $K$  is a subfield of a cyclotomic field  $\mathbb{Q}(\omega)$ , with  $\omega$  a 2-power root of 1. In the case  $m = 2$ ,  $K$  must be a subfield of  $\mathbb{Q}(\omega + \omega^{-1})$ .*

Proof. The arguments used to prove (74.15) and (74.17) show that  $K \subseteq \mathbb{Q}(\omega)$

for some  $\omega$ , and there is a unique finite prime  $P_0$  of  $K$  dividing 2. Let  $m_p$  be the local index of  $D$  at  $P$ , for  $P$  a prime of  $K$ . Then  $m_p = 1$  for all finite primes  $P \neq P_0$ , while  $m_{P_0} = 1$  or 2. The latter case can only occur when  $m_p = 2$  for some real prime of  $K$ , by virtue of (74.14). Thus  $m = 1$  or 2, and when  $m = 2$ ,  $K$  must have at least one real prime. Thus  $K \subseteq Q(\omega + \omega^{-1})$  if  $m = 2$ .

**Remarks.** (i) For each subfield  $K$  of  $Q(\omega)$ , where  $\omega$  is a 2-power root of 1, there exists a 2-group  $G$  such that  $M_n(K)$  is a simple component of  $QG$ , for some  $n$ .

(ii) If  $G$  is a nilpotent group of odd order, then combining the results of (74.17) with those of (74.16), it follows that every simple component of  $QG$  is a full matrix algebra over a cyclotomic field  $Q(\sqrt[n]{1})$ , where  $n$  divides  $|G|$ .

(iii) For further results of this nature, see Feit [67, §14 and §16], and Rasmussen [74].

(iv) Let  $G$  be a finite group of exponent  $n$ , and let  $K$  be any field of characteristic 0. Let  $p$  be a prime, and suppose that a Sylow  $p$ -subgroup  $P$  of  $\text{Gal}(K(\sqrt[n]{1})/K)$  is cyclic. If  $|P|$  is even, assume further that  $\sqrt{-1} \in K$ . Then  $p/m_K(\zeta)$  for every irreducible complex character  $\zeta$  of  $G$ . This result, due to Goldschmidt-Isaacs [75], generalizes Schilling's Theorem 74.15.

### §74C. The Benard-Schacher Theorem

Let  $K$  be an algebraic number field. It is a natural question to ask which central simple  $K$ -algebras can occur as simple components of group algebras. If  $A$  is a central simple  $K$ -algebra occurring as a component of  $kH$ , where  $k$  is a subfield of  $K$  and  $H$  is a finite group, then by (74.5) and its proof we know that  $K = k(\zeta)$  for some  $\zeta \in \text{Irr } H$ , and that  $A$  is one of the simple components of  $KH$ . The Benard-Schacher Theorem is a beautiful and powerful result, which relates the index of  $A$  with the group of roots of 1 in  $K$ .

To fix the notation, let  $\varepsilon_m$  denote a primitive  $m$ -th root of 1 over  $Q$ . For a f.d. central simple  $K$ -algebra  $B$ , we may write  $B \cong M_k(D)$  where  $D$  is a skewfield with center  $K$ . We define

$$\text{index of } B = \text{index of } D = m, \quad \text{where } \dim_K D = m^2.$$

For each prime  $P$  of  $K$ , whether finite or infinite, the  $P$ -adic completion  $B_P$  is a central simple  $K_P$ -algebra; its index  $m_p$  is called the *local index* of  $B$  at  $P$ . We also consider the *Hasse invariant* of  $B$  at  $P$ , denoted by  $\text{inv}_P B$ , defined as in §74B. This invariant is an element of  $Q/Z$  of the form  $\text{inv}_P B = r_P/m_p$ , where  $r_P \in Z$  and  $(r_P, m_p) = 1$ .

The main result of this subsection is the following theorem, proved by Benard-Schacher [72]:

**(74.20) Benard-Schacher Theorem.** *Let  $K$  be an algebraic number field, and let*

*A be a central simple K-algebra occurring as a simple component of a group algebra kH, where k is a subfield of K, and H is a finite group. Let m be the index of A. Then*

- (i) *K contains  $\varepsilon_m$ .*
- (ii) *For each prime P of K and each  $\sigma \in \text{Aut}_\mathbb{Q} K$ ,*

$$(74.21) \quad \text{inv}_P A \equiv r \cdot \text{inv}_{P^\sigma} A \pmod{\mathbb{Z}},$$

*where  $\sigma(\varepsilon_m) = \varepsilon_m^r$ , and where  $P^\sigma$  is the conjugate (under  $\sigma$ ) of the prime P. Consequently,*

$$(74.22) \quad m_p(A) = m_{P^\sigma}(A) \quad \text{for each } \sigma \in \text{Aut}_\mathbb{Q} K.$$

As a first step in the proof, let us review some facts about the Brauer group  $B(K)$  of the algebraic number field  $K$ ; for details, see MO, §§ 28, 32, for example. Let  $A$  and  $A'$  be f.d. central simple  $K$ -algebras; we call them *similar*, and write  $A \sim A'$ , if there is an isomorphism of  $K$ -algebras

$$M_n(K) \otimes_K A \cong M_{n'}(K) \otimes_K A'$$

for some integers  $n, n'$ . The similarity classes  $[A]$  of such algebras, with multiplication defined via  $\otimes_K$ , form an abelian group  $B(K)$ , the *Brauer group* of  $K$ . For each prime  $P$  of  $K$ , the map

$$\text{inv}_P : B(K) \rightarrow \mathbb{Q}/\mathbb{Z},$$

which maps each class  $[A] \in B(K)$  onto its Hasse invariant  $\text{inv}_P A$ , is a well-defined homomorphism. The set of values  $\{\text{inv}_P A\}$ , as  $P$  varies over the primes of  $K$  (including the infinite ones), uniquely determines the element  $[A] \in B(K)$ .

Now let  $L$  be a finite Galois extension of  $K$ , with Galois group  $G = \text{Gal}(L/K)$ . We denote by  $B(L/K)$  the subgroup of  $B(K)$  consisting of all central simple  $K$ -algebras split by  $L$ . (Every element of  $B(K)$  lies in some  $B(L/K)$ .) There is an isomorphism

$$(74.23) \quad H^2(G, L) \cong B(L/K),$$

defined thus: given any factor set  $f : G \times G \rightarrow L$ , we may form the *crossed-product algebra*

$$(74.24) \quad (L/K, f) = \bigoplus_{x \in G} Lu_x,$$

whose structure is given by the formula

$$(74.25) \quad u_x u_y = f(x, y) u_{xy}, \quad u_x a = (xa) u_x \quad \text{for } a \in L, \quad x, y \in G.$$

The isomorphism in (74.23) maps the cohomology class of  $f$  onto the class of  $(L/K, f)$  in  $B(L/K)$ .

We recall finally that if  $A$  is a central simple  $K$ -algebra of index  $m$ , then  $m$  is also the order of  $[A]$  as an element of  $B(K)$ ; see MO (32.19). We have already noted that

$$m = \text{least common multiple of all } \{m_p\},$$

where  $P$  ranges over all primes of  $K$ .

The simplified proof of the Benard-Schacher Theorem given below is based on the work of Janusz [72]. The authors wish to thank G. Janusz for many helpful conversations during the preparation of the material which follows. As we shall see, the proof depends strongly on an extended form of the Brauer-Witt Theorem, to be established in (74.38) and (74.39) below. This latter theorem enables us to reduce the proof of the Benard-Schacher Theorem to the case of cyclotomic algebras. These are a special kind of crossed-product algebra, defined as follows. Let  $L = K(\omega)$  be a cyclotomic extension of the algebraic number field  $K$ , where  $\omega$  is a root of 1, and let  $G = \text{Gal}(L/K)$ . Then  $G$  is abelian, a fact needed later. Let  $f:G \times G \rightarrow \langle \omega \rangle$  be a factor set with values in the cyclic group  $\langle \omega \rangle$ . The crossed-product algebra  $(L/K, f)$  is called a *cyclotomic algebra*. As we shall see in (74.39), every central simple  $K$ -algebra  $B$ , which occurs as a component of a group algebra, must be similar to some cyclotomic algebra  $A$ . It thus suffices to establish (74.20) for  $A$  rather than  $B$ , since similar  $K$ -algebras have the same index and the same set of Hasse invariants.

Continuing with the proof of the Benard-Schacher Theorem, let  $A = (L/K, f)$  be a cyclotomic algebra of index  $m$ , where  $L = K(\omega)$  and  $G = \text{Gal}(L/K)$  as above, and where  $f:G \times G \rightarrow \langle \omega \rangle$  is a factor set. The values of  $f$  generate a cyclic subgroup  $\langle \zeta \rangle$  of  $\langle \omega \rangle$ , so now  $f:G \times G \rightarrow \langle \zeta \rangle$ . Each  $\sigma \in \text{Aut}_Q K$  lifts to an element  $\bar{\sigma} \in \text{Aut}_Q L$ , though not in a unique manner. We define a map

$$\bar{\sigma}f:G \times G \rightarrow \langle \zeta \rangle \text{ by } (\bar{\sigma}f)(x, y) = \bar{\sigma}\{f(x, y)\} \quad \text{for } x, y \in G.$$

The condition, that  $f$  be a factor set, is as follows:

$$(xf(y, z))f(x, yz) = f(x, y)f(xy, z) \quad \text{for all } x, y, z \in G.$$

Since the actions of  $\bar{\sigma}$  and  $x$  on  $\langle \zeta \rangle$  commute, it follows easily that  $\bar{\sigma}f$  is also a factor set. If  $\tilde{\sigma} \in \text{Aut}_Q L$  is another lifting of  $\sigma$ , we have

$$(L/K, \bar{\sigma}f) \cong (L/K, \tilde{\sigma}f)$$

by Exercise 74.5. Thus the class of  $(L/K, \bar{\sigma}f)$  in  $B(L/K)$  depends only on  $\sigma$ , and will be denoted by  $[\sigma A]$ . If  $\bar{\sigma}(\zeta) = \zeta^r$ , then  $\bar{\sigma}f = f^r$ , and therefore (by (74.23))

$$[\sigma A] = [A]^r \quad \text{in } B(L/K).$$

Keeping the above notation, suppose that  $\zeta$  has order  $n$ . Then  $f^n = 1$ , so  $[A]^n = 1$  in  $B(L/K)$ . Since  $[A]$  has order  $m$  in  $B(L/K)$ , it follows that  $m$  divides  $n$ . Therefore  $\varepsilon_m \in \langle \zeta \rangle$ , and so  $\bar{\sigma}(\varepsilon_m) = \varepsilon_m^r$ . We now apply these arguments to the case where  $\sigma = 1$ . In this situation  $[\sigma A] = [A]$ , so we obtain  $[A] = [A]^r$ . Therefore  $r \equiv 1 \pmod{m}$  and  $\bar{\sigma}(\varepsilon_m) = \varepsilon_m$ . This shows that every  $\bar{\sigma} \in \text{Gal}(L/K)$  fixes  $\varepsilon_m$ , so  $\varepsilon_m \in K$ , and we have proved the first part of the Benard-Schacher Theorem.

For the second part, let  $\sigma \in \text{Aut}_\mathbb{Q} K$  be arbitrary, and let  $P$  be any prime of  $K$ . The automorphism  $\sigma$  of  $K$  maps  $P$  onto a conjugate prime  $P^\sigma$ , and induces an isomorphism  $\sigma: K_P \cong K_{P^\sigma}$ . We now construct an isomorphism

$$\psi: K_P \otimes_K (L/K, f) \cong K_{P^\sigma} \otimes_K (L/K, \bar{\sigma}f)$$

as follows. Let  $(L/K, f)$  be as in (74.24), and correspondingly let

$$(L/K, \bar{\sigma}f) = \bigoplus_{x \in G} Lv_x, \quad \text{where} \quad v_x v_y = \bar{\sigma}f(x, y) v_{xy} \quad \text{for } x, y \in G.$$

Define  $\psi$  by the formula

$$\psi(a \otimes bu_x) = \sigma(a) \otimes \bar{\sigma}(b)v_x \quad \text{for } a \in K_p, \quad b \in L, \quad x \in G.$$

It is easily verified that for  $k \in K$ ,

$$\psi(ak \otimes bu_x) = \psi(a \otimes kbu_x),$$

so  $\psi$  is well defined. Clearly  $\psi$  is an isomorphism of simple algebras over local fields, and so these algebras have the same Hasse invariant. Therefore

$$\text{inv}_P A = \text{inv}_{P^\sigma} [\sigma A].$$

But  $[\sigma A] = [A]^r$ , where  $\sigma(\varepsilon_m) = \varepsilon_m^r$ ; since  $\text{inv}_{P^\sigma}: B(L/K) \rightarrow \mathbb{Q}/\mathbb{Z}$  is a homomorphism, we obtain

$$\text{inv}_{P^\sigma} [\sigma A] = r \cdot \text{inv}_{P^\sigma} [A],$$

as desired.

Finally, as remarked in §74B, the Hasse invariant  $\text{inv}_P A$  is a fraction in lowest terms, with denominator the local index  $m_P(A)$ . Since  $m_P$  divides the index  $m$  of  $A$ , and the integer  $r$  is relatively prime to  $m$ , we see that (74.22) is a direct consequence of (74.21). This completes the proof of the Benard-Schacher Theorem.

**Remark.** If  $K$  is a finite extension of a  $p$ -adic field  $\mathbb{Q}_p$ , where  $p$  is a rational prime, then part (i) of the Benard-Schacher Theorem remains valid. This is clear from the preceding proof, and the proof of the Brauer-Witt Theorem below. Assertion (74.20ii) does not apply in this local case.

We now give some immediate consequences of the above results to the theory of the Schur index  $m_K(\zeta)$  for  $\zeta \in \text{Irr } G$ , where  $G$  is any finite group. The first corollary is merely a restatement of the Benard-Schacher Theorem for our case.

**(74.26) Theorem.** *Let  $\zeta$  be an irreducible complex character of a finite group  $G$ , and let  $K = \mathbb{Q}(\zeta)$ . Let\**

$$m = m_{\mathbb{Q}}(\zeta) = m_K(\zeta)$$

*be the Schur index of  $\zeta$ . Then*

- (i)  *$K$  contains all  $m$ -th roots of 1.*
- (ii) *Let  $P$  and  $P'$  be primes of  $K$  lying over the same prime  $p$  of  $\mathbb{Q}$ , where  $p$  is either a rational prime number or  $p = \infty$ . Then*

$$m_{K_P}(\zeta) = m_{K_{P'}}(\zeta),$$

*that is,  $\zeta$  has the same Schur indices over the complete fields  $K_P$  and  $K_{P'}$ .*

It follows from (ii) that for each  $\zeta \in \text{Irr } G$  and each  $p$  the Schur index of  $m_{\mathbb{Q}_p}(\zeta)$  is well defined (as the common value of all  $m_{K_p}(\zeta)$ , where  $P$  extends  $p$ ), and is independent of the embedding of  $\mathbb{Q}(\zeta)$  into the algebraic closure of  $\mathbb{Q}_p$ .

Next, we have:

**(74.27) Brauer-Speiser Theorem.** *Let  $\zeta \in \text{Irr } G$  be real-valued. Then  $m_{\mathbb{Q}}(\zeta) = 1$  or 2, and  $m_{\mathbb{Q}}(\zeta) = 1$  if  $\zeta(1)$  is odd.*

*Proof.<sup>†</sup>* The only roots of 1 in  $\mathbb{Q}(\zeta)$  are  $\pm 1$ , so  $m_{\mathbb{Q}}(\zeta) = 1$  or 2. Further,  $m_{\mathbb{Q}}(\zeta)$  divides  $\zeta(1)$  by (74.8ii).

We now take up the proof of the Brauer-Witt Theorem, and its corollary that simple components of group algebras are similar to cyclotomic algebras. For the rest of our discussion,  $K$  may be any field of characteristic 0. As usual,  $\text{Irr } G$  denotes the set of irreducible complex characters of a finite group  $G$ . A character of  $G$  afforded by a  $KG$ -module is called a  $K$ -character of  $G$ . On the other hand, a character  $\eta$  of  $G$ , such that  $K(\eta) = K$ , is said to *lie in  $K$* .

By (74.5), for each  $\zeta \in \text{Irr } G$  there is a unique simple component  $A(K, \zeta)$  of  $KG$ , affording a  $K$ -character  $\eta$  of  $G$ , such that

$$\eta = m(\zeta_1 + \cdots + \zeta_t), \quad \text{where} \quad t = \dim_K K(\zeta),$$

and  $m = m_K(\zeta)$ . The  $\{\zeta_i\}$  are the distinct algebraic conjugates of  $\zeta$  under the action of  $\text{Gal}(K(\zeta)/K)$ , and are called the *Galois conjugates of  $\zeta$  over  $K$* . We have seen

\*In general,  $m_{\mathbb{Q}}(\zeta) = m_{\mathbb{Q}(\zeta)}\zeta$ , by (74.12).

<sup>†</sup>The Benard-Schacher Theorem is not required for the proof of (74.27). As an exercise, the reader can give a proof using (73.9) and (74.8ii).

that  $A(K, \zeta)$  has center  $K(\zeta)$ , and that

$$K(\zeta) \otimes_K A(K, \zeta) \cong \bigoplus_i A(K, \zeta_i).$$

In particular, for each  $\zeta \in \text{Irr } G$ ,

$$(74.28) \quad A(K(\zeta), \zeta) \cong A(K, \zeta), \quad m_{K(\zeta)}(\zeta) = m_K(\zeta).$$

In proving that each  $A(K, \zeta)$  is similar to a cyclotomic algebra, there is thus no loss of generality in assuming that  $K(\zeta) = K$ .

We shall follow the treatment of Yamada [74], with minor variations. Let us first recall the Witt-Berman Induction Theorem 21.6. Let  $\varepsilon_n$  be a primitive  $n$ -th root of 1, where  $G$  has exponent  $n$ , and let  $p$  be prime. A subgroup  $H \leq G$  is called  $(K, p)$ -elementary if  $H = \langle a \rangle \rtimes P$ , where  $\langle a \rangle$  is a cyclic  $p$ -group,  $P$  is a  $p$ -group, and for  $i \in \mathbb{Z}$ ,

$$a \text{ is } H\text{-conjugate to } a^i \Leftrightarrow \varepsilon_n \text{ is algebraically conjugate to } \varepsilon_n^i \text{ over } K.$$

(See §21.)

Examining the proof of (21.6), we find readily that the following stronger version is valid:

**(74.29) Witt-Berman Induction Theorem.** *Let  $p$  be prime, and let  $r \in \mathbb{Z}$  be prime to  $p$ . Denote by  $1_G$  the 1-character of  $G$ . Then  $r \cdot 1_G$  is a  $\mathbb{Z}$ -linear combination of induced characters  $\mu_i^G$ , where for each  $i$ ,  $\mu_i$  is a  $K$ -character of some  $(K, p)$ -elementary subgroup of  $G$ .*

We begin with an easy corollary, which slightly improves CR (70.25). As usual, let  $(\zeta, \eta)$  or  $(\zeta, \eta)_G$  denote inner products of characters, defined as in (9.22).

**(74.30) Lemma.** *Let  $p$  be prime, let  $\zeta \in \text{Irr } G$ , and let  $F$  be a field such that*

$$K(\zeta) \subseteq F \subseteq K(\varepsilon_m), \quad \dim_F K(\varepsilon_m) = \text{power of } p.$$

*Then there exist an  $(F, p)$ -elementary subgroup  $H$  of  $G$  and a character  $\xi \in \text{Irr } H$  such that*

$$p \nmid (\zeta_H, \xi) \quad \text{and} \quad F(\xi) = F.$$

*Proof.* Let  $r$  be the  $p'$ -part of  $|G|$ . By (74.29) we may write  $r \cdot 1_G = \sum a_i \mu_i^G$ , with  $\mu_i$  an  $F$ -character of an  $(F, p)$ -elementary subgroup  $H_i$  of  $G$ . Then

$$r\zeta = \sum a_i \zeta \mu_i^G = \sum a_i (\mu_i \cdot \zeta_{H_i})^G.$$

For  $H \leq G$  and  $\xi \in \text{Irr } H$ , let  $\text{Tr}_F(\xi)$  be the sum of the Galois conjugates of  $\xi$

over  $F$ . Each character  $\mu$  of  $H$  lying in  $F$  is then a  $\mathbb{Z}$ -linear combination of such traces  $\text{Tr}_F(\xi)$ , with  $\xi \in \text{Irr } H$ . We may apply this to each character  $\mu_i \cdot \zeta_{H_i}$  above, which lies in  $F$  since both  $\mu_i$  and  $\zeta$  lie in  $F$ . Therefore we may write

$$r\zeta = \sum b_i (\text{Tr}_F \xi_i)^G, \quad b_i \in \mathbb{Z}, \quad \xi_i \in \text{Irr } H_i.$$

Consequently we obtain

$$r = (\zeta, \sum b_i (\text{Tr}_F \xi_i)^G) = \sum b_i (\zeta_{H_i}, \text{Tr}_F \xi_i)_{H_i}.$$

But  $(\zeta_{H_i}, \xi_i) = (\zeta_{H_i}, \xi'_i)$  for each  $F$ -conjugate  $\xi'_i$  of  $\xi_i$ , since  $\zeta_{H_i}$  lies in  $F$ . If  $d_i = \dim_F F(\xi_i)$ , there are  $d_i$  such  $\{\xi'_i\}$ , and so

$$r = \sum b_i d_i (\zeta_{H_i}, \xi_i)_{H_i}.$$

Since  $p \nmid r$ , there is a subscript  $j$  for which  $p \nmid d_j (\zeta_{H_j}, \xi_j)$ . Therefore  $d_j = 1$ , since  $d_j$  divides  $\dim_F K(\xi_m)$ . Thus we obtain  $F(\xi_j) = F$  and  $p \nmid (\zeta_{H_j}, \xi_j)$ , which proves the lemma.

As our next step, let us show how cyclotomic algebras arise from group representations. By definition, a *cyclotomic algebra* is a crossed-product algebra  $(L/K, f)$ , where  $L = K(\omega)$  with  $\omega$  a root of 1, and  $f$  is a factor set on  $\text{Gal}(L/K)$  whose values are roots of 1 in  $L$ . We may assume that the values of  $f$  lie in  $\langle \omega \rangle$ , since we can always replace  $\omega$  by  $\omega'$ , where  $\langle \omega' \rangle = \langle \omega, \text{im } f \rangle$ .

**(74.31) Proposition.** *Let  $\zeta \in \text{Irr } G$ , and let  $K(\zeta) = K$ . Suppose that  $\zeta = \psi^G$  for some linear character  $\psi$  of  $N$ , where  $N \trianglelefteq G$ , and put  $\mathfrak{G} = \text{Gal}(K(\psi)/K)$ . Define*

$$(74.32) \quad G_0 = \{x \in G : {}^x \psi = \tau(x)\psi \quad \text{for some} \quad \tau(x) \in \mathfrak{G}\},$$

and set  $\psi_0 = \psi^{G_0}$ . Then  $\psi_0 \in \text{Irr } G_0$ ,  $K(\psi_0) = K$ , and the simple component  $A(K, \psi_0)$  of  $KG_0$ , which corresponds to  $\psi_0$ , is a cyclotomic algebra  $(K(\psi)/K, f)$  for some factor set  $f$ .

*Proof.* Step 1. Suppose first that  $\psi \in \text{Irr } N$ , but  $\psi$  need not be linear. For  $x \in G$ , the  $G$ -conjugate  ${}^x \psi$  of  $\psi$  also lies in  $\text{Irr } N$  (see §10B), and we have for  $n \in N$ ,  $x, y \in G$ :

$$({}^x \psi)n = \psi(n^x), \quad \text{and} \quad {}^{xy} \psi = {}^x({}^y \psi).$$

Next, for each  $\tau \in \mathfrak{G}$ ,  $\tau\psi$  is the Galois conjugate of  $\psi$  over  $K$  defined by  $(\tau\psi)n = \tau(\psi(n))$ ,  $n \in N$ . By Exercise 9.14,  $\tau\psi \in \text{Irr } N$ .

Let us set  $G = \bigcup_{i=1}^d Nx_i$ . Since  $\zeta = \psi^G$  is irreducible, it follows from (10.25) that the  $G$ -conjugates  $\{{}^{x_i} \psi\}$  are distinct. Further, since  $N \trianglelefteq G$ ,

$$\zeta = \psi^G = \sum_{i=1}^d {}^{x_i} \psi,$$

where  $\dot{\psi} = \psi$  on  $N$  and  $\dot{\psi} = 0$  on  $G - N$  (see (10.2)). In particular,

$$\zeta_N = \sum_i x_i \psi.$$

Note also that  $\mathfrak{G}$  is abelian.

Define  $G_0$  by (74.32); each  $x \in G_0$  determines a unique  $\tau(x) \in \mathfrak{G}$ , and the map  $x \rightarrow \tau(x)$  gives a homomorphism from  $G_0$  into  $\mathfrak{G}$ , with kernel  $N$ . Now write

$$G_0 = \bigcup_{i=1}^t Nx_i, \quad t = |G_0:N|, \quad \text{and set } \tau_i = \tau(x_i) \in \mathfrak{G}.$$

Then we have

$$G_0/N = \{\tau_1, \dots, \tau_t\} \leq \mathfrak{G}.$$

Setting  $\psi_0 = \psi^{G_0}$ , we shall now prove

$$(74.33) \quad \psi_0 \in \text{Irr } G_0, \quad K(\psi_0) = K, \quad \text{and} \quad \{\tau_1, \dots, \tau_t\} = \mathfrak{G}$$

First of all, from  $\zeta = \psi_0^G$  we conclude that  $\psi_0 \in \text{Irr } G_0$ . Next,

$$\psi_0 = \sum_{i=1}^t x_i \psi = \sum_i \tau_i \dot{\psi}.$$

Therefore  $\tau_j \psi_0 = \psi_0$  for each  $j$ , and therefore  $\tau_j \in \text{Gal}(K(\psi)/K(\psi_0))$ . Conversely, if  $\sigma \in \text{Gal}(K(\psi)/K(\psi_0))$ , then  $\sigma \psi_0 = \psi_0$ , so  $\sigma \psi = \tau_i \psi$  for some  $i$ , and then  $\sigma = \tau_i$ . We have thus shown that

$$\{\tau_1, \dots, \tau_t\} = \text{Gal}(K(\psi)/K(\psi_0)).$$

On the other hand, for  $\sigma \in \mathfrak{G}$  we have  $\sigma \zeta = \zeta$ , so  $\sigma$  permutes the  $G$ -conjugates  $\{x_i \psi : 1 \leq i \leq d\}$ , where  $d = |G:N|$ . In particular,  $\sigma \psi = x_i \psi$  for some  $i$ , and then  $x_i \in G_0$ , by the definition of  $G_0$ . Therefore  $\sigma = \tau_i$ , so we have proved that

$$\text{Gal}(K(\psi)/K(\psi_0)) = \text{Gal}(K(\psi)/K).$$

Thus  $K(\psi_0) = K$ , and (74.33) is established.

*Step 2.* Keeping the above notation, suppose hereafter that  $\psi$  is linear, and let  $G_0 = \dot{\cup} Nx_i$  as above, where  $1 \leq i \leq t = |G_0:N|$ . For  $1 \leq i, j \leq t$ , we may write

$$x_i x_j = n_{ij} x_{\pi(i,j)} \quad \text{with} \quad n_{ij} \in N, \quad 1 \leq \pi(i,j) \leq t.$$

Now define

$$f: \mathfrak{G} \times \mathfrak{G} \rightarrow \langle \text{values of } \psi \rangle \quad \text{by} \quad f(\tau_i, \tau_j) = \psi(n_{ij}), \quad 1 \leq i, j \leq t.$$

It is easily checked that  $f$  is a factor set whose values are roots of 1. We form the cyclotomic algebra

$$(L/K, f) = \bigoplus_{i=1}^t Lu_i, \quad \text{where } L = K(\psi),$$

with multiplication defined by

$$u_i u_j = f(\tau_i, \tau_j) u_{\pi(i,j)}, \quad u_i \cdot a = (\tau_i a) u_i \quad \text{for } a \in L.$$

It remains for us to prove that  $A(K, \psi_0) \cong (L/K, f)$ .

We may view  $L$  as a simple left  $KN$ -module, with  $n \in N$  acting on  $L$  as left multiplication by  $\psi(n)$ . Thus  $L$  affords the representation  $\psi$  of  $N$ , and  $\psi_0$  is afforded by the induced module

$$V = KG_0 \otimes_{KN} L = \bigoplus_{i=1}^t x_i \otimes L.$$

By (74.5),  $A(K, \psi_0)$  is isomorphic to the algebra  $(KG_0)_l$  of left multiplications on  $V$ . Now  $(KG_0)_l$  is spanned over  $K$  by the  $t^2$  products  $(x_i)_l \psi(n_j)$ ,  $1 \leq i, j \leq t$ , where the  $n_j \in N$  are chosen so that  $L = \bigoplus K\psi(n_j)$ . Thus  $\dim_K (KG_0)_l \leq t^2$ . On the other hand, there is a surjective homomorphism

$$(KG_0)_l \rightarrow (L/K, f), \quad \text{given by } (x_i)_l \rightarrow u_i, \quad a_l \rightarrow a,$$

for  $1 \leq i \leq t$ ,  $a \in L$ . This shows that  $(KG_0)_l \cong (L/K, f)$ , and the proposition is proved.

We shall apply the preceding proposition to a  $(K, p)$ -elementary group  $G$  and a character  $\zeta \in \text{Irr } G$  lying in  $K$ . Our object is to show that  $\zeta = \psi^G$  for some linear character  $\psi$  of a subgroup  $N$  of  $G$ , such that  $\psi^H$  lies in  $K$  for a suitable  $H$  containing  $N$ . Specifically, we show:

**(74.34) Proposition.** *Let  $G = \langle a \rangle \rtimes P$  be a  $(K, p)$ -elementary group, where  $\langle a \rangle$  is a cyclic  $p'$ -group and  $P$  is a  $p$ -group. Let  $\zeta \in \text{Irr } G$  lie in  $K$ . Then there exist groups  $N \leq H \leq G$ , and a linear character  $\psi$  of  $N$ , such that*

- (i)  $\zeta = \psi^G$ , and  $\langle a \rangle \leq N \trianglelefteq H$ .
- (ii) Each  $H$ -conjugate of  $\psi$  is a Galois conjugate of  $\psi$  over  $K$ .
- (iii)  $K(\psi^H) = K$ .

*Proof.* We use induction on  $|G|$ . Let  $T$  be a minimal normal subgroup of  $G$  such that

$$\begin{cases} \zeta = \theta^G \text{ for some } \theta \in \text{Irr } T, \text{ where every } G\text{-conjugate of } \theta \\ \text{is a Galois conjugate of } \theta \text{ over } K. \end{cases}$$

Since  $G$  itself satisfies the above condition, the existence of  $T$  is obvious.

If  $\theta(1) = 1$ , we need only choose  $N = T$ ,  $H = G$ , and  $\psi = \theta$ . For the rest of the proof, assume  $\theta(1) > 1$ . By Exercise 74.6,  $\theta$  is induced from a linear character of some proper subgroup of  $T$ . Therefore  $\theta = \rho^T$  for some  $\rho \in \text{Irr } S$  and some  $S \leq T$  of index  $p$ . Since  $\zeta = \theta^G = \rho^G$ , Exercise 74.6 shows that  $\langle a \rangle \leq S$ , and then necessarily  $S \triangleleft T$ . We shall use this information to construct a subgroup  $E < G$  and a character  $\lambda \in \text{Irr } E$ , such that  $\zeta = \lambda^G$  and  $K(\lambda) = K$ . The desired result will then follow by applying the induction hypothesis to  $E$  and  $\lambda$ .

Given  $S \triangleleft T$  of index  $p$ , and  $\theta = \rho^T \in \text{Irr } T$ , as above, we note first that  $\theta = 0$  on  $T - S$ . We wish to replace  $S$  by a subgroup  $T_0 < T$ , also of index  $p$ , such that  $T_0 \triangleleft G$ . For this purpose, define

$$X = \bigcap_{x \in G} {}^x S \triangleleft G, \quad \text{so} \quad X < T.$$

Then  $\langle a \rangle \leq X$ , and thus  $G/X$  is a  $p$ -group. We may then choose  $T_0 \triangleleft G$  such that

$$X \leq T_0 < T \trianglelefteq G, \quad |T:T_0| = p.$$

Now  $\theta = 0$  on  $T - S$ , and every  $G$ -conjugate of  $\theta$  is a Galois conjugate of  $\theta$ , so  $\theta = 0$  on  $T - X$ , and thus also on  $T - T_0$ . This gives

$$(\theta_{T_0}, \theta_{T_0}) = |T_0|^{-1} \sum_{t \in T_0} \theta(t)\theta(t^{-1}) = |T_0|^{-1} \sum_{t \in T} \theta(t)\theta(t^{-1}) = p.$$

By §11B, we deduce that  $\theta_{T_0}$  is a sum of  $p$  distinct  $T$ -conjugates of some  $\varphi \in \text{Irr } T_0$ , and that  $\theta = \varphi^T$ . Therefore  $\zeta = \varphi^G$ .

From the minimality of  $T$ , it follows that  $\text{Gal}(K(\varphi)/K)$  does *not* act transitively on the  $G$ -conjugates of  $\varphi$ . Setting

$$E = \{x \in G : {}^x \varphi = \tau(x)\varphi \quad \text{for some} \quad \tau(x) \in \text{Gal}(K(\varphi)/K)\},$$

it follows that  $\langle a \rangle \leq T_0 \leq E < G$ , and  $T_0 \trianglelefteq G$ . By Step 1 of the proof of (74.31), we obtain  $\zeta = (\varphi^E)^G$  and  $K(\varphi^E) = K$ . The existence of the desired groups  $N$  and  $H$ , and of the linear character  $\psi$  of  $N$ , now follows by applying the induction hypothesis to the group  $E$  and its irreducible character  $\varphi^E$ .

Continuing with the preliminary steps required for the Brauer-Witt Theorem, we now review some additional properties of the Brauer group  $B(K)$ . Let  $[A] \in B(K)$  have index  $m$  and order  $e$ . If  $K$  is an algebraic number field, or more generally any global field, then  $m = e$  (see MO (32.19)). In the case of arbitrary  $K$ , we can only assert that

$e|m$ , and  $e, m$  have the same prime factors (apart from multiplicity)

(see MO (29.22), (29.24)). This will suffice for our discussion below.

For a prime  $p$ , let  $B(K)_p$  be the  $p$ -torsion subgroup of  $B(K)$ . Each  $x \in B(K)$  is uniquely expressible as a product of  $p$ -torsion elements for various primes  $p$ .

More precisely, let  $D$  be a skewfield with center  $K$  and index  $m$ , and write  $m = \prod_{i=1}^t p_i^{e_i}$ , where the  $\{p_i\}$  are distinct primes and each  $e_i \geq 1$ . By MO, Exercise 29.7, there exist skewfields  $\{D_1, \dots, D_t\}$  where  $D_i$  has center  $K$  and index  $p_i^{e_i}$ , such that

$$D \cong D_1 \otimes_K \cdots \otimes_K D_t.$$

Thus in  $B(K)$  we have

$$[D] = \prod_{i=1}^t [D_i];$$

we call  $[D_i]$  the  $p_i$ -part of  $[D]$ , and write  $[D_i] = [D]_{p_i}$ . For  $p \nmid m$ , put  $[D]_p = 1$ .

Using these ideas, we shall prove:

**(74.35) Proposition.** *Given  $H \leq G$ ,  $\xi \in \text{Irr } H$ ,  $\zeta \in \text{Irr } G$ , where  $(\zeta_H, \xi) > 0$ , let  $K$  be a field with  $K(\zeta) = K(\xi) = K$ . Let  $A(K, \xi)$  and  $A(K, \zeta)$  be the simple components of  $KH$  and  $KG$ , respectively, corresponding to  $\xi$  and  $\zeta$ . Then  $A(K, \xi)$  and  $A(K, \zeta)$  are central simple  $K$ -algebras, and*

$$[A(K, \xi)]_p = [A(K, \zeta)]_p \quad \text{in } B(K)$$

for each prime  $p$  not dividing  $(\zeta_H, \xi)$ .

*Proof.* Let  $r = (\zeta_H, \xi)$ , and let  $p$  be a prime such that  $p \nmid r$ . Let  $\varepsilon$  be a primitive  $n$ -th root of 1, where  $G$  has exponent  $n$ . There is a unique field  $F$  such that

$$(74.36) \quad K \subseteq F \subseteq K(\varepsilon), \quad p \nmid \dim_K F, \quad \dim_F K(\varepsilon) = \text{power of } p.$$

By (74.5),  $A(K, \xi)$  and  $A(K, \zeta)$  are simple algebras with center  $K$ , while  $A(F, \xi)$  and  $A(F, \zeta)$  are simple algebras with center  $F$ . Further,

$$F \otimes_K A(K, \xi) \cong A(F, \xi), \quad F \otimes_K A(K, \zeta) \cong A(F, \zeta).$$

We note next that  $K(\varepsilon)$  is a splitting field for both of the central simple  $F$ -algebras  $A(F, \xi)$  and  $A(F, \zeta)$ , so by Exercise 74.4 their indices must divide  $\dim_F K(\varepsilon)$ , and are therefore powers of  $p$ . Since the homomorphism  $B(K)_p \rightarrow B(F)_p$ , defined by  $F \otimes_K *$ , is injective (see Exercise 74.7), the proposition will follow once we prove that

$$[A(F, \xi)] = [A(F, \zeta)] \quad \text{in } B(F).$$

Before proving this, we note for later use that, by the preceding discussion,

$$(74.37) \quad p\text{-part of } m_K(\zeta) = m_F(\zeta), \quad p\text{-part of } m_K(\xi) = m_F(\xi).$$

In order to show that  $[A(F, \xi)] = [A(F, \zeta)]$  in  $B(F)$ , we need some easy facts

about tensor products of simple components of group algebras. Given groups  $G_1$ ,  $G_2$  and characters  $\zeta_i \in \text{Irr } G_i$ ,  $i = 1, 2$ , let  $F$  be a field of characteristic 0 such that both  $\zeta_1$  and  $\zeta_2$  lie in  $F$ . Then  $\zeta_1 \otimes \zeta_2$  is an irreducible character of the direct product  $G_1 \times G_2$ . Since  $FG_1 \otimes_F FG_2 \cong F(G_1 \times G_2)$ , we deduce that

$$A(F, \zeta_1) \otimes_F A(F, \zeta_2) \cong A(F, \zeta_1 \otimes \zeta_2).$$

Now let  $\bar{\zeta}$  denote the complex conjugate of  $\zeta$ . Using contragredient modules, we find readily that  $A(F, \bar{\zeta})$  is antiisomorphic to  $A(F, \zeta)$ . From (3.60) we obtain

$$A(F, \zeta) \otimes_F A(F, \bar{\zeta}) \cong M_l(F)$$

for some  $l$ . The left-hand side is just  $A(F, \zeta \otimes \bar{\zeta})$ , where now  $\zeta \otimes \bar{\zeta} \in \text{Irr}(G \times G)$ . It follows that the character  $\zeta \otimes \bar{\zeta}$  of  $G \times G$  is realizable in the field  $F$ , whence so is the character  $\zeta_H \otimes \bar{\zeta}$  of  $H \times G$ . On the other hand,  $\xi \otimes \bar{\zeta} \in \text{Irr}(H \times G)$  has character values in  $F$ . Then (74.5) shows that

$$m_F(\xi \otimes \bar{\zeta}) \text{ divides } (\xi \otimes \bar{\zeta}, \zeta_H \otimes \bar{\zeta}).$$

However,

$$(\xi \otimes \bar{\zeta}, \zeta_H \otimes \bar{\zeta}) = (\xi, \zeta_H)(\bar{\zeta}, \bar{\zeta})_G = r,$$

so  $m_F(\xi \otimes \bar{\zeta})$  is prime to  $p$ . However,

$$A(F, \xi \otimes \bar{\zeta}) \cong A(F, \xi) \otimes_F A(F, \bar{\zeta}),$$

and each of the factors  $A(F, \xi)$  and  $A(F, \bar{\zeta})$  has  $p$ -power index, whence so does  $A(F, \xi \otimes \bar{\zeta})$ . This shows that  $m_F(\xi \otimes \bar{\zeta}) = 1$ , and so  $[A(F, \xi \otimes \bar{\zeta})] = 1$  in  $B(F)$ . Therefore

$$[A(F, \xi)] = [A(F, \bar{\zeta})]^{-1} = [A(F, \zeta)] \quad \text{in } B(F),$$

which completes the proof.

We are finally ready to state and prove an extended version of the Brauer-Witt Theorem, which involves not only the calculation of Schur indices of irreducible characters, but also gives information on the structure of simple components of group algebras. We continue to follow the approach of Yamada [74].

**(74.38) Brauer-Witt Theorem.** *Let  $\zeta \in \text{Irr } G$ , and let  $K$  be an algebraic number field such that  $K(\zeta) = K$ . Let  $p$  be a prime, and let  $F$  be the subfield of  $K(\zeta)$  defined in (74.36). Then there exist an  $(F, p)$ -elementary subgroup  $H \leq G$ , a character  $\xi \in \text{Irr } H$ , a group  $N \trianglelefteq H$ , and a linear character  $\psi$  of  $N$ , such that*

- (i)  $p \nmid (\zeta_H, \xi)$ , and  $F(\xi) = F$ .

(ii)  $\xi = \psi^H$ , and each  $H$ -conjugate of  $\psi$  is a Galois conjugate of  $\psi$  over  $F$ .

(iii) The simple component  $A(F, \xi)$  of  $FH$ , corresponding to  $\xi$ , is  $F$ -isomorphic to a cyclotomic algebra  $(F(\psi)/F, f)$ , where  $F$  is a factor set whose values are roots of 1 in  $F(\psi)$ .

(iv) In the Brauer group  $B(F)$ , we have

$$[A(F, \zeta)] = [A(F, \xi)] = [(F(\psi)/F, f)].$$

(v) The  $p$ -part of  $m_K(\zeta)$  equals  $m_F(\xi)$ .

*Proof.* By (74.30), there exist an  $(F, p)$ -elementary subgroup  $\tilde{H} \leq G$  and a character  $\tilde{\xi} \in \text{Irr } \tilde{H}$ , such that

$$p \nmid (\zeta, \tilde{\xi}^G) \quad \text{and} \quad F(\tilde{\xi}) = F.$$

We now apply (74.34) with  $G, K$ , and  $\zeta$  replaced by  $\tilde{H}, F$ , and  $\tilde{\xi}$ , respectively. Then there exist groups  $N \leq H \leq \tilde{H} \leq G$ , and a linear character  $\psi$  of  $N$ , such that

$$\begin{cases} \tilde{\xi} = \psi^{\tilde{H}}, & N \trianglelefteq H, \quad F(\psi^H) = F, \\ \text{and each } H\text{-conjugate of } \psi \text{ is a Galois conjugate of } \psi \text{ over } F. \end{cases}$$

Put  $\xi = \psi^H$ , so  $\xi^G = \tilde{\xi}^G = \zeta$ , and  $(\zeta_H, \xi) = (\zeta, \xi^G) = (\zeta, \tilde{\xi}^G)$ . Thus, assertions (i) and (ii) are valid for this choice of  $\xi, N, H$ , and  $\psi$ .

Now let us use (74.31), with  $G, K, \zeta$ , and  $G_0$  replaced by  $H, F, \xi$ , and  $H$ , respectively. It follows from (74.31) that  $A(F, \xi)$  is  $F$ -isomorphic to a cyclotomic algebra  $(F(\psi)/F, f)$ , constructed explicitly in Step 2 of the proof of (74.31). Further, since  $p \nmid (\zeta_H, \xi)$ , the proof of (74.35) shows that  $[A(F, \xi)] = [A(F, \zeta)]$  in  $B(F)$ . This proves (iv), and (v) then follows from (74.37).

**(74.39) Corollary.** Let  $K$  be a field of characteristic 0. Then every simple component  $A(K, \zeta)$  of a group algebra is similar to a cyclotomic algebra.

*Proof.* By (74.28), it suffices to treat the case where  $\xi \in \text{Irr } G$  is such that  $K(\zeta) = K$ , and we assume this holds from now on. Let  $A = A(K, \zeta)$ , so  $[A] \in B(K)$ . We shall show that for each prime  $p$ , there exists a cyclotomic algebra  $B^{(p)}$  with center  $K$ , such that  $[A]_p = [B^{(p)}]$  in  $B(K)$ . (Note that  $[A]_p = 1$  for all but a finite number of primes  $p_1, \dots, p_l$ , say.) Then

$$[A] = \prod_{i=1}^l [A]_{p_i} = \prod_{i=1}^l [B^{(p_i)}],$$

so  $A$  is similar to a tensor product of cyclotomic algebras:

$$A \sim B^{(p_1)} \otimes_K \cdots \otimes_K B^{(p_l)}.$$

Any such tensor product is similar to a cyclotomic algebra (see Exercise 74.8), so also  $A$  is similar to a cyclotomic algebra, as desired.

Now let  $p$  be any prime, and let  $F$  be the field defined in (74.38), so  $d = \dim_K F$  is prime to  $p$ . As shown in any standard reference\* on cohomology of groups, there exist homomorphisms

$$\text{res}: B(K) \rightarrow B(F), \quad \text{cor}: B(F) \rightarrow B(K),$$

called *restriction* and *corestriction* (or *transfer*), respectively. The composite  $\text{cor} \circ \text{res}$  is multiplication by  $d$ . In terms of factor sets and the isomorphism (74.23), we note that given  $x \in B(K)$  and  $y \in B(F)$ , we can find a finite Galois extension  $L/K$  such that  $x \in B(L/K)$ ,  $y \in B(L/F)$ . Put

$$\mathfrak{H} = \text{Gal}(L/F) \leq \mathfrak{G} = \text{Gal}(L/K).$$

The inclusion  $\mathfrak{H} \leq \mathfrak{G}$  induces a restriction homomorphism  $\text{res}: H^2(\mathfrak{G}, L) \rightarrow H^2(\mathfrak{H}, L)$ , and there is a commutative diagram

$$\begin{array}{ccc} B(L/K) & \xrightarrow{F \otimes_{K^*}} & B(L/F) \\ \downarrow & & \downarrow \\ H^2(\mathfrak{G}, L) & \longrightarrow & H^2(\mathfrak{H}, L) \end{array}.$$

The vertical arrows are the isomorphisms in (74.23), and we have

$$\text{res}[A]_p = [B] \quad \text{in } B(F),$$

where  $B$  is the cyclotomic algebra  $(F(\psi)/F, f)$  defined in (74.38).

On the other hand, the corestriction map on Brauer groups comes from the map  $\text{cor}: H^2(\mathfrak{H}, L) \rightarrow H^2(\mathfrak{G}, L)$ , which is described explicitly by Huppert [67, p. 114] or Weiss [69, p. 81]. In particular, if  $f: \mathfrak{H} \times \mathfrak{H} \rightarrow L$  is a factor set, the  $\text{cor}[f]$  is represented by a factor set  $g: \mathfrak{G} \times \mathfrak{G} \rightarrow L$ , whose values are products of values of  $f$ . Consequently, corestrictions of cyclotomic algebras are cyclotomic (up to similarity).

We apply all this to  $x = [A]_p \in B(K)$ , so

$$x^d = \text{cor} \circ \text{res}(x) = \text{cor}[B] \quad \text{in } B(K),$$

and  $\text{cor}[B]$  is (up to similarity) cyclotomic. Since  $x$  is  $p$ -torsion and  $p \nmid d$ , we conclude that

$$x = (\text{cor}[B])^r \quad \text{in } B(K)$$

for some  $r$ . Hence (by Exercise 74.8),  $x$  is a cyclotomic algebra (up to similarity).

\*See Cassels–Fröhlich [67], Huppert [67], or Weiss [69].

This shows that for each  $p$ ,  $[A]_p = [B^{(p)}]$  in  $B(K)$  for some cyclotomic algebra  $B^{(p)}$  over  $K$ . By the first paragraph of the proof, we conclude that  $A$  is similar to a cyclotomic algebra over  $K$ , as desired.

## Notes

- Let  $A$  be a central simple  $K$ -algebra, where  $K$  is an algebraic number field, and consider the group  $\text{Aut}_{\mathbb{Q}} A$  of  $\mathbb{Q}$ -automorphisms of  $K$ . Each  $\varphi \in \text{Aut}_{\mathbb{Q}} A$  induces a  $\mathbb{Q}$ -automorphism  $\varphi'$  of  $K$ . We set

$$\text{Aut}(K, A) = \{\sigma \in \text{Aut}_{\mathbb{Q}} K : \sigma = \varphi' \text{ for some } \varphi \in \text{Aut}_{\mathbb{Q}} A\}.$$

Janusz [76] showed that  $\text{Aut}(K, A)$  consists precisely of those  $\sigma \in \text{Aut}_{\mathbb{Q}} K$  such that for every prime  $P$  of  $K$ , there is an isomorphism of rings

$$K_P \otimes_K A \cong K_{P^\sigma} \otimes_K A.$$

(In this connection, see (74.20ii).)

- From the Brauer-Witt Theorem 74.38, part (v), the computation of Schur indices reduces to the case of  $(K, p)$ -elementary subgroups for various  $K$  and  $p$ . This special case, nevertheless, can be quite difficult, and few general results are available.
- For  $\zeta \in \text{Irr } G$ , and  $p$  a prime, define  $m_{\mathbb{Q}_p}(\zeta)$  as in the discussion following (74.26). Feit [83] proved:

Let  $x \in G$  be a  $p'$ -element such that  $\zeta_i(x) \in \mathbb{Q}_p(\zeta)$  for every  $\zeta_i \in \text{Irr } G$ . Then  $\zeta(x)/m_{\mathbb{Q}_p}(\zeta)$  is an algebraic integer.

Taking  $x = 1$ , this yields the well-known result that  $m_{\mathbb{Q}_p}(\zeta)$  divides  $\zeta(1)$ ; see (74.10ii) in this connection.

- It is easily shown that each cyclotomic algebra is a simple component of some group algebra (see Yamada [74, Prop. 2.1]).

- Let  $K$  be a finite extension of  $\mathbb{Q}_p$ , where  $p$  is prime, and let  $G$  be a  $p$ -hyper-elementary group (see (39.1)). Then

$$KG \cong \bigoplus M_{n_i}(D_i),$$

where for  $p$  odd, each  $D_i$  is a field, while for  $p = 2$ , each  $D_i$  is either a field or a skewfield of index 2. This result was proved by Oliver [81, Lemma 8, p. 187]. It suffices to establish the result for  $K = \mathbb{Q}_p$ , and for this case one must prove that for  $\zeta \in \text{Irr } G$ ,  $m_K(\zeta) = 1$  or 2. By Exercise 74.6,  $\zeta(1)$  is a power of  $p$ , and therefore so is  $m_K(\zeta)$ . On the other hand, Witt has shown that for  $F = K(\sqrt[p]{1})$ ,  $m_F(\zeta) = 1$  or 2. Oliver's Theorem now follows from Exercise 74.3.

## §74. Exercises

1. Let  $G$  be a finite group, and  $k$  any field. Show that there exists a finite Galois extension  $E$  of  $k$  that is a splitting field for  $G$  (that is,  $EG/\text{rad } EG$  is a split semisimple  $E$ -algebra).

[Hint: See the proof of (7.14). Instead of the hypothesis that  $k$  be a perfect field, use (7.10) and its proof.]

2. Let  $A = M_r(D)$ , where  $D$  is a skewfield with center  $K$  and index  $m$ . Let  $V$  be a simple  $(F \otimes_K A)$ -module, where  $F$  is an extension field of  $K$ . Show that  $V$  is absolutely simple if and only if  $F$  splits  $D$ , that is,  $F \otimes_K D \cong M_m(F)$ .

[Hint: Let  $\otimes$  denote  $\otimes_K$ . Then  $F \otimes A \cong M_r(F \otimes D)$ , and  $F \otimes D \cong M_s(D')$  for some skewfield  $D'$  with center  $F$ . Thus  $F \otimes A \cong M_{rs}(D')$ , and  $\text{End } V \cong D'$ . But  $V$  is absolutely simple if and only if  $D' = F$  (see (3.43)), that is,  $F$  splits  $D$ . It is easily checked that  $s = m$  in this case.]

3. Let  $k \subseteq F \subseteq \Omega$  be fields, where  $\dim_k F$  is finite, and where  $\Omega$  is a splitting field for  $G$ . Let  $\zeta$  be an irreducible  $\Omega$ -character of  $G$ , and let  $m_k(\zeta), m_F(\zeta)$  denote Schur indices. Prove that

$$m_k(\zeta) \text{ divides } m_F(\zeta) \cdot \dim_{k(\zeta)} F(\zeta).$$

4. Let  $D$  be a skewfield with center  $K$  and index  $m$ , and let  $E$  be an extension field of  $K$ . Prove

- (i)  $E \otimes_K D$  is a central simple  $E$ -algebra whose index divides  $m$ .
- (ii) If  $E$  splits  $D$  and  $\dim_K E$  is finite, then  $m$  divides  $\dim_K E$ .

[Hint: For (ii), see the end of the proof of (74.5).]

5. Let  $L/K$  be a finite Galois extension of number fields, and assume  $G = \text{Gal}(L/K)$  is abelian. Let  $f: G \times G \rightarrow L$  be a factor set. Fix  $\sigma \in G$ , and define  $g = \sigma f$ . Show that  $g$  is also a factor set, and that there is a  $K$ -algebra isomorphism  $(L/K, f) \cong (L/K, g)$  of crossed-product algebras.

[Hint: Since  $G$  is abelian,  $\sigma f$  is a factor set. Write  $(L/K, f) = \bigoplus L u_x$ ,  $(L/K, g) = \bigoplus L v_x$ , where the summation extends over  $x \in G$ . The map  $a u_x \mapsto \sigma(a) v_x$ ,  $a \in L$ ,  $x \in G$ , gives the desired isomorphism.]

6. Let  $G = \langle a \rangle \rtimes P$  be a  $(K, p)$ -elementary group, where  $\langle a \rangle$  is a cyclic  $p'$ -group and  $P$  is a  $p$ -group. Prove:

- (i) Each subgroup of  $G$  is  $(K, p)$ -elementary.
- (ii) For  $\xi \in \text{Irr } G$ ,  $\xi(1)$  is a power of  $p$ , and  $\xi = \lambda^G$  for some linear character  $\lambda$  of a subgroup of  $G$ .
- (iii) If  $H \leq G$  has  $p$ -power index, then  $a \in H$ .
- (iv) If  $H \leq G$ , and  $\mu \in \text{Irr } H$  is such that  $\mu^G \in \text{Irr } G$ , then  $|G:H| = p$ -power, and  $a \in H$ .

[Hint: For (ii), use Ito's Theorem 11.33 and Blichfeldt's Theorem 11.2. For (iv), we have  $\mu^G = |G:H| \mu(1)$ .]

7. Let  $K \subseteq E$  be algebraic number fields,  $n = \dim_K E$ , and let  $p$  be a prime such that  $p \nmid n$ .

Denote by  $B(K)_p$  the  $p$ -torsion subgroup of the Brauer group  $B(K)$ . Prove that there is an injective homomorphism

$$B(K)_p \rightarrow B(E)_p,$$

defined by  $E \otimes_K *$ .

[Hint: Let  $[A] \in B(K)_p$  have index  $m$ , so  $m$  is a power of  $p$ . If  $[E \otimes_K A] = 1$  in  $B(E)$ , then  $E$  splits  $A$ , so  $m|n$  by Exercise 4.]

8. Let  $B_i = (L_i/K, f_i)$ ,  $i = 1, 2$ , be cyclotomic algebras over  $K$ . Prove that  $B_1 \otimes_K B_2$  is similar to a cyclotomic algebra over  $K$ .

[Hint: After inflation (see MO (29.16)), we may assume that  $L_1 = L_2$ . Then use (74.23).]

## §75. REPRESENTATIONS AND CHARACTERS OF THE SYMMETRIC GROUP

### §75A. Specht Modules and Simple $FS_n$ -Modules

Throughout this subsection,  $n$  denotes a fixed positive integer. The group of permutations of the set  $\{1, 2, \dots, n\}$  will be called the *symmetric group* and denoted by  $S_n$ . The basic facts about cycle decomposition, conjugacy classes, etc. are assumed (see CR § 3).

The conjugacy classes of  $S_n$  are parametrized by the *partitions* of  $n$ . These are ordered sets of positive integers  $\alpha = (a_1, \dots, a_r)$  satisfying the conditions

$$a_1 \geq a_2 \geq \dots \geq a_r > 0 \quad \text{and} \quad a_1 + \dots + a_r = n.$$

The integers  $\{a_i : 1 \leq i \leq r\}$  are called the *parts* of  $\alpha$ . Each partition  $\alpha$  can be described uniquely by the exponential notation

$$\alpha = 1^{\alpha_1} 2^{\alpha_2} \dots n^{\alpha_n},$$

which means that  $\alpha$  has  $\alpha_1$  parts equal to 1,  $\alpha_2$  parts equal to 2, etc., so that  $\alpha_1 + 2\alpha_2 + \dots + n\alpha_n = n$ . For example,  $1^2 2^2 3$  stands for the partition 3 2 2 1 of 8.

The *Young diagram*  $[\alpha]$  associated with the partition  $\alpha = (a_1, \dots, a_r)$  is the set of points in the plane  $\{(i, j) : i, j \in \mathbb{Z}_+\}$  satisfying the conditions  $1 \leq i \leq r$  and for each  $i$ ,  $1 \leq j \leq a_i$ . The points  $(i, j)$  are called the nodes of the diagram, and are conveniently drawn as in the example

$$\begin{aligned} \alpha &= 1^2 2^2 3 \\ &\quad [\alpha] = \begin{array}{c} \text{xxx} \\ \text{xx} \\ \text{xx} \\ \text{x} \end{array} \end{aligned}$$

An  $\alpha$ -tableau  $T$  is one of the  $n!$  arrays obtained filling in the integers  $\{1, 2, \dots, n\}$ , without repetitions, at the nodes of a Young diagram  $\alpha$ . For example,

$$\begin{array}{ccc} & 3 & 1 & 2 \\ T = & 4 & 5 & \text{and} & T' = & 5 & 4 \\ & 7 & 6 & & & 3 & 2 \\ & & 8 & & & & 1 \end{array}$$

are  $\alpha$ -tableaux for the partition  $\alpha = 1^2 2^2 3$ .

For each  $\alpha$ -tableau  $T$ , we denote by  $R(T)$  the subgroup of  $S_n$  that permutes the elements of each row of  $T$ , and by  $C(T)$  the subgroup which permutes the elements of each column of  $T$ . We clearly have  $R(T) \cap C(T) = 1$  for each  $\alpha$ -tableau  $T$ , since the elements of  $C(T)$  stabilize the elements in each fixed column of  $T$ , while the corresponding statement for the rows applies to  $R(T)$ .

The *sign representation* of  $S_n$  will be denoted by  $\varepsilon$  (see (66.26)). It is the uniquely determined homomorphism  $\varepsilon: S_n \rightarrow \pm 1$  such that  $\varepsilon(t) = -1$  for each transposition  $t \in S_n$ .

The following result was proved in CR (28.15) (using different notation).

**(75.1) Theorem.** Set

$$e(T) = \sum_{p \in R(T), q \in C(T)} \varepsilon(q)pq$$

in the rational group algebra  $\mathbb{Q}S_n$  for each  $\alpha$ -tableau  $T$  and each partition  $\alpha$ . Then the following statements hold;

- (i)  $e(T)$  is a primitive idempotent in  $\mathbb{Q}S_n$ .
- (ii)  $\mathbb{Q}S_n e(T)$  is an absolutely simple  $\mathbb{Q}S_n$ -module.
- (iii)  $\mathbb{Q}S_n e(T) \cong \mathbb{Q}S_n e(T')$ , for an  $\alpha'$ -tableau  $T'$ , if and only if  $\alpha = \alpha'$ .
- (iv) Every simple  $\mathbb{Q}S_n$ -module is isomorphic to  $\mathbb{Q}S_n e(T)$  for some  $\alpha$ -tableau  $T$  and some partition  $\alpha$ .

In this subsection, we shall give a new proof of this theorem, and improve and extend it in several important ways. In particular, we shall obtain an explicit generating set for each simple  $\mathbb{Q}S_n$ -module, from which a matrix representation afforded by the module can be calculated. The approach also yields the simple  $FS_n$ -modules, for an arbitrary field  $F$  of any characteristic. Except for some minor changes, the entire discussion follows James [78] (see also James-Kerber [81]).

We first require several other concepts and preliminary results concerning them. We shall make heavy use of two order relations on the set of partitions of  $n$ . The first is a partial order, called *dominance* and denoted by  $\succeq$ . We set

$$(75.2) \quad \alpha \succeq \beta \text{ if and only if } \sum_{i=1}^j a_i \geq \sum_{i=1}^j b_i$$

for each  $j$ , where  $\{a_i\}$  and  $\{b_i\}$  are the parts of  $\alpha$  and  $\beta$ , respectively with zeros inserted if necessary. Thus

$$1^2 2^2 3 \succ 2^4 \quad \text{and} \quad 2^2 4 \succ 1^3 2 3$$

while  $2^2 3$  and  $1^3 4$  are not comparable with respect to dominance. If  $\alpha \succeq \beta$  and  $\alpha \neq \beta$ , we write  $\alpha > \beta$ .

The second is a total order on the set of partitions of  $n$ , called *lexicographic ordering*, and denoted by  $>$ . We set  $\alpha > \beta$  if for some  $i \geq 1$  we have  $a_i - b_i$  is positive while all differences (if any)  $a_j - b_j$  for  $j < i$  are zero, and  $\{a_i\}$  and  $\{b_i\}$  are the parts of  $\alpha$  and  $\beta$ , respectively.

We clearly have

$$\alpha \succeq \beta \Rightarrow \alpha \geq \beta,$$

but the reverse implication does not always hold.

We next initiate a close study of the permutation action of  $S_n$  and its subgroups on the set of  $\alpha$ -tableaux, for the various partitions of  $n$ , which will be denoted by  $\alpha, \beta, \gamma, \dots$  without further explanation.

Let  $\alpha$  be a fixed partition of  $n$ . The group  $S_n$  acts on the set of  $\alpha$ -tableaux  $\{T\}$  in the obvious way, with  $xT$  obtained by applying  $x$  to each entry in  $T$ , for each  $x \in S_n$ . The set of  $\alpha$ -tableaux  $\{T\}$  is clearly a transitive  $S_n$ -set, and we have

$$(75.3) \quad R(xT) = xR(T)x^{-1} \quad \text{and} \quad C(xT) = xC(T)x^{-1}, \quad \text{for } x \in S_n$$

where  $R(T)$  and  $C(T)$  are the groups of row and column permutations defined previously, for each  $\alpha$ -tableau  $T$ .

We next define an equivalence relation, denoted by  $\sim$ , on the set of  $\alpha$ -tableaux. We set

$$T_1 \sim T_2 \Leftrightarrow T_1 = pT_2 \quad \text{for some } p \in R(T_1).$$

The equivalence class of an  $\alpha$ -tableau  $T$  is denoted by  $[T]$ , and is called the  *$\alpha$ -tabloid* with representative  $T$ . An  $\alpha$ -tabloid can be viewed as an  $\alpha$ -tableaux with unordered rows. We shall use the notation

$$\begin{array}{c} 3 \ 1 \ 2 \\ \hline 4 \ 5 \\ \hline 7 \ 6 \\ \hline 8 \end{array},$$

with bars between the rows, to denote the  $\alpha$ -tabloid represented by the  $\alpha$ -tableaux

$$\begin{array}{ccc} 3 \ 1 \ 2 & & 2 \ 1 \ 3 \\ 4 \ 5 & \text{and} & 5 \ 4 \\ 7 \ 6 & & 6 \ 7 \\ 8 & & 8 \end{array} \quad \text{etc.}$$

The symmetric group  $S_n$  acts on the set of  $\alpha$ -tabloids as follows: we set

$$x[T] = [xT], \quad \text{for } x \in S_n,$$

for each  $\alpha$ -tabloid  $[T]$ . The action is well defined, since  $[T_1] = [T_2]$  implies that  $[xT_1] = [xT_2]$ . This is easily proved, since  $[T_1] = [T_2]$  implies that  $T_1 = pT_2$  for some  $p \in R(T_1)$ , and hence  $xT_1 = xpx^{-1} \cdot xT_2$ , with  $xpx^{-1} \in R(xT_1)$  by (75.3).

The  $\alpha$ -tabloids clearly form a transitive  $S_n$ -set. The stabilizer of an  $\alpha$ -tabloid  $[T]$  is the row subgroup  $R(T)$ , for a representative  $T$  of  $[T]$ . This gives a neat interpretation of the induced permutation modules  $(1_{R(T)})^{S_n}$ .

**(75.4) Lemma.** *Let  $\alpha$  be a fixed partition of  $n$ , and let  $F$  be a field. Let  $M_\alpha$  be the vector space over  $F$  with a basis identified with the set of  $\alpha$ -tabloids  $[T]$ , and define the action of  $S_n$  on  $M_\alpha$  by the rule*

$$x[T] = [xT]$$

for each  $x \in S_n$  and  $\alpha$ -tabloid  $[T]$ . Then  $M_\alpha$  is an  $FS_n$ -module, which affords the permutation representation  $(1_{R(T)})^{S_n}$ , where  $R(T)$  is the group of row permutations of any  $\alpha$ -tableau  $T$ .

The proof is immediate from §1B and the remarks preceding the lemma.

The row subgroups  $\{R(T)\}$  corresponding to the set of  $\alpha$ -tableaux  $\{T\}$ , for a fixed partition  $\alpha$ , form a conjugacy class of subgroups of  $S_n$ , called the *Young subgroups of type  $\alpha$* . (As an exercise, the reader should verify that the Young subgroups of type  $\alpha$  coincide with a conjugacy class of parabolic subgroups of  $S_n$ , in the sense of §64 (see also Exercise 64.1).) We now have:

**(75.5) Definition.** Let  $F$  be a field, and  $\alpha$  a fixed partition of  $n$ , with  $M_\alpha$  the permutation module defined in (75.4). For each  $\alpha$ -tableau  $T$ , the *Specht element*  $e_T$  is the element of  $M_\alpha$  defined by

$$e_T = \sum_{q \in C(T)} \varepsilon(q) q[T],$$

where  $C(T)$  is the group of column permutations of  $T$  and  $\varepsilon(q)$  is the value of the sign representation  $\varepsilon$  at  $q$ . The *Specht module*  $Z_\alpha$  is the  $FS_n$ -submodule of  $M_\alpha$  generated by the set of Specht elements  $\{e_T\}$ , corresponding to the set of  $\alpha$ -tableaux  $\{T\}$ .

We first note that the Specht element  $e_T$  can be expressed as

$$e_T = c(T)[T]$$

where  $c(T)$  is the element of the group algebra  $FS_n$  defined by

$$(75.6) \quad c(T) = \sum_{q \in C(T)} \varepsilon(q) q$$

and is called the *signed column sum* associated with the  $\alpha$ -tableau  $T$ .

**(75.7) Lemma.** *Each Specht module  $Z_\alpha$  is a cyclic  $FS_n$ -module, generated by any Specht element  $e_T$  associated with an  $\alpha$ -tableau  $T$ .*

*Proof.* Since  $S_n$  acts transitively on the set of  $\alpha$ -tableaux, it is sufficient to prove that

$$(75.8) \quad xe_T = e_{xT}, \quad \text{for } x \in S_n, \text{ and on } \alpha\text{-tableau } T.$$

To prove (75.8), we note that  $C(xT) = xC(T)x^{-1}$  for each  $x \in S_n$ , by (75.3), so that

$$xc(T)x^{-1} = \sum_{q \in C(T)} \varepsilon(q) x q x^{-1} = c(xT).$$

Then

$$xe_T = xc(T)[T] = xc(T)x^{-1}x[T] = c(xT)[xT] = e_{xT},$$

completing the proof.

**(75.9) Definition.** Let  $F$  be a field, and  $M_\alpha$  a Young module of type  $\alpha$  (see (75.4)). Define a bilinear form  $\langle , \rangle : M_\alpha \times M_\alpha \rightarrow F$  by setting

$$\langle [T], [T'] \rangle = \begin{cases} 1 & \text{if } [T] = [T'] \\ 0 & \text{if } [T] \neq [T'] \end{cases}$$

for each pair of  $\alpha$ -tabloids  $[T]$  and  $[T']$  in  $M_\alpha$ .

The following two results are straightforward, and are left as exercises for the reader.

**(75.10) Proposition.** *The bilinear form  $\langle , \rangle$  on  $M_\alpha$ , defined by (75.9), is symmetric, nondegenerate, and invariant under the action of  $S_n$  in the sense that  $\langle xt, xt' \rangle = \langle t, t' \rangle$  for all  $x \in S_n$  and  $t, t' \in M_\alpha$ .*

**(75.11) Proposition.** *Let  $F$  be a field,  $G$  a finite group, and let  $V$  be a f.g. left  $FG$ -module admitting a symmetric, nondegenerate,  $G$ -invariant bilinear form  $\langle , \rangle$ . Then we have:*

(i)  *$V$  is self-contragredient, in the sense that there is an isomorphism of  $FG$ -modules  $V \cong V^*$ , where  $V^*$  denotes the contragredient module.*

(ii) *Let  $W \subseteq V$  be an  $FG$ -submodule, and set*

$$W^\perp = \{v \in V : \langle v, w \rangle = 0 \quad \text{for all } w \in W\}.$$

*Then  $W/(W \cap W^\perp)$  is an  $FG$ -module, which is isomorphic to its contragredient module.*

(iii) Let  $\{e_1, \dots, e_m\}$  be an  $F$ -basis for  $W$ , and let  $\Gamma = (\langle e_i, e_j \rangle)_{1 \leq i, j \leq m}$  denote the matrix of the restriction  $\langle \cdot, \cdot \rangle|_W$  of the bilinear form, with respect to the basis  $\{e_i : 1 \leq i \leq m\}$ . Then we have

$$\dim_F W / (W \cap W^\perp) = \text{rank } \Gamma.$$

We can now state the first main result of this subsection, using the properties (75.10)–(75.11) of the bilinear form  $\langle \cdot, \cdot \rangle$  on  $M_\alpha$ .

**(75.12) Theorem** (James [78]). *Let  $F$  be an arbitrary field, let  $\alpha$  be a partition of  $n$ , and let  $M_\alpha$  denote the Young module of type  $\alpha$ . Then the following statements hold.*

(i) *Let  $U \subseteq M_\alpha$  be a  $FS_n$ -submodule of  $M_\alpha$ , and let  $Z_\alpha \subseteq M_\alpha$  be the Specht module (see (75.5)). Then we have either  $U \supseteq Z_\alpha$  or  $U \subseteq Z_\alpha^\perp$ .*

(ii) *The quotient  $Z_\alpha / (Z_\alpha \cap Z_\alpha^\perp)$  is either zero or an absolutely simple  $FS_n$ -module. If it is not zero, then  $Z_\alpha \cap Z_\alpha^\perp$  is the unique maximal submodule of  $Z_\alpha$ , and  $Z_\alpha / (Z_\alpha \cap Z_\alpha^\perp)$  is isomorphic to its contragredient.*

The proof involves a series of lemmas. The first is a variation of a result used in CR to prove (75.1) (see CR Lemma 28.11).

**(75.13) Basic Combinatorial Lemma.** *Let  $\alpha$  and  $\beta$  be partitions of  $n$ , and let  $T_1$  be an  $\alpha$ -tableau and  $T_2$  be a  $\beta$ -tableau. Assume that the entries in each row of  $T_2$  belong to different columns of  $T_1$ . Then  $\alpha \succeq \beta$  (see 75.2).*

*Proof.* Let  $\alpha = (a_1, \dots, a_r)$  and  $\beta = (b_1, \dots, b_s)$ . Applying the hypothesis to the first row of  $T_2$ , we see that  $T_1$  has at least  $b_1$  columns, so  $a_1 \geq b_1$ . Upon replacing  $T_1$  by  $gT_1$  for a suitable element  $g \in C(T_1)$ , we may assume that the elements in the first row of  $T_2$  all belong to the first row of  $T_1$ , and that the hypotheses of the lemma are satisfied for  $T_2$  and the new choice of  $T_1$ . Since the elements in the second row of  $T_2$  appear in different columns of  $T_1$ , it follows that either  $a_2 \geq b_2$  or else there are  $b_2 - a_2$  extra spaces in the first row of the new choice of  $T_1$  not occupied by elements of the first row of  $T_2$ . In either case, we have  $a_1 + a_2 \geq b_1 + b_2$ , and we may assume that the entries of the first two rows of  $T_2$  are a subset of the entries of the first two rows of  $T_1$ . The argument is easily continued by induction, and we obtain  $\alpha \succeq \beta$ , as required.

**(75.14) Lemma.** *Keep the notation of (75.13), assume that  $c(T_1)[T_2] \neq 0$  in  $M_\beta$ , where  $c(T_1)$  is the signed column sum (75.6) of the  $\alpha$ -tableau  $T_1$ . Then we have  $\alpha \succeq \beta$ . Moreover, if  $\alpha = \beta$ , then we have*

$$c(T_1)[T_2] = \pm c(T_1)[T_1] = \pm e_{T_1},$$

where  $e_{T_1}$  is the Specht element (75.5) in  $M_\alpha$  associated with  $T_1$ .

*Proof.* Let  $\{i, j\}$  be two numbers belonging to the same row of  $T_2$ . Then  $(1 - (ij))[T_2] = 0$ , and it follows that  $i$  and  $j$  belong to different columns of  $T_1$ . Otherwise  $(ij) \in C(T_1)$ , and we have  $c(T_1)[T_2] = 0$  contrary to the hypothesis, since we have

$$c(T_1) = u(1 - (ij))$$

where  $u \in FC(T_1)$  is the alternating sum of coset representatives in  $C(T_1)$  of the subgroup generated by  $(ij)$ . This implies that any two entries in a row of  $T_2$  belong to different columns of  $T_1$ , and hence  $\alpha \succeq \beta$ , by the Basic Combinatorial Lemma 75.13.

Now assume  $\alpha = \beta$ . Then  $T_2$  belongs to the  $C(T_1)$ -orbit of  $T_1$ . It follows that  $T_2 = gT_1$  for some element  $g \in C(T_1)$ , and we obtain

$$[T_2] = g[T_1] \quad \text{and} \quad c(T_1)[T_2] = c(T_1)g[T_1] = \epsilon(g)e_{T_1},$$

since  $g \in C(T_1)$  and  $e_{T_1} = c(T_1)[T_1]$ .

**(75.15) Corollary.** *Let  $u \in M_\alpha$ , and let  $T$  be an  $\alpha$ -tableau. Then  $c(T)u$  is a multiple of  $e_T$ .*

*Proof.* By (75.4),  $u$  is a linear combination of  $\alpha$ -tabloids  $[T_j]$ , and for each  $\alpha$ -tabloid  $[T_j]$ ,  $c(T)[T_j]$  is either zero or a multiple of  $e_T$ , by (75.14).

We next introduce the bilinear form  $\langle \cdot, \cdot \rangle : M_\alpha \times M_\alpha \rightarrow F$  defined in (75.9), and recall that it is symmetric, nondegenerate and  $S_n$ -invariant, by (75.10). We also have:

**(75.16) Lemma.** *Let  $u, v \in M$  and let  $T$  be an arbitrary  $\alpha$ -tableau. Then*

$$\langle c(T)u, v \rangle = \langle u, c(T)v \rangle.$$

*Proof.* We have

$$\begin{aligned} \langle c(T)u, v \rangle &= \sum_{q \in C(T)} \epsilon(q) \langle qu, v \rangle = \sum_{q \in C(T)} \epsilon(q) \langle qu, qq^{-1}v \rangle \\ &= \sum_{q \in C(T)} \epsilon(q) \langle u, q^{-1}v \rangle = \langle u, c(T)v \rangle, \end{aligned}$$

since the form is  $S_n$ -invariant.

We are now in a position to prove part (i) of Theorem 75.12, which we single out for later reference.

**(75.17) Submodule Lemma.** *Let  $U$  be an  $FS_n$ -submodule of a Young module  $M_\alpha$ , and let  $Z_\alpha \subseteq M$  be the Specht submodule of  $M_\alpha$ . Then either  $Z_\alpha \subseteq U$  or  $U \subseteq Z_\alpha^\perp$ .*

*Proof.* Let  $u \in U$  and let  $T$  be an  $\alpha$ -tableau. By (75.15), either  $c(T)u = 0$  or  $e_T \in U$ .

Thus if  $c(T)u \neq 0$  for some  $\alpha$ -tableau  $T$ , we have  $Z_\alpha \subseteq U$ , using (75.15) and the fact that  $Z_\alpha$  is a cyclic  $FS_n$ -module generated by an arbitrary Specht element by (75.7).

Next assume that  $Z_\alpha \not\subseteq U$ . Then  $c(T)u = 0$  for all  $u \in U$  and all  $\alpha$ -tableaux  $T$ , by the first part of the proof. Then

$$\langle c(T)u, [T] \rangle = \langle u, c(T)[T] \rangle = \langle u, e_T \rangle = 0$$

for each  $\alpha$ -tableau  $T$ , by (75.16), and hence  $U \subseteq Z_\alpha^\perp$ , completing the proof.

