

METHODS OF REPRESENTATION THEORY WITH APPLICATIONS TO FINITE GROUPS AND ORDERS

CHARLES W. CURTIS

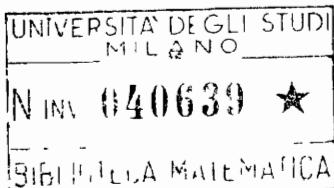
University of Oregon

IRVING REINER

University of Illinois at Urbana-Champaign

VOLUME I

Hobya



A WILEY-INTERSCIENCE PUBLICATION

JOHN WILEY & SONS, New York · Chichester · Brisbane · Toronto

Copyright © 1981 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 Sections 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.”

Bibliography: p.

Includes index.

1. Representations of groups. 2. Finite groups. I. Reiner, Irving. II. Title.

III. Series: Pure and applied mathematics (Wiley).

QA171.C85 512'.2 81-7416

ISBN 0-471-18994-4 AACR2

Printed in the United States of America

10 9 8 7 6 5 4 3 2 1

*To our wives
Betsy and Irma*

PREFACE

In the past 20 years, representation theory of finite groups and associative algebras has enjoyed a period of vigorous development. The foundations have been strengthened and reorganized from new points of view. The applications and connections with other parts of mathematics, while already substantial, have grown in depth and variety and now include powerful results in directions only dimly perceived 20 years ago. It therefore seemed worthwhile and challenging to attempt a survey of the developments since the appearance of our first book (Curtis and Reiner [62]), in the hope that such an effort might encourage the continuation of work already begun, and might lead to further applications.

Representation theory is concerned with the following kind of situation. We are given an action of a finite group on some object, such as a set, a vector space or module over a commutative ring, a simplicial complex, or an algebraic variety. We then introduce a ring (usually a group algebra or a twisted group algebra over an appropriate commutative ring), and we consider modules over the ring, which capture some features of the group action. The next step is to classify the modules so obtained, in terms of the structure of the group algebra, the endomorphism algebras of the modules, the extension problem for the modules, and their character theory. The aim of these efforts is to obtain algebraic or number-theoretical information which may yield new insight about the structure of the finite groups considered, or about their actions on the objects studied initially.

The most extensively developed part of the subject has been the application of representation theory and character theory to the structure of finite groups. This area has been dominated, during the period of our survey, by the work of Richard Brauer (1901–1977). The strength and originality of his own work, combined with the friendly encouragement and inspiration he provided to younger colleagues and students, make his place in the subject a special one. He lived to see the near completion of the work that he and his predecessors Frobenius, Burnside, and Schur all viewed as the grand task to which character theory could make a central contribution, namely, the complete classification of finite simple groups. It is perhaps not too much to hope that new ideas from representation theory, combined with the extraordinary achievements of the past decade on the structure of finite groups, will lead to

simplifications of proofs and a better understanding of this classification problem.

Another subject, algebraic K -theory, has recently approached maturity, and exerts a strong influence on integral representation theory. This area of research, guided by parallels with certain constructions in topology, has suggested new problems of major importance in representation theory. Their solution, in turn, has led to fresh applications to topology and algebraic number theory.

A second interaction between representation theory and geometry has occurred in the representation theory of finite groups of Lie type. In the examples where character tables were known, there were certain representations that were elusive and difficult to construct by standard methods. In a dramatic breakthrough, Deligne and Lusztig discovered general methods for constructing these and other representations through a systematic study of actions of the groups on algebraic varieties.

Our objective in this volume, and in Volume II, is to give an essentially self-contained account of the three main branches of representation theory: ordinary, modular, and integral representation theory. We exhibit here numerous interrelationships among these three subjects, thereby obtaining deeper understanding of each of them. Our approach is not intended to be encyclopedic, but each topic is considered in sufficient depth that the reader may obtain a clear idea of some of the major results in the area. Our selection of topics, from what has now become a vast subject, was guided by our aim of preparing the reader for further work in representation theory and its applications as described above.

As in our first book (hereafter referred to as CR), we have concentrated on general methods. However, the present book also contains considerably sharper and more powerful computational techniques, some of which have been developed in the past few decades. The reader will also find a greater emphasis on methods from homological algebra and commutative ring theory, and somewhat less on purely ring-theoretic considerations.

We have attempted to make this book relatively self-contained, and do not presuppose familiarity with all of the contents of our previous book CR. On the other hand, we occasionally omit details of some of the more elementary results and refer instead to material in CR for background and further information. While it has not been possible to include in this work all of the results in CR, the reader will find that most of the contents of CR are treated here in greater depth and generality. Furthermore, in many areas we go far beyond the contents of CR.

In a few of the sections in this book, we have also inserted references to the book on *Maximal Orders* (see Reiner [75]), which we cite as MO for brevity. In particular, some of the introductory material in Chapter 3, especially in §§24 and 26, would have required much longer discussion had we included the relevant proofs from MO. We have tried to include enough of the material from MO, however, so that the reader will not feel compelled to refer back to MO during a first reading of Chapter 3.

Generally speaking, we assume that the reader has a good general background in algebra, with no more familiarity with representation theory than what is contained in the usual first year graduate course in algebra. Where this approach results in overlapping between this book and CR, we have tried always to give either new proofs or a revised presentation.

This volume begins with a substantial Introduction (§§1–8) which covers the background from group theory, algebraic number theory, commutative and noncommutative ring theory, modules, and homological algebra, needed for both this volume and the next. Here some topics (such as the Morita theorems) are treated in detail, while others are surveyed without proofs, with appropriate references. Many readers will no doubt be familiar with substantial parts, at least, of the Introduction, and in any case can omit (at a first reading) whatever is not essential for those parts of the book they wish to study.

Chapters 1 and 2 provide a comprehensive survey of ordinary and modular representation theory. At least the first parts of most sections are essential for a good understanding of the theory. Two of the main themes of Chapter 1 are the orthogonality relations for characters, and the theory of induced modules and characters. Our treatment of the latter, in §11, includes the Conlon-Tucker-Ward extension of Clifford's theory to describe the decomposition of modules induced from normal subgroups, and the accompanying theory of projective representations and twisted group algebras. We have tried to include in §§11 and 15 a fairly complete survey of known cases where invariant characters of normal subgroups can be extended to the group, including Gallagher's result on characters of normal Hall subgroups. The decomposition of induced modules from non-normal subgroups is treated from the point of view of Hecke algebras, and prepares the way for applications to finite groups of Lie type in Chapter 7. There are also sections on tensor induction and transfer, special classes and exceptional characters, and the Brauer Induction Theorem. Applications include Mackey's results on the decomposition of symmetric and skew-symmetric squares, Suzuki's CA-group Theorem, the Brauer-Suzuki Theorem on generalized quaternion Sylow 2-subgroups, and G. Higman's illustration of the problem of classifying simple groups in terms of centralizers of involutions.

Chapter 2 introduces modular representation theory through the study of the Cartan-Brauer triangle. Here, to some extent, we have followed Serre's elegant treatment of this subject. We then give a detailed account of Green's theory of vertices and sources of RG -lattices, including a new proof due to Conlon and Ward of Green's Indecomposability Criterion. We also discuss the Green correspondence, and Thompson's application of it to the character theory of a group with a self-centralizing cyclic Sylow p -subgroup.

Chapters 3 and 4 are fundamental for the theory of integral representations and can be read independently of Chapters 1 and 2, although there are many connections among all four chapters.

In Chapter 3 the following sections are of special importance, both in this volume and the next: the introductory §23; §24 on the Jordan-Zassenhaus

theorem; the introductory section on maximal orders, including Theorems 26.12, 26.20–26.21a; the beginning of §§27 and 28, especially Theorems 27.1, 28.5, and 28.7; and the first half of §29.

In Chapter 4 the following sections are fundamental: §30 on the local theory; the relation between global and local theory in §31; and the results in §32 on projective lattices over integral group rings.

These chapters also contain numerous examples of integral representations of group rings and orders. Here the basic sections are: §28 on twisted group rings; §§33 and 34 on finite representation type and explicit calculations; and §37 on Bass and Gorenstein orders. The results in §35 will be important in our discussion of Picard groups in Chapter 11. The material in §37 is a brief introduction to a rich circle of ideas in representation theory.

In most cases, we have tried to carry each topic in this volume to the point where further research and extensions of the methods can be considered.

The material in this volume has been used by us as a basis for full year courses on ordinary and modular representation theory, and integral representation theory. We have included exercises after almost every section, to increase the book's usefulness in connection with graduate courses or for self-study, and to present examples and auxiliary results that should prove useful to the researcher.

The bibliography lists only the books and articles referred to in the text of this volume. References are listed according to the last two digits of the year in which they appeared. More extensive bibliographies, and surveys of current research, are available in CR and also in the books listed on the first page of the bibliography.

There remain major parts of the subject to be discussed in Volume II. These include:

Burnside rings and representation rings (Chapter 5).

Rationality properties of group representations (Chapter 6).

Representations of finite groups of Lie type (Chapter 7).

Indecomposable modules (Chapter 8).

Blocks (Chapter 9).

Algebraic K -theory (Chapter 10).

Class groups (Chapter 11).

We have profited enormously from the generous suggestions, criticisms, and encouragement that we have received from students, friends, and colleagues. In particular, we wish to acknowledge the help of David Gluck, Michael Fry, Gerald Janusz, Robert Kilmoyer, and Gary Seitz.

We wish to acknowledge the support we have received from the National Science Foundation for our own research reported on in these volumes.

From the beginning, we have benefited from the continued interest of Beatrice Shube, editor of Wiley-Interscience, and at a later stage from the assistance and attention of David B. Kaplan, associate editor for mathematics, and the production staff at Wiley-Interscience.

It is a pleasure to thank the very capable office staff, in particular Melody Armstrong, Hilda Britt, Karen Cagle, Lillie Douglas, Mabel Jones, and Janet Largent, who cheerfully kept the project moving ahead.

The entire work required the constant support, affection, and understanding of our wives, Betsy and Irma.

CHARLES W. CURTIS
IRVING REINER

Eugene, Oregon

Urbana, Illinois

June 1981

CONTENTS

Notation	xix
Introduction	1
§1. Background material on algebras and groups	1
§1A. <i>Algebras over commutative rings. Integral closure</i>	1
§1B. <i>Background from group theory</i>	6
§2. The functors Hom and \otimes . Projective, injective, and flat modules	13
§2A. <i>Homomorphisms</i>	14
§2B. <i>Tensor products</i>	23
§2C. <i>Categories and functors</i>	27
§2D. <i>Projective, injective, and flat modules</i>	29
§3. Semisimple rings and modules. The Wedderburn and Morita Theorems	40
§3A. <i>Finiteness conditions</i>	40
§3B. <i>Semisimple modules and rings</i>	42
§3C. <i>Semisimple algebras over fields. The theorems of Burnside and Frobenius-Schur</i>	50
§3D. <i>The Morita theorems</i>	55
§3E. <i>Tensor products of simple algebras and modules. The Skolem-Noether Theorem</i>	64
§4. Dedekind domains	73
§4A. <i>Localization</i>	73
§4B. <i>Ideal theory</i>	76
§4C. <i>Valuations, completions, localizations</i>	81
§4D. <i>Modules over Dedekind domains</i>	84
§4E. <i>Duals of lattices</i>	89
§4F. <i>Ideal class groups; global fields</i>	92
§4G. <i>Primary decompositions</i>	93
§4H. <i>Cyclotomic fields</i>	94

§5. Radicals	101
§5A. Basic definitions	101
§5B. Radicals of artinian rings	109
§5C. Local rings	111
§6. Idempotents, indecomposable modules, and the Krull-Schmidt-Azumaya Theorem. Projective covers and injective hulls	119
§6A. Idempotents	119
§6B. The Krull-Schmidt-Azumaya Theorem	127
§6C. Projective covers	131
§6D. Injective hulls	134
§7. Separable algebras and splitting fields	142
§7A. Separable algebras and modules	142
§7B. Splitting fields	149
§7C. Splitting fields for division algebras	154
§7D. Reduced norms	158
§8. Ext, Tor; cohomology of groups	171
§8A. Ext, Tor	171
§8B. Cohomology of groups	179
§8C. The Schur Criterion for split extensions	184
§8D. Tate cohomology groups	187
Chapter 1. Group representations and character theory	195
§9. Orthogonality relations and central idempotents	195
§9A. Frobenius and symmetric algebras	195
§9B. Characters and central idempotents in split semisimple algebras; orthogonality relations	202
§9C. Orthogonality relations for characters of finite groups	206
§9D. The character table	214
§9E. Burnside's p^aq^b -Theorem	221
§10. Induced modules	227
§10A. Definition of induced modules. Frobenius Reciprocity	227
§10B. Mackey's Subgroup Theorem and Tensor Product Theorem	235
§10C. The Intertwining Number Theorem	243
§10D. Contragredient modules	245
§10E. Outer tensor products	249
§11. Decomposition of induced modules. Clifford theory and Hecke algebras	259
§11A. Clifford's Theorem	259
§11B. Applications of Clifford's Theorem to character theory	262
§11C. Decomposition of induced modules from normal subgroups	267

Contents

xv

§11D. Hecke algebras and induced modules	279
§11E. Projective representations and central extensions	291
§12. Tensor algebras	308
§12A. Tensor algebras	308
§12B. Adams operators on the ring of virtual characters	313
§12C. Symmetric and skew-symmetric squares of induced modules	318
§13. Tensor induction and transfer	331
§13A. Tensor induction	331
§13B. Transfer and the determinant map	337
§13C. Normal p -complements and the transfer	341
§14. Special classes and exceptional characters	343
§14A. Frobenius groups	344
§14B. Special classes	348
§14C. Exceptional characters. Suzuki's CA-group Theorem	353
§14D. Characters of A_5 . Examples of exceptional characters	363
§14E. The Brauer-Suzuki Theorem on generalized quaternion Sylow 2-groups	366
§14F. Centralizers of involutions and special classes	370
§15. The Artin and Brauer Induction Theorems	377
§15A. Artin's Induction Theorem revisited	377
§15B. Character rings and the Brauer Induction Theorem	380
§15C. Applications of the Brauer Induction Theorem	384
§15D. Extensions of invariant characters	388
§15E. A criterion for existence of normal complements	392
§15F. A converse to Brauer's Theorem	395
§15G. The Aramata-Brauer Induction Theorem	396
Chapter 2. Introduction to modular representations	401
§16. The decomposition map	402
§16A. Notation and terminology	402
§16B. Grothendieck groups	403
§16C. Reduction mod \mathfrak{p} and the decomposition map	408
§16D. Behavior of Grothendieck groups under extension of ground field	414
§17. Brauer characters	417
§17A. Splitting fields	417
§17B. Brauer characters	419

§18.	The Cartan-Brauer triangle	427
	§18A. <i>The Cartan map and the Cartan-Brauer triangle</i>	428
	§18B. <i>Properties of the Cartan-Brauer triangle (K sufficiently large)</i>	432
	§18C. <i>Orthogonality relations for Brauer characters</i>	437
§19.	Vertices and sources	448
	§19A. <i>Relative projective and injective modules over group rings</i>	449
	§19B. <i>Vertices and sources of indecomposable lattices</i>	453
	§19C. <i>The Green Indecomposability Theorem</i>	459
§20.	The Green correspondence. Applications to character theory	470
	§20A. <i>The Green correspondence</i>	470
	§20B. <i>Applications to character theory</i>	475
§21.	The induction theorem for arbitrary fields	491
	§21A. <i>The Witt-Berman Induction Theorem</i>	491
	§21B. <i>The induction theorem over fields of characteristic $p > 0$</i>	500
	§21C. <i>The Cartan-Brauer triangle (general case)</i>	503
§22.	Modular representations of p -solvable groups	513
Chapter 3. Integral representations: Orders and lattices		520
§23.	Lattices and orders	522
§24.	Jordan-Zassenhaus Theorem	534
§25.	Extensions of lattices	538
§26.	Maximal and hereditary orders	559
	§26A. <i>Existence of maximal orders in separable algebras</i>	559
	§26B. <i>Maximal orders are hereditary</i>	565
	§26C. <i>Structure theorems for maximal and hereditary orders</i>	571
§27.	Group rings and maximal orders	581
§28.	Twisted group rings and crossed product orders	588
§29.	Annihilator of Ext	603
	§29A. <i>Annihilator of Ext; Higman ideal</i>	603
	§29B. <i>Projective endomorphisms</i>	609
Chapter 4. Local and global theory of integral representations		617
§30.	Local theory	618
	§30A. <i>Reduction mod P^k</i>	621
	§30B. <i>Extension of the ground ring</i>	631
	§30C. <i>Representations mod P^k</i>	637

§31.	Genus	642
§31A.	<i>Basic properties</i>	643
§31B.	<i>Idèles and class groups</i>	651
§31C.	<i>Roiter's Theorem on genera</i>	659
§32.	Projective lattices over group rings; Swan's Theorem	670
§32A.	<i>Local case</i>	671
§32B.	<i>Global case</i>	676
§32C.	<i>Characters afforded by projective lattices</i>	679
§33.	Finite representation type	686
§33A.	<i>Jones' Theorem. Jacobinski's criterion for group rings</i>	687
§33B.	<i>Dade's Theorem</i>	691
§33C.	<i>Commutative orders</i>	695
§34.	Examples of integral representations	711
§34A.	<i>Extensions of lattices</i>	712
§34B.	<i>Cyclic p-groups</i>	719
§34C.	<i>Cyclic groups of order p^2</i>	730
§34D.	<i>An order in a matrix algebra</i>	742
§34E.	<i>Dihedral and metacyclic groups</i>	747
§35.	Invertible ideals	755
§36.	The Krull-Schmidt-Azumaya Theorem over discrete valuation rings	767
§37.	Bass and Gorenstein orders	776
Bibliography		795
Index		813

NOTATION

Abbreviations

ACC	ascending chain condition	G.C.D.	greatest common divisor
a.e.	almost everywhere (that is, for all but finitely many exceptions)	im	image
alg. int.	algebraic integers	ind	induction
ann	annihilator	Ind	indecomposable
Aut	automorphism group	inv	invariant
card	cardinality	Irr	irreducible
char	characteristic	ker	kernel
cok	cokernel	K-S-A	Krull-Schmidt- Azumaya
DCC	descending chain condition	nr	reduced norm
deg	degree	ord	order ideal
det	determinant	P.I.D.	principal ideal domain
dim	dimension	pol.	polynomial
disc	discriminant	rad	Jacobson radical
d.v.r.	discrete valuation ring	red.	reduced
End	endomorphism ring	res	restriction
f.d.	finite dimensional	ses	short exact sequence
f.g.	finitely generated (as module)	soc	socle
		tr	reduced trace
		Tr	trace

Set Theory

\emptyset = empty set

$|A|$ = card A = number of elements in set A

$A \subseteq B$	set inclusion
$A \subset B$	proper inclusion of sets
$F \circ G$	composition of maps (first G , then F)
$\forall x$	for all x
\Rightarrow	implies
\Leftrightarrow	if and only if
$\dot{\cup}$	disjoint union

Miscellaneous

\mathbb{Z} =ring of rational integers

\mathbb{Q} =rational field

\mathbb{R} =real field

\mathbb{C} =complex field

$a|b$ a divides b (for elements or ideals)

$a \nmid b$ a does not divide b (for elements or ideals)

$p^m \| a$ means $p^m | a, p^{m+1} \nmid a$

Group Theory

$H \leq G$ ($H < G$) subgroup inclusion (proper inclusion)

$H \trianglelefteq G$ ($H \triangleleft G$) H is a normal subgroup of G (proper)

$|G|=\text{card } G, |G:H|=\text{index of } H \text{ in } G$

$\langle x \rangle =$ cyclic group generated by x

$\langle x, y, \dots \rangle =$ group generated by the elements x, y, \dots

$G_1 \times G_2 =$ direct product of groups

$H \rtimes K =$ semidirect product of normal subgroup H with subgroup K

$G/H = \{xH : x \in G\} =$ left cosets of H in G

$H \setminus G = \{Hx : x \in G\} =$ right cosets of H in G

$H \setminus G / K = \{HxK : x \in G\} =$ collection of (H, K) -double cosets in G

$C_G(\) =$ centralizer in G ; $N_G(\) =$ normalizer in G

$=_G, (\leq_G) =$ equality (or inclusion) up to G -conjugacy

Linear Algebra

$\text{Tr}(x, M) =$ trace of x acting on M

$M_n(R) =$ ring of $n \times n$ matrices over a ring R

$R^{m \times n} =$ additive group of $m \times n$ matrices over R

$GL_n(R) =$ group of invertible $n \times n$ matrices over R

$SL_n(R) = \{X \in GL_n(R) : \det X = 1\}$, if R is commutative

$'X =$ transpose of matrix X

$\text{Tr } \mathbf{X}$ =trace of matrix \mathbf{X}

$\text{char. pol. } \mathbf{X}$ =characteristic polynomial of matrix \mathbf{X}

$\text{diag}(a_1, \dots, a_n)$ =diagonal matrix with diagonal entries a_1, \dots, a_n

Rings and Modules

RG =group algebra of a finite group G over a commutative ring R

$\text{Hom}_A(M, N)$ =group of homomorphisms from A -module M to A -module N

$\text{End}_A M = \text{Hom}_A(M, M)$

$\text{id}_M, 1_M$ =identity map on module M

$\coprod_{i \in I} M_i, M_1 + M_2, M_1 \amalg M_2$ =external direct sums of modules

$\bigoplus_{i \in I} M_i, M_1 \oplus M_2$ =internal direct sums of modules

$M^{(s)}$ =direct sum of s copies of M

$\text{ann}_A M = \{a \in A : aM = 0\}$ =annihilator of M

$\mu_A(M)$ =minimal number of generators of M as A -module

x_r =right multiplication by x ; x_l =left multiplication by x

$c(A)$ =center of ring A

$_A A$ =left regular module (=ring A , as left A -module)

$u(A) = A^\circ$ =units of ring A

A° =opposite ring of A

Category Theory

\mathcal{AB} =category of abelian groups

$_A \mathfrak{M}$ =category of left A -modules (A =ring)

$_A \mathfrak{M}_B$ =category of A, B -bimodules

$_A \text{mod}$ =category of f.g. left A -modules

$\mathcal{P}(A)$ =category of f.g. projective left A -modules

Representation Theory

$M \# N$ =outer tensor product of modules

$\text{Irr}(G)$ =full set of irreducible complex characters of group G

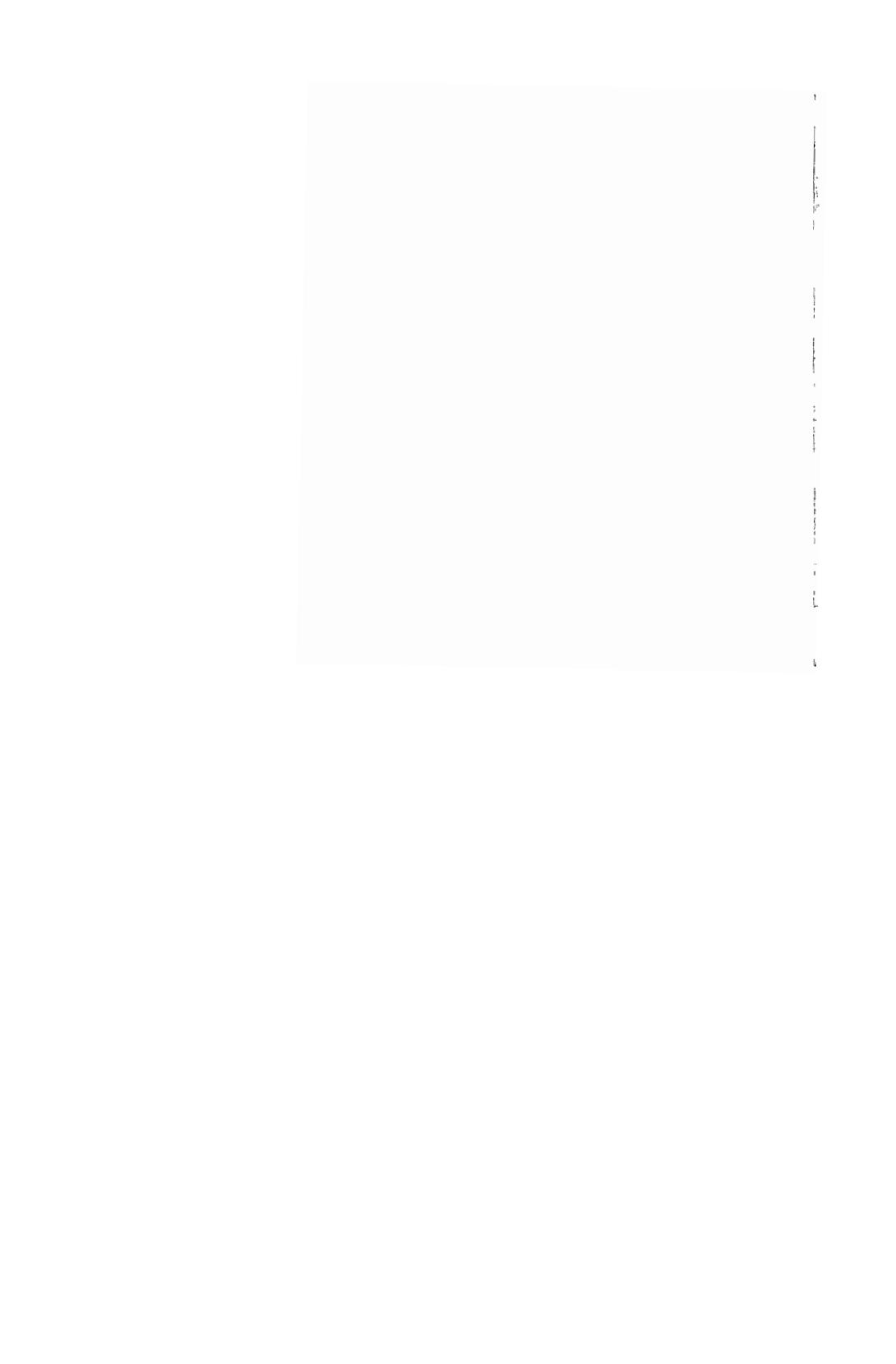
$\text{Irr}_K(G)$ =full set of characters afforded by simple KG -modules

$\text{Ind } RG$ =set of indecomposable RG -lattices

$\text{ch } KG$ =ring of virtual characters afforded by KG -modules

$\text{Bch } kG$ =ring of Brauer characters of G

$\text{cf}_K(G)$ =ring of K -valued class functions on G



METHODS OF REPRESENTATION THEORY

Introduction

§1. BACKGROUND MATERIAL ON ALGEBRAS AND GROUPS

§1A. Algebras over Commutative Rings. Integral Closure

We presuppose familiarity with the basic concepts of rings and modules. Each ring A under consideration is assumed to have an identity element (usually denoted by 1_A or 1), which acts as the identity operator on each A -module. We abbreviate “finitely generated” as “f.g.,” and write M is f.g./ A to indicate that M is a finitely generated A -module.

(1.1) Definition. A ring A is said to be an *algebra over a commutative ring R* , or an *R -algebra*, if there exists a homomorphism $\psi: R \rightarrow c(A)$ from R into the center $c(A)$ of A , such that $\psi(1_R) = 1_A$.

(1.2) Examples. (i) Every ring is a \mathbb{Z} -algebra.

(ii) If G is a group, the *group ring RG* is the set of all formal finite sums

$$\left\{ \sum_{x \in G} \alpha_x x : \alpha_x \in R \right\},$$

with addition and multiplication defined by

$$(\sum \alpha_x x) + (\sum \beta_x x) = \sum (\alpha_x + \beta_x) x, \quad (\sum \alpha_x x)(\sum \beta_y y) = \sum_{x,y} \alpha_x \beta_y xy.$$

This group ring RG is an R -algebra by virtue of the embedding $R \rightarrow RG$, given by $\alpha \mapsto \alpha \cdot 1_G$, $\alpha \in R$, where 1_G is the identity element of G .

In the special case where we start with a field K , we may form the group ring KG , which is usually called the *group algebra* of G relative to K . As shown in CR §10, the study of matrix representations of G over K is essentially equivalent to the study of KG -modules. This point of view will be fundamental throughout our discussion of representations of groups in Chapters 1 and 2.

When R is a ring of integers, we often call RG an *integral group ring*. This concept is important in our discussion of cohomology of groups in §8B, where we make use of the integral group ring $\mathbb{Z}G$. It also plays a basic role in Chapters 3 and 4 on integral representations of groups.

(iii) The ring $M_n(R)$ of all $n \times n$ matrices over R is an R -algebra.

(iv) Given any inclusion $R \subseteq S$ of commutative rings, S is an R algebra.

Let $\psi: R \rightarrow c(A)$ be a homomorphism as in (1.1). We can then define a composition $R \times A \rightarrow A$ by

$$(r, a) \mapsto ra = \psi(r)a, r \in R, a \in A.$$

Under this composition, A becomes a left R -module with the additional property that

$$r(ab) = (ra)b = a(rb), a, b \in A, r \in R.$$

Conversely, let A be a ring which is a left R -module satisfying the above, over a commutative ring R . Then the map $\psi: R \rightarrow A$ defined by $\psi(r) = r \cdot 1_A$, $r \in R$, has the property that $\psi(r) \in c(A)$ for all $r \in R$, and $\psi(1_R) = 1_A$; thus the conditions in Definition 1.1 are satisfied.

An R -subalgebra B of an R -algebra A is a subring B containing 1_A such that B is an R -submodule of A .

Let $\psi: R \rightarrow c(A)$ define the structure of an R -algebra, and let M be a left A -module. Then M becomes a left R -module with composition given by

$$rm = \psi(r)m, r \in R, m \in M,$$

and satisfies the condition

$$r(am) = (ra)m = a(rm), r \in R, a \in A, m \in M.$$

Clearly, A -submodules of M are also R -submodules. In particular, left or right ideals in A are R -submodules of A .

In case A and A' are R -algebras, a homomorphism of rings $f: A \rightarrow A'$ is called a *homomorphism of R -algebras* provided that f preserves the R -module structure on A and A' , that is, $f(ra) = rf(a)$, $r \in R$, $a \in A$. A homomorphism of R -algebras $A \rightarrow M_n(R)$ (see (1.2iii)) is called an *R -representation* of A . If M and M' are A -modules, and A is an R -algebra, an A -homomorphism $f: M \rightarrow M'$ is automatically a homomorphism of R -modules because, if $\psi: R \rightarrow c(A)$ defines the R -structure on A , we have

$$f(rm) = f(\psi(r)m) = \psi(r)f(m) = rf(m),$$

for all $r \in R$, $m \in M$.

It is understood that discussions of rings and modules (in §§2 and 3, for example) carry over to R -algebras and modules without further explanation.

Let A be an R -algebra, for a commutative ring R . We shall define the important concept of integral dependence of elements of A over R . A nonzero polynomial $f(X) \in R[X]$ is *monic* if its leading coefficient is 1. An element $\alpha \in A$ is *integrally dependent* on R , or *integral* over R , if there exists a monic polynomial $f(X) \in R[X]$ such that $f(\alpha) = 0$.

(1.3) Lemma. *Let A be an R -algebra, and let $\alpha \in A$. The following conditions are equivalent:*

(i) α is integral over R .

(ii) $R[\alpha]$ is f.g./ R .

(iii) *There exists an R -subalgebra B of A such that $\alpha \in B$ and B is a f.g. R -submodule of A .*

The proof is left as an exercise (or see MO (1.10)).

(1.4) Corollary. *Let $\alpha, \beta \in A$ be integral over R , and suppose that $\alpha\beta = \beta\alpha$. Then $\alpha \pm \beta$ and $\alpha\beta$ are also integral over R .*

(1.5) Corollary. *Let A be a commutative R -algebra. The set of all R -integral elements of A forms an R -subalgebra of A .*

Remark. It is easy to see that when A is not commutative, sums and products of integral elements are not necessarily integral.

Example. The *algebraic integers* of an algebraic number field L are the elements of L which are integral over \mathbb{Z} . By (1.5), they form a \mathbb{Z} -subalgebra of L , hereafter denoted by $\text{alg. int. } \{L\}$.

(1.6) Definition. Let A be an R -algebra. The *integral closure* of R in A is the set of all R -integral elements in A . The ring R is said to be *integrally closed* in A if the integral closure of R in A coincides with the R -subalgebra $R \cdot 1_A$. An integral domain R is *integrally closed* if it is integrally closed in its quotient field.

Some examples of integrally closed integral domains are:

- (a) P.I.D.'s (principal ideal domains)
- (b) U.F.D.'s (unique factorization domains)
- (c) Dedekind domains (see §4).

- (d) Let R be an integral domain with quotient field K , and let K' be an extension field of K . The integral closure R' of R in K' is an integrally closed domain with quotient field K' .
- (e) Let S be a multiplicative subset of an integrally closed domain R . Then the ring of quotients $S^{-1}R$ is integrally closed (see §4).
- (f) Let R be a U.F.D. Then the polynomial ring $R[X_1, \dots, X_n]$ in indeterminates $\{X_1, \dots, X_n\}$ is a U.F.D., and is integrally closed by b).

Let $R = \mathbb{Z} + \mathbb{Z}(2i)$, a domain with quotient field $\mathbb{Q}(i)$ (viewed as a subfield of the complex field \mathbb{C} , where $i^2 = -1$). Then i is integral over R , but $i \notin R$, so R is not integrally closed. The integral closure of R in $\mathbb{Q}(i)$ is the ring of Gaussian integers $\mathbb{Z} + \mathbb{Z}i$ in $\mathbb{Q}(i)$.

A basic factorization property of polynomials over integrally closed domains is due to Gauss.

(1.7) Gauss's Lemma. *Let R be an integrally closed domain with quotient field K , and let $f(X) \in R[X]$ be a monic polynomial which factors in $K[X]$,*

$$f(X) = g(X)h(X),$$

with $g(X)$ and $h(X)$ monic polynomials in $K[X]$. Then $g(X)$ and $h(X)$ lie in $R[X]$.

Now let R be an integral domain with quotient field K , and A a f.d. K -algebra. For each $\alpha \in A$, the *minimal polynomial* of α over K , denoted by

$$\text{min. pol.}_K(\alpha),$$

is the monic polynomial $f(X) \in K[X]$ of least degree, if one exists, such that $f(\alpha) = 0$. Because $\dim_K A$ is finite, every element $\alpha \in A$ has a minimal polynomial, and $\text{min. pol.}_K(\alpha)$ is uniquely determined by α . Moreover, the existence of a division algorithm in $K[X]$ implies that if $h(X) \in K[X]$ is such that $h(\alpha) = 0$, then $\text{min. pol.}_K(\alpha)$ divides $h(X)$ in $K[X]$. A basic criterion for integral dependence in finite dimensional K -algebras is the following:

(1.8) Proposition. *Let R be an integrally closed domain with quotient field K , and let A be a finite dimensional K -algebra. An element $\alpha \in A$ is integral over R if and only if $\text{min. pol.}_K(\alpha) \in R[X]$.*

The proof is straightforward, using Gauss's Lemma 1.7 (see MO (1.14)).

We recall that for $\alpha \in A$, the *characteristic polynomial*

$$\text{char. pol.}_{A/K}(\alpha)$$

is the characteristic polynomial of the K -linear map $a \mapsto \alpha a$, $a \in A$. From linear algebra, we know that $\text{min. pol.}_K(\alpha)$ and $\text{char. pol.}_{A/K}(\alpha)$ have the same irreducible factors in $K[X]$, apart from multiplicities, and that $\text{min. pol.}_K(\alpha)$ divides $\text{char. pol.}_{A/K}(\alpha)$ in $K[X]$. Keeping the notation of (1.8) and again using Gauss's Lemma, we thus obtain:

(1.9) Proposition. *Let R be integrally closed. An element $\alpha \in A$ is integral over R if and only if $\text{char. pol.}_{A/K}(\alpha) \in R[X]$.*

Remark. For $\alpha \in A$, $\text{char. pol.}_{A/K}(\alpha)$ depends not only on α , but on the choice of the algebra A containing α . On the other hand, if $\alpha \in A \subset B$, where B is another finite dimensional K -algebra, then $\text{min. pol.}_K(\alpha)$ is the same whether we regard α as an element of A or B .

Now let $\{v_1, \dots, v_m\}$ be a K -basis of A , and let $\alpha \in A$. Then we have

$$\alpha v_j = \sum_{i=1}^m a_{ij} v_i, \text{ with } a_{ij} \in K, 1 \leq j \leq m.$$

Let X be an indeterminate over K . Then,

$$\begin{aligned} (1.10) \quad \text{char. pol.}_{A/K}(\alpha) &= \det(\delta_{ij} X - a_{ij}) \\ &= X^m - T_{A/K}(\alpha) X^{m-1} + \cdots + (-1)^m N_{A/K}(\alpha). \end{aligned}$$

We call $T_{A/K}$ the *trace map* (from A to K), and $N_{A/K}$ the *norm map*. Evidently, $T_{A/K}(\alpha)$ is the sum, and $N_{A/K}(\alpha)$ the product, of the eigenvalues of the matrix (a_{ij}) ; $T_{A/K}(\alpha)$ and $N_{A/K}(\alpha)$ are also the trace and determinant, respectively, of the linear transformation $v \mapsto \alpha v$, $v \in A$. From properties of the trace and determinant, and the fact that the map $\alpha \mapsto (a_{ij})$ defines a homomorphism of K -algebras, it follows that

$$(1.11) \quad \begin{cases} T_{A/K}(a\alpha + b\beta) = aT_{A/K}(\alpha) + bT_{A/K}(\beta), T_{A/K}(\alpha\beta) = T_{A/K}(\beta\alpha), \\ N_{A/K}(\alpha\beta) = N_{A/K}(\alpha)N_{A/K}(\beta), N_{A/K}(a\alpha) = a^{\dim_K A} N_{A/K}(\alpha), \end{cases}$$

for all $a, b \in K$, $\alpha, \beta \in A$.

More generally, let V be any f.d. K -space, and let $f \in \text{End}_K V$. Choosing a K -basis for V , we may represent f by a matrix \mathbf{f} over K . We define

$$\text{Tr}(f, V) = \text{trace of } \mathbf{f},$$

and clearly this trace $\text{Tr}(f, V)$ is independent of the choice of K -basis of V . If V is a left A -module, where A is a K -algebra, then each $x \in A$ defines a K -linear map $x_f: V \rightarrow V$, where

$$x_f(v) = xv, v \in V.$$

We then write

$$\mathrm{Tr}(x, V) \text{ or } \mathrm{Tr}(x_l, V)$$

for the trace of x_l acting on V . The analogues of the formulas in (1.11) remain true for this situation.

Each K -algebra A may be viewed as a left A -module, called the *left regular A -module*, ${}_A A$. The map $x \rightarrow x_l$, $x \in A$, is called the *left regular representation* of A , and represents each $x \in A$ by a K -linear transformation $x_l \in \mathrm{End}_K A$. Clearly

$$T_{A/K}(x) = \mathrm{Tr}(x, {}_A A) \text{ for } x \in A.$$

§1B. Background from Group Theory

We assume the reader has an understanding of basic group theory. In this subsection, we review definitions, notation, and elementary facts from three topics in group theory with which we shall frequently be concerned. These are: homomorphisms and group extensions, actions of groups on sets, and presentations of groups in terms of generators and relations. For proofs, and further discussion, the reader may consult CR §§1–7, and introductory material in Hall [59], Huppert [67], or Gorenstein [68].

(1.12) Fundamental Theorem on Homomorphisms. (i) *Let G be a group, and H a normal subgroup of G . The cosets of H in G form a group G/H , and there is a natural epimorphism of groups $\pi: G \rightarrow G/H$, given by $\pi(x) = xH$, $x \in G$.*

(ii) *Let $\varphi: G \rightarrow \bar{G}$ be a homomorphism of groups, and set*

$$\mathrm{im} \varphi = \{\varphi(x) : x \in G\}, \quad \ker \varphi = \{x \in G : \varphi(x) = 1\}.$$

Then $\mathrm{im} \varphi \leq \bar{G}$ and $\ker \varphi \trianglelefteq G$. Moreover, there exists a factorization

$$\varphi = \tilde{\varphi} \circ \pi,$$

where $\pi: G \rightarrow G/\ker \varphi$ is the natural epimorphism in (i) above, and where $\tilde{\varphi}: G/\ker \varphi \rightarrow \mathrm{im} \varphi$ is the isomorphism given by $\tilde{\varphi}(x \cdot \ker \varphi) = \varphi(x)$, for all $x \in G$.

(iii) *Let $\varphi: G \rightarrow \bar{G}$ be an epimorphism of groups. There is a bijection between the family of all subgroups $\bar{H} \leq \bar{G}$, and the family of all subgroups H of G such that $H \geq \ker \varphi$. The bijection is given by $H \rightarrow \varphi(H) = \bar{H}$, and $\bar{H} \rightarrow \varphi^{-1}(\bar{H}) = H$, for subgroups $H \leq G$ such that $H \geq \ker \varphi$, and subgroups $\bar{H} \leq \bar{G}$. We have $\bar{H} \trianglelefteq \bar{G}$ if and only if $\varphi^{-1}(\bar{H}) \trianglelefteq G$, and if this occurs, then*

$$G/\varphi^{-1}(\bar{H}) \cong \bar{G}/\bar{H}.$$

The preceding result is the first step towards analyzing groups in terms of normal subgroups and homomorphic images.

(1.13) Definition. A group G is an *extension* of a group H with kernel N if there exists an epimorphism $\varphi: G \rightarrow H$ such that $N = \ker \varphi$.

Extensions can be described using the language of exact sequences (see §§2 and 8 for further discussion.) Thus, G is an extension of H with kernel N if and only if there exists an exact sequence of groups

$$1 \rightarrow N \xrightarrow{\psi} G \xrightarrow{\varphi} H \rightarrow 1.$$

Exactness means that $\psi: N \rightarrow G$ is injective, φ is surjective, and $\text{im } \psi = \ker \varphi$; then we have $H \cong G/\psi(N)$, by (1.12).

The simplest type of extension is, of course, a direct product $G = H \times N$. A more general case, of great importance in practice, is that where G is a split extension of H , defined as follows:

(1.14) Definition. An extension $\varphi: G \rightarrow H$ is *split* if there exists a homomorphism $\lambda: H \rightarrow G$ such that $\varphi \circ \lambda = \text{id}_H$; such a map λ is sometimes called a *splitting map*.

(1.15) Proposition. An extension $\varphi: G \rightarrow H$ with kernel N is split if and only if there exists a subgroup H_1 of G such that $G = H_1N$ and $H_1 \cap N = 1$.

In case $G = H_1N$ as in (1.15), we call G a *semidirect product* of the normal subgroup N and the subgroup H_1 , and use the notation

$$G = N \rtimes H_1$$

when this occurs.

Thus, semidirect products are the same as split extensions. For example, one of the non-abelian groups of order 8 is a split extension (the dihedral group) while the other is a nonsplit extension (the quaternion group). In both cases, the normal subgroup N and the quotient G/N are the same, but the groups are not isomorphic.

Groups which cannot be analyzed in terms of extensions are the *simple groups*, that is, groups having no proper normal subgroups. These are the basic objects from which other groups are constructed. The classification of finite simple groups has been, for many years, the central problem in finite group theory, and has stimulated much of the current research in character theory.

(1.16) Definition. A *normal series of length s* of a group G is a chain of subgroups

$$G = G_1 \geq G_2 \geq \cdots \geq G_s \geq G_{s+1} = 1,$$

such that $G_{i+1} \trianglelefteq G_i$ for $1 \leq i \leq s$. The *factors* of the normal series are the groups $\{G_i/G_{i+1} : 1 \leq i \leq s\}$. In case the factors are simple and non-trivial, the normal series above is called a *composition series* for G .

(1.17) Jordan-Hölder Theorem. Let G have two composition series

$$G = G_1 \geq \cdots \geq G_{s+1} = 1, \quad G = H_1 \geq \cdots \geq H_{t+1} = 1,$$

of lengths s and t , respectively. Then $s=t$, and there exists a permutation σ of $\{1, \dots, s\}$ such that $G_i/G_{i+1} \cong H_{\sigma(i)}/H_{\sigma(i+1)}$, $1 \leq i \leq s$.

Examples of Normal Series. (i) The *derived series*: The *derived subgroup* G' (or *commutator subgroup*) of a group G is the subgroup generated by all commutators $\{(a, b) = aba^{-1}b^{-1} : a, b \in G\}$. Then G' is the smallest normal subgroup of G such that the quotient group is abelian. The *derived series* of G is the normal series

$$G \geq G^{(1)} \geq G^{(2)} \geq \cdots,$$

where $G^{(i)}$ is the derived subgroup of $G^{(i-1)}$, for each i .

(ii) The *lower central series* of G is

$$G = G_1 \geq G_2 \geq G_3 \geq \cdots,$$

where G_i is the subgroup $[G_{i-1}, G]$ generated by all commutators $\{(x, y) : x \in G_{i-1}, y \in G\}$.

(iii) The *upper central series* of G is

$$1 \leq Z_1 \leq Z_2 \leq \cdots,$$

where Z_1 is the center $Z(G)$ of G , Z_2 is the subgroup of G containing Z_1 such that $Z_2/Z_1 = Z(G/Z_1)$, and so on.

We recall that a group G is *solvable* if some term $G^{(i)}$ in the derived series coincides with the trivial subgroup 1. A group G is *nilpotent* if $G_m = 1$ for some term G_m in the lower central series, or equivalently, if $Z_n = G$ for some term Z_n in the upper central series. A finite group is solvable if and only if it has a composition series whose factors are cyclic of prime order. A finite group G is

supersolvable if G is solvable, and in addition, G has a composition series

$$G \geq G_1 \geq \cdots \geq G_{s+1} = 1$$

in which all of the subgroups $\{G_i\}$ are normal subgroups of G .

We now turn to arithmetical considerations. Let p be a prime. An element x of a finite group G is a *p-element* if the order of x is a power of p , and a *p' -element* (or a *p-regular element*) if the order of x is prime to p . The identity element is the only element of G which is simultaneously a *p-element* and a *p' -element*. The primary decomposition of the cyclic group $\langle x \rangle$ shows that for each prime p , there exists a factorization

$$x = x'x'',$$

with x' a *p' -element* and x'' a *p-element*, and $x'x'' = x''x'$. The factors x' and x'' are called the *p' -part* (or *p-regular part*) of x , and the *p-part* of x , respectively; the elements x' and x'' are uniquely determined by the above properties.

The order of a finite group G is denoted by $|G|$, and the index of a subgroup H by $|G:H|$. A group G whose order is a power of a prime p is called a *p-group*, while a group whose order is not divisible by p is called a *p' -group*. We assume the reader is familiar with the existence and properties of the Sylow *p*-subgroups of a finite group (see CR §6).

A group G is *p-solvable*, for a prime p , if G has a normal series such that each factor is either a *p-group* or a *p' -group*. We have inclusions

$$\{p\text{-groups}\} \subseteq \left\{ \begin{array}{l} \text{nilpotent} \\ \text{groups} \end{array} \right\} \subseteq \left\{ \begin{array}{l} \text{supersolvable} \\ \text{groups} \end{array} \right\} \subseteq \left\{ \begin{array}{l} \text{solvable} \\ \text{groups} \end{array} \right\} \subseteq \left\{ \begin{array}{l} p\text{-solvable} \\ \text{groups} \end{array} \right\},$$

with strict inclusions at each stage.

A group G has a *normal p-complement* if there exists a normal subgroup $H \trianglelefteq G$ such that

$$G = H \times S,$$

for some Sylow *p*-subgroup S of G . A group having a normal *p*-complement is clearly *p*-solvable, but is not necessarily solvable. For Burnside's Theorem on normal *p*-complements, see (13.20) below.

The symmetric groups $\{S_n\}$ and alternating groups $\{A_n\}$ are solvable for $n \leq 4$, and not solvable for $n \geq 5$.

Nilpotent groups are easily shown to have the property that each proper subgroup is properly contained in its normalizer. From this it follows that finite nilpotent groups are direct products of their Sylow subgroups (CR (6.12)).

We next consider groups acting on sets. Using this approach, many problems in group theory can be translated into the more concrete language of permutation groups.

(1.18) Definition. A *G-set* Ω is a pair consisting of a group G , a set Ω , and a map from $G \times \Omega$ to Ω (notation: $(x, w) \rightarrow xw$, $x \in G$, $w \in \Omega$) such that

$$1w = w, \quad x(xy) = (xy)w, \quad x, y \in G, \quad w \in \Omega.$$

The map $G \times \Omega \rightarrow \Omega$ is called the *action* of G on Ω , and we shall say that G *acts* on Ω . Two G -sets Ω and Ω' are *isomorphic* (notation: $\Omega \cong \Omega'$) if there exists a bijection $f: \Omega \rightarrow \Omega'$ such that $f(xw) = xf(w)$ for all $w \in \Omega$, $x \in G$.

Let Ω be a G -set. For each $x \in G$, the *left multiplication* $x_l: \Omega \rightarrow \Omega$ is the map defined by $x_l w = xw$, $w \in \Omega$. These maps have the properties:

$$1_l = \text{id}_\Omega, \quad (xy)_l = x_l y_l, \quad x, y \in G,$$

by the definition of G -sets. It follows that the map defined by $x \rightarrow x_l$, $x \in G$, is a homomorphism from G into the group of permutations of Ω .

Let Ω be a finite G -set, and let R be any commutative ring. Let M be a free R -module with basis $\{m_w : w \in \Omega\}$, where the basis elements are symbols corresponding bijectively to the elements of Ω . Each element $x \in G$ defines an R -linear map $T(x): M \rightarrow M$, where $T(x)m_w = m_{xw}$, for $w \in \Omega$. As in the case of left multiplications, it follows that $T(1) = 1_M$, and $T(xy) = T(x)T(y)$, for $x, y \in G$. Thus we have a homomorphism T from G into the group of R -automorphisms of M .

The maps $x \rightarrow x_l$ and $x \rightarrow T(x)$, associated with a fixed G -set Ω , are called *permutation representations* of G defined by the G -set Ω . For the case where G acts on the *permutation module* M defined above, the trace function,

$$x \rightarrow \text{Tr}(x, M) \in R, \quad x \in G,$$

is called the *permutation character* associated with the G -set Ω .

For each G -set Ω , there is an equivalence relation \sim on Ω , defined by $v \sim w$ if $w = xv$ for some $x \in G$, where $v, w \in \Omega$. The equivalence classes are called the *G-orbits*, or simply *orbits*, of the action of G on Ω . A G -set is called *transitive* if there is only one orbit.

(1.19) Definition. Let Ω be a G -set, and let $w \in \Omega$. The *stabilizer* of w in G (notation: $\text{Stab}_G w$) is defined by

$$\text{Stab}_G w = \{x \in G : xw = w\}.$$

We note that $\text{Stab}_G w$ is a subgroup of G , for each $w \in \Omega$. If H is any subgroup of G , the left cosets $G/H = \{yH : y \in G\}$ form a transitive G -set, with the action of G defined by

$$(x, yH) \rightarrow xyH, \quad x \in G, \quad yH \in G/H.$$

In this case, $H = \text{Stab}_G H$, since $H = \{x \in G : xH = H\}$.

The G -sets of the form G/H are characterized in the following:

(1.20) Proposition. *Let Ω be a G -set. Then the following statements hold:*

(i) *Let Ω be transitive, and let $w, w' \in \Omega$. Set $H = \text{Stab}_G w$ and $H' = \text{Stab}_G w'$. Then $w' = xw$ for some $x \in G$, and $H' = xHx^{-1}$. For each element $w \in \Omega$, there is an isomorphism of G -sets*

$$\Omega \cong G/H, \text{ where } H = \text{Stab}_G w.$$

(ii) *Let Ω be transitive, and assume that both G and Ω are finite. Then $|\Omega| = |G : \text{Stab}_G w|$ for each $w \in \Omega$. In particular, $|\Omega|$ divides $|G|$.*

(iii) *Let Ω be finite, but not necessarily transitive, and let $\{\Omega_i : i \in I\}$ be the G -orbits in Ω . Then we have*

$$|\Omega| = \sum_{i \in I} |\Omega_i|,$$

and

$$|\Omega_i| = |G : \text{Stab}_G w_i|, \text{ for any } w_i \in \Omega_i, i \in I.$$

We now recall some familiar examples of G -sets.

(1.21) Examples. (i) Let $H \leq G$. Then H acts on G by left multiplication $(h, x) \rightarrow hx$, and by right multiplication $(x, h) \rightarrow xh$, for $x \in G$, $h \in H$. The H -orbits are the *right cosets* $\{Hx\}$ in the first case, and the *left cosets* $\{xH\}$ in the second. For example, Hx is the right H -coset containing x , for $x \in G$.

(ii) Let H, K be subgroups of G . Then the direct product $H \times K$ acts on G as follows:

$$((h, k), x) \rightarrow hxk^{-1}, x \in G, h \in H, k \in K.$$

The orbits in this case are the (H, K) -double cosets $\{HxK\}$.

(iii) The group G acts on itself through inner automorphisms:

$$(x, y) \rightarrow xyx^{-1} = i_x(y), x, y \in G,$$

where the map i_x is the *inner automorphism* associated with x . The homomorphism $x \rightarrow i_x$, $x \in G$, maps G onto the group of *inner automorphisms* of G . The kernel of this homomorphism is the *center* of G , and is denoted by $Z(G)$.

Relative to the action by inner automorphisms, the orbits of G are the *conjugacy classes* of G . If \mathfrak{C} is a conjugacy class, and $x \in \mathfrak{C}$, the stabilizer of x in G is the *centralizer* $C_G(x)$ of $x \in G$, and is defined by

$$C_G(x) = \{y \in G : yxy^{-1} = x\}.$$

In case G is finite, the equations in (1.20iii) yield the *class equation*:

$$(1.22) \quad |G| = |Z(G)| + \sum_{C_G(x) < G} |G : C_G(x)|.$$

Here, the center is the union of conjugacy classes containing elements $x \in G$ whose stabilizer $C_G(x) = G$; in the second summation, x ranges over representatives of conjugacy classes containing more than one element. The class equation is used, for example, to prove that the center of a p -group $G \neq 1$ is nontrivial.

(iv) Let $H \leq G$, and let Ω be the set of G -conjugates $\{xHx^{-1} : x \in G\}$ of H . Then Ω is a G -set, with the action of G given by

$$(y, xHx^{-1}) \rightarrow yxHx^{-1}y^{-1}, x, y \in G.$$

In other words, G acts on Ω through inner automorphisms. We have $\text{Stab}_G H = \{x \in G : xHx^{-1} = H\}$. This subgroup is called the *normalizer* $N_G(H)$ of H , and is the largest subgroup E of G for which $H \trianglelefteq E$. By (1.20ii), the number of distinct conjugates of a subgroup H is the index $|G : N_G(H)|$.

Proofs of the Sylow Theorems using these ideas are given in CR §6.

Our third topic is the definition of a group by generators and relations.

(1.23) Definition. Let G be a group, and let $\{a_1, \dots, a_n\}$ be elements of G , and $\{w_1, \dots, w_t\}$ a set of products of the elements a_i and their inverses (possibly with repetitions). Then G has a *presentation*

$$G = \langle a_1, \dots, a_n : w_1 = \dots = w_t = 1 \rangle,$$

provided that the following conditions are satisfied:

(i) $G = \langle a_1, \dots, a_n \rangle$, (that is, G is generated by the elements a_1, \dots, a_n), and the relations $w_1 = 1, \dots, w_t = 1$ all hold.

(ii) If G' is another group containing elements a'_1, \dots, a'_n such that $w'_1 = \dots = w'_t = 1$ in G' , where the $\{w'_i\}$ are the expressions in G' corresponding to the $\{w_i\}$ in G , then there exists a unique homomorphism $\varphi: G \rightarrow G'$ such that $\varphi(a_i) = a'_i$, $1 \leq i \leq n$.

It follows easily from the definition that two groups with the same presentation are isomorphic. It is also not difficult to show, using the theory of free

groups, that given any expressions $\{w_1, \dots, w_t\}$ in the symbols $\{a_1, \dots, a_n\}$, there exists a group G having the presentation

$$G = \langle a_1, \dots, a_n : w_1 = \dots = w_t = 1 \rangle.$$

Of course, there is no guarantee that the group G is non-trivial.

(1.24) Examples. (i) *The dihedral groups.* For each n , the dihedral group D_n of order $2n$ has a presentation

$$D_n = \langle a, b : a^n = 1, b^2 = 1, (ab)^2 = 1 \rangle.$$

(ii) *The generalized quaternion groups.* For each positive integer m , there exists a finite group Q_m of order $4m$, having the presentation

$$Q_m = \langle a, b : a^{2m} = 1, b^2 = a^m, bab^{-1} = a^{-1} \rangle.$$

For $m=2$, we have a presentation of the *quaternion group* Q of order 8. We call Q_m a *generalized quaternion group*.

In Chapter 7, we shall discuss presentations of Coxeter groups, which include the symmetric groups and hyper-octahedral groups.

§1. Exercises

1. Let A be a f.d. K -algebra, where K is a field, and let $\alpha \in A$. Show that there exists an element $\beta \in K[\alpha]$ such that

$$\alpha\beta = \beta\alpha = N_{A/K}(\alpha).$$

[Hint: Use the fact that α is a zero of its characteristic polynomial.]

2. Keep the above notation, and let R be an integrally closed domain with quotient field K . Show that if $\alpha \in A$ is integral over R , then there exists an element $\beta \in R[\alpha]$ such that $\alpha\beta = \beta\alpha = N_{A/K}(\alpha)$, and β is also integral over R .

[Hint: Use (1.9).]

§2. THE FUNCTORS HOM AND \otimes . PROJECTIVE, INJECTIVE, AND FLAT MODULES

This section contains a review of basic concepts from homological algebra. Later (§8) we shall survey some more advanced topics, including the functors Ext and Tor, and the cohomology of finite groups. Proofs will be omitted in most cases, and are often easy exercises for the reader who may be unfamiliar with them. For the theory of tensor products, we shall assume knowledge of



the material in CR §12. A list of references on Homological Algebra is given at the end of this section, just before the Exercises.

Throughout this book, all rings are assumed to have identity elements, which act as identity operators on all modules over the rings. We abbreviate “finitely generated” as “f.g.”, and write “ M is f.g./ A ” to indicate that M is a finitely generated module over the ring A .

§2A. Homomorphisms

Let A be a ring (associative, but not necessarily commutative), and let M, N be left A -modules. We denote by $\text{Hom}_A(M, N)$ the additive group consisting of all A -homomorphisms from M into N . For $f \in \text{Hom}_A(M, N)$, let

$$(2.1) \quad \begin{cases} \ker f = \text{kernel of } f = \{m \in M : f(m) = 0\}, \\ \text{im } f = \text{image of } f = f(M) = \{f(m) : m \in M\}, \\ \text{cok } f = \text{cokernel of } f = N/f(M). \end{cases}$$

A sequence of A -modules and A -homomorphisms

$$M_1 \xrightarrow{f_1} M_2 \xrightarrow{f_2} M_3 \rightarrow \cdots \xrightarrow{f_{n-1}} M_n$$

is *exact* at M_i if $\ker f_i = \text{im } f_{i-1}$. The sequence is *exact* if it is exact at each M_i , that is, $\ker f_i = \text{im } f_{i-1}$ for $2 \leq i \leq n-1$.

A *short exact sequence* (abbreviated hereafter as “ses”) is an exact sequence of the form

$$(2.2) \quad 0 \rightarrow L \xrightarrow{f} M \xrightarrow{g} N \rightarrow 0.$$

Exactness of this sequence is equivalent to the following three conditions:

$$f \text{ is injective, } \text{im } f = \ker g, \text{ } g \text{ is surjective.}$$

In this case, g induces an A -isomorphism $M/f(L) \cong N$.

We call the ses (2.2) *split* if $f(L)$ is a direct summand of M . Let id_L (or 1_L) denote the identity map on the module L . We state without proof (see references):

(2.3) Proposition. *Given a short exact sequence (2.2), the following conditions are equivalent:*

(i) *The sequence is split.*

(ii) *There exists an $h \in \text{Hom}_A(M, L)$ such that hf is an automorphism of L .*

(iii) There exists an $h' \in \text{Hom}_A(N, M)$ such that gh' is an automorphism of N .

A diagram of A -modules and A -homomorphisms

$$\begin{array}{ccc} L_1 & \xrightarrow{f_1} & L_2 \\ g_1 \downarrow & & \downarrow f_2 \\ M_1 & \xrightarrow{g_2} & M_2 \end{array}$$

is *commutative* if $f_2 f_1 = g_2 g_1$. Likewise, the diagram

$$\begin{array}{ccc} L & \xrightarrow{f} & M \\ & \searrow h & \downarrow g \\ & & N \end{array}$$

is *commutative* if $gf = h$.

Before listing some standard properties of Hom, let us briefly discuss the concept of a bimodule. Let A and B be rings; an (A, B) -bimodule ${}_A M_B$ is an additive group M which is simultaneously a left A -module and a right B -module, such that

$$a(mb) = (am)b, \quad a \in A, m \in M, b \in B.$$

We sometimes say that “the action of A on M commutes with the action of B on M ”. It is easy to give examples of bimodules: every ring A is automatically an (A, A) -bimodule ${}_A A_A$. Further, every left A -module M may be viewed as a right Z -module, and then M is an (A, Z) -bimodule. Finally, if A is a commutative ring and M is a left A -module, we may let A act on the right on M by defining $m \cdot a = am$, $a \in A$, $m \in M$; then M becomes a bimodule ${}_A M_A$. Trivial though it may be, this last observation has many useful consequences, as we shall see later.

Now let $f \in \text{Hom}_A(M, N)$, where M, N are left A -modules. For each left A -module X , the homomorphism f induces an additive homomorphism

$$(2.4) \quad f^* : \text{Hom}_A(N, X) \rightarrow \text{Hom}_A(M, X),$$

defined by

$$f^* \alpha = \alpha f, \quad \alpha \in \text{Hom}_A(N, X).$$

This definition may be understood more clearly in terms of diagrams: the

map f^* is defined by the condition that for each α , the diagram

$$\begin{array}{ccc} M & \xrightarrow{f} & N \\ & \searrow f^*\alpha & \downarrow \alpha \\ & & X \end{array}$$

is commutative.

We may observe that the map f^* goes “in the opposite direction” from f , that is, f maps M into N whereas f^* maps $\text{Hom}(N, X)$ into $\text{Hom}(M, X)$. Since f^* arises from a change in the first variable in Hom , we call Hom *contravariant* in the first variable. It is easily verified that

$$(gf)^* = f^*g^*, \text{ for all } f \in \text{Hom}_A(M, N), g \in \text{Hom}_A(N, N').$$

Thus, contravariance reverses the order of composition of homomorphisms!

Let us once more start with an $f \in \text{Hom}_A(M, N)$ and an A -module X ; then f induces an additive homomorphism

$$(2.5) \quad f_* : \text{Hom}_A(X, M) \rightarrow \text{Hom}_A(X, N),$$

defined by

$$f_*\alpha = f\alpha, \alpha \in \text{Hom}_A(X, M).$$

In terms of diagrams, f_* is defined by the condition that the diagram

$$\begin{array}{ccc} X & \xrightarrow{f_*\alpha} & M \\ \downarrow \alpha & \nearrow f & \rightarrow N \end{array}$$

commutes for each α .

We observe that the map f_* goes “in the same direction” as f , since f maps M into N whereas f_* maps $\text{Hom}(X, M)$ into $\text{Hom}(X, N)$. Since f_* arises from a change in the second variable in Hom , we say that Hom is *covariant* in the second variable. One easily checks that

$$(gf)_* = g_*f_* \text{ for all } f \in \text{Hom}_A(M, N), g \in \text{Hom}_A(N, N').$$

Thus, covariance preserves the order of composition of homomorphisms.

The concepts of covariance and contravariance are extremely important in dealing with modules. For example, let A and B be rings, and let us start with

the data

$${}_A L = \text{left } A\text{-module}, {}_A M_B = (A, B)\text{-bimodule}.$$

As we shall see, the additive group $\text{Hom}_A(L, M)$ can be given the structure of a B -module, because of the bimodule structure of M . Indeed, since M is a *right* B -module occurring in a *covariant* position, it will automatically turn out that $\text{Hom}_A(L, M)$ will be a *right* B -module. Let us proceed to describe this construction explicitly: for each $b \in B$, let $b' \in \text{Hom}_A(M, M)$ be the map defined by

$$b'(m) = mb, m \in M.$$

Clearly $(bc)' = c'b'$ for $b, c \in B$. As in (2.5), there is an induced additive homomorphism

$$(b')_* : \text{Hom}_A(L, M) \rightarrow \text{Hom}_A(L, M),$$

given by $(b')_* \alpha = b'\alpha$, $\alpha \in \text{Hom}_A(L, M)$. We now *define* the action of B on $\text{Hom}_A(L, M)$ by setting

$$\alpha \cdot b = (b')_* \alpha, b \in B, \alpha \in \text{Hom}_A(L, M).$$

Then for $c \in B$ we have

$$\begin{aligned} \alpha \cdot (bc) &= \{(bc)'\}_* \alpha = \{c'b'\}_* \alpha = \{(c')_*(b')_*\} \alpha \\ &= (c')_* \{\alpha \cdot b\} = \{\alpha \cdot b\} \cdot c \end{aligned}$$

for each α . Hence $\text{Hom}_A(L, M)$ is a *right* B -module, as claimed. To be explicit, we have

$$(\alpha \cdot b)x = (b')_* \alpha x = b'(\alpha x) = (\alpha x)b, x \in L,$$

for all $b \in B$, $\alpha \in \text{Hom}_A(L, M)$. We could have predicted the final formula $(\alpha b)x = (\alpha x)b$ in advance, since it must arise from the fact that M is a *right* B -module, so b must act from the right on some element of M .

Analogously, starting with the same data as above, we may make $\text{Hom}_A(M, L)$ into a *left* B -module, since M is a *right* B -module occurring in a *contravariant* position. Indeed, for each $b \in B$ the above-defined b' induces a map

$$(b')^* : \text{Hom}_A(M, L) \rightarrow \text{Hom}_A(M, L)$$

by setting $(b')^*\beta = \beta b'$, $\beta \in \text{Hom}_A(M, L)$. We now *define* the action of B on

$\text{Hom}_A(M, L)$ by the formula

$$b \cdot \beta = (b')^* \beta, \quad b \in B, \beta \in \text{Hom}_A(M, L).$$

Then for $b, c \in B$ we have

$$\begin{aligned} (bc) \cdot \beta &= \{(bc)'^*\} \beta = \{c'b'\}^* \beta = (b')^*(c')^* \beta \\ &= b \cdot \{c \cdot \beta\} \end{aligned}$$

for all β , as desired. Explicitly, we obtain

$$(b\beta)m = \beta(mb), \quad b \in B, m \in M, \beta \in \text{Hom}_A(M, L).$$

As an example of the above, let M be a left A -module and view A as an (A, A) -bimodule. We may form the group $\text{Hom}_A(A, {}_A M)$ of left A -homomorphisms from A into M . By the preceding paragraph, this group $\text{Hom}_A(A, M)$ is then automatically a left A -module, according to the formula

$$(af)x = f(xa), \quad a \in A, x \in {}_A A, f \in \text{Hom}_A(A, M).$$

It is easily verified that there is an isomorphism

$$(2.6) \quad \text{Hom}_A(A, M) \cong M$$

as left A -modules; the isomorphism is given by $f \mapsto f(1)$, for $f \in \text{Hom}_A(A, M)$.

We may also remark that the isomorphism in (2.6) is *natural*, in the following sense: if θ_M denotes this isomorphism, then for every pair of left A -modules M and N , and for every $h \in \text{Hom}_A(M, N)$, the diagram

$$\begin{array}{ccc} \text{Hom}_A(A, M) & \xrightarrow{\theta_M} & M \\ h_* \downarrow & & \downarrow h \\ \text{Hom}_A(A, N) & \xrightarrow{\theta_N} & N \end{array}$$

is commutative.

As a second illustration of the above type of reasoning, suppose for the moment that the ring A is commutative. Every one-sided A -module can then be viewed as (A, A) -bimodule, with elements of A acting the same on the left as on the right. Hence in this case, for A -modules L and M , the additive group $\text{Hom}_A(L, M)$ automatically acquires the structure of A -module. In the same way, the tensor product $L \otimes_A M$ may be viewed as A -module.

Given a pair M_1 and M_2 of left A -modules, where A is an arbitrary ring, we define their *external direct sum* as

$$M_1 \dot{+} M_2 = \{(m_1, m_2) : m_1 \in M_1, m_2 \in M_2\},$$

where these pairs are added componentwise, and where

$$a(m_1, m_2) = (am_1, am_2) \text{ for all } a \in A, m_1 \in M_1, m_2 \in M_2.$$

More generally, let $\{M_i : i \in I\}$ be a possibly infinite family of left A -modules. Let M be the set of all I -tuples $(m_i : i \in I)$ with $m_i \in M_i$ for each $i \in I$, such that $m_i = 0$ a.e. (Here, “a.e.” means “almost everywhere,” that is, for all but a finite number of values of the index i .) We make M into a left A -module by using componentwise addition of I -tuples, and by setting

$$a(m_i) = (am_i) \text{ for } a \in A, m_i \in M.$$

Call M the *external direct sum* of the family $\{M_i : i \in I\}$; we denote M by either $\dot{\bigoplus}_{i \in I} M_i$ or $\coprod_{i \in I} M_i$ (see below).*

On the other hand, let N be a left A -module, and let N_1 and N_2 be a pair of submodules of N such that each $n \in N$ is uniquely expressible as a sum $n = n_1 + n_2$, $n_i \in N_i$. We call N the (*internal*) *direct sum* of the submodules N_1 and N_2 , and write $N = N_1 \oplus N_2$. We note that if $N = N_1 + N_2$, then the sum is direct if and only if $N_1 \cap N_2 = 0$. Likewise, we write $N = \bigoplus_{i \in I} N_i$ as an *internal direct sum* of a family $\{N_i : i \in I\}$ of submodules, if each $n \in N$ is uniquely expressible as a sum $n = \sum n_i$, with $n_i \in N_i$ and $n_i = 0$ a.e.

There is an obvious connection between the two concepts. Consider an external direct sum* $M = \coprod_{i \in I} M_i$; for each $i_0 \in I$ and each $m_{i_0} \in M_{i_0}$, we may form the I -tuple $\langle m_{i_0} \rangle$ which has entry m_{i_0} at the i_0 -th place, and zeros elsewhere. Let N_{i_0} be defined as $\{\langle m_{i_0} \rangle : m_{i_0} \in M_{i_0}\}$. Clearly we have $N_{i_0} \cong M_{i_0}$ for each i_0 , and M is the direct sum of the family $\{N_{i_0} : i_0 \in I\}$ of submodules of M . Conversely, given any internal direct sum $\bigoplus_{i \in I} N_i$ of submodules $\{N_i\}$ of N , we have

$$\bigoplus_{i \in I} N_i \cong \coprod_{i \in I} N_i.$$

It is sometimes vital to be able to distinguish between internal direct sums and external direct sums. For example, $\coprod_{i=1}^n A$ would denote the A -module consisting of all n -tuples from A (often denoted by $A^{(n)}$), whereas the sum $A + \cdots + A$ formed within A is *not* a direct sum if $n > 1$. This situation occurs in §4, when we are studying R -lattices with R a Dedekind ring. Every

*The direct sum symbol \coprod is the inverted version of the product symbol \prod . Direct products of modules rarely occur in this book.

R -lattice is (up to isomorphism) an external direct sum $\coprod_{i=1}^n \alpha_i$, with each α_i a nonzero ideal of R . However, if $n > 1$ this sum is *not* isomorphic to the internal sum $\sum_{i=1}^n \alpha_i$ of ideals of the ring R , and indeed the sum cannot be direct.

Associated with an internal direct sum $M = \bigoplus_{i \in I} M_i$ we have a family of *projection maps* $\{\pi_i : i \in I\}$, defined by

$$\pi_i \left(\sum_{j \in I} m_j \right) = m_i, \quad i \in I.$$

Each $\pi_i \in \text{End}_A(M)$, and we have for all $m \in M$,

$$m = \sum_{i \in I} \pi_i(m), \quad \pi_i(m) = 0 \text{ a.e.}$$

Further,

$$\pi_i^2 = \pi_i \text{ for } i \in I, \quad \pi_i \pi_j = 0 \text{ for } i \neq j, \quad 1 = \sum_{i \in I} \pi_i.$$

If $M_i \neq 0$, then $\pi_i \neq 0$. We also call the $\{\pi_i\}$ a set of *orthogonal idempotents* associated with the direct sum decomposition of M . Here, “orthogonal” refers to the property that $\pi_i \pi_j = 0$ for $i \neq j$, while “idempotent” means that $\pi_i^2 = \pi_i \neq 0$ for each i . Conversely, given a set of orthogonal idempotents $\{\pi_i : i \in I\}$ in $\text{End}_A(M)$, such that for each m ,

$$1 = \sum_{i \in I} \pi_i, \quad \text{and } \pi_i(m) = 0 \text{ a.e.,}$$

we obtain an (internal) direct sum decomposition

$$M = \bigoplus_{i \in I} M_i, \quad \text{where } M_i = \pi_i(M) \text{ for each } i \in I.$$

External direct sums $M = \coprod M_i$ give rise to projection maps $\pi_i : M \rightarrow M_i$, but π_i does not act on M_i , and it is only after we rewrite M as an internal direct sum $M = \bigoplus N_i$, $N_i \cong M_i$, that we can apply the preceding remarks.

Returning now to our study of Hom, we remark first that there are obvious isomorphisms of additive groups

$$(2.7) \quad \begin{cases} \text{Hom}_A(M \oplus M', L) \cong \text{Hom}_A(M, L) \oplus \text{Hom}_A(M', L), \\ \text{Hom}_A(L, M \oplus M') \cong \text{Hom}_A(L, M) \oplus \text{Hom}_A(L, M'), \end{cases}$$

for every left A -module L .

Somewhat less obvious is the following property of Hom:

(2.8) Proposition. (i) *For each A-module X and each A-exact sequence*

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

the sequence of additive groups

$$0 \rightarrow \text{Hom}_A(X, L) \xrightarrow{f_*} \text{Hom}_A(X, M) \xrightarrow{g_*} \text{Hom}_A(X, N)$$

is also exact.

(ii) *For each A-module Y and each A-exact sequence*

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

there is an exact sequence of additive groups

$$0 \rightarrow \text{Hom}_A(N, Y) \xrightarrow{g_*} \text{Hom}_A(M, Y) \xrightarrow{f_*} \text{Hom}_A(L, Y).$$

For proofs, see references listed at the end of §2. We may remark that these exact sequences of Hom's can be extended to the right, by introducing the groups Ext defined in §8.

To conclude this subsection, let us introduce the concepts of pushouts and pullbacks of a pair of maps. Given a pair of left A-homomorphisms $f_i: T \rightarrow M_i$, $i=1, 2$, we define a left A-module X , called the *pushout* of the pair $\{f_1, f_2\}$, by the formula

$$X = (M_1 + M_2) / \{(f_1 t, -f_2 t) : t \in T\}.$$

Thus the module X is obtained from the external direct sum $M_1 + M_2$ by identifying the image of T in M_1 with the image of T in M_2 . There is a commutative *pushout diagram*

$$(2.9) \quad \begin{array}{ccc} T & \xrightarrow{f_1} & M_1 \\ f_2 \downarrow & & \downarrow g_1 \\ M_2 & \xrightarrow{g_2} & X \end{array}$$

where g_i is given by composition of maps: $M_i \rightarrow M_1 + M_2 \rightarrow X$, $i=1, 2$.

Analogously, given a pair of A -homomorphisms $f_i: M_i \rightarrow U$, $i=1, 2$, we can form their *pullback* (or *fibre product*)

$$Y = \{(m_1, m_2) \in M_1 \times M_2 : f_1 m_1 = f_2 m_2\}.$$

Then there is a commutative *pullback diagram*

$$(2.10) \quad \begin{array}{ccc} Y & \xrightarrow{g_1} & M_1 \\ g_2 \downarrow & & \downarrow f_1 \\ M_2 & \xrightarrow{f_2} & U \end{array}$$

where $g_i(m_1, m_2) = m_i$, $i=1, 2$.

The concept of fibre products of rings is equally important. First let us recall the definition of the *external direct product* $A \times B$ of a pair of rings A and B . This product consists of all ordered pairs (a, b) , $a \in A$, $b \in B$, added and multiplied componentwise. Clearly $A \times B$ is a ring, and there are canonical ring homomorphisms

$$A \rightarrow A \times B, \quad A \times B \rightarrow A,$$

given by $a \mapsto (a, 1)$, $a \in A$, and $(a, b) \mapsto a$, $(a, b) \in A \times B$, respectively. The first of these maps is an injection, the second a surjection. This same construction may be used for any collection of rings $\{A_i : i \in I\}$, where the index set I may possibly be infinite.

Now let A_1 , A_2 and \bar{A} be rings, and let $f_i: A_i \rightarrow \bar{A}$, $i=1, 2$, be a pair of ring homomorphisms. (We assume always that ring homomorphisms map identity elements onto identity elements). We now define the *fibre product* of the pair $\{f_1, f_2\}$ as

$$(2.11) \quad A = \{(a_1, a_2) : a_i \in A_i, f_1 a_1 = f_2 a_2\}.$$

Then A is a ring, and there is a commutative diagram

$$\begin{array}{ccc} A & \xrightarrow{g_1} & A_1 \\ g_2 \downarrow & & \downarrow f_1 \\ A_2 & \xrightarrow{f_2} & \bar{A} \end{array}$$

where $g_i(a_1, a_2) = a_i$, $i=1, 2$.

Two examples of fibre products of rings arise often. First, let I and J be two-sided ideals of an arbitrary ring A . Then there is a fibre product diagram

$$(2.12) \quad \begin{array}{ccc} \frac{A}{I \cap J} & \longrightarrow & \frac{A}{I} \\ \downarrow & & \downarrow f_1 \\ \frac{A}{J} & \xrightarrow{f_2} & \frac{A}{I+J} \end{array}$$

where all of the arrows represent canonical ring surjections. (We leave it to the reader to verify that $A/I \cap J$ is isomorphic to the fibre product of the pair $\{f_1, f_2\}$.)

Secondly, suppose that there is an inclusion of rings $A \subseteq B$, and that I is a two-sided ideal of B contained in A . Then there is a fibre product diagram

$$(2.13) \quad \begin{array}{ccc} A & \longrightarrow & B \\ \downarrow & & \downarrow f_1 \\ \frac{A}{I} & \xrightarrow{f_2} & \frac{B}{I} \end{array}$$

in which f_1 is surjective, but f_2 usually not.

§2B. Tensor Products

Throughout this section let A and B be rings. We shall write ${}_A M$ to indicate that M is a left A -module; likewise L_A denotes a right A -module, and ${}_A N_B$ a left A -, right B -bimodule. Let us recall the definition of the tensor product $L \otimes_A M$ of L_A and ${}_A M$. Denote by F the free abelian group generated by all ordered pairs from the Cartesian product $L \times M$, and let F_0 be the subgroup of F generated by all expressions

$$\left\{ \begin{array}{l} (l_1 + l_2, m) - (l_1, m) - (l_2, m), \\ (l, m_1 + m_2) - (l, m_1) - (l, m_2), \\ (l, am) - (la, m), \end{array} \right.$$

for all $l_i \in L$, $m_i \in M$, $a \in A$. We set $L \otimes_A M = F/F_0$, an additive abelian group. Every element of $L \otimes_A M$ is expressible as a finite sum $\sum l_i \otimes m_i$, though not uniquely so.

In what follows, we shall often be discussing additive homomorphisms $f' : L \otimes_A M \rightarrow G$, where G is an abelian additive group. Obviously the map f' is completely determined once the images $\{f'(l \otimes m) : l \in L, m \in M\}$ are known.

The difficulty in constructing such homomorphisms f' lies in proving that a proposed mapping is well defined. In order to overcome this difficulty, we shall need the characterization of $L \otimes_A M$ in terms of a universal mapping property, as described below.

Given a pair of modules L_A and $_A M$, and an abelian group G , consider a map $f: L \times M \rightarrow G$. Call f a *balanced map* if

$$\begin{cases} f(l_1 + l_2, m) = f(l_1, m) + f(l_2, m), \\ f(l, m_1 + m_2) = f(l, m_1) + f(l, m_2), \\ f(l, am) = f(la, m) \end{cases}$$

for all $l_i \in L$, $m_i \in M$, $a \in A$. The following result is shown in CR §12:

(2.14) Proposition. *Each balanced map $f: L \times M \rightarrow G$, where G is an abelian group and L_A , $_A M$ are modules, determines a unique additive homomorphism $f': L \otimes_A M \rightarrow G$ such that*

$$f'(l \otimes m) = f(l, m) \text{ for all } l \in L, m \in M.$$

As an application of this result, let us show that $L \otimes_A M$ is covariant in each variable, that is, given $f \in \text{Hom}_A(L, L_1)$ and $g \in \text{Hom}_A(M, M_1)$, there exists an additive homomorphism

$$(2.15) \quad f \otimes g: L \otimes M \rightarrow L_1 \otimes M_1.$$

(Here, the L 's are right A -modules, the M 's are left A -modules, and we write \otimes instead of \otimes_A for convenience.) Consider the map

$$\psi: L \times M \rightarrow L_1 \otimes M_1$$

defined by

$$\psi(l, m) = f(l) \otimes g(m), \quad l \in L, m \in M.$$

It is easily verified that ψ is a balanced map. Therefore by (2.14), ψ determines an additive homomorphism $\psi': L \otimes M \rightarrow L_1 \otimes M_1$ such that $\psi'(l \otimes m) = f(l) \otimes g(m)$, $l \in L$, $m \in M$. Denoting ψ' by $f \otimes g$, we have obtained the desired homomorphism (2.15), with

$$(f \otimes g)(l \otimes m) = f(l) \otimes g(m), \quad l \in L, m \in M.$$

Since we know that $f \otimes g$ is well defined, we also have

$$(f \otimes g)\{\sum l_i \otimes m_i\} = \sum f(l_i) \otimes g(m_i)$$

for every finite sum $\sum l_i \otimes m_i$, $l_i \in L$, $m_i \in M$. However, it would not have been

permissible to just define $f \otimes g$ by this last formula, since we would then have had to prove that if $\sum l_i \otimes m_i = \sum l'_j \otimes m'_j$ in $L \otimes M$, then $\sum f(l_i) \otimes g(m_i) = \sum f(l'_j) \otimes g(m'_j)$. The use of (2.14) avoids this difficulty.

Suppose next that ${}_B L_A$ is a bimodule, and ${}_A M$ a module. Then $L \otimes_A M$ may be made into a left B -module, since L is a left B -module occurring in a covariant position. Specifically, we have

$$b(l \otimes m) = bl \otimes m, \quad b \in B, \quad l \in L, \quad m \in M.$$

We omit the obvious argument that this formula gives a well defined action of B on the additive group $L \otimes_A M$, and that $L \otimes_A M$ becomes a left B -module.

In particular, the ring A is itself an (A, A) -bimodule. Hence for each left A -module M , there is a left A -module structure on $A \otimes M$, given by the formula

$$a(x \otimes m) = ax \otimes m, \quad a \in A, \quad x \in {}_A A_A, \quad m \in M.$$

As is well known (see CR §12), there is a natural isomorphism of left A -modules:

$$(2.16) \quad A \otimes M \cong M,$$

determined by the map $a \otimes m \rightarrow am$, $a \in A$, $m \in M$. [To be precise, the balanced map $\psi: A \times M \rightarrow M$ given by $\psi(a, m) = am$, determines an additive homomorphism $\psi': A \otimes M \rightarrow M$ such that $\psi'(a \otimes m) = am$. Then ψ' is a left A -isomorphism.]

We list without proof a pair of isomorphism formulas:

$$\begin{cases} (L \oplus L') \otimes M \cong (L \otimes M) \oplus (L' \otimes M), \\ L \otimes (M \oplus M') \cong (L \otimes M) \oplus (L \otimes M'). \end{cases}$$

In fact, a stronger result holds true: given any family $\{L_\alpha\}$ of right A -modules, and any left A -module M , there is a natural isomorphism of additive groups:

$$(2.17) \quad (\coprod L_\alpha) \otimes_A M \cong \coprod_\alpha (L_\alpha \otimes_A M).$$

A corresponding result holds for expressions of the type $L \otimes \coprod M_\beta$.

The following basic result is easily proved (see CR §12):

(2.18) Proposition (*Associativity of tensor products*). *Given rings A and B , and the data L_A , ${}_A M_B$, ${}_B N$, there is a natural isomorphism of additive groups*

$$(L \otimes_A M) \otimes_B N \cong L \otimes_A (M \otimes_B N),$$

determined by the formula $(l \otimes m) \otimes n \rightarrow l \otimes (m \otimes n)$ for all $l \in L$, $m \in M$, $n \in N$.

This proposition will play a basic role in our later discussion of induced representations of groups, since it implies at once that the induction map is transitive (see (10.6)). Equally important will be the following “adjointness” formula connecting Hom and \otimes , since it will imply the Frobenius reciprocity law for group representations (see (10.8)).

(2.19) Adjointness Theorem. *Given rings A and B , and the data $_A L$, ${}_B M_A$, ${}_B N$, there is a natural isomorphism*

$$\tau : \text{Hom}_A(L, \text{Hom}_B(M, N)) \cong \text{Hom}_B(M \otimes_A L, N)$$

of additive groups, given by the formula

$$(\tau f)(m \otimes l) = f_l(m), \quad m \in M, l \in L,$$

where f ranges over all elements of $\text{Hom}_B(M, N)$, and f_l denotes the image of l under the map f .

Sketch of Proof. First verify that $\text{Hom}_B(M, N)$ is a left A -module, and that $M \otimes_A L$ is a left B -module. Then check that τf is well defined. Finally, show that τ has an inverse λ defined as follows: for each $g \in \text{Hom}_B(M \otimes_A L, N)$, let

$$\{(\lambda g)_l\} m = g(m \otimes l), \quad m \in M, l \in L.$$

Here, $(\lambda g)_l$ denotes the image of l under the map λg .

[For those familiar with category theory, we may remark that the preceding result asserts that the functor $M \otimes_A \cdot$ is left adjoint to $\text{Hom}_B(M, \cdot)$. The first of these functors carries left A -modules to left B -modules, while the second functor does the opposite.]

To conclude this subsection, let us state the analogue of (2.8) for tensor products; for proofs, see Rotman [79], or do as exercise.

(2.20) Proposition. (i) *Given an exact sequence of left A -modules $L \xrightarrow{f} M \xrightarrow{g} N \rightarrow 0$, and given any right A -module X , the sequence of additive groups*

$$X \otimes_A L \xrightarrow{1 \otimes f} X \otimes_A M \xrightarrow{1 \otimes g} X \otimes_A N \rightarrow 0$$

is exact.

(ii) Given an exact sequence of right A -modules $U \rightarrow V \rightarrow W \rightarrow 0$, and given any left A -module L , the sequence

$$U \otimes_A L \rightarrow V \otimes_A L \rightarrow W \otimes_A L \rightarrow 0$$

is an exact sequence of additive groups.

§2C. Categories and Functors

We shall introduce here some ideas and terminology from category theory, since the language of category theory provides a clarifying and unifying approach to the ideas introduced earlier in this section, as well as to other areas of mathematics. For simplicity, we shall deal only with categories of modules over a ring, and subcategories thereof. For a ring A , denote by \mathcal{M}_A the *category* of right A -modules; the *objects* of \mathcal{M}_A are right A -modules. For each pair of objects $M, N \in \mathcal{M}_A$, there is a set of *morphisms* (or *maps*) from M to N , namely $\text{Hom}_A(M, N)$. In the same way, we can speak of the category ${}_A\mathcal{M}$ of left A -modules, the category ${}_A\mathcal{M}_B$ of A, B -bimodules, or the category $\mathcal{C}\mathcal{B}$ of abelian groups.

Now let \mathcal{Q} be a category with objects A, A' , etc., and \mathcal{B} a category with objects B, B' , etc. A *covariant functor* $F: \mathcal{Q} \rightarrow \mathcal{B}$ assigns to each object $A \in \mathcal{Q}$ an object $FA \in \mathcal{B}$, and carries each $\alpha \in \text{Hom}_{\mathcal{Q}}(A, A')$ onto a map $F\alpha \in \text{Hom}_{\mathcal{B}}(FA, FA')$, in such a way as to preserve identity maps and compositions of maps. We assume always that the functor is *additive*, that is, $F(\alpha + \alpha') = F\alpha + F\alpha'$.

For example, let $X \in {}_A\mathcal{M}$ be fixed, and define a functor $F: {}_A\mathcal{M} \rightarrow \mathcal{C}\mathcal{B}$ by setting $FM = \text{Hom}_A(X, M)$ for each left A -module M . We must also describe the action of F on maps. For each $\alpha \in \text{Hom}_A(M, N)$, let $F\alpha: FM \rightarrow FN$ be the map denoted by α_* (see (2.5)). It is easily checked that F is a covariant functor; it is often denoted symbolically by $\text{Hom}_A(X, *)$ or $\text{Hom}_A(X, \cdot)$.

As another example of a covariant functor, let $X \in {}_A\mathcal{M}$ be fixed, and define $G: \mathcal{M}_A \rightarrow \mathcal{C}\mathcal{B}$ by setting $GM = M \otimes_A X$ for each right A -module M . The action of G on maps is easily defined; namely, for each $\alpha \in \text{Hom}_A(M, N)$ we set $G\alpha: GM \rightarrow GN$, where $G\alpha = \alpha \otimes 1$. We denote G symbolically by $* \otimes_A X$.

It is also necessary to consider *contravariant functors* $F: \mathcal{Q} \rightarrow \mathcal{B}$. Such an F assigns to each $A \in \mathcal{Q}$ an object $FA \in \mathcal{B}$, and carries each $\alpha \in \text{Hom}_{\mathcal{Q}}(A, A')$ onto a map $F\alpha \in \text{Hom}_{\mathcal{B}}(FA', FA)$, in such a way as to preserve identity maps, but reversing compositions (that is, $F(\alpha\beta) = F(\beta)F(\alpha)$ for maps α, β). As usual, we assume always that F is additive. As an example of a contravariant functor $F: {}_A\mathcal{M} \rightarrow \mathcal{C}\mathcal{B}$, we cite the following: fix a module $X \in {}_A\mathcal{M}$, and for each left A -module M let $FM = \text{Hom}_A(M, X)$. To each $\alpha \in \text{Hom}_A(M, N)$ we let correspond the map $F\alpha \in \text{Hom}_A(FN, FM)$, where $F\alpha$ is the map α^* defined as in (2.4). Then F is a contravariant functor, usually denoted by $\text{Hom}_A(*, X)$.

A covariant functor $F: \mathcal{Q} \rightarrow \mathcal{B}$ is called *right exact* if for each exact sequence $A_1 \rightarrow A_2 \rightarrow A_3 \rightarrow 0$ in \mathcal{Q} , the sequence $FA_1 \rightarrow FA_2 \rightarrow FA_3 \rightarrow 0$ is exact in \mathcal{B} . Proposition 2.20 is just the assertion that the functors $X \otimes_A *$ and $* \otimes_A L$ are right exact. Analogously, a contravariant functor $G: \mathcal{Q} \rightarrow \mathcal{B}$ is *right exact* if the exactness of $0 \rightarrow A_1 \rightarrow A_2 \rightarrow A_3$ implies that of $GA_3 \rightarrow GA_2 \rightarrow GA_1 \rightarrow 0$.

On the other hand, the covariant functor $F: \mathcal{Q} \rightarrow \mathcal{B}$ is *left exact* if the exactness of $0 \rightarrow A_1 \rightarrow A_2 \rightarrow A_3$ implies that of $0 \rightarrow FA_1 \rightarrow FA_2 \rightarrow FA_3$. Proposition 2.8i) asserts that the functor $\text{Hom}_A(X, *)$ is left exact. Likewise, a contravariant functor $G: \mathcal{Q} \rightarrow \mathcal{B}$ is *left exact* if the exactness of $A_1 \rightarrow A_2 \rightarrow A_3 \rightarrow 0$ implies that of $0 \rightarrow GA_3 \rightarrow GA_2 \rightarrow GA_1$. By Proposition 2.8ii), $\text{Hom}_A(*, Y)$ is a left exact contravariant functor from ${}_A\mathcal{M}$ to $\mathcal{Q}\mathcal{B}$.

Finally, an *exact* functor is one which is both left and right exact. It is easily shown (see references) that the following holds true:

(2.21) Proposition. *Let $F: \mathcal{Q} \rightarrow \mathcal{B}$ be a functor. The following conditions are equivalent:*

- (i) F is exact.
- (ii) F preserves exactness of short exact sequences.
- (iii) F preserves exactness of all exact sequences.

Sketch of Proof. The implications (i) \Rightarrow (ii) and (iii) \Rightarrow (i) are obvious, and we need only prove that (ii) \Rightarrow (iii). Assume (ii), and let $A_1 \xrightarrow{\alpha} A_2 \xrightarrow{\beta} A_3$ be exact in \mathcal{Q} ; we must show that

$$FA_1 \xrightarrow{F\alpha} FA_2 \xrightarrow{F\beta} FA_3$$

is exact in \mathcal{B} . Consider the commutative diagram with exact rows and

$$\begin{array}{ccccccc} & & & 0 & & & \\ & & & \downarrow & & & \\ & & & 0 & & & \\ & & & \downarrow & & & \\ 0 & \longrightarrow & \ker \alpha & \xrightarrow{i} & A_1 & \xrightarrow{\alpha} & \text{im } \alpha \longrightarrow 0 \\ & & \downarrow & & \downarrow & & \downarrow \\ & & & & A_2 & \xrightarrow{\beta} & \\ & & \downarrow \alpha & & \downarrow i & & \\ & & 0 & \longrightarrow & \text{im } \beta & \xrightarrow{i} & \text{cok } \beta \longrightarrow 0 \\ & & & & \downarrow & & \\ & & & & 0 & & \end{array}$$

where each i is an inclusion map. Since F preserves exactness of short exact sequences, when we apply the functor F to this diagram we obtain a new commutative diagram in \mathcal{B} , with exact rows and exact columns. It is then trivial to check that $\ker F\beta = \text{im } F\alpha$, which completes the proof.

§2D. Projective, Injective, and Flat Modules

Throughout this section let A be a ring, and let the term “ A -module” mean “left A -module”, unless explicitly stated otherwise. An A -module F is said to have a *free A -basis* $\{x_\alpha\}$, where α ranges over some index set, if there exist elements $x_\alpha \in F$ such that each $x \in F$ is expressible as a finite sum $\sum a_\alpha x_\alpha$ with uniquely determined coefficients $a_\alpha \in A$. Such modules F are called *free A -modules*. Thus, F is A -free if and only if F is isomorphic to a direct sum of copies of A .

A *projective A -module* is a direct summand of a free module; every free module is of course projective, but the converse need not hold for arbitrary rings A . If $\{M_i\}$ is any family of A -modules, it is immediate from the definition of projective modules that the direct sum $\coprod M_i$ is projective if and only if each M_i is projective.

We may observe next that every A -module M is a homomorphic image of some free module F . In fact, we need only choose any set of elements $m_\alpha \in M$ such that $M = \sum A m_\alpha$; now let F be free with basis $\{x_\alpha\}$, and define the surjection $\psi: F \rightarrow M$ by letting $\psi(x_\alpha) = m_\alpha$ for each α . We also remark that if M is finitely generated as A -module, then the free module F may be chosen free with a finite basis.

We state without proof (see references):

(2.22) Proposition. *Let P be any A -module. The following conditions are equivalent:*

- (i) *P is projective.*
- (ii) *Every short exact sequence $0 \rightarrow X \rightarrow Y \rightarrow P \rightarrow 0$ of A -modules must split.*
- (iii) *For each diagram with exact bottom row*

$$\begin{array}{ccccc} & & P & & \\ & h \swarrow & \downarrow f & & \\ X & \xrightarrow{g} & Y & \longrightarrow & 0 \end{array}$$

there exists an A -homomorphism h such that $f = gh$.

- (iv) *For each surjection $g: X \rightarrow Y$, the induced map*

$$g_*: \text{Hom}_A(P, X) \rightarrow \text{Hom}_A(P, Y)$$

is also surjective.

- (v) *The functor $\text{Hom}_A(P, *)$ is exact.*

(2.23) Remark. The preceding result may be sharpened slightly in the case where P is a finitely generated A -module. In this case, P is projective if and only if every short exact sequence $0 \rightarrow X \rightarrow Y \rightarrow P \rightarrow 0$, in which Y is finitely generated, is A -split.

For later use, we prove:

(2.24) Schanuel's Lemma. *Given two short exact sequences of left A -modules*

$$0 \rightarrow M \rightarrow P \xrightarrow{f} X \rightarrow 0, \quad 0 \rightarrow M' \rightarrow P' \xrightarrow{g} X \rightarrow 0$$

in which P and P' are projective, there is an A -isomorphism

$$M' \oplus P \cong M \oplus P'.$$

Proof. Let Y be the pullback of the pair of maps $\{f, g\}$ (see (2.10)), so there is a commutative diagram

$$\begin{array}{ccc} Y & \xrightarrow{g_1} & P \\ f_1 \downarrow & & \downarrow f \\ P' & \xrightarrow{g} & X \end{array}$$

By Exercise 2.3, it follows that $\ker g_1 \cong \ker g$, and that g_1 is surjective. An analogous result holds for f_1 . Thus there are exact sequences

$$0 \rightarrow M' \rightarrow Y \xrightarrow{g_1} P \rightarrow 0, \quad 0 \rightarrow M \rightarrow Y \xrightarrow{f_1} P' \rightarrow 0.$$

Since P and P' are projective, both sequences are A -split, and hence

$$Y \cong M' \oplus P \cong M \oplus P'.$$

This completes the proof.

Next we turn to the concept of *injective* modules, dual to that of projective modules. A module Q is called *injective* if every short exact sequence $0 \rightarrow Q \rightarrow X \rightarrow Y \rightarrow 0$ is split. We state without proof (see references):

(2.25) Proposition. *Let Q be a left A -module. The following are equivalent:*

- (i) Q is injective.
- (ii) Every short exact sequence $0 \rightarrow Q \rightarrow X \rightarrow Y \rightarrow 0$ must split.

(iii) For each diagram with exact top row

$$\begin{array}{ccccc} 0 & \longrightarrow & X & \xrightarrow{f} & Y \\ & & \downarrow g & & \swarrow h \\ & & Q & & \end{array}$$

there exists an h such that $g = hf$.

(iv) For each injection $f \in \text{Hom}_A(X, Y)$, the induced map $f^* : \text{Hom}_A(Y, Q) \rightarrow \text{Hom}_A(X, Q)$ is surjective.

(v) The functor $\text{Hom}_A(*, Q)$ is exact.

(vi) For every left ideal I of A and every $g \in \text{Hom}_A(I, Q)$, there exists an $h \in \text{Hom}_A(A, Q)$ such that $g = h|_I$ (the restriction of h to I).

(2.26) Remarks. (i) In the preceding proposition, condition (ii) is just the restatement of the definition of injectivity, and is included for convenience.

(ii) Proposition 2.25 is somewhat more difficult to prove than the corresponding Proposition 2.22 for projective modules. In particular, the equivalence of (iii) and (vi) is proved by an appeal to Zorn's Lemma.

(iii) Given any family $\{M_i\}$ of A -modules, it is easily shown that the direct product $\prod M_i$ is injective if and only if each M_i is injective. From this it follows at once that $M_1 \oplus M_2$ is injective if and only if both M_1 and M_2 are injective.

(iv) We showed earlier that every module M can be expressed as a homomorphic image of a projective module (and, indeed, of a free module). The dual statement also holds true:

Every A -module can be embedded in an injective module. (For proof, see CR §57).

We shall need the dual of (2.23):

(2.27) Proposition. *Let E be a finitely generated A -module. Then E is injective if and only if every short exact sequence*

$$0 \rightarrow E \rightarrow X \rightarrow Y \rightarrow 0,$$

in which X and Y are finitely generated, is necessarily A -split.

Proof. If E is injective, every such sequence splits by (2.25). Conversely, suppose each such sequence splits, and consider a diagram

$$\begin{array}{ccccc} 0 & \longrightarrow & I & \xrightarrow{i} & A \\ & & \downarrow g & & \\ & & E & & \end{array}$$

in which i is the inclusion map, and $g \in \text{Hom}_A(I, E)$. If X denotes the pushout of the pair of maps $\{i, g\}$, then using Exercise 2.2, we obtain a commutative diagram

$$\begin{array}{ccccccc} 0 & \longrightarrow & I & \xrightarrow{i} & A & \longrightarrow & A/I \longrightarrow 0 \\ & & \downarrow g & & \downarrow g' & & \downarrow 1 \\ 0 & \longrightarrow & E & \xrightarrow{i'} & X & \longrightarrow & A/I \longrightarrow 0 \end{array}$$

with exact rows. Since X is a quotient of $E \oplus A$, it is clear that X is finitely generated as A -module. By hypothesis, the bottom row in the above diagram is A -split. Hence, there exists a map $p \in \text{Hom}_A(X, E)$ such that $pi' = 1_E$. But then $pg' \in \text{Hom}_A(A, E)$ is such that $(pg')i = g$, so we have lifted the map g :

$$\begin{array}{ccccc} 0 & \longrightarrow & I & \xrightarrow{i} & A \\ & & \downarrow g & & \\ & & E & \xrightarrow{\quad pg' \quad} & \end{array}$$

Hence by (2.25vi) it follows that E is injective. This completes the proof.

We turn next to the concept of *flatness*: a left A -module X is *flat* if $* \otimes_A X$ is an exact functor, that is, for each exact sequence

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

of right A -modules, the sequence of additive groups

$$L \otimes_A X \xrightarrow{f \otimes 1} M \otimes_A X \xrightarrow{g \otimes 1} N \otimes_A X$$

is also exact. Let us prove at once that every projective module is flat; this

result is useful, but even more important is the type of reasoning used in the proof.

(2.28) Proposition. *Every projective module is flat.*

Proof. By virtue of the isomorphism $M \otimes A \cong M$ (see (2.16)), it follows at once that the left A -module $_A A$ is flat. Since “tensor product commutes with direct sum” by (2.17), we deduce that every free module is flat. Now let X be any projective left A -module; then X is a direct summand of some free module F , and we may write $F = X \oplus X'$ (internal direct sum) for some module X' .

Next let $L \xrightarrow{f} M \xrightarrow{g} N$ be an exact sequence of right A -modules. We have $L \otimes F \cong L \otimes X \oplus L \otimes X'$, where \otimes means \otimes_A . Hence there is a commutative diagram

$$\begin{array}{ccccccc} L \otimes F & \xrightarrow{f \otimes 1_F} & M \otimes F & \xrightarrow{g \otimes 1_F} & N \otimes F \\ \downarrow & & \downarrow & & \downarrow \\ L \otimes X \oplus L \otimes X' & \xrightarrow{\varphi} & M \otimes X \oplus M \otimes X' & \xrightarrow{\psi} & N \otimes X \oplus N \otimes X', \end{array}$$

where the vertical maps are isomorphisms, and where

$$\varphi = f \otimes 1_X \oplus f \otimes 1_{X'}, \quad \psi = g \otimes 1_X \oplus g \otimes 1_{X'}.$$

Since the top row is exact (because F is flat), it follows that the bottom row is also exact. Therefore the sequence

$$L \otimes X \rightarrow M \otimes X \rightarrow N \otimes X$$

is exact, and so X is flat.

As another illustration of this method of reasoning, we prove

(2.29) Proposition. *Let L be a finitely generated projective right A -module, and let M be any right A -module. Then there is a natural isomorphism of additive groups*

$$(2.30) \quad L \otimes_A \text{Hom}_A(M, A) \cong \text{Hom}_A(M, L),$$

given thus: for each $x \in L$ and $f \in \text{Hom}_A(M, A)$, we map $x \otimes f \in L \otimes \text{Hom}_A(M, A)$ onto the element $[x, f] \in \text{Hom}_A(M, L)$, where

$$(2.31) \quad [x, f]m = x \cdot f(m), \quad m \in M.$$

Proof. Observe first that $\text{Hom}_A(M_A, {}_A A_A)$ is a left A -module, since Hom is covariant in the second variable. Next, both sides of (2.30) represent covariant (additive) functors of L , that is, for fixed M the functors

$$\text{Hom}_A(M, *) \text{ and } * \otimes_A \text{Hom}_A(M, A)$$

are covariant functors from \mathfrak{M}_A to \mathfrak{QB} . As in the proof of (2.28), it follows that (2.30) is valid for a direct sum $L \oplus L'$ if and only if it holds for both L and L' .

Now (2.30) holds true when $L = A_A$, by virtue of the isomorphisms given in (2.6) and (2.16). Of course, one must verify that these isomorphisms agree with the map defined by (2.31), but we shall omit this routine calculation. By the remarks in the preceding paragraph, it follows that (2.30) holds whenever L is a free A -module on a finite basis. But then (2.30) is true for every finitely generated projective right A -module L , since each such L is a direct summand of a free module on a finite basis.

[We caution the reader that (2.30) need not hold when L is not finitely generated.]

The same method of proof yields

$$(2.32) \quad \text{Hom}_A(M, A) \otimes_A L \cong \text{Hom}_A(M, L)$$

if M, L are left A -modules, with M finitely generated and projective.

We have shown above that every projective module is flat. However, in later work we shall need to know that every torsionfree module over a Dedekind ring is flat (see Exercise 4.3), and such modules need not be projective. A key step in proving this needed result is the following proposition, valid for arbitrary rings A .

(2.33) Proposition. *A right A -module X is flat if every f.g. submodule of X is flat.*

Proof. Let \otimes denote \otimes_A , and suppose that each f.g. submodule of X is flat. In order to prove that X is flat, it suffices to show (by virtue of (2.21)) that for each inclusion $i: L \rightarrow M$ of left A -modules, the map

$$1 \otimes i: X \otimes L \rightarrow X \otimes M$$

is injective.

By §2B, the tensor product $X \otimes M$ may be defined as F/F_0 , with F the free abelian group generated by all ordered pairs (x, m) , $x \in X$, $m \in M$, and where F_0 is the subgroup of F generated by expressions of the form $(x+x', m) - (x, m) - (x', m)$, and so on. Now let

$$u = \sum_{j=1}^r x_j \otimes l_j \in X \otimes L$$

be such that $(1 \otimes i)u = 0$ in $X \otimes M$. Then $\Sigma(x_j, i(l_j)) \in F_0$, and so $\Sigma(x_j, i(l_j))$ may be expressed as a finite sum, each term of which is ± 1 times a generator of F_0 . These terms involve only finitely many elements of X ; let X' be the submodule of X generated by these elements, together with the elements x_1, \dots, x_r occurring in u . Let $u' = \sum x_j \otimes l_j$, viewed as an element of $X' \otimes L$. The above discussion implies at once that the map $\psi: X' \otimes L \rightarrow X' \otimes M$ carries u' onto the zero element of $X' \otimes M$. But ψ is injective since X' is flat by hypothesis, and hence $u' = 0$. However, u' maps onto u under the map $X' \otimes L \rightarrow X \otimes L$. Thus $u = 0$, which completes the proof that $1 \otimes i$ is injective, and establishes the proposition.

(2.34) Corollary. *Every torsionfree module over a P.I.D.* is flat.*

Proof. Let R be a (commutative) P.I.D., and X any torsionfree R -module (that is, $rx = 0 \Rightarrow r = 0$ or $x = 0$, for $r \in R$, $x \in X$). To prove X flat, we need show that each f.g. submodule X' of X is flat. But X' is torsionfree, and by the Structure Theorem for f.g. modules over a P.I.D. (see CR §16) it follows that X' is a free R -module. Hence X' is flat by (2.28). This completes the proof.

As an example, we note that \mathbf{Q} is a flat \mathbf{Z} -module. Indeed, every torsionfree \mathbf{Z} -module is flat.

The concept of flatness plays an important role in the “Change of Rings” Theorem given below (see (2.38)). In order to state this theorem, we need a number of definitions which are important in their own right. We recall the following (see (1.1)):

(2.35) Definition. Let R be a commutative ring. An arbitrary ring A is called an R -algebra if there exists a ring homomorphism $\psi: R \rightarrow$ center of A . Using ψ , every A -module (including A itself) may be viewed as R -module.

If A is a left noetherian ring, then for each f.g. left A -module M there is an exact sequence

$$(2.36) \quad A^{(s)} \rightarrow A^{(r)} \rightarrow M \rightarrow 0,$$

with r, s positive integers. Even when A is not necessarily noetherian, there may be such a sequence for M ; in such case, we call M *finitely presented*. We emphasize that when A is left noetherian, every f.g. left A -module is necessarily finitely presented.

Now let A and B be R -algebras, where R is a commutative ring, and let M, N be left A -modules. We set

$$A' = B \otimes_R A, \quad M' = B \otimes_R M,$$

*P.I.D. is an abbreviation for “principal ideal domain”.

so M' is a left module over the R -algebra A' . There exists an R -homomorphism

$$(2.37) \quad \alpha: B \otimes_R \text{Hom}_A(M, N) \rightarrow \text{Hom}_{A'}(M', N'),$$

given by

$$\alpha(b \otimes f) = b_r \otimes f, \quad b \in B, f \in \text{Hom}_A(M, N),$$

where b_r denotes right multiplication by b acting on B . There are bimodule structures ${}_B B_R$ and ${}_{A'}(M')_B$, so that both sides of (2.37) have the structure of left B -modules. Likewise, the bimodule structures* $B_{B, R}$ and ${}_{A'}(N')_B$ make the expressions in (2.37) into right B -modules. It is easily verified that the map α defined in (2.37) is a two-sided B -homomorphism.

(2.38) Theorem (Change of rings). *Let A and B be R -algebras, where R is a commutative ring, and let M and N be left A -modules. Put $A' = B \otimes_R A$, $M' = B \otimes_R M$, and let*

$$\alpha: B \otimes_R \text{Hom}_A(M, N) \rightarrow \text{Hom}_{A'}(M', N')$$

be the two-sided B -homomorphism defined in (2.37). Assume that B is a flat R -module.

- (i) *If M is finitely generated as left A -module, then α is a monomorphism.*
- (ii) *If M is finitely presented as left A -module, then α is an isomorphism.*

For the proof, see MO §2e. The result is often applied in the special case where B is some commutative ring R' containing R . For example, suppose that R is an integral domain and R' is some ring of quotients of R (see §4A). Then R' is necessarily R -flat, and we obtain

$$(2.39) \quad R' \otimes_R \text{Hom}_A(M, N) \cong \text{Hom}_{A'}(M', N')$$

if A is a left noetherian R -algebra, and M is a finitely presented A -module. Here, $A' = R' \otimes_R A$, $M' = R' \otimes_R M$.

We list here some standard references on Homological Algebra:

Properties of Hom:	Rotman [79].
Tensor products:	Curtis-Reiner [66].
Ext and Tor:	Cartan-Eilenberg [56], Rotman [79].
Cohomology of groups:	preceding list, and also Babakhanian [72], Gruenberg [70], Weiss [69].

*The notation $B_{B, R}$ indicates that B is a right B -, right R -bimodule.

§2. Exercises

1. Given a ring A and left A -modules L, M, X, Y , let $f \in \text{Hom}_A(L, M)$, $g \in \text{Hom}_A(X, Y)$. Show that for all $\alpha \in \text{Hom}_A(M, X)$,

$$g_* f^* \alpha = f^* g_* \alpha = g \alpha f,$$

where f^*, g_* are defined as in (2.4) and (2.5).

2. Given a pushout diagram (2.9), show that g_1 induces an isomorphism: $\text{cok } f_1 \cong \text{cok } g_2$. Show also that if f_1 is injective, then so is g_2 .
3. Given a pullback diagram (2.10), prove that g_2 induces an isomorphism: $\ker g_1 \cong \ker f_2$. Show also that if f_2 is surjective, then so is g_1 .
4. Using the method of proof of (2.19), show that for rings A, B and data $L_A, {}_A M_B, N_B$, there is a natural isomorphism

$$\text{Hom}_A(L, \text{Hom}_B(M, N)) \cong \text{Hom}_B(L \otimes_A M, N).$$

5. Prove the **Snake Lemma**: *Given a commutative diagram of modules, with exact rows:*

$$\begin{array}{ccccccc} A & \xrightarrow{\rho} & B & \longrightarrow & C & \longrightarrow & 0 \\ \alpha \downarrow & & \beta \downarrow & & \gamma \downarrow & & \\ 0 & \longrightarrow & A' & \longrightarrow & B' & \longrightarrow & C' \end{array}$$

there is an exact sequence

$$\ker \alpha \xrightarrow{\rho_*} \ker \beta \rightarrow \ker \gamma \rightarrow \text{cok } \alpha \rightarrow \text{cok } \beta \xrightarrow{\sigma_*} \text{cok } \gamma.$$

Further, if ρ is injective so is ρ_ ; if σ is surjective, so is σ_* .*

[Hint: Define δ by $\delta(c) = a' + \text{im } \alpha$, where

$$a' \rightarrow b', b' = \beta(b), b \rightarrow c.]$$

6. Let R be a commutative noetherian ring, and let A be an R -algebra as in (2.36). Suppose that A is f.g. as R -module, and let M, N be f.g. left A -modules. Show that $\text{Hom}_A(M, N)$ is f.g./ R .

[Hint: $\text{Hom}_A(M, N)$ is an R -submodule of $\text{Hom}_R(M, N)$, and both M, N are f.g./ R . If $R^{(k)} \rightarrow M \rightarrow 0$ is R -exact, then so is

$$0 \rightarrow \text{Hom}_R(M, N) \rightarrow \text{Hom}_R(R^{(k)}, N).$$

The last term is isomorphic to $N^{(k)}$ as R -module, hence is f.g./ R .]

7. Let A be a finite dimensional algebra over a field K , and let M be any f.g. left

A -module. For any field E containing K , define

$$A^E = E \otimes_K A, M^E = E \otimes_K M,$$

so A^E is a finite dimensional E -algebra and M^E is a f.g. left A^E -module. Let N be any left A -module. Show that

$$(2.40) \quad E \otimes_K \text{Hom}_A(M, N) \cong \text{Hom}_{A^E}(M^E, N^E)$$

as vector spaces over E .

[Hint: Use (2.38) with $R = K$, $B = E$. A direct proof may be found in CR (29.5).]

8. Prove that (2.40) remains valid even when $\dim_K(A)$ is infinite, provided we assume that M and N are A -modules of finite dimension over K .

[Hint: For each $a \in A$, let $a_!$ denote left multiplication by a on the A -module $M \oplus N$. Then M and N are $A_!$ -modules, and $\text{Hom}_A(M, N) = \text{Hom}_{A_!}(M, N)$. Further, $\dim_K(A_!)$ is finite. Now use the preceding exercise with $A_!$ in place of A .]

9. Let A be a K -algebra, where K is a field, and let M be a left A -module such that $\dim_K(M)$ is finite. Let E be any field containing K . Prove that there is an isomorphism of E -algebras:

$$(2.41) \quad \text{End}_{A^E}(M^E) \cong E \otimes_K \text{End}_A(M).$$

10. Given a pushout diagram (2.9), show that the pushout X has the following universal mapping property: for every commutative diagram

$$\begin{array}{ccc} T & \xrightarrow{f_1} & M_1 \\ f_2 \downarrow & & \downarrow h_1 \\ M_2 & \xrightarrow{h_2} & V \end{array}$$

there is a unique A -homomorphism $h: X \rightarrow V$ such that

$$\begin{array}{ccccc} T & \xrightarrow{\quad} & M_1 & & \\ \downarrow & & \downarrow h_1 & & \\ M_2 & \xrightarrow{\quad} & X & \xrightarrow{h} & V \\ & & \searrow h_2 & & \end{array}$$

commutes.

11. Given a pullback diagram (2.10), show that the pullback Y has the following

universal mapping property: for every commutative diagram

$$\begin{array}{ccc} W & \xrightarrow{h_1} & M_1 \\ h_2 \downarrow & & \downarrow f_1 \\ M_2 & \xrightarrow{f_2} & U \end{array}$$

there is a unique A -homomorphism $h: W \rightarrow Y$ such that

$$\begin{array}{ccccc} W & \xrightarrow{h_1} & & & M_1 \\ h \swarrow & & \searrow g_1 & & \\ & Y & \xrightarrow{g_2} & M_2 & \\ h_2 \searrow & & \downarrow f_1 & & \\ & M_2 & \xrightarrow{f_2} & U & \end{array}$$

commutes.

12. Let

$$\begin{array}{ccccccc} 0 & \longrightarrow & L_1 & \xrightarrow{\alpha_1} & M_1 & \xrightarrow{\beta_1} & N_1 & \longrightarrow 0 \\ & & \lambda \downarrow & & \mu \downarrow & & \nu \downarrow & \\ 0 & \longrightarrow & L_2 & \xrightarrow{\alpha_2} & M_2 & \xrightarrow{\beta_2} & N_2 & \longrightarrow 0 \end{array}$$

be a commutative diagram of left A -modules and A -homomorphisms, with exact rows. Let X be the pushout of $\{\lambda, \alpha_1\}$, and let Y be the pullback of $\{\nu, \beta_2\}$. Show that there exist maps μ_i ($i = 1, 2, 3$) and a commutative diagram

$$\begin{array}{ccccccc} 0 & \longrightarrow & L_1 & \xrightarrow{\alpha_1} & M_1 & \xrightarrow{\beta_1} & N_1 & \longrightarrow 0 \\ & & \lambda \downarrow & & \mu_1 \downarrow & & 1 \downarrow & \\ 0 & \longrightarrow & L_2 & \xrightarrow{\alpha_2} & X & \longrightarrow & N_1 & \longrightarrow 0 \\ & & 1 \downarrow & & \mu_2 \downarrow & & 1 \downarrow & \\ 0 & \longrightarrow & L_2 & \longrightarrow & Y & \longrightarrow & N_1 & \longrightarrow 0 \\ & & 1 \downarrow & & \mu_3 \downarrow & & \nu \downarrow & \\ 0 & \longrightarrow & L_2 & \xrightarrow{\alpha_2} & M_2 & \xrightarrow{\beta_2} & N_2 & \longrightarrow 0 \end{array}$$

such that $\mu_3 \mu_2 \mu_1 = \mu$.

[Hint: Use the previous two exercises.]

13. Let R be a P.I.D., and let $\bar{R} = R/aR$, where a is a nonzero element of R . Prove that \bar{R} is self-injective, that is, \bar{R} is an injective \bar{R} -module.

[Hint: Use (2.25vi)].

§3. SEMISIMPLE RINGS AND MODULES. THE WEDDERBURN AND MORITA THEOREMS

This section begins by reviewing finiteness conditions for rings and modules. Next comes the theory of semisimple modules and rings, including the Wedderburn Theorems and the Chevalley-Jacobson Density Theorem. Applications are given to finite dimensional algebras over fields, and in particular, to the theory of group representations. An account of the Morita theorems for categories of modules is given, with applications to tensor products of simple algebras and modules.

§3A. Finiteness Conditions

The definition and elementary properties of noetherian and artinian rings and modules will be sketched without proofs. Modules satisfying both finiteness conditions have composition series, and an important numerical invariant (the *length* of such a module) is introduced, as well as the possibility of analyzing modules of finite lengths in terms of simple modules.

(3.1) Proposition. *Let M be a left module over a ring A . The following conditions are equivalent:* (a) *The submodules of M satisfy the ascending chain condition (ACC): For every increasing sequence of submodules of M ,*

$$M_1 \subseteq M_2 \subseteq \cdots,$$

there exists an integer n such that $M_n = M_{n+1} = \cdots$. (b) The submodules of M satisfy the maximum condition: every non-empty set of submodules, partially ordered by inclusion, has a maximal element. (c) Every submodule of M is finitely generated.

(3.2) Definition. A left A -module satisfying any one of the equivalent conditions stated in (3.1) is called a *noetherian module*. A ring A whose left regular module $_A A$ is noetherian is called a *left noetherian ring* (with a similar definition for a right noetherian ring).

Principal ideal domains, and (by the Hilbert Basis Theorem) polynomial rings $R[X_1, \dots, X_n]$ over a left noetherian ring R , are examples of left noetherian rings. Noetherian modules can often be identified by the following result:

(3.3) Proposition. *A finitely generated left module over a left noetherian ring is noetherian.* (For a proof see CR §11).

(3.4) Corollary. *Let A be an algebra over a commutative noetherian ring R , such that A is a finitely generated left R -module. Then every finitely generated left A -module is noetherian.*

Another finiteness condition on rings and modules is described in the following result:

(3.5) Proposition. *Let A be an arbitrary ring, and let M be a left A -module. The following conditions are equivalent:*

(i) *The submodules of M satisfy the descending chain condition (DCC): for every descending sequence of submodules of M ,*

$$M_1 \supseteq M_2 \supseteq \cdots,$$

there exists an integer k such that $M_k = M_{k+1} = \cdots$.

(ii) *The submodules of M satisfy the minimum condition: every non-empty family of submodules, viewed as a partially ordered set under inclusion, has a minimal element.*

(3.6) Definition. A left A -module M is called *artinian* in case its submodules satisfy the DCC, or equivalently, the minimum condition. A *left artinian ring* is a ring A whose left regular module ${}_A A$ is artinian.

The following criterion will be used repeatedly in practice:

(3.7) Proposition. *Every f.g. left module M over a left artinian ring A is both artinian and noetherian.*

Proof. Hopkin's Theorem (see CR (54.1)) states that every left artinian ring is necessarily left noetherian. Thus M is a noetherian module by (3.4). But since A is artinian, so is M (see CR (11.15), for example).

(3.8) Definition. A left A -module P is *simple* (or *irreducible*) in case $P \neq 0$, and the only submodules of P are P and 0 . A left A -module M has a *composition series* if there exists a descending chain of submodules of M :

$$M = M_1 \supset M_2 \supset \cdots \supset M_s \supset M_{s+1} = 0,$$

such that the factor modules $\{M_i/M_{i+1} : 1 \leq i \leq s\}$ are simple. The modules $\{M_i/M_{i+1}\}$ are called the *factors* of the composition series, and the number of factors (in this case s) is called the *length* of the composition series. (See (1.17) for finite groups.)

(3.9) Proposition. *A necessary and sufficient condition for a left A -module to have a composition series is that it be both left noetherian and left artinian. In case this occurs, any two composition series have the same length. (For a proof see CR §11.)*

(3.10) Definition. Let M be a left A -module with a composition series. The length of a composition series of M is called the *length* of M , and is denoted by $l(M)$.

Proposition 3.9 shows that the length of a module with a composition series is independent of the choice of the composition series, and is therefore a numerical invariant of the module.

(3.11) Jordan-Hölder Theorem. Suppose M is a module having two composition series. Then the numbers of factors in the two series are the same, and a bijection from one set of factors to the other can be defined in such a way that corresponding factors are isomorphic.

§3B. Semisimple Modules and Rings

The least complicated behavior of a left A -module M with reference to simple submodules is described by the following result:

(3.12) Proposition. Let M be a left A -module over an arbitrary ring A . The following statements are equivalent:

$$(i) \quad M = \bigoplus_{i \in I} M_i \text{ for some family } \{M_i\}_{i \in I} \text{ of simple submodules of } M.$$

$$(ii) \quad M = \sum_{j \in J} M_j \text{ for some family } \{M_j\}_{j \in J} \text{ of simple submodules.}$$

(iii) For every submodule $M' \subseteq M$, there exists a submodule $M'' \subseteq M$ such that $M = M' \oplus M''$.

The proof is available in many places, for example in CR §12. Notice that no finiteness conditions are assumed in Proposition 3.12; note also that (i) implies the existence of simple submodules of M .

(3.13) Definition. A left A -module satisfying the conditions of (3.12) is called a *semisimple module* (or a *completely reducible* module, as in CR, for example).

Some important examples of semisimple modules are (i) vector spaces over fields or division rings, and (ii) finitely generated modules M over a principal ideal domain R , where $\text{ann}_R(M) = R\alpha$ for an element α which is a product of distinct primes. (See Exercise 3.17.)

The following basic result concerning the semisimplicity of modules over group algebras illustrates the use of condition (3.12iii).

(3.14) Maschke's Theorem. Let KG be the group algebra of a finite group G over a field K (see (1.2ii)). Assume that $|G| \neq 0$ in K , that is, $|G|$ is not a

multiple of the characteristic of K . Then every f.g. left KG -module M is semisimple.

Sketch of Proof. Let N be a KG -submodule of M , so N is a K -subspace of M such that $xN \subseteq N$ for all $x \in G$. By linear algebra, there exists a K -subspace N' of M such that $M = N \oplus N'$. Let $E \in \text{End}_K(M)$ be the projection of M onto N arising from this direct sum decomposition. Then $EM \subseteq N$, and $E|_N = 1_N$ (=identity map on N). The idea is to find an element $E^* \in \text{End}_{KG}(M)$ satisfying these same conditions; in that case, $(1 - E^*)M$ will be the required KG -complement of N in M .

The solution arises from setting

$$E^* = |G|^{-1} \sum_{x \in G} xEx^{-1}.$$

For each $y \in G$, we have

$$yE^*y^{-1} = |G|^{-1} \sum_{x \in G} yxE(yx)^{-1} = E^*,$$

so $E^* \in \text{End}_{KG}(M)$. Further, $E^*M \subseteq N$ and $E^*|_N = 1$, as is easily checked. Therefore E^* is the required KG -projection of M onto N , which completes the proof that M is semisimple.

It is natural to ask what can be said about rings (or algebras) for which every f.g. module is semisimple, as in the case of group algebras considered in Maschke's theorem.

(3.15) Proposition. *The following conditions concerning a ring A are equivalent:*

- (i) *Every left A -module is semisimple.*
- (ii) *Every f.g. left A -module is semisimple.*
- (iii) *The left regular module ${}_A A$ is semisimple, and is a direct sum $A = L_1 \oplus \cdots \oplus L_m$ of a finite number of minimal* left ideals $\{L_1, \dots, L_m\}$.*

Proof. Clearly (i) \Rightarrow (ii). Assume (ii). Then ${}_A A$ is finitely generated (because $A = A \cdot 1$) and thus is semisimple, so that by (3.12)

$$A = \bigoplus_{i \in I} L_i$$

for some family $\{L_i\}_{i \in I}$ of minimal left ideals. Let

$$1 = l_{i_1} + \cdots + l_{i_n},$$

*A *minimal* left ideal of A is a nonzero left ideal L which does not properly contain any nonzero left ideals, that is, L is a simple submodule of the left regular module ${}_A A$.

with $l_{i_j} \in L_{i_j}$, for some indices $\{i_j\}$ in I . Then each $a \in A$ can be expressed in the form

$$a = al_{i_1} + \cdots + al_{i_n},$$

and hence $A = L_{i_1} + \cdots + L_{i_n}$, and (iii) follows.

Finally assume (iii), and let M be an arbitrary left A -module. Then

$$M = AM = \sum_{m \in M} \sum_{i \in I} L_i m.$$

By (3.12) it is sufficient to prove that each submodule $L_i m$ is either zero or simple. This is clear, because for each L_i and $m \in M$, there exists a surjection of A -modules $\varphi: L_i \rightarrow L_i m$, given by $\varphi(l) = lm$, $l \in L_i$. The assertion about $L_i m$ then follows from the fundamental theorem on homomorphisms because L_i is simple. This completes the proof.

(3.16) Definition. A ring A is (*left*) *semisimple* if A satisfies any one of the conditions of (3.15).

The basic problems concerning semisimple rings are to classify their simple modules, and to determine the structure of the rings themselves. We begin with a result showing that the simple modules are all isomorphic to left ideals generated by idempotents. We first require a basic lemma.

(3.17) Schur's Lemma. Let M be a simple A -module over an arbitrary ring A . Then $\text{End}_A(M)$ is a division ring.

Sketch of Proof. Let $f \neq 0$ be an element of $\text{End}_A(M)$. Since M is simple, the fundamental homomorphism theorem implies that f is an A -automorphism of M , and hence is invertible. Therefore $\text{End}_A(M)$ is a division ring.

An *idempotent* is a nonzero element e of a ring A such that $e^2 = e$.

(3.18) Proposition. Let A be a semisimple ring. Then the following statements hold.

- (i) Every nonzero left ideal L in A is generated by an idempotent: $L = Ae$ for some idempotent $e \in A$.
- (ii) Every element $f \in \text{Hom}_A(L, A)$ is given by a right multiplication: $f = a_r$, for some $a \in A$.
- (iii) A left ideal Ae generated by an idempotent e is simple if and only if eAe is a division ring.
- (iv) Every simple left A -module is isomorphic to a left ideal in A .

Proof. (i) By semisimplicity, we may write $A=L\oplus L'$ for a left ideal L' , and put $1=e+e'$, with $e\in L$, $e'\in L'$. Then $e=e^2+ee'$, and $e-e^2=ee'\in L\cap L'=0$. Therefore $e^2=e$, and for all $x\in L$, $x=xe+xe'$, and $x-xe=xe'\in L\cap L'=0$, so that $L=Ae$ as required. Note that $e\neq 0$ since $L\neq 0$.

(ii) Let $f\in \text{Hom}_A(Ae, A)$, where $e^2=e$. Then, setting $a=f(e)$, we have

$$f(x)=f(xe)=xf(e)=xa,$$

for all $x\in Ae$, using the fact that e acts as a right identity operator on Ae . We have thus shown that $f=a_r$, as required.

Before proving (iii), we need one more general lemma.

(3.19) Lemma. *Let e be an idempotent in an arbitrary ring A . Then*

$$\text{End}_A(Ae)\cong(eAe)^\circ \text{ (opposite ring)}.$$

Proof. Let $f\in \text{End}_A(Ae)$. Then $f=a_r$, for $a=f(e)$ (see the proof of (3.18ii)). It follows that $f=(eae)_r$, because

$$f(x)=xa=xiae, \text{ for } x\in Ae \text{ and } f(x)\in Ae.$$

It is then easily checked that the map $f\rightarrow ef(e)e$ is an anti-isomorphism of $\text{End}_A(Ae)$ to eAe , and the lemma is proved.

We now return to the proof of (3.18).

Proof. (iii) First assume that $L=Ae$ is a simple A -module. By Schur's Lemma 3.17, $\text{End}_A(Ae)$ is a division ring, and hence by Lemma 3.19, eAe is also a division ring. Conversely, suppose $L=Ae$ is not simple. Then L contains a nonzero proper submodule L_1 , and $L=L_1\oplus L'_1$ by semisimplicity, where L'_1 is also a nonzero proper submodule of L . The projections associated with this direct decomposition belong to $\text{End}_A(L)$, and are nonzero elements whose product is zero. Therefore $\text{End}_A(L)$ is not a division ring, and by Lemma 3.19, eAe is not a division ring.

(iv) Let M be a simple left A -module, and let $A=\sum L_i$ for simple left ideals $\{L_i\}$. Then $M=AM=\sum L_iM$, and some $L_iM\neq 0$. It follows that $L_iM\neq 0$ for some $m\in M$, and because M is simple, we have $L_iM=M$. The map $x\rightarrow xm$, $x\in L_i$, is an A -surjection of L_i onto M ; it is an isomorphism because L_i is simple (thereby forcing the kernel to be zero).

The next step in analyzing semisimple rings and modules is to sort the simple modules into isomorphism classes; for example, the question arises as to whether a semisimple ring has only a finite number of nonisomorphic simple modules. As an exercise the reader can easily settle this point using

(3.18) and the Jordan-Hölder Theorem. A key result on this type of question is the following general proposition about semisimple modules:

(3.20) Proposition. *Let M be a semisimple left A -module over an arbitrary ring A . Let $\{M_i\}_{i \in I}$ be a set of representatives of the isomorphism classes of simple submodules, and let*

$$H_i = \sum_{\substack{P \cong M_i \\ P \subseteq M}} P.$$

Then the following statements hold:

- (i) $M = \bigoplus_{i \in I} H_i$.
- (ii) Every simple submodule of H_i is isomorphic to M_i .
- (iii) $\text{Hom}_A(H_i, H_{i'}) = 0$ if $i \neq i'$.
- (iv) Let $M = \bigoplus_{j \in J} P_j$ be an arbitrary direct decomposition of M into simple submodules P_j , and for each $i \in I$, let $\tilde{H}_i = \sum_{j \in J, P_j \cong M_i} P_j$. Then $\tilde{H}_i = H_i$ for all $i \in I$.

Proof. We shall prove several statements which, taken together, will establish the proposition.

(a) Let $M = \bigoplus_{j \in J} P_j$, for a set of simple submodules $\{P_j\}$, and let Q be an arbitrary simple submodule of M . Then $Q \cong P_j$ for some $j \in J$.

Proof of (a). Let $\{\pi_j\}_{j \in J}$ be the projections associated with the direct decomposition $M = \bigoplus P_j$. Then $\pi_j(Q) \neq 0$ for some j , and it follows that $\pi_j|_Q: Q \rightarrow P_j$ is an isomorphism because both Q and P_j are simple.

(b) Let $\tilde{H}_i = \sum_{j \in J, P_j \cong M_i} P_j$, as in (iv). Then $M = \bigoplus_{i \in I} \tilde{H}_i$, and every simple submodule of \tilde{H}_i is isomorphic to M_i , for all $i \in I$.

Proof of (b). The first part of (b) follows from the definition of direct sum, and the second statement follows from (a), applied to \tilde{H}_i .

(c) Let Q be an arbitrary simple submodule of M . Then $Q \cong M_i$ for a unique $i \in I$, and $Q \subseteq \tilde{H}_i$.

Proof of (c). Let $q \in Q$, and write

$$q = \sum_{j \in J} q_j, q_j \in P_j.$$

The proof of (a) shows that if any summand $q_j \neq 0$, then $\pi_j(Q) \neq 0$, and $Q \cong P_j$. Therefore $q_j = 0$ unless $P_j \cong M_i$, and hence $q \in \tilde{H}_i$.

(d) Let $f \in \text{Hom}_A(\tilde{H}_i, \tilde{H}_{i'})$ for $i \neq i'$. Then $f=0$.

Proof of (d). If $f \neq 0$, then $f(P) \neq 0$ for some simple submodule P of \tilde{H}_i , and it follows that $f(P)$ is a simple submodule of $\tilde{H}_{i'}$ isomorphic to P . These statements contradict (c), and therefore $f=0$.

Statements (a)–(d) now show that $\tilde{H}_i = H_i$ for each $i \in I$, and also imply the other statements of the proposition.

(3.21) Definition. Let M be a semisimple left A -module, and $\{M_i\}_{i \in I}$ a set of representatives of the isomorphism classes of simple left A -modules of M . The submodules $\{H_i\}_{i \in I}$ defined in (3.20) are called the *homogeneous components* of M (or the *isotypic components* of type M_i).

A ring with identity element is called *simple* if it has no nonzero proper two-sided ideals. The first main structure theorem on semisimple rings can now be stated.

(3.22) Theorem (Wedderburn). *Let A be a left semisimple ring. The number of homogeneous components $\{A_i\}$ of the left regular module $_A A$ is finite, and A is their direct sum:*

$$A = A_1 \oplus \cdots \oplus A_m.$$

Each homogeneous component A_i is a two-sided ideal in A , and $A_i A_{i'} = 0$ if $i \neq i'$. Moreover, each A_i is a simple artinian ring (with identity element).

Proof. From (3.15iii), the left regular module is a finite direct sum of minimal left ideals. By statement (a) in the proof of (3.20), every simple left A -module is isomorphic to one of these summands, and it follows that the number of homogeneous components of $_A A$ is finite.

Let L be a minimal left ideal contained in A_i , and let $a \in A_{i'}$ with $i' \neq i$. Then $La \subseteq A_i$, because $A_{i'}$ is a left ideal, and La is either zero or a minimal left ideal isomorphic to L . Because A_i and $A_{i'}$ are different homogeneous components, we have $La = 0$. Therefore $A_i A_{i'} = 0$ if $i \neq i'$, and the $\{A_i\}$ are two-sided ideals in A .

Letting $1 = e_1 + \cdots + e_m$, with $e_i \in A_i$, $1 \leq i \leq m$, the proof of (3.18) shows that $A_i = Ae_i = e_i A$ (using the fact that A_i is a two-sided ideal), and that $e_i^2 = e_i$, $1 \leq i \leq m$; this proves that the $\{e_i\}$ are identity elements in the ideals A_i to which they belong.

Finally, let S be a nonzero two-sided ideal in A_i , for some i . Because $A_i A_{i'} = 0$ if $i \neq i'$, it follows that S is a two-sided ideal in A . Let L be a minimal left ideal contained in S , and let L' be another minimal left ideal contained in A_i . Then $L \cong L'$, and by (3.18), $L' = La$ for some $a \in A$. Because S is a two-sided ideal in A , $L' \subseteq S$, and it follows that $S = A_i$, because A_i is the sum of all simple left ideals isomorphic to L . Therefore A_i is a simple ring,

and is artinian because it is a finite direct sum of simple modules, and hence has a composition series. This completes the proof.

(3.23) Definition. The ideals $\{A_i\}$ defined in Theorem 3.22 are called the *Wedderburn components* of A .

The preceding result shows that the multiplicative structure of a semisimple ring is determined by the structure of simple artinian rings. Among the many ways of proving the main structure theorem on simple artinian rings, we shall follow Jacobson's original proof of the density theorem (for another proof, see CR §26; a more general version of that argument appears later in this section, in §3D on the Morita Theorems).

The first two results about simple rings clarify their connections with semisimple rings, and set up a situation leading to the density theorem.

(3.24) Proposition. *Every simple artinian ring A is semisimple.*

Proof. Let L be a minimal left ideal of A ; then $B = \sum_{a \in A} La$ is a semisimple submodule of ${}_A A$, and coincides with A because B is a non-zero two-sided ideal of A . Therefore ${}_A A$ is a semisimple module, and A is semisimple.

(3.25) Proposition. *Let A be a simple artinian ring. Then A is isomorphic to a subring A_1 of the endomorphism ring of an abelian group M , where M is a simple A -module. Moreover, $A_1 \subseteq \text{End}_D(M)$, where $D = \text{End}_A(M)$ is a division ring.*

Proof. Let M be a minimal left ideal in A , (such an M exists by the minimum condition.) The map $a \rightarrow a_1$, $a \in A$, is a homomorphism $A \rightarrow A_1$ from A into the endomorphism ring of M . Because A is simple, $A \cong A_1$. Finally, $D = \text{End}_A(M)$ is a division ring by Schur's Lemma because M is a simple module.

The structure of a ring of linear transformations over a division ring satisfying the conditions in (3.25) is determined by the density theorem.

(3.26) Definition. A ring of linear transformation on a left vector space M over a division ring D is called a *dense* ring of linear transformations, if, for every $k = 1, 2, \dots$, and every set of $2k$ elements of M , $\{x_1, \dots, x_k; y_1, \dots, y_k\}$, with $\{x_1, \dots, x_k\}$ linearly independent over D , and $\{y_1, \dots, y_k\}$ arbitrary, there exists an element $a \in A$ such that $ax_i = y_i$, $i = 1, 2, \dots, k$.

(3.27) Density Theorem. *Let A be a subring of the endomorphism ring of an abelian group M , $A \subseteq \text{End}_Z(M)$, such that M is a simple left A -module. Then $D = \text{End}_A(M)$ is a division ring, and A is a dense ring of linear transformations on the vector space M over D .*

Proof (Jacobson [45a]). We use induction on k , starting from an arbitrary set of $2k$ elements $\{x_1, \dots, x_k; y_1, \dots, y_k\}$, as in (3.26), with x_1, \dots, x_k linearly independent. First, let $k=1$. In this case, $x_1 \neq 0$, and $Ax_1 \neq 0$, so that $Ax_1 = M$ because M is simple. Therefore $y_1 = ax_1$ for some $a \in A$.

Next, let $k=2$. First we prove that there exists $a_2 \in A$ such that $a_2 x_1 = 0$, and $a_2 x_2 \neq 0$. If no such $a_2 \in A$ exists, then $ax_1 \rightarrow ax_2$, for $a \in A$, is a well-defined map from Ax_1 to Ax_2 , and is an A -endomorphism of M because $Ax_1 = Ax_2 = M$, again because M is simple. Therefore $ax_1 \rightarrow ax_2$ is given by left multiplication by some $\delta \in D = \text{End}_A(M)$, and in particular, $x_2 = \delta x_1$, contradicting the linear independence of x_1 and x_2 . Thus a_2 exists. Similarly there exists $a_1 \in A$ such that $a_1 x_1 \neq 0$, $a_1 x_2 = 0$. By the case $k=1$, there exist $b_1, b_2 \in A$ such that $b_1 a_1 x_1 = y_1$ and $b_2 a_2 x_2 = y_2$. Then $a = b_1 a_1 + b_2 a_2$ satisfies our requirements.

Now let k be arbitrary. We assume $k > 2$, and that the result holds for any set of $2m$ elements of the required sort, with $m < k$. By the argument in the case $k=2$, it is sufficient to find $a_k \in A$ such that $a_k x_1 = \dots = a_k x_{k-1} = 0$, and $a_k x_k \neq 0$. By induction, there exists an element $b \in A$ such that

$$bx_1 = \dots = bx_{k-2} = 0, \quad bx_k \neq 0.$$

Now let $B \subseteq A$ be the set of all such elements b . If either $bx_{k-1} = 0$ or bx_k are linearly independent, then it is easy to construct the required a_k , using the case $k=2$ in the second case to find $c \in A$ with $cbx_{k-1} = 0$, $cbx_k \neq 0$ and putting $a_k = cb$. Therefore we may assume that $bx_{k-1} = \beta bx_k$ for some $\beta \neq 0$ in D . Then $x_{k-1} - \beta x_k \neq 0$, and by induction there exists $d \in A$ with $dx_1 = \dots = dx_{k-2} = 0$, $d(x_{k-1} - \beta x_k) \neq 0$. If $dx_k = 0$ (and hence $dx_{k-1} \neq 0$), there exists $u \in A$ such that $udx_{k-1} = bx_{k-1}$. Then, for $a_k = b - ud$, we have

$$a_k x_1 = \dots = a_k x_{k-1} = 0, \quad a_k x_k = bx_k \neq 0.$$

So we may assume that $dx_k \neq 0$, and hence $d \in B$. If either $dx_{k-1} = 0$ or dx_k are D -independent, then the previous discussion applies.

So we may suppose that $dx_{k-1} = \delta dx_k$, for $\delta \neq 0$. Then $\delta \neq \beta$. We can find $v \in A$ such that

$$vdx_{k-1} = bx_{k-1}.$$

Then

$$vdx_k = vd\delta^{-1}x_{k-1} = \delta^{-1}vdx_{k-1} = \delta^{-1}bx_{k-1} = \delta^{-1}\beta bx_k,$$

and hence $(vd - \delta^{-1}\beta b)x_k = 0$. Now put $a_k = b - vd$, then

$$a_k x_1 = \dots = a_k x_{k-1} = 0$$

and $a_k x_k = (b - vd)x_k \neq 0$, because $(vd - \delta^{-1}\beta b)x_k = 0$ and $\delta^{-1}\beta \neq 1$. This completes the proof.

The first application of the Density Theorem completes our present discussion of semisimple rings.

(3.28) Main Structure Theorem on Simple Artinian Rings. *Let A be a simple artinian ring. Then $A \cong \text{End}_D(M)$, for a finite dimensional left vector space M over a division ring D .*

Proof. Let M be a minimal left ideal in A . By Prop. (3.25), $A \cong A_1 \subseteq \text{End}_Z(M)$, $D = \text{End}_A(M)$ is a division ring, and $A \subseteq \text{End}_D(M)$. By the Density Theorem (3.27), A_1 is a dense ring of linear transformations on M over D . It is sufficient to prove that $\dim_D(M) < \infty$. If this is not the case, there exists an infinite sequence x_1, x_2, \dots of linearly independent elements of M . For each $j = 1, 2, \dots$, let $I_j = \{a \in A_1 : ax_1 = \dots = ax_j = 0\}$. Then the $\{I_j\}$ are left ideals, and

$$I_1 \supseteq I_2 \supseteq \dots.$$

Moreover, the inclusions $I_j \supseteq I_{j+1}$ are strict, because of the Density Theorem, and we have contradicted the assumption that A is artinian. This completes the proof.

The converse of (3.28), that $M_n(D)$ is simple and artinian, and the uniqueness of D and $\dim_D(M)$ in Theorem 3.28, are sketched in Exercises 3.3 and 3.6.

§3C. Semisimple Algebras over Fields. The Theorems of Burnside and Frobenius-Schur

In this section we apply the results of §3A, B to investigate algebras which act on semisimple modules. It will not be necessary to assume that the algebras themselves are semisimple, and in fact we shall later apply these results to non-semisimple algebras.

Throughout this section, A denotes a finite dimensional algebra over a field K . All A -modules under consideration are assumed to be finitely generated over A , and hence are finite dimensional K -spaces. For such a left A -module M , $\text{End}_A(M)$ is a subalgebra of $\text{End}_K(M)$; thus $\text{End}_A(M)$ is a finite dimensional K -algebra, called the *centralizer* (or *commutant*) of M . Finally, we recall that there is a homomorphism of K -algebras $\lambda: A \rightarrow A_1 \subseteq \text{End}_K(M)$, given by $\lambda(a) = a_1$, $a \in A$, where $a_1(m) = am$ for $m \in M$.

(3.29) Definition. A left A -module M is *faithful* if $\text{ann } M = \{0\}$, where $\text{ann } M = \{a \in A : aM = 0\}$.

Evidently M is a faithful left A -module if and only if $\lambda: A \rightarrow A_1$ is an isomorphism of K -algebras, because $\text{ann } M = \ker \lambda$.

(3.30) Lemma. (*Bourbaki* [58], p. 26). *Let M be a faithful left A -module, and let $\{x_j : 1 \leq j \leq s\}$ be a set of generators of M as a module over $\text{End}_A(M)$. Then the map $_A A \rightarrow M^{(s)}$ defined by*

$$a \mapsto (ax_1, \dots, ax_s), \quad a \in A,$$

is a monomorphism of left A -modules.

Proof. The map is clearly an A -homomorphism. Suppose a is in the kernel. Then $ax_j = 0$ for all j , whence for every set $\{c_1, \dots, c_s\}$ of elements belonging to $\text{End}_A(M)$, we have

$$a(\sum c_j x_j) = \sum c_j (ax_j) = 0.$$

Because $M = \sum \text{End}_A(M)x_j$, we have $aM = 0$, and hence $a = 0$ by the hypothesis that M is faithful.

(3.31) Proposition. *Suppose M is a semisimple left A -module. Then A_I is a semisimple K -algebra. If M is a simple left A -module, then A_I is a simple K -algebra.*

Proof. To prove the first statement, we note that M is a faithful semisimple left A_I -module. Hence by Lemma 3.30, there is a left A_I -isomorphism of A_I onto a submodule of $M^{(s)}$ for some s . But $M^{(s)}$ is a semisimple A_I -module, whence so is A_I .

Turning to the proof of the second assertion, we observe that for each s , $M^{(s)}$ is a homogeneous semisimple left A_I -module. Therefore by (3.30) A_I is also a homogeneous left A_I -module, so A is a simple K -algebra by Theorem 3.22.

(3.32) Burnside's Theorem. *Let M be a simple left A -module, and suppose that $\text{End}_A(M) = K \cdot 1_M$. Then $A_I = \text{End}_K(M)$, that is, every K -endomorphism of M is realized by left multiplication by some element of A .*

Proof. By the Density Theorem, A_I is a dense ring of linear transformations on the vector space M over $D = \text{End}_A(M)$. Because $D = K \cdot 1_M$ and M is finite dimensional, it follows that $A_I = \text{End}_K(M)$, as required.

An important case where Burnside's Theorem can be applied is described by:

(3.33) Proposition. *Let M be a simple left A -module, and assume that the base field K is algebraically closed. Then $\text{End}_A(M) = K \cdot 1_M$.*

Proof. By Schur's Lemma, $\text{End}_A(M)$ is a division ring D , and $\dim_K(D)$ is finite. Let $\delta \in D$, and let $m(X) = \min. \text{pol.}_K(\delta)$. Then $m(X)$ is irreducible in

$K[X]$, since otherwise $m(X) = m_1(X)m_2(X)$, where both $m_1(X)$ and $m_2(X)$ have smaller degree than $m(X)$. But then $m_1(\delta) \neq 0$, $m_2(\delta) \neq 0$, whereas $m(\delta) = 0$, contradicting the fact that D is a division ring. Thus $m(X)$ must be irreducible. But then $m(X) = X - \alpha$ for some $\alpha \in K$, since K is algebraically closed. Therefore $\delta = \alpha \cdot 1_M \in K \cdot 1_M$, and the result is proved.

(3.34) Theorem. *A necessary and sufficient condition for a semisimple K -algebra A to have a two-sided Wedderburn decomposition of the form*

$$A = \bigoplus_{j=1}^m B_j, \text{ with } B_j \cong M_{n_j}(K), j = 1, \dots, m,$$

is that $\text{End}_A(M) = K \cdot 1_M$ for each simple left A -module M .

This result follows directly from Burnside's Theorem.

(3.35) Definition. A semisimple K -algebra satisfying the conditions of Theorem 3.34 is called a *split semisimple K -algebra*.

In particular, by (3.32)–(3.34), every semisimple K -algebra over an algebraically closed field K is a split semisimple K -algebra.

We obtain next some results about split semisimple group algebras, which provide a first link between the representation theory and the structure of groups.

We begin by introducing some useful terminology:

(3.36) Definition. Let A be a finite dimensional algebra over a field K . A set of representatives of the isomorphism classes of simple left A -modules will be called a *basic set* of simple A -modules.

Thus $\{M_1, \dots, M_r\}$ is a basic set of simple A -modules if every simple A -module is isomorphic to some M_j , $1 \leq j \leq r$, and if $M_i \neq M_j$ for $i \neq j$.

(3.37) Theorem. *Let G be a finite group, and K a field such that KG is a split semisimple K -algebra. Let $\{M_1, \dots, M_r\}$ be a basic set of simple KG -modules. Then*

$$(i) \quad |G| = \sum_{j=1}^r (\dim_K(M_j))^2.$$

(ii) *r equals the number of conjugacy classes in G .*

(iii) *The number of times M_j occurs as a composition factor of the left regular module $_{KG}(KG)$ is equal to $\dim_K(M_j)$.*

Sketch of Proof. The proofs of (i) and (iii) are immediate from the structure theorems (§3B). The proof of (ii) is based on the following:

(3.37a) Lemma. *Let R be a commutative ring, and G a finite group. The center $c(RG)$ of the group algebra RG is a free R -module, with an R -basis consisting of the class sums*

$$C_i = \sum_{x \in \mathfrak{C}_i} x,$$

where the $\{\mathfrak{C}_i\}$ are the conjugacy classes of G .

The proof of the lemma is left as an exercise for the reader (see CR(27.24)). For further discussion of Theorem 3.37iii, see Exercise 3.10.

We now use the Lemma to complete the proof of (ii) of Theorem 3.37, by showing that if KG is split semisimple, then $\dim_K(c(KG))$ is the number of isomorphism classes of simple left KG -modules. From the first Wedderburn Theorem, it follows that this number of isomorphism classes is the number of Wedderburn components. The center of KG is easily shown to be the direct sum of the centers of the Wedderburn components; since KG is split semisimple, each of these is one-dimensional over K , and the theorem follows.

(3.38) Definition. Let M be a left A -module of dimension n over K . A set of *matrix coordinate functions* of M is a set of n^2 functions $\{X_{ij}: 1 \leq i, j \leq n\}$ from A to K defined as follows: Let $T: A \rightarrow M_n(K)$ be a matrix representation afforded by M . The matrix coordinate function X_{ij} is the function that assigns to each $a \in A$ the (i, j) entry of the matrix $T(a)$.

We remark that different sets of matrix coordinate functions on M are obtained by varying the choice of a K -basis of M .

(3.39) Proposition. *Let M be a simple left A -module of dimension n over K , such that $\text{End}_A(M)$ consists of the scalar multiplications by elements of K . Let $\{X_{ij}\}$ be a set of matrix coordinate functions of M . Then the functions $\{X_{ij}\}$ are linearly independent over K .*

Sketch of Proof. We have to prove that if

$$\sum_{i,j} \xi_{ij} X_{ij}(a) = 0 \text{ for all } a \in A,$$

where the $\{\xi_{ij}\}$ are in K , then each $\xi_{ij} = 0$. By Burnside's Theorem, $A_I = \text{End}_K(M)$. Therefore for each pair (i, j) , $1 \leq i, j \leq n$, there exists an $a \in A$ such that $X_{ij}(a) = 1$, $X_{i'j'}(a) = 0$, $(i', j') \neq (i, j)$. The result follows at once.

(3.40) Corollary. *Let G be a group and $T: G \rightarrow GL(M)$ an irreducible representation of G on a finite dimensional space M . Assume that the centralizer of the set of matrices $\{T(a), a \in G\}$ in $\text{End}_K(M)$ is the set of scalar multiplications by elements of K . Then the functions $X_{ij}: G \rightarrow K$ defined as in (3.38) are linearly independent over K .*

Proof. Let A be the K -algebra generated by the matrices $\{T(g) : g \in G\}$. Then A consists of all K -linear combinations of these matrices, and so M is a faithful simple A -module for which $\text{End}_A(M) = K \cdot 1_M$. Now let $\{\xi_{ij}\} \in K$, and suppose that $\sum \xi_{ij} X_{ij}(g) = 0$ for all $g \in G$. It follows that $\sum \xi_{ij} X_{ij}(a) = 0$ for all $a \in A$, where the $\{X_{ij}\}$ are now a set of matrix coordinate functions defined on A . Then each $\xi_{ij} = 0$ by Prop. 3.39, and the result is proved.

(3.41) Frobenius-Schur Theorem. *Let $\{M_1, \dots, M_d\}$ be a basic set of simple left A -modules such that $\text{End}_A(M_k) = K$ for $1 \leq k \leq d$. For each k , $1 \leq k \leq d$, let $n_k = \dim_K(M_k)$ and let $\{X_{ij}^k : 1 \leq i, j \leq n_k\}$ be a set of matrix coordinate functions of M_k . Then the set of $\sum n_k^2$ matrix coordinate functions $\{X_{ij}^k\}$ is linearly independent over K .*

Sketch of Proof. Let the $\{\xi_{ij}^k\} \in K$ be such that

$$\sum_{k=1}^d \sum_{i,j=1}^{n_k} \xi_{ij}^k X_{ij}^k(a) = 0 \text{ for all } a \in A.$$

We must show that each $\xi_{ij}^k = 0$. Let $M = \coprod_{k=1}^d M_k$, and let $A_M \subseteq \text{End}_K(M)$ be the algebra consisting of all left multiplications by elements of A acting on M . Then M is a faithful semisimple left A_M -module, and $\{M_1, \dots, M_d\}$ are a basic set of simple left A -modules. By Burnside's Theorem 3.32, the Wedderburn component of A_M corresponding to M_k affords all K -endomorphisms on M_k , and annihilates each $M_{k'}$ for $k' \neq k$. It follows that for each triple $\{i, j, k\}$, where $1 \leq k \leq d$, $1 \leq i, j \leq n_k$, there exists an $a \in A$ such that

$$X_{ij}^k(a) = 1, \quad X_{i'j'}^{k'}(a) = 0 \text{ for all } \{i', j', k'\} \neq \{i, j, k\}.$$

This gives the desired result.

For E an extension field of K , and M a left A -module, we define

$$M^E = E \otimes_K M = \text{left } A^E\text{-module, where } A^E = E \otimes_K A.$$

(3.42) Definition. A left A -module M is *absolutely simple* if for every extension field $E \supseteq K$, M^E is a simple A^E -module. Correspondingly, an irreducible K -representation of A is *absolutely irreducible* if for every $E \supseteq K$, the representation obtained by extending the ground field from K to E remains irreducible.

Burnside's Theorem yields the following useful criterion for a left A -module M to be absolutely simple.

(3.43) Theorem. *A simple left A -module M is absolutely simple if and only if $\text{End}_A(M) = K \cdot 1_M$.*

Sketch of Proof. (See CR, pp. 202, 203). In case $\text{End}_A(M) = K \cdot 1_M$, Burnside's Theorem implies that $A_1 = \text{End}_K(M)$. Thus A_1 induces $(\dim_K M)^2$ linearly independent K -endomorphisms on M , for example, a set of matrix units relative to some K -basis. Then $(A^E)_1$ induces a set of matrix units on the extended vector space M^E , and hence M^E is a simple A^E -module. Conversely, suppose M^E is simple for all E . From Exercise 2.7 it follows that $\dim_K(\text{End}_A(M)) = \dim_E(\text{End}_{A^E}(M^E))$ for all extension fields E of K . Letting E be algebraically closed, we have $\dim_E(\text{End}_{A^E}(M^E)) = 1$, because M^E is assumed to be simple. Then $\dim_K(\text{End}_A(M)) = 1$, and the proof is completed.

Theorem 3.43 is especially important because it provides an intrinsic test for a module to be absolutely simple, involving only the computation of $\text{End}_A(M)$, rather than the consideration of extension fields.

§3D. The Morita Theorems

Wedderburn's Theorem 3.28 establishes a deep connection between the structure of a simple artinian ring A and the division ring D obtained as the centralizer $\text{End}_A(M)$ of a simple left A -module M . Moreover, the categories of left A -modules and left D -modules are essentially the same: every left A -module is a direct sum of copies of a single simple module, and the same is true for D -modules. Morita [58] showed that this phenomenon was a special case of a general criterion for the category of modules over one ring to be equivalent to the category of modules over another ring. Part of the idea is to analyze the familiar isomorphism of vector spaces

$$\text{End}_K(V) \cong \text{Hom}_K(V, K) \otimes_K V$$

from a more general point of view. In this section we follow unpublished notes of Bass, and present some of Morita's results in a form suitable for later applications.

We must first introduce some additional concepts from category theory (see §2 C). Let \mathcal{Q} and \mathcal{B} be categories, and let F, G be covariant functors from \mathcal{Q} to \mathcal{B} . A *natural transformation* $\tau: F \rightarrow G$ is a rule which assigns to each object $A \in \mathcal{Q}$ a map $\tau_A: F(A) \rightarrow G(A)$, such that for every map $f: A_1 \rightarrow A_2$ in \mathcal{Q} , the following diagram is commutative

$$\begin{array}{ccc} F(A_1) & \xrightarrow{\tau_{A_1}} & G(A_1) \\ F(f) \downarrow & & \downarrow G(f) \\ F(A_2) & \xrightarrow{\tau_{A_2}} & G(A_2). \end{array}$$

In case the maps τ_A are isomorphisms for all $A \in \mathcal{Q}$, τ is called a *natural equivalence of functors*.

The composite of two covariant functors $F: \mathcal{C} \rightarrow \mathcal{B}$ and $G: \mathcal{B} \rightarrow \mathcal{C}$ is well defined, and yields a covariant functor $G \circ F: \mathcal{C} \rightarrow \mathcal{C}$. The identity functor $\text{id}_{\mathcal{C}}$ of a category \mathcal{C} is the functor which assigns each object and map of \mathcal{C} to itself.

Definition. Two categories \mathcal{C} and \mathcal{B} are *equivalent* provided there exist covariant functors $F: \mathcal{C} \rightarrow \mathcal{B}$ and $G: \mathcal{B} \rightarrow \mathcal{C}$ such that the composites $G \circ F$ and $F \circ G$ are naturally equivalent to the identity functors in \mathcal{C} and \mathcal{B} , respectively. Equivalent categories (of modules) are often said to be *Morita equivalent*.

Properties of objects or maps in \mathcal{C} are *categorical* if these properties carry over to their images under arbitrary equivalences of categories.

In a category of modules ${}_A\mathfrak{M}$, a module P is called a *generator* of ${}_A\mathfrak{M}$ if every module $X \in {}_A\mathfrak{M}$ is a homomorphic image of a direct sum $\bigoplus_{i \in I} P_i$ of copies of P . Our first result is to characterize generators in categorical terms.

(3.44) Lemma. A module $P \in {}_A\mathfrak{M}$ is a generator of ${}_A\mathfrak{M}$ if and only if for any two distinct maps $g_1, g_2 \in \text{Hom}_A(N, N')$, there exists a map $f: P \rightarrow N$ such that $g_1 f \neq g_2 f$.

Proof. First suppose P is a generator, and let g_1 and g_2 be distinct maps from N to N' . Suppose that for every map $f: P \rightarrow N$ we have $g_1 f = g_2 f$. Since N is expressible as a homomorphic image of a direct sum of copies of P , it follows that for each $n \in N$ there exists a finite set of homomorphisms $f_i: P \rightarrow N$ such that $n = \sum f_i(p_i)$ for some elements p_i in P . Then $g_1 n = \sum g_1 f_i(p_i) = \sum g_2 f_i(p_i) = g_2 n$, contrary to our assumption. Therefore there must exist a map $f: P \rightarrow N$ with the required property that $g_1 f \neq g_2 f$.

Conversely, suppose that $P \in {}_A\mathfrak{M}$ has the property that for each pair of distinct maps $g_1, g_2 \in \text{Hom}_A(N, N')$, there exists an $f \in \text{Hom}_A(P, N)$ with $g_1 f \neq g_2 f$. We must show that P is a generator of ${}_A\mathfrak{M}$. Given $N \in {}_A\mathfrak{M}$, consider the set of all submodules $L \subseteq N$ which are images of direct sums of copies of P . This set is nonempty (since it contains the zero submodule of L), and for every increasing chain of such L 's, their union is again an image of a direct sum of copies of P . Hence by Zorn's Lemma, this set has a maximal element N^* , say. We wish to show that $N^* = N$; if $N^* \neq N$, then the natural surjection $h: N \rightarrow N/N^*$ is not the zero map. By hypothesis, there must then exist an $f \in \text{Hom}_A(P, N)$ such that $h f \neq 0$, that is, $f(P) \not\subseteq N^*$. But then $N^* + f(P)$ is a homomorphic image of a direct sum of copies of P , which contradicts the maximality of N^* . Thus $N^* = N$, that is, N is an image of a direct sum of copies of P , and the proof is finished.

Thus, if ${}_A\mathfrak{M}$ and ${}_B\mathfrak{M}$ are equivalent categories and P is a generator of ${}_A\mathfrak{M}$, then the image of P in ${}_B\mathfrak{M}$ is a generator of ${}_B\mathfrak{M}$. Other properties of modules preserved under category equivalences are described in the exercises.

(3.45) Lemma. *For a module P in the category ${}_A\mathfrak{M}$, the following are equivalent:*

- (i) P is a generator of ${}_A\mathfrak{M}$.
- (ii) $\sum_{u \in P'} u(P) = A$, where $P' = \text{Hom}_A(P, A)$.
- (iii) A is a direct summand of a direct sum of copies of P .

Proof. (i) \Rightarrow (ii): Let $I = \sum_{u \in P'} u(P)$. Then I is a left ideal in A . If $I \neq A$, then the natural map $h: A \rightarrow A/I$ is different from zero, whence by Lemma 3.44 there exists a map $g: P \rightarrow A$ such that $hg \neq 0$. On the other hand, $g(P) \subseteq I$ and hence $hg = 0$, contradicting the assumption that $I \neq A$, and proving that (i) \Rightarrow (ii).

(ii) \Rightarrow (iii): Let $M = \bigoplus_{u \in P'} P_u$, a direct sum of copies of P indexed by the set P' . The map $f: M \rightarrow A$, given by $f|_{P_u} = u$, is well defined and surjective by (ii). But A is projective in ${}_A\mathfrak{M}$, and hence A is a direct summand of M .

(iii) \Rightarrow (i): Let $\bigoplus_{i \in I} P_i = A \oplus A'$, and let $f: N \rightarrow N'$ be a nonzero map. Then there exists a map $\bar{g}: A \rightarrow N$ such that $f \bar{g} \neq 0$. The map \bar{g} can be extended to a map $g: \bigoplus P_i \rightarrow N$, in such a way that fg remains different from zero. For at least one index i , the restriction $fg|_{P_i}$ is nonzero. Hence $g|_{P_i}$ defines a map from P to N whose composite with f is not zero, which proves (i).

(3.46) Dual Basis Lemma. *A left module $P \in {}_A\mathfrak{M}$ is projective if and only if there exist elements $\{x_i\}$ in P and $\{u_i\} \in P'$, where $P' = \text{Hom}_A(P, A)$, such that*

- (a) for $x \in P$, $u_i(x) = 0$ for almost all i ;
- (b) for $x \in P$, $x = \sum u_i(x)x_i$.

Moreover, any generating set of P can be used as a set $\{x_i\}$ satisfying (a) and (b); conversely, any set $\{x_i\}$, for which (a) and (b) hold, is a set of generators.

Proof. Let $P = \sum_{i \in I} Ax_i$ be a projective A -module, and define a free A -module $F = \bigoplus_{i \in I} AX_i$ with free basis $\{X_i : i \in I\}$. Then there is a surjection $\varphi: F \rightarrow P$ given by $\varphi(X_i) = x_i$, $i \in I$. This surjection is split since P is A -projective. Thus we may view P as a direct summand of F , and φ as a projection map of F onto its summand P . For each $x \in P$, we can express x as an A -linear combination of the basis elements $\{X_i\}$ of F ,

$$x = \sum_{i \in I} a_i(x)X_i.$$

The coefficients $\{a_i(x)\}$ are uniquely determined, and vanish for almost all i because the above sum is finite. It follows that each coefficient function

$x \rightarrow a_i(x)$, $x \in P$, defines an element of P' . Using the fact that $\varphi(X_i) = x_i$ for $i \in I$, we have

$$x = \varphi(x) = \sum_{i \in I} a_i(x) \varphi(X_i) = \sum_{i \in I} a_i(x) x_i.$$

Finally, we note that in this construction, the $\{x_i\}$ are an arbitrary set of generators for P .

Conversely, given elements $x_i \in P$, $u_i \in P'$ for $i \in I$, such that (a) and (b) hold, we may form the free module $F = \bigoplus_{i \in I} A X_i$. Then define $\varphi: F \rightarrow P$ by $\varphi(X_i) = x_i$, $i \in I$, extended by linearity to all of F . By (b), φ is a surjection and $\{x_i\}$ is a generating set for P . Now we define a map $\psi: P \rightarrow F$ by

$$\psi(x) = \sum u_i(x) X_i, \quad x \in P.$$

Then $\psi \in \text{Hom}_A(P, F)$, and is such that $\varphi\psi = 1_P$, since for $x \in P$ we have $x = \sum u_i(x) x_i = \varphi\psi(x)$. Thus P is a direct summand of F , hence is projective. This completes the proof of the lemma.

Let M be a left A -module, and consider the ring $\text{End}_A(M)$, where multiplication is defined as usual by composition of maps: for $u, u' \in \text{End}_A(M)$,

$$(uu')m = u(u'(m)), \quad m \in M.$$

It is convenient to introduce the opposite ring $B = \{\text{End}_A(M)\}^\circ$, having the same elements as $\text{End}_A(M)$, but with multiplication reversed. The left $\text{End}_A(M)$ -module M then becomes a right B -module: for $u, u' \in B$ and $m \in M$, we have

$$m(uu') = u'(u(m)) = u'(mu) = (mu)u'.$$

Thus, the left A -module M becomes a left A -, right $\{\text{End}_A(M)\}^\circ$ -bimodule: $M \in {}_A\mathfrak{M}_B$. We describe this situation by saying that the endomorphism ring $\text{End}_A(M)$ acts from the opposite side from the action of A , and we shall adopt this convention for the remainder of this section. In a similar fashion, each right A -module N is an $(\text{End}_A(N), A)$ -bimodule.

The situation to which the Morita Theorems apply involves the following data: a ring A , a module $P \in {}_A\mathfrak{M}$, and the ring $B = \{\text{End}_A(P)\}^\circ$ acting from the right on P . Thus $P \in {}_A\mathfrak{M}_B$, as explained above. We set $Q = \text{Hom}_A(P, A)$; then

$$Q = \text{Hom}_A({}_A P, {}_A A_A) \in {}_B\mathfrak{M}_A,$$

by the discussion in §2. There are compositions of A and B on Q satisfying

$$(bu)a = [u(xb)]a \text{ for } a \in A, b \in B, u \in Q, x \in P.$$

For the following discussion, we consistently let $a \in A$, $b \in B$, $x, y, z \in P$, $u, v, w \in Q$.

We now define biadditive maps

$$(\ , \): P \times Q \rightarrow A, [\ , \]: Q \times P \rightarrow B,$$

by the rules

$$(3.47) \quad (x, u) = xu, y[u, x] = (y, u)x.$$

Then $(\ , \)$ is a B -balanced map, that is,

$$(xb, u) = (x, bu) \text{ for all } x, b, u.$$

It therefore defines a homomorphism

$$(3.48) \quad (\): P \otimes_B Q \rightarrow A$$

of (A, A) -bimodules, by $(x \otimes u) = (x, u)$.

We can now reformulate Lemma 3.45 thus:

(3.49) Lemma. *Let $P \in {}_A\mathfrak{M}$. The following are equivalent:*

- (i) *P is a generator of ${}_A\mathfrak{M}$.*
- (ii) *The homomorphism (3.48) of (A, A) -bimodules is surjective.*
- (iii) *A is a direct summand of a direct sum of copies of P .*

The map $[\ , \]$ is easily shown to be A -balanced, and defines a homomorphism of (B, B) -bimodules

$$[\]: Q \otimes_A P \rightarrow B, \text{ given by } [u \otimes x] \rightarrow [u, x] \text{ for all } u, x.$$

The maps $(\ , \)$ and $[\ , \]$ also satisfy the relation

$$(3.50) \quad [u, x]v = u(x, v) \text{ for all } u, x, v,$$

as can be seen by letting both sides act on an element $y \in P$ and using (3.47).

We may now restate the Dual Basis Lemma 3.46 in terms of the map $[\ , \]$, as follows:

(3.51) Lemma. *Let $P \in {}_A\mathfrak{M}$, and let $[\ , \]$ be defined as in (3.47). Then P is finitely generated and projective if and only if the homomorphism of (B, B) -bimodules $[\]: Q \otimes_A P \rightarrow B$ is surjective.*

Proof. The image of $[\]$ is a two-sided ideal in B ; hence $[\]$ is surjective if and only if the identity element 1 of B belongs to the image of $[\]$. Statement

(b) in the Dual Basis Lemma, that $x = \sum u_i(x)x_i$, is equivalent to the assertion that

$$x = \sum (x, u_i)x_i = \sum x[u_i, x_i],$$

and hence to the condition that $1 = \sum [u_i, x_i]$. The proof follows easily from these remarks.

Returning to the ideas in the introductory paragraph of this section, we note that the map $[,]: Q \times P \rightarrow B$ generalizes the K -bilinear map of vector spaces $\text{Hom}_K(V, K) \times V \rightarrow \text{End}_K(V)$. This latter map is used in proving that $\text{Hom}_K(V, K) \otimes_K V \cong \text{End}_K(V)$ for a f.d. vector space V over a field K .

(3.52) Definition. A module $P \in {}_A\mathcal{M}$ is a *progenerator* (in ${}_A\mathcal{M}$) if and only if P is a f.g. projective generator of ${}_A\mathcal{M}$.

(3.53) Definition. A *Morita context* consists of rings A, B , bimodules $P \in {}_A\mathcal{M}_B$, $Q \in {}_B\mathcal{M}_A$, and biadditive, balanced maps $(,): P \times Q \rightarrow A$ and $[,]: Q \times P \rightarrow B$ which define homomorphisms of bimodules

$$(): P \otimes_B Q \rightarrow A \text{ and } []: Q \otimes_A P \rightarrow B$$

such that

$$(x \otimes u) = (x, u), [u \otimes x] = [u, x],$$

and satisfy the conditions:

$$y[u, x] = (y, u)x, \text{ and } [u, x]v = u(x, v),$$

for all $x, y \in P$, and $u, v \in Q$.

The situation we have considered, with $B = \{\text{End}_A(P)\}^\circ$, $Q = \text{Hom}_A(P, A)$, etc., is a special case of a Morita context. The main theorem below shows that when the bimodule homomorphisms $()$ and $[]$ are surjective, the Morita context coincides with the example we have constructed. There are many other consequences as well, which are handled most efficiently using the general concept of a Morita context. The formulation of the main theorem and its proof are due to Bass.

(3.54) Morita Theorem. Let A and B be rings, and let $\{P \in {}_A\mathcal{M}_B, Q \in {}_B\mathcal{M}_A, (,), [,]\}$ be a Morita context for which the bimodule homomorphisms $()$ and $[]$ are surjective. Then the following statements hold:

- (i) P is a progenerator for ${}_A\mathcal{M}$ and \mathcal{M}_B ; Q is a progenerator for \mathcal{M}_A and ${}_B\mathcal{M}$.

(ii) Both $(\)$ and $[\]$ are isomorphisms of bimodules.

(iii) There are bimodule isomorphisms

$$Q \cong \text{Hom}_A({}_A P, {}_A A) \cong \text{Hom}_B(P_B, B_B),$$

$$P \cong \text{Hom}_A(Q_A, A_A) \cong \text{Hom}_B({}_B Q, B_B).$$

(iv) (Double Centralizer Property). There are ring isomorphisms

$$A \cong \{\text{End}_B(Q)\}^\circ \cong \text{End}_B(P), B \cong \text{End}_A(Q) \cong \{\text{End}_A(P)\}^\circ.$$

(v) The covariant functors

$$P \otimes_B * : {}_B \mathcal{M} \rightarrow {}_A \mathcal{M} \text{ and } Q \otimes_A * : {}_A \mathcal{M} \rightarrow {}_B \mathcal{M}$$

define an equivalence of categories between ${}_A \mathcal{M}$ and ${}_B \mathcal{M}$. Similarly, $* \otimes_A P : \mathcal{M}_A \rightarrow \mathcal{M}_B$ and $* \otimes_B Q : \mathcal{M}_B \rightarrow \mathcal{M}_A$ define an equivalence of categories between \mathcal{M}_A and \mathcal{M}_B .

(vi) The set of A -submodules of P , ordered by inclusion, is isomorphic (as a partially ordered set) to the set of left ideals in B , ordered by inclusion. The (A, B) -submodules of P correspond to two-sided ideals of B . Similar statements follow from symmetry. In particular, A and B have isomorphic inclusion-ordered sets of two-sided ideals.

Remarks. (a) The inclusion-ordered set of A -submodules of P is a lattice, with $P_1 \wedge P_2 = P_1 \cap P_2$ and $P_1 \vee P_2 = P_1 + P_2$. It is immediate that isomorphisms of partially ordered sets, in this situation, define lattice isomorphisms (preserving $P_1 \wedge P_2$ and $P_1 \vee P_2$), so that the isomorphisms in (vi) are in fact lattice isomorphisms.

(b) When A is an algebra over a commutative ring R (see §1), a left A -module P becomes an R -module, and the composition $A \times P \rightarrow P$ is R -bilinear. Then $B = \text{End}_A(P)$ is also an R -algebra, and all isomorphisms and equivalences in the main theorem are easily seen to be compatible with the action of R .

Proof. (Remember our agreement to write $a \in A$, $b \in B$, $x, y, z \in P$, $u, v, w \in Q$.)

(i) Each element $u \in Q$ defines an A -homomorphism $(\ , u) : P \rightarrow A$. Since $(\ , \)$ is surjective, there exist elements $\{x_i\} \in P$, $\{u_i\} \in Q$, such that $\Sigma(x_i, u_i) = 1$. By Lemma 3.49, it follows that P is a generator for ${}_A \mathcal{M}$. In exactly the same way, using $[\ ,]$ instead of $(\ , \)$, it follows that P is a generator for \mathcal{M}_B . Since $[\ ,]$ is surjective, there exist $v_j \in Q$, $y_j \in P$ such that $\Sigma[v_j, y_j] = 1$. Using the

relations between $(,)$ and $[,]$ in a Morita context and Lemma 3.51, it follows that P is a f.g. projective left A -module. Applying the same lemma to P_B , using the fact that $\Sigma(x_i, u_i) = 1$, we conclude that P is a f.g. projective right B -module. We have now proved the statement (i) for P , and the corresponding statements for Q follow by symmetry.

For the rest of the proof, we assume that elements $x_i \in P$, $u_i \in Q$, etc., have been chosen so that

$$\sum (x_i, u_i) = 1 \text{ in } A, \quad \sum [v_j, y_j] = 1 \text{ in } B.$$

(ii) We prove that the kernel of $()$ is zero. Suppose $z_k \in P$, $w_k \in Q$ are such that $(\sum z_k \otimes w_k) = 0$. Then

$$\begin{aligned} \sum z_k \otimes w_k &= \left(\sum_k z_k \otimes w_k \right) \sum_i (x_i, u_i) = \sum_{i, k} z_k \otimes [w_k, x_i] u_i \\ &= \sum_{i, k} z_k [w_k, x_i] \otimes u_i = \sum_i \sum_k (z_k, w_k) x_i \otimes u_i = 0. \end{aligned}$$

Similarly, using the fact that $\sum [y_j, v_j] = 1$ in B , it follows that the kernel of $[]$ is zero. Since $()$ and $[]$ are surjective by assumption, they are isomorphisms, and (ii) is proved.

(iii) We prove first that $Q \cong \text{Hom}_A(P, {}_A A)$. As we have already remarked, the map $\varphi: u \rightarrow (, u)$, takes Q into $\text{Hom}_A(P, {}_A A)$. Suppose $(x, u) = 0$ for all $x \in P$. Then $u = 1u = \sum [v_j, y_j] u = \sum v_j (y_j, u) = 0$, so φ is injective. Now let $f \in \text{Hom}_A(P, {}_A A)$; we shall prove that $f = (\sum v_j (y_j f))$. We have

$$\begin{aligned} (x, \sum v_j (y_j f)) &= \sum (x, v_j) (y_j f) = [\sum (x, v_j) y_j] f \\ &= \{\sum x [v_j, y_j]\} f = xf, \end{aligned}$$

as required. Finally, the map φ is a (B, A) -homomorphism because

$$(x, bua) = (xb, u)a.$$

In exactly the same way, it is shown that there exist isomorphisms of bimodules

$$Q \cong \text{Hom}_B(P_B, B_B) \text{ via } u \rightarrow [u,];$$

$$P \cong \text{Hom}_B(Q_B, {}_B B) \text{ via } x \rightarrow [, x];$$

$$P \cong \text{Hom}_A(Q_A, {}_A A) \text{ via } x \rightarrow (x,).$$

(iv) The map $a \mapsto a_l$, where a_l denotes left multiplication by a on P , is a homomorphism of rings $A \rightarrow \text{End}_B(P)$, because P is an (A, B) -bimodule. We

shall prove this map is an isomorphism. Suppose $ax=0$ for all $x \in P$. Then $a=a \cdot 1=a\Sigma(x_i, u_i)=\Sigma(ax_i, u_i)=0$, and the map $a \rightarrow a_1$ is injective. Now let $s \in \text{End}_B(P)$. We prove that $s=(\Sigma(sx_i, u_i))_l$. For $x \in P$ we have

$$\begin{aligned}\Sigma(sx_i, u_i)x &= \Sigma(sx_i)[u_i, x] = s\{\Sigma x_i[u_i, x]\} \\ &= s\{\Sigma(x_i, u_i)x\} = sx,\end{aligned}$$

and we have proved the first isomorphism. Similarly $B \cong \text{End}_A(Q)$ via left multiplication by elements of B . As we saw in our discussion of the examples of a Morita context, there is a homomorphism of rings $A \rightarrow \{\text{End}_B(BQ)\}^\circ$, given by right multiplication. Just as in the case of the first isomorphism, we see that it is an isomorphism of rings; similarly, $B \cong \{\text{End}_A(AP)\}^\circ$.

(v) Let F be the functor $Q \otimes_A * : {}_A\mathfrak{M} \rightarrow {}_B\mathfrak{M}$, and G the functor $P \otimes_B * : {}_B\mathfrak{M} \rightarrow {}_A\mathfrak{M}$. For $M \in {}_A\mathfrak{M}$, we have

$$\begin{aligned}GF(M) &= P \otimes_B (Q \otimes_A M) \\ &\cong (P \otimes_B Q) \otimes_A M \\ &\cong A \otimes_A M \cong M.\end{aligned}$$

Here, the crucial point is the bimodule isomorphism $P \otimes_B Q \cong A$ established in (ii). Similarly $FG(N) \cong N$ for all $N \in {}_B\mathfrak{M}$, again using (ii). The isomorphisms are natural in M and N , and consequently define an equivalence of categories. The same arguments, again based on (ii), establish an equivalence of categories between \mathfrak{M}_A and \mathfrak{M}_B , completing the proof of (v).

(vi) Finally, the functor $G : {}_B\mathfrak{M} \rightarrow {}_A\mathfrak{M}$ defines an equivalence of categories, with $G(B)$ naturally isomorphic to P . It follows easily that there is an isomorphism (of partially ordered sets) between the inclusion-ordered set of left ideals of B ($= B$ -submodules of B) and the corresponding inclusion-ordered set of A -submodules of $G(B)$ ($= P$). This isomorphism is a lattice isomorphism, by the remark following the statement of the Theorem. This completes the proof.

The above result will be adequate for the applications in this book; however it is by no means the last word on the Morita Theorems. For further results on them, see Morita [58], MO §16, or Anderson-Fuller [73]. Also note the similarities between parts of the preceding proof and the correspondences, given in CR §66, between submodules and ideals in endomorphism rings.

As an illustration, we give another version of the Wedderburn Theorem on the structure of simple artinian rings; the previous proof in §3C made use of the Density Theorem. The argument to follow is essentially a special case of the proof of the double centralizer property given in CR, pp. 175–177.

(3.55) Corollary. *Let A be a simple left artinian ring, and let P be a simple left A -module. Let $D = \{\text{End}_A(P)\}^\circ$, so that $P \in {}_A\mathcal{M}_D$. Then D is a division ring, P is finite dimensional over D , and $A \cong \text{End}_D(P_D)$.*

Proof. From the first part of §3, the ring A is isomorphic to a direct sum of a finite number of copies of P , and P is finitely generated and projective. By Lemma 3.45, P is a progenerator in ${}_A\mathcal{M}$. Letting $Q = \text{Hom}_A({}_AP, {}_AA)$, we have a Morita context with $(,)$ and $[,]$ defined as in (3.47). Moreover, by (3.49) and (3.51), the homomorphisms of bimodules

$$(): P \otimes_B Q \rightarrow A \text{ and } [] : Q \otimes_A P \rightarrow B$$

are surjective. The main theorem (3.54) can now be applied to show that P is also a progenerator in \mathcal{M}_D , and hence $\dim_D P$ is finite. The double centralizer property $\text{End}_D(P_D) \cong A$ follows from part (iv) of the main theorem, and the proof is complete.

We recommend to the reader the instructive task of determining what the other parts of the Morita Theorem contribute to the situation in Corollary 3.55.

Example. Another frequently-used special case of the Morita Theorem is as follows (with proofs of the assertions left to the reader). Let A be a ring and P a free left A -module with a finite basis $\{X_1, \dots, X_n\}$. Then P is a progenerator in ${}_A\mathcal{M}$. Let $B = \{\text{End}_A(P)\}^\circ$. Then B is isomorphic to the matrix ring $M_n(A)$, via the map $b \mapsto (a_{ij})$, where $x_i b = \sum_j a_{ij} x_j$, $b \in B$, $a_{ij} \in A$. Let $Q = \text{Hom}_A({}_AP, {}_AA)$. Then $P \in {}_A\mathcal{M}_B$, $Q \in {}_B\mathcal{M}_A$, and $\{A, B, P, Q\}$ define a Morita context for which the maps $()$ and $[]$, defined as in (3.48), etc., are surjective. It follows that for $M \in {}_A\mathcal{M}$, $N \in {}_B\mathcal{M}$,

$$M \rightarrow Q \otimes_A M, \text{ and } N \rightarrow P \otimes_B N,$$

define an equivalence of categories between ${}_A\mathcal{M}$ and ${}_{M_n(A)}\mathcal{M}$.

§3E. Tensor Products of Simple Algebras and Modules. The Skolem-Noether Theorem

We shall apply the Morita Theorem 3.54 to prove some basic results about tensor products of simple modules and algebras. These will provide a foundation for the theory of separable algebras and splitting fields to be developed in §7. Throughout this section K denotes a field; though our interest here is mainly with finite dimensional K -algebras and modules, we shall prove the principal results in somewhat greater generality, which will be needed later.*

*For example, completions of fields, algebras, and modules are not usually f.g. over the ground field.

We begin with a new proof of a special case of a result of Azumaya and Nakayama ([44], [47]) (see also Jacobson [56], Bourbaki [58].)

(3.56) Proposition. *Let A and B be K -algebras, and let M be a simple left A -module, and N a simple left B -module. Assume that A and B are left artinian rings (but not necessarily f.d./ K). Let D and E be the division algebras over K defined by*

$$D = \{\text{End}_A(M)\}^\circ, E = \{\text{End}_B(N)\}^\circ.$$

Letting \otimes denote \otimes_K , we obtain bimodule structures

$$M \in {}_A\mathfrak{M}_D, N \in {}_B\mathfrak{M}_E, M \otimes N \in {}_{A \otimes B}\mathfrak{M}_{D \otimes E}.$$

Then the following statements are valid:

- (i) $M \otimes N$ is a free right $(D \otimes E)$ -module with a finite basis.
- (ii) Let $(A \otimes B)_l$ denote the K -algebra of left multiplications on $M \otimes N$ by the elements of $A \otimes B$. Then

$$\text{End}_{D \otimes E}(M \otimes N) = (A \otimes B)_l.$$

- (iii) The lattice of left $(A \otimes B)$ -submodules of $M \otimes N$ is isomorphic to the lattice of left ideals in $D \otimes E$. (See §3D for a discussion of lattice isomorphisms.)

- (iv) $\text{End}_{A \otimes B}(M \otimes N)$ is the algebra of right multiplications on $M \otimes N$ by elements of $D \otimes E$.

Proof. We begin by proving (i); it clearly implies that $M \otimes N$ is a progenerator in $\mathfrak{M}_{D \otimes E}$. In the example of a Morita context given in §3D, we shall let $D \otimes E$ play the role of the ring A in §3D, and the right $(D \otimes E)$ -module $M \otimes N$ play the role of the left A -module P in §3D. We shall deduce from (ii) that the algebra $(A \otimes B)_l$ occurring here corresponds to the ring $B = \{\text{End}_A(P)\}^\circ$ of §3D. The remaining statements (iii) and (iv) will then follow from Morita's Theorem 3.54.

- (i) The vector spaces M_D and N_E are finite dimensional over the division rings D and E , respectively, by the proof of (3.28), since A and B are left artinian. If $M \cong D^{(r)}$ and $N \cong E^{(s)}$, then clearly

$$M \otimes N \cong D^{(r)} \otimes E^{(s)} \cong (D \otimes E)^{(rs)},$$

so $M \otimes N$ is a free $(D \otimes E)$ -module on rs generators, and is thus a progenerator in $\mathfrak{M}_{D \otimes E}$.

(ii) Let $\{m_i\}$ be a D -basis of M_D , and $\{n_j\}$ an E -basis of N_E . The above shows that the elements $\{m_i \otimes n_j\}$ form a $(D \otimes E)$ -basis of $M \otimes N$. Let $f \in \text{End}_{D \otimes E}(M \otimes N)$. It is then sufficient to prove the existence of an element $c \in A \otimes B$ such that

$$c(m_i \otimes n_j) = f(m_i \otimes n_j)$$

for all i and j . We can write

$$f(m_i \otimes n_j) = \sum_{k,l} m_k d_{ki} \otimes n_l e_{lj}$$

with $d_{ki} \in D$ and $e_{lj} \in E$. By the Density Theorem again, there exist elements $a_{ki} \in A$ and $b_{lj} \in B$ such that

$$a_{ki}m_i = m_k d_{ki}, a_{ki}m_{i'} = 0, i' \neq i, \text{ and } b_{lj}n_j = n_l e_{lj}, b_{lj}n_{j'} = 0, j' \neq j.$$

Then

$$\left(\sum_{k,l} a_{ki} \otimes b_{lj} \right) (m_i \otimes n_j) = f(m_i \otimes n_j),$$

and

$$\left(\sum_{k,l} a_{ki} \otimes b_{lj} \right) (m_{i'} \otimes n_{j'}) = 0 \text{ if } (i, j) \neq (i', j').$$

It follows that the element

$$c = \sum_{i,j} \sum_{k,l} a_{ki} \otimes b_{lj} \in A \otimes B$$

has the property that $c(m_i \otimes n_j) = f(m_i \otimes n_j)$ for all i and j , and (ii) is proved.

As we explained earlier, (iii) and (iv) now follow from Theorem 3.54, and the proposition is proved.

We shall now apply (3.56) to the study of tensor products of simple algebras. Let A be a K -algebra, not necessarily finite dimensional over K . For $a \in A$, let a_l denote left multiplication by a on A , and a_r right multiplication. Then there are K -algebra homomorphisms

$$A \rightarrow A_l \subseteq \text{End}_K(A), A^o \rightarrow A_r \subseteq \text{End}_K(A),$$

where A^o is the opposite ring of A , and $A_l = \{a_l : a \in A\}$, $A_r = \{a_r : a \in A\}$. The associativity of A implies that $a_l b_r = b_r a_l$ for all $a, b \in A$. Therefore A becomes

a left $(A \otimes_K A^\circ)$ -module upon defining

$$(a \otimes b^\circ)x = (a, b_r)x = axb, \quad a, b, x \in A.$$

(3.57) Lemma. $\text{End}_{A \otimes_K A^\circ}(A) = \{c(A)\}_I$, where $c(A)$ is the center of A .

Proof. We are assuming, as usual, that A contains an identity 1. The inclusion one way is clear. Conversely, suppose $f \in \text{End}_{A \otimes_K A^\circ}(A)$. Then $f=f(1)$, by an easy computation, and one then checks that $f(1) \in c(A)$ since $f \in \text{End}_{A \otimes_K A^\circ}(A)$.

(3.58) Lemma. Let A be a K -algebra. Then

- (i) A is a simple* K -algebra if and only if A is a simple left $(A \otimes_K A^\circ)$ -module.
- (ii) If A is a simple K -algebra, then its center $c(A)$ is a field.

Proof. The two-sided ideals in A are precisely the $(A \otimes_K A^\circ)$ -submodules of A , proving the first statement. For the second, by (i) we know that A is a simple $(A \otimes_K A^\circ)$ -module; hence $\text{End}_{A \otimes_K A^\circ}(A)$ is a division algebra over K , by Schur's Lemma. From Lemma 3.57 it follows that $\text{End}_{A \otimes_K A^\circ}(A) \cong c(A)$, whence $c(A)$ is a field, as required.

(3.59) Definition. A simple K -algebra A is a central simple K -algebra if A is f.d./ K , and the natural embedding $K \rightarrow c(A)$ gives an isomorphism $K \cong c(A)$.

(3.60) Theorem. Let A and B be simple K -algebras, with centers S and T , respectively. Let \otimes denote \otimes_K . Then the following statements hold:

- (i) If both $\dim_K A$ and $\dim_K B$ are finite, then the lattice of two-sided ideals in $A \otimes_K B$ is isomorphic to the lattice of ideals in the commutative ring $S \otimes T$.
- (ii) Let A and B satisfy the hypothesis of (i) above. Then $A \otimes B$ is semisimple if and only if $S \otimes T$ is semisimple.
- (iii) If A is a central simple K -algebra, and B is an arbitrary simple K -algebra (not necessarily f.d./ K), then $A \otimes B$ is simple with center $1 \otimes T$.
- (iv) If A and B are central simple K -algebras, then so is $A \otimes B$.

Proof. (i) By (3.58), A is a simple left $(A \otimes_K A^\circ)$ -module, and

$$\text{End}_{A \otimes_K A^\circ}(A) \cong S$$

*This means that A is a simple ring; we do not assume here that $\dim_K A$ is finite.

by (3.57). Since S is a commutative K -algebra, we can view A as an $(A \otimes A^\circ, S)$ -bimodule. Likewise, B is a $(B \otimes B^\circ, T)$ -bimodule. We conclude from (3.56) that the lattice of $(A \otimes A^\circ, B \otimes B^\circ)$ -submodules of $A \otimes B$ is isomorphic to the lattice of ideals in the commutative K -algebra $S \otimes T$. But on the other hand, the $(A \otimes A^\circ, B \otimes B^\circ)$ -submodules of $A \otimes B$ are precisely the two-sided ideals of $A \otimes B$. This proves assertion (i). Statement (ii) is an immediate consequence of (i).

(iii) We first determine the center $c(A \otimes B)$ of $A \otimes B$. Clearly $1 \otimes T \subseteq c(A \otimes B)$. Now let $\sum a_i \otimes b_i \in c(A \otimes B)$, where we may assume that the elements $\{b_i\}$ are linearly independent over K . Then for all $a \in A$, we have

$$0 = (a \otimes 1) \left(\sum a_i \otimes b_i \right) - \left(\sum a_i \otimes b_i \right) (a \otimes 1) = \sum (aa_i - a_i a) \otimes b_i.$$

Therefore $aa_i - a_i a = 0$ for all $a \in A$ and each i , so each $a_i \in c(A)$. Identifying the center of A with K , it follows that $\sum a_i \otimes b_i \in 1 \otimes B$, and hence $\sum a_i \otimes b_i \in 1 \otimes T$.

We now turn to the question of the simplicity of $A \otimes B$. By (3.58) and the Density Theorem, $A \otimes A^\circ$ is a dense algebra of K -linear transformations on A . If $z = \sum x_j \otimes y_j^\circ \in A \otimes A^\circ$, then $z \otimes 1$ acts on $A \otimes B$ by the formula

$$(z \otimes 1)(a \otimes b) = za \otimes b = \sum x_j a y_j^\circ \otimes b = \sum_j (x_j \otimes 1)_r (y_j^\circ \otimes 1)_l (a \otimes b).$$

It follows that $zI \subseteq I$ for each two-sided ideal I in $A \otimes B$ and each $z \in A \otimes A^\circ$.

To complete the proof of (iii), it suffices to show that every two-sided ideal I in $A \otimes B$ is of the form $I = A \otimes I'$ for some two-sided ideal I' in B . Let us identify A with $A \otimes 1$, and B with $1 \otimes B$, and set $I' = I \cap B$. Then I' is a two-sided ideal in B , and clearly $AI' \subseteq I$. Now let $\sum a_i b_i \in I$, where we may assume that the elements $\{a_i\}$ are linearly independent over K . By the density of $A \otimes A^\circ$ acting on A , for each fixed index i_0 , $1 \leq i_0 \leq m$, there exists an element $z_0 \in A \otimes A^\circ$ such that $z_0(a_{i_0}) = 1$, $z_0(a_i) = 0$ for $i \neq i_0$. Since $z_0 I \subseteq I$ for each z_0 , we obtain

$$z_0 \left(\sum a_i b_i \right) = b_{i_0} \in I \cap B = I'.$$

Hence $\sum a_i b_i \in AI'$, which proves that $I = AI'$, and establishes (iii).

Statement (iv) is a direct consequence of (iii), and the theorem is proved.

(3.61) Corollary. *Let A be a central simple K -algebra, and let E be an arbitrary extension field of K . Then $E \otimes_K A$ is a central simple E -algebra.*

To conclude this section, we apply our results to the study of automorphisms of central simple algebras. Let A be a K -algebra, and let $a \in A$ be an invertible element. The map $x \mapsto axa^{-1}$, $x \in A$, is an *inner automorphism* of A . It is a K -algebra automorphism, and it leaves fixed each element in the center

of A (compare this concept with that of inner automorphisms of groups). However, in contrast with the situation occurring in group theory, we shall prove here that when A is a central simple K -algebra, then every automorphism of A which acts as the identity on $c(A)$ must be an inner automorphism. This is a consequence of the following basic result:

(3.62) Skolem-Noether Theorem. *Let B be a simple K -subalgebra of a central simple K -algebra A . Then every isomorphism of K -algebras $\varphi: B \rightarrow B' \subseteq A$ can be extended to an inner automorphism of A , that is, there exists an element $a \in A$ such that*

$$\varphi(b) = aba^{-1} \text{ for all } b \in B.$$

Proof. We let \otimes stand for \otimes_K throughout the proof. Let M be a simple left A -module, and let $D = \text{End}_A(M)$. Then D is a division algebra with center $K \cdot 1_M$, and by (3.60), $B \otimes D$ is a simple K -algebra, which acts on M according to the rule

$$(b \otimes d)m = b(dm), \quad b \in B, d \in D, m \in M.$$

Using the automorphism φ , we define a second left $(B \otimes D)$ -module M' , whose underlying vector space over K is M , and with the action of $B \otimes D$ given by

$$(b \otimes d)m' = \varphi(b)(dm), \quad b \in B, d \in D, m' \in M'.$$

Then M and M' are left modules over the finite dimensional simple K -algebra $B \otimes D$, and have the same dimension over K . From §3B, it follows that there exists an isomorphism of $(B \otimes D)$ -modules $\theta: M \cong M'$. Because $\theta \in \text{End}_{D}(M)$, it follows from (3.28) that θ is a left multiplication a , for some element $a \in A$. The element a is invertible in A because θ is an isomorphism. Finally, since $\theta (= a)$ is a $(B \otimes D)$ -isomorphism, we have

$$a(b(dm)) = \varphi(b)d(am) \text{ for all } b \in B, d \in D, m \in M.$$

Taking $d = 1$, and using the fact that A acts faithfully on M , it follows that $ab = \varphi(b)a$, so $\varphi(b) = aba^{-1}$, for all $b \in B$, completing the proof.

(3.63) Corollary. *Let A be a central simple K -algebra, and let φ be an automorphism of A which fixes each element of $K \cdot 1$. Then φ is an inner automorphism.*

§3. Exercises

1. Let D be a division ring, D° its opposite ring, and $\delta \rightarrow \delta^\circ$, $\delta \in D$, an anti-isomorphism from D to D° . Let $V = \bigoplus_{i=1}^n Dv_i$ be a left vector space over D with basis

$\{v_i\}$. Let $A = \text{End}_D(V)$, and for each $a \in A$ let

$$av_j = \sum_{i=1}^n \alpha_{ij} v_i, \quad \alpha_{ij} \in D, \quad 1 \leq j \leq n.$$

Prove that the map $a \rightarrow (\alpha_{ij}^\circ)$ gives a ring isomorphism

$$\text{End}_D(V) \cong M_n(D^\circ).$$

Show also that V is a simple left A -module.

2. Let A be a simple artinian ring, M a simple left A -module, and let $D = \text{End}_A(M)$. Let D° be as above. Prove that $A \cong M_n(D^\circ)$ where n is the dimension of M as left vector space over the division ring D .

3. Let $A = M_n(E)$ for a division ring E . For each i , $1 \leq i \leq n$, let L_i be the set of all matrices in A whose entries are zero except in the i -th column.

(a) Prove that $\{L_1, \dots, L_n\}$ are A -isomorphic minimal left ideals, such that $A = \bigoplus_{i=1}^n L_i$.

(b) Prove that A is a left and right artinian simple ring, and that the center of A consists of all scalar matrices αI , where α ranges over the center of E .

(c) Let M be a simple left A -module, and $D = \text{End}_A(M)$. Prove that $D \cong E^\circ$, and that $\dim_D M = n$.

4. Prove that a ring A is left semisimple if and only if it is right semisimple. In particular, show that a semisimple ring is both left and right artinian.

[Hint: Use (3.22) and (3.28).]

5. Let A be a semisimple ring, and M_1, \dots, M_s a basic set of simple left A -modules. Let $D_i = \text{End}_A(M_i)$, $1 \leq i \leq s$. Prove that D_i is a division ring, and that if $n_i = \dim_{D_i}(M_i)$, then the Wedderburn component of A corresponding to M_i is isomorphic to $M_{n_i}(D_i^\circ)$, where D_i° is the opposite ring of D_i .

6. From Exercise 5, every semisimple ring A is a direct sum $\bigoplus_{i=1}^n M_{n_i}(D_i)$ for some division rings D_i . Prove that the integers $\{n_i\}$ and the division rings $\{D_i\}$ are uniquely determined by A .

7. Keeping the notation of Exercise 5, let M be a left A -module for which

$$M \cong \coprod_{i=1}^s M_i^{(k_i)}.$$

Show that

$$\text{End}_A M \cong \coprod_{i=1}^s \text{End}_A(M_i^{(k_i)}) \cong \coprod_{i=1}^s M_{k_i}(D_i^\circ),$$

where

$$D_i = \text{End}_A M_i, \quad 1 \leq i \leq s.$$

8. An idempotent e in a semisimple ring A is called *primitive* if Ae is a simple left A -module. Prove that e is primitive if and only if it is impossible to express e as a sum $e=e'+e''$ of idempotents e', e'' such that $e'e''=e''e'=0$. (Remember that all idempotents are, by definition, different from zero.)

9. Let A be a semisimple ring. An idempotent e in the center of A is *primitive* (or *central primitive*) if Ae is a Wedderburn component of A .

(a) State and prove a criterion for central primitivity along the lines of Exercise 8.

(b) Prove that a central primitive idempotent in A is characterized as a central idempotent that acts as the identity operator on one simple left A -module M , and annihilates all other simple modules not isomorphic to M .

10. Let A be a f.d. algebra over a field K . Let M be a f.g. left A -module, and let e be an idempotent in A .

(a) Prove that there exists a K -isomorphism

$$\text{Hom}_A(Ae, M) \cong eM.$$

(b) Prove that if A is a split semisimple K -algebra, and Ae is a simple left A -module generated by an idempotent e , then $\dim_K eM =$ number of direct summands of M isomorphic to Ae .

(c) In particular, prove that a simple A -module M , for a split semisimple K -algebra A , appears in the left regular module $_A A$ with multiplicity equal to $\dim_K M$. (Note that this result proves 3.37iii).)

11. Let $A = \coprod_{i=1}^r M_{n_i}(K)$ be a split semisimple K -algebra over a field K . Prove that there exists a K -basis of A consisting of elements $\{e_{jk}^i\}$, $1 \leq i \leq r$, $1 \leq j, k \leq n_i$, for which the multiplication is given by

$$e_{jk}^i e_{lm}^{i'} = \delta_{ii'} \delta_{kl} e_{jm}^i \quad (\delta_{ii'}, \delta_{kl} = \text{Kronecker deltas}).$$

Prove conversely that every K -algebra, with a basis satisfying the above multiplication table, is a split semisimple K -algebra.

12. Let A and B be rings, and $F: {}_A \mathfrak{M} \rightarrow {}_B \mathfrak{M}$ and $G: {}_B \mathfrak{M} \rightarrow {}_A \mathfrak{M}$ covariant functors defining an equivalence of categories between ${}_A \mathfrak{M}$ and ${}_B \mathfrak{M}$. Prove that the following properties of morphisms and objects are *categorical* in the sense that if $f: M \rightarrow N$ has the property in ${}_A \mathfrak{M}$, so does $F(f)$ in ${}_B \mathfrak{M}$, and similarly for objects:

(i) $f: M \rightarrow N$ is surjective (first prove that the condition is equivalent to the following: $g_1 f = g_2 f \Rightarrow g_1 = g_2$).

- (ii) $f: M \rightarrow N$ is injective (first prove that the condition is equivalent to the following: $fg_1 = fg_2 \Rightarrow g_1 = g_2$).
- (iii) An object $M \in {}_A\mathfrak{M}$ is projective (use (2.22)).
- (iv) An object $M \in {}_A\mathfrak{M}$ is injective (dualize (iii)).
- (v) An object $M \in {}_A\mathfrak{M}$ is a generator (see (3.44)).

13. (See Anderson-Fuller [73, §21]). Let A , B , F and G be as in Exercise 12. Let

$$i_{N \subseteq M}: N \rightarrow M$$

denote the inclusion map from a submodule N into a module $M \in {}_A\mathfrak{M}$. Prove that

$$N \rightarrow \text{Im } F(i_{N \subseteq M})$$

is a lattice isomorphism from the family of submodules of M to the family of submodules of $F(M)$. (This result was used without proof in (vi) of Theorem 3.54.)

14. Keep the above notation. Prove that a left A -module M is simple, semisimple, indecomposable, or finitely generated if and only if the same is true for $F(M)$. Also prove that $\text{rad } M = 0$ if and only if $\text{rad } F(M) = 0$.

[Hint: Show that each of these conditions can be formulated in terms of the lattice of submodules of M , and use Exercise 13. See §5 for a discussion of radicals of modules.]

15. With the above notation, prove that there is an isomorphism of rings

$$\text{End}_A(M) \cong \text{End}_B(F(M)).$$

16. Let A be a f.d. K -algebra, and let V be a f.g. left A -module. Suppose that $e \in A$ is an idempotent which annihilates every composition factor of V . Prove that $eV = 0$.

[Hint: Relative to a K -basis of V adapted to an A -composition series for V , the action of e on V is represented by an upper triangular matrix of the form

$$\begin{bmatrix} 0 & & * \\ \vdots & \ddots & \\ 0 & \dots & 0 \end{bmatrix}.$$

Since this matrix is nilpotent, and $e^2 = e$, it follows that $eV = 0$.

Another proof is as follows: Let $V = V_1 \supseteq V_2 \supseteq \dots \supseteq V_n = 0$ be a composition series for V . Then $eV_i \subseteq V_{i+1}$ for each i , so $eV = 0$ because $e^2 = e$.]

17. Let M be a f.g. module over a P.I.D. R , and let $\text{ann}_R M = R\alpha$ for some nonzero α which is a product of distinct primes of R . Prove that M is a semisimple R -module.

§4. DEDEKIND DOMAINS

§4A. Localization

Throughout, R denotes a commutative ring. A *multiplicative subset* of R is a subset S of R closed under multiplication, such that $1 \in S$ and $0 \notin S$. For example, suppose that P is an ideal of R , and let

$$R - P = \{x \in R : x \notin P\}.$$

Then $R - P$ is a multiplicative subset of R if and only if P is a prime ideal of R (that is, a proper ideal such that $ab \in P$, $a, b \in R$, implies that either $a \in P$ or $b \in P$). Given a (left) R -module M , define an equivalence relation on the Cartesian product $M \times S$ by writing $(m, s) \sim (m', s')$ if and only if $t(s'm - sm') = 0$ for some $t \in S$. Let m/s , or $s^{-1}m$, denote the equivalence class of the pair (m, s) , and let $S^{-1}M$ be the set of all equivalence classes $\{m/s\}$.

In particular, $S^{-1}R$ can be made into a commutative ring by defining

$$(a/s) \pm (b/t) = (ta \pm sb)/st, \quad (a/s) \cdot (b/t) = ab/st$$

for $a, b \in R$, $s, t \in S$. The map $R \rightarrow S^{-1}R$, defined by $a \mapsto a/1$, $a \in R$, gives a ring homomorphism of R into $S^{-1}R$. The kernel of this homomorphism is

$$\{a \in R : sa = 0 \text{ for some } s \in S\},$$

the *S -torsion submodule* of R . By virtue of this homomorphism, each $S^{-1}R$ -module becomes an R -module; in particular, $S^{-1}R$ is itself an R -module, with $a \in R$ acting as does $a/1$.

Likewise, for each R -module M we may introduce an additive structure on $S^{-1}M$ by setting

$$(m/s) \pm (m'/s') = (s'm \pm sm')/ss', \quad m, m' \in M, s, s' \in S.$$

There is an additive homomorphism $M \rightarrow S^{-1}M$, given by $m \mapsto m/1$, whose kernel is

$$\{m \in M : sm = 0 \text{ for some } s \in S\},$$

the *S -torsion submodule* of M . (This is clearly an R -submodule of M .) Further, $S^{-1}M$ can be made into a (left) $S^{-1}R$ -module, by setting

$$(a/s)(m/t) = am/st, \quad a \in R, m \in M, s, t \in S.$$

The elements of S act invertibly on $S^{-1}M$, that is, for each $s \in S$ the map $x \mapsto sx$, $x \in S^{-1}M$, is a bijection of $S^{-1}M$ onto itself. It is easily verified (see MO, §3b) that there is an isomorphism of $S^{-1}R$ -modules:

$$S^{-1}M \cong S^{-1}R \otimes_R M,$$

given by $m/s \rightarrow (1/s) \otimes m$, $m \in M$, $s \in S$. Hereafter, we shall always identify these two modules.

We call $S^{-1}R$ a *ring of quotients* of R , and $S^{-1}M$ a *module of quotients*. Roughly speaking, $S^{-1}R$ is the smallest ring into which R maps in such a way that the elements of S become units in $S^{-1}R$. Likewise, $S^{-1}M$ is the smallest module on which all elements of S act invertibly.

For example, let R be an integral domain, and set $S = R - \{0\}$. Then S is a multiplicative subset of R , and $S^{-1}R$ is precisely the field of quotients of R . Further, for each R -module M , the module of quotients $S^{-1}M$ is a vector space over the field $S^{-1}R$. The homomorphism $M \rightarrow S^{-1}M$ has as kernel

$$\{m \in M : rm = 0 \text{ for some } r \in R, r \neq 0\},$$

the *torsion submodule* of M . In particular, call M *R -torsionfree* if this submodule is 0. In that case, there is an embedding of M in the vector space $S^{-1}M$, given by $m \mapsto m/1$, $m \in M$.

Let us return to the general case. The ring homomorphism $R \rightarrow S^{-1}R$ enables us to view $S^{-1}R$ as an R -module. (Indeed, every $S^{-1}R$ -module is then also an R -module!) An important fact is that $S^{-1}R$ is a *flat* R -module (see MO, §3c), that is, for each exact sequence

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

of R -modules, the corresponding sequence of $S^{-1}R$ -modules

$$S^{-1}L \xrightarrow{f_*} S^{-1}M \xrightarrow{g_*} S^{-1}N$$

is also exact. Here, $f_*(x/s) = f(x)/s$, $x \in L$, $s \in S$, and g_* is defined analogously. The fact that $S^{-1}R$ is R -flat permits us to apply the “Change of Rings” Theorem 2.38 and Theorem 8.16. We have:

(4.1) Proposition. *Let A be an R -algebra, and let S be a multiplicative subset of the commutative ring R . Let M, N be left A -modules such that M is finitely presented. Then*

$$S^{-1}R \otimes_R \text{Hom}_A(M, N) \cong \text{Hom}_{S^{-1}A}(S^{-1}M, S^{-1}N)$$

as $S^{-1}R$ -modules. If we assume further that A is left noetherian, then

$$S^{-1}R \otimes_R \text{Ext}_A^n(M, N) \cong \text{Ext}_{S^{-1}A}^n(S^{-1}M, S^{-1}N), n \geq 0,$$

as $S^{-1}R$ -modules.

Now let P be a prime ideal of the commutative ring R ; we may form the ring of quotients $S^{-1}R$ relative to the multiplicative set $S = R - P$ in R . This ring, denoted by R_P , is called the *localization* of R at P . Likewise, each R -module M has a localization M_P , and we always identify M_P with $R_P \otimes_R M$. Generally speaking, it is easier to deal with R_P -modules rather than R -modules, and localization techniques permit us to pass from information about the set of *all* localizations $\{M_P\}$ back to information about M itself. It usually suffices to let P range over all maximal ideals of R .

Let us state without proof a number of results on localizations; detailed proofs may be found in MO §3d. First of all, R_P is a *local* ring, that is, R_P has a unique maximal ideal, namely $P \cdot R_P$. If P is a *maximal* ideal of R , then

$$R/P \cong R_P/P \cdot R_P$$

as fields, and as R_P -modules. More generally, if P is maximal and $r > 0$, then R/P^r may be viewed as R_P -module, and

$$R/P^r \cong R_P/P^r \cdot R_P$$

as R_P -modules.

Next, each $f \in \text{Hom}_R(M, N)$ induces a map $f_P \in \text{Hom}_{R_P}(M_P, N_P)$, defined by $f_P(m/s) = f(m)/s$, $m \in M$, $s \in R - P$. We have:

(4.2) Proposition. *Let P range over all maximal ideals of R .*

- (i) *For each R -module M , the map $M \rightarrow \prod_P M_P$ is injective.*
- (ii) *A sequence of R -modules $L \xrightarrow{f} M \xrightarrow{g} N$ is exact if and only if for each P ,*

$$L_P \xrightarrow{f_P} M_P \xrightarrow{g_P} N_P$$

is exact. In particular, f is injective if and only if each f_P is injective, and g is surjective if and only if each g_P is surjective. Further,

$$\ker f_P \cong (\ker f)_P, \quad \text{im } f_P \cong (\text{im } f)_P, \quad \text{cok } f_P \cong (\text{cok } f)_P.$$

- (iii) *Let A be an R -algebra, and let*

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

be an exact sequence of left A -modules, with N finitely presented. Then the sequence is A -split if and only if for each P , the sequence

$$0 \rightarrow L_P \xrightarrow{f_P} M_P \xrightarrow{g_P} N_P \rightarrow 0$$

is A_P -split. In particular, N is A -projective if and only if N_P is A_P -projective for each P .

(iv) Let R be an integral domain with field of quotients K , and view each R_P as a subring of K . Then

$$R = \bigcap_P R_P,$$

where P ranges over all maximal ideals of R .

A ring A is *left hereditary* if every left ideal of A is projective as left A -module. Hereditary rings are important because a *Dedekind domain* is precisely a hereditary integral domain. Of course, every semisimple artinian ring is also hereditary. (Less trivially, each maximal order over a Dedekind domain is hereditary; see (26.12).) Part of the structure theorem for modules over a principal ideal domain carries over to hereditary rings:

(4.3) Proposition. For A a left hereditary ring, every submodule of a free left A -module is isomorphic to an external direct sum of left ideals of A , and is therefore projective.

Sketch of Proof. For convenience, we treat only the most common case, where N is a submodule of the free module $M = \bigoplus_{i=1}^k Am_i$ on a finite basis.

We must show that N is isomorphic to a direct sum of ideals, and we use induction on k , the result being clear when $k=1$. Each $n \in N$ is expressible as $n = \sum r_i m_i$, $r_i \in A$. Let J be the set of all coefficients r_1 which occur as n ranges over all elements of N . Then J is a left ideal of A , hence projective, and the correspondence $n \rightarrow r_1$ gives a surjection $N \rightarrow J$. The kernel N' is given by

$$N' = N \cap \bigoplus_{i=1}^{k-1} Am_i.$$

Then $N \cong N' \oplus J$, and N' is isomorphic to a direct sum of ideals by the induction hypothesis. This completes the proof.

Finally, we remark (see MO, (3.24)) that a left noetherian R -algebra A is left hereditary if and only if A_P is left hereditary for each maximal ideal P of R .

§4B. Ideal Theory

Throughout, let R be an integral domain with field of quotients K . We assume that $R \neq K$, to avoid trivial cases. Call R a *Dedekind domain* if “classical ideal theory” holds true in R , that is, every proper nonzero ideal of

R is uniquely expressible as a product of nonzero prime ideals, apart from order of occurrence of the factors. Every P.I.D. (principal ideal domain) is thus automatically a Dedekind domain, and from the standpoint of ideal theory, the concept of a Dedekind domain is a natural generalization of that of a P.I.D.

Let L be a finite extension of K ; an element $x \in L$ is called *integral* over R if x satisfies an equation of the form

$$x^n + a_1 x^{n-1} + \cdots + a_n = 0, \quad a_i \in R.$$

The set of all such x is the *integral closure* of R in L , and is a ring S in L such that $K \cdot S = L$ (see §1A or CR §17). The basic result here, which shows how Dedekind domains arise in practice, is as follows:

(4.4) Proposition. *Let R be a P.I.D. (or more generally, a Dedekind domain) with field of quotients K . Let L be a finite extension field of K , and let S be the integral closure of R in L . Then S is a Dedekind ring with field of quotients L , and $K \cdot S = L$. Furthermore, if L is a separable extension of K , then S is finitely generated* and torsionfree as R -module.*

In particular, suppose that L is an *algebraic number field*, that is, a finite extension of the rational field \mathbb{Q} . The integral closure of \mathbb{Z} in L , denoted by $\text{alg. int. } \{L\}$, is called the ring of *algebraic integers* in L . This ring may be determined quite explicitly, once the field L is given. For example, we have (CR(21.13)):

(4.5) Proposition. *Let $L = \mathbb{Q}(\omega)$, where ω is a primitive n -th root of 1. Then $\text{alg. int. } \{L\} = \mathbb{Z}[\omega]$, and*

$$\min. \text{ pol.}_\mathbb{Q} \omega = \Phi_n(X),$$

the cyclotomic polynomial of order n and degree $\varphi(n)$.

In order to prove (4.4), other characterizations of Dedekind domains are needed. We have

(4.6) Proposition. *The following assertions about a commutative integral domain R are equivalent:*

- (i) R is a Dedekind domain, that is, every proper nonzero ideal of R is uniquely a product of nonzero prime ideals (up to order of occurrence), and if $J \subseteq J'$ is an inclusion of ideals, then the factors of J' are a subset of those of J .

*This need not hold if L/K is not separable. (See Kaplansky [70, Th. 100].)

(ii) R is noetherian, integrally closed*, and every nonzero prime ideal of R is maximal.

(iii) R is hereditary.

The implication (ii) \Rightarrow (i) is proved in CR §18; for (ii) \Rightarrow (iii), see Exercise 4.1 below. In van der Waerden [59], (i) \Rightarrow (ii) is established. A proof that (iii) \Rightarrow (ii) is given in Auslander-Buchsbaum [74, Ch. 13]. In connection with (i), see also (45.2).

From here on, let R be a Dedekind domain. A *fractional* R -ideal, or “ R -ideal in K ”, is a nonzero f.g. R -submodule of K . Every nonzero ideal of R is such, since R is noetherian; nonzero ideals of R are called *integral* ideals. For a fractional ideal J , we set

$$J^{-1} = \{x \in K : xJ \subseteq R\}.$$

Then (CR §18) the R -ideals in K form a free abelian group generated by the nonzero prime ideals of R , with identity element R , and inverse given as above. From the factorizations of a pair of fractional ideals J, J' into products of powers of prime ideals:

$$J = \prod P_i^{a_i}, J' = \prod P_i^{b_i},$$

one can at once compute their sum $J + J'$ and intersection $J \cap J'$, namely,

$$J + J' = \prod P_i^{\min(a_i, b_i)}, J \cap J' = \prod P_i^{\max(a_i, b_i)}.$$

If J and J' are integral ideals such that $J + J' = R$, call them *relatively prime*. One version of the Chinese Remainder Theorem (CR, §18) is as follows: *If A_1, \dots, A_n are pairwise relatively prime ideals of R , then there is a ring isomorphism*

$$(4.7) \quad R/(A_1 \cdots A_n) \cong \prod_{i=1}^n R/A_i.$$

A slightly more general version of this can be stated in terms of localizations. For each maximal ideal P of R , we may form the localization R_P . Explicitly,

$$R_P = \{a/b : a \in R, b \in R - P\}.$$

By §4A, we know that R_P has a unique maximal ideal, namely $P \cdot R_P$. Furthermore (see CR §19) R_P is a P.I.D., and all nonzero ideals in R_P are powers of $P \cdot R_P$. Then we have (CR §18):

*This means that each element of the quotient field of R , which is integral over R , must lie in R .

(4.8) Strong Approximation Theorem. *Let P_1, \dots, P_n be distinct maximal ideals of R , and let $a_1, \dots, a_n \in K$, $r_1, \dots, r_n \in \mathbb{Z}$. Then there exists an $x \in K$ such that*

$$x - a_i \in P_i^{r_i} \cdot R_{P_i}, \quad 1 \leq i \leq n,$$

$$x \in R_P \text{ for each } P \neq P_1, \dots, P_n.$$

Now let L be a finite separable extension of K , and let S be the integral closure of R in L . Given a maximal ideal P of R , let

$$(4.9) \quad P \cdot S = \prod_{i=1}^g P_i^{e_i}, \quad e_i > 0,$$

where the $\{P_i\}$ are distinct prime ideals of S . Call e_i the *ramification index* of P_i relative to the extension L/K , and write $e_i = e(P_i, L/K)$. On the other hand, the residue class field S/P_i is an extension of the field R/P , since $P_i \cap R = P$. Let

$$f_i = f(P_i, L/K) = \dim_{R/P} S/P_i,$$

the *residue class degree* of P_i for L/K . We call P_i *unramified* in L/K if $e_i = 1$ and S/P_i is separable over R/P ; otherwise, P_i is *ramified*. (If R/P is a finite field, as is certainly the case when L is an algebraic number field, then S/P_i is automatically separable over R/P ; hence in this case P_i ramifies if and only if $e_i > 1$.) The fundamental relationship relating the $\{e_i\}$ and $\{f_i\}$ is as follows (see CR(20.18), MO (4.30)):

$$(4.10) \quad \sum_{i=1}^g e_i f_i = \dim_K L.$$

This shows incidentally that each f_i is finite. It is a key result in many parts of algebraic number theory, and is used in the proof of (4.5), for example.

We next turn to a brief review of norms, different and discriminant. For $a \in L$, let $\min. \text{pol.}_K(a)$ be the monic polynomial in $K[X]$ of least degree, which vanishes at a ; it is obviously irreducible. On the other hand, consider the K -linear transformation $x \mapsto ax$, $x \in L$; the characteristic polynomial of this transformation is denoted by $\text{char. pol.}_{L/K}(a)$. Clearly (see MO, §1)

$$(4.11) \quad \text{char. pol.}_{L/K} a = (\min. \text{pol.}_K a)^m, \quad m = \dim_{K(a)} L.$$

We define *trace* $T: L \rightarrow K$ and *norm* $N: L \rightarrow K$ by the equation

$$\text{char. pol.}_{L/K}(a) = X^n - T(a)X^{n-1} + \cdots + (-1)^n N(a), \quad a \in L,$$

where $n = \dim_K L$. By §1A, T is a K -linear map, and N is multiplicative. It

follows from (4.11) that

$$T(a) = m\alpha, N(a) = \beta^m, \text{ where } \min. \text{ pol.}_K a = X^r - \alpha X^{r-1} + \cdots + (-1)^r \beta,$$

with $r = n/m$.

Since R is a Dedekind domain, it is integrally closed in K . Hence Gauss's Lemma holds: a monic polynomial which factors in $K[X]$ already factors in $R[X]$ (see (1.7)). It follows at once that $a \in S$ if and only if $\min. \text{ pol.}_K(a) \in R[X]$; for each such a , we conclude that $T(a)$ and $N(a)$ lie in R .

For a subset S_0 of S , let $T(S_0) = \{T(x) : x \in S_0\}$. We now define the *inverse different*

$$\tilde{S} = \{x \in L : T(xS) \subseteq R\}.$$

Then \tilde{S} is an S -ideal in L containing S (MO, §4d). The *different* of S with respect to R is then defined by

$$D(S/R) = \tilde{S}^{-1},$$

an integral ideal of S . By MO (4.37), a maximal ideal P_i of S is unramified in the extension L/K if and only if $P_i \nmid D(S/R)$.

Above, we have defined the norm of an element of L ; we wish to extend this concept to ideals. Keeping the notation of (4.9) and (4.10), we define

$$\text{norm of } P_i = N(P_i) = P_i^{f_i}.$$

The norm of an arbitrary S -ideal in L is then computed from the above, by requiring the norm to be multiplicative on ideals. By MO Ex. 4.9, we have

$$N(Sa) = R \cdot N(a), a \in L.$$

In the special case where $K = \mathbb{Q}$, and $R = \mathbb{Z}$ it turns out that for each integral ideal J in S , the norm $N(J) = \mathbb{Z} \cdot \mathcal{N}(J)$, where $\mathcal{N}(J)$ is the number of elements in the residue class ring S/J . We call $\mathcal{N}(J)$ the *absolute norm* or *counting norm* of J .

The *discriminant* of S/R is defined by

$$d(S/R) = N\{D(S/R)\},$$

the norm of the different; it is a nonzero ideal of R . If S has a free R -basis, say $S = \coprod_{i=1}^n Rx_i$, where $n = \dim_K L$, then (MO (4.35)) we have

$$d(S/R) = R \cdot \det(T(x_i x_j))_{1 \leq i, j \leq n}.$$

A maximal ideal P of R is said to *ramify* in L if some P_i of S dividing P

ramifies in L/K . Then by MO (4.37) we know that P ramifies in L if and only if P divides $d(S/R)$. We say that S is *unramified* over R if no maximal ideal of R ramifies in L . It follows at once that S is unramified over R if and only if $d(S/R)=R$.

Finally, we remark that in the special case where $S=R[a]$, the discriminant $d(S/R)$ is precisely the principal ideal $R \cdot d(a)$, where $d(a)$ is *discriminant* of the element a . (Recall that

$$d(a) = \prod (a_i - a_j)^2, \quad 1 \leq i < j \leq n,$$

where a_1, \dots, a_n are the distinct zeros of min. pol. $\kappa(a)$ in an algebraic closure of K .)

§4C. Valuations, Completions, Localizations

Let \mathbf{R}^+ be the set of nonnegative real numbers. A *valuation* on a field K is a map $\varphi: K \rightarrow \mathbf{R}^+$ such that for all $a, b \in K$,

$$\begin{cases} \varphi(a) = 0 \text{ if and only if } a = 0, \\ \varphi(ab) = \varphi(a)\varphi(b), \\ \varphi(a+b) \leq \varphi(a) + \varphi(b). \end{cases}$$

A *non-archimedean* valuation is one which satisfies the stronger condition:

$$\varphi(a+b) \leq \max(\varphi(a), \varphi(b)).$$

A *discrete* valuation is one for which the *value group* $\{\varphi(a): a \in K, a \neq 0\}$, is an infinite cyclic group; it is necessarily non-archimedean. We exclude always the *trivial* valuation defined by $\varphi(0)=0$, $\varphi(a)=1$ for $a \in K - \{0\}$.

Each valuation φ gives rise to a metric on the space K , by choosing as neighborhoods of an element $a \in K$ the open spheres

$$\{x \in K: \varphi(x-a) < \varepsilon\},$$

with ε ranging over all positive real numbers. Two valuations are called *equivalent* if they yield the same topology on K . By a *prime* of K we mean an equivalence class of valuations of K .

Given a non-archimedean prime φ on K , let

$$R = \{a \in K: \varphi(a) \leq 1\}, \quad P = \{a \in K: \varphi(a) < 1\}.$$

Then R is a ring, the *valuation ring* of φ , and P is the unique maximal ideal of R . If φ is discrete, then $P = R\pi$ is a principal ideal, generated by any element $\pi \in P$ for which $\varphi(\pi)$ generates the value group of φ . In this case, the ring R is called a *discrete valuation ring* (abbreviation: d.v.r.); each nonzero ideal of R is of the form $\pi^k R$, for some $k \geq 0$.

Discrete valuations arise in the following manner. Let R be any Dedekind domain, with quotient field K , and let P be a maximal ideal of R . For each $a \in K$, let $v_P(a)$ denote the exponent to which P occurs in the factorization of Ra into a product of prime ideal powers, and set $v_P(0) = +\infty$. Now choose a real number $\kappa > 1$, and define

$$\varphi_P(a) = \kappa^{-v_P(a)}, \quad a \in K,$$

with $\varphi_P(0) = 0$. Then φ_P is a discrete non-archimedean valuation on K , called the *P -adic valuation* of K . (Changing the value of κ does not change the equivalence class of the valuation.) The valuation ring of φ_P is precisely

$$R_P = \{x/s : x \in R, s \in R - P\},$$

that is, the localization of R at P . We have remarked in §4A that residue class fields are unchanged in the passage from R to R_P :

$$R/P \cong R_P/P \cdot R_P.$$

Keeping the above notation, let J be an R -ideal in K ; its localization J_P is then an R_P -ideal in K . Let $v_P(J)$ be the exponent to which P occurs in the factorization of J into prime ideal powers. It is easily shown (CR §19) that

$$J_P = (P \cdot R_P)^{v_P(J)}, \text{ and } v_P(J) = \min\{v_P(a) : a \in J\}.$$

Thus, we can recover J from its localizations; in fact, we have

$$J = \bigcap_P J_P.$$

Now let L/K be a finite separable extension, and let S be the integral closure of R in L . For each maximal ideal P , we may form the localization S_P since S is an R -module. We leave it as an exercise for the reader to verify that S_P is the integral closure of R_P in K . Furthermore, keeping the notation of (4.9) and (4.10), we have

$$P \cdot S_P = \prod_{i=1}^g (P_i \cdot S_P)^{e_i}, \quad S_P/P_i \cdot S_P \cong S/P_i, \quad 1 \leq i \leq g.$$

Thus, the maximal ideals of S_P dividing P are precisely the g ideals $\{P_i \cdot S_P\}$. In the passage from R to R_P , and from S to S_P , the ramification indices $\{e_i\}$ and residue class degrees $\{f_i\}$ are unchanged.

Likewise, it is easily verified that norms, differentials and discriminants behave properly under localization:

$$N(J_P) = \{N(J)\}_P, \quad D(S_P/R_P) = \{D(S/R)\}_P, \quad d(S_P/R_P) = \{d(S/R)\}_P$$

for each P and each S -ideal J in L .

We are now ready to consider the process of completion. Starting with any (nontrivial) valuation φ on K , not necessarily non-archimedean, we have seen above that K may be made into a metric space. We may then form the completion \hat{K} of this metric space in the usual way, namely, the elements of \hat{K} are equivalence classes of Cauchy sequences from K . Then \hat{K} is a field, called the φ -adic completion of K , and K is embedded in \hat{K} . The valuation φ extends uniquely to a valuation $\hat{\varphi}$ on \hat{K} , and \hat{K} is complete with respect to its $\hat{\varphi}$ -adic metric. If φ is an archimedean valuation, then so is $\hat{\varphi}$, and \hat{K} is either \mathbb{R} or \mathbb{C} , with $\hat{\varphi}$ equivalent to the usual absolute value (see Weiss [63, §1.8]). On the other hand, if φ is non-archimedean so is $\hat{\varphi}$, and $\hat{\varphi}$ has the same value group as φ (thus, if φ is a discrete valuation, so is $\hat{\varphi}$).

Now let φ be a discrete valuation on K , $\hat{\varphi}$ its extension to the φ -adic completion \hat{K} , and set

$$\hat{R} = \{a \in \hat{K} : \hat{\varphi}(a) \leq 1\}, \quad \hat{P} = \{a \in \hat{K} : \hat{\varphi}(a) < 1\}.$$

Thus \hat{R} is the discrete valuation ring associated with $\hat{\varphi}$, and \hat{P} is its unique maximal ideal. Then (Weiss [63, §1.9]) we have an isomorphism of fields: $R/P \cong \hat{R}/\hat{P}$, where R is the valuation ring of φ and P is the maximal ideal of R . Indeed, more generally, there is a ring isomorphism

$$\hat{R}/\hat{P}^k \cong R/P^k, \text{ for each } k \geq 1.$$

We may observe further that

$$\hat{P} = P \cdot \hat{R}, \quad P = \hat{P} \cap R.$$

Keeping the above notation, let $P = R\pi$ and let \mathcal{S} be a full set of representatives of the residue classes in R/P , with $0 \in \mathcal{S}$. Then each element of \hat{K} is uniquely expressible as a Laurent series

$$\pi^{-k}(a_0 + a_1\pi + a_2\pi^2 + \cdots), \quad a_i \in \mathcal{S}, \quad a_0 \neq 0, \quad k \in \mathbb{Z}.$$

For further reading on completions, see CR §19, Weiss [63, §1.7], or the elementary introduction by Bachmann [64].

Now let K be an algebraic number field. An *infinite prime* of K is an equivalence class of archimedean valuations on K . Such primes P arise from embeddings of K in the real field \mathbb{R} or the complex field \mathbb{C} . If the completion K_P coincides with \mathbb{R} , we call P a *real* prime of K . On the other hand, if $K_P = \mathbb{C}$ we call P a *complex* prime of K . Let $K = \mathbb{Q}(a)$, and write

$$\min. \text{ pol.}_\mathbb{Q}(a) = \prod_{j=1}^n (X - a_j), \quad a_j \in \mathbb{C}.$$

Let a_1, \dots, a_r be real, and let the remaining zeros be arranged in nonreal conjugate pairs a_{r+j}, \bar{a}_{r+j} , $1 \leq j \leq s$. Then there are r real primes of K , given

by the embeddings

$$\theta_j : \mathbb{Q}(a) \rightarrow \mathbb{R}, \text{ where } \theta_j(a) = a_j, 1 \leq j \leq r.$$

Likewise, there are s complex primes of K , given by the embeddings

$$\theta_j : \mathbb{Q}(a) \rightarrow \mathbb{C}, \text{ where } \theta_j(a) = a_j, r+1 \leq j \leq r+s.$$

§4D. Modules over Dedekind Domains

Throughout, R denotes a Dedekind domain with field of quotients K . The *torsion submodule* of an R -module M is defined by

$$t(M) = \{m \in M : rm = 0 \text{ for some nonzero } r \in R\}.$$

By §4A, $t(M)$ is the kernel of the homomorphism $M \rightarrow K \otimes_R M$. Call M *R -torsionfree* if $t(M) = 0$; in that case, this homomorphism is an embedding. We shall always identify M with its image $1 \otimes M$ in $K \otimes_R M$, assuming that $t(M) = 0$; then $K \otimes_R M = K(1 \otimes M) = KM$, the set of K -linear combinations of elements of M . It is clear that for each $v \in KM$, there exists a nonzero $r \in R$ such that $rv \in M$.

An *R -lattice* is a finitely generated R -torsionfree R -module. Each R -lattice M may be embedded in a finite dimensional K -space V such that $KM = V$ (namely, choose $V = K \otimes_R M$), and we call M a *full R -lattice* in V . If M and N are a pair of full R -lattices in V , then for each $m \in M$ there is some nonzero $r \in R$ such that $rm \in N$. Since M is finitely generated as R -module, it follows at once that there exist nonzero $r, s \in R$ such that

$$rN \subseteq M \subseteq sN.$$

In particular, we may choose $N = \bigcup Rv_i$, where $\{v_i\}$ is a K -basis of V . It follows that every R -lattice M is squeezed between a pair of free R -modules on n generators, where $n = \dim_K KM$, the R -rank of M . Since R is hereditary, M is R -projective by (4.3).

Let M be an R -lattice, and let L be a sublattice of M ; we call L an *R -pure* sublattice of M if M/L is R -torsionfree. But then M/L is R -projective, so the sequence

$$0 \rightarrow L \rightarrow M \rightarrow M/L \rightarrow 0$$

is R -split, that is, L is a direct summand of M . Conversely, each direct summand of M is R -pure in M . The importance of purity arises from the following result, whose proof is left to the reader:

(4.12) Proposition. *Let M be an R -lattice. The correspondence $N \leftrightarrow W$ is bijective and inclusion-preserving, where N ranges over all R -pure sublattices of M , and W ranges over all K -subspaces of the K -space KM .*

Now let M be an R -lattice of rank n ; since M may be embedded in a free R -lattice, it follows from (4.3) not only that M is R -projective, but also that M is isomorphic to an external direct sum $\coprod J_i$ of ideals of R . There must be n summands, since M has rank n . The next result tells us when two such sums are isomorphic (for a proof, see CR §22):

(4.13) Steinitz' Theorem. *Each R -lattice M is R -projective, and $M \cong \coprod_{i=1}^n J_i$, where the J_i are ideals of R and where n is the R -rank of M . Further, the external direct sums $\coprod_{i=1}^n J_i$ and $\coprod_{i=1}^m J'_i$ are isomorphic if and only if $m=n$ and the products (in K) $J_1 \dots J_n$ and $J'_1 \dots J'_n$ are in the same ideal class.* This ideal class is called the Steinitz class of the lattice.*

The invariant factor theorem for lattices over principal ideal domains extends readily to Dedekind domains (see CR, §22), and we have

(4.14) Invariant Factor Theorem. *Let M, N be R -lattices such that $N \subseteq KM$. Then there exist elements $\{m_i\}$ in M , and fractional R -ideals $\{J_i\}$ and $\{E_i\}$, such that*

$$M = \bigoplus_{i=1}^r J_i m_i, \quad N = \bigoplus_{i=1}^s E_i J_i m_i \text{ (internal direct sums),}$$

where $r = R$ -rank of M , $s = R$ -rank of N , $s \leq r$, and where

$$E_1 \supseteq E_2 \supseteq \dots \supseteq E_s.$$

Further, if $N \subseteq M$ then each E_i is an integral ideal, that is, $E_i \subseteq R$.

The ideals $\{E_i\}$ are called the *invariant factors* of the pair M, N ; they are uniquely determined by the inclusion $N \subseteq KM$. If $N \subseteq M$, then

$$M/N \cong \coprod_1^s J_i / E_i J_i \oplus \coprod_{s+1}^r J_i.$$

However, for any fractional ideal J and any integral ideal E of R , there is an R -isomorphism (see CR (18.24))

$$(4.15) \quad J/EJ \cong R/E.$$

Since every f.g. R -module is a homomorphic image of a free module of finite rank, the above discussion yields the following structure theorem:

*Two R -ideals J, J' are in the same *ideal class* if $J' = Jx$ for some nonzero $x \in K$.