*Proof of Theorem 75.12ii.* All the statements in part (ii) of (75.12) follow at once from part (i) (which is the Submodule Lemma 75.17) and 75.11iii, except the fact that  $Z_\alpha/(Z_\alpha \cap Z_\alpha^\perp)$  is an absolutely simple  $FS_n$ -module if it is different from zero. To settle this point, we first note that  $Z_\alpha$  has a basis consisting of Specht elements  $\{e_{T_i} : 1 \leq i \leq m\}$  for certain  $\alpha$ -tableaux  $\{T_i\}$ , by (75.5). For each pair of basis elements, we have  $\langle e_{T_i}, e_{T_j} \rangle \in F_0$ , where  $F_0$  is the prime field in  $F$ , by (75.9). Thus the matrix  $\Gamma = (\langle e_{T_i}, e_{T_j} \rangle)_{1 \leq i, j \leq m}$  of the restriction of the bilinear form to  $Z_\alpha$  has entries in  $F_0$ , and consequently its rank over any field containing  $F_0$  is the same as its rank over  $F_0$ . Now let  $K$  be a field containing  $F$ . Letting  $Z_\alpha^K$  denote  $K \otimes_F Z_\alpha$ , etc., we note that  $Z_\alpha^K$  is the Specht submodule of the Young module  $M_\alpha^K$  of type  $\alpha$ , over  $KS_n$ . Using (75.11iii) and the preceding remarks, it follows that

$$(75.18) \quad (Z_\alpha / Z_\alpha \cap Z_\alpha^\perp)^K \cong Z_\alpha^K / (Z_\alpha^K \cap (Z_\alpha^K)^\perp),$$

where  $Z_\alpha^K \cap (Z_\alpha^K)^\perp$  is the radical of the bilinear form  $\langle \cdot, \cdot \rangle$ , extended to  $Z_\alpha^K$ . Since  $Z_\alpha^K / (Z_\alpha^K \cap (Z_\alpha^K)^\perp)$  is a simple  $KS_n$ -module if  $Z_\alpha / (Z_\alpha \cap Z_\alpha^\perp) \neq 0$  by the preceding discussion, we conclude that  $Z_\alpha / (Z_\alpha \cap Z_\alpha^\perp)$  is absolutely simple by (75.18), completing the proof.

We next turn to the question of the completeness of the set of simple  $FS_n$ -modules provided by Theorem 75.12. We first consider the case of a field  $F$  of characteristic zero, where it will turn out that the Specht modules themselves are the simple modules.

**(75.19) Theorem.** *The Specht modules  $\{Z_\alpha\}$  (over the rational field  $\mathbb{Q}$ ), corresponding to the set of partitions  $\{\alpha\}$  of  $n$ , are absolutely simple  $\mathbb{Q}S_n$ -modules, and provide a basic set of simple  $\mathbb{Q}S_n$ -modules.*

*Proof.* The bilinear form  $\langle \cdot, \cdot \rangle$  on the Young module  $M_\alpha$  over  $\mathbb{Q}S_n$ , is clearly positive definite, by (75.9), so its restriction to the Specht module  $Z_\alpha$  is also positive definite, for each partition  $\alpha$ . Then we have

$$(75.20) \quad Z_\alpha \cap Z_\alpha^\perp = 0 \quad \text{and} \quad M_\alpha = Z_\alpha \oplus Z_\alpha^\perp,$$

and hence  $Z_\alpha$  is an absolutely simple  $\mathbb{Q}S_n$ -module for each partition  $\alpha$ , by (75.12).

The partitions of  $n$  are in bijective correspondence with the conjugacy classes of  $S_n$ , and hence with the number of isomorphism classes of simple  $CS_n$ -modules. The Specht modules  $\{Z_\alpha\}$  over  $QS_n$  are absolutely simple by the first part of the proof, and hence provide a basic set of simple  $QS_n$ -modules if we can prove that

$$(75.21) \quad Z_\alpha \not\cong Z_\beta \quad \text{if} \quad \alpha \neq \beta,$$

for arbitrary partitions  $\alpha$  and  $\beta$ . Let  $f:Z_\alpha \rightarrow Z_\beta$  be a nonzero homomorphism of  $QS_n$ -modules. By (75.20),  $f$  extends to a nonzero homomorphism  $\tilde{f}:M_\alpha \rightarrow M_\beta$  such that  $Z_\alpha \not\subseteq \ker \tilde{f}$ . Let  $T$  be an  $\alpha$ -tableau; then  $e_T \notin \ker \tilde{f}$  by (75.7), so

$$\tilde{f}(e_T) = f(c(T)[T]) = c(T)f([T]) \neq 0.$$

It follows that  $c(T)[T'] \neq 0$  for some  $\beta$ -tableau  $T'$ , and hence  $\alpha \succeq \beta$  by (75.14). Thus if  $Z_\alpha \cong Z_\beta$  we have  $\alpha \succeq \beta$  and  $\beta \succeq \alpha$ , and hence  $\alpha = \beta$ , completing the proof.

Continuing with the characteristic zero case, we give a new proof of part of Theorem 75.1, based on (75.12). (The remaining assertions of (75.1) are easily verified and are left to the reader.)

**(75.22) Theorem.** *Let  $T$  be an  $\alpha$ -tableau, and let  $I_T$  be the left ideal in  $QS_n$  generated by the element*

$$e' = \sum_{p \in R(T), q \in C(T)} e(q)qp,$$

as in (75.1). Then there is an isomorphism of  $QS_n$ -modules

$$I_T \cong Z_\alpha.$$

*Proof.* Let  $e_{R(T)} = \sum_{p \in R(T)} p$ . Then the left ideal  $QS_n e_{R(T)}$  affords the permutation representation  $(1_{R(T)})^{S_n}$ , and hence there is an isomorphism of  $QS_n$ -modules

$$h: QS_n e_{R(T)} \rightarrow M_\alpha$$

such that  $h(e_{R(T)}) = [T]$ , by (75.4). Since the element  $e'$  in the statement of the Theorem is given by  $e' = c(T)e_{R(T)}$ , we obtain

$$h(e') = h(c(T)e_{R(T)}) = c(T)h(e_{R(T)}) = c(T)[T] = e_T.$$

The result now follows from (75.7).

**Remark.** It is worthwhile to compare the descriptions of the simple  $QS_n$ -modules in terms of primitive idempotents (see (75.1)) with the approach based on Specht modules, in (75.19). The former provides no generating set for a simple module, and hence no explicit formula for the  $S_n$ -action on the module, while the

latter does provide a set of generators (the Specht elements) and gives the  $S_n$ -action on them (see (75.8)). With further discussion, this information can be refined to describe explicitly the matrices of the  $S_n$ -action on a Specht module  $Z_\alpha$  with respect to a suitable basis (see James [78] and James-Kerber [81]).

Our next task is to understand the information contained in Theorem 75.12, for fields  $F$  of characteristic  $p > 0$ . We first require:

**(75.23) Definition.** Let

$$\alpha = 1^{n_1} 2^{n_2} \cdots r^{n_r}$$

be a partition of  $n$ , with  $n_1$  parts equal to 1,  $n_2$  equal to 2, etc. The partition  $\alpha$  is called *p-regular* if the numbers  $n_j$  satisfy the condition

$$n_j < p \quad \text{for all } j = 1, 2, \dots, r.$$

We then have:

**(75.24) Proposition.** Let  $p$  be a prime number. The number of  $p$ -regular classes in  $S_n$  is equal to the number of  $p$ -regular partitions.

*Proof.* The  $p$ -regular conjugacy classes in  $S_n$  are clearly in bijective correspondence with the set of partitions

$$\alpha = 1^{n_1} 2^{n_2} \cdots$$

with property that  $n_j = 0$  if  $p \mid j$ , that is, no part of  $\alpha$  is divisible by  $p$ .

Now consider the formal power series over  $\mathbb{Q}$ :

$$P(t) = (1 - x^p)(1 - x^{2p}) \cdots / (1 - x)(1 - x^2) \cdots,$$

and calculate it in two ways, as follows.

(i) Cancel factors  $1 - x^{jp}$  in the numerator and denominator. This leaves

$$P(t) = \prod_{p \nmid i} (1 - x^i)^{-1} = \prod_{p \nmid i} (1 + x^i + x^{2i} + \cdots),$$

so the coefficient of  $x^n$  is the number of partitions of  $n$  in which no part is divisible by  $p$ .

(ii) For each  $j$ , divide the term  $1 - x^{jp}$  in the numerator by  $1 - x^j$  in the denominator. This gives

$$P(t) = \prod_{j=1}^{\infty} (1 + x^j + x^{2j} + \cdots + x^{(p-1)j}),$$

and we see that the coefficient of  $x^n$  is equal to the number of partitions of  $n$  in which no part occurs  $p$  or more times.

The proposition follows from a comparison of (i) and (ii).

Now let  $F$  be a field of characteristic  $p$ . Let  $\alpha$  be a partition of  $n$ , and let  $M_\alpha, Z_\alpha, e_T, \langle \cdot, \cdot \rangle$  be the objects defined earlier in the section. In the following results, integers involved in calculations in  $F$ , of course, are taken mod  $p$ , so that  $n$  denotes  $n \cdot 1 \in F$ , for  $n \in \mathbb{Z}$ . We also use the convention that  $0! = 1$ .

**(75.25) Proposition.** *Let  $\alpha = 1^{n_1} 2^{n_2} \dots r^{n_r}$  be a partition of  $n$ . Then we have:*

$$(i) \quad \langle e_T, e_{T'} \rangle = \left( \prod_{j=1}^r n_j! \right) n_{T, T'},$$

for all  $\alpha$ -tableaux  $T$  and  $T'$ , and some element  $n_{T, T'}$  depending on  $T$  and  $T'$ ; and

$$(ii) \quad \prod_{j=1}^r (n_j!)^j = \langle e_{T_0}, e_{T'_0} \rangle$$

for some pair of  $\alpha$ -tableaux  $\{T_0, T'_0\}$ .

*Proof.* (i) Define an equivalence relation  $\sim$  on the  $\alpha$ -tabloids, putting  $[T_1] \sim [T_2]$  whenever  $[T_1]$  can be obtained from  $[T_2]$  by permuting rows of equal length. The size of an equivalence class is clearly  $\prod_{j=1}^r n_j!$ .

Now assume that an  $\alpha$ -tabloid  $[T_1]$  appears with a nonzero coefficient  $a_1$  in the expression of a Specht element  $e_T$  as a linear combination of  $\alpha$ -tabloids. It is easily checked that, for all tabloids  $[T_2]$  in the equivalence class of  $[T_1]$ ,  $[T_2]$  appears with the nonzero coefficient  $\varepsilon a_1$  in  $e_T$ , where  $\varepsilon$  is the sign of the permutation required to exchange  $[T_1]$  and  $[T_2]$ . The proof of part (i) of (75.25) follows easily from these remarks and the definition (75.9) of the bilinear form  $\langle \cdot, \cdot \rangle$  on  $M_\alpha$ .

(ii) Let  $T$  be an  $\alpha$ -tableau, and let  $T^*$  be the  $\alpha$ -tableau obtained from  $T$  by reversing the order of the entries in each row. Let  $C_0(T)$  denote the subgroup of the group  $C(T)$  consisting of elements that permute rows of  $T$  having equal lengths. We clearly have

$$|C_0(T)| = \prod_{j=1}^r (n_j!)^j.$$

If  $[T'] = q[T]$  for some  $q \in C_0(T)$ , then  $[T']$  appears in  $e_T$  and  $e_{T^*}$  with the same coefficient. It can also be readily verified that all tabloids that appear with nonzero coefficients in  $e_T$  and  $e_{T^*}$  are related in this way. Thus we obtain

$$\langle e_T, e_{T^*} \rangle = \prod_{j=1}^r (n_j!)^j$$

as required.

**(75.26) Corollary.** Let  $Z_\alpha$  denote the Specht module of type  $\alpha$ , over the group algebra  $FS_n$ . Then

$$Z_\alpha/(Z_\alpha \cap Z_\alpha^\perp) \neq 0$$

if and only if  $\alpha$  is  $p$ -regular.

*Proof.* Let  $\alpha$  be  $p$ -regular; then there exist  $\alpha$ -tableaux  $T_0$  and  $T'_0$  such that  $\langle e_{T_0}, e_{T'_0} \rangle \neq 0$ , by (75.25ii). Then  $e_{T_0} \notin Z_\alpha \cap Z_\alpha^\perp$ , and hence  $Z_\alpha/(Z_\alpha \cap Z_\alpha^\perp) \neq 0$ . Conversely, if  $\alpha$  is not  $p$ -regular, then  $\langle e_T, e_{T'} \rangle = 0$  for all  $\alpha$ -tableau  $T$  and  $T'$ , by (75.25i). Then  $Z_\alpha \subseteq Z_\alpha^\perp$ , and we obtain  $Z_\alpha/(Z_\alpha \cap Z_\alpha^\perp) = 0$ , completing the proof.

In order to complete the determination of the simple  $FS_n$ -modules using Theorem 75.12, we will, of course, use (17.11), which asserts that the number of isomorphism classes of simple  $FS_n$ -modules is equal to the number of  $p$ -regular conjugacy classes. We also require:

**(75.27) Lemma.** Let  $\alpha$  and  $\beta$  be partitions of  $n$ , and assume that  $\alpha$  is  $p$ -regular. Let  $U$  be an  $FS_n$ -submodule of  $M_\beta$ , and let  $f: Z_\alpha \rightarrow M_\beta/U$  be a nonzero homomorphism of  $FS_n$ -modules. Then  $\alpha \succeq \beta$ .

*Proof.* (Peel [75].) (Notice that the result is simply an adaptation, for nonsemisimple modules, of the last part of the proof of (75.19).) Let  $T$  be an  $\alpha$ -tableau, and let  $T^*$  be the  $\alpha$ -tableau obtained by reversing the order of the entries of the rows of  $T$ . By (75.15), we have

$$(75.28) \quad c(T)e_{T^*} = ae_T,$$

where

$$a = \langle [T], c(T)e_{T^*} \rangle = \langle c(T)[T], e_{T^*} \rangle = \langle e_T, e_{T^*} \rangle \neq 0$$

by (75.16) and (75.25), using the fact that  $\alpha$  is  $p$ -regular. Since  $f: Z_\alpha \rightarrow M_\beta/U$  is different from zero, there exists an  $\alpha$ -tableau  $T$  such that  $f(e_T) \neq 0$  in  $M_\beta/U$ . Apply  $f$  to (75.28), and obtain

$$c(T)f(e_{T^*}) = af(e_T) \neq 0 \quad \text{in } M_\beta/U.$$

It follows that  $c(T)m \notin U$  for some  $m \in M_\beta$ , and hence  $\alpha \succeq \beta$  by Lemma 75.14, completing the proof.

**(75.29) Theorem.** Let  $F$  be an arbitrary field of characteristic  $p > 0$ . For a partition  $\alpha$ , we have

$$Z_\alpha/(Z_\alpha \cap Z_\alpha^\perp) \neq 0 \Leftrightarrow \alpha \text{ is } p\text{-regular.}$$

For two  $p$ -regular partitions  $\alpha$  and  $\beta$ , we have

$$Z_\alpha/(Z_\alpha \cap Z_\alpha^\perp) \cong Z_\beta/(Z_\beta \cap Z_\beta^\perp) \Leftrightarrow \alpha = \beta.$$

The modules

$$\{Z_\alpha/(Z_\alpha \cap Z_\alpha^\perp) : \alpha \text{ } p\text{-regular}\}$$

are absolutely simple, and form a basic set of simple  $FS_n$ -modules.

*Proof.* The first statement is Corollary 75.26. For the second statement, assume we have

$$Z_\alpha/(Z_\alpha \cap Z_\alpha^\perp) \cong Z_\beta/(Z_\beta \cap Z_\beta^\perp)$$

for  $p$ -regular partitions  $\alpha$  and  $\beta$ . Since  $Z_\alpha/(Z_\alpha \cap Z_\alpha^\perp)$  and  $Z_\beta/(Z_\beta \cap Z_\beta^\perp)$  are submodules of  $M_\alpha/(Z_\alpha \cap Z_\alpha^\perp)$  and  $M_\beta/(Z_\beta \cap Z_\beta^\perp)$ , respectively, we can apply Lemma 25.27 and obtain  $\alpha \succeq \beta$  and  $\beta \succeq \alpha$ . Then  $\alpha = \beta$ , and the second statement is proved.

Now let  $E \supseteq F$  be a splitting field for  $S_n$ . By Theorem 75.12 and the first part of the proof, the modules

$$(75.30) \quad \{Z_\alpha^E/(Z_\alpha^E \cap (Z_\alpha^E)^\perp) : \alpha \text{ } p\text{-regular}\}$$

are simple  $ES_n$ -modules, and no two of them are isomorphic. By (75.24) and (17.11), it follows that the modules (75.30) form a basic set of simple  $ES_n$ -modules. It is now a standard argument to show that the modules  $\{Z_\alpha/(Z_\alpha \cap Z_\alpha^\perp) : \alpha \text{ } p\text{-regular}\}$  form a basic set of simple  $FS_n$ -modules. Let  $V$  be an arbitrary simple  $FS_n$ -module. Then

$$\mathrm{Hom}_{ES_n}(V^E, (Z_\alpha/Z_\alpha \cap Z_\alpha^\perp)^E) \neq 0$$

for some  $p$ -regular partition  $\alpha$ , because the modules in (75.30) form a basic set. Then

$$\mathrm{Hom}_{FS_n}(V, Z_\alpha/(Z_\alpha \cap Z_\alpha^\perp)) \neq 0$$

by (2.40), and hence  $V \cong Z_\alpha/(Z_\alpha \cap Z_\alpha^\perp)$ , since  $Z_\alpha/(Z_\alpha \cap Z_\alpha^\perp)$  is an absolutely simple  $FS_n$ -module, by (75.12) and the first part of the proof. This fact, together with what has been shown, completes the proof of the theorem.

### §75B. Solomon's Theorem and the Irreducible Characters of $S_n$

Let  $G$  be a finite group. As usual, we let  $\mathrm{ch} QG$  denote the subring of  $\mathrm{ch} G$  generated by characters afforded by  $QG$ -modules. We shall denote by  $\mathrm{ch}' QG$  the subring of  $\mathrm{ch} G$  generated by the set of rational-valued characters; then we have

$$\operatorname{ch} \mathbb{Q}G \leq \operatorname{ch}' \mathbb{Q}G \leq \operatorname{ch} G.$$

In this subsection, we shall prove a theorem of Solomon [74] on the relation between  $\operatorname{ch}' \mathbb{Q}G$  and the  $\mathbb{Z}$ -submodules of  $\operatorname{ch}' \mathbb{Q}G$  generated by permutation characters defined by certain families of subgroups, for an arbitrary finite group  $G$ . This result has several applications, including a new proof of an extension to  $\operatorname{ch}' \mathbb{Q}G$  of the Artin Induction Theorem 15.4, and a theorem of Frobenius on the characters of the symmetric group  $S_n$ . In §67B, it was shown how Frobenius's theorem can be used to decompose  $(1_B)^G$ , for the groups  $G = GL_n(\mathbb{F}_q)$ .

We begin with some general considerations. Let  $G$  be a finite group, and let  $A$  be a mapping from  $G$  to the set of subgroups of  $G$  such that the following conditions are satisfied:

- (i)  $x \in A(x)$ ;
- (ii)  $y \in A(x) \Rightarrow A(y) \leq A(x)$ ; and
- (iii)  ${}^y A(x) = A({}^y x)$ ,

for all  $x, y \in G$ . Let  $\mathcal{A}$  denote the family of subgroups  $\{A(x) : x \in G\}$ .

A good example to keep in mind is the mapping  $A$  that assigns to each  $x \in G$  the cyclic group  $\langle x \rangle$  generated by  $x$ . It is easily verified that the mapping  $A : x \mapsto A(x) = \langle x \rangle$  satisfies the axioms. The family of subgroups  $\mathcal{A}$ , in this case, is the family of all cyclic subgroups of  $G$ .

Returning to a general mapping  $A$  satisfying (i)–(iii), we define an equivalence relation  $\sim_A$  on  $G$ , setting  $x \sim_A y$  whenever  $A(x) =_G A(y)$ , where  $=_G$ , as usual, denotes conjugacy in  $G$ . The equivalence classes relative to  $\sim_A$  are called  $A$ -classes, and we let  $\operatorname{ch}_{\mathcal{A}} G$  denote the subring of  $\operatorname{ch}' \mathbb{Q}G$  consisting of virtual rational valued characters that are constant on the  $A$ -classes, where  $\operatorname{ch}' \mathbb{Q}G$  is the ring of rational-valued characters of  $G$ .

We next define another  $\mathbb{Z}$ -submodule of  $\operatorname{ch}' \mathbb{Q}G$ :

$$P(G, \mathcal{A}) = \left\{ \sum_{x \in G} \mathbb{Z}(1_{A(x)})^G \right\}.$$

Now let  $\{\langle x_1 \rangle, \dots, \langle x_t \rangle\}$  be a set of representative of the conjugacy classes of cyclic subgroups of  $G$ . Let  $\mathfrak{G} = \operatorname{Gal}(\mathbb{Q}(\epsilon)/\mathbb{Q})$ , where  $\epsilon$  is a primitive  $n$ -th root of 1,  $n = |G|$ . Then  $\mathfrak{G}$  permutes the set  $X = \operatorname{Irr} G$  consisting of the absolutely irreducible characters of  $G$ , and also permutes the set  $Y$  consisting of  $G$ -conjugacy classes (see §21A). By (11.9) and the proof of 11.10, these permutation actions of  $\mathfrak{G}$  both have the same number of orbits, and this number is equal to the number  $t$  of conjugacy classes of cyclic subgroups, by Exercise 15.4. Let  $\{X_1, \dots, X_t\}$  and  $\{Y_1, \dots, Y_t\}$  denote the  $\mathfrak{G}$ -orbits on the sets  $X = \operatorname{Irr} G$  and  $Y$ , respectively, and choose notation so that the  $G$ -conjugacy class  $\mathfrak{C}_i$  containing  $x_i$  belongs to  $Y_i$ , for  $1 \leq i \leq t$ . Let

$$a_i = |X_i|, \quad b_i = |Y_i|, \quad \text{for } 1 \leq i \leq t,$$

and set

$$v = (a_1 \cdots a_t)^{-1} b_1 \cdots b_r.$$

**(75.31) Theorem** (Solomon [74].) *Let  $G$  be a finite group, and let  $\{A(x) : x \in G\}$  be a family of subgroups satisfying the conditions (i)–(iii). Then we have:*

- (i)  $P(G, \mathcal{A}) \subseteq \text{ch}_{\mathcal{A}} G$ , and the index  $|\text{ch}_{\mathcal{A}} G : P(G, \mathcal{A})|$  is finite.
- (ii) The exponent of the quotient group  $(\text{ch}_{\mathcal{A}} G)/P(G, \mathcal{A})$  divides  $|G|$ .
- (iii) Assume, for all  $x, y \in G$ , that  $A(x) = {}_G A(y)$  implies  $\langle x \rangle = {}_G \langle y \rangle$ . Then  $P(G, \mathcal{A})$  is of finite index in  $\text{ch}' QG$ , and we have

$$|\text{ch}' QG : P(G, \mathcal{A})|^2 = v \prod_{i=1}^t |N_G(A_i)|^2 |C_i|^{-1},$$

where

$$A_i = A(x_i), \quad N_i = N_G(A_i), \quad \text{and} \quad C_i = C_G(x_i), \quad 1 \leq i \leq t.$$

*Proof.* (i) and (ii). Let  $H \leq G$ . It is clear that, for all  $x \in G$ ,

$$|H|(1_H)^G(x) = \text{card} \{g \in G : {}^g x = gxg^{-1} \in H\}.$$

Suppose  $x \sim_A y$ ; then  $A(x) = {}_G A(y)$  for some  $g \in G$ . By the axioms (i)–(iii), we obtain, for each  $z \in G$ ,

$${}^h x \in A(z) \Leftrightarrow {}^h A(x) \leq A(z) \Leftrightarrow {}^{hg} A(y) \leq A(z) \Leftrightarrow {}^{hg} y \in A(z),$$

for all  $h \in G$ . It follows that

$$(1_{A(z)})^G(x) = (1_{A(z)})^G({}^g y) = (1_{A(z)})^G(y),$$

and we have proved that  $P(G, \mathcal{A}) \subseteq \text{ch}_{\mathcal{A}} G$ .

We next observe that if  $\langle x \rangle = {}_G \langle y \rangle$ , then  $A(x) = {}_G A(y)$  by (i)–(iii), and hence  $x \sim_A y$ . Therefore we may choose a subset of  $\{x_1, \dots, x_s\}$  as representatives of the  $A$ -classes. By renumbering, we may assume that  $\{x_1, \dots, x_s\}$  is a cross section of the  $A$ -classes, and that

$$A(x_i) \leq_G A(x_j) \Rightarrow i \leq j, \quad \text{for } 1 \leq i, j \leq s.$$

Let us set

$$\alpha_{ki} = (1_{A(x_k)})^G(x_i), \quad 1 \leq i, k \leq s;$$

then we have

$$\alpha_{ki} = |G| |\mathfrak{C}_i \cap A(x_k)| |A(x_k)|^{-1} |\mathfrak{C}_i|^{-1},$$

by Exercise 10.5.

Suppose  $\alpha_{ki} \neq 0$ . Then  $\mathfrak{C}_i \cap A(x_k) \neq \emptyset$ , so  ${}^y x_i \in A(x_k)$  for some  $y \in G$ . Then  ${}^y A(x_i) \leq A(x_k)$  by the axioms (i)–(iii), and hence  $i \leq k$ . Therefore the  $s \times s$  matrix  $(\alpha_{ki})$  is triangular. If  ${}^y x_i \in A(x_i)$  for some  $y \in G$ , then  ${}^y A(x_i) \leq A(x_i)$ , and hence  $y \in N_i = N_G(A(x_i))$ . Conversely, if  $y \in N_i$ , then  ${}^y x_i \in {}^y A(x_i) = A(x_i)$ . This shows that the diagonal elements of the matrix  $(\alpha_{ki})$  are given by

$$(75.32) \quad \alpha_{ii} = |N_i : A_i|, \quad 1 \leq i \leq s.$$

Now let  $\mathfrak{X}_i$  be the  $A$ -class of  $x_i$ , for  $1 \leq i \leq s$ , and let  $\lambda_i$  denote its characteristic function, so  $\lambda_i(x) = 1$  if  $x \sim_A x_i$  and is zero otherwise. Then we obtain

$$\begin{aligned} (1_{A(x_j)})^G &= \sum_{i=1}^s (1_{A(x_j)})^G(x_i) \lambda_i = \sum_{i=1}^s \alpha_{ji} \lambda_i \\ &= \sum_{i=1}^{j-1} \alpha_{ji} \lambda_i + \alpha_{jj} \lambda_j \in P(G, \mathcal{A}), \end{aligned}$$

using the fact that the matrix  $(\alpha_{ji})$  is triangular. Since  $\alpha_{jj} = |N_j : A_j|$  by (75.32), for  $1 \leq j \leq s$ , it follows by induction that

$$|G| \lambda_j \in P(G, \mathcal{A}) \quad \text{for } 1 \leq j \leq s.$$

If  $\varphi \in \text{ch}_{\mathcal{A}} G$ , then  $\varphi$  is constant on the  $A$ -classes, so

$$|G| \varphi = \sum_{j=1}^s \varphi(x_j) |G| \lambda_j \in P(G, \mathcal{A}),$$

completing the proof of parts (i) and (ii).

(iii) By the hypothesis of part (iii), we have  $s = t$ . Moreover,  $P(G, \mathcal{A})$  is of finite index in  $\text{ch}' QG$ , by part (i). Indeed let  $\xi_j$  denote the sum of the characters in the  $\mathfrak{G}$ -orbit  $X_j$ , for  $1 \leq j \leq t$ . Then  $\{\xi_1, \dots, \xi_t\}$  is a  $Z$ -basis of  $\text{ch}' QG$ , and  $\text{ch}' QG = \text{ch}_{\mathcal{A}} G$ , by the proof of (21.5). For each  $k$ ,  $1 \leq k \leq t$ , let  $\mathfrak{Y}_k$  be the set consisting of all elements of  $G$  whose conjugacy class belongs to the  $\mathfrak{G}$ -orbit  $Y_k$ . If  $x \in \mathfrak{C}_k$ , then  $\xi_j(x) = \xi_j(x_k)$ , for  $1 \leq j \leq t$ , by (21.5). We also note that  $\mathfrak{Y}_k$  is the union of  $b_k$  conjugacy classes, all of cardinality  $|G : C_k|$ . On the other hand, each character  $\xi_j$  is the sum of  $a_j$  distinct absolutely irreducible characters, for  $1 \leq j \leq t$ . By the orthogonality relations (9.23), we obtain

$$(75.33) \quad a_i \delta_{ij} = (\xi_i, \xi_j) = |G|^{-1} \sum_{x \in G} \xi_i(x) \xi_j(x^{-1}) = \sum_{k=1}^t b_k |C_k|^{-1} \xi_i(x_k) \xi_j(x_k).$$

Here we have used the fact that  $\xi_j(x^{-1}) = \xi_j(x)$ , since  $\xi_j$  is a rational-valued character. Next, define  $t \times t$  matrices

$$\mathbf{A} = (\alpha_{ij}), \quad \mathbf{B} = (\xi_i(x_j)), \quad \mathbf{D} = (a_i \delta_{ij}), \quad \mathbf{E} = (b_i |C_i|^{-1} \delta_{ij}),$$

where  $\alpha_{ij} = (1_{A(x_i)})^G(x_j)$  as in parts (i) and (ii). By (75.33), we have

$$\mathbf{D} = \mathbf{B}\mathbf{E}'\mathbf{B}.$$

Taking determinants, we obtain

$$(75.34) \quad v^{-1} \prod_{i=1}^k |C_i| = (\det \mathbf{B})^2, \quad \text{where} \quad v = (\prod a_i)^{-1} (\prod b_i) \quad \text{as above.}$$

Since  $(1_{A(x_k)})^G \in \text{ch}' QG$ , we may write

$$(1_{A(x_k)})^G = \sum_{j=1}^t c_{kj} \xi_j, \quad \text{with} \quad c_{kj} \in \mathbb{Z}, \quad 1 \leq j, k \leq t.$$

Using the facts that  $\{(1_{A(x_1)})^G, \dots, (1_{A(x_t)})^G\}$  and  $\{\xi_1, \dots, \xi_t\}$  are  $\mathbb{Z}$ -bases for  $P(G, \mathcal{A})$  and  $\text{ch}' QG$ , respectively, we obtain

$$|\text{ch}' QG : P(G, \mathcal{A})| = \det \mathbf{C},$$

where  $\mathbf{C} = (c_{kj})$  as above. We also have

$$(75.35) \quad \det \mathbf{A} = \det \mathbf{C} \det \mathbf{B} = |\text{ch}' QG : P(G, \mathcal{A})| \det \mathbf{B},$$

by the formula expressing the characters  $(1_{A(x_k)})^G$  in terms of the  $\{\xi_j\}$  and the definition of the matrices  $\mathbf{A}$  and  $\mathbf{B}$ . Since  $\mathbf{A}$  is a triangular matrix whose diagonal entries are  $\{|N_i : A_i| : 1 \leq i \leq t\}$ , by (75.32), we obtain the desired formula for the index  $|\text{ch}' QG : P(G, \mathcal{A})|$  by comparing (75.34) and (75.35). This completes the proof of the theorem.

**Remark.** In case  $A(x) = \langle x \rangle$  for  $x \in G$ , parts (i) and (ii) of the preceding theorem give another proof of the Artin Induction Theorem 15.4. For yet another proof, see CR (39.1)

We conclude this section with the following application of Solomon's Theorem to the characters of  $S_n$ . We recall from the discussion following Lemma 75.4 that the Young subgroups of type  $\alpha$  are the row subgroups  $\{R(T)\}$ , as  $T$  ranges over the set of  $\alpha$ -tableaux, and that they form a conjugacy class of subgroups of  $S_n$ , for each partition  $\alpha$ . We now have:

**(75.36) Theorem (Frobenius).** *Let  $\mathcal{A}$  be the family of Young subgroups of  $S_n$  of type  $\alpha$ , for all partitions  $\alpha$ . Then*

$$\text{ch } QS_n = P(S_n, \mathcal{A}).$$

*Proof.* (Solomon [74].) If  $x \in S_n$ , let  $\alpha_i = \alpha_i(x)$  denote the number of  $\langle x \rangle$ -orbits

in  $\Omega = \{1, \dots, n\}$  of cardinality  $i$ , and set

$$(75.37) \quad \alpha = \alpha(x) = (\alpha_1(x), \dots, \alpha_n(x)).$$

Let  $f(\alpha)$  and  $g(\alpha)$  be the positive integers defined by

$$f(\alpha) = \alpha_1! \cdots \alpha_n!, \quad g(\alpha) = 1^{\alpha_1} 2^{\alpha_2} \cdots n^{\alpha_n},$$

where we set  $\alpha_i! = 1$  if  $\alpha_i = 0$ . Let  $A(x)$  be the subgroup of  $S_n$  defined by

$$A(x) = \{y \in S_n : y\Delta_i = \Delta_i \text{ for each } i\}$$

where  $\{\Delta_i\}$  are the  $\langle x \rangle$ -orbits in  $\Omega$ . Then  $A(x)$  is clearly a Young subgroup of type  $\alpha$ , where  $\alpha$  is the partition of  $n$  defined by (75.37), and the map  $x \rightarrow A(x)$  satisfies the axioms (i)–(iii). We also have  $A(x) = {}_G A(y) \Rightarrow \alpha(x) = \alpha(y)$ , and hence

$$A(x) = {}_G A(y) \Rightarrow \langle x \rangle = {}_G \langle y \rangle.$$

By Theorem 75.19, we have  $\text{ch}' QG = \text{ch } QG$ . Thus we may apply Theorem 75.31 to calculate the index

$$|\text{ch } QS_n : P(S_n, \mathcal{A})|,$$

where  $\mathcal{A}$  is the family of subgroups  $\{A(x) : x \in S_n\}$ , and Frobenius's Theorem will follow if we can show that the index is 1.

We first compute  $|N(A(x)) : A(x)|$ , where  $N(A(x)) = N_{S_n}(A(x))$ . If  $y \in N(A(x))$  then

$$xy\Delta_i = yy^{-1}xy\Delta_i = y\Delta_i$$

for each  $\langle x \rangle$ -orbit  $\Delta_i \subseteq \Omega$ , since  $y^{-1}xy \in A(x)$ . Then  $y\Delta_i$  is stable under the action of  $x$ , and is an  $\langle x \rangle$ -orbit. Moreover,  $|y\Delta_i| = |\Delta_i|$  for each  $i$ , and hence  $y$  permutes the set of  $\alpha_i$  orbits of cardinality  $i$ , for each  $i$ . Therefore we obtain a homomorphism

$$\theta : N(A(x)) \rightarrow S_{\alpha_1} \times S_{\alpha_2} \times \cdots \times S_{\alpha_n}.$$

If  $\Delta = \{k_1, \dots, k_i\}$  and  $\Delta' = \{k'_1, \dots, k'_i\}$  are two  $x$ -orbits of cardinality  $i$ , then we may choose  $y \in S_n$  that interchanges  $k_j$  and  $k'_j$  for  $j = 1, \dots, i$  and fixes the remaining elements of  $\Omega$ . Then  $y \in N(A(x))$ , and  $y$  interchanges  $\Delta$  and  $\Delta'$  and fixes the remaining orbits. Since the symmetric groups  $\{S_{\alpha_i}\}$  are generated by transpositions, it follows that the homomorphism  $\theta$  is surjective. Its kernel consists of the elements  $y \in S_n$  such that  $y\Delta_i = \Delta_i$  for each  $i$ , and this is the subgroup  $A(x)$ . We have proved that

$$|N(A(x)) : A(x)| = f(\alpha).$$

Letting  $C(x)$  denote the centralizer of  $x$  in  $S_n$ , it is easily proved that

$$|C(x)| = f(\alpha)g(\alpha).$$

Before we can apply Theorem 75.31, we calculate the integer  $v = (a_1 \cdots a_r)^{-1} b_1 \cdots b_t$ , where  $a_i = |X_i|$  and  $b_i = |Y_i|$  and  $X_i$  is a  $\mathfrak{G}$ -orbit in  $\text{Irr } G$  and  $Y_i$  is a  $\mathfrak{G}$ -orbit in the conjugacy classes of  $S_n$ . But in the case of  $S_n$ , we have  $a_i = 1$  for all  $i$ , since the irreducible characters are rational valued (see Theorem 75.19 or §21A) and it is easily checked that the cardinalities  $b_i = |Y_i|$  are all 1. Thus  $v = 1$ , and Solomon's Theorem 75.31 implies that

$$|\text{ch } QS_n : P(S_n, \mathcal{A})|^2 = \prod_{\alpha} f(\alpha)g(\alpha)^{-1},$$

where the product is taken over all  $n$ -tuples  $\alpha = (\alpha_1, \dots, \alpha_n)$  of nonnegative integers such that  $\alpha_1 + 2\alpha_2 + \cdots + n\alpha_n = n$ . The Frobenius Theorem, that  $\text{ch } QS_n = P(S_n, \mathcal{A})$ , is a consequence of the following combinational result.

**(75.38) Lemma.**  $\prod_{\alpha} f(\alpha) = \prod_{\alpha} g(\alpha)$ .

*Proof.* For  $n \in \mathbb{Z}$ , let  $\Lambda(n)$  be the set of partitions of  $n$ , with the conventions that  $\Lambda(0)$  consists of a single partition and  $\Lambda(n)$  is empty if  $n < 0$ . Let

$$\Lambda = \bigcup_{n \in \mathbb{Z}} \Lambda(n).$$

If  $\lambda \in \Lambda$  and  $i$  is a positive integer, we let  $\alpha_i(\lambda)$  be the number of parts of  $\lambda$  of cardinality equal to  $i$ .

Let  $j$  be a positive integer, which will remain fixed throughout the rest of the discussion. If  $\lambda \in \Lambda$ , let  $S_j(\lambda)$  be the set of partitions in  $\Lambda$  obtained by deleting from  $\lambda$  any positive integral number of parts of size  $j$ . If  $\lambda \in \Lambda(n)$  and  $\mu \in S_j(\lambda)$  then  $\mu \in \Lambda(n - jk)$  for some  $k = 1, 2, \dots$ . Conversely, if  $\mu \in \Lambda(n - jk)$ , then by adjoining  $k$ -parts of size  $j$  to  $\mu$ , we obtain an element of  $\Lambda(n)$ . This shows that

$$\bigcup_{\lambda \in \Lambda(n)} S_j(\lambda) = \bigcup_{k \geq 1} \Lambda(n - jk).$$

Now let  $\lambda, \lambda' \in \Lambda(n)$  and assume that  $S_j(\lambda) \cap S_j(\lambda') \neq \emptyset$ . Let  $\mu \in S_j(\lambda) \cap S_j(\lambda')$ . Then  $\alpha_k(\lambda) = \alpha_k(\lambda') = \alpha_k(\mu)$  for  $k \neq j$ . Since  $\lambda$  and  $\lambda'$  are both partitions of  $n$ , this forces  $\alpha_j(\lambda) = \alpha_j(\lambda')$ , and hence  $\lambda = \lambda'$ . Thus we have

$$(75.39) \quad \sum_{\lambda \in \Lambda(n)} |S_j(\lambda)| = \sum_{k \geq 1} |\Lambda(n - jk)|.$$

Now let  $\lambda \in \Lambda$  and let  $T_j(\lambda)$  be the set of partitions obtained from  $\lambda$  by omitting  $j$  parts of the same size. If  $\alpha_k(\lambda) < j$  for all  $k = 1, 2, \dots$ , then  $T_j(\lambda)$  is empty. If  $\lambda \in \Lambda(n)$  and  $\mu \in T_j(\lambda)$ , then  $\mu \in \Lambda(n - jk)$  for some  $k = 1, 2, \dots$ . Conversely, if  $\mu \in \Lambda(n - jk)$ ,

we can adjoin  $j$  parts of size  $k$  to  $\mu$ , to obtain an element of  $\Lambda(n)$ . Therefore

$$\bigcup_{\lambda \in \Lambda(n)} T_j(\lambda) = \bigcup_{k \geq 1} \Lambda(n - jk).$$

Now suppose  $T_j(\lambda) \cap T_j(\lambda') \neq \emptyset$  for  $\lambda, \lambda' \in \Lambda(n)$ , and let  $\mu \in T_j(\lambda) \cap T_j(\lambda')$ . Then there exist positive integers  $i$  and  $i'$  such that

$$\begin{aligned} \alpha_i(\mu) &= \alpha_i(\lambda) - j, & \alpha_k(\mu) &= \alpha_k(\lambda) \quad \text{for } k \neq i \\ \alpha_{i'}(\mu) &= \alpha_{i'}(\lambda) - j, & \alpha_k(\mu) &= \alpha_k(\lambda') \quad \text{for } k \neq i'. \end{aligned}$$

Since  $\lambda$  and  $\lambda'$  are both partitions of the same integer, we have

$$\begin{aligned} ij + \sum_{k \geq 1} k\alpha_k(\mu) &= \sum_{k \geq 1} k\alpha_k(\lambda) = \sum_{k \geq 1} k\alpha_k(\lambda') \\ &= i'j + \sum_{k \geq 1} k\alpha_k(\mu). \end{aligned}$$

Then  $i = i'$  and  $\lambda = \lambda'$ . This proves that

$$(75.40) \quad \sum_{\lambda \in \Lambda(n)} |T_j(\lambda)| = \sum_{k \geq 1} |\Lambda(n - jk)|.$$

Upon comparing (75.40) and (75.39), we obtain

$$\sum_{\lambda \in \Lambda(n)} |S_j(\lambda)| = \sum_{\lambda \in \Lambda(n)} |T_j(\lambda)|.$$

This implies that

$$(75.41) \quad \sum_{\lambda \in \Lambda(n)} \alpha_j(\lambda) = \sum_{\lambda \in \Lambda(n)} \sum_{\alpha_i(\lambda) \geq j} 1.$$

Since this holds for  $j = 1, 2, \dots$ , the assertion of the lemma follows. This is shown by noting that the left side of (75.41), suitably interpreted, is the contribution of  $j$  to  $\prod g(\alpha)$ , while the right side is the contribution of  $j$  to  $\prod f(\alpha)$ . This completes the proof of (75.38).

By Theorem 75.19, every irreducible character afforded by a simple  $CS_n$ -module belongs to  $\text{ch } QS_n$ . Since  $S_n$  is a Coxeter group of type  $A_{n-1}$ , and the Young subgroups of  $S_n$  coincide with the parabolic subgroups defined by a Coxeter system of type  $A_{n-1}$  in  $S_n$ , we obtain the following result (see the remark following (67.9)).

**(75.42) Corollary.** *Let  $(W, S)$  be a finite Coxeter system of type  $A_n$ , and let  $\zeta \in \text{Irr } W$ . Then there exist integers  $\{n_J : J \subseteq S\}$  such that*

$$\zeta = \sum_{J \subseteq S} n_J (1_{W_J})^W.$$

For related results concerning other types of Coxeter groups, see Mayer [75], Solomon [74], and Tokuyama [84].

## §76. THE ARTIN EXPONENT

Throughout this section, let  $G$  be a finite group of order  $n$ , and let  $\mathcal{C}(= \mathcal{C}(G))$  be the set of cyclic subgroups of  $G$ . As usual,  $\text{ch } \mathbb{Q}G$  denotes the ring of virtual characters afforded by  $\mathbb{Q}G$ -modules. By (15.5),  $\sum_{C \in \mathcal{C}} \text{ind}_C^G \text{ch } \mathbb{Q}C$  is an ideal in  $\text{ch } \mathbb{Q}G$ . We define the *Artin cokernel* of  $G$ , denoted by  $AC(G)$ , as follows:

$$(76.1) \quad AC(G) = \text{Artin cokernel of } G = (\text{ch } \mathbb{Q}G) \left/ \sum_{C \in \mathcal{C}} \text{ind}_C^G \text{ch } \mathbb{Q}C \right.$$

Then  $AC(G)$  is a commutative ring with identity element. The characteristic of  $AC(G)$  is by definition the *Artin exponent*  $A(G)$  of  $G$ . Thus,  $A(G)$  is the least positive integer  $m$  such that

$$(76.2) \quad m \cdot \text{ch } \mathbb{Q}G \subseteq \sum_{C \in \mathcal{C}} \text{ind}_C^G \mathbb{Q}C,$$

and  $A(G)$  divides any  $m$  for which (76.2) is valid. Now let  $\varphi$  be a rational-valued character of  $G$ . By Solomon's Theorem 75.31, we may write

$$(76.3) \quad n\varphi = \sum_{C \in \mathcal{C}} a_C (1_C)^G \quad \text{with coefficients } a_C \in \mathbb{Z}.$$

It follows that (76.2) holds when  $m$  is replaced by  $n$ , and consequently

$$(76.4) \quad A(G) \text{ divides } n, \quad \text{where } n = |G|.$$

We note also that since  $\sum_{C \in \mathcal{C}} \text{ind}_C^G \text{ch } \mathbb{Q}C$  is an ideal of  $\text{ch } \mathbb{Q}G$ ,  $A(G)$  is the least positive  $m$  such that  $m \cdot 1_G$  is a  $\mathbb{Z}$ -linear combination of characters induced from rational characters of cyclic subgroups of  $G$ .

The importance of the Artin exponent stems from the theory of Frobenius functors and Frobenius modules. By (16.10) we have  $\text{ch } \mathbb{Q}G \cong G_0(\mathbb{Q}G)$ , and so  $\text{ch } \mathbb{Q}G$  is a Frobenius functor. We have shown in §49C that the locally free class group  $\text{Cl } \mathbb{Z}G$ , the kernel group  $D(\mathbb{Z}G)$ , and the projective class group  $K_0(\mathbb{Z}G)$  are Frobenius modules over  $G_0(\mathbb{Q}G)$ . From (38.14) we thus obtain:

**(76.5) Proposition.** *Let  $A(G)$  be the Artin exponent of  $G$ , and let  $M(G)$  be any Frobenius module over the Frobenius functor  $\text{ch } \mathbb{Q}G$ .*

- (i) *Let  $x \in M(G)$  be such that  $\text{res}_C^G x = 0$  for all  $C \in \mathcal{C}$ . Then  $A(G) \cdot x = 0$ .*
- (ii) *We have*

$$A(G) \cdot M(G) \subseteq \sum_{C \in \mathcal{C}} \text{ind}_C^G M(C).$$

In particular, these results hold when  $M(G)$  is chosen to be

$$\text{Cl}(ZG), \quad D(ZG), \quad \text{or} \quad K_0(ZG).$$

This proposition plays a key role in the proof of Ullom's Theorem 53.12, which asserts that  $A(G)$  annihilates the Swan subgroup  $T(G)$  defined in §53A. On the other hand, taking for granted the values of  $A(G)$  for  $G$  a  $p$ -group, Taylor's Theorem 54.15 shows that for  $p$  odd,  $|T(G)| = A(G)$  for each  $p$ -group  $G$ . Further, for  $p = 2$ ,  $|T(G)| = A(G)/2$  apart from a few exceptional cases.

In computations of the Artin exponent  $A(G)$ , it is often useful to work with permutation characters  $(1_C)^G$  rather than arbitrary rational characters of  $G$ . The justification for this procedure comes from the following key result of Lam [68b], which is based on an earlier argument by Swan [63].

**(76.6) Proposition.** *For  $G$  a cyclic group,*

$$\text{ch } QG = \sum_{C \leq G} Z \cdot (1_C)^G,$$

where  $C$  ranges over all subgroups of  $G$ .

*Proof.* The result is trivial for  $|G| = 1$ . Next, let  $G = \langle x \rangle$  be a cyclic  $p$ -group of order  $p^m$ , where  $p$  is prime and  $m \geq 1$ . The simple  $QG$ -modules are given by  $K_r = Q[x]/(\Phi_{p^r}(x))$ ,  $0 \leq r \leq m$ , where  $\Phi_{p^r}(x)$  denotes the cyclotomic polynomial of order  $p^r$ . For  $r \geq 1$ ,

$$(x^{p^r} - 1) = (x^{p^{r-1}} - 1)\Phi_{p^r}(x),$$

and thus we obtain

$$Q[x]/(x^{p^r} - 1) \cong K_r \oplus Q[x]/(x^{p^{r-1}} - 1).$$

However,  $Q[x]/(x^{p^r} - 1)$  affords the permutation character  $(1_C)^G$  of  $G$ , where  $C \leq G$  has index  $p^r$ . It follows from the above that the character of  $G$  afforded by  $K_r$  is a difference of permutation characters for  $r \geq 1$ . On the other hand,  $K_0$  affords the trivial character  $1_G$ . This completes the proof when  $G$  is a cyclic  $p$ -group.

Now let  $G$  be arbitrary, and use induction on  $|G|$ . We may assume that  $G = G_1 \times G_2$ , where  $G_1$  and  $G_2$  are nontrivial cyclic groups of relatively prime orders, and where the proposition holds for both  $G_1$  and  $G_2$ . Each simple  $QG$ -module is a cyclotomic field of the form  $L_1 \otimes_Q L_2$ , with  $L_i$  a simple  $QG_i$ -module,  $i = 1, 2$ . If  $L_i$  affords the irreducible character  $\varphi_i$  of  $G_i$ , then  $L_1 \otimes L_2$  affords the character  $\varphi_1 \times \varphi_2$  of  $G_1 \times G_2$ . Let  $C_i$  range over the subgroups of  $G_i$ ,  $i = 1, 2$ . The proposition then holds for  $G$ , by virtue of the obvious formula

$$(76.7) \quad (1_{C_1})^{G_1} \times (1_{C_2})^{G_2} \cong (1_{C_1 \times C_2})^{G_1 \times G_2}.$$

This completes the proof.

Returning to arbitrary groups  $G$ , we note next that conjugate subgroups of  $G$  yield the same induced characters, by (10.12ii). Hence in all of our previous remarks, we may replace  $\mathcal{C}$  by  $\mathcal{C}_0$ , where  $\mathcal{C}_0$  is a full set of nonconjugate cyclic subgroups of  $G$ . By Exercise 15.4, the permutation characters  $\{(1_C)^G : C \in \mathcal{C}_0\}$  are linearly independent over  $\mathbb{Q}$ , and span the space of all  $\mathbb{Q}$ -valued class functions on  $G$ . Thus, in expressing a virtual character  $\varphi \in \text{ch } QG$  as a linear combination of characters  $\{(1_C)^G : C \in \mathcal{C}_0\}$ , the coefficients are rational numbers that are uniquely determined by  $\varphi$ . Further, by the tensor identity (15.5), (76.2) holds if and only if  $m \cdot 1_G$  lies in the right hand expression in (76.2). From these remarks, together with (76.6), we obtain at once:

**(76.8) Corollary.** *Let  $G$  be an arbitrary finite group, and  $\mathcal{C}_0$  a full set of nonconjugate cyclic subgroups of  $G$ . Then  $A(G)$  is the smallest positive integer  $m$  such that*

$$(76.9) \quad m \cdot 1_G = \sum_{C \in \mathcal{C}_0} a_C (1_C)^G \quad \text{with each } a_C \in \mathbb{Z}.$$

**(76.10) Remarks.** (i) If  $m$  is a positive integer, and (76.9) holds for some set of integers  $\{a_C\}$  with G.C.D. 1, then necessarily  $m = A(G)$ .

(ii) Given a group  $G$ , one can compute the characters  $\{(1_C)^G\}$  explicitly, and then use (76.8) to determine  $A(G)$ . For example, let  $G = S_3$ , and take  $\mathcal{C}_0 = \{C_1, C_2, C_3\}$ , with  $C_i$  cyclic of order  $i$ . It is easily verified that

$$2 \cdot 1_G = -(1_{C_1})^G + 2(1_{C_2})^G + (1_{C_3})^G,$$

and therefore  $A(G) = 2$ . For other examples, see Exercises 76.1, 76.2.

We turn next to some functorial properties of the Artin exponent, all due to Lam [68b]. We use repeatedly the fact that for  $m \in \mathbb{Z}$ ,

$$(76.11) \quad m \cdot 1_G \in \sum_{C \leq G} \mathbb{Z} \cdot (1_C)^G \quad \text{if and only if } A(G) \text{ divides } m,$$

where  $C$  ranges over all cyclic subgroups of  $G$ . Using this, we show:

**(76.12) Proposition.** (i) *If  $H \leq G$ , then  $A(H)$  divides  $A(G)$ .*

(ii) *If  $\bar{G}$  is a homomorphic image of  $G$ , then  $A(\bar{G})$  divides  $A(G)$ .*

(iii)  *$A(G_1 \times G_2) = A(G_1)A(G_2)$  if  $(|G_1|, |G_2|) = 1$ .*

*Proof.* (i) We may write

$$(76.13) \quad A(G) \cdot 1_G = \sum_{C < G} a_C (1_C)^G, \quad a_C \in \mathbb{Z}.$$

For  $H \leq G$ , this gives

$$A(G) \cdot 1_H = \sum_C a_C \text{res}_H^G(1_C)^G.$$

But  $\text{res}_H^G(1_C)^G$  is a sum of permutation characters of  $H$ , by Mackey's Subgroup Theorem 10.13. Therefore  $A(H)$  divides  $A(G)$ .

(ii) The homomorphism  $G \rightarrow \bar{G}$  extends to a surjection of rings  $\mathbb{Q}G \rightarrow \mathbb{Q}\bar{G}$ , inducing a surjection  $G_0(\mathbb{Q}G) \rightarrow G_0(\mathbb{Q}\bar{G})$  of Grothendieck groups. Each cyclic subgroup  $C \leq G$  maps onto a cyclic subgroup  $\bar{C} \leq \bar{G}$ , and the diagram

$$\begin{array}{ccc} G_0(\mathbb{Q}C) & \longrightarrow & G_0(\mathbb{Q}\bar{C}) \\ \downarrow \text{ind} & & \downarrow \text{ind} \\ G_0(\mathbb{Q}G) & \longrightarrow & G_0(\mathbb{Q}\bar{G}) \end{array}$$

commutes. It follows that the Artin cokernel of  $G$  maps *onto* that of  $\bar{G}$ , and therefore  $A(G)$  annihilates the Artin cokernel of  $\bar{G}$ . This implies that  $A(G)$  is a multiple of  $A(\bar{G})$ , as claimed.

(iii)  $A(G_1)A(G_2)$  divides  $A(G_1 \times G_2)$ , by (i). On the other hand from (76.7), and (76.13) for  $G_1$  and  $G_2$ , we deduce that  $A(G_1 \times G_2)$  divides  $A(G_1)A(G_2)$ . This completes the proof of the proposition.

It is obvious that if  $G$  is cyclic, then  $A(G) = 1$ . As shown by Lam [68b], the converse also holds, and thus we have:

**(76.14) Theorem.** *The Artin exponent  $A(G) = 1$  if and only if  $G$  is cyclic.*

*Proof.* Assume  $A(G) = 1$ , so by (76.12i),  $A(P) = 1$  for each Sylow  $p$ -subgroup  $P$  of  $G$ . Therefore the exponent of  $P$  equals the order of  $P$ , by Exercise 76.3, and so  $P$  is cyclic. It follows that  $G$  must be metacyclic (see Hall [59, Th. 9.4.3]), and so there exists a normal series

$$1 \leq H \trianglelefteq G, \quad \text{with } H, G/H \text{ cyclic.}$$

Since  $[G, G] \leq H$ , each  $H_0$  with  $H \leq H_0 \leq G$  is also normal in  $G$ . Increasing  $H$  if need be, we may assume that  $H$  is a maximal cyclic subgroup of  $G$ . Now consider the equation

$$A(G)1_G = a_H(1_H)^G + \sum_C a_C(1_C)^G,$$

where the coefficients  $a_H, a_C$  are integers, and where  $C$  ranges over some set of cyclic subgroups of  $G$ , none of which contains a conjugate of  $H$ . Evaluating both sides of the above equation at a generator  $h$  of  $H$ , we obtain

$$A(G) = a_H |N_G(H):H|,$$

since  $(1_C)^G(h) = 0$  for each  $C$  above. Since  $A(G) = 1$  by hypothesis, we conclude that  $N_G(H) = H$ , that is,  $G = H$ . This completes the proof.

For noncyclic  $p$ -groups, where  $p$  is an odd prime, the Artin exponent can be evaluated easily. The next result is due to Lam [68b].

**(76.15) Theorem.** *Let  $G$  be a noncyclic  $p$ -group of order  $p^m$ , where  $p$  is an odd prime. Then  $A(G) = p^{m-1}$ .*

*Proof.* By the Artin Induction Theorem 15.4, we have

$$(76.16) \quad 1_G = \sum_{C \leq G} a_C (1_C)^G, \quad \text{where } a_C = \frac{1}{|G:C|} \sum_{C^* \geq C} \mu(|C^*:C|).$$

Here,  $C$  ranges over all cyclic subgroups of  $G$ , and  $C^*$  over all cyclic subgroups of  $G$  containing  $C$ . Let  $\mathcal{C}_0$  be a full set of nonconjugate cyclic subgroups of  $G$ . A given  $C \in \mathcal{C}_0$  has  $|G:N_G(C)|$  distinct conjugates, so (76.16) becomes

$$(76.17) \quad 1_G = \sum_{C \in \mathcal{C}_0} b_C (1_C)^G, \quad \text{where } b_C = \frac{1}{|N_G(C):C|} \sum_{C^* \geq C} \mu(|C^*:C|).$$

Note that since  $G$  is a  $p$ -group,  $\mu(|C^*:C|) = 0$  except when  $|C^*:C| = 1$  or  $p$ . Of course,  $A(G)$  is the least positive integer such that  $A(G)b_C \in \mathbb{Z}$  for each  $C \in \mathcal{C}_0$ .

We now evaluate  $b_1$ , corresponding to  $C = \{1\}$ . Then

$$b_1 = |G|^{-1}(1 - k),$$

where  $k$  is the number of subgroups of  $G$  of order  $p$ . Since  $G$  is noncyclic, we may apply Kulakoff's Theorem (see page 368) to conclude that the number of elements of order  $p$  in  $G$  is a multiple of  $p^2$ . This gives

$$k(p-1) + 1 \equiv 0 \pmod{p^2}, \quad \text{whence } k \equiv p+1 \pmod{p^2}.$$

Therefore  $b_1 = l/p^{m-1}$  for some  $l \in \mathbb{Z}$ , where  $p \nmid l$ . This shows that  $p^{m-1} \mid A(G)$ . On the other hand,  $A(G) \neq p^m$  by Exercise 76.3, and the proof is complete.

The situation for 2-groups is somewhat more complicated, and we state the results without proof (see Lam [68b]):

**(76.18) Theorem.** *Let  $G$  be a group of order  $2^m$ . Then  $A(G) = 2^{m-1}$ , with the following exceptions:*

$A(G) = 1$  if  $G$  is cyclic.

$A(G) = 2$  if  $G$  is a generalized quaternion group (with  $m \geq 3$ ) or a dihedral group (with  $m \geq 2$ ).

$A(G) = 4$  if  $G$  is a semidihedral group\* (with  $m \geq 4$ ).

\*S. Endo pointed out that  $A(G) = 4$  in this case; Lam gave the incorrect formula  $A(G) = 2$ .

For arbitrary groups  $G$ , Lam has shown how to compute  $A(G)$ , by determining its  $p$ -part  $A_p(G)$  for each prime  $p$ . The proofs are based on formula (76.17), and are given in detail in Lam [68b]. Here, we shall summarize the main results, denoting by  $G_p$  a Sylow  $p$ -subgroup of  $G$ .

**(76.19) Theorem.** *Let  $p$  be an odd prime, and suppose  $G$  has a noncyclic Sylow subgroup  $G_p$  of order  $p^m$ . Then*

(i)  $A_p(G) = p^{m-1}$  if  $G$  contains a cyclic  $p'$ -group  $D$ , normalized by  $G_p$ , with  $G_p$  acting faithfully by conjugation on  $D$ .

(ii)  $A_p(G) = p^m$  otherwise.

**(76.20) Corollary.** *Keeping the above notation,  $A_p(G) = p^{m-1}$  if  $G_p \trianglelefteq G$  or if  $G_p$  is non-abelian.*

On the other hand, Lam [68b] proved:

**(76.21) Theorem.** *Let  $p$  be any prime, and suppose  $G$  has a cyclic Sylow  $p$ -subgroup  $G_p$ . Then  $A_p(G) = p^s$ , where  $s$  is the smallest positive integer such that the following property holds:*

*For each  $x \in G_p$ , and each cyclic  $p'$ -subgroup  $D$  of  $G$ ,*

$$x \in N_G(D) \Rightarrow x^{p^s} \in C_G(D).$$

**(76.22) Corollary.**  $A_p(G) = 1$  if and only if

(i)  $G_p$  is cyclic, and

(ii) for each  $P \leq G_p$  and each cyclic  $p'$ -subgroup  $D \leq G$ ,  $P$  normalizes  $D$  if and only if  $P$  centralizes  $D$ .

**(76.23) Corollary.** *Assume  $G_p$  cyclic. Then  $A_p(G) = 1$  if any of the following hold:*

(i)  $G_p \trianglelefteq G$ .

(ii)  $p \nmid (q - 1)$  for each prime divisor  $q$  of  $|G|$ .

(iii)  $p$  is the largest prime divisor of  $|G|$ .

For further results on the Artin exponent, see Rasmussen [74], [77].

We turn next to the question of determining the order of the Artin cokernel  $AC(G)$ , rather than its characteristic  $A(G)$ . Before stating the result, let us introduce some notation, and review some facts from §74. Let  $\mathcal{C}_0$  be a full set of non-conjugate cyclic subgroups of  $G$ , say

$$\mathcal{C}_0 = \{C_1, \dots, C_s\}, \quad C_i = \langle x_i \rangle.$$

For each  $i$ , let  $\varphi_i = (1_{C_i})^G$  be the corresponding permutation character of  $G$ . We

have seen that these  $\{\varphi_i\}$  are linearly independent, and there are inclusions

$$P(G) = \bigoplus_{i=1}^s \mathbb{Z}\varphi_i \subseteq \text{ch } \mathbb{Q}G \subseteq \text{ch}' \mathbb{Q}G,$$

where  $\text{ch}' \mathbb{Q}G$  is the ring of rational-valued characters on  $G$ . By definition,  $AC(G) = (\text{ch } \mathbb{Q}G)/P(G)$ , and we are trying to calculate  $|\text{ch } \mathbb{Q}G : P(G)|$ .

Let  $\mathfrak{G} = \text{Gal}(\mathbb{Q}(\varepsilon)/\mathbb{Q})$ , where  $\varepsilon$  is a primitive  $n$ -th root of 1,  $n = |G|$ . Then  $\mathfrak{G}$  permutes the absolutely irreducible characters of  $G$ , and there are  $s$  orbits  $X_1, \dots, X_s$  in  $\text{Irr } G$  under the action of  $\mathfrak{G}$ . Correspondingly,

$$\mathbb{Q}G \cong \bigoplus_{i=1}^s A_i, \quad A_i = \text{simple component.}$$

Let  $m_i = \text{index of } A_i$ ; the character of  $G$  afforded by a simple  $A_i$ -module is given by  $m_i \psi_i$ , with

$$\psi_i = \sum_{\zeta \in X_i} \zeta,$$

and  $m_i$  is the Schur index  $m_Q(\zeta)$  for each  $\zeta \in X_i$ . We have (from §74)

$$\text{ch}' \mathbb{Q}G = \bigoplus_{i=1}^s \mathbb{Z}\psi_i \supseteq \text{ch } \mathbb{Q}G = \bigoplus_{i=1}^s \mathbb{Z}m_i \psi_i.$$

Thus  $|\text{ch}' \mathbb{Q}G : \text{ch } \mathbb{Q}G| = \prod m_i$ .

The group  $\mathfrak{G}$  also acts on the conjugacy classes of  $G$ . If  $\sigma \in \mathfrak{G}$  is such that  $\sigma(\varepsilon) = \varepsilon^k$ , where  $(k, n) = 1$ , then  $\sigma$  carries the conjugacy class of a given element  $x$  onto the class of  $x^k$ . Suppose that the conjugacy classes of  $G$ , under the action of  $\mathfrak{G}$ , are partitioned into orbits  $Y_1, \dots, Y_s$ . Each  $Y_i$  corresponds to a family of conjugate cyclic subgroups of  $G$ , so the number of orbits equals the number of simple components of  $\mathbb{Q}G$ . Let  $|Y_i| = \text{card } Y_i$ , and  $|X_i| = \text{card } X_i$ ,  $1 \leq i \leq s$ . Finally, put

$$N_i = N_G(C_i), \quad H_i = C_G(C_i), \quad 1 \leq i \leq s.$$

Keeping all of the above notation, we now give Solomon's formula for the order of the Artin cokernel  $AC(G)$  of  $G$ .

**(76.24) Theorem.** *The order of  $AC(G)$  is given by the formula*

$$|AC(G)|^2 = v \cdot \prod_{i=1}^s |N_i : C_i|^2 / |H_i| m_i^2, \quad \text{where } v = \prod_{i=1}^s |Y_i| / |X_i|.$$

*Proof.* By the preceding discussion, it suffices to show that

$$|\text{ch}' \mathbb{Q}G : P(G)|^2 = v \cdot \prod_i |N_i : C_i|^2 / |H_i|,$$

which was proved in §75B (see Theorem 75.31).

At the end of §54, we stated without proof a different version of the formula for  $|AC(G)|^2$ , due to Oliver. We leave it to the reader to verify the equivalence of Oliver's formula with that of Solomon.

## §76. Exercises

- Let  $G$  be an elementary abelian  $p$ -group on  $n$  generators, where  $p$  is prime. Prove that  $A(G) = p^{n-1}$ .

[Hint: Use (76.8).]

- Let  $|G| = pq$ , where  $p < q$  are primes, and  $G$  is not cyclic. Prove that  $A(G) = p$ .

[Hint (T.Y. Lam): We may write  $G = C_q \rtimes C_p$ . Now compute  $(1_C)^G$  for  $C$  cyclic of order 1,  $p$  and  $q$ , and use (76.8).]

- Let  $G$  be a group of order  $n$  and exponent  $e$ . Then prove that  $n/e$  divides  $A(G)$ .

[Hint: Evaluating both sides of (76.13) at 1, we obtain

$$A(G) = \sum_C a_C |G:C|.$$

But  $n/e$  divides  $|G:C|$  for each cyclic  $C \leq G$ .]

- Let  $\mathcal{H}$  be the set of hyper-elementary subgroups of  $G$ . Show that

$$A(G) = \text{L.C.M.} \{ A(H) : H \in \mathcal{H} \}.$$

[Hint: Denote this L.C.M. by  $m$ , so  $m|A(G)$  by (76.12). On the other hand, for  $H \in \mathcal{H}$ ,  $m \cdot 1_H$  is a  $\mathbb{Z}$ -linear combination of characters  $\{(1_C)^H : C \leq H, C \text{ cyclic}\}$ . Now use Solomon's Theorem 15.10 to obtain an expression for  $m \cdot 1_G$ .]

# Indecomposable Modules

This chapter contains some of the new ideas that underlie, at least to some extent, the recent surge of interest in the classification of indecomposable modules.

We begin in §77 with a proof of Gabriel’s theorem on the classification of graphs (or quivers) of finite representation type, and their indecomposable representations. The proof, by Bernstein-Gelfand-Ponomarev, is a spectacular example of how root systems and finite reflection groups can appear unexpectedly in contexts apparently far removed from their natural environment, and provide exactly the information needed to solve a difficult classification problem. The discussion takes place in a category that is not a module category. Nevertheless, the ideas have been applied successfully to representations of Artin algebras (see Reiten [85] for a survey).

Section 78 contains an introduction to Auslander-Reiten sequences (or almost-split sequences), first in the category of modules over group algebras of finite groups, and then for the case of f.d. algebras over a field. It now appears that this topic has much to contribute not only to representations of artinian rings and algebras, but also to finite group representation theory. This point is illustrated by an application of almost-split sequences to the Green ring in finite group representation theory in §81. Another application of almost-split sequences occurs in §79, where we give a new proof of Roiter’s Theorem, which settled the Brauer-Thrall conjecture on Artin algebras of finite representation type.

## §77. REPRESENTATIONS OF GRAPHS AND GABRIEL’S THEOREM

### §77A. Representations of Graphs and Coxeter Functors

Throughout this section,  $\Gamma$  denotes a *finite, connected, oriented graph*. We denote the set of vertices of  $\Gamma$  by  $\{\alpha\}$ , and let  $\{e\}$  denote the set of edges. We shall write  $e = (\alpha, \beta)$  to indicate that  $e$  goes from  $\alpha$  to  $\beta$ . At this point, we do not exclude the possibility of more than one edge having the same pair of vertices, or of edges whose vertices coincide (called *loops*). We shall denote by  $|\Gamma|$  the unoriented graph defined by  $\Gamma$ , with the same vertices and edges.

**(77.1) Definitions.** Let  $K$  be an algebraically closed field, and let  $\Gamma$  be a finite

connected oriented graph. The category  $\mathcal{L}(\Gamma)$  of *K-representations* of  $\Gamma$  is defined as follows. An *object*  $(V, f) \in \mathcal{L}(\Gamma)$  consists of a family  $\{V_\alpha\}$  of f.d. *K*-spaces, indexed by the set of vertices  $\{\alpha\}$  of  $\Gamma$ , and a family of *K*-linear maps  $f_e: V_\alpha \rightarrow V_\beta$ , indexed by the set of edges  $\{e = (\alpha, \beta)\}$  of  $\Gamma$ . A *morphism*  $\varphi: (V, f) \rightarrow (W, g)$  between two objects in  $\mathcal{L}(\Gamma)$  consists of a family of *K*-linear maps  $\varphi_\alpha: V_\alpha \rightarrow W_\alpha$ , one for each vertex  $\alpha$ , such that for each edge  $e = (\alpha, \beta)$ , the diagram commutes:

$$\begin{array}{ccc} V_\alpha & \xrightarrow{f_e} & V_\beta \\ \varphi_\alpha \downarrow & & \downarrow \varphi_\beta \\ W_\alpha & \xrightarrow{g_e} & W_\beta \end{array}$$

A morphism  $\varphi: (V, f) \rightarrow (W, g)$  is called an *isomorphism* if each map  $\varphi_\alpha: V_\alpha \rightarrow W_\alpha$  is an isomorphism. The set of morphisms from  $(V, f)$  to  $(W, g)$  is denoted by  $\text{Hom}((V, f), (W, g))$ , or by  $\text{End}(V, f)$ , in case  $(W, g) = (V, f)$ . For each object  $(V, f) \in \mathcal{L}(\Gamma)$ , the *dimension*  $\dim(V, f)$  is defined by the *n*-tuple

$$\dim(V, f) = (\dim_K V_\alpha) \in \mathbb{Z}^n,$$

where *n* is the cardinal number of the vertex set  $\{\alpha\}$ .

The terminology of categories was introduced in §2C, for modules over rings, and is used here with appropriate modifications.

The *direct sum*  $(V, f) \oplus (W, g)$  of two objects in  $\mathcal{L}(\Gamma)$  is defined in the obvious way. The *trivial object*, whose *K*-spaces and maps are all zero, is denoted by 0. An object is *indecomposable* if it is not the trivial object, and is not isomorphic to a direct sum of nontrivial objects.

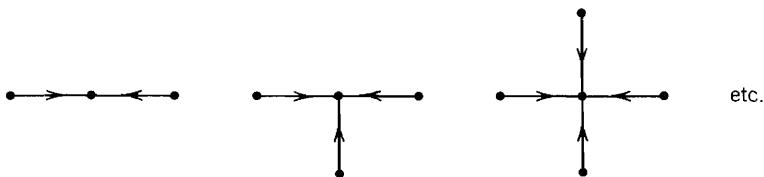
**(77.2) Proposition.** *Every object in  $\mathcal{L}(\Gamma)$  is isomorphic to a direct sum of a finite set of indecomposable objects, and these are uniquely determined up to isomorphism and order of occurrence.*

The proof is left as an exercise. It is essentially the same as the proof of the K-S-A Theorem 6.12. The key step is the observation that, for each object  $(V, f) \in \mathcal{L}(\Gamma)$ ,  $\text{End}(V, f)$  is a local *K*-algebra if and only if  $(V, f)$  is an indecomposable object (see §6A).

**Examples.** (i) Weierstrass raised the problem of classifying pairs of linear maps  $f, g: V_1 \rightarrow V_2$ , up to automorphisms of the vector spaces  $V_1, V_2$ . The problem remained open for more than 20 years, and was solved by Kronecker (see the Kronecker-Weierstrass Theorem 34.40). It involves the category  $\mathcal{L}(\Gamma)$ , for the graph  $\circ \rightrightarrows \circ$ .

(ii) Gelfand-Ponomarev (1970) considered the problem of classifying inclusion-ordered families of subspaces  $\{V_i\}$  of a f.d. *K*-space  $V$ , up to

automorphisms of  $V$ . For example, in the case of two subspaces  $\{V_1, V_2\}$ , the problem is solved using the arithmetic invariants ( $\dim V_1, \dim V_2, \dim V_1 \cap V_2$ ). The solution for three subspaces is a special case of Gabriel's Theorem (see §77B). These problems, in general, involve categories  $\mathcal{L}(\Gamma)$  for the graphs



(iii) The classification of linear maps  $f \in \text{End}_K V$ , up to automorphisms of  $V$ , involves the category  $\mathcal{L}(\Gamma)$ , for the graph  $\bigcirc$ . The indecomposable objects in  $\mathcal{L}(\Gamma)$ , in this case, are described by the Jordan canonical forms of the endomorphisms  $\{f\}$ .

Our objective, in view of (77.2), is the construction of the indecomposable objects in  $\mathcal{L}(\Gamma)$ . We shall present a solution of this problem in §77B, for categories  $\mathcal{L}(\Gamma)$  of finite type (that is, having at most a finite number of isomorphism classes of indecomposable objects).

Besides the indecomposable objects, we also need to consider the *simple objects*  $\{L_\alpha\}$  in  $\mathcal{L}(\Gamma)$ . For each vertex  $\alpha$ , there exists a unique simple object  $L_\alpha$ , such that  $L_\alpha$  is the one-dimensional space  $K$ , the vector spaces associated with other vertices  $\gamma \neq \alpha$  are zero, and all maps are zero.

Following Bernstein-Gelfand-Ponomarev [73], we consider certain changes in orientation of the graphs, and functors between the representation categories resulting from them. We recall, from §2C, that a *covariant functor*  $F$  from a category  $\mathcal{C}$  to a category  $\mathcal{C}'$  assigns to each object  $C$  of  $\mathcal{C}$  an object  $C' = FC$  of  $\mathcal{C}'$ . Moreover,  $F$  assigns, to each morphism  $\varphi: C \rightarrow D$  in  $\mathcal{C}$ , a morphism  $F\varphi: FC \rightarrow FD$  in  $\mathcal{C}'$ , such that  $F$  preserves identity maps and composition of morphisms.

**(77.3) Definition.** Let  $\Gamma$  be an oriented connected graph, and  $\alpha$  a vertex of  $\Gamma$ . Define  $\sigma_\alpha \Gamma$  to be the oriented graph with the same set of vertices and unoriented edges as  $\Gamma$ , which is obtained from  $\Gamma$  by reversing the orientation of all edges starting or ending at  $\alpha$ , and leaving the rest of the graph unchanged.

**(77.4) Definition.** A vertex  $\beta$  of  $\Gamma$  is called a *sink* (or *+ -accessible vertex*) if each edge through  $\beta$  ends at  $\beta$  (in particular there are no loops at  $\beta$ ). For each sink  $\beta$ , we shall define a covariant functor  $F_\beta^+: \mathcal{L}(\Gamma) \rightarrow \mathcal{L}(\sigma_\beta \Gamma)$ , as follows. We first define an object  $F_\beta^+(V, f) = (W, g)$  in  $\mathcal{L}(\sigma_\beta \Gamma)$ , for each object  $(V, f)$  in  $\mathcal{L}(\Gamma)$ , where

$$W_\gamma = V_\gamma, \quad \text{for each vertex } \gamma \neq \beta.$$

In order to define  $W_\beta$ , let  $e_1 = (\alpha_1, \beta), \dots, e_k = (\alpha_k, \beta)$  be the edges ending at  $\beta$ , and

set

$$W_\beta = \left\{ \sum_{i=1}^k v_i \in \bigoplus_{i=1}^k V_{\alpha_i} : \sum_{i=1}^k f_{e_i}(v_i) = 0 \right\}.$$

In other words,  $W_\beta = \ker h$ , where  $h: \bigoplus V_{\alpha_i} \rightarrow V_\beta$  in the map given by  $h = \bigoplus f_{e_i}$ . The maps  $\{g_e\}$  associated with  $W$  are defined by setting

$$g_e = f_e \quad \text{if } e \neq e_i \quad \text{for } 1 \leq i \leq k,$$

and

$$g_{e_i} = \pi_i \circ i_\beta, \quad \text{for } 1 \leq i \leq k, \quad \text{and } e_i = (\alpha_i, \beta),$$

where  $i_\beta: W_\beta \rightarrow \bigoplus_{i=1}^k V_{\alpha_i}$  is the natural embedding, and  $\pi_i: \bigoplus V_{\alpha_i} \rightarrow V_{\alpha_i}$  is the projection on the  $i$ -th summand.