(4.16) Proposition. *Every f.g. R-module is isomorphic to an external direct sum of fractional ideals and cyclic* modules R/E, where E denotes an integral ideal.*

We shall now define the *order ideal* $\text{ord } X$ of a f.g. R -module X . Set $\text{ord } X=R$ if $X=0$, and $\text{ord } X=0$ if X is not an R -torsion[†] module. If X is a nonzero torsion module, it has an R -composition series; the composition factors are given by $\{R/P_i\}$, with the P_i maximal ideals of R . We set $\text{ord } X=\prod P_i$, a nonzero proper ideal of R . It is easily seen that $\text{ord } X$ is well defined. If X is a f.g. torsion \mathbf{Z} -module, then obviously $\text{ord}_{\mathbf{Z}} X$ is the principal ideal $\mathbf{Z} \cdot \text{card } X$. Thus, for R -modules the order ideal measures their “size” in some sense. We have at once (see MO (4.17)):

(4.17) Proposition. *If $L \subseteq M$ are f.g. R -modules, then*

$$\text{ord } M = (\text{ord } L)(\text{ord } M/L).$$

Further, for each ideal J of R we have

$$\text{ord } R/J = J.$$

An immediate consequence is:

(4.18) Corollary. *Let $R \subseteq S$ be an inclusion of Dedekind domains. Then for every f.g. R -module X , we have*

$$(4.19) \quad \text{ord}_S(S \otimes_R X) = S \otimes_R \text{ord } X.$$

Proof. By (4.15) and (4.16), it suffices to verify the result for $X=J$ and for $X=R/J$, where J is an ideal of R . For the latter case, we start with the R -exact sequence $0 \rightarrow J \rightarrow R \rightarrow R/J \rightarrow 0$. Since S is R -flat by Exercise 4.3, we obtain an S -exact sequence

$$0 \rightarrow S \otimes J \rightarrow S \rightarrow S \otimes (R/J) \rightarrow 0,$$

where \otimes means \otimes_R . The image of $S \otimes J$ in S is precisely JS , and therefore

$$S \otimes J \cong JS, \quad S \otimes (R/J) \cong S/JS.$$

Thus

$$\text{ord}_S(S \otimes (R/J)) = \text{ord}_S(S/JS) = JS = S \otimes \text{ord}(R/J),$$

as desired. On the other hand, when $X=J$ we see that $S \otimes J$ is S -torsionfree, so both sides of (4.19) are zero. This completes the proof.

*An R -module M is *cyclic* if it is of the form Rx for some $x \in M$.

[†] X is an R -torsion module if $rX=0$ for some nonzero $r \in R$.

In particular, for each maximal ideal P of R , and each f.g. R -module X , we have

$$(4.20) \quad \text{ord } X_P = (\text{ord } X)_P.$$

We shall deduce from this:

(4.20a) Proposition. *Let f be an R -endomorphism of the R -lattice M . Then*

$$\text{ord } M/f(M) = R \cdot \det(f)$$

where $\det(f)$ is computed by extending f to a K -endomorphism of KM .

Proof. By (4.20), it suffices to prove the result when R is replaced by R_P , and so we may assume that R is a principal ideal domain. In this case, both M and $f(M)$ have free R -bases, say

$$M = \bigoplus_{i=1}^r Rm_i, \quad f(M) = \bigoplus_{j=1}^r Rn_j, \quad \text{where } n_j = \sum \alpha_{ji} m_i, \quad \alpha_{ji} \in R.$$

Changing R -bases in M and $f(M)$, we may assume that the matrix (α_{ij}) is diagonal. Note that $\det f = \det(\alpha_{ij})$, and that this change does not affect the ideal $R \cdot \det f$. But if (α_{ij}) is a diagonal matrix, then

$$\text{ord } M/f(M) = \prod \text{ord } R/R\alpha_{ii} = \prod R\alpha_{ii} = R \cdot \det(\alpha_{ij}),$$

as desired.

Now let M be a f.g. R -module, and let P be a maximal ideal of R . We have denoted by M_P the *localization* of M at P , that is,

$$M_P = \{m/s : m \in M, s \in R - P\} \cong R_P \otimes_R M.$$

On the other hand, we may form the P -adic completion \hat{K}_P of the field; let \hat{R}_P be the valuation ring of the P -adic valuation on \hat{K}_P , and \hat{P} its maximal ideal. Let us set

$$\hat{M}_P = \hat{R}_P \otimes_R M \cong \hat{R}_P \otimes_{R_P} M_P,$$

the *P -adic completion* of M . (We may also view \hat{M}_P as the completion of M , where M is topologized by requiring that $\{P^k M : k = 0, 1, 2, \dots\}$ be a basis for the open neighborhoods of 0. See MO (6.16).) We shall state without proof a number of properties of completions of modules, generalizing results given above in §4C about completions of rings; the module results follow readily from those about rings, by use of (4.16).

(4.21) Proposition. *Let M be a f.g. R -module. Then*

(i) *M is dense in \hat{M}_P .*

(ii) *For each $k \geq 1$, there are ring isomorphisms*

$$\hat{R}/\hat{P}^k \cong R_P/P^k R_P \cong R/P^k,$$

(iii) *The map $M_P \rightarrow \hat{M}_P$ is always injective.*

(iv) *For $k \geq 0$,*

$$M_P \cap \hat{P}^k \hat{M}_P = P^k M_P.$$

(v) *Let V be a f.d. K -space, and set $\hat{V}_P = \hat{K}_P \otimes_K V$. There is a bijection $M \leftrightarrow T$ which preserves inclusions, where M ranges over all R_P -lattices in V for which $KM = V$, and T ranges over all \hat{R}_P -lattices in \hat{V}_P for which $\hat{K}_P T = \hat{V}_P$.*

(vi) *For each R -lattice M , we have $M_P = KM \cap \hat{M}_P$ for each P , and*

$$M = \bigcap_P (KM \cap M_P) = \bigcap_P (KM \cap \hat{M}_P).$$

(vii) *Let V be a f.d. K -space, and let M be a full* R -lattice in V . Suppose that for each P , there is given a full R_P -lattice $X(P)$ in V , such that $X(P) = M_P$ a.e.[†] Define*

$$N = \bigcap_P X(P),$$

the intersection being formed within V . Then N is a full R -lattice in V , and

$$N_P = X(P) \text{ for each } P.$$

(viii) *Keeping the above notation, suppose that for each P there is given a full \hat{R}_P -lattice $Y(P)$ in \hat{V}_P , such that $Y(P) = \hat{M}_P$ a.e. Define*

$$L = \bigcap_P \{V \cap Y(P)\}.$$

Then L is a full R -lattice in V , and $\hat{L}_P = Y(P)$ for all P .

Proofs may be found in MO, §4b and §5a.

*This means that $KM = V$.

[†]"a.e." means "almost everywhere," that is, for all but a finite number of P 's.

§4E. Duals of Lattices

Let R be a Dedekind domain with field of quotients K , and let V be an n -dimensional K -space. Given a nondegenerate bilinear symmetric form $\tau: V \times V \rightarrow K$, we can form duals with respect to τ . If $\{x_i\}$ is a K -basis of V , the *dual basis* $\{y_j\}$ is the K -basis of V determined by the condition

$$\tau(x_i, y_j) = \delta_{ij}, \quad 1 \leq i, j \leq n.$$

Clearly, the dual of the basis $\{y_j\}$ is the original basis $\{x_i\}$.

Now let M be a full R -lattice in V , and define the *dual* of M (with respect to τ) by

$$(4.22) \quad \tilde{M} = \{x \in V : \tau(x, M) \subseteq R\}.$$

We have at once (if M is R -free)

$$(4.23) \quad M = \coprod_1^n Rx_i \Rightarrow \tilde{M} = \coprod_1^n Ry_j,$$

where $\{y_j\}$ is a dual basis for $\{x_i\}$. Hence $\tilde{\tilde{M}} = M$ whenever M is R -free; also, \tilde{M} is a full R -lattice in V .

(4.24) Proposition. *For any full R -lattice M in V , its dual \tilde{M} is also a full R -lattice in V . Further, $\tilde{\tilde{M}} = M$.*

Proof. We may choose free full R -lattices N_1, N_2 in V such that $N_1 \subseteq M \subseteq N_2$. Then $\tilde{N}_2 \subseteq \tilde{M} \subseteq \tilde{N}_1$, whence \tilde{M} is also a full R -lattice in V .

In order to verify that $\tilde{M} = M$, we observe first that the process of localization (at a maximal ideal P or R) commutes with formation of duals:

$$(\tilde{M})_P = \text{dual of } M_P.$$

It thus suffices to verify that $\tilde{M}_P = M_P$ for each P ; but this is clear, since M_P is a full free R_P -lattice in V .

Keeping the above notation, we define the *discriminant ideal* of a full R -lattice M in V as the R -ideal in K generated by all elements

$$(4.25) \quad \alpha = \det[\tau(x_i, x_j)]_{1 \leq i, j \leq n}, \quad x_1, \dots, x_n \in M.$$

If we denote this ideal by $d(M)$, then clearly

$$\{d(M)\}_P = d(M_P)$$

for each maximal ideal P of R . Since τ is nondegenerate, $d(M) \neq 0$. Furthermore, if $M = \prod_n Rx$, then $d(M) = \alpha R$, with α given by (4.25). Obviously, if N is also a full R -lattice in V , then

$$N \subseteq M \Rightarrow d(N) \supseteq d(M).$$

(4.26) Proposition. *Let $N \subseteq M$, where M and N are full R -lattices in V . Then*

$$d(N) = \{\text{ord } M/N\}^2 d(M),$$

where $\text{ord}(M/N)$ denotes the R -order ideal defined in §4D. Therefore $M = N$ if and only if $d(M) = d(N)$.

Proof. It suffices to establish the result after replacing R by its localization R_P at an arbitrary maximal ideal P of R . Changing notation, assume hereafter that R is a P.I.D. Then we may find $x_1, \dots, x_n \in M$ and $\alpha_1, \dots, \alpha_n \in R$ such that

$$M = Rx_1 \oplus \cdots \oplus Rx_n, \quad N = R\alpha_1 x_1 \oplus \cdots \oplus R\alpha_n x_n.$$

Then (as in the proof of (4.21))

$$\text{ord } M/N = \prod \text{ord } R/R\alpha_i = \prod R\alpha_i.$$

On the other hand, $d(M) = \alpha R$ with α as in (4.25), while $d(N) = \alpha \cdot \prod \alpha_i^2 \cdot R$. This establishes the relation between $d(M)$ and $d(N)$. Finally, if $d(M) = d(N)$ then $\text{ord } M/N = R$, whence $M = N$.

Suppose now that Λ is an R -algebra which acts from the left on the R -lattice M , in such a way that

$$\lambda \cdot \alpha m = \alpha \cdot \lambda m \text{ for all } \lambda \in \Lambda, \alpha \in R, m \in M.$$

We call M a *left Λ -lattice* to indicate that the R -lattice M is a left Λ -module. We can make V into a left Λ -module by writing $V = K \otimes_R M$, and then defining

$$\lambda(\alpha \otimes m) = \alpha \otimes \lambda m \text{ for } \lambda \in \Lambda, \alpha \in K, m \in M.$$

Next, the nondegenerate form $\tau: V \times V \rightarrow K$ enables us to define the transpose ' f ' of an arbitrary $f \in \text{End}_K(V)$. This transpose also lies in $\text{End}_K(V)$, and is defined by the condition

$$\tau(^t f x, y) = \tau(x, fy) \text{ for all } x, y \in V.$$

We use this idea to define a *right Λ -module structure* on V , as follows: for

each $\lambda \in \Lambda$ and $x \in V$, let $x\lambda \in V$ be the element defined by the identity

$$\tau(x\lambda, y) = \tau(x, \lambda y) \text{ for all } y \in V.$$

Let us show that the dual \tilde{M} is a right Λ -lattice in V . This follows at once from the fact that for any $x \in \tilde{M}$ and $\lambda \in \Lambda$,

$$\tau(x\lambda, M) = \tau(x, \lambda M) \subseteq \tau(x, M) \subseteq R.$$

The above discussion shows that there is a 1–1 inclusion-reversing correspondence $M \leftrightarrow \tilde{M}$, which associates to each left Λ -lattice M its dual \tilde{M} . Then \tilde{M} is a right Λ -lattice, and there is a left Λ -isomorphism $\tilde{M} \cong M$. (Indeed, $\tilde{M} = M$.)

Now let K' be a field containing K , and set $V' = K' \otimes_K V$. The form τ extends to a nondegenerate bilinear form $\tau': V' \times V' \rightarrow K'$, where $\tau' = 1 \otimes \tau$. Let R' be the integral closure of R in K' . Each full R -lattice M in V gives rise to a full R' -lattice M' in V' , defined by $M' = R' \otimes_R M$. It is easily verified that the dual of M' (with respect to τ') is precisely $R' \otimes_R \tilde{M}$, and further that

$$d(M') = R' \cdot d(M),$$

where $d(M')$ is the discriminant computed relative to τ' .

We shall use this fact to establish an important property of unramified extensions:

(4.26a) Theorem. *Let L be a finite separable extension of K , and let S be the integral closure of R in L . Assume that S is unramified over R . Let K' be any finite extension of K , and R' the integral closure of R in K' . Then*

- (i) $K' \otimes_K L \cong \coprod_{i=1}^t F_i$, where each F_i is a finite separable extension field of K' .
- (ii) $R' \otimes_R S \cong \coprod_{i=1}^t R_i$, where R_i is the integral closure of R' in F_i .
- (iii) Each R_i is unramified over R' .

Proof. Assertion (i) is obvious, once we write $L = K[x]/(f(x))$, with $f(x) \in K[x]$ separable and irreducible; for then

$$K' \otimes_K L \cong K'[x]/(f(x)) \cong \coprod_i K'[x]/(g_i(x)),$$

where $f(x) = \prod g_i(x)$ is the factorization of $f(x)$ into irreducible factors in $K'[x]$.

We observe next that $R' \otimes S \subseteq \prod_i R_i$, and that the discriminant $d(R' \otimes S)$, relative to the bilinear form $1 \otimes T_{L/K}$, is equal to $R' \cdot d(S/R)$. This follows from the remarks preceding the theorem. But $d(S/R) = R$ since S/R is unramified, so $d((R' \otimes S)/R') = R'$. On the other hand, by (4.26)

$$d((R' \otimes S)/R') = \{\text{ord}_{R'}(\prod_i R_i)/(R' \otimes S)\}^2 \cdot \prod_{i=1}^t d(R_i/R').$$

Therefore each factor on the right must equal R' , which establishes both (ii) and (iii), and completes the proof.

§4F. Ideal Class Groups; Global Fields

Let R be a Dedekind domain with field of quotients K . An *R-ideal* in K is a nonzero f.g. R -submodule of K ; such ideals are also called *fractional R-ideals*. For each fractional R -ideal J , there exists a nonzero $\alpha \in R$ such that αJ is an ordinary ideal of the domain R . Two R -ideals J, J' are called *equivalent* if $J' = Jx$ for some nonzero $x \in K$; thus J, J' are equivalent if and only if $J \cong J'$ as R -modules. The *ideal class* $[J]$ is defined as the set of all fractional ideals equivalent to J .

We may define multiplication of ideal classes by the formula

$$[J][J'] = [JJ'],$$

where JJ' is the R -ideal consisting of all finite sums $\sum x_i y_i$, $x_i \in J, y_i \in J'$. This multiplication is well defined, and the ideal class $[R]$ is the unity element for this multiplication. The ideals in the class $[R]$ are called *principal ideals*; they are of the form Rx , with $x \in K, x \neq 0$.

Given a fractional R -ideal J , define its *inverse* as

$$J^{-1} = \{x \in K : xJ \subseteq R\}$$

Then J^{-1} is also a fractional R -ideal, and

$$JJ^{-1} = J^{-1}J = R.$$

Thus $[J^{-1}][J] = [R]$, and so the ideal classes form an abelian multiplicative group, hereafter denoted by $Cl(R)$, the *ideal class group* of R . The order of this group is called the *ideal class number* of R , and is usually denoted by $h(R)$. Thus, $h(R) = 1$ if and only if R is a principal ideal domain.

A *global field* is either an *algebraic number field* (that is, a finite extension of the rational field \mathbb{Q}), or else a *function field* (that is, a finite extension of a simple transcendental extension $k(X)$ of a finite field k .) One of the basic facts about global fields is as follows:

(4.27) Theorem. *Let R be a Dedekind domain whose field of quotients K is a global field. Then the ideal class group of R is finite.*

The theorem is proved in CR (20.6) for the case where K is an algebraic number field and $R = \text{alg. int. } \{K\}$.

In a later section (§24) we shall state the Jordan-Zassenhaus Theorem, which generalizes the above result to the case of non-commutative rings of integers.

§4G. Primary Decompositions

Throughout this subsection, R denotes a Dedekind domain with quotient field K , and P, P_1, \dots , denote maximal ideals of R . For an R -module M , M_P is the localization of M at P .

(4.28) Definition. The P -primary submodule of an R -module M is defined as

$$\{m \in M : P^e m = 0 \text{ for some integer } e \geq 0\}.$$

A P -primary module is one which coincides with its P -primary submodule.

(4.29) Proposition. Let M be a f.g. P -primary R -module. Then $M \cong M_P$.

Proof. For $\alpha \in R - P$ we have $\alpha R + P = R$, whence $\alpha R + P^e = R$ for each $e \geq 0$. Since M is P -primary and f.g., we may choose e so that $P^e M = 0$. But then α acts invertibly on M , whence $(R - P)^{-1} M \cong M$ as claimed.

(4.30) Proposition. Let M be a f.g. P -primary R -module, and let Q be a maximal ideal of R distinct from P . Then $M_Q = 0$.

Proof. We have $Q + \text{ann}_R M = R$, so $M_Q = 0$ by Exercise 4.5.

An R -module M is called a *torsion module* if each $m \in M$ is annihilated by some nonzero element of R . We now prove

(4.31) Primary Decomposition Theorem. Let M be a f.g. torsion R -module. Then $M_P = 0$ a.e., and M is expressible as a finite direct sum

$$M = \bigoplus_P M_P.$$

Further, for each P , M_P is the P -primary submodule of M .

Proof. Since M is f.g. and a torsion module, we have $aM = 0$ for some nonzero $a \in R$. Let

$$Ra = \prod_{i=1}^n P_i^{e_i}$$

be the factorization of Ra into powers of distinct maximal ideals $\{P_i\}$ of R .

Then by (4.7) we have

$$R/Ra \cong \coprod R/P_i^{e_i}.$$

But M may be viewed as (R/Ra) -module, and thus

$$M = (R/Ra)M \cong \coprod (R/P_i^{e_i})M = \coprod M/P_i^{e_i}M.$$

Now $M/P_i^{e_i}M$ is P_i -primary, so by (4.29) and (4.30) we have

$$(M/P_i^{e_i}M)_P = \begin{cases} M/P_i^{e_i}M & \text{if } P = P_i \\ 0 & \text{if } P \neq P_i. \end{cases}$$

Clearly $M/P_i^{e_i}M$ is the P_i -primary submodule of M . But

$$M_P \cong \coprod (M/P_i^{e_i}M)_P,$$

so we obtain $M/P_i^{e_i}M = M_{P_i}$ for $1 \leq i \leq n$. Therefore $M = \coprod M_P$ as claimed, and $M_P = 0$ except when P is one of P_1, \dots, P_n . This completes the proof.

§4H. Cyclotomic Fields

Let ω_m denote a primitive m -th root of 1 over the rational field \mathbb{Q} , and let

$$(4.32) \quad K_m = \mathbb{Q}(\omega_m), \quad R_m = \mathbb{Z}[\omega_m] = \text{alg. int. } \{K_m\}$$

(see (4.5)). Then

$$\min. \text{ pol.}_{\mathbb{Q}}(\omega_m) = \Phi_m(x),$$

the cyclotomic polynomial of order m and degree $\varphi(m)$, where φ is the Euler φ -function. From CR §21, we know that $\Phi_m(x)$ is irreducible in $\mathbb{Q}[x]$, and

$$(4.33) \quad \Phi_m(x) = \prod_{\substack{1 \leq k \leq m \\ (k, m) = 1}} (x - \omega_m^k).$$

These $\{\omega_m^k\}$ are a full set of primitive m -th roots of 1 over \mathbb{Q} .

Now let p be a fixed rational prime. We wish to describe the factorization of pR_m into a product of prime ideal powers. This is essentially an exercise in the use of Kummer's Theorem (see Weiss [63, Th. 4-9-1]), though we shall give a self-contained discussion below. Let us begin with the case where $p \nmid m$.

(4.34) Proposition. *Let $p \nmid m$, and let P be a prime ideal of R_m containing p . Set $\bar{R}_m = R_m/P$, $\bar{\mathbb{Z}} = \mathbb{Z}/p\mathbb{Z}$, and let bars denote images in \bar{R}_m or $\bar{\mathbb{Z}}$, according to the context.*

(i) *The $\varphi(m)$ elements*

$$\{\bar{\omega}_m^k : 1 \leq k \leq m, (k, m) = 1\}$$

are a full set of $\varphi(m)$ distinct primitive m -th roots of 1 over $\bar{\mathbb{Z}}$. They are the zeros of $\bar{\Phi}_m(x)$ in \bar{R}_m .

(ii) Let f be the order of $p \pmod{m}$, that is, the least positive integer such that $p^f \equiv 1 \pmod{m}$. Then

$$(4.35) \quad \min. \text{ pol.}_{\bar{\mathbb{Z}}}(\bar{\omega}_m) = \prod_{j=0}^{f-1} (x - \bar{\omega}_m^{p^j}) \in \bar{\mathbb{Z}}[x].$$

Denoting this polynomial by $F_1(x)$, we have

$$\bar{R}_m = \bar{\mathbb{Z}}[x]/(F_1(x)) = \text{field extension of } \bar{\mathbb{Z}} \text{ of degree } f.$$

(iii) The prime p is unramified in R_m , that is, pR_m is a product of distinct prime ideals of R_m . Let

$$(4.36) \quad \bar{\Phi}_m(x) = \prod_{i=1}^g F_i(x), \quad F_i(x) \text{ irreducible in } \bar{\mathbb{Z}}[x].$$

Then the $\{F_i\}$ are distinct, and we have

$$(4.37) \quad pR_m = \prod_{i=1}^g P_{mi}, \quad \text{where } P_{mi} = (p, F_i(\omega_m)) = \text{prime ideal of } R_m.$$

Proof. The notation $(p, F_i(\omega_m))$ is somewhat confusing at first, and should be interpreted as follows: pick any polynomial $G_i(x) \in \mathbb{Z}[x]$ such that $\bar{G}_i = F_i$ in $\bar{\mathbb{Z}}[x]$. Then the ideal $(p, G_i(\omega_m))$ of R_m , generated by p and $G_i(\omega_m)$, does not depend on the choice of $G_i(x)$. We are denoting this ideal by $(p, F_i(\omega_m))$.

To begin the proof, we deduce from (4.33) that

$$\bar{\Phi}_m(x) = \prod_k (x - \bar{\omega}_m^k).$$

Since $\bar{\Phi}_m(x)$ divides $x^m - 1$ in $\bar{\mathbb{Z}}[x]$, and the latter has no repeated factors because $p \nmid m$, it follows that the $\varphi(m)$ elements $\{\bar{\omega}_m^k\}$ are distinct. This implies at once that $\bar{\omega}_m$ is a primitive m -th root of 1 over $\bar{\mathbb{Z}}$, and that the $\varphi(m)$ elements $\{\bar{\omega}_m^k\}$ are a full set of primitive m -th roots of 1 over $\bar{\mathbb{Z}}$.

Next, since $R_m = \mathbb{Z}[\omega_m]$ we have $\bar{R}_m = \bar{\mathbb{Z}}[\bar{\omega}_m]$, and we must compute the minimum polynomial of $\bar{\omega}_m$ over $\bar{\mathbb{Z}}$. The Galois group of $\bar{\mathbb{Z}}(\bar{\omega}_m)$ over $\bar{\mathbb{Z}}$ is generated by the Frobenius automorphism θ defined by $\theta(a) = a^p$, $a \in \bar{\mathbb{Z}}(\bar{\omega}_m)$.

But

$$\theta^n(\bar{\omega}_m) = \bar{\omega}_m^{p^n}, n=1, 2, \dots.$$

Thus $\theta^n = 1$ if and only if $p^n \equiv 1 \pmod{m}$. This shows that θ has order f , and establishes (4.35). It proves also that $\bar{R}_m \cong \bar{\mathbb{Z}}[x]/(F_1(x))$.

Finally, let (4.36) be the factorization of $\Phi_m(x)$ over $\bar{\mathbb{Z}}$. Since $\bar{\Phi}_m(x)$ has no repeated zeros, the $\{F_i\}$ are distinct. Each F_i has degree f , since if $\bar{\omega}$ is any zero of $F_i(x)$, then the distinct zeros of $F_i(x)$ are given by

$$\{\bar{\omega}^{p^j} : 0 \leq j \leq f-1\}.$$

Now we have

$$\begin{aligned} R_m/pR_m &\cong \mathbb{Z}[x]/(p, \Phi_m(x)) \cong \bar{\mathbb{Z}}[x]/(\bar{\Phi}_m(x)) \\ &\cong \coprod_{i=1}^g \bar{\mathbb{Z}}[x]/(F_i(x)), \end{aligned}$$

with each summand $\bar{\mathbb{Z}}[x]/(F_i(x))$ a field extension of $\bar{\mathbb{Z}}$ of degree f . Therefore pR_m has no repeated prime ideal factors. Further, the maximal ideals of R_m containing pR_m are precisely the inverse images, under the map $R_m \rightarrow R_m/pR_m$, of the maximal ideals of the above direct sum $\coprod \bar{\mathbb{Z}}[x]/(F_i(x))$. This gives the formulas for the $\{P_{mi}\}$ listed in (4.37). We remark that the originally specified prime ideal P is given by $(p, F_1(x))$. This completes the proof of the proposition.

The other extreme case is that where $m=p^b$ for some $b \geq 0$ and some prime p :

(4.38) Proposition. *Let $m=p^b$, where p is prime, and let P be a prime ideal of R_m containing p . Set $\bar{R}_m = R_m/P$, $\bar{\mathbb{Z}} = \mathbb{Z}/p\mathbb{Z}$.*

(i) *We have $\bar{R}_m = \bar{\mathbb{Z}}$, and*

$$(4.39) \quad \bar{\Phi}_m(x) = (x-1)^{\varphi(m)} \text{ in } \bar{\mathbb{Z}}[x].$$

Further, P is the principal ideal $(1-\omega_m)R_m$.

(ii) *p is completely ramified in R_m , that is, $pR_m = P^{\varphi(m)}$.*

Proof. Every m -th root of 1 over $\bar{\mathbb{Z}}$ equals 1, since $m=p^b$; this gives (4.39) at once. Therefore

$$\begin{aligned} R_m/pR_m &\cong \mathbb{Z}[x]/(p, \Phi_m(x)) \\ &\cong \bar{\mathbb{Z}}[x]/(1-x)^{\varphi(m)}. \end{aligned}$$

Thus there is a unique prime ideal P of R_m containing p , namely $P = (p, 1 - \omega_m)$. Further, we have $R_m/P \cong \bar{\mathbb{Z}}[x]/(1-x) = \bar{\mathbb{Z}}$, and $pR_m = P^{\varphi(m)}$. Finally,

$$N_{K_m/\mathbb{Q}}(1 - \omega_m) = \Phi_m(1) = p,$$

where N denotes the norm. This shows that p is a multiple of $1 - \omega_m$ in R_m , whence $P = (1 - \omega_m)R$. This completes the proof.

Turning to the general case, we now prove

(4.40) Theorem. *Let $m = p^b s$, where p is prime and $p \nmid s$. Let f be the order of p mod s . Let $\{P_{mi}\}$ range over the prime ideals of R_m containing p , and $\{P_{si}\}$ over those of R_s . Put $\bar{\mathbb{Z}} = \mathbb{Z}/p\mathbb{Z}$, and let*

$$\bar{\Phi}_s(x) = \prod_{i=1}^g F_i(x), \quad F_i(x) \text{ irreducible in } \bar{\mathbb{Z}}[x].$$

(i) *The $\{F_i\}$ are distinct, and we have (with suitable numbering)*

$$pR_s = \prod_{i=1}^g P_{si}, \quad P_{si}R_m = (P_{mi})^{\varphi(p^b)} \text{ for each } i.$$

(ii) *For $1 \leq i \leq g$, $R_s/P_{si} \cong \bar{\mathbb{Z}}[x]/(F_i(x))$, a field extension of $\bar{\mathbb{Z}}$ of degree f . Further,*

$$R_m/P_{mi} \cong R_s/P_{si} \text{ for each } i.$$

(iii) *In $\bar{\mathbb{Z}}[x]$ we have $\bar{\Phi}_m(x) = \{\bar{\Phi}_s(x)\}^{\varphi(p^b)}$.*

In brief, in the extension K_s/\mathbb{Q} , the prime p splits into g distinct primes $\{P_{si} : 1 \leq i \leq g\}$ and p is unramified in this extension. In the extension K_m/K_s , each of the primes P_{si} is completely ramified.

Proof. Let ω range over the $\varphi(s)$ primitive s -th roots of 1 over \mathbb{Q} , and ζ over the $\varphi(p^b)$ primitive p^b -th roots of 1. Then $\omega\zeta$ ranges over a full set of $\varphi(m)$ primitive m -th roots of 1. Therefore

$$\Phi_m(x) = \prod_{\omega, \zeta} (x - \omega\zeta), \quad \Phi_s(x) = \prod_{\omega} (x - \omega).$$

But $\bar{\xi} = \bar{1}$ in $\bar{\mathbb{Z}}$ by (4.38), whence

$$\bar{\Phi}_m(x) = \prod_{\omega, \zeta} (x - \bar{\omega}\bar{\xi}) = \left\{ \prod_{\omega} (x - \bar{\omega}) \right\}^{\varphi(p^b)} = \{\bar{\Phi}_s(x)\}^{\varphi(p^b)}.$$

We now have

$$R_m/pR_m \cong \bar{\mathbb{Z}}[x]/(\bar{\Phi}_m(x)) \cong \bar{\mathbb{Z}}[x]/(\bar{\Phi}_s(x))^{\varphi(p^b)}.$$

Since

$$\bar{\mathbb{Z}}[x]/(\bar{\Phi}_s(x))^{\varphi(p^b)} \cong \coprod_{i=1}^g \bar{\mathbb{Z}}[x]/(F_i(x))^{\varphi(p^b)},$$

it follows at once that there are g distinct prime ideals $\{P_{mi}\}$ of R_m containing p . Further, we have

$$R_m/P_{mi} \cong \bar{\mathbb{Z}}[x]/(F_i(x)), \quad 1 \leq i \leq g.$$

On the other hand,

$$R_m/pR_m = R_m / \prod_i P_{si} R_m \cong \prod_{i=1}^g R_m / P_{si} R_m.$$

Comparing this with the previous formula, we obtain $P_{si} R_m = P_{mi}^{\varphi(p^b)}$, and $R_m/P_{mi} \cong R_s/P_{si}$ for each i . This completes the proof.

§4. Exercises

1. Prove that every Dedekind domain R is hereditary.

[Hint: Let J be an ideal of R . Since $JJ^{-1} = R$, we may write $1 = \sum_{i=1}^n x_i y_i$, $x_i \in J$, $y_i \in J^{-1}$. Define maps α, β , where

$$R^{(n)} \xrightleftharpoons[\beta]{\alpha} J,$$

by

$$\alpha(r_1, \dots, r_n) = \sum r_i x_i, \quad \beta(x) = (xy_1, \dots, xy_n).$$

Then $\alpha\beta = 1_J$, whence J is a direct summand of $R^{(n)}$. See also (3.46).]

2. Let L be a sublattice of the R -lattice M , where R is any integral domain. Prove that L is R -pure in M if and only if $L \cap rM = rL$ for each nonzero $r \in R$.

3. Let R be a Dedekind domain. Show that every torsionfree R -module M is R -flat.

[Hint: Use (2.33) and the fact that every R -lattice is projective.]

4. Keeping the notation of (4.9), show that $N_{L/K}(P_i) = \text{ord}_R S/P_i$. Deduce that for each integral ideal J of S , $N_{L/K}(J) = \text{ord}_R S/J$.

[Hint: See MO, (4.31iii).]

5. Let P be a maximal ideal of the commutative ring R , and let M be a finitely generated R -module. Set

$$\text{ann}_R M = \{r \in R : rM = 0\}.$$

Prove that the localization M_P is 0 if and only if $P + \text{ann}_R M = R$.

6. Let $R' = S^{-1}R$, where S is a multiplicative subset of the commutative ring R . Show that for each R' -module M , there is an R' -isomorphism $\mu: R' \otimes_R M \cong M$ defined by setting $\mu(r' \otimes m) = r'm$, $r' \in R'$, $m \in M$.

[Hint: Each element of $R' \otimes_R M$ is expressible as a finite sum $\sum s^{-1}r_i \otimes m_i$, where $s \in S$, $r_i \in R$, $m_i \in M$. If this element lies in the kernel of μ , then $\sum r_i m_i = 0$, whence also $\sum s^{-1}r_i \otimes m_i = s^{-1} \otimes \sum r_i m_i = 0$.]

7. Let R be a Dedekind domain with quotient field K , and let M and N be a pair of full R -lattices in a f.d. K -space V . Show that $M_P = N_P$ a.e., as P ranges over all maximal ideals of R .

[Hint: Choose nonzero $r, s \in R$ such that $rM \subseteq N \subseteq sM$. Then $M_P = N_P$ whenever $rs \notin P$.]

8. Let L be a finite separable extension of the field K , and let S be the integral closure of R in L , where R is a Dedekind domain with field of quotients K . Let T be the trace map $T_{L/K}$, and let D be the different $D(S/R)$ as in §4B. Put

$$J = T_{L/K}(S) = \{T(s) : s \in S\}.$$

Show that J is the smallest ideal of R such that JS divides D .

[Hint: Clearly $T_{L/K}(S)$ is a nonzero ideal of R . For any nonzero ideal I of R , we have

$$T(S) \subseteq I \Leftrightarrow T(I^{-1}S) \subseteq R \Leftrightarrow I^{-1}S \subseteq D^{-1} \Leftrightarrow D \subseteq IS.$$

Then J is the smallest such I .]

9. Let the subscript P denote localization at a maximal ideal P of R . Show that

$$T_{L/K}(S_P) = \{T_{L/K}(S)\}_P.$$

10. Keep the notation of (4.9) and the discussion following it, and let $\bar{R} = R/P$, $\bar{S}_i = S/P_i$, and let $\varphi_i: S \rightarrow \bar{S}_i$ be the canonical surjection, $1 \leq i \leq g$. For each $a \in S$, let $f(X) = \text{char. pol.}_{L/K}(a) \in R[X]$, and let $\bar{f}(X)$ be its image in $\bar{R}[X]$. Then a acts on the \bar{R} -module \bar{S}_i as multiplication by $\varphi_i(a)$. Let

$$h_i(X) = \text{char. pol}_{\bar{S}_i/\bar{R}}(\varphi_i(a)), \quad 1 \leq i \leq g.$$

Show that

$$\overline{f(X)} = \prod_{i=1}^g \{h_i(X)\}^{e_i}.$$

Deduce from this that

$$(4.41) \quad \overline{T_{L/K}(a)} = \sum_{i=1}^g \bar{e}_i T_i(\varphi_i(a)),$$

where T_i denotes the trace from \bar{S}_i to \bar{R} .

[Hint: If we replace R by its localization R_P , and S by S_P , then the hypotheses and conclusions are unchanged. Changing notation, assume now that R is a P.I.D., and let $S = \bigoplus_1^n Rx_i$. Set

$$ax_j = \sum_i \alpha_{ij}x_i, \alpha_{ij} \in R,$$

so $f(X)$ is the characteristic polynomial of the $n \times n$ matrix (α_{ij}) . Then $S/PS = \bigoplus \bar{R}\bar{x}_i$, so $\overline{f(X)}$ is the characteristic polynomial of a acting on the \bar{R} -space S/PS .

Now $S/PS \cong \coprod_{i=1}^g S/P_i^{e_i}$ by (4.9), and each $S/P_i^{e_i}$ has an S -composition series

$$S/P_i^{e_i} \supset P_i/P_i^{e_i} \supset P_i^2/P_i^{e_i} \supset \dots \supset P_i^{e_i}/P_i^{e_i} = 0.$$

Each of the e_i composition factors is isomorphic to \bar{S}_i (see CR (18.24)). Therefore the characteristic polynomial of a acting on $S/P_i^{e_i}$ is $\{h_i(X)\}^{e_i}$, which gives the formula for $\overline{f(X)}$. This formula implies (4.41) at once.]

11. Keep the above notation. Show that $P_i^{e_i-1}$ divides the different $D(S/R)$ for each i . Prove also that

$$(4.42) \quad PS|D \Leftrightarrow T_{L/K}(S) \subseteq P \Leftrightarrow \bar{e}_i T_i(\bar{S}_i) = 0 \text{ for } 1 \leq i \leq g.$$

[Hint: Since each $\varphi_i(a) = 0$ for $a \in P_1 \dots P_g$, (4.41) gives

$$T(P_1 \dots P_g) \subseteq P,$$

whence $P^{-1}P_1 \dots P_g \subseteq D^{-1}$. Therefore $D \subseteq \prod P_i^{e_i-1}$. The first equivalence in (4.42) follows from Exercise 7, the second from (4.41).]

12. Keeping the above notation, call the maximal ideal P_i *tamely ramified* over R if $\bar{e}_i \bar{T}_i$ is not the zero map on \bar{S}_i . Show that P_i is tamely ramified if and only if

$$\bar{e}_i \neq 0 \text{ and } \bar{S}_i \text{ is separable over } \bar{R}.$$

Show further that $T_{L/K}(S) \not\subseteq P$ if and only if there exists at least one maximal ideal P_i of S containing P such that P_i is tamely ramified over R .

13. We call S *tamely ramified** over R if for each maximal ideal P of R , there exists at least one maximal ideal P_i of S such that

$$P_i \supseteq P, P_i \text{ is tamely ramified over } R.$$

Show that S is tamely ramified over R if and only if $T_{L/K}(S) = R$.

[Hint: $T_{L/K}(S) = R$ if and only if $T_{L/K}(S) \not\subset P$ for each P .]

14. Keep the notation of (4.32), and let $m=p^b$ where p is an odd prime and $b \geq 1$. Show that R_m is tamely ramified over \mathbb{Z} if and only if $b=1$. What is the corresponding result when $p=2$?

[Hint: Use (4.40) with $b=1$.]

15. Let R be a Dedekind domain with quotient field K , and let S be the integral closure of R in a finite Galois extension L of K with Galois group G . View S as left RG -module, by setting

$$\left(\sum_{\sigma \in G} \alpha_\sigma \sigma \right) s = \sum_{\sigma \in G} \alpha_\sigma \sigma(s), \alpha_\sigma \in R.$$

Show that if $T_{L/K}(S) = R$, then S is a projective RG -module.

[Hint: Let X be any RG -module, and let $\theta: X \rightarrow S$ be an RG -surjection. Since S is R -projective, there exists an R -homomorphism $\psi: S \rightarrow X$ such that $\theta\psi = \text{identity map on } S$. Put

$$\psi' = \sum_{\sigma \in G} \sigma \cdot \psi s_0 \cdot \sigma^{-1},$$

where s_0 is an element of S of trace 1. Then ψ' is an RG -homomorphism from S to X such that $\theta\psi' = \text{identity map on } S$. Thus, every RG -surjection $\theta: X \rightarrow S$ is RG -split, so S is RG -projective.]

§5. RADICALS

§5A. Basic Definitions

Throughout, let A be a ring with 1, and let “ A -module” mean “left A -module”, unless otherwise stated. A *simple* A -module is a nonzero A -module X whose only submodules are 0 and X . By a *maximal* submodule of an A -module M we mean a submodule $N \subset M$ such that there are no submodules L with $N \subset L \subset M$; thus N is maximal in M if and only if M/N is a simple module.

*Some authors reserve this terminology for the case where *every* maximal ideal P_i of S is tamely ramified over R ; we shall not take this point of view here, since for our purposes the crucial question will be whether $T_{L/K}(S) = R$.

We show at once (by using Zorn's Lemma) that every finitely generated nonzero module M contains maximal submodules. Indeed, we shall prove that given any submodule $N \subseteq M$, there exists a maximal submodule L of M with $N \subseteq L \subset M$. Consider the set

$$S = \{L : N \subseteq L \subset M\},$$

a non-empty subset of submodules of M (note that $N \in S$), and let S be partially ordered by inclusion. We wish to assert that S contains a maximal element. This will follow from Zorn's Lemma as soon as we show that each chain* $\{L_\alpha\}$ from S has an upper bound in S . Clearly $\cup L_\alpha$ is a submodule of M , and we need only show that this union lies in S , that is, that it is a proper submodule of M . Suppose to the contrary that $\cup L_\alpha = M$. Since M is f.g., we have $M = \sum_{i=1}^n Am_i$ for some elements m_1, \dots, m_n . Then each m_i lies in some L_{α_i} , $1 \leq i \leq n$, whence $M = \bigcup_{i=1}^n L_{\alpha_i}$. But for each i, j between 1 and n , one of $L_{\alpha_i}, L_{\alpha_j}$ contains the other, since $\{L_\alpha\}$ is a chain. Thus $\bigcup_{i=1}^n L_{\alpha_i}$ is some L_{α_k} , which gives $M = L_{\alpha_k}$, a contradiction. We have thus shown that every chain $\{L_\alpha\}$ from S has an upper bound in S . Thus, by Zorn's Lemma, S has a maximal element L . Clearly $N \subseteq L \subset M$, and L is a maximal submodule of M , as desired.

For each surjection $f: M \rightarrow X$ with X simple, clearly $\ker f$ is a maximal submodule of M . Conversely, if L is maximal in M , then L is the kernel of the natural surjection $M \rightarrow M/L$. Thus, we can characterize maximal submodules of M as kernels of surjections $M \rightarrow X$, with X simple.

The *radical* of an A -module (denoted by $\text{rad } M$) is defined as the intersection of all maximal submodules of M . (If M has no maximal submodules, set $\text{rad } M = M$.) By the preceding remarks,

$$\text{rad } M \subset M$$

for every nonzero finitely generated A -module M . Furthermore, for any module M , we have

$$\text{rad } M = \bigcap_{f: M \rightarrow X} \ker f,$$

where the intersection is taken over all surjections $f: M \rightarrow X$ with X simple.

(5.0) Example. If M is a simple A -module, then $\text{rad } M = 0$ since 0 is the only maximal submodule of M . More generally, we claim that $\text{rad } M = 0$ for every semisimple left A -module M . Indeed, by (3.12) we may express M as a direct

*A chain $\{L_\alpha\}$ in a partially ordered set (S, \leq) is a subset of S such that for each α and β , either $L_\alpha \leq L_\beta$ or $L_\beta \leq L_\alpha$.

sum $\bigoplus_{i \in I} M_i$ of simple submodules $\{M_i\}$. If any summand is omitted, the remaining direct sum is a maximal submodule of M . Therefore the intersection of all maximal submodules of M is 0, that is, $\text{rad } M = 0$.

It may well happen that $\text{rad } M = 0$ even though M is not a semisimple module. For example, let $M = \mathbb{Z}$, a left \mathbb{Z} -module. The maximal submodules of M are given by $\{p\mathbb{Z} : p \text{ prime}\}$, and their intersection is 0. Thus $\text{rad } M = 0$, but M cannot be expressed as a direct sum of simple submodules.

(5.1) Proposition. *Let L, M be A -modules.*

(i) *For each A -homomorphism $g: L \rightarrow M$, we have*

$$g(\text{rad } L) \subseteq \text{rad } M.$$

(ii) *If $L \subseteq M$, then*

$$\text{rad } L \subseteq \text{rad } M, \text{ and } (\text{rad } M + L)/L \subseteq \text{rad}(M/L).$$

(iii) *If $L \subseteq \text{rad } M$, then*

$$(\text{rad } M)/L = \text{rad}(M/L).$$

Proof. To prove (i), let $f: M \rightarrow X$ be any surjection with X simple. Then there is a map $fg: L \rightarrow X$, and the image $(fg)(L)$ is a submodule of X . Since X is simple, it follows that either $(fg)(L) = X$ or $(fg)(L) = 0$. In the first case we have a surjection $fg: L \rightarrow X$, whence $(fg)(\text{rad } L) = 0$, and so $g(\text{rad } L) \subseteq \ker f$. In the second case we have $g(\text{rad } L) \subseteq g(L) \subseteq \ker f$. Thus for each f we have $g(\text{rad } L) \subseteq \ker f$, and hence

$$g(\text{rad } L) \subseteq \bigcap_f \ker f = \text{rad } M.$$

This proves (i).

Now let $L \subseteq M$; this inclusion map yields an inclusion $\text{rad } L \subseteq \text{rad } M$, by (i). On the other hand, let $g: M \rightarrow M/L$ be the natural surjection. Then by (i),

$$(\text{rad } M + L)/L = g(\text{rad } M) \subseteq \text{rad}(M/L),$$

which establishes the second assertion in (ii).

Finally, suppose that $L \subseteq \text{rad } M$. The correspondence $N \rightarrow N/L$ maps each maximal submodule N of M containing L onto a maximal submodule N/L of M/L , and is bijective. However, since $\text{rad } M$ is the intersection of all maximal submodules of M , the hypothesis on L implies that every maximal submodule N of M must contain L . Therefore

$$(\text{rad } M)/L = (\bigcap N)/L = \bigcap(N/L) = \text{rad}(N/L),$$

where the intersections are taken over all maximal submodules N of M . This completes the proof of the proposition.

(5.2) Corollary. *Let M be an A -module. Then $M/\text{rad } M$ has radical 0, and $\text{rad } M$ is the smallest submodule M' of M such that $\text{rad}(M/M')=0$.*

Proof. By (5.1iii), with $L=\text{rad } M$, we have

$$\text{rad}\{M/(\text{rad } M)\}=(\text{rad } M)/(\text{rad } M)=0.$$

On the other hand, if $\text{rad}(M/M')=0$ then by (5.1) it follows that $\text{rad } M \subseteq M'$. This completes the proof.

(5.3) Corollary. *Let M be a finitely generated A -module, and let L be a submodule such that $L+\text{rad } M=M$. Then necessarily $L=M$.*

Proof. By (5.1ii) we deduce that $M/L \subseteq \text{rad}(M/L)$, whence equality must hold. But M/L is a finitely generated A -module, since M is finitely generated. We have already remarked above that $\text{rad } X \subset X$ for every nonzero finitely generated module X . Thus M/L must be zero, and the proof is finished.

(5.4) Definition. The *Jacobson radical* of A , denoted by $\text{rad } A$, is the radical of the left regular module ${}_A A$. (Jacobson [45b]). Thus

$$\text{rad } A = \bigcap L, \quad L \text{ ranging over all maximal left ideals of } A.$$

Let us give another description of $\text{rad } A$. For each A -module X , define its *annihilator* as

$$\text{ann } X = \{a \in A : aX = 0\},$$

which is obviously a two-sided ideal of A .

(5.5) Proposition. *We have $\text{rad } A = \bigcap_X \text{ann } X$, where X ranges over all simple left A -modules. Thus $\text{rad } A$ is a two-sided ideal of A .*

Proof. Let X be simple; then $X = Ax$ for each nonzero $x \in X$, and there is a surjection $A \rightarrow X$ given by $a \mapsto ax$, $a \in A$. The kernel of this surjection must be a maximal left ideal L of A , and clearly $L = \text{ann } x = \{a \in A : ax = 0\}$. Thus

$$\bigcap_X \text{ann } X = \bigcap_X \left\{ \bigcap_{x \in X} \text{ann } x \right\} \supseteq \bigcap L' = \text{rad } A,$$

where L' ranges over all maximal left ideals of A .

To prove the reverse inclusion, observe that by the preceding paragraph, every simple X is of the form A/L for some maximal left ideal L of A . If $aX = 0$ then $aA \subseteq L$, whence $a \in L$ since $1 \in A$. This shows that $\text{ann } X \subseteq L$, and

hence

$$\bigcap_X \text{ann } X \subseteq \bigcap_L L = \text{rad } A,$$

since L may range over all maximal left ideals of A . This completes the proof of the formula

$$\text{rad } A = \bigcap_X \text{ann } X.$$

Finally, each $\text{ann } X$ is a two-sided ideal of A , whence so is $\text{rad } A$.

For future reference, we list some direct consequences of (5.1); these are assertions about radicals of *rings*, and as we shall see, they follow readily from results about radicals of *modules*.

(5.6) Proposition. (i) *For each ring A , the factor ring $A/\text{rad } A$ has radical 0.*

(ii) *For any surjection of rings $f: A \rightarrow B$, we have $f(\text{rad } A) \subseteq \text{rad } B$, and f induces a surjection $A/\text{rad } A \rightarrow B/\text{rad } B$.*

(iii) *For each A -module M , $(\text{rad } A)M \subseteq \text{rad } M$.*

Proof. Assertion (i) follows by applying (5.2) with $M = {}_A A$. To prove (ii), view B as a left A -module by means of f . By (5.1) we have $f(\text{rad } A) \subseteq \text{rad}_A B$, where $\text{rad}_A B$ is the intersection of the maximal A -submodules of B . But the left A -submodules of B coincide with the left B -submodules of B , since f is surjective. Thus $\text{rad}_A B$ is identical with the Jacobson radical $\text{rad } B$ of the ring B . We have thus established that $f(\text{rad } A) \subseteq \text{rad } B$, which implies at once that f induces a surjection of rings: $A/\text{rad } A \rightarrow B/\text{rad } B$.

Finally, let M be any left A -module, and consider a surjection $g: M \rightarrow X$ with X simple. Then

$$g((\text{rad } A)M) \subseteq (\text{rad } A)X = 0,$$

whence $(\text{rad } A)M \subseteq \text{rad } M$ as claimed.

(5.7) Nakayama's Lemma. *Let M be a finitely generated left A -module, and let $L \subseteq M$ be a submodule such that*

$$L + (\text{rad } A)M = M.$$

Then necessarily $L = M$.

Proof. Since $(\text{rad } A)M \subseteq \text{rad } M$ by (5.6), the hypotheses imply that $L + \text{rad } M = M$. Therefore $L = M$ by (5.3), and the proof is finished.

There is another characterization of radicals of rings in terms of units, which is extremely useful. We begin with some results of independent interest.

(5.8) Proposition. *Let M be a noetherian A -module, and let $f \in \text{End}_A M$ be such that $f(M) = M$. Then f is an isomorphism.*

Proof. We need only show that f is injective. For $n \geq 1$, set

$$K_n = \ker f^n = \{m \in M : f^n(m) = 0\}.$$

Then $K_1 \subseteq K_2 \subseteq \dots$ is an ascending chain of submodules of M . Since M is noetherian, the chain must terminate, so $K_n = K_{n+1}$ for some n . Now let $m \in M$ be such that $f(m) = 0$. Since $M = f(M)$ we have also $M = f^n(M)$, so $m = f^n(m')$ for some $m' \in M$. Then $0 = f(m) = f^{n+1}(m')$, whence $m' \in K_{n+1}$. But then $m' \in K_n$, so $f^n(m') = 0$, that is, $m = 0$ as desired. This completes the proof.

An element $u \in A$ is a *unit* if there exists an element $v \in A$ such that $uv = vu = 1$. The group of units in A will be denoted by A^\times or $u(A)$. In many cases which occur in this book, each $u \in A$ having one-sided inverse is necessarily a unit of A . In fact, we have:

(5.9) Proposition. *Let A be a left noetherian ring, and let $ab = 1$ in A . Then also $ba = 1$, so $a, b \in A^\times$.*

Proof. We apply (5.8) with M the noetherian A -module $_AA$. We have

$$A = Aab \subseteq Ab \subseteq A,$$

whence $Ab = A$. Thus the left A -endomorphism $x \mapsto xb$, $x \in A$, is surjective. Hence it is injective by (5.8). But then from $(1 - ba)b = b - bab = 0$ we may conclude that $1 - ba = 0$, as claimed.

We now prove the following basic result:

(5.10) Theorem. *For any ring A with 1, we have*

$$\begin{aligned} \text{rad } A &= \{x \in A : 1 - axb \in A^\times \text{ for all } a, b \in A\} \\ &= \{x \in A : 1 - ax \text{ has a left inverse for all } a \in A\}. \end{aligned}$$

Further, for each $x \in \text{rad } A$ and each $a \in A$, a left inverse of $1 - ax$ is necessarily a two-sided inverse.

Proof. Step 1. Let $x \in \text{rad } A$, and let $a, b \in A$; we shall show that $1 - axb$ has a two-sided inverse in A . Since $axb \in \text{rad } A$, it suffices to show that for

each $x \in \text{rad } A$, we have $1-x \in A'$. Consider the left ideal $A(1-x)$ of A ; if $A(1-x) \neq A$, then

$$A(1-x) \subseteq L \subset A$$

for some maximal left ideal L of A . But then $1-x \in L$, and also $x \in \text{rad } A \subseteq L$, whence also $1 = (1-x) + x \in L$. This is impossible, and proves that $A(1-x) = A$. Therefore

$$1 = t(1-x) \text{ for some } t \in A.$$

This gives

$$1-t = -tx \in \text{rad } A,$$

so by the same reasoning there is an element $u \in A$ such that

$$1 = u(1-(1-t)).$$

Thus $ut = 1$, and so

$$u = ut(1-x) = 1-x.$$

This proves that t is a two-sided inverse of $1-x$, so $1-x \in A'$ as desired.

Step 2. Let $x \in A$ be such that $1-ax$ has a left inverse in A , for each $a \in A$. To complete the proof of the theorem, we must show that $x \in \text{rad } A$. By (5.5) it suffices to show that $xW=0$ for each simple left A -module W . If $xW \neq 0$, then $xw \neq 0$ for some $w \in W$, and so $W = A \cdot xw$. Therefore $w = axw$ for some $a \in A$, that is, $(1-ax)w = 0$. But then $w = 0$, since $1-ax$ has a left inverse in A . This is a contradiction, and establishes the following inclusion:

$$\{x \in A : 1-ax \text{ has a left inverse for all } a \in A\} \subseteq \text{rad } A.$$

Thus the theorem is proved, since the final assertion thereof is obvious from the preceding assertions.

(5.11) Corollary. *The radical of the right regular module A_A coincides with $\text{rad } A$. Thus*

$$\text{rad } A = \bigcap R = \bigcap \text{ann } Y,$$

where R ranges over all maximal right ideals of A , and Y ranges over all simple right A -modules.

Proof. The first formula for $\text{rad } A$ in (5.10) is left-right symmetric, which implies the desired result.

We note also that by virtue of this symmetry we have

$$(5.12) \quad \text{rad } A = \{x \in A : 1 - xb \text{ has a right inverse for all } b \in A\}.$$

To conclude this subsection, we shall compute the radicals of some rings related to the ring A . Recall that an *idempotent* in A is a nonzero $e \in A$ such that $e^2 = e$. Thus eAe is a ring with identity element e . We prove (following the treatment in Behrens [72, p. 154, Th. 8]):

(5.13) Proposition. *Let $e \in A$ be idempotent, and let $J = \text{rad } A$. Then*

$$\text{rad } eAe = eJe.$$

If $\bar{A} = A/J$, then

$$eAe / \text{rad}(eAe) \cong \bar{e}\bar{A}\bar{e}.$$

Proof. Clearly

$$eJe = J \cap eAe,$$

since for each $x \in J \cap eAe$, we have $x = exe \in eJe$. This shows that eJe contains the intersection, and the reverse inclusion is obvious.

Suppose now that $x \in eJe$; then $ex = xe = x$, and for each $a \in eAe$, $1 - ax$ has a left inverse $y \in A$. Thus $y(1 - ax) = 1$, so

$$ey(e - ax) = ey(1 - ax)e = e.$$

This shows that $e - ax$ has a left inverse in eAe , whence $x \in \text{rad } eAe$ by (5.10). Thus $eJe \supseteq \text{rad } eAe$.

Conversely, let $x \in \text{rad } eAe$. To prove that $x \in eJe$, it suffices to show that $x \in J$. By (5.10), we need only verify that for each $a \in A$, the element $1 - ax$ has a left inverse in A . But $eae \in A$, so $e - eae \cdot x$ has a left inverse z in eAe . Thus

$$z(e - eae \cdot x) = e, \quad ze = ez = e,$$

and so

$$z - zax = e.$$

Therefore

$$\begin{aligned} (1 - e + z)(1 - ax) &= (1 - e)(1 - ax) + z(1 - ax) \\ &= (1 - e)(1 - ax) + e = 1 - (1 - e)ax = 1 - y, \end{aligned}$$

where $y = (1 - e)ax$. But $y^2 = 0$, so $(1 + y)(1 - y) = 1$. This gives

$$(1 + y)(1 - e + z)(1 - ax) = (1 + y)(1 - y) = 1,$$

so $1 - ax$ has a left inverse in A . This completes the proof that $eJe = \text{rad } eAe$.

Finally, the kernel of the surjection $eAe \rightarrow \bar{e}\bar{A}\bar{e}$ is $eAe \cap J$. Since we have just shown that this intersection equals the radical of eAe , the final assertion of the proposition is established.

(5.14) Proposition. *Let $B = M_n(A)$ be a full matrix ring over the ring A , and let $J = \text{rad } A$. Then*

$$\text{rad } B = M_n(J)$$

and

$$B/\text{rad } B \cong M_n(A/J).$$

Proof. Since the rings A and B are Morita equivalent, every two-sided ideal of B is of the form $M_n(I)$, with I a two-sided ideal of A . Let us write $\text{rad } B = M_n(I)$, and let $\{e_{ij} : 1 \leq i, j \leq n\}$ be a set of matrix units in B . Then $e_{11}Be_{11}$ consists of all $n \times n$ matrices with arbitrary elements of A in the $(1, 1)$ -position, and zeros elsewhere. We shall treat the ring isomorphism $e_{11}Be_{11} \cong A$ as an identification. By (5.13) we then obtain

$$I = e_{11}(\text{rad } B)e_{11} = \text{rad}(e_{11}Be_{11}) = \text{rad } A = J,$$

so $\text{rad } B = M_n(J)$ as claimed. The formula for $B/\text{rad } B$ is then obvious.

§5B. Radicals of Artinian Rings

We recall that a left ideal N in a ring A is *nilpotent* if there exists a positive integer k such that the k -fold product $N \cdot N \cdots N$ equals 0, or equivalently, if $x_1x_2 \cdots x_k = 0$ for all $\{x_i\} \subset N$. An element $x \in A$ is *nilpotent* if $x^k = 0$ for some k , and a left ideal is a *nil ideal* if each of its elements is nilpotent. Nilpotent ideals are clearly nil ideals, but there exist rings for which the reverse is not true.

(5.15) Proposition. *In a left artinian ring A , $\text{rad } A$ is a nilpotent ideal. Moreover $\text{rad } A$ contains all nilpotent one-sided ideals (left or right) and all one-sided nil ideals.*

Proof. (Jacobson [45b]). Let $J = \text{rad } A$. By the minimum condition there exists an integer $m > 0$ such that $J^m = J^{m+1} = \cdots$. We shall prove that $J^m = 0$. If this is not the case, then $J^m = J^{2m} \neq 0$, and there exist left ideals I such that $J^m I \neq 0$. Again by the minimum condition, there is a minimal such left ideal I_0 . Then $J^m I_0 \neq 0$, which implies that $J^m a \neq 0$ for some $a \in I_0$. But $J^m a \subseteq I_0$, and moreover, $J^m (J^m a) = J^{2m} a = J^m a \neq 0$. By the minimality of I_0 , we have $I_0 = J^m a$; hence $a \in J^m a$, and so $a = xa$ for some $x \in J^m$. Then $(1-x)a = 0$, with $x \in J^m \subset J$, and hence $a = 0$ because $1-x$ is invertible by (5.10). This is a contradiction, and we have proved that J is nilpotent.

Now let N be a nil left ideal; then for each $x \in N$, $x^k = 0$ for some k , and hence $1 - x$ is invertible, with inverse $\sum_{i=0}^{\infty} (-1)^i x^i$ (which is just a finite sum because $x^k = 0$). For each $x \in N$, $ax \in N$ for all $a \in A$, and so $1 - ax$ is invertible for all $a \in A$, and $x \in \text{rad } A$ by (5.10). A similar argument shows that each nil right ideal is contained in $\text{rad } A$, and because nilpotent ideals are nil ideals, the proposition is proved.

In a left artinian ring, there is a useful connection between nilpotence of ideals and the existence of idempotents.

(5.16) Proposition. *In a left artinian ring, each non-nilpotent left ideal contains an idempotent element.*

Proof. CR (24.2) or MO (6.8).

The proof in CR (24.2) can be modified to prove the existence of idempotents under weaker hypotheses:

(5.17) Proposition. *Let N be a nilpotent left ideal in an arbitrary ring A , and let $x \in A$ be a non-nilpotent element such that $x^2 - x \in N$. Then the left ideal Ax contains an idempotent element y such that $y - x \in N$.*

Proof. MO (6.7).

For left artinian rings there is a close connection between radicals and the concept of semisimplicity introduced in §3. Recall that a left A -module M is *semisimple* if M is a direct sum of some family of simple submodules, or equivalently (see (3.12)) if every submodule of M is a direct summand of M . The ring A is (left) *semisimple* if every left A -module is semisimple. We now prove the following basic result.

(5.18) Theorem. *A left artinian ring A is left semisimple if and only if $\text{rad } A = 0$.*

Proof. By (5.5), $\text{rad } A$ annihilates every simple left A -module. Hence if A is left semisimple, then $(\text{rad } A)A = 0$, and therefore $\text{rad } A = 0$ since $1 \in A$.

Conversely, suppose that $\text{rad } A = 0$, so by (5.15) the ring A contains no nilpotent left ideals except 0. Hence by (5.16) every nonzero left ideal of A contains an idempotent element. Now define a *minimal left ideal* of A to be a simple submodule of $_A A$. Under our assumption that $\text{rad } A = 0$, each minimal left ideal L contains an idempotent e . Clearly $Ae \subseteq L$, and Ae is a nonzero submodule of L since $e = e^2 \in Ae$. Therefore $L = Ae$, which shows that when $\text{rad } A = 0$, every minimal left ideal L of A is generated by an idempotent e ; indeed, we have further

$$Le = Ae \cdot e = Ae = L.$$

Using this, let us show that L is a direct summand of each left ideal L' of A containing L . In fact, there is a direct sum decomposition of left A -modules:

$$L' = L \oplus L'(1 - e),$$

since the inclusions

$$L = Ae \supseteq L'e \supseteq Le = L$$

show that $L'e = L$.

Now the left artinian module ${}_A A$ clearly is expressible as a finite direct sum of indecomposable modules. By the above, each of these indecomposable summands must be a minimal left ideal of A . Therefore ${}_A A$ is a semisimple module, that is, A is a left semisimple ring.

By Exercise 3.4, a ring is left semisimple if and only if it is right semisimple. For convenience of terminology, we omit the adjectives “left”, “right”, and refer to such rings as *semisimple* rings. We have at once

(5.19) Proposition. *For each left artinian ring A , the factor ring $A/\text{rad } A$ is an artinian semisimple ring.*

Proof. Let $B = A/\text{rad } A$; then $\text{rad } B = 0$ by (5.6i). Further, since A is left artinian, so is B . Hence B is semisimple by (5.18).

(5.20) Hopkin's Theorem. *Every left artinian ring (with 1) is necessarily left noetherian.*

Proof. See CR (54.1).

§5C. Local Rings

A ring A is *local* (or *completely primary*) if A has a unique maximal left ideal. It follows at once, from Definition 5.4 of $\text{rad } A$, that A is local if and only if $\text{rad } A$ is a maximal left ideal of A .

(5.21) Proposition. *The following are equivalent:*

- (i) A is local.
- (ii) The set S of non-units in A is a left ideal.
- (iii) $A/\text{rad } A$ is a division ring, that is, a skewfield.

Proof. (i) \Rightarrow (ii). We are given that $\text{rad } A$ is a maximal left ideal. We shall prove that $\text{rad } A$ coincides with the set of S of non-units. Clearly $\text{rad } A \subseteq S$.

Conversely, let $x \in S$, and consider the left ideal Ax . If $Ax \neq A$, then Ax is contained in a maximal left ideal, hence $Ax \subseteq \text{rad } A$. If $Ax = A$, then for some $y \in A$, $yx = 1$. Clearly $y \notin \text{rad } A$, hence $Ay = A$ and there exists z such that $zy = 1$. Then y is invertible, and hence x is invertible, contrary to assumption.

(ii) \Rightarrow (iii). If the set S of non-units in A is a left ideal, then clearly $S = \text{rad } A$, and A is local. Then $A/\text{rad } A$ contains no nontrivial left ideals, and is a division ring.

Finally, (iii) \Rightarrow (i) by an easy argument, and the result is proved.

In §4A, we have already encountered an example of a local ring. Namely, let P be a prime ideal in a commutative ring R ; then the localization R_P of R at P is a local ring, and $\text{rad } R_P = P \cdot R_P$. Likewise the discrete valuation rings occurring in §4C are local rings. Of course, every field or division ring is local. Much more important for us, however, is the fact that under suitable hypotheses, a module (over a ring) is indecomposable if and only if its endomorphism ring is local (see §6 below).

For the remainder of this section, we fix the following notation:

R = commutative local ring

$P = \text{rad } R$ = unique maximal ideal of R

$\bar{R} = R/P$ = residue class field of R

A = R -algebra

$\bar{A} = A/PA$.

We recall that an R -algebra A comes equipped with a homomorphism Φ of R into the center of A , such that $\Phi(1_R) = 1_A$. By virtue of this homomorphism, every A -module may be viewed as R -module. In particular, A is itself an R -module, and \bar{A} is an algebra over the field \bar{R} . The following basic result relates $\text{rad } A$ with $\text{rad } \bar{A}$.

(5.22) Proposition. *Let R be a commutative local ring with residue class field $\bar{R} = R/P$, and let A be an R -algebra which is finitely generated as R -module. Set $\bar{A} = A/PA$, a finite dimensional \bar{R} -algebra, and let $\varphi: A \rightarrow \bar{A}$ be the natural surjection. Then*

$$(i) \quad \text{rad } A = \varphi^{-1}(\text{rad } \bar{A}) \supseteq PA.$$

(ii) *The map φ induces an isomorphism of \bar{R} -algebras*

$$A/\text{rad } A \cong \bar{A}/\text{rad } \bar{A}.$$

(iii) *$A/\text{rad } A$ is a semisimple artinian ring.*

(iv) *There exists a positive integer k such that*

$$(\text{rad } A)^k \subseteq PA.$$

Proof. We show first that $PA \subseteq \text{rad } A$ by proving that $PA \cdot M = 0$ for each simple left A -module M . Since $M = Am$ for each nonzero $m \in M$, it follows that M is finitely generated as R -module. Now PM is an A -submodule of M , and hence is either M or 0. But $PM \neq M$ by Nakayama's Lemma 5.7, since otherwise $M = 0$. Thus $PM = 0$, whence $PA \cdot M = 0$ for each simple A -module M . This proves that $PA \subseteq \text{rad } A$.

By (5.6ii), the surjection $\varphi: A \rightarrow \bar{A}$ induces a surjection

$$A/\text{rad } A \rightarrow \bar{A}/\text{rad } \bar{A}.$$

On the other hand, since $PA \subseteq \text{rad } A$ there is also a surjection

$$\psi: \bar{A} \rightarrow A/\text{rad } A.$$

By (5.6) we have

$$\psi(\text{rad } \bar{A}) \subseteq \text{rad}(A/\text{rad } A) = 0,$$



and therefore ψ induces a surjection

$$\bar{A}/\text{rad } \bar{A} \rightarrow A/\text{rad } A.$$

But both $A/\text{rad } A$ and $\bar{A}/\text{rad } \bar{A}$ are finite dimensional algebras over the field \bar{R} , and each is a homomorphic image of the other. Hence each of these surjections must be an isomorphism, which proves (i) and (ii). Assertion (iii) follows at once from (ii), by use of (5.19).

Finally, since \bar{A} is artinian it follows from (5.15) that $(\text{rad } \bar{A})^k = 0$ for some k . Therefore $\varphi((\text{rad } A)^k) = 0$, whence $(\text{rad } A)^k \subseteq \ker \varphi = PA$. This completes the proof of the proposition.

Keeping the above notation, let us briefly discuss completions (see §4C). Given a finitely generated R -module X , we give X a *P-adic topology* by choosing as basis for the neighborhoods of a point $x \in X$ the open sets

$$\{x + P^k X : k = 0, 1, 2, \dots\}.$$

Let \hat{X} denote the *P-adic completion* of X in this topology, and in particular let \hat{R} be the completion of R .

If, for example, $X = \bigoplus_{i=1}^m Rx_i$ is R -free, then $P^k X = \bigoplus_{i=1}^m P^k x_i$. If $\{y_n\}$ is a sequence of elements of X , we may write

$$y_n = \sum_{i=1}^m r_n^{(i)} x_i, \quad r_n^{(i)} \in R.$$

It is then obvious that $\{y_n\}$ is a Cauchy sequence relative to the *P-adic topology* on X if and only if for each i , $\{r_n^{(i)}\}$ is a Cauchy sequence relative to the *P-adic topology* on R . Further, $\{y_n\}$ converges in X if and only if each

$\{r_n^{(i)}\}$ converges in R , and we have

$$\lim_{n \rightarrow \infty} \sum_{i=1}^m r_n^{(i)} x_i = \sum_{i=1}^m \left(\lim_{n \rightarrow \infty} r_n^{(i)} \right) x_i.$$

Thus X is complete if and only if R is complete.

When R is not complete, we may form the P -adic completions \hat{R} and \hat{X} , and the preceding discussion shows that there is a topological \hat{R} -isomorphism

$$(5.23) \quad \hat{X} \cong \hat{R} \otimes_R X.$$

As a matter of fact (see MO (6.16) and references listed there), the isomorphism (5.23) holds true for any finitely generated R -module X , provided that R is a commutative noetherian local ring. Furthermore, \hat{R} and \hat{X} are complete Hausdorff spaces relative to the topologies induced on them by the P -adic topologies of R and X . We shall use this fact primarily for the case where R is the P -adic completion of a discrete valuation ring with maximal ideal P (see §4C).

Let us conclude this subsection with some important examples of local rings. We prove

(5.24) Theorem. *Let G be a finite p -group, and let K be a field of characteristic p . Then there is exactly one simple left KG -module, namely, the field K on which the elements of G act trivially. Further, KG is a local ring, and*

$$\text{rad } KG = \bigoplus_{x \in G - \{1\}} K(x-1),$$

the augmentation ideal of KG . Moreover, every f.g. projective KG -module is free.

Proof. The result is clear if $|G|=1$, so assume now that $|G|=p^n$, $n > 0$, and use induction on n . Let V be any simple KG -module, and let

$$H = \{x \in G : x \text{ acts trivially on } V\}.$$

Then $H \trianglelefteq G$, and V is also a simple $K(G/H)$ -module. If $H \neq 1$, then V is the trivial module K by the induction hypothesis. So now suppose that $H=1$, that is, if $(x-1)V=0$ for some $x \in G$, then $x=1$. By §1, the group G has a nontrivial center $Z(G)$; choosing $x \in Z(G)$, $x \neq 1$, it is then clear that $(x-1)V$ is a nonzero submodule of V . Hence $V=(x-1)V$. But then for all $n \geq 1$,

$$V = (x-1)V = (x-1)^2V = \cdots = (x-1)^{p^n}V = (x^{p^n}-1)V = 0,$$

a contradiction. This completes the proof that $V \cong K$.

Now $\text{rad } KG$ is the intersection of the annihilators of the simple KG -modules, and thus $\text{rad } KG$ is the annihilator of K . Let $J = \bigoplus K(x-1)$, summed over all $x \in G - \{1\}$. Then J annihilates the simple module K , so $J \subseteq \text{rad } KG$. But $\dim_K J = |G| - 1$, and $\text{rad } KG \subset KG$. Therefore $\text{rad } KG = J$, as claimed. Hence KG is local by (5.21). The final assertion now follows from Exercise 6.9.

(5.25) Corollary. *Let G be a p -group, and let R be a commutative local ring with $P = \text{rad } R$, and let $\bar{R} = R/P$ be a field of characteristic p . Then the group ring RG is local, and*

$$\text{rad } RG = PG + I, \quad RG/\text{rad } RG \cong R/P,$$

where

$$I = \bigoplus_{\substack{x \in G \\ x \neq 1}} R(x-1)$$

is the augmentation ideal of RG . Further, every f.g. projective RG -module is free.

Proof. By (5.22), $\text{rad } RG$ is the inverse image of $\text{rad } \bar{R}G$ under the surjection

$$RG \rightarrow RG/P \cdot RG \cong \bar{R}G, \text{ where } \bar{R} = R/P.$$

The result now follows from (5.24) and Exercise 6.9.

(5.26) Proposition. *Let p be prime, and let D be a normal p -subgroup of a finite group G . Let R be a commutative local ring whose residue class field \bar{R} has characteristic p . Then the natural surjection $\tau: RG \rightarrow R(G/D)$ has the property that $\ker \tau$ is nilpotent mod PG , and hence $\ker \tau \subseteq \text{rad}(RG)$.*

Proof. By the preceding discussion, it is sufficient to work over the field \bar{R} . As an exercise, the reader can verify that $\ker \tau$ is generated by elements of the form $g(x-1)$, with $g \in G$, $x \in D$. The identity

$$g(x-1)g'(x'-1) = gg'((g')^{-1}xg' - 1)(x'-1),$$

combined with (5.24), shows that $\ker \tau$ is nilpotent mod PG , and the result follows. (See also (17.16).)

We end this subsection with a few remarks about semilocal rings.

(5.27) Definition. The ring A is *semilocal* if $A/\text{rad } A$ is a semisimple artinian ring. (Local rings are automatically semilocal!)

By (5.6i), the factor ring $A/\text{rad } A$ has radical 0. Thus by (3.16) and (5.18), this factor ring is semisimple if and only if it is artinian. Hence the ring A is semilocal if and only if $A/\text{rad } A$ is (left) artinian. This gives

(5.28) Proposition. (i) *Every left artinian ring is semilocal.*

(ii) *Every R -algebra A , as in (5.22), is semilocal.*

Let us point out that \mathbf{Z} is *not* semilocal, so there exist rings which are not semilocal. More generally, any Dedekind domain A with an infinite number of maximal ideals is not semilocal.

For semilocal rings, there is an important relation between radicals of modules and the Jacobson radical of the ring. We have:

(5.29) Proposition. *Let M be a left A -module, where A is any semilocal ring. Then*

$$\text{rad } M = (\text{rad } A)M.$$

Proof. Put $J = \text{rad } A$, $\bar{A} = A/J$, so \bar{A} is a semisimple artinian ring. Then M/JM is a left \bar{A} -module, hence is semisimple by (3.15). Thus $\text{rad}(M/JM) = 0$ by (5.0). However,

$$\text{rad}(M/JM) = (\text{rad } M)/JM$$

by (5.1iii), since we already know that $\text{rad } M \subseteq JM$ from (5.6). Thus $\text{rad } M = JM$, as claimed.

§5. Exercises

1. Prove that every maximal two-sided ideal J of the ring A must contain $\text{rad } A$.

[Hint: If not, then $J + \text{rad } A = A$; now use Nakayama's Lemma.]

2. Show that an element x of a ring A is a unit if and only if the image of x in $A/\text{rad } A$ is a unit.

3. Let A be a ring such that $A/\text{rad } A$ is semisimple artinian, and let J be a one-sided ideal of A such that $J'' \subseteq \text{rad } A$. Prove that $J \subseteq \text{rad } A$.

[Hint: The image of J in the semisimple artinian ring $A/\text{rad } A$ is a nilpotent one-sided ideal, hence is 0 by (5.15).]

4. Let $e \in A$ be idempotent, where A is any ring. Show that

$$S \cap eAe = eSe$$

for every subset S of A . Deduce that

$$L = AL \cap eAe$$

for each left ideal L of eAe . Show from this that if A is left noetherian, then so is the ring eAe . Prove the corresponding result when “noetherian” is replaced by “artinian”.

5. Prove that any monomorphism $f: M \rightarrow M$ of an artinian A -module M must be an isomorphism. Here, A is an arbitrary ring.

[Hint: Imitate the proof of (5.8).]

6. Let A be a f.d. algebra over a field K , and let $T: A \times A \rightarrow K$ be the bilinear trace form given by $T(a, b) = T_{A/K}(ab)$, $a, b \in A$, where $T_{A/K}$ is the ordinary trace. Show that if T is nondegenerate then A is semisimple. (See also Exercise 7.6.)

[Hint: Each element of $\text{rad } A$ is nilpotent by (5.15), so has trace 0. For $x \in \text{rad } A$, we obtain $\text{Tr}(x, A) = T_{A/K}(xA) = 0$, so $x = 0$.]

7. Let A be an R -algebra as in (5.22), and let \hat{R} denote the P -adic completion of R . Let $\hat{A} = \hat{R} \otimes_R A$, the P -adic completion of A . Show that

$$\text{rad } \hat{A} = \hat{R} \otimes_R \text{rad } A, \quad \hat{A}/\text{rad } \hat{A} \cong A/\text{rad } A.$$

[Hint: Since P annihilates $A/\text{rad } A$, we have

$$A/\text{rad } A \cong \hat{R} \otimes (A/\text{rad } A) \cong \hat{A}/(\hat{R} \otimes \text{rad } A),$$

where \otimes means \otimes_R . Therefore $\hat{R} \otimes \text{rad } A \subseteq \text{rad } \hat{A}$, since $A/\text{rad } A$ is semisimple. On the other hand, $(\hat{R} \otimes \text{rad } A)^k \subseteq P\hat{A}$ with k as in (5.22iv), whence $\hat{R} \otimes \text{rad } A \subseteq \text{rad } \hat{A}$.]

8. Let R be a commutative local noetherian ring with maximal ideal P , and let M be a f.g. left R -module. Let $f \in \text{Aut}_R(M)$ and $g \in \text{End}_R(M)$ be such that $f \equiv g \pmod{P}$, that is,

$$f - g \in P \cdot \text{End}_R(M).$$

Prove that also $g \in \text{Aut}_R(M)$.

[Hint: The hypothesis implies that $M = g(M) + PM$. Now use (5.7) and (5.8).]

9. Let R be a complete d.v.r. of characteristic zero, with maximal ideal πR and residue class field of characteristic p . Let G be a cyclic p -group of order p^n , where $n \geq 1$. Show that the RG -module $\text{rad } RG$ is indecomposable except possibly when $n = 1$. (The result is due to Ayoub and Ayoub [69] and J. Schmidt.)

[Hint: Let $J = \text{rad } RG = \pi R + (x - 1)RG$, where $G = \langle x \rangle$. Then $\text{End}_{RG}(J) = \{y \in KG : J \cdot y \subseteq J\}$, where K is the quotient field of R . Then J is indecomposable if and only if $\text{End}_{RG}(J)$ contains no nontrivial idempotents. For $0 \leq i \leq n$, let

$$e_i = (x^{p^n} - 1)/(x^{p^i} - 1)p^{n-i} \in K[x]/(x^{p^n} - 1).$$

Show that the primitive idempotents of KG are

$$e_{n-1}, 1 - e_{n-1}, 1 - e_{n-1} - e_{n-2}, \dots, 1 - e_{n-1} - e_{n-2} - \dots - e_0.$$

Here, $e_{n-1} = (1 + x^{p^{n-1}} + x^{2p^{n-1}} + \dots + x^{(p-1)p^{n-1}})/p$. Show that the only idempotents $e \in KG$ such that $Je \subseteq J$ are e_{n-1} and $1 - e_{n-1}$, and this only when $n = 1$ and $\pi R = pR$; in this special case, J is decomposable.]

10. Let M be a f.g. left A -module, where A is a left artinian ring. Show that M is semisimple if and only if $\text{rad } M = 0$.

[Hint: Use (5.29) and (5.5).]

11. Let M and N be A -modules, where A is arbitrary. Prove that

$$\text{rad}(M \oplus N) = \text{rad } M \oplus \text{rad } N.$$

[Hint: Throughout, let X , M' , and N' denote maximal submodules of $M \oplus N$, M , and N , respectively. If $X \supseteq M$ then $X = M \oplus N'$ for some N' ; likewise, if $X \supseteq N$ then $X = M' \oplus N$ for some M' . Suppose now that X does not contain M or N , and let $S = (M \oplus N)/X$, so S is simple. The composition of maps

$$M \rightarrow M \oplus N \rightarrow S$$

is not zero, so $M/M' \cong S$ for some M' . Likewise, $N/N' \cong S$ for some N' . Since

$$(M \oplus N)/(M' \oplus N') \cong S \oplus S,$$

it follows from (5.0) that

$$\bigcap_{X \supseteq M' \oplus N'} X = M' \oplus N'.$$

Therefore

$$\begin{aligned} \text{rad}(M \oplus N) &= \bigcap_{M', N'} \left\{ \left(\bigcap_{X \supseteq M' \oplus N'} X \right) \cap (M' \oplus N) \cap (M \oplus N') \right\} \\ &= \left(\bigcap_{M'} M' \right) \cap \left(\bigcap_{N'} N' \right) = \text{rad } M \oplus \text{rad } N. \end{aligned}$$

The proof is due to Janusz.]

12. Let A be an R -algebra as in (5.22), I any two-sided ideal of A . Show that the surjection $A \rightarrow A/I$ gives a surjection $u(A) \rightarrow u(A/I)$ of unit groups.

[Hint: By (5.6), $\text{rad}(A/I) \supseteq (I + \text{rad } A)/I$. On the other hand,

$$\bar{A} = (A/I)/((I + \text{rad } A)/I) \cong A/(I + \text{rad } A) = \text{factor ring of } A/\text{rad } A.$$

Thus \bar{A} is semisimple artinian, so $\text{rad}(A/I) = (I + \text{rad } A)/I$. Consider the commutative diagram

$$\begin{array}{ccc} A & \longrightarrow & A/I \\ \downarrow & & \downarrow f \\ A/\text{rad } A & \xrightarrow{g} & \bar{A} \end{array}$$

in which each arrow is a ring surjection. For $x \in u(A/I)$, $f(x) \in u(\bar{A})$. But $f(x) = g(y)$ for some $y \in u(A/\text{rad } A)$, since $A/\text{rad } A$ is semisimple. Then y is the image of some $a \in u(A)$, and $a - x \in I + \text{rad } A$. Changing a mod $(\text{rad } A)$ and x mod I , we then have $x = \text{image of an element in } u(A)$.]

§6. IDEMPOTENTS, INDECOMPOSABLE MODULES, AND THE KRULL-SCHMIDT-AZUMAYA THEOREM. PROJECTIVE COVERS AND INJECTIVE HULLS

§6A. Idempotents

Given an arbitrary ring A (with 1), let

$$(6.1) \quad A = L_1 \oplus \cdots \oplus L_n$$

be a direct sum decomposition of A into left ideals $\{L_i\}$, and set

$$1 = e_1 + \cdots + e_n, \quad e_i \in L_i.$$

Then for $x \in A$, we have

$$x = xe_1 + \cdots + xe_n, \quad \text{and } xe_i \in L_i.$$

This shows at once that if $x \in L_i$, then $x = xe_i$ and $xe_j = 0$ for $j \neq i$. Hence we have

$$(6.2) \quad L_i = Ae_i, \quad e_i^2 = e_i, \quad e_i e_j = 0 \text{ for } j \neq i, \quad \text{where } 1 \leq i \leq n.$$

We call $\{e_1, \dots, e_n\}$ a set of *orthogonal idempotents** of A ; they are completely determined by the decomposition (6.1), although there may be many such decompositions of A . Conversely, it is clear that each set of orthogonal idempotents $\{e_1, \dots, e_n\}$ such that $\sum e_i = 1$, gives rise to a direct sum decomposition $A = \bigoplus Ae_i$ into left ideals.

If $e_1 = e' + e''$, where e' and e'' are orthogonal idempotents, then $L_1 = L_1 e' \oplus L_1 e''$; the sum is direct, since right multiplication by e' acts as the identity on $L_1 e'$, and annihilates $L_1 e''$. Conversely, if $L_1 = L' \oplus L''$ is a direct sum of left ideals of A , then we may write $e_1 = e' + e''$ with e', e'' orthogonal idempotents. An idempotent $e \in A$ is called *primitive* if e is not expressible as a sum of two orthogonal idempotents. We have just shown that e is primitive if and only if Ae is an indecomposable left ideal of A . Since the condition of primitivity is left-right symmetric, it follows that e is primitive if and only if

*Recall that $e \in A$ is *idempotent* if $e^2 = e \neq 0$.

eA is an indecomposable right ideal of A . Hence if

$$A = \bigoplus_1^n Ae_i$$

is a decomposition of A into indecomposable left ideals, when the $\{e_i\}$ are a set of orthogonal idempotents, then

$$A = \bigoplus_1^n e_i A$$

is a decomposition into indecomposable right ideals.

Now let M be a left A -module, where A is an arbitrary ring. Let

$$E = \text{End}_A M = \text{Hom}_A(M, M)$$

be the endomorphism ring of M . It will be convenient to regard E as a ring of right operators on M , so that M becomes a bimodule $_A M_E$. We shall imitate the discussion of Morita equivalence in §3D, this time with somewhat different categories, in order to prove the following result of Dress, which extends earlier work of Fitting:

(6.3) Proposition. *Let $_A M_E$ be a bimodule, where $E = \text{End}_A M$. Let $\mathcal{C} = \mathcal{C}(M)$ be the category of all left A -modules which are isomorphic to A -direct summands of $M^{(k)}$ for some k , with $\text{Hom}_{\mathcal{C}}$ just Hom_A . Let \mathcal{P} be the category of all finitely generated projective left E -modules. Then \mathcal{P} and \mathcal{C} are Morita equivalent, that is, there exist covariant functors $F: \mathcal{C} \rightarrow \mathcal{P}$ and $G: \mathcal{P} \rightarrow \mathcal{C}$ such that*

$$GF = \text{id}_{\mathcal{C}}, FG = \text{id}_{\mathcal{P}},$$

up to natural isomorphisms. Thus there is a bijection between isomorphism classes of objects in \mathcal{C} and such classes in \mathcal{P} .

In particular, there is a one-to-one correspondence between decompositions

$$M = \bigoplus_{i=1}^n M_i, M_i = \text{nonzero } A\text{-submodule of } M,$$

and decompositions

$$E = \bigoplus_{i=1}^n E_i, E_i = \text{nonzero left ideal of } E,$$

given as follows: starting with the decomposition of M , let $\pi_i: M \rightarrow M_i$ be the i -th projection map. Then π_i is an idempotent in E , and

$$(6.3a) \quad M_i = M\pi_i, E_i = E\pi_i, M_i = ME_i.$$

Conversely, given a decomposition of E , let $\{\pi_i\}$ be the corresponding set of orthogonal idempotents of E ; then the $\{M_i\}$ are given by (6.3a).

Sketch of Proof. We define functors F, G by

$$F = \text{Hom}_{\mathcal{A}}({}_A M_E, *), G = ({}_A M_E) \otimes_E *.$$

Then (all isomorphisms being natural)

$$F({}_A M) = \text{Hom}_{\mathcal{A}}({}_A M_E, {}_A M) \cong E \text{ as left } E\text{-modules.}$$

Hence $F(M^{(k)}) \cong E^{(k)}$ for each k , whence F maps each A -direct summand of $M^{(k)}$ onto an E -direct summand of $E^{(k)}$; this proves that F is a functor from \mathcal{C} to \mathcal{P} .

Conversely,

$$G({}_E E) = ({}_A M_E) \otimes_E ({}_E E) \cong M \text{ as left } A\text{-modules,}$$

so $G(E^{(k)}) \cong M^{(k)}$, and thus G is a functor from \mathcal{P} to \mathcal{C} . Finally,

$$GF({}_A M) \cong G({}_E E) \cong {}_A M,$$

whence also $GF(X) \cong X$ (naturally) for all $X \in \mathcal{C}$. Likewise

$$FG({}_E E) \cong F({}_A M) \cong {}_E E,$$

so also $GF(P) \cong P$ (naturally) for all $P \in \mathcal{P}$. This completes the proof that \mathcal{C} is Morita equivalent to \mathcal{P} .

In particular, if $\pi : M \rightarrow M'$ is the projection of M onto a nonzero A -direct summand M' , then π is an idempotent in E . The object $M' \in \mathcal{C}$ corresponds to the object

$$F(M') = \text{Hom}_{\mathcal{A}}(M, M') \in \mathcal{P}.$$

But

$$\text{Hom}_{\mathcal{A}}(M, M') = \{f \in \text{End}_{\mathcal{A}} M : f\pi = f\} = E\pi,$$

and further, $M' = M\pi = M \cdot E\pi$. The remaining assertions of the proposition are now obvious.

The preceding result contains the following elementary fact, which can easily be proved directly:

(6.4) Corollary. *A nonzero left A -module M is indecomposable if and only if its endomorphism ring $\text{End}_{\mathcal{A}} M$ has no idempotents except 1.*

A direct proof is an immediate consequence of the correspondence between direct sum decompositions of M and projections in $\text{End}_A M$, and will be omitted.

We shall use this result repeatedly in testing for indecomposability, and so we need some way of testing whether a ring E has a nontrivial idempotent. Certainly, if E is a local ring, its only idempotent is 1; for suppose that $e \in E$ is idempotent, $e \neq 1$. Since $e(1-e)=0$, both e and $1-e$ are non-units; but then so is their sum, since E is local, which gives a contradiction. *Under suitable hypotheses*, the converse also holds: if E has no idempotent except 1, then E is local. In order to prove this, we shall investigate the important question of “lifting idempotents”: if \bar{E} is a factor ring of E , is every idempotent in \bar{E} the image of some idempotent in E ?

Changing notation, let A be an arbitrary ring and let N be a two-sided ideal of A such that $N \subseteq \text{rad } A$. Set $\bar{A} = A/N$, and let $e \in A$. We claim that if $e \in A$ is idempotent, then so is \bar{e} ; since $e^2 = e$ it is clear that $\bar{e}^2 = \bar{e}$. Further, if $\bar{e} = 0$ then $e \in N \subseteq \text{rad } A$; hence $1-e \in u(A)$, so from $e(1-e)=0$ it follows that $e=0$, a contradiction. This shows that each decomposition $1 = \sum e_i$ into orthogonal idempotents in A yields a decomposition $\bar{1} = \sum \bar{e}_i$ of the same kind in \bar{A} . We intend to show that under suitable hypotheses, \bar{e}_i is primitive whenever e_i is primitive, and that each decomposition of $\bar{1}$ “lifts” to a decomposition of 1.

To begin with, we may give A the *N-adic topology*, in which a basis for the open neighborhoods of an element $a \in A$ is given by the sets $\{a + N^k : k = 0, 1, 2, \dots\}$. Call A *complete* in the *N-adic topology* if each Cauchy sequence from A (relative to the *N-adic topology*) converges to a unique element of A . There are two important cases in which A is necessarily complete in the *N-adic topology*:

(6.5) Proposition. *Let N be a two-sided ideal of A contained in $\text{rad } A$. Then A is complete in the *N-adic topology* if either*

(i) *A is left artinian, or*

(ii) *A is an R -algebra which is finitely generated as R -module, where R is a complete commutative noetherian local ring.*

Proof. In case (i), N is nilpotent by (5.15), so any Cauchy sequence (relative to the *N-adic topology* of A) must be constant from some point on. In case (ii), let $P = \text{rad } R$. By (5.22iv), $N^k \subseteq PA$ for some k . Hence any Cauchy sequence relative to the *N-adic topology* is also a Cauchy sequence in A relative to the *P-adic topology*. But A is complete in the *P-adic topology*, by the discussion at the end of §5C. This finishes the proof.

Remark. The hypotheses of the previous proposition hold whenever A is a f.d. algebra over a field, and also whenever A is an R -algebra f.g. as

R -module, where R is a complete discrete valuation ring. These are the two situations which will arise most frequently.

(6.6) Proposition. *Let N be a two-sided ideal in A such that $N \subseteq \text{rad } A$. Let Q and Q' be f.g. projective left \bar{A} -modules. Then $Q \cong Q'$ if and only if $Q/NQ \cong Q'/NQ'$ as A -modules (where $\bar{A} = A/N$).*

Proof (Bass). One way is clear. Conversely, suppose that $Q/NQ \cong Q'/NQ' \cong X$. Since A is projective, there exists a homomorphism $f: Q \rightarrow Q'$ making the diagram

$$\begin{array}{ccc} Q & \xrightarrow{f} & Q' \\ j \searrow & & \swarrow i \\ & X & \end{array}$$

commute, where i and j are homomorphisms with kernels NQ' and NQ , respectively. Let $T = Q'/f(Q)$, the cokernel of f . Then T is finitely generated, and it is easily checked from the diagram that $T = NT$. By Nakayama's Lemma 5.7, we have $T = 0$, so f is surjective. Since Q' is projective, $\ker f$ is a direct summand of Q , and is finitely generated. Again from the diagram it follows that $\ker f = N \cdot \ker f$, and hence $\ker f = 0$ by a second application of Nakayama's Lemma.

In particular, left ideals Ae generated by idempotents e are f.g. projective modules to which (6.6) applies, and we shall shortly make use of this fact.

(6.7) Theorem on Lifting Idempotents. *Let N be a two-sided ideal of A , and set $\bar{A} = A/N$. Suppose that $N \subseteq \text{rad } A$, and that A is complete in the N -adic topology. Then the following statements hold.*

- (i) *For every idempotent $\epsilon \in \bar{A}$ there exists an idempotent $e \in A$ such that $\bar{e} = \epsilon$.*
- (ii) *$Ae_1 \cong Ae_2$ as left A -modules if and only if $\bar{A}\bar{e}_1 \cong \bar{A}\bar{e}_2$, for arbitrary idempotents $e_1, e_2 \in A$.*
- (iii) *An idempotent $e \in A$ is primitive if and only if \bar{e} is primitive in \bar{A} .*

Proof. (i) We start from the identity in $\mathbf{Z}[X]$

$$1 = (X + (1 - X))^{2^n} = \sum_{j=0}^{2^n} \binom{2^n}{j} X^{2^n-j} (1 - X)^j, \quad n = 1, 2, \dots$$

Let

$$f_n(X) = \sum_{j=0}^n \binom{2n}{j} X^{2n-j}(1-X)^j.$$

Then the polynomials $f_n(X)$ have the following properties:

- (a) $f_n(X) \in \mathbf{Z}[X]$;
- (b) $f_n(X) \equiv 0 \pmod{X^n}$ and $f_n(X) \equiv 1 \pmod{(X-1)^n}$
- (c) $\{f_n(X)\}^2 \equiv f_n(X) \pmod{X^n(1-X)^n}$
- (d) $f_n(X) \equiv f_{n-1}(X) \pmod{X^{n-1}(X-1)^{n-1}}$
- (e) $f_1(X) \equiv X \pmod{(X-X^2)}$.

The proofs of (a)–(e) are immediate and will be omitted. Now let ϵ be an idempotent in \bar{A} , and find $a \in A$ such that $\bar{a} = \epsilon$. Then $a^2 - a = 0$, $a^2 - a \in N$, and it follows from (d) that $f_j(a) \equiv f_{j-1}(a) \pmod{N^{j-1}}$. Because A is complete in the N -adic topology, $\lim_{j \rightarrow \infty} f_j(a) = e$ exists in A . From (c) we have $e^2 = e$, and from (e), $e \equiv a \pmod{N}$ so that $\bar{e} = \bar{a} = \epsilon$, completing the proof of (i).

(ii) Follows from (6.6).

(iii) Let e be an idempotent in A , and suppose that \bar{e} is not primitive, so that

$$\bar{e} = \epsilon_1 + \epsilon_2$$

where ϵ_1 and ϵ_2 are orthogonal idempotents in \bar{A} . Choose $a \in A$ such that $\bar{a} = \epsilon_1$, and set $b = eae$. Then $\bar{b} = \bar{e}\bar{a}\bar{e} = \epsilon_1$, and $be = eb = b$. As in the proof of (i), $\lim_{j \rightarrow \infty} f_j(b) = e_1$ exists in A , and it follows that

$$\bar{e}_1 = \bar{b} = \epsilon_1, \text{ and } e_1e = ee_1 = e_1.$$

Letting $e_2 = e - e_1$, we have $e_2^2 = e_2 \neq 0$, and $e_1e_2 = e_2e_1 = 0$, proving that e is not primitive in A . The converse is clear, and (iii) is proved.

Remark. The preceding argument was used in CR Chapter XI, in a less general situation. Other proofs of these results may be found in MO §6.

(6.8) Theorem. Let $\bar{A} = A/N$, where N is a two-sided ideal of A contained in $\text{rad } A$. Assume that either

(i) A is left artinian, or

(ii) A is an R -algebra, finitely generated as R -module, where R is a commutative complete local noetherian ring.

Then A is complete in the N -adic topology, and each decomposition

$$A = Ae_1 \oplus \cdots \oplus Ae_n$$

into indecomposable left ideals $\{Ae_i\}$ of A , yields a decomposition

$$\bar{A} = \bar{A}\bar{e}_1 \oplus \cdots \oplus \bar{A}\bar{e}_n$$

into indecomposable left ideals $\{\bar{A}\bar{e}_i\}$ of \bar{A} . Conversely, each such decomposition of \bar{A} comes from a decomposition of A .

Furthermore, for $1 \leq i, j \leq n$, we have

$$Ae_i \cong Ae_j \Leftrightarrow \bar{A}\bar{e}_i \cong \bar{A}\bar{e}_j.$$

Sketch of Proof. From Proposition 6.5, it follows in both cases that A is complete in the N -adic topology. The proof is then immediate from the preceding two results.

(6.9) Corollary. Let $N = \text{rad } A$, and keep the above notation and hypotheses. Then for each i , $1 \leq i \leq n$, the quotient Ae_i/Ne_i is a simple left A -module, and Ne_i is the unique maximal A -submodule of Ae_i .

Proof. By (5.22) the ring \bar{A} is semisimple, and so indecomposable \bar{A} -modules must be simple. Thus $\bar{A}\bar{e}_i$ is a simple A -module, and hence also a simple left A -module. Since $\bar{A}\bar{e}_i = Ae_i/Ne_i$, it follows that Ne_i is a maximal submodule of Ae_i .

If X is another maximal submodule of Ae_i , then $X + Ne_i = Ae_i$. Therefore

$$X + (\text{rad } A)Ae_i = Ae_i,$$

whence $X = Ae_i$ by Nakayama's Lemma. This is a contradiction, and shows that no such X exists. This completes the proof.

The next result plays a crucial role in our future considerations, and explains to some extent the importance of the Theorem on Lifting Idempotents 6.7. We prove:

(6.10) Proposition. Let M be a nonzero left A -module, and let $E = \text{End}_A M$ be its endomorphism ring. Suppose that either

(i) The A -submodules of M satisfy both chain conditions, or

(ii) M is a f.g. A -module, where A is an R -algebra as in (6.8ii).

Then M is an indecomposable A -module if and only if E is a local ring.

Proof. We have already seen in (6.4) that M is indecomposable if and only if E has no idempotents except 1. The remarks following (6.4) show that a local ring has no idempotents except 1, and thus if E is local, then M is indecomposable. We must prove that, conversely, if M is indecomposable then E is local.

Case (i). Assume M indecomposable and satisfying both chain conditions. To prove that E is local, it suffices (by (5.21)) to show that the sum of two non-units in E is a non-unit. For this, we need only show that there cannot exist non-units $\alpha, \beta \in E$ for which $\alpha + \beta = 1$. If such elements exist, then β is not nilpotent, since otherwise $1 - \beta$ has inverse $1 + \beta + \beta^2 + \dots$. Hence the descending chain of A -submodules of M :

$$M \supseteq M\beta \supseteq M\beta^2 \supseteq \dots$$

must terminate in a nonzero module, say at $M\beta'$. Put $\gamma = \beta' \in E$, so γ is a surjection of $M\beta'$ onto itself. Since $M\beta'$ is a noetherian module, by (5.8) γ must be an automorphism. If $i: M\beta' \rightarrow M$ is the inclusion map, we have

$$M\beta' \xrightleftharpoons[\gamma]{i\gamma^{-1}} M,$$

with composite $(i\gamma^{-1}) \cdot \gamma$ the identity on $M\beta'$. Hence $M\beta'$ is a direct summand of M , and therefore $M\beta' = M$ because M is indecomposable. But then β' is an automorphism of M , whence β is a unit of E . This is a contradiction, and completes the proof that E is local in case (i).

Case (ii). Assume M indecomposable, and that the hypotheses (ii) are satisfied. Since $E \subseteq \text{End}_R M$, which is a finitely generated R -module by Exercise 2.6, it follows that E is also a finitely generated R -module. Hence by (5.22), $E/\text{rad } E$ is semisimple, and idempotents can be lifted from $E/\text{rad } E$ to E by (6.7). If $E/\text{rad } E$ is not a skewfield, then it has at least one proper nonzero left ideal, and this ideal is a direct summand of the semisimple ring $E/\text{rad } E$. It follows from the discussion at the beginning of this section that $E/\text{rad } E$ contains an idempotent $\epsilon \neq 1$. But then by (6.7) there exists an idempotent $e \in E$ lifting ϵ , and so $e \neq 1$. But E cannot contain any idempotents except 1, since M is indecomposable. Thus we have shown that $E/\text{rad } E$ must be a skewfield. Therefore E is local by (5.21), and the proposition is proved.

A ring A is called *primary* if $A/\text{rad } A$ is a simple artinian ring. Under suitable hypotheses, every primary ring is a full matrix ring over a local ring. In fact, we prove now

(6.11) Proposition. *If B is a local ring, then for each positive integer n , the ring $M_n(B)$ is primary. Conversely, let A be a primary ring, and assume that A is*

either left artinian or an R -algebra as in (6.8). Then $A \cong M_n(B)$ for some local ring B and some integer n .

Proof. Suppose B is a local ring, so $B/\text{rad } B = S$ (say) is a skewfield by (5.21). From (5.14) we know that

$$\text{rad } M_n(B) = M_n(\text{rad } B).$$

Therefore

$$M_n(B)/\text{rad } M_n(B) \cong M_n(B/\text{rad } B) = M_n(S).$$

But $M_n(S)$ is a simple artinian ring by §3D, which proves that $M_n(B)$ is primary.

Conversely, let A be a primary ring satisfying the given hypotheses, and let $N = \text{rad } A$. Keep the notation and terminology of (6.8), so $\bar{A} = A/N = \bigoplus \bar{A}\bar{e}_i$. Since \bar{A} is a simple artinian ring (because A is primary), it follows that the $\{\bar{A}\bar{e}_i\}$ are mutually isomorphic simple left \bar{A} -modules. Hence by (6.8), the $\{Ae_i\}$ are mutually isomorphic indecomposable A -modules, and thus

$$A \cong (Ae_1)^{(n)} \text{ as left } A\text{-modules.}$$

Therefore*

$$A^\circ = \text{End}_A(AA) \cong \text{End}_A((Ae_1)^{(n)}) = M_n(B),$$

where $B = \text{End}_A(Ae_1)$. Since Ae_1 is indecomposable, B is a local ring by (6.10). Therefore we obtain $A \cong M_n(B^\circ)$. However, if S is a skewfield then so is S° . Furthermore, under the anti-isomorphism $B \rightarrow B^\circ$, we have $\text{rad } B \rightarrow \text{rad } B^\circ$ by (5.11). Thus B° is local, since

$$B^\circ/\text{rad } B^\circ \cong (B/\text{rad } B)^\circ = S^\circ,$$

where S is the skewfield $B/\text{rad } B$. This completes the proof.

§6B. The Krull-Schmidt-Azumaya Theorem

Let A be a ring, M a left A -module, and $E = \text{End}_A M$ its endomorphism ring. Call M *indecomposable* if $M \neq 0$ and M is not expressible as a direct sum of nonzero A -submodules. We saw in (6.10) that under suitable hypotheses, M is indecomposable if and only if E is a local ring. This is the key fact in proving the following fundamental result, hereafter abbreviated as the K-S-A Theorem:

* A° denotes the opposite ring A , having the same elements as A , but with multiplication reversed.

(6.12) Krull-Schmidt-Azumaya Theorem. Let M be a finitely generated left A -module, and assume that either:

- (i) The A -submodules of M satisfy both chain conditions, or
- (ii) A is an R -algebra, f.g. as R -module, where R is a complete commutative noetherian local ring (such as, for example, a field or a complete discrete valuation ring).

Then M is expressible as a finite direct sum of indecomposable submodules. Further, if

$$(6.13) \quad M = \bigoplus_{i=1}^r M_i = \bigoplus_{j=1}^s N_j$$

are two such sums, then $r=s$ and $M_1 \cong N_{j_1}, \dots, M_r \cong N_{j_r}$, where $\{j_1, \dots, j_r\}$ is some permutation of $\{1, \dots, r\}$. In brief, M is uniquely a finite sum of indecomposables, up to isomorphism and order of occurrence of the summands.

Proof. In both cases (i) and (ii), M is a noetherian module, hence is expressible as a finite direct sum of indecomposable submodules. We now prove the uniqueness assertion by induction on the integer r in (6.13), observing first that the result is obvious when $r=1$. Now let $r \geq 2$, and let $\mu_i: M \rightarrow M_i$, and $\nu_j: M \rightarrow N_j$, be the projection maps associated with the decompositions in (6.13). Then $\sum \nu_j = \text{id}_M$, whence

$$\sum \mu_i \nu_j = \text{identity map on } M_1,$$

and where each map $\mu_i \nu_j$ is restricted to M_1 . However, by (6.10) the endomorphism ring $\text{End}_A M_1$ is local, that is, the sum of non-units in this ring is a non-unit. The above equation thus implies that some $\mu_i \nu_j$ is an automorphism of M_1 . Renumbering the N_j 's if need be, we may assume that $\mu_1 \nu_1 = \varphi \in \text{Aut}_A M_1$. But then in the diagram

$$M_1 \xrightleftharpoons[\varphi^{-1}\mu_1]{\nu_1} N_1$$

we have $(\varphi^{-1}\mu_1)\nu_1 = \text{id}_{M_1}$, whence $\nu_1 M_1$ is a direct summand of N_1 . Since both M_1, N_1 are indecomposable, it follows that ν_1 is an isomorphism $M_1 \cong N_1$, and that $\varphi^{-1}\mu_1: N_1 \rightarrow M_1$ is its inverse.

$$M' = N_1 \oplus M_2 \oplus \cdots \oplus M_r.$$

(Note that the sum is direct, since if

$$n_1 + m_2 + \cdots + m_r = 0, n_1 \in N_1, m_j \in M_j,$$

then applying μ_1 we see that $\mu_1(n_1) = 0$, whence $n_1 = 0$. But then each $m_j = 0$, $j = 2, \dots, r$.) Next, for $x \in N_1$ we have

$$\mu_1(x) = x - \mu_2(x) - \cdots - \mu_r(x) \in M',$$

and so $M_1 = \mu_1(N_1) \subset M'$. Therefore $M' = M$, so we have

$$M = M_1 \oplus M_2 \oplus \cdots \oplus M_r = N_1 \oplus M_2 \oplus \cdots \oplus M_r.$$

Now set $\rho = \nu_1\mu_1 + \mu_2 + \cdots + \mu_r$; clearly ρ defines an A -automorphism of M which carries M_1 onto N_1 , and each M_j onto itself for $j = 2, \dots, r$. Hence ρ induces an A -automorphism $M/M_1 \cong M/N_1$; but $M/N_1 = \bigoplus_{j=2}^r N_j$, so we have $\bigoplus_2^r M_i \cong \bigoplus_2^s N_j$. Now use the induction hypothesis to conclude that the $\{M_i : 2 \leq i \leq r\}$ are, up to isomorphism, a rearrangement of the $\{N_j : 2 \leq j \leq s\}$. This completes the proof.

(6.14) Remark. Examination of the preceding proof shows that the uniqueness part of Theorem 6.12 holds for all direct decompositions as in (6.13) for which the endomorphism rings of the indecomposable summands are local rings (without any hypothesis on the ring A .)

(6.15) Corollary. Let L, M, N be left A -modules satisfying the conditions of (6.12), and suppose that

$$L \oplus M \cong L \oplus N.$$

Then $M \cong N$.

Proof. Write $L = \bigoplus L_i$, $M = \bigoplus M_j$, $N = \bigoplus N_k$, direct sums of indecomposables. Then the hypothesis implies, by virtue of the K-S-A Theorem, that the $\{M_j\}$ coincide with the $\{N_k\}$, up to isomorphism and order of occurrence. Hence $M \cong N$ as claimed.

(6.16) Corollary. Let L be a direct summand of the A -module M given as in (6.12). Then L is isomorphic to a subsum of $\bigoplus M_i$.

Proof. We may write $M = L \oplus L'$ for some submodule L' of M . Now let $L = \bigoplus L_k$, $L' = \bigoplus L'_j$, be decompositions into indecomposables. By (6.12), the modules $\{L_k\} \cup \{L'_j\}$ coincide with the $\{M_i\}$, up to isomorphism. Hence

$$L = \bigoplus L_k \cong M_{i_1} \oplus \cdots \oplus M_{i_t}$$

for some subset $\{i_1, \dots, i_t\}$ of $\{1, \dots, r\}$.

We remark that K-S-A Theorem need not hold for algebras over a local ring R which is not complete. (See §36.)

The K-S-A Theorem has many important consequences. Let us give one immediately. For a ring A , we have denoted by $\mathcal{P}(A)$ the category of all finitely generated left A -modules. We now prove

(6.17) Proposition. *Let A be a ring which is either left artinian, or else is an R -algebra over a complete local ring R as in (6.8ii). Let N be any two-sided ideal of A contained in $\text{rad } A$, and set $\bar{A} = A/N$. For each A -module X , let $\bar{X} = X/NX$ be the corresponding \bar{A} -module. Let*

$$A = Ae_1 \oplus \cdots \oplus Ae_n$$

be a decomposition of A into indecomposable left ideals, numbered so that Ae_1, \dots, Ae_m are a full set of non-isomorphic modules among the $\{Ae_i\}$. Then

- (i) *For each $P \in \mathcal{P}(A)$, there exist non-negative integers $\{r_i\}$ such that*

$$(6.18) \quad P \cong \coprod_{i=1}^m (Ae_i)^{(r_i)}.$$

- (ii) *If $\{r_i\}$ and $\{s_i\}$ are non-negative integers, then*

$$\coprod_{i=1}^m (Ae_i)^{(r_i)} \cong \coprod_{i=1}^m (Ae_i)^{(s_i)} \text{ if and only if } r_i = s_i \text{ for each } i.$$

- (iii) *For each $Y \in \mathcal{P}(\bar{A})$, there exist non-negative integers $\{r_i\}$ such that*

$$(6.19) \quad Y \cong \coprod_{i=1}^m (\bar{A}\bar{e}_i)^{(r_i)},$$

and the $\{r_i\}$ are uniquely determined by the isomorphism class of Y .

- (iv) *The isomorphism classes in $\mathcal{P}(A)$ correspond bijectively with those in $\mathcal{P}(\bar{A})$, the correspondence being given by mapping the class of $P \in \mathcal{P}(A)$ onto the class of $\bar{P} \in \mathcal{P}(\bar{A})$.*

Proof. The hypotheses on A imply that the K-S-A Theorem, and its corollaries, hold for A -modules and also for \bar{A} -modules. Each $P \in \mathcal{P}(A)$ is isomorphic to a direct summand of $A^{(k)}$ for some k . But

$$A^{(k)} \cong \coprod_{i=1}^n (Ae_i)^{(k)} \cong \coprod_{i=1}^m (Ae_i)^{(k_i)}$$

for some positive integers $\{k_i\}$. It follows at once from (6.16) that (6.18) holds for some integers $\{r_i\}$ with $0 \leq r_i \leq k_i$ for each i . This proves the first assertion in the proposition. Assertion (ii) is a direct consequence of the K-S-A Theorem.

Next, it follows from (6.8) that the formula $\bar{A} = \bigoplus_{i=1}^n \bar{A}\bar{e}_i$ gives a decomposition of \bar{A} into indecomposable left ideals, and furthermore that $\bar{A}\bar{e}_1, \dots, \bar{A}\bar{e}_m$ are a full set of non-isomorphic modules among the $\{\bar{A}\bar{e}_i\}$. We conclude, just as above, that every $Y \in \mathcal{P}(\bar{A})$ is isomorphic to a direct sum of copies of the $\{\bar{A}\bar{e}_i : 1 \leq i \leq m\}$, and that the number of summands of each type is uniquely determined by the isomorphism class of Y .

It is now clear that the bijection, whose existence is asserted in (iv), is given by the correspondence

$$\coprod_{i=1}^m (Ae_i)^{(r_i)} \leftrightarrow \coprod_{i=1}^m (\bar{A}\bar{e}_i)^{(r_i)},$$

where the $\{r_i\}$ are non-negative integers.

§6C. Projective Covers

Let A be a ring, and let M, N be left A -modules. A map $f \in \text{Hom}_A(M, N)$ is called *essential* if f is surjective, and if for each sequence of A -modules $X \xrightarrow{g} M \xrightarrow{f} N$ such that fg is surjective, the map g is also surjective. In other words, a surjection $f: M \rightarrow N$ is essential if no proper submodule of M is mapped onto N by f .

A *projective cover* of a module M is a diagram $P \xrightarrow{f} M$ with P projective and f essential.

(6.20) Proposition. *Projective covers are unique up to isomorphism, assuming there are any. In other words, given two projective covers $P \xrightarrow{f} M$ and $P' \xrightarrow{f'} M$, there exists an isomorphism $\theta: P \cong P'$ such that $f = f'\theta$.*

Proof. Consider the diagram

$$\begin{array}{ccc} & \theta & \\ P' & \xrightarrow{f'} & M \\ & \downarrow f & \\ & \xleftarrow{P} & \end{array}$$

There exists a homomorphism θ with $f = f'\theta$, since P is projective and f' is a surjection. Then θ is surjective, since $f'\theta$ is surjective and f' is essential. Since P' is projective, there is a splitting map $\varphi: P' \rightarrow P$ such that $\theta\varphi = \text{id}_{P'}$. Then $f\varphi = f'\theta\varphi = f'$, whence φ is surjective since $f\varphi$ is surjective and f is essential. Hence both φ and θ are isomorphisms.

Some modules need not have projective covers. For example, the \mathbb{Z} -module $\mathbb{Z}/2\mathbb{Z}$ has none; for let $f: P \rightarrow \mathbb{Z}/2\mathbb{Z}$ be a projective cover, with P \mathbb{Z} -projective. Then P is \mathbb{Z} -free, and $3P$ is a proper submodule of P for which $f(3P) = \mathbb{Z}/2\mathbb{Z}$.

The next result shows how projective covers may be determined in some cases. We begin with:

(6.21) Lemma. *Let $f: X \rightarrow M$ be a surjection of f.g. A -modules. If*

$$\ker f \subseteq (\text{rad } A)X,$$

then f is essential.

Proof. Let $Y \subseteq X$ be a submodule such that $f(Y) = M$. Then

$$X = Y + \ker f = Y + (\text{rad } A)X.$$

Thus $X = Y$ by Nakayama's Lemma, which proves that f is essential.

(6.22) Corollary. *Let P be a f.g. projective A -module, and let J be any two-sided ideal of A contained in $\text{rad } A$. Then the natural map $P \rightarrow P/JP$ gives a projective cover of the A -module P/JP .*

Proof. The surjection $P \rightarrow P/JP$ is essential, by (6.21).

We shall call the ring A *semiperfect* if $A/\text{rad } A$ is a semisimple artinian ring and every idempotent in $A/\text{rad } A$ is the image of an idempotent in A . It follows from (5.19), (6.5) and (6.7) that left artinian rings are always semiperfect; by (5.22), (6.5) and (6.7), so are R -algebras of the type described in (6.5ii). If we set $N = \text{rad } A$ in (6.8), then the proof of (6.8) carries over equally well to the case where A is any semiperfect ring. In particular, let $\bar{A} = A/\text{rad } A$. Keeping the notation of (6.8), the decomposition $\bar{A} = \bigoplus \bar{A}\bar{e}_i$ gives a decomposition of \bar{A} into simple left \bar{A} -modules, and thus every simple left- \bar{A} -module is (up to isomorphism) of the form $\bar{A}\bar{e}_i$. Using this, we prove:

(6.23) Theorem. *Let A be a semiperfect ring and set $N = \text{rad } A$, $\bar{A} = A/N$. Then every f.g. left A -module X has a projective cover. Specifically, there exists a f.g. projective A -module P such that $P/NP \cong X/NX$ as A -modules, and this isomorphism lifts to a surjection $P \rightarrow X$ giving a projective cover of X .*

Proof. Set $\bar{X} = X/NX$, a f.g. \bar{A} -module. Since \bar{A} is semisimple, it follows from the discussion that \bar{X} is (up to \bar{A} -isomorphism) a direct sum of copies of the \bar{A} -modules $\{\bar{A}\bar{e}_i\}$. For each i , Ae_i is a projective A -module such that $Ae_i/N(Ae_i) = \bar{A}\bar{e}_i$. Hence there exists a f.g. projective A -module P such that*

$$P/NP \cong X/NX \text{ as } \bar{A}\text{-modules.}$$

This isomorphism is also an A -isomorphism, of course.

*This same type of argument also occurred in the proof of (6.17).

Now consider the diagram

$$(6.24) \quad \begin{array}{ccc} P & \longrightarrow & P/NP \\ f \downarrow & & \downarrow h \\ X & \longrightarrow & X/NX, \end{array}$$

where h is the isomorphism given above. Since P is projective, there exists an A -homomorphism $f: P \rightarrow X$ making the diagram commute. For each $x \in X$, there exists an element $p \in P$ for which $\bar{x} = h(\bar{p})$ in \bar{X} . This shows that

$$f(P) + NX = X,$$

whence $f(P) = X$ by Nakayama's Lemma. Furthermore, it is easily seen that $\ker f \subseteq NP$, since h is injective. Thus we have obtained a surjection $f: P \rightarrow X$ for which $\ker f \subseteq NP$, and so f gives a projective cover of X by (6.22).