To complete the definition of the functor  $F_\beta^+$ , we also have to define a morphism

$$F_\beta^+ \varphi: F_\beta^+(V, f) \rightarrow F_\beta^+(V', f') \quad \text{in } \mathcal{L}(\sigma_\beta \Gamma)$$

for each morphism  $\varphi: (V, f) \rightarrow (V', f')$  in  $\mathcal{L}(\Gamma)$ . For each vertex  $\gamma \neq \beta$ , we set

$$(F_\beta^+ \varphi)_\gamma = \varphi_\gamma.$$

Letting  $(W, g) = F_\beta^+(V, f)$  and  $(W', g') = F_\beta^+(V', f')$ , we define a map

$$(F_\beta^+ \varphi)_\beta: W_\beta \rightarrow W'_\beta$$

which takes  $\sum v_i \in W_\beta \subseteq \bigoplus_{i=1}^k V_{\alpha_i}$  to  $\sum \varphi_{\alpha_i} v_i \in W'_\beta \subseteq \bigoplus_{i=1}^k V'_{\alpha_i}$ .

In order to check that  $F_\beta^+ \varphi$  is indeed a morphism in the category  $\mathcal{L}(\sigma_\beta \Gamma)$ , it is enough to show that  $(F_\beta^+ \varphi)_\beta$  takes  $\ker h \rightarrow \ker h'$ , where  $h$  and  $h'$  are the maps defined in (77.4). Since  $\varphi$  is a morphism in  $\mathcal{L}(\Gamma)$ , we have

$$\varphi_\beta f_{e_i} = f'_{e_i} \varphi_{\alpha_i} \quad \text{for each edge } e_i = (\alpha_i, \beta) \quad \text{in } \Gamma.$$

Then, for each element  $\sum v_i \in \ker h$ , we have

$$h'(\sum \varphi_{\alpha_i} v_i) = (\sum f'_{e_i} \varphi_{\alpha_i} v_i = \sum \varphi_\beta f_{e_i} v_i = \varphi_\beta(h(\sum v_i)) = 0,$$

as required.

We next have:

**(77.5) Definition.** A vertex  $\alpha$  of  $\Gamma$  is called a *source* (or *-accessible vertex*) if all

edges having  $\alpha$  as a vertex start at  $\alpha$ . For each source  $\alpha$ , we shall define a covariant functor  $F_\alpha^-: \mathcal{L}(\Gamma) \rightarrow \mathcal{L}(\sigma_\alpha\Gamma)$ . Let  $(V, f)$  be an object in  $\mathcal{L}(\Gamma)$ . The corresponding object  $F_\alpha^-(V, f) = (W, g)$  in  $\mathcal{L}(\sigma_\alpha\Gamma)$  is obtained by setting

$$\begin{aligned} W_\gamma &= V_\gamma \quad \text{for all vertices } \gamma \neq \alpha, \quad \text{and} \\ g_e &= f_e \quad \text{for all edges } e \text{ not having } \alpha \text{ as a vertex.} \end{aligned}$$

Now let  $e_1 = (\alpha, \beta_1), \dots, e_m = (\alpha, \beta_m)$  be the edges having  $\alpha$  as a vertex, and set

$$W_\alpha = \left( \bigoplus_{i=1}^m V_{\beta_i} \right) / \text{im } \tilde{h},$$

where

$$\tilde{h}: V_\alpha \rightarrow \bigoplus_{i=1}^m V_{\beta_i}$$

is the map defined by

$$v \rightarrow \tilde{h}(v) = \sum f_{e_i}(v) \in \bigoplus_{i=1}^m V_{\beta_i}$$

The maps  $g_{e_i}: W_{\beta_i} \rightarrow W_\alpha$ ,  $1 \leq i \leq m$ , are defined by

$$g_{e_i} = v \circ j_{\beta_i},$$

where  $j_{\beta_i}: W_{\beta_i} \rightarrow \bigoplus_{j=1}^m W_{\beta_j}$  is the natural embedding, and  $v: \bigoplus_{j=1}^m W_{\beta_j} \rightarrow (\bigoplus_{j=1}^m W_{\beta_j})/\text{im } \tilde{h}$  is the quotient map with kernel  $\text{im } \tilde{h}$ .

The morphism  $F_\alpha^- \psi: (W, g) \rightarrow (W', g')$  in  $\mathcal{L}(\sigma_\alpha\Gamma)$ , where  $(W, g) = F_\alpha^-(V, f)$ ,  $(W', g') = F_\alpha^-(V', f')$ , and  $\psi: (V, f) \rightarrow (V', f')$  is a morphism in  $\mathcal{L}(\Gamma)$ , is defined as follows. We set

$$(F_\alpha^- \psi)_\gamma = \psi_\gamma \quad \text{for all vertices } \gamma \neq \alpha,$$

and define  $(F_\alpha^- \psi)_\alpha: W_\alpha \rightarrow W'_\alpha$  to be the map

$$v \left( \sum_{i=1}^m v_i \right) \rightarrow v' \left( \sum \psi_{\beta_i} v_i \right),$$

where  $v$  and  $v'$  are quotient maps as above, and  $\sum v_i \in V_{\beta_i}$ .

We leave it to the reader to check that  $F_\alpha^-$  is a covariant functor from  $\mathcal{L}(\Gamma) \rightarrow \mathcal{L}(\sigma\Gamma)$ .

The functors  $\{F_\beta^+\}$  and  $\{F_\alpha^-\}$  defined in (77.4) and (77.5) are called *Coxeter functors*. We shall see that they operate on the dimension vectors  $\dim(V, f)$  of

objects in  $\mathcal{L}(\Gamma)$  in a manner similar to the action of reflections in a g.g.r. (see §64). (In the following discussion,  $\dim$  always means  $\dim_K$ .)

**(77.6) Theorem.** *Let  $(V, f)$  be an indecomposable object in  $\mathcal{L}(\Gamma)$ , for a finite connected oriented graph  $\Gamma$ . Then the following statements hold.*

(i) *Let  $\beta$  be a sink. Then either  $(V, f)$  is isomorphic to the simple object  $L_\beta$ , or we have:*

$F_\beta^+(V, f)$  *is an indecomposable object in  $\mathcal{L}(\sigma_\beta\Gamma)$ ,*

$$F_\beta^- F_\beta^+(V, f) \cong (V, f),$$

*and*

$$\dim(F_\beta^+ V)_\gamma = \dim V_\gamma \quad \text{for all vertices } \gamma \neq \beta$$

$$\dim(F_\beta^+ V)_\beta = -\dim V_\beta + \sum_{i=1}^k \dim V_{\alpha_i}$$

*where  $\{(\alpha_1, \beta), \dots, (\alpha_k, \beta)\}$  are the edges in  $\Gamma$  having  $\beta$  as a vertex.*

(ii) *Let  $\alpha$  be a source. Then either  $(V, f) \cong L_\alpha$ , or we have:*

$F_\alpha^-(V, f)$  *is an indecomposable object in  $\mathcal{L}(\sigma_\alpha\Gamma)$ ,*

$$F_\alpha^+ F_\alpha^-(V, f) \cong (V, f)$$

*and*

$$\dim(F_\alpha^- V)_\gamma = \dim V_\gamma \quad \text{for all vertices } \gamma \neq \alpha$$

$$\dim(F_\alpha^- V)_\alpha = -\dim V_\alpha + \sum_{i=1}^m \dim V_{\beta_i},$$

*where  $\{(\alpha, \beta_i), 1 \leq i \leq m\}$  are the edges having  $\alpha$  as a vertex.*

The rest of the subsection is devoted to a proof of this theorem and a corollary. First let  $\beta$  be a sink. We shall construct a morphism.

$$\lambda_V^\beta : F_\beta^- F_\beta^+(V, f) \rightarrow (V, f),$$

for each object  $(V, f)$  in  $\mathcal{L}(\Gamma)$ . We set

$$(\lambda_V^\beta)_\gamma = \text{id}_{V_\gamma} \quad \text{for all vertices } \gamma \neq \beta,$$

noting that  $F_\beta^- F_\beta^+(V, f)_\gamma = V_\gamma$  if  $\gamma \neq \beta$ . The map

$$(\lambda_V^\beta)_\beta : F_\beta^- F_\beta^+(V, f)_\beta \rightarrow V_\beta$$

is defined as follows. From (77.4), we have

$$F_\beta^+(V, f)_\beta = \ker h, \quad \text{where } h = \bigoplus f_{e_i},$$

and  $\{e_i = (\alpha_i, \beta) : 1 \leq i \leq k\}$  are the edges having  $\beta$  as a vertex. The maps  $g_{e_i} : (F_\beta^+ V)_\beta \rightarrow (F_\beta^+ V)_{\alpha_i} = V_{\alpha_i}$ , associated with the object  $F_\beta^+(V, f)$  are given by  $g_{e_i} = \pi_i \circ i_\beta$  where  $i_\beta : (F_\beta^+ V)_\beta \rightarrow \bigoplus V_{\alpha_i}$  is the natural embedding, and  $\pi_i$  the projection upon  $V_{\alpha_i}$ . From (77.5), we have

$$F_\beta^- F_\beta^+(V, f)_\beta = (\bigoplus V_{\alpha_i}) / \text{im } \tilde{h}$$

where  $\tilde{h} = \bigoplus g_{e_i} = \bigoplus \pi_i \circ i_\beta$ , by the preceding remarks. We clearly have

$$\text{im } \tilde{h} = \ker h \quad \text{in } \bigoplus_{i=1}^k V_{\alpha_i},$$

and it follows that there exists an injective  $K$ -linear map

$$(\lambda_V^\beta)_\beta : (F_\beta^- F_\beta^+ V)_\beta = (\bigoplus V_{\alpha_i}) / \text{im } \tilde{h} = (\bigoplus V_{\alpha_i}) / \ker h \rightarrow V_\beta.$$

It is easily verified that the family of maps  $\{(\lambda_V^\beta)_\beta\}$  is a morphism in the category  $\mathcal{L}(\Gamma)$ .

Now let  $\alpha$  be a source. In this case, we shall construct a morphism

$$\mu_V^\alpha : (V, f) \rightarrow F_\alpha^+ F_\alpha^-(V, f),$$

for each object  $(V, f)$  in  $\mathcal{L}(\Gamma)$ . As in the previous case, the maps  $\{(\mu_V^\alpha)_\gamma : \gamma \neq \alpha\}$  are all taken as identity maps. At  $\alpha$ , we have

$$(F_\alpha^-(V, f))_\alpha = (\bigoplus V_{\beta_i}) / \text{im } \tilde{h} = \bigoplus (V_{\beta_i} / f_{e_i} V),$$

where  $\{e_i = (\alpha, \beta_i)\}$  are the edges containing  $\alpha$  as a vertex, and  $\tilde{h} = \bigoplus f_{e_i}$ , as in (77.5). We then obtain, from (77.4), the identification

$$F_\alpha^+ F_\alpha^-(V, f)_\alpha = \ker h,$$

where  $h = \bigoplus g_{e_i}$  in the category  $\mathcal{L}(\sigma_\alpha \Gamma)$ , and the maps  $\{g_{e_i}\}$  are given by

$$g_{e_i} : V_{\beta_i} \rightarrow \bigoplus V_{\beta_j} \rightarrow V_{\beta_i} / f_{e_i}(V_\alpha).$$

It follows that  $\ker h \cong \bigoplus f_{e_i}(V_\alpha)$ , and hence there exists a surjective  $K$ -linear map

$$(\mu_V^\alpha)_\alpha : V_\alpha \rightarrow F_\alpha^+ F_\alpha^-(V, f)_\alpha.$$

As in the previous case, we leave it to the reader to check that the family of maps  $\{(\mu_V^\alpha)_\gamma\}$  defines a morphism  $\mu_V^\alpha$  in  $\mathcal{L}(\Gamma)$ .

The next lemma summarizes the properties of the morphisms  $\{\lambda_V^\beta\}$  and  $\{\mu_V^\alpha\}$ .

**(77.7) Lemma.** *Let  $\beta$  be a sink, and  $\alpha$  a source in the graph  $\Gamma$ . Then the following statements hold.*

- (i) *The functors  $F_\beta^+$  and  $F_\alpha^-$  preserve direct sums.*
- (ii) *The morphisms*

$$\lambda_V^\beta: F_\beta^- F_\beta^+(V, f) \rightarrow (V, f) \quad \text{and} \quad \mu_V^\alpha: (V, f) \rightarrow F_\alpha^+ F_\alpha^-(V, f)$$

*are injective and surjective, respectively, for all objects  $(V, f)$  in  $\mathcal{L}(\Gamma)$ .*

(iii) *For each object  $(V, f)$  in  $\mathcal{L}(\Gamma)$ , there exists a quotient object  $(V, f)/\text{im } \lambda_V^\beta$  in  $\mathcal{L}(\Gamma)$  such that  $((V, f)/\text{im } \lambda_V^\beta)_\gamma = 0$  for all vertices  $\gamma \neq \beta$ . Similarly, there exists an object  $\ker \mu_V^\alpha$  in  $\mathcal{L}(\Gamma)$  such that  $(\ker \mu_V^\alpha)_\gamma = 0$  for all vertices  $\gamma \neq \alpha$ .*

(iv) *Let  $(V, f) = F_\beta^-(W, g)$ , for some object  $(W, g)$  in  $\mathcal{L}(\sigma_\beta \Gamma)$ . Then  $\lambda_V^\beta: F_\beta^- F_\beta^+(V, f) \rightarrow (V, f)$  is an isomorphism. On the other hand, if  $(V, f) = F_\alpha^+(W, g)$  for some object  $(W, g)$  in  $\mathcal{L}(\sigma_\alpha \Gamma)$ , then  $\mu_V^\alpha: (V, f) \rightarrow F_\alpha^+ F_\alpha^-(V, f)$  is an isomorphism.*

- (v) *For each object  $(V, f)$  in  $\mathcal{L}(\Gamma)$ , there exist direct sum decompositions*

$$(V, f) \cong F_\beta^- F_\beta^+(V, f) \oplus ((V, f)/\text{im } \lambda_V^\beta)$$

*and*

$$(V, f) \cong \ker \mu_V^\alpha \oplus F_\alpha^+ F_\alpha^-(V, f).$$

The proof is straightforward, in view of the preceding discussion, and is left to the reader.

Now we can complete the proof of Theorem 77.6. Let  $(V, f)$  be an indecomposable object in  $\mathcal{L}(\Gamma)$ . If  $(V, f)$  is the simple object  $L_\beta$ , for a sink  $\beta$  in  $\Gamma$ , then we obtain  $F_\beta^+(V, f) = 0$ , by the definition of the functor  $F_\beta^+$ , while if  $(V, f) = L_\alpha$ , at a source  $\alpha$ , we have  $F_\alpha^-(V, f) = 0$ , again by the definition of  $F_\alpha^-$ .

Let us assume next that  $\beta$  is a sink, and  $(V, f)$  is indecomposable, but not the simple object  $L_\beta$ . Then  $F_\beta^+(V, f) \neq 0$ , and we shall prove it is indecomposable and calculate its dimension. First assume that

$$F_\beta^+(V, f) = (W_1, g_1) \oplus (W_2, g_2)$$

in  $\mathcal{L}(\sigma_\beta \Gamma)$ . Then we obtain

$$(V, f) \cong F_\beta^- F_\beta^+(V, f) = F_\beta^- (W_1, g_1) \oplus F_\beta^- (W_2, g_2)$$

by (77.7v) and (77.7i), so one of the objects  $F_\beta^-(W_i, g_i)$ ,  $i = 1, 2$ , is 0. Suppose  $F_\beta^-(W_1, g_1) = 0$ . By (77.7iv),

$$\mu_V^\beta: F_\beta^+(V, f) \rightarrow F_\beta^+ F_\beta^-(F_\beta^+(V, f))$$

is an isomorphism, and it follows that  $(W_1, g_1) = 0$ , since  $F_\beta^+ F_\beta^- (W_1, g_1) = 0$ . Thus  $F_\beta^+(V, f)$  is indecomposable, and we shall calculate its dimension. We have

$$\dim F_\beta^+(V, f)_\gamma = \dim V_\gamma \quad \text{for all vertices } \gamma \neq \beta.$$

Moreover, using (77.7v),  $\lambda_V^\beta$  defines an isomorphism

$$(V, f) \cong F_\beta^- F_\beta^+(V, f),$$

and hence

$$\dim V_\beta = \dim (\bigoplus V_{\alpha_i}) / \ker h = \sum \dim V_{\alpha_i} - \dim F_\beta^+(V, f)_\beta,$$

which is the required formula for  $\dim F_\beta^+(V, f)_\beta$ . This completes the proof of part (i) of the theorem. The proof of part (ii) is similar, using properties of the morphism  $\{\mu_V^\alpha\}$ , and is left to the reader.

Iteration of Coxeter functors can be defined, relative to certain sequences of vertices, and provides a useful method for constructing indecomposable objects in  $\mathcal{L}(\Gamma)$ . More precisely, a sequence  $\{\beta_1, \dots, \beta_m\}$  of vertices in  $\Gamma$  (possibly with repetitions) is called a  $+$ -sequence if  $\beta_1$  is a sink in  $\Gamma$ ,  $\beta_2$  is a sink in  $\sigma_{\beta_1}\Gamma$ , etc. We have:

**(77.8) Corollary.** *Let  $\Gamma$  be a finite, connected, oriented graph, and let  $\{\beta_1, \dots, \beta_m\}$  be a  $+$ -sequence of vertices in  $\Gamma$ . Then the following statements hold.*

(i) *For each  $i$ ,  $1 \leq i \leq m$ , let  $L_{\beta_i}$  denote the simple object in the category  $\mathcal{L}(\sigma_{\beta_{i-1}} \cdots \sigma_{\beta_1}\Gamma)$ , associated with the vertex  $\beta_i$ . Then  $F_{\beta_1}^- \cdots F_{\beta_{i-1}}^- L_{\beta_i}$  is either 0 or an indecomposable object in  $\mathcal{L}(\Gamma)$ .*

(ii) *Let  $(V, f)$  be an indecomposable object in  $\mathcal{L}(\Gamma)$ , and assume that  $F_{\beta_m}^+ \cdots F_{\beta_1}^+(V, f) = 0$ . Then we have*

$$(V, f) \cong F_{\beta_1}^- \cdots F_{\beta_{i-1}}^- L_{\beta_i},$$

for some  $i$ ,  $1 \leq i \leq m$ .

The first statement follows directly from Theorem 77.6. The hypothesis of part (ii) implies that for some  $i$ ,  $1 \leq i \leq m$ , we have

$$F_{\beta_{i-1}}^+ \cdots F_{\beta_1}^+(V, f) \cong L_{\beta_i}$$

Then  $F_{\beta_i}^+ F_{\beta_{i-1}}^+ \cdots F_{\beta_1}^+(V, f) = 0$ , and it follows that  $F_{\beta_1}^+(V, f), \dots, F_{\beta_{i-1}}^+ \cdots F_{\beta_1}^+(V, f)$  are all indecomposable objects, by (77.6). Then, by (77.6), we obtain

$$F_{\beta_{i-1}}^- L_{\beta_i} \cong F_{\beta_{i-1}}^- F_{\beta_{i-1}}^+ \cdots F_{\beta_1}^+(V, f) \cong F_{\beta_{i-2}}^+ \cdots F_{\beta_1}^+(V, f).$$

This argument can be repeated, and the result follows.

### §77B. Representation Categories of Finite Type (Gabriel's Theorem)

Let  $\Gamma$  be a finite, oriented, connected graph. The category  $\mathcal{L}(\Gamma)$  is said to be of *finite type* if there exist at most a finite number of isomorphism classes of indecomposable objects. In this subsection, we shall prove Gabriel's Theorem [72], which determines the graphs  $\Gamma$  for which  $\mathcal{L}(\Gamma)$  is offinite type, and describes a basic set of indecomposable objects in this situation. The proof we shall give is due to Bernstein-Gelfand-Ponomarev [73], and is based on the theory of Coxeter functors and root systems.

We may assume at the outset that  $\Gamma$  is without loops, since otherwise  $\mathcal{L}(\Gamma)$  is not of finite type. We shall denote by  $E_\Gamma$  the vector space over  $\mathbb{R}$  consisting of all vectors  $\{x = (x_\alpha)\}$ , with  $x_\alpha \in \mathbb{R}\}$ , whose components are indexed by the set of vertices  $\{\alpha\}$  of  $\Gamma$ . A vector  $x \in E_\Gamma$  is called *positive* if  $x \neq 0$  and  $x_\alpha \geq 0$  for all vertices  $\alpha$ , while  $x \in E_\Gamma$  is called *integral* if  $x_\alpha \in \mathbb{Z}$  for all  $\alpha$ . The vector space  $E_\Gamma$  has an  $\mathbb{R}$ -basis consisting of the vectors  $\{\tilde{\alpha}\}$ , where for each vertex  $\alpha$ ,  $\tilde{\alpha}$  is the vector such that  $\tilde{\alpha}_\alpha = 1$  and  $\tilde{\alpha}_\gamma = 0$  is  $\gamma \neq \alpha$ .

The proof of Gabriel's Theorem is based on a study of a certain quadratic form  $Q$  on the vector space  $E_\Gamma$ , defined by the formula

$$(77.9) \quad Q(x) = \sum_{\alpha} x_{\alpha}^2 - \sum_{(\alpha, \beta)} x_{\alpha} x_{\beta}, \quad \text{for } x = (x_{\alpha}) \in E_\Gamma,$$

where the first sum is taken over the set of vertices  $\{\alpha\}$ , and the second is taken over the set of oriented edges  $\{(\alpha, \beta)\}$ . The quadratic form  $Q$  is associated with a symmetric bilinear form  $B$  on  $E_\Gamma$ , given by

$$B(x, y) = \frac{1}{2}(Q(x + y) - Q(x) - Q(y)), \quad \text{for } x, y \in E_\Gamma.$$

In this case, we have

$$B(x, y) = \frac{1}{2} \left( \sum_{\alpha} 2x_{\alpha}y_{\alpha} - \sum_{(\alpha, \beta)} x_{\alpha}y_{\beta} - \sum_{(\beta, \alpha)} y_{\alpha}x_{\beta} \right),$$

for  $x, y \in E_\Gamma$ . For each vertex  $\beta$  of  $\Gamma$ , we define a linear endomorphism  $S_{\beta}$  of  $E_\Gamma$ , where, for  $x \in E_\Gamma$ ,

$$(S_{\beta}x)_{\gamma} = x_{\gamma} \quad \text{if } \gamma \neq \beta$$

and

$$(S_{\beta}x)_{\beta} = -x_{\beta} + \sum_{\gamma} x_{\gamma},$$

where the sum is taken over the set of vertices of  $\Gamma$  that are joined to  $\beta$  by an edge. (Since we have assumed that  $\Gamma$  is a graph without loops, the vertices joined to  $\beta$  may start or end at  $\beta$ , but not both.)

The next result summarizes some of the basic properties of  $Q$  and  $B$ , and the maps  $S_{\beta}$ .

**(77.10) Lemma.** (i)  $Q(\tilde{\alpha}) = 1$ , for each vertex  $\alpha$  of  $\Gamma$ .

(ii) Let  $\alpha, \beta$  be distinct vertices. Then  $-2B(\tilde{\alpha}, \tilde{\beta})$  is the cardinal number of the set of all undirected edges joining  $\alpha$  and  $\beta$ .

(iii) For each vertex  $\beta$ , we have  $S_{\beta}^2 = 1$ , and  $S_{\beta}(x) = x - 2B(\tilde{\beta}, x)\tilde{\beta}$ , for all  $x \in E_{\Gamma}$ .

(iv) Each linear map  $S_{\beta}$  leaves the bilinear form  $B$  invariant:

$$B(S_{\beta}x, S_{\beta}y) = B(x, y) \quad \text{for all } x, y \in E_{\Gamma}.$$

(v) Each map  $S_{\beta}$  maps the set of integral vectors in  $E_{\Gamma}$  onto itself.

The proof is straightforward from the definitions, and is left as an exercise.

By (77.10i), each basis vector  $\tilde{\beta}$  is nonisotropic with respect to the bilinear form  $B$ , and we have  $E_{\Gamma} = \langle \tilde{\beta} \rangle \oplus \langle \tilde{\beta} \rangle^{\perp}$ . By (77.10), the linear maps  $\{S_{\beta}\}$  belong to the orthogonal group  $O(E_{\Gamma})$  defined by the bilinear form  $B$ , and each linear map  $S_{\beta}$  is a reflection that fixes the hyperplane  $\langle \tilde{\beta} \rangle^{\perp}$ . We shall denote the group generated by the reflections  $\{S_{\beta}\}$  by  $W$ . In contrast to §64A, however, the bilinear form  $B$  is not necessarily positive definite, and the group  $W$  may be infinite.

**(77.11) Proposition.** If the quadratic form  $Q$  is positive definite, then  $W$  is a finite group.

*Proof.* If  $Q$  is positive definite, the orthogonal group  $O(E_{\Gamma})$  is compact. Moreover,  $W$  is a closed subgroup of  $O(E_{\Gamma})$ , and hence  $W$  is compact. On the other hand,  $W$  preserves the lattice of integral vectors in  $E_{\Gamma}$  by (77.10v), and consequently is a discrete subgroup of  $O(E_{\Gamma})$ . It follows that  $W$  is a compact and discrete subgroup of  $O(E_{\Gamma})$ , and hence is finite, as required.

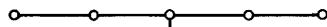
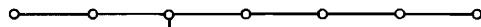
**(77.12) Proposition.** Assume that the quadratic form  $Q$  is positive definite. Let  $\Delta$  be the subset of  $E_{\Gamma}$  consisting of all vectors of the form  $x = w\tilde{\alpha}$ , where  $w \in W$  and  $\alpha$  is a vertex of  $\Gamma$ . Then  $\Delta$  is a root system in  $E_{\Gamma}$  satisfying the crystallographic condition, and  $W$  is the Weyl group associated with  $\Delta$ .

The proof follows easily from (77.10), (77.11), and §64A, and is left to the reader.

We now introduce the following types of unoriented graphs:

$$A_n : \circ - \circ - \circ - \cdots - \circ - \circ \quad n \text{ vertices}, \quad n \geq 1$$

$$D_n : \circ - \circ - \circ - \cdots - \circ - \circ \quad n \text{ vertices}, \quad n \geq 4$$

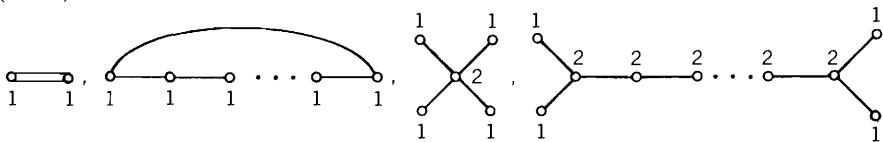
$E_6:$  $E_7:$  $E_8:$ 

In the rest of this subsection, it will be convenient to use the notation  $|\Gamma|$  for the unoriented graph associated with  $\Gamma$ .

**(77.14) Proposition.** *Let  $Q$  be the quadratic form (77.9). Then  $Q$  is positive definite if and only if  $|\Gamma|$  is of type  $A_n$  ( $n \geq 1$ ),  $D_n$  ( $n \geq 4$ ), or  $E_n$  ( $n = 6, 7, 8$ ).*

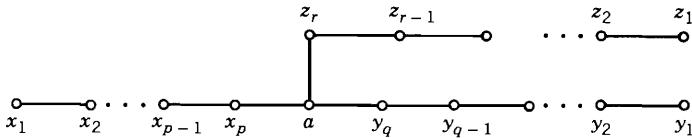
*Proof.* Step 1. If  $|\Gamma|$  contains a subgraph of the form

(77.15)



then  $Q$  is not positive definite. This is shown by taking a vector  $x$  with components indicated at the vertices in (77.15), zeros at all other vertices, and checking that  $Q(x) \leq 0$ . Thus if  $Q$  is positive definite,  $|\Gamma|$  has the form

(77.16)



where  $p, q, r$  are nonnegative integers.

Step 2. For each nonnegative integer  $p$ , let  $C_p(x_1, \dots, x_{p+1})$  be the quadratic form given by

$$\begin{aligned} C_p(x_1, \dots, x_{p+1}) &= x_1^2 + \dots + x_p^2 + \frac{1}{2}p(p+1)^{-1}x_{p+1}^2 \\ &\quad - x_1x_2 - x_2x_3 - \dots - x_px_{p+1} \end{aligned}$$

Then  $C_p$  is nonnegative definite. Moreover, if  $x \neq 0$  and  $C_p(x) = 0$ , then all components of  $x$  are different from zero. These assertions are proved by rewriting

$C_p(x)$  in the form

$$C_p(x) = \sum_{i=1}^p \frac{i}{2(i+1)} \left( x_{i+1} - \frac{i+1}{i} x_i \right)^2$$

*Step 3.* Define a vector  $x \in E_\Gamma$  by placing  $x_1, \dots, x_p, y_1, \dots, y_q, z_1, \dots, z_r, a$  at the vertices of  $|\Gamma|$  as in (77.16). Then we obtain

$$Q(x) = C_p(x_1, \dots, x_p, a) + C_q(y_1, \dots, y_q, a) + C_r(z_1, \dots, z_r, a) + Ca^2.$$

It follows that  $Q$  is positive definite if and only if

$$C = 1 - \frac{p}{2(p+1)} - \frac{q}{2(q+1)} - \frac{r}{2(r+1)} > 0,$$

that is,

$$A = \frac{1}{p+1} + \frac{1}{q+1} + \frac{1}{r+1} > 1.$$

*Step 4.* Let  $p \leq q \leq r$ . We examine the possible cases, using Step 3.

- (i)  $p = 0$ ,  $q$  and  $r$  are arbitrary. Then  $A > 1$ , so  $Q$  is positive definite, and  $|\Gamma|$  is of type  $A_n$  ( $n \geq 1$ ).
- (ii)  $p = 1$ ,  $q = 1$ ,  $r$  arbitrary. Then  $A > 1$  and  $|\Gamma|$  is of type  $D_n$  ( $n \geq 4$ ).
- (iii)  $p = 1$ ,  $q = 2$ ,  $r = 2, 3, 4$ . Then  $A > 1$ , and  $|\Gamma|$  is of type  $E_6, E_7$  or  $E_8$ .
- (iv)  $p = 1, q = 2, r \geq 5$ , or  $p = 1, q = 3, r \geq 3$ , or  $p \geq 2, q \geq 2$ , and  $r \geq 2$ . In all these cases  $A \leq 1$ , and the form is not positive definite.

Thus  $Q$  is positive definite for graphs  $\Gamma$  such that  $|\Gamma|$  is of type  $A_n, D_n, E_6, E_7, E_8$ , and only for these, completing the proof.

**(77.17) Definition.** Let  $\{\alpha_1, \dots, \alpha_n\}$  be an ordering of the vertices of  $\Gamma$ . The element  $c \in W$  defined by

$$c = S_{\alpha_1} S_{\alpha_2} \cdots S_{\alpha_n}$$

is called a *Coxeter element* (with respect to the given ordering of the vertices.)

**(77.18) Proposition.** Assume that the quadratic form  $Q$  is positive definite, and let  $c$  be an arbitrary Coxeter element in  $W$ . Then the following statements hold:

- (i) No eigenvalue of  $c$  is equal to 1.
- (ii) Let  $x \in E_\Gamma, x \neq 0$ . Then there exists a positive integer  $i$  (depending on  $x$ ) such that  $c^i x$  is not positive.

*Proof.* (i) Let  $c = S_{\alpha_1} \cdots S_{\alpha_n}$ , and assume that  $cy = y$  for some vector  $y \in E_\Gamma$ . We shall prove that  $y = 0$ . We first observe that, for all vectors  $z \in E_\Gamma$ , we have

$$(S_{\alpha_2} S_{\alpha_3} \cdots S_{\alpha_n} z)_{\alpha_1} = z_{\alpha_1},$$

by (77.10iii). Apply this remark to the equation  $cy = y$ , and obtain

$$(S_{\alpha_1} y)_{\alpha_1} = y_{\alpha_1} = (cy)_{\alpha_1}$$

using the facts that  $S_{\alpha_1}^2 = 1$  and  $cy = y$ . It follows that  $S_{\alpha_1} y = y$ , by (77.10iii). The argument can be repeated, and yields the result that

$$S_{\alpha_1} y = S_{\alpha_2} y = \cdots = S_{\alpha_n} y = y.$$

Then  $B(y, \tilde{\alpha}_1) = B(y, \tilde{\alpha}_2) = \cdots = B(y, \tilde{\alpha}_n) = 0$  by (77.10iii) again. Since  $\{\tilde{\alpha}_1, \dots, \tilde{\alpha}_n\}$  is a basis of  $E_\Gamma$ , and  $Q$  is positive definite, we obtain  $y = 0$ , completing the proof of part (i).

(ii) The group  $W$  is finite, by (77.11). Then  $c^h = 1$  for some positive integer  $h$ . If  $\{x, cx, \dots, c^{h-1}x\}$  are all positive, then

$$x + cx + \cdots + c^{h-1}x$$

is positive, and fixed by  $c$ . This contradicts part (i), and completes the proof.

We can now state the main result of the section.

**(77.19) Theorem (Gabriel [72]).** *Let  $\Gamma$  be a finite, oriented, connected graph. Then the following statements hold.*

(i) *If the category  $\mathcal{L}(\Gamma)$  is of finite type, then the quadratic form  $Q$ , given by (77.9), is positive definite, and  $|\Gamma|$  is a graph of type  $A_n$  ( $n \geq 1$ ),  $D_n$  ( $n \geq 4$ ), or  $E_n$  ( $n = 6, 7, 8$ ).*

(ii) *Let  $|\Gamma|$  be a graph of type  $A_n$  ( $n \geq 1$ ),  $D_n$  ( $n \geq 4$ ), or  $E_n$  ( $n = 6, 7, 8$ ). Then  $\mathcal{L}(\Gamma)$  is of finite type. Moreover, the map*

$$(V, f) \rightarrow \dim(V, f) = (\dim V_\alpha) \in E_\Gamma$$

*defines a bijection from the set of isomorphism classes of indecomposable objects  $\{(V, f)\}$  in  $\mathcal{L}(\Gamma)$ , to the set of positive roots in the root system  $\Delta$  (see (77.12)), for a suitable ordering of the roots.*

*Proof.* (i) (Tits) Consider the set of all objects  $(V, f)$  in  $\mathcal{L}(\Gamma)$  of a fixed dimension  $d = (d_\alpha)$ . Let  $\{V_\alpha\}$  be a fixed set of  $K$ -spaces, indexed by the vertices of  $\Gamma$ , such that  $\dim V_\alpha = d_\alpha$ , for each  $\alpha$ . An object of dimension  $d$  is determined uniquely

by a family of linear maps

$$f_e: V_\alpha \rightarrow V_\beta, \quad e = (\alpha, \beta),$$

and hence by an element

$$f = (f_e) \in \prod_{e=(\alpha, \beta)} \text{Hom}_K(V_\alpha, V_\beta),$$

where the product is taken over the set of edges in  $\Gamma$ . Let  $f = (f_e)$  and  $f' = (f'_e)$  represent two objects of dimension  $d$ . A morphism  $\varphi$  from the object represented by  $f$  to the one represented by  $f'$  is described by a set of  $K$ -linear maps  $\{\varphi_\alpha \in \text{End}_K V_\alpha\}$  such that the diagrams commute:

$$\begin{array}{ccc} V_\alpha & \xrightarrow{f_e} & V_\beta \\ \varphi_\alpha \downarrow & & \downarrow \varphi_\beta \quad \text{for each edge } e = (\alpha, \beta). \\ V_\alpha & \xrightarrow{f'_e} & V_\beta \end{array}$$

The objects corresponding to  $f$  and  $f'$  are isomorphic if and only if  $\varphi_\alpha \in GL(V_\alpha)$  for each  $\alpha$ , and

$$f'_e = \varphi_\beta f_e \varphi_\alpha^{-1} \quad \text{for each edge } e = (\alpha, \beta).$$

The group  $G = \prod_\alpha GL(V_\alpha)$  acts on the vector space  $\prod_{e=(\alpha, \beta)} \text{Hom}_K(V_\alpha, V_\beta)$  in a natural way. From the preceding remarks, it is clear that two elements  $f$  and  $f'$  belong to the same  $G$ -orbit if and only if the corresponding objects of  $\mathcal{L}(\Gamma)$  are isomorphic.

Now assume that  $\mathcal{L}(\Gamma)$  is of finite type. By the preceding discussion, this means that, in a given dimension  $d = (d_\alpha)$ , the number of  $G$ -orbits on  $\prod_{(\alpha, \beta)} \text{Hom}_K(V_\alpha, V_\beta)$  is finite, where  $G = \prod_\alpha GL(V_\alpha)$ . Since  $G$  is a connected affine algebraic group over an algebraically closed field, the finiteness of the number of orbits means that there exists an open dense orbit. The dimension of this orbit is equal to

$$\delta(d) = \sum_{e=(\alpha, \beta)} \dim_K \text{Hom}_K(V_\alpha, V_\beta) = \sum_{e=(\alpha, \beta)} d_\alpha d_\beta,$$

and satisfies the inequality

$$\delta(d) \leq \dim G - 1,$$

since  $G$  contains a one-dimensional subgroup that acts trivially on  $\prod_{(\alpha, \beta)} \text{Hom}_K(V_\alpha, V_\beta)$ . (For proofs of these facts, see any book on linear algebraic

groups.) Since  $\dim G = \sum_\alpha d_\alpha^2$ , it follows that

$$\sum_\alpha d_\alpha^2 - \sum_{(\alpha, \beta)} d_\alpha d_\beta \geq 1 > 0.$$

Therefore the quadratic form  $Q$ , defined in (77.9), is positive definite, because the preceding result shows that  $Q(d) > 0$  for each positive integral vector  $d = (d_\alpha)$ . Part (i) of the theorem now follows at once from (77.14).

(ii) Let  $\Gamma$  be a graph such that  $|\Gamma|$  is of type  $A_n$  ( $n \geq 1$ ),  $D_n$  ( $n \geq 4$ ), or  $E_n$  ( $n = 6, 7, 8$ ). Then the quadratic form  $Q$  defined in (77.9) is positive definite, by (77.14). This implies that the group  $W$  generated by the reflections  $\{S_\beta\}$  is finite, by (77.11). Moreover, by (77.12), the set  $\Delta$  consisting of the  $W$ -transforms  $\{w\tilde{\alpha}\}_{w \in W}$  of the basis elements  $\{\tilde{\alpha}\}$  is a root system in  $E_\Gamma$  satisfying the crystallographic condition. The basis elements  $\{\tilde{\alpha}\}$  of  $E_\Gamma$  clearly form a fundamental system of roots in  $\Delta$ , and  $\{S_\alpha\}$  is the corresponding set of fundamental reflections in  $W$  (see (64.9)). By (64.10), there exists a unique set of positive roots  $\Delta_+$  containing the fundamental system  $\{\tilde{\alpha}\}$ .

We next consider the effect of the reflections  $\{S_\alpha\}$  on the dimension vectors  $d = (d_\alpha) \in E_\Gamma$  associated with indecomposable objects  $(V, f)$  in  $\mathcal{L}(\Gamma)$  (see (77.6)).

**(77.20) Lemma.** *Let  $\beta$  be a sink in  $\Gamma$ , and let  $(V, f)$  be an indecomposable object in  $\mathcal{L}(\Gamma)$  of dimension  $d = (d_\alpha)$ . Then either  $(V, f) \cong L_\beta$ ,  $F_\beta^+(V, f) = 0$ , and  $S_\beta(d)$  is not a positive vector in  $E_\Gamma$ , or  $F_\beta^+(V, f)$  is indecomposable, and  $\dim F_\beta^+(V, f) = S_\beta d \in \Delta_+$ . A similar statement holds for a source vertex  $\alpha$ , and the functor  $F_\alpha^-$ .*

In the following corollary, we recall the concept of a  $+$ -sequence of vertices  $\{\beta_1, \beta_2, \dots, \beta_m\}$ , which is a sequence, possibly with repetitions, such that  $\beta_i$  is a sink in  $\sigma_{\beta_{i-1}} \cdots \sigma_{\beta_1} \Gamma$ , for each  $i > 1$  (see (77.8)).

**(77.21) Corollary.** *Let  $\{\beta_1, \dots, \beta_m\}$  be a  $+$ -sequence of vertices in  $\Gamma$ , and let  $(V, f)$  be an indecomposable object in  $\mathcal{L}(\Gamma)$ , of dimension  $d$ . Put*

$$(V_j, f_j) = F_{\beta_j}^+ \cdots F_{\beta_1}^+(V, f),$$

and

$$d_j = S_{\beta_j} \cdots S_{\beta_1} d, \quad \text{for } 1 \leq j \leq m.$$

Let  $i$  be the largest integer such that  $i \leq m$  and  $d_j \in \Delta_+$  for  $j \leq i$ . Then we have  $(V_i, f_i) \cong L_{\beta_{i+1}}$ ,  $(V_j, f_j) = 0$  for  $j > i$ , and for  $j \leq i$ ,  $(V_j, f_j)$  is indecomposable and

$$(V, f) \cong F_{\beta_1}^- \cdots F_{\beta_{j-1}}^-(V_j, f_j).$$

The proofs of the lemma and corollary are left as exercises.

We can now complete the proof of part (ii) of Gabriel's Theorem, which

establishes a bijection between isomorphism classes of indecomposable objects and positive roots in  $\Delta$ . Since  $|\Gamma|$  is a graph of type  $A_n$ ,  $D_n$ , or  $E_n$ , it is easily shown that the vertices  $\{\beta_1, \dots, \beta_n\}$  can be ordered so that for each edge  $e = (\alpha, \beta)$ ,  $\alpha$  has a greater index than  $\beta$ . We then extend the vertex set to the infinite periodic sequence of vertices  $\{\beta_1, \beta_2, \dots\}$ , by requiring that  $\beta_i = \beta_{i+n}$  for all positive integers  $i$ . Then  $\{\beta_1, \beta_2, \dots\}$  is clearly a  $+$ -sequence of vertices.

Let  $c = S_{\beta_n} \cdots S_{\beta_1}$  be the Coxeter element of  $W$ , relative to the ordering  $(\beta_n, \dots, \beta_1)$  (see (77.17)). Let  $(V, f)$  be an indecomposable object in  $\mathcal{L}(\Gamma)$ , of dimension  $d$ . By (77.18),  $c^j d$  is not positive in  $E_\Gamma$ , for some integer  $j > 0$ . By (77.21), there exists an integer  $i$ , depending only on the dimension  $d$ , such that

$$(V, f) \cong F_{\beta_1}^- \cdots F_{\beta_i}^- L_{\beta_{i+1}}.$$

and

$$d = S_{\beta_1} \cdots S_{\beta_i} \tilde{\beta}_{i+1}.$$

Moreover,  $d \in \Delta_+$ , and  $(V, f)$  is determined, up to isomorphism, by  $d = \dim(V, f)$ . It follows that the category  $\mathcal{L}(\Gamma)$  is of finite type.

It remains to prove that every positive root in  $\Delta_+$  corresponds to an indecomposable object. Let  $x \in \Delta_+$ ; then  $c^j x$  is not positive, for some integer  $j > 0$ . Let  $i$  be the greatest integer such that  $S_{\beta_j} \cdots S_{\beta_1} x \in \Delta_+$  for all  $j \leq i$ . Then we have  $S_{\beta_1} \cdots S_{\beta_i} x = \tilde{\beta}_{i+1}$ , by the Main Lemma 64.13. It follows that

$$(V, f) = F_{\beta_1}^- \cdots F_{\beta_i}^- L_{\beta_{i+1}}$$

is indecomposable, of dimension

$$S_{\beta_1} \cdots S_{\beta_i} \tilde{\beta}_{i+1} = x,$$

by (77.21). This completes the proof of Theorem 77.19.

## §78. AUSLANDER-REITEN SEQUENCES

This section is intended to serve as an introduction to the extensive theory of Auslander-Reiten sequences, with special emphasis on the case of group algebras. The results for this case will be sufficiently powerful to yield significant information about the Green ring of a group algebra (see §81D). A full treatment of Auslander-Reiten sequences over arbitrary rings is beyond the scope of this book.

The fundamental ideas leading to the theory of almost split sequences were first introduced by M. Auslander, and played a key role in his generalization of Roiter's proof of the first Brauer-Thrall conjecture (see §79). Later, Auslander and Reiten developed the theory of almost split sequences from a module-

theoretic viewpoint, rather than that of functor categories. These sequences are now called Auslander-Reiten sequences.

The authors wish to thank P. Landrock and P. Webb for many helpful comments on the material in this section.

In §78A, we review the theory of the Heller loop-space operator for modules over group algebras (see §62E), since this plays an important role in our treatment of Auslander-Reiten sequences. The existence of such sequences, for the group algebra case, is established in §78B. In §78C, we consider the general case of f.d. algebras over a field.

Throughout this section, let  $A$  be a ring. We assume once and for all that all  $A$ -modules considered below are f.g./ $A$ . Denote by  $\mathcal{P}(A)$  the category of f.g. projective  $A$ -modules, and  $\mathcal{I}(A)$  the category of f.g. injective  $A$ -modules. Let  $\text{Ind } A$  be the set of isomorphism classes of f.g. indecomposable  $A$ -modules. We also write  $M \in \text{Ind } A$  to indicate that  $M$  is an indecomposable module. Thus,

$$\text{Ind } A - \mathcal{P}(A) = \text{set of (isomorphism classes of) nonprojective indecomposable } A\text{-modules},$$

while  $\text{Ind } A \cap \mathcal{P}(A)$  is the set of projective indecomposable  $A$ -modules, and so on.

### §78A. Heller Loop-Space Operator

Throughout this subsection, let  $A = KG$ , where  $K$  is a field and  $G$  a finite group. Consider only f.g.  $A$ -modules in what follows. Each left  $A$ -module  $M$  determines a right  $A$ -module  $M'$ , called the  *$K$ -dual* of  $M$ , given by

$$M' = \text{Hom}_K(M, K).$$

The action of  $G$  on  $M'$  is defined by the formula

$$(fx)m = f(xm) \quad \text{for all } f \in M', \quad x \in G, \quad m \in M.$$

We may also form the *contragredient* module  $M^*$ , which is a *left*  $A$ -module whose underlying space is  $M'$ , and where  $G$  acts by the rule

$$(xf)m = f(x^{-1}m) \quad \text{for } f \in M^*, \quad x \in G, \quad m \in M.$$

We shall repeatedly use:

**(78.1) Proposition.** *Let  $P$  be a f.g. projective left  $A$ -module. Then so is its contragredient  $P^*$ , while its  $K$ -dual  $P'$  is a f.g. projective right  $A$ -module.*

*Proof.* The result for contragredients follows from the isomorphism

$$A^* \cong A \text{ as left } A\text{-modules}$$

(see (10.29)). That for duals follows from the isomorphism

$$({}_A A)^* \cong A_A \text{ as right } A\text{-modules,}$$

which holds since  $A$  is a symmetric  $K$ -algebra by (9.6).

**(78.2) Corollary.** *A f.g.  $A$ -module is projective if and only if it is injective.*

*Proof.* Taking contragredients reverses all arrows in a diagram.

Given an  $A$ -module  $M$ , we may write

$$\begin{aligned} M = N_1 \oplus \cdots \oplus N_r \oplus P_1 \oplus \cdots \oplus P_s, \quad N_i &\in \text{Ind } A - \mathcal{P}(A), \\ P_j &\in \text{Ind } A \cap \mathcal{P}(A). \end{aligned}$$

Then we have  $M = N \oplus P$ , with  $P \in \mathcal{P}(A)$ , and where  $N$  has no projective direct summand. We shall call  $N$  the *core* of  $M$ ; it is unique up to isomorphism, by the Krull-Schmidt-Azumaya Theorem. When  $M = N$  and  $P = 0$ , we call  $M$  a *core*. In particular, each  $M \in \text{Ind } A - \mathcal{P}(A)$  is a core.

For any left  $A$ -module  $M$ , there is an exact sequence

$$0 \rightarrow N \rightarrow P \rightarrow M \rightarrow 0 \text{ with } P \in \mathcal{P}(A).$$

Now define

$$\Omega(M) = \text{core of } N.$$

By Schanuel's Lemma, the isomorphism class of  $M$  uniquely determines that of  $\Omega(M)$ . The operator  $\Omega$ , defined on isomorphism classes of  $A$ -modules, is the *Heller loop-space operator*, introduced previously in §62E.

We leave it to the reader to verify the formulas

$$(78.3) \quad \Omega(M \oplus P) \cong \Omega(M), \quad \Omega(M \oplus N) \cong \Omega(M) \oplus \Omega(N)$$

for all  $A$ -modules  $M$  and  $N$ , and all  $P \in \mathcal{P}(A)$ . Next, we show:

**(78.4) Proposition.** *For  $A = KG$ , the loop-space operator  $\Omega$  gives a bijection from the set of isomorphism classes of cores onto itself, preserving indecomposability.*

*Proof.* For any  $A$ -module  $M$ , there is an exact sequence

$$0 \rightarrow \Omega(M) \oplus P_0 \rightarrow P_1 \rightarrow M \rightarrow 0 \text{ with } P_i \in \mathcal{P}(A).$$

Taking contragredients, we obtain a new exact sequence

$$0 \rightarrow M^* \rightarrow P_1^* \rightarrow \Omega(M)^* \oplus P_0^* \rightarrow 0,$$

and each  $P_i^* \in \mathcal{P}(A)$ . Therefore

$$\text{core of } M^* \cong \Omega((\Omega M)^*).$$

Suppose now that  $M$  is a core; then so is  $M^*$ , by (78.1), and we obtain

$$M^* \cong \Omega((\Omega M)^*)$$

in this case. Thus  $\Omega M$  determines  $M^*$  (and hence  $M$ ) up to isomorphism; further, every core  $N$  is of the form  $M^*$  for some  $M$ , and so  $N \in \text{im } \Omega$ . This completes the proof.

For any core  $N$ , we may write  $N \cong \Omega M$  for some core  $M$ , unique up to isomorphism; we denote this  $M$  by  $\Omega^{-1}N$ . For an arbitrary  $A$ -module  $X$ , define  $\Omega^{-1}X = \Omega^{-1}(\text{core of } X)$ . The following result will be used repeatedly:

**(78.5) Proposition.** (i) *For any core  $M$ , there is an exact sequence*

$$(78.6) \quad 0 \rightarrow \Omega M \rightarrow P_M \rightarrow M \rightarrow 0,$$

where  $P_M$  is a projective cover of  $M$ . In this sequence,  $P_M$  is also an injective hull of  $\Omega M$ .

(ii) *Dually, for each core  $N$  there is an exact sequence*

$$(78.7) \quad 0 \rightarrow N \rightarrow I_N \rightarrow \Omega^{-1}N \rightarrow 0,$$

where  $I_N$  is an injective hull of  $N$ ; then  $I_N$  is also a projective cover of  $\Omega^{-1}N$ .

(iii) *Given any exact sequence of  $A$ -modules*

$$0 \rightarrow X \rightarrow P \rightarrow Y \rightarrow 0 \quad \text{with } P \in \mathcal{P}(A),$$

we have

$$\text{core of } X \cong \Omega Y, \quad \text{core of } Y \cong \Omega^{-1}X.$$

*Proof.* (i) Let  $M$  be a core,  $P_M$  its projective cover, and let

$$0 \rightarrow X \rightarrow P_M \rightarrow M \rightarrow 0$$

be exact. To prove that  $X \cong \Omega M$ , it suffices to show that  $X$  is a core. However, any projective direct summand  $X$  is also injective, and can therefore be split off from  $P_M$ ; this would contradict the assumption that  $P_M$  is a projective cover of  $M$ . The dual of Schanuel's Lemma now shows that  $P_M$  is an injective hull of  $\Omega M$ . The proof of (ii) is similar, and is left to the reader. It is then easy to verify (iii), again left as exercise for the reader.

**(78.8) Example.** Let  $A = KG$ , where  $\text{char } K = p > 0$ , and  $p$  divides  $|G|$ . Given a nonsimple  $P \in \mathcal{P}(A) \cap \text{Ind } A$ , put  $S = \text{soc } P$ . By (18.1),  $P$  has a unique maximal submodule  $JP$ , where  $J = \text{rad } A$ . Further,  $S$  is simple, and

$$P/JP \cong S, \quad 0 \subset S \subseteq JP \subset P.$$

Since  $P$  has a unique maximal submodule, each factor module of  $P$  must be indecomposable. Likewise, since  $S$  is simple, every submodule of  $P$  is indecomposable. From the exact sequence

$$0 \rightarrow JP \rightarrow P \rightarrow S \rightarrow 0$$

we conclude that

$$JP = \Omega(S),$$

noting that  $JP \neq 0$  because of our hypothesis that  $P \neq S$ . Since the sequence

$$0 \rightarrow S \rightarrow P \rightarrow P/S \rightarrow 0$$

is also exact, we obtain

$$S = \Omega(P/S), \quad \text{and thus } JP = \Omega(S) = \Omega^2(P/S).$$

For later use, we observe that there is a fiber product of  $A$ -modules:

$$\begin{array}{ccc} JP & \xrightarrow{i} & P \\ j \downarrow & & j \downarrow \\ JP/S & \xrightarrow{i} & P/S, \end{array}$$

with each  $i$  an inclusion, each  $j$  a canonical surjection. This gives a nonsplit ses:

$$(78.9) \quad 0 \rightarrow JP \rightarrow P \oplus (JP/\text{soc } P) \rightarrow P/\text{soc } P \rightarrow 0.$$

We now digress slightly to the topic of projective homomorphisms, which generalizes the discussion of projective endomorphisms given in §29B (see also §62A). Given a commutative ring  $R$  and a finite group  $G$ , let  $\Lambda = RG$ . Let us recall some facts about extensions of  $\Lambda$ -modules (see the discussion in Volume I, pp. 175–176). We write  $\text{Ext}$  in place of  $\text{Ext}_{\Lambda}^1$ , for brevity.

Given a pair of left  $\Lambda$ -modules  $M$  and  $N$ , and any  $f \in \text{Hom}_{\Lambda}(N, M)$ , there is an induced map

$$f^* : \text{Ext}(M, X) \rightarrow \text{Ext}(N, X)$$

for each  $\Lambda$ -module  $X$ . To describe  $f^*$ , note that each  $\xi \in \text{Ext}(M, X)$  determines an extension  $Y$  of  $M$  by  $X$ , unique up to equivalence:

$$\xi: 0 \rightarrow X \rightarrow Y \rightarrow M \rightarrow 0.$$

Then  $f^*\xi = \xi f$ , where  $\xi f$  is the extension of  $N$  by  $X$  occurring in the commutative diagram

$$\begin{array}{ccccccc} \xi: & 0 & \longrightarrow & X & \longrightarrow & Y & \xrightarrow{\theta} M \longrightarrow 0 \\ & & \uparrow 1 & & \uparrow & & \uparrow f \\ \xi f: & 0 & \longrightarrow & X & \longrightarrow & Y_1 & \longrightarrow N \longrightarrow 0, \end{array}$$

in which  $Y_1$  is the pullback of the pair of maps  $(f, \theta)$ . We call  $f$  a *projective homomorphism* if  $f^*$  is the zero map for every  $X$ , that is, if  $\xi f$  is a split exact sequence for every ses  $\xi$  ending in  $M$ .

**(78.10) Lemma.** *A map  $f \in \text{Hom}_\Lambda(N, M)$  is a projective homomorphism if and only if  $f$  “factors through a projective,” that is, there exists a commutative diagram*

$$\begin{array}{ccc} N & \xrightarrow{f} & M \\ & \searrow & \nearrow \\ & P & \end{array}$$

with  $P \in \mathcal{P}(\Lambda)$ .

*Proof.* If  $f$  factors through a projective  $P$ , then  $f = f_2 f_1$  where  $f_1: N \rightarrow P$  and  $f_2: P \rightarrow M$ . For any  $\xi \in \text{Ext}(M, X)$ , we have  $\xi f = (\xi f_2) f_1 = 0$ , since  $\xi f_2 = 0$  because  $P$  is projective. Conversely, suppose  $f$  is a projective homomorphism, and choose  $\xi$  with middle term  $Y \in \mathcal{P}(\Lambda)$ . Since  $\xi f$  splits, we obtain a map  $N \rightarrow Y$  lifting  $f$ .

As in (29.15), there is a map

$$\text{Hom}_\Lambda(N, \Lambda) \otimes_\Lambda M \rightarrow \text{Hom}_\Lambda(N, M),$$

whose image is precisely the set of projective homomorphisms from  $N$  to  $M$ . We may then carry over the proof of (29.18) to the present more general situation, to obtain:

**(78.11) Proposition.** *Let  $M$  and  $N$  be left  $\Lambda$ -lattices. Then  $f \in \text{Hom}_\Lambda(N, M)$  is a projective homomorphism if and only if*

$$f = \sum_{x \in G} x h x^{-1} \quad \text{for some } h \in \text{Hom}_R(N, M).$$

Let us now return to the case where  $A = KG$ , with  $K$  a field. Given left  $A$ -modules  $M$  and  $N$ , let  $\text{Hom}_A(M, N)_{G/1}$  denote the subspace of  $\text{Hom}_A(M, N)$  consisting of all projective homomorphisms from  $M$  to  $N$ , that is, all those homomorphisms which factor through a projective. We define

$$(78.12) \quad \mathbf{Hom}_A(M, N) = \text{Hom}_A(M, N)/\text{Hom}_A(M, N)_{G/1}.$$

We leave it as an easy exercise to check that

$$(78.13) \quad \mathbf{Hom}_A(M \oplus P, N) \cong \mathbf{Hom}_A(M, N) \quad \text{for any } P \in \mathcal{P}(A).$$

It follows readily from the definition, or from (78.11), that  $\text{Hom}_A(M, M)_{G/1}$  is a two-sided ideal of the endomorphism ring  $\text{End}_A M$ . We set

$$(78.14) \quad \mathbf{End}_A M = (\text{End}_A M)/\text{Hom}_A(M, M)_{G/1},$$

a factor ring of  $\text{End}_A M$ . If  $M \in \mathcal{P}(A)$ , then of course  $\mathbf{End}_A M = 0$ . The converse also holds, since if the identity map  $\text{id}_M$  factors through a projective module  $P$ , then  $M|P$ , so  $M$  is projective.

Now let  $M$  and  $N$  be a pair of  $A$ -modules, and let  $\Omega$  be the Heller loop-space operator. In our discussion of Auslander-Reiten sequences in §78B, it will be vital to use the relation between  $\mathbf{Hom}_A(M, N)$  and extensions of  $N$  by  $\Omega^2 M$ , where of course  $\Omega^2 M = \Omega(\Omega M)$ . The following proof is based on the work of Auslander-Reiten [75].

**(78.15) Theorem.\*** *Let  $M$  and  $N$  be left  $A$ -modules, where  $A = KG$ . There is a natural  $K$ -isomorphism*

$$\text{Ext}_A^1(N, \Omega^2 M) \cong K\text{-dual of } \mathbf{Hom}_A(M, N).$$

*Proof.* Step 1. Neither side of the proposed isomorphism changes if we delete projective summands of  $M$  or  $N$ , so we may assume that both  $M$  and  $N$  are cores. We show first that

$$\text{Ext}_A^1(M, N) \cong \text{Ext}_A^1(\Omega M, \Omega N).$$

By (78.5), there are exact sequences

$$0 \rightarrow \Omega M \rightarrow P_M \rightarrow M \rightarrow 0, \quad 0 \rightarrow \Omega N \rightarrow P_N \rightarrow N \rightarrow 0.$$

Using (8.9) twice, we obtain

$$\text{Ext}_A^1(M, N) \cong \text{Ext}_A^2(M, \Omega N) \cong \text{Ext}_A^1(\Omega M, \Omega N),$$

\*See (78.34) for the generalization to f.d.  $K$ -algebras.

as desired. Thus we have

$$\mathrm{Ext}_A^1(N, \Omega^2 M) \cong \mathrm{Ext}_A^1(\Omega^{-1} N, \Omega M).$$

We claim next that

$$\mathrm{Ext}_A^1(\Omega^{-1} N, L) \cong \mathbf{Hom}(N, L)$$

for any  $A$ -module  $L$ , where **Hom** means  $\mathbf{Hom}_A$ . Using the exact sequence (78.7) and (8.9iii), we have

$$\mathrm{Ext}_A^1(\Omega^{-1} N, L) \cong \mathrm{Hom}(N, L)/\mathrm{im} \, \mathrm{Hom}(I_N, L).$$

Since every map from  $N$  to  $L$  that factors through an injective must factor through  $I_N$ , the right-hand side is precisely  $\mathbf{Hom}(N, L)$ , as desired. Therefore

$$\mathrm{Ext}_A^1(\Omega^{-1} N, \Omega M) \cong \mathbf{Hom}(N, \Omega M),$$

and it remains for us to establish

$$(78.16) \quad \mathbf{Hom}(N, \Omega M) \cong K\text{-dual of } \mathbf{Hom}(M, N).$$

*Step 2.* We shall now simplify the problem by reducing the verification of the above isomorphism to the special case in which  $N$  is the  $G$ -trivial module  $K$ . Given any  $A$ -modules  $X$  and  $Y$ , we show at once that there are natural isomorphisms

$$(78.17) \quad \mathrm{Hom}(X, Y) \cong \mathrm{Hom}(K, X^* \otimes Y) \cong \mathrm{Hom}(X \otimes Y^*, K),$$

where  $\otimes$  denotes inner tensor product (over  $K$ ) of  $A$ -modules. By (10.31), we have

$$\mathrm{Hom}(X, Y) \cong \mathrm{inv}_G(X^* \otimes Y) = \mathrm{inv}_G(K^* \otimes (X^* \otimes Y)) \cong \mathrm{Hom}(K, X^* \otimes Y),$$

which proves the first isomorphism. The second then follows from (10.32) and the identity  $(X \otimes Y^*)^* \cong X^* \otimes Y$ .

Using the characterization of projective homomorphisms given in (78.11), it follows from (78.17) that

$$\mathbf{Hom}(X, Y) \cong \mathbf{Hom}(K, X^* \otimes Y) \cong \mathbf{Hom}(X \otimes Y^*, K).$$

The isomorphism (78.16), which we wish to prove, now takes the form

$$\mathbf{Hom}(K, N^* \otimes \Omega M) \cong K\text{-dual of } \mathbf{Hom}(N^* \otimes M, K).$$

On the other hand, from the exact sequence

$$0 \rightarrow N^* \otimes \Omega M \rightarrow N^* \otimes P_M \rightarrow N^* \otimes M \rightarrow 0,$$

whose middle term is projective by Exercise 10.19, we deduce that

$$N^* \otimes \Omega M \cong \Omega(N^* \otimes M) \oplus P \quad \text{for some } P \in \mathcal{P}(A).$$

Therefore

$$\mathbf{Hom}(K, N^* \otimes \Omega M) \cong \mathbf{Hom}(K, \Omega(N^* \otimes M)).$$

Setting  $V = N^* \otimes M$ , the problem reduces to proving that

$$(78.18) \quad \mathbf{Hom}(K, \Omega V) \cong K\text{-dual of } \mathbf{Hom}(V, K).$$

*Step 3.* In proving (78.18), we may assume that  $V$  is a core, so let

$$0 \rightarrow \Omega V \rightarrow P \rightarrow V \rightarrow 0$$

be an exact sequence, with  $P$  a projective cover of  $V$ . By Exercise 78.2, we may replace  $\mathbf{Hom}$  by  $\text{Hom}$  in (78.18). By (78.5),  $P$  is an injective hull of  $\Omega V$ , so  $P$  has the same socle as  $\Omega V$ . Therefore

$$\text{Hom}(K, \Omega V) = \text{Hom}(K, \text{soc } \Omega V) = \text{Hom}(K, \text{soc } P) = \text{Hom}(K, P).$$

On the other hand,

$$\text{Hom}(V, K) = \text{Hom}(P, K)$$

by Exercise 78.3, so we need only prove that

$$\text{Hom}_A(K, P) \cong K\text{-dual of } \text{Hom}_A(P, K).$$

Since both sides are covariant additive functors of  $P$ , it suffices to verify the result when  $P = {}_A A$ . But in this case the result is a special case of (10.21), using  $H = \{1\}$  and  $M = L = K$  in (10.21).

We leave it to the reader to check that all the isomorphisms used in the proof are natural.

It is now necessary to discuss the bimodule structures of the  $K$ -spaces occurring in Theorem 78.15. To begin with, we observe that  $\text{Hom}_A(M, N)$  is a bimodule on which  $\text{End}_A N$  acts from the left, and  $\text{End}_A M$  from the right. We call  $\text{Hom}_A(M, N)$  an  $(\text{End}_A N, \text{End}_A M)$ -bimodule, to indicate this fact. We leave it to the reader to verify that  $\mathbf{Hom}_A(M, N)$  has this same bimodule structure. Further, by Exercise 78.5,  $\text{End}_A M$  acts from the left on  $\text{Ext}_A^1(N, \Omega^2 M)$ . It then follows that this  $\text{Ext}$  group is an  $(\text{End}_A M, \text{End}_A N)$ -bimodule. Its  $K$ -dual is therefore an  $(\text{End}_A N, \text{End}_A M)$ -bimodule. Since all of the isomorphisms occurring in (78.15) are natural ones, they commute with endomorphisms of the modules involved. Thus we obtain:

**(78.19) Corollary.** *The isomorphisms in (78.15) are  $(\text{End}_A N, \text{End}_A M)$ -bimodule*

*isomorphisms. In particular, for each left  $A$ -module  $M$ , there is a two-sided  $(\text{End}_A M)$ -isomorphism*

$$\text{Ext}_A^1(M, \Omega^2 M) \cong (\text{End}_A M)',$$

*where  $\text{End}_A M$  is given by (78.14), and prime denotes  $K$ -dual.*

Now let  $M$  be a left  $A$ -module, with endomorphism ring  $E = \text{End}_A M$ . Denote by  $\text{End}_A M$  the factor ring of  $E$  defined in (78.14), and view  $\text{End}_A M$  as an  $(E, E)$ -bimodule. The discussion following (78.14) shows that  $\text{End}_A M = 0$  if and only if  $M \in \mathcal{P}(A)$ . The bimodule structure of  $\text{End}_A M$  allows us to make its  $K$ -dual  $(\text{End}_A M)'$  into an  $(E, E)$ -bimodule, and the correspondence between submodules and their  $K$ -duals is inclusion-reversing. This shows that the minimal submodules of  $(\text{End}_A M)'$  are in bijective correspondence with the maximal submodules of  $\text{End}_A M$ . This is the key fact needed to establish the following result, which will be used in §78B to prove the existence of Auslander-Reiten sequences for  $A$ -modules.

**(78.20) Proposition.** *Let  $M$  be a nonprojective indecomposable left  $A$ -module, where  $A = KG$ , and let  $E = \text{End}_A M$  be its endomorphism ring. Let  $\Omega$  denote the Heller loop-space operator, and form the left  $A$ -module  $\Omega^2 M$ . Then*

$$\text{Ext}_A^1(M, \Omega^2 M)$$

*is an  $(E, E)$ -bimodule. As a one-sided  $E$ -module (left or right), its socle*

$$\text{soc } \text{Ext}_A^1(M, \Omega^2 M)$$

*is a simple  $E$ -module.*

*Proof.* Since  $M$  is indecomposable, its endomorphism ring  $E$  is a local ring (see (6.10)), whose radical  $\text{rad } E$  is the unique maximal left (or right) ideal of  $E$ . The factor ring  $\text{End}_A M$  of  $E$  is not zero, since  $M$  is (by hypothesis) nonprojective. It follows that as left  $E$ -module (or as right  $E$ -module),  $\text{End}_A M$  has a unique maximal submodule. Therefore its  $K$ -dual  $(\text{End}_A M)'$  has a unique minimal submodule, that is, this  $K$ -dual has a simple socle as left (or right)  $E$ -module.

On the other hand, there is an  $(E, E)$ -bimodule isomorphism

$$\text{Ext}_A^1(M, \Omega^2 M) \cong (\text{End}_A M)'$$

by (78.19). Thus  $\text{soc } \text{Ext}_A^1(M, \Omega^2 M)$  is simple as claimed, and the proposition is established.

## §78B. Auslander-Reiten Sequences for Group Algebras

Our aim in this subsection is to define Auslander-Reiten sequences for  $A$ -modules, where  $A$  is an arbitrary artinian ring. We shall then follow an approach

shown to us by P. Webb, based on the fundamental work of Auslander-Reiten [75], to prove the existence of such sequences in the special case where  $A = KG$ , with  $K$  a field and  $G$  a finite group. In §81D, we will indicate the significance of such sequences for studying the representation theory of  $G$  over the field  $K$ .

From now on,  $A$  denotes a left artinian ring, and all  $A$ -modules considered below are assumed to be finitely generated. Denote by  $\mathcal{P}(A)$ ,  $\mathcal{I}(A)$ , and  $\text{Ind } A$ , respectively, the sets of (isomorphism classes of) projective, injective, and indecomposable  $A$ -modules. Thus,  $\text{Ind } A - \mathcal{P}(A)$  consists of all nonprojective indecomposable modules.

**(78.21) Definition.** An *Auslander-Reiten sequence* (or *almost-split sequence*) for an indecomposable  $A$ -module  $M$  is a nonsplit ses

$$(78.22) \quad 0 \rightarrow N \rightarrow E \rightarrow M \rightarrow 0,$$

in which  $N$  is indecomposable, with the following universal mapping property:

For each  $A$ -module  $X$ , each map  $f: X \rightarrow M$ , that is *not* a split surjection factors through  $E$ . In other words, for each such  $f$ , there exists a map  $g$  making the diagram

$$\begin{array}{ccccc} & & X & & \\ & \swarrow g & \downarrow f & \searrow & \\ 0 \rightarrow N \rightarrow E \rightarrow M \rightarrow 0 & & & & \end{array}$$

commute. We call (78.22) an *AR-sequence* for  $M$ .

In the example (78.8) given earlier, it will turn out that the sequence

$$0 \rightarrow JP \rightarrow P \oplus (JP/\text{soc } P) \rightarrow P/\text{soc } P \rightarrow 0$$

is an *AR-sequence* for  $P/\text{soc } P$ . This is not obvious now, however.

**(78.23) Remarks.** (i) A map  $f: X \rightarrow M$  is a split surjection if and only if there exists an  $f': M \rightarrow X$  such that  $ff' = \text{id}_M$ . If this occurs, then  $M \mid X$ .

(ii) If  $M$  is projective or  $N$  is injective, any sequence (78.22) must split, and so cannot be an *AR-sequence*.

(iii) Let (78.22) be an *AR-sequence* for  $M$ , and let

$$0 \rightarrow X \rightarrow Y \rightarrow M \rightarrow 0$$

be any nonsplit ses. From the definition of *AR-sequence*, it follows at once that there must exist homomorphisms (indicated by dotted arrows) for which the diagram

$$\begin{array}{ccccccc} 0 & \rightarrow & X & \rightarrow & Y & \rightarrow & M & \rightarrow 0 \\ & & \downarrow & & \downarrow & & 1\downarrow \\ 0 & \rightarrow & N & \rightarrow & E & \rightarrow & M & \rightarrow 0 \end{array}$$

commutes.

(iv) There is a dual notion: an *AR'-sequence* for an indecomposable  $A$ -module  $N$  is a nonsplit ses (78.22) in which  $M$  is indecomposable, such that:

For each  $A$ -module  $Y$ , each map  $h: N \rightarrow Y$ , that is not a split monomorphism extends to a map  $E \rightarrow Y$ .

It is by no means obvious that there exists an *AR*-sequence for each  $M \in \text{Ind } A - \mathcal{P}(A)$ . Likewise, for each  $N \in \text{Ind } A - \mathcal{I}(A)$ , is there an *AR'*-sequence for  $N$ ? Further, what is the connection between these two concepts?

We quote without proof:

**(78.24) Theorem (Auslander).** *Let  $M$  and  $N$  denote f.g. left  $A$ -modules, where  $A$  is an artinian ring, f.g. as module over its center.\* Then we have:*

(i) *For each  $M \in \text{Ind } A - \mathcal{P}(A)$ , there exists an *AR*-sequence for  $M$ . It is unique up to isomorphism, that is, for any pair of *AR*-sequences for  $M$ , there is a commutative diagram*

$$\begin{array}{ccccccc} 0 & \rightarrow & N & \rightarrow & E & \rightarrow & M & \rightarrow 0 \\ & & \alpha \downarrow & & \beta \downarrow & & 1\downarrow & , \\ 0 & \rightarrow & N' & \rightarrow & E' & \rightarrow & M & \rightarrow 0 \end{array}$$

with  $\alpha$  and  $\beta$  isomorphisms.

(ii) *Dually, for each  $N \in \text{Ind } A - \mathcal{I}(A)$ , there exists an *AR'*-sequence for  $N$ , unique up to isomorphism.*

(iii) *The concepts of *AR*- and *AR'*-sequences coincide, in the sense that (78.22) is an *AR*-sequence for  $M$  if and only if it is an *AR'*-sequence for  $N$ .*

We shall prove this result in the special case where  $A$  is a group algebra  $KG$ , by using the machinery developed in §78A. Indeed, we shall be able to exhibit *AR*-sequences explicitly in this situation, by using the following result, due to Auslander-Reiten [75]:

**(78.25) Theorem.** *Let  $M$  be a nonprojective indecomposable left  $A$ -module, where  $A = KG$ , with  $K$  a field and  $G$  a finite group. Set  $E = \text{End}_A M$ , a local f.d.  $K$ -algebra. Let  $\Omega$  be the Heller loop-space operator, and view  $\text{Ext}_A^1(M, \Omega^2 M)$  as left  $E$ -module via the action\*\* of  $E$  on  $\text{Ext}(*, \Omega^2 M)$ .*

\*Every f.d.  $K$ -algebra  $A$  over a field  $K$  satisfies this hypothesis.

\*\*See Exercise 78.5.

Then  $\text{Ext}_A^1(M, \Omega^2 M)$  has a simple socle as left  $E$ -module, and any generator  $\xi$  of this socle determines an extension

$$(78.26) \quad \xi : 0 \rightarrow \Omega^2 M \rightarrow L \rightarrow M \rightarrow 0,$$

unique up to equivalence of extensions. For each  $\xi$ , the above is an Auslander-Reiten sequence for  $M$ .

Furthermore,  $\Omega$  is bijective on nonprojective (= noninjective) indecomposable  $A$ -modules, so each nonprojective indecomposable module  $N$  can be written as  $N = \Omega^2 M$  for some  $M$ , unique up to isomorphism. For this  $M$ , the sequence (78.26) is an  $AR'$ -sequence for  $N$ .

*Proof.* Write  $\text{Ext}$  instead of  $\text{Ext}_A^1$ , for brevity. By (78.20),  $\text{soc } \text{Ext}(M, \Omega^2 M)$  is a simple left  $E$ -module. Let  $\xi$  be any generator of this socle, that is, any nonzero element of the socle, and let (78.26) be an extension of  $M$  by  $\Omega^2 M$  defined by  $\xi$ . Then  $\Omega^2 M$  is indecomposable and the sequence is nonsplit, so in order to show that it is an  $AR$ -sequence for  $M$ , it remains to verify the universal mapping property: given any  $f \in \text{Hom}_A(X, M)$  which is not a split surjection, we must show that  $f$  factors through  $L$ :

$$\begin{array}{c} X \\ \swarrow f \downarrow \\ 0 \rightarrow \Omega^2 M \rightarrow L \rightarrow M \rightarrow 0 \end{array}$$

The map  $f \in \text{Hom}_A(X, M)$  induces a map

$$f_* : \text{Hom}_A(M, X) \rightarrow \text{Hom}_A(M, M).$$

If  $f_*$  is surjective, then  $fh = \text{id}_M$  for some  $h : M \rightarrow X$ , which contradicts the hypothesis that  $f$  is not a split surjection. We have thus shown that  $f_*$  is not surjective.

Next,  $f_*$  induces a map  $\tilde{f}$  on  $\mathbf{Hom}$ 's, making the diagram

$$\begin{array}{ccc} \text{Hom}_A(M, X) & \xrightarrow{f_*} & \text{Hom}_A(M, M) = E \\ \downarrow & \tilde{f} & \downarrow \varphi \\ \mathbf{Hom}_A(M, X) & \xrightarrow{\tilde{f}} & \mathbf{Hom}_A(M, M) = \mathbf{E} \end{array}$$

commute. As shown in the proof of (78.20),  $\mathbf{E}$  is a nonzero local ring, since it is a nonzero factor ring of the local ring  $E$ . Therefore  $\ker \varphi \subseteq \text{rad } E$ . This shows that  $\tilde{f}$  is not surjective, since otherwise we would obtain

$$E = \text{im } f_* + \ker \varphi = \text{im } f_* + \text{rad } E,$$

and then  $E = \text{im } f_*$  by Nakayama's Lemma, contradicting the fact that  $f_*$  is not surjective.

We are now ready to use (78.15); we have

$$\text{Ext}(X, \Omega^2 M) \cong K\text{-dual of } \mathbf{Hom}_A(M, X), \quad \text{Ext}(M, \Omega^2 M) \cong K\text{-dual of } \mathbf{E}.$$

Therefore  $\tilde{f}$  induces a map

$$f': \text{Ext}(M, \Omega^2 M) \rightarrow \text{Ext}(X, \Omega^2 M),$$

and  $f'$  is not injective since  $\tilde{f}$  is not surjective. View both Ext groups as left  $E$ -modules; then  $f'$  is an  $E$ -homomorphism, and

$$\ker f' \supseteq \text{soc Ext}(M, \Omega^2 M),$$

since  $\ker f' \neq 0$  and the socle is a simple  $E$ -module. It follows that  $f'(\xi) = 0$ , so there is a commutative diagram

$$\begin{array}{ccccccc} \xi: 0 & \rightarrow & \Omega^2 M & \xrightarrow{h} & M & \rightarrow & 0 \\ & & \uparrow 1 & & \uparrow g & & \uparrow f \\ \xi f: 0 & \rightarrow & \Omega^2 M & \rightarrow & L_1 & \xrightarrow{j} & X \rightarrow 0 \end{array}$$

in which the bottom sequence  $\xi f$  is split (because  $f'(\xi) = 0$ ). Hence there is a map  $i: X \rightarrow L_1$  with  $ji = \text{id}_X$ . But then  $h(gi) = f$ , so we have factored the map  $f$  through  $L$ , as desired.

Let  $\mathbf{E} = \mathbf{End}_A M$  as above. By virtue of the isomorphism

$$\mathbf{E} \cong \mathbf{End}_A \Omega^2 M$$

(see Exercise 78.5), and the action of  $\mathbf{End}_A \Omega^2 M$  on  $\text{Ext}(*, \Omega^2 M)$ , we may view  $\text{Ext}(M, \Omega^2 M)$  as left  $\mathbf{E}$ -module. We have shown above that, as  $\mathbf{E}$ -module,  $\text{Ext}(M, \Omega^2 M)$  has simple socle, and any generator of this socle yields an  $AR$ -sequence for  $M$ .

Dually, let  $N$  be any nonprojective indecomposable module; since  $\Omega$  is bijective on such modules, the module  $\Omega^{-2} N$  is uniquely determined up to isomorphism. The isomorphism

$$\mathbf{End}_A N \cong \mathbf{End}_A \Omega^{-2} N$$

allows us to view  $\text{Ext}(\Omega^{-2} N, *)$  as right  $(\mathbf{End}_A N)$ -module. Then any generator of  $\text{soc Ext}(\Omega^{-2} N, N)$  yields an  $AR'$ -sequence for  $N$ .

In particular, an  $AR'$ -sequence for  $\Omega^2 M$  arises from a generator of  $\text{soc Ext}(M, \Omega^2 M)$  as right  $\mathbf{E}$ -module. However, the proof of (78.20) shows that this

socle coincides with  $\text{soc Ext}(M, \Omega^2 M)$  as left  $\mathbf{E}$ -module. It follows at once that the sequence (78.26) is also an  $AR'$ -sequence for  $\Omega^2 M$ , as claimed, and the theorem is established.

Finally, we prove that  $AR$ -sequences are unique up to isomorphism.

**(78.27) Theorem.** *Let  $M$  be a nonprojective indecomposable  $A$ -module, with  $A$  any artinian ring, f.g. over its center. Let*

$$\xi_i : 0 \rightarrow N_i \xrightarrow{f_i} E_i \xrightarrow{g_i} M \rightarrow 0, \quad i = 1, 2,$$

be a pair of  $AR$ -sequences for  $M$ . Then there exists a commutative diagram

$$\begin{array}{ccccccc} \xi_1 : 0 & \longrightarrow & N_1 & \xrightarrow{f_1} & E_1 & \xrightarrow{g_1} & M \longrightarrow 0 \\ & & \alpha \downarrow & & \beta \downarrow & & 1 \downarrow \\ \xi_2 : 0 & \longrightarrow & N_2 & \longrightarrow & E_2 & \longrightarrow & M \longrightarrow 0 \end{array}$$

in which  $\alpha$  and  $\beta$  are isomorphisms.

*Proof.* If such a diagram exists, we indicate it by the notation

$$\xi_2 = (\alpha, \beta, 1)\xi_1.$$

By Remark 78.23iii,  $\beta$  exists since  $\xi_2$  is an  $AR$ -sequence for  $M$ . Then  $\beta$  induces the map  $\alpha$ , and it remains to show that  $\alpha$  and  $\beta$  are isomorphisms.

Reversing the roles of  $\xi_1$  and  $\xi_2$ , we obtain

$$\xi_1 = (\alpha', \beta', 1)\xi_2$$

for some maps  $\alpha'$ ,  $\beta'$ . Therefore

$$\xi_1 = (\alpha'\alpha, \beta'\beta, 1)\xi_1.$$

Now  $\alpha'\alpha \in \text{End}_A N_1$ , and  $\text{End}_A N_1$  is a local ring since  $N_1$  is indecomposable. Thus either  $\alpha'\alpha \in \text{Aut}_A N_1$ , or else  $\alpha'\alpha \in \text{rad End}_A N_1$ . In the latter case we have  $(\alpha'\alpha)^n = 0$  for some  $n$ , since the hypotheses on  $A$  imply that  $\text{rad End}_A N_1$  is nilpotent. Therefore

$$\xi_1 = ((\alpha'\alpha)^n, (\beta'\beta)^n, 1)\xi_1 = (0, *, 1)\xi_1 = 0,$$

so  $\xi_1$  is split exact, contradicting the hypothesis that  $\xi_1$  is an  $AR$ -sequence.

We have thus shown that  $\alpha'\alpha \in \text{Aut}_A N_1$ . Similarly, we obtain  $\alpha\alpha' \in \text{Aut}_A N_2$ , so  $\alpha$  and  $\alpha'$  are isomorphisms. The same then holds for  $\beta$  and  $\beta'$ , by the Snake Lemma, and the result is established.

As a special case of Theorem 78.25, we have:

**(78.28) Proposition.** *Let  $S$  be a simple left  $A$ -module that is not projective, where  $A = KG$ .*

(i) *Every non-split exact sequence*

$$0 \rightarrow \Omega^2 S \rightarrow L \rightarrow S \rightarrow 0$$

*is an AR-sequence for  $S$ , and an AR'-sequence for  $\Omega^2 S$ .*

(ii) *Every non-split exact sequence*

$$0 \rightarrow \Omega S \rightarrow M \rightarrow \Omega^{-1} S \rightarrow 0$$

*is an AR-sequence for  $\Omega^{-1} S$  and an AR'-sequence for  $\Omega S$ .*

*Proof.* We have  $\text{End}_A S$  a skewfield, and then  $\text{End}_A S = \text{End}_A S$  since  $S$  is not projective. Then  $\text{Ext}_A^1(S, \Omega^2 S)$  is a one-dimensional space over this skewfield, so any nonzero element of this Ext group generates its socle. Assertion (i) now follows from (78.25).

For (ii), we note that  $\text{End}_A \Omega^{-1} S$  is also a skewfield (see Exercise 78.4), and we again apply (78.25).

As an illustration of (78.28ii), consider the example (78.8) above. We saw there that

$$\Omega^{-1} S \cong P/\text{soc } P, \quad \Omega S = JP,$$

so the non-split sequence (78.9) is always an AR-sequence.

## Notes

Let  $\Lambda$  be an  $R$ -order in a separable  $K$ -algebra  $A$ , where  $R$  is a complete d.v.r. with quotient field  $K$ . We can then define AR-sequences for the category of  $\Lambda$ -lattices (rather than  $\Lambda$ -modules). As shown by Auslander, AR-sequences exist for every nonprojective indecomposable  $\Lambda$ -lattice. See also Roggenkamp-Schmidt [76].

An explicit construction of such sequences, for the special case where  $\Lambda = RG$  with  $G$  a finite group, was given by Roggenkamp [77], using the techniques of the proof of Theorem 78.25. The result is also inherent in the work of Auslander. The loop-space operator  $\Omega$  is well defined, and for each nonprojective indecomposable  $\Lambda$ -lattice  $M$ , there is an analogue of (78.20), namely:  $\text{Ext}_\Lambda^1(M, \Omega M)$  has a simple socle as  $(\text{End}_\Lambda M)$ -module. Then any generator of this socle gives rise to an extension

$$0 \rightarrow \Omega M \rightarrow L \rightarrow M \rightarrow 0,$$

which is an AR-sequence for  $M$ . (See Roggenkamp [77] for other references.)

### §78C. Auslander-Reiten Sequences for Algebras

Throughout, let  $A$  be a f.d. algebra over a field  $K$ , and consider only f.g.  $A$ -modules in this subsection. Our aim here is to generalize the results of §78B, so as to show the existence of  $AR$ -sequences for  $A$ -modules. The results are due to Auslander-Reiten [74], [75], and we follow here the treatment in Gabriel [80].

For left  $A$ -modules  $M, N$ , we denote  $\text{Hom}_A(M, N)$  by  $(M, N)$  for brevity. Let  $P(M, N)$  be the space of projective homomorphisms from  $M$  to  $N$  (see (78.10)), and let

$$\mathbf{Hom}(M, N) = (M, N)/P(M, N).$$

In order to construct  $AR$ -sequences, the key step is to generalize (78.15) and (78.19) by replacing  $\Omega^2 M$  by some suitable module  $\mathcal{A}(M)$ . For each  $A$ -module  $M$ , put

$$DM = \text{Hom}_K(M, K) = K\text{-dual of } M.$$

Then  $D$  is an exact contravariant functor with  $D^2 = 1$ , and  $D$  takes left  $A$ -modules into right  $A$ -modules, and vice versa. Further,  $D$  maps projective modules onto injective modules, and vice versa. Next, define another contravariant functor  $d$  by

$$dM = \text{Hom}_A(M, A).$$

Then  $d$  is left exact, takes left  $A$ -modules to right  $A$ -modules, and carries projectives to projectives. We now define the *Nakayama functor*  $\mathcal{N} = Dd$ , so for each left  $A$ -module  $M$ ,

$$(78.29) \quad \mathcal{N}M = DdM = K\text{-dual of } \text{Hom}_A(M, A) = D(M, A).$$

We note that for each idempotent  $e \in A$ , we have

$$(78.30) \quad d(Ae) = \text{Hom}_A(Ae, A) \cong eA$$

Furthermore,  $\mathcal{N}$  is a covariant right exact functor, taking left  $A$ -modules to left  $A$ -modules, and carrying projective modules to injective modules.

We now define the *Auslander-Reiten translate\**  $\mathcal{A}M$  of a left  $A$ -module  $M$  as follows. Choose any exact sequence

$$(78.31) \quad P_1 \xrightarrow{f_1} P_0 \xrightarrow{f_0} M \rightarrow 0, \quad P_i \text{ projective},$$

and apply  $\mathcal{N}$  to obtain an exact sequence of left  $A$ -modules

$$\mathcal{N}P_1 \xrightarrow{\mathcal{N}f_1} \mathcal{N}P_0 \xrightarrow{\mathcal{N}f_0} \mathcal{NM} \rightarrow 0.$$

\*Also denoted by  $D\text{Tr } M$ , the *dual transpose* of  $M$ .

Then define  $\mathcal{A}M = \ker \mathcal{N}f_1$ , so there is an exact sequence

$$(78.32) \quad 0 \rightarrow \mathcal{A}M \rightarrow \mathcal{N}P_1 \xrightarrow{\mathcal{N}f_1} \mathcal{N}P_0 \xrightarrow{\mathcal{N}f_0} \mathcal{NM} \rightarrow 0$$

Then  $\mathcal{A}M$  depends on the choice of the  $P_i$ , but is unique up to injective direct summands. In particular, if (78.31) is part of a minimal projective resolution<sup>†</sup> of  $M$ , then  $\mathcal{A}M$  has no injective direct summands.

**Example.** If  $A = KG$ , where  $G$  is a finite group, then by (10.21) for each  $A$ -module  $M$  we have

$$\text{Hom}_A(M, A) \cong \text{Hom}_K(M, K).$$

Thus in this case  $\mathcal{NM} = M$ , and so  $\mathcal{A}M = \Omega^2 M$ .

We shall show that the entire discussion in §78B carries over to the more general case of f.d.  $K$ -algebras, provided that we replace  $\Omega^2 M$  in §78B by the above-defined module  $\mathcal{A}M$ . In fact, it suffices to establish two fundamental results:

For the first, let  ${}_A\text{mod}$  denote the category of f.g. left  $A$ -modules modulo projectives. Thus,  $M$  and  $M'$  determine the same object in  ${}_A\text{mod}$  if and only if  $M \oplus P \cong M' \oplus P'$  for some projectives  $P, P'$ . Morphisms are defined as above, i.e.,

$$\text{Hom}_A(M, N) = (M, N)/P(M, N).$$

Dually, let  $\overline{{}_A\text{mod}}$  be the category of f.g. left  $A$ -modules, modulo injectives. Our first key result is as follows:

**(78.33) Theorem.** *There is a bijection of isomorphism classes  $M \leftrightarrow \mathcal{A}M$  giving an equivalence of categories  ${}_A\text{mod} \cong \overline{{}_A\text{mod}}$ . Hence  $M$  is a nonprojective indecomposable module if and only if  $\mathcal{A}M$  is a noninjective indecomposable module (up to projective and injective summands of  $M$  and  $\mathcal{A}M$ , respectively).*

The second key fact, generalizing (78.15) and (78.19), is given by the following theorem (Auslander-Reiten [75, Props. 7.2, 7.3]):

**(78.34) Theorem.** *Let  $S$  and  $M$  be left  $A$ -modules. There is a natural  $K$ -isomorphism*

$$\text{Ext}_A^1(S, \mathcal{A}M) \cong K\text{-dual of } (M, S)/P(M, S) = D[(M, S)/P(M, S)].$$

Further, the above is an  $(E(M), E(S))$ -bimodule isomorphism, where  $E(M)$  denotes  $\text{End}_A M$ , and  $E(S)$  is defined analogously.

<sup>†</sup>In this situation, this means that  $P_0$  is a projective cover of  $M$ , and  $P_1$  is a projective cover of  $\ker f_0$  (see §6C).

In particular, there is a two-sided  $E(M)$ -isomorphism

$$\mathrm{Ext}_A^1(M, \mathcal{A}M) \cong D(\mathrm{End}_A M).$$

Once we have proved these two theorems, the entire discussion in §78B carries over to the more general case. In particular, (78.25) generalizes as follows: let  $M$  be a nonprojective indecomposable left  $A$ -module, where  $A$  is any f.d.  $K$ -algebra, and let  $N$  be an injective-free core of  $\mathcal{A}M$ . Then  $\mathrm{Ext}_A^1(M, N)$  has a simple socle as left  $E(M)$ -module, and any generator  $\xi$  of this socle determines an extension

$$\xi : 0 \rightarrow N \rightarrow L \rightarrow M \rightarrow 0,$$

which is an  $AR$ -sequence for  $M$  and an  $AR'$ -sequence for  $N$ . The “uniqueness” of such sequences is proved as in (78.27).

The proof of (78.33), which we now give, is a routine exercise on projective covers and injective hulls of modules. For an  $A$ -module  $M$ , consider an exact sequence

$$(*) \quad P_1 \rightarrow P_0 \rightarrow M \rightarrow 0, \quad P_i \text{ projective.}$$

Since the Nakayama function  $\mathcal{N}$  preserves direct sums, it follows from Exercise 78.8 that  $\mathcal{A}M$  is unique up to injective direct summands, and further that no such summands occur if  $(*)$  is part of a minimal projective resolution of  $M$ .

We now construct a functor  $\mathcal{B}$  on left  $A$ -modules, which will turn out to be an inverse for  $\mathcal{A}$ . Given a left  $A$ -module  $N$ , choose any exact sequence

$$0 \rightarrow N \rightarrow I_0 \xrightarrow{h} I_1, I_0, I_1 \text{ injective.}$$

Then there is an exact sequence

$$(78.35) \quad 0 \rightarrow dDN \rightarrow dDI_0 \xrightarrow{h^*} dDI_1 \rightarrow \mathcal{B}(N) \rightarrow 0,$$

where  $\mathcal{B}(N)$  is defined as  $\mathrm{cok } h^*$ .

For an  $A$ -module  $M$ , there is an exact sequence

$$0 \rightarrow \mathcal{A}M \rightarrow DdP_1 \rightarrow DdP_0,$$

which is part of an injective resolution of  $\mathcal{A}M$ . By definition, the sequence

$$(dD)(DdP_1) \rightarrow (dD)(DdP_0) \rightarrow \mathcal{B}(\mathcal{A}M) \rightarrow 0$$

is exact. However, for each projective  $A$ -module  $P$ , there are natural isomorphisms

$$(dD)(DdP) \cong d^2P \cong P.$$

It follows that  $\mathcal{B}(\mathcal{A}M) \cong \text{cok}(P_1 \rightarrow P_0) \cong M$ , as desired. Dually, we obtain  $\mathcal{A}(\mathcal{B}N) \cong N$  for each  $N$ . It is easily verified that for given  $N$ ,  $\mathcal{B}N$  is unique up to projective direct summands and no such summands occur when we use a minimal injective resolution of  $N$ .

Finally, we show that if  $M$  is an  $A$ -module such that  $\mathcal{A}M$  is decomposable (ignoring injective summands), then  $M$  is also decomposable (ignoring projective summands). Indeed, if  $\mathcal{A}M$  has a proper decomposition, then so does its injective resolution, by (6.27). This gives rise to a decomposition of the modules  $dDI_0$ ,  $dDI_1$ , and the map  $h^*$  occurring in (78.35), where now  $N = \mathcal{A}M$ ,  $I_0 = DdP_0$ ,  $I_1 = DdP_1$ . It follows as above that the modules  $P_1, P_0$  and the map  $P_1 \rightarrow P_0$  decompose, and therefore so does  $M$ . A dual argument proves that if  $\mathcal{B}N$  is decomposable, then so is  $N$ . This completes the proof of (78.33).

We begin the proof of (78.34) with an easy result:

**(78.36) Lemma.** *Let  $X$  and  $P$  be left  $A$ -modules, with  $P$  projective. There is a  $K$ -isomorphism*

$$\alpha_X : D(P, X) \cong (X, \mathcal{N}P)$$

which is natural in  $X$ .

*Proof.* Since both sides are additive in  $P$ , it suffices to treat the case  $P = Ae$ , with  $e \in A$  idempotent. Since  $\text{Hom}_A(Ae, X) \cong eX$  as  $K$ -spaces, and  $\text{Hom}_A(Ae, A) \cong eA$  as right  $A$ -modules, it suffices to find maps  $\alpha, \gamma$  that are inverses of one another, where now

$$\text{Hom}_K(eX, K) \xrightleftharpoons[\gamma]{\alpha} \text{Hom}_A(X, \text{Hom}_K(eA, K)).$$

For  $f \in \text{Hom}_K(eX, K)$ , define  $\alpha f$  by the formula

$$[(\alpha f)(x)](ea) = f(ex), \quad x \in X, \quad a \in A.$$

For  $g \in \text{Hom}_A(X, \text{Hom}_K(eA, K))$ , define  $\gamma g$  by

$$(\gamma g)(ex) = [g(ex)](e), \quad x \in X.$$

It is easily checked that  $\alpha, \gamma$  are well-defined, and that  $\alpha\gamma = 1$ ,  $\gamma\alpha = 1$ , so  $\alpha$  is an isomorphism with inverse  $\gamma$ .

Now start with the exact sequence (78.31), and let  $X$  be a left  $A$ -module. Then

$$0 \rightarrow (M, X) \rightarrow (P_0, X) \rightarrow (P_1, X)$$

is exact, whence so is

$$D(P_1, X) \xrightarrow{f'_1} D(P_0, X) \xrightarrow{f'_0} D(M, X) \rightarrow 0.$$

From (78.36), it follows that there is a commutative diagram with exact rows:

$$\begin{array}{ccccccc} D(P_1, X) & \xrightarrow{f'_1} & D(P_0, X) & \xrightarrow{f'_0} & D(M, X) & \rightarrow 0 \\ \alpha_1 \downarrow & & \alpha_0 \downarrow & & 1 \downarrow & \\ 0 \rightarrow (X, \mathcal{A}M) \rightarrow (X, \mathcal{N}P_1) & \longrightarrow & (X, \mathcal{N}P_0) & \xrightarrow{\beta} & D(M, X) & \rightarrow 0, \end{array}$$

where  $\alpha_0, \alpha_1$  are isomorphisms, and  $\beta = f'_0 \alpha_0^{-1}$ .

Now let  $S$  be any left  $A$ -module; for each  $\theta \in (S, \mathcal{N}P_0)$ , let  $E(\theta)$  be the module defined by the pullback diagram

$$\begin{array}{ccc} E(\theta) & \xrightarrow{h} & \mathcal{N}P_1 \\ g \downarrow & & \downarrow \mathcal{N}f_1 \\ S & \xrightarrow{\theta} & \mathcal{N}P_0, \end{array}$$

with  $g, h$  canonical projection maps. It follows that the sequence

$$(*) \quad 0 \rightarrow \mathcal{A}M \rightarrow E(\theta) \xrightarrow{g} S$$

is exact. Furthermore,

$$g \text{ surjective} \Leftrightarrow \text{im } \theta \subseteq \text{im } \mathcal{N}f_1 \Leftrightarrow \text{im } \theta \subseteq \ker \mathcal{N}f_0.$$

Applying  $(X, \cdot)$  to  $(*)$ , we obtain a larger commutative diagram with exact rows:

$$\begin{array}{ccccccc} D(P_1, X) & \xrightarrow{f'_1} & D(P_0, X) & \xrightarrow{f'_0} & D(M, X) & \longrightarrow 0 \\ \downarrow & & \downarrow & & \downarrow & \\ 0 \longrightarrow (X, \mathcal{A}M) \longrightarrow (X, \mathcal{N}P_1) \longrightarrow (X, \mathcal{N}P_0) & \xrightarrow{\beta_X} & D(M, X) \\ 1 \uparrow & h_X \uparrow & \theta_X \uparrow & & 1 \uparrow \\ 0 \longrightarrow (X, \mathcal{A}M) \longrightarrow (X, E(\theta)) \longrightarrow (X, S) & \xrightarrow{g_X} & D(M, X), & & \end{array}$$

where  $a_X = \beta_X \theta_X$ . The lower half is natural in  $X$ , so for each  $\varphi \in (X, S)$ , there is a commutative diagram

$$\begin{array}{ccc} (S, S) & \xrightarrow{a_S} & D(M, S) \\ \varphi^* \downarrow & & \varphi' \downarrow \\ (X, S) & \xrightarrow{a_X} & D(M, X), \end{array}$$

where  $\varphi$  induces  $\varphi^*$  and  $\varphi'$ . Since  $\varphi^*(\text{id}_S) = \varphi$ , we obtain

$$a_X(\varphi) = \varphi'(t_\theta), \quad \text{where } t_\theta = a_S(\text{id}_S) \in D(M, S).$$

Note that  $a_X(\varphi) \in \text{Hom}_K((M, X), K)$ , and for each  $\psi \in (M, X)$ ,

$$[a_X(\varphi)]\psi = [\varphi'(t_\theta)]\psi = t_\theta(\varphi\psi).$$

It follows that

$$\ker a_X = \{\varphi \in (X, S) : a_X(\varphi) = 0\} = \{\varphi \in (X, S) : \varphi \circ (M, X) \subseteq \ker t_\theta\}.$$

Furthermore,  $g_X$  is surjective if and only if  $\ker a_X = (X, S)$ .

Choosing  $X = A$  in the above, we conclude that the map  $(A, E(\theta)) \rightarrow (A, S)$  is surjective if and only if

$$(A, S) \circ (M, A) \subseteq \ker t_\theta,$$

where the left-hand expression is defined as the  $K$ -span of all composites  $hh'$ ,  $h \in (A, S)$ ,  $h' \in (M, A)$ . By Exercise 78.7,  $(A, S) \circ (M, A) = P(M, S)$ . On the other hand,  $(A, E(\theta)) \rightarrow (A, S)$  is surjective if and only if  $g: E(\theta) \rightarrow S$  is surjective, or equivalently, if and only if  $\text{im } \theta \subseteq \text{im } \mathcal{N}f_1$ . Thus we obtain

$$(78.37) \quad \text{im } \theta \subseteq \text{im } \mathcal{N}f_1 \Leftrightarrow t_\theta(P(M, S)) = 0.$$

Continuing with the proof of (78.34), we identify  $D[(M, S)/P(M, S)]$  with a  $K$ -subspace of  $D(M, S)$ , namely,

$$(78.38) \quad D[(M, S)/P(M, S)] = \{\varphi \in \text{Hom}_K((M, S), K) : \varphi(P(M, S)) = 0\}.$$

We are trying to establish an isomorphism  $\text{Ext}_A^1(S, \mathcal{AM}) \cong D[(M, S)/P(M, S)]$ ; and (78.37) and (78.38) will enable us to calculate the right-hand side. Turning to the left-hand side, we use the exact sequence (see (78.32))

$$0 \rightarrow \mathcal{AM} \rightarrow \mathcal{NP}_1 \xrightarrow{\mathcal{N}f_1} \text{im } \mathcal{N}f_1 \rightarrow 0.$$

Since  $\mathcal{NP}_1$  is injective and so  $\text{Ext}_A^1(\cdot, \mathcal{NP}_1) = 0$  (see (8.4v)), it follows from (8.10) that there is a  $K$ -isomorphism

$$\text{Ext}_A^1(S, \mathcal{AM}) \cong (S, \text{im } \mathcal{N}f_1)/\text{im}(S, \mathcal{NP}_1)$$

that is natural in  $S$ .

From the exact sequence

$$(S, \mathcal{NP}_1) \rightarrow (S, \mathcal{NP}_0) \xrightarrow{\beta_S} D(M, S) \rightarrow 0,$$

we conclude that

$$\text{im}(S, \mathcal{N}P_1) = \ker \beta_S.$$

Next, we must determine which elements  $\theta \in (S, \mathcal{N}P_0)$  have the property that  $\beta_S \theta$  represents an element of  $D[(M, S)/P(M, S)]$ , that is, such that  $(\beta_S \theta)P(M, S) = 0$ . Choosing  $X = S$  in the discussion following (78.36), we have

$$(\beta_S \theta)P(M, S) = [a_S(\text{id}_S)]P(M, S) = t_\theta(P(M, S)).$$

Thus by (78.37)

$$\begin{aligned} \{\theta \in (S, \mathcal{N}P_0) : \beta_S \theta \in D[(M, S)/P(M, S)]\} &= \{\theta \in (S, \mathcal{N}P_0) : t_\theta(P(M, S)) = 0\} \\ &= \{\theta \in (S, \mathcal{N}P_0) : \text{im } \theta \subseteq \text{im } \mathcal{N}f_1\} = (S, \text{im } \mathcal{N}f_1). \end{aligned}$$

We have thus shown that  $\beta_S$  maps  $(S, \text{im } \mathcal{N}f_1)$  onto  $D[(M, S)/P(M, S)]$ , with kernel  $\text{im}(S, \mathcal{N}P_1)$ . This establishes the desired isomorphism, and completes the proof of Theorem 78.34.

We leave it to the reader to verify that the entire discussion of §78B carries over to the case where  $A$  is a f.d.  $K$ -algebra, provided we replace  $\Omega^2 M$  by  $\mathcal{A}M$  throughout that discussion. In particular, we have now proved:

**(78.39) Theorem (Auslander).** *All the assertions in (78.24) are valid when  $A$  is a f.d. algebra over a field.*

## Exercises

Throughout, let  $A = KG$ .

- Let  $M$  be an  $A$ -module, where  $A = KG$ , and consider an exact sequence of  $A$ -modules

$$0 \rightarrow L \rightarrow P_r \rightarrow \cdots \rightarrow P_0 \rightarrow M \rightarrow 0, \quad \text{with each } P_i \in \mathcal{P}(A).$$

Prove that

$$\text{core of } L \cong \Omega^{r+1} M,$$

where  $\Omega$  is the Heller loop-space operator.

- Let  $S$  be a simple  $A$ -module and  $M$  a core. Show that

$$\text{Hom}_A(M, S) = \mathbf{Hom}_A(M, S), \quad \text{Hom}_A(S, M) = \mathbf{Hom}_A(S, M).$$

[Hint: Let  $f \in \text{Hom}_A(M, S)$ ,  $f \neq 0$ ; then  $f$  is surjective. If  $f$  factors through a projective,

then  $f$  factors through a projective cover  $P$  of  $S$ , so there is a commutative diagram

$$\begin{array}{c} M \\ \swarrow f \\ g \\ \downarrow \\ 0 \rightarrow X \rightarrow P \rightarrow S \rightarrow 0. \end{array}$$

Then  $X = \text{rad } P$ , and since  $f$  is surjective we have  $P = g(M) + X$ . Therefore  $P = g(M)$ , so  $P \mid M$ , a contradiction. The second isomorphism follows in a similar way.]

3. Let  $S$  be a simple  $A$ -module, and let  $P$  be a projective cover of an  $A$ -module  $V$ . Show that

$$\text{Hom}_A(V, S) \cong \text{Hom}_A(P, S).$$

[Hint: Each  $f: V \rightarrow S$  lifts to a map  $g: P \rightarrow S$ . Conversely, given  $g$ , let  $X = \ker(P \rightarrow V)$ ; then  $X \subseteq (\text{rad } A)P$  by (6.25), so  $g(X) = 0$ . Therefore  $g$  induces a map  $f$ .]

4. Let  $S$  be a simple nonprojective  $A$ -module. Prove that

$$\mathbf{End}_A S = \text{End}_A S = \text{skewfield}.$$

5. Prove that

$$\mathbf{End}_A M \cong \mathbf{End}_A \Omega M \cong \mathbf{End}_A \Omega^2 M,$$

and that  $\text{Ext}_A^1(X, \Omega^2 M)$  is naturally a left  $(\mathbf{End}_A M)$ -module.

[Hint: Each  $f \in \text{End } M$  induces a map  $g \in \text{End } \Omega M$ , shown in the diagram

$$\begin{array}{ccccccc} 0 & \longrightarrow & \Omega M & \longrightarrow & P & \longrightarrow & M \longrightarrow 0 \\ & & \downarrow g & & \downarrow & & \downarrow f \\ 0 & \longrightarrow & \Omega M & \longrightarrow & P & \longrightarrow & M \longrightarrow 0, \end{array}$$

where  $P$  is a projective cover of  $M$ . If  $f$  factors through  $P$ , we may choose  $g = 0$ . If both  $h$  and  $h'$  lift  $f$ , then  $h - h': P \rightarrow \Omega M$ , so  $g - g'$  factors through a projective.]

6. Let  $A = KG$ , where  $\text{char } K = p > 0$ , and  $G$  is a cyclic  $p$ -group  $\langle x: x^q = 1 \rangle$ . Prove

- (i) There are exactly  $q$  indecomposable  $A$ -modules, and these are given by

$$V_i = (1 - x)^{q-i} A \cong A/(1 - x)^i A, \quad \text{for } 1 \leq i \leq q.$$

Further,  $\dim_K V_i = i$ , and

$$\Omega V_i \cong V_{q-i}, \quad \Omega^2 V_i \cong V_i \quad \text{for } 1 \leq i < q.$$

- (ii) For  $1 \leq i < q$ , there is an  $AR$ -sequence of  $A$ -modules

$$0 \rightarrow V_i \rightarrow V_{i-1} \oplus V_{i+1} \rightarrow V_i \rightarrow 0.$$

[Hint: for (ii): Let  $\bar{A} = A/(1 - x)^{i+1} A$ , and view the above modules as  $\bar{A}$ -modules. Then

$V_{i+1} \cong \bar{A}$ , and the above sequence is that given in (78.9). Finally, check that this  $AR$ -sequence of  $\bar{A}$ -modules is also one over  $A$ .]

In Exercises 7 and 8,  $A$  is a f.d.  $K$ -algebra, over a field  $K$ .

7. Let  $M, S$  be left  $A$ -modules. Prove that

$$(A, S)^\circ(M, A) = P(M, S),$$

where the left-hand side is the  $K$ -space spanned by all composites  $hg$ ,  $h \in (A, S)$ ,  $g \in (M, A)$ , and  $P(M, S)$  denotes the space of projective maps.

[Hint: Each  $f \in P(M, S)$  factors through a free  $A$ -module.]

8. Let  $M$  be a left  $A$ -module, and let  $\bar{P}_1 \rightarrow \bar{P}_0 \rightarrow M \rightarrow 0$  be part of a minimal projective resolution of  $M$ . Show that for any exact sequence  $P_1 \rightarrow P_0 \rightarrow M \rightarrow 0$ , with  $P_i$  projective, there exists a commutative diagram with exact rows:

$$\begin{array}{ccccccc} P_1 & \longrightarrow & P_0 & & M & \longrightarrow & 0 \\ \downarrow & & \downarrow & & 1 \downarrow & & \\ P_1 \oplus Q_0 \oplus Q_1 & \longrightarrow & \bar{P}_0 \oplus Q_0 & \longrightarrow & M & \longrightarrow & 0, \end{array}$$

where the vertical maps are isomorphisms and the  $Q_1$  are projective. Dualize to obtain a corresponding result for injective resolutions.

[Hint: Let  $P_M$  denote a projective cover of  $M$ , with kernel  $N$ . We choose  $\bar{P}_0 = P_M$ ,  $\bar{P}_1 = P_N$ , and  $f: P_N \rightarrow N \rightarrow P_M$  the composite map. The surjection  $\bar{P}_0 \rightarrow M$  factors through a surjection  $P_0 \rightarrow P_M$ , so we may take  $P_0 = P_M \oplus Q_0$ . Now consider

$$\begin{array}{ccccccc} 0 & \longrightarrow & N & \longrightarrow & P_M & \longrightarrow & M \longrightarrow 0 \\ & & & & \downarrow (1, 0) & & \downarrow \\ 0 & \longrightarrow & N' & \longrightarrow & P_M \oplus Q_0 & \longrightarrow & M \longrightarrow 0. \end{array}$$

Then  $N' \cong N \oplus Q_0$ , and  $P_1$  maps onto  $N'$ , so  $P_1 = P^* \oplus Q_0$ , where  $P^* \rightarrow N$  is surjective. As above,  $P^* \cong P_N \oplus Q_1$  for some  $Q_1$ .]

## §79. ALGEBRAS OF FINITE REPRESENTATION TYPE

In this section,  $K$  denotes an arbitrary field, and  $A$  a f.d.  $K$ -algebra. Our objective is to prove a theorem of Roiter [68], which asserts that if the composition lengths (or dimensions over  $K$ ) of the f.g. indecomposable left  $A$ -modules are bounded, then the number of isomorphism classes of indecomposable left  $A$ -modules is finite. This result settled the long-standing conjecture of Brauer-Thrall for f.d.  $K$ -algebras. The corresponding result was proved by Auslander [74] for artinian rings. The fact that the Brauer-Thrall conjecture holds for group algebras of finite groups was proved earlier by D. Higman [54] (see CR §64, and §62 below.)

We shall give a new proof of Roiter's theorem for f.d.  $K$ -algebras, which is

due to Yamagata [78], and is based on the theory of *AR*-sequences (from §78C). Yamagata's approach also describes a procedure for constructing indecomposable left  $A$ -modules from the simple modules, using the theory of *AR*-sequences, for f.d.  $K$ -algebras  $A$  of finite representation type. The result is not as explicit, however, as the construction of the indecomposable  $KG$ -modules in a block with a cyclic defect group, by Janusz [69] and Kupisch [68], [69] (see also Feit [82, Chapter VII]). We remark also that Yamagata's theorems are all established for artinian rings, while our approach is restricted to f.d.  $K$ -algebras, since we have only proved the existence of *AR*-sequences in that case (in §78C).

We begin with some preliminary remarks. It is assumed that all left  $A$ -modules  $M$  under consideration are f.g., over the given f.d.  $K$ -algebra  $A$ . The composition length of  $M$  is denoted by  $c(M)$ , and its isomorphism class by  $(M)$ . The set of isomorphism classes of f.g. indecomposable  $A$ -modules is denoted by  $\text{Ind } A$ . The algebra  $A$  is said to have *finite representation type* if  $\text{Ind } A$  is a finite set, and *bounded representation type* if the set of composition lengths  $\{c(M) : (M) \in \text{Ind } A\}$  is bounded.

Let  $(M) \in \text{Ind } A$ . We recall from §78 that an *AR-sequence* for  $M$  (or *Auslander-Reiten sequence*) is a nonsplit ses

$$(79.1) \quad 0 \rightarrow N \rightarrow E \xrightarrow{f} M \rightarrow 0,$$

with  $N$  indecomposable, and having the universal mapping property that each homomorphism of  $A$ -modules  $g: X \rightarrow M$ , which is not a split surjection, factors through  $E$ . The existence and uniqueness of *AR*-sequences, for all nonprojective indecomposable modules over a f.d.  $K$ -algebra  $A$ , was proved in §78C.

The preceding discussion does not apply to a projective indecomposable  $A$ -module  $M$ . In this case, however,  $\text{rad } M$  is the unique maximal submodule of  $M$ , and the inclusion map  $f: \text{rad } M \rightarrow M$  has the universal property that each homomorphism of  $A$ -modules  $g: X \rightarrow M$ , which is not a split surjection, factors through  $\text{rad } M$ .

Thus we are led to define an *almost-split homomorphism*  $(E, f)$ , for an indecomposable  $A$ -module  $M$ , to be a homomorphism of  $A$ -modules  $f: E \rightarrow M$  such that either (a)  $M$  is not projective and

$$0 \rightarrow \ker f \rightarrow E \xrightarrow{f} M \rightarrow 0$$

is an *AR*-sequence for  $M$ , or (b)  $M$  is projective,  $E = \text{rad } M$ , and  $f$  is the inclusion map. As we have pointed out, each almost-split homomorphism  $f: E \rightarrow M$  has the universal property that homomorphisms  $g: X \rightarrow M$ , which are not split surjections, factor through  $E$ . In particular,  $E$  is uniquely determined, up to isomorphism, in both cases.

Now let  $\{M_i : i \in I\}$  be a family of indecomposable left  $A$ -modules, possibly with repetitions, indexed by a set  $I$ . The family is called *noetherian* if for each

sequence of nonisomorphisms

$$M_{i_1} \xrightarrow{f_{i_1}} M_{i_2} \xrightarrow{f_{i_2}} M_{i_3} \rightarrow \cdots \quad (i_j \in I),$$

there exists an integer  $n$  such that  $f_{i_n} \cdots f_{i_2} f_{i_1} = 0$ . The family is called *conoetherian* if, for each sequence of nonisomorphisms

$$\cdots \rightarrow M_{j_3} \xrightarrow{g_{j_2}} M_{j_2} \xrightarrow{g_{j_1}} M_{j_1} \quad (j_i \in I)$$

there exists an integer  $m > 0$  such that  $g_{j_m} g_{j_{m-1}} \cdots g_{j_1} = 0$ .

The first result holds for families of modules over artinian rings.

**(79.2) Lemma (Harada-Sai [70]).** *Let  $A$  be an artinian ring, and  $\{M_i : i \in I\}$  a family of f.g. indecomposable left  $A$ -modules whose composition lengths are bounded above. Then the family  $\{M_i : i \in I\}$  is noetherian and conoetherian.*

*Proof.* By hypothesis there exists an integer  $N > 0$  such that  $c(M_i) < N$  for all  $i \in I$ . Let us first consider a sequence of nonisomorphisms

$$(79.3) \quad M_{i_1} \xrightarrow{f_{i_1}} M_{i_2} \xrightarrow{f_{i_2}} M_{i_3} \rightarrow \cdots.$$

Then any sequence of  $N + 1$  or more consecutive maps  $\{f_{i_p}, \dots, f_{i_{p+N}}\}$  contains at least one map with a nonzero kernel. Therefore, in order to prove the noetherian condition, it is sufficient to consider a sequence (79.3) in which  $\ker f_{i_j} \neq 0$  for all  $j$ . This reduction is accomplished by taking a suitable subsequence of the index set in (79.3), and replacing the maps by products of consecutive ones. By a second reduction of this type, we may assume that the composition lengths  $\{c(M_{i_j})\}$  of the modules occurring in (79.3) are constant.

In this situation, we shall prove that there exists an integer  $n_0$  such that  $f_{i_{n_0}} \cdots f_{i_1} = 0$ . This is a consequence of the following general argument. Consider a sequence of f.g. indecomposable modules  $\{M_i\}$ , all having the same composition length, and homomorphisms  $\{h_i\}$ ,

$$M_1 \xrightarrow{h_1} M_2 \xrightarrow{h_2} M_3 \rightarrow \cdots$$

such that  $\ker h_i \neq 0$  for all  $i$ . Then there exists an integer  $q > 0$  such that  $c(M_i) = q$  for all  $i$ . For the purposes of this argument, let

$$\Pi(i, j) = h_{j+i-1} \cdots h_{j+1} h_j, \quad \text{for all } i \text{ and } j.$$

We shall prove, by induction on  $m$ , that, for all  $m$ , we have

$$(79.4) \quad c(\Pi(2^m, 1)M_1) \leq q - m - 1.$$

We first note that  $c(h_1(M_1)) \leq q - 1$  since  $\ker h_1 \neq 0$ , which proves (79.4) in case  $m = 0$ . Now assume that, for some  $m$ ,  $c(\Pi(2^m, 1)M_1) \leq q - m - 1$  for any sequence as above. Then  $c(\Pi(2^{m+1}, 1)M_1) \leq q - m - 1$ . If the inequality is strict, then (79.4) follows, since  $q - m - 2 = q - (m + 1) - 1$ . Thus we must rule out the possibility that  $c(\Pi(2^{m+1}, 1)M_1) = q - m - 1$ . If this occurs, then the restriction of the map  $\Pi(2^m, 2^m + 1)$  to  $\Pi(2^m, 1)M_1 \subseteq M_{2^{m+1}}$  is injective. On the other hand,

$$c(\Pi(2^m, 2^m + 1)M_{2^{m+1}}) \leq q - m - 1$$

by the induction hypothesis, and we obtain

$$\Pi(2^m, 2^m + 1)M_{2^{m+1}} = \Pi(2^m, 2^m + 1)\Pi(2^m, 1)M_1$$

by comparing composition lengths. It follows that

$$M_{2^{m+1}} = \Pi(2^m, 1)M_1 \oplus \ker \Pi(2^m, 2^m + 1),$$

contrary to the assumption that the modules  $\{M_i\}$  are indecomposable. This completes the proof of (79.4). The assertion that  $f_{i_{n_0}} \cdots f_{i_1} = 0$  for some  $n_0$  follows at once from (79.4). It follows that the family  $\{M_i : i \in I\}$  is noetherian.

We next consider a sequence of nonisomorphisms

$$\cdots \rightarrow M_{j_3} \xrightarrow{g_{j_2}} M_{j_2} \xrightarrow{g_{j_1}} M_{j_1}.$$

By the first part of the proof, it follows that for some block of consecutive terms, we have

$$g_{j_r} \cdots g_{j_{r+s}} = 0.$$

This shows that the family is conoetherian, and completes the proof of the lemma.

For the rest of this section, we return to the situation where  $A$  is a f.d.  $K$ -algebra.

**(79.5) Lemma.** *Let  $M$  be an indecomposable left  $A$ -module, and let  $f: E \rightarrow M$  be an almost split homomorphism. Let  $E = \bigoplus_{i=1}^m E_i$ , with each  $E_i$  indecomposable, and let  $\varepsilon_i: E_i \rightarrow E$  be the injection associated with the direct sum decomposition, for  $1 \leq i \leq m$ . Then  $f \varepsilon_i$  is not an isomorphism, for each  $i$ ,  $1 \leq i \leq m$ .*

*Proof.* Suppose, to the contrary, that  $f \varepsilon_i: E_i \rightarrow M$  is an isomorphism. Then  $f$  is surjective. Moreover, setting  $g_i = f \varepsilon_i$ ,  $\varepsilon_i g_i^{-1}$  is a map from  $M \rightarrow E$  such that  $f \varepsilon_i g_i^{-1}$  is the identity map on  $M$ . Thus  $f$  is a split surjection, which is impossible for an almost-split homomorphism  $f$ .

Now let  $M$  be an arbitrary indecomposable  $A$ -module. We shall define, for

each integer  $n \geq 0$ , a finite set  $\mathbf{E}_n(M)$  of isomorphism classes of indecomposable modules, as follows:

- (i)  $\mathbf{E}_0(M) = \{(M)\};$
- (ii)  $(X) \in \mathbf{E}_{n+1}(M)$ , for an indecomposable module  $X$ , if and only if there exists an almost-split homomorphism  $f:E \rightarrow Y$  such that

$$(Y) \in \mathbf{E}_n(M) \quad \text{and} \quad X|E.*$$

The finiteness of the  $\mathbf{E}_n(M)$  follows from the fact that if  $f:E \rightarrow Y$  is an almost split homomorphism, then  $E$  is determined, up to isomorphism, by  $Y$ .

The main theorem, which settles the Brauer-Thrall conjecture, is stated as follows.

**(79.6) Theorem.** *Let  $A$  be a f.d.  $K$ -algebra, and let  $\{S_1, \dots, S_n\}$  be a basic set of simple left  $A$ -modules. Then the following statements are equivalent.*

- (i)  $A$  is of finite representation type.
- (ii)  $A$  is of bounded representation type.
- (iii) The family of f.g. indecomposable  $A$ -modules satisfies the noetherian and conoetherian conditions.
- (iv) There exists a positive integer  $m$  such that

$$\text{Ind } A = \bigcup_{\substack{1 \leq i \leq n, 0 \leq j \leq m}} \mathbf{E}_j(S_i).$$

*Proof.* The implication (i)  $\Rightarrow$  (ii) is clear from the definitions. The implication (ii)  $\Rightarrow$  (iii) follows from Lemma 79.2, while the fact that (iv)  $\Rightarrow$  (i) is a consequence of the finiteness of the sets  $\mathbf{E}_j(S_i)$ , for all  $i$  and  $j$ .

Thus it is sufficient to prove that (iii)  $\Rightarrow$  (iv). For each simple module  $S_i$ ,  $1 \leq i \leq n$ , and each integer  $j \geq 1$ , we shall define a finite set  $\mathbf{H}_j(S_i)$  consisting of nonisomorphisms  $h_j:M_j \rightarrow M_{j-1}$ , where  $(M_j)$  and  $(M_{j-1})$  are certain isomorphism classes in  $\mathbf{E}_j(S_i)$  and  $\mathbf{E}_{j-1}(S_i)$ , respectively. We first choose, for each  $j$ , a fixed set of representatives  $\{M_j\}$  of the isomorphism classes in  $\mathbf{E}_j(S_i)$ . For each module  $M_{j-1}$ , with  $(M_{j-1}) \in \mathbf{E}_{j-1}(S_i)$ , choose a fixed almost-split homomorphism  $f_j:E_j \rightarrow M_{j-1}$ . For each module  $M_j$  such that  $M_j|E_j$ , we have  $(M_j) \in \mathbf{E}_j(S_i)$ , and define a map  $h_j:M_j \rightarrow M_{j-1}$  by setting  $h_j = f_j \varepsilon_j$ , where  $\varepsilon_j$  is a fixed injection from  $M_j$  to a direct summand of  $E_j$ . If two representative modules  $M_j$  and  $M_{j-1}$  are not related in this way, we define  $h_j:M_j \rightarrow M_{j-1}$  to be zero. The set  $\mathbf{H}_j(S_i)$  consists of precisely the maps  $h_j:M_j \rightarrow M_{j-1}$ , defined in the preceding discussion. Each map  $h_j \in \mathbf{H}_j(S_i)$  is a nonisomorphism, by Lemma 79.5. Moreover,  $\mathbf{H}_j(S_i)$  is a finite set, since the sets  $\mathbf{E}_j(S_i)$  and  $\mathbf{E}_{j-1}(S_i)$  are both finite, for each  $j$ .

We next let  $A_{i,r}$ ,  $r = 1, 2, \dots$ , denote the finite set consisting of all nonzero products  $\{h_1 \cdots h_r : h_j \in \mathbf{H}_j(S_i), 1 \leq j \leq r, \text{ and } h_1 \cdots h_r \neq 0\}$ . We also need to consider

\*As usual,  $X|E$  means that  $X$  is isomorphic to a direct summand of  $E$ .

the family  $F_i$  consisting of the maps  $\{\theta_{i,r}: r = 1, 2, \dots\}$ , where  $\theta_{i,r}$  is the map from  $A_{i,r}$  to the power set of  $A_{i,r+1}$  such that  $\theta_{i,r}(a_r)$  is the set of all nonzero products  $a_r h_{r+1}$ , with  $h_{r+1} \in \mathbf{H}_{r+1}(S_i)$ , for each element  $a_r \in A_{i,r}$ .

If, for some positive integer  $r$ ,  $A_{i,r}$  is empty, then it follows that  $h_1 \cdots h_r = 0$  for all elements  $h_j \in \mathbf{H}_j(S_i)$ ,  $1 \leq j \leq r$ . On the other hand, if all the sets  $A_{i,r}$  are nonempty, then they provide an example of a *König graph*, according to the following definition.

A *König graph*  $\{A_r, F: r = 0, 1, 2, \dots\}$  consists of a countable family of finite non-empty sets  $\{A_r\}$  and a set of mappings  $F = \{\theta_r: r = 0, 1, 2, \dots\}$ , where each  $\theta_r$  is a map from  $A_r$  to the power set of  $A_{r+1}$ . A *path* in the graph is a finite or infinite sequence  $\{a_0, a_1, a_2, \dots\}$  such that  $a_0 \in A_0$ , and  $a_i \in \theta_{i-1}(a_{i-1})$  for each  $i \geq 1$ . We have:

**(79.7) Lemma** (Osofsky [66]). *If the König graph  $\{A_r, F\}$  has arbitrarily long paths, then it has a path of infinite length.*

*Proof of (79.7).* The result is known as König's Graph Theorem. Call an element  $a_r \in A_r$  *special* if there exist arbitrarily long paths containing  $a_r$ . For convenience, define another set  $A_{-1} = \{a_{-1}\}$ , and define  $\theta_{-1} \in F$  such that  $\theta_{-1}(a_{-1}) = A_0$ . Then  $a_{-1}$  is special, by hypothesis. Assume  $a_r$  is special, for some  $a_r \in A_r$ . If no element of the finite set  $\theta_r(a_r)$  is special, then there is an upper bound on the lengths of all paths through each of these elements. The maximum of these upper bounds is clearly an upper bound on lengths of all paths through  $a_r$ , contradicting the assumption that  $a_r$  is special. It follows that some element of  $\theta_r(a_r)$  is special. We then obtain a path of infinite length by selecting a special element  $a_0 \in \theta_{-1}(A_{-1})$ , and for each  $r$ , choosing a special element  $a_r \in \theta_{r-1}(a_{r-1})$ . This proves the lemma.

We apply the preceding lemma to the König graph  $\{A_{i,r}, F_i\}$ , in case all the sets  $A_{i,r}$  are nonempty. If the graph contains arbitrarily long paths, then there is an infinite path, by the lemma, and this contradicts the hypothesis (iii), that the family of all indecomposable  $A$ -modules satisfies the conoetherian condition. It follows that in all cases, whether some set  $A_{i,r}$  is empty or not, that there exists an integer  $m_i > 0$  such that  $h_1 \cdots h_{m_i} = 0$  for all products of elements  $h_j \in \mathbf{H}_j(S_i)$ ,  $1 \leq j \leq m_i$ . Let us set  $m = \max \{m_i: 1 \leq i \leq n\}$ , and let

$$\mathbf{E} = \bigcup_{1 \leq i \leq n, 0 \leq r \leq m} \mathbf{E}_j(S_i).$$

We have to prove that  $\mathbf{E} = \text{Ind } A$ . Suppose, to the contrary, that  $(M) \notin \mathbf{E}$ , for some indecomposable  $A$ -module  $M$ . Since the isomorphism classes of the simple modules are all in  $\mathbf{E}$ ,  $M$  is not simple, and there exists a nonprojective simple module  $S_i$ , for  $1 \leq i \leq n$ , and a nonzero nonsplit homomorphism  $g: M \rightarrow S_i$ . Then there exists an almost-split homomorphism  $f_1: E_1 \rightarrow S_i$ , as in the first part of the proof. Moreover, the homomorphism  $g: M \rightarrow S_i$  factors through  $E_1$ . It follows that there exists a representative  $M_1$  of an isomorphism class in  $\mathbf{E}_1(S_i)$  such

that  $M_1|E_1$ , and maps  $g_1:M \rightarrow M_1$  and  $h_1:M_1 \rightarrow S_i$  such that  $h_1g_1 \neq 0$ , and  $h_1 \in \mathbf{H}_1(S_i)$ . Then  $g_1$  is a nonzero nonsplit nonisomorphism from  $M$  to  $M_1$ , since  $(M) \notin \mathbf{E}$ . Continuing with  $g_1$  instead of  $g$ , it follows that there exists an almost-split homomorphism  $f_2:E_2 \rightarrow M_1$ , and the map  $g_1:M \rightarrow M_1$  factors through  $E_2$ , so that  $g_1 = f_2\varphi$ , for some map  $\varphi:M \rightarrow E_2$ . Then  $h_1g_1 \neq 0$  implies that  $h_1f_2\varphi \neq 0$ . Using the same reasoning as in the first step, we obtain an indecomposable module  $M_2|E_2$ , and maps  $g_2:M \rightarrow M_2$  and  $h_2:M_2 \rightarrow M_1$ , such that  $h_2 \in \mathbf{H}_2(S_i)$  and  $h_1h_2g_2 \neq 0$ . The argument can be repeated, and yields elements  $h_j \in \mathbf{H}_j(S_i)$ ,  $1 \leq j \leq m$ , such that  $h_1h_2 \cdots h_m \neq 0$ , contrary to the definition of  $m$ . This proves that  $(M) \in \mathbf{E}$ , so  $\text{Ind } A = \mathbf{E}$ , and the implication (iii)  $\Rightarrow$  (iv) is proved. This completes the proof of the theorem.

**Remarks.** A criterion for a  $K$ -algebra to have finite representation type, which was shown by Janusz [69] to hold for all group algebras of finite representation type, was obtained by Curtis-Jans [65].

# The Burnside Ring and the Representation Ring of a Finite Group

This chapter contains a study of two commutative rings associated with categories of  $G$ -modules, in much the same way as the ring  $\text{ch } G$  of virtual complex characters arises from the category of f.g.  $CG$ -modules.

The first is the Burnside ring  $\Omega(G)$ , which is the commutative ring consisting of all formal  $\mathbf{Z}$ -linear combinations of finite  $G$ -sets, with addition defined by taking disjoint unions, and multiplication by cartesian products. The main results include the construction of a family of homomorphisms from  $\Omega(G)$  to  $\mathbf{Z}$  that separate elements of  $\Omega(G)$ , a description of the set of prime ideals of  $\Omega(G)$ , and an induction theorem due to Conlon, which is a generalization of the Artin Induction Theorem.

The second is the representation ring  $a(RG)$ , for a commutative integral domain  $R$ . It consists of the formal linear combinations of the isomorphism classes of f.g.  $RG$ -modules, with addition defined by taking direct sums, and multiplication by inner tensor products. The ring  $a(RG)$  is sometimes called the Green ring, after J. A. Green [62b], who studied it in case  $R$  is a field of characteristic  $p$ . The representation algebra  $A(kG) = \mathbf{C} \otimes_{\mathbf{Z}} a(kG)$ , for a field  $k$ , has been examined thoroughly, and §81 contains a survey of some of the high points, including some new insights by Benson, Carlson, and Parker (see Benson [84a] for references and further results).

Let  $k$  be part of a  $p$ -modular system  $(K, R, k)$ , with  $K$  a subfield of  $\mathbf{C}$ . In this situation, the  $\mathbf{C}$ -algebra homomorphisms from  $A(kG)$  to  $\mathbf{C}$ , called species, give a new interpretation of Brauer characters. The idea is that for each  $p'$ -element  $x \in G$ , we obtain a species  $b_x$ , defined by setting  $b_x(V) = \varphi_V(x)$ , for each  $kG$ -module  $V$ , where  $\varphi_V$  is the Brauer character of  $V$ . When the group algebra  $kG$  is of finite representation type, the representation algebra  $A(kG)$  is semisimple, and the species separate elements of  $A(kG)$ . A startling development is that, when the Sylow  $p$ -subgroups of  $G$  are not cyclic, the algebra  $A(kG)$  may have nonzero nilpotent elements, so the species do not separate elements in general (see §§81E, F). Section 81 also contains an induction theorem of Conlon, and a construction of a set of dual elements in  $A(kG)$  with respect to certain bilinear forms, by a nice application of Auslander-Reiten sequences (from §78).

Representation rings have been applied in topology to the study of the

classifying space  $B_G$  of a finite group  $G$ . The first step in this direction was taken by Atiyah [61], who constructed an isomorphism from the algebra  $K^*(B_G)$  (defined by complex vector bundles over  $B_G$ ) to the completion of the character ring  $\text{ch } G$  with respect to the topology defined by the powers of its augmentation ideal. Another result, linking the stable homotopy of  $B_G$  with a suitable completion of the Burnside ring, has been obtained by G. Carlsson [84] (see also Adams-Gunawardena-Miller [85]).

## §80. PERMUTATION REPRESENTATIONS AND BURNSIDE RINGS

The concept of a finite group  $G$  acting as a group of permutations on a finite set  $S$  arises naturally in many applications of group theory. We have already met this idea in §§1, 10, and 11. Of course, a permutation representation of  $G$  can be described by permutation matrices with entries in a field or a commutative ring. However, permutation representations have various formal properties that are independent of the choice of ground ring. These properties may be viewed as the framework of a number of standard constructions in representation theory over fields or rings. This connection will be made explicit in the discussion to follow, when we develop the formal properties of permutation representations.

As in §1, a *G-set* is a finite set  $S$  on which a finite group  $G$  acts (from the left) as a group of permutations. In studying  $G$ -sets for a given group  $G$ , it is convenient to introduce the *Burnside ring*  $\Omega(G)$  consisting of formal sums and differences of  $G$ -sets. This procedure is analogous to the step from characters of  $G$  to the character ring  $\text{ch } FG$  over some field  $F$ .

Throughout this section,  $G$  denotes a finite group, and  $H, K$  denote subgroups of  $G$ . For a pair of  $G$ -sets  $S$  and  $T$ , we let  $S \dot{\cup} T$  be their disjoint union, and  $S \times T$  their cartesian product.

### §80A. Burnside Rings

Throughout, let  $G$  be a finite group. After defining various operations on  $G$ -sets, we shall introduce the Burnside ring  $\Omega(G)$  consisting of formal  $\mathbb{Z}$ -linear combinations of  $G$ -sets. We shall discuss the structure of the ring  $\Omega(G)$ . The results in this subsection are due mainly to Burnside, A. Dress, and L. Solomon, and our treatment follows the approach in Dress-Küchler [70] and Dress [71].

A (*left*) *G-set* is a finite set  $S$  on which  $G$  acts from the left as a group of permutations (see (1.18)–(1.21)). For  $H \leq G$ , the collection  $G/H$  of left cosets  $\{yH\}$  of  $H$  in  $G$  is a transitive  $G$ -set, and indeed every transitive  $G$ -set is isomorphic to  $G/H$  for some  $H$  (see (1.20)). Let  $e_G$  denote the  $G$ -set consisting of a single element, also denoted by  $e_G$ , with  $xe_G = e_G$  for all  $x \in G$ . Clearly  $e_G \cong G/G$  as  $G$ -sets.

Given arbitrary  $G$ -sets  $S$  and  $T$ , we may form their disjoint union  $S \dot{\cup} T$  and their cartesian product  $S \times T$ , both of which are  $G$ -sets. The action of  $G$  on

$S \times T$  is defined by

$$x(s, t) = (xs, xt) \quad \text{for } x \in G, \quad s \in S, \quad t \in T.$$

View  $S \dot{\cup} T$  as the “sum,” and  $S \times T$  as the “product,” of the  $G$ -sets  $S$  and  $T$ .

By definition, a  $G$ -map  $f: S \rightarrow T$  is a set map such that

$$f(xs) = xf(s) \quad \text{for all } x \in G, \quad s \in S.$$

Let  $\text{Hom}_G(S, T)$  denote the collection of all such maps  $f: S \rightarrow T$ . Note that  $\text{Hom}_G(S, T)$  is not in general a  $G$ -set. We write  $S \cong T$  if there is a  $G$ -bijection from  $S$  onto  $T$ .

For each element  $s$  in a  $G$ -set  $S$ , its *orbit*  $Gs = \{xs : x \in G\}$  is the smallest  $G$ -set containing  $s$ . Then  $S$  is uniquely expressible as a disjoint union of its distinct  $G$ -orbits. For  $s \in S$ , its *stabilizer* is defined by

$$G_s = \{x \in G : xs = s\} \leq G.$$

By (1.20), the orbit of  $s$  is isomorphic to the left coset space  $G/G_s$  as  $G$ -sets.

By definition, a *simple*  $G$ -set is a nonempty  $G$ -set with no proper  $G$ -subsets. It must consist of a single orbit, and hence is a left coset space  $G/H$  for some  $H \leq G$ . Conversely, each  $G/H$  is simple.

**(80.1) Definition.** The *Burnside ring*  $\Omega(G)$  of a finite group  $G$  is the abelian group generated by symbols  $[S]$ , one for each isomorphism class of finite  $G$ -sets  $S$ , with relations

$$(80.2) \quad [S \dot{\cup} T] = [S] + [T] \quad \text{for } S, T \text{ } G\text{-sets.}$$

Multiplication is defined by

$$(80.3) \quad [S][T] = [S \times T] \quad \text{for } S, T \text{ } G\text{-sets,}$$

extended to  $\Omega(G)$  by linearity. Then  $\Omega(G)$  is a commutative ring with identity element  $[e_G]$ .

To be more precise,  $\Omega(G)$  is defined in a manner similar to (16.3), where we introduced the Grothendieck group of a category of modules. In the present case, we define  $\Omega(G) = \mathbf{F}/\mathbf{F}_0$ , where  $\mathbf{F}$  is the free abelian group generated by symbols  $(S)$ , one for each isomorphism class of  $G$ -sets  $S$ , and where  $\mathbf{F}_0$  is the subgroup of  $\mathbf{F}$  generated by all expressions  $(S \dot{\cup} T) - (S) - (T)$ . Then  $\Omega(G)$  is an abelian additive group. Defining multiplication as in (80.3) on the generators of  $\mathbf{F}$ , we see easily that  $\mathbf{F}_0$  is an ideal of  $\mathbf{F}$ , and therefore  $\Omega(G)$  has a well-defined ring structure. Since  $S \times T \cong T \times S$  for any  $G$ -sets  $S$  and  $T$ , it is clear that the ring  $\Omega(G)$  is commutative. Furthermore,  $e_G \times T \cong T$  for each  $G$ -set  $T$ , so  $[e_G]$  is the identity element of  $\Omega(G)$ .

We prove at once:

**(80.4) Lemma.** *Let  $S, T$  be  $G$ -sets. Then  $[S] = [T]$  in  $\Omega(G)$  if and only if  $S \cong T$  as  $G$ -sets.*

*Proof.* If  $[S] = [T]$  in  $\Omega(G)$ , then  $S \dot{\cup} X \cong T \dot{\cup} X$  for some  $G$ -set  $X$  (see proof of (38.20)). We must show that  $S \cong T$ . Let  $\{S_1, \dots, S_k\}$  be a full set of nonisomorphic simple  $G$ -sets. From the orbit decomposition of  $S$ , it follows that

$$S \cong S_1^{(n_1)} \dot{\cup} \dots \dot{\cup} S_k^{(n_k)},$$

where  $S_i^{(n_i)}$  denotes the disjoint union of  $n_i$  copies of  $S_i$ . The isomorphism class of  $S$  uniquely determines the  $k$ -tuple  $(n_1, \dots, n_k)$ . Therefore, if  $S \dot{\cup} X \cong T \dot{\cup} X$ , then  $S$  and  $T$  must have the same orbit structure, so  $S \cong T$ , as claimed. Conversely,  $S \cong T$  implies  $[S] = [T]$ , and the lemma is proved.

(We have in fact shown that  $[S_1], \dots, [S_k]$  is a free  $\mathbb{Z}$ -basis of  $\Omega(G)$ ; compare the above argument with the proof of (16.6).)

Some notation will be needed for the discussion to follow. Let  $H, K$  denote subgroups of the finite group  $G$ . As in §1, call  $H$  and  $K$   $G$ -conjugate (notation:  $H =_G K$ ) if  $x^{-1}Hx = K$  for some  $x \in G$ . Also, if  $x^{-1}Hx \subseteq K$  for some  $x \in G$ , we write  $H \leq_G K$ , and say that  $H$  is subconjugate to  $K$ .

Now let  $\mathcal{S} = \mathcal{S}(G)$  be a full set of nonconjugate subgroups of  $G$ . We intend to show that the  $G$ -sets  $\{G/H : H \in \mathcal{S}\}$  form a  $\mathbb{Z}$ -basis of  $\Omega(G)$ , and the only difficulty in proving this lies in showing that if  $G/H \cong G/K$ , then necessarily  $H =_G K$ . For this purpose, we need the concept (already encountered in §10E) of the  $G$ -invariant subset  $\text{inv}_G(S)$  of a  $G$ -set  $S$ . We define

$$\text{inv}_G(S) = \{s \in S : xs = s \text{ for all } x \in G\}.$$

We now establish:

**(80.5) Proposition.** *Let  $H$  and  $K$  be subgroups of  $G$ , and let  $S$  be any  $G$ -set. Then*

- (i) *There is a bijection*

$$\text{Hom}_G(G/H, S) \leftrightarrow \text{inv}_H(S).$$

- (ii) *There is a bijection*

$$\text{Hom}_G(G/H, G/K) \leftrightarrow \text{inv}_H(G/K).$$

Further,  $\text{inv}_H(G/K) = \{xK : x \in G, x^{-1}Hx \leq K\}$ .

- (iii)  $\text{inv}_H(G/K) = \emptyset$  unless  $H \leq_G K$ .

- (iv)  $G/H \cong G/K$  as  $G$ -sets if and only if  $H =_G K$ .

*Proof.* (i) Each  $f \in \text{Hom}_G(G/H, S)$  maps the  $H$ -trivial element  $1 \cdot H \in G/H$  onto an  $H$ -trivial element  $s_0 \in S$ . Further,  $f$  is completely determined by  $s_0$ , since  $f(xH) = xs_0$  for all  $x \in G$ . The correspondence  $f \leftrightarrow s_0$  gives the desired bijection.

(ii) Taking  $S = G/K$  in (i), we note that the left coset  $xK$  is  $H$ -invariant if and only if  $H \cdot xK = xK$ , that is,  $x^{-1}Hx \leq K$ . This establishes (ii), as well as (iii).

(iii) If  $H =_G K$ , write  $K = xHx^{-1}$  with  $x \in G$ . Then there is a  $G$ -isomorphism  $\theta: G/K \cong G/H$ , given by

$$\theta(gK) = \theta(gxHx^{-1}) = gxH, \quad \text{for } g \in G.$$

Conversely, suppose that  $G/H \cong G/K$ . Then  $\text{Hom}_G(G/H, G/K) \neq \emptyset$ , so  $H \leq_G K$  by (iii). Therefore  $H =_G K$  by symmetry, and the proposition is proved.

As an immediate consequence of (80.5iv) and our earlier remarks, we have:

**(80.6) Corollary.** *Let  $\mathcal{S}$  be a full set of nonconjugate subgroups of  $G$ . Then*

$$\Omega(G) = \bigoplus_{H \in \mathcal{S}} \mathbb{Z}[G/H].$$

Now let  $H$  be a subgroup of  $G$ . If  $S$  and  $T$  are  $G$ -sets, it is clear that

$$\begin{aligned} \text{inv}_H(S \cup T) &= \text{inv}_H(S) \cup \text{inv}_H(T), \\ \text{inv}_H(S \times T) &= \text{inv}_H(S) \times \text{inv}_H(T). \end{aligned}$$

These formulas suggest that we introduce a map

$$(80.7) \quad \varphi_H: \Omega(G) \rightarrow \mathbb{Z}, \text{ defined by } \varphi_H[S] = |\text{inv}_H(S)|, \quad S = G\text{-set}.$$

It is easily seen that  $\varphi_H$  is well defined. The preceding formulas show that, in fact, the map  $\varphi_H$  is a ring homomorphism.

If  $H$  and  $K$  are  $G$ -conjugate, it is easily shown that  $\varphi_H = \varphi_K$ . In fact, for any  $x \in G$  and any  $G$ -set  $S$ , we have

$$s \in \text{inv}_H(S) \Leftrightarrow xs \in \text{inv}_{xHx^{-1}}(S).$$

Therefore  $\varphi_H = \varphi_K$  whenever  $H =_G K$ . As we shall see below in (80.19), the converse also holds.

Let  $H \leq G$ ; using (80.5ii) with  $K = H$ , we have

$$(80.8) \quad \varphi_H[G/H] = |N_G(H):H|,$$

where  $N_G(H)$  is the normalizer of  $H$  in  $G$ . Further, (80.5iii) gives

$$(80.9) \quad \varphi_H[G/K] \neq 0 \Leftrightarrow H \leq_G K.$$

We shall use the above formulas to prove that the collection of ring homomorphisms  $\{\varphi_H : H \in \mathcal{S}(G)\}$ , from  $\Omega(G)$  to  $\mathbb{Z}$ , suffice to distinguish the elements of the Burnside ring  $\Omega(G)$  from one another. To be explicit, we shall establish:

**(80.10) Theorem (Burnside).** *Let  $S$  and  $T$  be  $G$ -sets, and let  $\mathcal{S}$  be a full set of nonconjugate subgroups of  $G$ . Then  $S \cong T$  if and only if  $\varphi_H[S] = \varphi_H[T]$  for all  $H \in \mathcal{S}$ .*

*Proof.* The result is obvious in one direction, so now assume that  $\varphi_H[S] = \varphi_H[T]$  for all  $H \in \mathcal{S}$ , and let us prove that  $S \cong T$ . We may write

$$[S] = \sum m_i [G/H_i], \quad [T] = \sum n_i [G/H_i], \quad m_i, n_i \in \mathbb{Z},$$

where  $H_i$  ranges over all elements of  $\mathcal{S}$ . We must prove that  $m_i = n_i$  for each  $i$ . Suppose this is false, and let

$$\mathcal{S}_0 = \{H_i \in \mathcal{S} : m_i \neq n_i\}.$$

Partially order  $\mathcal{S}$  with respect to  $\leq_G$ , and let  $H_0$  be a maximal element of  $\mathcal{S}_0$ . By (80.9),

$$(*) \quad \varphi_{H_0}[G/H] = 0 \quad \text{for all } H \in \mathcal{S}_0 \text{ different from } H_0.$$

Since  $\varphi_{H_0}[S] = \varphi_{H_0}[T]$  by hypothesis, and since  $m_i = n_i$  whenever  $H_i \notin \mathcal{S}_0$ , we obtain

$$\sum_{H_i \in \mathcal{S}_0} m_i \varphi_{H_0}[G/H_i] = \sum_{H_i \in \mathcal{S}_0} n_i \varphi_{H_0}[G/H_i].$$

Using (\*) above, it follows that  $m_0 \varphi_{H_0}[G/H_0] = n_0 \varphi_{H_0}[G/H_0]$ , and therefore  $m_0 = n_0$  because  $\varphi_{H_0}[G/H_0] \neq 0$  by (80.9). But  $m_0 \neq n_0$  because  $H_0 \in \mathcal{S}_0$ , so we have obtained a contradiction. Thus  $\mathcal{S}_0$  is empty, and  $m_i = n_i$  for each  $H_i \in \mathcal{S}$ . Therefore  $S \cong T$  as claimed, and the proof is complete.

We shall now combine all of the ring homomorphisms  $\{\varphi_H : H \in \mathcal{S}\}$  into a single homomorphism  $\varphi$ . Let

$$\mathcal{S}(G) = \{H_1, \dots, H_m\},$$

and define

$$(80.11) \quad \varphi : \Omega(G) \rightarrow \mathbb{Z}^{(m)} \quad \text{by} \quad \varphi[S] = (\varphi_{H_1}[S], \dots, \varphi_{H_m}[S]), \quad S = G\text{-set}.$$

Then  $\varphi$  is a ring homomorphism, and  $\varphi[e_G]$  is the identity element of the ring  $\mathbb{Z}^{(m)}$ . We now prove:

**(80.12) Proposition.** *The map  $\varphi: \Omega(G) \rightarrow \mathbb{Z}^{(m)}$ , defined above, is a ring monomorphism. Its image is a full\*  $\mathbb{Z}$ -lattice in  $\mathbb{Z}^{(m)}$ . Further, the  $m$  functions  $\{\varphi_H: 1 \leq i \leq m\}$  are linearly independent over  $\mathbb{Z}$ .*

*Proof.* To show that  $\varphi$  is a monomorphism, suppose that  $S$  and  $T$  are  $G$ -sets, and that  $\varphi[S] = \varphi[T]$ . Then  $\varphi_H[S] = \varphi_H[T]$  for all  $H \in \mathcal{S}$ , and therefore  $S \cong T$  by Burnside's Theorem 80.10. This proves that  $\varphi$  is a monomorphism. Since  $\Omega(G)$  is  $\mathbb{Z}$ -free of rank  $m$ , so is  $\text{im}(\varphi)$ , and thus  $\text{im}(\varphi)$  is a full  $\mathbb{Z}$ -sublattice of  $\mathbb{Z}^{(m)}$ . Finally, the maps  $\{\varphi_H: H \in \mathcal{S}\}$  must be linearly independent over  $\mathbb{Z}$ , since otherwise  $\text{im}(\varphi)$  cannot have  $\mathbb{Z}$ -rank  $m$ .

For the above-defined  $\varphi: \Omega(G) \rightarrow \mathbb{Z}^{(m)}$ , the cokernel of  $\varphi$  is a  $\mathbb{Z}$ -torsion module. Therefore  $\varphi$  induces an isomorphism of  $\mathbb{Q}$ -algebras

$$(80.13) \quad \mathbb{Q} \otimes_{\mathbb{Z}} \Omega(G) \cong \mathbb{Q}^{(m)}.$$

This result was first proved by Solomon [67]; it shows in particular that  $\mathbb{Q} \otimes_{\mathbb{Z}} \Omega(G)$  is a semisimple  $\mathbb{Q}$ -algebra.

For  $H \leq G$ , we set

$$(80.14) \quad H^* = \coprod_{K \in \mathcal{S}(G)} \frac{\varphi_K[G/H]}{\varphi_H[G/H]} \in \mathbb{Z}^{(m)}.$$

(By Exercise 80.4,  $H^*$  is indeed an element of  $\mathbb{Z}^{(m)}$ .) We prove next:

**(80.15) Proposition.** *The elements  $\{H^*: H \in \mathcal{S}(G)\}$  form a free  $\mathbb{Z}$ -basis of  $\mathbb{Z}^{(m)}$ .*

*Proof.* Let  $\Omega^* = \sum_{H \in \mathcal{S}} \mathbb{Z} \cdot H^*$ . Since there are  $m$  elements  $H^*$ , we need only show that  $\Omega^* = \mathbb{Z}^{(m)}$ . Let  $\{\delta_1, \dots, \delta_m\}$  be a standard basis of  $\mathbb{Z}^{(m)}$ , so  $\delta_i$  is the  $m$ -tuple with 1 at position  $i$  and zeros elsewhere. If  $\Omega^* \subset \mathbb{Z}^{(m)}$ , let  $H_r \in \mathcal{S}$  be a minimal element of  $\mathcal{S}$  such that  $\delta_r \notin \Omega^*$ ; here, we view  $\mathcal{S}$  as partially ordered with respect to  $\leq_G$ , as usual. Then  $\delta_i \in \Omega^*$  for all  $H_i \in (H_r)^-$ , where  $(H_r)^-$  consists of all  $H \in \mathcal{S}$  that are conjugate to proper subgroups of  $H_r$ .

By (80.9),  $H^*$  has nonzero  $K$ -th component if and only if  $K \leq_G H$ , and  $H^*$  obviously has  $H$ -th component 1. Therefore

$$H_r^* = \delta_r + \sum_{H_i \in (H_r)^-} \alpha_i \delta_i, \quad \alpha_i \in \mathbb{Z}.$$

But each  $\delta_i$  occurring in the summation lies in  $\Omega^*$ , and so does  $H_r^*$ . Therefore also  $\delta_r \in \Omega^*$ , which is a contradiction. This completes the proof.

**(80.16) Corollary.** *Let  $n \in \mathbb{Z}$ . Then  $n \cdot \mathbb{Z}^{(m)} \subseteq \varphi\{\Omega(G)\}$  if and only if and only if  $n \equiv 0 \pmod{|G|}$ .*

\*If  $A$  is a free  $\mathbb{Z}$ -module on  $m$  generators, a full  $\mathbb{Z}$ -lattice in  $A$  is a  $\mathbb{Z}$ -submodule that also has  $m$  free generators.

*Proof.* We have

$$\mathbb{Z}^{(m)} = \bigoplus_{H \in \mathcal{S}} \mathbb{Z} H^*, \quad \varphi\{\Omega(G)\} = \bigoplus_{H \in \mathcal{S}} \mathbb{Z} \cdot \varphi[G/H],$$

while for each  $H \leq G$ ,

$$\varphi[G/H] = \varphi_H[G/H] \cdot H^*.$$

Therefore  $n \cdot \text{cok } \varphi = 0$  if and only if  $n$  is a multiple of  $\varphi_H[G/H]$  for each  $H \in \mathcal{S}$ . But  $\varphi_H[G/H] = |N_G(H):H|$ , which equals  $|G|$  for  $H = 1$ , and otherwise is a divisor of  $|G|$ . This implies the result.

The above techniques allow one to find a full set of primitive orthogonal idempotents in  $\mathbb{Q} \otimes_{\mathbb{Z}} \Omega(G)$ ; for details, see Gluck [81].