(6.25) Corollary. *Let A be a semiperfect ring, and consider only finitely generated A -modules. Let $N = \text{rad } A$.*

(i) *Let $f: P \rightarrow X$ be a surjection, with P projective. Then f gives a projective cover of X if and only if $\ker f \subseteq N \cdot P$.*

(ii) *For each A -module X , the modules X and X/NX have the same projective cover as A -modules.*

(iii) *Projective covers are additive, that is, if $f_i: P_i \rightarrow X_i$, $1 \leq i \leq k$, are projective covers, then so is*

$$\coprod_1^k f_i: \coprod_1^k P_i \rightarrow \coprod_1^k X_i.$$

Proof. (i) Given a surjection $f: P \rightarrow X$ with $\ker f \subseteq N \cdot P$, we have already remarked in (6.22) that f gives a projective cover of X . Conversely, starting with a projective cover $f: P \rightarrow X$, we know by (6.20) that P is unique up to isomorphism. Hence by the proof of (6.23), there is a commutative diagram (6.24), with h an isomorphism. This implies at once that $\ker f \subseteq N \cdot P$, as claimed.

(ii) Let $Y = X/NX$, viewed as A -module. Then $X/NX \cong Y/NY$, so by (6.23), X and Y have the same projective cover.

(iii) This is obvious from the fact that

$$\left(\coprod P_i \right) / \left(N \cdot \coprod P_i \right) \cong \coprod (P_i/NP_i) \cong \coprod X_i/NX_i.$$

(6.26) Remarks. (i) The converse of Theorem 6.23 also holds: if every f.g. left A -module has a projective cover, then the ring A is semiperfect. See Anderson-Fuller, [73, Th. 27.6, p. 304] for a proof of this result. Other interesting results on semiperfect rings are given in this reference (see §27), as well as a discussion of perfect rings (see §28).

(ii) The results of Theorem 6.8 can be interpreted naturally in terms of projective covers. It follows at once from (6.22) that the natural map $Ae_i \rightarrow \bar{A}\bar{e}_i$ gives a projective cover of the A -module $\bar{A}\bar{e}_i$. By the uniqueness of projective covers (6.20), we conclude immediately that

$$Ae_i \cong Ae_j \text{ if and only if } \bar{A}\bar{e}_i \cong \bar{A}\bar{e}_j,$$

using the notation of (6.8). (Of course, we are using the fact that two \bar{A} -modules are \bar{A} -isomorphic if and only if they are A -isomorphic when viewed as A -modules.)

(iii) Gruenberg-Roggenkamp [75] discuss the question as to whether augmentation ideals of group rings have projective covers. Let G be a finite group, and let

$$\mathbf{Z}' = \{a/b : a, b \in \mathbf{Z}, (b, |G|) = 1\}.$$

The *augmentation ideal* I' of $\mathbf{Z}'G$ is by definition $\bigoplus \mathbf{Z}'(x-1)$, with x ranging over all elements of $G - \{1\}$. They show that I' has a projective $\mathbf{Z}'G$ -cover if and only if G is a p -group (for some prime p) or else G is cyclic. They also deal with this problem for the more general case in which \mathbf{Z}' is replaced by some semilocal ring of integers in an algebraic number field. Gruenberg [70, Prop. 3, p. 254] showed that *every* f.g. $\mathbf{Z}'G$ -module has a projective cover if and only if G is a p -group for some prime p .

§6D. Injective Hulls

Let M, N be A -modules. An *essential monomorphism** $f: M \rightarrow N$ is a monomorphism such that for each sequence of A -modules

$$M \xrightarrow{f} N \xrightarrow{g} Y \text{ with } gf \text{ monic,}$$

the map g is necessarily monic. Thus, a monomorphism $f: M \rightarrow N$ is essential if and only if for each nonzero submodule N' of N , the intersection $N' \cap f(M)$ is nonzero.

An *injective hull* (or *injective envelope*) of a module M is a diagram $0 \rightarrow M \xrightarrow{f} E$ with f an essential monomorphism and E an injective module.

*In CR pp. 389–390, we refer to N as a *related extension* of its submodule $f(M)$.

As shown in CR (57.13), every module M has an injective hull [Eckman-Schopf Theorem], which is uniquely determined up to isomorphism. For example, \mathbf{Q} is the injective hull of the \mathbf{Z} -module \mathbf{Z} .

Other references for this topic are Anderson-Fuller [73, pp. 72–75, pp. 206–209] and Behrens [72, pp. 179–182].

(6.27) Proposition. *Injective hulls are additive.*

Proof. Let $0 \rightarrow M_i \rightarrow E_i$, $i=1,2$, be sequences of A -modules, where E_i is the injective hull of M_i , and view M_i as submodule of E_i . We claim that $E_1 + E_2$ is the injective hull of $M_1 + M_2$. Clearly $E_1 + E_2$ is injective, so we need only show that the map $M_1 + M_2 \subseteq E_1 + E_2$ is essential, that is, for each nonzero submodule Y of $E_1 + E_2$, the intersection $Y \cap (M_1 + M_2) \neq 0$. Let $(e_1, e_2) \in Y$ be nonzero; then (say $e_1 \neq 0$) Ae_1 is a nonzero submodule of E_1 , hence meets M_1 . Thus there exists an $a \in A$ with $ae_1 = m_1 \in M_1$, $m_1 \neq 0$. But $a(e_1, e_2) \in Y$, so now Y contains (m_1, e'_2) . If $e'_2 = 0$, then $(m_1, e'_2) \in (M_1 + M_2) \cap Y$, and Y meets $M_1 + M_2$. If $e'_2 \neq 0$, then $Ae'_2 \cap M_2 \neq 0$, so there exists an element $b \in A$ with $be'_2 = m_2 \in M_2$, $m_2 \neq 0$. But then

$$b(m_1, e'_2) = (bm_1, m_2) \in (M_1 + M_2) \cap Y$$

so again Y meets $M_1 + M_2$. This completes the proof that

$$E(M_1 + M_2) \cong E(M_1) + E(M_2),$$

if $E(\)$ denotes injective hull.

Now let A be a left artinian ring such that the left regular module ${}_A A$ is A -injective; we call A (left) *self-injective*, or *quasi-Frobenius*. As shown in CR §58, remarks following (58.5), such a ring A is necessarily right artinian. Further (CR, Exercise 58.5), ${}_A A$ is an injective right A -module. Thus the condition that A be quasi-Frobenius is left-right symmetric, and “left $q\text{-}F$ ” = “right $q\text{-}F$ ”.

(6.28) Remarks. (i) The group algebra KG of a finite group G over an arbitrary field K is always self-injective (see (9.6) and (9.9iii), and also Exercise 10.23).

(ii) Let A be any artinian self-injective ring, and set $N = \text{rad } A$. Define

$$r(N) = \text{right annihilator of } N = \{a \in A : N \cdot a = 0\},$$

$$l(N) = \text{left annihilator of } N = \{a \in A : a \cdot N = 0\}.$$

Then (CR(58.12) or Behrens [72, pp. 182–184])

$$r(N) = l(N) = \text{left socle of } A = \text{right socle of } A,$$

where the *socle* of a module is the sum of its simple submodules. For the case of Frobenius algebras, see (9.9).

(iii) Let A be an artinian self-injective ring. If e is a primitive idempotent of A , then Ae has a unique simple submodule, given by $l(N)e$. Thus (see CR (58.12)),

$$\text{soc } A = \bigoplus_i l(N)e_i,$$

where $1_A = \sum e_i$ is the decomposition of 1_A into primitive idempotents. Furthermore,

$$\begin{aligned} l(N)e &\cong \text{dual of the simple right } A\text{-module } eA/eN \\ &= \text{Hom}_A(eA/eN, A). \end{aligned}$$

We have

$$Ae_i \cong Ae_j \Leftrightarrow Ae_i/Ne_i \cong Ae_j/Ne_j \Leftrightarrow l(N)e_i \cong l(N)e_j.$$

(Note: Ne is the unique maximal submodule of Ae (see (6.9)), and $\text{soc } A$ denotes the socle of A .) (See (9.9ii) for the case of Frobenius algebras.)

(6.29) Proposition. *Let P be any f.g. projective left A -module. Then*

$$(\text{soc } A)P = \text{soc } P.$$

Proof. Since $N \cdot \text{soc } A = 0$ we have $N((\text{soc } A)P) = 0$, so $(\text{soc } A)P$ is a semisimple A -module, hence lies in $\text{soc } P$. We must prove equality. Write P as a direct sum $\prod Ae_i$, where the $\{e_i\}$ are primitive idempotents, and there may be repetitions. Then $\text{soc } P = \prod \text{soc } Ae_i$, so it suffices to prove that

$$(\text{soc } A) \cdot Ae = \text{soc } Ae$$

for each primitive idempotent e . By (ii) above, $\text{soc } Ae$ is simple so we need only show that $(\text{soc } A)Ae \neq 0$ (because the previous remarks already imply that $(\text{soc } A)Ae \subseteq \text{soc } Ae$. But

$$(\text{soc } A)Ae \supseteq l(N)e \cdot Ae \supseteq l(N)e \neq 0.$$

This completes the proof.

(6.30) Theorem (E. L. Green). *Let M be a f.g. left A -module, where A is an artinian self-injective ring. Then*

$$(\text{soc } A)M \neq 0 \text{ if and only if } M \text{ has a projective and injective direct summand.}$$

Proof. If P is a nonzero projective A -module which is a direct summand of M , then $(\text{soc } A)M \supseteq (\text{soc } A)P = \text{soc } P \neq 0$, by (6.29).

Suppose conversely that $(\text{soc } A)M \neq 0$, and let $f: P \rightarrow M$ be a projective cover of M . Then $f((\text{soc } A)P) = (\text{soc } A)M \neq 0$, so there exists a primitive idempotent $e \in A$ with $f((\text{soc } A) \cdot Ae) \neq 0$, that is, $f(\text{soc } Ae) \neq 0$. We have a commutative diagram

$$\begin{array}{ccc} \text{soc } Ae & \xrightarrow{f'} & \text{soc } M \\ \downarrow & & \downarrow \\ Ae & \xrightarrow{f} & M, \end{array}$$

with f' nonzero (and hence an injection, since $\text{soc } Ae$ is simple). But $\ker f$ is a submodule of Ae , and if $\ker f \neq 0$, then $\ker f$ would contain the unique simple submodule $\text{soc } Ae$ of Ae .

This would imply that f vanishes on $\text{soc } Ae$, a contradiction since f' is the restriction of f to $\text{soc } Ae$. Hence $\ker f = 0$, so $Ae \rightarrow M$ is an injection. But Ae is injective (because A is self-injective), and therefore Ae is a direct summand of M , as desired.

The following theorem generalizes earlier results of Alperin-Janusz [73] and Heller [61b].

(6.31) Theorem. *Let A be an artinian self-injective ring, and let*

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

be an exact sequence of f.g. A -modules, with X projective. Then the following conditions are equivalent:

- (i) M is indecomposable, non-projective, and $g: X \rightarrow M$ is a projective cover of M .
- (ii) N is indecomposable, non-injective, and $f: N \rightarrow X$ is an injective hull of N .

Proof. Since A is quasi-Frobenius, X is also injective. We prove that (i) \Rightarrow (ii), so assume (i). If N were injective, the sequence would split, whence M would be projective. Thus N is not injective. Now $g: X \rightarrow M$ is a projective cover, whence by (6.25i) we have

$$N \subseteq J \cdot X, \text{ where } J = \text{rad } A,$$

and where we are viewing f as an inclusion map.

Next, by (6.30) we have $(\text{soc } A)M=0$, since otherwise M would have a projective direct summand. Consequently,

$$g((\text{soc } A)X)=(\text{soc } A)g(X)=0.$$

But $(\text{soc } A)X=\text{soc } X$ by (6.29). Therefore $g(\text{soc } X)=0$, so $\text{soc } X \subseteq N$. Hence $\text{soc } X \subseteq \text{soc } N$, whence $\text{soc } X=\text{soc } N$. Thus there is a commutative diagram

$$\begin{array}{ccc} \text{soc } N & = & \text{soc } X \\ \downarrow & & \downarrow \\ N & \subseteq & X, \end{array}$$

where the vertical maps are inclusions. Any nonzero submodule Y of X meets $\text{soc } X$, hence meets $\text{soc } N$, hence meets N . This shows that the inclusion $N \subseteq X$ gives an injective hull of N .

Finally, if $N=N_1 \oplus N_2$, and X_i is an injective hull of N_i , $i=1, 2$, there is a commutative diagram

$$\begin{array}{ccccccc} 0 & \longrightarrow & N & \longrightarrow & X & \longrightarrow & M & \longrightarrow 0 \\ & & \alpha \downarrow & & \beta \downarrow & & \gamma \downarrow & \\ 0 & \longrightarrow & N_1 \oplus N_2 & \longrightarrow & X_1 \oplus X_2 & \longrightarrow & M_1 \oplus M_2 & \longrightarrow 0, \end{array}$$

where $M_i=X_i/N_i$, in which α, β are isomorphisms. Hence γ is an isomorphism, so M decomposes unless (say) $M_1=0$. But then $N_1=X_1$, while we know already that $N_1 \subseteq JX_1$ because $N \subseteq JX$; this gives $X_1=JX_1$, whence $X_1=0$ and $N_1=0$. Therefore N is indecomposable, as claimed.

The proof that (ii) \Rightarrow (i) is similar, and we omit it.

§6. Exercises

1. Let L, M be left A -modules satisfying the conditions of (6.12). Show that if $L^{(k)} \cong M^{(k)}$ for some positive integer k , then $L \cong M$.

2. Let A be a f.d. K -algebra, where K is a field, and let M be a f.g. left A -module. For E a field containing K , set

$$A^E=E \otimes_K A, \quad M^E=E \otimes_K M,$$

so M^E is a module over the E -algebra A^E . Let L be another f.g. left A -module. Prove that if $\dim_K(E)$ is finite, then

$$(6.32) \quad L^E \cong M^E \text{ as } A^E\text{-modules} \Leftrightarrow L \cong M \text{ as } A\text{-modules}.$$

[Hint: The map $a \mapsto 1 \otimes a$, $a \in A$, embeds A into A^E . Each A^E -module X gives rise to an A -module $X|_A$ by restriction of operators. If $n=\dim_K(E)$, then

$$M^E|_A \cong M^{(n)}.$$

Hence $L^E \cong M^E$ implies $L^{(n)} \cong M^{(n)}$, whence $L \cong M$ by Exercise 1.]

3. (Generalization) Let A be an R -algebra f.g./ R , where R is a complete local ring as in (6.12). Let R' be a commutative ring containing R , and suppose that R' has a free R -basis $\{x_1, \dots, x_n\}$ with $x_1 = 1$. Let M be any f.g. left A -module, and set

$$A' = R' \otimes_R A, M' = R' \otimes_R M \cong A' \otimes_A M.$$

Let L be another f.g. left A -module. Prove that

$$L' \cong M' \text{ as } A'\text{-modules} \Leftrightarrow L \cong M \text{ as } A\text{-modules}.$$

[Hint: $L'|_A \cong L^{(n)}$ as above.]

4. Let A be a left K -algebra, L and M f.g. A -modules, where $\dim_K(A)$ is finite. Assume that $\dim_K(L) = \dim_K(M) = n$, and let X_1, \dots, X_r be a K -basis for $\text{Hom}_A(L, M)$. Put

$$f(t_1, \dots, t_r) = \det(t_1X_1 + \dots + t_rX_r),$$

where the $\{t_i\}$ are indeterminates over K . Show that $L \cong M$ as A -modules if and only if there exist elements $\{\alpha_i\}$ in K such that $f(\alpha_1, \dots, \alpha_r) \neq 0$.

5. Keep the above notation, and suppose that the polynomial $f(t_1, \dots, t_r)$ is not the zero polynomial. Show that if $\text{card } K > n$, then there exist elements $\{\alpha_i\} \in K$ with $f(\alpha_1, \dots, \alpha_r) \neq 0$.

[Hint: $f(t_1, \dots, t_r)$ is homogeneous of degree n . Use induction on r to show that f cannot vanish on all r -tuples from K .]

6. (Noether-Deuring Theorem). Let A be a f.d. K -algebra, where K is a field, and let L and M be f.g. left A -modules. Let E be any field containing K . Prove that if $L^E \cong M^E$ as left A^E -modules, then $L \cong M$ as left A -modules, and conversely.

[Hint: Suppose that $L^E \cong M^E$; then

$$\dim_K(L) = \dim_E(L^E) = \dim_E(M^E) = \dim_K(M) = n \text{ (say).}$$

Let the $\{X_i\}$ be as in Exercise 4. By Exercise 2.7, these $\{X_i\}$ are also an E -basis for $\text{Hom}_{A^E}(L^E, M^E)$, so by Exercise 4 there exist elements $\{\beta_i\}$ in E for which $f(\beta_1, \dots, \beta_r) \neq 0$. Hence $f(t_1, \dots, t_r)$ is not the zero polynomial. If $\text{card } K > n$, then there exist $\{\alpha_i\}$ in K with $f(\alpha_1, \dots, \alpha_r) \neq 0$, whence $L \cong M$. If $\text{card } K \leq n$, let F be a finite extension of K with $\text{card } F > n$. Then there exist elements $\{\gamma_i\} \in F$ with $f(\gamma_1, \dots, \gamma_r) \neq 0$, whence $F \otimes_K L \cong F \otimes_K M$ by the preceding step. But then $L \cong M$ by Exercise 2.] (See also §30B for algebras over valuation rings.)

7. Does the Noether-Deuring Theorem remain valid if we assume that L and M are left A -modules of finite K -dimension, but drop the hypothesis that $\dim_K(A)$ be finite?

[Hint: See Exercise 2.8.]

8. Let A be an R -algebra as in (6.5), and set $\bar{A} = A/PA$, where $P = \text{rad } R$. Show that if $e \in A$ is an idempotent for which \bar{e} lies in the center of \bar{A} , then e lies in the center of A .

[Hint: Consider the “Pierce decomposition”]

$$A = eAe \oplus eA(1-e) \oplus (1-e)Ae \oplus (1-e)A(1-e)$$

of A into R -submodules. Passing to \bar{A} , we obtain a corresponding decomposition of \bar{A} . But $\bar{e}\bar{A}(\bar{1}-\bar{e})=0$, so $eA(1-e)$ is an R -direct summand of A such that $eA(1-e)/P \cdot eA(1-e)=0$. Hence $eA(1-e)=0$, and likewise $(1-e)Ae=0$. Therefore

$$A = eAe \oplus (1-e)A(1-e),$$

so each $a \in A$ commutes with e . (This result is due to Dade.)]

9. Let A be a local ring, M any f.g. projective left A -module. Prove that M is a free A -module.

[Hint: Let bars denote reduction modulo $\text{rad } A$. Then \bar{A} is a skewfield, and \bar{M} is a left \bar{A} -module. (Further, if $M \neq 0$ then $\bar{M} \neq 0$ by Nakayama’s Lemma.) Thus $\bar{M} \cong \bar{A}^{(k)}$ for some k . But then $M \cong A^{(k)}$ by (6.6).]

10. Let A be a semiperfect ring with radical N , and let $I \subseteq N$, I = two-sided ideal of A . Let X be any f.g. projective left (A/I) -module. Show that there exists a f.g. projective left A -module P such that $P/IP \cong X$, and that this isomorphism lifts to a projective cover $P \rightarrow X$ of X viewed as A -module.

[Hint: By (6.23), there is an A -projective cover $f: P \rightarrow X$. This yields a commutative diagram

$$\begin{array}{ccccc} P & \longrightarrow & P/IP & \longrightarrow & P/NP \\ f \downarrow & & g \downarrow & & h \downarrow \\ X & \longrightarrow & X/IX & \longrightarrow & X/NX, \end{array}$$

where f induces g and h , and where h is an isomorphism. But $IX=0$, so X/IX is (A/I) -projective. Therefore

$$P/IP \cong (X/IX) \oplus Y$$

for some (A/I) -module Y . This gives

$$P/NP \cong (X/NX) \oplus (Y/NY),$$

whence $Y/NY=0$, so $Y=0$.]

11. (**Hensel’s Lemma**). Let R be a complete commutative local noetherian ring (such as, for example, a complete discrete valuation ring), and let $\bar{R}=R/\text{rad } R$ be its residue class field. Let $f(X) \in R[X]$ be a monic polynomial, and let \bar{f} denote its image in $\bar{R}[X]$. Prove that every factorization of \bar{f} into pairwise relatively prime monic polynomials $\{\varphi_i\}$ in $\bar{R}[X]$ lifts to a factorization of $f(X)$ in $R[X]$.

[Hint: Set $A=R[X]/(f(X))$, an R -algebra which is R -free on $\deg f$ generators. Then

$\bar{A} = A / (\text{rad } R)A = \bar{R}[X]/(\bar{f}(X))$. If $\bar{f} = \prod_{i=1}^m \varphi_i$, $\varphi_i \in \bar{R}[X]$, then there is a decomposition of \bar{A} into left ideals:

$$\bar{A} \cong \prod_1^m \bar{R}[X]/(\varphi_i(X)).$$

Correspondingly, we may write $\bar{1} = \sum_1^m \varepsilon_i$, with the $\{\varepsilon_i\}$ idempotents in \bar{A} , and where ε_i generates the i -th summand. By (6.8), there is a corresponding decomposition of A , given by $A = \bigoplus A\varepsilon_i$, where $\bar{\varepsilon}_i = \varepsilon_i$. Then $A\varepsilon_i \cong \bar{R}[X]/(g_i(X))$, for some monic $g_i(X) \in R[X]$ such that $g_i(X) | f(X)$, and $\bar{g}_i = \varphi_i$. Thus $f = \prod g_i$ is the desired factorization of f .]

12. Let A be a ring, and M an artinian left A -module. Denote by $\text{soc } M$ the *socle* of M , that is, the sum of all simple submodules of M . Show that M and $\text{soc } M$ have the same injective hull.

[Hint: Let $0 \rightarrow M \rightarrow E$ be exact, where E is an injective hull of M . Then also $0 \rightarrow \text{soc } M \rightarrow E$ is exact. If X is a nonzero submodule of E , then $X \cap M \neq 0$ since E is an injective hull of M . But $X \cap M$ is a nonzero submodule of the artinian module M , and hence contains a simple submodule S . Then $X \cap \text{soc } M \supseteq S$, which proves that E is also an injective hull of $\text{soc } M$.]

13. Let the ring A be either left artinian, or else an R -algebra as in (6.5). Let P be a f.g. projective A -module. Show that if P is indecomposable (as A -module), then every factor module of P is also indecomposable.

[Hint: Let $N = \text{rad } A$; then P has a unique maximal submodule, namely $N \cdot P$. If $f: P \rightarrow X$ is a surjection, where $X \neq 0$, then $\ker f \subseteq N \cdot P$. Hence f gives a projective cover of X . But if X decomposes, so does its projective cover by (6.25iii).]

14. Let A be an arbitrary ring, and let

$$1 = e_1 + \cdots + e_n = f_1 + \cdots + f_n$$

be two decompositions of 1_A into a sum of orthogonal idempotents. Suppose that $Ae_i \cong Af_i$ as left A -modules, $1 \leq i \leq n$. Show that there exists a unit $u \in A$ such that

$$uf_i u^{-1} = e_i \text{ for each } i.$$

[Hint: Let φ be the automorphism of the left A -module A which maps each Ae_i isomorphically onto Af_i . Then $\varphi = u_r$ for some unit $u \in A$, and

$$Ae_i \cdot u = Af_i, Af_i \cdot u^{-1} = Ae_i, 1 \leq i \leq n.$$

Then

$$1 = \sum_{i=1}^n uf_i u^{-1}, uf_i u^{-1} \in Ae_i \text{ for each } i.$$

Hence $uf_i u^{-1} = e_i$ for each i .]

15. Let e and f be idempotents in a semisimple ring A , and suppose that $Ae \cong Af$. Show that $e = ufu^{-1}$ for some unit $u \in A$.

[Hint: The left A -isomorphism

$$Ae \oplus A(1-e) \cong Af \oplus A(1-f)$$

shows that if $Ae \cong Af$, then also $A(1-e) \cong A(1-f)$.]

16. Let R be a d.v.r. with maximal ideal P and quotient field K , and let A be a split semisimple K -algebra. Let Λ be an R -order in A , that is, an R -subalgebra of A such that $K\Lambda = A$ and Λ is f.g./ R as module. Let $\bar{\Lambda} = \Lambda/P\Lambda$. Show that every idempotent ϵ of $\bar{\Lambda}$ lifts to an idempotent e_0 of Λ , and that if ϵ is central so is e_0 .

[Hint: Let $\hat{\cdot}$ denote P -adic completions. Then $\hat{\Lambda}/P\hat{\Lambda} \cong \bar{\Lambda}$, and ϵ lifts to an idempotent $e \in \hat{\Lambda}$. The hypothesis on A implies that every f.g. left $\hat{\Lambda}$ -module is the completion of some f.g. left A -module. Therefore $\hat{A}e = \hat{A}e_1$ for some idempotent $e_1 \in A$. But then $e = ue_1u^{-1}$ for some invertible element $u \in \hat{\Lambda}$ (see Exercise 15). Choose $v \in A$ close to u in the P -adic topology on $\hat{\Lambda}$; then v^{-1} exists in A , and is close to u^{-1} . Set $e_0 = ve_1v^{-1} \in A$, so e_0 is idempotent and close to e . Since $\{P^n\hat{\Lambda} : n=0, 1, 2, \dots\}$ is a fundamental system of neighborhoods of 0 in $\hat{\Lambda}$, it follows that $e_0 \in \hat{\Lambda}$ and $\bar{e}_0 = \bar{e} = \epsilon$. Then $e_0 \in A \cap \hat{\Lambda}$, so $e_0 \in \Lambda$. If ϵ is central, so is e_0 , by Exercise 8.]

§7. SEPARABLE ALGEBRAS AND SPLITTING FIELDS

Throughout this section, K denotes a field. The underlying vector spaces of K -algebras A and A -modules M are assumed to be finite dimensional. For extension fields E of K , we shall use the notations A^E , M^E , etc., for the algebras $E \otimes_K A$ and modules $E \otimes_K M$ obtained by extension of the ground field from K to E (see CR §12). We do not require $\dim_K E$ to be finite.

§7A. Separable Algebras and Modules

(7.1) Definition. Let A be a K -algebra, and M a left A -module. We call A a *separable K -algebra* if for every extension field E over K , including K itself, A^E is a semisimple E -algebra. Similarly, M is a *separable A -module* if M^E is a semisimple A^E -module for every extension field E over K .

Remarks. (i) A is a separable K -algebra if and only if the left regular module ${}_A A$ is a separable A -module (by (3.15)).

(ii) Every module M over a separable algebra A is separable (again by (3.15)).

(7.2) Lemma. *The following statements concerning a K -algebra A are equivalent:*

- (i) A is a separable K -algebra.

(ii) A^E is a split semisimple E -algebra for some finite extension field E over K .

(iii) A^Ω is a split semisimple Ω -algebra, where Ω is an algebraic closure of K .

Proof. (i) \Rightarrow (iii). By the definition of separability, A^Ω is a semisimple Ω -algebra, and hence is split semisimple, from §3C (see, in particular, the remark following (3.35)).

(iii) \Rightarrow (ii). Let $\{e'_{jk}\}$ be a set of matrix units in A^Ω such that for each fixed i , $\{e'_{jk}\}_{j,k}$ is an Ω -basis for a Wedderburn component of A^Ω (see Exercise 3.11). The matrix units $\{e'_{jk}\}$ can be expressed as Ω -linear combinations of a fixed K -basis of A , in such a way that only a finite number of elements of Ω are involved. These coefficients generate a finite algebraic extension E of K , and the matrix units $\{e'_{jk}\}$ then belong to A^E , and form an E -basis of A^E . It follows from Exercise 3.11 that A^E is a split semisimple E -algebra.

(ii) \Rightarrow (i). Let A^E be a split semisimple E -algebra for some finite extension field E of K . Suppose that A^F is not semisimple for some other extension field F of K , and let L be a composite field extension of E and F over K (see Exercise 7.10). Then there are K -embeddings $\sigma: E \rightarrow L$ and $\tau: F \rightarrow L$, which we shall view as inclusions, such that $L = E \cdot F$. Then A^L is a split semisimple L -algebra, since $A^L = (A^E)^L$. On the other hand, $\text{rad } A^F \neq 0$ since A^F is not semisimple (see (5.18)). But then $L \otimes_F \text{rad } A^F$ is a nonzero nilpotent two-sided ideal in A^L , which contradicts our previous statement that A^L is semisimple. We have thus shown that A^F is semisimple for every F over E , which completes the proof.

(7.3) Lemma. *A K -algebra A is separable if and only if A^E is semisimple for all extension fields E of K such that $\dim_K E$ is finite.*

Proof. One way is clear. For the other, suppose that A^E is semisimple for every finite extension E of K , and let Ω be an algebraic closure of K . Let E range over all fields such that

$$K \subseteq E \subseteq \Omega, \quad \dim_K E \text{ finite.}$$

For each such E , $(\text{rad } A^\Omega) \cap A^E$ is a nilpotent ideal of A^E , hence is 0 since $\text{rad } A^E = 0$ by hypothesis. But every element of A^Ω lies in A^E for some E , which shows that $\text{rad } A^\Omega = 0$. The first part of the proof of (7.2) then implies that A is separable, and the lemma is established.

Let E be a finite extension field of K of degree n . We call E a *separable extension* of K if there exist n distinct embeddings $\{\sigma_1, \dots, \sigma_n\}$ of E into some algebraic closure Ω of K , such that each σ_i fixes K elementwise (see Lang [65, VII, §4]. Equivalently, E is separable over K if $E \cong K[x]/(f(x))$, where $f(x) \in K[x]$ is a monic separable polynomial which is irreducible in $K[x]$.

(7.4) Proposition. *Let E be a finite extension field of K . Then E is separable as an extension field of K if and only if E is a separable K -algebra.*

Proof. Assume E is a separable field extension of K , and let Ω be an algebraic closure of K . Let $\{\sigma_1, \dots, \sigma_n\}$ be the distinct K -embeddings of E into Ω . By Artin's Theorem (see Exercise 7.11), $\{\sigma_1, \dots, \sigma_n\}$ are linearly independent over Ω . Now let $\{w_1, \dots, w_n\}$ be a K -basis of E , and put

$$\xi_i = (\sigma_i(w_1), \dots, \sigma_i(w_n)), \quad 1 \leq i \leq n.$$

Then the vectors ξ_1, \dots, ξ_n in $\Omega^{(n)}$ are linearly independent over Ω . It follows that the $n \times n$ matrix $(\sigma_i(w_j))$ is invertible, and so its columns are also linearly independent over Ω . Let η_i be the transpose of the i -th column, that is,

$$\eta_i = (\sigma_1(w_i), \dots, \sigma_n(w_i)), \quad 1 \leq i \leq n.$$

Then the vectors $\{\eta_i\}$ are linearly independent over Ω .

View each η_i as an element of the *algebra* $\Omega^{(n)} = \Omega \oplus \cdots \oplus \Omega$. Then for $1 \leq i, j \leq n$,

$$w_i w_j = \sum \alpha_{ijk} w_k, \quad \alpha_{ijk} \in K \Rightarrow \eta_i \eta_j = \sum \alpha_{ijk} \eta_k.$$

Let $\varphi: \Omega \otimes_K E \rightarrow \Omega^{(n)}$ be the map defined by

$$\varphi \left\{ \sum_{i=1}^n c_i (1 \otimes w_i) \right\} = \sum_{i=1}^n c_i \eta_i, \quad c_i \in \Omega, \quad 1 \leq i \leq n.$$

Then φ gives an isomorphism of Ω -algebras. But $\Omega^{(n)}$ is a split semisimple Ω -algebra, whence so is $\Omega \otimes_K E$. This shows that E^Ω is split semisimple, whence E is a separable K -algebra by Lemma 7.2.

Conversely, suppose that E is a separable K -algebra, and let Ω be an algebraic closure of K , as above. Then $\Omega \otimes_K E$ is a commutative split semisimple Ω -algebra (by (7.2)), since E is a separable K -algebra. Hence there exists an isomorphism of Ω -algebras

$$\varphi: \Omega \otimes_K E \cong \Omega^{(n)} = \Omega \oplus \cdots \oplus \Omega.$$

For each $a \in \Omega \otimes_K E$, let us write

$$\varphi(a) = (\omega_1(a), \dots, \omega_n(a)) \in \Omega^{(n)}.$$

For each i , the map $\alpha \mapsto 1 \otimes \alpha \mapsto \omega_i(1 \otimes \alpha)$, $\alpha \in E$, gives a K -embedding of E into Ω . For $i \neq j$ the embeddings are distinct, since otherwise $\omega_i(a) = \omega_j(a)$ for all $a \in \Omega \otimes_K E$, contradicting the fact that φ is an Ω -isomorphism. This completes the proof.

We now seek a criterion for a semisimple left A -module M to be separable, where A is an arbitrary f.d. K -algebra. We note first that submodules of separable modules are separable, and direct sums of separable modules are separable. Moreover, if M is a separable left A -module, then M^E is a separable left A^E -module for every extension E of K . The main result is the following theorem from Bourbaki [58], for which we supply a new proof, based on the Morita theorem and its applications to tensor products in §3E.

(7.5) Theorem. *A semisimple left A -module L is separable if and only if for every simple submodule M of L , the center of the division algebra $\text{End}_A(M)$ is a finite separable extension field of K .*

Proof. By the remarks preceding the statement of the theorem, it suffices to prove that a simple left A -module M is separable if and only if the center F of $\text{End}_A(M)$ is separable over K . By Lemma 7.3, we can test for separability by using finite extension fields E over K . Let \otimes denote \otimes_K for this proof, and let E be a finite extension field of K . Then $E \otimes M$ is a left $(E \otimes A)$ -module. Put

$$D = \{\text{End}_A(M)\}^\circ, E = \{\text{End}_E(E)\}^\circ \cong E,$$

so D is a division algebra with center F . View M as an (A, D) -bimodule, and E as (E, E) -bimodule. By Prop. 3.56, the lattice of $(E \otimes A)$ -submodules of $E \otimes M$ is isomorphic to the lattice of left ideals in $E \otimes D$.

Next, $E \otimes M$ is semisimple if and only if $\text{rad}(E \otimes M) = 0$ by Exercise 5.10. Further, by §5, the radical of a module is the intersection of its maximal submodules. Hence the vanishing of the radical is preserved under a lattice isomorphism, which shows that $E \otimes M$ is semisimple if and only if $E \otimes D$ is semisimple. Thus, M is separable over K if and only if $E \otimes D$ is semisimple for each finite extension field E of K .

We have set $F = \text{center of } D$; then E and D are finite dimensional simple K -algebras, with centers E and F , respectively. By Theorem 3.60(ii), it follows that $E \otimes D$ is semisimple if and only if $E \otimes F$ is semisimple. But $E \otimes F$ is semisimple for all E (finite over K) if and only if F is a separable field extension of K , by (7.4). This completes the proof of the theorem.

(7.6) Corollary. *Let A be a semisimple K -algebra. A necessary and sufficient condition for A to be separable is that the centers of the division algebras associated with the Wedderburn components of A are separable extension fields of K .*

Proof. From the Wedderburn Theorems in §3B, the division algebras associated with the Wedderburn components coincide with the division algebras $\{\text{End}_A(M)\}$, where M ranges over the simple submodules of the left regular module ${}_AA$. The result now follows from (7.5) because of the fact, noted earlier, that A is a separable K -algebra if and only if the left regular module is separable.

We now give a number of useful applications of the main theorem.

(7.7) Proposition. *Let A and B be K -algebras, let M and N be semisimple modules over A and B , and assume that N is separable over K . Then $M \otimes_K N$ is a semisimple $(A \otimes_K B)$ -module.*

Proof. First consider the case where both M and N are simple, and N is separable. Let $D = \{\text{End}_A(M)\}^\circ$, $E = \{\text{End}_B(N)\}^\circ$, and let $S = c(D)$ and $T = c(E)$ be the centers of the division algebras D and E . By Theorem 7.5, T is a separable extension field of K , and by Proposition 7.4, $S \otimes_K T$ is a semisimple K -algebra. By Theorem 3.60, $D \otimes_K E$ is a semisimple K -algebra, and by Proposition 3.56(iii), it follows that $M \otimes_K N$ is a semisimple $(A \otimes_K B)$ -module.

In the general case we have $M = \bigoplus M_i$, $N = \bigoplus N_j$, with $\{M_i\}$ and $\{N_j\}$ simple submodules of M and N . Moreover, the submodules N_j are all separable, as submodules of a separable module. Then $M \otimes_K N = \bigoplus_{i,j} M_i \otimes_K N_j$. By the first part of the proof all the modules $M_i \otimes_K N_j$ are semisimple, and hence $M \otimes_K N$ is semisimple, as required.

(7.8) Corollary. (i) *Let A be a semisimple K -algebra and B a separable K -algebra. Then $A \otimes_K B$ is a semisimple algebra.*

(ii) *Let M be a semisimple left A -module, and E a finite separable extension field of K . Then M^E is a semisimple A^E -module.*

(7.9) Theorem. *Let A be a K -algebra, E an extension field of K , and suppose that for each simple A -module M , the A^E -module M^E is semisimple. (This hypothesis certainly holds whenever E is a finite separable extension of K .) Then*

(i) $(A/\text{rad } A)^E \cong A^E/(\text{rad } A)^E$, and $\text{rad}(A^E) = (\text{rad } A)^E$.

(ii) *Let $\{M_1, \dots, M_s\}$ be a basic set of simple left A -modules, and let*

$$(M_i)^E \cong \coprod_{j=1}^{r_i} N_{ij}, \quad N_{ij} = \text{simple left } A^E\text{-module}.$$

Then every simple A^E -module is isomorphic to some N_{ij} . Further, $N_{ij} \cong N_{i'j'}$ implies that $i = i'$, that is, there is no overlap between the sets of simple A^E -modules which come from different simple A -modules.

Proof. We may write $A/\text{rad } A \cong \coprod M$, with M ranging over a collection of simple left $(A/\text{rad } A)$ -modules, viewed as simple A -modules. Each M_i occurs at least once in this decomposition. Therefore

$$(A/\text{rad } A)^E \cong \coprod M^E,$$

and $\coprod M^E$ is a semisimple A^E -module by virtue of the hypotheses. Since $\text{rad}(A^E)$ annihilates every semisimple A^E -module, it follows that $\text{rad}(A^E)$ annihilates $(A/\text{rad } A)^E$, that is,

$$\text{rad}(A^E) \cdot \{A^E / (\text{rad } A)^E\} = 0.$$

This gives $\text{rad}(A^E) \subseteq (\text{rad } A)^E$; the reverse inclusion is clear, so (i) is established. Further, we have

$$A^E / \text{rad}(A^E) \cong \coprod M^E,$$

which shows that *every* simple A^E -module is a direct summand of some $(M_i)^E$. Finally, for $i \neq j$ we have (by Exercise 2.7)

$$\text{Hom}_{A^E}((M_i)^E, (M_j)^E) \cong E \otimes_K \text{Hom}_A(M_i, M_j) = 0,$$

so M_i^E, M_j^E have no common summand.

(7.10) Theorem. *Let K be an arbitrary field, and G a finite group. Then $KG/\text{rad } KG$ is a separable K -algebra.*

Proof. By Maschke's Theorem 3.14, the result holds if either $\text{char } K=0$ or $\text{char } K \nmid |G|$. Thus, we may hereafter assume that $\text{char } K=p > 0$; it will not matter whether $p \nmid |G|$ or not, in the rest of the proof. The prime field k in K is the field \mathbf{F}_p of p elements, and is a perfect field. Hence every finite extension field E of k is separable over k , so $\text{rad } EG = (\text{rad } kG)^E$ by (7.9i). Then, by (7.9i) again,

$$(kG/\text{rad } kG)^E = EG / (\text{rad } kG)^E = EG / \text{rad } EG,$$

and hence $(kG/\text{rad } kG)^E$ is semisimple for each finite extension field E over k . Therefore $kG/\text{rad } kG$ is a separable k -algebra, by Lemma 7.3. But then $(kG/\text{rad } kG)^K$ is semisimple, and hence $\text{rad } KG = (\text{rad } kG)^K$. Finally, if F is any extension field of K , then

$$\begin{aligned} (KG/\text{rad } KG)^F &\cong FG / (\text{rad } KG)^F \\ &\cong FG / ((\text{rad } kG)^K)^F \cong (kG/\text{rad } kG)^F, \end{aligned}$$

and the last is semisimple. This completes the proof that $KG/\text{rad } KG$ is a separable K -algebra. Notice that the proof depends only on the fact that a group algebra KG has a distinguished basis consisting of the elements of G , so that KG is obtained from kG by extension of the base field from k to K , where $k = \mathbf{F}_p$.

The above discussion allows us to prove a stronger version of (7.9ii) for a field K of nonzero characteristic, as follows:

(7.11) Corollary. *Let $\text{char } K = p > 0$, let E be any extension field of K , and let G be a finite group. Then for each simple left KG -module V , the module V^E is a direct sum of simple EG -modules, no two of which are isomorphic.*

Proof. Let k be the prime field \mathbb{F}_p of K , so

$$KG/\text{rad } KG \cong (kG/\text{rad } kG)^K$$

by the preceding proof. Now we may write

$$kG/\text{rad } kG \cong \coprod_{i=1}^s M_{n_i}(k_i),$$

where each k_i is a division algebra over k . Then each k_i is a finite skewfield, so by Wedderburn's Theorem (see CR (68.9)), each k_i is a field, and is finite and separable over k . Therefore by (7.8i), $K \otimes_k k_i$ is a direct sum of fields, so

$$KG/\text{rad } KG \cong \coprod M_{n_i}(K \otimes_k k_i) \cong \coprod M_{n_j}(K_j),$$

with each K_j a separable field extension of K , by Exercise 7.1i.

Now let V be a simple left KG -module; then V is a simple $(KG/\text{rad } KG)$ -module, and can therefore be viewed as a simple module relative to one of the Wedderburn components of $KG/\text{rad } KG$. Denoting this component by $M_n(F)$, where F is some finite separable extension of K , we then have

$$M_n(F) \cong V^{(n)} \quad (n \text{ copies of } V)$$

as KG -modules. Therefore, if E is any extension field of K , we obtain

$$E \otimes_K M_n(F) \cong M_n(E \otimes_K F) \cong (V^E)^{(n)},$$

where $V^E = E \otimes_K V$. But $E \otimes_K F$ is a direct sum of fields $\coprod E_i$ (say), so

$$M_n(E \otimes_K F) \cong \coprod_i M_n(E_i).$$

If W_i denotes a simple left $M_n(E_i)$ -module, then $M_n(E_i) \cong W_i^{(n)}$, and we obtain

$$\coprod_i W_i^{(n)} \cong (V^E)^{(n)}.$$

Therefore $V^E \cong \coprod_i W_i$ by the Jordan-Hölder Theorem 3.11. Since the $\{W_i\}$ are

simple modules belonging to different Wedderburn components of $EG/\text{rad } EG$, it follows that these $\{W_i\}$ are non-isomorphic simple EG -modules. This shows that V^E is a direct sum of non-isomorphic simple EG -modules, as required.

§7B. Splitting Fields

(7.12) Definition. Let A be a finite dimensional algebra over a field K , and let E be an extension field of K (possibly of infinite dimension over K). Put $A^E = E \otimes_K A$. We call E a *splitting field* for A over K , and write E splits A/K , if every simple left A^E -module is absolutely simple.

Remarks. (i) The simple left A -modules coincide with the simple left $(A/\text{rad } A)$ -modules, by §5.

(ii) For a K -algebra A , every algebraically closed field containing K splits A/K , by (3.33) and (3.43).

(iii) An extension field E of K is a splitting field for A over K if and only if $A^E/\text{rad}(A^E)$ is a split semisimple E -algebra (see §3C).

(iv) If E is a splitting field for A/K , then so is every extension field F containing E .

(7.13) Proposition. Every f.d. K -algebra A has a splitting field E over K such that $\dim_K E$ is finite.

Proof. Let Ω be an algebraic closure of K . By §3C, we know that $A^\Omega/\text{rad}(A^\Omega)$ is a split semisimple Ω -algebra. Let $\varphi: A^\Omega \rightarrow A^\Omega/\text{rad}(A^\Omega)$ be the natural surjection. Choose an Ω -basis $\{b_1, \dots, b_n\}$ of A^Ω such that

$$\text{rad } A^\Omega = \bigoplus_{i=1}^r \Omega b_i \quad (\text{where } 1 \leq r < n),$$

and such that the elements $\{\varphi(b_j) : r+1 \leq j \leq n\}$ are an Ω -basis of $A^\Omega/\text{rad}(A^\Omega)$, consisting of matrix units in the various Wedderburn components of $A^\Omega/\text{rad}(A^\Omega)$. Let

$$b_i b_j = \sum_k \beta_{ijk} b_k, \quad \beta_{ijk} \in \Omega.$$

Next, we know that any K -basis $\{a_1, \dots, a_n\}$ of A gives rise to an Ω -basis $\{1 \otimes a_1, \dots, 1 \otimes a_n\}$ of A^Ω ; note also that $\dim_K A = \dim_\Omega A^\Omega = n$. We may therefore write

$$b_i = \sum_j \alpha_{ij} (1 \otimes a_j), \quad \alpha_{ij} \in \Omega.$$

Now let $E = K(\{\beta_{ijk}\}, \{\alpha_i\})$, a finite extension field of K . Viewing A^E as E -subspace of A^Ω , it follows that each b_i lies in A^E , and so $A^E = \bigoplus_{i=1}^r Eb_i$.

Since the $\{\beta_{ijk}\}$ lie in E , A^E is indeed an E -algebra. Put $N = \bigoplus_{i=1}^r Eb_i$, a nilpotent two-sided ideal of A^E , so $N \subseteq \text{rad}(A^E)$. On the other hand, A^E/N is a split semisimple E -algebra. Therefore $N = \text{rad}(A^E)$, and so $A^E/\text{rad}(A^E)$ is a split semisimple E -algebra. Hence E is a splitting field for A over K , as claimed.

Caution. In the above proof, we have *not* shown that $(A/\text{rad } A)^E \cong A^E/\text{rad}(A^E)$, nor that $E \otimes_K \text{rad } A = \text{rad}(A^E)$. We can assert only that $E \otimes \text{rad } A \subseteq \text{rad } A^E$; see (7.9) in this connection.

(7.14) Corollary. *Let A be a f.d. algebra over a perfect field K . There exists a splitting field F of A over K such that F is a finite Galois extension of K . Furthermore,*

$$F \otimes_K (A/\text{rad } A) \cong A^F/\text{rad}(A^F),$$

and $A^F/\text{rad}(A^F)$ is a split semisimple F -algebra.

Proof. By (7.13), there exists a finite extension E of K which splits A/K . Let F be a finite normal extension of K containing E . Then F is separable over K (since K is perfect), and so F is a finite Galois extension of K . Since $F \supseteq E$, the remarks following (7.12) show that F splits A over K . The remaining assertion is clear from (7.9).

(7.15) Proposition. *Let A be a f.d. K -algebra, and let E be any extension field of K . The following statements are equivalent:*

- (i) *E is a splitting field for A over K .*
- (ii) *For each simple A^E -module M , $\text{End}_{A^E}(M) = E \cdot 1_M$.*
- (iii) *There exists a finite separable extension field F of E such that F splits A/K , and such that every simple A^F -module N is of the form $M^F (= F \otimes_E M)$ for some simple A^E -module M .*

Proof. Assertions (i) and (ii) are equivalent by (3.43) and the definition of a splitting field. Clearly (i) implies (iii), by choosing $F=E$. Finally, assume that (iii) holds. Let $\{M_i\}$ be a basic set of simple A^E -modules. By (7.9), the direct summands of the A^F -modules $\{M_i^F\}$ include a basic set of simple A^F -modules. Since we are assuming (iii), it follows that each M_i^F is a simple A^F -module. Now

$$F \otimes_E \text{End}_{A^E}(M_i) \cong \text{End}_{A^F}(M_i^F) \cong F \cdot 1_M,$$

the first by (2.39), the second since M_i^F is an absolutely simple A^F -module. Thus $\text{End}_{A^E}(M_i)$ has dimension 1 over E , hence coincides with $E \cdot 1_{M_i}$, which implies that M_i is absolutely simple. Therefore E is a splitting field for A over K , as desired, and the Proposition is established.

Remarks. Parts (ii) and (iii) provide useful tests for splitting fields. For example, in CR §27, it is shown that $\text{End}_{\mathbb{Q}S_n}(M) = \mathbb{Q} \cdot 1_M$ for each simple $\mathbb{Q}S_n$ -module M ; Proposition 7.15(ii) then implies that the rational field \mathbb{Q} is a splitting field for the symmetric group S_n .

Part (iii) is often used in the theory of group representations as follows. Suppose an algebraic number field F has been found which is a splitting field for a group algebra of a finite group QG . Let $\{\mathbf{T}_1, \dots, \mathbf{T}_s\}$ be a basic set of irreducible matrix representations $\mathbf{T}_i : G \rightarrow GL_{n_i}(F)$. Suppose that for suitably chosen bases in the FG -modules affording $\{\mathbf{T}_1, \dots, \mathbf{T}_s\}$, all of the entries of the matrices $\{\mathbf{T}_i(x), x \in G, 1 \leq i \leq s\}$ belong to a field E , with $\mathbb{Q} \subseteq E \subseteq F$. Then (iii) of Proposition 7.15 implies that E is a splitting field for QG . In this situation, we say that the F -representations $\{\mathbf{T}_i\}$ are *realized* in the field E .

We conclude this section with an important result on the behavior of a simple A -module U , upon extension of the base field to a finite Galois extension which is a splitting field for A (as in Corollary 7.14). Let A be a K -algebra with K -basis $\{a_1, \dots, a_n\}$, and E a finite Galois extension field of K . Then we have structure equations

$$a_i a_j = \sum \alpha_{ijk} a_k, \text{ with } \alpha_{ijk} \in K,$$

and these also become the structure equations for the algebra A^E , relative to the E -basis $\{1 \otimes a_i\}_{1 \leq i \leq n}$:

$$(1 \otimes a_i)(1 \otimes a_j) = \sum \alpha_{ijk} (1 \otimes a_k).$$

Now let σ be an element of the Galois group $G_{E/K}$, and define a map $\sigma \otimes 1 : A^E \rightarrow A^E$ by

$$(\sigma \otimes 1) \left(\sum_{i=1}^n \xi_i \otimes a_i \right) = \sum_{i=1}^n \sigma(\xi_i) \otimes a_i, \quad \xi_i \in E, \quad a_i \in A.$$

Then $\sigma \otimes 1$ is an automorphism of the ring A^E , but is not an E -automorphism of the E -algebra A^E . Indeed, we have instead

$$(\sigma \otimes 1)(\xi y) = \sigma(\xi)(\sigma \otimes 1)y \text{ for } \xi \in E, y \in A^E.$$

Now K is the subfield of E fixed by $G_{E/K}$, that is

$$K = \{\xi \in E : \sigma(\xi) = \xi \text{ for all } \sigma \in G_{E/K}\}.$$

It follows readily that for $y \in A^E$,

$$(\sigma \otimes 1)y = y \text{ for all } \sigma \in G_{E/K} \Leftrightarrow y \in A.$$

Let \mathbf{T} be a matrix representation of A^E by matrices over E , so

$$\mathbf{T}: A^E \rightarrow M_n(E)$$

is a homomorphism of E -algebras. For each $\sigma \in G_{E/K}$, let ${}^\sigma \mathbf{T}$ be the map defined by composition of K -algebra homomorphisms

$${}^\sigma \mathbf{T}: A^E \xrightarrow{\sigma^{-1} \otimes 1} A^E \xrightarrow{\mathbf{T}} M_n(E) \xrightarrow{\sigma} M_n(E),$$

where the last map σ is given by the action of σ on the entries of the matrices over E . Thus

$$(7.16) \quad {}^\sigma \mathbf{T} = \sigma \mathbf{T}(\sigma^{-1} \otimes 1).$$

Then ${}^\sigma \mathbf{T}$ is also a homomorphism of E -algebras, since for $\xi \in E$, $a \in A$, we have

$$\begin{aligned} {}^\sigma \mathbf{T}(\xi \otimes a) &= \sigma \mathbf{T}(\sigma^{-1} \xi \otimes a) = \sigma\{\sigma^{-1} \xi \mathbf{T}(1 \otimes a)\} \\ &= \xi \sigma \mathbf{T}(1 \otimes a) = \xi \cdot {}^\sigma \mathbf{T}(1 \otimes a). \end{aligned}$$

We say that the representation ${}^\sigma \mathbf{T}$ is *conjugate* to \mathbf{T} . Clearly

$${}^\tau({}^\sigma \mathbf{T}) = {}^{(\tau\sigma)} \mathbf{T}, \quad \sigma, \tau \in G_{E/K}.$$

Furthermore, if M is a left A^E -module affording the matrix representation \mathbf{T} relative to some E -basis of M , then change of E -basis replaces \mathbf{T} by \mathbf{PTP}^{-1} for some invertible matrix \mathbf{P} , where

$$(\mathbf{PTP}^{-1})(y) = \mathbf{PT}(y)\mathbf{P}^{-1}, \quad y \in A^E.$$

Then ${}^\sigma \mathbf{T}$ is replaced by ${}^\sigma(\mathbf{PTP}^{-1})$, and we have for $\xi \in E$, $a \in A$:

$$\begin{aligned} {}^\sigma(\mathbf{PTP}^{-1})(\xi \otimes a) &= \sigma\{(\mathbf{PTP}^{-1})(\sigma^{-1} \xi \otimes a)\} \\ &= \sigma\{\mathbf{PT}(\sigma^{-1} \xi \otimes a)\mathbf{P}^{-1}\} = \sigma(\mathbf{P}) \cdot {}^\sigma \mathbf{T}(\xi \otimes a) \cdot \sigma(\mathbf{P})^{-1}. \end{aligned}$$

Hence, change of basis in M has the effect of replacing ${}^\sigma \mathbf{T}$ by an equivalent matrix representation of A^E over E . There is thus a left A^E -module, unique up to isomorphism, which affords the conjugate representation ${}^\sigma \mathbf{T}$; we denote this module by ${}^\sigma M$.

Remarks. (i) The conjugacy operation permutes the simple modules.

(ii) Let $A=KG$ for a finite group G , and let $E, G_{E/K}$ be as above. If $T: G \rightarrow GL_n(E)$ is an E -representation of G , then for $\sigma \in G_{E/K}$, the conjugate ${}^\sigma T$ is simply the E -representation of G obtained by applying σ to the entries of the matrices $T(x), x \in G$.

(7.17) Lemma. *Let A^E be a semisimple E -algebra, and M a simple left A^E -module. Let e_M be a central primitive idempotent in A^E which acts as identity operator on M . Then for $\sigma \in G_{E/K}$, $(\sigma \otimes 1)e_M$ is a central primitive idempotent which acts as the identity on the conjugate simple A^E -module ${}^\sigma M$.*

Proof. Let M afford the representation T , and ${}^\sigma M$ afford ${}^\sigma T$. From (7.16) we have

$${}^\sigma T((\sigma \otimes 1)e_M) = \sigma T((\sigma^{-1} \otimes 1)(\sigma \otimes 1)e_M) = \sigma T(e_M) = \text{identity matrix.}$$

Since e_M is a central primitive idempotent, so is $(\sigma \otimes 1)e_M$ because $\sigma \otimes 1$ is a ring automorphism of A^E . This completes the proof.

(7.18) Proposition. *Let U be a simple left A -module, and let E be a finite Galois extension of K . Then U^E is a semisimple A^E -module, and is a direct sum of conjugates of one simple A^E -module M . Moreover, all conjugates of M , under the action of Galois group $G_{E/K}$, appear in U^E with the same multiplicity.*

Proof. Let e be a central primitive idempotent in $A/\text{rad } A$, which acts as the identity on U . From (7.9), U^E is a semisimple A^E -module, and by (7.9), $(A/\text{rad } A)^E \cong A^E/\text{rad}(A^E)$. The idempotent e , viewed as an element in the semisimple E -algebra $A^E/\text{rad}(A^E) \cong (A/\text{rad } A)^E$, is a sum of central primitive idempotents. Because e is fixed by the automorphisms $\sigma \otimes 1$ for $\sigma \in G_{E/K}$, it follows that the summands of e are permuted by the automorphisms $\{\sigma \otimes 1\}$. We prove next that if $e = e_1 + \dots + e_m$, with $\{e_i\}$ central primitive idempotents in $(A/\text{rad } A)^E$, then $G_{E/K}$ permutes the e_i transitively. Otherwise, if there are several orbits relative to $G_{E/K}$, we would have

$$e = e' + e'' + \dots$$

where e' is the sum of the idempotents in one orbit, e'' the sum of those in the next, etc. Then e' is fixed by all automorphisms $\{\sigma \otimes 1 : \sigma \in G_{E/K}\}$, and hence belongs to $A/\text{rad } A$. Similarly $e'' \in A/\text{rad } A$, etc., which contradicts the assumption that e is primitive in the center of $A/\text{rad } A$.

Thus we have $e = e_1 + \dots + e_m$, where each $e_i = (\sigma_i \otimes 1)e_1$ for some $\sigma_i \in G_{E/K}$. Let e_1 act as the identity operator on the simple A^E -module M . Then by (7.17), for each i , e_i acts as the identity operator on ${}^{\sigma_i} M$. Moreover, it follows from the characteristic property of central primitive idempotents (see

Exercise 3.9) that each simple component of U^E is associated with one of the idempotents $\{e_i\}$, and hence is a conjugate of M . Therefore

$$U^E \cong \bigoplus (\sigma \cdot M)^{(m_i)},$$

where $(\sigma \cdot M)^{(m_i)}$ is the external direct sum of m_i copies of $\sigma \cdot M$. Finally, the automorphisms $\{\sigma \otimes 1 : \sigma \in G_{E/K}\}$ permute the summands of U^E transitively, and leave U^E fixed (up to A^E -isomorphism). It follows from the K-S-A Theorem (§6) that the multiplicities $\{m_i\}$ are all equal, and the theorem is proved.

(7.19) Corollary. *Let A be a K -algebra, and E a finite Galois extension of K which is a splitting field for A . Let $\{M_1, \dots, M_r\}$ be a basic set of absolutely simple A^E -modules. Then the Galois group $G_{E/K}$ permutes the simple modules $\{M_1, \dots, M_r\}$. The simple A -modules are in bijective correspondence with the $G_{E/K}$ -orbits in the set $\{M_1, \dots, M_r\}$, and the simple A -module corresponding to an orbit Θ is given by*

$$\left(\bigoplus_{i \in \Theta} M_i \right)^{(m)}$$

for some positive integer m .

§7C. Splitting Fields for Division Algebras

The general results on splitting fields in §7B leave open the question of how splitting fields are constructed. This gap is filled, to some extent, by the main results of this section, which show that maximal subfields of division algebras are splitting fields. *The assumptions stated at the beginning of §7 about finite dimensionality of algebras and vector spaces remain in force.*

(7.20) Proposition. *Let D be a division algebra with center K , M a left vector space over D , $A = \text{End}_D(M)$, and let E be a maximal subfield of D . Then there is an isomorphism of E -algebras*

$$A^E \cong \text{End}_E(M).$$

Proof. From Exercises 3.1 and 3.3, we know that A is a simple algebra with center K . By (3.61), A^E is a central simple E -algebra. Moreover, A^E acts on M according to the rule $(a \otimes \epsilon)m = a(\epsilon m)$, $a \in A$, $\epsilon \in E$, $m \in M$. Because A^E is simple, there is an isomorphism of E -algebras from A^E to the algebra of left multiplications $(A^E)_l$ on M by elements of A^E . By Exercise 3.1, M is a simple left A -module, and hence a simple left A^E -module. Let $\delta \in \text{End}_{A^E}(M)$; then $\delta \in \text{End}_A(M)$, and hence $\delta = d \cdot 1_M$ for some element $d \in D$. The fact that δ also commutes with the elements of $E \cdot 1_M$ implies that d commutes with the

elements of E , and hence $E(d)$ is a subfield of D containing E . Since E is a maximal subfield of D , we have $\delta \in E \cdot 1_M$, and hence $\text{End}_{A^E}(M) = E \cdot 1_M$. Applying the Density Theorem 3.27, and using the finite dimensionality of M over E as in (3.28), we have $(A^E)_I \cong \text{End}_E(M)$. Therefore $A^E \cong \text{End}_E(M)$ as required, because of the isomorphism $A^E \cong (A^E)_I$.

(7.21) Corollary. *Let A be a central simple K -algebra, M a simple left A -module, $D = \text{End}_A(M)$, and E a maximal subfield of D . Then E is a splitting field for A .*

The proof is immediate from (7.20), using Lemma 7.2 and the fact that $\text{End}_E(M)$ is a split semisimple E -algebra.

(7.22) Corollary. *Let D be a division algebra with center K , and let E be a maximal subfield of D . Then E is a splitting field for D , and we have*

$$\dim_E D = \dim_K E, \quad \dim_K D = (\dim_K E)^2.$$

Proof. The first statement follows from (7.20), with M the left regular module $_D D$; for then $\text{End}_D(D) \cong D^\circ$, and E is a maximal subfield of $\text{End}_D(D)$. To prove the second statement, we observe that

$$D^E \cong \text{End}_E(D)$$

in the present situation. Therefore

$$\dim_K D = \dim_E (D^E) = (\dim_E D)^2.$$

But

$$\dim_K D = \dim_E D \cdot \dim_K E,$$

so comparing this with the preceding equation, we find that $\dim_K E = \dim_E D$. This completes the proof of the corollary.

Our next objective is to show that every division algebra D with center K contains a maximal subfield E of D such that E is separable over K . (By (7.22), this field E will be a splitting field for D over K .) The result is clear if $\text{char } K = 0$, so suppose now that $\text{char } K = p \neq 0$. Our proof of the lemma below follows the treatment in Bourbaki [58], §10, No. 4; for another proof, see MO §7b.

(7.23) Lemma. *Let $\text{char } K = p \neq 0$, and let D be a division algebra with center K , where $D \neq K$. Then there exists a field E such that $K \subset E \subset D$, with E separable over K .*

Proof. Recall that an element $\delta \in D$ is *purely inseparable* over K if $\min. \text{pol.}_K(\delta) = X^{p^e} - \alpha$ for some $e \geq 0$ and some $\alpha \in K$. Let us write $D - K = \{\delta : \delta \in D, \delta \notin K\}$. If there exists an element $\delta \in D - K$ such that δ is *not* purely inseparable over K , then

$$\min. \text{pol.}_K(\delta) = f(X^{p^e})$$

for some $e \geq 0$ and some irreducible polynomial $f(X) \in K[X]$ of degree > 1 . Setting $\gamma = \delta^{p^e}$, it follows that $\gamma \in D - K$ and γ is separable over K . Then $K(\gamma)$ is a separable extension of K , and $K \subset K(\gamma) \subset D$, as desired.

We are thus left with the case where *every* element of $D - K$ is purely inseparable over K . Then there exists an element $\delta \in D - K$ such that

$$\min. \text{pol.}_K(\delta) = X^{p^{a+1}} - \alpha,$$

where $a \geq 0$ and $\alpha \in K$. Setting $\xi = \delta^{p^a}$, we have $\xi \in D - K$ and $\xi^p \in K$. Let σ be the automorphism of the K -space D given by $\sigma(x) = \xi x \xi^{-1}$, $x \in D$. Then $\sigma \neq 1$ since $\xi \notin$ center of D ; on the other hand, $(\sigma - 1)^p = \sigma^p - 1 = 0$. Hence there exists a positive integer r such that

$$(\sigma - 1)^r \neq 0, (\sigma - 1)^{r+1} = 0.$$

Choose $x \in D$ such that $(\sigma - 1)^r x \neq 0$, and set

$$y = (\sigma - 1)^{r-1} x, z = (\sigma - 1)y = (\sigma - 1)^r x.$$

Then $(\sigma - 1)z = 0$, so $\sigma z = z \neq 0$. Now put $\gamma = z^{-1}y$; then

$$\sigma(\gamma) = z^{-1}\sigma(y) = z^{-1}(z + y) = 1 + \gamma \neq \gamma.$$

Thus $\sigma(\gamma) \neq \gamma$, so σ is a K -automorphism of the field $K(\gamma)$, and $\sigma \neq 1$ on $K(\gamma)$. It follows that $K(\gamma)$ contains a separable extension field E of K with $E \neq K$, which completes the proof of the lemma.

(7.24) Proposition. *Every division algebra D with center K contains a maximal subfield E which is separable over K .*

Proof. We may assume that $D \neq K$, and that $\text{char } K = p \neq 0$. We prove the result by induction on $\dim_K D$. In Lemma 7.23 we proved the existence of a separable field extension E of K , with $K \subset E \subset D$. Let us set

$$D' = \{x \in D : xy = yx \text{ for all } y \in E\},$$

the centralizer of E in D . Then $E \subseteq D' \subseteq D$, and D' is also a division algebra; the inclusion $D' \subseteq D$ is proper, since otherwise E lies in the center K of D . By the induction hypothesis, there exists a maximal subfield F of D' such that F

is separable over E . Since separability is transitive, it follows that F is separable over K . It remains for us to verify that F is a maximal subfield of D . If this is false, then F is centralized by some element $\delta \in D - F$. Then δ centralizes E , whence $\delta \in D'$, so $F(\delta)$ is a subfield of D' properly containing F . This contradicts our assumption that F is a maximal subfield of D' . Hence F is a maximal subfield of D and F is separable over K , which completes the induction argument and proves the proposition.

We may use the preceding result to strengthen our earlier theorems about splitting fields for separable algebras. If A is a separable K -algebra, then by (7.2) there exists a splitting field E for A over K , that is, a field E such that $E \otimes_K A$ is a direct sum of full matrix algebras over E . Our aim is to establish the following improvement:

(7.25) Proposition. *Let A be a separable K -algebra. Then there exists a field E which is a finite separable extension of K , such that E is a splitting field for A over K .*

Proof. Let $A = A_1 \oplus \cdots \oplus A_s$ be the Wedderburn decomposition of A into simple components A_i . Keep i fixed for the moment, where $1 \leq i \leq s$. Let K_i be the center of A_i , so K_i is a finite separable extension of K by (7.6). We may choose a finite separable extension E_i of K_i which splits A_i over K_i , so

$$E_i \otimes_{K_i} A_i \cong M_{n_i}(E_i),$$

where $n_i^2 = \dim_{K_i} A_i$. We shall now determine the desired field E as a composite of all of the fields $\{E_i : 1 \leq i \leq s\}$.

For each i , $1 \leq i \leq s$, we may write $K_i \cong K[x]/(f_i(x))$, where $f_i(x)$ is an irreducible separable polynomial over K . Let E'_i be a splitting field for $f_i(x)$ over K , so E'_i is a finite separable extension of K which contains all the zeros of $f_i(x)$. By Exercise 7.10, we can find a composite E of the fields $E_1, \dots, E_s, E'_1, \dots, E'_s$ over K . This field E is a finite separable extension of K which contains the fields $\{E_i\}$ and $\{E'_i\}$ (or, more precisely, contains K -isomorphic copies of them.) Therefore,

$$E \otimes_K K_i \cong E[x]/(f_i(x)) \cong \prod E,$$

with the number of summands on the right equal to $\deg f_i(x)$.

We now have

$$E \otimes_K A = \bigoplus_{i=1}^s E \otimes_{K_i} A_i,$$

and

$$E \otimes_K A_i \cong (E \otimes_K K_i) \otimes_{K_i} A_i \cong \prod E \otimes_{K_i} A_i.$$

But

$$E \otimes_{K_i} A_i \cong E \otimes_{E_i} (E_i \otimes_{K_i} A_i) \cong E \otimes_{E_i} M_{n_i}(E_i) \cong M_{n_i}(E).$$

This gives the desired result, and in fact we have shown that with this choice of E , we have

$$E \otimes_K A \cong \coprod_{i=1}^s \left(\coprod M_{n_i}(E) \right),$$

where for each i , $1 \leq i \leq s$, the number of summands $M_{n_i}(E)$ is equal to $\dim_K K_i$, and where $n_i^2 = \dim_{K_i} A_i$.

§7D. Reduced Norms

Let A be a K -algebra, and let $a \in A$. As in (1.10), let $\text{char. pol.}_{A/K}(a)$ be the characteristic polynomial of the K -linear map $x \mapsto ax$, $x \in A$. The *trace map* $T_{A/K}$ and *norm map* $N_{A/K}$ are then defined by

$$(7.26) \quad \text{char. pol.}_{A/K} a = X^m - (T_{A/K} a)X^{m-1} + \cdots + (-1)^m N_{A/K} a,$$

where $m = \dim_K A$.

Suppose for the moment that $A = M_n(K)$, so each $\mathbf{a} \in A$ is a matrix over K . If $n > 1$, $T_{A/K} \mathbf{a}$ is *not* the trace of the matrix \mathbf{a} , nor is $N_{A/K} \mathbf{a}$ its determinant. Indeed, if V is a simple left A -module, then the matrix \mathbf{a} is the matrix describing the linear transformation $v \mapsto \mathbf{a}v$, $v \in V$, relative to a suitable K -basis of V . Since $A \cong V^{(n)}$, we have at once

$$\text{char. pol.}_{A/K} \mathbf{a} = \{\text{char. pol. of matrix } \mathbf{a}\}^n,$$

whence

$$T_{A/K} \mathbf{a} = n \cdot \text{trace of matrix } \mathbf{a}, \quad N_{A/K} \mathbf{a} = (\det \mathbf{a})^n.$$

This suggests that $\text{char. pol.}_{A/K}$, $T_{A/K}$ and $N_{A/K}$ may not be sufficiently delicate for certain types of calculations. Instead, it is necessary to use “reduced” versions of them, which we define below.

We now assume that A is an arbitrary separable K -algebra. Let E be a splitting field for A over K , so there is an isomorphism of E -algebras

$$(7.27) \quad h: E \otimes_K A \cong \coprod_{i=1}^s M_{n_i}(E).$$

For each $a \in A$, let

$$(7.28) \quad h(1 \otimes a) = \coprod \varphi_i(a), \text{ where } \varphi_i(a) \in M_{n_i}(E), 1 \leq i \leq s.$$

We now define the *reduced characteristic polynomial* of a by

$$(7.29) \quad \text{red. char. pol.}_{A/K} a = \prod_{i=1}^s \text{char. pol. } \varphi_i(a), \forall a \in A,$$

where $\text{char. pol. } \varphi_i(a)$ is the characteristic polynomial of the matrix $\varphi_i(a) \in M_{n_i}(E)$. As shown in MO §9 (see especially Exercise 9.3), this reduced characteristic polynomial is independent of the choice of E and of the isomorphism h in (7.27). Further, its coefficients all lie in the ground field K .

The relation between $\text{char. pol.}_{A/E}(a)$ and $\text{red. char. pol.}_{A/K}(a)$ may be obtained as follows. Let $A^E = E \otimes_K A$, where E is a splitting field for A over K , and let $\{V_1, \dots, V_s\}$ be a basic set of simple left A^E -modules. Then for each i , $1 \leq i \leq s$, $\varphi_i(a)$ is the matrix of the E -linear transformation $v \mapsto (1 \otimes a)v$, $v \in V_i$, relative to a suitable E -basis of V_i . Since

$$A^E \cong \coprod_{i=1}^s V_i^{(n_i)}$$

as left A^E -modules, we obtain

$$(7.30) \quad \text{char. pol.}_{A/E} a = \text{char. pol.}_{A^E/E} a = \prod_{i=1}^s \{\text{char. pol. } \varphi_i(a)\}^{n_i}$$

for all $a \in A$. This shows that $\text{red. char. pol.}(a)$ and $\text{char. pol.}(a)$ have the same irreducible factors, apart from multiplicities. We caution the reader that $\text{red. char. pol.}_{A/K}(a)$ need not coincide with $\text{min. pol.}_{A/K}(a)$, and is in fact a multiple of it. Further, we have $\dim_E V_i = n_i$ for each i , so $\text{red. char. pol.}_{A/K}(a)$ has degree $\sum_i n_i$.

Now let us write

$$(7.31) \quad \text{red. char. pol.}_{A/K} a = X^m - (\text{tr}_{A/K} a)X^{m-1} + \cdots + (-1)^m \text{nr}_{A/K} a$$

for $a \in A$. (Here, $m = \sum n_i$.) We call $\text{tr}_{A/K}$ the *reduced trace*, and $\text{nr}_{A/K}$ the *reduced norm*. It is easily verified that $\text{tr}_{A/K}$ is a K -linear map from A to K , and the following formulas hold true for all $a, b \in A$ and all $\alpha \in K$:

$$(7.32) \quad \text{tr } ab = \text{tr } ba, \quad \text{nr } ab = (\text{nr } a)(\text{nr } b), \quad \text{nr } \alpha a = \alpha^m \text{nr } a.$$

We note next that reduced characteristic polynomial is unchanged by extension of the ground field:

$$(7.33) \quad \text{red. char. pol.}_{A/K}(a) = \text{red. char. pol.}_{(L \otimes_K A)/L}(1 \otimes a)$$

for all $a \in A$ and all fields L containing K . This follows easily from the definition of $\text{red. char. pol.}(a)$, by choosing the splitting field E for A over K so that $E \supseteq L$.

Let us consider in more detail the special case where A is a simple algebra whose center L is separable over K . Put

$$\dim_L A = m^2, \dim_K L = n.$$

As shown in the proof of (7.25), we may choose a field E containing L , such that E splits A over K , and for such a field E we have

$$E \otimes_K A \cong \coprod M_m(E) \text{ (}n \text{ summands).}$$

From (7.30) we obtain the important relation

$$(7.34) \quad \text{char. pol.}_{A/K}(a) = \{\text{red. char. pol.}_{A/K} a\}^m, \forall a \in A,$$

valid for a simple K -algebra A of dimension m^2 over its center. This formula yields

$$(7.35) \quad T_{A/K} a = m \cdot \text{tr}_{A/K} a, N_{A/K} a = (\text{nr}_{A/K} a)^m, \forall a \in A.$$

We note finally (see MO (9.14) for proof)

$$(7.36) \quad \text{tr}_{A/K} a = T_{L/K}(\text{tr}_{A/L} a), \text{nr}_{A/K} a = N_{L/K}(\text{nr}_{A/L} a)$$

for $a \in A$. This result will play a vital role in proving Jacobinski's formula for the conductor of a maximal order into an integral group ring (see (27.8)).

We now give a number of examples to illustrate how to compute reduced norms and traces, especially for group algebras.

(7.37) Example. Let

$$A = \mathbb{Q} \oplus \mathbb{Q}i \oplus \mathbb{Q}j \oplus \mathbb{Q}k, i^2 = j^2 = -1, ij = k = -ji,$$

the skewfield of rational quaternions. Then A is a central simple \mathbb{Q} -algebra, and $E = \mathbb{Q}(i)$ is a maximal subfield of A . Each $a \in A$ is uniquely expressible as $a = \alpha + \beta j$ with $\alpha, \beta \in E$. There is then an E -isomorphism

$$f: E \otimes_{\mathbb{Q}} A \cong M_2(E), \text{ given by } f(1 \otimes a) = \begin{pmatrix} \alpha & \beta \\ -\bar{\beta} & \bar{\alpha} \end{pmatrix},$$

where bars denote complex conjugation. Then

$$\begin{aligned} \text{red. char. pol.}_{A/\mathbb{Q}} a &= \text{char. pol.} \begin{pmatrix} \alpha & \beta \\ -\bar{\beta} & \bar{\alpha} \end{pmatrix} \\ &= X^2 - (\alpha + \bar{\alpha})X + (\alpha\bar{\alpha} + \beta\bar{\beta}), \end{aligned}$$

and

$$\mathrm{tr}_{A/\mathbb{Q}} a = \alpha + \bar{\alpha}, \quad \mathrm{nr}_{A/\mathbb{Q}} a = \alpha\bar{\alpha} + \beta\bar{\beta}.$$

Note that

$$\mathrm{char. pol.}_{A/\mathbb{Q}} a = \{\mathrm{red. char. pol.}_{A/\mathbb{Q}} a\}^2,$$

and

$$T_{A/\mathbb{Q}} a = 2 \mathrm{tr}_{A/\mathbb{Q}} a, \quad N_{A/\mathbb{K}} a = (\mathrm{nr}_{A/\mathbb{Q}} a)^2.$$

(7.38) Example. Let $A = KG$, where $\mathrm{char} K = 0$ and G is abelian. Then

$$KG \cong \coprod_{i=1}^s K_i,$$

with each K_i some cyclotomic extension field of K . In this case,

$$\mathrm{nr}_{A/K} = N_{A/K} = \prod_{i=1}^s N_{K_i/K}.$$

(7.39) Example. Let $A = \mathbb{Q}G$, where

$$G = \langle x, y : x^n = 1, y^2 = 1, yxy^{-1} = x^{-1} \rangle,$$

the dihedral group D_n of order $2n$. Let d range over the positive divisors of n , and let ζ_d denote a primitive d -th root of 1 over \mathbb{Q} . Let $K_d = \mathbb{Q}(\zeta_d)$, so $\dim_{\mathbb{Q}} K_d = \varphi(d)$. Let E_d be the maximal real subfield of K_d , that is

$$E_d = \{\alpha \in K_d : \alpha = \bar{\alpha}\},$$

where bar denotes the complex conjugation. We have $\dim_{E_d} K_d = 2$ if $d > 2$, while $K_d = E_d = \mathbb{Q}$ if $d = 1$ or 2.

We may view K_d as a left A -module, on which x acts as multiplication by ζ_d , and y acts as complex conjugation. Note that the action of A on K_d is well defined, since (for d dividing n)

$$(\zeta_d)^n = 1, \quad y^2 \alpha = \bar{\alpha} = \alpha,$$

$$(yxy^{-1})\alpha = (yx)\bar{\alpha} = y(\zeta_d \bar{\alpha}) = \bar{\zeta}_d \alpha = x^{-1}\alpha, \quad \forall \alpha \in K_d.$$

Let us introduce the “twisted group algebra”

$$A_d = K_d \circ \langle y \rangle = K_d \oplus K_d y, \quad y^2 = 1, \quad y\alpha = \bar{\alpha}y, \quad \alpha \in K_d.$$

The preceding discussion shows that K_d is a simple left A_d -module, and that K_d is a simple left A -module by virtue of the surjection

$$A \rightarrow A_d, \text{ defined by } x \mapsto \xi_d, y \mapsto y.$$

The center of A_d is E_d if $d > 2$, while A_d is commutative if $d = 1$ or 2 . For $d = 1$ or 2 we have $A_d \cong \mathbb{Q} \oplus \mathbb{Q}$. On the other hand, for $d > 2$ the semisimple E_d -algebra A_d has center E_d , and is not commutative. But A_d is not a division algebra, since $y^2 = 1$ and $y \neq 1$. Therefore

$$A_d \cong M_2(E_d), d > 2.$$

Next, we observe that

$$A \cong \coprod_{d|n} A_d,$$

as is clear by comparing dimensions of both sides. Let us denote by π_d the projection map $A \rightarrow A_d$. For $a \in A$, we have

$$\text{nr}_{A/\mathbb{Q}} a = \prod_{d|n} \text{nr}_{A_d/\mathbb{Q}}(\pi_d(a)),$$

and it remains for us to compute $\text{nr}_{A_d/\mathbb{Q}}$. For $d = 1$ or 2 , A_d is commutative and $\text{nr}_{A_d/\mathbb{Q}}$ is merely the identity map. Now let $d > 2$, and let us note that

$$\text{nr}_{A_d/\mathbb{Q}} = N_{E_d/\mathbb{Q}} \text{nr}_{A_d/E_d},$$

so we must describe the reduced norm map from A_d to its center E_d . Each $a \in A_d$ is representable by a 2×2 matrix over E_d , and nr_{A_d/E_d} is the determinant of this matrix. A more convenient formulation is as follows: the map

$$\alpha \mapsto \begin{pmatrix} \alpha & 0 \\ 0 & \bar{\alpha} \end{pmatrix}, y \mapsto \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \alpha \in K_d,$$

gives an irreducible matrix representation of A_d over the field K_d . It must come from the unique simple A_d -module by ground field extension. Hence for $\alpha + \beta y \in A_d$, we have

$$\begin{aligned} \text{red. char. pol.}_{A_d/E_d}(\alpha + \beta y) &= \text{char. pol. of the matrix} \begin{pmatrix} \alpha & \beta \\ \bar{\beta} & \bar{\alpha} \end{pmatrix} \\ &= X^2 - (\alpha + \bar{\alpha})X + (\alpha\bar{\alpha} - \beta\bar{\beta}): \end{aligned}$$

Therefore

$$\text{nr}_{A_d/E_d}(\alpha + \beta y) = \alpha\bar{\alpha} - \beta\bar{\beta}, \text{ tr}_{A_d/E_d}(\alpha + \beta y) = \alpha + \bar{\alpha},$$

for all $\alpha, \beta \in K_d$. Further,

$$\text{nr}_{A_d/\mathbb{Q}}(\alpha + \beta y) = N_{E_d/\mathbb{Q}}(\alpha\bar{\alpha} - \beta\bar{\beta}),$$

and a corresponding formula holds for reduced traces. A more general version of this calculation is given in Exercise 28.2.

The reader should compare these results with those obtained in (10.11), noting that

$$\mathbb{C}G = \mathbb{C} \otimes_{\mathbb{Q}} A \cong \coprod_{d|n} \mathbb{C} \otimes_{\mathbb{Q}} A_d.$$

Here, $\mathbb{C} \otimes_{\mathbb{Q}} A_d \cong \mathbb{C} \oplus \mathbb{C}$ if $d=1$ or 2 . For $d>2$,

$$\mathbb{C} \otimes_{\mathbb{Q}} A_d \cong \mathbb{C} \otimes_{\mathbb{Q}} M_2(E_d) \cong M_2(\mathbb{C} \otimes_{\mathbb{Q}} E_d).$$

But $\mathbb{C} \otimes_{\mathbb{Q}} E_d$ is isomorphic to a direct sum of $\varphi(d)$ copies of \mathbb{C} , so

$$\mathbb{C} \otimes_{\mathbb{Q}} E_d = \coprod_{\varphi(d) \text{ copies}} M_2(\mathbb{C}).$$

(7.40) Example. Let $A = \mathbb{Q}G$, where

$$G = Q_m = \langle x, y : x^{2m} = 1, y^2 = x^m, yxy^{-1} = x^{-1} \rangle,$$

the generalized quaternion group of order $4m$. Put

$$e_1 = (1 - x^m)/2, \quad e_{-1} = (x^m + 1)/2.$$

Then e_1 and e_{-1} are orthogonal central idempotents in $\mathbb{Q}G$, so

$$\mathbb{Q}G = \mathbb{Q}G \cdot e_1 \oplus \mathbb{Q}G \cdot e_{-1}.$$

Since x^m acts as 1 on $\mathbb{Q}G \cdot e_{-1}$, we have $\mathbb{Q}G \cdot e_{-1} \cong \mathbb{Q}D_m$, with D_m dihedral of order $2m$. On the other hand,

$$\mathbb{Q}G \cdot e_1 \cong \mathbb{Q}[x, y]/(x^m + 1, y^2 - x^m, yxy^{-1} - x^{-1}).$$

Thus, in any representation of $\mathbb{Q}G \cdot e_1$, we must have

$$x^m \rightarrow -1, \quad y^2 \rightarrow -1, \quad yxy^{-1} \rightarrow 1.$$

Case 1. m even, $m = 2^r m_0$, m_0 odd, $r \geq 1$. We form

$$K_d = \mathbb{Q}(\xi_d), \quad E_d = \mathbb{Q}(\xi_d + \xi_d^{-1}), \quad d = 2^{r+1}d_0, \quad d_0|m_0.$$

Now consider the quaternion skewfield

$$\mathbb{H}_d = E_d \oplus E_d i \oplus E_d j \oplus E_d k = E_d \otimes_{\mathbb{Q}} \mathbb{H},$$

with $H = Q \oplus Qi \oplus Qj \oplus Qk$. Then $K_d = E_d \oplus E_d i$, and we may write

$$H_d = K_d \oplus K_d j, \text{ where } j^2 = -1, j\alpha = \bar{\alpha}j, \forall \alpha \in K_d.$$

For each such d , we obtain a representation of $QG \cdot e_1$ by means of the map

$$x \rightarrow \zeta_d, y \rightarrow j.$$

(Note that $\zeta_d^m = -1$, since we chose d so that $d \mid 2m$ but $d \nmid m$.) Hence we have

$$QG \cdot e_1 \cong \coprod_d H_d,$$

where $d = 2^{r+1}d_0$, $d_0 \mid m_0$. (The Q -dimension of the right hand expression is

$$2 \sum_d \varphi(d) = 2 \cdot 2^r \sum_{d_0 \mid m_0} \varphi(d_0) = 2^{r+1}m_0 = 2m,$$

so we have enough simple summands of $QG \cdot e_1$.)

We note that

$$\begin{aligned} CG \cdot e_1 &\cong \coprod_d C \otimes_Q (E_d \otimes_Q H) = \coprod_d (C \otimes_Q E_d) \otimes_Q H \\ &\cong \coprod_d \{M_2(C)\}^{\varphi(d/2)}, \end{aligned}$$

since $C \otimes_Q E_d$ is a direct sum of $\varphi(d/2)$ copies of C .

Case 2. m odd. The analysis in this case is slightly different from that above. We now set $d = 2d_0$, where $d_0 \mid m$, and now $\zeta_d = -\zeta_{d_0}$. The representation of $QG \cdot e_1$ corresponding to the value $d_0 = 1$ is given by $x \rightarrow -1$, $y \rightarrow i$, and is afforded by the Wedderburn component $Q(i)$ of $QG \cdot e_1$. For $d_0 > 1$, let

$$E_d = Q(\zeta_d + \zeta_d^{-1}), \quad K_d = E_d(i), \quad H_d = K_d \oplus K_d j,$$

where j acts as complex conjugation on K_d . Then H_d is a quaternion skewfield with center E_d , and is a Wedderburn component of $QG \cdot e_1$. Thus we obtain

$$QG \cdot e_1 \cong Q(i) \oplus \coprod_{\substack{d_0 \mid m, \\ d_0 > 1}} H_d,$$

and both sides have dimension $2m$ over Q .

In either case, we may compute reduced norms as follows: let $\alpha + \beta j \in H_d$, where $\alpha, \beta \in K_d$. As matrices over K_d , we have

$$\alpha \rightarrow \begin{pmatrix} \alpha & 0 \\ 0 & \bar{\alpha} \end{pmatrix}, j \rightarrow \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix},$$

therefore

$$\text{nr}_{H_d/E_d}(\alpha + \beta j) = \begin{vmatrix} \alpha & -\beta \\ \bar{\beta} & \bar{\alpha} \end{vmatrix} = \alpha\bar{\alpha} + \beta\bar{\beta}.$$

The fact that $\alpha\bar{\alpha} + \beta\bar{\beta} > 0$ in the real field E_d , provided not both α and β are 0, gives another verification that H_d is a skewfield.

The preceding examples show how to evaluate reduced norms in a number of cases. The last two examples are quite useful, since they exhibit the Wedderburn decompositions of the rational group algebra QG for the cases where G is a dihedral or generalized quaternion group.

Returning to the general theory, suppose now that A is a simple K -algebra of dimension m^2 over its center. If $\text{char } K$ divides m , it follows from (7.35) that the ordinary trace function $T_{A/K}$ is identically zero. As we shall see in §9A, it is desirable to have at our disposal a nondegenerate bilinear form from A to K . In the “classical” case where A is a semisimple algebra over a field of characteristic 0, the ordinary trace form $T_{A/K}$ provides such a nondegenerate form. As pointed out, this need not be the case for modular fields K , and this is one of the reasons for using $\text{tr}_{A/K}$ instead of $T_{A/K}$. We state without proof (see MO (9.26)):

(7.41) Proposition. *Let A be a separable K -algebra. Then the reduced trace $\text{tr}_{A/K}$ gives a symmetric bilinear associative nondegenerate trace form from $A \times A$ to K , namely,*

$$(a, b) \rightarrow \text{tr}_{A/K} ab, \forall a, b \in A.$$

Suppose now that $A = M_n(D)$, where D is a skewfield with center K , and let $K^\circ = K - \{0\}$. Then

$$\text{nr}_{A/K}: GL_n(D) \rightarrow K^\circ$$

gives a multiplicative homomorphism, which we may regard as a “determinant” map in some sense. Set

$$D^\circ = D - \{0\}, D^\# = D^\circ / [D^\circ, D^\circ].$$

Then $\text{nr}_{D/K}: D^\circ \rightarrow K^\circ$ is also a homomorphism, and induces a map

$$\text{nr}_{D/K}: D^\# \rightarrow K^\circ.$$

On the other hand, there is also a homomorphism

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

given by the Dieudonné determinant (see Artin [57]). We shall review its properties, and then show that

$$(7.42) \quad \text{nr}_{D/K} \det a = \text{nr}_{A/K} a \text{ for all } a \in GL_n(D).$$

By an *elementary* matrix $\mathbf{E} \in GL_n(D)$ we mean a matrix \mathbf{E} obtained from the identity matrix by replacing exactly one off-diagonal zero entry by some element of D . For $\mathbf{X} \in GL_n(D)$, $\mathbf{E}\mathbf{X}$ is obtained from \mathbf{X} by increasing some row of \mathbf{X} by a left multiple of another row; likewise, $\mathbf{X}\mathbf{E}$ is obtained by increasing some column of \mathbf{X} by a right multiple of another column of \mathbf{X} . Given any $\mathbf{X} \in GL_n(D)$, we can find products \mathbf{P} and \mathbf{Q} of elementary matrices, such that

$$\mathbf{P}\mathbf{X}\mathbf{Q} = \text{diag}(a_1, \dots, a_n), a_i \in D.$$

Since $\text{diag}(a, a^{-1})$ is itself a product of elementary matrices (see (34.20)), we may in fact choose \mathbf{P} and \mathbf{Q} so that

$$(7.43) \quad \mathbf{P}\mathbf{X}\mathbf{Q} = \text{diag}(1, \dots, 1, a), a = \prod_1^n a_i \in D.$$

The image of a in $D^\#$ is called the *Dieudonné determinant* of \mathbf{X} , $\det \mathbf{X}$. (If D is a field, then $D^\# = D$, and $\det \mathbf{X}$ is the usual determinant of \mathbf{X} . If D is not a field, then the element $a \in D$ above is not uniquely determined by \mathbf{X} , but its image in $D^\#$ is uniquely determined by \mathbf{X} .)

In particular, each elementary matrix has determinant 1. Further,

$$\det \begin{pmatrix} \mathbf{X} & * \\ \mathbf{0} & \mathbf{Y} \end{pmatrix} = (\det \mathbf{X})(\det \mathbf{Y}) \text{ for } \mathbf{X} \in GL_n(D), \mathbf{Y} \in GL_m(D),$$

and

$$\det(\mathbf{XY}) = (\det \mathbf{X})(\det \mathbf{Y}) \text{ for } \mathbf{X}, \mathbf{Y} \in GL_n(D).$$

Now apply $\text{nr}_{A/K}$ to both sides of (7.43), and use Exercise 7.3. This gives

$$\text{nr}_{A/K} \mathbf{X} = \prod_{i=1}^n \text{nr}_{D/K}(a_i) = \text{nr}_{D/K} \det \mathbf{X},$$

which establishes (7.42).

In Chapter 10, it will be necessary to know both the kernel and the image of the reduced norm map

$$\text{nr}_{A/K}: A^\times \rightarrow K^\times,$$

where A is a central simple K -algebra, and A^\times is its group of units. We shall

restrict our attention to the case where K is a global field or its completion. For each prime P of K , the completion A_P is a central simple K_P -algebra. For an infinite prime P of K , the field K_P is either the real field \mathbb{R} or the complex field \mathbb{C} .

If A is a central simple \mathbb{C} -algebra, then of course $A \cong M_n(\mathbb{C})$ for some n , and then $\text{nr } A = \mathbb{C}$. If A is a central simple \mathbb{R} -algebra, then we have

$$A \cong M_n(\mathbb{R}) \text{ or } A \cong M_n(\mathbb{H}),$$

where \mathbb{H} is the skewfield of real quaternions; this follows from the fact that \mathbb{R} and \mathbb{H} are the only f.d. skewfields with center \mathbb{R} (see MO (32.2)). It is easily seen that $\text{nr } A = \mathbb{R}$ in the first case, whereas

$$(7.44) \quad \text{nr } A = \{\alpha \in \mathbb{R} : \alpha > 0\} \text{ when } A \cong M_n(\mathbb{H}).$$

On the other hand, the following result is not hard to prove (see MO, Exercise 14.6):

(7.45) Theorem. *Let A be a central simple K -algebra, where K is the quotient field of a complete d.v.r R with finite residue class field. Then $\text{nr } A = K^\times$.*

In order to describe $\text{nr } A$ when K is a global field, we need some notation and definitions. These will play an important role in our later considerations.

(7.46) Definition. Let A be a central simple K -algebra, and let P be any prime of the global field K . Then

$$A_P \cong M_{m_P}(\Omega), (\Omega : K_P) = m_P^2,$$

where Ω is a skewfield with center K_P . Call m_P the *local index* of A at P , and κ_P the *local capacity*. The prime P is *ramified* in A if $m_P > 1$, and *unramified* if $m_P = 1$. Define

$$(7.47) \quad K^+ = \{\alpha \in K : \alpha_P > 0 \text{ at each real prime } P \text{ of } K \text{ ramified in } A\}.$$

(Thus, $K^+ = K^\times$ if K has no real primes, or if each real prime of K is unramified in A . In any case, K^+ is a subgroup of K^\times of index a power of 2.)

The following deep result is proved in MO (33.15):

(7.48) Hasse-Schilling-Maass Norm Theorem. *Let A be a central simple K -algebra, where K is a global field. Then*

$$\text{nr}_{A/K} A^\times = K^+,$$

that is, a nonzero element $\alpha \in K$ is the reduced norm of an element of A if and only if $\alpha_P > 0$ at every real prime P of K ramified in A .

The fact that $\text{nr } A^\circ \subseteq K^+$ follows readily from (7.44) and the inclusions

$$\{\text{nr } A^\circ\}_P \subseteq \text{nr}\{(A^\circ)_P\} \subseteq \text{nr}\{(A_P)^\circ\}.$$

The converse is a much deeper result.

Turning next to the question of the kernel of the map $\text{nr}: A^\circ \rightarrow K^\circ$, we observe first that the commutator subgroup $[A^\circ, A^\circ]$ of A° surely lies in this kernel. For the local case, we quote without proof:

(7.49) Theorem (Nakayama-Matsushima [43]). *Let A be a central simple K -algebra, where K is the quotient field of a complete d.v.r. with finite residue class field. Then the kernel of the surjection*

$$\text{nr}_{A/K}: A^\circ \rightarrow K^\circ$$

is precisely the commutator subgroup $[A^\circ, A^\circ]$ of A° . Thus there is an isomorphism

$$A^\circ / [A^\circ, A^\circ] \cong K^\circ.$$

As a special case of the above, we have

$$(7.50) \quad \text{nr}_{D/K}: D^\# \cong K^\circ,$$

where D is a skewfield whose center K is a local field as above. We remark that the analogue of (7.49) is also correct when $K = \mathbb{R}$ or \mathbb{C} .

The global version of these results is considerably deeper, and we state without proof:

(7.51) Theorem (Wang-Platonov). *Let K be a global field, and A a central simple K -algebra. Then $[A^\circ, A^\circ]$ is the kernel of the reduced norm map $\text{nr}_{A/K}: A^\circ \rightarrow K^+$, and there is an isomorphism*

$$A^\circ / [A^\circ, A^\circ] \cong K^+.$$

The theorem was proved by Wang [50] for the case where K is an algebraic number field. For many years, it was an open question as to whether the result holds for arbitrary K . Platonov [76] recently established the theorem for the case where K is any global field, not necessarily an algebraic number field. His work gives another proof of Wang's original theorem.

Platonov also gave examples in which $\ker(\text{nr}_{A/K})$ properly contains $[A^\circ, A^\circ]$; his field K is a field of formal power series in two variables. Earlier work of Kodama [56], [60], attempting to establish (7.51) for all fields of characteristic

0, contained some errors. Indeed, Platonov's counterexamples include some cases where $\text{char } K = 0$.

§7. Exercises

1. Let A and B be f.d. separable K -algebras, and let K' be an arbitrary extension field of K . Show

$$(i) \quad K' \otimes_K A \text{ is a separable } K'\text{-algebra.}$$

$$(ii) \quad A \otimes_K B \text{ is a separable } K\text{-algebra.}$$

[Hint: Let Ω, Ω' be algebraic closures of K and K' , respectively, with $\Omega \subseteq \Omega'$, and put

$$A^{K'} = K' \otimes_K A, \quad A^\Omega = \Omega \otimes_K A.$$

Then

$$\Omega' \otimes_{K'} A^{K'} \cong \Omega' \otimes_\Omega A^\Omega,$$

and

$$A^\Omega \otimes_\Omega B^\Omega \cong (A \otimes_K B)^\Omega.$$

Now use (7.2).]

2. If A is a separable K -algebra, show that there exists a finite Galois extension E of K which splits A over K .

3. Let $A = M_n(D)$, where D is a skewfield with center K . Let E be a splitting field for D over K , and let

$$\mu: D \rightarrow E \otimes_K D \cong M_m(E), \quad m^2 = \dim_K D.$$

There is an embedding

$$A \rightarrow E \otimes_K A \cong M_{mn}(E),$$

given by

$$a = (\alpha_{ij}) \in M_n(D) \rightarrow (\mu(\alpha_{ij})) \in M_{mn}(E).$$

Show that

$$\text{nr}_{A/K} a = \det(\mu(\alpha_{ij})).$$

Deduce from this that if the matrix a is upper triangular, then

$$\text{nr}_{A/K} a = \prod_{i=1}^n \text{nr}_{D/K} \alpha_{ii},$$

whence $\text{nr}_{A/K} a = 1$ for every elementary matrix $a \in A$.

4. Keeping the above notation, show that $\text{nr}_{A/K} a = 0$ if and only if a is a nonunit of A .

5. Keep the above notation. Show that $\text{nr}_{A/K}(A) = \text{nr}_{D/K}(D)$.

6. Let A be a f.d. K -algebra, $T: A \times A \rightarrow K$ the ordinary trace form defined by $T(a, b) = T_{A/K}(ab)$ for $a, b \in A$. Show that if T is nondegenerate, then A is a separable K -algebra.

[Hint: For any field $E \supseteq K$, $T^E: A^E \times A^E \rightarrow E$ is nondegenerate. Then A^E is semisimple by Exercise 5.6.]

7. Prove the analogue of (7.49) when $K = \mathbb{R}$ or \mathbb{C} .

8. Let D be a f.d. division algebra over its center K , and let $[D, D]$ be the K -space consisting of all finite sums $\sum (a_i b_i - b_i a_i)$, $a_i, b_i \in D$. Show that $[D, D]$ is properly contained in D .

[Hint: Let E be a maximal subfield of D , and put $D^E = E \otimes_K D$. It suffices to prove that $[D^E, D^E] \neq D^E$. But this is obvious because $D^E \cong M_n(E)$ for some n , and every element of $[D^E, D^E]$ has trace zero.]

9. Let A be a f.d. K -algebra, and let V, W be f.g. left A -modules. For E an extension field of K , let $A^E = E \otimes_K A$, $V^E = E \otimes_K V$, and so on. Show that the A^E -modules V^E and W^E have a common composition factor if and only if V and W have a common composition factor as A -modules.

[Hint: Let $\text{cf}(V)$ be the set of composition factors of V . If $\text{cf}(V) = \{V_i\}$, then $\text{cf}(V^E) = \bigcup_i \text{cf}(V_i^E)$. Hence if V and W have a common composition factor, then so do V^E and W^E . To prove the converse, we need only show that for V and W non-isomorphic simple A -modules, V^E and W^E have no common composition factor. Viewing V and W as simple $(A/\text{rad } A)$ -modules, we can find an element $a \in A$ whose image acts as 1 on V and as 0 on W . Then a itself acts in this manner on V and W , so $1 \otimes a \in A^E$ acts as 1 on each composition factor of V^E , and as 0 on each composition factor of W^E .]

10. (a) Let E_1, E_2 be arbitrary extension fields of K . Prove that there exists a composite field extension E of K , with K -embeddings $\tau_i: E_i \rightarrow E$, $i=1, 2$, such that $E = \tau_1(E_1) \cdot \tau_2(E_2)$.

(b) Let E_1, \dots, E_n be a set of finite separable extensions of the field K . Show that there exists a finite separable extension field E containing K for which there exist K -isomorphisms $\mu_i: E_i \rightarrow E$, $1 \leq i \leq n$.

[Hint: (a) Take a maximal ideal I in the K -algebra $E_1 \otimes_K E_2$, and let $E = (E_1 \otimes E_2)/I$.

(b) The desired E is just a composite of the $\{E_i\}$ over K , and may be constructed as follows: let

$$B = E_1 \otimes_K \cdots \otimes_K E_n,$$

a commutative separable K -algebra. Then B is expressible as a direct sum $\coprod B_j$, with

each B_j a finite separable field extension of K . For each i , the desired embedding of E_i in the field B_1 is given by composition of maps

$$E_i \rightarrow 1 \otimes \cdots \otimes E_i \otimes \cdots \otimes 1 \subseteq B \rightarrow B_1.]$$

11. Let E be a finite extension of the field K , and let Ω be an algebraic closure of K . Let $\{\sigma_1, \dots, \sigma_n\}$ be the distinct K -embeddings of E into Ω . Prove **Artin's Theorem**:

As maps from E to Ω , the functions $\{\sigma_1, \dots, \sigma_n\}$ are linearly independent over Ω .

[Hint: Suppose the result false, and let

$$a_1\sigma_1 + \cdots + a_r\sigma_r = 0, \quad a_i \in \Omega, \quad a_i \neq 0,$$

be a relation of shortest length r . Clearly $r \geq 2$, and there exists an $x_0 \in E$ for which $\sigma_1(x_0) \neq \sigma_2(x_0)$. Then

$$\sum_{i=1}^r a_i \sigma_i(x_0) \sigma_i(x) = 0, \quad \sum_{i=1}^r a_i \sigma_1(x_0) \sigma_i(x) = 0$$

for all $x \in E$. Subtracting one equation from the other, we obtain a shorter relation of linear dependence, connecting $\sigma_2, \dots, \sigma_r$. (See also (28.3) below.)] (As Artin pointed out, the same argument shows that any set of distinct homomorphisms $\{\sigma_1, \dots, \sigma_n\}$ of a group G (not necessarily finite) into the multiplicative group of a field Ω , are linearly independent over Ω .)

12. Let E be a finite extension of the field K . Show that E is separable over K if and only if there exists an element $x_0 \in E$ for which $T_{E/K}(x_0) \neq 0$.

[Hint: Use Exercises 6 and 11.]

13. Let A be a f.d. separable K -algebra, and V any f.g. left A -module. Prove that $\text{End}_A V$ is also a f.d. separable K -algebra.

[Hint: Use Exercise 3.7.]

§8. EXT, TOR; COHOMOLOGY OF GROUPS

§8A. Ext, Tor

In this section we shall give the definitions of the groups Ext^n and Tor_n , and shall list some of their most important properties. For proofs and details, the reader may consult the references listed at the end of §2 before the exercises.

Let A be a ring; until further notice, all A -modules are assumed to be left A -modules. Given any A -module, N , choose a surjection $\varphi_0: F_0 \rightarrow N$ with F_0 free. Then choose a surjection $\varphi_1: F_1 \rightarrow \ker \varphi_0$, with F_1 free, etc. This yields a *free resolution* of N :

$$\cdots \rightarrow F_2 \xrightarrow{\varphi_2} F_1 \xrightarrow{\varphi_1} F_0 \xrightarrow{\varphi_0} N \rightarrow 0,$$

namely, an exact sequence in which each F_j is free. It is often desirable to work instead with a more general concept: a *projective resolution* of N is an exact sequence

$$(8.1) \quad \cdots \rightarrow P_2 \xrightarrow{\varphi_2} P_1 \xrightarrow{\varphi_1} P_0 \xrightarrow{\varphi_0} N \rightarrow 0$$

in which each P_i is projective. It should be remarked that if the ring A is left noetherian, and N is f.g., then we may choose the resolution (8.1) so that each P_i is f.g.

Now let L be any other A -module, and form the sequence of additive groups

$$(8.2) \quad 0 \rightarrow \text{Hom}(P_0, L) \xrightarrow{\varphi_1^*} \text{Hom}(P_1, L) \xrightarrow{\varphi_2^*} \text{Hom}(P_2, L) \rightarrow \cdots,$$

where the φ_i^* are defined as in (2.4), and where Hom means Hom_A . Then

$$\varphi_{i+1}^* \varphi_i^* = (\varphi_i \varphi_{i+1})^* = 0, \quad i \geq 1,$$

so

$$\text{im } \varphi_i^* \subseteq \ker \varphi_{i+1}^*, \quad i \geq 1.$$

We define

$$(8.3) \quad \text{Ext}_A^n(N, L) = \frac{\ker \varphi_{n+1}^*}{\text{im } \varphi_n^*}, \quad n \geq 1.$$

This yields a family of additive groups $\text{Ext}_A^1(N, L)$, $\text{Ext}_A^2(N, L)$, and so on. Below we shall give an interpretation of Ext^1 in terms of extensions of modules. For the moment, however, there are a number of comments which must be made.

(8.4) Remarks. (i) Up to natural isomorphisms, the groups $\text{Ext}_A^n(N, L)$ depend only upon the modules N and L , and not upon the choice of the projective resolution of N .

(ii) We could have defined $\text{Ext}_A^0(N, L)$ as $\ker \varphi_1^*$. However,

$$0 \rightarrow \text{Hom}(N, L) \xrightarrow{\varphi_0^*} \text{Hom}(P_0, L) \xrightarrow{\varphi_1^*} \text{Hom}(P_1, L)$$

is exact by (2.8), whence $\ker \varphi_1^* \cong \text{Hom}(N, L)$. It is customary to identify $\text{Ext}_A^0(N, L)$ with $\text{Hom}_A(N, L)$.

(iii) The groups $\text{Ext}_A^n(N, L)$ can also be computed by using an injective resolution of L . Specifically, let $\psi_0: L \rightarrow Q_0$ be an embedding of L in the

injective module Q_0 . Then let $\psi_1 : \text{cok } \psi_0 \rightarrow Q_1$ embed the cokernel of ψ_0 in an injective module Q_1 , and so on. We obtain an exact sequence

$$(8.5) \quad 0 \rightarrow L \xrightarrow{\psi_0} Q_0 \xrightarrow{\psi_1} Q_1 \xrightarrow{\psi_2} Q_2 \rightarrow \dots$$

in which each Q_i is injective; this sequence is called an *injective resolution* of L .

Now apply $\text{Hom}_A(N, *)$, obtaining a new sequence

$$0 \rightarrow \text{Hom}(N, Q_0) \xrightarrow{(\psi_1)_*} \text{Hom}(N, Q_1) \xrightarrow{(\psi_2)_*} \text{Hom}(N, Q_2) \rightarrow \dots$$

in which $(\psi_{i+1})_* (\psi_i)_* = 0$ for $i \geq 1$. It turns out that

$$\text{Ext}_A^n(N, L) \cong \frac{\ker(\psi_{n+1})_*}{\text{im}(\psi_n)_*}, \quad n \geq 1,$$

and that $\ker(\psi_1)_* \cong \text{Hom}(N, L)$.

(iv) The groups $\text{Ext}^n(N, L)$, $n \geq 1$, have many of the same properties as $\text{Hom}(N, L)$. For example, Ext^n is additive in each variable separately, and is contravariant in the first variable and covariant in the second variable. Thus, each $f \in \text{Hom}(N, N')$ induces additive homomorphisms

$$(f_n)^* : \text{Ext}_A^n(N', L) \rightarrow \text{Ext}_A^n(N, L), \quad n \geq 1,$$

and likewise for $g : L \rightarrow L'$.

(v) If N is a projective module, then $0 \rightarrow N \rightarrow N \rightarrow 0$ is a projective resolution of N . From Definition 8.3 we conclude that $\text{Ext}_A^n(N, *) = 0$ for $n \geq 1$, that is, $\text{Ext}_A^n(N, L) = 0$ for all L and all $n \geq 1$. Conversely, it is easily shown that if $\text{Ext}^1(N, *) = 0$ then N is projective.

Analogously, if L is *injective* then $\text{Ext}^n(*, L) = 0$ for $n \geq 1$. Conversely, if $\text{Ext}^1(*, L) = 0$ then L is injective.

One of the most important properties of Ext, and one of the most useful for purposes of calculation, is the following:

(8.6) Theorem (Long exact sequence for Ext). Let

$$(8.7) \quad 0 \rightarrow L \xrightarrow{f} M \xrightarrow{g} N \rightarrow 0$$

be any short exact sequence of left A -modules, and let X be any left A -module.

Then there is a long exact sequence of additive groups

$$(8.8) \quad \begin{aligned} 0 \rightarrow \text{Hom}(N, X) &\xrightarrow{g^*} \text{Hom}(M, X) \xrightarrow{f^*} \text{Hom}(L, X) \xrightarrow{\partial} \text{Ext}^1(N, X) \\ &\xrightarrow{g^*} \text{Ext}^1(M, X) \xrightarrow{f^*} \text{Ext}^1(L, X) \xrightarrow{\partial} \text{Ext}^2(N, X) \xrightarrow{g^*} \text{Ext}^2(M, X) \\ &\xrightarrow{f^*} \text{Ext}^2(L, X) \xrightarrow{\partial} \text{Ext}^3(N, X) \rightarrow \cdots \end{aligned}$$

(8.9) Remarks. (i) We have written Hom, Ext in place of Hom_A , Ext_A , for brevity. We have omitted the subscripts on the various maps f^* , g^* , ∂ .

(ii) This result should be compared with Prop. 2.8. Given the exact sequence (8.7), Proposition 2.8 asserts the exactness of the part of (8.8) up to the first Ext term. The present theorem may be viewed as an extension of Prop. 2.8.

(iii) If M is projective then $\text{Ext}^1(M, X) = 0$, and we obtain

$$\text{Ext}^1(N, X) \cong \frac{\text{Hom}_A(L, X)}{f^*\{\text{Hom}_A(M, X)\}}.$$

We shall give below another interpretation of this formula, and thereby explain the significance of the “connecting homomorphism”

$$\partial_0: \text{Hom}_A(L, X) \rightarrow \text{Ext}_A^1(N, X).$$

Corresponding interpretations of the higher ∂ 's are less easily given, and we do not attempt this here.

(iv) Let Y be any left A -module, and let (8.7) be exact. Then there is a long exact sequence of additive groups

$$(8.10) \quad \begin{aligned} 0 \rightarrow \text{Hom}(Y, L) &\xrightarrow{f_*} \text{Hom}(Y, M) \xrightarrow{g_*} \text{Hom}(Y, N) \xrightarrow{\partial} \text{Ext}^1(Y, L) \\ &\xrightarrow{f_*} \text{Ext}^1(Y, M) \xrightarrow{g_*} \text{Ext}^1(Y, N) \xrightarrow{\partial} \text{Ext}^2(Y, L) \rightarrow \cdots. \end{aligned}$$

We conclude this informal discussion with a theorem on finite generation of extension groups. Let R be a commutative ring, and let A be an R -algebra; then A itself, and all A -modules, can be viewed as R -modules. If L, M, \dots are A -modules, then all of the additive groups $\text{Hom}_A(L, M)$, $\text{Ext}_A^n(L, M)$, $n \geq 1$, are R -modules, and all of the maps mentioned above are R -homomorphisms.

In particular, let R be a noetherian commutative ring and let A be an R -algebra which is finitely generated as R -module. For any A -module N which is f.g. over R , all of the A -modules occurring in a projective A -resolution of N may be chosen f.g. over R . From this one easily obtains (see references for details):

(8.11) Proposition. *Let A be an R -algebra, f.g. as module over the commutative noetherian ring R . Let L, M be left A -modules which are f.g. over R (or, equivalently, over A). Then the R -modules*

$$\mathrm{Hom}_A(L, M), \mathrm{Ext}_A^n(L, M), n \geq 1,$$

are also f.g. over R .

Let us now give an intuitive discussion of Ext^1 (for details, see Rotman [79]). Let A be an arbitrary ring, and let L, M, \dots be left A -modules. An A -exact sequence $0 \rightarrow L \rightarrow X \rightarrow N \rightarrow 0$ is called an *extension* of N by L ; sometimes the module X itself is referred to as the extension. Two extensions are *equivalent* if there exists a commutative diagram

$$\begin{array}{ccccccc} 0 & \longrightarrow & L & \longrightarrow & X & \longrightarrow & N & \longrightarrow 0 \\ & & 1 \downarrow & & \theta \downarrow & & 1 \downarrow & \\ 0 & \longrightarrow & L & \longrightarrow & X' & \longrightarrow & N & \longrightarrow 0. \end{array}$$

(The map θ is necessarily an A -isomorphism.)

Now let $\varphi: P \rightarrow N$ be a surjection, where P is A -projective, and let $K = \ker \varphi$. Then there is an exact sequence of A -modules

$$0 \rightarrow K \xrightarrow{i} P \xrightarrow{\varphi} N \rightarrow 0.$$

Hence for each A -module L , we have an exact sequence

$$(8.12) \quad \mathrm{Hom}(P, L) \xrightarrow{i^*} \mathrm{Hom}(K, L) \xrightarrow{\partial} \mathrm{Ext}_A^1(N, L) \rightarrow 0.$$

We shall describe ∂ explicitly. Given any $\sigma \in \mathrm{Hom}(K, L)$, we may form the pushout X of the pair of maps $\{i, \sigma\}$, thereby obtaining a commutative diagram

$$\begin{array}{ccc} K & \xrightarrow{i} & P \\ \sigma \downarrow & & \downarrow \\ L & \xrightarrow{i'} & X. \end{array}$$

By Exercise 2.2 we know that i' is injective, and that $\text{cok } i \cong \text{cok } i'$. Hence we obtain a commutative diagram with exact rows:

$$(8.13) \quad \begin{array}{ccccccc} 0 & \longrightarrow & K & \xrightarrow{i} & P & \xrightarrow{\varphi} & N \longrightarrow 0 \\ & & \downarrow \sigma & & \downarrow & & \downarrow 1 \\ 0 & \longrightarrow & L & \xrightarrow{i'} & X & \longrightarrow & N \longrightarrow 0. \end{array}$$

Thus each σ determines an extension of N by L , namely, the bottom row of the above diagram. Further, it is easily shown that σ and σ' determine equivalent extensions if and only if $\sigma - \sigma' \in i^*(\text{Hom}(P, L))$. Hence it follows from (8.12) that each element of $\text{Ext}_A^1(N, L)$ uniquely determines an equivalence class of extensions of N by L .

On the other hand, consider a given extension $0 \rightarrow L \rightarrow X \rightarrow N \rightarrow 0$ of N by L . Then in the diagram

$$\begin{array}{ccccccc} 0 & \longrightarrow & K & \xrightarrow{i} & P & \xrightarrow{\varphi} & N \longrightarrow 0 \\ & & \downarrow & & \downarrow \tau & & \downarrow 1 \\ 0 & \longrightarrow & L & \longrightarrow & X & \longrightarrow & N \longrightarrow 0, \end{array}$$

we can choose τ making the right hand square commute, since P is projective. It is easily seen that τ induces a map $\sigma: K \rightarrow L$, and we obtain a commutative diagram as in (8.13). This shows that *every* extension of N by L arises by means of the construction in (8.13). Further, the equivalence class of the extension determines σ modulo the image $i^*(\text{Hom}(P, L))$, and we thus obtain a bijection between $\text{Ext}_A^1(N, L)$ and the set of equivalence classes of extensions of L by N .

In terms of the above interpretation of Ext^1 , we may give an explicit description of the connecting homomorphism

$$\partial: \text{Hom}_A(L, X) \rightarrow \text{Ext}_A^1(N, X)$$

occurring in (8.8). Starting with the exact sequence (8.7), and any $\nu \in \text{Hom}_A(L, X)$, $\partial\nu$ is simply the equivalence class of the extension of N by X occurring as the bottom row of the commutative diagram with exact rows:

$$\begin{array}{ccccccc} 0 & \longrightarrow & L & \xrightarrow{f} & M & \longrightarrow & N \longrightarrow 0 \\ & & \downarrow \nu & & \downarrow & & \downarrow 1 \\ 0 & \longrightarrow & X & \longrightarrow & M' & \longrightarrow & N \longrightarrow 0. \end{array}$$

(Here, M' is the pushout of the pair of maps $\{f, \nu\}$).

A brief discussion of the torsion groups $\{\text{Tor}_n\}$ is desirable. Let (8.1) be a projective resolution of the left A -module N , and let L be any *right* A -module. We form the sequence of additive groups

$$\cdots \rightarrow L \otimes_A P_2 \xrightarrow{1 \otimes \varphi_2} L \otimes_A P_1 \xrightarrow{1 \otimes \varphi_1} L \otimes_A P_0 \rightarrow 0.$$

Since $(1 \otimes \varphi_i)(1 \otimes \varphi_{i+1}) = 1 \otimes \varphi_i \varphi_{i+1} = 0$ for $i \geq 1$, it follows that $\text{im}(1 \otimes \varphi_{i+1}) \subseteq \ker(1 \otimes \varphi_i)$ for $i \geq 1$. We now define

$$\text{Tor}_n^A(L, N) = \frac{\ker(1 \otimes \varphi_n)}{\text{im}(1 \otimes \varphi_{n+1})}, \quad n \geq 1.$$

This yields a family of additive groups $\{\text{Tor}_n^A(L, N), n \geq 1\}$, about which we note the following:

(8.14) Remarks. (i) Up to natural isomorphisms, the groups $\text{Tor}_n^A(L, N)$ depend only upon the modules N and L , and not upon the choice of the projective resolution of N .

(ii) We could have defined $\text{Tor}_0^A(L, N)$ as $\text{cok}(1 \otimes \varphi_1)$. However, by (2.20) we find that $\text{cok}(1 \otimes \varphi_1) \cong L \otimes_A N$. It is customary to identify $\text{Tor}_0^A(L, N)$ with $L \otimes_A N$.

(iii) The groups $\text{Tor}_n^A(L, N)$ could also be computed using a projective resolution of L .

(iv) The torsion groups $\text{Tor}_n^A(L, N)$ have many of the properties of $L \otimes_A N$. For example, Tor_n is covariant and additive in each variable. Each $f: L \rightarrow L'$ induces maps $(f_n)_*: \text{Tor}_n(L, N) \rightarrow \text{Tor}_n(L', N)$, and likewise for maps $g: N \rightarrow N'$.