We turn next to the question of finding all prime ideals of  $\Omega(G)$ , and begin with an analogue of Mackey's Tensor Product Theorem for  $G$ -sets:

**(80.17) Proposition.** *Let  $H \leq G$ , and let  $S$  be any  $G$ -set. Define*

$$H^- = \{K \in \mathcal{S}(G) : K <_G H\},$$

so  $H^-$  does not include the subgroup  $H$  itself. Then in  $\Omega(G)$  we have

$$(80.18) \quad [G/H][S] = \varphi_H[S] \cdot [G/H] + \sum_{K \in H^-} n_K[G/K]$$

for some nonnegative integers  $\{n_K\}$ .

*Proof.* By definition of multiplication in the Burnside ring  $\Omega(G)$ , we have

$$(*) \quad [G/H][S] = [(G/H) \times S] = \sum_{K \in \mathcal{S}} n_K[G/K]$$

for some nonnegative integers  $\{n_K\}$ . For fixed  $K_0 \in \mathcal{S}$ , we apply  $\varphi_{K_0}$  to both sides of the preceding equation, obtaining

$$\varphi_{K_0}[G/H] \cdot \varphi_{K_0}[S] = \sum_K n_K \varphi_{K_0}[G/K] \geq 0.$$

Strict inequality holds whenever  $n_{K_0} > 0$ , and in that case we must have  $\varphi_{K_0}[G/H] \neq 0$ ; but by (80.9), this implies that either  $K_0 = H$  or else  $K_0 \in H^-$ . Equation  $(*)$  now becomes

$$[G/H][S] = \varphi_H[G/H] + \sum_{K \in H^-} n_K[G/K],$$

and it remains for us to calculate the integer  $n_H$ . Apply  $\varphi_H$  to the above equation;

by (81.9),  $\varphi_H[G/K] = 0$  for each  $K \in H^-$ , so we get

$$\varphi_H[G/H]\varphi_H[S] = n_H\varphi_H[G/H].$$

Since  $\varphi_H[G/H] \neq 0$  by (80.8), we have  $n_H = \varphi_H[S]$ , which completes the proof.

**(80.18) Corollary.** *Let  $R$  be an integral domain, and let  $\theta: \Omega(G) \rightarrow R$  be a ring homomorphism. Then there exists a subgroup  $H$  of  $G$  such that*

$$(80.19) \quad \theta[S] = \varphi_H[S] \cdot 1_R \quad \text{for each } G\text{-set } S.$$

*Proof.* Partially order  $\mathcal{S}$  with respect to  $\leq_G$ , and let  $H \in \mathcal{S}$  be minimal such that  $\theta[G/H] \neq 0$ ; then  $\theta[G/K] = 0$  for  $K \in H^-$ . Applying  $\theta$  to both sides of (80.18), we obtain (80.19) at once.

If  $R$  is an integral domain of characteristic zero, and if  $H$  and  $H'$  are subgroups of  $G$  giving rise to a pair of ring homomorphisms  $\theta$  and  $\theta'$  from  $\Omega(G)$  into  $R$ , then we may conclude from Burnside's Theorem 80.10 that  $\theta = \theta'$  if and only if  $H$  is  $G$ -conjugate to  $H'$ . The situation changes drastically when  $R$  is a domain of characteristic  $p$ , where  $p$  is a positive prime.

In the discussion below,  $p$  denotes either a rational prime number or zero. The prime ideals of the Burnside ring  $\Omega(G)$  are precisely the kernels of ring homomorphisms from  $\Omega(G)$  into an integral domain. Each ring homomorphism is given by a map  $\theta$  as in (80.19), for some  $H \leq G$ . This suggests that for each  $H \leq G$  and each  $p$ , we should consider the ideal

$$(80.20) \quad I(H, p) = \{x \in \Omega(G) : \varphi_H(x) \equiv 0 \pmod{p}\}.$$

Each such  $I(H, p)$  is then necessarily a prime ideal of  $\Omega(G)$ , since obviously  $I(H, p)$  is a proper ideal of  $\Omega(G)$  because  $[e_G] \notin I(H, p)$ . We now prove:

**(80.21) Proposition (Dress).** *The prime ideals of the Burnside ring  $\Omega(G)$  are precisely the ideals  $I(H, p)$  defined in (80.20), where  $p$  is either a rational prime or else  $p = 0$ .*

*Proof.* By virtue of the preceding discussion, we need only show that every prime ideal  $P$  of  $\Omega(G)$  is of the form  $I(H, p)$  for some  $H$  and  $p$ . But the natural map  $\Omega(G) \rightarrow \Omega(G)/P = R$  is a ring homomorphism, and hence is of the form (80.19) for some  $H \leq G$ . This map carries  $x \in \Omega(G)$  onto  $\varphi_H(x) \cdot 1_R$ . If  $R$  has characteristic  $p$ , the kernel of the map is precisely  $I(H, p)$ . Therefore  $P = I(H, p)$ , as claimed, and the result is proved.

Following Dress [71], we now consider the question as to when two prime ideals  $I(H, p)$  and  $I(K, q)$  of  $\Omega(G)$  coincide. Since  $p$  is the characteristic of the factor ring  $\Omega(G)/I(H, p)$ , it follows that necessarily  $p = q$ . We must therefore decide

under which conditions it happens that  $I(H, p) = I(K, p)$ . The case  $p = 0$  is straightforward:

**(80.22) Proposition.** *The prime ideals  $I(H, 0)$  and  $I(K, 0)$  of  $\Omega(G)$  coincide if and only if  $H =_G K$ , or equivalently,  $\varphi_H = \varphi_K$ .*

*Proof.* We have already seen that

$$H =_G K \Rightarrow \varphi_H = \varphi_K \Rightarrow I(H, 0) = I(K, 0).$$

Conversely, suppose that  $I(H, 0) = I(K, 0)$ . Then for  $x \in \Omega(G)$ ,

$$\varphi_H(x) = 0 \Leftrightarrow \varphi_K(x) = 0.$$

But  $\varphi_H[G/H] \neq 0$  by (80.8), so  $\varphi_K[G/H] \neq 0$ , and therefore  $K \leq_G H$  by (80.9). By symmetry, we obtain  $H \leq_G K$ , so  $H$  and  $K$  must be  $G$ -conjugate. This completes the proof.

Now let  $p > 0$ , and denote by  $H^{(p)}$  the smallest normal subgroup of  $H$  whose index is a power of  $p$ . Then  $H^{(p)}$  is a uniquely determined characteristic subgroup of  $H$ . We now state without proof (see Dress [71] and Dress-Küchler [70]):

**(80.23) Dress's Theorem.** *Let  $p > 0$  be prime. The following are equivalent:*

- (i)  $\varphi_H \equiv \varphi_K \pmod{p}$ , that is,  $\varphi_H[S] \equiv \varphi_K[S] \pmod{p}$  for each  $G$ -set  $S$ .
- (ii)  $I(H, p) = I(K, p)$ .
- (iii)  $H^{(p)}$  is  $G$ -conjugate to  $K^{(p)}$ .

## Notes

(i) Using (80.23), Dress showed that the prime spectrum of the ring  $\Omega(G)$  is connected if and only if  $G$  is solvable. This leads to the tantalizing result:  $G$  is solvable and of odd order if and only if the only units in  $\Omega(G)$  are  $\pm 1$ . For details, see Dress-Küchler [70].

(ii) For further results on Burnside rings, see Gustafson [77], Li [74], Gluck [81], Matsuda [82], and Yoshida [83].

## §80B. $G$ -Sets and Induction Maps

Keeping the notation of §80A, let  $G$  be a finite group and  $S$  a left  $G$ -set. Given a commutative ring  $R$ , let  $R[S]$  be the *permutation module* having as  $R$ -basis the elements of  $S$ , on which  $G$  acts as permutation group. We may view  $R[S]$  as a left  $RG$ -module, in an obvious way. There is a close analogy between the theory of permutation modules and the theory of  $G$ -sets. Certain standard concepts, such as restriction, induction, the Mackey theorems, and Frobenius

reciprocity, apply equally well to modules and to  $G$ -sets. In a sense, the theory of  $G$ -sets is more fundamental, and underlies many proofs that depend on manipulations in the lattice of subgroups of  $G$ . For example, the Burnside ring  $\Omega(G)$  is the basic instance of a Frobenius functor, and character rings, Grothendieck groups, etc. are modules over  $\Omega(G)$ .

In this subsection, we develop Dress's theory of  $G$ -sets, following the treatment in Dress-Küchler [70] and Dress [71]. We shall occasionally omit details of proofs, especially in those cases where the module analogue is already familiar to the reader.

Let  $H \leq G$ , and let  $S$  be a  $G$ -set. By restriction of operators from  $G$  to  $H$ , we obtain an  $H$ -set  $\text{res}_H^G S$ , the *restriction* of  $S$ , also denoted by  $S_H$  for brevity. On the other hand, for each  $H$ -set  $T$ , we define an *induced*  $G$ -set  $\text{ind}_H^G T$  (or  $T^G$  for brevity), as follows. We make the cartesian product  $G \times T$  into a left  $H$ -set by setting

$$h(g, t) = (gh^{-1}, ht) \quad \text{for } h \in H, \quad g \in G, \quad t \in T.$$

The  $H$ -orbit  $H \cdot (g, t)$  thus consists of all pairs  $\{(gh^{-1}, ht) : h \in H\}$ . Denote by  $G \times_H T$  the set of  $H$ -orbits in  $G \times T$ , and make  $G \times_H T$  into a left  $G$ -set by defining

$$g' \cdot (\text{orbit of } (g, t)) = \text{orbit of } (g'g, t) \quad \text{for } g, g' \in G, \quad t \in T.$$

Now define  $\text{ind}_H^G T = G \times_H T$ , the  $G$ -set *induced* from  $T$ .

From the viewpoint of permutation modules, the above construction is quite natural. Given an  $H$ -set  $T$  and a commutative ring  $R$ , we form the  $RH$ -permutation module  $R[T]$ . The induced  $RG$ -module is given by  $RG \otimes_{RH} R[T]$ , and clearly we have

$$RG \otimes_{RH} R[T] \cong R[\text{ind}_H^G T] \quad \text{for each } H\text{-set } T.$$

The basic properties of the restriction and induction maps on sets are as follows:

**(80.24) Proposition.** *Let  $H \leq G$ . Then*

- (i) *The restriction and induction maps are additive on disjoint unions of sets.*
- (ii) *Let  $H \leq E \leq G$ , and let  $S$  be an  $H$ -set. Then*

$$G \times_E (E \times_H S) \cong G \times_H S \text{ as } G\text{-sets,}$$

*that is, induction is transitive. Likewise, restriction is transitive.*

- (iii) *If  $e_H$  is the 1-point  $H$ -set, then*

$$G \times_H e_H \cong G/H \text{ as left } G\text{-sets.}$$

The proof is left as exercise for the reader. It follows from the above that

for  $H \leq G$ , there are additive homomorphisms

$$\text{res}_H^G: \Omega(G) \rightarrow \Omega(H), \quad \text{ind}_H^G: \Omega(H) \rightarrow \Omega(G),$$

defined via restriction of  $G$ -sets and induction of  $H$ -sets, respectively. Note that  $\text{res}_H^G$  is a ring homomorphism, but  $\text{ind}_H^G$  is not (unless  $H = G$ ).

We now consider the analogues of the Frobenius Reciprocity Theorems. Let  $H \leq G$ , and let  $L$  and  $M$  be  $RG$ - and  $RH$ -modules, respectively, where  $R$  is a commutative ring. In (10.8) and (10.21) we showed that

(80.25)

$$\text{Hom}_{RG}(M^G, L) \cong \text{Hom}_{RH}(M, L_H), \quad \text{Hom}_{RG}(L, M^G) \cong \text{Hom}_{RH}(L_H, M).$$

The analogue of the first isomorphism is straightforward:

**(80.26) Proposition.** *Let  $H \leq G$ , and let  $S$  be an  $H$ -set, and  $T$  a  $G$ -set. Then there is a set bijection*

$$\text{Hom}_G(S^G, T) \cong \text{Hom}_H(S, T_H).$$

*Proof.* It suffices to treat the case where  $S$  is a simple  $H$ -set, so let  $S = H/E$ , where  $E \leq H$ . Then

$$S^G = G \times_H (H/E) = G \times_H (H \times_E e_E) \cong G/E.$$

Therefore  $\text{Hom}_G(S^G, T) \cong \text{Hom}_G(G/E, T) \cong \text{inv}_E T$  by (80.5). But also  $\text{Hom}_H(H/E, T_H) \cong \text{inv}_E T_H$  by (80.5), and the result follows.

The  $G$ -set version of the second isomorphism in (80.25) is more complicated, and will involve the concept of tensor induction defined in §13A. We postpone this discussion to §80C.

We shall now consider the  $G$ -set analogues of the Mackey theorems, using the ordinary restriction and induction maps defined as in (80.24). Let  $H \leq G$ , let  $S$  be an  $H$ -set, and  $T$  a  $G$ -set; for convenience of notation, write

$$S^G = \text{ind}_H^G S, \quad T_H = \text{res}_H^G T,$$

when there is no danger of confusion. Then we have:

**(80.27) Subgroup Theorem.** *Let  $H, K \leq G$ , and let  $S$  be an  $H$ -set. Then*

$$(S^G)_K \cong \bigcup_{G = \cup KaH} (^aS|_{aH \cap K})^K \text{ as left } K\text{-sets.}$$

*The union is taken over all  $(K, H)$ -double cosets  $KaH$  of  $G$ , and for  $a \in G$ ,  ${}^aS$  denotes the  ${}^aH$ -set defined by conjugation.*

*Proof.* This follows from the proof of Mackey's Subgroup Theorem 10.13, by calculating the  $K$ -orbits and stabilizers of elements in  $S^G$ . The reader may verify the details as an exercise. For the special case where  $S = e_H$ , see Exercise 80.8.

In a similar manner, we obtain the  $G$ -set analogue of Mackey's Tensor Product Theorem 10.18, and again we omit the proof:

**(80.28) Tensor Product Theorem.** *Let  $H_i \leq G$  and let  $S_i$  be an  $H_i$ -set,  $i = 1, 2$ . Then*

$$S_1^G \times S_2^G \cong \bigcup_{x^{-1}y \in D} (({}^x S_1 \times {}^y S_2)|_{xH_1 \cap {}^y H_2})^G,$$

where  $D$  ranges over all  $(H_1, H_2)$ -double cosets of  $G$ . There is one summand for each  $D$ , namely, we may choose any pair of elements  $x, y \in G$  such that  $x^{-1}y \in D$ .

Note that Exercise 80.2 is a special case of the above result. Another special case, which is needed to show that  $\Omega(G)$  is a Frobenius functor, is the analogue of (10.20), namely:

**(80.29) Frobenius Reciprocity Theorem.** *Let  $H \leq G$ , and let  $S$  be an  $H$ -set,  $T$  a  $G$ -set. Then*

$$S^G \times T \cong (S \times T_H)^G \text{ as } G\text{-sets.}$$

Starting with the concept of Frobenius functors, Green [71] introduced a somewhat richer axiomatic theory, which includes the idea of conjugation within a group  $G$ , and the analogue of Mackey's Subgroup Theorem 10.13. Further, instead of considering all finite groups  $G$  simultaneously, we focus our attention on the set of subgroups of a given group  $G$ .

We begin with a preliminary definition. Let  $R$  be a commutative ring, and  $F$  an  $R$ -module. A *pairing* is an  $R$ -bilinear map  $F \times F \rightarrow F$ ; the image of  $(x, y) \in F \times F$  is called the *product*  $xy$ . In general, we do not assume that this multiplication is commutative, or even associative, and there need not be an identity element. We call  $F$  a *multiplicative  $R$ -module*. (For example, every additive group is a multiplicative  $\mathbb{Z}$ -module, with all products zero. As another example, one can take the cohomology ring of a group, with multiplication given by cup products.)

**(80.30) Definition.** Let  $G$  be a finite group, and  $R$  a commutative ring. A  *$G$ -functor* (over  $R$ ) consists of the data:

- (i) A correspondence  $F$  that assigns to each  $H \leq G$  a multiplicative  $R$ -module  $F(H)$ .

(ii) For  $E \leq H \leq G$ , there are maps

$$\text{res}_E^H : F(H) \rightarrow F(E), \quad \text{ind}_E^H : F(E) \rightarrow F(H),$$

which are transitive, and such that  $\text{res}_H^H = \text{ind}_H^H = 1$ .

(iii) For each  $H \leq G$  and each  $g \in G$ , let  $H^g = g^{-1}Hg$ . There is an isomorphism (called *conjugation*)

$$C_g^H : F(H) \cong F(H^g),$$

such that for  $g, g' \in G$  and  $h \in H$ ,

$$C_{g'}^{H^g} \cdot C_g^H = C_{gg'}^H, \quad \text{and} \quad C_h^H = 1.$$

(iv) The restriction and induction maps satisfy the Frobenius identities (see (38.1.iv)) and commute with conjugation.

(v) (Mackey condition.) Let  $K \leq G$ , and let  $E, H \leq K$ . Set

$$K = \bigcup_{i=1}^n Eg_iH, \quad \text{and} \quad E_i = E \cap g_iHg_i^{-1}, \quad 1 \leq i \leq n.$$

Then for each  $y \in F(H)$ ,

$$(y^K)_E = \sum_{i=1}^n ({}^{g_i}y|_{E_i})^E, \quad \text{where } {}^g y \text{ means } C_g^H(y).$$

For example, let  $H$  range over all subgroups of some fixed group  $G$ . Then  $\Omega(H)$  and  $\text{ch } QH$  are  $G$ -functors over  $\mathbb{Z}$ , as is  $K_0(\mathbb{Z}H)$ . Also,  $\Omega \otimes_{\mathbb{Z}} \Omega(H)$  is a  $G$ -functor over  $\mathbb{Q}$ .

**(80.31) Definition.** A  $G$ -functor  $F$  is *multiplicative* if each restriction map preserves products. In addition, we say that  $F$  has a *unit* if there exists a collection of elements  $\{u_H : H \leq G\}$ , such that

$$u_H y = y u_H = y \quad \text{for all } y \in F(H), \quad \text{res}_E^H u_H = u_E \quad \text{for } E \leq H,$$

$$C_g^H u_H = u_{H^g} \quad \text{for } g \in G.$$

Thus,  $\Omega(H)$  and  $\text{ch } QH$  are multiplicative  $G$ -functors with unit, while  $K_0(\mathbb{Z}H)$  is multiplicative but has no unit.

Given a multiplicative  $G$ -functor  $F$  with unit, it is clear how to define the concept of  $F$ -module, analogous to that of a Frobenius module over a Frobenius functor. The results in §38A carry over readily to modules over  $G$ -functors, and we leave it to the reader to work out the necessary details.

We note that for each commutative ring  $R$ , the Grothendieck group  $G_0(RH)$  is a module over the functor  $\Omega(H)$ . The action of  $\Omega(H)$  on  $G_0(RH)$  is given as follows: for each  $H$ -set  $S$ , let  $R[S]$  be the permutation  $RH$ -module, with  $R$ -basis the elements of  $S$ . We then define

$$[S] \cdot (M) = (R[S] \otimes_R M) \quad \text{for each } RH\text{-module } M.$$

The Mackey theorems on *modules* then appear as formal consequences of the Mackey theorems on *sets*. In this sense, the properties of Burnside rings relative to induction, restriction, conjugation, and Mackey formulas provide a “universal” combinatorial foundation for the corresponding concepts for various algebraic objects associated with a group, such as character rings, Grothendieck groups, projective class groups, cohomology rings, and so on. In particular, induction theorems for Burnside rings then yield induction theorems for these various other algebraic objects. We shall exploit this fact in §80D and §81.

To illustrate this idea, we start with any set  $\mathcal{C}$  of subgroups of  $G$ , and define

$$\Omega(G)_{\mathcal{C}} = \sum_{H \in \mathcal{C}} \{\Omega(H)\}^G, \quad \Omega(G)^{\mathcal{C}} = \{x \in \Omega(G) : x_H = 0 \text{ for all } H \in \mathcal{C}\},$$

so  $\Omega(G)_{\mathcal{C}}$  and  $\Omega(G)^{\mathcal{C}}$  are ideals of  $\Omega(G)$ . We now prove:

**(80.32) Theorem.** *Let  $G$  be a group of order  $n$ , and  $\mathcal{C}$  any set of subgroups of  $G$ . Then*

$$n\Omega(G) \subseteq \Omega(G)^{\mathcal{C}} \oplus \Omega(G)_{\mathcal{C}}.$$

*Proof.* We shall use the results and notation of §80A. Without loss of generality, we may enlarge  $\mathcal{C}$  so that if  $E \leq_G H \in \mathcal{C}$ , then also  $E \in \mathcal{C}$ . (Call  $\mathcal{C}$  *subconjugately closed* in this case.) By (80.16) we can choose  $x, y \in \Omega(G)$  such that for  $H \leq G$ ,

$$\varphi_H(x) = \begin{cases} n, & H \in \mathcal{C}, \\ 0, & H \notin \mathcal{C}, \end{cases} \quad \text{and} \quad \varphi_H(y) = \begin{cases} 0, & H \in \mathcal{C}, \\ n, & H \notin \mathcal{C}. \end{cases}$$

Then  $ne_G = x + y$ , and we shall prove that  $x \in \Omega(G)_{\mathcal{C}}$ ,  $y \in \Omega(G)^{\mathcal{C}}$ . For the latter, we must show that  $y_H = 0$  for each  $H \in \mathcal{C}$ . But for every  $E \leq H$  we have  $E \in \mathcal{C}$ , and therefore  $\varphi_E(y_H) = \varphi_E(y_E) = 0$ . Thus  $y_H = 0$ , by (80.12).

Next, let  $\mathcal{S}$  be a full set of nonconjugate subgroups of  $G$ , and write

$$x = \sum_{H \in \mathcal{S}} n_H [G/H], \quad \text{where } n_H \in \mathbb{Z}.$$

To prove that  $x \in \Omega(G)_{\mathcal{C}}$ , it suffices to show that  $n_H = 0$  for each  $H \in \mathcal{S} - \mathcal{C}$ . If this is not the case, let  $H \in \mathcal{S} - \mathcal{C}$  be a maximal element (with respect to  $\leq_G$ ) among all such  $H$  for which  $n_H \neq 0$ . Now let  $K \in \mathcal{S}$ , and suppose that  $\varphi_H(n_K[G/K]) \neq 0$ . By (80.9) we have  $H \leq_G K$  and also  $n_K \neq 0$ , so  $K = H$  by the maximality of  $H$ . It follows that  $\varphi_H(n_K[G/K]) = 0$  for  $K \in \mathcal{S}$ ,  $K \neq H$ . But then

$\varphi_H(x) = n_H \varphi_H[G/H] \neq 0$ , contradicting the choice of  $x$ . This proves that  $x \in \Omega(G)_\varnothing$ , so we deduce that

$$n\Omega(G) \subseteq \Omega(G)^\varnothing + \Omega(G)_\varnothing.$$

The right-hand side is a direct sum, since if  $z \in \Omega(G)^\varnothing \cap \Omega(G)_\varnothing$ , then  $z^2 = 0$  by (38.13iii), and so  $z = 0$  by (80.12).

**(80.33) Corollary.** *Let  $M(G)$  be a Frobenius module over  $\Omega(G)$ ; then*

$$n \cdot M(G) \leq M(G)^\varnothing + M(G)_\varnothing,$$

and  $n \cdot (M(G)^\varnothing \cap M(G)_\varnothing) = 0$ . In particular, if  $n$  acts invertibly on  $M(G)$ , then

$$M(G) = M(G)^\varnothing \oplus M(G)_\varnothing.$$

### §80C. Tensor Induction and Algebraic Maps

We shall define tensor induction of  $H$ -sets, where  $H \leq G$ , and shall show how this operation defines a multiplicative map from the Burnside ring  $\Omega(H)$  to  $\Omega(G)$ . The techniques are due to Dress, and we begin by recalling some results from §13A.

Let  $H$  be a subgroup of  $G$  of index  $n$ , and let

$$G = \bigcup_{i=1}^n g_i H.$$

For each  $x \in G$ , we may write

$$(80.34) \quad xg_i = g_{\pi(i)} h_i, \quad \text{where } h_i \in H, \quad 1 \leq i \leq n,$$

and  $\pi \in S_n$  is a permutation on  $\{1, \dots, n\}$ . Let  $H^n \rtimes S_n$  denote the wreath product  $H \wr S_n$  (see §13A). Then there is a monomorphism

$$(80.35) \quad \varphi: G \rightarrow H^n \rtimes S_n, \quad \text{given by } \varphi(x) = \pi \cdot (h_1, \dots, h_n),$$

using the notation in (80.34).

Now let  $T$  be any  $H$ -set, and let  $T^n = T \times \dots \times T$  ( $n$  factors). Then  $H^n \rtimes S_n$  acts from the left as a permutation group on  $T^n$ , by means of the formulas

$$\begin{cases} (h_1, \dots, h_n)(t_1, \dots, t_n) = (h_1 t_1, \dots, h_n t_n), & h_i \in H, \quad t_i \in T, \\ \pi(t_1, \dots, t_n) = (t_{\pi^{-1}(1)}, \dots, t_{\pi^{-1}(n)}), & \pi \in S_n. \end{cases}$$

Note that if  $\pi(j) = i$ , then the  $i$ -th entry of  $\pi(t_1, \dots, t_n)$  is  $t_j$ . By virtue of the map  $\varphi$  in (80.35), we may view  $T^n$  as a left  $G$ -set, called the *tensor-induced*  $G$ -set obtained from  $T$ , and denoted by  $T^{\otimes G}$ . Specifically, for  $x \in G$  and  $(t_1, \dots, t_n) \in T^{\otimes G}$ ,

we have

$$x(t_1, \dots, t_n) = \pi(h_1, \dots, h_n)(t_1, \dots, t_n) = \pi(h_1 t_1, \dots, h_n t_n),$$

keeping the notation in (80.34). In particular, we have for  $1 \leq i \leq n$  and  $x \in G$ ,

$$(80.36) \quad i\text{-th entry of } x(t_1, \dots, t_n) = ht_j, \quad \text{where } xg_j = g_i h, \quad h \in H.$$

We shall see below that tensor induction on  $H$ -sets is closely related to tensor induction of modules defined in §13A.

We are now ready to prove the analogue of the second isomorphism in (80.25).

**(80.37) Theorem (Dress).** *Let  $H \leq G$ , let  $S$  be a  $G$ -set, and  $T$  an  $H$ -set. Then there is a bijection of sets*

$$\mathrm{Hom}_H(S_H, T) \cong \mathrm{Hom}_G(S, T^{\otimes G}).$$

*Proof.* Given  $F \in \mathrm{Hom}_H(S_H, T)$ , we shall construct a corresponding map  $F' \in \mathrm{Hom}_G(S, T^{\otimes G})$  as follows. Let  $G = \cup g_i H$  as above, and define

$$F': S \rightarrow T^{\otimes G} \text{ by } F'(s) = (F(g_1^{-1}s), \dots, F(g_n^{-1}s)) \quad \text{for } s \in S.$$

Let us verify that  $F'$  is a  $G$ -map, that is,  $F'(xs) = xF'(s)$  for  $x \in G$ ,  $s \in S$ . Keeping  $x, s$  fixed, let  $1 \leq i \leq n$ . By (80.34),

$$i\text{-th entry of } xF'(s) = hF(g_j^{-1}s) \quad \text{where } xg_j = g_i h, \quad h \in H.$$

On the other hand,

$$i\text{-th entry of } F'(xs) = F(g_i^{-1}xs) = F(hg_j^{-1}s) = hF(g_j^{-1}s).$$

It follows that  $F'(xs) = xF'(s)$ , so  $F'$  is a  $G$ -map, as claimed.

Each  $F$  determines a unique  $F'$ , and  $F$  can be recovered from  $F'$  in an obvious way. It remains for us to show that each  $\Phi \in \mathrm{Hom}_G(S, T^{\otimes G})$  is an  $F'$  for some  $F \in \mathrm{Hom}_H(S_H, T)$ . Given  $\Phi$ , we may write

$$\Phi(s) = (F_1(g_1^{-1}s), \dots, F_n(g_n^{-1}s)), \quad s \in S,$$

with each  $F_i$  a set map from  $S$  into  $T$ . From the fact that  $\Phi$  is a  $G$ -map, it follows easily that

$$F_1 = \dots = F_n \in \mathrm{Hom}_H(S_H, T),$$

and thus  $\Phi = (F_1)'$ . This completes the proof.

We leave it to the reader to verify the following properties:

**(80.38) Proposition.** Let  $H \leq G$ , and let  $T$  and  $T_1$  be  $H$ -sets.

(i) There is an isomorphism of  $G$ -sets

$$(T \times T_1)^{\otimes G} \cong (T^{\otimes G}) \times (T_1^{\otimes G}).$$

(ii) Let  $R$  be any commutative ring. There is an  $RG$ -isomorphism

$$R[T^{\otimes G}] \cong (R[T])^{\otimes G}$$

of permutation modules, where the right-hand expression is a tensor-induced module defined as in (13.5).

Now define

$$(80.39) \quad \Omega^+(G) = \{ \sum a_i [S_i] : a_i \in \mathbb{Z}, \quad a_i \geq 0, \quad S_i = G\text{-set} \},$$

an additive semigroup of the Burnside ring  $\Omega(G)$ . Note that  $\Omega^+(G)$  is closed under multiplication. Each additive homomorphism  $\psi: \Omega^+(G) \rightarrow A$ , where  $A$  is an abelian group, extends uniquely to a homomorphism  $\Omega(G) \rightarrow A$ . Thus for  $H \leq G$ , the maps  $\text{res}_H^G$  and  $\text{ind}_H^G$ , defined originally on  $G$ -sets (and hence on  $\Omega^+$ ), extend to maps of Burnside rings. It will be important, in our later considerations, to extend the tensor-induction map  $\Omega^+(H) \rightarrow \Omega^+(G)$  to a map  $\Omega(H) \rightarrow \Omega(G)$ . Since tensor induction is not additive, we must now explain how such an extension can be defined. This will be done via Dress's theory of "algebraic maps," which we now describe.

### Algebraic Maps

In this discussion, let  $A$  be an additive semigroup with zero element, and let  $E$  be an additive group. We consider set maps  $f: A \rightarrow E$ , not necessarily homomorphisms. Given such an  $f$ , for each  $a \in A$  we define

$$D_a f: A \rightarrow E \text{ by } (D_a f)(x) = f(x + a) - f(x), \quad x \in A.$$

Then  $D_a D_b = D_b D_a$  for  $a, b \in A$ . Further,

$$(80.40) \quad (D_a D_b f)(x) = f(x + a + b) - f(x + a) - f(x + b) + f(x), \quad x \in A.$$

We say that  $f: A \rightarrow E$  is *algebraic of degree  $n$*  if  $n$  is the least integer such that

$$D_{a_1} D_{a_2} \cdots D_{a_{n+1}} f = 0 \quad \text{for all } a_1, \dots, a_{n+1} \in A.$$

(Of course, for many maps  $f$ , no such  $n$  exists.)

**(80.41) Remarks.** (i)  $f$  is algebraic of degree 0 if and only if  $f$  is constant on  $A$ .

(ii) A nonconstant map  $f: A \rightarrow E$  is algebraic of degree 1 if and only if

$f = h + c$ , where  $c$  is constant and  $h:A \rightarrow E$  is a nonzero additive map. To prove this, we note that by (80.40),  $f$  is algebraic of degree  $\leq 1$  if and only if

$$(*) \quad f(x+a+b) = f(x+a) + f(x+b) - f(x) \quad \text{for all } x, a, b \in A.$$

Clearly  $f = h + c$  satisfies this condition. Conversely, if  $(*)$  holds, then setting  $x = 0$  in  $(*)$ , and defining  $h(y) = f(y) - f(0)$ ,  $y \in A$ , we obtain

$$h(a+b) = h(a) + h(b) \quad \text{for } a, b \in A.$$

Thus  $h$  is additive, and  $f = h + f(0)$ , as desired.

(iii) Let  $f:\mathbb{R} \rightarrow \mathbb{R}$  be a polynomial map, given by  $x \in \mathbb{R} \mapsto f(x)$ , where  $f$  is an  $n$ -th degree polynomial. For each  $a \in \mathbb{R}$ ,  $D_a f$  is a polynomial of degree  $n-1$ . An easy induction argument shows that  $f$  is algebraic of degree  $n$ .

The next example, involving  $G$ -sets, is of basic importance for our later discussion. Let  $H \leq G$ , and put  $n = |G:H|$ . Then  $\Omega^+(H)$  is an additive semigroup (see (80.39)), and  $\Omega(G)$  is an additive group. There is then a map (tensor-induction)

$$(80.42) \quad \otimes: \Omega^+(H) \rightarrow \Omega(G), \text{ given by } [S] \mapsto [S^{\otimes G}]$$

for every  $H$ -set  $S$ . We now prove:

**(80.43) Proposition (Dress).** *Let  $H \leq G$ ,  $n = |G:H|$ . Then the tensor-induction map, defined above, is an algebraic map of degree  $n$ .*

*Proof.* Let  $S, T$  be  $H$ -sets; each element of  $S^{\otimes G}$  is an ordered  $n$ -tuple of elements of  $S$ . Let  $f:\Omega^+(H) \rightarrow \Omega(G)$  be the map given by  $f[S] = [S^{\otimes G}]$ . Then

$$(D_T f)[S] = f[S \cup T] - f[S] = [(S \cup T)^{\otimes G}] - [S^{\otimes G}].$$

But we may write

$$(S \cup T)^{\otimes G} = S^{\otimes G} \cup K_1, \quad \text{where } K_1 = K_1(S, T),$$

and  $K_1(S, T)$  is the  $G$ -subset of  $(S \cup T)^n$  of ordered  $n$ -tuples having at least one entry in  $T$ . Clearly  $(D_T f)[S] = [K_1(S, T)]$  in  $\Omega(G)$ .

Now let  $S, T, T'$  be  $H$ -sets. Then

$$(D_{T'} D_T f)[S] = [K_1(S \cup T', T)] - [K_1(S, T)] = [K_2(S, T, T')]$$

in  $\Omega(G)$ , where  $K_2(S, T, T')$  is the  $G$ -subset of  $(S \cup T \cup T')^n$  consisting of all  $n$ -tuples from  $S \cup T \cup T'$  having at least one entry from  $T$  and one from  $T'$ . Continuing in this fashion, we find that for  $H$ -sets  $T_1, \dots, T_n$ ,

$$(D_{T_n} \cdots D_{T_1} f)[S] \neq 0 \quad \text{in } \Omega(G),$$

and is independent of  $S$ . It follows at once that  $f$  is algebraic of degree  $n$ , as claimed.

Given an additive semigroup  $A$  with zero element, let  $\bar{A}$  be the additive group generated by the elements of  $A$ . To define  $\bar{A}$ , we introduce an equivalence relation on  $A \times A$  by writing

$$(x, y) \sim (x', y') \text{ if and only if } x + y + z = x' + y + z \text{ for some } z \in A.$$

Let  $\bar{A}$  be the set of equivalence classes of ordered pairs, and denote the class of  $(x, y)$  by  $x - y$ . Then  $\bar{A}$  is an additive group, and there is an additive map  $A \rightarrow \bar{A}$ , given by  $a \in A \mapsto (a + z, z) \in \bar{A}$  for any  $z \in A$ . For  $a \in A$ , we denote the class of  $(a + z, z)$  by  $a \in \bar{A}$ , and there is then an additive homomorphism  $A \rightarrow \bar{A}$  given by  $a \mapsto a$ , which need not be injective, generally speaking.

Now let  $f: A \rightarrow E$  be a map, not necessarily additive, from the additive semigroup  $A$  into an additive group  $E$ . We wish to find a map  $\bar{f}: \bar{A} \rightarrow E$  extending  $f$ ; note that  $\bar{f}$  need not be a homomorphism. We give two examples:

(i) Given a constant map  $f: A \rightarrow E$ , with  $f(a) = c \in E$  for all  $a \in A$ , define  $\bar{f}(x - y) = c$  for all  $x, y \in A$ . Then  $\bar{f}$  is a constant map that extends  $f$ .

(ii) Let  $f = h + c$ , where  $h$  is additive and  $c$  is constant. We set

$$\bar{f}(x - y) = h(x) - h(y) + c, \quad \text{for } x - y \in \bar{A}.$$

It is easily checked that  $\bar{f}$  is well-defined, and extends  $f$ .

More generally, we prove:

**(80.44) Theorem (Dress).** *Let  $f: A \rightarrow E$  be an algebraic map of degree  $n$  from an additive semigroup  $A$  into an additive group  $E$ . Let  $\bar{A}$  be the additive group generated by  $A$ . Then there is a unique map  $\bar{f}: \bar{A} \rightarrow E$  extending  $f$ , and  $\bar{f}$  is also algebraic of degree  $n$ .*

*Proof.* We shall give a “symbolic” proof that captures the essence of the construction; a detailed proof, via induction on  $n$ , is given in Dress-Küchler [70, pp. 60–76]. Suppose that  $\bar{f}$  has been constructed in some way, and let  $x, y \in A$ . Then

$$\begin{aligned} \{(1 + D_y)\bar{f}\}(x - y) &= \bar{f}(x - y) + (D_y \bar{f})(x - y) \\ &= \bar{f}(x - y) + \bar{f}(x) - \bar{f}(x - y) = f(x), \end{aligned}$$

that is,

$$\bar{f}(x - y) = (1 + D_y)^{-1}f(x) = (1 - D_y + D_y^2 + \dots)f(x).$$

Since  $D_y^{n+1} = 0$ , we obtain for  $x, y \in A$ ,

$$\begin{aligned}
 (80.45) \quad \bar{f}(x-y) &= f(x) - (D_y f)(x) + (D_y^2 f)(x) - \dots \\
 &= f(x) - \{f(x+y) - f(x)\} \\
 &\quad + \{f(x+2y) - 2f(x+y) + f(x)\} + \dots,
 \end{aligned}$$

a terminating series. Note that when  $y = 0$ , this gives  $\bar{f}(x) = f(x)$ .

We shall define  $\bar{f}$  by (80.45), and must verify that if  $(x, y) \sim (x', y')$  in  $A \times A$ , then  $\bar{f}(x-y) = \bar{f}(x'-y')$ . Increasing both  $x$  and  $y$  by some  $z \in A$ , and changing notation, we may assume that  $x+y' = x'+y$ . We must prove that

$$\{(1+D_y)^{-1}f\}(x) = \{(1+D_{y'})^{-1}f\}(x') \quad \text{in } E.$$

Since  $D_y$  and  $D_{y'}$  commute, it suffices to check that

$$\{(1+D_{y'})f\}(x) = \{(1+D_y)f\}(x'),$$

that is,  $f(x+y') = f(x'+y)$ . But this is clear, so we have now shown that  $\bar{f}: \bar{A} \rightarrow E$  is a well-defined extension of  $f$ .

Finally, let us prove that  $\bar{f}$  is algebraic of degree  $n$ . For  $x, y, z \in A$ , we have

$$(D_{y-z}\bar{f})(x) = (D_y\bar{f})(x-z) - (D_z\bar{f})(x-z).$$

From this and (80.45) it follows at once that  $\bar{f}$  is algebraic of degree  $\leq n$ . The degree cannot be less than  $n$ , since  $\bar{f}$  extends  $f$ . This completes the proof.

**Remarks.** (i) If  $f$  is constant, then so is  $\bar{f}$  by (80.45), and  $\bar{f}(x-y) = f(x)$ .

(ii) For  $\xi, \eta \in \bar{A}$ , the analogue of (80.45) is valid, that is,

$$(80.46) \quad \bar{f}(\xi-\eta) = \{(1-D_\eta+D_\eta^2-\dots)f\}(\xi).$$

Suppose now that for each  $x, y \in A$ , there is a product  $xy \in A$ , and that this multiplication is commutative, associative, and satisfies the distributive law. Then there is a well-defined multiplication in  $\bar{A}$ , and  $\bar{A}$  becomes a commutative ring (not necessarily having an identity element).

**(80.47) Theorem.** Let  $A$  be an additive semigroup with products, and let  $f: A \rightarrow E$  be an algebraic map from  $A$  into a commutative ring  $E$ . Suppose that  $f$  is multiplicative, that is,

$$f(xy) = f(x)f(y) \quad \text{for all } x, y \in A.$$

Then the unique extension  $\bar{f}$  of  $f$  to  $\bar{A}$  is also multiplicative.

*Proof.* For fixed  $y \in A$ , there is an algebraic map  $\varphi: A \rightarrow E$ , defined by

$$\varphi(x) = f(x)f(y), \quad x \in A.$$

Then  $\varphi$  lifts uniquely to a map  $\bar{\varphi}:\bar{A}\rightarrow E$ . But clearly the formula

$$\bar{\varphi}(\xi)=\bar{f}(\xi)f(y), \quad \xi\in\bar{A},$$

gives a lifting of  $\varphi$ . On the other hand, since  $\varphi(x)=f(xy)$  for all  $x\in A$ ,  $\bar{\varphi}$  is also given by

$$\bar{\varphi}(\xi)=\bar{f}(\xi y), \quad \xi\in\bar{A}.$$

This implies that

$$\bar{f}(\xi y)=\bar{f}(\xi)f(y) \quad \text{for all } \xi\in\bar{A}, \quad y\in A.$$

Now keep  $\xi\in\bar{A}$  fixed, and let  $\psi:A\rightarrow E$  be the algebraic map for which  $\psi(y)=\bar{f}(\xi)f(y)$ ,  $y\in A$ . Then  $\psi$  lifts to a map  $\bar{\psi}$  on  $\bar{A}$ , and as above we obtain

$$\bar{f}(\xi)\bar{f}(\eta)=\bar{f}(\xi\eta) \quad \text{for all } \xi, \eta\in\bar{A}.$$

This completes the proof.

We now apply this result to the study of Burnside rings. To begin with, the additive semigroup  $\Omega^+(G)$  defined in (80.39) is embedded in the Burnside ring  $\Omega(G)$ , by virtue of (80.4). From (80.43) and (80.47) we obtain at once:

**(80.48) Theorem (Dress).** *Let  $H\leq G$  be finite groups. There is a unique multiplicative map  $\varphi':\Omega(H)\rightarrow\Omega(G)$ , called tensor induction, such that*

$$\varphi'[S]=[S^{\otimes G}] \quad \text{for each } H\text{-set } S.$$

The map  $\varphi'$  is algebraic of degree  $|G:H|$ .

We remark that  $\varphi'$  is not additive if  $H < G$ . Next, for  $y\in\Omega(H)$  we denote  $\varphi'(y)$  by  $y^{\otimes G}$ . For any  $H$ -sets  $S$  and  $T$ , it follows from (80.45) that

$$\begin{aligned} ([S]-[T])^{\otimes G} &= [S^{\otimes G}] - \{[(S\dot{\cup} T)^{\otimes G} - [S^{\otimes G}]] \\ &\quad + \{[(S\dot{\cup} T\dot{\cup} T)^{\otimes G} - 2[(S\dot{\cup} T)^{\otimes G}] + [S^{\otimes G}]]\} - \dots, \end{aligned}$$

and only finitely many braces are nonzero. We may rewrite this formula in a nicer form, as follows:

**(80.49) Corollary.** *Let  $H$  be a subgroup of  $G$  of index  $n$ , and let  $S, T$  be  $H$ -sets. For each  $i$ ,  $0 \leq i \leq n$ , let  $V_i$  be the  $G$ -subset of  $(S\dot{\cup} T)^{\otimes G}$  consisting of all elements having exactly  $i$  entries from  $S$  and  $n-i$  entries from  $T$ . Then*

$$([S]-[T])^{\otimes G} = [V_n] - [V_{n-1}] + \dots + (-1)^n[V_0] \quad \text{in } \Omega(G).$$

*Proof.* This follows readily from the preceding discussion, together with the proof of (80.43). We leave it to the reader to check the details.

### §80D. Conlon's Induction Theorem

Throughout let  $K$  be a field of characteristic  $p \geq 0$ , and let  $G$  be a finite group. We shall prove Conlon's generalization of the Artin Induction Theorem, following the proof given by Dress [73], with minor simplifications. The calculations will take place in the *representation ring*  $a(KG)$ , also called the *Green ring*, defined as follows. Restricting our attention to f.g. left  $KG$ -modules, let  $a(KG)$  be the ring consisting of  $\mathbb{Z}$ -linear combinations of symbols  $[M]$ , one for each isomorphism class of  $KG$ -modules  $M$ , with relations given by direct sum:  $[M \oplus M'] = [M] + [M']$  for  $KG$ -modules  $M$  and  $M'$ . Multiplication is defined by inner tensor products (over  $K$ ) of  $KG$ -modules. Since the Krull-Schmidt-Azumaya Theorem holds for  $KG$ -modules, it follows that  $a(KG)$  has a  $\mathbb{Z}$ -basis consisting of all  $[M]$  with  $M$  indecomposable. Further, for  $KG$ -modules  $N$  and  $N'$ , we have  $[N] = [N']$  in  $a(KG)$  if and only if  $N \cong N'$ .

It is convenient to introduce the *representation algebra*

$$A(KG) = \mathbb{Q} \otimes_{\mathbb{Z}} a(KG).$$

Then  $a(KG)$  is embedded in  $A(KG)$  as a subring, and both have the same identity element  $[K_G]$ , where  $K_G$  is the field  $K$  on which  $G$  acts trivially. There are induction maps  $a(KH) \rightarrow a(KG)$ , and  $A(KH) \rightarrow A(KG)$ , for each  $H \leq G$ . As usual, for  $x \in a(KH)$ , let  $x^G$  denote its image in  $a(KG)$ . However, we shall avoid using a subscript  $H$  to denote restriction, in view of our notation  $K_G$  just introduced.

Our object is to express the element  $[K_G] \in A(KG)$  as a  $\mathbb{Q}$ -linear combination of induced elements  $[K_H]^G$ , with  $H$  ranging over a suitably chosen family of subgroups of  $G$ . If  $\text{char } K = 0$ , it suffices to let  $H$  range over all cyclic subgroups of  $G$ , by the Artin Induction Theorem 15.4. For  $\text{char } K = p > 0$ , we need instead the family  $\mathcal{H}'$  of all  $p$ -hypo-elementary subgroups of  $G$ , given as follows:

**(80.50) Definition.** A group  $H$  is  *$p$ -hypo-elementary*, or *cyclic mod  $p$* , if  $H = P \rtimes C$ , where  $P$  is a normal  $p$ -subgroup and  $C$  is a cyclic  $p'$ -group. (For  $p = 0$ ,  $H$  may be any cyclic group.) By way of contrast, the  $p$ -hyper-elementary groups have the form  $C \rtimes P$ , with  $C, P$  as above.

The main result is as follows:

**(80.51) Conlon Induction Theorem.\*** Let  $K$  be a field of characteristic  $p$ , and let  $\mathcal{H}'$  be the set of  $p$ -hypo-elementary subgroups of a given group  $G$ . Then there is a relation in  $A(KG)$ :

$$(80.52) \quad [K_G] = \sum_{H \in \mathcal{H}'} \alpha_H [K_H]^G \quad \text{for some rational numbers } \{\alpha_H\}.$$

\*See also (81.31).

*Proof.* Step 1. We first consider the *Burnside algebra*  $\Omega_0(KG)$ , defined as the  $\mathbb{Q}$ -subalgebra of  $A(KG)$  generated by all permutation representations of  $G$  over  $K$ . Since each  $G$ -set is a disjoint union of left  $G$ -sets  $G/H$  with  $H \leq G$ , and since the permutation module  $K[G/H]$  is  $KG$ -isomorphic to the induced module  $(K_H)^G$ , it follows that

$$(80.53) \quad \Omega_0(KG) = \sum_{H \leq G} \mathbb{Q} \cdot [K_H]^G$$

For convenience of notation, let us set  $F(H) = \Omega_0(KH)$  for each  $H \leq G$ . Then in the terminology of §80B,  $F$  is a multiplicative  $G$ -functor with unit  $\{[K_H] : H \leq G\}$ .

Next, we note that

$$\begin{aligned} \sum_{H \in \mathcal{H}'} F(H)^G &= \left\{ \sum_{H \in \mathcal{H}'} \left( \sum_{E \leq H} \mathbb{Q} \cdot [K_E]^H \right)^G \right\} \\ &= \sum_{E \leq H \in \mathcal{H}'} \mathbb{Q} \cdot [K_E]^G. \end{aligned}$$

If  $E \leq H \in \mathcal{H}'$ , then  $E \in \mathcal{H}'$  (see Exercise 80.16), and therefore

$$\sum_{H \in \mathcal{H}'} F(H)^G = \sum_{H \in \mathcal{H}'} \mathbb{Q} \cdot [K_H]^G.$$

The left-hand side, usually denoted by  $F(G)_{\mathcal{H}'}$ , is an ideal of the ring  $F(G)$ . Thus, the existence of a formula (80.52) is equivalent to the assertion that

$$F(G)_{\mathcal{H}'} = F(G).$$

Step 2. Here we make some general observations about induction theorems of the above type. Let  $F$  be any  $G$ -functor, which assigns to each  $H \leq G$  a commutative ring  $F(H)$  with unit  $u_H$ , as in Definition 80.31. We wish to show that  $F(G)_{\mathcal{C}} = F(G)$  for some suitably chosen class  $\mathcal{C}$  of subgroups of  $G$ .

We set

$$F'(G) = \sum_{H \lessdot G} \text{ind}_H^G F(H) = \text{ideal of } F(G).$$

If  $F'(G) = F(G)$ , we call  $G$  “good”; if  $F'(G)$  is a proper ideal of  $F(G)$ , we call  $G$  “bad.” This terminology is temporary and is helpful in stating the argument that follows. Obviously we have

$$F(G) = \sum_{H \leq G} \text{ind}_H^G F(H) = \sum_{\substack{H \leq G \\ H \text{ bad}}} \text{ind}_H^G F(H).$$

Thus,  $F(G)_{\mathcal{C}} = F(G)$  whenever  $\mathcal{C}$  contains all bad  $H \leq G$ .

In practice, we choose a collection  $\mathcal{C}$  of subgroups of  $G$ , and try to prove that

each  $H \leq G$ , for which  $F'(H) \neq F(H)$ , must lie in  $\mathcal{C}$ . This is usually accomplished in three steps:

- (i) Find a collection  $\mathcal{C}^*$  of good groups.
- (ii) Show that homomorphic images of bad groups are bad.
- (iii) Show that subgroups of bad groups are bad.

It will then follow that if  $H$  is a bad subgroup of  $G$ , then no subgroup or homomorphic image of  $H$  can lie in  $\mathcal{C}^*$ . A group-theoretic argument is then used to prove that  $H \in \mathcal{C}$ . Note that the trivial group  $\{1\}$  is necessarily *bad*.

The proofs of (ii) and (iii), for the cases needed here, depend on a pair of lemmas, which we now establish.

**(80.54) Lemma.** *Let  $\bar{H} = H/N$ , where  $N \trianglelefteq H$ , and set  $\bar{E} = E/N$  for each  $E$  with  $N \leq E \leq H$ . Suppose that for each  $H$ , there is an inflation map  $F(\bar{H}) \rightarrow F(H)$ , which is a ring homomorphism such that*

$$u_H \rightarrow u_{\bar{H}}, \quad \text{and} \quad F(\bar{E})^{\bar{H}} \rightarrow F(E)^H.$$

*Then if  $H$  is bad, so is  $\bar{H}$ .*

*Proof.* Assume  $\bar{H}$  good, so  $F'(\bar{H}) = F(\bar{H})$ , or equivalently,

$$u_H \in \sum_{E < H} F(\bar{E})^{\bar{H}}.$$

Applying the inflation map to the above, we obtain  $u_H \in F'(H)$ , so  $H$  is good. This completes the proof.

**(80.55) Lemma.** *Suppose that for  $H \leq G$ , there is a multiplicative map  $\mu: F(H) \rightarrow F(G)$  such that*

$$\begin{aligned} \mu(u_H) &= u_G, \quad \mu(F'(H)) \subseteq F'(G), \\ \mu(x y) &\equiv \mu(x) + \mu(y) \pmod{F'(G)} \quad \text{for } x, y \in F(H). \end{aligned}$$

*Then  $\mu$  induces a ring homomorphism*

$$F(H)/F'(H) \rightarrow F(G)/F'(G).$$

*Therefore if  $G$  is bad, so is  $H$ .*

*Proof.* A group  $G$  is good if and only if  $u_G \in F'(G)$ , that is,  $F(G)/F'(G)$  is the zero ring. If  $H$  is good, then  $u_H \in F'(H)$ , so  $u_G = \mu(u_H) \in F'(G)$ , and therefore  $G$  is good.

*Step 3.* Let us apply the above discussion to the case where  $F(H) = \Omega_0(KH)$ , and begin by verifying the hypotheses of the lemmas. Let  $\bar{H} = H/N$  as in (80.54). The inflation map carries  $K_H$  into  $K_{\bar{H}}$ , and induces a ring homomorphism

$F(\bar{H}) \rightarrow F(H)$ . Further,

$$\text{inflation of } (K_E)^{\bar{H}} \cong (K_E)^H \quad \text{as } KH\text{-modules.}$$

It follows from (80.54) that if  $H$  is bad, so is  $\bar{H}$ .

Second, let  $H \leq G$  and consider the tensor induction map  $\Omega(H) \rightarrow \Omega(G)$  defined in (80.48). This map induces a well-defined multiplicative map  $\mu: F(H) \rightarrow F(G)$ , defined by

$$\mu[M] = [M^{\otimes G}] \quad \text{for } M = (K_E)^H, \quad E \leq H.$$

Clearly  $\mu[K_H] = [K_G]$ . Further, by the analogue of Exercise 80.14 for permutation modules, we obtain

$$\mu(x + y) \equiv \mu(x) + \mu(y) \pmod{F'(G)} \quad \text{for } x, y \in F(H).$$

Furthermore, the analogue of Exercise 80.15 implies that  $\mu(F'(H)) \subseteq F'(G)$ . The hypotheses of (80.55) are therefore satisfied in this case, and we may conclude that subgroups of bad groups are also bad.

*Step 4.* It remains for us to construct a collection  $\mathcal{C}^*$  of good groups (for the choice  $F(H) = \Omega_0(KH)$ ), and using this collection, to show that every bad group must lie in the set  $\mathcal{H}'$  of  $p$ -hypo-elementary subgroups of  $G$ . We assume from now on that  $p > 0$ , since (80.52) follows from the Artin Induction Theorem when  $p = 0$ .

**(80.56) Lemma.** *Let  $H = C \times C$ , where  $C$  is cyclic of prime order  $q$ , and  $q \neq p$ . Then there exist integers  $\{m_E : E < H\}$  such that*

$$(80.57) \quad q[K_H] = \sum_{E < H} m_E [K_E]^H \quad \text{in } a(KH).$$

Therefore  $H$  (is good (relative to  $\Omega_0(KH)$ ).

*Proof.* By Exercise 76.1, there is a relation (80.57) with  $K$  replaced by  $\mathbb{Q}$ . Let  $R = \mathbb{Z}_{(p)}$  be the localization of  $\mathbb{Z}$  at  $p$ , and let  $R_H$  be  $R$  on which  $H$  acts trivially. By (76.16) we obtain

$$q[R_H] = \sum_{E < H} m_E [R_E]^H \quad \text{in } a(RH).$$

Reducing the permutation representations mod  $p$ , we obtain the same relation in  $a(\bar{R}H)$ , where  $R_H$  is replaced by  $\bar{R}_H$ , etc., with  $\bar{R} = R/pR \cong \mathbb{Z}/p\mathbb{Z}$ . Since  $K$  is an extension field of  $\bar{R}$ , there is a map  $a(\bar{R}H) \rightarrow a(KH)$ , and thus (80.57) is proved.

**(80.58) Lemma.** *Let  $H = C \rtimes A$ , where  $C$  is cyclic of prime order  $q \neq p$ , and  $A = \text{Aut } C$ . Let  $H_0 = C \rtimes A_0$ , where  $1 < A_0 \leq A$ . Then there exist integers*

$\{m_E : E < H\}$  such that

$$(80.59) \quad (q-1)[K_{H_0}] = \sum_{E < H_0} m_E [K_E]^{H_0} \quad \text{in} \quad a(KH_0),$$

and thus  $H_0$  is good (relative to  $\Omega_Q(KH_0)$ ).

*Proof.* Let  $C = \langle c : c^q = 1 \rangle$ ,  $A = \langle a : a^{q-1} = 1 \rangle$ , and  $aca^{-1} = c^m$ , where  $m$  is a primitive root  $(\bmod q)$ . Let

$$R = \mathbb{Z}_{(p)}, \quad S = R[\omega], \quad \omega = \text{primitive } q\text{-th root of 1.}$$

If  $S_A$  denotes  $S$  on which  $A$  acts trivially, we have

$$SH \otimes_{S_A} S_A \cong SC,$$

where  $A$  acts by conjugation on  $SC$ . But  $q \in S^*$ , so as  $SC$ -modules,

$$SC \cong \coprod_{i=0}^{q-1} S_i, \quad \text{where } S_i = S \text{ on which } c \text{ acts as } \omega^i.$$

Then  $S_0$  is the  $H$ -trivial module  $S_H$ , while  $a \cdot S_i = S_{mi}$  for  $1 \leq i \leq q-1$ . Thus  $\coprod_1^{q-1} S_i$  is a system of imprimitivity for  $H$ , and the stabilizer of  $S_1$  is  $C$ . It follows that  $\coprod_1^{q-1} S_i \cong SH \otimes_{SC} S_1$ , and therefore

$$SH \otimes_{S_A} S_A \cong SH \oplus (SH \otimes_{SC} S_1) \quad \text{as } SH\text{-modules.}$$

Now  $S$  is  $R$ -free of rank  $q-1$ . In the above, we restrict operators to  $RH_0$ , obtaining a relation in  $a(RH_0)$ :

$$(*) \quad (q-1)\text{res}_{H_0}^H \text{ind}_A^H[R_A] = (q-1)[S_{H_0}] + \text{res}_{H_0}^H \text{ind}_C^H[S_1].$$

However,  $RC \cong R_C \oplus S_1$ , where  $C$  acts trivially on  $R_C$ , so  $(*)$  becomes

$$(q-1)\text{res}_{H_0}^H \text{ind}_A^H[R_A] + \text{res}_{H_0}^H \text{ind}_C^H[R_C] = (q-1)[S_{H_0}] + \text{res}_{H_0}^H \text{ind}_{\{1\}}^H[R_{\{1\}}].$$

The Mackey Subgroup Theorem then yields a relation of the form (80.59), with  $R$  in place of  $K$  throughout. Since  $K$  is an extension field of  $R/pR$ , the rest of the proof is as above.

*Step 5.* We have now established that for each prime  $q \neq p$ , the groups  $C \times C$  and  $C \rtimes A_0$  are good (for the functor  $F(H) = \Omega_Q(KH)$ ), where  $C$  is cyclic of order  $q$ , and  $A_0$  is any nontrivial subgroup of  $\text{Aut } C$ . We must show that every bad group  $H$  is  $p$ -hypo-elementary.

Let  $q$  be any prime dividing  $|H|$ ,  $q \neq p$ . Since  $H$  is bad by hypothesis, each Sylow  $q$ -subgroup  $H_q$  of  $H$  must also be bad. Therefore  $H_q$  must be cyclic, since

otherwise  $H_q$  would have a factor group of the form  $C \times C$ , where  $|C| = q$ , which is impossible by Lemma 80.56. We now show that  $H$  contains a normal  $q$ -complement, that is, there exists an  $N_q \trianglelefteq H$  with  $|N_q| = q'$ -part of  $|H|$ . By the Burnside Transfer Theorem 13.20, to show the existence of  $N_q$ , we need only verify that  $C_H(H_q) = N_H(H_q)$ . Omitting the subscript  $H$  for brevity, suppose that there exists an  $x \in N(H_q) - C(H_q)$ , and let us obtain a contradiction. Write  $x = x'y$ , where  $x'$  is a  $q$ -element,  $y$  a  $q'$ -element, with  $x'$ ,  $y$  powers of  $x$ . Then  $x' \in N(H_q)$ , and therefore  $x' \in H_q$  since  $H_q$  is a Sylow  $q$ -subgroup of  $H$ . Since  $H_q$  is cyclic,  $x'$  centralizes  $H_q$ , and therefore  $y \in N(H_q) - C(H_q)$ . Let  $r > 0$  be minimal such that  $y^r \in C(H_q)$ , let  $l$  be a given prime factor of  $r$ , and let  $z = y^{rl}$ . Then  $z^l \in C(H_q)$ , while  $z \in N(H_q) - C(H_q)$ . Setting  $H_q = \langle h \rangle$ , define

$$E = \langle h, z \rangle / \langle h^q, z \rangle \cong C \rtimes \langle z \rangle,$$

with  $|C| = q$ . Then  $E$  is a factor group of a subgroup of  $H$ , so  $E$  must be bad, which contradicts (80.58).

We have now shown that for each prime divisor  $q$  of  $|H|$ ,  $q \neq p$ ,  $H$  contains a normal  $q$ -complement  $N_q$ . We set

$$N = \bigcap_q N_q \trianglelefteq H.$$

Then obviously  $N$  is a Sylow  $p$ -subgroup of  $H$ . Further, for each  $q$  as above,  $H/N$  has a cyclic Sylow  $q$ -subgroup and a normal  $q$ -complement. It follows that  $H/N$  is a direct product of its Sylow subgroups, so  $H/N$  is a cyclic  $p'$ -group. Therefore by the Schur-Zassenhaus Theorem,  $H = N \rtimes T$  for some  $T \leq H$ , with  $T \cong H/N$ , and so  $H$  is  $p$ -hypo-elementary. This completes the proof of the Conlon Induction Theorem. For another proof, see (81.31).

The field  $K$  plays a subsidiary role in the above proofs. The heart of the argument consists of Lemmas 80.56 and 80.58, together with some general facts about permutation modules, and Dress's Theorem 80.48 on the existence of a multiplicative tensor-induction map on Burnside rings. These key lemmas were established by working over the localization  $Z_{(p)}$  of  $Z$  at  $p$ , and then reducing to case of fields. Thus, the preceding proofs yield a stronger result, which we now formulate.

For  $R$  any commutative ring, let  $a(RG)$  be the *representation ring* of  $RG$ , generated by  $RG$ -lattices with relations coming from direct sum (see §81A). Set  $A(RG) = \mathbb{Q} \otimes_Z a(RG)$ , the *representation algebra* of  $RG$ . Then we have:

**(80.60) Theorem.** *Given a group  $G$  and a prime  $p$ , let  $R$  be a commutative ring such that each prime divisor of  $|G|$ , except possibly  $p$ , is invertible in  $R$ . Then the Conlon Induction Theorem remains true when the field  $K$  is replaced throughout by  $R$ .*

Since the representation algebra  $A(KG)$  is a Frobenius module over the Frobenius functor  $\Omega_0(KG)$ , we obtain the following consequence of Conlon's Theorem:

**(80.61) Corollary.** Let  $K$  be a field of characteristic  $p \geq 0$ , and let  $\mathcal{H}'$  denote the set of  $p$ -hypo-elementary subgroups of  $G$ . Then

$$A(KG) = \sum_{H \in \mathcal{H}'} \text{ind}_H^G A(KH).$$

Further, if  $x \in A(KG)$  is such that  $\text{res}_H^G x = 0$  for all  $H \in \mathcal{H}'$ , then  $x = 0$ . (These assertions remain valid when  $K$  is replaced by a ring  $R$  as in (80.60).)

*Proof.* The result is immediate from (38.14).

## §80. Exercises

Throughout,  $G$  is a finite group,  $S, T$  are  $G$ -sets, and  $H, K \leq G$ .

1. Let  $s \in S$  and  $H \leq G$ . Prove that for  $x \in G$ ,  $s \in \text{Inv}_H S$  if and only if  $sx \in \text{inv}_{xHx^{-1}} S$ . Deduce that

$$|\text{inv}_H S| = |\text{inv}_K S| \quad \text{whenever } H =_G K.$$

2. Let  $H \backslash G/K$  be the collection of all  $(H, K)$ -double cosets  $HgK$  of  $G$ . Show that each  $G$ -orbit of the left  $G$ -set  $(G/H) \times (G/K)$  determines a double coset  $HgK$ , by the rule:

$$\text{G-orbit of } (xH, yK) \rightarrow H \cdot x^{-1}y \cdot K.$$

Show that this correspondence gives a bijection between the collection of  $G$ -orbits of  $(G/H) \times (G/K)$  and the double coset space  $H \backslash G/K$ .

[Hint: Let  $G = \bigcup_a HaK$ . The  $G$ -orbit of  $(G/H) \times (G/K)$  corresponding to  $HaK$  consists of all distinct pairs in the collection  $\{(xH, yK) : x^{-1}y \in HaK\}$ . The stabilizer of the pair  $(H, aK)$  is precisely  $H \cap aKa^{-1}$ . Deduce that the orbit of  $(G/H) \times (G/K)$  corresponding to  $HaK$  is isomorphic (as  $G$ -set) to  $G/(H \cap aKa^{-1})$ , and therefore

$$(G/H) \times (G/K) \cong \bigcup_a G/(H \cap aKa^{-1}).$$

Compare this with Mackey's Theorem 10.18.]

3. Say that the group  $G$  acts freely on a  $G$ -set  $S$  if for each  $s \in S$ , its stabilizer  $G_s$  equals 1. Prove

- (i)  $G$  acts freely on a  $G$ -set  $S$  if and only if  $S$  is a disjoint union of copies of the left  $G$ -set  $G$ .
  - (ii) If  $G$  acts freely on  $S$ , then  $|G|$  divides  $|S|$ .
  - (iii) If  $G$  acts freely on  $S$ , and  $H$  is a subgroup of  $G$ , then  $H$  acts freely on  $S$ . Show further that  $H$  acts freely on every  $H$ -subset of  $S$ , and deduce that  $|H|$  divides the number of elements in any  $H$ -subset of  $S$ .
4. For  $H \leq G$ , let  $N_G(H)$  act from the left as permutation group on the coset space  $G/H$ ,

by setting

$$x \cdot gH = gx^{-1}H, \quad x \in N_G(H), \quad gH \in G/H.$$

Since the subgroup  $H$  of  $N_G(H)$  acts trivially on  $G/H$  under the above definition, it follows that  $G/H$  is a left  $N_G(H)/H$ -set. Prove:

(i)  $N_G(H)/H$  acts freely on  $G/H$ .

(ii) For  $K \leq G$ , let

$$\begin{aligned} \text{inv}_K(G/H) &= \{gH : x \cdot gH = gH \text{ for all } x \in K\} \\ &= \{gH : K \cdot gH = gH\}. \end{aligned}$$

Show that  $\text{inv}_K(G/H)$  is an  $N_G(H)/H$ -subset of  $G/H$ . Deduce that  $N_G(H)/H$  acts freely on  $\text{inv}_K(G/H)$ .

(iii) Keeping the above notation, prove that

$$|N_G(H):H| \text{ divides } |\text{inv}_K(G/H)|$$

for each subgroup  $K$  of  $G$ .

5. Keeping the notation of the preceding exercise, prove that

$$N_G(H)/H \cong \text{Hom}_G(G/H, G/H)$$

as permutation groups on  $G/H$ .

[Hint: For  $x \in N_G(H)$ , let  $\theta_x : G/H \rightarrow G/H$  be the  $G$ -map defined by  $\theta_x(gH) = gx^{-1}H$  for  $gH \in G/H$ . Then  $\theta : xH \rightarrow \theta_x$ ,  $x \in N_G(H)$ , gives the desired isomorphism.]

6. Prove that if  $G$  acts freely on  $S$ , it also acts freely on  $S \times T$  for each  $T$ .

7. Let  $|G| = p = \text{prime}$ . Find all simple  $G$ -sets; compute  $\Omega(G)$  and its image under the monomorphism  $\varphi$  defined in (80.12). Determine all prime ideals of  $\Omega(G)$ , and also all units in  $\Omega(G)$ . Answer the same questions for the case  $G = S_3$ .

8. For  $H, K \leq G$ , let  $(G/H)_K$  be the  $K$ -set obtained by restriction of operators on the  $G$ -set  $G/H$ . Show that each  $K$ -orbit of  $(G/H)_K$  is precisely the collection of all left cosets  $gH$  in some  $(K, H)$ -double coset of  $G$ . If  $G = \bigcup_g KgH$ , then each  $g$  determines a  $K$ -orbit of  $(G/H)_K$ . Prove that

$$KgH \cong K/(K \cap {}^g H) \text{ as left } K\text{-sets.}$$

9. Let  $H \leq G$ . Show there exists an  $x \in \Omega(G)$  with

$$\varphi_H(x) \neq 0, \quad \varphi_K(x) = 0 \quad \text{for } K \neq G/H.$$

[Hint: Using the notation in (80.11) and (80.12), we may assume  $H$  is some  $H_i$ . Let  $\varepsilon_i$  be the element of  $Z^{(m)}$  that has  $i$ -th component 1, all others 0. By (80.16),  $|G|\varepsilon_i = \varphi(x)$  for some  $x \in \Omega(G)$ . For this  $x$  we have  $\varphi_H(x) = |G|$ ,  $\varphi_K(x) = 0$  if  $K \neq G/H$ .]

10. Each group homomorphism  $\tau:H \rightarrow G$  induces an additive map  $\tau^*:\Omega(G) \rightarrow \Omega(H)$ , by viewing each  $G$ -set as an  $H$ -set via  $\tau$ . Prove that  $\tau$  is surjective if and only if  $\tau^*$  is injective.

[Hint: If  $\tau$  is surjective, then two  $G$ -sets are  $G$ -isomorphic if and only if they are  $\tau(H)$ -isomorphic, that is,  $H$ -isomorphic. Thus  $\tau^*$  is injective in this case. Conversely, assume  $\tau^*$  injective. By Exercise 9, we may choose  $x \in \Omega(G)$  such that  $\varphi_G(x) \neq 0$ ,  $\varphi_K(x) = 0$  for  $K < G$ . Then the restriction  $x_H$  (via  $\tau$ ) is nonzero in  $\Omega(H)$ , so  $\varphi_E(x_H) \neq 0$  for some  $E \leq H$ . But

$$\varphi_E(x_H) = |\text{inv}_E x_H| = |\text{inv}_{\tau(E)} x|,$$

so  $|\text{inv}_{\tau(E)} x| \neq 0$ . Therefore  $\tau(E) = G$ , so  $\tau$  is surjective.]

11. Let  $S, T$  be left  $G$ -sets, and define

$$S^T = \{f:T \rightarrow S\}, \text{ with } (xf)t = xf(x^{-1}t), \quad x \in G, \quad t \in T.$$

Then  $S^T$  is a left  $G$ -set. Prove:

(i) The map  $\psi:\Omega^+(G) \rightarrow \Omega(G)$ , defined by  $\psi[S] = [S^T]$ , is multiplicative, and is algebraic of degree  $\leq |T|$ .

(ii)  $\psi$  extends uniquely to a multiplicative map  $\psi':\Omega(G) \rightarrow \Omega(G)$ . For  $x \in \Omega(G)$ , denote  $\psi'(x)$  by  $x^T$ . Then:

(iii) For  $x, y \in \Omega(G)$  and for  $G$ -sets  $T, U$ , we have

$$(xy)^T = x^T y^T, \quad x^{T \cup U} = x^T \cdot x^U.$$

(iv) For  $H \leq G$ ,  $x \in \Omega(G)$ ,

$$\varphi_G(x^{G/H}) = |\text{inv}_G x^{G/H}| = |\text{inv}_H x| = \varphi_H(x),$$

where  $\varphi_G, \varphi_H$  are defined as in (80.7).

[Hint: See Dress-Küchler [70, p. 82] for details.]

12. Let  $S$  be an  $H$ -set, where  $H \leq G$ , and let  $\varphi_H, \varphi_G$  be as in (80.7). Show that  $\varphi_H[S] = \varphi_G[S^{\otimes G}]$ .

[Hint: Use (80.37) with  $S = e_G$ .]

13. Show that there is a homomorphism  $\Omega(G) \rightarrow \text{ch } QG$ , given by mapping each  $G$ -set  $S$  onto the character of  $G$  afforded by the permutation module  $Q[S]$ . Prove that there is a surjection of  $Q$ -algebras

$$Q \otimes_{\mathbb{Z}} \Omega(G) \rightarrow Q \otimes_{\mathbb{Z}} \text{ch } QG,$$

and show by example that the map need not be injective.

14. Let  $H \leq G$ ,  $|G:H| = n$ , and let  $S, T$  be  $H$ -sets. Prove that

$$(S \dot{\cup} T)^{\otimes G} \cong S^{\otimes G} \dot{\cup} T^{\otimes G} \dot{\cup} \left\{ \bigcup_i X_i \right\},$$

with each  $X_i$  a  $G$ -set induced from some proper subgroup of  $G$ .

[Hint: Define  $V_k$  as in (80.49), and show that for  $1 \leq k \leq n - 1$ , the  $G$ -stabilizer of each  $v \in V_k$  is a proper subgroup of  $G$ .]

15. Let  $E < H < G$ , and let  $S$  be an  $E$ -set. Prove that

$$(\text{ind}_E^H S)^{\otimes G}$$

is disjoint union of  $G$ -sets induced from proper subgroups of  $G$ .

16. Show that subgroups and factor groups of  $p$ -hypo-elementary groups are  $p$ -hypo-elementary.

17. Show that every  $G$ -functor  $F$  is a module over the Burnside functor  $\Omega$ .

[Hint: For  $H \leq G$ , let  $\Omega(H)$  act on  $F(H)$  thus:

$$[H/E] \cdot x = (e_E)^H \cdot x = (x_E)^H,$$

where  $E \leq H$  and  $x \in F(H)$ . Then check Frobenius reciprocity.]

## §81. REPRESENTATION RINGS

We shall study representations of a finite group  $G$  over some integral domain  $R$ , usually chosen as a field of characteristic  $p$  or a ring of  $p$ -adic integers. We restrict our attention always to  $RG$ -lattices, that is, f.g.  $RG$ -modules that are  $R$ -projective. For  $R$  a field, every f.g.  $RG$ -module is automatically a lattice; for  $R$  a P.I.D., the lattices are  $RG$ -modules with finite  $R$ -bases.

The algebraic framework for our investigation is the *representation ring*  $a(RG)$ . This is also called the *Green ring*, after J. A. Green [62b]. By definition,  $a(RG)$  is spanned over  $\mathbb{Z}$  by elements  $[M]$ , one for each isomorphism class of  $RG$ -modules. These elements are combined according to the formulas

$$[M] + [M'] = [M \oplus M'], \quad [M][M'] = [M \otimes_R M'],$$

where  $G$  acts diagonally in the inner tensor product  $M \otimes_R M'$ . Then  $a(RG)$  is a commutative ring with identity element  $[R]$ , where  $G$  acts trivially on  $R$ . Let  $M, N$  be  $RG$ -lattices; as in the proof of (38.20), we have  $[M] = [N]$  in  $a(RG)$  if and only if  $M \oplus X \cong N \oplus X$  for some  $RG$ -lattice  $X$ . If cancellation holds for  $RG$ -lattices, as is the case if  $R$  is a field or a complete d.v.r., then  $[M] = [N]$  if and only if  $M \cong N$ .

We are interested here in the problems about  $RG$ -lattices that arise from studying the algebraic structures of  $a(RG)$ . It is usually easier to work with the *representation algebra* (or *Green algebra*)

$$A_C(RG) = \mathbb{C} \otimes_{\mathbb{Z}} a(RG).$$

One also studies the rings

$$A_Q(RG) = Q \otimes_{\mathbb{Z}} a(RG), \quad \text{and} \quad A_Z(RG) = Z' \otimes_{\mathbb{Z}} a(RG),$$

where  $Z'$  is any commutative ring.

### §81A. Preliminary Results

In this section we shall collect some fundamental definitions and notation, involving ground field extension, relative projective modules, and induced modules. In many cases, the proofs are easy generalizations of those given in earlier sections, and are sketched briefly or sometimes omitted.

#### (I) *Ground Field Extension*

Throughout let  $G$  be a finite group, and  $K$  a field with  $\text{char } K = p \geq 0$ . We collect here some facts about indecomposability of  $KG$ -modules  $M$  where as usual we consider only f.g. modules. Given a  $KG$ -module  $M$ , we set

$$(81.1) \quad E(M) = \text{End}_{KG} M, \quad \tilde{E}(M) = E(M)/\text{rad } E(M).$$

By §6A,  $M$  is indecomposable if and only if  $E(M)$  is a local ring, or equivalently,  $\tilde{E}(M)$  is a division algebra. Note that both  $E(M)$  and  $\tilde{E}(M)$  are f.d./ $K$ , so if  $K$  is algebraically closed, then  $M$  is indecomposable if and only if  $\tilde{E}(M) \cong K$ .

In general, we call a  $KG$ -module  $M$  *absolutely indecomposable* if for each field  $K' \supseteq K$ , the  $K'G$ -module  $K' \otimes_K M$  is indecomposable. The discussion in §30B carries over to the present case, and we obtain the following analogue of (30.34), whose proof is left to the reader:

**(81.2) Theorem.** *For  $M$  a  $KG$ -module, define  $\tilde{E}(M)$  by (81.1). Then  $M$  is absolutely indecomposable if and only if  $\tilde{E}(M)$  is a field that is purely inseparable over  $K$ . In particular,  $M$  is absolutely indecomposable whenever  $\tilde{E}(M) \cong K$ . If  $K$  is algebraically closed, then every indecomposable  $KG$ -module is absolutely indecomposable.*

We shall next give a generalization of Exercises 15.6 and 15.7, concerning properties of direct summands under ground field extension. For a  $KG$ -module  $X$ , and a field  $L$  containing  $K$ , set  $X^L = L \otimes_K X$ , an  $LG$ -module. By (2.40) we have

$$\text{End}_{LG}(X^L) \cong L \otimes_K \text{End}_{KG} X.$$

As usual,  $X|Y$  means that  $X$  is isomorphic to a direct summand of  $Y$ . The following result may be viewed as a generalization of the Noether-Deuring Theorem (see Exercise 6.6):

**(81.3) Theorem.** *Let  $X$  and  $Y$  be  $KG$ -modules, and let  $L$  be an extension field of  $K$ . Then  $X^L|Y^L$  if and only if  $X|Y$ .*

*Proof.* Clearly  $X|Y$  implies  $X^L|Y^L$ . For the reverse implication, let  $X \cong V \oplus X_0$ ,  $Y \cong V \oplus Y_0$ . Then  $X_0^L|Y_0^L$ , and it suffices to prove that  $X_0|Y_0$ . Changing notation, we may assume that  $X$  and  $Y$  have no common direct summand, and that  $X^L|Y^L$ . We must show that  $X = 0$ , so assume  $X \neq 0$  and let us obtain a contradiction. Extending the field  $L$  if need be, we may assume that  $L$  contains an algebraic closure  $E$  of  $K$ . Then  $X^L = (X^E)^L$ , and we set

$$(*) \quad X^E = \bigoplus X_i, \quad Y^E = \bigoplus Y_j,$$

where the  $\{X_i\}$  and  $\{Y_j\}$  are absolutely indecomposable  $EG$ -modules (see (81.2) and the discussion preceding it). Then  $X_1^L$  is indecomposable, and is a direct summand of  $(Y^E)^L$ , so  $X_1^L \cong Y_j^L$  for some  $j$ , say  $j = 1$  to fix the notation. Therefore  $X_1 \cong Y_1$  by the Noether-Deuring Theorem.

Now let  $\pi: X^E \rightarrow X_1$  and  $\pi': Y^E \rightarrow Y_1$  be the idempotent projection maps associated with the decompositions in (\*). Then  $\pi \in \text{End}_{EG}(X^E) = E \otimes_K \text{End}_{KG} X$ , and since  $E/K$  is algebraic, it follows that  $E$  contains a field  $F$  that is f.d./ $K$ , and such that

$$\pi \in \text{End}_{FG}(X^F), \quad \pi' \in \text{End}_{FG}(Y^F).$$

We have

$$X_1 = \{\pi(X^F)\}^E \cong Y_1 = \{\{\pi'(Y^F)\}^E\},$$

so  $\pi(X^F) \cong \pi'(Y^F)$  by the Noether-Deuring Theorem. This shows that  $X^F$  and  $Y^F$  have a common direct summand. However,  $X^F \cong X^{(n)}$  and  $Y^F \cong Y^{(n)}$  as  $KG$ -modules, where  $n = \dim_K F$ . It follows that the  $KG$ -modules  $X^{(n)}$  and  $Y^{(n)}$  have a common direct summand, and therefore so do  $X$  and  $Y$ . This is a contradiction, and completes the proof.

**Remark.** The above argument also shows that if  $X^L$  and  $Y^L$  have a common direct summand, then so do  $X$  and  $Y$ .

To conclude these remarks about ground field extension, we consider the representation ring  $a(KG)$  and the representation algebra  $A(KG) = C \otimes_Z a(KG)$ . We note that for  $KG$ -modules  $M$  and  $N$ , we have  $[M] = [N]$  in  $a(KG)$  if and only if  $M \cong N$ . The Noether-Deuring Theorem (Exercise 6.6) then gives:

**(81.4) Proposition.** *Let  $E$  be an extension field of  $K$ . Then there are ring monomorphisms*

$$a(KG) \rightarrow a(EG), \quad A(KG) \rightarrow A(EG),$$

given by  $[X] \rightarrow [E \otimes_K X]$  for each  $KG$ -module  $X$ .

We now view  $A(KG)$  as embedded in  $A(EG)$ , and prove the following result of Benson-Parker [84]:

**(81.5) Theorem.** *Let  $E/K$  be a separable algebraic extension of fields. Then  $A(EG)$  is integral over its subring  $A(KG)$ .*

*Proof.* Each  $EG$ -module  $M$  affords a matrix representation of  $G$  with entries in some finite extension field of  $K$ . Thus for each  $x \in A(EG)$ ,  $E$  contains a subfield  $F$  finite over  $K$ , such that  $x$  lies in the image of  $A(FG)$  in  $A(EG)$ . It is therefore sufficient to prove the result for  $E/K$  finite.

Extending  $E$  if need be, we may assume that  $E/K$  is a finite Galois extension with Galois group  $\mathfrak{G}$ . Then  $\mathfrak{G}$  acts on  $A(EG)$ . Let  $a \in A(EG)$ . Clearly  $a$  is a zero of the polynomial

$$\prod_{\sigma \in \mathfrak{G}} (X - a^\sigma),$$

so we need only show that each coefficient lies in  $A(KG)$ . We note that each coefficient  $b$  lies in  $A(EG)$  and is fixed by  $\mathfrak{G}$ .

Let  $b = \sum \lambda_i [M_i]$ ,  $\lambda_i \in \mathbb{C}$ ,  $M_i = EG$ -module. For each  $EG$ -module  $M$  occurring in  $b$ , all of its  $\mathfrak{G}$ -conjugates also occur, and with the same coefficient. It thus suffices to show that if  $M_1, \dots, M_t$  are the distinct  $\mathfrak{G}$ -conjugates of  $M$ , then  $c = \sum_{i=1}^t [M_i] \in A(KG)$ . Now we have

$$\coprod_{\sigma \in \mathfrak{G}} M^\sigma \cong E \otimes_K M$$

by the proof of (33.18). On the other hand,  $\coprod_{\sigma \in \mathfrak{G}} [M^\sigma] = nc$ , where  $n$  is the order of the  $\mathfrak{G}$ -stabilizer of  $M$ . Thus  $nc \in A(KG)$ , so also  $c \in A(KG)$ , as desired.

## (II) Restriction, Induction, Conjugation

Let  $G$  be a finite group,  $R$  an integral domain, and denote the representation ring  $a(RG)$  by  $a(G)$ , for brevity. For  $H \leq G$ , the *restriction map*  $\text{res}_H^G: a(G) \rightarrow a(H)$  is a ring homomorphism. For  $x \in a(G)$ , set  $x_H = \text{res}_H^G x$  for brevity. The *induction map*  $\text{ind}_H^G: a(H) \rightarrow a(G)$ , given by  $y \mapsto y^G$ , is an additive homomorphism. Then  $a(G)$  is a Frobenius functor of  $G$  (see § 38A).

For  $H, K \leq G$ , write  $H \leq_G K$  to indicate that some  $G$ -conjugate of  $H$  is contained in  $K$ . A collection  $\mathcal{C}$  of subgroups of  $G$  is called *subconjugately closed* if

$$E \leq_G H \in \mathcal{C} \Rightarrow E \in \mathcal{C}.$$

For any  $\mathcal{C}$ , define

$$a(G)_{\mathcal{C}} = \sum_{H \in \mathcal{C}} a(H)^G, \quad a(G)^{\mathcal{C}} = \{x \in a(G): x_H = 0 \text{ for all } H \in \mathcal{C}\},$$

where  $a(H)^G$  means  $\text{ind}_H^G a(H)$ . By the Frobenius identities, both  $a(G)_{\mathcal{C}}$  and  $a(G)^{\mathcal{C}}$  are ideals of  $a(G)$ ; further,

$$a(G)_{\mathcal{C}} \cdot a(G)^{\mathcal{C}} = 0$$

by (38.13). Both ideals are unchanged if  $\mathcal{C}$  is replaced by its subconjugate closure. In keeping with the above notation, for  $H \leq G$  we write

$$a(G)^H = \{x \in a(G) : x_H = 0\}.$$

This notation is unorthodox, but unambiguous since for  $H \leq G$ , the superscript  $H$  cannot possibly indicate induction.

### (III) Relative Splitting and Relative Projective Modules

Throughout, “ $G$ -module” means “ $RG$ -lattice,” where  $R$  is some integral domain fixed during the discussion. Let

$$(81.6) \quad \xi: 0 \rightarrow L \rightarrow M \rightarrow N \rightarrow 0$$

be a  $G$ -ses, that is, a short exact sequence of  $G$ -modules. For  $H \leq G$ , restriction of operators gives an  $H$ -ses

$$\xi_H: 0 \rightarrow L_H \rightarrow M_H \rightarrow N_H \rightarrow 0.$$

If this latter sequence is split exact, we call  $\xi$   *$H$ -split*.

**(81.7) Proposition.** *Let  $H \leq G$ , and let  $\xi$  be any  $G$ -ses.*

- (i) *If  $\xi$  is  $H$ -split, then also  $\xi$  is  $E$ -split whenever  $E \leq_G H$ .*
- (ii)  *$\xi$  is  $H$ -split if and only if  $(\xi_H)^G$  is  $G$ -split.*
- (iii) *Let  $E \leq H$  be such that  $|H:E| \in R^*$ . Then  $\xi$  is  $H$ -split if and only if  $\xi$  is  $E$ -split.*
- (iv) *For any  $G$ -module  $M$ , set  $(M_H)^G = RG \otimes_{RH} M$ , and define a  $G$ -surjection  $\mu: (M_H)^G \rightarrow M$  by  $\mu(g \otimes m) = gm$ ,  $g \in G$ ,  $m \in M$ . Then the  $G$ -ses*

$$0 \rightarrow \ker \mu \rightarrow (M_H)^G \xrightarrow{\mu} M \rightarrow 0$$

*is  $H$ -split, and the splitting map  $i: M \rightarrow (M_H)^G$  such that  $\mu i = \text{id}_M$  is given by  $i(m) = 1 \otimes m$ ,  $m \in M$ .*

*Proof.* To prove (i), consider an  $H$ -splitting  $\theta: N \rightarrow M$  of a  $G$ -surjection  $f: M \rightarrow N$ . For  $E \leq H$ ,  $\theta$  is also an  $E$ -homomorphism. Thus if  $\xi$  is  $H$ -split, it is also  $E$ -split. Further, for  $x \in G$ , the  $x$ -conjugate of  $\theta$  gives an  $E^x$ -splitting of  $f$ . This completes the proof of (i). Assertion (iii) is obvious, while (iv) is established as in the proof of (19.3b).

To prove (ii), consider the diagram

$$\begin{array}{ccc} (M_H)^G & \xrightarrow{1 \otimes f} & (N_H)^G \\ \mu \downarrow \uparrow i & & \mu' \downarrow \uparrow i' \\ M & \xrightarrow{f} & N, \end{array}$$

where  $f$  is a  $G$ -surjection, and the vertical maps are as in (iv). The diagram commutes, using either upward or downward arrows. To prove (ii), it suffices to show that a  $G$ -splitting  $\psi:(N_H)^G \rightarrow (M_H)^G$  of  $1 \otimes f$  gives rise to an  $H$ -splitting of  $f$ . It is easily verified that  $\mu\psi i'$  is the desired  $H$ -splitting of  $f$ , which completes the proof.

Let  $H \leq G$ ; a  $G$ -module  $M$  is called  $(G, H)$ -projective if every  $G$ -ses

$$(81.8) \quad 0 \rightarrow X \rightarrow Y \rightarrow M \rightarrow 0$$

which is  $H$ -split is also necessarily  $G$ -split. There is a dual concept of  $(G, H)$ -injective  $G$ -modules. By (19.2), the following conditions are equivalent\*:

- (i)  $M$  is  $(G, H)$ -projective.
- (ii)  $M$  is  $(G, H)$ -injective.
- (iii) If  $G = \cup g_i H$ , then  $\sum_i g_i \gamma g_i^{-1} = \text{id}_M$  for some  $\gamma \in \text{End}_{RH} M$ .
- (iv)  $M \mid (M_H)^G$
- (v)  $M \mid L^G$  for some  $H$ -module  $L$ .

Every  $G$ -module is  $(G, G)$ -projective. At the other extreme, the  $(G, 1)$ -projective  $G$ -modules are the usual f.g. projective  $RG$ -modules, because of our agreement that “ $G$ -module” means “ $RG$ -lattice.” Note that if  $|G:H| \in R^*$ , we may choose  $\gamma = |G:H|^{-1}$  in (iii), so every  $G$ -module is  $(G, H)$ -projective in this case.

Generalizing the above, let  $\mathcal{C}$  be any collection of subgroups of  $G$ . We say that a  $G$ -ses  $\xi$  is  $\mathcal{C}$ -split if  $\xi$  is  $H$ -split for every  $H \in \mathcal{C}$ . A  $G$ -module  $M$  is  $(G, \mathcal{C})$ -projective if each  $G$ -ses (81.8) that is  $\mathcal{C}$ -split is necessarily  $G$ -split. Just as above, we have:

**(81.9) Proposition.** *Let  $\mathcal{C}$  be a nonempty set of subgroups of  $G$ , and let  $M$  be a  $G$ -module ( $= RG$ -lattice). The following are equivalent:*

- (i)  $M$  is  $(G, \mathcal{C})$ -projective.
- (ii)  $M$  is  $(G, \mathcal{C})$ -injective.
- (iii) There exist endomorphisms  $\varphi_C \in \text{End}_{RC} M$  such that

$$\sum_{C \in \mathcal{C}} \sum_{g_C} g_C \varphi_C g_C^{-1} = \text{id}_M,$$

where for each  $C \in \mathcal{C}$  the element  $g_C$  ranges over a cross section of left cosets  $G \setminus C$ .

- (iv)  $M \mid \coprod_{C \in \mathcal{C}} (M_C)^G$ .
- (v)  $M \mid \coprod_{C \in \mathcal{C}} (L(C))^G$ , where each  $L(C)$  is a  $C$ -module.

\*As usual,  $X \mid Y$  means  $X$  is isomorphic to a direct summand of  $Y$ .

*Sketch of Proof.* The  $G$ -surjection

$$f: \coprod_{C \in \mathcal{C}} (M_C)^G \rightarrow M$$

is always  $\mathcal{C}$ -split. If  $M$  is  $(G, \mathcal{C})$ -projective, there is a  $G$ -homomorphism  $\theta: M \rightarrow \coprod (M_C)^G$  that splits  $f$ . As in the proof of (19.2), it is easily seen that  $\theta = \coprod \theta_C$ , where for  $C \in \mathcal{C}$ ,

$$\theta_C(m) = \sum_{g_C} g_C \otimes \varphi_C(g_C^{-1}m), \quad m \in M,$$

with  $\varphi_C \in \text{End}_{RC} M$ . Then (iii) follows from the formula  $f\theta = \text{id}_M$ .

Next, for each  $C \in \mathcal{C}$  we can find a  $C$ -homomorphism  $\psi_C: M \rightarrow (M_C)^G$  splitting the  $G$ -surjection  $(M_C)^G \rightarrow M$ . Suppose now that (iii) holds. It is then easily checked that

$$\sum_{C \in \mathcal{C}} \sum_{g_C} g_C \psi_C \varphi_C g_C^{-1}$$

is a  $G$ -homomorphism from  $M$  into  $\coprod (M_C)^G$  that splits  $f$ . The proofs of the remaining equivalences among the above five conditions are as in (19.2), and are left to the reader.

It follows readily that if  $M$  is  $(G, \mathcal{C})$ -projective, so is  $M \otimes_R X$  for each  $G$ -module  $X$ . Further, if  $N$  is a  $C$ -module where  $C \in \mathcal{C}$ , the induced  $G$ -module  $N^G$  is necessarily  $(G, \mathcal{C})$ -projective and so is each direct summand of  $N^G$ . Now define  $a(G, \mathcal{C}) = \text{subgroup of } a(G) \text{ spanned by all } (G, \mathcal{C})\text{-projectives}$ . Then by the above,  $a(G, \mathcal{C})$  is an ideal of  $a(G)$ , and

$$(81.10) \quad a(G)_{\mathcal{C}} = \sum_{C \in \mathcal{C}} a(C)^G \subseteq a(G, \mathcal{C}) \subseteq a(G).$$

Furthermore, in  $a(G)$  we have

$$(81.11) \quad a(G, \mathcal{C}) \cdot a(G)^{\mathcal{C}} = 0.$$

(A. Dress has introduced a variant of the above concepts. Given a  $G$ -set  $S$ , form the permutation module  $R[S]$ . For any  $G$ -module  $M$ , let us set

$$M[S] = R[S] \otimes_R M \text{ (inner tensor product).}$$

We say that the  $G$ -ses  $\xi$  in (81.6) is  $S$ -split if the  $G$ -ses

$$\xi[S]: 0 \rightarrow L[S] \rightarrow M[S] \rightarrow N[S] \rightarrow 0$$

is  $G$ -split. Let  $S = \cup S_i$  be a partition of  $G$ -sets, and let  $f: M \rightarrow N$  be a  $G$ -homomorphism. Then  $1 \otimes f: R[S] \otimes M \rightarrow R[S] \otimes N$  carries  $M[S_i]$  onto  $N[S_i]$ . Therefore  $\xi$  is  $S$ -split if and only if  $\xi$  is  $S_i$ -split for each  $i$ .

Now let  $S_i$  be a transitive  $G$ -set, say  $S_i \cong G/H_i$  for some  $H_i \leq G$ . By (10.20),

$$R(G/H_i) \otimes_R M \cong (R_{H_i})^G \otimes_R M \cong (M_{H_i})^G.$$

Thus  $\xi[S_i]$  splits if and only if  $(\xi_{H_i})^G$  splits, and by (81.7ii) this occurs if and only if  $\xi$  is  $H_i$ -split. Given a  $G$ -set  $S$ , let

$$\mathcal{U}(S) = \{H \leq G : \text{inv}_H S \neq \emptyset\},$$

so  $\mathcal{U}(S)$  consists of all subgroups  $H \leq G$  that stabilize at least one element of the  $G$ -set  $S$ . The above discussion gives

$$\xi \text{ is } S\text{-split} \Leftrightarrow \xi \text{ is } H\text{-split for each } H \in \mathcal{U}(S).$$

In the same way, we can define what is meant by a  $G$ -module  $M$  to be  $(G, S)$ -projective. It is easily seen that  $M$  is  $(G, S)$ -projective if and only if  $M$  is  $(G, \mathcal{U}(S))$ -projective.)

#### (IV) Change of Groups

In § 80D, we used the Conlon Induction Theorem to establish a relation (80.61) between the representation algebra  $A(KG)$  and the algebras  $A(KH)$ , with  $H$  ranging over all  $p$ -hypo-elementary subgroups of  $G$ . Here,  $K$  is a field of characteristic  $p \geq 0$ . We now concentrate on a related question, that of comparing the algebras  $A(KG)$  and  $A(KH)$ , where  $H$  is a subgroup of  $G$ . The results are due to Benson-Parker [84], and the first is an easy consequence of our earlier calculations with Burnside rings.

**(81.12) Theorem.** *Let  $H \leq G$ , and let  $K$  be any field. Let*

$$A(KG) = C \otimes_Z a(KG), \quad A(KH)^G = \text{ind}_H^G A(KH), \quad A(KG)^H = \{x \in A(KG) : x_H = 0\}.$$

*Then  $A(KG)$  is a direct sum of ideals:*

$$A(KG) = A(KH)^G \oplus A(KG)^H.$$

*Proof.* Let  $\Omega(G)$  be the Burnside ring of  $G$  (see (80.1)). Then  $A(KG)$  is a Frobenius module over  $\Omega(G)$ , and so the desired result follows from the special case of (80.33) in which  $\mathcal{C}$  consists of the single subgroup  $H$ . Benson and Parker prove this theorem directly, but their argument is essentially the same as that which establishes the general formula (see (80.33))

$$A(KG) = A(KG)_{\mathcal{C}} \oplus A(KG)^{\mathcal{C}}$$

for any set  $\mathcal{C}$  of subgroups of  $G$ .

The next result, again due to Benson-Parker, is a bit more complicated. The simplified proof below is due to Landrock.

**(81.13) Theorem.** *Let  $H \leq G$ , and let  $K$  be any field. Set*

$$A(KG)_H = \text{res}_H^G A(KG), \quad {}^G A(KH) = \{x \in A(KH) : x^G = 0\}.$$

*Then  $A(KG)_H$  is an ideal of  $A(KH)$ , and*

$$A(KH) = A(KG)_H \oplus {}^G A(KH),$$

*a direct sum of vector spaces over  $\mathbb{C}$ .*

*Proof.* We show first that  $A(KH) = \tilde{A}$ , where we temporarily write

$$A(KG)_H + {}^G A(KH) = \tilde{A}.$$

For  $E \leq H$ , we shall prove by induction on  $|E|$  that

$$(*) \quad M^H \in \tilde{A} \text{ for each } KE\text{-module } M.$$

Once this is established, we take  $E = H$ , to obtain  $A(KH) = \tilde{A}$ .

When  $E = 1$ , we have

$$[(K_E)^H] = [KH] = |G:H|^{-1} \text{res}_H^G [KG] \in A(KG)_H,$$

so  $(*)$  holds when  $E = 1$ . Now let  $|E| > 1$ , and let  $M$  be a  $KE$ -module. Mackey's Formula gives

$$(M^G)_H \cong \coprod_x ({}^x M|_{x_E \cap H})^H, \quad \text{where } G = \dot{\cup} HxE.$$

The left-hand expression lies in  $A(KG)_H$ ; the terms on the right for which  $|{}^x E \cap H| < |E|$  lie in  $\tilde{A}$ , by the induction hypothesis. Finally, if  $x \in G$  is such that  ${}^x E \leq H$ , then the corresponding term on the right is

$$({}^x M|_{x_E})^H,$$

which differs from  $(M_E)^H$  by an element of  ${}^G A(KH)$ . It follows that

$$k[(M_E)^H] \in \tilde{A},$$

where  $k$  is the number of double coset representatives  $x$  for which  ${}^x E \leq H$ . This proves  $(*)$ , and shows that  $A(KH) = \tilde{A}$ .

It remains to show that

$$A(KG)_H \cap {}^G A(KH) = 0.$$

Let  $x$  lie in the intersection, and write  $x = z_H$  for some  $z \in A(KG)$ . Now

$$A(KG)_H \cdot {}^G A(KH) \subseteq {}^G A(KH)$$

by a Frobenius identity. Since  $A(KH) = \tilde{A}$ , we deduce that

$$A(KH) \cdot x \subseteq {}^G A(KH).$$

Therefore

$$z \cdot A(KH)^G = (z_H \cdot A(KH))^G = (x \cdot A(KH))^G = 0.$$

It follows from (81.12) that  $z \in A(KG)^H$ , that is,  $z_H = 0$ . This proves that  $x = 0$ , and establishes the theorem.

We conclude with an interesting result of Puig (see Benson-Parker [84, Prop. 5.3]), needed for our later work.

**(81.14) Theorem.** *For  $H \leq G$ ,  $A(KH)$  is integral over its subring  $\text{res}_H^G A(KG)$ .*

*Proof.* We drop the symbol  $K$ , and write  $A(G)_H$  instead of  $\text{res}_H^G A(KG)$ , so  $A(G)_H$  is an ideal in  $A(H)$ . Let  $N = N_G(H)$ , so  $N$  acts by conjugation on  $A(H)$ . Denote by  $\text{inv}_N A(H)$  the  $N$ -fixed subalgebra of  $A(H)$ . For  $a \in A(H)$ , the polynomial

$$\prod_{x \in N} (X - a^x)$$

has coefficients in  $\text{inv}_N A(H)$ , and  $X = a$  is a zero of the polynomial. Therefore  $A(H)$  is integral over  $\text{inv}_N A(H)$ . By “transitivity of integrality,” it thus suffices to show that  $\text{inv}_N A(H)$  is integral over  $A(G)_H$ . Using induction on  $|H|$ , we may assume the result for each  $E < H$ .

Given  $a \in \text{inv}_N A(H)$ , for each  $E < H$  we put

$$X(E) = \{\text{res}_E^{H^g}(a^g) : g \in G \text{ such that } E < H^g\},$$

and let

$$Y(E) = \text{subring of } A(E) \text{ generated by } A(G)_E \text{ and the finite set } X(E).$$

Then  $Y(E)$  is f.g. over  $A(G)_E$ , by the induction hypothesis. We now set

$$B = A(G)_H + \sum_{E < H} (Y(E))^H \subseteq A(H),$$

which is an  $A(G)_H$ -submodule of  $A(H)$ , since for  $\alpha \in A(G)$ ,  $\beta \in Y(E)$ , we have

$$\alpha_H \cdot \beta^H = (\alpha_E \cdot \beta)^H \in Y(E)^H.$$

We shall show that  $B$  is a ring containing  $a$ , and that  $B$  is f.g. as  $A(G)_H$ -module,

which will imply the desired conclusion that  $a$  is integral over  $A(G)_H$ . To show that  $a \in B$ , we use the fact that  $a^g = a$  for all  $g \in N$ , so Mackey's Formula gives

$$(a^G)_H = |N:H|a + \sum_x ((a^x)_{H \cap H^x})^H,$$

where  $x$  ranges over some elements of  $G - N$ . Each summand thus lies in  $X(E)^H$ , hence in  $B$ . Since  $(a^G)_H \in A(G)_H$ , we deduce that  $a \in B$ , as claimed.

To prove that  $B$  is a ring, let  $D < H$ ,  $E < H$ ,  $y \in Y(D)$ ,  $z \in Y(E)$ , and consider  $y^H \cdot z^H$  in  $A(H)$ . By Mackey's Formula,

$$y^H \cdot z^H = \sum_g ((y \cdot z^g)_{F_g})^H,$$

where  $g$  ranges over certain elements of  $G$ , and where  $F_g = D \cap E^g$ . Since  $y$  lies in the subring of  $A(E)$  generated by  $A(G)_E$  and  $X(E)$ , its restriction to  $F_g$  lies in the subring of  $A(F_g)$  generated by  $A(G)_{F_g}$  and  $X(E)_{F_g}$ . But  $X(E)_{F_g} \subseteq X(F_g)$  from the definitions of  $X(E)$  and  $X(F_g)$ . Likewise,  $(z^g)_{F_g} \in X(F_g)$ , so

$$((y \cdot z^g)_{F_g})^H \in X(F_g)^H \subseteq B.$$

Finally, for each  $E < H$ ,  $Y(E)$  is a f.g. module over  $A(G)_E$ , say

$$Y(E) = \sum A(G)_E \cdot c,$$

with  $c$  ranging over some finite subset of  $A(E)$ . For  $\alpha \in A(G)$ , we have

$$(\alpha_E \cdot c)^H = ((\alpha_H)_E \cdot c)^H = \alpha_H \cdot c^H \in A(G)_H c^H,$$

so

$$Y(E)^H = \sum A(G)_H c^H.$$

Thus  $B$  is f.g. as  $A(G)_H$ -module, and the proof is finished.

### §81B. Conlon's Theorems

Let  $R$  be either a complete d.v.r. with  $R/\mathfrak{p} = k$ ,  $\text{char } k = p > 0$ , or else  $R = k$  (and  $p > 0$ ). Our aim here is to prove Conlon's Theorems concerning decompositions of the representation algebra  $A(RG)$ , and the relations between idempotents in  $A(RG)$  and those in the Burnside algebra  $C \otimes_z \Omega(G)$ , where  $\Omega(G)$  is the Burnside ring of  $G$ . We shall follow the approach given in Benson [84a]. (For other treatments, see Conlon [68a], [68b], and Feit [82].)

An  $RG$ -lattice  $M$  will be called *permutation projective* (notation: pp), or a *trivial source module*, if  $M$  is a direct summand of a permutation module. The terminology is justified by the following result, used repeatedly throughout our discussion (see also Exercise 57.3).

**(81.15) Lemma.** *Let  $P \leq G$ , where  $P$  is a  $p$ -group.*

- (i) *The trivial module  $1_P$  has vertex  $P$ .*
- (ii) *For  $M \in \text{Ind } RG$ ,  $M$  is a pp module if and only if  $M$  has trivial source.*
- (iii) *If  $P \trianglelefteq G$ , then every indecomposable summand of  $(1_P)^G$  has vertex  $P$ .*
- (iv) *Let  $N = N_G(P)$ . For each indecomposable pp  $RN$ -lattice  $X$  of vertex  $P$  (and source  $1_P$ ), there exists an indecomposable  $RG$ -lattice  $Y$  of vertex  $P$  and source  $1_P$ , such that*

$$Y_N = X \oplus X'',$$

*where each indecomposable summand of  $X''$  has vertex  $< P$ . Further, for  $P \leq H \leq N$ ,*

$$Y_H = X_H \oplus (X'')_H,$$

*where the indecomposable summands of  $X_H$  have vertex  $P$ , while those of  $(X'')_H$  have vertices  $< P$ .*

*Proof.* Assertion (i) was proved in (57.29). For (ii), let  $M \in \text{Ind } RG$  be such that  $M|(1_H)^G$  for some  $H \leq G$ , and let  $\text{vtx } M = P$ . Then  $M_P|((1_H)^G)_P$ , so by Mackey's Formula the only summand of  $M_P$  of vertex  $P$  is  $1_P$ . Thus  $1_P$  is a source of  $M$ , by (19.15).

For (iii), assume  $P \trianglelefteq G$  and let  $M$  be an indecomposable summand of  $(1_P)^G$ , with vertex  $D$ . Then  $P$  acts trivially on  $M$ , and  $D \leq P$  since  $M$  is  $(G, P)$ -projective. Using the notation in §57A, we may write

$$\text{id}_M = T_{G/P} T_{P/D} \varphi \text{ for some } \varphi \in \text{End}_{RD} M.$$

But  $T_{P/D} \varphi = |P:D| \varphi$  since  $M$  is  $P$ -trivial. Therefore  $P = D$ , as desired.

To prove (iv), we start with a pp module  $X \in \text{Ind } RN$  of vertex  $P$ , and let  $Y \in \text{Ind } RG$  be its Green correspondent. By §20A,  $Y$  has vertex  $P$  and source  $1_P$ , and has a decomposition  $Y = X \oplus X''$  as above. Each indecomposable summand of  $X''_H$  has vertex  $< P$ , so it remains to prove that each indecomposable summand  $W$  of  $X_H$  has vertex  $P$ . Since  $X|(1_P)^N$  we have  $W|((1_P)^N)_H$ , so  $W|(1_P)^H$  by Mackey's Formula. But then  $W$  has vertex  $P$ , by (iii), and the lemma is established.

We next observe that the inner tensor product of pp modules is again pp, by virtue of Mackey's Formula

$$(81.16) \quad (1_E)^G \otimes (1_H)^G \cong \coprod_x (1_{E \cap H^x})^G,$$

where  $G = \dot{\cup} HxE$ .

We denote by  $PP(RG)$  the subring of the Green algebra  $A(RG)$  spanned (over  $\mathbb{C}$ ) by all pp  $RG$ -modules. This subring is also denoted by  $A(RG, \text{Triv})$ , the subring of trivial source modules. Note that for  $H \leq G$ ,  $\text{res}_H^G PP(RG) \subseteq PP(RH)$ .

**(81.17) Proposition.** *Let  $R$  be a complete d.v.r., with  $R/\mathfrak{p} = k$ . Reduction mod  $\mathfrak{p}$  gives a ring isomorphism*

$$PP(RG) \cong PP(kG).$$

*Proof.* We show first that for pp  $RG$ -lattices  $M$  and  $N$ , the map

$$(81.18) \quad \text{Hom}_{RG}(M, N) \rightarrow \text{Hom}_{kG}(\bar{M}, \bar{N})$$

is surjective, where  $\bar{M} = M/\mathfrak{p}M$ . It suffices to prove this when  $M = (1_E)^G$ ,  $N = (1_H)^G$ , with  $E, H \leq G$ , and we need only verify that the  $R$ -rank of the left-hand side of (81.18) equals the  $k$ -dimension of the right hand side. But

$$\text{Hom}_{RG}(M, N) \cong \text{inv}_G M^* \otimes N,$$

so it suffices to calculate the rank of  $\text{inv}_G [(1_E)^G \otimes (1_H)^G]$ . By (81.16), this rank is precisely the number of  $(H, E)$ -double cosets in  $G$ , since  $\text{inv}_G (1_{E \cap H^\ast})^G$  has rank 1. This completes the proof that the map (81.18) is surjective.

Now let  $M$  be any pp  $RG$ -lattice; then, by the above, the ring homomorphism  $\text{End}_{RG} M \rightarrow \text{End}_{kG} \bar{M}$  is surjective. By lifting idempotents, it follows that every direct sum decomposition of  $\bar{M}$  can be lifted to one of  $M$ . Further, if  $X$  and  $Y$  are summands of  $M$ , both of which are lifts of the summand  $V$  of  $\bar{M}$ , then  $\text{id}_V$  lifts to a pair of  $RG$ -maps  $f: X \rightarrow Y$  and  $g: Y \rightarrow X$ , whose composites  $fg$  and  $gf$  are  $1 \pmod{\mathfrak{p}}$ . Thus  $f$  and  $g$  are isomorphisms, by Nakayama's Lemma. It now follows that every pp  $kG$ -module lifts uniquely (up to isomorphism) to a pp  $RG$ -module, and the proof is complete.

We next introduce Brauer characters. For each  $kG$ -module  $V$ , we may define its Brauer character  $\varphi_V$  by first extending  $k$  to a sufficiently large field  $k'$ , and then computing the Brauer character of  $G$  afforded by the  $k'G$ -module  $k' \otimes_k V$ . This character  $\varphi_V$ , which is a complex valued function defined on  $G_{p'} (= \text{set of } p\text{-regular elements of } G)$ , determines the composition factors of  $k' \otimes_k V$ , by (17.10). These, in turn, determines the composition factors of  $V$ , by virtue of (16.22). In particular, if  $V$  is a *projective*  $kG$ -module, then by (21.23)  $V$  is determined up to isomorphism by its composition factors, and hence also by its Brauer character  $\varphi_V$ . In other words,  $V$  is determined by the map  $x \mapsto \varphi_V(x)$ ,  $x \in G_{p'}$ .

We apply this to prove:

**(81.19) Lemma.** *Let  $P$  be a normal  $p$ -subgroup of  $N$ , and let  $X \in \text{Ind } RN$  be a pp module with vertex  $P$ . Then  $P$  acts trivially on  $X$ , and  $X$  is projective as*

$R(N/P)$ -module. The  $k(N/P)$ -module  $\bar{X} = X/\mathfrak{p}X$  affords a Brauer character  $\varphi_{\bar{X}}$  of the group  $N/P$ , and this Brauer character determines  $\bar{X}$  (and  $X$ ) uniquely, up to isomorphism.

*Proof.* The hypotheses imply that  $X|(1_P)^N$ , so  $X$  is  $P$ -trivial because  $P \trianglelefteq N$ . Further,  $(1_P)^N \cong R(N/P)$  as  $(N/P)$ -modules, so  $X$  is projective as  $R(N/P)$ -module. Then  $\bar{X}$  determines  $X$  by (81.17), and  $\bar{X}$  is determined up to isomorphism by  $\varphi_{\bar{X}}$ .

Now let  $\mathcal{H}'$  be the set of  $p$ -hypo-elementary subgroups of  $G$ , defined as the set of all subgroups  $H \leq G$  with the property that  $H/O_p(H)$  is a cyclic  $p'$ -group, where  $O_p(H)$  denotes the largest normal  $p$ -subgroup of  $H$ . By Schur's Theorem 8.35, each  $p$ -hypo-elementary subgroup  $H$  can be expressed as a semidirect product:

$$H = P \rtimes C,$$

with  $P = O_p(H)$  and  $C$  a cyclic  $p'$ -subgroup. Note that  $C$  is not uniquely determined, although it is always true that  $C \cong H/P$ . (See also §80D.)

For each  $H \in \mathcal{H}'$  and each  $c \in H/P$ , we shall define a nonzero  $\mathbb{C}$ -algebra homomorphism (called a *species*)

$$s_{H,c}: PP(kG) \rightarrow \mathbb{C}$$

by defining the map on pp modules and then extending linearly. Specifically, given any pp  $kG$ -module  $V$ , we write

$$(81.20) \quad V_H = V' \oplus V'',$$

where each indecomposable summand of  $V'$  has vertex  $P$ , and each summand of  $V''$  has vertex  $< P$ . (Note that the vertex of any summand of  $V_H$  is necessarily  $\leq P$ .) Then both  $V'$  and  $V''$  are pp modules, since  $V_H$  is a pp module. By (81.19),  $V'$  is  $P$ -trivial, and is projective as  $k(H/P)$ -module, affording a Brauer character  $\varphi_{V'}$  of  $H/P$ . Let  $c$  be any element of the cyclic  $p'$ -group  $H/P$  (we will later assume  $c$  generates  $H/P$ ), and define

$$(81.21) \quad s_{H,c}[V] = \varphi_{V'}(c).$$

It follows readily that  $s_{H,c}$ , extended linearly, is a  $\mathbb{C}$ -algebra homomorphism from  $PP(kG)$  to  $\mathbb{C}$ .

**(81.22) Lemma.** *Keep the above notation.*

- (i)  $s_{H,c}$  is not the zero map.
- (ii) Assume that  $k$  is a splitting field for  $G$  and its subgroups, and let  $c, c' \in H/P$ . Then  $s_{H,c} = s_{H,c'}$  if and only if  $c$  and  $c'$  are conjugate in  $N/P$ , where  $N = N_G(P)$ .

*Proof.* Let  $X$  range over the indecomposable  $kN$ -modules of vertex  $P$  and source  $1_P$ , or equivalently, over all indecomposable projective  $k(N/P)$ -modules. By (81.15iv), for each  $X$  we can find an indecomposable  $kG$ -module  $V$  of vertex  $P$  and source  $1_P$ , such that

$$V_H = X_H \oplus V'',$$

where each indecomposable summand of  $X_H$  has vertex  $P$ , and where the summands of  $V''$  have smaller vertex. Then by definition of  $s_{H,c}$ , we have

$$s_{H,c}[V] = \varphi_X(c),$$

where  $X$  is viewed as a  $k(N/P)$ -module affording the Brauer character  $\varphi_X$ . By (21.22), the trivial character of  $N/P$  is expressible as a C-linear combination of the restrictions  $(\varphi_{X|H})$ . Hence it is impossible that  $\varphi_X(c) = 0$  for all  $X$ , which proves (i). Further, if  $k$  is a splitting field, the Brauer characters  $\{\varphi_X\}$  form a C-basis for the space of C-valued class functions on the  $p$ -regular elements of  $N/P$ , which implies (ii) and completes the proof.

**(81.23) Remark.** Dropping the hypothesis that  $k$  be a splitting field for  $G$ , we can still decide whether  $s_{H,c} = s_{H,c'}$ , where  $c, c'$  are  $p'$ -elements of  $N/P$ . We partition  $N/P$  into  $k$ -conjugacy classes as in §21C. Then by the Witt-Berman Theorem 21.25 and Theorem 21.22, the Brauer characters  $\{\varphi_X\}$  occurring above form a C-basis for the space of complex-valued functions that are constant on the  $p$ -regular  $k$ -conjugacy classes of  $N/P$ . Hence  $s_{H,c} = s_{H,c'}$  if and only if  $c$  and  $c'$  belong to the same  $k$ -conjugacy class of  $N/P$ . In particular, in this situation, the cyclic subgroups  $\langle c \rangle$  and  $\langle c' \rangle$  must be conjugate in  $N/P$ .

We have now constructed a family  $\{s_{H,c}\}$  of species of  $PP(kG)$ . We emphasize that if  $P = O_p(H)$ , then  $s_{H,c}$  vanishes on each indecomposable pp  $kG$ -module  $V$  of vertex  $< P$ , and is nonzero at some  $V$  of vertex  $P$ . It follows that if  $s_{H,c} = s_{H',c'}$ , then  $O_p(H') =_G P$ . Replacing  $H'$  by a conjugate subgroup, we may thus assume that  $O_p(H') = P$ , and therefore  $H' \leq N = N_G(P)$ . It follows that  $c$  and  $c'$  must be  $k$ -conjugate elements of  $N/P$ , by the above Remark 81.23, and the cyclic groups  $\langle c \rangle$ ,  $\langle c' \rangle$  must be conjugate in  $N/P$ . Further, if  $k$  is a splitting field, then  $c$  and  $c'$  are conjugate in  $N/P$ .

Whether or not  $k$  is a splitting field, let  $S = \{s_{H,c}\}$  be the set of species obtained by letting  $O_p(H)$  range over a full set of nonconjugate  $p$ -subgroups of  $G$ , and letting  $c$  range over nonconjugate  $p'$ -elements of  $N_G(P)/P$  such that  $H/P = \langle c \rangle$ . We now prove:

**(81.24) Theorem.** *The above-defined set  $S$  of species of  $PP(kG)$  separates elements of  $PP(kG)$ , that is, if  $\xi, \eta \in PP(kG)$  are such that  $s(\xi) = s(\eta)$  for all  $s \in S$ , then  $\xi = \eta$ .*

*Proof.* It suffices to prove the result when  $\eta = 0$ , so let  $\xi = \sum_{i=1}^t \alpha_i [M_i] \in PP(kG)$ ,

where  $\alpha_i \in C$  are nonzero, and the  $\{M_i\}$  are nonisomorphic indecomposable pp  $kG$ -modules. We assume  $t \geq 1$ , and that  $s(\xi) = 0$  for all  $s \in S$ , and try to obtain a contradiction.

Choose  $P \leq G$  maximal among the set of vertices of the  $\{M_i\}$ , and to fix the notation, suppose that  $M_1$  has vertex  $P$ . Set  $N = N_G(P)$ , and write

$$(M_i)_N = X_i \oplus Y_i, \quad 1 \leq i \leq t,$$

where the indecomposable summands of  $X_i$  have vertex  $P$ , and those of  $Y_i$  do not. From the choice of  $P$ , the vertices of the summands of  $Y_i$  do not contain  $P$ . Further,  $X_1 \neq 0$  since  $M_1$  has vertex  $P$ .

Now let  $c \in N/P$  range over a full set of nonconjugate  $p'$ -elements of  $N/P$ . For each  $c$ , choose  $H \in \mathcal{H}'$  so that  $O_p(H) = P$  and  $H/P = \langle c \rangle$ . Then we obtain a species  $s_{H,c} \in S$ . Now the vertex of each indecomposable summand of  $(Y_i)_H$  is  $< P$ . The proof of (81.15iv) then gives

$$s_{H,c}[M_i] = \varphi_{X_i}(c), \quad 1 \leq i \leq t,$$

where now  $X_i$  is viewed as a projective  $k(N/P)$ -module, and affords the Brauer character  $\varphi_{X_i}$  of  $N/P$ .

From the assumption that  $s(\xi) = 0$  for all  $s \in S$ , we thus conclude that

$$\sum_{i=1}^t \alpha_i \varphi_{X_i}(c) = 0$$

for each  $p'$ -element  $c \in N/P$ . However, the Brauer characters associated with nonisomorphic P.I.M.'s of  $N/P$  are linearly independent over  $C$ , by (18.26) and (18.27). It follows that for some  $i > 1$ ,  $X_i$  and  $X_1$  have a common indecomposable summand. By §20A, the Green correspondent of each indecomposable summand of  $X_1$  (of vertex  $P$ ) is an indecomposable  $kG$ -module of vertex  $P$ , and must therefore coincide with  $M_1$ . It follows that  $M_i \cong M_1$ , which is the desired contradiction, and completes the proof.

**(81.25) Corollary.** *Let  $M, N$  be pp RG-modules. Then  $M \cong N$  if and only if  $M_H \cong N_H$  for all  $H \in \mathcal{H}'$ .*

*Proof.* For an RG-lattice  $M$ , let  $\bar{M} = M/\mathfrak{p}M$ . Since  $PP(RG) \cong PP(kG)$  via reduction mod  $\mathfrak{p}$ , we need only show that if  $\bar{M}_H \cong \bar{N}_H$  for all  $H \in \mathcal{H}'$ , then  $\bar{M} \cong \bar{N}$ . But this is clear from (81.24).

**(81.26) Corollary.**  *$PP(RG)$  is a f.d. semisimple C-algebra. Letting  $s_i$  range over the distinct species in  $S$ , there exist primitive orthogonal idempotents  $\{e_i\}$  in  $PP(RG)$ , with sum 1, such that  $s_i(e_j) = \delta_{ij}$ .*

*Proof.* The commutative C-algebra  $PP(RG)$  is f.d./C, since it is spanned by the indecomposable components of  $(1_H)^G$ , with  $H \leq G$ . The algebra has no nonzero

nilpotent elements, since if  $\xi \in PP(RG)$  is such that  $\xi^n = 0$ , then  $s(\xi)^n = 0$  for each  $s \in S$ , and therefore  $s(\xi) = 0$  for each  $s$ . The assertions of the corollary are now clear.

We may use these ideas to give another proof of the Conlon Induction Theorem 80.51, and indeed what follows is essentially the same as Conlon's original proof. Starting with an arbitrary group  $G$ , let  $\Omega(G)$  be its Burnside ring, defined as in §80A, and let  $C \otimes_z \Omega(G)$  be its Burnside algebra. Let

$$\mathcal{S} = \{H_1, \dots, H_m\}$$

be a full set of nonconjugate subgroups of  $G$ . By (80.6) we have

$$C \otimes_z \Omega(G) = \bigoplus_{H \in \mathcal{S}} C[G/H].$$

By (80.12), there is a  $C$ -algebra isomorphism

$$\varphi: C \otimes_z \Omega(G) \cong C^{(m)},$$

given by

$$[T] \rightarrow ([\text{inv}_{H_1} T], \dots, [\text{inv}_{H_m} T])$$

for each  $G$ -set  $T$ . We may therefore find a set of orthogonal primitive idempotents  $\{\varepsilon_H : H \in \mathcal{S}\}$  in  $C \otimes_z \Omega(G)$ , such that

$$1 = \sum_{H \in \mathcal{S}} \varepsilon_H, \quad \text{and} \quad \varphi(\varepsilon_H) = (0, \dots, 1, 0, \dots, 0) \in C^{(m)},$$

where the  $m$ -tuple has entry 1 at the  $H$ -th place, and zeros elsewhere. In fact, the discussion in §80A shows that  $\varepsilon_H \in Q \otimes_z \Omega(G)$  for each  $H \in \mathcal{S}$ . Let us write

$$\varepsilon_H = \sum_{i=1}^m \alpha_i [G/H_i], \quad \alpha_i \in Q.$$

If  $\alpha_i \neq 0$  for some  $H_i$  not contained in a conjugate of  $H$ , choose a maximal such  $H_i$  (relative to  $\leq_G$ ). By (80.9), it follows that the  $i$ -th component of  $\varphi(\varepsilon_H)$  is nonzero, which is impossible. Therefore

$$(81.27) \quad \varepsilon_H = \sum_{H_i \leq_G H} \alpha_i [G/H_i]$$

for some rational coefficients  $\{\alpha_i\}$ .

Now let  $R$  be a complete d.v.r. and consider the algebra  $PP(RG)$  of pp  $RG$ -lattices. This is a  $C$ -subalgebra of the representation algebra  $A(RG)$ , and there is a  $C$ -algebra homomorphism

$$C \otimes_z \Omega(G) \rightarrow PP(RG), \quad \text{given by} \quad [T] \rightarrow [R[T]]$$

for each  $G$ -set  $T$ , where  $R[T]$  is the permutation module with the elements of  $T$  as  $R$ -basis. We shall use the idempotents  $\{\varepsilon_H : H \in \mathcal{S}\}$  in  $\mathbb{C} \otimes_z \Omega(G)$  to construct idempotents in  $PP(RG)$ . It is clear that for each  $\varepsilon_H$ , its image  $e_H \in PP(RG)$  is either idempotent or 0, and that  $1 = \sum e_H$  in  $PP(RG)$ .

Let  $S_0$  consist of the *distinct* species in the collection  $\{s_{H,c}\}$ , where  $H \in \mathcal{H}'$  ranges over all  $p$ -hypo-elementary subgroups of  $G$  (up to conjugacy), and  $H/O_p(H) = \langle c \rangle$ . Then there is an isomorphism of  $\mathbb{C}$ -algebras

$$\psi : PP(RG) \cong \mathbb{C}^{(n)}, \quad \text{where } n = |S_0|, \quad S_0 = \{s_1, \dots, s_n\},$$

given by

$$[M] \rightarrow (s_1[M], \dots, s_n[M])$$

for each pp  $RG$ -lattice  $M$ . We show at once:

**(81.28) Lemma.** *Keeping the above notation, there is a commutative diagram*

$$\begin{array}{ccc} \mathbb{C} \otimes_z \Omega(G) & \xrightarrow{\varphi} & \mathbb{C}^{(m)} \\ \downarrow & & \downarrow \rho \\ PP(RG) & \xrightarrow{\psi} & \mathbb{C}^{(n)}, \end{array}$$

where for  $f \in \mathbb{C}^{(m)}$ ,  $(\rho f)(s_{H,c}) = f(H)$ ,  $H \in \mathcal{H}'$ . Further, for each  $H \in \mathcal{S}$ , let the idempotent  $\varepsilon_H \in \mathbb{C} \otimes_z \Omega(G)$  have image  $e_H \in PP(RG)$ . Then  $e_H$  is a nonzero idempotent if and only if  $H \in \mathcal{H}'$ .

*Proof.* To prove the diagram commutative, we must show that for each  $G$ -set  $T$ ,

$$\rho \varphi[T] = \psi(R[T]),$$

that is, for each  $H \in \mathcal{H}'$  and  $H/O_p(H) = \langle c \rangle$ , we have

$$s_{H,c}(R[T]) = |\text{inv}_H T|.$$

It suffices to check this for  $T = G/D$ , a transitive  $G$ -set, where  $D \leq G$ . Let  $M = R[T]$ , so  $M \cong (R_D)^G$ , where  $R_D$  is the  $D$ -trivial module  $R$ . Then

$$M_H = \bigoplus_x (R_{D^x \cap H})^H, \quad \text{where } G = \dot{\cup} D x H.$$

To compute  $s_{H,c}(M)$ , we need to find the indecomposable summands of  $M_H$  of vertex  $P$ . The sum of these is precisely

$$M' = \bigoplus_x (R_{D^x \cap H})^H, \quad \text{where } D^x \cap H \geq P,$$

and then

$$\begin{aligned}s_{H,c}(M) &= \text{Brauer character of } \bar{M}' \text{ evaluated at } c. \\ &= \text{trace of } c \text{ acting on } M'.\end{aligned}$$

But if  $D^x \cap H < H$ , then the trace of  $c$  on  $(R_{D^x \cap H})^H$  is 0, and therefore

$$s_{H,c}(M) = \begin{cases} \text{number of double coset representatives } x \\ \text{such that } D^x \geq H. \end{cases}$$

But then  $s_{H,c}(M) = |\text{inv}_H G/D|$  by (80.5), which completes the proof of the first assertion of the lemma. The second follows at once from the first.

We remark that for  $H \in \mathcal{H}'$ ,  $\varphi(\varepsilon_H)$  is the  $m$ -tuple  $(0, \dots, 1, 0, \dots, 0)$ , with 1 at position  $H$ . It follows that

$$\psi(e_H) = (0, \dots, 0, 1, \dots, 1, 0, \dots, 0) \in \mathbb{C}^{(n)}$$

with 1's occurring at entries corresponding to the distinct species of  $PP(RG)$  of the form  $s_{H,c}$ . Thus we obtain for  $H \in \mathcal{H}'$ :

$$(81.29) \quad e_H = \sum_c e_{H,c},$$

the sum extending over generators  $c$  of  $H/O_p(H)$  for which the species  $s_{H,c}$  are distinct from one another. This gives a decomposition of  $e_H$  into primitive orthogonal idempotents in  $PP(RG)$ . Further, from (81.27) we obtain a formula

$$(81.30) \quad e_H = \sum_{H_i \leq H} \alpha_i [(1_{H_i})^G],$$

for some  $\alpha_i \in \mathbb{Q}$  and subgroups  $H_i$  of  $H$ . Each term in  $e_H$  is therefore  $(G, P)$ -projective, where  $P = O_p(H)$ . Since  $s_{H,c}(e_H) = 1$  for each  $c$ , it follows that  $e_H$  contains at least one term with vertex  $P$ .

As a first consequence of the preceding results, we obtain a new proof of the following theorem (compare with (80.51)):

**(81.31) Conlon's Induction Theorem.** *There exist rational numbers  $\{\alpha_H : H \in \mathcal{H}'\}$  such that*

$$[R_G] = \sum_{H \in \mathcal{H}'} \alpha_H [(R_H)^G] \quad \text{in } PP(RG).$$

*Proof.* From the formula

$$1 = \sum_{H \in \mathcal{S}} \varepsilon_H \quad \text{in } \mathbb{C} \otimes_{\mathbb{Z}} \Omega(G),$$

we obtain the equality

$$1 = \sum_{H \in \mathcal{H}'} e_H \quad \text{in } PP(RG),$$

with one summand  $e_H$  for each conjugacy class of groups in  $\mathcal{H}'$ . But we may write  $e_H$  as a  $\mathbb{Q}$ -linear combination of permutation modules, by (81.30). The rest of the argument is the same as in Step 1 of the proof of (80.51).

By (38.14), we obtain:

**(81.32) Corollary.** *Let  $\mathcal{H}'$  be the set of  $p$ -hypo-elementary subgroups of  $G$ . Then*

$$PP(RG) = \sum_{H \in \mathcal{H}'} \{PP(RH)\}^G, \quad A(RG) = \sum_{H \in \mathcal{H}'} \{A(RH)\}^G.$$

Further, if  $x \in A(RG)$  (or  $x \in PP(RG)$ ) is such that  $x_H = 0$  for all  $H \in \mathcal{H}'$ , then  $x = 0$ .

Combining the above results with formula (81.30), we obtain decompositions of  $1 \in A(RG)$  into orthogonal idempotents:

$$1 = \sum_{H \in \mathcal{H}'} e_H = \sum_{H,c} e_{H,c},$$

where  $H$  ranges over a full set of nonconjugate  $p$ -hypo-elementary subgroups of  $G$ , and for each  $H$ ,  $c$  ranges over generators of  $H/O_p(H)$  for which the species  $s_{H,c}$  of  $PP(RG)$  are distinct from one another. Consequently we obtain

$$(81.33) \quad A(RG) = \bigoplus_{H \in \mathcal{H}'} A(RG)e_H = \bigoplus_{H,c} A(RG)e_{H,c}.$$

Our next aim is to relate the above decomposition of  $A(RG)$  to the ideals  $A(G, H)$  of  $A(RG)$ , where, by definition  $A(G, H)$  is spanned over  $\mathbb{C}$  by the  $(G, H)$ -projective  $RG$ -modules. We remark that if  $P$  is a Sylow  $p$ -subgroup of  $H$ , then by (19.5) an  $RG$ -module is  $(G, H)$ -projective if and only if it is  $(G, P)$ -projective. Hence  $A(G, H) = A(G, P)$ , so in studying the ideals  $A(G, H)$ , there is no loss of generality in assuming that  $H$  is a  $p$ -group.

We begin with some simple remarks on ideals and rings. Let  $A$  be a commutative ring with 1, and let  $I$  be an ideal of  $A$ . Write  $I|A$  to indicate that  $I$  is an ideal direct summand of  $A$ , that is,  $A = I \oplus I'$  for some ideal  $I'$ . It will be convenient to view  $I$  as a ring, possibly without identity element. We leave it as exercise for the reader to prove:

**(81.34) Lemma.** *Let  $A$  be a commutative ring with 1, and let  $I$  be an ideal of  $A$ . Then we have:*

$$I|A \Leftrightarrow I \text{ has an identity element } e \Leftrightarrow I = Ae \text{ for some idempotent } e.$$

In this case,  $A$  decomposes uniquely as  $A = I \oplus A(1 - e)$ . Further,  $I|J$  for each bigger ideal  $J$ .

Next, assume that  $I \mid A$ , and that  $I \subseteq J \subseteq A$ . If  $J/I$  has an identity element, then

$J \mid A$ , and  $J = I \oplus L$  for some unique ideal  $L$  of  $A$ .

We have  $L \mid A$ , and  $J/I \cong L$ .

Now let  $P$  be a  $p$ -subgroup of  $G$ , and denote by  $a(G, P)$  the ideal of  $a(RG)$  spanned by  $(G, P)$ -projective  $RG$ -lattices. We need next a result of Green [64], which reduces the study of  $a(G, P)$  to the case where  $P \trianglelefteq G$ . We set

$$a'(G, P) = \sum_{D \leq P} a(G, D), \quad A'(G, P) = C \otimes_Z a'(G, P).$$

Then we have, as a direct consequence of (20.8):

**(81.35) Green's Transfer Theorem.** Let  $P$  be a  $p$ -subgroup of  $G$ , and let  $N_G(P) \leq H \leq G$ . There is an isomorphism of rings

$$a(G, P)/a'(G, P) \cong a(H, P)/a'(H, P),$$

induced by the Green correspondence in (20.8). Specifically, the left-hand side is spanned by all  $M \in \text{Ind } RH$  with vertex  $P$ , and the isomorphism is given by

$$[M] + a'(G, P) \rightarrow [N] + a'(H, P),$$

where  $N \in \text{Ind } RH$  is the Green correspondent of  $M$ , i.e.,

$$M_H \cong N \oplus \text{element of } a'(H, P), \quad N^G \cong M \oplus \text{element of } a'(G, P).$$

The isomorphism preserves the property of being permutation projective. We conclude the subsection with two results that will be applied in §81E.

**(81.36) Conlon's Theorem.** Let  $R$  be either a complete d.v.r. with  $R/\mathfrak{p} = k$ , or else  $R = k$ , where  $k$  be a field of characteristic  $p > 0$ . Let  $P$  be a  $p$ -subgroup of  $G$ , and define  $A(G) = A(RG)$ ,  $A(G, P)$ , and  $A'(G, P)$  as above.

(i)  $A(G, P)$  is an ideal direct summand of  $A(G)$ , with an idempotent generator  $e_P$  that belongs to  $PP(RG)$ .

(ii) There is a uniquely determined ideal direct summand  $A''(G, P)$  of  $A(G)$ , such that

$$A(G, P) = A'(G, P) \oplus A''(G, P).$$

(iii) We have

$$A(G, P) = \bigoplus_{D \leq P} A''(G, D)$$

where  $D$  ranges over a cross section of the  $G$ -conjugacy classes of subgroups of  $P$ .

*Proof.* Step 1. Assume that  $P \trianglelefteq G$ , and that  $R = k$ . Denote by  $i(G, P)$  the ideal of  $a(G)$  spanned (over  $\mathbb{Z}$ ) by all expressions  $[X] - [X'] - [X'']$  arising from ses's of  $kG$ -modules

$$0 \rightarrow X' \rightarrow X \rightarrow X'' \rightarrow 0$$

which are  $P$ -split (see §81A), and let  $I(G, P) = \mathbb{C} \otimes_{\mathbb{Z}} i(G, P)$ . In the extreme case where  $P = 1$ , the quotient  $a(G)/i(G, 1)$  is precisely the Grothendieck ring  $G_0(kG)$  defined in §16C. Further,  $a(G, 1)$  is the ideal of  $a(G)$  spanned by projective  $kG$ -modules, i.e.,  $a(G, 1) = K_0(kG)$ . The map

$$K_0(kG) = a(G, 1) \rightarrow a(G)/i(G, 1) = G_0(kG)$$

is just the Cartan homomorphism  $c$ . By (21.22),  $c$  is an isomorphism mod torsion, so there are isomorphisms

$$\mathbb{C} \otimes_{\mathbb{Z}} a(G, 1) \cong A(G)/I(G, 1) \cong \mathbb{C} \otimes_{\mathbb{Z}} G_0(kG).$$

We apply the above with  $G$  replaced by  $\bar{G}$ , where  $\bar{G} = G/P$ . It follows that there exists an element  $y_0 \in A(\bar{G}, 1)$  whose image (under the Cartan map) is the identity element of  $A(\bar{G})/I(\bar{G}, 1)$ , and thus  $1 - y_0 \in I(\bar{G}, 1)$ . By inflation, each  $\bar{G}$ -module becomes a  $G$ -module on which  $P$  acts trivially. It follows that the map  $\inf: A(\bar{G}) \rightarrow A(G)$  maps  $A(\bar{G}, 1)$  into  $A(G, P)$ , and  $I(\bar{G}, 1)$  into  $I(G, P)$ . Letting  $y = \inf y_0$ , we now have

$$y \in A(G, P), \quad 1 - y \in I(G, P).$$

But  $A(G, P) \cdot I(G, P) = 0$  by (81.11), so  $y(1 - y) = 0$  and  $y$  is an idempotent. Further, since

$$\inf k\bar{G} \cong (k_p)^G,$$

we have  $y \in PP(kG)$ . Thus we obtain

$$A(G) = A(G, P) \oplus I(G, P),$$

and the idempotent generator  $y$  of  $A(G, P)$  lies in  $PP(kG)$ , so (i) holds in this case.

Step 2. We continue with our assumption  $P \trianglelefteq G$  and deal with the case when  $R$  is a d.v.r. It follows from Maranda's Theorem (30.14) that for some integer  $t$ , reduction mod  $p^t$  gives an embedding of  $A(RG)$  into  $A((R/p^t)G)$ . Note that Maranda's Theorem works in our situation with a group ring, because the property used in the proof is that  $|G|$  annihilates Ext groups. Now the argument of Step 1 works exactly as given to yield (in an obvious notation)

$$A((R/p^t)G) = A((R/p^t)G, H) \oplus I((R/p^t)G, P),$$

where the first summand is generated by an idempotent  $x$  lying in  $PP((R/p^t)G)$ . By liftability of permutation projective modules (as in (81.17)),  $x$  is the reduction mod  $p^t$  of an idempotent  $y \in PP(RG)$ , and furthermore  $1 - y$  annihilates  $A(RG, P)$  in  $A(RG)$ , since its image  $1 - x$  annihilates  $A((R/p^t)G, P)$  and this contains the image of  $A(RG, P)$  under reduction. Thus since  $y$  lies in  $A(RG, P)$ , it generates it as an ideal of  $A(RG)$  and we obtain

$$A(RG) = A(RG, P) \oplus I(RG, P)$$

where the second summand is the ideal generated by  $1 - y$ .

*Step 3.* We have now established (i) for the case  $P \trianglelefteq G$ , and proceed to prove the theorem by induction on  $|P|$ , noting that it holds for  $P = 1$  by the previous steps. Let  $|P| > 1$ , and assume the theorem holds for  $p$ -groups  $D < P$ . Then for each such  $D$ , we have (choosing one  $D$  from each class of  $G$ -conjugates):

$$A(G, D) = A(G)i_D, \quad A(G, D) = \bigoplus_{E \leq D} A''(G, E) \quad i_D \in PP(RG).$$

Now set

$$e = 1 - \prod_{D < P} (1 - i_D) \in A'(G, P).$$

Then  $e$  acts as 1 on  $A'(G, P)$ , and  $e \in PP(RG)$ . Further,  $e \neq 0$  since  $e$  acts as 1 on  $A(G, 1)$ , so  $e$  is an idempotent. Therefore (ii) holds with  $A''(G, P) = A(G, P) \cdot (1 - e)$ .

We now use the ring isomorphism in (81.35), with  $H = N_G(P)$ , to obtain:

$$A(N, P)/A'(N, P) \cong A(G, P)/A'(G, P) \cong A''(G, P).$$

By the previous steps,  $A(N, P)/A'(N, P)$  has an identity element, namely, the idempotent generator of  $A(N, P)$ . It follows from (81.34) that  $A''(G, P)$  has an idempotent generator in  $PP(kG)$ , which establishes both (i) and (ii). Assertion (iii) follows from the fact that  $A''(G, P)$  has as basis  $\{[M] + A'(G, P) : M \in \text{Ind } RG, \text{ vertex } M = P\}$ . This completes the proof of the theorem.

The above proof shows that for each  $p$ -subgroup  $P \leq G$ , there exist idempotents  $i_P$ ,  $i'_P$ , and  $i''_P \in PP(kG)$ , such that

$$(81.37) \quad A(G, P) = A(G)i_P, \quad A'(G, P) = A(G)i'_P, \quad A''(G, P) = A(G)i''_P,$$

with  $i_P = i'_P + i''_P$ ,  $i'_Pi''_P = 0$ . Next, we may express those idempotents in terms of the primitive idempotents  $\{e_{H,c}\}$  of  $PP(kG)$ . Clearly,  $i_P$  is the sum (over all pairs  $H, c$  yielding distinct species of  $PP(kG)$ ) of those  $e_{H,c}$  that lie in  $A(G, P)$ . The discussion preceding (81.31) shows that  $e_{H,c} \in A(G, P)$  if and only if  $O_p(H) \leq P$ . Therefore we

obtain

$$(81.38) \quad i_P = \sum_{\substack{H,c \\ O_p(H) \leq P}} e_{H,c} \quad i'_P = \sum_{\substack{H,c \\ O_p(H) < P}} e_{H,c}, \quad i''_P = \sum_{\substack{H,c \\ O_p(H) = P}} e_{H,c}.$$

Note that by (81.29) we may also write

$$(81.39) \quad i_P = \sum_{O_p(H) \leq P} e_H, \quad i'_P = \sum_{O_p(H) < P} e_H, \quad i''_P = \sum_{O_p(H) = P} e_H.$$

In view of formula (81.30), we may write

$$(81.40) \quad i''_P = \sum_j \beta_j [(1_{H_j})^G], \quad \beta_j \in \mathbb{Q}$$

where the  $H_j$  are  $p$ -hypo-elementary subgroups of  $G$  such that  $O_p(H_j) \leq P$ . Using this, we prove:

**(81.41) Proposition (Conlon).** *Let  $P$  be a  $p$ -subgroup of  $G$ , and let  $\mathcal{H}^*$  be the set of  $p$ -hypo-elementary subgroups  $H$  of  $G$  for which  $O_p(H) = P$ . Then there is a monomorphism of  $\mathbb{C}$ -algebras*

$$A''(G, P) \rightarrow \coprod_{H \in \mathcal{H}^*} A''(H, P).$$

*Proof.* For  $H \in \mathcal{H}^*$ , we identify  $A''(H, P)$  with  $A(H, P)/A'(H, P)$ , and define the map  $A''(G, P) \rightarrow A''(H, P)$  via restriction from  $G$  to  $H$ . Now let  $\xi \in A''(G, P)$  be such that  $\xi \rightarrow 0$  at each  $H \in \mathcal{H}^*$ , i.e.,  $\xi_H \in A'(H, P)$  for each  $H \in \mathcal{H}^*$ . We must prove that  $\xi = 0$ . By (81.40),

$$\xi = i''_P \xi = \sum_j \beta_j [(1_{H_j})^G \otimes \xi] = \sum_j \beta_j (\xi_{H_j})^G.$$

But for those  $H_j$  with  $O_p(H_j) < P$ , we have  $\xi_{H_j} \in A'(G, P)$ . Thus in  $A''(G, P)$  we may write

$$\xi = \sum_{O_p(H_j) = P} \beta_j ((\xi_{H_j})^G).$$

By hypothesis,  $\xi_{H_j} = 0$  for each  $H_j$  in the above, so  $\xi = 0$  as desired.

The preceding results will play a vital role in the proof of the Benson-Carlson Theorem 81.87 below.

### §81C. Species

Let  $G$  be a finite group, and  $k$  a field of characteristic  $p$ . In §§81A, B we studied the representation algebra  $A(kG)$ , spanned over  $\mathbb{C}$  by all f.g.  $kG$ -modules. This is a commutative  $\mathbb{C}$ -algebra, and is f.d./ $\mathbb{C}$  if and only if the Sylow  $p$ -subgroups of  $G$  are

cyclic. In  $A(kG)$  there is the important subalgebra  $PP(kG)$ , spanned by permutation projective  $kG$ -modules. We have seen in §81B that the decomposition of  $PP(kG)$  into ideals yields important information about  $A(kG)$  itself. Furthermore, the structure of  $PP(kG)$  can be determined by constructing a set of nonzero algebra homomorphisms (called *species*) from  $PP(kG)$  into  $\mathbb{C}$ . We shall discuss here the Benson-Parker theory of species on the  $\mathbb{C}$ -algebra  $A(kG)$ , as described in Benson-Parker [84] and Benson [84a].

It should be pointed out that  $A(kG)$  may contain nonzero nilpotent elements, and for each such element  $x$  we have  $f(x) = 0$  for every species  $f$  of  $A(kG)$ . Thus, we cannot expect that species can serve to separate the elements of  $A(kG)$ , but nevertheless they may provide interesting information about its structure.

We begin with some general remarks on species of arbitrary commutative  $\mathbb{C}$ -algebras.

Let  $A$  be a commutative  $\mathbb{C}$ -algebra, not necessarily f.d. A *species* of  $A$  is a nonzero  $\mathbb{C}$ -algebra homomorphism  $f:A \rightarrow \mathbb{C}$ . We use the same terminology whether or not  $A$  has an identity element, so in particular we can talk about species of ideals of  $A$ . If  $\{e_1, \dots, e_n\}$  are a set of orthogonal idempotents of  $A$  with  $\sum e_i = 1$ , then for each species  $f$  of  $A$ , there is a unique  $i$  such that  $f(e_i) = 1$ ,  $f(e_j) = 0$  for  $j \neq i$ , and in this case  $f$  is also a species of  $Ae_i$ . In particular, when  $A$  is  $\mathbb{C} \times \dots \times \mathbb{C}$  ( $n$  copies), then  $A$  has precisely  $n$  distinct species.

We note that any set of distinct species of a  $\mathbb{C}$ -algebra  $A$  must be linearly independent over  $\mathbb{C}$ , by the proof of Artin's Theorem in Exercise 7.11. Next, if  $I$  is any ideal of  $A$ , then each species  $f:I \rightarrow \mathbb{C}$  extends uniquely to a species  $g$  of  $A$ . Indeed, choose  $x \in I$  such that  $f(x) = 1$ , and then set  $g(a) = f(ax)$ ,  $a \in A$ . It is easily verified that  $g$  is the unique extension of  $f$  and is independent of the choice of  $x$ .

Given an algebra homomorphism  $\varphi:A \rightarrow B$ , each species  $g:B \rightarrow \mathbb{C}$  lifts to a homomorphism  $f:A \rightarrow \mathbb{C}$ , with  $f = g\varphi$ . Then  $f$  is a species of  $A$  if and only if  $g(\varphi(A)) \neq 0$ , i.e.,  $\varphi(A) \not\subseteq \ker g$ . In particular, if  $\varphi$  maps  $A$  onto  $B$ , then every species of  $B$  lifts uniquely to a species of  $A$ .

**(81.42) Example.** Let  $(K, R, k)$  be a  $p$ -modular system for  $G$ . With each  $kG$ -module  $V$  there is associated its Brauer character  $\varphi_V$ , defined as the Brauer character of  $k' \otimes_k V$  for  $k'$  sufficiently large. Then  $\varphi_V$  is a complex-valued class function defined in  $G_{p'}$ , the set of  $p'$ -elements of  $G$ . For each  $x \in G_{p'}$ , define a homomorphism  $b_x:A(kG) \rightarrow \mathbb{C}$  by the formula

$$b_x[V] = \varphi_V(x) \quad \text{for each } kG\text{-module } V,$$

and then extend  $b_x$  by linearity. Since  $b_x[1] = 1$ ,  $b_x \neq 0$ . It follows from (17.13) that  $b_x$  is a species of  $A(kG)$ , and is called a *Brauer species*.

Let  $G_0(kG)$  be the Grothendieck ring of  $kG$ . The map  $b_x$  defined above is actually a species of  $\mathbb{C} \otimes_{\mathbb{Z}} G_0(kG)$ , which lifts to a species of  $A(kG)$  via the surjection  $A(kG) \rightarrow \mathbb{C} \otimes_{\mathbb{Z}} G_0(kG)$ .

If  $K$  is sufficiently large, then by §17,

$$\begin{aligned} \mathbb{C} \otimes_{\mathbb{Z}} G_0(kG) &\cong \mathbb{C} \otimes_{\mathbb{Z}} \text{Bch } kG \\ &\cong \text{ring of complex-valued class functions on } G_{p'}. \end{aligned}$$

If  $r$  denotes the number of  $p$ -regular classes of  $G$ , then we obtain  $r$  distinct species  $\{b_x\}$  on  $A(kG)$ , by letting  $x$  range over representatives of the  $p$ -regular classes.

**(81.43) Example.** Let  $k = \mathbb{F}_2$  and let  $G$  be cyclic of order 2. The indecomposable  $kG$ -modules are  $k$  and  $kG$ , and so

$$A(kG) = \mathbb{C} \cdot 1 \oplus \mathbb{C} \cdot y, \quad \text{where } y = [kG].$$

We have  $y^2 = 2y$  in  $A(kG)$ . There is only one Brauer species of  $A(kG)$ , given by  $[V] \mapsto \dim_K V$  for  $V = kG$ -module. There is a second species  $f$ , given by  $f(1) = 1$ ,  $f(y) = 0$ .

Keeping the field  $k$  fixed, let us write  $A(G)$  instead of  $A(kG)$ . We may often construct species of  $A(G)$  by lifting species of  $A(H)$ , where  $H \leq G$ . Consider the diagram

$$\begin{array}{ccc} A(G) & \xrightarrow{\text{res}} & A(H) \\ & f \searrow & \downarrow g \\ & & \mathbb{C} \end{array}$$

Starting with a species  $g$ , we may define  $f$  as  $g \circ \text{res}$ , and then  $f$  is a species if and only if  $g(\text{res } A(G)) \neq 0$ . Conversely, starting with a species  $f$ , we say that  $f$  factors through  $H$  if there exists a species  $g$  for which the diagram commutes, that is, for which

$$(81.44) \quad f(x) = g(x_H) \quad \text{for all } x \in A(G).$$

(In this case, we write  $g \rightarrow f$ , and say that  $g$  fuses to  $f$ .)

**(81.45) Lemma.** Let  $H \leq G$ , and let  $f$  be a species of  $A(G)$ . The following are equivalent:

- (i)  $f$  factors through  $H$ .
- (ii)  $\ker f \supseteq A(G)^H = \{x \in A(G) : x_H = 0\}$ .
- (iii)  $\ker f \not\supseteq A(H)^G = \text{ind}_H^G A(H)$ .

*Proof.* The implication (i)  $\Rightarrow$  (ii) is clear from (81.44). Conversely, assume (ii):

then there is a unique species  $f': A(G)_H \rightarrow C$ , defined by

$$f'(\xi_H) = f(\xi) \quad \text{for } \xi \in A(G).$$

By (81.14),  $A(H)$  is integral over its subring  $A(G)_H$ . By the “Going-Up Theorem” (see Atiyah-MacDonald [69, p. 62]),  $f'$  lifts to a species  $g$  of  $A(H)$ , so  $f$  factors through  $H$ .

Next, we use the decomposition of  $A(G)$  into ideals

$$A(G) = A(H)^G \oplus A(G)^H$$

(see (81.12)). Given a species  $f$ , let  $I = \ker f$ ; then  $A(G)/I \cong C$ , so  $I$  is a maximal ideal of  $A(G)$ . Thus  $I$  contains exactly one of the ideals  $A(H)^G$  and  $A(G)^H$ , so (ii) and (iii) are equivalent.

**(81.46) Definition.** Let  $f$  be a species of  $A(G)$ . An *origin* of  $f$  is a subgroup  $H \leq G$  that is minimal among those subgroups of  $G$  through which  $f$  factors.

By (81.45), the origin of  $f = H$  if and only if

$$f(A(H)^G) \neq 0 \quad \text{and} \quad f(A(K)^G) = 0 \quad \text{for } K <_G H.$$

Further, if  $g$  is a species of  $A(H)$  that fuses to  $f$ , and the origin of  $f = H$ , then also the origin of  $g = H$  (see Exercise 11).

**(81.47) Proposition.** *For a species  $f$  of  $A(G)$ , its origins form a class of conjugate subgroups of  $G$ .*

*Proof.* It is clear from the preceding remarks that conjugates of origins are again origins. Now let  $H$  and  $K$  be two origins of  $f$ . Then  $\ker f$  is a maximal ideal of  $A(G)$  that does not contain either  $A(H)^G$  or  $A(K)^G$ , and so does not contain their product. But Mackey’s Formula gives

$$A(H)^G \cdot A(K)^G \subseteq \sum_x A(H^x \cap K)^G,$$

summed over certain elements  $x \in G$ . Therefore  $\ker f \not\supseteq A(H^x \cap K)^G$  for some  $x$ , and so  $f$  factors through  $H^x \cap K$ . The minimality of  $H$  and  $K$  then gives  $H^x = K$ , as desired.

In the preceding discussion, we can replace the representation algebra  $A(G)$  by the algebra  $PP(kG)$  of pp  $kG$ -modules, and omit the symbol  $k$  for convenience. The algebra  $PP(G)$  behaves well with respect to the induction and restriction maps, and the Mackey Formulas still hold in this context. The proof of (81.14) carries over to the algebra  $PP(G)$ , to show that for  $H \leq G$ ,  $PP(H)$  is integral over its subring  $\text{res}_H^G PP(G)$ . Furthermore, using (80.33) with  $M(G) = PP(G)$ , we obtain

$$(81.48) \quad PP(G) = PP(E)^G \oplus PP(G)^E = \text{ind}_E^G PP(E) \oplus \{x \in PP(G) : x_E = 0\}.$$

The analogue of Lemma 81.45 clearly holds for the present case, and we can again define species of  $PP(G)$ , and their origins, just as above.

We now determine the origin of the species  $s = s_{H,c}$  of  $PP(G)$  constructed in §81B, where  $H$  is a  $p$ -hypo-elementary subgroup of  $G$ , and  $H/O_p(H) = \langle c \rangle$ .