(v) If L or N is projective, then $\text{Tor}_n^A(L, N) = 0$ for $n \geq 1$. Indeed, this holds if either L or N is a flat A -module. Conversely, if $\text{Tor}_1^A(L, *) = 0$ then L is flat, while if $\text{Tor}_1^A(*, N) = 0$ then N is flat.

The analogue of (8.6) holds true:

(8.15) Theorem (Long Exact Sequence for Tor). *Let*

$$0 \rightarrow L \rightarrow M \rightarrow N \rightarrow 0$$

be any short exact sequence of right A -modules, and let X be any left A -module. Then there is a long exact sequence of additive groups

$$\begin{aligned} \cdots &\rightarrow \text{Tor}_3(N, X) \rightarrow \text{Tor}_2(L, X) \rightarrow \text{Tor}_2(M, X) \rightarrow \text{Tor}_2(N, X) \rightarrow \text{Tor}_1(L, X) \\ &\rightarrow \text{Tor}_1(M, X) \rightarrow \text{Tor}_1(N, X) \rightarrow L \otimes X \rightarrow M \otimes X \rightarrow N \otimes X \rightarrow 0. \end{aligned}$$

In the above, we have written \otimes , Tor in place of \otimes_A , Tor^A , for brevity. This result should be compared with Prop. 2.20, and may be regarded as an extension thereof. Finally, we note that the analogue of Prop. 8.11 holds for $L \otimes_{\Lambda} N$ and $\text{Tor}_n^{\Lambda}(L, N)$, $n \geq 1$.

To end this section, we state a “Change of Rings” Theorem for Ext and Tor , which may be viewed as a generalization of the analogous Theorem 2.38 for Hom . The hypotheses of (2.38) must be strengthened slightly, though this causes no difficulty in practice. We have (see MO §2e for proof):

(8.16) Change of Rings Theorem. *Let A and B be R -algebras, where R is a commutative ring. Suppose that A is left noetherian and B is R -flat. Let M be a finitely generated left A -module, and N any left A -module. Set*

$$A' = B \otimes_R A, \quad M' = B \otimes_R M, \quad N' = B \otimes_R N.$$

Then the two-sided B -isomorphism α given in (2.37) is the first of a family of two-sided B -isomorphisms

$$(8.17) \quad B \otimes_R \text{Ext}_A^n(M, N) \cong \text{Ext}_{A'}^n(M', N'), \quad n \geq 0.$$

An analogous result holds with Ext^n replaced by Tor_n , with M now chosen to be a right A -module.

We shall often apply (8.16) to the special case where B is itself a commutative ring R' containing R . For example, if R is a commutative ring and $R' = S^{-1}R$, a ring of quotients of R , then R' is necessarily R -flat (see MO §3c). Thus we obtain:

(8.18) Corollary. *Let A be a left noetherian R -algebra, where R is a commutative ring. Let M, N be left A -modules, with M f.g./ A . Let S be a multiplicative subset of R . Then*

$$S^{-1}R \otimes_R \text{Ext}_A^n(M, N) \cong \text{Ext}_{S^{-1}A}^n(S^{-1}M, S^{-1}N), \quad n \geq 0.$$

If L is a f.g. right A -module, then

$$S^{-1}R \otimes_R \text{Tor}_n^A(L, N) \cong \text{Tor}_n^{S^{-1}A}(S^{-1}L, S^{-1}N), \quad n \geq 0.$$

We shall use repeatedly the following consequence of the above:

(8.19) Proposition. *Let A be a left noetherian R -algebra, where R is a commutative ring, and let M be a f.g. left A -module. For each maximal ideal P of R , let the subscript P denote localization at P . Then M is a projective A -module if and only if for each P , M_P is a projective A_P -module.*

Proof. If M is A -projective, then M is a direct summand of a free A -module. It follows at once that M_P is a direct summand of a free A_P -module, and is therefore A_P -projective. Conversely, if M_P is projective for each P , then $\text{Ext}_A^1(M, \ast) = 0$ by (8.18) and (4.2), so M is projective by (8.4v).

§8B. Cohomology of Groups

Here we shall define the *cohomology groups* $H^n(G, A)$, and the *homology groups* $H_n(G, A)$, $n \geq 0$, where G is a group acting from the left on a module A . To begin with, let $\mathbb{Z}G$ denote the integral group ring consisting of all formal finite sums $\left\{ \sum_{x \in G} \alpha_x x : \alpha_x \in \mathbb{Z} \right\}$, with addition and multiplication defined by the formulas

$$(\Sigma \alpha_x x) + (\Sigma \beta_x x) = \Sigma (\alpha_x + \beta_x) x,$$

$$(\Sigma \alpha_x x)(\Sigma \beta_y y) = \sum_{x, y} (\alpha_x \beta_y) xy.$$

Let A be a left G -module, that is, A is an additive group on which the elements of G act from the left as additive homomorphisms, such that

$$x(ya) = (xy)a, 1_G a = a \text{ for all } x, y \in G, a \in A.$$

Then we may make A into a left $\mathbb{Z}G$ -module, by defining

$$(\Sigma \alpha_x x)a = \Sigma \alpha_x (xa), a \in A.$$

Conversely, every left $\mathbb{Z}G$ -module may also be viewed as a G -module.

In the definitions below, a special role is played by the *trivial* G -module \mathbb{Z} ; this is the additive group \mathbb{Z} on which G acts trivially, that is, $gz = z$ for all $g \in G, z \in \mathbb{Z}$. For a left G -module A , we define

$$H^n(G, A) = \text{Ext}_{\mathbb{Z}G}^n(\mathbb{Z}, A), H_n(G, A) = \text{Tor}_n^{\mathbb{Z}G}(\mathbb{Z}, A), n \geq 0.$$

To make these definitions more explicit, we shall use a free resolution of the left $\mathbb{Z}G$ -module \mathbb{Z} . We now proceed to give such a resolution.

For $n \geq 0$, let F_n be the free left $\mathbb{Z}G$ -module with free basis consisting of all ordered n -tuples $\{(x_1, \dots, x_n) : x_i \in G\}$. For $n=0$, we interpret F_0 as the free $\mathbb{Z}G$ -module with a single basis element which is the “empty parentheses” denoted by the symbol $()$; thus $F_0 = \mathbb{Z}G \cdot () \cong \mathbb{Z}G$. Elements of F_n are finite sums of terms of the form $\xi(x_1, \dots, x_n)$, with $\xi \in \mathbb{Z}G$, and each $x_i \in G$.

Now consider the sequence

$$(8.20) \quad \cdots \rightarrow F_n \xrightarrow{d_n} F_{n-1} \xrightarrow{d_{n-1}} \cdots \rightarrow F_1 \xrightarrow{d_1} F_0 \xrightarrow{d_0} \mathbb{Z} \rightarrow 0,$$

where each d_n is a left $\mathbb{Z}G$ -homomorphism whose action on the given free basis of F_n is specified as follows:

$$\left\{ \begin{array}{l} d_0(\) = 1, \\ d_1(x) = x(\) - (\) = (x-1)(), \\ d_2(x, y) = x(y) - (xy) + (x), \\ \dots \\ d_n(x_1, \dots, x_n) = x_1(x_2, \dots, x_n) \\ \quad + \sum_{i=1}^{n-1} (-1)^i (x_1, \dots, x_{i-1}, x_i x_{i+1}, \dots, x_n) \\ \quad + (-1)^n (x_1, \dots, x_{n-1}). \end{array} \right.$$

It can be verified (see references) that (8.20) is an exact sequence of left $\mathbb{Z}G$ -modules, and hence gives a free $\mathbb{Z}G$ -resolution of the trivial G -module \mathbb{Z} . We now proceed to form $\text{Ext}_{\mathbb{Z}G}^n(\mathbb{Z}, A)$, where A is any left $\mathbb{Z}G$ -module. To be explicit, we consider the sequence of additive groups

$$0 \rightarrow \text{Hom}_{\mathbb{Z}G}(F_0, A) \xrightarrow{(d_1)^*} \text{Hom}_{\mathbb{Z}G}(F_1, A) \xrightarrow{(d_2)^*} \text{Hom}_{\mathbb{Z}G}(F_2, A) \rightarrow \dots$$

Then $\text{im}(d_n)^* \subseteq \ker(d_{n+1})^*$, $n \geq 1$, and we define

$$(8.21) \quad \left\{ \begin{array}{l} H^n(G, A) = \frac{\ker(d_{n+1})^*}{\text{im}(d_n)^*} = \text{Ext}_{\mathbb{Z}G}^n(\mathbb{Z}, A), n \geq 1, \\ H^0(G, A) = \ker(d_1)^* \cong \text{Hom}_{\mathbb{Z}G}(\mathbb{Z}, A). \end{array} \right.$$

We call $H^n(G, A)$ the n th cohomology group of G with coefficients in the module A .

We shall describe these groups $H^n(G, A)$ more concretely. Each $f \in \text{Hom}_{\mathbb{Z}G}(F_n, A)$ is completely determined by the images $\{f(x_1, \dots, x_n) : x_i \in G\}$, that is, by its action on a free $\mathbb{Z}G$ -basis of F_n . Hence we may identify $\text{Hom}_{\mathbb{Z}G}(F_n, A)$ with the set of all functions from $G \times \dots \times G$ into A , where the factor G occurs n times. Given a function $f: G \times \dots \times G \rightarrow A$, we have

$$d_{n+1}^* f = f d_{n+1} \in \text{Hom}_{\mathbb{Z}G}(F_n, A), n \geq 0,$$

by definition of d_{n+1}^* (see (2.4)). Explicitly, we obtain

$$(8.22) \quad \left\{ \begin{array}{l} (d_1^*f)(x) = fd_1(x) = f\{(x-1)()\} = (x-1)f(), \\ (d_2^*f)(x, y) = fd_2(x, y) = xf(y) - f(xy) + f(x), \\ (d_3^*f)(x, y, z) = xf(y, z) - f(xy, z) + f(x, yz) - f(x, y), \\ \dots \\ (d_{n+1}^*f)(x_1, \dots, x_{n+1}) = x_1 f(x_2, \dots, x_{n+1}) \\ \qquad + \sum_{i=1}^n (-1)^i f(x_1, \dots, x_{i-1}, x_i x_{i+1}, \dots, x_{n+1}) \\ \qquad + (-1)^{n+1} f(x_1, \dots, x_n). \end{array} \right.$$

In these formulas, the symbols x, x_i, y, z denote arbitrary elements of the group G , while f ranges over all elements of $\text{Hom}_{\mathbb{Z}G}(F_n, A)$ for various values of n .

In particular, $\ker d_2^*$ consists of all functions $f: G \rightarrow A$ such that

$$(8.23) \quad f(xy) = xf(y) + f(x) \text{ for all } x, y \in G.$$

Such functions are called *derivations* (or *crossed homomorphisms*) from G to A . On the other hand, those functions in $\text{im } d_1^*$ are called *principal derivations*; each $g \in \text{Hom}_{\mathbb{Z}G}(F_0, A)$ determines a principal derivation $f = d_1^*g$, given by

$$f(x) = (x-1)g(), \quad x \in G.$$

If we set $g() = a \in A$, then we have simply

$$(8.24) \quad f(x) = (x-1)a, \quad x \in G.$$

Then by definition,

$$(8.25) \quad H^1(G, A) = \frac{\text{derivations from } G \text{ to } A}{\text{principal derivations}}.$$

Later in this book, we shall meet various interpretations of this concept. For the moment, however, we merely remark that the elements of $H^1(G, A)$ correspond bijectively with classes of those automorphisms of the semidirect product $A \rtimes G$, which are the identity map on both A and G (see Rotman [79, Theorem 5.11]).

Turning next to the group $H^2(G, A)$, we note first that $\ker d_3^*$ consists of all functions $f: G \times G \rightarrow A$ such that

$$(8.26) \quad xf(y, z) - f(xy, z) + f(x, yz) - f(x, y) = 0$$

for all $x, y, z \in G$. Such an f is called a *factor set* from G to A . Those factor sets in $\text{im } d_2^*$ are called *principal factor sets*. Each function $g: G \rightarrow A$ determines a principal factor set $f = d_2^* g$, given by the formula

$$(8.27) \quad f(x, y) = xg(y) - g(xy) + g(x), \quad \forall x, y \in G.$$

Then by definition,

$$(8.28) \quad H^2(G, A) = \frac{\text{factor sets from } G \text{ to } A}{\text{principal factor sets}}.$$

(8.29) Example. Let A be a G -module, written multiplicatively, and consider an exact sequence of groups

$$(8.30) \quad 1 \rightarrow A \rightarrow E \xrightarrow{\pi} G \rightarrow 1.$$

Thus A is an abelian normal subgroup of E , with factor group isomorphic to G . Let $u: G \rightarrow E$ be a π -section*, that is, $\pi(u_x) = x$ for all $x \in G$. Since $A \trianglelefteq E$, we have $u_x A u_x^{-1} = A$ for all $x \in G$. We restrict our attention to those extensions (8.30) for which

$$(8.31) \quad u_x a u_x^{-1} = x \cdot a, \quad x \in G, a \in A,$$

where $x \cdot a$ indicates the action of x on the element a of the G -module A . (In this case, we shall say that the extension (8.30) “respects the G -module structure of A ”.) It should be pointed out that if $u': G \rightarrow E$ is another section of π , then for each $x \in G$, u_x and u'_x differ by a factor from A ; since A is abelian by hypothesis, we obtain

$$u_x a u_x^{-1} = u'_x a (u'_x)^{-1}, \quad x \in G, a \in A,$$

so condition (8.31) is independent of the choice of the π -section.

Each element of the group E is uniquely expressible in the form au_x , $a \in A$, $x \in G$, and we have

$$(au_x)(bu_y) = (a(x \cdot b))u_x u_y, \quad a, b \in A, \quad x, y \in G.$$

Hence the structure of E is completely determined once we know how to compute the products $u_x u_y$. It is easily seen that

$$(8.32) \quad u_x u_y = f(x, y) u_{xy}, \quad x, y \in G,$$

where $f: G \times G \rightarrow A$. The condition, that multiplication in E be associative,

* π is not necessarily a homomorphism of groups.

turns out to be equivalent to the condition that f be a factor set from G to A . Furthermore, if a section u' is used in place of u , we obtain a new factor set f' , which differs from f by a principal factor set. In this manner, each extension (8.30) which respects the module structure of A gives rise to a class in $H^2(G, A)$.

Now introduce the concept of equivalence of extensions: two extensions $1 \rightarrow A \rightarrow E \rightarrow G \rightarrow 1$, $1 \rightarrow A \rightarrow E' \rightarrow G \rightarrow 1$, are called *equivalent* if there exists an isomorphism $\theta: E \cong E'$ for which the diagram

$$\begin{array}{ccccccc} 1 & \longrightarrow & A & \longrightarrow & E & \longrightarrow & G & \longrightarrow 1 \\ & & \downarrow \text{id}_A & & \downarrow \theta & & \downarrow \text{id}_G & \\ 1 & \longrightarrow & A & \longrightarrow & E' & \longrightarrow & G & \longrightarrow 1 \end{array}$$

is commutative. It turns out (see Rotman [79, Theorem 10.24]) that there is a bijection between $H^2(G, A)$ and the set of equivalence classes of extensions (8.30) which respect the G -module structure of A . This bijection assigns to the class of (8.30) the class of the factor set f in $H^2(G, A)$, as described above.

(8.33) Examples. (i) Let K be a field, and let L be a finite Galois extension of K with Galois group G , so we may view L as a left G -module. We shall define an algebra $B = \coprod_{\sigma \in G} Lu_\sigma$, having as L -basis a set of symbols $\{u_\sigma : \sigma \in G\}$, which are to be manipulated according to the formulas

$$u_\sigma \cdot l = \sigma(l)u_\sigma, \quad u_\sigma u_\tau = f(\sigma, \tau)u_{\sigma\tau}, \quad l \in L, \quad \sigma, \tau \in G,$$

where each $f(\sigma, \tau) \in L^\times$. (Here, L^\times denotes the multiplicative group of nonzero elements of L .) The K -algebra B will be associative if and only if f is a factor set from G to L^\times . For such a factor set f , the algebra B is called a *crossed-product algebra*, and is denoted by $(L/K, f)$. The isomorphism class of B depends only upon the cohomology class of f in $H^2(G, L^\times)$. (See MO p. 242).

(ii) Let G be a finite group, and R any commutative ring. Let $f: G \times G \rightarrow R^\times$ be a factor set from G into the group of units of R . We define an R -algebra $(RG)_f$, called the *twisted group algebra* (of G relative to the factor set f) as follows:

$$(RG)_f = \bigoplus_{x \in G} Ru_x,$$

with multiplication defined by

$$u_x \alpha = \alpha u_x, \quad u_x u_y = f(x, y)u_{xy}, \quad \forall \alpha \in R, \quad \forall x, y \in G.$$

The terminology “twisted group algebra” is sometimes used in a different sense (see (7.39) and §28).

We finally consider $H^0(G, A)$; we have already remarked that $H^0(G, A) \cong \text{Hom}_{\mathbb{Z}G}(\mathbb{Z}, A)$, an obvious consequence of (8.4ii). Now an element $g \in \text{Hom}_{\mathbb{Z}G}(\mathbb{Z}, A)$ is completely determined by the image $g(1) \in A$. Since \mathbb{Z} is the trivial G -module, the image $g(1)$ must also be G -trivial. We set*

$$A^G = \{a \in A : xa = a \text{ for all } x \in G\},$$

the G -trivial submodule of A . The above remarks show that $\text{Hom}_{\mathbb{Z}G}(\mathbb{Z}, A) \cong A^G$ as additive groups. We now give another proof that $H^0(G, A) \cong A^G$. By definition,

$$H^0(G, A) = \{f \in \text{Hom}_{\mathbb{Z}G}(F_0, A) : d_1^* f = 0\}.$$

We identify $\text{Hom}_{\mathbb{Z}G}(F_0, A)$ with A , by letting f correspond to $f(\) = a \in A$. We have $d_1^* f = 0$ if and only if $(x - 1)a = 0$ for all $x \in G$, that is, if and only if $a \in A^G$. This proves that

$$H^0(G, A) \cong A^G \cong \text{Hom}_{\mathbb{Z}G}(\mathbb{Z}, A),$$

as claimed.

From the properties of Ext, we may read off properties of the cohomology groups. For example, we have

$$H^n(G, A) = 0 \text{ for } n \geq 1$$

for every projective $\mathbb{Z}G$ -module A . As another example, we obtain from (8.10) the following:

(8.34) Proposition. *For any G -module A , let A^G denote the G -trivial submodule of A . Then for each exact sequence*

$$0 \rightarrow A \rightarrow B \rightarrow C \rightarrow 0$$

of left $\mathbb{Z}G$ -modules, there is a long exact sequence of additive groups

$$0 \rightarrow A^G \rightarrow B^G \rightarrow C^G \rightarrow H^1(G, A) \rightarrow H^1(G, B) \rightarrow H^1(G, C) \rightarrow H^2(G, A) \rightarrow \cdots.$$

§8C. The Schur Criterion for Split Extensions

We shall apply the theory of extensions and $H^2(G, A)$, discussed in (8.29), to prove a basic result in finite group theory, attributed to Schur (see Zassenhaus [49]).

*Later, the G -trivial submodule of A will be denoted by $\text{inv}_G A$, to avoid confusion with the notation for induced modules.

(8.35) Theorem. *Let H be a normal subgroup of a finite group E such that the order $|H|$ and the index $|E:H|$ are relatively prime. Then there exists a subgroup $S \leq E$ of order $|E:H|$, and E is a semidirect product $H \rtimes S$.*

Before beginning the proof, we remark that in case either H or E/H is solvable, Zassenhaus proved [49] that any two subgroups of order $|E:H|$ are conjugate in E . This result, together with Theorem 8.35, is usually referred to as the *Schur-Zassenhaus Theorem*. For later use, we require only the existence theorem (8.35). For a proof of the conjugacy result, see Zassenhaus [49, p. 132], Gorenstein [68, p. 221] or Huppert [67, p. 128].

We begin the proof of Theorem 8.35 with some preliminary remarks about extensions. Let

$$(8.36) \quad 1 \rightarrow A \rightarrow E \xrightarrow{\pi} G \rightarrow 1$$

be a group extension as in (8.30), where A is an abelian multiplicative group. A π -section is a map $u: G \rightarrow E$ such that $\pi(u_x) = x$ for all $x \in G$. Each π -section determines an action of G on A by means of the formula

$$x \cdot a = u_x a u_x^{-1}, \quad x \in G, a \in A,$$

and we may then view A as a $\mathbb{Z}G$ -module. Let $f: G \times G \rightarrow A$ be the factor set associated with the extension, defined as in (8.32):

$$u_x u_y = f(x, y) u_{xy}, \text{ where } f(x, y) \in A, \text{ for all } x, y \in G.$$

Condition (8.26), in multiplicative form, becomes

$$(8.37) \quad \{x \cdot f(y, z)\}f(x, yz) = f(xy, z)f(x, y) \text{ for all } x, y, z \in G,$$

and is equivalent to the requirement that multiplication of the elements $\{u_x : x \in G\}$ be associative.

We say that the action of G on A is *trivial* if $x \cdot a = a$ for all $x \in G, a \in A$. This occurs if and only if E is a *central extension* of G , which means that the kernel A of the extension (8.36) is contained in the center of E . (For a more extensive discussion of central extensions, see §11E.)

Another observation is that the extension (8.36) splits if and only if the factor set f is equivalent to 1 (notation: $f \sim 1$), that is, the image of f in $H^2(G, A)$ is the identity. By the Definition (8.28) of $H^2(G, A)$, $f \sim 1$ if and only if f is a principal factor set. By (8.27), this means that there exists a map $g: G \rightarrow A$ such that

$$(8.38) \quad f(x, y) = \{x \cdot g(y)\}g(xy)^{-1}g(x) \text{ for all } x, y \in G.$$

Moreover, the extension (8.36) splits if and only if there exists a π -section $v: G \rightarrow E$ which is a homomorphism: $v_{xy} = v_x v_y$ for all $x, y \in G$. Using the fact that any two π -sections define the same action of G on A , it is easily verified that a π -section v is a splitting homomorphism if and only if the map $g: G \rightarrow A$ defined by $g(x) = u_x v_x^{-1}$, $x \in G$, satisfies condition (8.38). It can also be seen that the condition $f \sim 1$ is equivalent to the splitting of the extension, as a consequence of the correspondence in §8B between equivalence classes of extensions and elements of $H^2(G, A)$.

(8.39) Lemma. *Let G be a finite group acting on a finite abelian multiplicative group A . Then every element of $H^2(G, A)$ has order dividing both $|G|$ and the exponent of A .*

Proof. Let $f: G \times G \rightarrow A$ be a factor set. Fix $x, y \in G$, and define a map $g: G \rightarrow A$ by

$$g(y) = \prod_{z \in G} f(y, z).$$

Upon multiplying (8.37) over $z \in G$, and rearranging terms since A is abelian, we have

$$\left\{ \prod_{z \in G} x \cdot f(y, z) \right\} \left\{ \prod_{z \in G} f(x, yz) \right\} = \left\{ \prod_{z \in G} f(xy, z) \right\} \left\{ \prod_{z \in G} f(x, y) \right\}.$$

Since yz ranges over G as z does, the above formula becomes

$$\{x \cdot g(y)\}g(x) = g(xy)f(x, y)^n, \text{ where } n = |G|.$$

By (8.38), this implies that $f(x, y)^n$ is a principal factor set, hence every element of $H^2(G, A)$ has order dividing $|G|$. On the other hand, since f has values in A , we clearly have $f^m = 1$, where m is the exponent of A , and the result follows.

(8.40) Corollary. *Every extension*

$$1 \rightarrow A \rightarrow E \rightarrow G \rightarrow 1$$

of a finite group G by an abelian group A , such that the orders of A and G are relatively prime, is a split extension.

Proof. By Lemma 8.39, in this case we have $H^2(G, A) = 1$. By the remarks preceding (8.39), it follows that the extension splits, completing the proof.

We are now ready to finish the proof of Theorem 8.35. Let $H \trianglelefteq E$, $G = E/H$, and assume that the orders m of H and n of G are relatively prime.

It is clearly sufficient to prove that E has a subgroup S of order n , because then $|SH|$ will necessarily coincide with $|E|$, so that E will be a semidirect product $H]S$, as in the statement of the theorem.

We use induction on m , the theorem being trivial if $m=1$. Assume $m>1$, and let p be a prime dividing m . We note that all Sylow p -subgroups of E are contained in H ; for H contains at least one, so by normality of H and Sylow's Theorem, H contains all others. Hence the number of Sylow p -subgroups in H is the same as the number in E , and if P is one of them, we again apply the Sylow theorems (see CR (6.7)) to obtain

$$|E : N_E(P)| = |H : N_H(P)|.$$

Hence

$$|N_E(P) : N_H(P)| = |E : H| = n.$$

Moreover, $N_H(P) = H \cap N_E(P)$, and is normal in $N_E(P)$ by an isomorphism theorem (CR(2.8)). Thus, if $N_E(P)$ is properly contained in G , we can use the induction hypothesis to conclude that $N_E(P)$, and hence E , contains a subgroup of order n .

Thus we may now assume that $E = N_E(P)$, so that P is normal in E , and hence in H . If P is properly contained in H , then by induction E contains a subgroup S of order $|E : P|$ isomorphic to E/P . In this case we also have $|H : P| < m$, and H/P is a normal subgroup of E/P whose order and index are relatively prime. By a second application of the induction hypothesis, the subgroup $S \cong E/P$ contains a subgroup of order $|(E/P)/(H/P)| = |E : H| = n$, proving the theorem in this situation.

Finally, we are reduced to the case where $H=P$. If P is abelian, the extension E of G by P splits, by Corollary 8.40. If P is not abelian, its center Z is nontrivial, is properly contained in P , and is a characteristic subgroup of P . Hence Z is normal in E . By the induction hypothesis, E/Z contains a subgroup U/Z of order n , for some proper subgroup U of E . By induction once again, it follows that U , and hence E , contains a subgroup of order n , and the proof of Theorem 8.35 is complete.

§8D. Tate Cohomology Groups

When G is a finite group, it is sometimes desirable to use the *Tate cohomology groups* $\hat{H}^n(G, A)$, $n \geq 0$, in place of the usual groups $H^n(G, A)$. The groups \hat{H}^n may be defined thus: we set

$$(8.41) \quad N_G = \sum_{x \in G} x \in \mathbb{Z}G.$$

Then $yN_G = N_G$ for each $y \in G$, and indeed $\mathbb{Z} \cdot N_G$ is the G -trivial submodule of

$\mathbb{Z}G$. For any left G -module A , we define

$$(8.42) \quad \hat{H}^n(G, A) = \begin{cases} H^n(G, A), & n > 0 \\ A^G/N_G A, & n = 0. \end{cases}$$

For any $a \in A^G$, we have $N_G a = |G|a$; therefore the group order $|G|$ annihilates $\hat{H}^0(G, A)$. This same result holds for \hat{H}^n , as we see from the following result, which generalizes Maschke's Theorem 3.14, as well as Lemma 8.39:

(8.43) Proposition. *Let G be a finite group of order $|G|$, and let A be any left $\mathbb{Z}G$ -module. Then*

$$|G| \cdot \hat{H}^n(G, A) = 0, \quad n \geq 0.$$

Proof. We have already established the result for $n=0$, so now let $n \geq 1$, and let

$$f: \underbrace{G \times \cdots \times G}_{n} \rightarrow A$$

be a representative of a cohomology class in $H^n(G, A)$. Then $d_{n+1}^* f = 0$, and thus

$$\begin{aligned} 0 &= x_1 f(x_2, \dots, x_{n+1}) + \sum_{i=1}^{n-1} (-1)^i f(x_1, \dots, x_i x_{i+1}, \dots, x_{n+1}) \\ &\quad + (-1)^n f(x_1, \dots, x_n x_{n+1}) + (-1)^{n+1} f(x_1, \dots, x_n) \end{aligned}$$

for all $x_i \in G$. Sum over all $x_{n+1} \in G$, and set

$$g(x_1, \dots, x_n) = \sum_{x \in G} f(x_1, \dots, x_n, x).$$

Then we obtain

$$\begin{aligned} 0 &= x_1 g(x_2, \dots, x_n) + \sum_{i=1}^{n-1} (-1)^i g(x_1, \dots, x_i x_{i+1}, \dots, x_n) \\ &\quad + (-1)^n g(x_1, \dots, x_{n-1}) + (-1)^{n+1} |G| \cdot f(x_1, \dots, x_n) \end{aligned}$$

for all $x_i \in G$. This gives

$$0 = d_n^* g + (-1)^{n+1} |G| f,$$

whence $|G| \cdot f \in \text{im } d_n^*$. This proves that $|G|$ annihilates $\hat{H}^n(G, A)$, as claimed.

Let us turn next to a brief description of the homology groups $H_n(G, A)$, $n \geq 0$, where A is a left $\mathbb{Z}G$ -module and G is an arbitrary group (not necessarily finite). By slightly modifying the construction (8.20), we may obtain a free $\mathbb{Z}G$ -resolution

$$\cdots \rightarrow X_2 \xrightarrow{d_2} X_1 \xrightarrow{d_1} X_0 \xrightarrow{d_0} \mathbb{Z} \rightarrow 0$$

of the trivial *right* G -module \mathbb{Z} . Now let A be any left $\mathbb{Z}G$ -module; to construct the groups $\text{Tor}_n^{\mathbb{Z}G}(\mathbb{Z}, A)$, we form the sequence of additive groups

$$\cdots \rightarrow X_2 \otimes_{\mathbb{Z}G} A \xrightarrow{d_2 \otimes 1} X_1 \otimes_{\mathbb{Z}G} A \xrightarrow{d_1 \otimes 1} X_0 \otimes_{\mathbb{Z}G} A \rightarrow 0.$$

Then we have (by definition)

$$H_n(G, A) = \text{Tor}_n^{\mathbb{Z}G}(\mathbb{Z}, A) = \frac{\ker(d_n \otimes 1)}{\text{im}(d_{n+1} \otimes 1)}, \quad n \geq 1,$$

and

$$H_0(G, A) = \text{Tor}_0^{\mathbb{Z}G}(\mathbb{Z}, A) \cong \mathbb{Z} \otimes_{\mathbb{Z}G} A.$$

We shall calculate $H_0(G, A)$ explicitly. Let $\epsilon: \mathbb{Z}G \rightarrow \mathbb{Z}$ be the *augmentation map*, that is, ϵ is the ring homomorphism given by

$$(8.44) \quad \epsilon\left(\sum_{x \in G} \alpha_x x\right) = \sum \alpha_x.$$

The kernel of ϵ is the *augmentation ideal* I_G of $\mathbb{Z}G$; clearly I_G is a two-sided ideal of $\mathbb{Z}G$, and it is easily seen that

$$(8.45) \quad I_G = \bigoplus_{\substack{x \in G \\ x \neq 1}} \mathbb{Z} \cdot (x - 1).$$

There is an exact sequence of right $\mathbb{Z}G$ -modules

$$(8.46) \quad 0 \rightarrow I_G \rightarrow \mathbb{Z}G \rightarrow \mathbb{Z} \rightarrow 0,$$

where \mathbb{Z} is the trivial G -module. Hence by (2.20) the sequence

$$I_G \otimes A \rightarrow \mathbb{Z}G \otimes A \rightarrow \mathbb{Z} \otimes A \rightarrow 0$$

is exact, where \otimes means $\otimes_{\mathbb{Z}G}$. But under the isomorphism $\mathbb{Z}G \otimes A \cong A$ (see (2.16)), the image of $I_G \otimes A$ is precisely

$$I_G A = \left\{ \sum_{x \in G} (x - 1) a_x : a_x \in A \right\},$$

where only finite sums are intended. Hence we have

$$\mathbb{Z} \otimes_{\mathbb{Z}G} A \cong A/I_G A.$$

(In fact, $A/I_G A$ is the largest G -trivial quotient of the left G -module A .) This gives

$$H_0(G, A) \cong A/I_G A.$$

We shall not give explicit formulas for $H_n(G, A)$ for $n \geq 1$, since these are rather complicated.

Properties of the homology groups $H_n(G, A)$ may be read off from those of the torsion groups Tor_n . Thus we have

$$H_n(G, A) = 0 \text{ for } n \geq 1,$$

if A is any projective $\mathbb{Z}G$ -module (or more generally, if A is flat). Likewise, an exact sequence $0 \rightarrow A \rightarrow B \rightarrow C \rightarrow 0$ of left $\mathbb{Z}G$ -modules yields a long exact sequence of homology groups (see (8.15))

$$\begin{aligned} \dots &\rightarrow H_2(G, C) \rightarrow H_1(G, A) \rightarrow H_1(G, B) \rightarrow H_1(G, C) \\ &\rightarrow A/I_G A \rightarrow B/I_G B \rightarrow C/I_G C \rightarrow 0. \end{aligned}$$

When G is finite, one introduces the Tate cohomology groups $\hat{H}^n(G, A)$, $n \leq -1$, as follows: for a left $\mathbb{Z}G$ -module A , let

$$(8.47) \quad {}_{N_G} A = \{a \in A : N_G a = 0\},$$

where N_G is given in (8.41). We now put

$$(8.48) \quad \hat{H}^n(G, A) = \begin{cases} H_{-n-1}(G, A), & n \leq -2 \\ ({}_{N_G} A)/I_G A, & n = -1. \end{cases}$$

Thus $\hat{H}^{-1}(G, A)$ is a submodule of $H_0(G, A)$. The assertion in (8.43) remains valid for $n < 0$, though we shall not prove it here.

Suppose now that G is a finite cyclic group, with generator x of order m . Let

$$D = x - 1, N = x^{m-1} + x^{m-2} + \dots + x + 1,$$

viewed as left multiplications on the integral group ring $\mathbb{Z}G$. It is easily found that the sequence of left $\mathbb{Z}G$ -modules

$$\dots \rightarrow \mathbb{Z}G \xrightarrow{D} \mathbb{Z}G \xrightarrow{N} \mathbb{Z}G \xrightarrow{D} \dots \xrightarrow{N} \mathbb{Z}G \xrightarrow{D} \mathbb{Z}G \xrightarrow{\epsilon} \mathbb{Z} \rightarrow 0$$

is exact, where ϵ is the augmentation map. This sequence yields a free resolution of the trivial G -module \mathbf{Z} ; we may use it to compute the groups $H^n(G, A)$ for any left G -module A . Specifically, we form the sequence

$$0 \rightarrow \text{Hom}_{\mathbf{Z}G}(\mathbf{Z}G, A) \xrightarrow{D^*} \text{Hom}_{\mathbf{Z}G}(\mathbf{Z}G, A) \xrightarrow{N^*} \text{Hom}_{\mathbf{Z}G}(\mathbf{Z}G, A) \xrightarrow{D^*} \cdots.$$

Identify each $\text{Hom}_{\mathbf{Z}G}(\mathbf{Z}G, A)$ with A ; since $\mathbf{Z}G$ is commutative, the maps D^* , N^* are left $\mathbf{Z}G$ -homomorphisms. Then

$$\ker D^* \cong \{a \in A : Da = 0\} = A^G, \quad \ker N^* \cong \{a \in A : Na = 0\} = {}_NA,$$

$$\text{im } D^* = (x - 1)A = I_G A, \quad \text{im } N^* = NA.$$

We obtain

$$(8.49) \quad \begin{cases} \hat{H}^1(G, A) \cong \hat{H}^3(G, A) \cong \cdots \cong {}_NA/I_G A, \\ \hat{H}^2(G, A) \cong \hat{H}^4(G, A) \cong \cdots \cong A^G/NA. \end{cases}$$

It is easily checked that for all $n \in \mathbf{Z}$,

$$\hat{H}^{2n+1}(G, A) \cong {}_NA/I_G A, \quad \hat{H}^{2n}(G, A) \cong A^G/NA.$$

Throughout the rest of the discussion, let G be a finite group. Given a left $\mathbf{Z}G$ -module A , we have defined the Tate cohomology groups $\hat{H}^i(G, A)$ for each $i \in \mathbf{Z}$. For $i > 0$, we saw that \hat{H}^i coincides with the usual cohomology group H^i (see (8.42)), while for $i \leq -2$, \hat{H}^i is a homology group (see (8.48)). The modifications introduced for the values $i = 0, -1$ seem at first to be rather arbitrary. However, these modifications permit us to establish a close relationship between $\{\hat{H}^i, i \geq 0\}$ and $\{\hat{H}^i, i \leq 0\}$; this relationship is vital in many applications.

We state without proof a number of basic results (see Weiss [69] for proofs):

(8.50) Proposition. *Let $A = \mathbf{Z}G \otimes_{\mathbf{Z}} X$, where X is any \mathbf{Z} -module (call A “ G -induced”). Then*

$$\hat{H}^n(G, A) = 0 \text{ for all } n \in \mathbf{Z}.$$

(8.51) Proposition (Long Exact Sequence). *Let*

$$0 \rightarrow A \rightarrow B \rightarrow C \rightarrow 0$$

be an exact sequence of $\mathbf{Z}G$ -modules. Then there is a long exact sequence of

additive groups

$$\begin{aligned} \cdots &\rightarrow \hat{H}^{-2}(G, A) \rightarrow \hat{H}^{-2}(G, B) \rightarrow \hat{H}^{-2}(G, C) \rightarrow \hat{H}^{-1}(G, A) \rightarrow \hat{H}^{-1}(G, B) \\ &\rightarrow \hat{H}^{-1}(G, C) \rightarrow \hat{H}^0(G, A) \rightarrow \hat{H}^0(G, B) \rightarrow \hat{H}^0(G, C) \rightarrow \hat{H}^1(G, A) \\ &\rightarrow \hat{H}^1(G, B) \rightarrow \hat{H}^1(G, C) \rightarrow \hat{H}^2(G, A) \rightarrow \cdots . \end{aligned}$$

(8.52) Corollary (Dimension shifting). *Let $0 \rightarrow A \rightarrow B \rightarrow C \rightarrow 0$ be a $\mathbb{Z}G$ -exact sequence, in which B is G -induced. Then*

$$\hat{H}^i(G, C) \cong \hat{H}^{i+1}(G, A), i \in \mathbb{Z}.$$

In particular, let I_G be the augmentation ideal of $\mathbb{Z}G$, so there is an exact sequence of left $\mathbb{Z}G$ -modules given by (8.46). Then we obtain from (8.52)

$$\hat{H}^i(G, Z) \cong \hat{H}^{i+1}(G, I_G), i \in \mathbb{Z}.$$

Now every element of I_G is annihilated by N_G (see (8.41)), so we have by (8.48):

$$(8.53) \quad \hat{H}^{-1}(G, I_G) \cong I_G / I_G^2.$$

On the other hand, letting G' denote the commutator subgroup of G , there is an isomorphism

$$G/G' \cong I_G / I_G^2,$$

defined by sending xG' onto $x - 1 + I_G^2$, $x \in G$. Thus we have

$$(8.54) \quad \hat{H}^{-2}(G, Z) \cong \hat{H}^{-1}(G, I_G) \cong G/G'.$$

This result is of fundamental importance in the cohomological approach to class field theory.

As an illustration of the above techniques, we prove the following result, (Borevich-Faddeev [56], Gruenberg-Roggenkamp [75]) which is rather complicated to verify directly:

(8.55) Proposition. *The augmentation ideal I_G is a cyclic $\mathbb{Z}G$ -module if and only if G is a cyclic group.*

Proof. If $G = \langle x \rangle$ is cyclic, then clearly $I_G = \mathbb{Z}G \cdot (x - 1)$, so I_G has a single generator as $\mathbb{Z}G$ -module. Conversely, assume that I_G is a cyclic module; then there exists a $\mathbb{Z}G$ -exact sequence

$$0 \rightarrow A \rightarrow \mathbb{Z}G \rightarrow I_G \rightarrow 0.$$

Tensoring with \mathbb{Q} , we obtain

$$\mathbb{Q}G \cong \mathbb{Q}A \oplus \mathbb{Q}I_G.$$

On the other hand, tensoring (8.46) with \mathbb{Q} yields

$$\mathbb{Q}G \cong \mathbb{Q}I_G \oplus \mathbb{Q},$$

where G acts trivially on the second summand \mathbb{Q} . Therefore $\mathbb{Q}A \cong \mathbb{Q}$, which implies at once that $A \cong \mathbb{Z}$ (with trivial G -action). Hence the sequence

$$0 \rightarrow \mathbb{Z} \rightarrow \mathbb{Z}G \rightarrow I_G \rightarrow 0$$

is exact. Therefore by (8.52)

$$\hat{H}^{-1}(G, I_G) \cong \hat{H}^0(G, \mathbb{Z}).$$

But $\hat{H}^0(G, \mathbb{Z}) \cong \mathbb{Z}/n\mathbb{Z}$ by (8.42), where $n = |G|$. Combining this result with (8.54), we obtain

$$G/G' \cong \mathbb{Z}/n\mathbb{Z}.$$

But $|G| = n$, so this isomorphism implies first that $G' = 1$, and secondly that $G \cong \mathbb{Z}/n\mathbb{Z}$. We have thus shown that if I_G is a cyclic module, then G is a cyclic group. This completes the proof.

Remark. Let G be a group of order n , and define the ring

$$\mathbb{Z}' = \{a/b : a, b \in \mathbb{Z}, (b, n) = 1\},$$

so \mathbb{Z}' is a semi-localization of \mathbb{Z} ; the prime ideals of \mathbb{Z}' are of the form $m\mathbb{Z}'$, where $m \mid n$. If T is any f.g. \mathbb{Z} -module such that $nT = 0$, then we have

$$\mathbb{Z}' \otimes_{\mathbb{Z}} T \cong T.$$

Now \mathbb{Z}' is \mathbb{Z} -flat, since \mathbb{Z}' is a ring of quotients of \mathbb{Z} . Hence $\mathbb{Z}' \otimes_{\mathbb{Z}} \cdot$ preserves exactness, and we obtain an exact sequence

$$0 \rightarrow \mathbb{Z}' \otimes_{\mathbb{Z}} I_G \rightarrow \mathbb{Z}'G \rightarrow \mathbb{Z}' \rightarrow 0.$$

Here, $\mathbb{Z}' \otimes_{\mathbb{Z}} I_G$ is just the augmentation ideal of $\mathbb{Z}'G$. Further,

$$\mathbb{Z}'G = \mathbb{Z}G \otimes_{\mathbb{Z}} \mathbb{Z}',$$

so $\mathbb{Z}'G$ is G -induced. Thence we have, setting $I'_G = \mathbb{Z}' \otimes_{\mathbb{Z}} I_G$,

$$\hat{H}^i(G, \mathbb{Z}') \cong \hat{H}^{i+1}(G, I'_G).$$

In particular,

$$\hat{H}^{-2}(G, \mathbb{Z}') \cong \hat{H}^{-1}(G, I'_G) \cong I'_G / I_G \cdot I'_G.$$

But

$$I'_G / I_G \cdot I'_G \cong \mathbb{Z}' \otimes_{\mathbb{Z}} \{I_G / I_G^2\} \cong \mathbb{Z}' \otimes_{\mathbb{Z}} (G/G') \cong G/G',$$

since G/G' is annihilated by n (i.e., $(xG')^n = 1$ for each $x \in G$).

If G is cyclic, then of course I'_G is a cyclic module. The converse also holds:

If I'_G is a cyclic module, then G is a cyclic group.

Indeed, if I'_G is a cyclic module, then as in the proof of (8.55) we find that

$$\hat{H}^{-1}(G, I'_G) \cong \hat{H}^0(G, \mathbb{Z}') \cong \mathbb{Z}' / n\mathbb{Z}' \cong \mathbb{Z}/n\mathbb{Z}.$$

Thus we obtain $G/G' \cong \mathbb{Z}/n\mathbb{Z}$ as before, so G is cyclic of order n .

§8. Exercises

1. Let G be an arbitrary group, I_G the augmentation ideal of $\mathbb{Z}G$, and \mathbb{Z} the trivial G -module. Show that

$$H_1(G, \mathbb{Z}) \cong I_G / I_G^2 \cong G/G'.$$

[Hint: From (8.46) we obtain a long exact sequence

$$0 \rightarrow H_1(G, \mathbb{Z}) \rightarrow H_0(G, I_G) \rightarrow H_0(G, \mathbb{Z}G) \xrightarrow{\epsilon_*} H_0(G, \mathbb{Z}) \rightarrow 0.$$

Since ϵ_* is an isomorphism, we get $H_1(G, \mathbb{Z}) \cong H_0(G, I_G) \cong I_G / I_G^2$. The map $x \in G \rightarrow x - 1 \in I_G$, yields an isomorphism from the multiplicative group G/G' onto the additive group I_G / I_G^2 .]

2. Let R and S be Dedekind domains with quotient fields K and L , respectively, and suppose that

$$R \subseteq S, R = S \cap K.$$

Show that for each R -module M , the map $M \rightarrow S \otimes_R M$ (given by $m \mapsto 1 \otimes m$) is an R -monomorphism.

[Hint: The hypotheses imply that S/R is R -torsionfree, hence R -flat by Exercise 4.3. The R -exact sequence

$$0 \rightarrow R \rightarrow S \rightarrow S/R \rightarrow 0$$

yields an R -exact sequence

$$\text{Tor}_1^R(S/R, M) \rightarrow R \otimes_R M \rightarrow S \otimes_R M,$$

in which the first term is 0.]

Group Representations and Character Theory

In this chapter, we present the general properties of representations and characters of finite groups, with emphasis on the classical theory over fields of characteristic zero. Each section will focus on a particular method, and will contain applications of that method to a variety of problems. Parts of the chapter (§§9, 10, 11, 15) contain a more economical and, at times, more general account of much of the material in Chapters 5–7 of CR.

§9. ORTHOGONALITY RELATIONS AND CENTRAL IDEMPOTENTS

The orthogonality relations impose restrictions on the values of irreducible characters. These facts alone are sufficiently powerful to handle a surprisingly large number of applications. The account of the orthogonality relations in CR §31 follows closely the original work of Schur. The same is true for the treatment in Dornhoff [71] and Feit [67]. Our presentation below is based on the connection between irreducible characters of a split semisimple algebra and the central idempotents belonging to the Wedderburn components of the algebra which correspond to the irreducible characters. The extension of the results from group algebras to arbitrary semisimple algebras will be important in the discussion of Hecke algebras and centralizer rings (see §11D). The approach followed below was communicated to the authors by Robert Kilmoyer.

In §9A we review some facts about Frobenius and symmetric algebras. The main results relating characters and central idempotents are given in §9B, and are specialized to group characters in §9C. The remaining subsections deal with various applications of character theory, including in §9E a proof of Burnside's famous p^aq^b -Theorem.

§9A. Frobenius and Symmetric Algebras

In this subsection, A denotes a f.d. algebra over an arbitrary field K . Let $A^* = \text{Hom}_K(A, K)$, the space of K -linear maps from A to K .

(9.1) Definition. A bilinear form $\beta: A \times A \rightarrow K$ is called *associative* if $\beta(ab, c) = \beta(a, bc)$, $a, b, c \in A$, and *symmetric* if $\beta(a, b) = \beta(b, a)$ for all $a, b \in A$.

(9.2) Examples. (a) Let $\lambda: A \rightarrow K$ be an element of A^* . Then, letting

$$\beta(a, b) = \lambda(ab), \quad a, b \in A,$$

we obtain an associative bilinear form β .

(b) Let $A = KG$, the group algebra of a finite group G over the field K . We define

$$\beta(a, b) = \lambda(ab), \quad a, b \in A,$$

where $\lambda \in A^*$ is the map defined by

$$\lambda\left(\sum_{x \in G} \alpha_x x\right) = \alpha_1.$$

It is easily checked that, in this case, β is associative and symmetric.

(c) Let A be arbitrary, and define

$$\beta(a, b) = \text{Trace}(a_l b_l), \quad a, b \in A,$$

where $a_l \in \text{End}_K(A)$ is the left multiplication defined by $a_l: x \rightarrow ax$, $x \in A$. Then β is associative and symmetric. (Notice the similarity with the Killing form $\text{Trace}\{\text{ad } a\}(\text{ad } b)\}$ on a Lie algebra.)

In case an algebra A possesses an associative (and possibly symmetric) bilinear form which is nondegenerate, there are a number of connections between the form and the representation theory of A .

We leave it to the reader to check that the form given in (9.2b) is nondegenerate, for an arbitrary field K . The form given in (9.2c) is nondegenerate in case A is semisimple and K has characteristic zero. The proof goes as follows: The form is clearly nondegenerate for A/K if and only if it is nondegenerate for A^E/E , for an arbitrary extension field E of K . Since $\text{char } K = 0$, A is separable over K (see §7), and there exists an extension field E such that A^E is a split semisimple algebra over E , that is,

$$A^E \cong M_{n_1}(E) \oplus \cdots \oplus M_{n_s}(E),$$

a direct sum of total matrix algebras over E . The Wedderburn components $A_i \cong M_{n_i}(E)$ of A^E are orthogonal with respect to the form β ; hence β is nondegenerate if the form $\text{Tr}(a_l b_l)$ is nondegenerate on a total matrix algebra $M_n(E)$. In this case, the matrix of a_l with respect to a suitable basis is a direct

sum of n copies of the matrix a ; hence,

$$\mathrm{Tr}(a_I b_I) = \mathrm{Tr}((ab)_I) = n \mathrm{Tr}(ab), \text{ for } a, b \in M_n(E).$$

The latter form is easily shown to be nondegenerate on $M_n(E)$, whenever $n \neq 0$ in E .

The significance for representation theory of the existence of a nondegenerate form, as in (9.1), was first pointed out by Frobenius. Let A be a K -algebra, M an A -module, and let $M^* = \mathrm{Hom}_K(M, K)$. The correspondence $M \rightarrow M^*$ then defines a functor from right A -modules to left A -modules. Specifically, let M be a f.g. right A -module; then M^* becomes a *left* A -module once we define

$$(9.3) \quad (a\varphi)(m) = \varphi(ma), \quad a \in A, \varphi \in M^*, m \in M.$$

Indeed, M is a (K, A) -bimodule, and $\mathrm{Hom}_K(M, K)$ is a contravariant functor on M , so M^* becomes a left A -module by means of the right action of A on M . (See the discussion in §2A in this connection.)

In particular, the algebra A is itself an (A, A) -bimodule, and we may define the *left regular module* ${}_A A$ to be the module A on which the algebra A acts from the left. Likewise, the *right regular module* A_A is obtained by letting A act from the right. We may then form

$$(A_A)^* = \mathrm{Hom}_K(A_A, K),$$

a left A -module.

(9.4) Definition. A f.d. K -algebra A is a *Frobenius algebra* if the left A -modules ${}_A A$ and $(A_A)^*$ are isomorphic.

(9.5) Proposition. A f.d. K -algebra is a Frobenius algebra if and only if there exists a nondegenerate associative bilinear form $\beta: A \times A \rightarrow K$.

Proof. Suppose $\theta: {}_A A \rightarrow (A_A)^*$ is an isomorphism of left A -modules. Then $\theta(ab) = a\theta(b)$, and hence

$$\theta(ab)(c) = (a\theta(b))(c) = \theta(b)(ca) \quad \forall a, b, c \in A.$$

Define $\beta(a, b) = \theta(b)(a)$, $a, b \in A$. Then β is clearly bilinear, and is nondegenerate because θ is an isomorphism. To prove that β is associative, we have to compare $\beta(ab, c) = \theta(c)(ab)$ and $\beta(a, bc) = \theta(bc)(a)$; these are equal by the identity displayed above. Conversely, given such a form β , we can define θ as above. By reversing the argument, it is easy to show that θ is an A -isomorphism from ${}_A A$ to $(A_A)^*$.

A Frobenius algebra with a symmetric associative nondegenerate bilinear form β is called a *symmetric algebra*. Our previous discussion shows:

(9.6) Proposition. *Let G be a finite group, and K an arbitrary field. Then the group algebra KG is a symmetric K -algebra.*

Our earlier discussion also proves that f.d. semisimple algebras over fields of characteristic zero are symmetric algebras. However, for later use we need the fact that for every field K , whether or not $\text{char } K=0$, every f.d. semisimple K -algebra is a symmetric algebra. We begin with an obvious lemma:

(9.7) Lemma. *Let A be any f.d. K -algebra. Then A is a symmetric K -algebra if and only if there exists a K -linear map $\varphi: A \rightarrow K$ such that*

$$\varphi(ab) = \varphi(ba) \text{ for all } a, b \in A,$$

and such that φ does not annihilate any one-sided ideal of A .

Proof. Given such a φ , define $f: A \times A \rightarrow K$ by $f(a, b) = \varphi(ab)$ for $a, b \in A$. Then f has the desired properties. Conversely, given f , set $\varphi(a) = f(a, 1)$ for $a \in A$, and clearly φ behaves as required.

(9.8) Proposition (Eilenberg-Nakayama [55]). *Every f.d. semisimple K -algebra A is a symmetric K -algebra.*

Proof. It suffices to prove the result for each simple component of A , so (changing notation) we may assume that $A = M_n(D)$, where D is a division algebra over K . By Exercise 7.8, there exists a nonzero K -linear map $\theta: D \rightarrow K$ such that $\theta(\alpha\beta) = \theta(\beta\alpha)$ for all $\alpha, \beta \in D$. Now define $\varphi: A \rightarrow K$ by $\varphi(a) = \theta(\text{Trace } a)$, $a \in A$, where $\text{Trace}(a)$ is the usual trace of the matrix $a \in M_n(D)$. It is easily checked that φ has the properties described in (9.7). Indeed, if L is a nonzero left ideal of A , choose $a \in L$, $a \neq 0$, and write $a = (\alpha_{ij})$. Replacing a by xa for suitable $x \in A$, we may assume that for some i , $\alpha_{ii} \neq 0$ and all but the i -th row of a vanishes. But then L contains elements in which α_{ii} is arbitrary in D , so $\varphi(L) \supseteq \theta(D) = K$. This completes the proof.

For the rest of this subsection, let A be a f.d. K -algebra, and let $\beta: A \times A \rightarrow K$ be as in (9.5), so A is a Frobenius K -algebra. Let L denote an arbitrary left ideal of A , and

$$r(L) = \text{right annihilator of } L = \{x \in A : Lx = 0\},$$

$$L^\perp = \{x \in A : \beta(L, x) = 0\}.$$

Then $r(L)$ is clearly a right ideal of A , and $r(L) = L^\perp$ because for $x \in A$,

$$Lx = 0 \Leftrightarrow \beta(A, Lx) = 0 \Leftrightarrow \beta(AL, x) = 0 \Leftrightarrow \beta(L, x) = 0.$$

Similarly, for any right ideal R of A , define

$$I(R) = \text{left annihilator of } R = \{y \in A : yR = 0\},$$

$$R^\perp = \{y \in A : \beta(y, R) = 0\},$$

so $I(R)$ is a left ideal of A , and $I(R) = R^\perp$. Further, we have

$$(L^\perp)^\perp = L, (R^\perp)^\perp = R.$$

It follows at once that the correspondence $X \leftrightarrow Y$, given by $Y = X^\perp$, $X = Y^\perp$, is an inclusion-reversing bijection between the set of left ideals X of A contained in L , and the set of right ideals Y of A containing L^\perp . We thus obtain an inclusion-reversing bijection between the set of submodules of L and the set of submodules of A/L^\perp .

We apply these considerations to the case where $L = Ae$, with e an idempotent in A . Then for $x \in A$,

$$x \in L^\perp \Leftrightarrow Ae x = 0 \Leftrightarrow ex = 0 \Leftrightarrow x \in (1 - e)A,$$

so

$$(Ae)^\perp = (1 - e)A, A/(Ae)^\perp = (eA \oplus (1 - e)A)/(1 - e)A \cong eA.$$

We therefore obtain an inclusion-reversing bijection $X \leftrightarrow Y$ between the sets of submodules X of Ae and submodules Y of eA , given by

$$Y = \text{image of } X^\perp/(1 - e)A \text{ in } eA = eX^\perp.$$

We shall use this machinery to prove a basic result:

(9.9) Proposition. *Let A be a Frobenius K -algebra, and set $N = \text{rad } A$. Let*

$$r(N) = \{x \in A : Nx = 0\}, I(N) = \{y \in A : yN = 0\}.$$

Then

(i) $r(N) = I(N)$, and $r(N)$ is a two-sided ideal of A .

(ii) For each primitive idempotent $e \in A$, Ne is the unique maximal submodule of Ae , and $r(N)e$ is the unique minimal submodule of Ae . Therefore

$$r(N)e = \text{soc } Ae,$$

the socle of Ae (see §6D).

(iii) The algebra A is self-injective (=quasi-Frobenius), that is, the left regular module $_A A$ is injective (see §6D).

(iv) For each e as above, Ae is a projective cover of Ae/Ne , and is also an injective hull of $r(N)e$.

Proof. Since N is a two-sided ideal of A , so are its right and left annihilators $r(N)$ and $l(N)$. Let e be a primitive idempotent, so Ne is the unique maximal submodule of Ae , and the quotient Ae/Ne is a simple left A -module, by (6.9).

We choose $X=Ne$ in the discussion preceding (9.9). The corresponding Y equals eX^\perp , and is the unique minimal submodule of eA . Further, for $y \in A$, we have

$$y \in X^\perp \Leftrightarrow Ney = 0 \Leftrightarrow ey \in r(N),$$

which implies that $Y = e \cdot r(N)$. Thus, $e \cdot r(N)$ is the unique minimal submodule of eA .

Since N annihilates all simple A -modules, we obtain $(e \cdot r(N))N = 0$, and therefore $e \cdot r(N)N = 0$. Therefore $r(N)N$ is annihilated by every primitive idempotent $e \in A$. Since 1_A is expressible as a sum of such e 's, we conclude that $r(N)N = 0$, and therefore $r(N) \subseteq l(N)$. The reverse inclusion holds by symmetry, and (i) is established. The same argument (reversing left and right) also proves (ii).

We already know from §6C that Ae is a projective cover of Ae/Ne . By (2.27), to prove (iii) we need only show that every short exact sequence

$$(9.10) \quad 0 \rightarrow {}_A A \rightarrow V \rightarrow W \rightarrow 0,$$

in which V and W are f.g. left A -modules, is necessarily A -split. Let

$$V^* = \text{Hom}_K(V, K) = \text{dual of } V,$$

so V^* is a right A -module, and $(V^*)^* \cong V$. Since (9.10) is split over K (because K is a field), it follows that the sequence

$$(9.11) \quad 0 \rightarrow W^* \rightarrow V^* \rightarrow ({}_A A)^* \rightarrow 0$$

is also K -split, and is exact as sequence of right A -modules. But $({}_A A)^* \cong {}_A A$ by (9.4), so (9.11) is A -split. Taking duals of (9.11), we obtain an A -split exact sequence; but the sequence of duals of (9.11) is precisely the sequence (9.10), so (9.10) is A -split, as required. We have thus verified that every Frobenius algebra is a quasi-Frobenius ring.

(iv) Now let $e \in A$ be a primitive idempotent. Then Ae is a direct summand of the injective A -module ${}_A A$, and so Ae is an indecomposable injective module. To complete the proof of (iv), it suffices to show that Ae is an injective hull of each of its nonzero submodules M . Let E be any injective

hull of M , and consider the diagram

$$\begin{array}{ccccccc} & & 0 & \longrightarrow & M & \xrightarrow{j} & E \\ & & i \downarrow & & & & \theta \\ & & Ae & \xleftarrow{\quad} & & & \end{array}$$

in which i, j are inclusion maps. Then there exists a map θ making the diagram commute, since Ae is injective. Clearly $M \cap \ker \theta = 0$, and therefore $\ker \theta = 0$ because E is an injective hull of M . Thus we have an exact sequence

$$0 \rightarrow E \xrightarrow{\theta} Ae,$$

which must split since E is injective. Therefore $Ae \cong E$, so Ae is an injective hull of M , as claimed.

As remarked in (6.28), the assertions in (9.9) hold in the more general situation where A is any self-injective ring. However, the proof is somewhat more complicated, and we refer the reader to CR(58.12) for details.

Some additional information is available when A is not only a Frobenius algebra, but in fact a symmetric algebra. Let us prove:

(9.12) Proposition. *Let A be a symmetric K -algebra, and let e be any primitive idempotent of A . Then*

$$Ae/Ne \cong r(N)e,$$

that is, the socle of Ae is isomorphic to the unique simple factor module Ae/Ne of Ae .

Proof. Suppose that the bilinear form β is symmetric. We know by (9.9) that $r(N)e$ is the unique minimal submodule of Ae , and that $N \cdot r(N)e = 0$. Hence every $f \in \text{Hom}_A(Ae, r(N)e)$ induces a map $\tilde{f} \in \text{Hom}_A(Ae/Ne, r(N)e)$, and it suffices to find a nonzero f . Since there is an isomorphism of additive groups

$$\text{Hom}_A(Ae, r(N)e) \cong e \cdot r(N)e,$$

given by $f \mapsto f(e)$, we need only show that $e \cdot r(N)e \neq 0$.

Let us assume that $e \cdot r(N)e = 0$, and obtain a contradiction. We have, since β is symmetric and $r(N)$ is a left ideal of A ,

$$\begin{aligned} 0 &= \beta(1, e \cdot r(N)e) = \beta(e, r(N)e) = \beta(r(N)e, e) = \beta(r(N), e) \\ &= \beta(A \cdot r(N), e) = \beta(A, r(N)e). \end{aligned}$$

Therefore $r(N)e=0$, which is impossible. This completes the proof of the Proposition.

Since group algebras KG are always symmetric K -algebras, the results in (9.9) and (9.12) apply to the case where $A=KG$, with G any finite group. These results will be quite important in the study of modular representations.

§9B. Characters and Central Idempotents in Split Semisimple Algebras. Orthogonality Relations

In this section, A denotes a f.d. algebra over a field K . We shall be concerned mainly with the case where $\text{char } K=0$ and A is a split semisimple K -algebra (see Definition 3.35), but we shall not impose these restrictions until later.

Let M be a left A -module (always assumed f.d. over K in this subsection). The trace function $\mu: A \rightarrow K$ defined by

$$\mu(a) = \text{Trace}(a, M), \quad a \in A,$$

is called the *character* of A afforded by M . The *degree* of μ , denoted by $\deg \mu$, is defined as $\dim_K M$. Since μ is the trace map, we have

$$\deg \mu = \mu(1).$$

The fact that μ is a trace map has several important consequences:

(9.13) Proposition. (i) $\mu \in A^*$, where $A^* = \text{Hom}_K(A, K)$.

(ii) If M and M' are isomorphic left A -modules, with characters μ and μ' , respectively, then $\mu = \mu'$.

(iii) If $U_0 \supseteq U_1 \supseteq U_2 \supseteq \dots$ is a chain of A -submodules of a left A -module U_0 , and if $M_i = U_i / U_{i+1}$, $i=0, 1, \dots$ are the factor modules with characters μ_0, μ_1, \dots , respectively, then the character φ afforded by U_0 is given by

$$\varphi = \mu_0 + \mu_1 + \dots$$

Proof. (i) and (iii) are obvious, while (ii) holds because the trace is preserved under a similarity transformation.

The main theme of character theory is the study of left A -modules (which are complicated) in terms of their trace functions (which are less complicated).

Let $\{M_1, \dots, M_s\}$ be a basic set of simple left A -modules (see (3.36)), and let μ_i be the character of A afforded by M_i , $1 \leq i \leq s$. The characters $\{\mu_1, \dots, \mu_s\}$ are called a *basic set of irreducible characters* of A , and we use the notation

$$\text{Irr}(A) = \{\mu_1, \dots, \mu_s\}.$$

From (9.13ii), it follows that the irreducible characters $\{\mu_i\}$ are independent of the choice of representatives of the isomorphism classes of simple left A -modules.

From now on, we shall assume that A is a split semisimple K -algebra. The results of §3C apply whether or not $\text{char } K=0$, and we have:

(9.14) Proposition. *Let K be an arbitrary field, and let A be a split semisimple K -algebra. Then*

(i) *Each simple A -module M_i occurs in the left regular module ${}_A A$ with multiplicity equal to its K -dimension. Therefore the character ρ of the left regular module can be expressed in terms of the irreducible characters as follows:*

$$(9.15) \quad \rho = \sum_{i=1}^s (\deg \mu_i) \mu_i = \sum_{i=1}^s \mu_i(1) \mu_i.$$

(ii) *The irreducible characters $\{\mu_i\}$ are linearly independent over K .*

(iii) *Let $\{e_1, \dots, e_s\}$ be the central primitive idempotents in A . Then $\{e_1, \dots, e_s\}$ can be paired with the irreducible characters $\{\mu_i\}$ in such a way that e_i acts as the identity operator on M_i and annihilates $M_{i'}$, for $i' \neq i$. In terms of characters, $\mu_i(e_i) = \deg \mu_i$, and $\mu_i(e_{i'}) = 0$ if $i \neq i'$.*

(iv) *The idempotents $\{e_1, \dots, e_s\}$ form a K -basis for the center of A . In particular, e_i is, up to a scalar multiple, the only central element in the Wedderburn component Ae_i generated by e_i , for $1 \leq i \leq s$.*

Proof. (ii) follows from the Frobenius-Schur Theorem 3.41, while the other assertions are immediate from the results of §3C.

For the remainder of this subsection, we restrict our attention to the special case of greatest interest, where $\text{char } K=0$ and A is a split semisimple K -algebra. By (9.8), we know that A is a symmetric K -algebra, that is, there exists a nondegenerate symmetric associative bilinear form

$$\beta: A \times A \rightarrow K.$$

The main results of this subsection show how β can be used to express the central primitive idempotents $\{e_1, \dots, e_s\}$ explicitly in terms of the irreducible characters $\{\mu_i\}$ of A .

We first require the fact that, because β is nondegenerate, there exist K -bases $\{a_1, \dots, a_n\}$ and $\{b_1, \dots, b_n\}$ of A which are *dual** in the sense that

$$\beta(a_i, b_j) = \delta_{ij} \text{ (Kronecker delta).}$$

*See §4E.

(9.16) Example. Let KG be a split semisimple group algebra, and as in (9.2b), let β be the nondegenerate form defined by $\beta(a, b) = \lambda(ab)$ for $a, b \in KG$, where $\lambda \in (KG)^*$ is the linear map such that $\lambda\left(\sum_{x \in G} \alpha_x x\right) = \alpha_1$. If $G = \{x_1, \dots, x_n\}$, where $x_1 = 1$, then $\{x_1, \dots, x_n\}$ form a K -basis for KG , and it is easily checked that $\{x_1^{-1}, \dots, x_n^{-1}\}$ is the dual basis with respect to β .

(9.17) Proposition (Kilmoyer). Let A be a split semisimple K -algebra over a field of characteristic zero, and let $\{a_1, \dots, a_n\}$ and $\{b_1, \dots, b_n\}$ be dual bases of A with respect to a nondegenerate symmetric associative bilinear form $\beta: A \times A \rightarrow K$. Then the following statements hold:

(i) For each irreducible character $\mu_i \in \text{Irr}(A)$, let $d_i = \sum_{i=1}^n \mu_i(a_i)b_i$, $1 \leq i \leq s$. Then $\beta(d_i, a) = \mu_i(a)$, $a \in A$. Thus, the elements $\{d_i : 1 \leq i \leq s\}$ are defined independently of the choice of dual bases with respect to β .

(ii) We have $\mu_i(d_i) \neq 0$, and the central primitive idempotent e_i corresponding to M_i is given by

$$e_i = \mu_i(1)\mu_i(d_i)^{-1}d_i.$$

(iii) The element $\mu_i(d_i) \in K$ can be expressed as

$$\mu_i(d_i) = \sum_{j=1}^n \mu_i(a_j)\mu_i(b_j) = \mu_i(z)\mu_i(1)^{-1},$$

where $z = \sum_{j=1}^n a_j b_j$.

Proof. (i) Let $d_i = \sum_{j=1}^n \mu_i(a_j)b_j$. The fact that $\{a_j\}$ and $\{b_j\}$ are dual bases implies at once that

$$\beta(d_i, a_k) = \mu_i(a_k), \quad 1 \leq k \leq n.$$

Then by linearity we have $\beta(d_i, a) = \mu_i(a)$ for all $a \in A$. Hence each d_i is independent of the choice of dual bases, since β is nondegenerate. In other words, β identifies A with its dual space A^* , and the element of A corresponding to μ_i is precisely d_i .

(ii) Let Ae_i be the Wedderburn component of A corresponding to the central primitive idempotent e_i . Then for $i \neq j$,

$$\beta(Ae_i, Ae_j) = \beta(A, e_i Ae_j) = 0.$$

Therefore for each i , the restriction $\beta|_{Ae_i}$ is nondegenerate. Since $\mu_i(Ae_j) = 0$, we obtain

$$\beta(d_i e_j, Ae_j) = \beta(d_i, Ae_j) = \mu_i(Ae_j) = 0;$$

hence $d_i e_j = 0$ since $\beta|_{Ae_i}$ is nondegenerate. Since $1 = \sum e_k$, we obtain

$$d_i = d_i e_i + \sum_{j \neq i} d_i e_j = d_i e_i \in Ae_i, \quad 1 \leq i \leq s.$$

We prove next that d_i is central in A . For each $x, y \in A$ we have

$$\begin{aligned} \beta(xd_i, y) &= \beta(y, xd_i) = \beta(yx, d_i) = \mu_i(yx) \\ &= \mu_i(xy) = \beta(d_i, xy) = \beta(d_i x, y), \end{aligned}$$

using (i), the properties of β , and the fact that μ_i is a trace function (so that $\mu_i(xy) = \mu_i(yx)$). Therefore, by the nondegeneracy of β , $xd_i = d_i x$ for all $x \in A$; thus d_i is central in A , and hence central in the Wedderburn component Ae_i to which it belongs. Moreover, $d_i \neq 0$ by (i). Since the center of Ae_i is one-dimensional, we have

$$e_i = \xi d_i, \text{ for some } \xi \in K.$$

Then, applying e_i to M_i and taking the trace, we have

$$\mu_i(1) = \mu_i(e_i) = \xi \mu_i(d_i).$$

But $\mu_i(1) \neq 0$ because K has characteristic zero, so $\mu_i(d_i) \neq 0$, as claimed, and $\xi = \mu_i(1)\mu_i(d_i)^{-1}$; this gives the formula for e_i , and completes the proof of (ii).

(iii) Consider the element $z = \sum a_i b_i$, and let ρ be the character of A afforded by the left regular module. For $a \in A$, we put

$$aa_j = \sum_{k=1}^n \gamma_{kj}(a)a_k, \quad \gamma_{kj}(a) \in K, \quad 1 \leq j \leq n.$$

Then $\gamma_{jj}(a) = \beta(aa_j, b_j) = \beta(a, a_j b_j)$; summing over j , we have

$$(9.18) \quad \rho(a) = \sum_{j=1}^n \gamma_{jj}(a) = \beta(a, z), \quad a \in A.$$

From (9.15), we have $\rho = \sum \mu_i(1)\mu_i$. Therefore

$$\rho(d_i) = \sum_{j=1}^s \mu_j(1)\mu_j(d_i) = \mu_i(1)\mu_i(d_i)$$

since $\mu_j(Ae_i) = 0$ whenever $i \neq j$. Then by (i) and (9.18), we obtain

$$\mu_i(z) = \beta(d_i, z) = \rho(d_i) = \mu_i(1)\mu_i(d_i),$$

which establishes (iii), and completes the proof of the proposition.

(9.19) Proposition (Orthogonality Relations). *Keep the notation of (9.17), and let $z = \sum_{i=1}^n a_i b_i$. Let μ and μ' be irreducible characters of A . Then*

$$\sum_{j=1}^n \mu(a_j) \mu'(b_j) = \begin{cases} \mu(1)^{-1} \mu(z) & \text{if } \mu = \mu', \\ 0 & \text{if } \mu \neq \mu'. \end{cases}$$

Proof. The result when $\mu = \mu'$ follows from (9.17iii). On the other hand, if $\mu \neq \mu'$ then

$$\sum_j \mu(a_j) \mu'(b_j) = \mu' \left(\sum_j \mu(a_j) b_j \right) = 0$$

because, by (9.17ii), $\sum_j \mu(a_j) b_j$ is a multiple of the central primitive idempotent corresponding to μ .

§9C. Orthogonality Relations for Characters of Finite Groups

Throughout this subsection, G denotes a finite group, and K a field of characteristic 0. We shall be interested mainly in the case where KG is a split semisimple K -algebra, but we shall not impose these restrictions until later.

As in §9B, let $\mu: KG \rightarrow K$ be the character afforded by a left KG -module M . Then, by definition,

$$\mu(a) = \text{Trace}(a, M), a \in KG.$$

Restricting μ to the elements of G , we obtain a function $\mu: G \rightarrow K$, given by

$$\mu(x) = \text{Trace}(x, M), x \in G.$$

Since the elements of G form a K -basis for KG , the trace function $\mu: KG \rightarrow K$ can be recovered from the values $\{\mu(x): x \in G\}$, by means of the formula

$$\mu \left(\sum_{x \in G} \alpha_x x \right) = \sum_{x \in G} \alpha_x \mu(x), \alpha_x \in K.$$

The characters afforded by KG -modules, viewed as K -valued functions on G , will be called K -characters of G ; we shall use the same notation for both a K -character of G and its extension to KG .

In particular, the *irreducible K-characters* of G are given by

$$\text{Irr}_K(G) = \{\xi^{(1)}, \dots, \xi^{(s)}\},$$

where $\xi^{(i)}$ is the character afforded by Z_i , and $\{Z_1, \dots, Z_s\}$ are a basic set of simple left KG -modules. Let us show at once that every K -character μ of G can be uniquely expressed as a linear combination

$$\mu = a_1 \xi^{(1)} + \dots + a_s \xi^{(s)},$$

with non-negative integer coefficients $\{a_i\}$. In fact, suppose that μ is afforded by the KG -module M , and let M have composition factors Z_1 with multiplicity a_1, \dots, Z_s with multiplicity a_s . From (9.13iii), we obtain the desired formula for μ in terms of the ξ 's.

The uniqueness of the coefficients $\{a_i\}$ above is a direct consequence of the following assertion:

(9.20) Proposition. *Let*

$$\text{Irr}_K(G) = \{\xi^{(1)}, \dots, \xi^{(s)}\}$$

be a basic set of irreducible K -characters of G . Then $\{\xi^{(1)}, \dots, \xi^{(s)}\}$ are linearly independent over K .

Proof. We shall establish the result in the situation where $\text{char } K=0$. The result also holds when $\text{char } K \neq 0$, and is proved for that case in (17.3).

Suppose now that $\text{char } K=0$, and let E be an algebraic closure of K . Then EG is a semisimple E -algebra by Maschke's Theorem 3.14, and is a split semisimple E -algebra by §3C. Let $\{W_1, \dots, W_l\}$ be a basic set of simple left EG -modules, and let ω_j be the character of G afforded by W_j , $1 \leq j \leq l$. By the Frobenius-Schur Theorem 3.41, the characters $\{\omega_1, \dots, \omega_l\}$ are linearly independent over E .

Now let

$$Z_i^E = E \otimes_K Z_i, \quad 1 \leq i \leq s.$$

Clearly Z_i^E also affords the same character $\xi^{(i)}$ of G as does Z_i . On the other hand, each module Z_i^E is expressible as a direct sum of copies of the W 's, and no W occurs as a summand of both Z_i^E and Z_k^E if $i \neq k$, by Exercise 2.7. It follows that for each i , we can express $\xi^{(i)}$ as an integral linear combination of the ω 's, and that a given ω_j cannot occur in both $\xi^{(i)}$ and $\xi^{(k)}$ for $i \neq k$. Since the ω 's are linearly independent over E , the same must also hold for the ξ 's. Therefore $\{\xi^{(1)}, \dots, \xi^{(s)}\}$ are linearly independent over K , and the proposition is established.

The above discussion shows the importance of considering integral linear combinations $\sum a_i \xi^{(i)}$ of the irreducible K -characters $\{\xi^{(i)}\}$ of G . As we shall see later, it is extremely useful to extend this idea to the case where the $\{a_i\}$ are arbitrary rational integers, not necessarily positive. This significant step was taken by Brauer, in his work on the application of representation theory to the study of Artin L -functions. Let us set

$$\text{ch } KG = \mathbb{Z}\xi^{(1)} \oplus \cdots \oplus \mathbb{Z}\xi^{(s)} = \left\{ \sum_{i=1}^s a_i \xi^{(i)} : a_i \in \mathbb{Z} \right\}.$$

We shall call the elements of $\text{ch } KG$ *virtual K -characters* of G ; Brauer referred to them as *generalized characters* of G .

We also put

$$\text{ch}^+ KG = \left\{ \sum a_i \xi^{(i)} : a_i \in \mathbb{Z}, a_i \geq 0 \right\},$$

and call the elements of $\text{ch}^+ KG$ *ordinary characters*.

It should be pointed out that, by virtue of (9.20), the sum $\sum \mathbb{Z}\xi^{(i)}$ is a direct sum. Furthermore, $\text{ch } KG$ has the structure of a commutative ring with unit. Indeed, let M and N be KG -modules affording the characters μ and ν , respectively. We may form the KG -module $M \otimes_K N$, on which G acts by the rule

$$x(m \otimes n) = xm \otimes xn, \quad x \in G, m \in M, n \in N.$$

We extend the action from G to KG by linearity. Then the KG -module $M \otimes_K N$ affords the character $\mu\nu$, whose value at each $x \in G$ is $\mu(x)\nu(x)$. (See §10 for further discussion of tensor products of modules.)

In particular, for i and j between 1 and s , the KG -module $Z_i \otimes_K Z_j$ affords the character $\xi^{(i)}\xi^{(j)}$, where this product is viewed as a product of K -valued functions on G . Thus

$$(\xi^{(i)}\xi^{(j)})(x) = \xi^{(i)}(x)\xi^{(j)}(x) \text{ for } x \in G.$$

We caution the reader that this formula does *not* hold for elements of KG , and in fact we have

$$(\xi^{(i)}\xi^{(j)}) \left(\sum_{x \in G} \alpha_x x \right) = \sum_{x \in G} \alpha_x \xi^{(i)}(x)\xi^{(j)}(x)$$

for constants $\{\alpha_x\}$ from K .

The ring structure of $\text{ch } KG$ is now defined by using this multiplication $\xi^{(i)}\xi^{(j)}$ for the irreducible K -characters of G . The unit element of $\text{ch } KG$ is the

trivial character* $\xi^{(1)}$, where

$$\xi^{(1)}(x) = 1 \text{ for all } x \in G.$$

This character is afforded by the *trivial representation* of G , which maps each $x \in G$ onto 1; the underlying KG -module is the field K itself, on which G acts trivially.

We shall call $\text{ch } KG$ the *ring of virtual K -characters* of G . Clearly, $\text{ch } KG$ is a commutative associative ring with unit. It should be emphasized that multiplication in $\text{ch } KG$ has been defined by first defining multiplication in $\text{ch}^+ KG$, and then extending the definition by linearity. Multiplication of characters in $\text{ch}^+ KG$ corresponds to forming tensor products of KG -modules, as described above.

Besides the properties of characters described in §9B, the K -characters of G have the important property that they belong to the K -vector space of *class functions* on G . The vector space of class functions will be denoted by $\text{cf}_K(G)$, and consists of all functions constant on conjugacy classes. Thus

$$\text{cf}_K(G) = \{ \varphi : G \rightarrow K : \varphi(xy^{-1}) = \varphi(y), x, y \in G \}.$$

Let us prove that each K -character μ belongs to $\text{cf}_K(G)$. Relative to some K -basis, the module M affords a matrix representation $\mathbf{M} : G \rightarrow GL_n(K)$, where $n = \dim_K M$. We have $\mu(x) = \text{Trace } \mathbf{M}(x)$, $x \in G$. Since \mathbf{M} is a homomorphism, we have

$$\mathbf{M}(xyx^{-1}) = \mathbf{M}(x)\mathbf{M}(y)\mathbf{M}(x)^{-1}, \quad x, y \in G.$$

Taking traces, we obtain

$$\mu(xyx^{-1}) = \text{Trace}\{\mathbf{M}(x)\mathbf{M}(y)\mathbf{M}(x)^{-1}\} = \text{Trace } \mathbf{M}(y) = \mu(y),$$

so $\mu \in \text{cf}_K(G)$ as claimed.

(9.21) Proposition. *Let KG be a split semisimple K -algebra, where $\text{char } K = 0$.*

(i) *Let ξ and ξ' be irreducible K -characters of G . Then*

$$|G|^{-1} \sum_{x \in G} \xi(x)\xi'(x^{-1}) = \begin{cases} 0 & \text{if } \xi \neq \xi', \\ 1 & \text{if } \xi = \xi'. \end{cases}$$

(ii) *The central primitive idempotent e corresponding to ξ is given by*

$$e = \xi(1)|G|^{-1} \sum_{x \in G} \xi(x^{-1})x.$$

*The trivial character is sometimes called the *principal character*.

Proof. Both results are immediate from Propositions 9.17 and 9.19, using the dual basis of KG given in Example 9.16; in this situation, the element $z = \sum a_i b_i$ becomes $|G| \cdot 1$.

Remark. Other proofs of (9.21i), independent of the Wedderburn theorems and based instead on Schur's Lemma, are given in CR §31 and in the exercises at the end of this section.

We have shown that the irreducible K -characters $\{\xi^{(1)}, \dots, \xi^{(s)}\}$ belong to the space of class functions $\text{cf}_K(G)$, and are linearly independent (by the Frobenius-Schur Theorem 3.41). Moreover, in Theorem 3.37, it was proved that s is equal to the number of conjugacy classes in G . It follows that $\{\xi^{(1)}, \dots, \xi^{(s)}\}$ is a K -basis of $\text{cf}_K(G)$. This result is put in a more precise and useful form in the next part of our discussion.

In order to better understand the orthogonality formulas in (9.21), it will be useful to interpret them in terms of a hermitian scalar product on the space of complex-valued functions on G . Suppose to begin with that KG is a split semisimple K -algebra, where $\text{char } K=0$. We shall show how to identify $\text{Irr}_K G$ with $\text{Irr}_C G$, where C is the complex field.

Let L be a field which is a composite of K and C . Then K , C and L are splitting fields for G . Moreover, basic sets of simple KG -modules and simple CG -modules yield isomorphic basic sets of simple LG -modules. Such field extensions do not affect the characters viewed as class functions on G , and we may therefore identify* $\text{Irr}_K G$ with $\text{Irr}_C G$. This shows that the character theory of G over any splitting field of characteristic 0 is identical with the character theory of G over C .

For the rest of the subsection, we assume that K is a subfield of C , such that KG is a split semisimple K -algebra. As shown in §7B, there exist such fields K for which $\dim_Q K$ is finite. On the other hand, we can choose $K=C$ if desired.

We now introduce a hermitian scalar product on the space of all complex-valued functions on G , by setting

$$(9.22) \quad (\varphi, \psi)_G = |G|^{-1} \sum_{x \in G} \varphi(x) \overline{\psi(x)}, \quad \|\varphi\|^2 = (\varphi, \varphi)_G,$$

for arbitrary functions $\varphi, \psi: G \rightarrow K$, where $\overline{\psi(x)}$ denotes the complex conjugate of $\psi(x)$. We shall often write (φ, ψ) instead of $(\varphi, \psi)_G$ when it is clear from the context that G is the group under consideration.

We next observe that if $\mu: G \rightarrow K$ is a K -character of G , then

$$\mu(x^{-1}) = \overline{\mu(x)},$$

*This identification is made with respect to fixed embeddings of K and C in L .

for the following reason. Let $\{\varepsilon_1, \dots, \varepsilon_n\}$ denote the eigenvalues of $\mathbf{M}(x)$, where $\mathbf{M}: G \rightarrow GL_n(K)$ is a matrix representation affording μ , and $n = \deg \mu$. Then the $\{\varepsilon_i\}$ are roots of unity because \mathbf{M} is a homomorphism of the finite group G . Moreover,

$$\mu(x) = \varepsilon_1 + \cdots + \varepsilon_n,$$

and hence

$$\mu(x^{-1}) = \varepsilon_1^{-1} + \cdots + \varepsilon_n^{-1} = \overline{\varepsilon_1} + \cdots + \overline{\varepsilon_n} = \overline{\mu(x)}.$$

We combine these observations as follows:

(9.23) Proposition. *Let K be a subfield of the complex field such that KG is split semisimple. Then*

(i) *The irreducible K -characters $\{\xi^{(1)}, \dots, \xi^{(s)}\}$ form an orthonormal basis in the vector space $cf_K(G)$ of class functions, with respect to the hermitian scalar product (9.22). In particular, for $1 \leq i, j \leq s$,*

$$(\xi^{(i)}, \xi^{(j)})_G = \delta_{ij} \text{ (Kronecker delta).}$$

(ii) *Each class function $\varphi \in cf_K(G)$ is a K -linear combination of the irreducible K -characters,*

$$\varphi = \sum a_i \xi^{(i)}, a_i \in K,$$

where the coefficients $\{a_i\}$ are given by $a_i = (\varphi, \xi^{(i)})$, $1 \leq i \leq s$.

The proof is immediate from Proposition 9.21 and the preceding remarks, and is left as an exercise.

Remark. Proposition 9.23 can be viewed as the foundation for what might be called “Fourier analysis” in the space of class functions on the finite group G . Here, $\varphi = \sum a_i \xi^{(i)}$ is the Fourier series of $\varphi \in cf_K(G)$, and $\{a_i : 1 \leq i \leq s\}$ the Fourier coefficients of φ ; by (9.23), these coefficients are expressed as the scalar products $(\varphi, \xi^{(i)})$, $1 \leq i \leq s$.

Let M be a KG -module. We shall write

$$M \cong \coprod Z_i^{(a_i)}$$

to indicate that M is isomorphic to the direct sum of a_1 copies of Z_1 , a_2 copies of Z_2 , etc. The nonnegative integer a_i is called the *multiplicity* of Z_i in M . The multiplicities $\{a_i\}$ are uniquely determined by the Jordan-Hölder Theorem. The next result shows that they can be expressed in terms of the scalar product of characters.

(9.24) Proposition. (i) A class function μ is a K -character if and only if $\mu \neq 0$, and $(\mu, \zeta^{(i)})$ is a nonnegative integer for $1 \leq i \leq s$. If M is a left KG -module affording μ , then $(\mu, \zeta^{(i)})$ is the multiplicity of Z_i in M , for $1 \leq i \leq s$.

(ii) Let $\mu = \sum a_i \zeta^{(i)}$, $a_i \in \mathbb{C}$. Then

$$\|\mu\|^2 = (\mu, \mu) = \sum |a_i|^2.$$

In particular, if μ is a K -character (so that each a_i is a nonnegative integer), then μ is irreducible if and only if $(\mu, \mu) = 1$.

(iii) Let $\mu = \sum a_i \zeta^{(i)}$ be a K -character afforded by a left KG -module M . Then the multiplicities $\{a_i\}$ satisfy

$$a_i = \dim_K(\text{Hom}_{KG}(Z_i, M)), \quad 1 \leq i \leq s.$$

More generally, if M affords the K -character μ , and M' affords μ' , then

$$\dim_K(\text{Hom}_{KG}(M, M')) = (\mu, \mu')_G.$$

(Because of this formula, $(\mu, \mu')_G$ is sometimes called the intertwining number of μ and μ' .)

(iv) A class function μ is a virtual K -character (that is, $\mu \in \text{ch } KG$) if and only if each $(\mu, \zeta^{(i)}) \in \mathbb{Z}$.

Proof. (i) Suppose μ is a K -character afforded by a left KG -module M , and let $M \cong \coprod Z_i^{(a_i)}$. Then $\mu = \sum a_i \zeta^{(i)}$ by (9.13iii). Moreover, $\mu(1) = \dim_K(M) \neq 0$. Conversely, if $\mu = \sum a_i \zeta^{(i)}$, with each $a_i \in \mathbb{Z}$, $a_i \geq 0$, then μ is the K -character afforded by $\coprod Z_i^{(a_i)}$.

(ii) is immediate from (i) and Proposition 9.13ii.

(iii) Let $M \cong \coprod Z_j^{(a_j)}$, so that $\mu = \sum a_j \zeta^{(j)}$ as in (i). Then from (2.7),

$$\text{Hom}_{KG}(Z_i, M) \cong \bigoplus_j \{\text{Hom}_{KG}(Z_i, Z_j)\}^{(a_j)}.$$

Moreover, by Schur's Lemma 3.17 and the fact that KG is a split semisimple K -algebra, we have

$$\dim_K(\text{Hom}_{KG}(Z_i, Z_j)) = \delta_{ij}.$$

Therefore

$$\dim_K(\text{Hom}_{KG}(Z_i, M)) = a_i,$$

from which (iii) follows. Finally, (iv) follows from (9.23ii), and the proof is completed.

We introduce next a detailed list of notation, fixed once and for all for a given finite group G , which we shall use in a finer analysis of the orthogonality relations and their consequences.

(9.25) Definition. The *character table data* of G consists of the following information:

$\{Z_1 = K, Z_2, \dots, Z_s\}$ = basic set of simple KG -modules.*

$\{\zeta^{(1)} = 1_G, \zeta^{(2)}, \dots, \zeta^{(s)}\}$ = irreducible K -characters.

$\{z_i = \zeta^{(i)}(1), 1 \leq i \leq s\}$ = degrees of the irreducible K -characters

$\{\mathfrak{C}_1 = \{1\}, \mathfrak{C}_2, \dots, \mathfrak{C}_s\}$ = conjugacy classes in G , with

$$C_i = \sum_{x \in \mathfrak{C}_i} x, \quad 1 \leq i \leq s, \text{ the class sums (see (3.37a)).}$$

$$h_i = |\mathfrak{C}_i| = |G : C_G(x_i)|, \text{ for } x_i \in \mathfrak{C}_i, \quad 1 \leq i \leq s.$$

$$\zeta_j^{(i)} = \zeta^{(i)}(x), \text{ for } x \in \mathfrak{C}_j,$$

$$\zeta_{j*}^{(i)} = \zeta^{(i)}(x^{-1}), \quad x \in \mathfrak{C}_j.$$

The *character table* of G is the $s \times s$ matrix $\mathbf{Z} = (\zeta_j^{(i)})$ whose rows are indexed by the irreducible characters $\{\zeta^{(1)}, \dots, \zeta^{(s)}\}$, and columns by the conjugacy classes $\mathfrak{C}_1, \dots, \mathfrak{C}_s$; this matrix can be displayed in the form

$$\mathbf{Z} = \begin{array}{c|cccccc} & \mathfrak{C}_1 & \cdots & \mathfrak{C}_j & \cdots & \mathfrak{C}_s \\ \hline \zeta^{(1)} & & & \vdots & & \\ \vdots & & & \vdots & & \\ \zeta^{(i)} & \dots & \dots & \zeta_j^{(i)} & \dots & \\ \vdots & & & \vdots & & \\ \zeta^{(s)} & & & \vdots & & \end{array}$$

In terms of the data assembled in (9.25), we have

(9.26) Proposition (First and Second Orthogonality Relations).

$$(i) \quad \sum_{i=1}^s h_i \zeta_i^{(m)} \zeta_i^{(n)} = \delta_{mn} |G|.$$

$$(ii) \quad \sum_{m=1}^s \zeta_i^{(m)} \zeta_j^{(m)} = \delta_{ij} |C_G(x_i)|, \quad x_i \in \mathfrak{C}_i.$$

*Here, Z_1 is just the field K on which each $x \in G$ acts trivially.



Proof. The First Orthogonality Relation (i) is simply a restatement of Proposition (9.21i), using the facts that the characters are class functions. To derive the Second Orthogonality Relation, let $\mathbf{Z}=(\zeta^{(i)})$ be the character table, and let \mathbf{Y} be the $s \times s$ matrix whose (i, j) entry is $y_{ij} = h_i \zeta_j^{(j)}$. Then (i) implies that

$$\mathbf{ZY} = |G| \mathbf{I}_s,$$

where \mathbf{I}_s is the s -rowed identity matrix. It follows from linear algebra that

$$\mathbf{YZ} = |G| \mathbf{I}_s.$$

Using the entries of \mathbf{Z} and \mathbf{Y} , we obtain

$$\sum_{m=1}^s h_i \zeta_i^{(m)} \zeta_j^{(m)} = \delta_{ij} |G|.$$

Therefore

$$\sum_{m=1}^s \zeta_i^{(m)} \zeta_j^{(m)} = \delta_{ij} |G| h_i^{-1} = \delta_{ij} |C_G(x_i)|, \quad x_i \in \mathfrak{C}_i,$$

as required.

§9D. The Character Table

In this section we indicate how information about the structure of a finite group G may be deduced from its character table $\mathbf{Z}=(\zeta^{(i)})$ defined in (9.25).

First, we consider how normal subgroups of G may be identified from a knowledge of the characters of G . Let K be a splitting field contained in \mathbb{C} , as in §9C. Let μ be a K -character of G afforded by a representation $\mathbf{M}: G \rightarrow GL_d(K)$, where $d = \mu(1)$. Let $\{\epsilon_1(x), \dots, \epsilon_d(x)\}$ be the eigenvalues of $\mathbf{M}(x)$, for $x \in G$. Then the $\{\epsilon_i(x)\}$ are roots of unity, so $|\epsilon_i(x)| = 1$ for each i , $1 \leq i \leq d$. By the triangle inequality we have

$$|\mu(x)| = |\epsilon_1(x) + \dots + \epsilon_d(x)| \leq d,$$

with equality if and only if $\epsilon_1(x) = \dots = \epsilon_d(x)$. In the latter case, because $\min. \text{pol.}_K(\mathbf{M}(x))$ divides $X^{|G|} - 1$, and hence has no repeated factors, it follows that $\mathbf{M}(x) = \epsilon_1(x) \mathbf{I}_d$. The preceding remarks yield at once:

(9.27) Proposition. *Let μ be a K -character of G , afforded by a representation $\mathbf{M}: G \rightarrow GL_d(K)$. Then $|\mu(x)| \leq \mu(1)$ for all $x \in G$. The set $\{x \in G : |\mu(x)| = \mu(1)\}$ is a normal subgroup of G , and coincides with the set $\{x \in G : \mathbf{M}(x) \in K \cdot \mathbf{I}_d\}$. The kernel of the homomorphism $\mathbf{M}: G \rightarrow GL_d(K)$ is given by*

$$\ker \mathbf{M} = \{x \in G : \mu(x) = \mu(1)\}.$$

For a K -character μ , we define the *kernel* of μ (notation: $\ker \mu$) to be the kernel of a representation of G affording μ . Thus $\ker \mu$ is a normal subgroup of G , and (9.27) can be used to find the kernels of the irreducible characters. Another consequence is that the index $|G: G'|$ of the derived group G' in G is equal to the number of irreducible K -characters of G of degree 1. (For further details, see the exercises.)

Next we consider the multiplication of class sums. Recalling that the class sums $C_i = \sum_{x \in \mathfrak{C}_i} x$ form a K -basis for the center of KG , we have

$$(9.28) \quad C_i C_j = \sum c_{ijk} C_k,$$

with structure constants $c_{ijk} \in K$. Upon closer examination, we see that the $\{c_{ijk}\}$ are nonnegative integers, and in fact

$$c_{ijk} = \text{card } X_{ijk},$$

where

$$X_{ijk} = \{(x, y) \in G \times G : x \in \mathfrak{C}_i, y \in \mathfrak{C}_j, xy = z \in \mathfrak{C}_k, \text{ for a fixed element } z \in \mathfrak{C}_k\}$$

Now let $\{Z_m\}$ be the irreducible K -representations as in (9.25). Then $Z_m(C_i)$ is in the centralizer of the left KG -module Z_m , and since Z_m is absolutely simple, we have by (3.43):

$$Z_m(C_i) = \omega_i^{(m)} \mathbf{I}, \quad 1 \leq i \leq s, \quad 1 \leq m \leq s,$$

for some $\omega_i^{(m)} \in K$. Taking traces in this formula, we obtain

$$h_i \zeta_i^{(m)} = \omega_i^{(m)} z_m,$$

and hence

$$(9.29) \quad \omega_i^{(m)} = \frac{h_i \zeta_i^{(m)}}{z_m}, \quad 1 \leq i, m \leq s.$$

Applying Z_m to the formula (9.28), we have

$$(9.30) \quad \omega_i^{(m)} \omega_j^{(m)} = \sum_{k=1}^s c_{ijk} \omega_k^{(m)}, \quad 1 \leq m \leq s.$$

It follows that the system of s linear homogeneous equations, with coefficient matrix $(\delta_{jk} \omega_i^{(m)} - c_{ijk})_{1 \leq j, k \leq s}$, has a nontrivial solution $\{\omega_k^{(m)} : 1 \leq k \leq s\}$, since for fixed m at least one of these $\{\omega_k^{(m)}\}$ is nonzero. Therefore $\det(\delta_{jk} \omega_i^{(m)} - c_{ijk}) = 0$, so the elements $\{\omega_i^{(m)}\}$ are eigenvalues of the $s \times s$ matrix $(c_{ijk})_{1 \leq j, k \leq s}$. But the characteristic polynomial of this matrix is a

monic polynomial in $\mathbf{Z}[x]$, because the structure constants $\{c_{ijk}\}$ are integers. Using §1A, we obtain the following important result, which gives the first connection between character theory and the arithmetic structure of the field K :

(9.31) Proposition. *The elements $\omega_i^{(m)} \in \text{alg. int.}\{K\}$ for $1 \leq i, m \leq s$.*

An immediate consequence of (9.31) is the following important result about the degrees $\{z_m\}$ of the irreducible characters $\{\xi_j^{(m)}\}$:

(9.32) Proposition. *The degree z_m divides $|G|$, for $1 \leq m \leq s$.*

Proof. We have

$$\mathbf{Q} \cap \text{alg. int.}\{K\} = \mathbf{Z},$$

since \mathbf{Z} is integrally closed. It therefore suffices to prove that $|G|/z_m \in \text{alg. int.}\{K\}$ for each m . Let $n = |G|$; then for each j , $1 \leq j \leq s$, the character value $\xi_j^{(m)}$ is a sum of n -th roots of 1, hence is an algebraic integer. But $\xi_j^{(m)}$ lies in K , so $\xi_j^{(m)} \in \text{alg. int.}\{K\}$. Using (9.31), we obtain

$$\sum_{j=1}^s \omega_j^{(m)} \xi_j^{(m)} \in \text{alg. int.}\{K\}.$$

But by (9.29) and the First Orthogonality Relation (9.26i), we have

$$\sum_j \omega_j^{(m)} \xi_{j*}^{(m)} = z_m^{-1} \sum_j h_j \xi_j^{(m)} \xi_{j*}^{(m)} = |G|/z_m.$$

Therefore $|G|/z_m \in \text{alg. int.}\{K\}$ as claimed, and the result is proved.

Remark. See (11.32iv) for a much sharper result about the degrees $\{z_m\}$.

We next show that the structure constants $\{c_{ijk}\}$ in (9.28) can be recovered from the character table:

(9.33) Proposition. *We have for $1 \leq i, j, k \leq s$,*

$$c_{ijk} = \frac{h_i h_j}{|G|} \sum_{m=1}^s \frac{\xi_i^{(m)} \xi_j^{(m)} \xi_{k*}^{(m)}}{z_m}.$$

Proof. From (9.29) and (9.30), we have

$$h_i h_j \xi_i^{(m)} \xi_j^{(m)} = z_m \sum_{k=1}^s c_{ijk} h_k \xi_k^{(m)}.$$

Now multiply this formula by $\xi_{l^*}^{(m)}/z_m$, and sum over m . The Second Orthogonality Relation implies that

$$\begin{aligned} z_m^{-1} h_i h_j \sum_{m=1}^s \xi_i^{(m)} \xi_j^{(m)} \xi_{l^*}^{(m)} &= \sum_{k=1}^s c_{ijk} h_k \sum_{m=1}^s \xi_k^{(m)} \xi_{l^*}^{(m)} \\ &= c_{ijk} |G| / h_l \end{aligned}$$

which gives the desired formula for c_{ijk} . We remark again that each integer c_{ijk} counts the number of solutions of the equations $xy=z$, with $x \in \mathfrak{C}_i$, $y \in \mathfrak{C}_j$, and z fixed in \mathfrak{C}_k .

While it is easy to find examples of non-isomorphic groups with the same character table (see Exercise 9.9), no such examples of simple (nonabelian) groups are known. However, (9.33) has been used to prove that certain classes of finite simple groups, such as the alternating groups, are uniquely determined by their character tables (see G. Higman [71]).

We turn next to a beautiful result on multiplication of characters, due originally to Burnside, with improvements by Steinberg and Brauer. Let M and N be KG -modules affording characters μ and ν , respectively. We may form the KG -module $M \otimes_K N$ on which G acts by the rule

$$x(m \otimes n) = xm \otimes xn, \quad x \in G, m \in M, n \in N.$$

We extend the action from G to KG by linearity. Then the module $M \otimes_K N$ affords the character $\mu\nu$, whose value at each $x \in G$ is $\mu(x)\nu(x)$. (See §10B for further discussion of tensor products of modules.)

We shall also need the concept of a *faithful* K -character μ ; by definition, this is a character such that $\ker \mu = \{1\}$. Equivalently, μ is faithful if for $x \in G$, $\mu(x) = \mu(1)$ implies that $x = 1$. Note that the character table of G enables us to decide whether a given character μ is faithful, provided we know the irreducible characters occurring in μ , and their multiplicities.

Given a K -character μ , we put

$$\mu(G) = \{\mu(x) : x \in G\},$$

and $\text{card } \mu(G)$ the number of elements in the set $\mu(G)$. Thus, $\text{card } \mu(G)$ is the number of distinct values which μ assumes on G .

For a faithful K -character μ , the following striking result was proved by Brauer [64a], sharpening earlier results of Burnside [11] and Steinberg [62]:

(9.34) Theorem. *Let μ be a faithful K -character of G , and let $\text{card } \mu(G) = t$. Then each irreducible K -character ξ of G appears with positive multiplicity in at least one of $\mu^0 (= 1_G)$, μ , μ^2, \dots, μ^{t-1} .*

Before giving the proof, we note:

(9.35) Example. Let ρ be the character of the left regular module KG , where $G \neq \{1\}$. Then

$$\rho(x) = \begin{cases} |G|, & x=1 \\ 0, & x \neq 1. \end{cases}$$

Thus $\text{card } \rho(G) = 2$, and (9.34) asserts that every irreducible character is either 1_G or appears in ρ , which has already been proved in (3.37iii), using the Wedderburn Theorems.

Proof of (9.34). Let μ take on t distinct values $\{a_1, \dots, a_t\}$, and let $A_j = \{x \in G : \mu(x) = a_j\}$, $1 \leq j \leq t$. Assume that for some m , $(\mu^i, \xi^{(m)}) = 0$ for all i , $0 \leq i \leq t-1$. Then for each i ,

$$|G|(\mu^i, \xi^{(m)})_G = \sum_{j=1}^t \mu^i(x_j) \sum_{x \in A_j} \overline{\xi^{(m)}(x)} = 0,$$

where $x_j \in A_j$. The Vandermonde determinant $\det(\mu^i(x_j)) = \det(a_j^i)$ is not zero, hence

$$\sum_{x \in A_j} \xi^{(m)}(x) = 0$$

for all j . Number the $\{a_i\}$ so that $a_1 = \mu(1)$. Then $A_1 = \{1\}$ by (9.27), since μ is faithful. Taking $j = 1$, the above-displayed equation gives $\xi^{(m)}(1) = 0$, a contradiction, and the result is proved.

We next present what was historically the first approach to the problem of constructing character tables (Frobenius [96]; see also Feit [67, §7] and McKay [79].)

(9.36) Proposition. *A knowledge of the structure constants $\{c_{ijk}\}$ for the center of KG (see (9.28)) is equivalent to the knowledge of the character table $(\xi_j^{(i)})$ of G .*

Proof. By (9.33), the $\{c_{ijk}\}$ are determined by the character table, and by the constants $\{h_i : 1 \leq i \leq s\}$ and $|G|$. The group order $|G|$ and the $\{h_i\}$ are also determined by the character table, using the Second Orthogonality Relation.

Conversely, assume the $\{c_{ijk}\}$ are known, and let us see how to obtain the character table of G . We first show how to determine the constants $\{\omega_i^{(m)}\}$ defined in (9.29). We have

$$C_i C_j = \sum c_{ijk} C_k,$$

and assume that $C_1 = \{1\}$. Let \mathbf{A}_i be the $s \times s$ matrix $(c_{ijk})_{j,k}$, for $1 \leq i \leq s$, and let w_m be the column vector with entries $(\omega_1^{(m)}, \dots, \omega_s^{(m)})$, for $1 \leq m \leq s$. Note that $\omega_1^{(m)} = 1$ for $1 \leq m \leq s$, and that, by (9.30),

$$\mathbf{A}_i w_m = \omega_i^{(m)} w_m, \quad 1 \leq i, m \leq s.$$

Thus w_m is a common eigenvector for the matrices $\{\mathbf{A}_1, \dots, \mathbf{A}_s\}$, with eigenvalues $\{\omega_1^{(m)}, \dots, \omega_s^{(m)}\}$, respectively.

We next show that, up to multiplication by scalars, the vectors $\{w_m : 1 \leq m \leq s\}$ are the only common eigenvectors for the matrices $\{\mathbf{A}_i : 1 \leq i \leq s\}$. Let V be the vector space of s -rowed column vectors over K , and view the matrices $\{\mathbf{A}_i\}$ as linear transformations on V . It follows readily from (9.20) that the vectors $\{w_m : 1 \leq m \leq s\}$ are linearly independent over K , and therefore

$$V = \bigoplus_{m=1}^s Kw_m.$$

It is clear from the definition that the matrices $\{\mathbf{A}_i\}$ afford the regular matrix representation of the center of the group algebra with respect to the basis $\{C_i\}$. Therefore we have

$$\mathbf{A}_i \mathbf{A}_j = \sum_k c_{ijk} \mathbf{A}_k$$

as operators on V . It follows that the map $C_i \rightarrow \mathbf{A}_i$, $1 \leq i \leq s$, defines a representation of the center of KG on the space V . Furthermore, the subspaces $\{Kw_m : 1 \leq m \leq s\}$ afford one-dimensional representations of the center. These s representations are distinct, since for $m \neq n$ we cannot have $\omega_i^{(m)} = \omega_i^{(n)}$ for each i , $1 \leq i \leq s$. Thus these subspaces are a basic set of simple modules for the center of KG . It follows at once that any common eigenvector of the matrices $\{\mathbf{A}_1, \dots, \mathbf{A}_s\}$ affords an irreducible (one-dimensional) representation of the center of KG , and hence must be a scalar multiple of one of the vectors $\{w_m : 1 \leq m \leq s\}$.

We have now shown that $\{w_1, \dots, w_m\}$ are the uniquely determined common eigenvectors of the matrices $\{\mathbf{A}_i : 1 \leq i \leq s\}$, when normalized so that each w_i has first entry 1. Hence the $\{\omega_i^{(m)}\}$ are computable from the $\{c_{ijk}\}$. We have, by (9.29),

$$\omega_i^{(m)} = \frac{h_i \xi_i^{(m)}}{z_m}, \quad 1 \leq i, m \leq s.$$

Since $c_{ij1} = h_i \delta_{ij}$, for $1 \leq i, j \leq s$, the numbers $\{h_i\}$ are determined by the $\{c_{ijk}\}$, and hence so are the numbers $\{\xi_i^{(m)}/z_m : 1 \leq i, m \leq s\}$. Finally,

$$\sum_{i=1}^s \frac{\xi_i^{(m)}}{z_m} \cdot \omega_i^{(m)} = \frac{|G|}{z_m^2},$$

by the First Orthogonality Relation. Thus the degrees $\{z_m\}$ can be calculated from the $\{c_{ijk}\}$, and hence so can the character values $\{\xi_j^{(i)}\}$. This completes the proof.

We conclude this subsection with some examples of character tables, using the notation of (9.25), and letting S_n and A_n denote the symmetric and alternating groups on n objects, respectively. Other character tables, including that of A_5 , appear in §§14D, F. For the character tables of all simple groups of order $< 10^6$, see McKay [79]. Details of computation of the character tables below are left as exercises for the reader.

	x_1	x_2	x_3	x_4	x_5
$S_3:$	ξ^1	1	1	1	1
	ξ^2	1	-1	1	-1
	ξ^3	2	0	2	
$D_4:$	ξ^1	1	1	1	1
	ξ^2	1	-1	1	-1
	ξ^3	1	1	-1	-1
	ξ^4	1	-1	-1	1
	ξ^5	2	0	0	-2
$A_4:$	ξ^1	1	1	1	1
	ξ^2	3	-1	0	0
	ξ^3	1	1	ϵ	ϵ^2
	ξ^4	1	1	ϵ^2	ϵ
$S_4:$	ξ^1	1	1	1	1
	ξ^2	1	-1	1	-1
	ξ^3	2	0	-1	0
	ξ^4	3	1	0	-1
	ξ^5	3	-1	0	1

where ϵ is a primitive cube root of 1. Note that A_4 is isomorphic to the group of rotations of the tetrahedron, and D_4 is the dihedral group of order 8.

	x_1	x_2	x_3	x_4	x_5
Γ , the group of rotations of the cube:	ξ^1	1	1	1	1
	ξ^2	1	1	1	-1
	ξ^3	3	-1	0	1
	ξ^4	2	2	-1	0
	ξ^5	3	-1	0	-1

	x_1	x_2	x_3	x_4	x_5	x_6	x_7
$S_5:$	ξ^1	1	1	1	1	1	1
	ξ^2	1	-1	1	1	-1	1
	ξ^3	4	2	1	0	0	-1
	ξ^4	4	-2	1	0	0	-1
	ξ^5	5	1	-1	1	-1	1
	ξ^6	5	-1	-1	1	1	-1
	ξ^7	6	0	0	-2	0	1

For discussion of some of these examples, see CR §§32, 46.

§9E. Burnside's p^aq^b -Theorem

It would be a mistake to leave the scene without a glimpse of the power of some of the preceding results, when combined with a little algebraic number theory and group theory. We shall keep the notations set in (9.25), and assume that $\dim_Q K < \infty$.

We shall prove Burnside's Theorem (Burnside [11]) that if the order of a finite group G is of the form p^aq^b , where p and q are primes, then G is solvable. The nonsolvable alternating group A_5 , of order $60 = 2^2 \cdot 3 \cdot 5$, shows that the theorem cannot be improved without imposing further restrictions. We shall essentially follow Burnside's proof of the theorem, with emphasis on how the character theory is brought into the picture.

Assume that the result is false, and let G be a counterexample of minimal order. From elementary group theory, it is easy to show that G must be simple, nonabelian, and that both exponents a and b must be positive. Now let P be a p -Sylow subgroup of G , and let $h \neq 1$ be an element in the center $Z(P)$. Then $C_G(h) \geq P$, and $C_G(h) \neq G$ since otherwise $Z(G) \neq \{1\}$, contrary to our assumption that G is simple and nonabelian. It follows that $|G : C_G(h)| = q^d$ for some $d \neq 0$. The proof is completed by establishing the following result:

(9.37) Proposition (Burnside). *Let G be a finite group containing a conjugacy class \mathfrak{C} for which $|\mathfrak{C}| = q^d$ for some prime q and some $d > 0$. Then G cannot be simple.*

Proof. We first experiment with some easy consequences of the hypothesis. Let \mathfrak{C} be the class \mathfrak{C}_i , so i is fixed from now on, and (using the notation in (9.25)) $h_i = q^d$ and $i > 1$. But $|G| = \sum z_j^2$ by (3.37) or the Second Orthogonality Relation, so

$$|G| = \sum_{j=1}^s z_j^2 = 1 + \sum_{j>1} z_j^2, \quad |G| \equiv 0 \pmod{q},$$

whence $q \nmid z_j$ for some $j > 1$.

We next assert that $\xi_i^{(j)} \neq 0$ for some $j > 1$ such that $q \nmid z_j$. Suppose otherwise, so $\xi_i^{(j)} = 0$ whenever $j > 1$ and $q \nmid z_j$. Let $R = \text{alg. int.}\{K\}$, so $\mathbb{Q} \cap R = \mathbb{Z}$ because \mathbb{Z} is integrally closed. From the Second Orthogonality Relation we obtain (since $i > 1$)

$$0 = \sum_{j=1}^s \xi_1^{(j)} \xi_i^{(j)} = 1 + \sum_{j>1} z_j \xi_i^{(j)}.$$

Our supposition implies that each $z_j \xi_i^{(j)} \in qR$ for $j > 1$, whence we obtain $1 \in qR$. Then $q^{-1} \in R \cap \mathbb{Q}$, so $q^{-1} \in \mathbb{Z}$, which is impossible. This contradiction shows that $\xi_i^{(j)} \neq 0$ for some $j > 1$ such that $q \nmid z_j$.

Now let $j > 1$ be such that $q \nmid z_j$ and $\xi_i^{(j)} \neq 0$, and let us investigate $\ker \xi^{(j)}$, hoping to use (9.27) to find a normal subgroup of G . By (9.31),

$$\omega_i^{(j)} = h_i \xi_i^{(j)} / z_j \in R.$$

But $h_i = q^d$, whereas $q \nmid z_j$, so we may choose $a, b \in \mathbb{Z}$ such that $1 = ah_i + bz_j$. Therefore

$$a\omega_i^{(j)} = \frac{ah_i \xi_i^{(j)}}{z_j} = \frac{\xi_i^{(j)}}{z_j} - b\xi_i^{(j)},$$

and we conclude that $\xi_i^{(j)} / z_j \in R$. By (9.27) we have $|\xi_i^{(j)} / z_j| \leq 1$, and if we could prove that equality holds, then by (9.27) G would have a normal subgroup containing \mathfrak{C}_i . It is here that we must use some algebraic number theory. For convenience, let us denote the algebraic integer $\xi_i^{(j)} / z_j$ by ξ , so $\xi \neq 0$ and $|\xi| \leq 1$. Since $\xi \in R$ we have (see (1.9))

$$\text{char. pol.}_{K/\mathbb{Q}}(\xi) \in \mathbb{Z}[X],$$

whence $N(\xi) \in \mathbb{Z}$, where N denotes the norm map from K to \mathbb{Q} . On the other hand (see CR §20B), $N(\xi)$ is the product of the algebraic conjugates of ξ over \mathbb{Q} .

Suppose now that $|\xi_i^{(j)}| < z_j$, so $\xi_i^{(j)}$ is a sum of z_j roots of unity, not all of which are equal. But then every algebraic conjugate of $\xi_i^{(j)}$ is also such a sum. This proves that if $|\xi| < 1$, then also $|\xi^\sigma| < 1$ for every algebraic conjugate ξ^σ of ξ . Hence if $|\xi| < 1$, it follows that $|N(\xi)| < 1$; but this is impossible, since $N(\xi)$ is a nonzero rational integer. We have thus shown that $|\xi_i^{(j)}| = z_j$.

Now let \mathbf{Z}_j be an irreducible matrix representation of G affording the character $\xi^{(j)}$, and put

$$H = \{x \in G : \mathbf{Z}_j(x) \in K \cdot \mathbf{I}\}.$$

Then by (9.27) H is a normal subgroup of G containing the class \mathfrak{C}_i . Thus G cannot be simple unless $H = G$; but in that case, \mathbf{Z}_j is an irreducible representation of G by scalar matrices, and hence must be of degree 1. Further, \mathbf{Z}_j is not the 1-representation since $j > 1$. Thus G has at least two distinct one-dimensional representations, so $G/G' \neq 1$ by the remarks following (9.27). Since $G' \trianglelefteq G$ and G is simple, it follows that $G' = \{1\}$. But then G is abelian, which contradicts the fact that G has a conjugacy class \mathfrak{C} with $|\mathfrak{C}| > 1$. This completes the proof.

§9 Exercises

Unless otherwise stated, all representations and characters are taken in the field of complex numbers \mathbb{C} .

1. Show that the maps

$$a \rightarrow \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, b \rightarrow \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \text{ where } i = \sqrt{-1},$$

and

$$a \rightarrow \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, b \rightarrow \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix},$$

define representations of the dihedral group D_4 defined in (1.24i).

Discuss, from first principles, whether the representations are equivalent. Compute the characters of the representations, and use them to check equivalence.

2. The *regular character* ρ_G of G is the C-character afforded by the left regular module CG . Show that

$$\rho_G(x) = \begin{cases} |G| & \text{if } x=1, \\ 0 & \text{if } x \neq 1. \end{cases}$$

Show that if $\xi \in \text{Irr}(G)$, then $(\xi, \rho_G) = \deg \xi$ (compare with (3.37iii) and Exercise 3.10).

3. Let $H \trianglelefteq G$. Show that each character μ of G/H can be lifted to a character $\tilde{\mu}$ of G , given by $\tilde{\mu} = \mu \circ f$, where $f: G \rightarrow G/H$ is the natural homomorphism. Prove that $\tilde{\mu}$ is irreducible if and only if μ is irreducible.

Also show that

$$\tilde{\rho}_{G/H} = \sum \xi(1)\xi,$$

where $\rho_{G/H}$ is the regular character of G/H (Exercise 2), and the sum is taken over all $\xi \in \text{Irr}(G)$ such that $H \leq \ker \xi$.

4. Prove that a set of distinct irreducible characters $\{\xi_1, \dots, \xi_r\}$ forms a basic set (that is, coincides with $\text{Irr}(G)$) if and only if $\sum \{\xi_i(1)\}^2 = |G|$.

5. Prove that if $x \in G$ satisfies the condition $\xi(x) = \xi(1)$ for all $\xi \in \text{Irr}(G)$, then $x = 1$.

6. Let $G = G_1 \times G_2$, and let $\xi_i \in \text{Irr}(G_i)$, $i = 1, 2$. Define $\xi_1 \xi_2$ by $(\xi_1 \xi_2)(g_1, g_2) = \xi_1(g_1) \xi_2(g_2)$, $g_i \in G_i$. Show that $\xi_1 \xi_2 \in \text{Irr}(G_1 \times G_2)$. Using the orthogonality relations, prove that every irreducible complex character of G can be expressed in the form $\xi_1 \xi_2$, with uniquely determined characters $\xi_i \in \text{Irr}(G_i)$, $i = 1, 2$. (This result can also be proved by using representations, rather than characters, and applying Burnside's Theorem; see (10.33) and (10.38) below.)

7. Find all characters of a finite abelian group G , and give explicit formulas for the corresponding central primitive idempotents in CG . Prove that if m is the exponent of G , and ω_m is a primitive m -th root of 1, then $\mathbb{Q}(\omega_m)$ is a splitting field for G , (that is, $\mathbb{Q}(\omega_m)G$ is a split semisimple $\mathbb{Q}(\omega_m)$ -algebra).