**(81.49) Proposition.** *The species  $s_{H,c}$  of  $PP(G)$  has origin  $H$ .*

*Proof.* Let  $s = s_{H,c}$ ; we must show that  $s$  factors through  $H$ , but not through any proper subgroup  $K < H$ . Using the notation in (81.20), for each pp  $kG$ -module  $V$  we have  $s[V] = \varphi_V(c)$ , so  $s[V]$  is determined by  $V_H$ , and therefore  $s$  factors through  $H$ .

Now let  $H = P \rtimes C$ ,  $K = P_0 \rtimes C_0$ , where  $P_0 \leq P$ ,  $C_0 \leq C$ ,  $P = O_p(H)$ ,  $C = \langle c \rangle$ . If  $P_0 < P$ , then each indecomposable  $kG$ -module in  $PP(K)^G$  has vertex  $\leq P_0$ , and thus  $s$  vanishes on  $PP(K)^G$ . Therefore  $f$  cannot factor through  $K$  in this case, and so necessarily  $K = P \rtimes C_0$ . The proof of (81.22) shows that as  $X$  ranges over all indecomposable projective  $k(N/P)$ -modules, for each  $X$  there exists a pp  $kG$ -module  $V$  such that  $s[V] = \varphi_X(c)$ , where  $\varphi_X$  is the Brauer character of  $N/P$  afforded by  $X$ . If  $s$  factors through  $K$ , then  $s[V]$  is determined by  $V_K$ , or equivalently, by the way that  $c_0$  acts on  $X$ , where  $C_0 = \langle c_0 \rangle$ . By Remark 81.23 we conclude that  $c_0$  and  $c$  generate conjugate subgroups of  $N/P$ , and therefore  $C_0 = C$ , and  $K = H$ , as desired. This completes the proof.

**(81.50) Corollary.** *The Brauer species  $b_x$  of  $A(G)$ , defined in Example (81.42), has as origin the cyclic group  $\langle x \rangle$ .*

**(81.51) Remarks.** (i) Let  $H \leq G$ , and let  $g$  be a species of  $A(H)$ . Define the stabilizer of  $g$  as

$$\text{Stab}_G g = \{x \in N_G(H) : g(u) = g(u^x) \text{ for all } u \in A(H)\}.$$

Now let  $f$  be a species of  $A(G)$  with origin  $H$ , set  $N = N_G(H)$ , and denote by  $\text{inv}_N A(H)$  the  $N$ -trivial subalgebra of  $A(H)$ . Then (see Benson-Parker [84, Theorem 8.2])  $N$  acts transitively on the species  $g_1, \dots, g_r$  of  $A(H)$  that fuse to  $f$ , and the number  $r$  of such species is precisely  $|N : \text{Stab}_G g_1|$ .

(ii) Keep the above notation, and let  $M$  be a  $kE$ -module, where  $E \leq G$ . Benson-Parker established an *induction formula*

$$f(M^G) = \sum_{h \rightarrow f} c_h h(M),$$

where the sum extends over all species  $h$  of  $A(E)$  that fuse to  $f$ , and where

$$c_h = |N_G(\text{origin of } h) \cap \text{Stab}_G h : N_E(\text{origin of } h)|.$$

Now let  $E \leq G$ , and consider the algebra  $A(G) = A(kG)$ . By Theorem 81.12, we

may write

$$A(G) = A(E)^G \oplus A(G)^E = \text{ind}_E^G A(E) \oplus \{x \in A(G) : x_E = 0\},$$

a direct sum of two ideals. We shall determine idempotent generators of these ideals, in terms of the primitive idempotents  $\{e_{H,c}\}$  of  $PP(G)$  (see (81.29)). Using (81.48), we may write

$$1 = \alpha + \beta, \quad \alpha \in PP(E)^G, \quad \beta \in PP(G)^E, \quad \alpha\beta = 0.$$

Then we have

$$A(G) = A(G)\alpha \oplus A(G)\beta, \quad A(G)\alpha \subseteq A(E)^G, \quad A(G)\beta \subseteq A(G)^E,$$

and consequently

$$A(E)^G = A(G)\alpha, \quad A(G)^E = A(G)\beta.$$

It therefore suffices to determine the idempotents  $\alpha, \beta$  in  $PP(G)$ .

Now  $\alpha$  is the sum of all  $e_{H,c}$  for which  $e_{H,c} \in PP(E)^G$ , and  $\beta$  is the sum of the other  $e$ 's.

**(81.52) Lemma.** *We have*

$$e_{H,c} \in PP(E)^G \Leftrightarrow H \leq_G E.$$

*Proof.* Let  $H \leq_G E$ ; replacing  $E$  by a conjugate, we may assume that  $H \leq E$ . Then  $e_H \in PP(E)^G$  by (81.30), since for  $H_i \leq H$  we have

$$(1_{H_i})^G = ((1_{H_i})^E)^G \in PP(E)^G.$$

But then  $e_{H,c} = e_H \cdot e_{H,c} \in PP(E)^G$ , since  $PP(E)^G$  is an ideal of  $PP(G)$ .

On the other hand, suppose that  $e_{H,c} \in PP(E)^G$ . Then the species  $s_{H,c}$  of  $PP(G)$  does not vanish on  $PP(E)^G$ , and hence  $s_{H,c}$  factors through  $E$ . Therefore  $E$  contains an origin of  $s_{H,c}$ , so  $E \geq_G H$  by (81.49).

From the above discussion, we obtain:

**(81.53) Theorem.** *Let  $E \leq G$ . Then*

$$A(E)^G = A(G)\alpha, \quad A(G)^E = A(G)\beta,$$

where the orthogonal idempotents  $\alpha$  and  $\beta$  are given by

$$\alpha = \sum_{H < E} e_{H,c}, \quad \beta = \sum_{H \not\leq_G E} e_{H,c},$$

with  $H$  ranging over nonconjugate  $p$ -hypo-elementary subgroups of  $G$ , and  $c$  over generators of  $H/O_p(H)$  yielding distinct species  $s_{H,c}$ .

We may use Conlon's Induction Theorem to show:

**(81.54) Theorem.** *The origin of any species of  $A(G)$  is a  $p$ -hypo-elementary subgroup of  $G$ .*

*Proof.* Let  $f$  be a species of  $A(G)$  with origin  $H$ . By (81.31), we have

$$A(H) = \sum A(K)^H,$$

where  $K$  ranges over the  $p$ -hypo-elementary subgroups of  $H$ . Therefore

$$A(H)^G = \sum_K A(K)^G.$$

Since  $f$  factors through  $H$ , we have  $\ker f \not\supseteq A(H)^G$  by (81.45), so  $\ker f \not\supseteq A(K)^G$  for some  $K$ . Then  $f$  factors through  $K$ , so  $K = H$  by the minimality of  $H$ . This completes the proof.

We shall also introduce the concept of the *vertex* of a species  $f$  of  $A(G)$ , defined as a minimal element of the set of vertices of indecomposable  $kG$ -modules  $M$  for which  $f[M] \neq 0$ . We have:

**(81.55) Theorem.** *The vertices of a species  $f$  of  $A(G)$  form a conjugacy class of  $p$ -subgroups of  $G$ .*

*Proof.* Let  $P_1$  and  $P_2$  be vertices of  $f$ . Then for  $i = 1, 2$ , there exist  $M_i \in \text{Ind } kG$  with  $f[M_i] \neq 0$ , and  $P_i$  is a vertex of  $M_i$ . We have  $f[M_1 \otimes M_2] = f[M_1]f(M_2) \neq 0$ , so  $f[X] \neq 0$  for some indecomposable summand  $X$  of  $M_1 \otimes M_2$ . From the remarks in §81A,  $M_1 \otimes M_2$  is  $(G, P_i)$ -projective for  $i = 1, 2$ , so the vertices of  $X$  are conjugate to subgroups of both  $P_1$  and  $P_2$ . By the minimality of  $P_1$  and  $P_2$ , we conclude that  $P_1 =_G P_2$ .

There is a close connection between the origin and the vertex of a species  $f$  of  $A(G)$ , given as follows:

**(81.56) Theorem.** *Let  $f$  be a species of  $A(G)$  with origin  $H$ . Then the vertex of  $f$  is  $O_p(H)$ , up to  $G$ -conjugacy.*

*Proof.* By (81.54),  $H$  is  $p$ -hypo-elementary; let  $P = O_p(H)$ . Then

$$f(A(H)^G) \neq 0, \quad f(A(K)^G) = 0 \quad \text{for } K < H.$$

By (81.53),  $A(H)^G$  is generated by the idempotent  $\sum e_{K,c}$ , with  $K$  ranging over

subgroups of  $H$ , and various choices of  $c$ . Since  $e_{K,c} \in A(K)^G$ , it follows that  $f(e_{H,c}) \neq 0$  for some  $c$ . Therefore  $f(A''(G, P)) \neq 0$  by (81.37), so  $f[M] \neq 0$  for some  $M \in \text{Ind } kG$  of vertex  $P$ .

Next,  $f$  must vanish on  $A(G)^H$ , so by (81.53),  $f(e_{K,c}) = 0$  if  $K \leq_G H$ . Combining this fact with the previous argument, it follows from (81.37) that  $f(A'(G, P)) = 0$ , which completes the proof that  $f$  has vertex  $P$ .

For further reading on species of  $A(G)$ , and character tables that extend those involving Brauer characters, see Benson-Parker [84], Benson [84a], and Webb [84].

### §81D. Dual Elements in the Green Algebra

Throughout this section,  $G$  denotes a finite group, and  $K$  a field of characteristic  $p \geq 0$ . By a “ $G$ -module” we shall mean a f.g. (left)  $KG$ -module. Define the representation ring  $a(KG)$  and the representation algebra (= Green algebra)  $A(KG) = C \otimes_Z a(KG)$  as in §81A. Here we shall describe the work of Benson-Parker [84], who defined various inner product on  $A(KG)$ , and construct a kind of dual basis by using the theory of Auslander-Reiten sequences.

For a  $G$ -module  $M$ , let  $M^*$  denote its contragredient, and  $\text{inv}_G M$  its  $G$ -trivial submodule. Let  $K$  or  $K_G$  be the field  $K$  on which  $G$  acts trivially. For  $G$ -modules  $M$  and  $N$ , define their *intertwining number* as

$$(81.58) \quad (M, N)_G = \dim_K \text{Hom}_{KG}(M, N)$$

(see (9.24)). Write  $\otimes$  instead of  $\otimes_K$  for brevity. By (10.31ii) and (10.32), there are  $K$ -isomorphisms

$$(81.59) \quad \text{inv}_G M^* \otimes N \cong \text{Hom}_{KG}(M, N) \cong \text{Hom}_{KG}(N^*, M^*).$$

But we also have

$$\text{inv}_G M^* \otimes N \cong \text{Hom}_{KG}(K, M^* \otimes N),$$

so we immediately obtain the formulas

$$(M, N)_G = (K, M^* \otimes N)_G = (M \otimes N^*, K)_G = (N^*, M^*)_G.$$

Next, let  $H \leq G$  and let  $M$  be a  $G$ -module,  $L$  an  $H$ -module. The Frobenius reciprocity formulas (10.8) and (10.21) yield

$$(L^G, M)_G = (L, M_H)_H, \quad (M, L^G)_G = (M_H, L)_H.$$

If  $KG$  is semisimple (i.e.,  $p \nmid |G|$ ), then  $(M, N)_G = (N, M)_G$  for any  $G$ -modules  $M, N$ . Simple examples show that this need not hold when  $p$  divides  $|G|$ . Later,

we shall introduce a second inner product  $\langle \cdot, \cdot \rangle$  which is symmetric, and the entire theory can be developed equally well using it rather than  $(\cdot, \cdot)$ .

Continuing with our discussion, we note that the intertwining number  $(M, N)_G$ , defined in (81.58), is additive on direct sums of modules. We may therefore extend this symbol by linearity to obtain a pairing

$$(81.60) \quad A(KG) \times A(KG) \rightarrow \mathbb{C}, \text{ given by } (x \times y) \rightarrow (x, y)_G \in \mathbb{C}.$$

Generally speaking,  $(x, y)_G$  need not coincide with  $(y, x)_G$ . To simplify the calculations, we *assume K algebraically closed from now on*, unless stated otherwise. Let  $\text{char } K = p \geq 0$ . If  $p \nmid |G|$ , then  $KG$  is semisimple, and the representation ring  $a(KG)$  coincides with the Grothendieck ring  $G_0(KG)$  (see §16B, §38A). This ring has a  $\mathbb{Z}$ -basis consisting of a basic set of simple  $KG$ -modules. By (18.11), we have

$$G_0(KG) \cong G_0(CG) \cong \text{ch } CG, \quad A(KG) \cong \text{cf}_C G,$$

where  $\text{ch } CG$  is the ring of virtual complex characters of  $G$ , and  $\text{cf}_C G$  the ring of complex-valued class functions on  $G$ . By §9, the ring  $\text{cf}_C G$  is semisimple, and the pairing (81.58) is symmetric and nondegenerate.

Dropping the assumption that  $p \nmid |G|$ , we can no longer identify  $a(KG)$  with  $G_0(KG)$ . The ring  $a(KG)$  has as  $\mathbb{Z}$ -basis the set  $\{[M] : M \in \text{Ind } KG\}$ , where as usual  $\text{Ind } KG$  is the set of (isomorphism classes of) indecomposable  $KG$ -modules. This set is also a  $\mathbb{C}$ -basis for  $A(KG)$ , so  $A(KG)$  is f.d./ $\mathbb{C}$  if and only if  $KG$  has finite representation type. By D. G. Higman's Theorem (see Volume I, p. 469), this occurs if and only if  $G$  has a cyclic Sylow  $p$ -subgroup.

Returning to the general case, we now give the main result of this subsection:

**(81.61) Benson-Parker Theorem.** *Let  $K$  be an algebraically closed field of characteristic  $p \geq 0$ , let  $G$  be any finite group, and consider the pairing  $A(KG) \times A(KG) \rightarrow \mathbb{C}$  defined above. Then this pairing is nondegenerate in the following sense: for each  $M \in \text{Ind } KG$ , there exists an element  $\hat{M} \in A(KG)$  such that*

$$(N, \hat{M})_G = \delta_{MN} \quad \text{for } M, N \in \text{Ind } KG,$$

where  $\delta_{MN} = 1$  if  $M \cong N$ , and  $\delta_{MN} = 0$  otherwise.

Before giving the proof, which is based on the theory of Auslander-Reiten sequences developed in §78, we give an easy but surprising consequence:

**(81.62) Corollary.** (i) *The map*

$$A(KG) \rightarrow \text{Hom}_C(A(KG), \mathbb{C}), \text{ given by } x \rightarrow (x, \cdot)_G,$$

is injective.

(ii) A  $KG$ -module  $M$  is uniquely determined (up to isomorphism) by the set of values

$$\{(M, X)_G : X = KG\text{-module}\}.$$

*Proof.* For (i), let  $x \in A(KG)$  be such that  $(x, N)_G = 0$  for every  $KG$ -module  $N$ . We may write  $x$  as a finite sum

$$x = \sum \xi_i [M_i], \quad \text{with } \xi_i \in C, \quad M_i \in \text{Ind } KG,$$

and  $M_i \not\cong M_j$  for  $i \neq j$ . Then for each  $i$ ,

$$0 = (x, \hat{M}_i)_G = \xi_i (M_i, \hat{M}_i) = \xi_i,$$

so  $x = 0$ . Assertion (ii) follows from (i).

We begin the proof of (81.61) with a lemma, which uses the hypothesis that  $K$  is algebraically closed.

**(81.63) Lemma.** Consider a ses of  $KG$ -modules

$$(81.64) \quad 0 \rightarrow N \rightarrow E \xrightarrow{\varphi} M \rightarrow 0,$$

where  $M, N \in \text{Ind } KG$ . For each  $X \in \text{Ind } KG$ ,  $\varphi$  induces a  $K$ -linear map

$$\varphi_* : \text{Hom}_{KG}(X, E) \rightarrow \text{Hom}_{KG}(X, M).$$

Then (81.64) is an AR-sequence (for  $M$ ) if and only if

$$(81.65) \quad \dim_K(\text{cok } \varphi_*) = \delta_{XM} \text{ for all } X \in \text{Ind } KG.$$

*Proof.* For brevity, write Hom and End in place of  $\text{Hom}_{KG}$  and  $\text{End}_{KG}$ . Since  $M$  is indecomposable and  $K$  is algebraically closed, by §81A we know that  $\text{End}(M)$  is a local ring for which

$$\text{End}(M)/\text{rad } \text{End}(M) \cong K.$$

Now consider a  $KG$ -homomorphism  $f : X \rightarrow M$ , where  $X \in \text{Ind } KG$ . Then  $f$  is a split surjection if and only if  $f$  is an isomorphism, since both  $X$  and  $M$  are indecomposable. On the other hand,  $f$  factors through  $E$  if and only if  $f \in \text{Im } \varphi_*$ .

Suppose now that (81.64) is an AR-sequence, which means that the sequence is nonsplit, and that for each  $KG$ -module  $Y$ , each map  $Y \rightarrow M$  that is not a split surjection must factor through  $E$ . In particular, for  $X \in \text{Ind } KG$ , each non-isomorphism  $f : X \rightarrow M$  must lie in  $\text{im } \varphi_*$ . If  $X \cong M$ , then  $\text{im } \varphi_*$  contains all elements of  $\text{End } M$  that are not automorphisms of  $M$ ; further,  $\text{im } \varphi_*$  contains no automorphism of  $M$ , since otherwise the sequence (81.64) would split. Thus,

$\text{im } \varphi_*$  coincides with the radical  $\text{rad End}(M)$  of the local ring  $\text{End}(M)$ , and so  $\text{cok } \varphi_* \cong K$ . This shows that  $\dim_K \text{cok } \varphi_* = 1$  if  $X \cong M$ .

On the other hand, for any  $X \in \text{Ind } KG$  that is not isomorphic to  $M$ , every map  $f: X \rightarrow M$  is not a split surjection, and hence lies in  $\text{im } \varphi_*$ . Therefore  $\text{cok } \varphi_* = 0$  in this case. We have now shown that (81.65) holds whenever (81.64) is an *AR*-sequence. By using Exercise 81.4 the argument is easily reversed; we leave the details to the reader.

We are now ready to prove the Benson-Parker Theorem, and begin by defining the elements  $\{\hat{M}: M \in \text{Ind } KG\}$ .

**(81.66) Definition.** Let  $J = \text{rad } KG$ , and write  $\text{Hom}$ ,  $\text{End}$  in place of  $\text{Hom}_{KG}$ ,  $\text{End}_{KG}$  for brevity. Let  $M \in \text{Ind } KG$ .

(a) If  $M$  is projective, set

$$\hat{M} = [M] - [JM] \in A(KG).$$

(b) If  $M$  is nonprojective, set

$$\hat{M} = [M] - [E] + [\Omega^2 M] \in A(KG),$$

where

$$(81.67) \quad 0 \rightarrow \Omega^2 M \rightarrow E \xrightarrow{\varphi} M \rightarrow 0$$

is an *AR*-sequence for  $M$  (see (78.26)).

We proceed to verify that  $(N, \hat{M})_G = \delta_{MN}$  for  $M, N \in \text{Ind } KG$ . Suppose first that  $M$  is projective, and let  $S = M/JM$  be the “top” of  $M$ . Then

$$(M, \hat{M})_G = \dim_K \text{Hom}(M, M) - \dim_K \text{Hom}(M, JM) = \dim_K \text{Hom}(M, S)$$

since  $\text{Hom}(M, *)$  is an exact functor. But  $\text{Hom}(M, S) \cong \text{Hom}(S, S) \cong K$ , so  $(M, \hat{M})_G = 1$ . On the other hand, if  $N \in \text{Ind } KG$  is not isomorphic to  $M$ , then there are no surjections from  $N$  onto  $M$ . Hence for each  $f: N \rightarrow M$  we must have  $f(N) \subseteq JM$ , and therefore

$$\text{Hom}(N, M) = \text{Hom}(N, JM).$$

But then

$$(N, \hat{M})_G = \dim_K \text{Hom}(N, M) - \dim_K \text{Hom}(N, JM) = 0,$$

as desired.

Now suppose that  $M$  is a nonprojective indecomposable  $KG$ -module, and let (81.67) be its *AR*-sequence. For any  $N \in \text{Ind } KG$ , there is an exact sequence

of  $K$ -spaces

$$0 \rightarrow \text{Hom}(N, \Omega^2 M) \rightarrow \text{Hom}(N, E) \xrightarrow{\varphi_*} \text{Hom}(N, M) \rightarrow \text{cok } \varphi_* \rightarrow 0.$$

Therefore  $(N, \hat{M})_G = \dim_K \text{cok } (\varphi_*) = \delta_{NM}$  by Lemma 81.63. This completes the proof of the Benson-Parker Theorem.

We remark that the dual elements  $\{\hat{M} : M \in \text{Ind } KG\}$  are obviously linearly independent over  $C$ , and we may ask whether they span  $A(KG)$ . The answer, due to Auslander [84] and Brenner-Butler-Hughes, is as follows:

**(81.68) Theorem.** *The dual elements  $\{\hat{M} : M \in \text{Ind } KG\}$  are a  $C$ -basis for  $A(KG)$  if and only if  $KG$  is of finite representation type, that is,  $G$  has a cyclic Sylow  $p$ -subgroup.*

*Proof.* If  $KG$  has finite representation type, then  $A(KG)$  is a f.d.  $C$ -space; in this case, the elements  $\{\hat{M} : M \in \text{Ind } KG\}$  and  $\{[M] : M \in \text{Ind } KG\}$  are a pair of dual bases relative to the pairing  $( , )_G$ .

On the other hand, suppose that the  $\{\hat{M}\}$  span  $A(KG)$ . For each  $X \in \text{Ind } KG$ , we may write  $[X]$  as a finite sum

$$[X] = \sum \lambda_M \hat{M}, \text{ where } \lambda_M \in C.$$

Since  $\lambda_M = (M, X)_G$ , it follows that for each  $X$ , there are finitely many  $M \in \text{Ind } KG$  for which  $\text{Hom}(M, X) \neq 0$ .

Now let  $X_1, \dots, X_r$  be the indecomposable injective (= projective)  $KG$ -modules, up to isomorphism. Each  $M \in \text{Ind } KG$  embeds in some f.g. injective  $KG$ -module (for Exercise 10.26), and hence embeds in a direct sum of  $X_i$ 's. Thus for each  $M$ ,  $\text{Hom}(M, X_i) \neq 0$  for some  $i$ . But if  $KG$  has infinite representation type, there are infinitely many  $M$ 's, and so for some  $i$ ,  $1 \leq i \leq r$ , we must have  $\text{Hom}(M, X_i) \neq 0$  for infinitely many  $M \in \text{Ind } KG$ . This contradicts the conclusion of the previous paragraph, and establishes the theorem.

We shall next discuss another inner product  $\langle , \rangle$  on the representation algebra  $A(KG)$ . Let  $M$  and  $N$  be  $G$ -modules, and write  $\text{Hom}$  rather than  $\text{Hom}_{KG}$  for brevity. As in §62A and §78A, a map  $f \in \text{Hom}(M, N)$  is called a *projective homomorphism* if  $f$  factors through a projective, or equivalently,

$$f = \sum_{x \in G} xhx^{-1} \text{ for some } h \in \text{Hom}_K(M, N).$$

Denoting by  $\text{Hom}(M, N)_{G/1}$  the space of such  $f$ 's, we now define

$$(81.69) \quad \langle M, N \rangle = \dim_K \text{Hom}(M, N)_{G/1}.$$

Following Benson-Parker, we give an important characterization of this inner product:

**(81.70) Proposition.** *Let  $P_1$  be the projective cover of the trivial  $G$ -module  $K$ . Then*

$$\langle M, N \rangle = \text{multiplicity of } P_1 \text{ as direct summand of } M^* \otimes N,$$

where  $M^*$  is the contragredient of  $M$ , and  $\otimes$  means inner tensor product over  $K$ .

*Proof.* It is easily verified that the isomorphism

$$\text{Hom}(M, N) \cong \text{Hom}(K, M^* \otimes N),$$

given in (78.17), preserves projective homomorphisms. Therefore we have

$$\langle M, N \rangle = \langle K, M^* \otimes N \rangle.$$

Since  $P_1$  is indecomposable, it thus suffices to show that

$$(*) \quad \dim_K \text{Hom}(K, X)_{G/1} = \delta_{X, P_1}$$

for each indecomposable direct summand  $X$  of  $M^* \otimes N$ .

The projective cover  $P_1$  of  $K$  is also the injective hull of  $K$ . Each nonzero  $f \in \text{Hom}(K, X)_{G/1}$  is a monomorphism that factors through a projective (= injective) module, and therefore  $f$  factors uniquely through a monomorphism  $P_1 \rightarrow X$ . Since  $P_1$  is injective, this map must split, and therefore  $X \cong P_1$ . Thus,  $(*)$  surely holds if  $X \not\cong P_1$ . On the other hand, for  $X \cong P_1$ , the above discussion gives

$$\text{Hom}(K, P_1)_{G/1} = \text{Hom}(K, P_1) = \text{Hom}(K, K) \cong K,$$

so again  $(*)$  holds. This completes the proof.

**(81.71) Corollary.** *Let  $L, M$ , and  $N$  be  $G$ -modules. Then*

$$\langle M, N \rangle = \langle N, M \rangle = \langle M^*, N^* \rangle, \quad \langle L \otimes M, N \rangle = \langle L, M^* \otimes N \rangle,$$

and  $\langle M, N \rangle$  is additive on direct sums of modules.

*Proof.* Since  $K$  is self-contragredient, so is  $P_1$ . Thus the multiplicity of  $P_1$  as direct summand of  $M^* \otimes N$  is the same as in  $(M^* \otimes N)^*$ . The latter is isomorphic to  $N^* \otimes M$ , so  $\langle M, N \rangle = \langle N, M \rangle$ . Further,

$$M^* \otimes N \cong (N^*)^* \otimes M^*, \quad \text{so } \langle M, N \rangle = \langle M^*, N^* \rangle.$$

Also,

$$(L \otimes M)^* \otimes N \cong L^* \otimes (M^* \otimes N), \quad \text{so } \langle L \otimes M, N \rangle = \langle L, M^* \otimes N \rangle.$$

The additivity of  $\langle M, N \rangle$  is clear.

We may thus extend  $\langle \cdot, \cdot \rangle$  by linearity to a *symmetric* pairing

$$(81.72) \quad A(KG) \times A(KG) \rightarrow \mathbb{C}, \text{ given by } x \times y \mapsto \langle x, y \rangle.$$

The relation between this pairing and that defined in (81.60) is as follows:

**(81.73) Proposition.** *Let  $P_1$  be the projective cover of  $K$ , and let  $\Omega$  be the Heller operator defined in §78A. Let*

$$u = [P_1] - [\Omega^{-1}K], \quad v = [P_1] - [\Omega K],$$

*viewed as elements of  $A(KG)$ . Then  $uv = vu = 1$  in  $A(KG)$ , and*

$$(81.74) \quad \langle M, N \rangle = (uM, N)_G = (M, vN)_G$$

*for any  $G$ -modules  $M$  and  $N$ , where  $uM$  means the product  $u[M]$  in  $A(KG)$ .*

*Proof.* We start with the exact sequence

$$(81.75) \quad 0 \rightarrow K \rightarrow P_1 \rightarrow \Omega^{-1}K \rightarrow 0$$

(if  $K$  is projective, then  $p \nmid |G|$ , and we set  $\Omega^{-1}K = 0$ ). Tensoring with  $M$ , we obtain an exact sequence

$$0 \rightarrow M \rightarrow P_1 \otimes M \rightarrow \Omega^{-1}K \otimes M \rightarrow 0.$$

If  $M$  is projective, this sequence splits, and thus  $uM = M$  in  $A(KG)$ . But then

$$\langle M, N \rangle = \dim_K \text{Hom}(M, N)_{G/1} = \dim_K \text{Hom}(M, N) = (M, N)_G,$$

as desired.

Suppose now that  $M$  has no projective summands, so there is an exact sequence

$$0 \rightarrow \Omega M \rightarrow P_M \rightarrow M \rightarrow 0,$$

where  $P_M$  is a projective cover of  $M$ . Tensoring with  $\Omega^{-1}K$  and using Schanuel's Lemma, we obtain

$$(*) \quad M \oplus (\Omega^{-1}K \otimes P_M) \cong P_1 \otimes M \oplus (\Omega^{-1}K \otimes \Omega M).$$

On the other hand,

$$u(P_M - \Omega M) = P_1(P_M - \Omega M) - \Omega^{-1}K \cdot P_M + \Omega^{-1}K \cdot \Omega M \quad \text{in } A(KG).$$

But  $P_1(P_M - \Omega M) = P_1 \cdot M$ , so using  $(*)$  we have

$$u(P_M - \Omega M) = M \quad \text{in } A(KG).$$

In the same way, we find that

$$v(I_M - \Omega^{-1}M) = M \quad \text{in } A(KG),$$

where  $I_M$  is an injective hull of  $M$ . Choosing  $M = K$ , it follows that  $uv = vu = 1$  in  $A(KG)$ .

To prove (81.74), note that

$$\langle M, N \rangle = \langle K, M^* \otimes N \rangle, \quad (uM, N)_G = (u, M^* \otimes N)_G.$$

It thus suffices to verify that  $\langle K, X \rangle = (u, X)_G$  for each  $G$ -module  $X$ . Now  $\text{Hom}(K, X)_{G/1}$  consists of all  $f \in \text{Hom}(K, X)$  that factor through  $P_1$ . By (81.75), we obtain

$$\begin{aligned} \langle K, X \rangle &= \dim_K \text{Hom}(K, X)_{G/1} \\ &= \dim_K \text{Hom}(P_1, X) - \dim_K \text{Hom}(\Omega^{-1}K, X) = (u, X)_G. \end{aligned}$$

The second formula in (81.74) follows in a similar fashion.

We prove next a Frobenius reciprocity formula for the pairing  $\langle \cdot, \cdot \rangle$ .

**(81.76) Proposition.** *Let  $H \leq G$ , and let  $M$  be a  $G$ -module,  $N$  an  $H$ -module. Then*

$$\langle M, N^G \rangle = \langle M_H, N \rangle.$$

*Proof.* Let  $K'$  be the trivial  $H$ -module,  $P'$  its  $KH$ -projective cover. Comparing the two exact sequences

$$0 \rightarrow K' \rightarrow P' \rightarrow \Omega^{-1}K' \rightarrow 0, \quad 0 \rightarrow K' \rightarrow (P_1)_H \rightarrow (\Omega^{-1}K)_H \rightarrow 0,$$

Schanuel's Lemma shows that  $\text{res}_H^G u_G = u_H$ , where

$$u_G = P_1 - \Omega^{-1}K, \quad u_H = P' - \Omega^{-1}K'.$$

But then

$$\langle M, N^G \rangle = (u_G M, N^G)_G = (u_H M_H, N)_H = \langle M_H, N \rangle.$$

The dual elements for this symmetric pairing on  $A(KG)$  are given as follows:

- (i) If  $M$  is a projective indecomposable  $G$ -module, put

$$M' = [\text{socle of } M] \in A(KG).$$

(ii) If  $M$  is a nonprojective indecomposable  $G$ -module, define

$$M' = [X] - [\Omega M] - [\Omega^{-1}M] \in A(KG),$$

where

$$0 \rightarrow \Omega M \rightarrow X \rightarrow \Omega^{-1}M \rightarrow 0$$

is an  $AR$ -sequence. As in the proof of (81.61), or by using (81.61) and (81.74), we obtain

$$(81.77) \quad \langle N, M' \rangle = \delta_{NM} \quad \text{for } N, M \in \text{Ind } KG.$$

We leave the details to the reader.

### §81E. Semisimplicity of Representation Algebras

Let  $K$  be a field of characteristic  $p \geq 0$ , and let  $A(G)$  be the representation algebra, spanned over  $\mathbb{C}$  by the indecomposable  $KG$ -modules. If  $p = 0$ , then  $A(G)$  is isomorphic to the  $\mathbb{C}$ -algebra of class functions  $\text{cf}(G)$  and is necessarily semisimple. Thus, in discussing the semisimplicity of  $A(G)$ , we may as well restrict our attention to the case where  $p > 0$ . We have already remarked that  $A(G)$  is f.d./ $\mathbb{C}$  if and only if  $G$  has a cyclic Sylow  $p$ -subgroup. Our main aim here is to prove O'Reilly's Theorem, that  $A(G)$  is semisimple in this case. Rather than following the original proof (O'Reilly [65]; see also Feit [82]), we present a new proof due to Benson-Carlson [86], which is rather more conceptual.

On the other hand, if  $G$  has a noncyclic Sylow  $p$ -subgroup, then  $A(G)$  may contain nonzero nilpotent elements. Such examples were first found by Zemanek [71], [73], and in §81F we give the Benson-Carlson interpretation of these examples.

As a starting point of the Benson-Carlson method, we begin by giving a criterion as to when the  $G$ -trivial module  $K$  occurs as direct summand of  $M \otimes N$ , when  $M, N \in \text{Ind } KG$ . If  $KG$  is semisimple, then  $\text{Ind } KG$  consists of the simple  $KG$ -modules. For  $M, N$  simple, §81D gives

$$K | M \otimes N \Leftrightarrow (M^*, N)_G \neq 0 \Leftrightarrow N \cong M^*,$$

where  $M^*$  is the contragredient of  $M$ .

Now let  $\text{char } K = p > 0$ , where  $p$  divides  $|G|$ . Let  $N$  be any  $KG$ -module such that  $p \nmid d$ , where  $d = \dim_K N$ . As pointed out by Feit [82, III.2.2], we have  $K | (N^* \otimes N)$ . To see this, we first observe that

$$N^* \otimes N \cong \text{Hom}_K(N, N) \cong M_d(K).$$

The group  $G$  acts by conjugation on  $M_d(K)$ , and thus  $K \cdot \mathbf{I}_d$  is a  $KG$ -submodule

of  $M_d(K)$ . So also is

$$X = \{x \in M_d(K) : \text{trace } x = 0\}.$$

Since  $p/d$  by hypothesis, we have

$$(81.78) \quad M_d(K) = X \oplus K \cdot \mathbf{I}_d,$$

so  $K|(N^* \otimes N)$  as claimed.

We now prove the Benson-Carlson criterion for the tensor product of  $KG$ -modules to contain the trivial  $G$ -module  $K$  as direct summand.

**(81.79) Theorem.** *Let  $M, N \in \text{Ind } KG$  be such that  $\tilde{E}(M) \cong \tilde{E}(N) \cong K$  (using the notation in (81.1)). Then  $K|(M \otimes N)$  if and only if*

- (i)  $M \cong N^*$ , and (ii)  $p \nmid \dim_K N$ .

Further, if (i) and (ii) hold, then the multiplicity of  $K$  as direct summand of  $M \otimes N$  is precisely 1.

*Proof.* By (81.2),  $M$  and  $N$  are absolutely indecomposable. To determine whether  $K|(M \otimes N)$ , we may replace  $K$  by its algebraic closure by virtue of (81.3), so assume for the rest of the proof that  $K$  is algebraically closed. We have  $K|(M \otimes N)$  if and only if there exist  $K$ -homomorphisms

$$K \rightarrow M \otimes N \rightarrow K$$

whose composite is nonzero. Using the isomorphisms (81.59)

$$\text{inv}_G M \otimes N \cong \text{Hom}_{KG}(N^*, M), \quad \text{inv}_G(M \otimes N)^* \cong \text{Hom}_{KG}(M, N^*),$$

it suffices to determine whether the composite map  $ji \cong 0$ , where

$$\text{Hom}_{KG}(N^*, M) \xrightarrow{i} M \otimes N \xrightarrow{j} \{\text{Hom}_{KG}(M, N^*)\}.$$

The  $K$ -homomorphisms  $i, j$  are injective and surjective, respectively, and can be described explicitly as follows: let

$$N = \bigoplus_{i=1}^d Kn_r, \quad N^* = \bigoplus_{s=1}^d K\varphi_s, \quad \text{where } \varphi_s(n_r) = \delta_{rs}.$$

Then for  $g \in \text{Hom}_{KG}(N^*, M)$ , and  $h \in \text{Hom}_{KG}(M, N^*)$ , we have

$$i(g) = \sum_r g(\varphi_r) \otimes n_r, \quad \{j(m \otimes n)\}h = h(m)n.$$

Therefore

$$\{(ji)(g)\}h = \sum_r \{hg(\varphi_r)\}n_r = \text{trace of } hg \text{ acting on } N^*.$$

It follows that  $ji \neq 0$  if and only if the composite map

$$\eta: \text{Hom}_{KG}(N^*, M) \otimes_K \text{Hom}_{KG}(M, N^*) \xrightarrow{\tau} E(N^*) \xrightarrow{\text{trace}} K$$

is not the zero map, where  $\tau(g \otimes h) = hg$ , and where  $E(N^*) = \text{End}_{KG} N^*$ .

Now  $E(N^*) \cong E(N)$ , and  $E(N)/\text{rad } E(N) \cong K$ , so

$$E(N^*) = K \cdot 1 + \text{rad } E(N^*).$$

Since each element of  $\text{rad } E(N^*)$  is nilpotent (and thus has trace 0), we see that

$$\{\text{trace } y : y \in E(N^*)\} = K \cdot d, \text{ where } d = \dim_K N.$$

If  $p|d$ , then necessarily  $K \cdot d = 0$  and  $ji = 0$ , so  $K/(M \otimes N)$ . Suppose hereafter that  $p \nmid d$ ; then  $ji \neq 0$  if and only if there exist elements  $g, h$  for which  $hg \in \text{Aut}_{KG}(N^*)$ . Such elements exists if and only if  $N^* \mid M$ , or equivalently (since  $M$  is indecomposable)  $N^* \cong M$ . This proves the first part of the theorem.

Now suppose that (i), (ii) are satisfied. If  $K^{(2)} \mid (M \otimes N)$ , then  $\dim_K \text{im}(ji) > 1$ . This means that there exist  $K$ -subspaces of  $\text{Hom}_{KG}(N^*, M)$  and  $\text{Hom}_{KG}(M, N^*)$ , of dimension  $> 1$ , on which the map  $\eta$  is a nonsingular pairing. Thus there is a subspace of  $\text{Hom}_{KG}(N^*, M)$  of dimension  $> 1$ , each nonzero element of which is an isomorphism. This is impossible since  $\tilde{E}(N) \cong K$ , and the proof is complete.

**(81.80) Corollary.** *Let  $M, N \in \text{Ind } KG$  be distinct. Then  $K \nmid M \otimes N^*$ .*

*Proof.* Let  $E$  be an algebraic closure of  $K$ , and denote  $E \otimes_K M$  by  $EM$  for brevity. If  $K \mid M \otimes N^*$ , then  $E|(EM) \otimes (EN)^*$ . Writing  $EM$  and  $EN$  as direct sums of absolutely indecomposable  $EG$ -modules, it follows from (81.79) that  $EM$  and  $EN$  must have a common direct summand. But then  $M$  and  $N$  have a common summand, by the proof of (81.3), so  $M \cong N$ .

**(81.81) Corollary.** *Let  $M$  be an absolutely indecomposable  $KG$ -module such that  $p \nmid \dim_K M$ . Then for every  $KG$ -module  $N$  and every  $KG$ -direct summand  $U$  of  $M \otimes N$ , we have  $p \nmid \dim_K U$ .*

*Proof.* Assume  $U \mid M \otimes N$  and  $p \nmid \dim_K U$ . Then  $K \mid U^* \otimes U$  by the discussion preceding (81.78), and thus  $K$  is a direct summand of  $U^* \otimes M \otimes N$ , that is, of  $M \otimes (U^* \otimes N)$ . Passing to an algebraic closure of  $K$  and using (81.79), it follows that  $p \nmid \dim_K M$ . This is a contradiction, and completes the proof.

It will be convenient to introduce some temporary terminology. A  $KG$ -module  $M$  will be called a  $p$ -module if for each field  $K' \supseteq K$  and each  $K'G$ -direct summand  $X$  of  $K'M$ , we have  $p \nmid \dim_{K'} X$ . It is clear that direct sums (or direct summands) of  $p$ -modules are again  $p$ -modules. It follows readily from (81.2) that if  $E$  is an algebraic closure of  $K$ , and  $M$  is a  $KG$ -module, then  $M$  is a  $p$ -module if and

only if  $EM$  is a  $p$ -module. By (81.3) and (81.79), we obtain at once:

$$(81.82) \quad K/M \otimes M^* \text{ if and only if } M \text{ is a } p\text{-module.}$$

We now define

$$(81.83) \quad a(G, p) = \sum_{M=p\text{-module}} \mathbb{Z}[M], \quad A(G, p) = \sum_{M=p\text{-module}} \mathbb{C}[M],$$

where  $M$  ranges over all  $KG$ -modules that are  $p$ -modules. Following Benson-Carlson, we prove:

**(81.84) Proposition.**  *$a(G, p)$  and  $A(G, p)$  are ideals of the rings  $a(G)$  and  $A(G)$ , respectively. Further,*

$$(*) \quad a(G, p) = A(G, p) \cap a(G).$$

*Proof.* Let the  $KG$ -module  $M$  be a  $p$ -module; we must show that for any  $KG$ -module  $N$ ,  $M \otimes N$  is also a  $p$ -module. Replacing  $K$  by an algebraic closure, and changing notation, it suffices to establish the result for  $M$  absolutely indecomposable. But then the result holds by (81.81). Thus,  $a(G, p)$  is an ideal of  $a(G)$ , and  $A(G, p) = \mathbb{C} \otimes_{\mathbb{Z}} a(G, p)$ . Since  $a(G, p)$  has as  $\mathbb{Z}$ -basis all  $p$ -modules in the set  $\text{Ind } KG$ , it is clear that  $a(G, p)$  is a  $\mathbb{Z}$ -direct summand of  $a(G)$ . Assertion  $(*)$  is now obvious.

**(81.85) Theorem (Benson-Carlson).** *The ring  $A(G)/A(G, p)$  has no nilpotent elements (except 0).*

*Proof.* For  $x \in A(G)$ , write  $K|x$  to indicate that the trivial  $G$ -module  $K$  appears in  $x$  with nonzero coefficient. Clearly  $K/x$  for any  $x \in A(G, p)$ .

Now define an involution  $x \rightarrow x'$  on  $A(G)$ , by the formula

$$\{\sum \xi_i [M_i]\}' = \sum \bar{\xi}_i [M_i^*], \quad \xi_i \in \mathbb{C}, \quad M_i = KG\text{-module},$$

where  $\bar{\xi}_i$  = complex conjugate of  $\xi_i$ . We claim that for  $x \in A(G)$ ,

$$(81.86) \quad xx' \in A(G, p) \Rightarrow x \in A(G, p).$$

Let us write

$$x = \sum_i a_i [M_i], \quad a_i \in \mathbb{C}, \quad a_i \neq 0, \quad M_i \in \text{Ind } KG,$$

with the  $\{M_i\}$  distinct. Then

$$xx' = \sum_{i,j} a_i \bar{a}_j [M_i \otimes M_j^*],$$

For  $i \neq j$ ,  $K/M_i \otimes M_j^*$  by (81.80). Further,  $K \nmid xx'$  since  $xx' \in A(G, p)$ . It follows that for each  $i$ ,  $K \nmid M_i \otimes M_i^*$ , and thus  $M_i$  is a  $p$ -module by (81.82). This establishes (81.86).

We now prove that  $A(G)/A(G, p)$  has no nonzero nilpotent elements, and it suffices to show that there are no such elements whose square is 0. So let  $x \in A(G)$  be such that  $x^2 \in A(G, p)$ , and put  $y = xx'$ . Then  $yy' = x^2(x')^2 \in A(G, p)$ , and thus  $y \in A(G, p)$  by (81.86). But then  $x \in A(G, p)$  by (81.86), and the proof is finished.

Let us define

$$A(G, \text{Cyc}) = \sum_M C[M].$$

where  $M$  ranges over all indecomposable  $KG$ -modules having a cyclic vertex. (Of course, if  $G$  has a cyclic Sylow  $p$ -subgroup, then every  $M \in \text{Ind } KG$  has cyclic vertex, so in this case  $A(G, \text{Cyc})$  coincides with  $A(G)$ .) Note that  $A(G, \text{Cyc})$  is a f.d.  $C$ -algebra, since cyclic groups have only finitely many distinct indecomposable  $K$ -representations, and since the tensor product of modules of cyclic vertex is a direct sum of such modules. Our aim is to prove:

**(81.87) Benson-Carlson Theorem.**  $A(G, \text{Cyc})$  is a f.d. semisimple  $C$ -algebra.

Since  $A(G, \text{Cyc})$  is f.d./ $C$ , it will suffice to prove that it contains no nonzero nilpotent elements. The proof will depend on the Conlon Theorems in §81B. We begin with:

**(81.88) Lemma.** Let  $K$  be an algebraically closed field of characteristic  $p > 0$ , and let  $H = P \rtimes C$  be a  $p$ -hypo-elementary group, where  $P$  is a nontrivial cyclic  $p$ -group, and  $C$  is a cyclic  $p'$ -group. Let  $P_1$  be the unique subgroup of  $P$  of index  $p$ , and set  $H_1 = P_1 \rtimes C$ . Then

$$A(H, p) = \text{ind}_{H_1}^H A(H_1).$$

*Proof.* From (20.11) we have

$$KC = \bigoplus_{i=1}^r F_i, \dim_K F_i = 1,$$

$$KH_1 = \bigoplus_i V_i, \quad V_i = (F_i)^{H_1}; \quad KH = \bigoplus_i U_i, \quad U_i = (F_i)^H,$$

and  $\{V_i\}$  are the P.I.M.'s for  $H_1$ , while the  $\{U_i\}$  are those for  $H$ . The indecomposable  $KH$ -modules  $\{M_{ij}\}$  are given by

$$M_{ij} = U_i / (x - 1)^j U_i, \quad 1 \leq i \leq r, \quad 1 \leq j \leq p^d = |P|, P = \langle x \rangle.$$

Then  $\dim M_{ij} = j \dim F_i = j$ , and  $d \geq 1$  by hypothesis. Then  $M_{ij}$  is a  $p$ -module if

and only if  $p|j$ . For such  $j$ , write  $j = pn$  with  $1 \leq n \leq p^{d-1}$ . Then

$$M_{ij} = U_i/(x^p - 1)^n U_i \cong \text{ind}_{H_1}^H V_i / (x - 1)^n V_i \in \text{ind}_{H_1}^H A(H),$$

which gives the desired result.

**(81.89) Corollary.** *Keep the above notation, but drop the hypotheses that  $K$  be algebraically closed and that  $P \neq 1$ . Then  $A(KH)$  has no nonzero nilpotent elements.*

*Proof.* Let  $E$  be an algebraic closure of  $K$ . By (81.4),  $A(KH)$  embeds in  $A(EH)$ , so it suffices to show that  $A(EH)$  has no nonzero nilpotent elements. Changing notation, for the rest of the proof we may assume that  $K$  is algebraically closed. If  $P = 1$ , then  $H$  is a  $p'$ -group, and  $A(H)$  is isomorphic to the ring of class functions on  $H$ , hence is semisimple. Now use induction on  $|H|$ , and let  $P \neq 1$ . By (81.12) we have

$$\begin{aligned} A(H) &= \text{ind}_{H_1}^H A(H_1) \oplus \{x \in A(H) : x_{H_1} = 0\} \\ &= A(H, p) \oplus \text{kernel of } \text{res}_{H_1}^H. \end{aligned}$$

The restriction map  $\text{res}_{H_1}^H$  is thus a ring monomorphism of  $A(H, p)$  into  $A(H_1)$ , so by the induction hypothesis,  $A(H, p)$  has no nonzero nilpotent elements. On the other hand,  $A(H)/A(H, p)$  has no nonzero nilpotent elements by (81.85). It follows that the same holds for  $A(H)$ , as desired.

We are now ready to complete the proof of the Benson-Carlson Theorem. Given the group  $G$ , denote by  $\mathcal{H}_c$  a full set of nonconjugate  $p$ -hypo-elementary subgroups  $H \leq G$  such that  $O_p(H)$  is cyclic. Then  $A(H)$  has no nonzero nilpotent elements for  $H \in \mathcal{H}_c$ , by (81.89). We need only show that there is a ring monomorphism (given by restriction maps)

$$A(G, \text{Cyc}) \rightarrow \coprod_{H \in \mathcal{H}_c} A(H),$$

that is, if  $x \in A(G, \text{Cyc})$  satisfies the condition that  $x_H = 0$  for all  $H \in \mathcal{H}_c$ , then  $x = 0$ . By Conlon's Theorem 81.36, we may write

$$x = \sum_D x(D), \quad \text{where } x(D) \in A''(G, D),$$

with  $D$  ranging over a full set of nonconjugate  $p$ -subgroups of  $G$ . Each nonzero  $x(D)$  contains terms of vertex  $D$ , and it follows that  $x(D) = 0$  for noncyclic  $D$ , since  $x \in A(G, \text{Cyc})$ .

Now let  $D$  range over cyclic  $p$ -subgroups of  $G$ . By (81.41), for each  $D$  there is a monomorphism

$$A''(G, D) \rightarrow \coprod_{\substack{H \leq G \\ O_p(H) = D}} A''(H, D),$$

where  $H$  ranges over  $p$ -hypo-elementary subgroups of  $G$  for which  $O_p(H) = D$ . Each such  $H$  lies in  $\mathcal{H}_c$ , so the composite map

$$\coprod_{D \text{ cyclic}} A''(G, D) \rightarrow \coprod_D \coprod_{\substack{H \leqslant G \\ O_p(H) = D}} A''(H, D) \rightarrow \coprod_{H \in \mathcal{H}_c} A''(H)$$

is a monomorphism. Since  $x = \sum x(D)$ , with  $x(D) \in A''(G, D)$ , it follows that if  $x_H = 0$  for all  $H \in \mathcal{H}_c$ , then necessarily  $x = 0$ . This completes the proof of the Benson-Carlson Theorem 81.87.

In particular, if  $G$  has a cyclic Sylow  $p$ -subgroup, then  $A(G) = A(G, \text{Cyc})$ , as remarked above. Thus from (81.87) we obtain as a corollary:

**(81.90) O'Reilly's Theorem.** *If  $G$  has a cyclic Sylow  $p$ -subgroup, then  $A(G)$  is a f.d. semisimple  $\mathbb{C}$ -algebra.*

Benson-Carlson give the following example to show that even though the algebra  $A(G)/A(G, p)$  has no nonzero nilpotent elements, its structure may nevertheless be quite complicated. Let  $\text{char } K = p > 2$ , where  $K$  is an infinite field, and let  $G$  be an elementary abelian  $p$ -group with generators  $x$  and  $y$ . For each  $a \in K$ , let

$$M_a = KG/I_a, \quad \text{where } I_a = KG(x - 1)(y - 1) + KG((y - 1)^2 - a(x - 1)^{p-1}).$$

Then  $\dim_K M_a = p + 1$ , and the  $\{M_a : a \in K\}$  are distinct nonisomorphic modules. It turns out that  $[M_a]^2 = 1$  in  $A(G)/A(G, p)$ , so this quotient ring is an infinite-dimensional  $\mathbb{C}$ -algebra containing infinitely many elements of order 2.

### §81F. Nilpotent Elements in Representation Algebras

Throughout let  $K$  be a field,  $\text{char } K = p > 0$ , and consider  $KG$ -modules, writing  $A(G)$  instead of  $A(KG)$ . Let  $\Omega$  be the Heller operator, as in §78. Thus, for each  $G$ -module  $M$  there is a  $G$ -ses

$$0 \rightarrow \Omega M \rightarrow P \rightarrow M \rightarrow 0,$$

where  $P$  is a projective cover of  $M$ . Tensoring with an arbitrary  $G$ -module  $N$ , and using the fact that  $P \otimes N$  is projective, we obtain

$$(81.91) \quad \Omega M \otimes N \cong \Omega(M \otimes N) \oplus \text{proj},$$

where “proj” indicates a projective  $KG$ -module.

To construct nilpotent elements in  $A(G)$ , we begin with a simple generalization of Schanuel's Lemma:

**(81.92) Lemma.** *Consider a pair of ses's of  $G$ -modules:*

$$0 \rightarrow W_1 \rightarrow U_1 \xrightarrow{\sigma} V \rightarrow 0, \quad 0 \rightarrow W_2 \rightarrow P_2 \xrightarrow{\mu} V \rightarrow 0,$$

where  $P_2$  is projective, and where  $\sigma$  factors through a projective module. Then

$$W_1 \oplus P_2 \cong W_2 \oplus U_1.$$

*Proof.* Consider a diagram

$$\begin{array}{ccc} U_1 & & \\ \alpha \downarrow & \searrow \sigma & \\ P_1 & \xrightarrow{\tau} & V \\ \beta \downarrow & & 1 \downarrow \\ P_2 & \xrightarrow{\mu} & V, \end{array}$$

with  $P_1$  projective, and  $\sigma, \tau$  surjective. We may choose  $\beta$  so that  $\sigma = \mu\beta\alpha$ , and then we put

$$X = \{(u, y) \in U_1 \oplus P_2 : \sigma(u) = \mu(y)\},$$

the pullback of the pair of maps  $\sigma, \mu$ . Since  $\sigma$  is surjective, there is an exact sequence

$$0 \rightarrow \ker \sigma \rightarrow X \rightarrow P_2 \rightarrow 0,$$

and therefore  $X \cong W_1 \oplus P_2$ . On the other hand, the surjection  $X \rightarrow U_1$ , given by  $(u, y) \mapsto u$ , is split by the map  $u \in U_1 \rightarrow (u, \beta\alpha u) \in X$ . Therefore  $X \cong U_1 \oplus W_2$ , and the lemma is proved.

**(81.93) Lemma.** *Let  $K$  be the trivial  $G$ -module, and let*

$$0 \rightarrow L \rightarrow \Omega^2 K \xrightarrow{\zeta} K \rightarrow 0$$

be exact, where  $\Omega$  is the Heller-operator. Let  $M$  be a  $G$ -module such that the map

$$\zeta \otimes 1 : \Omega^2 K \otimes M \rightarrow K \otimes M \cong M$$

factors through a projective module. Then there exist projective modules  $E, E'$  such that

$$(L \otimes M) \oplus E \cong \Omega M \oplus \Omega^2 M \oplus E'.$$

*Proof.* There are exact sequences

$$0 \rightarrow L \otimes M \rightarrow \Omega^2 K \otimes M \xrightarrow{\zeta \otimes 1} M \rightarrow 0, \quad 0 \rightarrow \Omega M \rightarrow P \rightarrow M \rightarrow 0,$$

where  $P$  is a projective cover of  $M$ . By (81.92), the hypothesis implies that

$$(L \otimes M) \oplus P \cong \Omega M \oplus (\Omega^2 K \otimes M).$$

But, by (81.91),

$$\Omega^2 K \otimes M = \Omega^2(K \otimes M) \oplus \text{proj}$$

which gives the result.

**Remark.** Using the identification  $\text{Hom}(\Omega^2 K, K) \cong \text{Ext}^2(K, K)$ ,  $\zeta$  determines an element  $\hat{\zeta} \in \text{Ext}^2(K, K)$ . Then  $\hat{\zeta}$  acts (via cup product) on the cohomology ring  $\text{Ext}^*(M, M)$ , and  $\zeta \otimes 1$  factors through a projective if and only if  $\hat{\zeta} \cdot \text{Ext}^*(M, M) = 0$ .

**(81.94) Corollary.** Let  $G$  be a  $p$ -group, and let  $\zeta: \Omega^2 K \rightarrow K$  be a surjection with kernel  $L$ . Assume that

- (i) the map  $\zeta \otimes 1: \Omega^2 K \otimes L \rightarrow L$  factors through a projective and
- (ii)  $L \not\cong \Omega L$ ,  $L \cong \Omega^2 L$ , and  $\dim L = \dim \Omega L$ .

Then  $[L] - [\Omega L]$  is a nonzero element of  $A(G)$  whose square is 0.

*Proof.* In  $A(G)$  we have

$$([L] - [\Omega L])^2 = [L \otimes L] - 2[L \otimes \Omega L] + [\Omega L \otimes \Omega L].$$

Since  $\dim L = \dim \Omega L$ , the right-hand side has dimension 0. Further, projectives are free since  $G$  is a  $p$ -group, so it suffices to show that the right-hand side is 0 modulo projectives. But by (81.93) we have

$$L \otimes L \equiv \Omega L \oplus \Omega^2 L \oplus \text{proj},$$

and by (81.91),

$$L \otimes \Omega L \cong \Omega(L \otimes L) \oplus \text{proj}, \quad \Omega L \otimes \Omega L \cong \Omega^2(L \otimes L) \oplus \text{proj},$$

and the desired result follows since  $L \cong \Omega^2 L$ .

We shall apply this result to the special case where  $G = \langle x, y : x^p = y^p = 1, xy = yx \rangle$  is a  $(p, p)$ -group, with  $p > 2$ . There is an exact sequence

$$(81.95) \quad 0 \rightarrow \Omega^2 K \rightarrow KG \oplus KG \xrightarrow{\theta} KG \xrightarrow{\varepsilon} K \rightarrow 0,$$

where  $\varepsilon$  is the augmentation map, and where

$$\theta(\xi, \eta) = \xi(x - 1) + \eta(y - 1) \quad \text{for } \xi, \eta \in KG.$$

Therefore  $\ker \theta$  is generated by

$$a_0 = (0, N_y), \quad a_1 = (-(y-1), x-1), \quad a_2 = (N_x, 0),$$

where  $N_x = 1 + x + \dots + x^{p-1} = (x-1)^{p-1}$ , and the generators satisfy the relations

$$(x-1)a_0 = N_y a_1, \quad (y-1)a_2 = -N_x a_1.$$

(See Exercise 12.)

Now let

$$0 \rightarrow L \rightarrow \Omega^2 K \xrightarrow{\zeta} K \rightarrow 0$$

be exact, where  $\zeta$  is given by

$$a_0 \rightarrow 1, \quad a_1 \rightarrow 1, \quad a_2 \rightarrow \alpha,$$

for some fixed parameter  $\alpha \in K$ . Then  $L$  is the submodule of  $\Omega^2 K$  generated by

$$a_1 = (-(y-1), x-1) \quad \text{and} \quad b_1 = (N_x, -\alpha N_y).$$

We show that there is an exact sequence

$$(81.96) \quad 0 \rightarrow L \rightarrow KG \oplus KG \xrightarrow{f} KG \oplus KG \xrightarrow{g} L \rightarrow 0,$$

where  $g(\xi, \eta) = \xi b_1 + \eta a_1$ . Define

$$f(\rho, \sigma) = ((x-1)\rho + (y-1)\sigma, \quad \alpha N_y \rho + N_x \sigma),$$

so  $f(L) = 0$ , and  $gf = 0$ . We claim that  $L = \ker f$ . Let  $(\rho, \sigma) \in \ker f$ ; then  $(x-1)\rho + (y-1)\sigma = 0$ , so  $(\rho, \sigma) \in \Omega^2 K$ , and we may write

$$(\rho, \sigma) = t_0 a_0 + t_1 a_1 + t_2 a_2 = (t_2 N_x, t_0 N_y) + t_1 a_1.$$

From  $\alpha N_y \rho + N_x \sigma = 0$  we obtain  $(\alpha t_2 + t_0) N_x N_y = 0$ , and thus  $t_0 = -\alpha t_2 + u$  for some  $u$  in the augmentation ideal of  $KG$ . Therefore

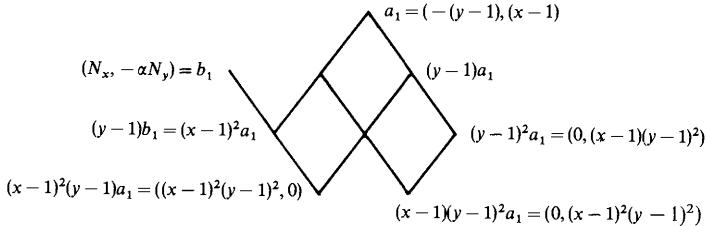
$$(\rho, \sigma) = t_2 (N_x, -\alpha N_y) + t_1 a_1 + (0, u N_y).$$

Since for  $i \geq 1$ ,

$$(0, (x-1)^i N_y) = (x-1)^i N_y (-(y-1), x-1) \in L,$$

it follows that  $(\rho, \sigma) \in L$ . This shows that  $\ker f = L$ , so comparing  $K$ -dimensions we obtain  $\text{im } f = \ker g$ , and the sequence is exact.

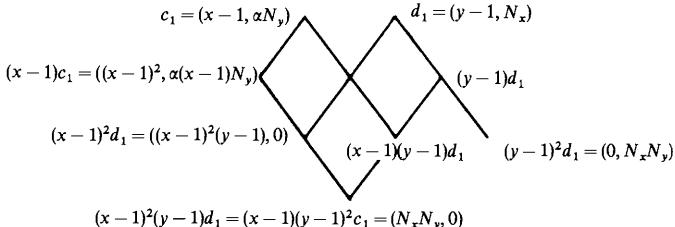
We may represent  $L$  by a picture, in which the lattice points form a  $K$ -basis for  $L$ , and where the diagonals represent multiplication by  $x - 1$  and  $y - 1$ , respectively. We illustrate the case  $p = 3$  below:



In general, we have  $\dim L = \dim \Omega^2 K - 1 = p^2$ . We leave it as exercise for the reader to show that  $L$  is indecomposable as  $KG$ -module. It follows from (81.96) that  $\Omega^2 L \cong L$ , and further that  $\Omega L \cong \ker g \cong \text{im } f$ . Thus,  $\Omega L$  is generated by

$$c_1 = (x - 1, \alpha N_y), \quad d_1 = (y - 1, N_x),$$

and  $\dim \Omega L = \dim (KG \oplus KG) - \dim L = p^2$ . The picture of  $\Omega L$  for  $p = 3$  is given by



Let  $M$  be the submodule of  $L$  spanned by all lattice points except  $b_1$ . Then there is an exact sequence of  $G$ -modules

$$0 \rightarrow M \rightarrow L \rightarrow K \rightarrow 0,$$

which splits when restricted to the cyclic subgroup  $\langle x \rangle$  of  $G$ . On the other hand, from the picture of  $\Omega L$  it is clear that there is no such  $\langle x \rangle$ -split  $G$ -exact sequence for  $\Omega L$  (in place of  $L$ ), and therefore  $L, \Omega L$  are not  $G$ -isomorphic. (But  $L \cong \Omega L$  when  $p = 2$ !)

It remains to prove that the  $KG$ -surjection

$$\zeta \otimes 1 : \Omega^2 K \otimes L \rightarrow K \otimes L \cong L, \quad u \otimes l \mapsto \zeta(u)l,$$

factors through a projective. Consider the diagram

$$\begin{array}{ccccccc} 0 & \longrightarrow & L & \longrightarrow & (KG)^{(2)} & \longrightarrow & (KG)^{(2)} \longrightarrow L \longrightarrow 0 \\ & & \downarrow \mu_2 & & \downarrow \mu_1 & & \downarrow \mu_0 \\ 0 & \longrightarrow & \Omega^2 K \otimes L & \longrightarrow & W_1 \otimes L & \longrightarrow & W_2 \otimes L \longrightarrow L \longrightarrow 0 \end{array}$$

where the bottom row is obtained by applying  $* \otimes L$  to the exact sequence

$$0 \rightarrow \Omega^2 K \rightarrow W_1 \rightarrow W_0 \rightarrow K \rightarrow 0$$

obtained from a minimal projective resolution of  $K$ . (Here,  $W_0 = KG$ ,  $W_1 = (KG)^{(2)}$ .) One can then find maps  $\{\mu_i\}$  making the diagram commute (see Benson-Carlson [86, Lemma 4.5]). It turns out that  $(\zeta \otimes 1) \circ \mu_2$  is the zero map from  $L$  to  $L$ . Thus, in the diagram

$$\begin{array}{ccccccc} 0 & \longrightarrow & \Omega^2 K \otimes L & \longrightarrow & W_1 \otimes L & \longrightarrow & W_0 \otimes L \longrightarrow L \longrightarrow 0 \\ & & \zeta \otimes 1 \downarrow & & \downarrow & & \downarrow & & 1 \downarrow \\ 0 & \longrightarrow & L & \longrightarrow & * & \longrightarrow & * & \longrightarrow & L \longrightarrow 0. \end{array}$$

the bottom row represents the element  $\hat{\zeta} \cdot \text{id}_L$  in  $\text{Ext}^2(L, L)$ , and is zero in  $\text{Ext}^2(L, L)$ . (See Remark, p. 914.) Thus  $\zeta \otimes 1$  factors through a projective, as claimed.

As shown by Zemanek [71], if the above group  $G$  is a Sylow  $p$ -subgroup of  $G_0$ , then the element  $[L^{G_0}] - [(\Omega L)^{G_0}] \in A(KG)$  is nonzero, and has square 0. To summarize the results known up to this point, we have:

**(81.97) Theorem.** *Let  $K$  be a field,  $\text{char } K = p > 0$ . Let  $G$  be an arbitrary group, and  $P$  a Sylow  $p$ -subgroup of  $G$ .*

- (i) *If  $P$  is cyclic, then  $A(KG)$  has no nilpotent elements except 0.*
- (ii) *Assume  $P$  is noncyclic. If  $p > 2$ , or if  $p = 2$  and  $P$  is not an elementary abelian 2-group, then  $A(KG)$  contains nonzero nilpotent elements.\**
- (iii) *If  $p = 2$  and  $P$  is a (2, 2)-group, then  $A(KG)$  contains no nonzero nilpotent elements.*

Assertion (i) is O'Reilly's Theorem 81.90. Part (ii) is due to Zemanek [71], [73], and is re-proved by Benson-Carlson [86] for the special case  $G = P$ . Part (iii) is due to Conlon [66].

The situation changes drastically when  $K$  is replaced by a  $p$ -adic ring  $R$ , i.e., a complete d.v.r. in a finite extension of  $\mathbb{Q}_p$ . Let  $\mathbb{Z}_p$  denote the ring of  $p$ -adic integers in  $\mathbb{Q}_p$ .

**(81.98) Theorem.** *Let  $R$  be a  $p$ -adic ring with maximal ideal  $\pi R$ .*

- (i) *Assume that  $G$  contains an element of order  $n$ , where  $n \in \pi^2 R$  if  $p > 2$ , and  $n \in 2\pi R$  if  $p = 2$ . Then  $A(RG)$  contains nonzero nilpotent elements. On the other hand, if  $p$  exactly divides  $|G|$ , then  $A(\mathbb{Z}_p G)$  contains no nonzero nilpotent elements.*

- (ii) *If  $G$  has a noncyclic Sylow  $p$ -subgroup, then  $A(\mathbb{Z}_p G)$  contains nonzero nilpotent elements.*

Part (i) is due to Reiner [66], while (ii) is proved in Zemanek [71].

### §81. Exercises

1. For  $x \in A(KG)$ , define its *contragredient*  $x^*$  as follows: if  $x = \sum_{M_i \in \text{Ind } KG} \xi_i [M_i]$ ,  $\xi_i \in \mathbb{C}$ , then

$$x^* = \sum \xi_i [M_i^*],$$

where  $M_i^*$  is the contragredient of  $M_i$ . Prove that for  $x, y \in A(KG)$  we have

$$(x, y)_G = (y^*, x^*)_G,$$

where  $(x, y)_G$  is the pairing defined in (81.60).

2. For each  $M \in \text{Ind } KG$ , let  $\hat{M} \in A(KG)$  be its dual, as in (81.61). Prove that for  $N \in \text{Ind } KG$

$$(\hat{M}^*, N^*)_G = \delta_{MN}.$$

Thus, each  $L \in \text{Ind } KG$  has a left dual  $(\hat{L}^*)^*$ , as well as a right dual  $\hat{L}$ .

3. Show that for  $M \in \text{Ind } KG$ , the element  $\hat{M} \in A(KG)$  is uniquely determined by the formula

$$(N, \hat{M})_G = \delta_{MN} \quad \text{for } N \in \text{Ind } KG.$$

4. Let  $M \in \text{Ind } KG$ , and let  $\varphi: E \rightarrow M$  be a surjection. For  $X$  any  $KG$ -module, let  $\mathcal{P}(X)$  be the following statement:

Each  $f \in \text{Hom}_{KG}(X, M)$  that is *not* a split surjection must factor through  $E$ .

Show that if  $\mathcal{P}(X)$  holds for every  $X \in \text{Ind } KG$ , then  $\mathcal{P}(Y)$  holds for every  $KG$ -module  $Y$ .

[Hint: Let  $f: Y \rightarrow M$ , and write  $Y = \coprod X_i$  as a sum of indecomposable modules  $\{X_i\}$ . Then  $f = \coprod f_i$ , where  $f_i: X_i \rightarrow M$ . For each  $i$ ,  $f_i$  is not an isomorphism, since otherwise  $f$  can be split. Then each  $f_i$  factors through  $E$ , whence so does  $f$ .]

5. Show that there exist left duals  $L$  of indecomposable  $KG$ -modules  $L$  analogous to the right duals given in (81.61). Explicitly, define

$$\check{L} = [L] - [L/\text{soc } L] \quad \text{if } L \text{ is projective.}$$

If  $L$  is not projective, let

$$0 \rightarrow L \rightarrow E \rightarrow \Omega^{-2}L \rightarrow 0$$

be an  $AR'$ -sequence for  $L$ , and set

$$\check{L} = [L] - [E] + [\Omega^{-2}L].$$

Prove that

$$(\check{L}, M)_G = \delta_{LM} \quad \text{for } M \in \text{Ind } KG.$$

Show also that

$$\check{L} = (\hat{L}^*)^* \quad \text{for } L \in \text{Ind } KG,$$

where  $*$  denotes contragredient, and  $\hat{\cdot}$  the dual defined in (81.61).

6. Let  $A$  be a f.d.  $K$ -algebra, and consider an ses of  $A$ -modules  $0 \rightarrow L \rightarrow M \rightarrow N \rightarrow 0$ . Prove that the sequence splits if and only if  $M \cong L \oplus N$ .

[Hint (Auslander): If  $M \cong L \oplus N$ , then the sequence

$$0 \rightarrow \text{Hom}(N, L) \rightarrow \text{Hom}(N, M) \rightarrow \text{Hom}(N, N) \rightarrow 0$$

is exact, by considering  $\dim_K$ .]

7. Let

$$0 \rightarrow A \rightarrow B \rightarrow C \rightarrow 0$$

be a ses of  $KG$ -modules, in which  $A$  and  $C$  are indecomposable. Suppose that

$$(*) \quad [A] - [B] + [C] = \hat{M}$$

for some nonprojective  $M \in \text{Ind } KG$ . Prove that  $C \cong M$ , and that the given sequence is the  $AR$ -sequence for  $M$ .

[Hint: Use (81.63).]

8. Let

$$0 \rightarrow M \rightarrow E \rightarrow N \rightarrow 0, \quad 0 \rightarrow N \rightarrow E \rightarrow M \rightarrow 0$$

be a pair of  $AR$ -sequences of  $KG$ -modules. Prove that  $M \cong N$ .

9. Keeping the notation of Exercise 7, drop the hypothesis that  $A$  and  $C$  are indecomposable, but suppose still that  $(*)$  holds for some nonprojective indecomposable  $M$ . Deduce that the given sequence is the direct sum of the  $AR$ -sequence for  $M$  and a split ses.

10. Let  $H \leq G$ , and let  $M, N$  be  $KH$ -modules. Prove that

$$M^G \cong N^G \Leftrightarrow M^G|_H \cong N^G|_H.$$

[Hint: Use (81.13).]

11. Let  $f: A(G) \rightarrow C$  be a species which factors through the subgroup  $H \leq G$ . Show

- (i) If  $H \leq_G E \leq G$ , then  $f$  factors through  $E$ .
- (ii) Let  $g$  be a species of  $A(H)$  which fuses to  $f$ , and suppose that  $g$  factors through a subgroup  $H_0 \leq H$ . Show that  $f$  factors through  $H_0$ .

12. Let  $G = \langle x \rangle \times \langle y \rangle$  be an elementary abelian  $(p, p)$ -group, and let  $\text{char } K = p$ . Put  $N_x = 1 + x + \cdots + x^{p-1}$ , and define  $N_y$  analogously. Starting with the projective resolution

$$\rightarrow K\langle x \rangle \xrightarrow{N_x} K\langle x \rangle \xrightarrow{x-1} K\langle x \rangle \xrightarrow{\varepsilon_1} K \rightarrow 0.$$

and similarly for  $\langle y \rangle$ , we may tensor the complexes (see Exercise 25.13) to obtain a projective resolution

$$\rightarrow (KG)^{(3)} \xrightarrow{\partial_3} (KG)^{(2)} \longrightarrow KG \xrightarrow{\varepsilon} K \rightarrow 0$$

of the trivial  $G$ -module  $K$ . Then  $\Omega^2 K = \text{im } \partial_3$ . Use this to determine generators for  $\Omega^2 K$ , and relations connecting these generators. Show that  $\dim_K \Omega^2 K = p^2 + 1$ .

# Bibliography

Adams, J. F., Gunawardena, J. H., Miller, H.

[85] The Segal conjecture for elementary abelian  $p$ -groups, *Topology* **24** (1985), 435–460.

Alperin, J. L.

[67] Sylow intersections and fusion, *J. Algebra* **6** (1967), 222–241.

[77] On the Brauer correspondence, *J. Algebra* **47** (1977), 197–200.

[86] *Local representation theory*, Cambridge University Press, Cambridge, 1986.

Alperin, J. L., Broué, M.

[79] Local methods in block theory, *Ann. Math.* **110** (1979), 143–157.

Alperin, J. L., Burry, D. W.

[80] Block theory with modules, *J. Algebra* **65** (1980), 225–233.

Alperin, J. L., Janusz, G. J.

[73] Resolutions and periodicity, *Proc. A.M.S.* **37** (1973), 403–406.

Alperin, R. C., Dennis, R. K., Oliver, R., Stein, M. R.

[86]  $SK_1$  of finite abelian groups II, *Invent. Math.* (1986), to appear.

Alperin, R. C., Dennis, R. K., Stein, M. R.

[73] The nontriviality of  $SK_1(ZG)$ , *Proc. Conf. Ohio State* 1972. Springer Lecture Notes Math. 353, Berlin, 1973, pp. 1–7.

[85]  $SK_1$  of finite abelian groups I, *Invent. Math.* **82** (1985), 1–18.

Alvis, D. L.

[80] Duality in the character ring of a finite Chevalley group, *Proc. Symp. Pure Math. (A.M.S.)* **37** (1980), 353–357.

[82] Duality and character values of finite groups of Lie type, *J. Algebra* **74** (1982), 211–222.

Arnold, J. E., Jr.

[81] Homological algebra based on permutation modules, *J. Algebra* **70** (1981), 250–260.

Artin, E.

[57] *Geometric algebra*, Interscience, New York, 1957.

Atiyah, M. F.

[61] Characters and cohomology of finite groups, *Inst. Hautes Etudes Scientifiques, Publ. Math.* **9** (1961), 23–64.

Atiyah, M. F., MacDonald, I. G.

- [69] *Introduction to commutative algebra*, Addison-Wesley, Reading, Mass., 1969.

Auslander, M.

- [74] Representation theory of Artin algebras II, *Comm. Algebra* **1** (1974), 269–310.
- [84] Relations for Grothendieck groups of artin algebras, *Proc. A.M.S. (3)* **91** (1984), 336–340.

Auslander, M., Reiten, I.

- [74] Almost split sequences II, Paper No. 2, 13 pp. Carleton Math. Lecture Notes, No. 9, Carleton Univ. Ottawa, Ont., 1974.
- [75] Representation theory of Artin algebras III, *Comm. Algebra* **3** (1975), 239–294.

Ballard, J. W.

- [76] Some generalized characters of finite Chevalley groups, *Math. Z.* **147** (1976), 163–174.

Bak, A.

- [84] *Algebraic K-theory, number theory, geometry and analysis*, A. Bak, ed., Springer Lecture Notes 1046, Berlin, 1984.

Bass, H.

- [68] *Algebraic K-theory*, Benjamin, New York, 1968.
- [73a] *Algebraic K-theory I, Higher K-theories*, H. Bass, ed. Springer Lecture Notes 341, Berlin, 1973.
- [73b] *Algebraic K-theory II, Classical algebraic K-theory and connections with arithmetic*, H. Bass, ed. Springer Lecture Notes 342, Berlin 1973.
- [73c] *Algebraic K-theory III, Hermitian K-theory and geometric applications*, H. Bass, ed. Springer Lecture Notes 343, Berlin, 1973.
- [74] *Introduction to some methods of algebraic K-theory*, CBMS Regional Conf. Series, No. 20, Amer. Math. Soc., Providence, 1974.
- [79] The Grothendieck group of the category of abelian group automorphisms of finite order, Preprint, Columbia Univ., New York, 1979.
- [81] Lenstra's calculation of  $G_0(R\pi)$ , and applications to Morse-Smale diffeomorphisms, Springer Lecture Notes 882, Berlin, 1981, pp. 287–318.

Bass, H., Milnor, J., Serre, J.-P.

- [67] Solution of the congruence subgroup problem for  $SL_n(n \geq 3)$ , and  $Sp_{2n}(n \geq 2)$ , *Inst. Hautes Études Sci. Publ. Math.* **33** (1967).

Benard, M., Schacher, M. M.

- [72] The Schur subgroup II, *J. Algebra* **22** (1972), 378–385.

Benson, C. T., Curtis, C. W.