8. A *linear character* of G is a character of degree 1. Prove that the number of distinct linear characters is $|G: G'|$, where G' is the commutator subgroup of G . Show how G' can be determined from the character table of G .

9. Find the character tables of S_3 , D_4 , and Q , where Q is the quaternion group of order 8. Note that D_4 and Q have the same character tables, but are not isomorphic. Show that the group algebras $\mathbb{C}D_4$ and $\mathbb{C}Q$ are isomorphic. (An example of two non-isomorphic groups, having isomorphic group algebras over algebraically closed fields of all characteristics, was found by Dade [71]).

10. Let M be a left CG -module, and let $\text{inv}_G(M) = \{m \in M : gm = m, \forall g \in G\}$.[†] Prove that if μ is the character afforded by M , then $(\mu, 1_G) = \dim_{\mathbb{C}}(\text{inv}_G(M))$. Also show that $\left(|G|^{-1} \sum_{g \in G} g\right)_f$ is a projection in $\text{End}_{CG}(M)$, and that it carries M onto $\text{inv}_G(M)$.

11. (This exercise contains another approach to the orthogonality relations). Let M, N be simple left CG -modules, with characters μ and ν , respectively. Let M^* be the contragredient module of M , defined as $M^* = \text{Hom}_{\mathbb{C}}(M, \mathbb{C})$, with the action of G given by

$$(xf)(m) = f(x^{-1}m), \quad m \in M, f \in M^*, x \in G.$$

(i) Show that M^* is a simple CG -module, whose character μ^* is given by $\mu^*(x) = \overline{\mu(x^{-1})} = \overline{\mu(x)}, x \in G$.

(ii) Prove that the vector spaces $M^* \otimes_{\mathbb{C}} N$ and $\text{Hom}_{\mathbb{C}}(M, N)$ are isomorphic, via the map $\sum f_i \otimes n_i \rightarrow \tau$, where $\tau(m) = \sum f_i(m)n_i$ for all $m \in M$.

(iii) View $M^* \otimes_{\mathbb{C}} N$ as a CG -module, with character $\mu^* \cdot \nu$, as in §9C. Prove that the isomorphism given in part (ii) carries $\text{inv}_G(M^* \otimes_{\mathbb{C}} N)$ onto $\text{Hom}_{CG}(M, N)$.

(iv) Prove that

$$\begin{aligned} \text{Tr}\left(\frac{1}{|G|} \sum_{g \in G} g, M^* \otimes N\right) &= \frac{1}{|G|} \sum_{g \in G} \mu^*(g)\nu(g) \\ &= (\nu, \mu) = \dim_{\mathbb{C}}(\text{inv}_G(M^* \otimes N)). \end{aligned}$$

(v) Using (iii) and Schur's Lemma, prove that

$$(\nu, \mu) = \begin{cases} 1 & \text{if } \mu = \nu, \\ 0 & \text{otherwise.} \end{cases}$$

(A discussion of contragredient modules in a more general setting appears in §11D).

In problems 12–14, E denotes an arbitrary subfield of \mathbb{C} .

[†] $\text{inv}_G(M)$ is the submodule of G -invariants of M , and will often be called the *G-trivial* submodule of M .

12. Let T be an E -representation of G , with E -character τ , and let U be an irreducible E -representation, with character η . Prove that $(\tau, \eta) \neq 0$ if and only if U is a direct summand of T .

13. Prove that if M and N are EG -modules, with characters μ and ν , respectively, then $M \cong N$ if and only if $\mu = \nu$.

14. (Schur). Let E be a subfield of C , and F a finite Galois extension of E such that FG is a split semisimple F -algebra (see §7B). Let $\text{Gal}(F/E)$ denote the Galois group of F over E . For each F -representation $M: G \rightarrow GL_n(F)$, and each automorphism $\sigma \in \text{Gal}(F/E)$, let ${}^\sigma M$ be the F -representation, which assigns to each $x \in G$ the matrix obtained by applying σ to all the entries of $M(x)$ (see the last part of §7B for a more general version of this construction.) The representations $\{{}^\sigma M: \sigma \in \text{Gal}(F/E)\}$ are called E -conjugates of M . If μ is the character of M , $\sigma(\mu)$ denotes the character of the representation ${}^\sigma M$, and is called an E -conjugate of μ .

(i) Prove that if $\zeta \in \text{Irr}_F(G)$, then $\sigma(\zeta) \in \text{Irr}_F(G)$ for all $\sigma \in \text{Gal}(F/E)$.

(ii) Prove that every character $\mu \in \text{Irr}_E(G)$ can be expressed in the form

$$\mu = m \left(\sum_{\sigma} \sigma(\zeta) \right),$$

where ζ is an irreducible F -character ζ such that $(\zeta, \mu) \neq 0$, $\{\sigma(\zeta)\}$ is the set of distinct conjugates of ζ , and m is a positive integer.

[*Hints:* (i) Show that $(\sigma(\mu), \sigma(\mu)) = (\mu, \mu)$ for each F -character μ and each $\sigma \in \text{Gal}(F/E)$. (ii) Let M be an irreducible E -representation of G with character μ . Apply Proposition 7.18 to conclude that M^F is a direct sum of conjugates of one simple F -representation, with the different conjugates all appearing with the same multiplicity in the direct sum. Translate into the language of characters to obtain (ii).]

In the remaining problems, we return to C -characters of G .

15. (Feit-Thompson [63]). Let $H \trianglelefteq G$, and let $x \in G$ be an element such that $C_G(x) \cap H = 1$. Prove that $\zeta^{(i)}(x) = 0$ for all $\zeta^{(i)} \in \text{Irr}(G)$ such that $H \not\subseteq \ker \zeta^{(i)}$.

[*Hint:* The Second Orthogonality Relation (9.26) asserts that $\sum |\zeta^{(i)}(x)|^2 = |C_G(x)|$. Letting $G/H = \bar{G}$, $xH = \bar{x} \in \bar{G}$, etc., show that $|C_G(x)| \leq |C_{\bar{G}}(\bar{x})|$, and apply the Second Orthogonality Relation to the characters of \bar{G} , lifted to G as in Exercise 3.]

16. (Littlewood). Let e be a primitive idempotent in CG such that CGe is a simple module affording the character ζ . Let $e = \sum_{x \in G} \alpha_x x$. For each $t \in G$ belonging to a conjugacy class \mathfrak{C} of G , prove that

$$\zeta(t^{-1}) = |C_G(t)| \sum_{x \in \mathfrak{C}} \alpha_x.$$

[*Hint:* For each conjugacy class \mathfrak{C} in G , define a linear map $T: CG \rightarrow C$, depending

on \mathbb{C} , as follows:

$$T\left(\sum_{x \in G} \alpha_x x\right) = \sum_{x \in \mathbb{C}} \alpha_x.$$

Prove that $T(ab) = T(ba)$ for all $a, b \in CG$, and hence that $T(aba^{-1}) = T(b)$ if a is invertible. Now let e_ζ be a central primitive idempotent in CG corresponding to ζ , as in (9.21). Then

$$e_\zeta = e_1 + \cdots + e_n, \quad n = \zeta(1),$$

where the $\{e_i\}$ are primitive orthogonal idempotents in the Wedderburn component CGe_ζ . Prove that all such idempotents have the same elementary divisors, and hence are conjugate in CG (see also Exercise 6.15). For each conjugacy class \mathbb{C} in G , apply T as above to the expression for e_ζ , and obtain Littlewood's formula.]

17. (G. Higman [40]; see also CR §37). Consider the integral group ring $\mathbb{Z}G$, for a finite abelian group G . Let u be a unit of finite order in $\mathbb{Z}G$. Prove that $u = \pm x$, for some $x \in G$.

[Hint: Let $\text{Irr}(G) = \{\zeta^{(1)}, \dots, \zeta^{(s)}\}$. Show that the central primitive idempotents in CG are

$$e_i = |G|^{-1} \sum_{x \in G} \overline{\zeta^{(i)}(x)} x, \quad 1 \leq i \leq s.$$

Show that since G is abelian, $\{e_1, \dots, e_s\}$ is a basis of CG , so that each $u \in CG$ can be expressed in two ways:

$$u = \sum_{x \in G} \alpha_x x = \sum_{i=1}^s \beta_i e_i.$$

Show that the coefficients $\{\alpha_x\}$ and $\{\beta_i\}$ are related by:

$$\beta_i = \sum_{x \in G} \alpha_x \overline{\zeta^{(i)}(x)}, \quad \alpha_x = |G|^{-1} \sum_{i=1}^s \beta_i \overline{\zeta^{(i)}(x)}.$$

Now let $u \in \mathbb{Z}G$, and suppose $u^m = 1$ for some positive integer m . Then $\beta_i^m = 1$, $1 \leq i \leq s$. Suppose $x \in G$ is an element such that $\alpha_x \neq 0$. Then

$$|\alpha_x| = |G|^{-1} \left| \sum \beta_i \overline{\zeta^{(i)}(x)} \right| \leq |G|^{-1} \sum |\beta_i| \overline{|\zeta^{(i)}(x)|} \leq 1.$$

Since $\alpha_x \in \mathbb{Z}$, we have equality, and consequently $\alpha_x = \beta_i \overline{\zeta^{(i)}(x)}$, $1 \leq i \leq s$. Hence, if $y \neq x$,

$$\alpha_y = |G|^{-1} \sum_{i=1}^s \alpha_x \zeta^{(i)}(x) \overline{\zeta^{(i)}(y)} = 0.]$$

18. (Frobenius ([96, pp. 13, 14]). Let $g \in G$, and let N be the number of pairs (x, y) such that $g = xyx^{-1}y^{-1}$. Prove that

$$N = |G| \cdot \sum_{\xi \in \text{Irr}(G)} (\xi(g)/\xi(1)).$$

(See also Gallagher [62a].)

§10. INDUCED MODULES

The technique of induced representations is one of the most important methods in the entire theory of representations of groups. It establishes strong connections between the representation theory of a group G and the representations of the subgroups of G . The method does not extend readily to algebras, however, and is used primarily in the context of group algebras. We shall develop most of the theory, including the Frobenius Reciprocity Theorem, and the Mackey Decomposition Theorems, for the group algebra RG of a finite group G over an arbitrary commutative ring R . In case the coefficient ring is a splitting field K contained in the complex field, as in §9C, more precise versions of the theorems are available, and will be established at the appropriate places in the discussion.

§10A. Definition of Induced Modules. Frobenius Reciprocity

In this section, R denotes an arbitrary commutative ring, G a finite group, and H a fixed subgroup of G .

The problem to be considered is the construction of RG -modules from RH -modules, and the reverse problem. Both can be understood in a general ring-theoretical setting. Let $\varphi: B \rightarrow A$ be a homomorphism from a ring B into a ring A such that $\varphi(1)=1$. One way is easy. Let M be a left A -module; then we obtain a B -module $\varphi_*(M)$, whose underlying abelian group is M , and for which the composition is given by

$$b \cdot m = \varphi(b)m, \quad b \in B, \quad m \in M.$$

Then φ_* defines a covariant functor (see §2C) from the category $_A\mathfrak{M}$ of left A -modules to the category $_B\mathfrak{M}$ of left B -modules. The operation $M \mapsto \varphi_*(M)$ is called *restriction of scalars*.

For the reverse construction, we first note that A becomes an (A, B) -bimodule, with the action of $b \in B$ on A given by right multiplication by $\varphi(b)$. Then each left B -module L defines a left A -module $\varphi^*(L)$, where

$$\varphi^*(L) = A \otimes_B L.$$

This time we obtain a covariant function $\varphi^*: _B\mathfrak{M} \rightarrow _A\mathfrak{M}$, called *induction*. Note that $\varphi^*(B) = A$.

Now let us apply these constructions to the categories of left RG -modules and left RH -modules, where $\varphi: RH \rightarrow RG$ is the injective homomorphism from RH into RG arising from the inclusion map $H \subseteq G$. We shall view φ as an inclusion map whenever $H \subseteq G$, and write $RH \subseteq RG$.

Then the operation of *restriction of scalars* from RG to RH assigns to each left RG -module M a left RH -module $\text{res}_H^G(M)$, which we shall often write in abbreviated form as $M|_H$, or M_H . If $\mathbf{M}: G \rightarrow GL(M)$ is a matrix representation of G afforded by an R -free RG -module M with a finite basis, then the representation $\mathbf{M}|_H$ of H afforded by the restriction $M|_H$ is simply the restriction of the homomorphism $\mathbf{M}: G \rightarrow GL(M)$ to the subgroup H . Similarly, if $\mu: G \rightarrow R$ is the trace function (or character) of an R -matrix representation \mathbf{M} , then the character $\mu|_H$ of the restriction $\mathbf{M}|_H$ is again the restriction of the function $\mu: G \rightarrow R$ to H .

The operation of *induction* from RH -modules to RG -modules assigns to each left RH -module L a left RG -module $\text{ind}_H^G(L)$, given by

$$\text{ind}_H^G(L) = RG \otimes_{RH} L.$$

We shall often abbreviate $\text{ind}_H^G(L)$ as L^G . Note that $\text{ind}_H^G(RH) = RG$.

As we pointed out in the introduction to this section, RG is an (RG, RH) -bimodule, with operations given by left and right multiplication in RG . Thus $\text{ind}_H^G(L)$ consists of all elements $\sum g_i \otimes l_i$, with $g_i \in G$, $l_i \in L$, with the action of $g \in G$ given by

$$g(\sum g_i \otimes l_i) = \sum gg_i \otimes l_i.$$

If \mathbf{L} is a matrix representation of H over the ring R , then \mathbf{L}^G (or $\text{ind}_H^G(\mathbf{L})$) denotes the matrix representation of G afforded by induction from the RH -module defined by \mathbf{L} . If $\lambda: H \rightarrow R$ is the character of \mathbf{L} , then λ^G (or $\text{ind}_H^G(\lambda)$) denotes the character of the induced representation \mathbf{L}^G . We call λ^G an *induced character*.

Our first task is to work out in detail the action of G on L^G , so that when L affords a matrix representation \mathbf{L} , the induced representation \mathbf{L}^G and induced character λ^G can be computed explicitly.

Let $G = g_1 H \cup \dots \cup g_n H$ be a left coset decomposition of G relative to H , with $n = |G:H|$, and $g_1 = 1 \in H$. Then

$$RG = \bigoplus_{i=1}^n g_i RH.$$

Now let L be a left RH -module. From the direct sum theorem for tensor products (2.17), we have

$$L^G = RG \otimes_{RH} L = \bigoplus_{i=1}^n g_i RH \otimes L = \bigoplus_{i=1}^n g_i \otimes L,$$

using the fact that $g_i RH \otimes L = g_i \otimes (RH)L = g_i \otimes L$ because the tensor product is taken with respect to RH .

We next observe that $g_i \otimes L = 1 \otimes L$ is an RH -submodule of $L^G|_{RH}$, and the map

$$l \mapsto 1 \otimes l, \quad l \in L,$$

is an RH -monomorphism from L into L^G , because of the isomorphism $RH \otimes_{RH} L \cong L$ (see (2.16)). Finally, each summand $g_i \otimes L$ of L^G can be expressed as $g_i(1 \otimes L)$, and hence $1 \otimes L \cong g_i \otimes L$ as R -modules, with the isomorphism given by left multiplication by g_i .

Now let $g \in G$; for each i , $1 \leq i \leq n$, we have $gg_i \in g_j H$ for some left coset $g_j H$. Hence there is a uniquely determined coset representative g_j and an element $h \in H$ such that

$$gg_i = g_j h.$$

Thus $g(g_i \otimes L) = g_j \otimes L$, so that g permutes the summands $\{g_i \otimes L\}$. The action of g on an individual summand $g_i \otimes L$ is given by

$$g(g_i \otimes l) = g_j h \otimes l = g_j \otimes hl, \quad l \in L.$$

We next suppose that L affords a matrix representation \mathbf{L} , with respect to a finite R -basis $\{l_1, \dots, l_m\}$ of L , so that

$$hl_j = \sum_{j=1}^m \alpha_{ij}(h)l_i, \quad \alpha_{ij}(h) \in R,$$

and $\mathbf{L}(h) = (\alpha_{ij}(h))$ for $h \in H$. To compute $\mathbf{L}^G(g)$ for $g \in G$, we first note that from what has been shown, the elements $\{g_i \otimes l_j\}$, $1 \leq i \leq n$, $1 \leq j \leq m$, form an R -basis for L^G . Letting $gg_i = g_j h$ as above, we have

$$g(g_i \otimes l_s) = g_j \otimes hl_s = \sum_{t=1}^m \alpha_{ts}(h)(g_j \otimes l_t)$$

for $1 \leq s \leq m$. These formulas can be described efficiently in the following way. Note first that the equation $gg_i = g_j h$ is equivalent to the statement $g_j^{-1}gg_i = h$. We next extend the matrix coefficient functions $\{\alpha_{ij}\}$ to maps $\dot{\alpha}_{ij}: G \rightarrow R$, where

$$\dot{\alpha}_{ij}(g) = \begin{cases} \alpha_{ij}(g) & \text{if } g \in H, \\ 0 & \text{if } g \notin H. \end{cases}$$

Then the action of g on the R -basis $\{g_i \otimes l_s\}$ of L^G is given by

$$\begin{aligned} g(g_i \otimes l_s) &= \sum_{t=1}^m \alpha_{ts}(h) g_j \otimes l_t \\ &= \sum_{j=1}^n \sum_{t=1}^m \dot{\alpha}_{ts}(g_j^{-1} gg_i)(g_j \otimes l_t). \end{aligned}$$

Likewise, we extend \mathbf{L} from H to G by defining

$$\mathbf{L}(g) = (\dot{\alpha}_{ij}(g)), \quad g \in G.$$

Then, relative to the R -basis

$$g_1 \otimes l_1, \dots, g_1 \otimes l_m, g_2 \otimes l_1, \dots, g_2 \otimes l_m, \dots,$$

the matrix representation afforded by L^G is given by

$$(10.1) \quad g \rightarrow \mathbf{L}^G(g) = \begin{bmatrix} \mathbf{L}(g_1^{-1} gg_1) & \cdots & \mathbf{L}(g_1^{-1} gg_n) \\ \vdots & & \vdots \\ \mathbf{L}(g_n^{-1} gg_1) & \cdots & \mathbf{L}(g_n^{-1} gg_n) \end{bmatrix}.$$

Letting $\lambda : H \rightarrow R$ be the character afforded by L , that is,

$$\lambda(h) = \text{Trace } \mathbf{L}(h), \quad h \in H,$$

it is immediate from (10.1) that the character λ^G afforded by L^G is given by

$$(10.2) \quad \lambda^G(g) = \sum_{i=1}^n \dot{\lambda}(g_i^{-1} gg_i).$$

Here $\dot{\lambda}$ is the extension to G of the function λ , and is defined by

$$\dot{\lambda}(g) = \begin{cases} \lambda(g), & g \in H, \\ 0, & g \notin H. \end{cases}$$

In case $|H|$ is a unit in R , the formula for λ^G can be written in the useful form

$$(10.3) \quad \lambda^G(g) = \frac{1}{|H|} \sum_{x \in G} \dot{\lambda}(x^{-1} gx),$$

which does not involve the coset representatives $\{g_i\}$. We note in passing the important formula:

$$(10.3a) \quad \deg \lambda^G = \lambda^G(1) = |G : H| \lambda(1).$$

(10.4) Example. Let 1_H denote the trivial representation of H , and let $V=Rv$ be a free R -module affording 1_H , so $hv=v$ for all $h \in H$. The action of $g \in G$ on the summands $R(g_i \otimes v)$ of the module affording 1_H^G is given by

$$g(g_i \otimes v) = g_j \otimes v, \text{ where } gg_i \in g_j H.$$

This formula shows that the G -set of submodules $R(g_i \otimes v)$ of V^G , with the action of G given as above, is isomorphic to the G -set G/H of left cosets $\{g_i H\}$ of H , with action of G given by left translation $g_i H \rightarrow gg_i H$, $g \in G$, $1 \leq i \leq n$. Thus the induced representation 1_H^G is equivalent to the permutation representation of G over R afforded by the G -set G/H , defined by introducing an R -basis $\{v_i\}$ corresponding to the left cosets $\{g_i H\}$, with action of $g \in G$ on the basis defined by

$$gv_i = v_j \text{ if } gg_i H = g_j H, \quad 1 \leq i \leq n.$$

In particular, the left regular module RG of G over R is isomorphic to the induced module 1_H^G , induced from the trivial representation 1_H of the trivial subgroup $H = \{1\}$.

We now turn to some general properties of induced modules. We begin with an important characterization of induced modules:

(10.5) Proposition. *Let M be a left RG -module whose restriction $M|_H$ contains an RH -submodule L such that M is the direct sum $\bigoplus_{i=1}^n g_i L$ of R -submodules $\{g_i L\}$, where $\{g_i : 1 \leq i \leq n\}$ is a set of left coset representatives of H in G . Then $M \cong L^G$ as left RG -modules.*

Proof. One checks that the map $RG \times L \rightarrow M$, given by $(g, l) \mapsto gl$, is R -bilinear and RH -balanced. It follows that there is an R -surjection $\varphi: RG \otimes_{RH} L \rightarrow M$, such that $\varphi(g_i \otimes L) = g_i L$, $1 \leq i \leq n$. The hypothesis implies the existence of an R -homomorphism from M to L^G which is an inverse to φ , and takes $g_i L$ onto $g_i \otimes L$, $1 \leq i \leq n$. Thus φ is an R -isomorphism, which from its definition is in fact an RG -isomorphism; this completes the proof.

(10.6) Proposition. (i) (*Additivity of induction*). *Let $H \leq G$, and let L_1 and L_2 be left RH -modules. Then*

$$\text{ind}_H^G(L_1 \oplus L_2) \cong \text{ind}_H^G(L_1) \oplus \text{ind}_H^G(L_2).$$

(ii) (*Transitivity of induction*). *Let $H_1 \leq H_2 \leq G$, and let L be a left RH_1 -module. Then*

$$\text{ind}_{H_2}^G(\text{ind}_{H_1}^{H_2}(L)) \cong \text{ind}_{H_1}^G(L).$$

Proof. (i) follows immediately from the distributivity of tensor products over direct sums (2.17).

(ii) By associativity of the tensor product (2.18), together with the isomorphism $M \otimes_A A \cong M$ for a right A -module M (see (2.16)), we have

$$\begin{aligned} \text{ind}_{H_2}^G(\text{ind}_{H_1}^{H_2}(L)) &= RG \otimes_{RH_2}(RH_2 \otimes_{RH_1} L) \\ &\cong (RG \otimes_{RH_2} RH_2) \otimes_{RH_1} L \\ &\cong RG \otimes_{RH_1} L = \text{ind}_{H_1}^G(L) \end{aligned}$$

as R -modules. The isomorphisms all commute with the action of G from the left and the result follows.

(10.7) Corollary. *Let λ be the character of H_1 afforded by a left RH_1 -module L with a finite free R -basis, and let $H_1 \leq H_2 \leq G$ as above. Then*

$$(\lambda^{H_2})^G = \lambda^G.$$

(10.8) Frobenius Reciprocity Theorem (for RG -modules). *Let $H \leq G$, and let L be a left RH -module, and M a left RG -module. Then there exists an isomorphism of R -modules*

$$\text{Hom}_{RH}(L, M|_H) \cong \text{Hom}_{RG}(L^G, M).$$

Proof. We shall apply the Adjointness Theorem (2.19), which asserts that there is an isomorphism of additive groups

$$\text{Hom}_A(L', \text{Hom}_B(M', N')) \cong \text{Hom}_B(M' \otimes_A L', N'),$$

for any pair of rings A and B , and modules

$$L' \in {}_A\mathfrak{M}, \quad M' \in {}_B\mathfrak{M}_A, \quad N' \in {}_B\mathfrak{M}.$$

In order to prove (10.8), we let $A = RH$, $B = RG$, $L' = L \in {}_{RH}\mathfrak{M}$ as in (10.8), $M' = RG \in {}_{RG}\mathfrak{M}_{RH}$, and $N' = M \in {}_{RG}\mathfrak{M}$. Then there exists an isomorphism of additive groups

$$\text{Hom}_{RH}(L, \text{Hom}_{RG}(RG, M)) \cong \text{Hom}_{RG}(L^G, M).$$

From the construction of the isomorphism in (2.19), it is clear that the above is an R -isomorphism.

It remains to check that the left RH -module $\text{Hom}_{RG}(RG, M)$ is isomorphic to $M|_H$. It is clear that the map

$$\tau: f \in \text{Hom}_{RG}(RG, M) \rightarrow f(1) \in M$$

is an isomorphism of R -modules. From §2, the action of RH on $\text{Hom}_{RG}(RG, M)$ is given by

$$(bf)(a) = f(ab), \quad a \in RG, \quad b \in RH.$$

Then for all $b \in RH$ and $f \in \text{Hom}_{RG}(RG, M)$, we have

$$\tau(bf) = (bf)(1) = f(b) = b(f(1)) = b\tau(f),$$

proving that $\text{Hom}_{RG}(RG, M) \cong M|_H$ as RH -modules, and completing the proof.

We conclude this section with some remarks on the Frobenius Reciprocity Theorem, when the ring R is a subfield K of the field of complex numbers.

First assume as in §9C that K is a splitting field for KG and KH . Let M be a left KG -module with K -character μ , and let L be a left KH -module with K -character λ . By Proposition 9.24iii we have

$$\dim_K(\text{Hom}_{RH}(L, M|_H)) = (\lambda, \mu|_H)_H,$$

while

$$\dim_K(\text{Hom}_{RG}(L^G, M)) = (\lambda^G, \mu)_G.$$

Therefore, the preceding result implies that

$$(\lambda, \mu|_H)_H = (\lambda^G, \mu)_G.$$

It will be useful to note that this identity can easily be proved in a more general form (for class functions), without making use of the adjointness theorem as in (10.8), using instead the formula (10.3) for λ^G .

(10.9) Frobenius Reciprocity Theorem (for class functions). *Let K be a subfield of \mathbb{C} , and let $H \leq G$. Let $\lambda \in \text{cf}_K(H)$ and $\mu \in \text{cf}_K(G)$, and define $\lambda^G: G \rightarrow K$ by*

$$\lambda^G(g) = \frac{1}{|H|} \sum_{x \in G} \dot{\lambda}(x^{-1}gx),$$

where $\dot{\lambda}$ is the function λ extended to G as in (10.3). Then $\lambda^G \in \text{cf}_K(G)$, and we

have

$$(\lambda^G, \mu)_G = (\lambda, \mu|_H)_H.$$

Proof. It is immediate from the definition that $\lambda^G \in \text{cf}_K(G)$. We have

$$\begin{aligned} (\lambda^G, \mu)_G &= \frac{1}{|G|} \frac{1}{|H|} \sum_{x \in G} \sum_{y \in G} \dot{\lambda}(y^{-1}xy) \overline{\mu(x)} \\ &= \frac{1}{|G|} \frac{1}{|H|} \sum_{x \in G} \sum_{y \in G} \dot{\lambda}(y^{-1}xy) \overline{\mu(y^{-1}xy)} \\ &= \frac{1}{|H|} \sum_{z \in G} \dot{\lambda}(z) \overline{\mu(z)} = \frac{1}{|H|} \sum_{z \in H} \dot{\lambda}(z) \overline{\mu(z)} = (\lambda, \mu|_H)_H, \end{aligned}$$

using the facts that μ is a class function, and that for fixed z , the equation $y^{-1}xy=z$ has exactly $|G|$ solutions.

Examples. In both of the following examples of the use of the Frobenius Reciprocity Theorem, K denotes the field of complex numbers.

(10.10) As a first example of (10.9), we show how to prove that for a K -character λ of H , the induced class function $\lambda^G \in \text{cf}_K(G)$, as defined in (10.9), is a K -character of G . The proof uses only (10.9) and the orthogonality relations in §9C, and is independent of the interpretation of λ^G as the character of an induced module L^G , given in the first part of this section.

In order to prove that λ^G is a K -character of G , it is sufficient to prove that for all irreducible K -characters $\{\xi\}$ of G , the multiplicity $(\lambda^G, \xi)_G$ is a non-negative integer. From (10.9), we have

$$(\lambda^G, \xi)_G = (\lambda, \xi|_H)_H = \text{non-negative integer},$$

because both λ and $\xi|_H$ are K -characters of H , and our assertion now follows from Proposition 9.24i.

(10.11) Characters of the dihedral groups. Let D_m be the dihedral group of order $2m$, with the presentation

$$\langle a, b : a^m = b^2 = (ab)^2 = 1 \rangle.$$

We shall compute all the irreducible K -characters of D_m . Let $\lambda : \langle a \rangle \rightarrow K^\times$ be an irreducible character of $\langle a \rangle$ of degree 1. Letting ϵ be a primitive m -th root of 1, we have $\lambda(a) = \epsilon^i$ for some i . Using formula (10.2) for the induced character λ^G , we obtain

$$\lambda^G(x) = \dot{\lambda}(x) + \dot{\lambda}(bx b^{-1}).$$

For $x \in \langle a \rangle$, $bxb^{-1} = x^{-1}$, so we have

$$\lambda^G|_{\langle a \rangle} = \lambda + \bar{\lambda},$$

and by Proposition 10.9,

$$(\lambda^G, \lambda^G)_G = (\lambda, \lambda^G|_{\langle a \rangle})_{\langle a \rangle} = (\lambda, \lambda + \bar{\lambda})_{\langle a \rangle}.$$

From §9C, λ^G is irreducible if and only if $(\lambda^G, \lambda^G) = 1$. Therefore λ^G is irreducible if and only if $\lambda \neq \bar{\lambda}$. Moreover, if both λ^G and μ^G are irreducible, for homomorphisms $\lambda, \mu: \langle a \rangle \rightarrow K$, we have

$$(\lambda^G, \mu^G) = (\lambda, \mu + \bar{\mu})_{\langle a \rangle} = \begin{cases} 0, & \lambda \neq \mu, \bar{\mu}, \\ 1, & \lambda = \mu \text{ or } \bar{\mu}. \end{cases}$$

We now distinguish two cases:

(i) m is odd. In this case there are two characters of degree 1 (because $|D_m : D'_m| = 2$), and $\frac{1}{2}(m-1)$ distinct irreducible characters of the form λ^G as above. Adding up the squares of the degrees we obtain

$$2 + \frac{1}{2}(m-1)(4) = 2 + 2(m-1) = 2m = |D_m|,$$

and it follows that we have determined all the irreducible characters (by Proposition 3.37i).

(ii) m is even. In this case there are 4 characters of D_m of degree 1, and $\frac{1}{2}(m-2)$ distinct irreducible characters of degree 2. Adding up the squares of the degrees, we have

$$4 + \frac{1}{2}(m-2)(4) = 4 + 2(m-2) = 2m = |D_m|,$$

and again we have a complete set of irreducible characters. (See also Example 7.39.)

§10B. Mackey's Subgroup Theorem and Tensor Product Theorem

The results in this section were proved by Mackey [51] for representations of finite groups over fields of characteristic zero, and served as an introduction to the corresponding theorems on induced representations of locally compact groups.

As in §9A, we shall be concerned in this section with finite groups G and left RG -modules, where R is an arbitrary commutative ring. The extension of Mackey's results to the case of an arbitrary commutative coefficient ring will be crucial for J. A. Green's approach to modular representations of finite groups, as we shall see in §19.

Let H be a subgroup of G , and recall our notation for conjugates of elements of H :

$${}^a h = aha^{-1}, \quad h^b = b^{-1}hb = {}^{b^{-1}}h, \quad a, b \in G, h \in H.$$

Then

$${}^{ab} h = {}^a({}^b h), \quad h^{ab} = (h^a)^b.$$

Similarly, the conjugates ${}^a H$ and H^a of the subgroup H are defined by

$${}^a H = aHa^{-1} = H^{{a^{-1}}}, \quad a \in G.$$

In the theory of modules, it is sometimes convenient to change from left modules to right modules, and the same is true for notations involving conjugations. We shall give a one-sided version of most formulas, but it will be useful for the reader to become ambidextrous.

Now let L be a left RH -module, and let $a \in G$. The *conjugate* ${}^a L$ of L is the left $R({}^a H)$ -module, with underlying R -module L , and ${}^a H$ -action $*$ defined by

$${}^a h * l = h \cdot l, \quad h \in H, l \in L.$$

If L is R -free with a finite R -basis, and \mathbf{L} is the representation of H afforded by L , with character λ , we define the *conjugate representation* ${}^a \mathbf{L}$ and *conjugate character* ${}^a \lambda$ of ${}^a H$ by the formulas

$${}^a \mathbf{L}({}^a h) = \mathbf{L}(h), \quad {}^a \lambda({}^a h) = \lambda(h), \quad h \in H.$$

It is easily checked that these definitions are consistent with the definition of the conjugate module, so that ${}^a L$ affords the representation ${}^a \mathbf{L}$ of ${}^a H$, with character ${}^a \lambda$.

We collect a few useful facts about conjugates.

(10.12) Lemma. *Let H be a subgroup of G , and L a left RH -module.*

- (i) *If L is a submodule of $M|_H$ for some RG-module M , then aL is a left $R({}^a H)$ -module, and $aL \cong {}^a L$.*
- (ii) *$({}^a L)^G \cong L^G$ as RG-modules, for all $a \in G$.*
- (iii) *${}^a L \cong L$ as RH-modules if $a \in H$.*

Proof. (i) The map $\varphi: l \mapsto al$ is an R -isomorphism from L to aL . Moreover, $({}^a h)(al) = a(hl)$ for all $h \in H$, $l \in L$, so that aL is an $R({}^a H)$ -module. Finally, for $h \in H$ and $l \in L$, we have

$$\varphi({}^a h * l) = \varphi(hl) = ahl = {}^a h(al) = ({}^a h)\varphi(l),$$

as required.

(ii) Let $L^G = \bigoplus_{i=1}^n g_i \otimes L = \bigoplus_{i=1}^n g_i(1 \otimes L)$, for a set of left coset representatives $\{g_i\}_{1 \leq i \leq n}$ of H in G . Then $G = \cup g_i H$ implies that $G = \cup ag_i a^{-1} \cdot {}^a H$, and it follows that $\{ag_i a^{-1}\}_{1 \leq i \leq n}$ is a set of left coset representatives of ${}^a H$ in G . Moreover, we have

$$L^G = \bigoplus_{i=1}^n g_i(1 \otimes L) = \bigoplus_{i=1}^n ag_i(1 \otimes L) = \bigoplus_{i=1}^n (ag_i a^{-1})(a(1 \otimes L)).$$

From §9A, $1 \otimes L \cong L$ as left RH -modules, hence $a(1 \otimes L) \cong {}^a L$ by part (i) of this lemma. Finally, we have $L^G \cong ({}^a L)^G$ by Proposition 10.5.

(iii) The map $l \in {}^a L \rightarrow al \in L$ gives the desired isomorphism.

For the next result, and subsequently in this book, we shall use the notation $X \setminus G / Y$ to denote the (X, Y) -double cosets XgY of G relative to a pair of subgroups X and Y , and $X \setminus G$ for the right cosets $\{Xg\}_{g \in G}$, and G/Y for the left cosets $\{gY\}$. We shall also use the symbols H, X, Y, Z for subgroups of G , and L, M, N , etc., for modules.

(10.13) Subgroup Theorem. *Let X, Y be subgroups of G , and let L be a left RX -module. Then*

$$L^G|_Y \cong \bigoplus_{D=Y a X} ({}^a L|_{{}^a X \cap Y})^Y,$$

where the sum is taken over $Y \setminus G / X$. The summands are independent of the choice of the double coset representatives, in the sense that

$$({}^a L|_{{}^a X \cap Y})^Y \cong ({}^b L|_{{}^b X \cap Y})^Y$$

as RY -modules whenever $YaX = YbX$.

Note. In terms of our notations *ind* and *res*, the Theorem reads:

$$\text{res}_Y^G(\text{ind}_X^G(L)) \cong \bigoplus_{D=Y a X} \text{ind}_{{}^a X \cap Y}^Y (\text{res}_{{}^a X \cap Y}^X({}^a L)).$$

Proof. Letting $G = \bigcup_{i=1}^n g_i X$, we have

$$L^G = \bigoplus_{i=1}^n g_i \otimes L.$$

For each double coset $D \in Y \setminus G / X$, let

$$W(D) = \bigoplus_{g_i X \subseteq D} g_i \otimes L.$$

Then $W(D)$ is an RY -submodule of $L^G|_Y$, clearly independent of the choice of the coset representatives $\{g_i\}$. Moreover, we have

$$L^G|_Y = \bigoplus_D W(D).$$

It remains to work out the structure of the RY -modules $W(D)$. Let $D = YaX$, and let

$$Y = \bigcup s_j({}^a X \cap Y).$$

Then

$$YaX = \bigcup s_j({}^a X \cap Y) aX = \bigcup s_j aX,$$

because

$$saX = s'aX \Leftrightarrow s^{-1}s' \in {}^a X \cap Y.$$

Thus the elements $\{s_j a\}$ are representatives of the left X -cosets in D , and we have

$$W(D) = \bigoplus_j s_j a \otimes L = \bigoplus_j s_j(a(1 \otimes L)).$$

By Lemma 10.12, $a(1 \otimes L) \cong {}^a L$ as $R({}^a X)$ -modules; hence $a(1 \otimes L) \cong {}^a L$ as $R({}^a X \cap Y)$ -modules, so by Proposition 10.5, we have

$$W(D) \cong ({}^a L|_{{}^a X \cap Y})^Y.$$

Finally, the same argument proves that

$$W(D) \cong ({}^b L|_{{}^b X \cap Y})^Y$$

for any other $b \in D$, and the theorem is proved.

(10.14) Remarks. We give two illustrations of the use of the Subgroup Theorem.

(i) Let $X \trianglelefteq G$ (normal subgroup) and let L be an RX -module. Then, putting $Y = X$ in (10.13), we have

$$L^G|_X \cong \bigoplus_{aX \in G/X} {}^a L,$$

where the sum is taken over all cosets in G/X ; in this case, the conjugates ${}^a L$ are RX -modules because $X \trianglelefteq G$.

(ii) We apply the theorem to permutation representations (see Example 10.4). Let $X \leq G$. By (10.13),

$$(1_X)^G|_X \cong \bigoplus_{D=XaX} (1_{^aX \cap X})^X,$$

a direct sum of induced permutation representations. In terms of G -sets, we have the result that

$$\text{res}_X^G(G/X) \cong \coprod_{XaX \in X \setminus G / X} X/(^aX \cap X),$$

giving the decomposition of a transitive G -set G/X as a direct sum of transitive X -sets, where X is the stabilizer of a point in G/X . (See Chapter 5 for amplification of these remarks on G -sets.)

By Frobenius Reciprocity 10.9 and Exercise 10.2 we have

$$(1_X^G, 1_X^G)_G = (1_X, \{1_X^G\}|_X) = \sum_{XaX \in X \setminus G / X} (1_X, \{1_{^aX \cap X}\}^X) = |X \setminus G / X|,$$

where $|X \setminus G / X|$ is the number of (X, X) -double cosets in G .

The number $(1_X^G, 1_X^G)_G$ is called the *rank* of the transitive permutation representation 1_X^G , and the numbers $|X : {}^aX \cap X|$ corresponding to the degrees of the direct summands $(1_{^aX \cap X})^X$ of $(1_X^G)|_X$, the *subdegrees*. These numerical invariants provide a starting point for the decomposition of permutation representations (see §11D).

For the next result, we consider two subgroups H_1 and H_2 of G , and modules L_1 over RH_1 and L_2 over RH_2 . Let $H_1 \times H_2$ be the direct product of H_1 and H_2 .

(10.15) Definition. The *outer tensor product* $L_1 \# L_2$ of L_1 and L_2 is the $R(H_1 \times H_2)$ -module with underlying R -module $L_1 \otimes_R L_2$, and action of $H_1 \times H_2$ given by

$$(h_1, h_2) \cdot (l_1 \otimes l_2) = h_1 l_1 \otimes h_2 l_2.$$

In case $H_1 = H_2 = H$, the *(inner) tensor product* $L_1 \otimes L_2$ is the RH -module whose underlying R -module is $L_1 \otimes_R L_2$, with H -action given by

$$h(l_1 \otimes l_2) = h l_1 \otimes h l_2.$$

(10.16) Remark. Let L_1 and L_2 be RH -modules, and let H_0 be the diagonal subgroup of $H \times H$ consisting of all pairs $\{(h, h) : h \in H\}$ in $H \times H$. Then $H_0 \cong H$ under the isomorphism $(h, h) \mapsto h$; if we identify H_0 with H using this

isomorphism, then it is clear that

$$(L_1 \# L_2)|_{H_0} \cong L_1 \otimes L_2$$

as RH -modules. To put it another way, there is an R -isomorphism $L_1 \# L_2 \cong L_1 \otimes L_2$, which intertwines the actions of H_0 and H .

(10.17) Lemma. *The formation of outer tensor products commutes with induction. More precisely, let $H_1 \leq G_1$, $H_2 \leq G_2$, and let L_1 and L_2 be modules as in Definition 10.15. Then we have*

$$L_1^{G_1} \# L_2^{G_2} \cong (L_1 \# L_2)^{G_1 \times G_2} \text{ as } R(G_1 \times G_2)\text{-modules.}$$

Proof. We may identify $R(G_1 \times G_2)$ with $RG_1 \otimes RG_2$ as R -algebras. It is left to the reader to check that there is an isomorphism of $R(G_1 \times G_2)$ -modules

$$\varphi: R(G_1 \times G_2) \otimes_{R(H_1 \times H_2)} (L_1 \otimes_R L_2) \rightarrow (RG_1 \otimes_{RH_1} L_1) \otimes_R (RG_2 \otimes_{RH_2} L_2),$$

such that

$$\varphi(a \otimes b \otimes l_1 \otimes l_2) = a \otimes l_1 \otimes b \otimes l_2,$$

with the tensor products taken as indicated.

(10.18) Tensor Product Theorem. *Let $H_1, H_2 \leq G$, and let L_1 and L_2 be left modules over RH_1 and RH_2 , respectively. Then*

$$L_1^G \otimes L_2^G \cong \bigoplus_{x^{-1}y \in D} (({}^x L_1 \otimes {}^y L_2)|_{{}^x H_1 \cap {}^y H_2})^G,$$

where the sum extends over all (H_1, H_2) -double cosets D in G . There is one summand for each D ; namely, we choose a pair (x, y) with $x^{-1}y \in D$, and take the indicated summand. If also $u^{-1}v \in D$, then

$$(({}^x L_1 \otimes {}^y L_2)|_{{}^x H_1 \cap {}^y H_2})^G \cong (({}^u L_1 \otimes {}^v L_2)|_{{}^u H_1 \cap {}^v H_2})^G.$$

Proof. Let G_0 denote the diagonal subgroup of $G \times G$. Upon identifying G_0 with G using the map $(g, g) \mapsto g$, $g \in G$, we have an isomorphism of RG -modules

$$L_1^G \otimes L_2^G \cong (L_1 \# L_2)^{G \times G}|_{G_0},$$

by (10.16). We can now apply the Subgroup Theorem 10.13 to the right hand

side, using the following identifications:

Tensor Product Theorem	Subgroup Theorem
$G \times G$	G
$H_1 \times H_2$	X
G_0	Y
$L_1 \# L_2$	L

The result is that

$$(L_1 \# L_2)^{G \times G}|_{G_0} = \bigoplus_{\tilde{D}} {}^{(x,y)}(L_1 \# L_2)|_{(x,y)(H_1 \times H_2) \cap G_0}^{G_0},$$

where the sum is taken over double cosets

$$\tilde{D} = G_0(x, y)(H_1 \times H_2) \text{ in } G \times G.$$

It remains to translate the information on the right hand side from G_0 to G , using the isomorphism between them. We may identify ${}^{(x,y)}(L_1 \# L_2)$ with $(x, y) \otimes (L_1 \# L_2)$ in $(L_1 \# L_2)^{G_1 \times G_2}$, and hence there is an R -isomorphism, defined in Lemma 10.17, as follows:

$${}^{(x,y)}(L_1 \# L_2) \cong (x \otimes L_1) \otimes (y \otimes L_2) \subseteq L_1^G \otimes L_2^G.$$

The subgroup ${}^{(x,y)}(H_1 \times H_2) \cap G_0$ of $G_1 \times G_2$ corresponds to the subgroup ${}^x H_1 \cap {}^y H_2$ of G under the isomorphism from G_0 to G . Moreover, $x \otimes L_1 \approx {}^x L_1$ and $y \otimes L_2 \cong {}^y L_2$, so that we can identify the $R({}^{(x,y)}(H_1 \times H_2) \cap G_0)$ -module ${}^{(x,y)}(L_1 \# L_2)$ with the $R({}^x H_1 \cap {}^y H_2)$ -module $({}^x L_1 \otimes {}^y L_2)|_{{}^x H_1 \cap {}^y H_2}$, using the R -isomorphism given above. Hence the summand

$$\left({}^{(x,y)}(L_1 \# L_2) |_{{}^{(x,y)}(H_1 \times H_2) \cap G_0} \right)^{G_0} \text{ of } (L_1 \# L_2)^{G \times G}|_{G_0}$$

corresponds to the direct summand

$$\left(({}^x L_1 \otimes {}^y L_2) |_{{}^x H_1 \cap {}^y H_2} \right)^G \text{ of } L_1^G \otimes L_2^G.$$

Finally, we have to check that the $(G_0, H_1 \times H_2)$ -double cosets in $G \times G$ correspond to the (H_1, H_2) -double cosets in G . More precisely, we have to show that (x, y) and (u, v) belong to the same $(G_0, H_1 \times H_2)$ -double coset if and only if $H_1 x^{-1} y H_2 = H_1 u^{-1} v H_2$. Suppose

$$G_0(x, y)(H_1 \times H_2) = G_0(u, v)(H_1 \times H_2).$$

Then for some elements $h_1, h'_1 \in H_1$, $h_2, h'_2 \in H_2$, and $g, g' \in G$, we have

$$(gxh_1, gyh_2) = (g'u h'_1, g'v h'_2).$$

Upon eliminating g and g' from these equations, we obtain $H_1 x^{-1} y H_2 = H_1 u^{-1} v H_2$. The steps can be reversed, and our assertion is proved. This completes the proof of the theorem.

(10.19) Corollary. *Let H_1, H_2, G, L_1, L_2 be as in (10.18), and assume that L_1 and L_2 are R -free modules with finite bases, affording characters λ_1 and λ_2 of H_1 and H_2 , respectively. Then the modules $L_1^G, L_2^G, L_1^G \otimes L_2^G$ and $[({}^x L_1 \otimes {}^y L_2)|_{{}^x H_1 \cap {}^y H_2}]^G$ are all R -free modules with finite bases. The character $\lambda_1^G \lambda_2^G$ afforded by $L_1^G \otimes L_2^G$ is given by*

$$\lambda_1^G \lambda_2^G = \sum_{x^{-1}y \in D} \left[({}^x \lambda_1 {}^y \lambda_2)|_{{}^x H_1 \cap {}^y H_2} \right]^G,$$

where the sum is taken over the (H_1, H_2) -double cosets D . Moreover,

$$\left[({}^x \lambda_1 {}^y \lambda_2)|_{{}^x H_1 \cap {}^y H_2} \right]^G = \left[({}^u \lambda_1 {}^v \lambda_2)|_{{}^u H_1 \cap {}^v H_2} \right]^G$$

whenever $x^{-1}y$ and $u^{-1}v$ belong to the same double coset D .

The proof is immediate from Theorem 10.18, using the fact that the character of the inner tensor product of R -free RG -modules is the product of the characters of the factors. The fact that the modules L_1^G, L_2^G , etc., are R -free with finite basis follows from the discussion in §10A and the proof of the Subgroup Theorem.

Example. We interpret Corollary 10.19 in the context of permutation characters (see Example 10.4). Let H_1 and H_2 be subgroups of G , and 1_{H_1} and 1_{H_2} the R -characters of H_1 and H_2 afforded by the trivial modules. Then

$$1_{H_1}^G \cdot 1_{H_2}^G = \bigoplus_{x^{-1} \in D} (1|_{{}^x H_1 \cap H_2})^G,$$

where the sum is taken over the double cosets D in $H_1 \backslash G / H_2$. Thus the set of \mathbb{Z} -linear combinations of the induced permutation characters from subgroups of G is closed under multiplication, and is called the *Burnside ring* of G (see Chapter 5).

We conclude this section with a useful special case of the Tensor Product Theorem:

(10.20) Corollary. *Let L be a left RH -module, for a subgroup H of G , and let M be a left RG -module. Then there is an isomorphism of RG -modules:*

$$M \otimes_R L^G \cong (M_H \otimes_R L)^G.$$

§10C. The Intertwining Number Theorem

Our objective is to compute $\text{Hom}_{RG}(L_1^G, L_2^G)$, where L_1 is an RH_1 -module, L_2 , an RH_2 -module, with H_1 and H_2 subgroups of G . Throughout this subsection, G denotes a finite group and R an arbitrary commutative ring. We begin with a new version of the Frobenius Reciprocity Theorem:

(10.21) Proposition. *Let $H \leq G$, and let M be an RG -module, L an RH -module. Then there is an R -isomorphism*

$$\text{Hom}_{RG}(M, L^G) \cong \text{Hom}_{RH}(M_H, L).$$

Proof. Let $G = \bigcup_{i=1}^n g_i H$, $n = |G:H|$, $g_1 = 1$. Given $\varphi \in \text{Hom}_{RG}(M, L^G)$ we may write

$$\varphi(m) = \sum_{i=1}^n g_i \otimes \theta_i(m), \quad m \in M,$$

with each $\theta_i \in \text{Hom}_R(M, L)$. From the equation $g_i^{-1}\varphi(m) = \varphi(g_i^{-1}m)$ we obtain $\theta_1(g_i^{-1}m) = \theta_i(m)$, so

$$(10.22) \quad \varphi(m) = 1 \otimes \theta(m) + g_2 \otimes \theta(g_2^{-1}m) + \cdots + g_n \otimes \theta(g_n^{-1}m), \quad m \in M,$$

where θ denotes θ_1 . Clearly $\theta \in \text{Hom}_{RH}(M_H, L)$, and we claim that the desired isomorphism is given by $\varphi \rightarrow \theta$. It suffices to show that for each θ , formula (10.22) defines a G -homomorphism φ . For $x \in G$, we have

$$\varphi(xm) = \sum g_j \otimes \theta(g_j^{-1}xm), \quad x\varphi(m) = \sum xg_j \otimes \theta(g_j^{-1}m), \quad m \in M.$$

Write $xg_i = g_j h$, where $h \in H$; as i ranges from 1 to n , so does j . Further, for $m \in M$ we have

$$xg_i \otimes \theta(g_i^{-1}m) = g_j \otimes h\theta(g_i^{-1}m) = g_j \otimes \theta(hg_i^{-1}m) = g_j \otimes \theta(g_j^{-1}xm).$$

It follows that $\varphi(xm) = x\varphi(m)$ for all $x \in G$, $m \in M$, which completes the proof.

Using this, we obtain our first main result:

(10.23) Theorem. Let L_1 be an RH_1 -module, L_2 an RH_2 -module, where H_1 and H_2 are subgroups of G . For $x, y \in G$, the R -module

$$\text{Hom}_{R(xH_1 \cap {}^yH_2)}({}^xL_1, {}^yL_2)$$

depends only upon the double coset $D \in H_1 \backslash G / H_2$ to which $x^{-1}y$ belongs. Moreover,

$$\text{Hom}_{RG}(L_1^G, L_2^G) \cong \bigoplus_{x^{-1}y \in D} \text{Hom}_{R(xH_1 \cap {}^yH_2)}({}^xL_1, {}^yL_2)$$

as R -modules, where the sum is taken over all $D \in H_1 \backslash G / H_2$.

Proof. By the Subgroup Theorem and the two versions of the Frobenius Reciprocity Theorem, we have R -isomorphisms

$$\begin{aligned} \text{Hom}_{RG}(L_1^G, L_2^G) &\cong \text{Hom}_{RH_1}(L_1, L_2^G|_{H_1}) \\ &\cong \bigoplus_{D = H_1 a H_2} \text{Hom}_{RH_1}\left(L_1, \left\{{}^a L_2|_{H_1 \cap {}^a H_2}\right\}^{H_1}\right) \\ &\cong \bigoplus_D \text{Hom}_{R(H_1 \cap {}^a H_2)}(L_1, {}^a L_2). \end{aligned}$$

If we write $a = x^{-1}y$ and apply conjugation by x to all of the modules and subgroups occurring in the D -th summand above, we obtain the result in the originally-stated form.

Let us apply this result to the familiar situation where K is a subfield of the complex field, and is a splitting field for G and all its subgroups (as in §9C). Then (9.24iii) gives

$$\dim_K \text{Hom}_{KG}(M, M') = (\mu, \mu')_G,$$

where M and M' are f.g. left KG -modules affording characters μ and μ' , respectively. As an immediate consequence of (10.23), we obtain:

(10.24) Intertwining Number Theorem. Let K be a subfield of \mathbb{C} which is a splitting field for G and its subgroups, and let λ_i be the K -character of G afforded by a KH_i -module L_i , where $H_i \leq G$, $i = 1, 2$. Then

$$(\lambda_1^G, \lambda_2^G) = \sum_{x^{-1}y \in D} ({}^x\lambda_1, {}^y\lambda_2)_{xH_1 \cap {}^yH_2},$$

where the sum extends over $D \in H_1 \backslash G / H_2$.

As a corollary, we have

(10.25) Criterion for Irreducibility of Induced Characters. Let K be a splitting field for G as above, and let λ be an irreducible K -character of H . Then λ^G is an irreducible K -character of G if and only if

$$(\lambda, {}^x\lambda)_{H \cap {}^xH} = 0$$

for all $x \notin H$.

Proof. The criterion for irreducibility of λ^G is that $(\lambda^G, \lambda^G) = 1$, by (9.24ii). The equivalence of this statement with the assertion of (10.25) is immediate from the Intertwining Number Theorem.

§10D. Contragredient Modules

Throughout this section let G be a finite group and R an arbitrary commutative ring. An R -lattice is a f.g. projective left R -module. An RG -lattice is a left RG -module whose underlying R -module is an R -lattice.

The *dual* L^* of an R -lattice L is the R -module $\text{Hom}_R(L, R)$. The following lemma shows that duals of R -lattices are again R -lattices:

(10.26) Lemma. Let L and M be R -lattices. Then

- (i) $(L \oplus M)^* \cong L^* \oplus M^*$,
- (ii) L^* is an R -lattice,
- (iii) $(L^*)^* \cong L$,
- (iv) $\text{Hom}_R(L, M)$ and $L \otimes_R M$ are R -lattices.

Proof. (i) follows from the additivity of the Hom functor (see §2). Next, assertions (ii)–(iv) are easily checked when L and M are R -free R -lattices. Since direct summands of lattices are lattices, and since the expressions in (ii)–(iv) are additive in the variables involved, it follows that (ii)–(iv) are true for arbitrary lattices.

Given a left RG -lattice L , we wish to define an action of G on L^* so as to make L^* into a left RG -lattice. By (10.26ii), L^* is already an R -lattice, so we must make L^* into a left G -module. For $x \in G$ and $\varphi \in L^*$, define $x\varphi \in L^*$ by

$$(x\varphi)(l) = \varphi(x^{-1}l), \quad l \in L.$$

Then $(xy)\varphi = x(y\varphi)$ for all $x, y \in G$, $\varphi \in L^*$, so L^* is indeed a left RG -lattice, called the *contragredient* of L . The action of $\Sigma \alpha_x x \in RG$ on L^* is given by

$$\{(\Sigma \alpha_x x)\varphi\}l = \Sigma \alpha_x \varphi(x^{-1}l), \quad l \in L.$$

(10.27) Remarks. (i) Since L is an (RG, R) -bimodule, $\text{Hom}_R(L, R)$ acquires the structure of a *right* RG -module by virtue of the action of RG from the left on L (see §2A). We then use the anti-automorphism $\Sigma \alpha_x x \rightarrow \Sigma \alpha_x x^{-1}$ of RG to make $\text{Hom}_R(L, R)$ into a *left* RG -module, thereby obtaining the contragredient L^* of L .

(ii) It is easily verified that the isomorphisms in (10.26) are RG -isomorphisms in case L and M are RG -lattices.

When L is an R -free RG -lattice, affording the matrix representation \mathbf{L} of G with respect to an R -basis $\{l_i\}$ of L , we may compute the matrix representation afforded by the contragredient L^* as follows: let $\{\varphi_j\}$ be the dual basis of L^* , so $\varphi_j(l_i) = \delta_{ij}$. Relative to this basis $\{\varphi_j\}$, L^* affords the matrix representation \mathbf{L}^* , where

$$\mathbf{L}^*(x) = {}^t \mathbf{L}(x^{-1}), \quad x \in G,$$

and the superscript t denotes “transpose”. If L affords the character λ of G , and L^* affords λ^* , we have

$$\lambda^*(x) = \lambda(x^{-1}), \quad x \in G.$$

In particular, if L is a f.g. KG -module, where K is a subfield of the complex field as in §9C, then the contragredient character λ^* is given by

$$\lambda^*(x) = \overline{\lambda(x)}, \quad x \in G,$$

where bar denotes complex conjugation.

(10.28) Proposition. Let $H \leq G$, and let L be an RH -lattice. Then L^G , $(L^G)^*$ and $(L^*)^G$ are RG -lattices, and there is an RG -isomorphism

$$(L^G)^* \cong (L^*)^G.$$

Remark. If R is a subfield of the complex field, the character afforded by L^* is $\bar{\lambda}$, where L affords λ . In this case, the proposition is the simple fact that $\overline{\lambda^G} = (\bar{\lambda})^G$.

Proof. Let $G = \bigcup_{i=1}^n g_i H$, where $n = |G : H|$. As already pointed out in §10A, L^G is R -isomorphic to the direct sum of n copies of L , and is thus an R -lattice. Thus L^* and $(L^G)^*$ are also R -lattices by (10.26). We have R -module decompositions

$$L^G = \bigoplus_{i=1}^n g_i \otimes L, \quad (L^*)^G = \bigoplus_{i=1}^n g_i \otimes L^*.$$

For each i , $1 \leq i \leq n$, define $f_i: L^* \rightarrow (L^G)^*$ by

$$f_i(\varphi)(g_j \otimes l) = \delta_{ij}\varphi(l), \quad \delta_{ij} = \text{Kronecker delta.}$$

The map $F: (L^*)^G \rightarrow (L^G)^*$ given by

$$F(\sum g_i \otimes \varphi_i) = \sum f_i(\varphi_i)$$

is easily shown to be an R -isomorphism. To check that it is an RG -isomorphism, we must verify that

$$F(xg_i \otimes \varphi) = xf_i(\varphi) \text{ for all } x \in G, \varphi \in L^*.$$

As usual, write $xg_i = gh$ where $h \in H$ and $1 \leq j \leq n$; then

$$F(xg_i \otimes \varphi) = F(g_j \otimes h\varphi) = f_j(h\varphi).$$

For $1 \leq k \leq n$ and $l \in L$, we obtain

$$F(xg_i \otimes \varphi) \cdot (g_k \otimes l) = \{f_j(h\varphi)\} \cdot (g_k \otimes l) = \delta_{jk}(h\varphi)l = \delta_{jk}\varphi(h^{-1}l),$$

while

$$\{xf_i(\varphi)\} \cdot (g_k \otimes l) = f_i(\varphi) \cdot (x^{-1}g_k \otimes l) = \begin{cases} 0, & k \neq j, \\ \varphi(h^{-1}l), & k = j, \end{cases}$$

and the proof is completed.

An important consequence is as follows:

(10.29) Corollary. *The group ring RG is self-contragredient, that is, $(RG)^* \cong RG$ as left RG -modules. For each f.g. projective RG -module P , its contragredient P^* is also projective.*

Proof. The formula $(RG)^* \cong RG$ follows from (10.28), by taking $H = \{1\}$ and L the RH -module R on which H acts trivially. If P is projective, then $P \oplus Q = (RG)^{(n)}$ for some Q and n , whence P^* is a summand of $((RG)^*)^{(n)}$.

Given a pair of RG -lattices M and N , we constructed a new RG -lattice $M \otimes_R N$ by using the actions of G on M and N . There is an analogous construction in which we form the R -lattice $\text{Hom}_R(M, N)$, and let G act on it. Since G acts from the left on both M and N , it follows from §2A that $\text{Hom}_R(M, N)$ is naturally a (G, G) -bimodule. In order to make it into a *left* G -module, we define

$$(x * f)m = xf(x^{-1}m) \text{ for } x \in G, f \in \text{Hom}_R(M, N), m \in M.$$

Then $\text{Hom}_R(M, N)$ becomes a left RG -lattice (by linearity). Its relation to inner tensor products is given by

(10.30) Proposition. *Let M and N be left RG -lattices. Then*

$$M^* \otimes_R N \cong \text{Hom}_R(M, N)$$

as left RG -lattices.

Proof. We define a map

$$\theta: M^* \otimes_R N \rightarrow \text{Hom}_R(M, N)$$

by

$$f \otimes n \mapsto [f, n] \text{ for } f \in M^*, n \in N, \text{ where } [f, n]m = f(m)n \text{ for } m \in M.$$

Since M is an R -lattice, θ is an R -isomorphism by (2.32). We must verify that θ is a left G -homomorphism. For $x \in G$, we have

$$\theta\{x(f \otimes n)\} = \theta(xf \otimes xn) = [xf, xn].$$

For all $m \in M$,

$$[xf, xn]m = (xf)(m) \cdot xn = f(x^{-1}m)xn = xf(x^{-1}m)n.$$

On the other hand,

$$\{x * \theta(f \otimes n)\}m = (x * [f, n])m = x[f, n]x^{-1}m = xf(x^{-1}m)n.$$

This shows that θ is a left G -homomorphism, and establishes the Proposition.

We now introduce the functor

$$\text{inv}_G: {}_{RG}\mathcal{M} \rightarrow {}_R\mathcal{M}$$

which assigns to each RG -module M the R -module $\text{inv}_G(M)$ defined by

$$\text{inv}_G(M) = \{m \in M : xm = m \text{ for all } x \in G\}.$$

We call $\text{inv}_G(M)$ the module of G -invariants of M . It is clear from the definition that inv_G is a functor (see §2C).

The connection between the functor inv_G and Hom_{RG} , given in (ii) below, already occurred in a special case in Exercise 9.11.

(10.31) Proposition. (i) *Let $H \leq G$, and let L be an RH -lattice. Then*

$$\text{inv}_H(L) \cong \text{inv}_G(L^G)$$

as R -modules.

(ii) Let M and N be RG -lattices. Then

$$\text{inv}_G(M^* \otimes_R N) \cong \text{Hom}_{RG}(M, N)$$

as R -modules.

Proof. (i) If $G = \dot{\cup} g_i H$, then $L^G = \bigoplus g_i \otimes L$ by §10A. It is then easily checked that

$$\text{inv}_G(L^G) = (\Sigma g_i) \otimes \text{inv}_H(L),$$

which implies (i).

For (ii), use the isomorphism in (10.30), so

$$\text{inv}_G(M^* \otimes_R N) \cong \text{inv}_G \text{Hom}_R(M, N).$$

But an element $f \in \text{Hom}_R(M, N)$ is G -invariant if and only if $x * f = f$ for all $x \in G$, that is, $xfx^{-1} = f$ for all $x \in G$, and this in turn means that $f \in \text{Hom}_{RG}(M, N)$.

Each left RG -lattice M determines another left RG -lattice M^* , the contragredient of M . If L and M are left RG -lattices, then each $f \in \text{Hom}_{RG}(L, M)$ determines a map $f^* \in \text{Hom}_{RG}(M^*, L^*)$. Indeed, for each $\varphi \in M^*$ we have

$$f^*(\varphi) = \varphi f$$

(compare with §2A), and it is easily checked that f^* is an RG -homomorphism. The correspondence $M \rightarrow M^*$, $f \rightarrow f^*$, thus yields a contravariant functor from the category of left RG -lattices to itself. This functor is an involution, that is,

$$M^{**} \cong M, f^{**} \cong f.$$

It follows at once that there is an isomorphism of R -modules

$$(10.32) \quad \text{Hom}_{RG}(L, M) \cong \text{Hom}_{RG}(M^*, L^*),$$

given by $f \rightarrow f^*$, $f \in \text{Hom}_{RG}(L, M)$. This also follows from (10.31ii), since both sides of (10.32) are R -isomorphic to $\text{inv}_G(L^* \otimes_R M)$.

§10E. Outer Tensor Products

Throughout this subsection, K denotes an arbitrary field, and all modules which occur are assumed to be f.d./ K . Given a left KG -module M and a left KH -module N , we may form their *outer tensor product* $M \# N$. This is a left $K(G \times H)$ -module, defined as the K -vector space $M \otimes_K N$, on which the direct product $G \times H$ acts according to the formula

$$(g, h) \cdot \sum m_i \otimes n_i = \sum gm_i \otimes hn_i, g \in G, h \in H, m_i \in M, n_i \in N.$$

In §10B, we have already seen the importance of this concept. Our aim here is to study the relation between simple modules for G , H and $G \times H$.

Our first main result is that if the field K is a splitting field for both G and H , and if both M and N are simple modules, then $M \# N$ is also a simple module. Furthermore, in this case, every simple $K(G \times H)$ -module is of the form $M \# N$, with M and N unique up to isomorphism. (This generalizes the result of Exercise 9.6.) As Example 10.36 shows, the hypothesis on K cannot be omitted in general. We should emphasize the fact that the results given below are valid even when $\text{char } K$ divides $|G|$ or $|H|$.

As we shall see, these facts about simple modules over group algebras are special cases of more general results about modules over K -algebras A for which $A/\text{rad } A$ is a separable K -algebra. Group algebras have this property, as we have already proved in (7.10).

We begin with:

(10.33) Theorem. *Let K be a field which is a splitting field for the finite groups G and H . Then:*

- (i) *For each simple KG -module M and each simple KH -module N , the outer tensor product $M \# N$ is a simple $K(G \times H)$ -module.*
- (ii) *Every simple $K(G \times H)$ -module is of the above form $M \# N$, with M and N uniquely determined (up to isomorphism).*

Proof. We shall use the isomorphism of K -algebras

$$(10.34) \quad \text{End}_K(M \otimes N) \cong (\text{End}_K M) \otimes (\text{End}_K N),$$

where \otimes means \otimes_K , and M, N are any f.d. K -spaces. Now let M be a simple left KG -module; then the ring of left multiplications $(KG)_l$ on M coincides with $\text{End}_K M$ by Burnside's Theorem 3.32, since K is a splitting field for G . Likewise, $(KH)_l = \text{End}_K N$ as rings of operators on N . From (10.34) we obtain

$$\text{End}_K(M \otimes N) \cong (KG)_l \otimes (KH)_l.$$

But there is an obvious isomorphism of K -algebras

$$(10.35) \quad K(G \times H) \cong KG \otimes KH,$$

which we treat as an identification. Therefore

$$\text{End}_K(M \otimes N) \cong \{K(G \times H)\}_l.$$

Since $M \otimes N$ is simple as $\{\text{End}_K(M \otimes N)\}$ -module, it follows that $M \otimes N$ is simple as $K(G \otimes H)$ -module, so (i) is proved.

Now let M' and N' be simple KG - and KH -modules, respectively, such that

$$M' \# N' \cong M \# N \text{ as } K(G \times H)\text{-modules.}$$

Restricting the operator domain to $K(G \times 1)$, we obtain

$$(M')^{(n')} \cong M^{(n)} \text{ as } KG\text{-modules,}$$

where $n' = \dim_K N'$, $n = \dim_K N$. Since M is simple, it follows that $M' \cong M^{(k)}$ for some k . Likewise, $N' \cong N^{(j)}$ for some j . But then $k=j=1$, so $M' \cong M$, $N' \cong N$, as desired.

Finally, let $\{M_i : 1 \leq i \leq s\}$ be a basic set of simple left KG -modules, and let $\{N_j : 1 \leq j \leq t\}$ be a corresponding set for KH . To complete the proof of the theorem, we need to show that the st modules $\{M_i \# N_j\}$ are a basic set of simple $K(G \times H)$ -modules. This is clear from (3.37) when $\text{char } K=0$, since s and t are the number of conjugacy classes in G and H , respectively, while st is the corresponding number for $G \times H$. On the other hand, when $\text{char } K=p > 0$, the desired result follows from (17.11), since s and t are the number of p -regular conjugacy classes in G and H , respectively. This establishes the theorem. For another proof, see (10.38) below. Also see Exercise 9.6 for the case where $K=\mathbb{C}$.

Before generalizing the above theorem, let us give Serre's example to show that the hypothesis on K cannot be omitted.

(10.36) Example. Let $G = \{\pm 1, \pm i, \pm j, \pm k\}$ be the quaternion group of order 8, acting from the left on the skewfield of rational quaternions

$$\mathsf{H} = \mathbb{Q} \oplus \mathbb{Q}i \oplus \mathbb{Q}j \oplus \mathbb{Q}k.$$

By (7.40), H is a simple left $\mathbb{Q}G$ -module. Now let $H = \langle x \rangle$ be a cyclic group of order 3, and let

$$\xi = -(1+i+j+k)/2 \in \mathsf{H}.$$

Then $\xi^3 = 1$ in H , and we may let x act on H by right multiplication by ξ . Then H is a simple left $\mathbb{Q}(G \times H)$ -module, and H cannot be expressed in the form $M \# N$, with M and N simple $\mathbb{Q}G$ - and $\mathbb{Q}H$ -modules. For further discussion of this point, see the last paragraph in this subsection.

In the proof of Theorem 10.33, we needed to work with group algebras (rather than arbitrary f.d. K -algebras) in order to use (10.35), and also for counting the number of modules in a basic set of simple modules. We shall give a generalization of (10.33), whose proof is based on somewhat different ideas. This has the advantage of avoiding the counting argument, as well as providing information about what happens when K is not a splitting field.

As a first step, we prove an easy lemma:

(10.37) Lemma. *Let A and B be f.d. K -algebras, and let M and N be left A - and B -modules, respectively. Denote \otimes_K by \otimes , for brevity. Let $M \otimes N$ be the left $(A \otimes B)$ -module on which $A \otimes B$ acts by the formula*

$$(\sum a_i \otimes b_i)(\sum m_j \otimes n_j) = \sum a_i m_j \otimes b_i n_j.$$

Then

$$\text{End}_{A \otimes B}(M \otimes N) \cong (\text{End}_A M) \otimes (\text{End}_B N).$$

Proof. It suffices to prove that

$$\text{End}_{A \otimes B}(M \otimes N) \subseteq (\text{End}_A M) \otimes (\text{End}_B N),$$

the reverse inclusion being obvious. By (10.34), each $z \in \text{End}_{A \otimes B}(M \otimes N)$ is expressible as

$$z = \sum \alpha_i \otimes \beta_i, \quad \alpha_i \in \text{End}_K M, \quad \beta_i \in \text{End}_K N,$$

where we may assume the $\{\beta_i\}$ are linearly independent over K . For each $a \in A$, we have $(a \otimes 1)z = z(a \otimes 1)$, so

$$\sum (a\alpha_i - \alpha_i a) \otimes \beta_i = 0 \text{ for all } a \in A.$$

Therefore

$$a\alpha_i = \alpha_i a \text{ for each } i \text{ and for all } a \in A,$$

and thus each $\alpha_i \in \text{End}_A M$. We may now rewrite z as

$$z = \sum \lambda_j \otimes \mu_j, \quad \lambda_j \in \text{End}_A M, \quad \mu_j \in \text{End}_K N,$$

with the $\{\lambda_j\}$ linearly independent over K . The preceding argument then shows that each $\mu_j \in \text{End}_B N$, and the lemma is established.

Our second main result, which includes (10.33) as a special case, is as follows:

(10.38) Theorem. *Let A and B be f.d. K -algebras such that both $A/\text{rad } A$ and $B/\text{rad } B$ are separable K -algebras. Let \otimes denote \otimes_K . Then*

(i) *For each simple A -module M and each simple B -module N , the $(A \otimes B)$ -module $M \otimes N$ is semisimple. Furthermore, $M \otimes N$ is a simple $(A \otimes B)$ -module if and only if*

$$(\text{End}_A M) \otimes_K (\text{End}_K N) \text{ is a division algebra.}$$

(ii) If either $A/\text{rad } A$ or $B/\text{rad } B$ is a split semisimple K -algebra, then for each simple A -module M and each simple B -module N , $M \otimes N$ is a simple $(A \otimes B)$ -module.

(iii) Under the hypotheses of (ii), every simple $(A \otimes B)$ -module is of the form $M \otimes N$, with M and N as above. Further, if $M' \otimes N' \cong M \otimes N$, then $M' \cong M$ and $N' \cong N$.

Proof. Let $\bar{A} = A/\text{rad } A$, $\bar{B} = B/\text{rad } B$, so \bar{A} and \bar{B} are f.d. separable K -algebras, by hypothesis. Then $\bar{A} \otimes \bar{B}$ is also a separable K -algebra, by Exercise 7.1. Let us show that

$$(10.39) \quad \bar{A} \otimes \bar{B} \cong (A \otimes B)/\text{rad}(A \otimes B).$$

We note first that the homomorphism theorem implies:

$$\bar{A} \otimes \bar{B} \cong (A \otimes B)/\{(\text{rad } A) \otimes B + A \otimes (\text{rad } B)\}.$$

The denominator (on the right hand side above) is a nilpotent ideal of $A \otimes B$, and is therefore contained in $\text{rad}(A \otimes B)$. On the other hand, this denominator contains $\text{rad}(A \otimes B)$, since $\bar{A} \otimes \bar{B}$ is separable (and therefore semisimple). This establishes formula (10.39).

Now let $\{M_i\}$ be a basic set of simple left A -modules, and let $\{N_j\}$ be a basic set of simple left B -modules. There are isomorphisms (of modules):

$$\bar{A} \cong \coprod M_i^{(m_i)}, \quad \bar{B} \cong \coprod N_j^{(n_j)}.$$

Therefore

$$\bar{A} \otimes \bar{B} \cong \coprod_{i,j} (M_i \otimes N_j)^{(m_i, n_j)}.$$

It follows at once from (10.39) that each $M_i \otimes N_j$ is a semisimple $(A \otimes B)$ -module, so the first part of (i) is proved. However, once we know that $M_i \otimes N_j$ is semisimple, we can test whether it is simple by calculating its endomorphism ring $\text{End}_{A \otimes B}(M_i \otimes N_j)$; indeed, by Exercise 3.7, $M_i \otimes N_j$ is simple if and only if this ring is a division algebra. Taking (10.37) into account, the proof of (i) is completed.

(ii) Suppose that $A/\text{rad } A$ is a split semisimple K -algebra. Then $\text{End}_A M \cong K$, while $\text{End}_B N$ is a division algebra D . Therefore

$$(\text{End}_A M) \otimes (\text{End}_B N) \cong K \otimes D \cong D,$$

so $M \otimes N$ is a simple module. Finally, (iii) follows at once from (ii), since every simple $(A \otimes B)$ -module occurs as a direct summand of $\bar{A} \otimes \bar{B}$, and is

therefore of the form $M_i \otimes N_j$ for some i and j . This completes the proof of the Theorem, since the uniqueness assertion follows as in the proof of (10.33).

We may now analyze Example 10.36 in more detail. Let $M = Q \oplus Qi \oplus Qj \oplus Qk$, viewed as left QG -module; then $\text{End}_{QG} M \cong H$, the skewfield of rational quaternions. The simple QH -modules are Q and $Q(\omega)$, where ω is a primitive cube root of 1, and where x acts as 1 and ω , respectively, on these modules. If $N = Q(\omega)$, then $\text{End}_{QH} N \cong Q(\omega)$, and

$$\text{End}_{Q(G \times H)}(M \# N) \cong H \otimes_Q Q(\omega).$$

It is easily verified that

$$H \otimes_Q Q(\omega) \cong M_2(Q(\omega)),$$

and therefore $M \# N \cong W \oplus W$, where W is a simple $Q(G \times H)$ -module. (In fact, W is precisely the module constructed in Example 10.36).

§10. Exercises

Throughout these exercises, R denotes a commutative ring, G is a finite group, and K is a field of characteristic 0 which is a splitting field for G and all of its subgroups.

- Let G be a finite group of order n , and R a commutative ring. Let $1_{\{1\}}$ denote the trivial R -representation of the trivial subgroup $\{1\}$. Prove that the induced representation $1_{\{1\}}^G$ is equivalent to the representation afforded by the left regular module RG . Further, prove that RG affords a matrix representation $U: G \rightarrow M_n(R)$, where

$$U(g) = (\delta_{g_i, gg_j})_{1 \leq i, j \leq n}, \quad g \in G,$$

and $G = \{g_1, \dots, g_n\}$.

[Hint: Compare $U(g)$ with the matrix (10.1).]

- Let G be a finite group, Ω a G -set, and K a splitting field of characteristic zero, as in §9C. Let θ be the character of the permutation representation of G on Ω (see (10.4)); we shall call θ the *permutation character* associated with the G -set Ω .

- For each $x \in G$, prove that $\theta(x)$ is the number of points in Ω fixed by x , so

$$\theta(x) = \text{card}\{w \in \Omega : xw = w\}.$$

- Prove that the scalar product $(\theta, 1_G)$ is the number of G -orbits in Ω , where 1_G is the trivial character of G . In particular, show that Ω is a transitive G -set if and only if $(\theta, 1_G) = 1$.

- If Ω and Ω' are transitive G -sets with permutation characters θ and θ' , respectively, prove that $\theta\theta'$ is the character of the G -set $\Omega \times \Omega'$ with diagonal action of

G . Hence

$$(\theta, \theta') = (\theta\theta', 1_G) = \text{number of } G\text{-orbits in } \Omega \times \Omega'.$$

As an application, show that if $X, Y \leq G$, then

$$(1_X^G, 1_Y^G) = \text{card}\{X \setminus G / Y\}.$$

3. Keep the notation of Exercise 2. A transitive G -set Ω is called *2-transitive* (or *doubly transitive*) if for any two ordered pairs $(u, v), (u', v')$ from $\Omega \times \Omega$, with $u \neq v, u' \neq v'$, there exists $g \in G$ such that $gu = u'$ and $gv = v'$.

(i) Prove that Ω is 2-transitive if and only if $(\theta, \theta) = 2$, or equivalently, if and only if $\text{card}\{H \setminus G / H\} = 2$, where θ is the permutation character and $H = \text{Stab}_G w$ for some $w \in \Omega$.

(ii) Prove that if Ω is 2-transitive, then

$$\theta = 1_G + \zeta$$

for some non-trivial character $\zeta \in \text{Irr}_K G$.

4. (Gluck). Let $G = GL_3(k)$, where k is a finite field, and let Ω be the left G -set consisting of all nonzero 3×1 column vectors over k . The stabilizer of

$$e_1 = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} \in \Omega \text{ is } H = \left\{ \begin{bmatrix} 1 & * & * \\ 0 & * & * \\ 0 & * & * \end{bmatrix} \in G \right\}.$$

Now G acts transitively on Ω , so $\Omega \cong G/H$ as left G -sets, by §1B. For $g \in G$, we have

$$1_H^G(g) = \text{card}\{w \in \Omega : (g-1)w = 0\}.$$

Now let Ω' be the set of nonzero 1×3 row vectors, and view Ω' as a left G -set with action given by

$$gw' = w'g^{-1}, \quad g \in G, w' \in \Omega'.$$

The stabilizer of $(1, 0, 0)$ in G is

$$H' = \left\{ \begin{bmatrix} 1 & 0 & 0 \\ * & * & * \\ * & * & * \end{bmatrix} \in G \right\}.$$

Show that H' is not G -conjugate to H , since H' does not stabilize any element of Ω . For $g \in G$, show that

$$1_H^G \cong 1_{H'}^G,$$

but the G -sets G/H and G/H' are not isomorphic.

5. Let H be a subgroup of G , and ψ a K -character of H . Let $x \in G$, and let \mathfrak{C} be the conjugacy class containing x . Prove that

$$\psi^G(x) = \frac{|C_G(x)|}{|H|} \sum_{y \in \mathfrak{C} \cap H} \psi(y).$$

6. Prove that the Frobenius Reciprocity Formula characterizes induction of class functions. In other words, show that if $\psi \in \text{cf}_K H$ and $\psi' \in \text{cf}_K G$ satisfy the condition

$$(\psi', \xi) = (\psi, \xi_H)$$

for all $\xi \in \text{cf}_K G$, then $\psi' = \psi^G$.

7. (Janusz [66]). Let $H \leq G$, $\xi \in \text{Irr}_K G$, and $\psi \in \text{Irr}_K H$. Assume that $(\xi, \psi^G) = 1$. Let e be the central primitive idempotent in KG corresponding to ξ , and e a primitive idempotent in KH such that KHe affords ψ . Prove that the left ideal KGe affords ψ^G , and that ee is a primitive idempotent in KG such that $KGee$ affords ξ .

[Hint: First show that $KGe \cong KG \otimes_{KH} KHe$, so KGe affords ψ^G . Then show that $eKGe = KGee$ is the homogeneous component of KGe which is the sum of all simple submodules of KGe affording ξ .] (See (11.27) for another proof.)

8. Let $H \trianglelefteq G$. Prove that $1_H^G = \tilde{\rho}_{G/H}$, where $\tilde{\rho}_{G/H}$ is the lift of the regular character of G/H (see Exercise 9.3).

9. Let $H \trianglelefteq G$, and let $\psi \in \text{Irr}_K H$. Then for each $x \in G$, the conjugate character ${}^x\psi \in \text{Irr}_K H$. Prove that $\psi^G \in \text{Irr}_K G$ if and only if $\psi \neq {}^x\psi$ for all $x \notin H$.

[Hint: Use (10.25).]

10. Apply the preceding exercise to give an alternative construction of $\text{Irr}_K G$, for G the dihedral group of order $2m$ (see (10.11)). Apply the same method to determine $\text{Irr}_K G$ for the generalized quaternion group Q_m of order $4m$.

11. Apply the Tensor Product Theorem 10.18 to decompose products of irreducible characters of the dihedral group D_m (as in (10.11)) into their irreducible constituents. (See also CR §48.)

12. Find the character tables of the symmetric and alternating groups S_4 and A_4 .

[Hint: Find proper normal subgroups, and study the induced characters from these normal subgroups, and the characters having the normal subgroup contained in their kernels.]

13. Let $H \leq G$. Prove that if M is a simple KG -module, then $M \mid L^G$ for some simple KH -module. (Here, as usual, $M \mid L^G$ means that M is isomorphic to a direct summand of L^G .) Apply this result to show that for every $\xi \in \text{Irr}_K G$, $\deg \xi \leq |G : A|$, where A is an arbitrary abelian subgroup of G .

14. Let $H \leq G$, and let L be the KH -module K , on which H acts in some way (in other words L affords a *linear representation* of H). Call L^G a *monomial representation*

of G . Prove that for each subgroup S of G , $(L^G)_S$ is a direct sum of monomial representations of S .

From this point on, R denotes a commutative ring, and H a subgroup of G .

15. For an RG -module M , show that the G -trivial submodule of M is R -isomorphic to $\text{Hom}_{RG}(R, M)$, where G acts trivially on R .

16. (D. G. Higman [55a]). Let $H \leq G$, and let L be a left RH -module. Consider a left RG -module $i(L)$ with the following properties:

(i) There exists an RH -homomorphism $\lambda: L \rightarrow i(L)$ such that $i(L)$ is generated over RG by $\lambda(L)$;

(ii) For each RH -homomorphism $\mu: L \rightarrow M_H$ from L into M_H , where M is any RG -module, there exists a homomorphism of RG -modules $\hat{\mu}: i(L) \rightarrow M$ such that $\hat{\mu}\lambda = \mu$.

Prove that λ is an isomorphism, and that $i(L) \cong L^G$ as RG -modules.

[Hint: Prove that any two modules $i(L)$ and $i'(L)$ satisfying conditions (i) and (ii) are RG -isomorphic. Then show that L^G satisfies these conditions, where $\lambda: L \rightarrow L^G$ is the homomorphism $L \rightarrow 1 \otimes L$.]

17. (Mackey [51]). Keep the notation of the preceding exercise. Show that $\text{Hom}_{RH}(RG, L)$ becomes a left RG -module if we define

$$(xf)(y) = f(yx), \quad x, y \in G, f \in \text{Hom}_{RH}(RG, L).$$

Define a map $\lambda: L \rightarrow \text{Hom}_{RH}(RG, L)$ by setting $\lambda(l) = f_l$, $l \in L$, where f_l is the element of $\text{Hom}_{RH}(RG, L)$ such that $f_l(1) = l$. Prove that λ satisfies conditions (i) and (ii) of Exercise 16, and hence that $\text{Hom}_{RH}(RG, L) \cong L^G$ as RG -modules.

18. Let M be a left RG -module which is R -free on r generators. Then the inner tensor product $RG \otimes_R M$ is RG -free on r generators.

[Hint: Apply (10.20), with $L = 1_H$, $H = \{1\}$, $L^G = RG$ (see Exercise 1). Then we have

$$RG \otimes M \cong 1_H^G \otimes M \cong (1_H \otimes M_H)^G$$

by (10.20), since the inner tensor product is a commutative operation. Then $1_H \otimes M_H$ is a direct sum of r copies of 1_H , and the result follows from (2.17).]

19. Let M be a left RG -lattice. Prove that the inner tensor product $RG \otimes_R M$ is RG -projective.

[Hint: Let M' be a G -trivial R -module such that $M \amalg M'$ is R -free. Then use the preceding exercise to show that $RG \otimes (M \amalg M')$ is RG -free.]

20. Given an exact sequence $L \rightarrow M \rightarrow N$ of RH -modules, show that the sequence of RG -modules $L^G \rightarrow M^G \rightarrow N^G$ is also exact.

[Hint: RG is RH -free, hence flat as RH -module.]

21. Let L, M be left RG -lattices. Prove that

$$(L \otimes_R M)^* \cong L^* \otimes_R M^*$$

as RG -modules, where L^* is the contragredient of L , and M^* that of M .

22. Let L, M and N be left RG -lattices, and let L^*, M^* and N^* be their contragredients.

(i) Show that if

$$(\xi) \quad 0 \rightarrow L \rightarrow M \rightarrow N \rightarrow 0$$

is an exact sequence of left RG -lattices, then so is

$$(\xi^*) \quad 0 \rightarrow N^* \rightarrow M^* \rightarrow L^* \rightarrow 0.$$

(ii) Deduce from the above that the sequence (ξ) is exact if and only if the sequence (ξ^*) is exact.

(iii) Show that (ξ) is split if and only if (ξ^*) is split.

[Hint: Use the fact that $\text{Hom}_R(\cdot, R)$ preserves exactness of exact sequences of R -lattices, and that $L^{**} \cong L$ as RG -lattices.]

23. Show that the group algebra EG of a finite group G over an arbitrary field E is injective (as left EG -module).

[Hint: By (2.23), EG is injective if and only if each exact sequence

$$0 \rightarrow EG \rightarrow X \rightarrow Y \rightarrow 0,$$

with X, Y f.g. EG -modules, is split. But X and Y are EG -lattices, since E is a field. Then $0 \rightarrow Y^* \rightarrow X^* \rightarrow (EG)^* \rightarrow 0$ is exact, and $(EG)^* \cong EG$, by (10.29).] (See §9A and §19A for other proofs.)

24. Deduce from the preceding exercise that if E is a field, then every f.g. projective EG -module is injective.

25. Returning to modules over a commutative ring R , show that any exact sequence

$$0 \rightarrow RG \rightarrow X \rightarrow Y \rightarrow 0,$$

in which X and Y are RG -lattices, is RG -split. Hence $\text{Ext}_{RG}^1(Y, RG) = 0$ for each RG -lattice Y . Deduce that each sequence of RG -lattices

$$0 \rightarrow M \rightarrow X \rightarrow Y \rightarrow 0$$

in which M is RG -projective, necessarily splits.

[Hint: Imitate the proof of Exercise 23. Further $M|(RG)^{(n)}$ for some n , so $\text{Ext}_{RG}^1(Y, M)$ is a summand of $\text{Ext}_{RG}^1(Y, RG^{(n)})$.]

26. Show that every RG -lattice can be embedded in a free RG -module on a finite number of generators.

[Hint: For a left RG -lattice L , let L^* be its contragredient. Then $(RG)^{(n)}$ maps onto L^* , for some n . Now use Exercise 22 and (10.29).]

27. Show that every injective RG -lattice M is RG -projective.

[Hint: By Exercise 26, M can be embedded in $(RG)^{(n)}$ for some n , so $M|(RG)^{(n)}$.]

§11. DECOMPOSITION OF INDUCED MODULES. CLIFFORD THEORY AND HECKE ALGEBRAS

The decomposition of induced modules and characters is one of the most powerful methods for constructing irreducible representations of finite groups. For modules induced from normal subgroups, the main results are due to Frobenius, Clifford and Gallagher, and are presented in §11A, B. In some cases (see §11B), one can use these methods to construct all irreducible characters for certain families of groups. In §11C, one of Clifford's theorems is presented in a generalized form due to Tucker, Conlon and Ward. This result leads to the theory of projective representations, and in §11E we discuss some of Schur's results relating projective representations to central extensions of finite groups. The decomposition of induced modules from arbitrary subgroups is discussed in §11D, following Curtis-Fossum, Ree and D. Higman. These methods will play an important role in the representation theory of finite groups of Lie type, to come in Volume II.

§11A. Clifford's Theorem

The analysis of representations of a finite group G over a field K , in terms of induced representations, is simplified in case G has a normal subgroup.

(11.1) Clifford's Theorem (Clifford [37]). *Let K be an arbitrary field, H a normal subgroup of a finite group G , M a simple KG -module, and L a simple KH -submodule of $\text{res}_H^G(M)$. Then the following statements hold:*

(i) *$\text{res}_H^G(M)$ is a semisimple KH -module, and is isomorphic to a direct sum of conjugates of L .*

(ii) *The KH -homogeneous components of $\text{res}_H^G(M)$ are permuted transitively by G .*

(iii) *Let \tilde{L} be the KH -homogeneous component of $\text{res}_H^G(M)$ containing L , and let $\tilde{H} = \{x \in G : x\tilde{L} = \tilde{L}\}$, the stabilizer of \tilde{L} . Write G as a disjoint union $G = \bigcup_{i=1}^n g_i \tilde{H}$. Then $\{g_i L : 1 \leq i \leq n\}$ is a complete set of non-isomorphic con-*

jugates of L , and each appears with the same multiplicity e in $\text{res}_H^G(M)$:

$$\text{res}_H^G(M) \cong \left(\bigoplus_{i=1}^n g_i L \right)^{(e)}.$$

(iv) *Let \tilde{L} and \tilde{H} be as in (iii). Then \tilde{L} is a $K\tilde{H}$ -module, and*

$$M \cong \text{ind}_{\tilde{H}}^G(\tilde{L}).$$

Proof. (i) Let L be a simple submodule of $\text{res}_H^G(M)$, as above. For each $x \in G$, $xL \cong {}^xL$ as KH -modules, by Lemma 10.12 and the fact that ${}^xH = H$ because $H \trianglelefteq G$. We observe next that $\sum_{x \in G} xL$ is a KG -submodule of M , and hence coincides with M because M is simple. Thus M_H is a sum of conjugates $\{xL\}$ of L , and the conjugates $\{xL\}$ are clearly simple KH -modules. By (3.12), M_H is semisimple, and the proof of (3.12) shows that M is a direct sum of conjugates $\{xL\}$ of L , completing the proof of (i).

(ii) Let us prove that the RH -homogeneous components of $\text{res}_H^G(M)$ are permuted by G . Let L' and L'' be simple KH -submodules of $\text{res}_H^G(M)$. It suffices to prove that if $\varphi: L' \rightarrow L''$ is a KH -isomorphism, then $xL' \cong {}_xL''$ as KH -modules for each $x \in G$. But clearly $x\varphi x^{-1}: xL' \rightarrow {}_xL''$ is a K -isomorphism. It is also an H -isomorphism, since for $h \in H$, $l' \in L'$, we have

$$(x\varphi x^{-1})hx l' = x(x^{-1}hx)\varphi l' = h[(x\varphi x^{-1})x l'],$$

as required.

Now let \tilde{L} denote the homogeneous component of $\text{res}_H^G(M)$ containing L , so \tilde{L} is the direct sum of those summands xL of M which are KH -isomorphic to L . Then $x\tilde{L}$ is also a homogeneous component for each $x \in G$, and $\sum_{x \in G} x\tilde{L}$ is a KG -submodule of M . Therefore $\sum_{x \in G} x\tilde{L} = M$, and it follows from (3.20) that every homogeneous component of $\text{res}_H^G(M)$ is a translate $x\tilde{L}$ of \tilde{L} by some element $x \in G$. We have shown that G acts transitively on the homogeneous components of $\text{res}_H^G(M)$, completing the proof of (ii).

(iii) From part (ii), the homogeneous components of $\text{res}_H^G(M)$ form a single orbit under the action of G . Let \tilde{L} be a fixed homogeneous component, and \tilde{H} its stabilizer as defined in (iii). Then the elements of the G -orbit of \tilde{L} are in bijective correspondence with any set of left coset representatives $\{g_1, \dots, g_n\}$ of G/H , and we have

$$\text{res}_H^G(M) = \bigoplus_{i=1}^n g_i \tilde{L}.$$

From the proof of (ii), it follows that every conjugate of L is isomorphic to

some $g_i L$, where $1 \leq i \leq n$. Finally, since $M = g_i M$, the multiplicity of $g_i L$ in $g_i \tilde{L}$ is the same as the multiplicity e of L in \tilde{L} , and the proof of (iii) is completed.

(iv) From (iii), M , \tilde{L} and \tilde{H} satisfy the conditions of Proposition 10.5, so $M \cong \text{ind}_{\tilde{H}}^G(\tilde{L})$ as required.

The preceding result expresses every simple KG -module M as an induced module $\text{ind}_{\tilde{H}}^G(\tilde{L})$ for some subgroup \tilde{H} such that $H \leq \tilde{H} \leq G$. The problem of determining all simple KG -modules is thus reduced to the corresponding problem for proper subgroups of G , except when $\tilde{H} = G$. We are then led to two problems. First, to find in what circumstances the group \tilde{H} can be taken to be a proper subgroup of G . Second, to investigate what can be done in case the situation $\tilde{H} = G$ cannot be avoided. When K is algebraically closed, the second problem leads to a factorization of the representation afforded by M as a tensor product of projective representations (CR §51). An improved version of this construction will be given later, first for characters (in §11B), and then for modules (in §11C). We conclude this section with some important cases where a favorable solution of the first problem is possible.

(11.2) Proposition (Blichfeldt). *Let K be an algebraically closed field, and M a f.d. vector space over K . Let G be a finite subgroup of $GL(M)$ which acts irreducibly on M (so that M is a simple KG -module), and let A be an abelian normal subgroup of G not contained in the center of G . Let L be a simple submodule of $\text{res}_A^G(M)$, \tilde{L} a KA -homogeneous component of $\text{res}_A^G(M)$, and \tilde{A} the stabilizer of \tilde{L} as in Theorem 11.1. Then $\tilde{A} < G$, and $M \cong \text{ind}_{\tilde{A}}^G(\tilde{L})$.*

Proof. Because of Theorem 11.1, it is sufficient to prove that $\tilde{L} \neq M$. Since K is algebraically closed and A is abelian, we have $\dim_K L = 1$. By (11.li), $\text{res}_A^G(M)$ is a direct sum of conjugates of L . If $\tilde{L} = M$, the conjugates of L are mutually isomorphic as KA -modules, whence each $a \in A$ has the form $a = \alpha \cdot 1_M$ for some $\alpha \in K$. But this contradicts the assumption that A is not contained in the center of G , and the result is proved.

A KG -module M is called *imprimitive* if $M = \text{ind}_H^G(L)$ for some KH -module L , with H a proper subgroup of G ; call M *primitive* if it cannot be expressed in this way. We may thus refer to the preceding result as *Blichfeldt's Criterion for Imprimitivity*. We use this criterion to prove that if G is nilpotent, then every simple KG -module is imprimitive.

(11.3) Theorem. *Let G be a finite nilpotent group, and let K be an algebraically closed field. Every simple KG -module M can be expressed in the form $M = \text{ind}_H^G(L)$ for some subgroup $H \leq G$ and some one-dimensional KH -module L .*

Proof. We require two facts from elementary group theory (see §1):

- (i) Subgroups and homomorphic images of nilpotent groups are nilpotent.
- (ii) If G is nilpotent and not abelian, then there exists an abelian normal subgroup A not contained in the center $Z(G)$.

Let M be a simple KG -module, and let G_I be the homomorphic image of G consisting of all left multiplications $\{x_I : x \in G\}$ on M . Then $G_I \leq GL(M)$, and is either abelian, in which case $\dim_K M = 1$, or else G_I has a proper abelian normal subgroup not contained in the center. In the latter case, Blichfeldt's criterion (11.2) implies that $M = \text{ind}_{H_I}^G(L)$ for some subgroup $H_I < G_I$, and some KH_I -module L . But H_I comes from some subgroup $H < G$ by the homomorphism theorem, and L is then a KH -module. By (10.5) we have $M \cong \text{ind}_H^G(L)$. Using induction on $|G|$, we may assume that $L = \text{ind}_{H_1}^H(L_1)$ for a subgroup $H_1 \leq H$, and a one-dimensional KH_1 -module L_1 . By transitivity of induction (10.6), we have

$$M \cong \text{ind}_H^G(L) = \text{ind}_H^G(\text{ind}_{H_1}^H(L_1)) \cong \text{ind}_{H_1}^G(L_1),$$

completing the proof of the theorem.

The preceding theorem shows the importance of studying representations of G induced from one-dimensional representations of subgroups of G . Such induced representations are called *monomial representations* (see Exercise 10.14). Finite groups with the property that every simple module is induced from a one-dimensional module, as in Theorem 11.3, are called *M-groups* (for *monomial* groups). *M-groups* are always solvable (CR §53), but not every solvable group is an *M-group*. For further discussion of *M-groups*, see Exercises 11.1 and 11.2, as well as Huppert [67, Chapter V, §18].

§11B. Applications of Clifford's Theorem to Character Theory

We shall investigate the character-theoretic implications of Clifford's Theorem, particularly in the more difficult case in which the submodule L (in (11.1)) is isomorphic to all its conjugates.

In this section, we assume that K is a splitting field for a finite group G and all its subgroups, and that K is contained in the complex field; thus scalar products of characters can be related to multiplicities (see (9.24)). As in §9C, we use the notation $\text{Irr}_K(G)$ to denote the set of irreducible K -characters of G . The discussion to follow is based on a paper of Gallagher [62b].

Let $H \trianglelefteq G$, and let ψ be a K -character of H . Then for $x \in G$, the *conjugate* ${}^x\psi$ is also a K -character of H . We denote by G_ψ the *stabilizer* of ψ , defined by

$$G_\psi = \{x \in G : {}^x\psi = \psi\}.$$

Note that G_ψ is a subgroup containing H . Further, from (11.1iii) it follows that if L is a KH -module affording ψ , then G_ψ can also be characterized as

$$G_\psi = \{x \in G : {}^x L \cong L \text{ as } KH\text{-modules}\}.$$

(11.4) Proposition. (i) Let $\xi \in \text{Irr}_K(G)$, and let $H \trianglelefteq G$. Then

$$\xi|_H = e \left(\sum {}^x \psi \right),$$

where e is a positive integer, $\psi \in \text{Irr}_K(H)$, and the sum is taken over the distinct G -conjugates of ψ .

(ii) Let $\psi \in \text{Irr}_K(H)$, and let G_ψ be the stabilizer of ψ in G . For each $\xi \in \text{Irr}_K(G)$ such that $(\xi, \psi^G) > 0$, there exists an $\eta \in \text{Irr}_K(G_\psi)$ with the properties

$$\eta|_H = r\psi \text{ for some positive integer } r, \text{ and } \xi = \eta^G.$$

Remark. By Exercise 11.3, the above character η is the unique character $\eta \in \text{Irr}_K(G_\psi)$ satisfying the conditions that $(\eta^G, \xi) > 0$ and $(\eta, \psi^{G_\psi}) > 0$.

Proof. Part (i) is just the translation of (11.1iii) into the language of character theory.

(ii) By Frobenius Reciprocity (10.9), $(\xi, \psi^G) > 0$ implies $(\xi|_H, \psi) > 0$. Let ξ be afforded by the simple KG -module M ; then ψ is afforded by a simple KH -submodule L of $\text{res}_H^G(M)$. Keeping the notation of (11.1), let \tilde{L} be the KH -homogeneous component of $\text{res}_H^G(M)$ containing L . Then \tilde{L} is a KG_ψ -module; let η be the K -character of G_ψ afforded by \tilde{L} . Then $\eta|_H = r\psi$ for some positive integer r because all the simple components of \tilde{L} are isomorphic to L ; further, $\xi = \eta^G$ by (11.liv). Finally, $\xi \in \text{Irr}_K(G)$ implies $\eta \in \text{Irr}_K(G_\psi)$, by (10.6) and the fact that $\xi = \eta^G$. This completes the proof.

(11.5) Theorem. Let $\psi \in \text{Irr}_K(H)$ where $H \trianglelefteq G$, and let $S = G_\psi$, the stabilizer of ψ in G . Suppose that $\psi = \psi_1|_H$ for some K -character ψ_1 of S , that is, suppose that ψ can be extended to a character ψ_1 of S . Then

(i) $\psi_1 \in \text{Irr}_K(S)$.

(ii) Each $\omega \in \text{Irr}_K(S/H)$ can be viewed as an irreducible K -character of S , and we have $(\omega\psi_1)^G \in \text{Irr}_K(G)$ for each ω .

(iii) The formula $\psi^G = \sum \omega(l)(\omega\psi_1)^G$, where the sum extends over all $\omega \in \text{Irr}_K(S/H)$, gives ψ^G as a linear combination of distinct irreducible characters $(\omega\psi_1)^G$.

Proof. Assertion (i) is obvious. Next, ψ^S vanishes on $S-H$ by (10.2), and equals $|S:H|\psi$ on H . On the other hand,

$$\sum_{\omega} \omega(1)(\omega\psi_1) = \left\{ \sum_{\omega} \omega(1)\omega \right\} \psi_1,$$

and $\sum \omega(1)\omega$ is the regular character of S/H (see Exercise 9.3). This character vanishes on $S-H$ when viewed as a character of S , and takes the value $|S:H|$ on H . It follows that

$$\psi^S = \sum_{\omega} \omega(1)(\omega\psi_1),$$

which gives the formula for ψ^G in (iii), by transitivity of induction.

From the Intertwining Number Theorem 10.24 we have

$$(\psi^G, \psi^G) = \sum_{xH \in G/H} (\psi, {}^x\psi)_H = |S:H|.$$

On the other hand,

$$(11.6) \quad (\psi^G, \psi^G) = \sum_{\omega, \omega'} \omega(1)\omega'(1)((\omega\psi_1)^G, (\omega'\psi_1)^G),$$

and the terms where $\omega=\omega'$ already contribute at least $\sum \omega(1)^2$. This sum equals $|S:H|$, and since all terms on the right in (11.6) are non-negative, it follows that $((\omega\psi_1)^G, (\omega\psi_1)^G)=1$ for each ψ . Hence the characters $\{(\omega\psi_1)^G : \omega \in \text{Irr}_K(S/H)\}$ are irreducible and distinct, which completes the proof of the proposition.

It is worthwhile to state, as a corollary, the above result for the special case where $G_{\psi}=G$ and where ψ can be extended to a character of G . (Criteria for the existence of such an extension are given later in this section, as well as in Exercises 11.6 and 11.7, and in §15.)

(11.7) Corollary. *Let $H \trianglelefteq G$, and let $\psi \in \text{Irr}_K(H)$ be a character such that $G_{\psi}=G$. If ψ can be extended to a character ψ_1 of G , then every irreducible component ξ of ψ^G can be expressed in the form $\xi=\omega\psi_1$ for a uniquely determined irreducible character ω of G/H .*

This result is, of course, a special case of (11.5). We note also that $(\xi, \psi^G) > 0$ if and only if $(\xi|_H, \psi) > 0$. Thus, in this situation ξ is an irreducible K -character of G such that the components of $\xi|_H$ are mutually isomorphic. In terms of the notation in (11.1), ξ comes from a KG -module M such that $L \cong {}^xL$ for all $x \in G$, where L is a simple submodule of $\text{res}_H^G(M)$.

Combining the preceding results, we discover a rare phenomenon: a family of groups for which we can describe all the irreducible characters in terms of characters of proper subgroups. The technique described here is sometimes called *the method of little groups*.

(11.8) Proposition. *Let $G = A \rtimes B$ be a semidirect product of an abelian normal subgroup A and a subgroup B . Then the following statements hold:*

(i) *Every $\xi \in \text{Irr}_K(G)$ satisfies $(\xi, \psi^G) > 0$ for some $\psi \in \text{Irr}_K(A)$.*

(ii) *Each $\psi \in \text{Irr}_K(A)$ can be extended to a character ψ_1 of G_ψ . Moreover $G_\psi = AB_\psi$, where $B_\psi = G_\psi \cap B$, and (as in (11.5iii))*

$$\psi^G = \sum_{\omega \in \text{Irr}_K(B_\psi)} \omega(1)(\omega\psi_1)^G.$$

Proof. Let $\rho_A = \sum \psi(1)\psi$ be the regular character of A . Then $(\rho_A)^G = \sum \psi(1)\psi^G$ is the regular character of G , from which (i) follows.

Now let $\psi \in \text{Irr}_K(A)$. Then ψ is linear because A is abelian. It is also clear that $G_\psi = AB_\psi$, where $B_\psi = G_\psi \cap B$. It is then easy to check that the extension ψ_1 exists, and is defined by

$$\psi_1(ab) = \psi(a), \quad a \in A, b \in B.$$

The final statement is a consequence of Proposition 11.5.

We conclude this section with another application, where we obtain decisive information on the irreducible characters of groups belonging to a family which includes the important Frobenius groups (see §14A).

Let us begin with a general result, which will be applied in several different ways. If $H \trianglelefteq G$, then G acts on both $\text{Irr}_K(H)$ and the conjugacy classes in H , and it is not surprising that these actions are related. The situation leads to the following:

(11.9) Theorem (Brauer). *Let A be a group which acts on $\text{Irr}_K(G)$ and on the conjugacy classes of G , in such a way that**

$$\alpha(\xi)_{\alpha(\mathfrak{C})} = \xi_{\mathfrak{C}} \text{ for all } \alpha \in A, \xi \in \text{Irr}_K(G),$$

and all conjugacy classes \mathfrak{C} in G . Then for each $\alpha \in A$, the number of irreducible characters of G fixed by α is equal to the number of conjugacy classes fixed by α .

Proof. Let $\mathbf{Z} = (\zeta_j^{(i)})$ be the character table matrix of G , as in (9.25). Then each element $\alpha \in A$ permutes the rows and columns of \mathbf{Z} , sending the row

*In this discussion, $\xi_{\mathfrak{C}}$ means $\xi(x)$ for $x \in \mathfrak{C}$.

indexed by $\xi^{(i)}$ to the row indexed by $\alpha(\xi^{(i)})$, and the column indexed by the conjugacy class \mathfrak{C}_j to the column indexed by the class $\alpha^{-1}(\mathfrak{C}_j)$. (The reason for this choice will become clear in a moment.) The permutation of the rows is given by left multiplication $\mathbf{X}(\alpha)\mathbf{Z}$, and the permutation of the columns by right multiplication $\mathbf{Z}\mathbf{Y}(\alpha)$, where $\mathbf{X}(\alpha)$ and $\mathbf{Y}(\alpha)$ are permutation matrices. The hypothesis implies that

$$\alpha(\xi^{(i)})_{\mathfrak{C}_j} = \xi^{(i)}_{\alpha^{-1}(\mathfrak{C}_j)}.$$

Because of the way $\mathbf{X}(\alpha)$ and $\mathbf{Y}(\alpha)$ are defined, this equation implies that

$$\mathbf{X}(\alpha)\mathbf{Z} = \mathbf{Z}\mathbf{Y}(\alpha).$$

Since \mathbf{Z} is invertible, it follows that $\mathbf{X}(\alpha)$ and $\mathbf{Y}(\alpha)$ have the same trace. The conclusion of Theorem 11.9 is now an immediate consequence of the fact that the trace of a permutation matrix is the number of rows or columns (in the above situation) fixed by the permutation corresponding to α .

(11.10) Corollary. *Let $H \trianglelefteq G$, and let G act by conjugation on $\text{Irr}_K(H)$ and on the conjugacy classes of H . The number of G -orbits of these two G -actions coincide.*

Proof. The preceding theorem shows that the two permutation representations of G , one on $\text{Irr}_K(H)$, and the other on the conjugacy classes of H , have the same character θ . The number of G -orbits in a permutation representation with character θ is given by $(\theta, 1_G)$, by Exercise 10.2, and the result follows.

(11.11) Theorem. *Let $H \trianglelefteq G$, and assume that $C_G(h) \leq H$ for every $h \neq 1$ in H . Then the following statements hold:*

- (i) *Let $\psi \in \text{Irr}_K(H)$ be a character different from 1_H . Then $\psi^G \in \text{Irr}_K(G)$.*
- (ii) *Let $\xi \in \text{Irr}_K(G)$, and assume that $H \not\subseteq \ker \xi$. Then $\xi = \psi^G$ for some $\psi \in \text{Irr}_K(H)$.*

Proof. (i) Because $H \trianglelefteq G$, the Intertwining Number Theorem 10.24 asserts that

$$(\psi^G, \psi^G) = \sum_x (^x\psi, \psi),$$

where the sum is taken over a set of coset representatives of H in G . Thus to prove irreducibility of ψ^G , it is sufficient to prove that ${}^x\psi \neq \psi$ for each $x \notin H$. By Theorem 11.9, the irreducibility of ψ^G will follow if we can show that for each conjugacy class $\mathfrak{C} \neq 1$ in H and each $x \in G$, the equality $x\mathfrak{C}x^{-1} = \mathfrak{C}$ implies that $x \in H$. Let $h \in \mathfrak{C}$; then $x\mathfrak{C}x^{-1} = \mathfrak{C}$ implies that $xhx^{-1} = yhy^{-1}$ for

some $y \in H$, and hence $y^{-1}x \in C_G(h)$. Since $h \neq 1$, the hypothesis implies that $y^{-1}x \in H$, whence also $x \in H$ since $y \in H$. This completes the proof of (i).

(ii) Let $\xi \in \text{Irr}_K(G)$, and assume that $H \not\leq \ker \xi$. Then $\xi|_H$ has at least one component $\psi \in \text{Irr}_K(H)$ such that $\psi \neq 1_H$. Then $\psi^G \in \text{Irr}_K(G)$ by part (i), and $(\xi, \psi^G) \neq 0$ by Frobenius Reciprocity. It follows that $\xi = \psi^G$, and (11.11) is proved.

§11C. Decomposition of Induced Modules from Normal Subgroups

In this subsection, we shall settle the problem raised in §11A (see the remarks following Clifford's Theorem 11.1). The objective is to determine the structure of a simple KG -module M such that for some normal subgroup H of G , M_H contains a simple KH -module which is isomorphic to all its conjugates. In case K is a splitting field, the result is due to Clifford [37] (see also CR §51). The solution of the problem involves projective representations. Here we shall solve the problem for an arbitrary field K . Later, in §19C, we shall decompose induced modules L^G from normal subgroups H of G , where L is an absolutely indecomposable RH -lattice, and R is a discrete valuation ring.

Our approach is based on the work of Tucker ([62], [63], [65a], [65b]), and extensions and refinements of her work by Conlon [64], Ward [68], Dade [70], and Cline [72]. The key idea is to show that the endomorphism algebra of L^G has essentially the structure of a twisted group algebra over the quotient group G/H , with coefficients in the endomorphism algebra of the RH -module L . The work can be viewed as an extension of §10C, where results on the structure of $\text{Hom}_{RG}(L_1^G, L_2^G)$ were established in connection with the Intertwining Number Theorem.

As preparation for the discussion in this section and in §19, it will be useful to set up the problem in a more general context than that of group algebras.

(11.12) Definition. Let S be a finite group, R a commutative ring, and A an R -algebra, f.g./ R as module. A family of R -submodules $\{A_s\}_{s \in S}$ of A , indexed by the elements of S , is called an *S-graded Clifford system* in A , if the following conditions are satisfied:

- (i) $A_s A_t = A_{st}$ (module product).
- (ii) For each $s \in S$, there exists a unit $a_s \in A$ such that

$$A_s = a_s A_1 = A_1 a_s.$$
- (iii) $A = \bigoplus_{s \in S} A_s$. (This decomposition is called the *grading* of A).
- (iv) $1 \in A_1$.

An R -algebra satisfying these conditions will sometimes be called an *S-graded R-algebra*.

Examples. (a) Let $H \trianglelefteq G$, $S = G/H$, and $A = RG$. Then A has an S -graded Clifford system, where the R -submodule A_s corresponding to a coset $s \in G/H$ is given by

$$A_s = \sum_{x \in s} Rx,$$

and the element a_s can be taken as any representative x_s of the coset s .

(b) Let $H \trianglelefteq G$, $S = G/H$, and let $A = (RG)_\alpha$ be the *twisted group algebra* with factor set α , and trivial G -action on R (see (8.33ii)). The algebra $(RG)_\alpha$ has an R -basis $\{a_x\}_{x \in G}$, and (associative) multiplication given by the formulas

$$\xi a_x = a_x \xi, \quad a_x a_y = \alpha(x, y) a_{xy}, \quad \forall x, y \in G, \xi \in R,$$

for some factor set $\alpha: G \times G \rightarrow R$ satisfying (8.37), where, in the context of §8, G acts trivially on R : $x\xi = \xi$ for all $x \in G$ and $\xi \in R$. Then A is an S -graded Clifford system exactly as in (a), with

$$A_s = \sum_{x \in s} Ra_x,$$

and a_s taken to be any element a_x , $x \in s$. The fact that the elements $\{a_s\}$ are units follows from the definition of multiplication, and the assumption that the factor set α takes values in the units of R .

Returning to the general case of an R -algebra A satisfying Definition 11.12, we first note that A_1 is an R -subalgebra of A , and that we may take $a_1 = 1$. Moreover, A is a free right and left A_1 -module with basis $\{a_s\}_{s \in S}$. It also follows from the definition that

$$a_s a_t a_{st}^{-1} \in A_1, \quad a_s A_1 a_s^{-1} \subseteq A_1, \quad s, t \in S.$$

Thus

$$a_s a_t = \alpha(s, t) a_{st}, \quad s, t \in S, \text{ where } \alpha(s, t) \in A_1,$$

and for each $\xi \in A_1$ and $s \in S$,

$$a_s \xi = \xi^s a_s, \text{ for some } \xi^s \in A_1.$$

Therefore an S -graded Clifford system is a generalization of the idea of a twisted group algebra considered in Example (b), with coefficients in the possibly noncommutative ring A_1 .

For a left A_1 -module L , we shall denote by L^A , or by $\text{ind}_{A_1}^A(L)$ when there is risk of confusion, the *induced A -module* $A \otimes_{A_1} L$ (see §10A). Similarly, if M

is a left A -module, we denote by M_{A_1} , or $\text{res}_{A_1}^A(M)$, the A_1 -module obtained by restriction of scalars from A to A_1 .

In the discussion to follow, all modules are assumed to be f.g./ R . The symbol \otimes will denote \otimes_{A_1} , until later in the subsection, when several tensor products have to be considered at once.

For each A_1 -module L , we have

$$L^A = \bigoplus_{s \in S} a_s A_1 \otimes L = \bigoplus_{s \in S} a_s \otimes L,$$

because A is a free right A_1 -module with basis $\{a_s\}_{s \in S}$. By part (ii) of Definition 11.12, we have $A_1 a_s = a_s A_1$ for all $s \in S$; hence all of the R -submodules $\{a_s \otimes L\}$ are also A_1 -submodules of L^A , and are called the *conjugates* of L in L^A . Since the elements $\{a_s\}$ are units in A , left multiplication by a_s defines an R -isomorphism

$$1 \otimes L \cong a_s (1 \otimes L) = a_s \otimes L.$$

We also note that $L \cong 1 \otimes L$ as A_1 -modules, and that $a_s \otimes L = a'_s \otimes L$ as A_1 -modules for any two units a_s and a'_s of A contained in A_s . A left A_1 -module L is called *stable* (or *stable relative to A*) if L is A_1 -isomorphic to all its conjugates. In the situation of Example (a), a left RH -module L is stable if and only if it is isomorphic to all its conjugates $\{{}^x L\}_{x \in G}$.

In the course of our discussion, we shall require both versions of Frobenius Reciprocity considered earlier (see (10.8) and (10.21)) in a slightly generalized form, as follows. In this result, and subsequently in this subsection, we shall write homomorphisms of modules on the opposite side from the scalars, as in §3D.

(11.13) Proposition (Frobenius Reciprocity). *Let A be an R -algebra with an S -graded Clifford system, and let L be a left A_1 -module, and M a left A -module.*

(i) *There is an isomorphism of R -modules*

$$\text{Hom}_{A_1}(L, M_{A_1}) \cong \text{Hom}_A(L^A, M),$$

given by $\varphi \rightarrow \hat{\varphi}$, where

$$(a \otimes l)\hat{\varphi} = a(l\varphi), \quad a \in A, \quad l \in L, \quad \varphi \in \text{Hom}_{A_1}(L, M_{A_1}).$$

If we embed L in L^A using the isomorphism of A_1 -modules $L \cong 1 \otimes L$, then the restriction of $\hat{\varphi}$ to $1 \otimes L$ coincides with φ :

$$(1 \otimes l)\hat{\varphi} = l\varphi, \quad l \in L, \quad \varphi \in \text{Hom}_{A_1}(L, M_{A_1}).$$

(ii) *There is an isomorphism of R -modules,*

$$\text{Hom}_{A_1}(M_{A_1}, L) \cong \text{Hom}_A(M, L^A),$$

which assigns to each A_1 -homomorphism $\theta: M_{A_1} \rightarrow L$ the homomorphism $\tilde{\theta}: M \rightarrow L^A$ given by

$$\tilde{\theta}(m) = \sum_{s \in S} a_s \otimes \theta(a_s^{-1} m), \quad m \in M.$$

Sketch of Proof. The proof of (i) is the same as the proof of (10.8), and is omitted. Likewise, the proof of (ii) is an easy adaptation of the proof of (10.21). The key point is the verification that $\tilde{\theta}$, defined as above, is an A -homomorphism. To prove this, first let $x \in A_1$; then

$$\tilde{\theta}(xm) = \sum_{s \in S} a_s \otimes \theta(a_s^{-1} xm).$$

From the remarks about Clifford systems following the examples, for each $s \in S$ we may write $xa_s = a_s y$ for some $y \in A_1$. Then $a_s^{-1}x = ya_s^{-1}$, so for $m \in M$,

$$\begin{aligned} a_s \otimes \theta(a_s^{-1} xm) &= a_s \otimes \theta(ya_s^{-1} m) = a_s \otimes y\theta(a_s^{-1} m) \\ &= a_s y \otimes \theta(a_s^{-1} m) = x \{ a_s \otimes \theta(a_s^{-1} m) \}. \end{aligned}$$

This shows that $\tilde{\theta}(xm) = x\tilde{\theta}(m)$ for all $x \in A_1$, $m \in M$. It now suffices to prove that $\tilde{\theta}(a_t^{-1} m) = a_t^{-1} \tilde{\theta}(m)$ for all $t \in S$, $m \in M$. We have

$$\tilde{\theta}(a_t^{-1} m) = \sum_{s \in S} a_s \otimes \theta(a_s^{-1} a_t^{-1} m),$$

and by the preliminary remarks, $a_s^{-1} a_t^{-1} = \beta_{st} a_{ts}^{-1}$ for some $\beta_{st} \in A_1$. Then $a_s \beta_{st} = a_t^{-1} a_{ts}$, and

$$\tilde{\theta}(a_t^{-1} m) = \sum_{s \in S} a_s \beta_{st} \otimes \theta(a_{ts}^{-1} m) = a_t^{-1} \sum_{s \in S} a_{ts} \otimes \theta(a_{ts}^{-1} m).$$

Because S is a finite group, this shows that $\tilde{\theta}$ is an A -homomorphism. The rest of the proof is left as an exercise.