- [72] On the degrees and rationality of certain characters of finite Chevalley groups, *Trans. Am. Math. Soc.* **165** (1972), 251–273; **202** (1975), 405–406.

Benson, C. T., Grove, L. C.

- [71] *Finite reflection groups*, Bogden and Quigley, Tarrytown, N. Y., 1971.

Benson, D. J.

- [84a] *Modular representation theory: New trends and methods*, Springer Lecture Notes 1081, Berlin, 1984.

- [84b] Lambda and psi operations on Green rings, *J. Algebra* **87** (1984), 360–367.
- Benson, D. J., Carlson, J. F.  
 [86] Nilpotent elements in Green rings, *J. Algebra*, to appear.
- Benson, D. J., Parker, R. A.  
 [84] The Green ring of a finite group, *J. Algebra* **87** (1984), 290–331.
- Bernstein, I. N., Gelfand, I. M., Ponomarev, V. A.  
 [73] Coxeter functors and Gabriel's theorem, *Uspechi Mat. Nauk* **28** (1973), 19–33; English transl. *Russian Math. Surveys* **28** (1973), 17–32.
- Borel, A.  
 [70] Properties and linear representations of Chevalley groups. Springer Lecture Notes 131, Berlin, 1970, pp. 1–55.
- Borel, A., Tits, J.  
 [65] Groups réductifs, *Publ. Math. I.H.E.S.* **27** (1965), 55–151.
- Borevich, Z. I., Shafarevich, I. R.  
 [66] *Number theory*, Academic Press, New York, 1966.
- Bourbaki, N.  
 [64] *Algèbre commutative*, V, Hermann, Paris, 1964.  
 [68] *Groupes et algèbres de Lie*, IV, V, VI, Hermann, Paris, 1968.
- Brauer, R.  
 [41] Investigations on group characters, *Ann. Math. (2)* **42** (1941), 936–598.  
 [42a] [42b] On groups whose order contains a prime number to the first power I, *Am. J. Math.* **64** (1942), 401–420; II, ibid. 421–440.  
 [43] On permutation groups of prime degree and related classes of groups, *Ann. Math. (2)* **44** (1943), 57–79.  
 [56] Zur Darstellungstheorie der Gruppen endlicher Ordnung, *Math. Z.* **63** (1956), 406–444.  
 [59] Zur Darstellungstheorie der Gruppen endlicher Ordnung, II, *Math. Z.* **72** (1959), 25–46.  
 [64] Some applications of the theory of blocks of characters, I, *J. Algebra* **1** (1964), 152–167.  
 [67] On blocks and sections in finite groups, I, *Am. J. Math.* **89** (1967), 1115–1136.
- Brauer, R., Nesbitt, C.  
 [37] *On the modular representations of finite groups*, Univ. of Toronto Studies in Mathematics, No. 4, 1937.  
 [41] On the modular characters of groups, *Ann. Math. (2)* **42** (1941), 556–590.
- Brauer, R., Suzuki, M.  
 [59] On finite groups of even order whose 2-Sylow group is a quaternion group, *Proc. Natl. Acad. Sci. USA* **45** (1959), 1757–1759.
- Bredon, G.  
 [72] *Introduction to compact transformation groups*, Academic Press, New York, 1972.
- Broué, M.  
 [82] Dualité de Curtis et caractères de Brauer, *C. R. Acad. Sci. Paris, Ser. I. Math.* **295** (1982) 559–562.

- Broué, M., Puig, L.
- [80] A Frobenius theorem for blocks, *Invent. Math.* **56** (1980) 117–128.
- Burroughs, J.
- [74] Operations in Grothendieck rings and the symmetric group, *Can. J. Math.* **26** (1974), 543–550.
- Carlsson, G.
- [84] Equivariant stable homotopy and Segal's Burnside ring conjecture, *Ann. Math.* **120** (1984), 189–224.
- Carter, R. W.
- [72a] Conjugacy classes in the Weyl group, *Comp. Math.* **25** (1972), 1–59.
  - [72b] *Simple groups of Lie type*, Wiley, London, 1972.
  - [85] *Finite groups of Lie type: Conjugacy classes and irreducible characters*, Wiley, New York, 1985.
- Carter, R. W., Lusztig, G.
- [76] Modular representations of finite groups of Lie type, *Proc. London Math. Soc.* (3) **32** (1976), 347–384.
- Cassels, J. W. S., Fröhlich, A,
- [67] *Algebraic number theory*, Thompson Book Co., Washington, D.C., 1967.
- Cassou-Noguès, P.
- [72] *Classes d'idéaux d'un groupe abélien*, Thesis, Univ. Bordeaux, 1972.
  - [73] Classes d'idéaux de l'algèbre d'un groupe abélien, *C. R. Acad. Sci. Paris Ser. I Math.* **276** (1973), 973–975.
  - [74] Classes d'idéaux de l'algèbre d'un groupe abélien, *Bull. Soc. Math France, Mémoire* **37** (1974), 23–32.
  - [75] Groupe des classes de l'algèbre d'un groupe métacyclique, Sem. Th. Nombres 1974–75, Univ. Bordeaux I, Talence, no. 14. *J. Algebra* **41** (1976), 116–136.
  - [79] Structure galoisienne des anneaux d'entiers, *Proc. London Math. Soc.* (3) **38** (1979), 545–576.
- Cassou-Noguès, P., Queyrut, J.
- [82] Structure galoisienne des anneaux d'entiers d'extensions sauvagement ramifiés II, *Ann. Inst. Fourier Grenoble* **32** (1982), 7–27.
- Chang, B., Ree, R.
- [74] The characters of  $G_2(q)$ , *Symposia Math. XIII*, Academic Press, London, 395–413, 1974.
- Chase, S. U.
- [84] Ramification invariants and torsion galois module structure in number fields, *J. Algebra* **91** (1984), 207–257.
- Chevalley, C.
- [55] Sur certains groupes simples, *Tôhoku Math. J.* (2) **7** (1955), 14–66.
  - [56–58] *Séminaire Chevalley*, Vols. I, II, *Classification des groupes de Lie algébrique*, Paris, Inst. H. Poincaré, 1956–1958.
- Cline, E.
- [73] On minimal vertices and degrees of irreducible characters, *J. Algebra*, **24** (1973), 379–385.

Cohen, J. M.

- [78] On the number of generators of a module, *J. Pure Appl. Algebra* **12** (1978), 15–19.

Cohn, P. M.

- [66] On the structure of  $GL_2$  of a ring, *Inst. Hautes Études Sci. Publ. Math.* **30** (1966), 5–53.

Conlon, S. B.

- [66] The modular representation algebra of groups with Sylow 2-subgroups  $Z_2 \times Z_2$ , *J. Austral. Math. Soc.* **6** (1966), 76–88.
- [68a] Structure in representation algebras, *J. Algebra* **8** (1968), 478–503.
- [68b] Decompositions induced from the Burnside algebra, *J. Algebra* **10** (1968), 102–122.
- [72] A basis for monomial algebras, *J. Algebra* **20** (1972), 396–415.

Coxeter, H. S. M.

- [34] Discrete groups generated by reflections, *Ann Math.* **35** (1934), 588–621.
- [40] The binary polyhedral groups and other generalizations of the quaternion group, *Duke Math. J.* **7** (1940), 367–379.

Curtis, C. W.

- [65] Irreducible representations of finite groups of Lie type, *J. Reine Agnew. Math.* **219** (1965), 180–189.
- [66] The Steinberg character of a finite group with a BN-pair, *J. Algebra* **4** (1966), 433–441.
- [67] The classical groups as a source of algebraic problems, *Am. Math. Monthly* **74** (1967), 80–91.
- [70] Modular representations of finite groups with split BN-pairs, Springer Lecture Notes 131, Berlin, 1970, pp. 57–95.
- [75] Reduction theorems for characters of finite groups of Lie type, *J. Math. Soc. J.* **27** (1975), 666–688.
- [79] Representations of finite groups of Lie type, *Bull. Am. Math. Soc.* **1** (1979), 721–757.
- [80a] Truncation and duality in the character ring of a finite group of Lie type, *J. Algebra* **62** (1980), 320–332.
- [80b] Homology representations of finite groups, Springer Lecture Notes 832, Berlin, 1980, pp. 177–194.
- [82] A duality operation in the character ring of a finite group of Lie type, *Notre Dame Math. Lectures* **10** (1982), 39–71.

Curtis, C. W., Iwahori, N., Kilmoyer, R. W.

- [71] Hecke algebras and characters of parabolic type of finite groups with BN-pairs, *Publ. Math. I.H.E.S.* **40** (1971), 81–116.

Curtis, C. W., Jans, J. P.

- [65] On algebras with a finite number of indecomposable modules, *Trans. Am. Math. Soc.* **114** (1965), 122–132.

Curtis, C. W., Lehrer, G. I.

- [81] Homology representations of finite groups of Lie type, *Contemp. Math. (A.M.S.)* **9** (1981), 1–28.
- [82] A new proof of a theorem of Solomon-Tits, *Proc. Am. Math. Soc.* **85** (1982), 154–156.

Curtis, C. W., Lehrer, G. I., Tits, J.

- [80] Spherical buildings and the character of the Steinberg representation, *Invent. Math.* **58** (1980), 201–210.

- Curtis, C. W., Reiner, I.
- [62] *Representation theory of finite groups and associative algebras* (Pure and Applied Math. Vol. 11) Interscience New York, 1962; 2nd ed., 1966.
- Dade, E.
- [65] On Brauer's second main theorem, *J. Algebra* **2** (1965), 299–311.
  - [66] Blocks with cyclic defect groups, *Ann. Math.* (2) **84** (1966), 20–48.
  - [71] Character theory pertaining to finite simple groups, *Finite Simple Groups*, Academic Press, London, 249–327, 1971.
- Deligne, P.
- [76] Les constantes locales de l'équation fonctionnelle de la fonction  $L$  d'Artin d'une représentation orthogonale, *Invent. Math.* **35** (1976), 299–316.
- Deligne, P., Lusztig, G.
- [76] Representations of reductive groups over finite fields, *Ann. Math.* **103** (1976), 103–161.
  - [82] Duality for representations of a reductive group over a finite field, *J. Algebra* **74** (1982), 284–291.
  - [83] Duality for representations of a reductive group over a finite field, II, *J. Algebra* **81** (1983), 540–545.
- Dembowski, P.
- [68] *Finite geometries*, Springer-Verlag, New York, 1968.
- DeMeyer, F., Ingraham, E.
- [71] *Separable algebras over commutative rings*, Springer Lecture Notes 181, Berlin, 1971.
- DeMeyer, F. R., Janusz, G. J.
- [83] Group rings which are Azumaya algebras, *Trans. Am. Math. Soc.* **279** (1983), 389–395.
- Dennis, R. K.
- [73a] Stability for  $K_2$ , *Proc. Conf. on Orders, Group Rings and Related Topics*, Springer Lecture Notes 353, Berlin, 1973, pp. 85–94.
  - [73b] The computation of Whitehead groups, Notes of a course at Univ. Bielefeld, 1973.
  - [80] Structure of the unit group of a group ring, in *Ring Theory and Algebra III*, B. McDonald, ed., Lecture Notes in Pure and Appl. Math. **55** (1980), 103–130.
  - [82] *Algebraic K-theory*, Parts I, II R. K. Dennis, ed., Springer Lecture Notes 966, 967, Springer-Verlag, Berlin, 1982.
- Dennis, R. K., Stein, M. R.
- [73a] The functor  $K_2$ : a survey of computations and problems, pp. 243–280 in Bass [73b].
  - [73b]  $K_2$  of radical ideals and semilocal rings revisited, pp. 281–303 in Bass [73b].
- Deodhar, V.
- [82] On the root system of a Coxeter group, *Comm. Algebra* **10** (1982), 611–630.
- Desrochers, M.
- [84] Self-duality and torsion Galois modules in number fields, *J. Algebra* **90** (1984), 230–246.
- Dickson, L. E.
- [01] *Linear groups with an exposition of galoisfield theory*, Teubner, Leipzig, 1901; reprinted, Dover, New York, 1958.

- Digne, F., Michel, J.
- [82] Remarques sur la dualité de Curtis, *J. Algebra* **79** (1982), 151–160.
- Donkin, S.
- [80] The blocks of a semisimple algebraic group, *J. Algebra* **67** (1980), 36–53.
- Dress, A. W. M.
- [71] Notes on the theory of representations of finite groups, Bielefeld Notes, 1971.
  - [73] Contributions to the theory of induced representations, *Algebraic K-Theory II*, Springer Lecture Notes 342, Berlin, 1973, pp. 183–240.
  - [75] On relative Grothendieck rings, *Proc. Ottawa Conf. on Representations of Algebras* 1974; Springer Lecture Notes 488, Berlin, 1975.
- Dress, A. W. M., Küchler, M.
- [70] *Zur Darstellungstheorie endlicher Gruppen I*, Bielefeld Notes, 1970.
- Eichler, M.
- [38] Allgemeine Kongruenzklassen einteilungen der Ideale einfacher Algebren über algebraischen Zahlkörpern und ihre  $L$ -Reihen, *J. Reine Angew. Math.* **179** (1938), 227–251.
- Eilenberg, S., Steenrod, N.
- [52] *Foundations of algebraic topology*, Princeton Univ. Press, Princeton, 1952.
- Eisenbud, D., Evans, E. G., Jr.
- [73] Generating modules efficiently: theorems from algebraic K-theory, *J. Algebra* **27** (1973), 278–305.
- Endo, S., Hironaka, Y.
- [79] Finite groups with trivial class groups, *J. Math. Soc. Jpn.* **31** (1979), 161–174.
- Endo, S., Miyata, T.
- [73–74] Quasi-permutation modules over finite groups, I, II, *J. Math. Soc. Jpn.* **25** (1973), 397–421; **26** (1974), 698–713.
  - [76] On the projective class group of finite groups, *Osaka Math. J.* **13** (1976), 109–122.
  - [80] On the class groups of dihedral groups, *J. Algebra* **63** (1980), 548–573.
- Endo, S., Miyata, T., Sekiguchi, K.
- [82] Picard groups and automorphism groups of integral group rings of metacyclic groups, *J. Algebra* **77** (1982), 286–310.
- Fein, B.
- [74] Minimal splitting fields for group representations, *Pacific J. Math.* **51** (1974), 427–431.
- Feit, W.
- [67] *Characters of finite groups*, Benjamin, New York, 1967.
  - [69] Some properties of the Green correspondence, *Theory of Finite Groups*, Benjamin, New York, 1969, pp. 139–148.
  - [76] Divisibility of projective modules of finite groups, *J. Pure Appl. Algebra* **8** (1976), 183–185.
  - [80] Some consequences of the classification of finite simple groups, *Proc. Symp. Pure Math. (A.M.S.)* **37** (1980), 175–181.

- [82] *The representation theory of finite groups*, North-Holland, Amsterdam, 1982.
- [83] The computation of some Schur indices, *Israel J. Math.* **46** (1983), 274–300.
- Feit, W., Higman, G.  
 [64] The non-existence of certain generalized polygons, *J. Algebra* **1** (1964), 114–131.
- Fong, P., Seitz, G.  
 [73], [74] Groups with a BN-pair of rank 2, I, *Invent. Math.* **21** (1973), 1–57; II, *ibid.* **24** (1974), 191–239.
- Fong, P., Srinivasan, B.  
 [82] The blocks of finite general linear and unitary groups, *Invent. Math.* **69** (1982), 109–153.
- Friedlander, E. M., Stein, M.  
 [81] *Algebraic K-theory, Evanston, 1980*, E. M. Friedlander and M. Stein eds., Springer Lecture Notes 854, Berlin, 1981.
- Frobenius, G., Schur, I.  
 [06] Über die reellen Darstellungen der endlichen Gruppen, *Sitzber. Preuss. Akad. Wiss.* (1906), 186–208.
- Fröhlich, A.  
 [69], [72] On the classgroup of integral group rings of finite abelian groups, *Mathematika* **16** (1969), 143–152; II, *ibid.* **19** (1972), 51–56.  
 [73] The Picard group of non-commutative rings, in particular of orders, *Trans. Am. Math. Soc.* **180** (1973), 1–46.  
 [75] Locally free modules over arithmetic orders. *J. Reine Angew. Math.* **274/275** (1975), 112–124.  
 [76] Arithmetic and galois module structure for tame extensions, *J. Reine Angew. Math.* **286/287** (1976), 380–440.  
 [83] *Galois module structure of algebraic integers*, Springer-Verlag, Berlin, 1983.  
 [84] *Classgroups and hermitian modules*, Birkhauser, Basel, 1984.
- Frölich, A., Keating, M. E., Wilson, S. M. J.  
 [74] The class group of quaternion and dihedral 2-groups, *Mathematika* **21** (1974), 64–71.
- Fröhlich, A., Reiner, I., Ullom, S.  
 [74] Picard groups and class groups of orders, *Proc. London Math. Soc.* (3) **29** (1974), 405–434.
- Gabriel, P.  
 [72] Unzerlegbare Darstellungen, I, *Manuscripta Math.* **6** (1972), 71–103.  
 [73] Indecomposable representations II, *Symp. Math. Inst. Nazionale Alta Mat. (Rome)*, **11** (1973), 81–104.  
 [80] Auslander-Reiten sequences and representation finite algebras, Springer Lecture Notes 831, Berlin, 1980, pp. 1–71.
- Galovich, S.  
 [74] The class group of a cyclic  $p$ -group, *J. Algebra* **30** (1974), 368–387.
- Galovich, S., Reiner, I., Ullom, S.  
 [72] Class groups for integral representations of metacyclic groups, *Mathematika* **19** (1972), 105–111.

Garland, H.

- [73]  $p$ -adic curvature and the cohomology of discrete subgroups of  $p$ -adic groups, *Ann. Math.* **97** (1973), 375–423.

Gersten, S. M.

- [73] *Problems about higher K-functors*, Springer Lecture Notes 341, Berlin, 1973, pp. 43–56.

Glauberman, G.

- [66] Central elements in core-free groups, *J. Algebra* **4** (1966), 403–420.

Gluck, D.

- [81] Idempotent formula for the Burnside algebra with applications to the  $p$ -subgroup simplicial complex, *Illinois J. Math.* **25** (1981), 63–67.

Gluck, D., Isaacs, I. M.

- [83] Tensor induction of generalized characters and permutation characters, *Illinois J. Math.* **27** (1983), 514–518.

Godement, R.

- [64] *Théorie des faisceaux*, Act. Sci. et Indust. 1252, Hermann, Paris, 1964.

Goldschmidt, D. M., Isaacs, I. M.

- [75] Schur indices in finite groups, *J. Algebra* **33** (1975), 191–199.

Gorenstein, D.

- [68] *Finite groups*, Harper and Row, New York, 1968.

Green, J.A.

- [55] The characters of the finite general linear groups, *Trans. Am. Math. Soc.* **80** (1955), 402–447.  
 [62a] Blocks of modular representations, *Math. Z.* **79** (1962), 100–115.  
 [62b] The modular representation algebra of a finite group, *Illinois J. Math.* **6** (1962), 607–619.  
 [63] Some remarks on defect groups, *Math Z.* **107** (1963), 133–150.  
 [64] A transfer theorem for modular representations, *J. Algebra* **1** (1964) 73–84.  
 [70] The Steinberg characters of finite Chevalley groups, *Math. Z.* **117** (1970), 272–288.  
 [71] Axiomatic representation theory for finite groups, *J. Pure Appl. Algebra* **1** (1971), 41–77.  
 [72] Relative module categories for finite groups, *J. Pure Appl. Algebra* **2** (1972), 371–393.  
 [74] Walking around the Brauer tree, *J. Aust. Math. Soc.* **17** (1974), 197–213.  
 [76] Locally finite representations, *J. Algebra* **41** (1976), 137–171.  
 [78a] On the Brauer homomorphism, *J. London Math. Soc.* **17** (1978), 58–66.  
 [78b] On a theorem of H. Sawada, *J. London Math. Soc.* **18** (1978), 247–252.

Gruenberg, K. W.

- [67] Profinite groups, *Algebraic Number Theory* (Proc. Inst. Conf. Brighton), Thompson, Washington, D. C., 1967, pp. 116–127.  
 [70] *Cohomological topics in group theory*, Springer Lecture Notes 143, Berlin, 1970.  
 [76] *Relation modules of finite groups*, Regional Conference Math. 25, Amer. Math. Soc., Providence, 1976.

Gustafson, W. H.

- [72] Integral relative Grothendieck rings, *J. Algebra* **22** (1972), 461–479.  
 [77] Burnside rings which are Gorenstein, *Comm. Algebra* **5** (1977) 1–16.

Gyoja, A.

- [84] On the existence of a  $W$ -graph for an irreducible representation of a Coxeter group, *J. Algebra* **86** (1984), 422–438.

Hall, M.

- [59] *The theory of groups*, Macmillan, New York, 1959.

Hannula, T.

- [68] The integral group ring  $a(R_k G)$ , *Trans. Am. Math. Soc.* **133** (1968), 553–559.

Hannula, T., Ralley, T., Reiner, I.

- [67] Modular representation algebras, *Bull Am. Math. Soc.* **73** (1967) 100–101.

Harada, M.

- [64] Some criteria for hereditarity of crossed products, *Osaka J. Math.* **1** (1964), 69–80.

Harada, M., Sai, Y.

- [70] On categories of indecomposable modules, I, *Osaka J. Math.* **7** (1970), 323–344.

Harish-Chandra

- [70] Eisenstein series over finite fields, *Functional Analysis and Related Fields*, Springer, New York, pp. 76–88. 1970

Hasse, H.

- [52] *Über die Klassenzahl Abelscher Zahlkörper*, Akademie-Verlag, Berlin, 1952.

Heller, A., Reiner, I.

- [64] Grothendieck groups of orders in semisimple algebras, *Trans. Am. Math. Soc.* **112** (1964), 344–355.

- [65] Grothendieck groups of integral group rings, *Illinois J. Math.* **9** (1965), 349–360.

Higman, D. G.

- [54] Indecomposable representations at characteristic  $p$ , *Duke Math. J.* **21** (1954), 369–376.

- [75] Coherent configurations, Part I, Ordinary representation theory, *Geom. Dedicata* **4** (1975), 1–32.

- [76] Coherent configurations, Part II, Weights, *Geom. Dedicata* **5** (1976), 413–424.

Hilbert, D.

- [70] Die Theorie der algebraischen Zahlkörper, *Gesammelte Abh.*, Band 1, Springer-Verlag, New York, 1970.

Hilton P. J., Stammbach, U.

- [71] *A course in homological algebra*, Springer-Verlag, New York, 1971.

Hilton, P. J. and Wylie, S.

- [60] *Homology theory*, Cambridge Univ. Press, 1960.

Howlett, R. B., Lehrer, G. I.

- [80] Induced cuspidal representations and generalized Hecke rings, *Invent. Math.* **58** (1980), 37–64.

- [82] Duality in the normalizer of a parabolic subgroup of a finite Coxeter group, *Bull. London Math. Soc.* **14** (1982), 133–136.

- [83] Representations of generic algebras and finite groups of Lie type, *Trans. Am. Math. Soc.* **280** (1983), 753–777.
- Humphreys, J. E.
- [71] Defect groups for finite groups of Lie type, *Math. Z.* **119** (1971), 149–152.
  - [72] *Introduction to Lie algebras and representation theory*, Graduate Texts in Math. 9, Springer-Verlag, New York, 1972.
- Humphreys, J. E., Jantzen, J. C.
- [78] Blocks and indecomposable modules for semisimple algebraic groups, *J. Algebra* **54** (1978), 494–503.
- Huppert, B.
- [67] *Endliche Gruppen*, I, Springer-Verlag, Berlin, 1967.
- Huppert, B., Blackburn, N.
- [82] *Finite Groups* II, III, Springer-Verlag, Berlin, New York, 1982.
- Iizuka, K.
- [61] On Brauer's theorem on sections in the theory of blocks of group characters, *Math. Z.* **75** (1961), 299–304.
- Isaacs, I. M.
- [76] *Character theory of finite groups*, Academic Press, New York, 1976.
- Ito, N.
- [60] Zur Theorie der Permutationsgruppen vom Grad  $p$ , *Math. Z.* **74** (1960), 299–301.
- Iwahori, N.
- [64] On the structure of the Hecke ring of a Chevalley group over a finite field, *J. Fac. Sci. Univ. Tokyo* **10** (1964), 215–236.
- Jacobinski, H.
- [68a] Über die Geschlechter von Gittern über Ordnungen, *J. Reine Angew. Math.* **230** (1968), 29–39.
  - [68b] Genera and decompositions of lattices over orders, *Acta Math.* **121** (1968), 1–29.
- Jacobson, N.
- [80] *Basic algebra* II, Freeman, San Francisco, 1980.
- James, G. D.
- [78] *The representation theory of the symmetric groups*, Springer Lecture Notes 682, Berlin, 1978.
- James, G. D., Kerber, A.
- [81] *The representation theory of the symmetric group*, *Encyclopedia of Mathematics*, Vol. 16, Addison-Wesley, Reading, Mass., 1981.
- Janusz, G. J.
- [69] Indecomposable modules for finite groups, *Ann. Math.* (2) **89** (1969), 209–241.
  - [72] The Schur index and roots of unity, *Proc. Am. Math. Soc.* **35** (1972), 387–388.
  - [76] Automorphisms of simple algebras and group algebras, *Proc. Philadelphia Conf.*, Dekker Lecture Notes 37 (1976), 381–388.

Kawanaka, N.

- [82] Fourier transforms of nilpotently supported invariant functions on a simple Lie algebra over a finite field, *Invent. Math.* **69** (1982), 411–435.

Kazhdan, D., Lusztig, G.

- [79] Representations of Coxeter groups and Hecke algebras, *Invent. Math.* **53** (1979), 165–184.

Keating, M. E.

- [73] On the  $K$ -theory of the quaternion group, *Mathematika* **20** (1973), 59–62.
- [74] Classgroups of metacyclic groups of order  $p^r q, p$  a regular prime, *Mathematika* **21** (1974), 90–95.
- [76] Values of tame symbols on division algebras, *J. London Math. Soc.* (2) **14** (1976), 25–30.
- [79] Outer automorphisms and nontrivial Picard groups, *Mathematika* **26** (1979), 103–105.

Kervaire, M. A.

- [70] Multiplicateurs de Schur et  $K$ -théorie, in *Essays on topology and related topics*, Springer, New York, 1970, pp. 212–225.
- [76] Opérations d’Adams en théorie des représentations linéaires des groupes finis, *Enseign. Math.* (2) **22** (1976), 1–28.

Kervaire, M. A., Murthy, M. P.

- [77] On the projective class group of cyclic groups of prime power order, *Comm. Math. Helvetici* **52** (1977), 415–452.

Keune, F.

- [75]  $(t^2 - t)$ -Reciprocities on the affine line and Matsumoto’s theorem, *Invent. Math.* **28** (1975), 185–192.
- [78] The relativization of  $K_2$ , *J. Algebra* **54** (1978), 159–177.

Kilmoyer, R.

- [69] *Some irreducible complex representations of a finite group with a BN-pair*, Ph.D. dissertation, M.I.T., Cambridge, Mass., 1969.

Kilmoyer, R., Solomon, L.

- [73] On the theorem of Feit-Higman, *J. Combinatorial Theory* (A), **15** (1973), 310–322.

Klingenberg, W.

- [62] Die Struktur der linearen Gruppen über einem nichtkommutativen lokalen Ring, *Archiv Math.* **13** (1962), 73–81.

Kneser, M.

- [65] Starke Approximation in algebraischen Gruppen, I, *J. Reine Angew. Math.* **218** (1965), 190–203.

Knutson, D.

- [73]  $\lambda$ -rings and the representation theory of the symmetric group, Springer Lecture Notes 308, 1973.

Kratzer, C.

- [80] Opérations d’Adams et représentations de groupes, *Enseign. Math.* (2) **26** (1980), 141–154.
- [83] Rationalité des représentations de groupes finis, *J. Algebra* **81** (1983), 390–402.

Kuku, A. O.

- [76] Some finiteness theorems in the  $K$ -theory of orders in  $p$ -adic algebras, *J. London Math. Soc.* **(2) 13** (1976), 122–128.

Kupisch, H.

- [68] Projective Moduln endlicher Gruppen mit zyklischer  $p$ -Sylow Gruppe, *J. Algebra* **10** (1968), 1–7.
- [69] Unzerlegbare Moduln endlicher Gruppen mit zyklischer  $p$ -Sylow Gruppe, *Math. Z.* **108** (1969), 77–104.

Lam, T. Y.

- [68a] Induction theorems for Grothendieck groups and Whitehead groups of finite groups, *Ann. Sci. Ecole Norm. Sup.* **4** (1968), 91–148.
- [68b] Artin exponent of finite groups, *J. Algebra* **9** (1968), 94–119.
- [76] A refinement of Green’s theorem on the defect group of a  $p$ -block, *Proc. A.M.S.* **54** (1976), 45–48.
- [78] *Serre’s conjecture*, Springer Lecture Notes 635, Berlin, 1978.

Lam, T. Y., Reiner, I.

- [69a] Relative Grothendieck groups, *J. Algebra* **11** (1969), 213–242.
- [69b] Reduction theorems for relative Grothendieck rings, *Trans. Am. Math. Soc.* **142** (1969), 421–435.
- [69c] Finite generation of Grothendieck groups relative to cyclic subgroups, *Proc. Am. Math. Soc.* **23** (1969), 481–489.
- [70a] Restriction maps on relative Grothendieck groups, *J. Algebra* **14** (1970), 260–298.
- [70b] An excision theorem for Grothendieck rings, *Math. Z.* **115** (1970), 153–164.

Lam, T. Y., Reiner, I., Wigner, D.

- [71] Restriction of representations over fields of characteristic  $p$ , *Proc. Symp. Pure Math.* **21** (1971), 99–106.

Landrock, P.

- [83] *Finite group algebras and their modules*, London Math. Soc. Lecture Note Ser. 84, Cambridge Univ. Press, 1983.

Lang, S.

- [62] *Diophantine geometry*, Interscience, New York, 1962.

Lenstra, H. W.

- [81] Grothendieck groups of abelian group rings, *J. Pure Appl. Algebra* **20** (1981), 173–193.

Li, I.

- [74] Burnside algebra of a finite inverse semigroup, *Zap. Nauc. Steklov Inst.* **46** (1974), 41–52; *J. Soviet Math.* **9** (1978), 322–331.

Liehl, B.

- [81] On the group  $SL_2$  over orders of arithmetic type, *J. Reine Angew. Math.* **323** (1981), 153–171.

Liu, M.-L.

- [82] The group  $G_1(R\pi)$  for  $\pi$  a finite abelian group, *J. Pure Appl. Algebra* **24** (1982), 287–291.

Loday, J.-L.

- [78] Cohomologie et groupe de Steinberg relatifs, *J. Algebra* **54** (1978), 178–202.

Long, R. L.

- [77] *Algebraic number theory*, Marcel Dekker, New York, 1977.

Lusztig, G.

- [74] *The discrete series of  $GL_n$  over a finite field*, *Ann. Math. Studies* 81, Princeton Univ. Press, 1974.
- [76] Divisibility of projective modules of finite Chevalley groups by the Steinberg character, *Bull. London Math. Soc.* **8** (1976), 130–134.
- [79] On the reflection representation of a finite Chevalley group, *London Math. Soc. Lecture Note Ser.* 34, Cambridge Univ. Press, 1979, pp. 325–337.
- [80] Some problems in the representation theory of finite Chevalley groups, *Proc. Symp. Pure Math. (A.M.S.)* **37** (1980), 313–317.
- [81] On a theorem of Benson and Curtis, *J. Algebra* **71** (1981), 490–498.
- [84] *Characters of reductive groups over a finite field*, *Ann. Math. Studies* 107, Princeton Univ. Press, 1984.

Lusztig, G., Spaltenstein, N.

- [79] Induced unipotent classes, *J. London Math. Soc.* **19** (1979), 41–52.

MacWilliams, F. J., Sloane, N. J. A.

- [77] *The theory of error correcting codes*, North Holland, New York, 1977.

Madsen, I.

- [83] Reidemeister torsion, surgery invariants, and spherical space forms, *Proc. London Math. Soc. (3)* **46** (1983), 193–240.

Magurn, Bruce A.

- [78a] Images of  $SK_1ZG$ , *Pacific J. Math.* **79** (1978), 531–539.
- [78b]  $SK_1$  of dihedral groups, *J. Algebra* **51** (1978), 399–415.

Martinet, J.

- [71] Modules sur l’algèbre du groupe quaternion, *Ann. Sci. Ecole Norm. Sup.* **4** (1971), 399–408.
- [77] Character theory and Artin  $L$ -functions, in *Algebraic Number Fields*, A. Fröhlich, ed., Academic Press, New York, 1977.

Matchett, A.

- [76] *Some subgroups and homomorphisms of locally free class groups*, Thesis, Univ. Illinois, 1976.
- [77] Bimodule-induced homomorphisms of locally free class groups, *J. Algebra* **44** (1977), 196–202.
- [80] Exact sequences for locally free class groups, in *Algebraic K-theory II, Oberwolfach*, Springer Lecture Notes 967, Berlin, 1980, pp. 280–290.
- [81] Class groups of cyclic groups of squarefree order, *Trans. Am. Math. Soc.* **264** (1981), 251–254.

Matsuda, T.

- [82] On the unit groups of Burnside rings, *Jpn. J. Math.* **8** (1982), 71–93.

Matsumoto, H.

- [64] Générateurs et relations des groupes de Weyl généralisés, *C. R. Acad. Sci. Paris* **258** (1964), 3419–3422.

Mayer, S. J.

- [75] On the characters of the Weyl group of type C, *J. Algebra* **33** (1975), 59–67.

McDonald, B. R.

- [84] *Linear algebra over commutative rings*, Marcel Dekker Inc., New York, 1984.

McGovern, K.

- [82] Multiplicities of principal series representations of finite groups with split BN-pairs, *J. Algebra* **77** (1982), 419–442.

Michler, G.

- [72] Blocks and centers of group algebras, Springer Lecture Notes 246, Berlin, 1972, pp. 429–563.

- [75] Green correspondence between blocks with cyclic defect groups II, Springer Lecture Notes 488, Berlin, 1975, pp. 210–235.

- [76] Green correspondence between blocks with cyclic defect groups I, *J. Algebra* **39** (1976), 26–51.

Milgram, J.

- [81] Odd index subgroups of units in cyclotomic fields and applications, Springer Lecture Notes 854, Berlin, 1981, pp. 269–298.

- [82] A survey of the compact space form problem, *Contemp. Math.* **12**, (1982) 219–255.

Milnor, J.

- [66] Whithead torsion, *Bull. Am. Math. Soc.* **72** (1966), 358–426.

- [71] *Introduction to algebraic K-theory*, Ann. Math. Studies **72**, Princeton Univ. Press, 1971.

Morita, K.

- [51] On group rings over a commutative field which possess radicals expressible as principal ideals, *Science Reports Tokyo Daigaku* **4** (1951), 177–194.

Nagao, H.

- [63] A proof of Brauer's theorem on generalized decomposition numbers, *Nagoya Math. J.* **22** (1963), 73–77.

Nakayama, T.

- [40] Note on uniserial and generalized uniserial rings, *Proc. Imp. Acad. Jpn.* **16** (1940), 285–289.

Neukirch, J.

- [69] *Klassenkörpertheorie*, Bibliog. Inst., Mannheim, 1969.

Norton, P.

- [79] O-Hecke algebras, *J. Aust. Math. Soc. (Ser. A)* **27** (1979), 337–357.

Obayashi, T.

- [66] On the Grothendieck group of an abelian  $p$ -group, *Nagoya Math. J.* **26** (1966), 101–113.

- [73] The Whitehead groups of dihedral 2-groups, *J. Pure Appl. Algebra* **3** (1973), 59–71.

Okuyama, T.

- [78] A note on the Brauer correspondence, *Proc. Jpn. Acad. Ser. A Math. Sci.* **54** (1978), 27–28.

- [81] On blocks and subgroups, *Hokkaido Math. J.* **10** (1981), 555–563.

Oliver, R.

- [77]  $G$ -actions on disks and permutation representations II, *Math. Z.* **157** (1977), 237–263.
- [78] Subgroups generating  $D(ZG)$ , *J. Algebra* **55** (1978), 43–57.
- [80a]  $SK_1$  for finite group rings I, *Invent. Math.* **57** (1980), 183–204; correction, *ibid.* **64** (1981), 167–169.
- [80b]  $SK_1$  for finite group rings II, *Math. Scand.* **47** (1980), 195–231.
- [81]  $SK_1$  for finite group rings III, *Algebraic K-theory, Evanston 1980*, Springer Lecture Notes 854, Berlin, 1981, pp. 299–337.
- [83a]  $SK_1$  for finite group rings IV, *Proc. London Math. Soc.* (3) **46** (1983), 1–37.
- [83b]  $D(Z\Pi)^+$  and the Artin cokernel, *Comment. Math. Helvetici* **58** (1983), 291–311.
- [83c] Class groups of cyclic  $p$ -groups, *Mathematika* **30** (1983), 26–57.

O'Reilly, M. F.

- [65] On the modular representation algebra of a finite group, *Illinois J. Math.* **9** (1965), 261–276.

Osima, M.

- [55] Notes on blocks of group characters, *Math. J. Okayama Univ.* **4** (1955), 175–188.

Osofsky, B. L.

- [66] A generalization of quasi-Frobenius rings, *J. Algebra* **4** (1966), 373–387.

Peel, M. H.

- [75] *Modular representations of the symmetric groups*, Univ. of Calgary Research Paper 292, 1975.

Pontrjagin, L.

- [39] *Topological groups*, Princeton Univ. Press, Princeton, 1939.

Quillen, D.

- [73] Higher algebraic K-theory: I, in *Algebraic K-theory I*, Proc. Battelle Inst. Conf. 1972; Springer Lecture Notes 341, Berlin, 1973, pp. 85–147.
- [78] Homotopy properties of the poset of non-trivial  $p$ -subgroups of a group, *Adv. Math.* **28** (1978), 101–128.

Rasmussen, J. R.

- [74] Rationally represented characters and permutation characters of nilpotent groups, *J. Algebra* **29** (1974), 504–509.
- [77] The Artin index of characters of finite faithful metacyclic groups, *J. Algebra* **46** (1977), 511–522.

Rehmann, U.

- [78] Zentrale Erweiterungen der speziellen lineare Gruppe eines Schiefkörpers, *J. Reine Angew. Math.* **301** (1978), 77–104.

Reiner, I.

- [66] Nilpotent elements in rings of integral representations, *Proc. Am. Math. Soc.* **17** (1966), 270–274.
- [68] The action of an involution in  $K^0(ZG)$  (Russian), *Mat. Zametki* **3** (1968), 523–527.
- [75] *Maximal orders*, Academic Press, London, 1975.

Reiner, I., Roggenkamp, K. W.

- [79] *Integral representations*, Springer Lecture Notes 744, Berlin, 1979.

- Reiner, I., Ullom, S.
- [72] Class groups of integral group rings, *Trans. Am. Math. Soc.* **170** (1972), 1–30.
  - [74a] A Mayer-Vietoris sequence for class groups, *J. Algebra* **31** (1974), 305–342.
  - [74b] Remarks on class groups of integral group rings, *Symp. Math. Inst. Nazionale Alta Mat. (Rome)* **13** (1974), 501–516.
- Reiten, I.
- [85] An introduction to the representation theory of artin algebras, *Bull. London Math. Soc.* **17** (1985), 209–233.
- Ribes, L.
- [70] Introduction to profinite groups and Galois cohomology, *Queen's Univ. Papers Pure Appl. Math.* **24** (1970), Kingston, Canada.
- Richen, F.
- [69] Modular representations of split BN-pairs, *Trans. Am. Math. Soc.* **140** (1969), 435–460.
- Riehm, C.
- [70] The norm 1 group of a  $p$ -adic division algebra, *Am. J. Math.* **92** (1970), 499–523.
- Rim, D. S.
- [59] Modules over finite groups, *Ann. Math. (2)* **69** (1959), 700–712.
- Ritter, J.
- [82] On orthogonal and orthonormal characters, *J. Algebra* **76** (1982), 519–531.
- Robinson, G. R.
- [83] The number of blocks with a given defect group, *J. Algebra* **84** (1983), 493–502.
- Roggenkamp, K. W.
- [77] The construction of almost split sequences for integral group rings and orders, *Comm. Algebra* **5** (1977), 1363–1373.
- Roggenkamp, K. W., Schmidt, J. W.
- [76] Almost split sequences for integral group rings and orders, *Comm. Algebra* **4** (1976), 893–917.
- Roggenkamp, K. W., Scott, L. L.
- [83] Units in metabelian group rings: non-splitting examples for normalized units, *J. Pure Appl. Algebra* **27** (1983), 299–314.
- Roiter, A. V.
- [66] On integral representations belonging to a genus, *Izv. Akad. Nauk SSSR Ser. Mat.* **30** (1966), 1315–1324; English transl., *Am. Math. Soc. Transl. (2)* **71** (1968), 49–59.
  - [68] Unboundedness of the dimensions of the indecomposable representations of an algebra which has infinitely many indecomposable representations, *Izv. Akad. Nauk SSSR Ser. Mat.* **32** (1968), 1275–1282.
- Rosenberg, A.
- [61] Blocks and centres of group algebras, *Math. Z.* **76** (1967), 209–216.
- Rosenberg, A., Zelinsky, D.
- [61] Automorphisms of separable algebras, *Pacific J. Math.* **11** (1961), 1109–1117.

Rotman, J.

- [79] *An introduction to homological algebra*, Academic Press, New York, 1979.

Sah, C.-H.

- [68] Automorphisms of finite groups, *J. Algebra* **10** (1968), 47–68.

Santa-Pietro, J. J.

- [72] The Grothendieck ring of dihedral and quaternion groups, *J. Algebra* **22** (1972), 34–44.

Sawada, H.

- [77] A characterization of the modular representations of finite groups with split  $(B, N)$ -pairs, *Math. Z.* **155** (1977), 29–41.

Scott, L.

- [73] Modular permutation representations, *Trans. Am. Math. Soc.* **175** (1973), 101–121.

Sekiguchi, K.

- [83], [86] On the automorphism group of the  $p$ -adic group ring of a metacyclic  $p$ -group, *J. Algebra* **82** (1983), 488–507; II, *ibid.* **100** (1986), 191–213.

Serre, J.-P.

- [62] *Corps locaux*, Hermann, Paris, 1962.

- [71] Conducteurs d'Artin des caractères réels, *Invent. Math.* **14** (1971), 173–183.

- [77] *Linear representations of finite groups*, Springer-Verlag, New York, 1977.

Seshadri, C. S.

- [58] Triviality of vector bundles over the affine space  $K^2$ , *Proc. Natl. Acad. Sci. USA* **44** (1958), 456–458.

Siebeneicher, C.

- [76]  $\lambda$ -Ringstrukturen auf dem Burnsidering der Permutationsdarstellungen einer endlichen Gruppe, *Math. Z.* **146** (1976), 223–238.

Silvester, J. R.

- [81] *Introduction to algebraic K-theory*, Chapman and Hall, London–New York, 1981.

Smith, S.

- [82] Irreducible modules and parabolic subgroups, *J. Algebra* **75** (1982), 286–289.

Solomon, L.

- [66] The orders of the finite Chevalley groups, *J. Algebra* **3** (1966), 376–393.

- [67] The Burnside algebra of a finite group, *J. Combinatorial Theory* **2** (1967), 603–615.

- [69] The Steinberg character of a finite group with a  $BN$ -pair, *Theory of Finite Groups (Harvard Symposium)*, Benjamin, New York, 1969, pp. 213–221.

- [74] Rational characters and permutation characters, *Symp. Math. Inst. Nazionale Alta Mat. (Rome)*, **13** (1974), 453–466.

- [76] A Mackey formula in the group ring of a Coxeter group, *J. Algebra*, **41** (1976), 255–264.

Springer, T. A.

- [75] On the characters of certain finite groups, *Lie Groups and their Representations*, Halsted, New York, 1975, pp. 621–644.

- [80] A formula for the characteristic function of the unipotent set of a finite Chevalley group, *J. Algebra* **62** (1980), 393–399.
- Springer, T. A., Steinberg, R.
- [70] Conjugacy classes, Springer Lecture Notes 131, Berlin, 1970, pp. 167–266.
- Srinivasan, B.
- [68] The characters of the finite symplectic group  $Sp(4, q)$ , *Trans. Am. Math. Soc.* **131** (1968), 488–525.
- [79] *Representations of finite Chevalley groups*, Springer Lecture Notes 764, 1979.
- Stancl, D. L.
- [67] Multiplication in Grothendieck rings of integral group rings, *J. Algebra* **7** (1967), 77–90.
- Stein, M. R.
- [73] Surjective stability in dimension 0 in  $K_2$  and related functors, *Trans. Am. Math. Soc.* **178** (1973), 165–191.
- [76] *Algebraic K-theory*, Proc. Conf. Northwestern Univ. (M. Stein, ed.), Springer Lecture Notes 551, 1976.
- [78] Whitehead groups of finite groups, *Bull. Am. Math. Soc.* **84** (1978), 201–212.
- Steinberg, R.
- [51] A geometric approach to the representations of the full linear group over a Galois field, *Trans. Am. Math. Soc.* **71** (1951), 274–282.
- [56], [57] Prime power representations of finite linear groups I, II, *Canad. J. Math.* **8** (1956), 580–591; **9** (1957), 347–351.
- [62] *Générateurs, relations et revêtements de groupes algébriques*, Colloq. Théorie des Groupes Algébriques (Bruxelles, 1962), Librairie Universitaire, Louvain; Gauthier-Villars, Paris, 1962, pp. 113–127.
- [63] Representations of algebraic groups, *Nagoya Math. J.* **22** (1963), 33–56.
- [67] *Lectures on Chevalley Groups*, (Notes taken by J. Faulkner and R. Wilson), Yale Univ. Lecture Notes, 1967.
- [68] Endomorphisms of linear algebraic groups, *Mem. Am. Math. Soc.* **80** (1968).
- Sumioka, T.
- [73] A note on the Grothendieck group of a finite abelian group, *Osaka J. Math.* **10** (1973), 21–24.
- Suslin, A. A., Tulenbaev, M. S.
- [76] Stabilization theorem for the Milnor  $K_2$ -functor, *Zap. Nauchn. Sem. Leningrad. Otdel. Mat. Inst. Steklov* **64** (1976), 131–152 (translation in *J. Soviet Math.* **17** (1981), 1804–1819).
- Swan, R. G.
- [60a] Induced representations and projective modules, *Ann. Math.* **71** (1960), 552–578.
- [60b] Periodic resolutions of finite groups, *Ann. Math.* **72** (1960), 267–291.
- [62] Projective modules over group rings and maximal orders, *Ann. Math.* **76** (1962), 55–61.
- [63] The Grothendieck ring of a finite group, *Topology* **2** (1963), 85–110.
- [65] Minimal resolutions for finite groups, *Topology* **4** (1965), 193–208.
- [68] *Algebraic K-theory*, Springer Lecture Notes 76, Berlin, 1968.
- [71] Excision in algebraic K-theory, *J. Pure Appl. Algebra* **1** (1971), 221–252.
- [80] Strong approximation and locally free modules, in *Ring Theory and Algebra III*, B. McDonald, ed., Marcel Dekker, New York, 1980, pp. 153–223.

- [83] Projective modules over binary polyhedral groups, *J. Reine Angew. Math.* **342** (1983), 66–172.
- Swan, R. G., Evans, E. G.
- [70] *K-theory of finite groups and orders*, Springer Lecture Notes 149, Berlin, 1970.
- Taylor, M.
- [78a] Locally free classgroups of groups of prime power order, *J. Algebra* **50** (1978), 463–487.
  - [78b] Galois module structure of integers of relative abelian extensions, *J. Reine Angew. Math.* **303/304** (1978), 97–101.
  - [78c] On the self-duality of a ring of integers as a Galois module, *Invent. Math.* **46** (1978), 173–177.
  - [79] Adams operations, local root numbers, and the galois module structure of rings of integers, *Proc. London Math. Soc.* (3) **39** (1979), 147–175.
  - [80] A logarithmic approach to classgroups of integral group rings, *J. Algebra* **66** (1980), 321–353.
  - [82] On the structure of certain completed character rings, *J. Algebra* **76** (1982), 226–233.
  - [84] *Classgroups of group rings*, Cambridge Univ. Press, Cambridge, 1984.
- Thomas, C. B.
- [81] Integral representations in the theory of finite CW-complexes (Oberwolfach 1980), Springer Lecture Notes 882, Berlin, 1981, pp. 269–286.
- Thompson, J.
- [67a] Defect groups are Sylow intersections, *Math. Z.* **100** (1967), 146.
  - [67b] Vertices and sources, *J. Algebra* **6** (1967), 1–6.
- Tinberg, N. B.
- [79] Some indecomposable modules of groups with split  $(B, N)$ -pairs, *J. Algebra* **61** (1979), 508–526.
  - [80a] The Levi decomposition of a split  $BN$ -pair, *Pacific J. Math.* **91** (1980), 233–238.
  - [80b] Modular representations of finite groups with unsaturated split  $(B, N)$ -pairs, *Can. J. Math.* **32** (1980), 714–733.
- Tit, J.
- [62] Théorème de Bruhat et sous-groupes paraboliques, *C. R. Acad. Sci. Paris*, **254** (1962), 2910–2912.
  - [74] *Buildings of spherical type and finite BN-pairs*, Springer Lecture Notes 386, 1974.
- Tokuyama, T.
- [84] On the decomposition rules of tensor products of the representations of the classical Weyl groups, *J. Algebra* **88** (1984), 380–394.
- Uchida, K.
- [67] Remarks on Grothendieck groups, *Tohoku Math. J.* (2) **19** (1967), 341–348.
- Ullom, S.
- [70] A note on the classgroup of integral group rings of some cyclic groups, *Mathematika* **17** (1970), 79–81.
  - [74] The exponent of class groups, *J. Algebra* **29** (1974), 124–132.
  - [76] Nontrivial lower bounds for class groups of integral group rings, *Illinois J. Math.* **20** (1976), 361–371.

- [77] Fine structure of class groups of cyclic  $p$ -groups, *J. Algebra* **49** (1977), 112–124.
- [78] Class groups of cyclotomic fields and group rings, *J. London Math. Soc.* (2) **17** (1978), 231–239.
- [81] Character action on the classgroup of Fröhlich, in *Algebraic K-theory*, R. K. Dennis, Springer Lecture Notes 967, Berlin, 1981.

van der Kallen, W.

- [77] The  $K_2$  of rings with many units, *Ann. Sci. Ecole Norm. Sup.* (4) **10** (1977), 473–515.
- [80] Generators and relations in algebraic  $K$ -theory, *Proc. Int. Congr. Math. Helsinki* 1978, Vol. I, Helsinki, 1980, pp. 305–310.

Vaserstein, L. N.

- [69] On the stabilization of the general linear group over a ring, *Mat. Sb.* **79**(121)(1969), 405–424; translation *Math. USSR Sbornik* **8** (1969), 383–400.
- [71] Stable rank of rings and dimensionality of topological spaces, *Funkcional. Anal. i Prilozhen* (2) **5** (1971), 17–27 (Consultants Bureau Translation, pp. 102–110.)
- [72] On the group  $SL_2$  over Dedekind rings of arithmetic type, *Mat. Sb.* **89**(131)(1972), 313–322; translation *Math. USSR Sbornik* **18** (1972), 321–332.

Vignéras, M.-F.

- [80] *Arithmétique des algébres de quaternions*, Springer Lecture Notes 800, Berlin, 1980.

Wall, C. T. C.

- [65], [66] Finiteness conditions for CW-complexes, *Ann. Math.* (2) **81** (1965), 56–69; II, *Proc. Roy. Soc. Ser. A*, **295** (1966), 129–139.
- [70] On the classification of Hermitian forms: I. Rings of algebraic integers, *Comp. Math.* **22** (1970), 425–451.
- [72] II. Semisimple rings, *Invent. Math.* **18** (1972), 119–141.
- [73] III. Complete semilocal rings, *Invent. Math.* **19** (1973), 59–71.
- [74a] IV. Adèle rings, *Invent. Math.* **23** (1974), 241–260.
- [74b] V. Global rings, *Invent. Math.* **23** (1974), 261–288.
- [74c] Norms of units in group rings, *Proc. London Math. Soc.* (3) **29** (1974), 593–632.
- [76] VI. Group rings, *Ann. Math.* **103** (1976), 1–80.

Washington, L.

- [82] *Introduction to cyclotomic fields*, Graduate Texts in Math 83, Springer-Verlag, New York, 1982.

Webb, D. L.

- [83] *Gröthendieck groups of dihedral and quaternion group rings*, Thesis, Cornell Univ., Ithaca, N. Y., 1983.

Webb, P. J.

- [84] On the orthogonality coefficients for character tables of the Green ring of a finite group, *J. Algebra* **89** (1984), 247–263.

Weiss, E.

- [63] *Algebraic number theory*, McGraw-Hill, New York, 1963.
- [69] *Cohomology of groups*, Academic Press, New York, 1969.

Weyl, H.

- [25], [26] Theorie der Darstellung kontinuierlicher halb-einfacher Gruppen durch lineare

**Bibliography**

- Transformationen I, *Math. Z.* **23** (1925), 271–309; II, *Math. Z.* **24** (1926), 328–376; III, *Math. Z.* **24** (1926), 377–395.
- Williamson, S.
- [63] Crossed products and hereditary orders, *Nagoya Math. J.* **23** (1963), 103–120.
- Wilson, S. M. J.
- [77a] Reduced norms in the  $K$ -theory of orders, *J. Algebra* **46** (1977), 1–11.
  - [77b] Some orders with trivial kernel group, Research note, Univ. of Durham, Durham, England (1977), 1–11.
- Yamada, T.
- [74] *The Schur subgroup of the Brauer group*, Springer Lecture Notes 397, Berlin, 1974.
- Yamagata, K.
- [78] On artinian rings of finite representation type, *J. Algebra* **50** (1979), 278–283.
- Yoshida, T.
- [83] Idempotents of Burnside rings and Dress induction theorem, *J. Algebra* **80** (1983), 90–105.
- Zassenhaus, H.
- [36] Kennzeichnung endlicher linearer Gruppen als Permutationsgruppen, *Hamb. Abb.* **11** (1936), 17–40.
  - [49] *The theory of groups*, Chelsea, New York, 1949.
- Zemanek, J. R.
- [71] Nilpotent elements in representation rings, *J. Algebra* **19** (1971), 453–469.
  - [73] Nilpotent elements in representation rings over fields of characteristic 2, *J. Algebra* **25** (1973), 534–553.

# Notation Index

This index contains only notation introduced for the first time in Volume II. The terminology and notation from Volume I remain in use throughout this volume (see the section on Notation at the beginning of Volume I). For page references concerning the items listed below, see the Subject Index.

## Chapter 5: Algebraic $K$ -theory

$G_0(A)$ ,  $G_0^R(\Lambda)$ ,  $G_0^t(\Lambda)$  = Grothendieck groups

$K_0(A)$  = projective class group

$K_2(A)$  = Milnor group

$K_{\det}(A) \cong K_1(A) = GL(A)/GL'(A)$  = Whitehead group

$E(A)$  = elementary group, generated by all  $\{E_{ij}(a)\}$

$SK_1(A)$  = kernel of determinant map or reduced norm map

$K_i(A, J)$  = relative  $K$ -group

$Wh(RG) = K_1(RG)/(K_1(R) \times G^{ab})$  = Whitehead group

$Wh^F(RG) = Wh(RG)/\text{image of } SK_1(RG)$

$St(A)$  = Steinberg group

$St(A, J)$  = relative Steinberg group

$hd_A M$  = homological dimension

gl. dim. = global dimension

$S_{d+1}(A)$  = stable range condition

## Chapter 6: Class groups of integral group rings and orders

$Cl\Lambda$  = locally free class group

$D(\Lambda)$  = kernel group

$g(M)$  = genus of  $M$

$N \vee M$  means  $N \in g(M)$

$J(A)$ ,  $J^*(A)$  = idèle groups

$U(\Lambda)$ ,  $U^*(\Lambda)$  = unit idèles

$J_0(A)$ ,  $\tilde{J}(A)$  = kernel of reduced norm

$C^+$  = image of global reduced norm

$T(G)$  = Swan subgroup of  $D(\mathbb{Z}G)$

$\det$ ,  $\text{Det}$  = determinant maps

Pic, Picent = Picard groups  
 $LFP$  = locally free Picard group  
 Aut, Autcent = automorphism groups  
 Out, Outcent = outer automorphism groups  
 $LF_n(\Lambda)$  = locally free  $\Lambda$ -modules of rank  $n$

### Chapter 7: The theory of blocks

$B = p$ -block of  $G$   
 $B_1$  = principal  $p$ -block containing the trivial character  
 rad  $A$  = radical of  $A$   
 $T_{H/D}$  = trace map  
 $A_{H/D}$  = image of trace map in the  $G$ -algebra  $A$   
 $M|N$  means  $M$  is isomorphic to a direct summand of  $N$   
 $\text{inv}_H M$  = set of elements of  $M$  fixed by all  $h \in H$   
 $\Delta G$  = diagonal subgroup of  $G \times G = \{(g, g) : g \in G\}$   
 $\sigma$  = Brauer map (relative to a  $p$ -subgroup of  $G$ )  
 $B' \rightarrow (B')^G$  means Brauer Correspondence of  $p$ -blocks  
 $(M, N)_G = \text{Hom}_{RG}(M, N)$   
 $(M, N)_{G/\mathcal{L}} = \sum_{Z_i \in \mathcal{L}} T_{G/Z_i}(M, N)_{Z_i}$   
 $M \rightarrow \Omega M$  means Heller operator  
 $O_p(G)$  = maximal normal  $p$ -subgroup of  $G$   
 $O_{p'}(G)$  = maximal normal  $p'$ -subgroup  
 $\text{cf}(G, X(T)) = \{\alpha \in \text{cf}(G) : \alpha \text{ vanishes outside the union of } p\text{-sections } X(T)\}$

### Chapter 8: The representation theory of finite groups of Lie type

g.g.r. = group generated by reflections  
 $(W, S)$  = Coxeter system  
 $l(w)$  = length of  $w$   
 $\{W_J\}, \{P_J\}$  = parabolic subgroups of  $W$  and  $G$ , respectively  
 $D_{IJ}$  = set of distinguished double coset representatives  
 $\Lambda$  = Lefschetz character of a homology representation  
 $|\Gamma|$  = geometric realization = underlying topological space  
 $\mathcal{H}(G, B)$  = Hecke algebra  
 IND, SGN = index and sign homomorphisms  
 $d_\varphi, F_\varphi(u)$  = generic degree, generic degree polynomial  
 $T_L^G, R_L^G$  = truncation and generalized induction  
 $A_J, \mathcal{E}_J$  = association classes of parabolic subgroups, irreducible characters  
 $\text{St}_G$  = Steinberg character  
 $D_G$  = duality operation

**Chapter 9: Rationality questions** $c(M)$  = Frobenius-Schur indicator $m_K(\zeta)$  = Schur index $A(G)$  = Artin exponent**Chapter 10: Indecomposable modules** $F_\alpha^-, F_\alpha^+$  = Coxeter functors $\mathbf{Hom}_A(M, N) = \mathrm{Hom}_A(M, N)/\mathrm{Hom}_A(M, N)_{G/1}$  $\mathcal{N}$  = Nakayama functor $\mathcal{AM}$  = Auslander-Reiten translate $\lambda(M) = c(M)$  = composition length of  $M$ **Chapter 11: The Burnside ring and the representation ring of a finite group** $\Omega(G)$  = Burnside ring $T^{\otimes G}$  = tensor induction $a(G)$  = representation ring = Green ring $A(G)$  = representation algebra $PP(RG)$  = permutation projective  $RG$ -modules



# INDEX

- Absolutely indecomposable, 444, 869  
Adams operator, 360  
Adèle ring, 103  
Admissible  $p$ -modular system, 409, 413  
 $A(G)$ , 346, 365, 782  
Algebraic map, 854  
Almost split sequence, *see* AR-sequence  
Alperin-Dennis-Oliver-Stein Theorem, 211, 213, 214  
Alperin's Theorem, 459, 460  
Alvis's Theorem, 691  
AR-sequence, 816, 831  
AR'-sequence, 817  
Artin cokernel, 782, 787  
Artin exponent, 212, 346, 365, 782  
Artin Induction Theorem, 775, 778, 859  
Auslander-Reiten sequence, *see* AR-sequence  
Auslander-Reiten Theorem, 817, 823  
Auslander-Reiten translate, 822  
Auslander's Theorem, 817  
Autcent, 378  
Azumaya algebra, 403
- Ballard-Lusztig Theorem, 705  
Barycentric subdivision, 588  
Bass Cancellation Theorem, 83  
Bass-Heller-Swan Theorem, 113  
Bass-Milnor-Serre Theorem, 31  
Bass-Milnor Theorem, 211  
Bass Stable Range Theorem, 83  
Bass Theorem:  
    on rank of  $K_1$ , 153  
    on  $SK_1$ , 153  
Bass-Vaserstein Stability Theorem, 81  
Benard-Schacher Theorem, 746  
Benson-Carlson Theorem, 909  
Benson-Curtis Theorem, 648, 653  
Benson-Parker Theorem, 871, 876, 899  
Block, *see*  $p$ -Blocks  
Block ideals, 412  
    as trivial source modules, 444  
Block idempotents, 412  
    coefficients of, 425  
BN-pair, 576, 580
- Borel's Theorem, 155  
Borel subgroup, 577  
Brauer Correspondence, 451, 457, 458, 459, 464  
    and Brauer map, 452  
    and Green Correspondence, 466  
    transitivity of, 462  
Brauer group, 747  
Brauer map, 445, 450, 452, 463  
Brauer's First Main Theorem, 449  
Brauer species, 892  
Brauer-Speiser Theorem, 750  
Brauer's Second Main Theorem, 468, 470, 472, 683  
Brauer's Third Main Theorem, 494  
Brauer-Suzuki Theorem, 532  
Brauer-Thrall conjecture, 830  
Brauer tree, 529  
Brauer-Witt Theorem, 757  
Broué's Theorem, 703  
Bruhat decomposition, 577, 655  
Burnside algebra, 860  
Burnside ring, 839  
Burnside's Theorem, 842
- Cancellation, 232  
Cancellation law, 559, 570  
Canonical character, 492  
Cartan map, 9  
Cassou-Noguès Theorem, 253  
Cayley-Hamilton Theorem, 120  
Central character, 416, 417, 451  
Central separable  $R$ -algebra, 403  
Chain complex, 593  
Chamber, 600  
Characteristic sequence, 114  
Chase's Theorem, 352  
Class defect group, 434  
Class group, 50  
    functorial properties, 338  
Class group  $Cl(\Lambda)$ , 219, 221, 223, 226, 334  
Class group  $Cl_1(\Lambda)$ , 228  
Coherent, 156, 535  
Combinatorial building, 605

- Conjugate character, 156, 535  
 Conlon's Induction Theorem, 859, 864, 886  
 Colon's Theorem, 888, 911  
 Contragredient, 274, 688, 720  
 Core, 497, 499, 808  
 Corestriction, 759  
 Covering blocks, 485  
 Coxeter element, 802  
 Coxeter functors, 794  
 Coxeter graph, 565  
 Coxeter group, 561  
 Coxeter poset, 602  
 Coxeter system, 561, 580  
 Crossed product algebra, 291, 747  
 Crossed product order, 291  
 Crystallographic root system, 552, 800  
 Cuspidal representation, 676  
 Cyclic defect group, 512  
 Cyclic mod  $p$ , *see* Hypo-elementary group  
 Cyclotomic algebra, 748  
  
 $D(\Lambda)$ , 234, 338, 354  
 Decomposition group, 294  
 Decomposition problem, 679  
 Defect of conjugacy class, 425  
 Defect groups of idempotents, 433
  - of classes, 434
  - of  $p$ -blocks, 436, 467
  - as Sylow intersections, 442
  - as vertices, 438
 Defect of  $p$ -block, 422  
 Deformation Theorem of Tits, 641  
 Dennis-Stein symbols, 197, 200  
 Determinantal  $K_1$ , 16, 17, 62  
 Det homomorphism, 331  
 Dihedral group, 101, 553, 621  
 Dimension of prime ideal, 94  
 Distinguished double coset representative, 573  
 Double (of a ring relative to ideal), 126  
 Dress' theorem, 846, 853, 856, 858  
 Dual elements (in  $A(G)$ ), 898, 905  
 Duality operation, 689, 690  
 Dual of a module, 807, 822  
  
 Eichler condition, 139, 304  
 Eichler lattice, 324  
 Eichler's Theorem of Units, 328  
 Eichler-Swan Theorem, 312  
 Eisenbud-Evans Theorem, 93, 94  
 Elementary matrix, 73  
 Elementary operations, 79  
 Elementary subgroup, 73  
 Endo-Hironaka Theorem, 266  
  
 Endo-Miyata-Sekiguchi Theorem, 402  
 Endo-Miyata Theorem, 266  
 $E$ -surjective, 110  
 Euler characteristic, 594  
 Evaluation map, 185  
 Exchange condition, 559, 562, 570, 579  
 Excision Theorem, 121, 129, 194  
 Exp, 356  
 Exponential valuation, 202, 208  
 Extended First Main Theorem, 490  
 Extended module, 118  
  
 Feit-Higman Theorem, 627  
 Finite homological dimension, 19  
 Finite representation type, 504, 506, 799, 831  
 First ramification group, 294  
 Frobenius functor, 4, 346  
 Frobenius identity, 4  
 Frobenius module, 8, 238, 240, 850  
 Frobenius-Schur indicator, 725  
 Frobenius-Schur Theorem, 720, 726  
 Frobenius' Theorem, 778  
 Frölich-Keating-Wilson Theorem, 266, 272  
 Frölich-Reiner-Ullom Theorem, 384, 388  
 Frölich's Theorem, 237, 391, 397, 398  
 Full sublattice, 35  
 Fundamental domain, 601  
 Fundamental reflections, 556  
 Fundamental roots, 556  
 Fusing of species, 893  
  
 $G_1(A)$ , 17  
 Gabriel's Theorem, 803  
 $G$ -algebra, 429, 445, 463  
 Galois group (infinite), 159  
 Galovich-Reiner-Ullom Theorem, 259  
 Galovich's Theorem, 284, 287  
 Generalized  $m$ -gon, 624  
 Generalized restriction, induction, 667  
 Generalized Schanuel's Lemma, 20  
 General linear group, 61, 580  
 Generic algebra, 637  
 Generic degree, 649, 697  
 Generic degree polynomial, 651  
 Genus, 217
  - principal, 218, 304
 Geometric realization, 588  
 $G$ -functor, 849  
 Glauberman's  $Z^*$ -Theorem, 545  
 Global dimension, 21, 113  
 $G$ -poset, 587  
 Green algebra, *see* Representation algebra  
 Green Correspondence, 466, 517, 525
  - functorial properties, 500

- Green's Theorem, 442  
 Green's Theorem on Zeros of Characters, 467  
 Green's Transfer Theorem, 888  
 Grothendieck group, 5, 32  
 Grothendieck ring, 5, 44  
 Grothendieck's Theorem, 113  
 Group generated by reflections (g.g.r.), 552  
 G-set, 838  
  
 Hasse invariant, 746  
 Hecke algebra  $H(G, B)$ , 610  
 Heller operator, 522, 808, 904  
 Heller-Reiner Localization Sequence, 35  
 Heller-Reiner Theorem, 56  
 Higman's Theorem:  
     on indecomposable modules, 504  
     on units in group rings, 164  
 Hilbert Basis Theorem, 113  
 Hilbert Irreducibility Theorem, 651  
 Hilbert Reciprocity Theorem, 206  
 Hilbert symbol, 205  
 Hilbert Syzygy Theorem, 114  
 Hom<sup>+</sup>, 337  
 Homological dimension, 19  
 Homology groups, 152, 593  
 Homology representations, 593  
 Hopf Trace Formula, 594, 607  
 Horseshoe Lemma, 21  
 Hyper-elementary group, 44, 177  
 Hyperoctahedral group, 575  
 Hypo-elementary group, 859  
  
 Idèle, 218  
 Idèle group, 218  
 Idèle normalizer, 385  
 Incidence structure, 624  
 Indecomposable Coxeter system, 565  
 Indecomposable projective module, *see*  
     Principle indecomposable module  
     (P.I.M.)  
 Index, 732, 740  
 Index homomorphism, 614  
 Induced  $G$ -set, 847  
 Induction map, 850  
 Inertia group, 294  
 Inertial index, 493, 512, 526  
 Inertia subfield, 141  
 Injective stability, 81, 129  
 Integral adèles, 103  
 Intertwining number, 898  
 Intertwining Number Theorem, 671  
 Invariant basis number, 78  
 Inverse limit, 156  
 Inverse system, 156  
  
 Invertible bimodule, 370  
 Invertible ideal, 376  
 Involution (on class group), 274  
 Ito's Theorem, 480  
 Iwahori's Theorem, 610  
  
 Jacobinski's Cancellation Theorem, 323, 324  
 Jacobinski's Theorem, 325, 327  
 James' Theorem, 767  
  
 $K^+$ , 138  
 Karoubi square, 111  
 Keating's Theorem, 142, 144  
 Kernel group, 234  
     triviality of, 266  
 Kervaire-Murphy Theorem, 284, 287, 288  
 Kervaire's Theorem, 188  
 ( $K, p$ )-elementary subgroup, 751  
 Krull dimension, 93  
 Krull's Theorem, 160  
 Kuku's Theorem, 142  
 Kummer's Lemma, 281  
  
 Lam's Theorem, 212, 784, 786  
 Lattice, 5, 22  
 Lefschetz character, 594  
 Length  $l(w)$ , 558, 561  
 Lenstra's formula, 59  
 Levi decomposition, 661, 669  
 Linked, 414  
 Local capacity, 144, 312  
 Local index, 144, 312, 746  
 Localization sequence, 32, 35, 44, 65, 71,  
     72  
 Locally free, 218, 382  
 Locally free cancellation, 232, 303  
 Locally free class group, 50, 219, 221, 223,  
     226, 303, 334  
 Locally free Picard group, 383  
 Locally isomorphic, 217  
 Logarithm, 356  
  
 Matsumoto's Theorem, 199, 562  
 Mayer-Vietoris sequence, 101, 105, 195, 231,  
     237  
 Metacyclic group, 259, 349  
 Milnor group, 185  
 Milnor's Theorem, 105  
 Modular Hecke algebra, 707, 709  
 Morita's Theorem, 507, 509  
 Morphism:  
     of Frobenius functors, 8  
     of pairs, 17  
     of triples, 104

- Multiplicative module, 849
- Nagao decomposition, 464, 468
- Nakayama functor, 822
- Newton polygon, 310
- Non- $R$  prime, 139
- Norm, 172
- Normal integral basis, 336
- Normalizer of  $\Lambda$ , 377
- Numerical invariants, 639
- Oliver's Theorem, 212, 283, 354
- Order, 35
- Order ideal, 404
- O'Reilly's Theorem, 912
- Origin of species, 894, 897
- Orthogonal CG-module, 724
- Osima's Theorem, 425
- Outcent, 378
- Outer automorphism group, 372
- $p$ -adic ring, 166
- Parabolic subgroups, 571, 584, 662
- $p$ -Blocks, 412
  - and central characters, 418
  - congruence criterion, 420, 426
  - defect of, 422
  - defect group of, 436
  - of defect zero, 422
  - inertial index of, 493, 512, 526
  - kernel of, 530
  - and normal subgroups, 485
  - and P.I.M.'s, 414
  - principal, 421, 476, 494
  - uniserial, 509, 513
- Perfect group, 74
- Permutation module, 846
- Permutation projective, 878
- Picard group, 371
- Picent, 371
- $p$ -modular system, 407, 409
- $p$ -module, 908
- $pp$ -module, 444, 878
- Prime (of  $K$ ), 139
- Principal genus, 218, 304
- Principal idèle, 219
- Principal indecomposable module (P.I.M.), 411, 414, 427
- Principal  $p$ -block, 421, 476, 494
  - Brauer correspondent of, 453, 494
  - defect group of, 437
  - kernel of, 530
- Product formula, 310
- Product topology, 156
- Profinite completion, 158
- Profinite group, 157, 159
- Projective class group, 15
- Projective homomorphism, 497, 811
- Projective limit, 156
- Projective resolution, 527
- Properly irregular prime, 287
- Pro- $p$ -group, 157
- $p$ -section, 471
- $p$ -section orthogonality, 471
- $p$ -torsion, 166
- $p$ -torsion subgroup, 166, 211
- Puig's Theorem, 877
- Quadratic Reciprocity Theorem, 207
- Quaternion group, 273, 349
- Quillen's Localization Sequence, 71, 144
- Quillen-Suslin Theorem, 113
- Ramification:
  - tame, 295, 336
  - wild, 295
- Ramified, 295
- Rank, 30
- Realizable, 720, 736
- Reduced expression, 558
- Reduced norm, 138
- Reduced projective class group, 220
- Reflection, 551
- Reflection representation, 569, 631, 632
- Regular  $G$ -poset, 591
- Regular prime, 284
- Regular ring, 22
- Rehmann's Theorem, 200
- Reiner's Theorem, 917
- Reiner-Ullom Theorem, 231, 254
- Relative injective, 873
- Relative  $K_0$ -group, 72, 121, 190
- Relative  $K_1$ -group, 124, 126, 190
- Relative  $K_2$ -group, 192
- Relative  $K$ -theory, 123, 126, 191, 193
- Relative projective, 440, 873
- Relative Steinberg group, 191, 193
- Representation algebra, 859, 868
- Representation ring, 859
- Representations of graphs, 791
- Resolvent, 336
- Restriction map, 4, 759
- Rim's Theorem, 108, 244
- Roiter's Theorem, 830
- Root system, 552, 800
- $R$ -order (generalized), 404

- Rosenberg's Lemma, 432  
 Schanuel's Lemma (generalized), 20  
 Schilling's Theorem, 743  
 Schur index, 739  
 Schur multiplier, 152  
 Semidihedral group, 349  
 Semilocal ring, 47, 76  
 Serre's Induction Theorem, 729  
 Serre's Theorem, 83, 95  
 Seshadri's Theorem, 118  
 Sign representation, 602, 614, 695, 763  
 Similar algebras, 747  
 Simple roots, 556  
 Simplicial complex, 587  
 $\text{SK}_1$ , 31, 75, 141, 142, 210  
 of integral group rings, 167, 179  
 Snake Lemma for groups, 138  
 Solomon's Theorem, 604, 608, 776, 788  
 Solomon-Tits Theorem, 606  
 Specht module, 765, 769  
 Specialized algebra, 637  
 Special linear group, 75, 189  
 Species, 892  
 Split BN-pair, 653  
 Split exact sequence, 872  
 Split semisimple algebra, 732  
 $\text{St}(A)$ , 185  
 Stability theorems, 79, 81, 97, 129, 137  
 Stabilizer, 839  
 Stable isomorphism, 15, 78, 219, 303  
 Stable range, 79, 80, 97  
 Stably free, 79  
 $\text{St}(A,J)$ , 191  
 Steinberg group, 185  
 Steinberg relations, 73  
 Steinberg representation, 607, 616, 659, 698  
 Steinberg symbols, 197, 200  
 Steinitz class, 30  
 Strong Approximation Theorem (for kernel of the reduced norm), 312  
 Strong Conjugacy Theorem, 675  
 Subconjugate, 840  
 Sufficiently large, 407  
 Surjective stability, 81, 98  
 Swan-Forster Theorem, 83, 96  
 Swan module, 335, 343  
 Swan's Localization Sequence, 32, 72  
 Swan's Theorem, 47, 49, 53  
 Swan subgroup of the class group, 343, 354  
 Symbols, 197, 200  
 Symplectic  $\mathbb{C}G$ -module, 724  
 Symplectic character, 337, 724  
 System of finite groups with BN-pairs, 644  
 Tamely ramified extension, 336, 352  
 Tame symbol, 202, 208  
 Tate's Theorem, 202  
 Taylor's Theorem, 352, 365  
 Teichmuller map, 163  
 Tensor induction, 852, 855, 858  
 Totally definite quaternion algebra, 304  
 Trace map, 430, 445  
 Trace subgroup, 173  
 Transfer, 759  
 Trivial source module, 444. *See also pp-module*  
 Truncation, 669, 718  
 Twisted group ring, 291  
 Ullom's Theorem, 252, 256, 345, 347  
 Underlying topological space, 588  
 Unimodular, 76, 77  
 Unipotent, 116  
 Uniserial algebra, 505, 511  
 Uniserial block, 509, 513  
 Uniserial module, 505  
 Unitary  $\mathbb{C}G$ -module, 724  
 Unit idèle, 219, 225  
 Units (in semilocal rings), 246  
 Universal central extension, 187  
 Unramified, 144  
 Upper triangular subgroup, 310  
 Vaserstein's Theorem, 81  
 Vertex:  
     of an indecomposable module, 438, 467  
     of a species, 897  
 Very strong approximation theorem, 310  
 Wall square, 103  
 Wall's Theorem, 110, 154, 164, 179  
 Weber's Theorem, 272  
 Weight, 716  
 Weyl group of a root system, 552, 800  
 Weyl subgroup of  $\text{St}_n(A)$ , 198  
 Whitehead group, 17, 62, 164  
 Whitehead Lemma, 74  
 Wilson's Theorem, 291  
 Witt-Berman Theorem, 751  
 Yamagata's Theorem, 834  
 Zemanek's Theorem, 917