(11.14) Proposition. *Let A have an S -graded Clifford system, let L be a left A_1 -module, and let E denote the endomorphism algebra $\text{End}_A L^A$, viewed as a ring of right operators on L^A . For each $s \in S$, let*

$$E_s = \{ f \in E : (1 \otimes L)f \subseteq a_s \otimes L \}.$$

Then

- (i) For all $s, t \in S$, we have

$$\begin{aligned} A_s(a_t \otimes L) &= a_{st} \otimes L; \quad (a_s \otimes L)E_t \subseteq (a_{st} \otimes L); \\ E_s E_t &\subseteq E_{st}, \quad 1 \in E_1, \quad E = \bigoplus_{s \in S} E_s. \end{aligned}$$

(ii) Each element $\varphi \in \text{Hom}_{A_1}(1 \otimes L, a_s \otimes L)$ extends to a unique element $\hat{\varphi} \in E_s$, given by $(a \otimes l)\hat{\varphi} = a((1 \otimes l)\varphi)$ for $l \in L, a \in L$. The map $\varphi \rightarrow \hat{\varphi}$ defines an isomorphism of R -modules

$$\text{Hom}_{A_1}(1 \otimes L, a_s \otimes L) \cong E_s, \quad s \in S,$$

and this is an isomorphism of R -algebras when $a_s = 1$.

(iii) If L is stable and R is noetherian, then E has an S -graded Clifford system, with units $\hat{e}_s \in E_s$ defined by (ii) from A_1 -isomorphisms $e_s : 1 \otimes L \cong a_s \otimes L$, for all $s \in S$.

Proof. (i) We have

$$\begin{aligned} A_s(a_t \otimes L) &= a_s A_1(a_t \otimes L) = a_s(A_1 a_t \otimes L) \\ &= a_s(a_t A_1 \otimes L) = a_s a_t \otimes L = a_{st} \otimes L, \end{aligned}$$

since $A_1 a_t = a_t A_1$ for $t \in S$, and a_{st} differs from $a_s a_t$ by an element of A_1 . We next obtain

$$(a_s \otimes L)E_t = a_s(1 \otimes L)E_t \subseteq a_s(a_t \otimes L) = a_s a_t \otimes L = a_{st} \otimes L,$$

by the definition of E_t . From this fact we have

$$(1 \otimes L)E_s E_t \subseteq (a_s \otimes L)E_t \subseteq a_{st} \otimes L,$$

and hence $E_s E_t \subseteq E_{st}$. Clearly $1 \in E_1$. We postpone showing that $E = \bigoplus E_s$ until after we prove (ii).

(ii) By Proposition 11.13 with $M = L^A$, each $\varphi \in \text{Hom}_{A_1}(1 \otimes L, a_s \otimes L)$ extends to an element $\hat{\varphi} \in E$ satisfying

$$(a \otimes l)\hat{\varphi} = a((1 \otimes l)\varphi).$$

Then $(1 \otimes L)\hat{\varphi} = (1 \otimes L)\varphi \subseteq a_s \otimes L$, so $\hat{\varphi} \in E_s$. The map $\varphi \rightarrow \hat{\varphi}$ is R -injective, by (11.13). Moreover, if $f \in E_s$, then $\varphi = f|_{1 \otimes L}$ is an A_1 -homomorphism from $1 \otimes L$ to $a_s \otimes L$, and

$$(a \otimes l)f = (a(1 \otimes l))f = a((1 \otimes l)\varphi) \text{ for all } l \in L,$$

so that $f = \hat{\varphi}$. Therefore the map $\varphi \rightarrow \hat{\varphi}$ is surjective. It is clear from the definition of $\hat{\varphi}$ that the map $\varphi \rightarrow \hat{\varphi}$ is an isomorphism of R -algebras $\text{End}_{A_1}(1 \otimes L) \cong E_1$, and (ii) is proved.

We can now prove that $E = \bigoplus_s E_s$. If $f \in E$, then since $L^A = \bigoplus a_s \otimes L$, we have

$$f|_{1 \otimes L} = \sum_{s \in S} f_s,$$

where $f_s \in \text{Hom}_{A_1}(1 \otimes L, a_s \otimes L)$. Then $f = \sum \hat{f}_s$, where $\hat{f}_s \in E_s$ is the extension of f_s defined in (ii), because both sides agree on $1 \otimes L$, and $1 \otimes L$ generate L^A as A -module. This proves that $E = \sum_s E_s$. To show that the sum is direct, suppose that $\sum f_s = 0$, where $f_s \in E_s$. Then clearly each $f_s|_{1 \otimes L} = 0$, and by the proof of part (ii), $f_s = (f_s|_{1 \otimes L})^\wedge = 0$. This proves that $E = \bigoplus_s E_s$.

(iii) Now let L be stable, and for each $s \in S$, let $e_s : 1 \otimes L \cong a_s \otimes L$ be an A_1 -isomorphism. Then each extension \hat{e}_s defined in (ii) belongs to E_s , and satisfies

$$(a_t \otimes L) \hat{e}_s = a_t((1 \otimes L) \hat{e}_s) = a_t(a_s \otimes L) = a_{ts} \otimes L \text{ for all } t \in S.$$

Because S is a finite group, it follows that

$$L^A \hat{e}_s = \left(\sum a_i \otimes L \right) \hat{e}_s = \sum a_{is} \otimes L = L^A,$$

and hence \hat{e}_s is a unit in E by (5.8). Finally, we have to prove that

$$E_1 \hat{e}_s = \hat{e}_s E_1 = E_s, \text{ and } E_s E_t = E_{st},$$

for all $s, t \in S$. We have, by (i),

$$E_1 \hat{e}_s \subseteq E_1 E_s \subseteq E_s.$$

But also $E_s \hat{e}_s^{-1} \subseteq E_1$, using the definition of \hat{e}_s and the fact that it is invertible. Thus $E_1 \hat{e}_s = E_s$. On the other hand, $(a_{s^{-1}} \otimes L) \hat{e}_s \subseteq 1 \otimes L$ by (i), so $\hat{e}_s^{-1} \in E_{s^{-1}}$, and we have by (i):

$$\hat{e}_s E_1 \subseteq E_s, \text{ and } \hat{e}_s^{-1} E_s \subseteq E_{s^{-1}} E_s \subseteq E_1,$$

proving that $\hat{e}_s E_1 = E_s$. Moreover, from what has been proved, $\hat{e}_{st}^{-1} \hat{e}_s \hat{e}_t \in E_1$, and hence

$$E_s E_t = \hat{e}_s E_1 \hat{e}_t E_1 = \hat{e}_s \hat{e}_t E_1 = \hat{e}_{st} E_1 = E_{st},$$

completing the proof of (iii).

We remark that in case L is stable and R is noetherian, then E has an S -graded Clifford system over E_1 , and hence is a twisted group algebra over the endomorphism algebra of L , by the remarks preceding the proof.

We now begin the main theme of this subsection: the analysis of L^A , in case L is a simple A_1 -module, and the coefficient ring over which A is defined is a field K .

(11.15) Proposition. *Let A have an S -graded Clifford system over a field K , and let L be a simple A_1 -module. Then E_1 is a f.d. division algebra over K , and*

$$T = \{t \in S : 1 \otimes L \cong a_t \otimes L \text{ as } A_1\text{-modules}\}$$

is a subgroup of S . Further

$$E_T = \sum_{t \in T} E_t$$

is a T -graded R -algebra.

Proof. By Proposition 11.14ii, $E_1 \cong \text{End}_{A_1} L$, and E_1 is a division algebra because L is simple. We next prove that an element $t \in S$ belongs to T if and only if E_t contains a unit. If e_t is a unit in E_t , then $(1 \otimes L)e_t \subseteq a_t \otimes L$, and $\ker(e_t|_{1 \otimes L}) = 0$. From our preliminary remarks, $1 \otimes L$ and $a_t \otimes L$ are K -isomorphic, and so $(1 \otimes L)e_t = a_t \otimes L$ by counting dimensions over the field K . Therefore e_t defines an A_1 -isomorphism, as required, and thus $t \in T$. Conversely, if $t \in T$, and $\varphi : 1 \otimes L \cong a_t \otimes L$ is an A_1 -isomorphism, it follows from Proposition 11.14 that $\hat{\varphi} \in E_t$, and that $\hat{\varphi}$ is a unit in E . The above observation, combined with the fact that $E_s E_t \subseteq E_{st}$, shows that T is a subgroup of S .

The rest of the proof is an immediate application of Proposition 11.14iii to the A_1 -module L , which is stable relative to the T -graded Clifford system $B = \bigoplus_{t \in T} A_t$. Here $E_T = \bigoplus_{t \in T} E_t$ can be identified with the B -endomorphism algebra of L^B (see Exercise 11.8). This completes the proof.

The next result is a generalization of Clifford's Theorem 11.1.

(11.16) Proposition. *Let A be an S -graded Clifford system over a field K , M a simple A -module, and L a simple submodule of M_{A_1} . Then the following statements hold:*

- (i) M_{A_1} is a semisimple A_1 -module, whose simple summands are isomorphic to conjugates $\{a_s \otimes L : s \in S\}$ of L .
- (ii) Let $T = \{t \in S : L \cong a_t \otimes L \text{ as } A_1\text{-modules}\}$, and let $B = \sum_{t \in T} A_t$. Then the homogeneous component N of M_{A_1} containing L is a B -module, and M is A -isomorphic to the induced module $A \otimes_B N$.
- (iii) N is a simple submodule of L^B , and L is stable relative to B .

Sketch of Proof. The proofs of parts (i) and (ii) are essentially the same as the proofs of the corresponding parts of Theorem 11.1, and are left as exercises. The starting point is the observation that T is a subgroup of S , by Proposition 11.15. Let $\{s_1, \dots, s_m\}$ be a set of coset representatives of S/T ; then it is not difficult to prove that A is a free right B -module, with basis

$\{a_{s_1}, \dots, a_{s_m}\}$. It can then be shown that M is a direct sum of the modules $\{a_{s_i} \otimes N\}$ and that $M \cong A \otimes_B N$, as in the proof of Theorem 11.1.

Using (ii), it follows that N is a simple B -module; otherwise, if N_1 is a proper B -submodule of N , then $\sum_{i=1}^m a_{s_i} \otimes N_1$ is a proper A -submodule of $A \otimes_B N$. The latter is a simple A -module by part (ii), and we have reached a contradiction. We now apply Proposition 11.13ii to deduce that because L is an A_1 -submodule of N , there is a nonzero homomorphism from N to L^B . Since N is simple, this shows that N is isomorphic to a submodule of L^B . Finally, L is a B -stable submodule of N because N is a homogeneous component of M_A , and because of the way T is defined. This completes the proof.

By Propositions 11.15 and 11.16, a simple A -module is constructed in two stages. The first step is induction from a simple B -module N , for a T -graded Clifford system B associated with a subgroup T of S . The second stage is the analysis of the structure of a simple submodule N of L^B , for a simple A_1 -module L which is stable relative to B . The latter problem was left open in §11A, and is settled by the following theorem:

(11.17) Theorem. *Let A be an S -graded K -algebra, where K is a field, and let L be a simple A_1 -module which is stable relative to A . Let $E = \text{End}_A L^A$.*

(i) *There is an isomorphism θ from the lattice of left ideals I in E onto the lattice of A -submodules U of L^A , given by*

$$U = L^A \cdot I, \quad I = \{\gamma \in E : L^A \gamma \subseteq U\}.$$

(ii) *The A -module $L^A \cdot I$ corresponding to I is A -isomorphic to $L \otimes_{E_1} I$, where the action of A on this tensor product is given by*

$$a(l \otimes \gamma) = (al)\hat{e}_s^{-1} \otimes \hat{e}_s \gamma \text{ for } a \in A_s, l \in L, \gamma \in I,$$

with E_1 and the units $\{\hat{e}_s\}$ in E_s defined as in (11.14). Furthermore,

$$\dim_K(L \otimes_{E_1} I) = (\dim_{E_1} L)(\dim_K I).$$

(iii) *The lattice isomorphism θ is functorial, in the sense that E -homomorphisms $f: I \rightarrow I'$, between left ideals of E , correspond bijectively to A -homomorphisms $1 \otimes f: L \otimes_{E_1} I \rightarrow L \otimes_{E_1} I'$.*

Proof. We first recall that in this situation, by Propositions 11.14 and 11.15, E has an S -graded Clifford system, and E_1 is a f.d. division algebra over K . The units $\hat{e}_s \in E_s$ correspond as in (11.14iii) to A_1 -isomorphisms $e_s: 1 \otimes L \cong a_s \otimes L$, $s \in S$. The argument now proceeds in a number of steps.

Step 1. We show first that L^A is a free right E -module. Let $\{l_1, \dots, l_m\}$ be a basis of $1 \otimes L$ over the division algebra E_1 ; we shall prove that these elements

form an E -basis of L^A . We have

$$a_s \otimes L = (1 \otimes L) e_s = \left(\sum l_i E_1 \right) e_s = \sum l_i (E_1 \hat{e}_s),$$

and hence the elements $\{l_i\}$ generate L^A over E . Next, let

$$\sum l_i e_i = 0, \quad e_i \in E.$$

Each element e_i can be expressed in the form

$$e_i = \sum_{s \in S} \xi_{is} \hat{e}_s, \quad \xi_{is} \in E_1,$$

and we have

$$\sum_s \sum_i l_i \xi_{is} \hat{e}_s = 0.$$

Then

$$\sum_i l_i \xi_{is} = 0, \quad s \in S,$$

because

$$\left(\sum_i l_i \xi_{is} \right) \hat{e}_s \in a_s \otimes L,$$

and the sum $\sum a_s \otimes L$ is direct. Finally, each $\xi_{is} = 0$ because of the independence of the elements $\{l_i\}$ over E_1 .

Step 2. Let I be a left ideal of E . Since L^A is a free right E -module, the inclusion map $i: I \rightarrow E$ extends to a monomorphism

$$1 \otimes i: L^A \otimes_E I \rightarrow L^A \otimes_E E$$

by (2.28), and $L^A \otimes_E E \cong L^A$ by (2.16). The image of $1 \otimes i$ in L^A is clearly $L^A \cdot I$, so we have

$$L^A \otimes_E I \cong L^A \cdot I.$$

Step 3. Given a left ideal I of E , set $U = L^A \cdot I$, an A -submodule of L^A . We claim that

$$I = \{ \gamma \in E : L^A \cdot \gamma \subseteq U \}.$$

Since $L^A = A(1 \otimes L)$, it is clear that

$$\{\gamma \in E : L^A \gamma \subseteq U\} = \{\gamma \in E : (1 \otimes L) \gamma \subseteq U\}.$$

Next, by Step 1, a right E_1 -basis $\{l_j\}$ of $1 \otimes L$ is also an E -basis of L^A . It follows that each element of U can be expressed in the form $\sum l_j \gamma_j$, with uniquely determined coefficients $\{\gamma_j\}$ in I . Hence if $(1 \otimes L) \gamma \subseteq U$, then $\gamma \in I$. This shows that $\{\gamma \in E : L^A \cdot \gamma \subseteq U\} \subseteq I$; the reverse inclusion is obvious, and the equality is established.

Step 4. Now let U be an arbitrary A -submodule of L^A , and define I as in Step 3, so I is a left ideal of E such that $L^A \cdot I \subseteq U$. In order to prove that equality holds, we again start with an E_1 -basis $\{l_j\}$ of $1 \otimes L$. Suppose that $\sum l_j \gamma_j \in U$, $\gamma_j \in E$; we must prove that each $\gamma_j \in I$. Since $E_1 \cong \text{End}_{A_1}(1 \otimes L)$, and $1 \otimes L$ is a simple A_1 -module, it follows from the Density Theorem 3.27 that, for each i , there exists an element $a_i \in A_1$ such that $a_i l_i = l_i$, $a_i l_j = 0$ for $j \neq i$. Then (for each i)

$$a_i \left(\sum_j l_j \gamma_j \right) = l_i \gamma_i \in U.$$

Therefore also $(A_1 l_i) \gamma_i \subseteq U$. But $A_1 l_i = 1 \otimes L$ since $1 \otimes L$ is simple, so we have $(1 \otimes L) \gamma_i \subseteq U$, and therefore $\gamma_i \in I$, as desired. This completes the proof that $L^A \cdot I = U$, and shows that the correspondence $I \leftrightarrow U$ is indeed a lattice isomorphism.

Step 5. We now prove assertion (ii) of the theorem. We have $L^A = \sum_s (1 \otimes L) \hat{e}_s$, and $\hat{e}_s I = I$ for each $s \in S$, and hence

$$L^A I = \sum_{s \in S} (1 \otimes L) \hat{e}_s I = (1 \otimes L) I.$$

Now let $\{l_j\}$ be a right E_1 -basis of $1 \otimes L$. By Step 1, we have

$$(1 \otimes L) I = \bigoplus l_j I, \quad L \otimes_{E_1} I = \bigoplus (l_j \otimes I),$$

the latter because tensor products commute with direct sums. Since both $l_j I$ and $l_j \otimes I$ are isomorphic to I as K -spaces, there exists a K -isomorphism

$$(11.18) \quad L^A I = (1 \otimes L) I \cong L \otimes_{E_1} I.$$

If we identify L with the A_1 -submodule $1 \otimes L$ of L^A , then the isomorphism in (11.18) is given by

$$l \gamma \rightarrow l \otimes \gamma, \quad l \in L, \gamma \in I.$$

If $a \in A_s$, then for $l \in L$, $\gamma \in I$, we have

$$a(l\gamma) = (al\hat{e}_s^{-1})\hat{e}_s,$$

with $al\hat{e}_s^{-1} \in L$, $\hat{e}_s\gamma \in I$. The isomorphism in (11.18) maps this element onto

$$al\hat{e}_s^{-1} \otimes \hat{e}_s\gamma \in L \otimes_{E_1} I.$$

Thus if the action of A on $L \otimes_{E_1} I$ is defined as in part (ii) of the theorem, the K -isomorphism (11.18) becomes an A -isomorphism, and Step 5 is finished.

Step 6. As in Step 2, we can identify $L^A I$ with $L^A \otimes_E I$, for each left ideal I in E . Clearly each E -homomorphism $f: I \rightarrow I'$ defines an A -homomorphism $1 \otimes f: L^A \otimes_E I \rightarrow L^A \otimes_E I'$. Conversely, let $g: L^A I \rightarrow L^A I'$ be an A -homomorphism, where I and I' are left ideals in E . For each $\gamma \in I$, the map

$$1 \otimes l \mapsto ((1 \otimes l)\gamma)g, \quad l \in L,$$

lies in $\text{Hom}_{A_1}(1 \otimes L, L^A)$; hence, by reciprocity (11.13), there is a unique element $\hat{\gamma} \in E$ such that

$$(1 \otimes l)\hat{\gamma} = ((1 \otimes l)\gamma)g \in L^A I', \quad l \in L.$$

By Step 3, $\hat{\gamma} \in I'$, and it is easily checked that the map $\gamma \mapsto \hat{\gamma}$ is an E -homomorphism from I to I' , which we denote by f . Finally, to prove that $g = 1 \otimes f$, it is sufficient to check that both agree on $(1 \otimes L)I$, since both are A -homomorphisms, and $A((1 \otimes L)I) = L^A \cdot I$. For $l \in L$ and $\gamma \in I$, we have

$$((1 \otimes l)\gamma)(1 \otimes f) = (1 \otimes l)(\gamma f) = (1 \otimes l)\hat{\gamma} = ((1 \otimes l)\gamma)g.$$

Hence $g = 1 \otimes f$, and Step 6 is done.

This completes the proof of all parts of the theorem except the statement in part (ii) about dimensions, which we leave as an exercise.

Our final topic in this subsection is the long-awaited application of Theorem 11.17 to complete the discussion of Clifford's Theorem. (A more direct approach was given in CR §51.)

(11.19) Definition. Let K be a field, and G a finite group. A *projective representation* of G , with *factor set* α , is a map $T: G \rightarrow GL(M)$ for some f.d. vector space M over K , such that

$$T(x)T(y) = \alpha(x, y)T(xy), \quad x, y \in G,$$

where α is a map from $G \times G$ taking values in the multiplicative group K^\times of nonzero elements of K .

Using the associative law in G and in $GL(V)$, it is easily checked that the map α defined above is a factor set in the sense of (8.37), with $A=K^\circ$, and with trivial action of G on K° . In §11E below, we shall give a more extensive discussion of projective representations in the context of central extensions (see also CR §53).

The following theorem shows that projective representations arise in an unavoidable way in completing the analysis of simple KG -modules M in the stable case (see the remarks following Theorem 11.1).

(11.20) Theorem (Clifford [37]). *Let H be a normal subgroup of G , and let K be an algebraically closed field. Let M be a simple KG -module, and L a simple KH -submodule of M_H such that L is stable relative to G (that is, L is isomorphic to all of its conjugates). Set $S=G/H$. Then*

$$M \cong L \otimes_K I$$

for a left ideal I in the S -graded algebra $E=\text{End}_{KG} L^G$. The G -action on $L \otimes_K I$ is given by

$$x \rightarrow U(x) \otimes V(x), \quad x \in G,$$

where $U: G \rightarrow GL(L)$ is a projective representation of G on L , and $V: G \rightarrow GL(I)$ is a projective representation of S , that is, $V(x)$ depends only on the coset xH of x in S , for each $x \in G$. The factor sets associated with U and V are inverses of each other.

Proof. We view KG as an S -graded Clifford system, as in Example (a) following Definition 11.12. Then KH plays the role of A_1 , and L is a stable KH -module relative to KG . Since K is algebraically closed, we can identify the division algebra E_1 with K . The S -graded Clifford system $E=\text{End}_{KG} L^G$ becomes, in this case, a twisted group algebra $(KS)_\alpha$, as in Example (b) following (11.12), with a K -basis $\{\hat{e}_s\}_{s \in S}$, and multiplication given by

$$\hat{e}_s \hat{e}_t = \alpha(s, t) \hat{e}_{st}, \quad s, t \in S,$$

for some factor set $\alpha: S \times S \rightarrow K^\circ$. By part (ii) of Proposition 11.13, M is isomorphic to an A -submodule of L^G , hence by part (ii) of Theorem 11.17, we have

$$M \cong L \otimes_K I$$

for some left ideal I in E . The G -action on M is given by

$$x(l \otimes \gamma) = (xl) \hat{e}_s^{-1} \otimes e_s \gamma, \quad x \in G, \gamma \in I,$$

where s is the coset in $S=G/H$ containing x . We define

$$U(x)l = (xl) \hat{e}_s^{-1}, \quad V(x)\gamma = \hat{e}_s \gamma,$$

for $x \in G$ and $s \in S$ as above. It is then clear that V defines a projective representation of S on I with factor set α . Moreover, the action of G on M is given by

$$x \rightarrow U(x) \otimes V(x), \quad x \in G,$$

and it follows from this that U is a projective representation of G on L with factor set α^{-1} , completing the proof.

Remark. It is useful to make a few comments about the structure of the projective representation U on L , in (11.20). For each fixed $x \in G$, the map

$$U(x) : l \mapsto xl\hat{e}_s^{-1}, \quad l \in L,$$

is an isomorphism of vector spaces $L \cong U(x)L$, such that for all $h \in H$, $l \in L$, we have

$$hU(x)l = x(x^{-1}hx)l\hat{e}_s^{-1} = U(x)(h^x l).$$

Thus $U(x)$ defines a KH -isomorphism between L and its conjugate xL , for each $x \in G$ (see §10B). We also have, if $\hat{e}_1 = 1$,

$$U(h)l = hl, \quad h \in H, \quad l \in L,$$

so U extends the action of H on L . Thus, if the factor set associated with either U or V is identically 1, it follows that the action of H on the G -stable module L can be extended to an action of G .

Suppose next that $U' : G \rightarrow GL(L)$ is another projective representation of G on L , such that U' extends the action of H on L , and such that for each $x \in G$, $U'(x)$ gives a KH -isomorphism $L \cong {}^xL$ as above. Since L is absolutely simple, it is easy to prove that U' is equivalent to U , in the sense that there exists a map $\xi : G \rightarrow K$ such that

$$U'(x) = \xi(x)U(x), \quad x \in G$$

(see §11E). Given such a U' , we can modify the representation V occurring in (11.20) accordingly, by setting

$$V'(x) = \xi(x)^{-1}V(x), \quad x \in G.$$

Then V' is also a projective representation of G/H , and we have $U \otimes V \cong U' \otimes V'$.

§11D. Hecke Algebras and Induced Modules

In §11B, C, we discussed the decomposition of modules induced from normal subgroups. In this subsection, we consider the more general situation of modules induced from arbitrary subgroups. In order to obtain sharp results,

however, we shall restrict the base field K to be a subfield of the complex numbers, such that K is a splitting field for G and all its subgroups, as in §11B. We shall pay special attention to characters induced from linear characters of subgroups of G , and in particular, to the decomposition of transitive permutation representations of G . The main results are due to Curtis-Fossum [68] and Ree. As mentioned earlier, these results will be essential for the representation theory of finite groups of Lie type (Chapter 7).

As in §9C, characters of a group G will always be viewed as the restrictions to G of characters of the group algebra KG . We shall use the notation $\text{Irr } G$ to denote the characters of a basic set of simple KG -modules, and also for the restrictions of these characters to G .

It will sometimes be convenient to identify the group algebra KG with the set of K -valued functions f on G , with the element $\sum \alpha_x x \in KG$ corresponding to the function $f: G \rightarrow K$ defined by $f(x) = \alpha_x$, $x \in G$, $\alpha_x \in K$. The operation of multiplication in KG carries over to convolution of the corresponding functions. If f and g are K -valued functions on G , their *convolution product* $f \cdot g: G \rightarrow K$ is the function defined by

$$(f \cdot g)(x) = \sum_{y \in G} f(xy)g(y^{-1}), \quad x \in G.$$

Then KG is isomorphic (as K -algebra) to the algebra of functions $f: G \rightarrow K$, multiplied using the convolution product.

(11.21) Proposition. *Let $H \leq G$, and let $e \in KH$ be an idempotent such that the left ideal KHe affords the K -character ψ of H . Then KGe affords the induced character ψ^G . Moreover, if $\zeta \in \text{Irr } G$, then*

$$(\zeta, \psi^G) = \zeta(e) = \dim_K eM,$$

where M is a KG -module affording ζ .

Proof. For the first statement, it is easily checked that, since KG is a free right KH -module, there is an isomorphism of left KG -modules

$$KGe = KG \cdot KHe \cong KG \otimes_{KH} KHe;$$

hence KGe affords ψ^G . For the second statement, we have

$$\zeta(e) = \text{Tr}(e, M) = \dim_K eM,$$

since e is an idempotent. By Exercise 3.10, $eM \cong \text{Hom}_{KG}(KGe, M)$, and the dimension of the latter is equal to the scalar product of characters (ζ, ψ^G) by (9.24iii). This completes the proof.

Let e be an idempotent in KG . By (3.19), the subalgebra $e \cdot KG \cdot e$ of KG , with identity element e , is isomorphic to the opposite ring $\{\text{End}_{KG} KGe\}^\circ$,

where $\text{End}_{KG} KG e$ is viewed as an algebra of left operators on KGe . The algebra $e \cdot KG \cdot e$ is semisimple, by (5.13) and (5.18), since KG is semisimple.

(11.22) Definition. Let $H \leq G$, and let ψ be a K -character afforded by KHe for some idempotent $e \in KH$, as in (11.21). The *Hecke algebra* $\mathcal{H}(G, H, \psi)$ is the subalgebra $e \cdot KG \cdot e$ of KG . (We shall denote this Hecke algebra simply by \mathcal{H} , when H and ψ are fixed by the context.)

By the remarks preceding the definition, a Hecke algebra \mathcal{H} is a semisimple algebra with identity element e . Moreover, if $KHe \cong KHe'$ for another idempotent e' , then clearly $KGe \cong KGe'$ by the first statement of (11.21), and $eKGe \cong e'KGe'$ by (3.19). Thus the Hecke algebra \mathcal{H} is defined independently of the left ideal KHe affording ψ . G. Seitz has pointed out that many properties of Hecke algebras become transparent if we view KG as a split semisimple K -algebra, with Wedderburn components $A_i \cong M_{n_i}(K)$. Then an idempotent e as in (11.22) can be expressed in the form $e = \sum e_i e_i$, where e_i is the identity element of A_i . Properties of \mathcal{H} such as (11.23), (11.25), and (11.26) can then be checked easily by using the results of §3.

Example. Let $H \leq G$, and let ψ be the trivial character 1_H of H . Then 1_H is afforded by the idempotent $e_H = |H|^{-1} \sum_{h \in H} h$ of KH . The Hecke algebra $\mathcal{H}(G, H, 1_H)$ equals $e_H KGe_H$, and is easily shown to be isomorphic to the algebra of functions $f: G \rightarrow K$, with multiplication defined by convolution, which are constant on the (H, H) -double cosets of G . For the proof, we use the interpretation of KG as an algebra of functions, and then check that the subalgebra $e_H KGe_H$ corresponds to the functions constant on double cosets. As far as we know, this is the origin of the term *Hecke algebra* (see Shimura [71], p. 54). Hecke algebras of permutation representations, and generalizations of them called *S-rings* or *Schur algebras*, have been studied extensively by Tamaschke ([60], [64a], [64b]), Wielandt [64] and Roesler [72]. A different approach to the decomposition of permutation and monomial representations, based on the study of G -orbits in $X \times X$, where X is the set on which G acts, was given by Schur, Wielandt [64] and D. G. Higman ([64], [67]). The representation theory of Hecke algebras to follow was suggested partly by the analogy with the theory of spherical functions on symmetric spaces (see Helgason [62], Chapter X). This interpretation was pursued for finite groups by Travis [74].

Until further notice, we shall fix a finite group G , a subgroup H of G , an idempotent $e \in KH$ such that KHe affords the K -character ψ of H , and the Hecke algebra $\mathcal{H} = e \cdot KG \cdot e$.

(11.23) Lemma. An idempotent $u \in \mathcal{H}$ is primitive in \mathcal{H} if and only if it is primitive in KG .

Proof. We recall (Exercise 3.8) that an idempotent u in a semisimple ring A is primitive if and only if it generates a simple left ideal, and that the condition for this to occur is that uAu be a division ring, by (3.18iii). Since $u \in \mathcal{K}$ and e is the identity element in \mathcal{K} , we have $eu=ue=u$; hence

$$uKG u = ueKG e u = u\mathcal{K} u,$$

and the result follows.

(11.24) **Corollary.** *The field K is a splitting field for \mathcal{K} .*

Proof. We have to prove that each simple \mathcal{K} -module is absolutely simple. By (3.18) and (3.43), it is sufficient to prove that $u\mathcal{K} u = Ku$ for each primitive idempotent $u \in \mathcal{K}$. This is immediate by Lemma 11.23, since K is a splitting field for G .

(11.25) **Theorem.** *Let \mathcal{K} be the Hecke algebra associated with G , H , e and ψ , as above. The following statements hold:*

- (i) *Let $\xi \in \text{Irr } G$. Then the restriction $\xi|_{\mathcal{K}} \neq 0$ if and only if the multiplicity $(\xi, \psi^G) \neq 0$.*
- (ii) *The map $\xi \rightarrow \xi|_{\mathcal{K}}$ is a bijection from the set of irreducible characters ξ of G such that $(\xi, \psi^G) \neq 0$, to the set of all irreducible characters of the semisimple K -algebra \mathcal{K} .*
- (iii) *If φ is an irreducible character of \mathcal{K} corresponding to $\xi \in \text{Irr } G$ according to part (ii), then $\deg \varphi = (\xi, \psi^G)$.*

Proof. (i) Let M be a simple KG -module affording ξ , and suppose $\xi|_{\mathcal{K}} \neq 0$. Then $\xi(eae) \neq 0$ for some $a \in KG$, and hence $eM \neq 0$. By (11.21), $(\xi, \psi^G) \neq 0$. Conversely, if $(\xi, \psi^G) \neq 0$, the multiplicity formula (11.21) asserts that $\xi(e) \neq 0$, whence $\xi|_{\mathcal{K}} \neq 0$, and (i) is proved.

(ii) First let $\xi \in \text{Irr } G$, and suppose $\xi|_{\mathcal{K}} \neq 0$. Let M afford ξ , as in (i). Then $eM \neq 0$ by (i) and (11.21), and eM is a left \mathcal{K} -module since $\mathcal{K} = eKG e$. If $m \neq 0$ and $m \in eM$, then $\mathcal{K}m = eKGm = eM$, because M is a simple KG -module, so we have proved that eM is a simple \mathcal{K} -module. We now compute its character. For $x \in \mathcal{K}$, we have $xM \subseteq eM$, whence

$$\xi(x) = \text{Tr}(x, M) = \text{Tr}(x, eM).$$

Therefore $\xi|_{\mathcal{K}}$ is the character of the simple \mathcal{K} -module eM .

Next we prove that the map $\xi \rightarrow \xi|_{\mathcal{K}}$ is surjective. Let φ be the character of a simple \mathcal{K} -module. Then φ is afforded by a minimal left ideal $\mathcal{K}u$, generated by a primitive idempotent $u \in \mathcal{K}$. By Lemma 11.23, u is primitive in KG , and

KGu is a simple KG -module affording some irreducible character $\zeta \in \text{Irr } G$. Upon applying the argument in the preceding paragraph to KGu , we see that $\zeta|_{\mathcal{H}}$ is the character of the simple \mathcal{H} -module $eKGu = \mathcal{H}u$, and therefore $\zeta|_{\mathcal{H}} = \varphi$.

Finally suppose that $\zeta, \zeta' \in \text{Irr } G$ have the same nonzero restrictions to \mathcal{H} . By the first part of the argument, $\zeta|_{\mathcal{H}}$ is an irreducible character φ of \mathcal{H} , and there exists $\zeta_0 \in \text{Irr } G$ afforded by a minimal left ideal KGu with $u \in \mathcal{H}$, such that $\zeta_0|_{\mathcal{H}} = \varphi$. Let M be a simple module affording ζ . Then

$$\zeta(u) = \varphi(u) \neq 0,$$

whence $uM \neq 0$, and it follows that $KGu \cong M$. Similarly $KGu \cong M'$, where M' affords ζ' , and we conclude that $\zeta' = \zeta$.

(iii) Let $\varphi = \zeta|_{\mathcal{H}}$, for $\zeta \in \text{Irr } G$. By part (i), φ is afforded by eM , where M is a simple KG -module affording ζ . Then $\deg \varphi = \varphi(e) = \zeta(e) = \dim_K eM = (\zeta, \psi^G)$, by Proposition 11.21, and the proof is complete.

Let $\text{Irr } G = \{\zeta^1, \dots, \zeta^s\}$, and for $1 \leq i \leq s$, let ϵ_i be the central primitive idempotent in KG corresponding to ζ^i , given by

$$\epsilon_i = \zeta^i(1)|G|^{-1} \sum_{x \in G} \zeta^i(x^{-1})x,$$

according to (9.21).

(11.26) Corollary. *Let $I = \{i : 1 \leq i \leq s, \text{ and } (\zeta^i, \psi^G) \neq 0\}$. Then $\{e\epsilon_i\}_{i \in I}$ are the central primitive idempotents of \mathcal{H} .*

Proof. The central primitive idempotents in a semisimple algebra are characterized as elements which act as the identity on one simple module V , and annihilate all other simple modules not isomorphic to V . By Theorem 11.25, the simple \mathcal{H} -modules are all of the form eM , where M is a simple KG -module affording a character $\zeta^i \in \text{Irr } G$ for which $(\zeta^i, \psi^G) \neq 0$. It is then clear from what has been said that $e\epsilon_i$ acts as the identity on eM and annihilates all simple \mathcal{H} -modules not isomorphic to eM , proving the corollary.

(11.27) Corollary (Janusz [66]). *Let $\zeta^i \in \text{Irr } G$ be a character for which $(\zeta^i, \psi^G) = 1$. Then $e\epsilon_i$ is a primitive idempotent in KG such that the simple module $KGe\epsilon_i$ affords ζ^i .*

Proof. By Corollary 11.26 and Proposition 11.25iii, $e\epsilon_i$ is a central primitive idempotent in \mathcal{H} , which corresponds to a character of \mathcal{H} of degree one. Hence $e\epsilon_i$ is a primitive idempotent in \mathcal{H} , so by (11.23), $e\epsilon_i$ is also primitive in KG . The fact that $KGe\epsilon_i$ affords ζ^i follows from (11.25). For another proof see Exercise 10.7.

(11.28) Theorem (Ree). *Keep the notation of (11.25). Let $\xi \in \text{Irr } G$, and assume that $(\psi^G, \xi) \neq 0$. Let $t \in G$, and let \mathfrak{C} be the conjugacy class containing t , and C the class sum $\sum_{x \in \mathfrak{C}} x$. Then*

$$\xi(t) = |C_G(t)| \xi(eCe) \left\{ \sum_{x \in G} \xi(ex^{-1}e) \xi(exe) \right\}^{-1}.$$

Proof. Let \mathbf{M} be a matrix representation of G affording ξ . Then $eCe = Ce$ because C is contained in the center of KG , and

$$\mathbf{M}(C) = \omega \mathbf{I}, \text{ where } \omega = |\mathfrak{C}| \xi(t) \xi(1)^{-1},$$

as one sees by taking traces of both sides. Then

$$\mathbf{M}(eCe) = \mathbf{M}(C)\mathbf{M}(e) = \omega \mathbf{M}(e).$$

Taking traces again, we have

$$\xi(eCe) = \omega \xi(e) = |\mathfrak{C}| \xi(t) \xi(e) \xi(1)^{-1}.$$

Now let

$$\varepsilon = \xi(1)|G|^{-1} \sum_{x \in G} \xi(x^{-1})x$$

be the central primitive idempotent in KG corresponding to ξ . Then

$$\varepsilon e = \xi(1)|G|^{-1} \sum_{x \in G} \xi(x^{-1})exe.$$

Let $e = \sum_{h \in H} \alpha_h h$. Because $e^2 = e$, we have

$$\varepsilon e = \xi(1)|G|^{-1} \sum_{x \in G} \sum_{h, k \in H} \xi(x^{-1}) \alpha_h \alpha_k e h x k e.$$

Putting $y = h x k$, we have $x^{-1} = k y^{-1} h$, and

$$\varepsilon e = \xi(1)|G|^{-1} \sum_{y \in G} \xi \left(\sum_{h, k \in H} \alpha_h \alpha_k k y^{-1} h \right) e y e.$$

Therefore

$$(11.29) \quad \varepsilon e = \xi(1)|G|^{-1} \sum_{x \in G} \xi(ex^{-1}e)exe.$$

Now apply \mathbf{M} and take traces; since $\mathbf{M}(\varepsilon) = \mathbf{I}$, we obtain

$$\xi(e) = \xi(1)|G|^{-1} \sum_{x \in G} \xi(ex^{-1}e) \xi(exe).$$

Upon substituting this expression into the previous formula for $\zeta(eCe)$, we obtain the desired result.

The preceding theorem, combined with Theorem 11.25, gives the values of characters of G which appear with nonzero multiplicity in ψ^G , in terms of the values of the irreducible characters of the Hecke algebra. Thus Ree's formula reduces the problem of calculating character values from KG to \mathcal{H} , where \mathcal{H} is usually of much smaller dimension than KG . Nevertheless, Ree's formula is still not effectively computable without more information about the idempotent e . The following result provides an illustration of what can be said when the idempotent e is known explicitly.

We first recall from §10B that for $x \in G$, ${}^x\psi$ denotes the character of the conjugate subgroup xH , defined by

$${}^x\psi({}^xh) = \psi(h), \quad h \in H.$$

We also define the *index* of x by

$$\text{ind } x = |H : {}^xH \cap H|, \quad x \in G.$$

Then it is easily checked that $\text{ind } x$ is the number of left (or right) cosets of H contained in the double coset HxH . The numbers $\{\text{ind } x : x \in G\}$ coincide with the degrees of the transitive permutation representations appearing as direct summands of $(1_H^G)_H$, and were called *subdegrees* of 1_H^G in §10B.

(11.30) Proposition. *Keep the notation of (11.25), and assume further that ψ is a linear character of H , so $e = |H|^{-1} \sum_{h \in H} \psi(h^{-1})h$ is the central idempotent in KH which corresponds to ψ . Let*

$$H \setminus G / H = \{D_i\}_{1 \leq i \leq r}, \quad \text{where } D_i = Hx_iH, \quad 1 \leq i \leq r.$$

Then the following statements concerning the Hecke algebra \mathcal{H} hold:

(i) *Let $J = \{j : 1 \leq j \leq r, {}^{x_j}\psi = \psi \text{ on } H \cap {}^{x_j}H\}$, and define*

$$a_j = (\text{ind } x_j)ex_je, \quad j \in J.$$

Then $\{a_j\}_{j \in J}$ is a basis for \mathcal{H} . The basis elements $\{a_j\}$ are determined independently of the double coset representatives if $\psi = 1_H$, and up to multiplication by a root of unity if $\psi \neq 1_H$.

(ii) *For $i, j \in J$, we have*

$$a_i a_j = \sum_{k \in J} \mu_{ijk} a_k, \quad \mu_{ijk} \in K.$$

The structure constants are given by

$$\mu_{ijk} = |H| \sum_{y \in D_i \cap x_k D_j^{-1}} a_i(y) a_j(y^{-1} x_k),$$

where in this formula we identify the elements $a_i \in KG$ with K -valued functions on G . We have

$$\mu_{ijk} \in \text{alg. int.}\{K\} \text{ for all } i, j, k.$$

(iii) Define a linear function λ on \mathcal{K} by setting $\lambda(\sum_j \xi_j a_j) = \xi_0$, where $a_0 = e$. Then the bilinear form B on \mathcal{K} defined by $B(a, b) = \lambda(ab)$, $a, b \in \mathcal{K}$, is nondegenerate, symmetric and associative (§9A). Moreover,

$$\{a_j\}_{j \in J} \text{ and } \left\{(\text{ind } x_j)^{-1} \hat{a}_j\right\}_{j \in J}$$

are dual bases of \mathcal{K} with respect to the form λ , where

$$\hat{a}_j = (\text{ind } x_j) ex_j^{-1} e, j \in J.$$

Remark. The basis elements $\{a_j\}_{j \in J}$ are called *standard basis elements* of \mathcal{K} . The basis elements $\{\hat{a}_j\}_{j \in J}$ form another set of standard basis elements, differing from the first by permutation of the indices, and in case $D_j = D_j^{-1}$, by multiplication by a root of unity.

Proof. (i) We have $he = eh = \psi(h)e$ for all $h \in H$. First suppose $h \in H \cap {}^x H$, for some $x \in G$. Then $h = {}^x h_1$ for some $h_1 \in H$, and

$$\begin{aligned} {}^x \psi(h)exe &= \psi(h_1)exe = exeh_1 = exh_1e \\ &= e {}^x h_1 xe = \psi(h)exe. \end{aligned}$$

Therefore $exe \neq 0$ implies ${}^x \psi = \psi$ on $H \cap {}^x H$.

Conversely, suppose $\psi = {}^x \psi$ on $H \cap {}^x H$. We first calculate the coefficient of x in

$$exe = |H|^{-2} \sum_{h_1, h_2 \in H} \psi(h_1)^{-1} \psi(h_2)^{-1} h_1 x h_2.$$

If $h_1 x h_2 = x$, then $h_1 \in H \cap {}^x H$ and $h_1 = {}^x h_2^{-1}$. Since $\psi = {}^x \psi$ on $H \cap {}^x H$, we have $\psi(h_1) = \psi(h_2)^{-1}$, so the coefficient of x in exe is $|H|^{-2} |H \cap {}^x H|$. Similarly, the coefficient of $h_1 x h_2$ in exe is $\psi(h_1)^{-1} \psi(h_2)^{-1} |H|^{-2} |H \cap {}^x H|$. Therefore $a_j \neq 0$ if $j \in J$, and

$$(11.31) \quad a_j = |H|^{-1} \sum_{h_1 x h_2 \in D_j} \psi(h_1)^{-1} \psi(h_2)^{-1} h_1 x_j h_2,$$

where the sum is taken over distinct elements of D_j . From these remarks, it follows that the elements $\{a_j\}_{j \in J}$ are linearly independent, and form a basis for \mathcal{K} . It is also clear that changing the double coset representatives will multiply each basis element a_j by some root of unity, which is equal to 1 if $\psi = 1_H$.

(ii) Let

$$a_i a_j = \sum \mu_{ijk} a_k, \quad i, j, k \in J, \quad \mu_{ijk} \in K.$$

In order to compute the structure constants μ_{ijk} , we view the elements $\{a_i\}$ as complex-valued functions on G , multiplied by convolution. Evaluating both sides at x_k and using the results of part (i), we obtain

$$(a_i a_j)(x_k) = \mu_{ijk} |H|^{-1},$$

where

$$(a_i a_j)(x_k) = \sum_{y \in G} a_i(y) a_j(y^{-1} x_k) = \sum_{y \in D_i \cap x_k D_j^{-1}} a_i(y) a_j(y^{-1} x_k).$$

Comparing these expressions, we obtain the required formula for the $\{\mu_{ijk}\}$. It is now easily checked, using part (i), that for all $h \in H$ we have

$$a_i(y) a_j(y^{-1} x_k) = a_i(yh) a_j((yh)^{-1} x_k), \quad y \in G.$$

Finally, it follows by (11.31) that

$$\mu_{ijk} = |H|^2 |H|^{-2} \alpha$$

for some $\alpha \in \text{alg. int.}\{K\}$, and part (ii) is proved.

(iii) Upon using x_j^{-1} instead of x_j in (11.31), we obtain

$$\hat{a}_j = |H|^{-1} \sum_{h_1 x_j^{-1} h_2 \in D_j^{-1}} \psi(h_1)^{-1} \psi(h_2)^{-1} h_1 x_j^{-1} h_2.$$

Hence, by the same calculation used in part (ii) we have

$$\begin{aligned} \lambda(a_i \hat{a}_j) &= |H| \sum_{y \in D_i \cap D_j^{-1}} a_i(y) \hat{a}_j(y^{-1}) \\ &= \begin{cases} 0, & \text{if } D_i \neq D_j^{-1}, \\ |H| |H|^{-2} |H x_j H| = \text{ind } x_j, & \text{if } D_i = D_j^{-1}. \end{cases} \end{aligned}$$

This completes the proof of the proposition.

(11.32) Theorem. Let ψ be a linear character of the subgroup H of G and let \mathcal{H} be the Hecke algebra $\mathcal{H}(G, H, \psi)$.

(i) The central primitive idempotents $\{e\epsilon_i : (\xi^i, \psi^G) \neq 0\}$ of \mathcal{H} (see (11.26)) are given by

$$e\epsilon_i = \xi^i(1)|G:H|^{-1} \sum_{j \in J} (\text{ind } x_j)^{-1} \xi^i(\hat{a}_j) a_j,$$

where $\{a_j\}_{j \in J}$ and $\{(\text{ind } x_j)^{-1} \hat{a}_j\}_{j \in J}$ are the dual bases of \mathcal{H} defined in (11.30iii).

(ii) (Orthogonality relations). Let φ, φ' be irreducible characters of \mathcal{H} . Then

$$\sum_{j \in J} (\text{ind } x_j)^{-1} \varphi(\hat{a}_j) \varphi'(a_j) = \begin{cases} 0, & \varphi \neq \varphi', \\ \varphi(e)|G:H|\xi(1)^{-1}, & \varphi = \varphi', \text{ where } \xi|_{\mathcal{H}} = \varphi. \end{cases}$$

(iii) If $\xi|_{\mathcal{H}} = \varphi$, where $\xi \in \text{Irr } G$ and $(\xi, \psi^G) \neq 0$, then

$$\xi(1) = |G:H|(\xi, \psi^G) \left\{ \sum_{j \in J} (\text{ind } x_j)^{-1} \varphi(\hat{a}_j) \varphi(a_j) \right\}^{-1}.$$

(iv) Let $\xi \in \text{Irr } G$, and assume that $(\xi, \psi^G) \neq 0$. Then

$$\xi(1) \text{ divides } |G:H| \text{ L.C.M. } (\text{ind } x_j).$$

Proof. (i) By (11.26), the elements $\{e\epsilon_i : (\xi^i, \psi^G) \neq 0\}$ are the central primitive idempotents in \mathcal{H} . By (11.29), we have

$$e\epsilon_i = \xi^i(1)|G|^{-1} \sum_{x \in G} \xi^i(ex^{-1}e)exe,$$

for each $\xi^i \in \text{Irr } G$ such that $(\xi^i, \psi^G) \neq 0$. Let $x = hx_j, k \in D_j$, where $h, k \in H$. Then $x^{-1} = k^{-1}x_j^{-1}h^{-1}$, and

$$\begin{aligned} \xi(ex^{-1}e)exe &= \psi(h)\psi(h^{-1})\psi(k)\psi(k^{-1})\xi^i(ex_j^{-1}e)ex_j e \\ &= (\text{ind } x_j)^{-2} \xi^i(\hat{a}_j) a_j, \end{aligned}$$

by definition of $\{a_j\}$ and $\{\hat{a}_j\}$ (see (11.30)). It follows from this formula that

$$\begin{aligned} e\epsilon_i &= \xi^i(1)|G|^{-1} \sum_{j \in J} \sum_{x \in D_j} (\text{ind } x_j)^{-2} \xi^i(\hat{a}_j) a_j \\ &= \xi^i(1)|G|^{-1} \sum_{j \in J} |Hx_j H| (\text{ind } x_j)^{-2} \xi^i(\hat{a}_j) a_j \\ &= \xi^i(1)|G:H|^{-1} \sum_{j \in J} (\text{ind } x_j)^{-1} \xi^i(\hat{a}_j) a_j, \end{aligned}$$

as required, since $|Hx_j H| = |D_j| = (\text{ind } x_j)|H|$.

(ii) Let us set $\varphi_i = \zeta' |_{\mathcal{H}}$ where ζ^i ranges over all characters in $\text{Irr } G$ such that $(\zeta', \psi^G) \neq 0$. By (11.25ii), these φ_i are the irreducible characters of \mathcal{H} . Since $e\epsilon_i$ is the central primitive idempotent in \mathcal{H} corresponding to φ_i , we have

$$\varphi_{i'}(e\epsilon_i) = \begin{cases} 0, & i' \neq i, \\ \varphi_i(e\epsilon_i), & i' = i, \end{cases}$$

where $\varphi_i(e\epsilon_i) = \varphi_i(e)$. Upon substituting the formula for $e\epsilon_i$ from part (i) into this expression, we obtain the orthogonality formulas (ii).

(iii) From part (ii) we have

$$\zeta'(1) = \varphi_i(e) |G : H| \left\{ \sum_{j \in J} (\text{ind } x_j)^{-1} \varphi_i(\hat{a}_j^{-1}) \varphi_i(a_j) \right\}^{-1}.$$

Since $\varphi_i(e) = \zeta'(e) = (\zeta', \psi^G)$ by (11.21), we obtain (iii).

(iv) We may assume K is an algebraic number field which is, as usual, a splitting field for G and all of its subgroups. By (11.24), K is a splitting field for \mathcal{H} .

Let v range over the discrete valuations of K , and let R_v be the valuation ring associated with v . From §4, $\text{alg. int.}\{K\} = \cap_v R_v$.

Now let R be one of the R_v and set

$$\Lambda = \sum_{j \in J} Ra_j,$$

where $\{a_j\}$ is the basis of \mathcal{H} defined in (11.30). Then R is a P.I.D. with quotient field K , and Λ is an R -order* in \mathcal{H} because the structure constants $\{\mu_{ijk}\}$ lie in $\text{alg. int.}\{K\} \subseteq R$, by (11.30ii). Moreover, $\hat{a}_j \in \Lambda$ for all $j \in J$, since \hat{a}_j either coincides with one of the $\{a_j\}$ or differs from one by multiplication by a root of unity. Let $\varphi = \zeta' |_{\mathcal{H}}$ for some $\zeta \in \text{Irr } G$ with $(\zeta, \psi^G) \neq 0$, and let V be a simple \mathcal{H} -module affording φ . Since R is a P.I.D., V is R -free, and hence there exists a full R -lattice M in V such that $\Lambda M \subseteq M$ (see §23). Let $\{m_1, \dots, m_d\}$ be an R -basis of M , hence a K -basis of V , and let $\mathbf{T}: \mathcal{H} \rightarrow M_d(K)$ be the matrix representation of \mathcal{H} afforded by V with respect to this basis. Then

$$\mathbf{T}(a) \in M_d(R), \forall a \in \Lambda.$$

Let $m = \text{L.C.M.}_{j \in J} \{\text{ind } x_j\}$, and set

$$w = m \sum_{j \in J} (\text{ind } x_j)^{-1} \varphi(\hat{a}_j) a_j.$$

Then $w \in \Lambda$ since $\hat{a}_j \in \Lambda$, and $\varphi(\hat{a}_j) = \text{Tr}(\hat{a}_j, M) \in R$. From part (i), w belongs

*See Definition 23.1.

to the center of \mathcal{H} , so

$$\mathbf{T}(w) = \alpha \cdot \mathbf{I}$$

for some $\alpha \in R$, since K is a splitting field for \mathcal{H} , and $w \in \Lambda$. Taking the traces of both sides, we have

$$\varphi(w) = \alpha \varphi(e).$$

By part (i) again,

$$w = m|G:H|\xi(1)^{-1}\epsilon e,$$

where ϵ is the central primitive idempotent of KG associated with ξ . Then

$$\varphi(w) = m|G:H|\xi(1)^{-1}\varphi(e).$$

Comparing these expressions we have

$$m|G:H|\xi(1)^{-1} \in R.$$

Since this formula holds for every valuation ring $R = R_v$, we obtain

$$m|G:H|\xi(1)^{-1} \in \bigcap_v R_v = \mathbb{Q} \cap \text{alg. int.}\{K\} = \mathbb{Z},$$

as required. This completes the proof.

Part (iv) of the preceding theorem was proved independently by a different method by Keller [68]. It includes as a special case the basic result that $\xi'(1)$ divides $|G|$ for all $\xi' \in \text{Irr } G$ (see (9.32)). It also yields other interesting divisibility formulas, such as the following:

(11.33) Corollary (Ito [51]). *Let A be an abelian normal subgroup of G , and let $\xi \in \text{Irr } G$. Then $\deg \xi$ divides $|G:A|$.*

Proof. Since A is abelian, the irreducible characters of A are all linear. By Frobenius Reciprocity, $(\xi, \psi^G) \neq 0$ for some linear character ψ of A , and the result follows from part (iv) of (11.32).

Some aspects of the preceding discussion become significantly simpler in the important case of transitive permutation representations 1_H^G .

(11.34) Proposition. *Let $H \leq G$, let $\psi = 1_H$, and let \mathcal{H} be the Hecke algebra $\mathcal{H}(G, H, 1_H)$. Then the standard basis elements of \mathcal{H} are given by*

$$a_j = |H|^{-1} \sum_{x \in D_j} x, \quad j \in J,$$

where, in this case, $\{D_j\}_{j \in J}$ is the full set of (H, H) -double cosets. The structure constants $\{\mu_{ijk}\}$ associated with the basis $\{a_j\}$ are given by

$$\mu_{ijk} = |H|^{-1} |D_i \cap x_k D_j^{-1}|, \quad x_k \in D_k, \quad i, j, k \in J.$$

Finally, let $\xi \in \text{Irr } G$ appear with nonzero multiplicity in the permutation character $1_H \circ \xi$, and let $\varphi = \xi|_{\mathcal{H}}$ be the corresponding character of the Hecke algebra. Then the character formula (11.28) becomes

$$\begin{aligned} \xi(t) &= |C_G(t)| |H|^{-1} \left\{ \sum_{j \in J} (\text{ind } x_j)^{-1} \varphi(a_j) |\mathfrak{C} \cap D_j| \right\} \\ &\quad \times \left\{ \sum_{j \in J} (\text{ind } x_j)^{-1} \varphi(\hat{a}_j) \varphi(a_j) \right\}^{-1}, \end{aligned}$$

where t belongs to the conjugacy class \mathfrak{C} of G .

Proof. The first two statements are immediate consequences of parts (i) and (ii) of (11.30). For the character formula, Ree's Theorem 11.28 gives

$$\xi(t) = |C_G(t)| \xi(eCe) \left\{ \sum_{x \in G} \xi(ex^{-1}e) \xi(exe) \right\}^{-1}.$$

Since $exe = (\text{ind } x_j)^{-1} a_j$ for all $x \in D_j$, we have

$$\xi(eCe) = \sum_{j \in J} (\text{ind } x_j)^{-1} \varphi(a_j) |\mathfrak{C} \cap D_j|,$$

and

$$\begin{aligned} \sum_{x \in G} \xi(ex^{-1}e) \xi(exe) &= \sum_{j \in J} |D_j| (\text{ind } x_j)^{-2} \xi(\hat{a}_j) \xi(a_j) \\ &= |H| \sum_{j \in J} (\text{ind } x_j)^{-1} \varphi(\hat{a}_j) \varphi(a_j). \end{aligned}$$

From these results we obtain the desired formula for $\xi(t)$, completing the proof.

§11E. Projective Representations and Central Extensions

We have seen in Theorem 11.20 of §11C that Clifford's analysis of the structure of a simple KG -module in terms of a stable simple KH -module, for a normal subgroup H of G , leads in a natural way to the consideration of projective representations of finite groups. In this subsection, we shall give an

account of Schur's theory of projective representations and central extensions of finite groups. Our discussion will follow CR §53, with some additions and improvements from Yamazaki [64], Foote [67], and Isaacs ([76], Chapter 11).

Until further notice, G denotes a finite group and K an arbitrary field. Let $T: G \rightarrow GL(M)$ be a projective representation of G with factor set $\alpha: G \times G \rightarrow K^\circ$, as in Definition 11.19. The map T satisfies the condition

$$T(x)T(y) = \alpha(x, y)T(xy), \quad \forall x, y \in G,$$

and is not in general a homomorphism. Nevertheless, T does define a homomorphism $\tau: G \rightarrow PGL(M)$, where $PGL(M)$ is the *projective general linear group*, given by $PGL(M) = GL(M)/K^\circ \cdot 1_M$, where the set $K^\circ \cdot 1_M$ of nonzero scalar multiples of 1_M coincides with the center of $GL(M)$. The homomorphism τ is given by $\tau = \omega \circ T$, where $\omega: GL(M) \rightarrow PGL(M)$ is the natural homomorphism. We leave it to the reader to check that the map τ is indeed a homomorphism, and that conversely, all homomorphisms from G to $PGL(M)$ arise in this manner. This connection between projective representations and homomorphisms into the projective general linear group explains the terminology.

Now let $S: G \rightarrow GL(M)$ and $T: G \rightarrow GL(N)$ be projective representations of G , with factor sets α and β , respectively. We call S and T *equivalent* if there exists a K -isomorphism $X: M \cong N$ and a map $\mu: G \rightarrow K^\circ$ such that

$$\mu(x)XS(x) = T(x)X, \quad \forall x \in G.$$

When this occurs, the factor sets α and β differ by the principal factor set (see (8.38)) defined by the map μ . Thus we may associate with each equivalence class of projective representations a well defined element of the second cohomology group $H^2(G, K^\circ)$, where G acts trivially on the multiplicative group K° .

Our objective is to show that problems about projective representations of G can be transferred, to a great extent, to problems about representations of certain central extensions of G . We recall from §8C that a *central extension of G with kernel A* is an exact sequence

$$1 \rightarrow A \rightarrow E \xrightarrow{\pi} G \rightarrow 1,$$

with $A = \ker \pi$, and A contained in the center of E . We shall denote such a central extension of G by (E, π) . The factor set $f: G \times G \rightarrow A$ associated with the above central extension (E, π) is defined by

$$f(x, y) = u_x u_y u_{xy}^{-1}, \quad x, y \in G,$$

where $u: G \rightarrow E$ is a π -section (see (8.32) and §8C). In §8B, we defined equivalence of central extensions of G with kernel A , and pointed out that

these equivalence classes are in bijective correspondence with the elements of $H^2(G, A)$, with trivial action of G on A .

A central extension (E, π) of G is said to have the *projective lifting property* (relative to the field K) if every homomorphism $\tau: G \rightarrow PGL(M)$, for a f.d. K -space M , can be completed to a commutative diagram of homomorphisms of groups:

$$\begin{array}{ccccccc} E & \xrightarrow{\pi} & G & \longrightarrow & 1 \\ \downarrow \lambda & & \downarrow \tau & & & & \\ 1 & \longrightarrow & K[1_M] & \xrightarrow{\omega} & GL(M) & \xrightarrow{\tau} & PGL(M) \longrightarrow 1. \end{array}$$

When this can be done, we say that the projective representation of G defined by τ is *lifted* to the (ordinary) representation λ of E . Practically speaking, this means that if $T: G \rightarrow GL(M)$ is any projective representation of G , then there exists an (ordinary) representation $\lambda: E \rightarrow GL(M)$ of E , such that T is equivalent, as a projective representation of G , to the projective representation $\lambda \circ u: G \rightarrow GL(M)$, where $u: G \rightarrow E$ is a π -section.

Schur's theory is concerned with the existence of central extensions of G with the projective lifting property. We shall discuss the problem in the following more general context.

(11.35) Definition. Let G be a group, and B a multiplicative abelian group. A central extension (E, π) of G is said to be *B -universal* if for each central extension (E^*, π^*) of a group G^* with kernel B , and each homomorphism $\theta: G \rightarrow G^*$, there exists a homomorphism $\lambda: E \rightarrow E^*$ such that the diagram

$$\begin{array}{ccccccc} E & \xrightarrow{\pi} & G & \longrightarrow & 1 \\ \downarrow \lambda & & \downarrow \theta & & & & \\ 1 & \longrightarrow & B & \xrightarrow{\pi^*} & E^* & \xrightarrow{\theta} & G^* \longrightarrow 1 \end{array}$$

commutes.

Notice the connection between this concept and the projective lifting property: if (E, π) is a K -universal central extension of G , then (E, π) has the projective lifting property. We now seek a criterion for a given central extension to be B -universal, for an abelian group B . We omit some details in the proofs below, which we feel the reader can easily supply.

Let us first introduce some additional concepts from the theory of cohomology of groups. Let

$$1 \rightarrow A \rightarrow E \xrightarrow{\pi} G \rightarrow 1$$

be a central extension of G with kernel A , and let B be an arbitrary abelian multiplicative group. We let

$$\text{res} : \text{Hom}(E, B) \rightarrow \text{Hom}(A, B)$$

be the homomorphism defined by *restriction* of maps from E to A . Similarly, we define a homomorphism, called *inflation*:

$$\text{inf} : \text{Hom}(G, B) \rightarrow \text{Hom}(E, B),$$

where $\text{inf } \psi = \psi \circ \pi$, for $\psi \in \text{Hom}(G, B)$. There is also an inflation homomorphism

$$\text{inf} : H^2(G, B) \rightarrow H^2(E, B),$$

defined as follows. Let $b \in H^2(G, B)$, and let $f : G \times G \rightarrow B$ be a factor set representing the cohomology class b . Then $\text{inf } b$ is defined as the cohomology class in $H^2(E, B)$ represented by the factor set $g : E \times E \rightarrow B$, where

$$g(u, v) = f(\pi(u), \pi(v)), u, v \in E.$$

Another important homomorphism in this situation is the *transgression map*

$$t : \text{Hom}(A, B) \rightarrow H^2(G, B),$$

defined as follows. Let $f : G \times G \rightarrow A$ be a factor set defined by a π -section from the central extension (E, π) defined above, and let $\varphi \in \text{Hom}(A, B)$. The image of φ under the transgression map t is defined to be the cohomology class $t\varphi \in H^2(G, B)$ with representative factor set

$$(x, y) \mapsto \varphi(f(x, y)), x, y \in G.$$

We leave it to the reader to check that all these maps are well defined homomorphisms. They can be combined to form the *Hochschild-Serre sequence*

$$1 \rightarrow \text{Hom}(G, B) \xrightarrow{\text{inf}} \text{Hom}(E, B) \xrightarrow{\text{res}} \text{Hom}(A, B) \xrightarrow{t} H^2(G, B) \xrightarrow{\text{inf}} H^2(E, B).$$

It can be proved that this sequence is exact (Hochschild-Serre [53]; see also the latter half of the hint in Exercise 25.5). We do not require this fact here, but will merely make use of some of the mappings defined above.

(11.37) Proposition. *The central extension*

$$1 \rightarrow A \rightarrow E \xrightarrow{\pi} G \rightarrow 1, A = \ker \pi,$$

is B -universal, for an abelian group B , if and only if the transgression homomorphism

$$t: \text{Hom}(A, B) \rightarrow H^2(G, B)$$

is surjective.

Proof. Assume the extension (E, π) is B -universal, and let $b \in H^2(G, B)$. By the correspondence between central extensions of G by B and elements of $H^2(G, B)$ (see Rotman [79, Theorem 10.24]), there exists a central extension

$$1 \rightarrow B \rightarrow E^* \xrightarrow{\pi^*} G \rightarrow 1$$

such that the factor set associated with a π^* -section $u^*: G \rightarrow E^*$ is a representative of b . By B -universality, the identity map $1: G \rightarrow G$ can be completed to a commutative diagram

$$\begin{array}{ccccccc} 1 & \longrightarrow & A & \longrightarrow & E & \xrightarrow{\pi} & G \longrightarrow 1 \\ & & & & \downarrow \lambda & & \downarrow 1 \\ 1 & \longrightarrow & B & \longrightarrow & E^* & \xrightarrow{\pi^*} & G \longrightarrow 1. \end{array}$$

It is then easily checked that there exists a homomorphism $\varphi: A \rightarrow B$ making the diagram

$$\begin{array}{ccccccc} 1 & \longrightarrow & A & \longrightarrow & E & \longrightarrow & G \longrightarrow 1 \\ & & \downarrow \varphi & & \downarrow \lambda & & \downarrow 1 \\ 1 & \longrightarrow & B & \longrightarrow & E^* & \longrightarrow & G \longrightarrow 1 \end{array}$$

commutative. For such a map φ , we have $t(\varphi) = b$, and so t is surjective.

Conversely, let $t: \text{Hom}(A, B) \rightarrow H^2(G, B)$ be surjective. Let

$$1 \rightarrow B \rightarrow E^* \xrightarrow{\pi^*} G^* \rightarrow 1, \quad B = \ker \pi^*,$$

be a given central extension of a group G^* by B , and let $\theta: G \rightarrow G^*$ be a homomorphism. We have to construct a homomorphism $\lambda: E \rightarrow E^*$ such that $\pi^* \circ \lambda = \theta \circ \pi$. Let $u: G \rightarrow E$ be a π -section, and $v: G^* \rightarrow E^*$ a π^* -section. Let $f: G \times G \rightarrow A$ be the factor set associated with u , and $g: G^* \times G^* \rightarrow B$ the factor set associated with v . As in the previous discussion, we may form the inflation of g by the homomorphism $\theta: G \rightarrow G^*$, obtaining a factor set $g_\theta: G \times G \rightarrow B$ defined by

$$g_\theta(x, y) = g(\theta(x), \theta(y)), \quad x, y \in G.$$

Since the transgression map t is surjective, we may assume that there exists $\varphi \in \text{Hom}(A, B)$ for which the factor sets

$$g_\theta(x, y) \text{ and } \varphi(f(x, y)), \quad x, y \in G,$$

define the same element of $H^2(G, B)$. Therefore these factor sets differ by a principal factor set, and there exists a function $\tau: G \rightarrow B$ such that $\tau(1)=1$ and

$$\varphi(f(x, y)) = g(\theta(x), \theta(y))\tau(x)\tau(y)\tau(xy)^{-1}, \quad x, y \in G.$$

Now define $\lambda: E \rightarrow E^*$ by

$$\lambda(au_x) = \varphi(a)\tau(x)v_{\theta(x)}, \quad a \in A, x \in G.$$

It is then easily checked that λ is the required homomorphism.

Now let K be an algebraically closed field. We shall use the preceding result to give a new proof of Schur's Theorem (see Schur [04] or CR §53) that a finite group G always has a central extension (E, π) with kernel $H^2(G, K^\times)$ having the projective lifting property. This theorem will follow from the existence of a K^\times -universal central extension of G with kernel $H^2(G, K^\times)$. The connection between projective representations and central extensions is further clarified by the result that any central extension (E, π) of G with the projective lifting property is necessarily a K^\times -universal central extension.

(11.38) Lemma. *Let G be a finite group acting trivially on the multiplicative group K^\times of an algebraically closed field K . Then the second cohomology group $H^2(G, K^\times)$ is finite, of order not divisible by $\text{char } K$. Moreover, the order e of any class $c \in H^2(G, K^\times)$ is a divisor of $|G|$, and c can be represented by a factor set $\alpha: G \times G \rightarrow K^\times$ whose values are e -th roots of unity.*

Proof. Let $c \in H^2(G, K^\times)$, and let $\alpha: G \times G \rightarrow K^\times$ be a representative factor set of c . By Lemma 8.39, the order e of c is a divisor of $|G|$. If $\text{char } K=p > 0$, write $e=p^am$, where m is the p' -part of e . We must prove that $a=0$. We have

$$(11.39) \quad \alpha(x, y)^e = \mu(x)\mu(y)\mu(xy)^{-1},$$

for some principal factor set defined by $\mu: G \rightarrow K^\times$. Since K is algebraically closed of characteristic p , each of its elements has a unique p^a -th root, and we can write

$$(\alpha(x, y)^m)^{p^a} = (\mu(x)^{1/p^a}\mu(y)^{1/p^a}\mu(xy)^{-1/p^a})^{p^a}.$$

Since p^a -th roots are unique in K , we obtain

$$\alpha(x, y)^m = \mu(x)^{1/p^a}\mu(y)^{1/p^a}\mu(xy)^{-1/p^a},$$

which contradicts the assumption that c has order e , unless $p^a = 1$. This proves that c has order not divisible by $\text{char } K$.

Returning to (11.39), for each $x \in G$ we can find an element $\rho(x) \in K^\times$ such that $\rho(x)^e = \mu(x)^{-1}$. Then the map $\alpha': G \times G \rightarrow K^\times$ defined by

$$\alpha'(x, y) = \alpha(x, y)\rho(x)\rho(y)\rho(xy)^{-1}, \quad x, y \in G,$$

is also a representative factor set of c , and by (11.39) we have $\alpha'(x, y)^e = 1$ for all $x, y \in G$. This completes the proof.

Remark. The above proof shows incidentally that for any perfect field K of characteristic $p > 0$, $H^2(G, K^\times)$ contains no nontrivial p -elements, since each element in such a field has a unique p -th root.

(11.40) Theorem. Let G be a finite group, and K an algebraically closed field. Then the following statements hold:

(i) There exists a central extension (E, π) of G with kernel $H^2(G, K^\times)$, such that (E, π) has the projective lifting property.

(ii) Any central extension (E, π) of G with the projective lifting property is a K^\times -universal central extension.

Proof. (i) By Proposition 11.37 and the remark following (11.35), it is sufficient to construct a central extension

$$1 \rightarrow H^2(G, K^\times) \rightarrow E \rightarrow G \rightarrow 1$$

such that the transgression map

$$t: \text{Hom}(H^2(G, K^\times), K^\times) \rightarrow H^2(G, K^\times)$$

is surjective. We may express $H^2(G, K^\times)$ as a direct product of cyclic groups:

$$H^2(G, K^\times) = \langle c_1 \rangle \times \cdots \times \langle c_d \rangle,$$

with generators $\{c_i\}$ of orders $\{e_i\}$ not divisible by the characteristic of K , by Lemma 11.38. Since K is algebraically closed, for each i we can choose a primitive e_i -th root of unity ξ_i in K (the $\{\xi_i\}$ need not be distinct). By (11.38) again, for each i there exists a representative factor set α_i of $\langle c_i \rangle$ such that

$$\alpha_i(x, y) = \xi_i^{a_i(x, y)}, \quad x, y \in G, \quad 1 \leq i \leq d,$$

where the exponents $a_i(x, y)$ are uniquely determined integers such that $0 \leq a_i(x, y) < e_i$, $x, y \in G$, $1 \leq i \leq d$. For each pair $x, y \in G$, let

$$a(x, y) = c_1^{a_1(x, y)} \cdots c_d^{a_d(x, y)}.$$

The condition (8.37) gives

$$\alpha_i(y, z)\alpha_i(x, yz) = \alpha_i(xy, z)\alpha_i(x, y), \quad 1 \leq i \leq d,$$

which implies that for each i ,

$$\alpha_i(y, z) + \alpha_i(x, yz) \equiv \alpha_i(xy, z) + \alpha_i(x, y) \pmod{e_i}$$

for all $x, y, z \in G$. Since c_i has order e_i , for $1 \leq i \leq d$, it follows that $a(x, y)$ satisfies the condition (8.37), and defines a factor set $a: G \times G \rightarrow H^2(G, K^\circ)$. From §8B (see also Exercise 11.15), there exists a central extension

$$1 \rightarrow H^2(G, K^\circ) \rightarrow E \xrightarrow{\pi} G \rightarrow 1$$

such that a is the factor set associated with some π -section.

It remains to prove that the transgression map $t: \text{Hom}(H^2(G, K^\circ), K^\circ) \rightarrow H^2(G, K^\circ)$ is surjective. Let b be an arbitrary element of $H^2(G, K^\circ)$. Then $b = \prod_{i=1}^d c_i^{b_i}$, $b_i \in \mathbb{Z}$, and it follows that

$$\beta(x, y) = \prod_{i=1}^d \zeta_i^{b_i a(x, y)}, \quad x, y \in G,$$

is a representative factor set of b . Then there is a well defined homomorphism $\varphi: H^2(G, K^\circ) \rightarrow K^\circ$ such that

$$\varphi(c_i) = \zeta_i^{b_i}, \quad 1 \leq i \leq d,$$

and for this homomorphism we have

$$\varphi(a(x, y)) = \beta(x, y), \quad x, y \in G.$$

Then $t(\varphi) = b$, and we have proved that t is surjective, completing the proof of (i).

(ii) Let (E, π) be a central extension

$$1 \rightarrow A \rightarrow E \xrightarrow{\pi} G \rightarrow 1$$

with the projective lifting property, and let $f: G \times G \rightarrow A$ be a factor set associated with a π -section $u: G \rightarrow E$. In order to prove that (E, π) is a K° -universal central extension, it is sufficient by (11.37) to prove that the transgression map $t: \text{Hom}(A, K^\circ) \rightarrow H^2(G, K^\circ)$ is surjective. Let $a \in H^2(G, K^\circ)$, and let $\alpha: G \times G \rightarrow K^\circ$ be a representative factor set of a . By Exercise 11.10 there exists a projective K -representation $T: G \rightarrow GL(M)$ with factor set α . Letting $\tau: G \rightarrow PGL(M)$ be the corresponding homomorphism as

above, by the projective lifting property there exists a homomorphism $\lambda: E \rightarrow GL(M)$ such that the diagram

$$\begin{array}{ccccccc} 1 & \longrightarrow & A & \longrightarrow & E & \xrightarrow{\pi} & G & \longrightarrow 1 \\ & & & & \downarrow \lambda & & \downarrow \tau & \\ 1 & \longrightarrow & K^1_M & \longrightarrow & GL(M) & \xrightarrow{\omega} & PGL(M) & \longrightarrow 1 \end{array}$$

is commutative. Then the restriction $\varphi = \lambda|_A$ satisfies the condition $\varphi(A) \leq \ker \omega = K^1_M$, so we may view φ as an element of $\text{Hom}(A, K^1)$. Moreover, from the formula

$$u_x u_y = f(x, y) u_{xy}, \quad \forall x, y \in G,$$

we obtain

$$\lambda(u_x)\lambda(u_y) = \varphi(f(x, y))\lambda(u_{xy}).$$

The projective lifting property implies that the projective representation $x \rightarrow \lambda(u_x)$ of G is equivalent to T ; hence the factor set $\varphi \circ f$ is equivalent to the given factor set α , and we have $t(\varphi) = a$. Thus t is surjective, and the proof is completed.

For the remainder of this subsection, K always denotes an algebraically closed field of characteristic zero. In this situation, we shall obtain a group-theoretical characterization of minimal central extensions with the projective lifting property. This characterization can be used to discuss the uniqueness of such groups, and to investigate the structure of $H^2(G, K^1)$ (see Huppert [67], Kap. V, §23–25).

(11.41) Definition. A *representation group* of a finite group G is a central extension (E, π) of minimal order with the projective lifting property. The *Schur multiplier* of G is the cohomology group $H^2(G, K^1)$.

By Lemma 11.38, it follows easily that since K is algebraically closed, of characteristic zero, we have $H^2(G, K^1) \cong H^2(G, \mathbb{C})$, where \mathbb{C} is the complex field.

(11.42) Lemma. Let (E, π) be a central extension of G of finite order, with kernel A , and let $t: \text{Hom}(A, K^1) \rightarrow H^2(G, K^1)$ be the transgression map. Then

$$\ker t = (A \cap E')^\perp$$

where E' is the commutator subgroup of E , and

$$(A \cap E')^\perp = \{\varphi \in \text{Hom}(A, K^1) : A \cap E' \leq \ker \varphi\}.$$

Proof. Each $\varphi \in (A \cap E')^\perp$ can be extended to a linear K -character $\tilde{\varphi}$ of AE' , where

$$\tilde{\varphi}(au) = \varphi(a), \forall a \in A, u \in E'.$$

Then $E' \leq \ker \tilde{\varphi}$, and since every linear character of the finite abelian group AE'/E' can be extended to a character of E/E' (by Exercise 11.17), there exists a linear K -character ψ of E extending φ . Let $a: G \times G \rightarrow A$ be a factor set associated with a π -section $u: G \rightarrow E$ of the extension (E, π) . Applying ψ to the formula

$$u_x u_y = a(x, y) u_{xy}, \forall x, y \in G,$$

we obtain

$$\psi(u_x)\psi(u_y) = \varphi(a(x, y))\psi(u_{xy}).$$

Thus $\varphi \circ a$ is a principal factor set defined by the mapping $x \mapsto \psi(u_x) \in K^\times$, and we have shown that $\varphi \in \ker t$.

Conversely, let $\varphi \in \ker t$; then $\varphi \circ a$ is a principal factor set, and we have

$$\varphi(a(x, y)) = \mu(x)\mu(y)\mu(xy)^{-1}, \forall x, y \in G,$$

for some map $\mu: G \rightarrow K^\times$. Define a map $\tilde{\varphi}: E \rightarrow K^\times$ by setting $\tilde{\varphi}(au_x) = \varphi(a)\mu(x)$, $a \in A$, $x \in G$. Then it is easily checked that $\tilde{\varphi}$ is a linear K -character of E . Hence $E' \leq \ker \tilde{\varphi}$, and $E' \cap A \leq \ker \varphi$, as required.

(11.43) Theorem. *Let G be a finite group. Then representation groups of G exist, and are characterized as follows: a central extension (E, π) of G with kernel A is a representation group if and only if $A \leq E'$ and $|A| = |H^2(G, K^\times)|$. If these conditions are satisfied then, in addition, $A \cong H^2(G, K^\times)$.*

Proof. Representation groups certainly exist, by Theorem 11.40i. Let (E, π) be any one of them, and let A be the kernel. By (11.40ii), the transgression map $t: \text{Hom}(A, K^\times) \rightarrow H^2(G, K^\times)$ is surjective. Since $|\text{Hom}(A, K^\times)| = |A|$ for every finite abelian group A and every algebraically closed field K of characteristic zero, we have

$$|A| = |\text{Hom}(A, K^\times)| \geq |H^2(G, K^\times)|.$$

Since there exists a representation group with kernel $H^2(G, K^\times)$ by (11.40), and since (E, π) has minimal order, it follows that

$$|A| = |H^2(G, K^\times)|$$

for any representation group (E, π) . From this equality, since $|A| =$

$|\text{Hom}(A, K^\cdot)|$ and t is surjective, it follows that $\ker t = 1$. Therefore $A \cap E' = A$, and $A \leq E'$. Finally, we have shown that t is an isomorphism; hence $A \cong \text{Hom}(A, K^\cdot) \cong H^2(G, K^\cdot)$, using Exercise 11.16.

Conversely, let (E, π) be a central extension with kernel A such that the conditions $|A| = |H^2(G, K^\cdot)|$ and $A \leq E'$ are satisfied. We have to prove that (E, π) is a representation group, and for this it suffices to show that the transgression map

$$t: \text{Hom}(A, K^\cdot) \rightarrow H^2(G, K^\cdot)$$

is surjective. Since $A \leq E'$, we can apply Lemma 11.42 to obtain

$$\ker t = (A \cap E')^\perp = A^\perp = 1.$$

Since t is injective, and $|\text{Hom}(A, K^\cdot)| = |A| = |H^2(G, K^\cdot)|$ by assumption, it follows that t is surjective, as required. This completes the proof.

Example. Let K be the complex field, and G a metacyclic group given by

$$G = \langle a, b : a^m = 1, b^s = a^t, bab^{-1} = a^r \rangle.$$

Since b^s commutes with a , and b commutes with a^t , the positive integers m, r, s and t must satisfy the conditions that

$$r^s \equiv 1 \pmod{m}, \quad m|t(r-1).$$

We shall show how to compute $H^2(G, K^\cdot)$ by brute force.

Each factor set $f: G \times G \rightarrow K^\cdot$ gives rise to a twisted group algebra

$$(KG)_f = \bigoplus_{x \in G} Ku_x,$$

where the $\{u_x\}$ are units which commute with the elements of K , and where multiplication is given by

$$u_x u_y = f(x, y) u_{xy} \text{ for all } x, y \in G.$$

Replacing each u_x by $\alpha_x u_x$, with $\alpha_x \in K^\cdot$, replaces f by an equivalent factor set.

For convenience of notation, put $u_a = A$, $u_b = B$. We may then suppose (after suitable basis changes) that

$$A^m = 1, \quad B^s = A^t, \quad u_{a^i b^j} = A^i B^j \text{ for } 0 \leq i \leq m, 0 \leq j \leq s,$$

and that

$$BA = \xi A' B$$

for some $\xi \in K^\times$. We find readily that for each $i, j \in \mathbb{Z}$,

$$B^j A^i = \xi^{i(1+r+\cdots+r^{j-1})} A^{ir^j} B^j.$$

Taking $i=t, j=1$, and then $i=1, j=s$, we find that ξ must be a k -th root of 1, where $k = \text{G.C.D.}(t, 1+r+\cdots+r^{s-1})$. Further, each such choice for ξ yields a possible factor set.

On the other hand, we may replace A by ωA , and B by ζB , where ω and ζ are roots of unity such that

$$\omega^m = 1 \text{ and } \zeta^s = \omega^t.$$

This has the effect of replacing ξ by $\xi \omega^{r-1}$. The above conditions easily imply that $\omega^{(r-1)k} = 1$, so ω^{r-1} is a k -th root of 1, and $m|(r-1)k$. It follows that $l|k$, where $l=m/(r-1, m)$, and that ω^{r-1} ranges over all l -th roots of 1. Therefore

$$H^2(G, K^\times) \cong (\mathbb{Z}/k\mathbb{Z})/(q\mathbb{Z}/k\mathbb{Z}) \cong \mathbb{Z}/q\mathbb{Z},$$

where $q=k/l=k(r-1, m)/m$.

The representation group of G is therefore given by

$$G^* = \langle a, b, c : a^m = 1, b^s = a^t, c^q = 1, bab^{-1} = ca^r, ca = ac, cb = bc \rangle,$$

and $G \cong G^*/\langle c \rangle$.

For other calculations of this type, and other approaches to such computations, see Huppert [67].

We conclude with some applications of the preceding results. A projective representation $T: G \rightarrow GL(M)$ is called *irreducible* if M has no proper K -subspaces invariant under the set of linear transformations $\{T(x) : x \in G\}$.

(11.44) Proposition. *The degrees of the irreducible projective representations of G in an algebraically closed field K of characteristic zero are divisors of $|G|$.*

Proof. By Theorem 11.43, there exists a representation group (E, π) . Each irreducible projective representation $T: G \rightarrow GL(M)$ can be lifted to a representation $\lambda: E \rightarrow GL(M)$. It is clear that λ is an irreducible representation of E and that $\deg T = \deg \lambda$. Since K is algebraically closed and of characteristic zero, $\deg \lambda$ divides $|E : A|$ by Ito's Theorem (Corollary 11.33). But $|E : A| = |G|$, so the result follows.

We now return to the important problem of extendability of irreducible invariant K -characters ψ of a normal subgroup H of a finite group G (see §11B).

(11.45) Proposition. Let $H \trianglelefteq G$, and let ψ be an irreducible invariant K -character of H , that is, a character which coincides with all of its G -conjugates. If the Schur multiplier of G/H is trivial, that is, $H^2(G/H, K^\times) = 1$, then ψ can be extended to an irreducible K -character of G .

Proof. Let L be a simple KH -module affording ψ , and M a simple KG -module with $L \subseteq M_H$. By Cliffords Theorem 11.20,

$$M \cong L \otimes_K I,$$

where L and I afford projective representations U of G on L , and V of G/H on I , respectively. Since $H^2(G/H, K^\times) = 1$, we may assume that V is an ordinary representation of G/H (see Exercise 11.11). Hence U is an ordinary representation of G on L extending the action of H , and ψ can be extended to a character of G , as required.

(11.46) Proposition. Let p be a prime divisor of $|H^2(G, K^\times)|$. Then each Sylow p -subgroup of G is non-cyclic.

Proof (Isaacs [76], p. 186). By (11.43), there exists a representation group (E, π) . Let $A = \ker \pi$, so $E/A \cong G$; let S be a subgroup of E such that S/A is a Sylow p -subgroup of E/A , and suppose that S/A is cyclic. Since A is central in E , S is abelian, and it follows that E has an abelian Sylow p -subgroup. By Exercise 11.12, $p \nmid |E' \cap Z(E)|$, where $Z(E)$ is the center of E . Since $A \leq E' \cap Z(E)$ and $A \cong H^2(G, K^\times)$ by (11.43), we have $p \nmid |H^2(G, K^\times)|$, contrary to assumption.

Combining the last two results, we obtain:

(11.47) Corollary. Let $H \trianglelefteq G$, and let ψ be an irreducible invariant K -character of H . If G/H is cyclic, then ψ can be extended to a K -character of G .

Proof. By Proposition 11.46, $H^2(G/H, K^\times) = 1$. Then ψ can be extended to a character of G by Proposition 11.45.

§11. Exercises

All representations and characters are taken in an algebraically closed field K of characteristic 0, unless otherwise specified.

1. A finite group G is called *supersolvable* if there exists a normal series

$$G = G_1 \geq G_2 \geq \cdots \geq G_{s+1} = 1,$$

with cyclic factors of prime order, where each $G_i \trianglelefteq G$. (See §1B).

(i) Prove that there are inclusions

$$\{\text{nilpotent groups}\} \subseteq \{\text{supersolvable groups}\} \subseteq \{\text{solvable groups}\},$$

with strict inclusions at each stage.

(ii) Prove that supersolvable groups are M -groups.

[Hint: First prove that subgroups and homomorphic images of supersolvable groups are supersolvable, so that we can reduce to the case of a faithful irreducible representation (as in the proof of (11.3)). Then show that each non-abelian supersolvable group has an abelian normal subgroup not contained in the center, and apply (11.2).]

2. Find an example of a solvable group which is not an M -group.

3. Let $H \trianglelefteq G$, and let $\psi \in \text{Irr } H$, $\xi \in \text{Irr } G$, and assume $(\xi, \psi^G) > 0$. In (11.4), it was proved that there exists a character $\mu \in \text{Irr } G_\psi$ such that $\xi = \mu^G$ and $\mu_H = a\psi$ for some $a \in \mathbb{Z}$. Prove that μ is uniquely determined by these conditions.

4. Let E be a field of characteristic $p > 0$, and let H be a normal p -subgroup of a finite group G . Prove that H acts trivially on every simple EG -module.

[Hint: Use (11.1) and (5.24).]

5. Let G be the group of all rigid motions of a cube. Show that $|G| = 48$, and that G is isomorphic to the group of signed permutations.

$$\left\{ \begin{pmatrix} 1 & 2 & 3 \\ \pm i_1 & \pm i_2 & \pm i_3 \end{pmatrix}, 1 \leq i_j \leq 3 \right\}.$$

Show that the subgroup H , consisting of all permutations

$$\begin{pmatrix} 1 & 2 & 3 \\ \pm 1 & \pm 2 & \pm 3 \end{pmatrix},$$

is an abelian normal subgroup of G , and that $G = H \rtimes S$, for a subgroup $S \cong S_3$. Find $\text{Irr } G$. In particular, find the degree of each $\xi \in \text{Irr } G$, and express ξ in the form $(\tilde{\psi}\omega)^G$, where $\psi \in \text{Irr } H$, $\tilde{\psi}$ is the extension of ψ to G_ψ , and $\omega \in \text{Irr}(G_\psi/H)$.

[Hint: First show that the non-conjugate characters ψ of H can be described by the notations $(+++)$, $(++-)$, $(+-)$ and $(--)$, according as ψ takes a generator of H to $+1$ or -1 . Show that for these 4 choices of the character ψ , G_ψ/H has the structure S_3 , $S_2 \times S_1$, $S_1 \times S_2$, and S_3 , respectively. Then apply (11.8). The same method applies to the *hyper-octahedral* group, which is the symmetry group of an n -dimensional cube.]

6. Let H be a finite group whose characters are known, and let G be a semidirect product $(H \times H) \rtimes \langle \tau \rangle$, where τ has order 2 and acts on the direct product $H \times H$ as follows:

$$\tau(h, h')\tau^{-1} = (h', h), \forall h, h' \in H.$$

Show how to construct $\text{Irr } G$ from a knowledge of $\text{Irr } H$.

[Hint: Let $\varphi, \psi \in \text{Irr } H$. Prove that

$$(\varphi \cdot \psi)^G \in \text{Irr } G \text{ if } \varphi \neq \psi,$$

and that

$$(\varphi \cdot \varphi)^G = \zeta + \epsilon \zeta,$$

where ζ is an extension of $\varphi \cdot \varphi$ to G , and ϵ is the non-trivial character of $G/(H \times H)$. Prove that every irreducible character of G is obtained by one or the other of these constructions. The extension of $\varphi \cdot \varphi$ to G is obtained as follows. Let V be a KH -module affording φ ; then $V \# V$ affords $\varphi \cdot \varphi$. Prove that the action of τ on $V \otimes V$ given by $v \otimes v' \rightarrow v' \otimes v$, $v, v' \in V$, extends the action of $H \times H$.] (We remark that the group G is the *wreath product* $H \wr Z_2$ (see Hall [59, p. 81] or Huppert [67, p. 94]). Representations of wreath products were discussed in general by Kerber [68]. For extensions of the method, and applications to chemistry, see Alvis-Curtis-Dyke-Odutola [81].)

7. A metacyclic group G has a presentation

$$\langle a, b : a^m = 1, bab^{-1} = a^r, b^s = a^t \rangle,$$

where $\{m, s, r, t\}$ are integers such that

$$(m, r) = 1, m | t(r-1), m | (r^s - 1) \quad (\text{see CR §47}).$$

Find $\text{Irr } G$.

[Hint: First prove that if $H = \langle a \rangle$, then $H \leq G$, and each $\psi \in \text{Irr } H$ has an extension $\tilde{\psi}$ to G_ψ . Describe $\tilde{\psi}$ explicitly. Then apply (11.5) to construct $\text{Irr } G$.] (We remark that this exercise provides an illustration of (11.47), and includes more general cases than in (11.8), where G is assumed to be a semidirect product.)

8. Let A be an S -graded R -algebra, and let L, E , etc., be as in (11.14) and (11.15). Let $T \leq S$,

$$B = \sum_{t \in T} A_t, \quad L^B = \sum_t (a_t \otimes L) \subseteq L^A,$$

and $E_T = \sum_{t \in T} E_t$. Prove that $E_T \cong \text{End}_B L^B$, where the isomorphism is given by restriction of $f \in E_T \subseteq E$ to the submodule L^B .

9. Let $T: G \rightarrow GL(M)$ be a projective representation with factor set α , and let $d = \dim_K M$. Prove that $\alpha^d \sim 1$, that is, α^d is equivalent to a principal factor set.

[Hint: Take the determinant of both sides in the formula for $T(x)T(y)$.]

10. Let $\alpha: G \times G \rightarrow \mathbb{C}^\times$ be a factor set. Prove that there exists an irreducible projective representation of G with factor set α .

[Hint: Let $(KG)_\alpha$ be the twisted group algebra with factor set α (see (8.33ii)). Then show that each simple $(KG)_\alpha$ -module defines an irreducible projective representation of G with factor set α .]

11. Prove that if $H^2(G, K^\times) = 1$, then every irreducible projective representation of G with factor set α is equivalent to an ordinary representation.

[Hint: Use (11.43).]

12. Let p be a prime. Prove that if G has an abelian Sylow p -subgroup, then p does not divide $|G' \cap Z(G)|$, where G' is the derived group of G , and $Z(G)$ the center of G .

13. In (11.20), prove that if the action of H on L can be extended to an action of G on L , then both U and V can be taken to be ordinary representations.

14. Use the preceding exercise and (11.20) to prove that if K is an algebraically closed field (of any characteristic), and $G = G_1 \times G_2$, then every simple KG -module can be expressed in the form $L_1 \# L_2$, for simple modules L_1 and L_2 over KG_1 and KG_2 , respectively. (See also §10E.)

15. Let $\alpha: G \times G \rightarrow A$ be a factor set taking values in an abelian multiplicative group A , with G acting trivially on A . Prove that there exists a central extension

$$1 \rightarrow A \rightarrow E \xrightarrow{\pi} G \rightarrow 1$$

such that α is the factor set associated with some π -section.

16. Prove that every finite abelian group A is isomorphic to its character group $\text{Hom}(A, K^\times)$ (where K is algebraically closed and of characteristic 0.)

17. Let B be a subgroup of a finite abelian group A . Prove that every linear character $\lambda: B \rightarrow K^\times$ can be extended to a character of A .

[Hint: Consider the irreducible constituents of λ^A .]

18. Let $\mathcal{H}(G, H, \psi)$ be a Hecke algebra, as in (11.22). Prove that $\mathcal{H}(G, H, \psi)$ is a commutative algebra if and only if ψ^G is multiplicity-free, in the sense that

$$(\xi, \psi^G) = 0 \text{ or } 1 \quad \forall \xi \in \text{Irr } G.$$

19. The linear map $\text{ind}: \mathcal{H}(G, H, 1_H) \rightarrow K$, defined by $\text{ind}(a_j) = \text{index of } x_j$, where $x_j \in D_j$, is a homomorphism of K -algebras, corresponding to the trivial character 1_G according to (11.25).

The following result gives a useful method for computing degrees of irreducible components of permutation characters 1_H^G (compare with (11.32iii)).

20. (D. G. Higman [67]). Let $\mathcal{H} = \mathcal{H}(G, H, 1_H)$ be the Hecke algebra of a permutation representation 1_H^G , and assume that $\mathcal{H} = K[a_1]$ for some standard basis element a_1 (see (11.34)). Let $e = |H|^{-1} \sum_{h \in H} h$, $V = KG$, and view V as a (KG, \mathcal{H}) -bimodule, with $\mathcal{H} = eKG$ acting on the right in the obvious way. Let \mathbf{M} be the matrix of right multiplication by a_1 on \mathcal{H} , and \mathbf{A} the matrix of right multiplication by a_1 on V . The matrix \mathbf{M} is determined by the structure constants $\{\mu_{ijk}\}$, and is called the *intersection matrix* of the permutation representation. Prove that the following statements hold:

- (i) The minimal polynomials of \mathbf{M} and \mathbf{A} coincide, and are both equal to char. pol. \mathbf{M} .
- (ii) Let $p(t) = \text{char. pol. } \mathbf{M}$. Then $p(t)$ has distinct zeros $\{\theta_1, \dots, \theta_m\}$. The simple KG -submodules of V all appear with multiplicity 1, and coincide with the eigenspaces $\{V_{\theta_i}\}$ corresponding to the eigenvalues $\{\theta_i\}$ of \mathbf{A} .
- (iii) For each i , $1 \leq i \leq m$, let $p_i(t) = p(t)/(t - \theta_i)$. Then

$$\dim_K V_{\theta_i} = \frac{\text{Trace } p_i(\mathbf{A})}{p_i(\theta_i)}.$$

- (iv) Let $a_1^s = \sum_{i=0}^m \eta_{si} a_i$, $s = 1, 2, \dots$, where $a_0 = e$, and $\{a_0, \dots, a_m\}$ are the standard basis elements of \mathcal{K} . Then

$$\text{Trace } \mathbf{A}^s = |G:H| \eta_{s0},$$

so the dimensions of the simple submodules of 1_H^G given in (iii) are effectively computable from the intersection matrix \mathbf{M} .

[Hint: (i) We have $\mathcal{K} \cong K[t]/(m(t))$, where $m(t) = \min. \text{ pol. } \mathbf{M}$. Since \mathcal{K} is semisimple, and K is algebraically closed, $m(t)$ has distinct roots in K . Therefore $m(t) = p(t)$, where $p(t) = \text{char. pol. } \mathbf{M}$. From $p(\mathbf{M}) = \mathbf{0}$ we obtain $p((a_1)_r) = 0$; therefore $p(a_1) = 0$, since the map $a \mapsto a_r$, $a \in \mathcal{K}$, is a faithful representation. Then $V \cdot p(a_1) = 0$, and hence $p(\mathbf{A}) = \mathbf{0}$, so min. pol. \mathbf{A} divides $p(t)$. On the other hand, $\mathcal{K} = eKG e \subseteq V$, and \mathcal{K} is stable under right multiplication by a_1 on V . Hence for each polynomial $f(t) \in K[t]$, $f(\mathbf{A}) = \mathbf{0}$ implies that $\mathcal{K}f(a_1) = 0$, and therefore $p(t) \mid f(t)$.]

- (ii) By Exercise 18, 1_H^G is multiplicity-free, since \mathcal{K} is commutative. The irreducible characters ξ^i occurring in 1_H^G are afforded by submodules

$$e_i V = V e_i e, \text{ where } e_i \text{ is as in (11.26).}$$

Now $e_i e$ is a central primitive idempotent in \mathcal{K} by (11.26), and it follows that $e_i V = V_{\theta_i}$ for some θ_i , $1 \leq i \leq m$.

- (iii) The matrix \mathbf{A} is semisimple, with eigenvalues $\{\theta_i\}$. Hence for each $f(t) \in K[t]$, we have

$$\text{Tr } f(\mathbf{A}) = \sum_i (\dim V_{\theta_i}) f(\theta_i).$$

In particular, for each j we obtain

$$\text{Tr } p_j(\mathbf{A}) = \sum_i (\dim V_{\theta_i}) p_j(\theta_i) = (\dim V_{\theta_j}) p_j(\theta_j),$$

which is (iii).

- (iv) It is sufficient to check that if $a_j^s = \sum_0^{m-1} \eta_{sj} a_i$, $s = 1, 2, \dots$, then $\text{Tr}((a_0)_r, V) = |G:H|$ and $\text{Tr}((a_i)_r, V) = 0$ for $i \neq 0$. The first statement is clear since e acts as the

identity on V , and $\dim V = |G : H|$. Secondly, $V = KGe$ has a basis $\{hx_j e\}$ corresponding to the left H -cosets in the double cosets $\{D_j\}$. Right multiplication by a_i on these elements yields

$$(*) \quad (hx_j e)a_i = \sum \alpha(i; h, x_j, h', x_{j'})h'x_{j'}e,$$

with non-negative integer coefficients $\alpha(i; h, x_j, h', x_{j'})$, describing the partitioning of $hx_j D_i$ into H -cosets. For $i \neq 0$, a simple calculation shows that if $\text{Tr}((a_i)_r, V) \neq 0$, then some diagonal coefficient $\alpha(i; h_i, x_i, h_i, x_i) \neq 0$, and upon multiplication of $(*)$ by $(hx_j)^{-1}$, we obtain $D_i \cap H \neq \emptyset$, which is impossible.]

§12. TENSOR ALGEBRAS

We have already made frequent use of the fact that if M and N are left RG -modules, then $M \otimes_R N$ is a left RG -module, under the diagonal action of G . In this section we extend the scope of this construction to define actions of G on tensor algebras, and on exterior and symmetric algebras. In this context we shall define the Adams operators on the ring of virtual characters of G , and develop some of their basic properties. We finally present a result of Mackey on symmetric and antisymmetric squares of induced modules, relating the tensor constructions to the results of §10.

§12A. Tensor Algebras

Throughout this subsection, R denotes a commutative ring, G a group (not necessarily finite), and M a left RG -module. Unless otherwise stated, \otimes means \otimes_R . For each positive integer n , let

$$\otimes^n M = M \otimes \cdots \otimes M \text{ (n factors).}$$

Then $\otimes^n M$ is a left RG -module on which G acts diagonally:

$$g(m_1 \otimes \cdots \otimes m_n) = gm_1 \otimes \cdots \otimes gm_n, \quad g \in G, m_i \in M.$$

We interpret $\otimes^0 M$ as the RG -module R , on which G acts trivially. In much of the discussion to follow, the R -homomorphisms to be defined are automatically RG -homomorphisms, and the group G plays only a secondary role in the considerations.

There is an obvious homomorphism

$$(\otimes^k M) \otimes (\otimes^n M) \rightarrow \otimes^{k+n} M,$$

which we regard as multiplication of tensors, and denote by \otimes . We then put

$$T(M) = \coprod_{n=0}^{\infty} \otimes^n M = R \oplus M \oplus (M \otimes M) \oplus \cdots,$$

and call $\mathbf{T}(M)$ the *tensor algebra* of M . Clearly $\mathbf{T}(M)$ is an associative noncommutative R -algebra, and is also a left RG -module.

In case $M = \bigoplus_{i \in I} Rm_i$ is R -free, the elements

$$\{m_{i_1} \otimes \cdots \otimes m_{i_n} : i_1, \dots, i_n \in I\}$$

form a free R -basis for $\otimes^n M$. (We have previously used the fact that if $N = \bigoplus Rn_j$ is also R -free, then $\{m_i \otimes n_j\}$ forms a free R -basis for $M \otimes N$.) Further, if the index set I is finite, then $\otimes^n M$ affords the matrix representation

$$g \rightarrow \mathbf{M}(g) \otimes \cdots \otimes \mathbf{M}(g) \quad (n \text{ factors}), \quad g \in G,$$

where \mathbf{M} is the matrix representation of G afforded by M . If μ is the R -character afforded by M , then the R -character afforded by $\otimes^n M$ is the n -th power μ^n of μ .

In general, we remark that $\mathbf{T}(M)$ is a *graded* R -algebra, consisting of the ring R at degree zero, and the R -module $\otimes^n M$ at degree n , for $n \geq 1$. Each RG -homomorphism $M \rightarrow N$ gives rise to an R -algebra homomorphism $\mathbf{T}(M) \rightarrow \mathbf{T}(N)$, which is also a homomorphism of RG -modules. Finally, we note that

$$g(t \pm t') = gt \pm gt', \quad g(t \otimes t') = gt \otimes gt', \quad g \in G, \quad t, t' \in \mathbf{T}(M).$$

We next define the *symmetric algebra* $\mathbf{S}(M)$ of a left RG -module M . The elements of $\mathbf{S}(M)$ are finite sums of the form $\sum m_1 \vee \cdots \vee m_r$, $m_i \in M$, with the property that

$$m_1 \vee \cdots \vee m_r = m_{i_1} \vee \cdots \vee m_{i_r},$$

for any permutation $\{1, 2, \dots, r\} \rightarrow \{1', 2', \dots, r'\}$. In order to construct $\mathbf{S}(M)$, let J be the two-sided ideal in the tensor algebra $\mathbf{T}(M)$ generated by $\{m \otimes m' - m' \otimes m : m, m' \in M\}$, and set

$$\mathbf{S}(M) = \mathbf{T}(M)/J = \prod_{n=0}^{\infty} (\otimes^n M)/(J \cap \otimes^n M).$$

For each $x \in G$, we have

$$x(m \otimes m' - m' \otimes m) = xm \otimes xm' - xm' \otimes xm,$$

and it follows that J is an RG -submodule of $\mathbf{T}(M)$. Therefore $\mathbf{S}(M)$ is a commutative graded R -algebra:

$$\mathbf{S}(M) = \prod_{r=0}^{\infty} \mathbf{S}'(M),$$

and each submodule $\mathbf{S}'(M)$ is an RG -submodule, whose elements are called

symmetric tensors of degree r. The elements of $\mathbf{S}'(M)$ have the form

$$\sum m_1 \vee \cdots \vee m_r, \quad m_i \in M,$$

where $m_1 \vee \cdots \vee m_r = (m_1 \otimes \cdots \otimes m_r) + J$. We shall also use the notations

$$M \vee M = \mathbf{S}^2(M), \quad \underbrace{M \vee \cdots \vee M}_r = \mathbf{S}'(M).$$

In the special case where $M = \bigoplus_{i \in I} Rm_i$ is R -free, with R -basis $\{m_i\}_{i \in I}$ for some ordered set of indices I , the elements

$$\{m_{i_1} \vee \cdots \vee m_{i_r} : i_1 \leq i_2 \leq \cdots \leq i_r, i_k \in I\},$$

form a free R -basis for the symmetric tensors $\mathbf{S}'(M)$ of degree r .

As in the case of the tensor algebra, each RG -homomorphism $M \rightarrow N$ gives rise to an RG -homomorphism $\mathbf{S}(M) \rightarrow \mathbf{S}(N)$, such that $\mathbf{S}'(M) \rightarrow \mathbf{S}'(N)$, $r = 0, 1, 2, \dots$. We leave it to the reader to check that there is an RG -isomorphism

$$(12.1) \quad \mathbf{S}(M \oplus N) \cong \mathbf{S}(M) \otimes_R \mathbf{S}(N),$$

and

$$\mathbf{S}'(M \oplus N) \cong \prod_{k=0}^r \{\mathbf{S}^k(M) \otimes_R \mathbf{S}^{r-k}(N)\}.$$

We note that (12.1) is also an isomorphism of commutative R -algebras.

Another important construction involving $\mathbf{T}(M)$ leads to the *exterior algebra* $\wedge(M)$ of an RG -module M . The elements of $\wedge(M)$ are finite sums of the form $\sum m_1 \wedge \cdots \wedge m_r$, $m_i \in M$, with

$$m_{i'} \wedge \cdots \wedge m_{r'} = \epsilon(m_1 \wedge \cdots \wedge m_r),$$

where ϵ is the sign of the permutation $1 \rightarrow i', \dots, r \rightarrow r'$. To construct $\wedge(M)$, let I be the two-sided ideal in $\mathbf{T}(M)$ generated by the elements $\{m \otimes m : m \in M\}$. Then

$$I = \bigoplus_{r=0}^{\infty} (I \cap \otimes^r M),$$

and we may set

$$\wedge(M) = \mathbf{T}(M)/I = \bigoplus_{r=0}^{\infty} (\otimes^r M)/(I \cap \otimes^r M).$$

We shall write $m \wedge m'$ to denote the image in $\wedge(M)$ of $m \otimes m' \in \mathbf{T}(M)$. In

$\wedge(M)$, we have

$$m \wedge m = 0, \quad m \wedge n = -n \wedge m, \quad m, n \in M.$$

It is clear that the R -module $\wedge(M)$ is a graded R -algebra, and is an RG -module. Moreover, the component $\wedge^r(M) = \otimes^r M / (I \cap \otimes^r M)$ is an RG -submodule, called the module of *skew-symmetric tensors* of degree r . We shall often use the notation $M \wedge M$ instead of $\wedge^2(M)$.

In case $M = \bigoplus_{i \in I} Rm_i$ is R -free, with ordered R -basis $\{m_i\}_{i \in I}$, an R -basis of $\wedge^r(M)$ is given by

$$\{m_{i_1} \wedge m_{i_2} \wedge \cdots \wedge m_{i_r} : i_1 < i_2 < \cdots < i_r, i_k \in I\}.$$

In particular, if $M = \bigoplus_{i=1}^n Rm_i$, then $\wedge^r(M) = 0$ for $r > n$, while for $r \leq n$, the module $\wedge^r(M)$ has a basis containing $\binom{n}{r}$ elements.

We remind the reader of the interpretation of $\det f$, for a map $f \in \text{End}_R(M)$, with $M = \bigoplus_1^n Rm_i$ as above. In this case

$$\wedge^n(M) = R(m_1 \wedge \cdots \wedge m_n),$$

and it follows that there exists a well-defined element $\det f \in R$ such that

$$f^*(m_1 \wedge \cdots \wedge m_n) = (\det f)(m_1 \wedge \cdots \wedge m_n),$$

where $f^* : \wedge^n(M) \rightarrow \wedge^n(M)$ is the R -linear map induced by f . (To be explicit, $f^*(m_1 \wedge \cdots \wedge m_n) = f(m_1) \wedge \cdots \wedge f(m_n)$.) If $f, g \in \text{End}_R(M)$, then from the above definition we have

$$\det fg = (\det f)(\det g).$$

Returning to the general case, we note first that each RG -homomorphism $M \rightarrow N$ gives rise to an RG -homomorphism $\wedge(M) \rightarrow \wedge(N)$, which maps $\wedge^r(M)$ into $\wedge^r(N)$, for $r = 0, 1, 2, \dots$. Next, we observe that there is a isomorphism of left RG -modules

$$(12.2) \quad \wedge(M \oplus N) \cong \wedge(M) \otimes_R \wedge(N),$$

with

$$\wedge^r(M \oplus N) \cong \coprod_{k=0}^r \{\wedge^k(M) \otimes_R \wedge^{r-k}(N)\}.$$

The map in (12.2) is not an isomorphism of R -algebras, however, because the algebras involved are anticommutative. We may define an R -algebra structure on $\wedge(M) \otimes_R \wedge(N)$ by setting

$$(a \otimes b)(a' \otimes b') = (-1)^{jk} aa' \otimes bb',$$

whenever $b \in \wedge^r(N)$, $a' \in \wedge^k(M)$, and aa' , bb' denote products in the exterior algebras $\wedge(M)$ and $\wedge(N)$, respectively. With this definition, the R -isomorphism in (12.2) becomes an isomorphism of R -algebras. (For further details see Swan ([68], Ch. 8, Prop. 8.1).)

The algebras $\mathbf{T}(M)$, $\mathbf{S}(M)$ and $\wedge(M)$ can all be characterized by universal mapping properties. For example, let M be an R -module, and let

$$f: \underbrace{M \times \cdots \times M}_r \rightarrow W$$

be a symmetric R -multilinear map into an R -module W . Then there exists a unique R -linear map $f': \mathbf{S}'(M) \rightarrow W$ such that

$$f'(m_1 \vee \cdots \vee m_r) = f(m_1, \dots, m_r), \quad m_i \in M.$$

Finally, we point out a connection between the modules $\mathbf{S}'(M)$, $\wedge^r(M)$ and representations of the symmetric group. The symmetric group S_r acts on $\otimes^r M$ as follows. For $\sigma \in S_r$, there is a unique R -endomorphism of $\otimes^r M$, called a *symmetry operator*, defined by

$$m_1 \otimes \cdots \otimes m_r \rightarrow \sigma(m_1 \otimes \cdots \otimes m_r) = m_{\sigma^{-1}(1)} \otimes \cdots \otimes m_{\sigma^{-1}(r)}.$$

The permutation σ acts on the places in which the elements in the product $m_1 \otimes \cdots \otimes m_r$ are located, and not on the elements $m \in M$; in other words, σ rearranges the order of elements in the product, keeping the same factors. It is easily checked that if $\sigma, \tau \in S_r$, then

$$\sigma(\tau t) = (\sigma\tau)t, \quad t \in \otimes^r M,$$

and that if M is an RG -module, then the action of $\sigma \in S_r$ commutes with the diagonal action of G on $\otimes^r M$.

(12.3) Proposition. *Let $r! \in R$, the group of units of R . Then $\mathbf{S}'(M)$ and $\wedge^r(M)$ are isomorphic to submodules of $\otimes^r M$:*

$$\mathbf{S}'(M) \cong \{t \in \otimes^r M : \sigma t = t, \forall \sigma \in S_r\},$$

and

$$\wedge^r(M) \cong \{t \in \otimes^r M : \sigma t = \epsilon(\sigma)t, \forall \sigma \in S_r\},$$

where $\epsilon(\sigma)$ is the sign of the permutation σ .

Proof. We shall discuss only the first isomorphism, and leave the proof of the second one as an exercise. We first observe that $(r!)^{-1} \sum_{\sigma \in S_r} \sigma$ projects

$\otimes' M$ onto the submodule consisting of all tensors t such that $\sigma t = t$ for all $\sigma \in S_r$. Now let $f: \otimes' M \rightarrow \mathbf{S}'(M)$ be the natural map, so that

$$f(m_1 \otimes \cdots \otimes m_r) = m_1 \vee \cdots \vee m_r, \quad m_i \in M.$$

By the universal mapping property for symmetric tensors, there is an R -homomorphism $g: \mathbf{S}'(M) \rightarrow \otimes'(M)$ such that

$$g(m_1 \vee \cdots \vee m_r) = (r!)^{-1} \sum_{\sigma \in S_r} \sigma(m_1 \otimes \cdots \otimes m_r), \quad m_i \in M.$$

Then $f \circ g = 1$, hence g is a monomorphism from $\mathbf{S}'(M)$ onto the submodule of $\otimes' M$ defined in the statement of the proposition, as we wished to prove.

In case K is a field of characteristic zero, one can define KG -submodules of $\otimes' M$ corresponding to all irreducible K -representations of S_r . These were used by Schur to determine the irreducible tensor representations of $GL(M)$ (see Weyl [46], CR §67).

§12B. Adams Operators on the Ring of Virtual Characters

In this subsection, $\text{ch}(KG)$ denotes the ring of virtual characters of a finite group G over a field K of characteristic 0 (see §9C). We recall that a class function $\mu: G \rightarrow K$ lies in $\text{ch}(KG)$ if and only if μ is a \mathbb{Z} -linear combination of characters afforded by f.g. KG -modules.

Let M be a left KG -module affording the character μ , and let $n = \dim_K M$. For an element $x \in G$, let $\{\xi_1, \dots, \xi_n\}$ be the eigenvalues of the matrix describing the action of x on a K -basis for M . Then

$$\mu(x) = \xi_1 + \cdots + \xi_n,$$

by definition. From §12A, the eigenvalues of x acting on the exterior power $\wedge'(M)$ are

$$\{\xi_{i_1} \cdots \xi_{i_r} : 1 \leq i_1 < \cdots < i_r \leq n\}.$$

Thus $\wedge'(M)$ affords the character $\mu^{(r)}$ of G , defined by

$$\mu^{(r)}(x) = \sum_{1 \leq i_1 < \cdots < i_r \leq n} \xi_{i_1} \cdots \xi_{i_r}.$$

(Note that for $r > n$, $\wedge'(M) = 0$ and $\mu^r = 0$.) The value of $\mu^{(r)}$ at x is the r -th elementary symmetric function $s_r(\xi_1, \dots, \xi_n)$ of the eigenvalues of x on M . In this section, we shall introduce certain virtual characters $\{\psi_m(\mu) : m = 1, 2, \dots\}$, which are related to $\{\mu^{(r)} : r = 1, 2, \dots\}$ in the same way that the power sums $\sum_j \xi_j^m$ are related to the elementary symmetric functions $s_r(\xi_1, \dots, \xi_n)$ of n variables ξ_1, \dots, ξ_n .



Let $\mathbf{X} = \{X_1, \dots, X_n\}$ be a set of n variables, and define the *elementary symmetric functions* $\{s_r(\mathbf{X}) : r=1, 2, \dots\}$ by

$$s_1(\mathbf{X}) = X_1 + \cdots + X_n,$$

$$s_2(\mathbf{X}) = \sum_{1 \leq i < j \leq n} X_i X_j,$$

...

$$s_n(\mathbf{X}) = X_1 \cdots X_n.$$

We set $s_m(\mathbf{X}) = 0$ for $m > n$. Define the *power sums* $p_i(\mathbf{X})$ by

$$p_i(\mathbf{X}) = X_1^i + \cdots + X_n^i, \quad i = 1, 2, \dots$$

Let us first establish Newton's identities connecting the $\{s_r(\mathbf{X})\}$ and $\{p_i(\mathbf{X})\}$. We omit the symbol \mathbf{X} for brevity in the following calculations. Let t be a variable, and let

$$f(t) = \prod_{j=1}^n (1 + tX_j) = 1 + s_1 t + s_2 t^2 + \cdots + s_n t^n.$$

Then (using formal power series)

$$\begin{aligned} \frac{f'(t)}{f(t)} &= \frac{d}{dt} \log f(t) = \sum_{j=1}^n \frac{X_j}{1+tX_j}, \\ &= \sum_{k=0}^{\infty} \sum_{j=1}^n (-1)^k X_j^{k+1} t^k = \sum_{k=0}^{\infty} (-1)^k p_{k+1} t^k. \end{aligned}$$

This gives

$$s_1 + 2s_2 t + \cdots + ns_n t^{n-1} = \{p_1 - p_2 t + p_3 t^2 - \cdots\} \{1 + s_1 t + \cdots + s_n t^n\}.$$

Comparing coefficients of powers of t^k , we obtain *Newton's identities*:

$$(12.4) \quad \begin{cases} p_1 = s_1 \\ p_2 = s_1 p_1 - 2s_2 \\ p_3 = s_1 p_2 - s_2 p_1 + 3s_3 \\ \dots \\ p_{k+1} = s_1 p_k - s_2 p_{k-1} + \cdots + (-1)^{k-1} s_k p_1 + (-1)^k (k+1) s_{k+1}, \\ \dots \end{cases}$$

The last equation holds for all $k \geq 1$, if we interpret s_m as 0 for $m > n$.

We now imitate this procedure, working in the ring

$$A = \text{ch}(KG)[[t]],$$

the ring of formal power series in a variable t over the commutative ring $\text{ch}(KG)$ of virtual characters. Let M be a KG -module affording the character μ , and let $\{\mu^{(r)} : r \geq 1\}$ be defined as above. We now set

$$E_t(M) = \sum_{r=0}^{\infty} \mu^{(r)} t^r \in A,$$

where $\mu^{(0)} = 1_G$, the trivial character of G . Note that $E_t(M)$ is thus a power series whose constant term 1 is the identity element of the coefficient ring $\text{ch}(KG)$. It follows that $E_t(M)$ is a unit of the power series ring A . We shall often write $E_t(\mu)$ instead of $E_t(M)$.

Let N be another KG -module, affording the character ν of G . By (12.2) there is a KG -isomorphism

$$\wedge^r(M \oplus N) \cong \coprod_{i+j=r} (\wedge^i M) \otimes_K (\wedge^j N).$$

In terms of characters, this yields

$$(\mu + \nu)^{(r)} = \sum_{i+j=r} \mu^{(i)} \nu^{(j)}.$$

This formula is equivalent to the assertion

$$(12.5) \quad E_t(\mu + \nu) = E_t(\mu) E_t(\nu)$$

for any two characters μ, ν of G . It follows that we can extend E_t uniquely to a homomorphism from the additive group $\text{ch}(KG)$ into the multiplicative group A^\times of units of the power series ring A , by setting

$$E_t(\mu - \nu) = E_t(\mu) / E_t(\nu)$$

for any pair of characters μ, ν of G . Note that $E_t(-\nu) E_t(\nu) = 1$ for each $\nu \in \text{ch}(KG)$.

For real x close to 1, we have

$$\log x = \log(1 + (x - 1)) = (x - 1) - (x - 1)^2/2 + (x - 1)^3/3 - \dots$$

If we replace x by an element $a \in A$ with constant term 1, then the series

$$\sum_{n=1}^{\infty} (-1)^{n-1} (a-1)^n / n$$

defines an element of A . We denote this element by $\log a$. Clearly

$$\log ab = \log a + \log b$$

whenever a and b are elements of A with constant term 1. Moreover,

$$\frac{d}{dt}(\log a) = a^{-1} \frac{da}{dt},$$

where d/dt denotes formal differentiation in the power series ring A .

We shall use these concepts to define the *Adams operators*

$$\psi_m : \text{ch}(KG) \rightarrow \text{ch}(KG), \quad m = 1, 2, \dots.$$

Specifically, for each virtual character $\mu \in \text{ch}(KG)$, let $\psi_1(\mu), \psi_2(\mu), \dots$ be the uniquely determined coefficients of t, t^2, \dots , respectively, in the power series expansion of

$$-t \frac{d}{dt} \{\log E_{-t}(\mu)\}.$$

Thus, by definition,

$$(12.6) \quad \sum_{m=1}^{\infty} \psi_m(\mu) t^m = -t \frac{d}{dt} \{\log E_{-t}(\mu)\} = \frac{-t \frac{d}{dt} \{E_{-t}(\mu)\}}{E_{-t}(\mu)},$$

where

$$E_{-t}(\mu) = 1 - \mu t + \mu^{(2)} t^2 - \dots = \sum_{r=0}^{\infty} (-1)^r \mu^{(r)} t^r.$$

From the last expression in (12.6), we may deduce that for $m \geq 1$, $\psi_m(\mu)$ is expressible as a polynomial in $\mu^{(1)}, \mu^{(2)}, \dots, \mu^{(m)}$, with coefficients in \mathbb{Z} . These polynomials are defined recursively by the identity

$$\{1 - \mu^{(1)}t + \mu^{(2)}t^2 - \dots\} \{\psi_1(\mu)t + \psi_2(\mu)t^2 + \dots\} = \mu^{(1)}t - 2\mu^{(2)}t^2 + 3\mu^{(3)}t^3 - \dots$$

Comparing coefficients of powers of t , we obtain

$$(12.7) \quad \begin{cases} \psi_1(\mu) = \mu^{(1)} = \mu, \\ \psi_2(\mu) = \mu^{(1)}\psi_1(\mu) - 2\mu^{(2)}, \\ \psi_3(\mu) = \mu^{(1)}\psi_2(\mu) - \mu^{(2)}\psi_1(\mu) + 3\mu^{(3)}, \\ \dots \\ \psi_m(\mu) = \sum_{i=1}^{m-1} (-1)^{i-1} \mu^{(i)} \psi_{m-i}(\mu) + (-1)^{m-1} m \mu^{(m)}, \end{cases}$$

These formulas confirm our earlier statement that the Adams operators $\psi_i(\mu)$ are given in terms of the characters $\mu^{(j)}$ by the same formulas (12.4) (*Newton's identities*) which express the power sums $p_i(X_1, \dots, X_n) = \sum_k X_k^i$ in terms of the elementary symmetric functions $s_j(X_1, \dots, X_n)$. This connection is strengthened by

(12.8) Proposition. *For each $x \in G$ and each $\mu \in \text{ch}(KG)$, we have*

$$\{\psi_m(\mu)\}(x) = \mu(x^m), \quad m = 1, 2, \dots.$$

Before proving (12.8), we first establish

(12.9) Lemma. *For all $\mu, \nu \in \text{ch}(KG)$, and $m \geq 1$, we have*

$$\psi_m(\mu + \nu) = \psi_m(\mu) + \psi_m(\nu).$$

Proof. From (12.6), we have

$$\sum_{m=1}^{\infty} \psi_m(\mu + \nu) t^m = -t \frac{d}{dt} \{\log E_{-t}(\mu + \nu)\}.$$

Applying (12.5) to the right hand side, we obtain

$$\begin{aligned} -t \frac{d}{dt} \{\log E_{-t}(\mu + \nu)\} &= -t \frac{d}{dt} \{\log E_{-t}(\mu) E_{-t}(\nu)\} \\ &= -t \frac{d}{dt} \{\log E_{-t}(\mu)\} - t \frac{d}{dt} \{\log E_{-t}(\nu)\}. \end{aligned}$$

Upon expanding the summands using (12.6) and comparing coefficients of powers of t , we obtain (12.9).

Proof of (12.8). By Lemma 12.9, it suffices to prove (12.8) for a K -character μ afforded by a KG -module M . As above, let $x \in G$ and let $\{\xi_1, \dots, \xi_n\}$ be the eigenvalues of x on M . We have shown that

$$\mu^{(m)}(x) = s_m(\xi_1, \dots, \xi_n), \quad m \geq 1.$$

For each series $\sum \varphi_m t^m \in A$, we obtain a formal series in $K[[t]]$ by evaluation at x , namely

$$(\sum \varphi_m t^m)(x) = \sum \varphi_m(x) t^m, \quad x \in G.$$

Then from the fact that $\{\mu^{(m)}(x)\}$ are given by the elementary symmetric functions in $\{\xi_1, \dots, \xi_n\}$, we have

$$(E_t(\mu))(x) = \sum_{m=0}^{\infty} \mu^{(m)}(x) t^m = \prod_{i=1}^n (1 + \xi_i t).$$

Therefore

$$(\log E_{-t}(\mu))(x) = \sum_{i=1}^n \log(1 - \xi_i t),$$

and from (12.6) we obtain

$$\begin{aligned} \left(\sum_{m=1}^{\infty} \psi_m(\mu) t^m \right)(x) &= -t \frac{d}{dt} \{ \log E_{-t}(\mu) \}(x) \\ &= \sum_{i=1}^n \frac{\xi_i t}{1 - \xi_i t} = \sum_{i=1}^n \left(\sum_{m=1}^{\infty} \xi_i^m t^m \right). \end{aligned}$$

Comparing coefficients of t^m , we find that

$$\{ \psi_m(\mu) \}(x) = \sum_{i=1}^n \xi_i^m, \quad m \geq 1.$$

However, $\{\xi_1^m, \dots, \xi_n^m\}$ are precisely the eigenvalues of x^m acting on the module M , so that

$$\{ \psi_m(\mu) \}(x) = \mu(x^m), \quad x \in G,$$

and (12.8) is proved. (Compare this calculation with that which we used to establish (12.4).)

(12.10) Corollary. *The Adams operators $\{\psi_m\}$ satisfy*

$$\psi_m(\mu\nu) = \psi_m(\mu)\psi_m(\nu)$$

and

$$\psi_m(\psi_n(\nu)) = \psi_{mn}(\nu),$$

for all $m, n \geq 1$, and all $\mu, \nu \in \text{ch}(KG)$. In particular, each Adams operator is an endomorphism of the commutative ring $\text{ch}(KG)$.

Proof. The first two statements follow at once by evaluating both sides at $x \in G$, and using (12.8). The third statement follows from the first, and Lemma 12.9.

The Adams operators will play an important role in our discussion of λ -rings.

§12C. Symmetric and Skew-Symmetric Squares of Induced Modules

Throughout this section, R denotes a commutative ring in which 2 is a unit, that is, the equation $2x=1$ has a unique solution in R . Thus, in particular, $2 \neq 0$ in R . Let G be a finite group, and M a left RG -lattice (see §10D). Then

the inner tensor product $M \otimes M$ is also an RG -lattice (here, and throughout this subsection, \otimes always means \otimes_R .) By Proposition 12.3, the symmetric and skew-symmetric tensors of degree 2 over M can be identified with submodules of $M \otimes M$ as follows:

$$\begin{aligned} M \vee M &= \{t \in M \otimes M : \tau(t) = t\} = \text{symmetric tensors}, \\ M \wedge M &= \{t \in M \otimes M : \tau(t) = -t\} = \text{skew-symmetric tensors}, \end{aligned}$$

where τ is the symmetry operator corresponding to the transposition (12). Because of the hypothesis on R , we can write

$$t = \frac{1}{2}(t + \tau(t)) + \frac{1}{2}(t - \tau(t)) \in (M \vee M) + (M \wedge M),$$

for all $t \in M \otimes M$. Moreover, $(M \vee M) \cap (M \wedge M) = 0$, again by the hypothesis on R . This shows that

$$M \otimes M = (M \vee M) \oplus (M \wedge M).$$

This decomposition gives rise to a direct sum decomposition of $\text{Hom}_{RG}(M^*, M)$, where M^* is the RG -lattice which is the contragredient of M (see §10D). By (10.31) we have an R -isomorphism

$$\text{Hom}_{RG}(M^*, M) \cong \text{inv}_G(M \otimes M).$$

Using the above decomposition of $M \otimes M$, we obtain

$$\text{Hom}_{RG}(M^*, M) \cong \text{inv}_G(M \otimes M) = \text{inv}_G(M \vee M) \oplus \text{inv}_G(M \wedge M).$$

Suppose now that R is a field K , and define

$$i_s(M^*, M) = \dim_K(\text{inv}_G M \vee M), \quad i_a(M^*, M) = \dim_K(\text{inv}_G M \wedge M).$$

We shall call $i_s(M^*, M)$ the *symmetric intertwining number* of M^* and M , and $i_a(M^*, M)$ the *antisymmetric* (or *skew-symmetric*) *intertwining number*. Clearly,

$$i(M^*, M) = \dim_K \text{Hom}_{KG}(M^*, M) = i_s(M^*, M) + i_a(M^*, M),$$

the first equality merely recalling the definition of $i(M^*, M)$ as in (9.24iii).

We now introduce another important invariant of M , namely,

$$c(M) = i_s(M^*, M) - i_a(M^*, M).$$

If the field K is algebraically closed and M is a simple KG -module, it is easily shown that $i(M^*, M) = 1$ or 0 , so

$$c(M) = 1, -1 \text{ or } 0.$$

In Chapter 6 below, we shall prove a beautiful result of Frobenius and Schur, which describes the field of definition of M (and of its character) in terms of $c(M)$.

The next result summarizes some useful properties of the invariant $c(M)$. The proof is left as an exercise (see Mackey [53]).

(12.11) Proposition. *Let K be a field such that $\text{char } K \neq 2$. For each left KG -module M , define*

$$c(M) = i_s(M^*, M) - i_a(M^*, M).$$

Then

$$(i) \quad c(M \oplus N) = c(M) + c(N).$$

$$(ii) \quad \text{Further, if } \text{char } K = 0 \text{ or } \text{char } K \nmid |G|, \text{ then}$$

$$c(M \otimes N) = c(M)c(N) \text{ and } c(M^*) = c(M).$$

$$(iii) \quad \text{If } \text{char } K = 0, \text{ there are ring homomorphisms}$$

$$\dim : \text{ch}(KG) \rightarrow \mathbb{Z}, \quad c : \text{ch}(KG) \rightarrow \mathbb{Z},$$

defined by

$$\dim M = \dim_K(M), \quad c(M) = i_s(M^*, M) - i_a(M^*, M),$$

for every f.g. left KG -module M .

We now return to the general situation, with R a commutative ring such that $2 \in R$. Let $H \leq G$, and let L be a left RH -lattice. As we have seen in §10D, L^G is an RG -lattice. The main result (Mackey [53]) describes the structure of the symmetric square $L^G \vee L^G$ of L^G , and the skew-symmetric square $L^G \wedge L^G$ of L^G , in terms of induced modules.

In order to state Mackey's Theorem, some notation is needed. Let H be a subgroup of the finite group G , and consider the collection $H \setminus G / H$ of (H, H) -double cosets in G . Write

$$(12.12) \quad H \setminus G / H = H \cup \mathfrak{D}_1 \cup \mathfrak{D}_2,$$

where \mathfrak{D}_1 is the union of the self-inverse double cosets not equal to H , and \mathfrak{D}_2 is the union of the sets $\{d\}$ of the form $d = D \cup D^{-1}$, where D is a double coset such that $D \neq D^{-1}$. Keeping this notation, we have:

(12.13) Theorem (Mackey [53]). *Let R be any commutative ring in which 2 is a unit, let H be a subgroup of G , and L an RH -lattice. Then $L^G \vee L^G$ and*

$L^G \wedge L^G$ are direct sums of induced representations as follows:

$$L^G \vee L^G = (L \vee L)^G \oplus \coprod_{d \in \mathfrak{D}_1} M(d)^+ \oplus \coprod_{d \in \mathfrak{D}_2} N(d),$$

$$L^G \wedge L^G = (L \wedge L)^G \oplus \coprod_{d \in \mathfrak{D}_1} M(d)^- \oplus \coprod_{d \in \mathfrak{D}_2} N(d).$$

The modules $M(d)^\pm$ and $N(d)$ are given thus:

(i) Let $d = D \cup D^{-1} \in \mathfrak{D}_2$, and let $x, y \in G$ be such that $x^{-1}y \in D$. Then the induced module

$$\left\{({}^x L \otimes {}^y L)_{xH \cap {}^y H}\right\}^G$$

is independent of the choice of x and y , and is denoted by $N(d)$.

(ii) Let $d = D \in \mathfrak{D}_1$, so D is a double coset such that $D = D^{-1}$, $D \neq H$. Let $x, y \in G$ be such that $x^{-1}y \in D$; then $xHy^{-1} \cap yHx^{-1} \neq \emptyset$. Choose $z \in (xHy^{-1} \cap yHx^{-1})$, and set

$$H_z = \langle {}^x H \cap {}^y H, z \rangle,$$

a subgroup of G containing ${}^x H \cap {}^y H$ as a normal subgroup of index 2.

The $R({}^x H \cap {}^y H)$ -module ${}^x L \otimes {}^y L$ can be extended to two RH_z -modules $L_{x,y,z}^\pm$, whose direct sum is $({}^x L \otimes {}^y L)^{H_z}$. The modules $M(d)^\pm$ occurring in the decompositions of $L^G \vee L^G$ and $L^G \wedge L^G$ are then defined by

$$M(d)^+ = \text{ind}_{H_z}^G L_{x,y,z}^+, \quad M(d)^- = \text{ind}_{H_z}^G L_{x,y,z}^-.$$

These modules are independent of the choices of x, y, z (provided these are chosen so that $x^{-1}y \in D$, and $z \in xHy^{-1} \cap yHx^{-1}$).

Proof. The entire argument is based on the proof of the Tensor Product Theorem 10.18. We have

$$L^G \otimes L^G \cong (L \# L)^{G \times G}|_{G_0},$$

where G_0 is the diagonal subgroup of $G \times G$. From the Subgroup Theorem 10.13, we have

$$(12.14) \quad (L \# L)^{G \times G}|_{G_0} = \bigoplus_D \left\{ (x \otimes L \otimes y \otimes L)_{({}^x H \times {}^y H) \cap G_0} \right\}^{G_0},$$

where the sum is taken over (H, H) -double cosets D in G . The double cosets

D correspond bijectively to the $(G_0, H \times H)$ -double cosets in $G \times G$:

$$Hx^{-1}yH \leftrightarrow G_0(x, y)(H \times H).$$

The summand in (12.14) corresponding to D consists of all tensors of the form

$$\sum_{g \in G, l \in L, l' \in L'} (g, g)(x \otimes l \otimes y \otimes l') = \sum gx \otimes l \otimes gy \otimes l', \quad g \in G, l, l' \in L.$$

The symmetry operator $\tau: L^G \otimes L^G \rightarrow L^G \otimes L^G$, corresponding to the transposition (12), is defined by:

$$\tau: \sum gx \otimes l \otimes gy \otimes l' \rightarrow \sum gy \otimes l' \otimes gx \otimes l.$$

Note that τ commutes with the action of all elements $(g, g) \in G_0$. We recall from the beginning of §12C that $L^G \vee L^G$ is identified with the submodule consisting of all elements of $L^G \otimes L^G$ fixed by τ , and $L^G \wedge L^G$ with those elements mapped onto their negatives by τ .

We now see that $(L \# L)^{G \times G}|_{G_0}$ is the direct sum of RG_0 -modules, which correspond as follows to the decomposition (12.12) of $H \setminus G / H$:

(12.15)

$$\begin{cases} (1 \otimes L \otimes 1 \otimes L)^{G_0} \leftrightarrow H \\ (x \otimes L \otimes y \otimes L)^{G_0} \leftrightarrow D \in \mathfrak{D}_1, D = D^{-1}, x^{-1}y \in D, \\ (x \otimes L \otimes y \otimes L)^{G_0} + (y \otimes L \otimes x \otimes L)^{G_0} \leftrightarrow D \cup D^{-1}, D \neq D^{-1}, x^{-1}y \in D. \end{cases}$$

Note that in the last case, the double cosets in $G_0 \setminus (G \times G) / (H \times H)$ corresponding to D and D^{-1} have representatives (x, y) and (y, x) , respectively.

Each of the submodules in (12.15) is mapped onto itself by τ , so that in order to prove the theorem, it is sufficient to determine the symmetric and skew-symmetric summands of the modules appearing in (12.15).

The first and third cases in (12.15) are easy to handle. For the first case, we leave it to the reader to verify that under the isomorphism $G_0 \cong G$, the module $(1 \otimes L \otimes 1 \otimes L)^{G_0}$ corresponds to $(L \vee L)^G \oplus (L \wedge L)^G$, with $(L \vee L)^G \subseteq L^G \vee L^G$ and $(L \wedge L)^G \subseteq L^G \wedge L^G$.

For the third case, the symmetric and skew-symmetric summands of $(x \otimes L \otimes y \otimes L)^{G_0} + (y \otimes L \otimes x \otimes L)^{G_0}$ consist (respectively) of the elements

$$\{a + \tau(a) : a \in (x \otimes L \otimes y \otimes L)^{G_0}\}$$

and

$$\{a - \tau(a) : a \in (x \otimes L \otimes y \otimes L)^{G_0}\}.$$

It is easily checked that the maps

$$a \rightarrow a + \tau(a), a \rightarrow a - \tau(a), a \in (x \otimes L \otimes y \otimes L)^{G_0},$$

are RG_0 -isomorphisms. It follows that for each non-self-inverse double coset D , the third module listed in (12.15) contributes one summand to $L^G \vee L^G$ and one to $(L \wedge L)^G$, and that both are RG -isomorphic to $\{({}^x L \otimes {}^y L)_{xH \cap yH}\}^G$.

We now consider the most difficult case, that of a double coset D such that $D = D^{-1}$, $D \neq H$. Let $x^{-1}y \in D$; then $Hx^{-1}yH = Hy^{-1}xH$, and it follows that

$$xHy^{-1} \cap yHx^{-1} \neq \emptyset.$$

Choose $z \in xHy^{-1} \cap yHx^{-1}$. Then

$${}^z({}^xH) = {}^yH, \quad {}^z({}^yH) = {}^xH,$$

and hence

$${}^z({}^xH \cap {}^yH) = {}^xH \cap {}^yH.$$

Moreover $z^2 \in {}^xH \cap {}^yH$, so we may conclude that ${}^xH \cap {}^yH$ is a normal subgroup of index 2 in $\langle {}^xH \cap {}^yH, z \rangle$. We are going to prove that the $({}^xH \cap {}^yH)$ -module $x \otimes L \otimes y \otimes L$ can be made into a module over the group $\langle {}^xH \cap {}^yH, z \rangle$. Transferring the problem to the subgroup G_0 of $G \times G$, we define subgroups $H_{x,y}$ and $H_{x,y,z}$ as follows:

$${}^xH \cap {}^yH \leftrightarrow ({}^xH \times {}^yH) \cap G_0 = H_{x,y},$$

$$\langle {}^xH \cap {}^yH, z \rangle \rightarrow \langle ({}^xH \times {}^yH) \cap G_0, (z, z) \rangle = H_{x,y,z}.$$

We shall prove below that the action of $H_{x,y}$ on $x \otimes L \otimes y \otimes L$ can be extended to an action of $H_{x,y,z}$, thereby making $x \otimes L \otimes y \otimes L$ into an $RH_{x,y,z}$ -module.

Observe first that both of the elements $x^{-1}zy$ and $y^{-1}zx$ lie in H . Now define a linear map Z on $x \otimes L \otimes y \otimes L$ by

$$Z(x \otimes l \otimes y \otimes l') = x \otimes x^{-1}zyl' \otimes y \otimes y^{-1}zx l, \quad \forall l, l' \in L.$$

Then

$$\begin{aligned} Z^2(x \otimes l \otimes y \otimes l') &= x \otimes (x^{-1}zy)(y^{-1}zx l) \otimes y \otimes (y^{-1}zx)(x^{-1}zyl') \\ &= x \otimes x^{-1}z^2xl \otimes y \otimes y^{-1}z^2yl' = (z^2, z^2)(x \otimes l \otimes y \otimes l'). \end{aligned}$$

It is easily checked that for $h \in H_{x,y}$, the actions of $(z, z)h(z, z)^{-1}$ and ZhZ^{-1} on $x \otimes L \otimes y \otimes L$ agree; this depends on the fact that

$$Z^{-1}(x \otimes l \otimes y \otimes l') = x \otimes x^{-1}z^{-1}yl' \otimes y \otimes y^{-1}z^{-1}xl.$$

It now follows that the actions of $H_{x,y}$ and Z on $x \otimes L \otimes y \otimes L$ preserve the defining relations of the group $H_{x,y,z}$, so this larger group now acts on the module $x \otimes L \otimes y \otimes L$, by letting (z, z) act as Z .

If R were the field of complex numbers, we could now apply Corollary 11.7 to deduce that the action of $H_{x,y}$ on $x \otimes L \otimes y \otimes L$ could be extended in two ways to an action of $H_{x,y,z}$, thereby obtaining a pair of $RH_{x,y,z}$ -modules L^+ and L^- for which

$$\text{ind}_{H_{x,y}}^{H_{x,y,z}}(x \otimes L \otimes y \otimes L) = L^+ \oplus L^-.$$

This would give the formula

$$\text{ind}_{H_{x,y}}^{G_0}(x \otimes L \otimes y \otimes L) = (L^+)^{G_0} \oplus (L^-)^{G_0}.$$

We shall now establish these statements in the general case, where R is a *ring* (in which $2 \in R$), rather than \mathbb{C} . Further, as in the statement of the theorem, we shall identify $(L^+)^{G_0}$ with a direct summand of $L^G \vee L^G$, and $(L^-)^{G_0}$ with a direct summand of $L^G \wedge L^G$, after transferring back from G_0 to G , from $H_{x,y,z}$ to H_z , and so on.

The remainder of the proof hinges on the following lemma:

(12.16) Lemma. *Let R be a commutative ring such that $2 \in R$. Let U be a normal subgroup of index 2 in a finite group X , and let $X = \langle U, x \rangle$. Let N be a left RU -module, and assume that the action of U on N can be extended to an action of X . Then $N^X = N^+ \oplus N^-$, where N^+ and N^- are RX -modules such that $N^+|_U \cong N^-|_U \cong N$, and*

$$N^+ = \{1 \otimes n + x \otimes x^{-1}n : n \in N\}, \quad N^- = \{1 \otimes n - x \otimes x^{-1}n : n \in N\}.$$

The proof is deferred to the exercises. We can now complete the proof of (12.13). Using Lemma 12.16, we can write

$$(x \otimes L \otimes y \otimes L)^{H_{x,y,z}} = L^+ \oplus L^-,$$

where L^+ and L^- are defined as in the lemma. It remains to prove that $(L^+)^{G_0}$ and $(L^-)^{G_0}$ are indeed the symmetric and skew-symmetric parts of $(x \otimes L \otimes y \otimes L)^{G_0}$. We can identify L^+ with the submodule of $x \otimes L \otimes y \otimes L$ consisting of all sums

$$\Sigma\{x \otimes l \otimes y \otimes l' + (z, z)Z^{-1}(x \otimes l \otimes y \otimes l')\}, \quad l, l' \in L.$$

Then $(L^+)^{G_0}$ consists of all finite sums

$$\begin{aligned} a &= \sum_{g \in G; l, l' \in L} \{gx \otimes l \otimes gy \otimes l' + (g, g)(z, z)Z^{-1}(x \otimes l \otimes y \otimes l')\} \\ &= \Sigma\{gx \otimes l \otimes gy \otimes l' + gzx \otimes x^{-1}z^{-1}yl' \otimes gzy \otimes y^{-1}z^{-1}xl\}. \end{aligned}$$

Therefore

$$\tau a = \sum \{ gy \otimes l' \otimes gx \otimes I + gzy \otimes y^{-1}z^{-1}xI \otimes gzx \otimes x^{-1}z^{-1}yl' \}.$$

Using the fact that both $y^{-1}zx$ and $x^{-1}zy$ lie in H , it is easy to check that $\tau a = a$. A similar calculation shows that for all elements $b \in (L^-)^{G_0}$, we have $\tau b = -b$.

We can now transfer to G by using the isomorphism $G_0 \cong G$. The modules L^+ and L^- correspond to RH_z -modules $L_{x,y,z}^+$ and $L_{x,y,z}^-$, respectively, whose direct sum is $(^xL \otimes {}^yL)^{H_z}$. The modules $\text{ind}_{H_z}^G L_{x,y,z}^+$ and $\text{ind}_{H_z}^G L_{x,y,z}^-$ satisfy the requirements of the theorem, and the proof of (12.13) is complete.

It is worthwhile to restate Theorem 12.13 as it applies to a linear character of H , taken in the complex field C .

(12.17) Theorem. *Let $H \leq G$, and let λ be a linear C -character of H . Let $\lambda^G \vee \lambda^G$ and $\lambda^G \wedge \lambda^G$ denote the characters afforded by the symmetric and skew-symmetric parts of the tensor square of the module affording λ^G . Let*

$$H \setminus G / H = H \cup \mathfrak{D}_1 \cup \mathfrak{D}_2$$

as in (12.12). Then

$$\lambda^G \vee \lambda^G = (\lambda^2)^G + \sum_{d \in \mathfrak{D}_1} \mu(d)^+ + \sum_{d \in \mathfrak{D}_2} \nu(d),$$

$$\lambda^G \wedge \lambda^G = \sum_{d \in \mathfrak{D}_1} \mu(d)^- + \sum_{d \in \mathfrak{D}_2} \nu(d),$$

where $\mu(d)^+$, $\mu(d)^-$ and $\nu(d)$ are induced characters defined as follows:

(i) For $d \in \mathfrak{D}_2$, let $d = D \cup D^{-1}$ and let $x^{-1}y \in D$, where $x, y \in G$. Then

$$\nu(d) = \text{ind}_{^xH \cap {}^yH}^G {}^x\lambda \cdot {}^y\lambda,$$

and $\nu(d)$ is independent of the choice of x and y .

(ii) Now let $d = \{D\}$ be an element of \mathfrak{D}_1 , where $D = D^{-1}$. Let $z \in xHy^{-1} \cap yHx^{-1}$, and $H_z = \langle {}^xH \cap {}^yH, z \rangle$, as in (12.13). Then $(^x\lambda)(z^2) = ({}^y\lambda)(z^2)$, and $(^x\lambda \cdot {}^y\lambda)_{^xH \cap {}^yH}$ can be extended to a character φ of H_z such that

$$\varphi(z) = (^x\lambda)(z^2) = ({}^y\lambda)(z^2).$$

Then

$$((^x\lambda \cdot {}^y\lambda)_{^xH \cap {}^yH})^{H_z} = \varphi + \epsilon\varphi,$$

where ϵ is the unique nontrivial character of the factor group $H_z / (^xH \cap {}^yH)$. The

characters $\mu(d)^+$ and $\mu(d)^-$ are defined as

$$\mu(d)^+ = \text{ind}_{H_z}^G \varphi, \quad \mu(d)^- = \text{ind}_{H_z}^G \epsilon\varphi.$$

We make a few remarks on the proof, which is simply a translation of Theorem 12.13 to this more concrete situation. For a linear character λ , $\lambda \vee \lambda$ can be identified with λ^2 , and $\lambda \wedge \lambda = 0$. Let Z be the linear map (defined in the proof of (12.13)) which was used to extend the action of $H_{x,y}$ to $H_{x,y,z}$. For $d \in \mathfrak{D}_1$, the map Z is a scalar:

$$Z = \lambda(x^{-1}zy) \cdot \lambda(y^{-1}zx) = \lambda(x^{-1}z^2x) = ({}^x\lambda)(z^2),$$

because of the linearity of λ . Given the extension φ corresponding to Z , the fact that

$$[({}^x\lambda \cdot {}^y\lambda)_{xH \cap {}^yH}]^{H_z} = \varphi + \epsilon\varphi$$

follows from (11.7) (or from Lemma 12.16).

We can now apply Theorem 12.17, together with Proposition 10.30ii), to calculate $i_s(\bar{\lambda}^G, \lambda^G)$ and $i_a(\bar{\lambda}^G, \lambda^G)$ for an induced linear character λ^G (as in (12.17)). We require two facts: first, $\bar{\lambda}^G$ is the character afforded by the contragredient character $(\lambda^G)^*$ of λ^G , by (10.28); second,

$$i_s(\bar{\lambda}^G, \lambda^G) = \dim_K(\text{inv}_G \lambda^G \vee \lambda^G), \quad i_a(\bar{\lambda}^G, \lambda^G) = \dim_K(\text{inv}_G \lambda^G \wedge \lambda^G),$$

by definition. Before stating the result, let us define, for $d \in \mathfrak{D}_2$,

$$j(d) = \begin{cases} 1 & \text{if } {}^x\lambda \cdot {}^y\lambda = 1 \text{ on } {}^xH \cap {}^yH, \\ 0 & \text{otherwise,} \end{cases}$$

where $d = D$, and $x^{-1}y \in D$ as in (12.17). Note that $j(d)$ is independent of the choice of x and y . For $d \in \mathfrak{D}_1$, set $j(d) = 0$ if ${}^x\lambda \cdot {}^y\lambda \neq 1$ on ${}^xH \cap {}^yH$. If ${}^x\lambda \cdot {}^y\lambda = 1$ on ${}^xH \cap {}^yH$, then $({}^x\lambda)(z^2) = \pm 1$, and we set $j(d) = ({}^x\lambda)(z^2)$, again noting that $j(d)$ is independent of the choice of x, y and z .

(12.18) Theorem. *Let λ be a complex linear character of H . Then*

$$i_s(\bar{\lambda}^G, \lambda^G) = i(\bar{\lambda}, \lambda) + \sum_{d \in \mathfrak{D}_1} \frac{1}{2} j(d)(1 + j(d)) + \sum_{d \in \mathfrak{D}_2} j(d),$$

and

$$i_a(\bar{\lambda}^G, \lambda^G) = \sum_{d \in \mathfrak{D}_1} \frac{1}{2} j(d)(-1 + j(d)) + \sum_{d \in \mathfrak{D}_2} j(d).$$

The result is a corollary of the previous theorem, and the proof requires only a few comments. From (12.10), we have

$$i_s(\bar{\lambda}^G, \lambda^G) = \dim_K(\text{inv}_G \lambda^G \vee \lambda^G) = (\lambda^G \vee \lambda^G, 1_G).$$

Since $\lambda^G \vee \lambda^G$ is a sum of induced characters, by (12.17), the scalar product $(\lambda^G \vee \lambda^G, 1_G)$ is easily computed using Frobenius Reciprocity. For example

$$((\lambda^2)^G, 1_G) = (\lambda^2, 1_H) = (\lambda, \bar{\lambda}) = i(\lambda, \bar{\lambda}).$$

For $d \in \mathfrak{D}_1$, we have

$$(\varphi^G, 1_G) = (\varphi, 1_{H_d}) = \begin{cases} 0 & j(d) = -1, \\ 1 & j(d) = 1, \end{cases}$$

so that $(\varphi^G, 1_G) = \frac{1}{2} j(d)(1 + j(d))$. Similarly

$$((\epsilon\varphi)^G, 1_G) = (\epsilon\varphi, 1_{H_d}) = (\varphi, \epsilon) = \begin{cases} 0 & j(d) = 1, \\ 1 & j(d) = -1, \end{cases}$$

and we have $(\epsilon\varphi^G) = \frac{1}{2} j(d)(-1 + j(d))$. For $d \in \mathfrak{D}_2$ we have a contribution

$$(({}^x\lambda \cdot {}^y\lambda)^G, 1_G) = ({}^x\lambda \cdot {}^y\lambda, 1_{{}^xH \cap {}^yH}) = j(d).$$

Similar remarks apply to the computation of $i_a(\bar{\lambda}^G, \lambda^G)$.

(12.19) Corollary. *Let λ be a linear character of a subgroup H of G , as in (12.17). Then*

$$c(\lambda^G) = c(\lambda) + \sum_{d \in \mathfrak{D}_1} j(d).$$

In case $\lambda = 1_H$, we have $j(d) = 1$ for all $d \in \mathfrak{D}_1$, and we obtain a result due to Frame [41]:

(12.20) Corollary. *We have $c((1_H)^G) = \text{card } \mathfrak{D}_1$, where \mathfrak{D}_1 is the family of self-inverse (H, H) -double cosets in G .*

§12. Exercises

1. Prove Lemma 12.16 as follows. There is an R -exact sequence

$$0 \rightarrow N^- \rightarrow N^X \xrightarrow{\alpha} N \rightarrow 0.$$

where

$$\alpha(\sum a_i \otimes n_i) = \sum a_i n_i, \quad a_i \in RX, \quad n_i \in N,$$

and

$$N^- = \ker \alpha = \{1 \otimes n - x \otimes x^{-1}n : n \in N\}.$$

The map

$$n \mapsto 1 \otimes n - x \otimes x^{-1}n, \quad n \in N,$$

gives an RU -isomorphism $N \cong N^-|_U$. On the other hand, α is split by the RX -homomorphism $\beta: N \rightarrow N^X$, defined by

$$\beta(n) = \frac{1}{2}(1 \otimes n + x \otimes x^{-1}n), \quad n \in N.$$

Thus $N^X = N^+ \oplus N^-$, where $N^+ = \text{im } \beta$. It is easily verified that $N^+ \cong N|_U$.

2. Let R be a commutative ring, and let M be a free R -module with a finite basis. Prove that for each $r \geq 0$, $\wedge^r(M)$ is isomorphic to the R -submodule $\tilde{\wedge}^r(M)$ of $\otimes^r M$ generated by all tensors of the form

$$\sum_{\sigma \in S_r} \epsilon(\sigma)(x_{\sigma(1)} \otimes \cdots \otimes x_{\sigma(r)}), \quad x_i \in M,$$

where each $\sigma \in S_r$ acts as a symmetry operator on $\otimes^r M$. Show that $\tilde{\wedge}^r(M)$ is, in general, properly contained in the submodule $\{t \in \otimes^r M : \sigma t = \epsilon(\sigma)t\}$ (see (12.3)).

[Hint: Let $\{m_1, \dots, m_n\}$ be an R -basis of M , and for each sequence $\{i_1 < i_2 < \cdots < i_r, 1 \leq i_j \leq n\}$, let

$$m_{i_1} \tilde{\wedge} \cdots \tilde{\wedge} m_{i_r} = \sum_{\sigma \in S_r} \epsilon(\sigma) m_{i_{\sigma(1)}} \otimes \cdots \otimes m_{i_{\sigma(r)}}.$$

Prove that the elements $\{m_{i_1} \tilde{\wedge} \cdots \tilde{\wedge} m_{i_r}\}$ form a basis for the module in question.]

3. Let K be a field of characteristic zero, and let V be a vector space of dimension n over K , and V^* its K -dual. Let $\{v_1, \dots, v_n\}$ be a basis of V , and let $\{x_1, \dots, x_n\}$ be the dual basis. Prove that the symmetric algebra $S(V^*)$ is isomorphic to the K -algebra of functions $f: V \rightarrow K$ generated by $\{x_1, \dots, x_n\}$, and that $\{x_1, \dots, x_n\}$ are algebraically independent. We shall identify $S(V^*)$ with the algebra $K[x_1, \dots, x_n]$, and call it the *algebra of polynomial functions* on V . Note that if

$$f = \sum a_{i_1, \dots, i_n} x_1^{i_1} \cdots x_n^{i_n} \in K[x_1, \dots, x_n],$$

then f acts on V according to the rule

$$v \mapsto f(v) = \sum a_{i_1, \dots, i_n} x_1(v)^{i_1} \cdots x_n(v)^{i_n}.$$

4. Keep the notation of the preceding exercise. Let K be algebraically closed and of characteristic zero, let G be a finite group, and V a f.g. left KG -module. Prove that G acts on the algebra of polynomial functions on V according to the rule:

$$(xf)(v) = f(x^{-1}v), \quad x \in G, v \in V, f \in S(V^*),$$

and that the resulting operations on $S(V^*)$ are K -algebra automorphisms. The set

$$I(G) = \{f \in S(V^*) : xf = f \text{ for all } x \in G\}$$

is a K -subalgebra of $S(V^*)$, called the *algebra of polynomial invariants* of the KG -module V .

(i) For each $r \geq 0$, let S_r be the homogeneous component of $S(V^*)$ of degree r , that is, S_r is generated by all monomials

$$\{x_1^{i_1} \cdots x_n^{i_n} : i_1 + \cdots + i_n = r\}.$$

Prove that

$$I(G) = \bigoplus_{r \geq 0} I_r, \text{ where } I_r = I(G) \cap S_r, r \geq 0,$$

and that each S_r is stable under the action of G on $S(V^*)$.

(ii) For each $r \geq 0$, let $a_r = \dim_K I_r$. Prove that-

$$a_r = (\theta_r, 1_G) = |G|^{-1} \sum_{x \in G} \text{Tr}(x, S_r),$$

where θ_r is the character of the K -representation of G on S_r .

[Hint: Use Exercise 9.10.]

(iii) Let $x \in G$, and let $\{\xi_1, \dots, \xi_n\}$ be the eigenvalues of x acting on the vector space V , counted with multiplicities. Let t be an indeterminate over K . Prove that

$$\det(1 - tx) = \prod_{i=1}^n (1 - t\xi_i),$$

where $1 - tx$ is viewed as a K -endomorphism of $K(t) \otimes_K V$.

(iv) **Molien's Theorem.** Keep the notation of parts (i)–(iii). Prove that for each $x \in G$, $\det(1 - tx)$ is invertible in the ring $K[[t]]$ of formal power series over K , and that we have an identity in $K[[t]]$,

$$\sum_{r=0}^{\infty} a_r t^r = |G|^{-1} \sum_{x \in G} \frac{1}{\det(1 - tx)},$$

where $\sum a_r t^r$ is the generating function of the dimensions $\{a_r : r \geq 0\}$.

[Hint: By part (ii),

$$a_r = |G|^{-1} \sum_{x \in G} \text{Tr}(x, S_r).$$

For each $x \in G$, with eigenvalues $\{\xi_1, \dots, \xi_r\}$ on V , show that the eigenvalues of x acting on S_r are

$$\{\xi_1^{i_1} \cdots \xi_n^{i_n} : i_1 + \cdots + i_n = r\}.$$

Then apply (iii) to prove that

$$\begin{aligned} \frac{1}{\det(1-tx)} &= \frac{1}{(1-t\xi_1) \cdots (1-t\xi_n)} = \sum_{r=0}^{\infty} \left(\sum_{\sum i_j = r} \xi_1^{i_1} \cdots \xi_n^{i_n} \right) t^r \\ &= \sum_{r=0}^{\infty} \text{Tr}(x, S_r) t^r. \end{aligned}$$

Finally, combine these results to obtain the conclusion of Molien's Theorem.]

5. Let $\{\psi_m\}$ be the Adams operators on $\text{ch } KG$. Consider the character tables at the end of §9D, and also the table (14.22). For each irreducible character ζ in these tables, calculate $\psi_2(\zeta)$ and $\psi_3(\zeta)$. Then use (12.7) to find the characters of G afforded by the exterior powers $\wedge^2(Z_i)$ and $\wedge^3(Z_i)$, where Z_i ranges over a basic set of simple KG -modules.

6. Let $\mathbf{X} = \{X_1, \dots, X_n\}$ be a set of n variables, and let

$$q_1(\mathbf{X}) = X_1 + \cdots + X_n, \quad q_2(\mathbf{X}) = \sum_{i \leq j} X_i X_j, \quad q_3(\mathbf{X}) = \sum_{i \leq j \leq k} X_i X_j X_k,$$

and so on. Then

$$g(t) = \prod_{j=1}^n (1 + tX_j + t^2 X_j^2 + \cdots) = 1 + q_1 t + q_2 t^2 + \cdots.$$

Prove that

$$q_1 + 2q_2 t + 3q_3 t^2 + \cdots = \{p_1 + p_2 t + p_3 t^2 + \cdots\} \{1 + q_1 t + q_2 t^2 + \cdots\},$$

where the $\{p_i\}$ are the power sums occurring in (12.4). Find the identities, analogous to those in (12.4), which connect the $\{q_i\}$ and $\{p_i\}$.

7. Let M be a KG -module affording the character μ , and let $\{\psi_m\}$ be the Adams operators on $\text{ch } KG$. Using the results of the preceding Exercise, show how to calculate the characters afforded by the symmetric powers of M , in terms of the virtual characters $\{\psi_m(\mu) : m = 1, 2, \dots\}$. Determine the characters of $S^2(Z_i)$ and $S^3(Z_i)$ explicitly, where the $\{Z_i\}$ are as in Exercise 5.

§13. TENSOR INDUCTION AND TRANSFER

Let H be a subgroup of a finite group G , and let R be an arbitrary commutative ring. For each left RH -module L , we have defined an *induced* RG -module

$$\text{ind}_H^G(L) = RG \otimes_{RH} L = \bigoplus_{i=1}^n (g_i \otimes L),$$

where $G = \bigcup_{i=1}^n g_i H$, $|G:H|=n$. Let G/H denote the set of left cosets $\{g_i H\}$ of H in G , so the elements $\{g_i\}$ are a set of coset representatives. The action of an element $x \in G$ on $\text{ind}_H^G(L)$ involves a permutation action of x on the summands $\{g_i \otimes L\}$, as well as the action of H on L . It turns out (see (13.8)) that there is a family of RG -modules which can be constructed from the R -modules $\{g_i \otimes L\}$ by using this permutation action of G on the summands. These RG -modules correspond to the elementary symmetric functions of $\{g_i \otimes L\}$, with $\text{ind}_H^G(L)$ corresponding to the elementary symmetric function ΣX_i (see §12B). The RG -module associated with the elementary symmetric function ΠX_i has been studied extensively (Dress [71], Berger [77], Evens [63]), and is called the *tensor induced* module. We shall denote it by $\otimes \text{ind}_H^G(L)$, or briefly by $L^{\otimes G}$ when there is no danger of confusion. This section contains an introduction to tensor induction, and its connections with the group-theoretical transfer map. Relations between this transfer map and character theory are presented in §13B.

§13A. Tensor Induction

Let us begin with a close study of the permutation action of G on the set G/H of left cosets of H in G . Let H be any multiplicative group, and let $H^n = H \times \cdots \times H$ be the direct product of n copies of H . Let S_n be the symmetric group acting on $\{1, \dots, n\}$. Then S_n acts on H^n as a group of automorphisms, by means of the formula

$$\pi : (h_1, \dots, h_n) \rightarrow (h_{\pi^{-1}(1)}, \dots, h_{\pi^{-1}(n)}), \quad h_i \in H, \quad \pi \in S_n.$$

Thus, π moves the element h_i from the i -th place to the $\pi(i)$ -th place, for each i . We may therefore view π as a permutation of the places $\{\textcircled{1}, \dots, \textcircled{n}\}$ occurring in these n -tuples from H . Let us now form the semidirect product $H^n \rtimes S_n$, in which each $\pi \in S_n$ now acts as an inner automorphism on H :

$$(13.1) \quad \pi(h_1, \dots, h_n)\pi^{-1} = (h_{\pi^{-1}(1)}, \dots, h_{\pi^{-1}(n)}).$$

The group $H^n \rtimes S_n$ is often called the *wreath product* $H \wr S_n$.

Now let H be a subgroup of G , $|G:H|=n$, and let $G = \bigcup_{i=1}^n g_i H$. For $x \in G$, we have

$$(13.2) \quad xg_i = g_{\pi(i)} h_i, \quad h_i \in H, \quad 1 \leq i \leq n.$$

The permutation $\pi \in S_n$ and the elements $h_i \in H$ are uniquely determined by x .

(13.3) Lemma. Define a map $\varphi: G \rightarrow H^n \rtimes S_n$ by setting

$$\varphi(x) = \pi(h_1, \dots, h_n), \quad x \in G,$$

the product of π and the element (h_1, \dots, h_n) in $H^n \rtimes S_n$, where π and the elements $h_i \in H$ are given by (13.2). Then φ is a monomorphism of groups, and φ depends on the choice of the coset representatives $\{g_i\}$. If $\{g'_i\}$ is another set of representatives of G/H , then we have

$$g'_i = g_{\lambda(i)} h'_i, \quad h'_i \in H, \quad 1 \leq i \leq n,$$

for some $\lambda \in S_n$. The corresponding map $\varphi': G \rightarrow H^n \rtimes S_n$ satisfies

$$\varphi'(x) = s^{-1} \varphi(x) s, \quad x \in G,$$

where $s = \lambda(h'_1, \dots, h'_n)$ in $H^n \rtimes S_n$.

Proof. Given $x \in G$, let $\varphi(x)$ be defined as above. Let $y \in G$, and set $yg_i = g_{\sigma(i)} k_i$ for $1 \leq i \leq n$, with $\sigma \in S_n$ and $k_i \in H$, according to (13.2). Then

$$(xy)g_i = xg_{\sigma(i)} k_i = g_{\pi\sigma(i)} h_{\sigma(i)} k_i, \quad 1 \leq i \leq n,$$

so

$$\begin{aligned} \varphi(xy) &= \pi\sigma(h_{\sigma(1)} k_1, \dots, h_{\sigma(n)} k_n) \\ &= \pi\sigma(h_{\sigma(1)}, \dots, h_{\sigma(n)}) \sigma^{-1}\sigma(k_1, \dots, k_n) \\ &= \pi(h_1, \dots, h_n) \sigma(k_1, \dots, k_n) = \varphi(x)\varphi(y), \end{aligned}$$

using (13.1). The map φ is injective because, given only $\pi(1)$ and h_1 , x is determined uniquely by (13.2).

The proof of the second part of the lemma, on the conjugacy of $\varphi(G)$ and $\varphi'(G)$ in $H^n \rtimes S_n$, is left as an exercise.

We now apply these considerations to the construction of tensor induced modules. Keeping the preceding notation, let L be a left RH -module for some

commutative ring R . Let

$$\otimes^n L = L \otimes \cdots \otimes L \text{ (} n \text{ factors),}$$

where \otimes means \otimes_R , as in §12. Then $\otimes^n L$ is a left $R(H^n)$ -module, with the action of $(h_1, \dots, h_n) \in H^n$ on $l_1 \otimes \cdots \otimes l_n \in \otimes^n L$ given by

$$(h_1, \dots, h_n)(l_1 \otimes \cdots \otimes l_n) = h_1 l_1 \otimes \cdots \otimes h_n l_n.$$

(For $n=2$, this module is simply $L \# L$, the outer tensor product defined in (10.15).) The symmetric group S_n acts on $\otimes^n L$ as a group of symmetry operators (see §12A), with the action of $\pi \in S_n$ on $l_1 \otimes \cdots \otimes l_n \in \otimes^n L$ given by

$$\pi(l_1 \otimes \cdots \otimes l_n) = l_{\pi^{-1}(1)} \otimes \cdots \otimes l_{\pi^{-1}(n)}.$$

We now show that the combined actions of S_n and H^n on $\otimes^n L$ give $\otimes^n L$ the structure of a left $R(H^n \rtimes S_n)$ -module. For this, it is sufficient to check that both sides of (13.1) act in the same way on each $l_1 \otimes \cdots \otimes l_n \in \otimes^n L$. We have

$$\begin{aligned} \pi(h_1, \dots, h_n)\pi^{-1}(l_1 \otimes \cdots \otimes l_n) &= \pi(h_1, \dots, h_n)\{l_{\pi(1)} \otimes \cdots \otimes l_{\pi(n)}\} \\ &= \pi(h_1 l_{\pi(1)} \otimes \cdots \otimes h_n l_{\pi(n)}) = h_{\pi^{-1}(1)} l_1 \otimes \cdots \otimes h_{\pi^{-1}(n)} l_n, \end{aligned}$$

as required.

Now let $\varphi: G \rightarrow H^n \rtimes S_n$ be a monomorphism of groups, defined as in Lemma 13.3 relative to some set of coset representatives $\{g_i\}$ of G/H . We may use φ to give $\otimes^n L$ the structure of a left RG -module. The action of $x \in G$ on $l_1 \otimes \cdots \otimes l_n$ is then given by

$$\begin{aligned} (13.4) \quad x(l_1 \otimes \cdots \otimes l_n) &= \pi(h_1, \dots, h_n)(l_1 \otimes \cdots \otimes l_n) \\ &= h_{\pi^{-1}(1)} l_{\pi^{-1}(1)} \otimes \cdots \otimes h_{\pi^{-1}(n)} l_{\pi^{-1}(n)}, \end{aligned}$$

where $\varphi(x) = \pi(h_1, \dots, h_n)$ as in (13.3). It follows from the second part of Lemma 13.3 that any two actions of G on $\otimes^n L$, defined by use of two different sets of representatives of G/H , give rise to isomorphic RG -modules. The isomorphism is given by the action of an element $s \in H^n \rtimes S_n$ constructed as in (13.3).

(13.5) Definition. Let H be a subgroup of G of index n , and let L be a left RH -module. The operation which assigns to L the RG -module $\otimes^n L$, with the action of G given by (13.4), is called *tensor induction*, and will be denoted by

$$L \rightarrow \otimes \text{ind}_H^G(L),$$

or simply by

$$L \rightarrow L^{\otimes G}.$$

It is possible to give a somewhat more conceptual description of $\otimes \text{ind}_H^G(L)$, using the theory of additive induced modules from §10. For a set of representatives $\{g_i\}$ of G/H , we have a corresponding set of R -submodules $\{g_i \otimes L\}_{1 \leq i \leq n}$ of $\text{ind}_H^G(L) = RG \otimes_{RH} L$, and $\text{ind}_H^G(L)$ is their direct sum. We may instead form the tensor product $\bigotimes_{i=1}^n (g_i \otimes L)$ over R , and let G act diagonally on this R -module by the formula

(13.6)

$$x((g_1 \otimes l_1) \otimes \cdots \otimes (g_n \otimes l_n)) = (xg_1 \otimes l_1) \otimes \cdots \otimes (xg_n \otimes l_n), \quad x \in G, \quad l_i \in L.$$

In order to view the right hand side as an element of $\bigotimes_{i=1}^n (g_i \otimes L)$, it is necessary to identify

$$\bigotimes_{i=1}^n g_{\pi(i)} \otimes L \text{ with } \bigotimes_{i=1}^n g_i \otimes L,$$

for all $\pi \in S_n$, using the R -isomorphism

$$\bigotimes_{i=1}^n (g_{\pi(i)} \otimes l_i) \rightarrow \bigotimes_{i=1}^n g_i \otimes l_{\pi^{-1}(i)}.$$

We then use (13.2) to calculate the right hand side of (13.6), and obtain

$$\begin{aligned} (xg_1 \otimes l_1) \otimes \cdots \otimes (xg_n \otimes l_n) &= (g_{\pi(1)} h_1 \otimes l_1) \otimes \cdots \otimes (g_{\pi(n)} h_n \otimes l_n) \\ &= (g_{\pi(1)} \otimes h_1 l_1) \otimes \cdots \otimes (g_{\pi(n)} \otimes h_n l_n) \\ &= (g_1 \otimes h_{\pi^{-1}(1)} l_{\pi^{-1}(1)}) \otimes \cdots \otimes (g_n \otimes h_{\pi^{-1}(n)} l_{\pi^{-1}(n)}). \end{aligned}$$

Comparing this result with (13.4), we have

(13.7) Proposition. *Let L be an RH -module, and $\{g_i\}_{1 \leq i \leq n}$ a set of representatives of G/H . Then the tensor product of R -modules $\bigotimes_{i=1}^n (g_i \otimes L)$, with diagonal action of G defined by (13.6), is an RG -module. There is an isomorphism of RG -modules*

$$\bigotimes_{i=1}^n (g_i \otimes L) \cong \otimes \text{ind}_H^G(L),$$

given by

$$\bigotimes_{i=1}^n (g_i \otimes l_i) \in \bigotimes_{i=1}^n (g_i \otimes L) \rightarrow \bigotimes_{i=1}^n l_i \in \otimes^n L.$$

The previous discussion of $\otimes^n L$ as an $R(H^n \rtimes S_n)$ -module shows that $\otimes_{i=1}^n (g_i \otimes L)$ is independent (up to RG -isomorphism) of the choice of coset representatives $\{g_i\}_{1 \leq i \leq n}$.

Remark. The preceding discussion can be generalized to yield a family of RG -modules $s_k(L)$, $1 \leq k \leq n$. By definition,

$$(13.8) \quad s_k(L) = \coprod_{1 \leq i_1 < i_2 < \dots < i_k \leq n} (g_{i_1} \otimes L) \otimes_R \dots \otimes_R (g_{i_k} \otimes L),$$

with diagonal action of g as in (13.6). Thus

$$s_1(L) \cong \text{ind}_H^G(L), \quad s_n(L) \cong \otimes \text{ind}_H^G(L).$$

This collection of RG -modules $\{s_k(L) : 1 \leq k \leq n\}$ has properties analogous to those of the elementary symmetric functions.

We return to the consideration of $\otimes \text{ind}_H^G(L)$, which we abbreviate as $L^{\otimes G}$ as in (13.5). The next result shows that $L \rightarrow L^{\otimes G}$ is multiplicative, in the same sense that $L \rightarrow L^G$ is additive (see (10.6)).

(13.9) Proposition. *Let L and M be left RH-modules. Then*

$$(L \otimes M)^{\otimes G} \cong L^{\otimes G} \otimes M^{\otimes G},$$

where $L \otimes M$ denotes the inner tensor product of RH-modules, and $L^{\otimes G} \otimes M^{\otimes G}$ denotes the inner tensor product of RG-modules.

Proof. Letting $n = |G:H|$ as usual, it is sufficient to verify that the inner tensor product $(\otimes^n L) \otimes (\otimes^n M)$ of $R(H^n \rtimes S_n)$ -modules is isomorphic to the $R(H^n \rtimes S_n)$ -module $\otimes^n(L \otimes M)$, where $L \otimes M$ is the inner tensor product of RH-modules. We leave it to the reader to check that the R -isomorphism from $\otimes^n(L \otimes M)$ to $(\otimes^n L) \otimes (\otimes^n M)$, given by

$$(l_1 \otimes m_1) \otimes \dots \otimes (l_n \otimes m_n) \rightarrow (l_1 \otimes \dots \otimes l_n) \otimes (m_1 \otimes \dots \otimes m_n), \quad l_i \in L, \quad m_i \in M,$$

is the required $R(H^n \rtimes S_n)$ -isomorphism.

We conclude this section with the computation of the representation afforded by the tensor induced module $L^{\otimes G}$ in the simplest case, that in which L affords a linear representation $\lambda: H \rightarrow R$. In order to obtain the result, we shall need the group-theoretic *transfer map*

$$(13.10) \quad V_H^G: G/G' \rightarrow H/H',$$

where G/G' is the commutator factor group of G , and H/H' that of H .

Let $H \leq G$, $|G:H|=n$, $G = \dot{\cup} g_i H$ as above. For $x \in G$, write

$$xg_i = g_{\sigma(i)}h_i, \quad h_i \in H, \quad 1 \leq i \leq n,$$

as in (13.2). We now define

$$v(x) = \text{image of } \prod_{i=1}^n h_i \text{ in } H/H', \text{ for } x \in G.$$

For $y \in G$, let us write $yg_i = g_{\sigma(i)}k_i$, $k_i \in H$, as in the proof of (13.3). Then since H/H' is abelian, we obtain

$$v(xy) = \left\{ \prod_{i=1}^n h_{\sigma(i)}k_i \right\} H' = \{\prod h_i\} \{\prod k_i\} H' = v(x)v(y).$$

Thus v is a homomorphism from G into H/H' . If the set of coset representatives $\{g_i\}$ is replaced by another set $\{g'_i\}$, where

$$g'_i = g_{\tau(i)}z_i, \quad z_i \in H, \quad 1 \leq i \leq n,$$

for some $\tau \in S_n$, then it is easily checked that for $x \in G$,

$$xg'_i = g'_{\tau^{-1}\pi\tau(i)}h'_i, \text{ where } h'_i = z_{\tau^{-1}\pi\tau(i)}^{-1}h_{\tau(i)}z_i, \quad 1 \leq i \leq n.$$

It follows at once that $\prod_1^n h_i$ and $\prod_1^n h'_i$ have the same image in H/H' , so the map v is independent of the choice of coset representatives of G/H . Because H/H' is abelian, we thus obtain a well defined homomorphism (13.10), given by

$$(13.11) \quad V_H^G(xG') = \left\{ \prod_{i=1}^n h_i \right\} H', \quad x \in G,$$

where the $\{h_i\}$ are determined from x by (13.2). The homomorphism V_H^G is called the *transfer map* (or *Verlagerung*) from G/G' to H/H' .

(The transfer map can also be defined by using the Tate cohomology groups $\hat{H}^*(G, \mathbb{Z})$ introduced in §8C. The inclusion $H \leq G$ induces a homomorphism

$$\hat{H}^{-2}(G, \mathbb{Z}) \rightarrow \hat{H}^{-2}(H, \mathbb{Z}).$$

On the other hand,

$$\hat{H}^{-2}(G, \mathbb{Z}) \cong G/G', \quad \hat{H}^{-2}(H, \mathbb{Z}) \cong H/H',$$

by (8.54). It can be shown that the resulting homomorphism from G/G' to

H/H' coincides with the transfer V_H^G defined above. See Weiss [69, p. 116] for details.)

For applications of transfer to group theory, see Gorenstein [68, Chapter 7] or Huppert [67, Chapter IV]. In §13B, we shall follow Gallagher's approach [65] to the connection between transfer and induction and restriction of characters. Here, we shall content ourselves with using the transfer map to compute the character of a tensor induced module $L^{\otimes G}$ in the case where the original RH -module L affords a linear representation $\lambda: H \rightarrow R$. (As usual, $R = \text{units of } R$.) Thus, we start with an RH -module L having an R -basis consisting of a single element l , with the action of H on L given by

$$hl = \lambda(h)l, h \in H.$$

Then $L^{\otimes G}$ is also a free R -module with a single basis element m , where

$$m = \bigotimes_{i=1}^n (g_i \otimes l),$$

and $G = \dot{\cup} g_i H$. Let $x \in G$, and use (13.2) and (13.6) to obtain

$$\begin{aligned} xm &= \bigotimes_{i=1}^n (xg_i \otimes l) = \bigotimes_{i=1}^n g_{\pi(i)} \otimes h_i l \\ &= \bigotimes_{i=1}^n g_i \otimes h_{\pi^{-1}(i)} l = \left\{ \lambda \left(\prod_{i=1}^n h_i \right) \right\} m. \end{aligned}$$

(We have used the commutativity of the ring R .) But $H' \leq \ker \lambda$, so λ is well defined on H/H' . Since $V_H^G(x) = (\prod h_i)H'$ by (13.11), we obtain

(13.12) Proposition. *Let $\lambda: H \rightarrow R$ be a linear R -representation of H , afforded by an RH -module L which is R -free on one generator. Then $L^{\otimes G}$ is an RG -module which is R -free on one generator, and $L^{\otimes G}$ affords the linear representation $\lambda^{\otimes G}$ of G given by*

$$\lambda^{\otimes G}(x) = \lambda(V_H^G(x)), x \in G.$$

§13B. Transfer and the Determinant Map

We continue to study the permutation action of G on G/H , and its connection with character theory. Here we prove some results of Gallagher [65] which relate the transfer map (13.10) to the determinants of representations of finite groups. Another application of the determinant map, also due to Gallagher, appears in §15D.

In this subsection, all representations and character are taken in the complex field C .

Let G be a finite group, and M a left CG -module, affording a matrix representation \mathbf{M} with character μ . The multiplication theorem for determinants shows that the map $x \rightarrow \det \mathbf{M}(x)$, $x \in G$, is a linear representation of G , which depends only on the isomorphism class of M . We denote the character of the representation $x \rightarrow \det \mathbf{M}(x)$ by $\det \mu$, since μ determines M up to isomorphism. Then by definition,

$$(\det \mu)(x) = \det \mathbf{M}(x), \quad x \in G.$$

If μ and ν are \mathbb{C} -characters of G , then we have:

$$(13.13) \quad \begin{cases} \det(\mu + \nu) = (\det \mu)(\det \nu), \\ \det(\mu \nu) = (\det \mu)^{\nu(1)} (\det \nu)^{\mu(1)}. \end{cases}$$

The proofs of these formulas are left as exercises for the reader; they depend on the fact that the determinant of a matrix is the product of its eigenvalues.

Now let H be a subgroup of G , $n = |G : H|$, and let $G = \bigcup_{i=1}^n g_i H$ as in §13A. Set

$$xg_i = g_{\pi(i)} h_i, \quad \pi \in S_n, \quad h_i \in H, \quad 1 \leq i \leq n,$$

as in (13.2), and note that this formula can be rewritten as

$$(13.14) \quad g_{\pi(i)}^{-1} x g_i = h_i, \quad 1 \leq i \leq n.$$

Let $\epsilon_{G \rightarrow H}(x)$ denote the sign of the permutation π . The map $x \rightarrow \pi$ is the permutation representation of G on the left cosets G/H , and if $\mathbf{P}(x)$ is the permutation matrix corresponding to π , then $\epsilon_{G \rightarrow H}(x) = \det \mathbf{P}(x)$, $x \in G$.

(13.15) Proposition. *Let $H \leq G$, and let V_H^G be the transfer map.*

(i) *If λ is a \mathbb{C} -character of H , then*

$$\det \lambda^G = \left\{ \epsilon_{G \rightarrow H}^{\lambda(1)} \right\} \{ (\det \lambda) \circ V_H^G \},$$

that is,

$$(\det \lambda^G)(x) = \left\{ \epsilon_{G \rightarrow H}^{\lambda(1)}(x) \right\} \{ (\det \lambda)(V_H^G x) \} \text{ for all } x \in G.$$

(ii) *If ξ is a \mathbb{C} -character of G , then*

$$(\det \xi)^{|G:H|} = (\det \xi_H) \circ V_H^G.$$

Proof. Let \mathbf{L} be a matrix representation of H affording λ , and let $d = \deg \lambda$. Changing the notation of (10.1) slightly in order to conform to (13.14), we can

express $\mathbf{L}^G(x)$ as a matrix of $d \times d$ blocks:

$$\mathbf{L}^G(x) = (\dot{\mathbf{L}}(g_j^{-1}xg_i)), \quad x \in G,$$

where the j -th row of blocks of the matrix $\mathbf{L}^G(x)$ is

$$(\dot{\mathbf{L}}(g_j^{-1}xg_1), \dots, \dot{\mathbf{L}}(g_j^{-1}xg_n)).$$

Using this fact and (13.14), it is easily checked that we have a factorization

$$(13.16) \quad \mathbf{L}^G(x) = (\dot{\mathbf{I}}_d(g_j^{-1}xg_i)) \cdot \text{diag}(\mathbf{L}(h_1), \dots, \mathbf{L}(h_n)),$$

where for $h \in H$, $\mathbf{I}_d(h) = \mathbf{I}_d = d \times d$ identity matrix, and where $\dot{\mathbf{I}}_d$ denotes the extension of \mathbf{I}_d from H to G as in §10A. Taking determinants in (13.16), we obtain

$$\det \mathbf{L}^G(x) = \det(\dot{\mathbf{I}}_d(g_j^{-1}xg_i)) \cdot \prod_{i=1}^n \det \mathbf{L}(h_i).$$

Now $\det \mathbf{L}$ is a representation of H/H' , so by (13.11) the second factor on the right becomes

$$\prod_{i=1}^n \det \mathbf{L}(h_i) = (\det \mathbf{L}) \left(\prod_{i=1}^n h_i \right) = (\det \mathbf{L})(V_H^G x).$$

In order to compute the first factor $\det(\dot{\mathbf{I}}_d(g_j^{-1}xg_i))$, we note that if \mathbf{I}_d^G denotes $\text{ind}_H^G \mathbf{I}_d$, then $\mathbf{I}_d^G(x) = (\dot{\mathbf{I}}_d(g_j^{-1}xg_i))$ for $x \in G$. Letting $\mathbf{P}(x)$ be the permutation matrix corresponding to π in (13.14), we have

$$\mathbf{I}_d^G(x) = \mathbf{I}_d \otimes \mathbf{P}(x), \quad x \in G,$$

where \mathbf{I}_d is the d -rowed identity matrix. Then

$$\det \mathbf{I}_d^G(x) = \{\det \mathbf{P}(x)\}^d = \epsilon_{G \rightarrow H}^{\lambda(1)}(x),$$

by the definition of $\epsilon_{G \rightarrow H}$. Combining our results, we have proved part (i) of the proposition.

For the proof of (ii), we first observe that

$$\zeta_H^G = (1_H^G) \zeta.$$

Using this fact and (13.13), we obtain, after substituting ζ_H for λ in part (i),

$$(\det 1_H^G)^{\xi(1)} \cdot (\det \zeta)^{|G:H|} = \{\epsilon_{G \rightarrow H}^{\lambda(1)}\} \{(\det \zeta_H) \circ V_H^G\}.$$

Since $(\det 1_H^G)^{\zeta(1)} = \epsilon_{G \rightarrow H}^{\zeta(1)}$, we may cancel this factor, and obtain part (ii) of the proposition.

(13.17) Corollary. *Let $E \leq H \leq G$. Then*

$$\epsilon_{G \rightarrow E} = \{ \epsilon_{G \rightarrow H}^{|H : E|} \} \{ \epsilon_{H \rightarrow E} \circ V_H^G \}.$$

Proof. We have $\det(1_E^H) = \epsilon_{H \rightarrow E}$, and

$$\det(1_E^H)^G = \det 1_E^G = \epsilon_{G \rightarrow E},$$

by transitivity of induction. Applying Proposition 13.15i) to 1_E^H , we obtain

$$\epsilon_{G \rightarrow E} = \{ \epsilon_{G \rightarrow H}^{|H : E|} \} \{ \epsilon_{H \rightarrow E} \circ V_H^G \},$$

as required.

We conclude this section with some remarks, without complete proofs, on refinements of these results in case H is a normal subgroup of G . For details, see Gallagher [65].

Let N be a normal subgroup of G , and let $x \in G$ be such that the coset xN has order d in the factor group $F = G/N$. In the permutation action of G on the cosets G/N , the element x is therefore represented by a product of disjoint cycles, each of length d . It follows that

$$\epsilon_{G \rightarrow N}(x) = (-1)^{(d-1)(|F|/d)} = (-1)^{|F| - |F|/d}.$$

Consequently $\epsilon_{G \rightarrow N}(x) = 1$ unless $|F|$ is even and $|F|/d$ is odd. The latter case can occur only if a Sylow 2-subgroup S of F is contained in the cyclic group $\langle \bar{x} \rangle$ generated by the image \bar{x} of x in F . Thus $\epsilon_{G \rightarrow N} = 1_G$ unless the Sylow 2-subgroups of F are cyclic and non-trivial, and in that case $\epsilon_{G \rightarrow N} \neq 1$.

In the latter situation, in which a Sylow 2-subgroup S of F is cyclic of order 2^a , where $a > 0$, the automorphism group of S has order $\varphi(2^a) = 2^{a-1}$. It follows that $N_F(S)/C_F(S)$ has odd order dividing 2^{a-1} , hence $N_F(S) = C_F(S)$. By a theorem of Burnside (see §13C), it follows that F has a normal 2-complement. It is also possible to prove this directly, as follows. Let F_ϵ be the kernel of $\epsilon_{G \rightarrow N}$ in F . Then $F_\epsilon < F$, and by induction F_ϵ has a normal 2-complement H , which is* $O_2(F_\epsilon)$, and hence characteristic in F_ϵ . Then H is normal in F , and is the required normal 2-complement. From these considerations, we conclude that if $\epsilon_{G \rightarrow N} \neq 1$, then $\epsilon_{G \rightarrow N}$ is the only nontrivial homomorphism from G to $\{\pm 1\}$.

Returning to an arbitrary normal subgroup N , let $\zeta \in \text{Irr } G$, $\psi \in \text{Irr } N$, and assume that $(\zeta, \psi^G) > 0$. Let $T = G_\psi$, the stabilizer of ψ (see §11B); then by

* $O_2(F_\epsilon)$ denotes the maximal normal 2'-subgroup of F_ϵ .

(11.4) there exists $\zeta \in \text{Irr } T$ such that

$$\zeta = \xi^G \text{ and } \xi|_N = a\psi,$$

for some positive integer a . The integer a is the degree of an irreducible projective representation of T/N by (11.20), so a divides $|T:N|$ by (11.44). It follows that

$$\frac{\psi^G(1)}{\zeta(1)} = \frac{|G:N|\psi(1)}{a\psi(1)|G:T|} = \frac{|T:N|}{a} \in \mathbb{Z}.$$

We can now state

(13.18) Proposition. *Let $N \trianglelefteq G$, $\zeta \in \text{Irr } G$, $\psi \in \text{Irr } N$, and assume $(\zeta, \psi^G) > 0$. Let e be the integer $\psi^G(1)/\zeta(1)$. Then*

$$(\det \zeta)^e = \{e_{G \rightarrow H}^{e\psi(1)}\} \{(\det \psi) \circ V_N^G\}.$$

For finite groups, the Principal Ideal Theorem states that $V_{G'}^G$ is trivial (see Zassenhaus [49, Chapter V, §4]). Using this result and (13.18), Gallagher proved:

(13.19) Corollary. *For each pair of irreducible characters ζ of G and ψ of G' , with $(\zeta, \psi^G) > 0$, we have*

$$(\det \zeta)^f = \{e_{G \rightarrow G'}^{f\psi(1)}\} \cdot \det \psi,$$

where

$$f = \psi(1)|G:G'|/\zeta(1).$$

§13C. Normal p -Complements and the Transfer

A finite group G is said to have a *normal p -complement*, for some prime p , if G has a normal subgroup N whose order is the p' -part of the order of G . In this situation, N has order prime to p , and index $|G:N|$ equal to a power of p . If G has a normal p -complement, then G has a decomposition as a semidirect product, $G = N \rtimes S$, for any Sylow p -subgroup S of G (compare with Theorem 8.35). In case N is a normal p -complement in G , then N coincides with $O_p(G)$, the unique maximal normal subgroup of G whose order is prime to p . Therefore a normal p -complement is uniquely determined, if it exists.

Many theorems in finite group theory involve the existence of normal p -complements. Following M. Hall [59, §14.3], we shall derive one of the most important of these theorems, as an application of the transfer map V_H^G defined in §13A. Later, in §15E, we shall obtain a more general result, as an application of the Brauer Induction Theorem (see (15.25) and (15.27)).

(13.20) Burnside's Transfer Theorem. *Let S be a Sylow p -subgroup of a finite group G such that S is contained in the center of its normalizer. Then G contains a normal p -complement.*

We first require

(13.21) Lemma. *Let X and Y be subsets of a Sylow p -subgroup S of G . If both X and Y are normalized by S and are conjugate in G , then X and Y are conjugate in $N_G(S)$.*

Proof. Let $X^u = Y$, for some $u \in G$. Then X^u is normalized by S^u , and both S and S^u are contained in the normalizer N of Y . By Sylow's Theorem, S and S^u are conjugate in N , so $S^{uv} = S$ for some element v such that $Y^v = Y$. Setting $z = uv$, we have $z \in N_G(S)$, and

$$X^z = X^{uv} = (X^u)^v = Y^v = Y,$$

as required.

Proof of the Theorem. Since S is in the center of $N_G(S)$, S is abelian, and $S' = 1$. We shall investigate the transfer map $V_S^G: G/G' \rightarrow S$. By the discussion in §13A, formula (13.11) for V_S^G is independent of the choice of coset representatives. Thus we may compute $V_S^G(u)$, for each $u \in G$, by using coset representatives of G/S tailored to the element u . Given $u \in G$, we may partition the cosets in G/S into orbits under the action of left multiplication by $\langle u \rangle$. These orbits correspond to the decomposition of the permutation

$$xS \rightarrow uxS, x \in G,$$

as a product of disjoint cycles (see CR §1 for this approach to the cycle decomposition of a permutation). Letting $\{x_i S\}_{1 \leq i \leq m}$ be representatives of these orbits, we have as coset representatives of G/S the elements

$$\{u^j x_i : 0 \leq j \leq d_i - 1, 1 \leq i \leq m\},$$

where d_i is the length of the cycle corresponding to the orbit of $x_i S$ under the action of $\langle u \rangle$. The element u acts on the coset representatives as follows:

$$u \cdot u^j x_i = u^{j+1} x_i, \quad 0 \leq j \leq d_i - 1, \quad 1 \leq i \leq m,$$

and

$$u \cdot u^{d_i-1} x_i = x_i s_i, \text{ for some } s_i \in S.$$

It follows (by (13.11)) that

$$V_S^G(u) = \prod_{i=1}^m s_i = \prod_{i=1}^m x_i^{-1} u^{d_i} x_i.$$

In particular, for $u \in S$, u^{d_i} and $x_i^{-1}u^{d_i}x_i$ are both in S , and are normalized by S and conjugate in G . By the preceding lemma, they are conjugate in $N_G(S)$. Since S is contained in the center of $N_G(S)$, we have

$$x_i^{-1}u^{d_i}x_i = u^{d_i}, \quad 1 \leq i \leq m.$$

Consequently,

$$V_S^G(u) = u^{|G:S|}, \quad u \in S.$$

Since $|G:S|$ is prime to p , and S is an abelian p -group, it follows that $V_S^G: G/G' \rightarrow S$ is surjective, and the restriction of V_S^G to SG'/G' is an isomorphism. The kernel H of V_S^G is therefore a subgroup of G/G' of index $|S|$. Therefore there exists a normal subgroup N of G of index $|S|$, and N is the desired p -complement.

The above theorem provides a significant start towards the classification of 2-groups which can appear as Sylow 2-subgroups of non-abelian simple group (see §14E for a continuation of this project).

(13.22) Corollary. *A finite non-abelian group G with a non-trivial cyclic Sylow 2-subgroup must have a normal 2-complement. Hence G cannot be simple.*

Proof. Let S be a Sylow 2-subgroup of G , and assume S is cyclic of order 2^a , $a \geq 1$. Then the automorphism group of S has order $\varphi(2^a) = 2^{a-1}$, where φ is the Euler φ -function. Then $N_G(S)/S$ has order dividing 2^{a-1} . On the other hand, $N_G(S)/S$ has odd order, since S is a Sylow 2-subgroup by hypothesis. It follows that $N_G(S)$ acts trivially on S , and therefore S is contained in the center of $N_G(S)$. But then G has a normal 2-complement by Burnside's Theorem, which completes the proof.

§13. Exercise

1. Prove the analogue of the Mackey Subgroup Theorem for tensor induction. In other words, let E and H be subgroups of a finite group G , and let M be an RH -module. Then

$$(M^{\otimes G})_E \cong \bigotimes_g \{(g \otimes M)_{E_g}\}^{\otimes E},$$

where $G = \bigcup EgH$, and $E_g = E \cap {}^g H$.

§14. SPECIAL CLASSES AND EXCEPTIONAL CHARACTERS

The results in the present section, and their applications, form a vein in group theory which has perhaps released most of its treasures by now. Nevertheless, this approach retains an elusive and fresh aspect which suggests that it may

yet provide new insights. The method, due to Brauer and Suzuki, involves an extension of the character theory used in the proof of Frobenius' Theorem (see §14A), and is of extraordinary flexibility and strength. In the past, it has been one of the key steps in the proofs of some major classification theorems for finite simple groups.

This part of character theory, together with Brauer's work on blocks of characters, constitute the central contribution of representation theory to the theory of finite simple groups developed during the past two decades. There is a vast literature devoted to this topic alone. Our account begins with the proof of a theorem of Frobenius, where some of the essential ideas originated. This application of character theory to finite group theory motivates the later discussion, especially since all known proofs of Frobenius' Theorem rely on character-theoretic methods. We shall then give Suzuki's [59] technique of exceptional characters, which was historically the first attempt to describe the general method involved. Finally, we shall illustrate the application of these results to finite group theory. For other applications of exceptional characters and extensions of the method, see Feit [67], Isaacs [76], Feit-Thompson [63], and articles on character theory in the proceedings of symposia volumes (Madison and Santa Cruz) listed on the first page of the Bibliography.

§14A. Frobenius Groups

(14.1) Definition. A *Frobenius group* is a finite group G with a nontrivial subgroup H such that

$$H \cap H^x = 1, \forall x \in G - H.$$

The subgroup H is called the *Frobenius complement*. We shall show below that G contains a normal subgroup N such that $G = NH$ and $N \cap H = 1$; such an N is called a *Frobenius kernel* of G .

Frobenius groups occur abundantly, the simplest example being the dihedral group of order $2(2m+1)$:

$$D_{2m+1} = \langle a, b : a^{2m+1} = b^2 = (ab)^2 = 1 \rangle,$$

with Frobenius complement $H = \langle b \rangle$ and Frobenius kernel $N = \langle a \rangle$. This example illustrates the general fact that $(|G:H|, |H|) = 1$ for H a Frobenius complement in the Frobenius group G . This result is an easy consequence of the Sylow theorems and the fact that the center of a Sylow group is nontrivial.

The main theorem of this subsection is that in every Frobenius group, the Frobenius kernel exists and is uniquely determined. The proof is based on the character theory developed in §9C.

(14.2) Theorem (Frobenius). Let G be a Frobenius group with Frobenius complement H . Then there exists a unique Frobenius kernel N in G .

Proof. Step 1. Throughout this proof let K be the complex field, $\text{ch}(KG)$ the ring of virtual complex characters of G , $\text{cf}(G)$ the ring of complex-valued class functions on G , and $\text{Irr}(G)$ the set of irreducible complex characters of G . Let H be a Frobenius complement in the Frobenius group G , and set

$$S = \left(G - \bigcup_{x \in G} H^x \right) \cup \{1\}.$$

We shall show that S is the desired Frobenius kernel, and begin by proving that $|S| = |G : H|$. Indeed, from the definition of Frobenius complement it follows that $H = N_G(H)$, so there are exactly $|G : H|$ distinct subgroups H^x . These have only the identity element in common, so $\bigcup_x H^x$ consists of $1 + |G : H|(|H| - 1)$ elements. Therefore

$$|S| = |G| - |G : H|(|H| - 1) = |G : H|,$$

as claimed.

We remark that if G contains a Frobenius kernel N , then necessarily $N = S$. Indeed, if N exists then $|N| = |G : H| = |S|$, and furthermore $N \cap H^x = 1$ for all $x \in G$ (since $N \cap H = 1$ and $N \trianglelefteq G$), whence $N \subseteq S$. This shows that if N exists, then N is unique; the crux of the difficulty lies in proving that S is indeed a subgroup of G .

Step 2. Now let $\theta \in \text{cf}(H)$ be such that $\theta(1) = 0$, and let us show that $\theta^G|_H = \theta$. Clearly $\theta^G(1) = |G : H|\theta(1) = 0$. On the other hand, let $h \in H$, $h \neq 1$; then

$$\theta^G(h) = |H|^{-1} \sum_{x \in G} \dot{\theta}(x^{-1}hx)$$

by (10.3). If $\dot{\theta}(x^{-1}hx) \neq 0$ then $h^x \neq 1$ and $h^x \in H \cap H^x$. It follows that $x \in H$, so $\dot{\theta}(x^{-1}hx) = \theta(h)$ since $\theta \in \text{cf}(H)$. Thus

$$\theta^G(h) = |H|^{-1} \sum_{x \in H} \theta(x^{-1}hx) = \theta(h),$$

which proves that $\theta^G|_H = \theta$.

Step 3. We show next that the map $\theta \rightarrow \theta^G$ gives an isometry from $\{\theta \in \text{cf}(H) : \theta(1) = 0\}$ into $\text{cf}(G)$, where the isometry is with respect to the scalar products $(,)_H$ and $(,)_G$. Indeed, let $\theta, \eta \in \text{cf}(H)$ be such that

$\theta(1)=\eta(1)=0$. Then Step 2 and the Frobenius Reciprocity Theorem 10.9 yield

$$(\theta^G, \eta^G)_G = (\theta^G|_H, \eta)_H = (\theta, \eta)_H,$$

as desired.

Step 4. To complete the proof of the theorem, we shall exhibit the above-defined set S as an intersection of kernels of certain irreducible characters of G . Given $\varphi \in \text{Irr}(H)$, let $\theta = \varphi - \varphi(1)1_H$; then $\theta \in \text{cf}(H)$ and $\theta(1)=0$. Since $\theta \in \text{ch}(KH)$, it follows that $\theta^G \in \text{ch}(KG)$. Setting

$$\varphi^* = \theta^G + \varphi(1)1_G,$$

we have also $\varphi^* \in \text{ch}(KG)$. By Frobenius Reciprocity and Step 3, we obtain

$$\begin{aligned} \|\varphi^*\|_G^2 &= (\varphi^*, \varphi^*)_G = (\theta^G, \theta^G)_G + 2\varphi(1)(\theta^G, 1_G) + \varphi(1)^2 \\ &= (\theta, \theta)_H + 2\varphi(1)(\theta, 1_H) + \varphi(1)^2 \\ &= (\theta + \varphi(1)1_H, \theta + \varphi(1)1_H)_H = (\varphi, \varphi)_H = 1. \end{aligned}$$

But $\varphi^* \in \text{ch}(KG)$, so from $\|\varphi^*\|_G^2 = 1$ it follows that $\pm \varphi^* \in \text{Irr}(G)$. However,

$$\varphi^*(1) = \theta^G(1) + \varphi(1) = \varphi(1) > 0,$$

whence $\varphi^* \in \text{Irr}(G)$. This shows that $\varphi^* \in \text{Irr}(G)$ for every $\varphi \in \text{Irr}(H)$. Note that

$$(\varphi^*)_H = \theta^G|_H + \varphi(1)1_H = \theta + \varphi(1)1_H = \varphi.$$

Now set

$$M = \bigcap_{\varphi \in \text{Irr}(H)} \ker \varphi^*,$$

so $M \trianglelefteq G$. If $h \in M \cap H$, then for all $\varphi \in \text{Irr}(H)$ we have

$$\varphi^*(1) = \varphi^*(h) = \varphi(h).$$

Thus $\varphi(h) = \varphi(1)$ for all $\varphi \in \text{Irr}(H)$, so $h = 1$ by Exercise 9.5. This shows that $M \cap H = 1$, whence also $M \cap H^x = 1$ for all $x \in G$ since $M \trianglelefteq G$. Therefore $M \subseteq S$, where S is as defined in Step 1. Conversely, if $g \in S$, $g \neq 1$, then $g \notin H^x$ for all $x \in G$, whence $\theta^G(g) = 0$ for each θ , by definition of induced characters. But then $\varphi^*(g) = \varphi^*(1)$ for each φ , so $g \in M$. Thus $M = S$, and the preceding discussion gives $S \trianglelefteq G$, $S \cap H = 1$, $G = SH$, and S is the unique Frobenius kernel. This completes the proof of the theorem.

(14.3) Corollary. *Let G be a finite group acting transitively on a finite set X , and assume that each element $g \neq 1$ in G fixes at most one element of X . Then the set of elements of G having no fixed points, together with the identity, forms a transitive normal subgroup N of G .*

Remark. Let χ be the character of the permutation representation of G on X . In terms of χ , the hypothesis asserts that

$$\chi(g) \leq 1, \forall g \in G, g \neq 1.$$

Then the transitive normal subgroup N is defined by

$$N = \{g \in G : \chi(g) = 0\} \cup \{1\}.$$

Proof. Since X is a transitive G -set, $X \cong G/H$ as G -sets, where $H = \text{Stab}_G(x_0)$ for some $x_0 \in X$. An element $g \in G$ fixes a coset tH if and only if $g \in tHt^{-1}$. Thus the hypothesis implies that $H' \cap H = 1$ for all $t \in G - H$, so G is a Frobenius group with Frobenius complement H . The preceding remarks, together with Step 1 of the proof of (14.2), show that the Frobenius kernel coincides with the subgroup described in the statement of the corollary. Finally, N acts transitively on X because $NH = G$ and $X \cong G/H$.

Now that we have established the existence of the Frobenius kernel N of a Frobenius group G , we may use the results of §11B to describe the character theory of G :

(14.4) Proposition. *Let G be a Frobenius group with Frobenius kernel N . Then*

- (i) $C_G(n) \leq N$ for all $n \in N$, $n \neq 1$.
- (ii) If $\psi \in \text{Irr}(N)$ is such that $\psi \neq 1_N$, then $\psi^G \in \text{Irr}(G)$ and $N \not\leq \ker \psi^G$. Conversely, each $\xi \in \text{Irr}(G)$ such that $N \not\leq \ker \xi$ can be expressed as $\xi = \psi^G$ for some $\psi \in \text{Irr}(N)$, $\psi \neq 1_N$.

Proof. It suffices to prove (i), since the remaining statements then follow from Theorem 11.11. Let $n \in N$, $n \neq 1$, and suppose that $C_G(n) \not\leq N$. By the characterization of N in the proof of Theorem 14.2, we then have $C_G(n) \cap H^x \neq 1$ for some $x \in G$. After conjugating by x^{-1} and changing notation, we now have $C_G(n) \cap H \neq 1$ with $n \in N$, $n \neq 1$. Let $h \in C_G(n) \cap H$, $h \neq 1$; then $h \in H \cap H^n$, which contradicts the fact that H is a Frobenius complement, and completes the proof.

For further discussion of Frobenius groups, see Feit [67] and Isaacs [76].

§14B. Special Classes

We shall describe a general situation where part of the character table of a group G can be determined from a corresponding part of the character table of a subgroup. The method is due to Suzuki [59]; our account follows an exposition of Suzuki's work by G. Higman [68].

Throughout this subsection, H denotes a subgroup of a finite group G . For $x, y \in G$, we write $x =_G y$ if $x = y^g$ for some $g \in G$, and $x =_H y$ if $x = y^h$ for some $h \in H$. As in §14A, K denotes the complex field.

(14.5) Definition. A set of distinct conjugacy classes $\{\mathfrak{S}_1, \dots, \mathfrak{S}_n\}$ of H , with representatives $h_i \in \mathfrak{S}_i$, $1 \leq i \leq n$, is called a set of *special classes* in H provided that the following conditions hold:

$$(i) \quad C_G(h_i) \leq H \text{ for } 1 \leq i \leq n,$$

$$(ii) \quad h_i \neq_G h_j \text{ for } i \neq j,$$

$$(iii) \quad \text{If } \langle h \rangle = \langle h_j \rangle, \text{ where } h \in H \text{ and } 1 \leq j \leq n, \text{ then } h \in \mathfrak{S}_i \text{ for some } i, 1 \leq i \leq n, \text{ that is, } h \text{ is } H\text{-conjugate to some } h_i.$$

Condition (ii) above asserts that the elements $\{h_1, \dots, h_n\}$ belong to distinct conjugacy classes in G , as well as in H . Condition (iii) is a sort of completeness condition whose importance will become clear in the proof of Lemma 14.6.

Some additional notation is needed:

$$\mathfrak{S} = \mathfrak{S}_1 \cup \dots \cup \mathfrak{S}_n, \text{ the union of the special classes,}$$

$$\text{Irr}(H) = \{\psi^1 = 1_H, \psi^2, \dots, \psi^r\}, \text{ Irr}(G) = \{\zeta^1 = 1_G, \zeta^2, \dots, \zeta^s\},$$

$$\text{ch}(KH) = \sum \mathbb{Z} \psi^i, \text{ ch}(KG) = \sum \mathbb{Z} \zeta^i, \text{ the rings of virtual characters on } H \text{ and } G, \text{ respectively,}$$

$$W(\mathfrak{S}) = \{\varphi \in \text{cf}(H) : \varphi|_{H-\mathfrak{S}} = 0\}, \text{ the class functions on } H \text{ vanishing off the special classes.}$$

(14.6) Lemma. $W(\mathfrak{S})$ has a K -basis consisting of n virtual characters $\{\lambda_1, \dots, \lambda_n\}$ in $\text{ch}(KH)$.

Proof. Let $\{h_{n+1}, \dots, h_r\}$ be representatives of the H -conjugacy classes in $H - \mathfrak{S}$. A class function $\sum_{i=1}^r x_i \psi^i$, $x_i \in K$, belongs to $W(\mathfrak{S})$ if and only if

$$(14.7) \quad \sum_{i=1}^r x_i \psi^i(h_j) = 0 \text{ for } n+1 \leq j \leq r.$$

If W denotes the set of r -tuples (x_1, \dots, x_r) for which (14.7) holds, then the map $(x_1, \dots, x_r) \rightarrow \sum x_i \psi^i$ gives a K -isomorphism $W \cong W(\mathfrak{S})$, since the $\{\psi^i\}$ are linearly independent over K . Clearly $\dim_K W = n$, since the n characteristic functions on the special classes $\{\mathfrak{S}_i\}$ form a K -basis for $W(\mathfrak{S})$. We must show that W has a K -basis of r -tuples with entries in \mathbb{Z} .

Let ξ be a primitive $|H|$ -th root of 1, $E = \mathbb{Q}(\xi)$, and $G_{E/\mathbb{Q}}$ the Galois group of the Galois extension E of \mathbb{Q} . For each $\sigma \in G_{E/\mathbb{Q}}$ we have $\sigma(\xi) = \xi^j$ for some integer j such that $(j, |H|) = 1$. Let $h \in H$; since $\psi^i(h)$ is a sum of powers of ξ , it follows that

$$(14.8) \quad \sigma(\psi^i(h)) = \psi^i(h^j) \text{ for all } h \in H,$$

where $\sigma(\xi) = \xi^j$ as above. Finally, we note that if $(j, |H|) = 1$ then $\langle h^j \rangle = \langle h \rangle$ for all $h \in H$.

We show next that if $(j, |H|) = 1$, then $h \in H - \mathfrak{S}$ implies that also $h^j \in H - \mathfrak{S}$. Indeed, we have $\langle h \rangle = \langle h^j \rangle$, so if $h^j \in \mathfrak{S}$ then also $h \in \mathfrak{S}$ by condition (iii) of Definition 14.5. By virtue of (14.8), it follows that if $w = (x_1, \dots, x_r) \in W$, with each $x_i \in E$, then also $\sigma(w) = (\sigma(x_1), \dots, \sigma(x_r)) \in W$.

Now the coefficients $\{\psi^i(h_j)\}$ occurring in (14.7) all belong to E , so W has a K -basis w_1, \dots, w_n , with each w_i an r -tuple having entries in E . We may further assume that the $n \times r$ matrix with rows w_1, \dots, w_n , is in row echelon form, and that the first nonzero entry of each w_i equals 1. Let $\sigma \in G_{E/\mathbb{Q}}$; since $\sigma(w_i) \in W$ for each i , we can express $\sigma(w_i)$ as an E -linear combination of w_1, \dots, w_n . But then $\sigma(w_i) = w_i$, by virtue of the echelon form. Thus $\sigma(w_i) = w_i$ for all i and all $\sigma \in G_{E/\mathbb{Q}}$, whence each w_i has entries in \mathbb{Q} . Clearing denominators, we then obtain a K -basis of W in which the entries of the vectors all lie in \mathbb{Z} , completing the proof.

We show next that condition (i) in Definition 14.5 leads to a generalization of the isometry described in Step 3 of the proof of Theorem 14.2.

(14.9) Lemma. *Let \mathfrak{S} be the union $\cup \mathfrak{S}_i$ of the special classes. If $x \in G$ is such that $x\mathfrak{S}x^{-1} \cap \mathfrak{S} \neq \emptyset$, then $x \in H$ and $x\mathfrak{S}x^{-1} = \mathfrak{S}$. For class functions $\lambda, \mu \in \text{cf}(H)$ which vanish off the special classes, we have*

$$\lambda^G|_H = \lambda, \text{ and } (\lambda^G, \mu^G)_G = (\lambda, \mu)_H.$$

Proof. Let $x\mathfrak{S}x^{-1} \cap \mathfrak{S} \neq \emptyset$, where $x \in G$. After multiplying x on the left and right by elements of H , we may assume that $xh_i x^{-1} = h_j$, for some i, j , $1 \leq i, j \leq n$. By condition (ii) of Definition 14.5, we have $i = j$, and hence by (i) we have $x \in H$. Therefore $x\mathfrak{S}x^{-1} = \mathfrak{S}$ because \mathfrak{S} is a union of H -conjugacy classes. The rest of the proof is exactly the same as Steps 2 and 3 in the proof of Theorem 14.2.

We now introduce some additional notation. Recalling that $\text{Irr}(H) = \{\psi^1, \psi^2, \dots, \psi^r\}$, we write the $\{\lambda_i\}$ in (14.6) as

$$\lambda_i = \sum a_{ij} \psi^j, a_{ij} \in \mathbb{Z},$$

for some uniquely determined $n \times r$ matrix $\mathbf{A} = (a_{ij})$ over \mathbb{Z} . Similarly, the induced virtual characters λ_i^G can be expressed in terms of the characters $\{\xi^1, \dots, \xi^s\}$ in $\text{Irr}(G)$, say

$$\lambda_i^G = \sum b_{ij} \xi^j, b_{ij} \in \mathbb{Z},$$

for an $n \times s$ matrix $\mathbf{B} = (b_{ij})$ over \mathbb{Z} .

(14.10) Lemma. (i) $b_{i1} = a_{i1}$, $1 \leq i \leq n$.

$$\text{(ii)} \quad \sum_{k=1}^s b_{ik} b_{jk} = \sum_{k=1}^r a_{ik} a_{jk} \text{ for } 1 \leq i, j \leq n, \text{ that is, } \mathbf{B} \cdot {}^\dagger \mathbf{B} = \mathbf{A} \cdot {}^\dagger \mathbf{A}.$$

$$\text{(iii)} \quad \sum_{i=1}^s \xi^i(h_j) \xi^i(h_k) = \sum_{i=1}^r \psi^i(h_j) \psi^i(h_k), \quad 1 \leq j, k \leq n.$$

$$\text{(iv)} \quad \sum_{j=1}^s b_{ij} \xi^j(h_k) = \sum_{j=1}^r a_{ij} \psi^j(h_k), \quad 1 \leq k \leq n.$$

Proof. (i) Recalling that $\xi^1 = 1_G$ and $\psi^1 = 1_H$, we have

$$(\lambda_i, \psi^1) = (\lambda_i^G, \xi^1), \quad 1 \leq i \leq n,$$

by Frobenius Reciprocity, whence $a_{i1} = b_{i1}$.

(ii) For $1 \leq i, j \leq n$, λ_i and λ_j vanish off the special classes, hence by Lemma 14.9 we have

$$(\lambda_i^G, \lambda_j^G) = (\lambda_i, \lambda_j).$$

Statement (ii) now follows from the definitions of the matrices \mathbf{A} and \mathbf{B} , and the orthogonality relations in $\text{cf}(H)$ and $\text{cf}(G)$.

(iii) This result is immediate from the Second Orthogonality Relation (9.26ii), using conditions (i) and (ii) of Definition 14.5.

(iv) We have $\lambda_i^G = \sum b_{ij} \xi^j$, and $\lambda_i^G|_H = \lambda_i$, by Lemma 14.9. In particular, $\lambda_i^G(h_k) = \lambda_i(h_k)$ for $1 \leq k \leq n$, which implies (iv), and completes the proof of the lemma.

The main result of this subsection is that from the information in Lemma 14.10, it is possible (in a certain sense) to solve the equations

$$\sum \xi'(h_j)\xi'(h_k) = \sum \psi'(h_j)\psi'(h_k)$$

for the character values $\xi'(h_j)$, thus giving that part of the character table of G which involves the character values on the classes in G arising from the special classes in H .

(14.11) Theorem (Suzuki). *There exist uniquely determined elements $\{c_{jk}\}$ of K , $1 \leq j, k \leq n$, such that*

$$\psi'(h_j) = \sum_{k=1}^n c_{jk} a_{ki}.$$

For these elements $\{c_{jk}\}$, we have

$$\xi^i(h_j) = \sum_{k=1}^n c_{jk} b_{ki}.$$

In other words, there exists an $n \times n$ matrix \mathbf{C} such that

$${}^t(\psi'(h_j)) = \mathbf{CA},$$

and for this matrix we have

$${}^t(\xi^i(h_j)) = \mathbf{CB}.$$

Proof. For each j , $\sum_i \psi'(h_j)\psi'$ vanishes off the special classes, by the Second Orthogonality Relation for H . Since $\{\lambda_1, \dots, \lambda_n\}$ are a basis for $W(\mathfrak{S})$, we therefore have

$$\sum_i \psi'(h_j)\psi' = \sum_k c_{jk} \lambda_k,$$

for some uniquely determined elements $c_{jk} \in K$. Moreover, expressing the $\{\lambda_k\}$ in terms of the ψ' , we have

$$\sum_k c_{jk} (\sum_l a_{kl} \psi') = \sum_l (\sum_k c_{jk} a_{kl}) \psi'.$$

Comparing coefficients of the $\{\psi'\}$ we obtain

$$\psi'(h_j) = \sum_{k=1}^n c_{jk} a_{ki},$$

which is the first assertion of the theorem.

For the second, we first verify that equations (14.10iv) hold when the $\{\xi'(h_j)\}$ are replaced by $\sum_{k=1}^n c_{jk} b_{ki}$. We have

$$\begin{aligned} \sum_{j=1}^s b_{ij} \sum_{l=1}^n c_{kl} b_{lj} &= \sum_{l=1}^n c_{kl} \left(\sum_{j=1}^s b_{ij} b_{lj} \right) = \sum_{l=1}^n c_{kl} \left(\sum_{j=1}^r a_{ij} a_{lj} \right) \\ &= \sum_{j=1}^r a_{ij} \left(\sum_{l=1}^n c_{kl} a_{lj} \right) = \sum_{j=1}^r a_{ij} \psi^j(h_k), \end{aligned}$$

using Lemma 14.10ii). This means that if we set

$$\xi^i(h_j) = \sum_{k=1}^n c_{jk} b_{ki} + \epsilon_{ij}, \quad 1 \leq i \leq s, 1 \leq j \leq n,$$

then we have

$$(14.12) \quad \sum_{j=1}^s b_{ij} \epsilon_{jk} = 0 \text{ for } 1 \leq i \leq s, 1 \leq k \leq n.$$

Substituting in the left hand side of Lemma 14.10iii) we obtain

$$\sum_{i=1}^s \xi^i(h_j) \xi^i(h_k) = \sum_{i=1}^s \left(\sum_{p=1}^n c_{jp} b_{pi} + \epsilon_{ij} \right) \left(\sum_{q=1}^n c_{kq} b_{qi} + \epsilon_{ik} \right).$$

For the “cross terms” we have

$$\sum_{i=1}^s \epsilon_{ij} \left(\sum_{q=1}^n c_{kq} b_{qi} \right) = 0$$

by (14.12), and similarly

$$\sum_{i=1}^s \left(\sum_{p=1}^n c_{jp} b_{pi} \right) \epsilon_{ik} = 0.$$

For the “leading terms” we have by (14.10ii),

$$\begin{aligned} \sum_i \sum_p \sum_q c_{jp} b_{pi} c_{kq} b_{qi} &= \sum_{p,q} c_{jp} c_{kq} \sum_{i=1}^s b_{pi} b_{qi} \\ &= \sum_{p,q} c_{jp} c_{kq} \sum_{i=1}^r a_{pi} a_{qi} = \sum_{i=1}^r \psi^i(h_j) \psi^i(h_k), \end{aligned}$$

which is the right hand side of (14.10iii). Therefore

$$\sum_{i=1}^s \epsilon_{ij} \epsilon_{ik} = 0, \text{ for } 1 \leq j, k \leq n.$$

Finally, if $h_k =_H h_j^{-1}$, then

$$\psi'(h_k) = \sum_{p=1}^n c_{kp} a_{pi} = \overline{\psi'(h_j)} = \overline{\sum_p c_{jp} a_{pi}} = \sum_p \bar{c}_{jp} a_{pi},$$

and hence $c_{kp} = \overline{c_{jp}}$ for all p . It follows that

$$\xi'(h_k) = \sum_p c_{kp} b_{pi} + \epsilon_{ik} = \overline{\xi'(h_j)} = \sum_p \overline{c_{jp} b_{pi}} + \overline{\epsilon_{ij}},$$

and hence $\epsilon_{ik} = \overline{\epsilon_{ij}}$. Therefore

$$\sum_{i=1}^s \epsilon_{ij} \overline{\epsilon_{ij}} = 0$$

for all j , $1 \leq j \leq n$, and hence $\epsilon_{ij} = 0$ for all i and j . This completes the proof of Theorem 14.11.

§14C. Exceptional Characters. Suzuki's CA-Group Theorem

In applications to the classification of finite non-abelian simple groups, the theory of special classes and exceptional characters (see (14.5) and (14.18)) has typically been used to investigate the structure of simple groups in some minimal situation. In these cases, the possibilities for a purely group-theoretic analysis are limited because of the relatively small number of subgroups to interact with one another. In this subsection, we shall prove a result of Suzuki [57] dealing with one of these minimal situations.

(14.13) Definition. A finite group G is called a *CA-group* (for “abelian centralizer”) if the centralizer of every element $x \in G - \{1\}$ is abelian.

(14.14) Theorem (Suzuki). *Every finite simple non-abelian CA-group has even order.*

The preceding theorem is of course a special case of the Feit-Thompson Theorem (Feit-Thompson [63]), which asserts that every non-abelian simple group has even order. Historically, Suzuki's Theorem 14.14 was followed by a theorem on the non-existence of simple *CN*-groups of odd order (Feit-Hall-Thompson [60]), where a *CN*-group is defined as in (14.13), with “abelian”

replaced by “nilpotent.” These theorems were a part of the chain of results leading to the Feit-Thompson Theorem. The *CA*-groups also are interesting from the standpoint of classifying the known simple groups. Brauer-Suzuki-Wall [58] proved that every non-abelian simple *CA*-group of even order is isomorphic to a fractional linear group $PSL_2(2^a)$ over a finite field of characteristic 2.

The proof of (14.14) begins with the following observation, whose proof is immediate from the definitions:

(14.15) *Every maximal abelian subgroup A of a *CA*-group G has the property:*

$$A = C_G(a) \quad \forall a \in A, a \neq 1.$$

An abelian subgroup A of a finite group G satisfying the condition of (14.15) is called a *special abelian subgroup*, or an *SA-subgroup*. Besides occurring in *CA*-groups, special abelian subgroups may be present in other finite groups which are not *CA*-groups; for example, a Sylow p -subgroup in $PSL_2(p)$ is a *CA*-subgroup, for p odd.

As preparation for the proof of (14.14), and for its intrinsic interest as well, we begin with a discussion of the character theory of a group which contains an *SA*-subgroup.

(14.16) **Definition.** A subset S of a finite group G is called a *T.I. set* (*trivial intersection set*) if

$$S \subseteq N_G(S) \quad \text{and} \quad S \cap S^x \subseteq \{1\} \quad \text{for all } x \in G - N_G(S).$$

(For example, it follows from §14A that a Frobenius complement H in a Frobenius group G is a T.I. set in G . It follows from (14.9) that the union of a set of special classes (see (14.5)) is always a T.I. set.)

(14.17) **Proposition.** *Let A be an *SA*-subgroup of a finite group G . Let*

$$H = N_G(A), A^* = A - \{1\},$$

and set

$$m = |A|, e = |H : A|, n = (m - 1)/e.$$

Then the following statements hold:

- (i) *The subset A^* is a T.I. set in G , whose normalizer H is a Frobenius group with Frobenius kernel A .*
- (ii) *The index $e = |H : A|$ divides $m - 1$, and A^* is the union of exactly n distinct conjugacy classes of H . These are a set of special classes in H (see Definition 14.5).*

(iii) As ξ ranges over the non-trivial linear characters of A , the induced characters ξ^H give irreducible characters of H of degree e , which vanish on $H-A$. There are precisely n distinct irreducible characters $\{\psi_1, \dots, \psi_n\}$ in this collection $\{\xi^H\}$.

(iv) Assume $n \geq 2$, and let

$$\lambda_i = \psi_i - \psi_n, \quad 1 \leq i \leq n-1,$$

so each λ_i is a virtual character of H . These $\{\lambda_i\}$, together with any one virtual character $1_A^H - \psi_i$, where $1 \leq i \leq n$, form a \mathbb{Z} -basis for the set of virtual characters of H vanishing off A^* . There exists a sign $\epsilon = \pm 1$, and distinct non-trivial irreducible characters of G :

$$\{\xi_1, \dots, \xi_n; \theta_1, \dots, \theta_f\},$$

satisfying the conditions:

$$\left\{ \begin{array}{l} (\psi_i - \psi_j)^G = \epsilon(\xi_i - \xi_j), \quad 1 \leq i, j \leq n, \\ \psi_i^G = \epsilon\xi_i + \Delta \text{ for some virtual character } \Delta, \quad 1 \leq i \leq n, \\ (1_A^H - \psi_i)^G = 1_G - \epsilon\xi_i + a \sum_{l=1}^n \xi_l + \sum_{j=1}^f c_j \theta_j, \quad 1 \leq i \leq n, \end{array} \right.$$

where the virtual character Δ and the integers a and $\{c_j\}$ are independent of i .

Proof. To establish (i), let $a \in A \cap A^x$, $a \neq 1$, for some element $x \in G$. Then $C_G(a)$ contains both A and A^x . From the assumption that A is an SA -subgroup of G , it follows that $A = A^x$ and $x \in H$. Therefore A^* is a T.I. set in G , with normalizer H .

We now prove that H is a Frobenius group with Frobenius kernel A , and begin by showing that $|A|$ is relatively prime to $|H : A|$. Let p be a prime dividing $|A|$, and let S be a Sylow p -subgroup of H . Then $S \cap A \neq 1$. Since the center $Z(S)$ of S centralizes each element of A , and A is an SA -group, it follows that $Z(S) \leq A$. But $Z(S) \neq 1$, and S centralizes each element of $Z(S)$, so $S \leq A$. It follows that $|A|$ and $|H : A|$ are relatively prime.

By the Schur-Zassenhaus Theorem 8.35, we have $H = A \times B$ for some subgroup B , and it now suffices to show that B is a Frobenius complement in H . Since $H = AB$, it is enough to prove that if $B \cap B^a \neq 1$ for some $a \in A$, then $a = 1$. Suppose that $b \in B \cap B^{a^{-1}}$, where $a \in A$, $a \neq 1$. Then $b = ab_1a^{-1}$ for some $b_1 \in B$, and hence $ab_1 = ba$. Then $b_1^{-1}ab_1 = b_1^{-1}ba$, so $b_1^{-1}b \in A \cap B = 1$. Thus $b = b_1$, and $b \in C_H(a) \cap B = A \cap B = 1$, by the SA -hypothesis, completing the proof of (i).

(ii) From the proof of (i), it follows that if two elements of A are conjugate in G , then they are conjugate in H . Since A^* is a union of conjugacy classes of H , it is clear from what has been shown above that these H -conjugacy classes (whose union is A^*) form a set of special classes in H , according to (14.5). (Note that (14.5iii) holds trivially, since if $h \in H$ and $\langle h \rangle = \langle a \rangle$ for some $a \in A^*$, then also $h \in A^*$, so h is contained in some special class.) Moreover, $C_G(a) = A$ for each $a \in A^*$, and it follows that each H -conjugacy class in A^* contains $e = |H : A|$ elements. Therefore e divides $m - 1$, and there are exactly $(m - 1)/e$ special classes in A^* .

(iii) The set of nontrivial linear characters of A can be written as a disjoint union of H -orbits. By (11.10) the number of such H -orbits is the same as the number of H -conjugacy classes in A^* , which is n . The characters of H induced from representatives of these orbits are irreducible by (14.4), and distinct by the Intertwining Number Theorem 10.24. This completes the proof of (iii).

(iv) The first statement is clear from the properties of the characters $\{\psi_i : 1 \leq i \leq n\}$ established in (iii). Since $n \geq 2$, there are $n - 1 > 0$ virtual characters of H ,

$$\psi_1 - \psi_n, \dots, \psi_{n-1} - \psi_n,$$

vanishing off A^* . By (14.9) we have[†]

$$\|(\psi_i - \psi_n)^G\|^2 = \|\psi_i - \psi_n\|^2 = 2, \quad 1 \leq i \leq n - 1.$$

Thus $(\psi_i - \psi_n)^G$ contains two distinct irreducible characters of G , each with multiplicity ± 1 . It also follows from (14.9) that

$$(\psi_i - \psi_n)^G(1) = (\psi_i - \psi_n)(1) = 0,$$

since the characters $\{\psi_i\}$ all have the same degree, by part (iii). Therefore the multiplicities of the characters of G appearing in $(\psi_i - \psi_n)^G$ have opposite signs. Since, by (14.9),

$$((\psi_i - \psi_n)^G, (\psi_j - \psi_n)^G) = (\psi_i - \psi_n, \psi_j - \psi_n) = 1$$

if $i < j < n$, it is easily checked that there exists a fixed sign $\epsilon = \pm 1$, and exactly n irreducible characters $\{\zeta_1, \dots, \zeta_n\}$ of G , such that

$$(\psi_i - \psi_j)^G = \epsilon(\zeta_i - \zeta_j), \quad 1 \leq i, j \leq n.$$

[†]As in (9.24ii), for each class function μ we denote (μ, μ) by $\|\mu\|^2$.

From these relations we obtain

$$\psi_i^G - \epsilon \zeta_i = \psi_j^G - \epsilon \zeta_j, \quad 1 \leq i, j \leq n.$$

Hence

$$\psi_i^G = \epsilon \zeta_i + \Delta,$$

where Δ is a virtual character independent of i . In particular, Δ contains the characters $\{\zeta_i\}$ with equal multiplicities. Moreover, by (14.9) we have

$$(1_A^G, \zeta_i - \zeta_j) = \epsilon (1_A^G, (\psi_i - \psi_j)^G) = \epsilon (1_A^H, \psi_i - \psi_j) = 0,$$

so the characters $\{\zeta_i\}$ also appear with equal multiplicities in 1_A^G . Combining our results, we obtain the last statement of (iv), and the proof is completed.

From now on, we assume that $n \geq 2$, as in (iv) of the preceding result.

(14.18) Definition. The characters $\{\zeta_1, \dots, \zeta_n\}$ appearing in (14.17iv) are called the *exceptional characters* associated with the *SA*-subgroup A . The remaining non-trivial irreducible characters of G are called *non-exceptional characters* relative to A .

The next result contains detailed information about the values of the exceptional and non-exceptional characters; this information will be used in the proof of Suzuki's Theorem 14.14. Even more precise information will be obtained later, in §20B, as an application of modular representation theory.

(14.19) Proposition. Let $\{\zeta_1, \dots, \zeta_n; \theta_1, \dots, \theta_f\}$, $n \geq 2$, be the exceptional and non-exceptional characters associated with the subgroup A , as in (14.17). Then the following statements hold:

(i) $\zeta_i(x) = \zeta_j(x)$, $1 \leq i, j \leq n$, for each $x \in G$ not conjugate to an element of A^* . In particular, the exceptional characters all have the same degree.

(ii) If B is another *SA*-subgroup of G , not conjugate to A , then $\{\zeta_1, \dots, \zeta_n\}$ are non-exceptional characters relative to B .

(iii) The multiplicities a and $\{c_j\}_{1 \leq j \leq f}$ in the expression

$$(1_A - \psi_i)^G = 1_G - \epsilon \zeta_i + a \sum_{l=1}^n \zeta_l + \sum_{j=1}^f c_j \theta_j$$

satisfy the condition:

$$e = a^2(n-1) + (a-\epsilon)^2 + \sum_{j=1}^f c_j^2.$$

(iv) Each non-exceptional character θ_j , $1 \leq j \leq f$, takes constant rational integral values on the special classes in A^* . More precisely,

$$\theta_j(x) = c_j, \forall x \in A^*,$$

where c_j is the multiplicity of θ_j in $(1_A - \psi_i)^G$. The multiplicity c_j is characterized by the condition

$$c_j \equiv \theta_j(1) \pmod{m}, |c_j| \leq \frac{1}{2}(m-1).$$

In particular, θ_j vanishes on A^* if and only if m divides $\theta_j(1)$.

(v) If θ_j and $\theta_{j'}$ are non-exceptional characters with the same degree, then they appear with equal multiplicities in $(1_A - \psi_i)^G$ for each i , $1 \leq i \leq n$.

(vi) We have $\sum_{x \in A^*} |\zeta_i(x)|^2 \geq e(m-e)$.

Proof. (i) By (14.17iv), we have

$$\zeta_i - \zeta_j = \epsilon(\psi_i - \psi_j)^G, 1 \leq i, j \leq n.$$

By the definition of the characters $\{\psi_i\}$, it follows that $\zeta_i - \zeta_j$ vanishes on all $x \in G$ not conjugate to some element of A^* .

(ii) If B is a special abelian group not conjugate to A , then $B \cap A = 1$. Therefore by (i), $\zeta_i - \zeta_j$ vanishes on B^* for $1 \leq i, j \leq n$. Hence if one character ζ_i is exceptional relative to B , all characters $\{\zeta_j\}_{1 \leq j \leq n}$ have this property, by (14.17iv). By (i), this implies that $\zeta_i = \zeta_j$ for all i and j , contrary to the assumption $n \geq 2$.

(iii) By (14.17iv), $1_A^H - \psi_i$ vanishes off the special classes, so by (14.9) we have

$$\|(1_A - \psi_i)^G\|_G = \|1_A^H - \psi_i\|_H, 1 \leq i \leq n.$$

Moreover, 1_A^H is the regular character of H/A , and does not contain ψ_i . Therefore

$$\|(1_A - \psi_i)^G\|^2 = 1 + |H:A| = 1 + e.$$

Using the expression of $(1_A - \psi_i)^G$ in terms of the exceptional and non-exceptional characters, we obtain

$$\|(1_A - \psi_i)^G\|^2 = 1 + (a - e)^2 + a^2(n-1) + \sum_{j=1}^f c_j^2.$$

Assertion (iii) follows at once from comparing these two formulas for $\|(1_A - \psi_i)^G\|^2$.

(iv) and (v) Let ξ be a linear character of A . Then ξ^G coincides with ψ_i^G for some i . If θ is a non-exceptional character of G relative to A , then θ is contained in all $\{\psi_i^G\}$ with the same multiplicity, say α . If the multiplicity of θ in 1_A^G is β , then $(1_A - \psi_i)^G$ contains θ with multiplicity $\beta - \alpha$. By Frobenius Reciprocity, we also have

$$\theta|_A = \beta 1_A + \alpha(\sum \xi),$$

where the sum is taken over the nontrivial linear characters ξ of the abelian group A . Comparing degrees, we obtain

$$\theta(1) = \beta + \alpha(m-1) \equiv (\beta - \alpha) \pmod{m}.$$

Moreover, the Second Orthogonality Relation gives

$$(1_A + \sum \xi)(x) = 0, \forall x \in A^*.$$

We conclude that

$$\theta(x) = \beta - \alpha \in \mathbb{Z}, \forall x \in A^*.$$

Finally,

$$|c_j| \leq |c_j|^2 \leq e \leq (m-1)/2, 1 \leq j \leq f,$$

since $n \geq 2$. This completes the proof of (iv) and (v).

(vi) We first apply an argument, similar to the preceding one, to the exceptional characters $\{\zeta_i\}$. If ζ_i is exceptional, then for $j \neq i$, it follows from (14.15iv) that ζ_i appears with constant multiplicity, say α , in ψ_j^G . Again using (14.17iv), we have $(\zeta_i, \psi_i^G) = \alpha + \epsilon$. Letting $\beta = (\zeta_i, 1_A^G)$, it follows easily that

$$\zeta_i|_A = \beta 1_A + \alpha \sum \xi + \epsilon \sum \xi',$$

where the first sum is taken over all linear characters ξ of A , and the second over the linear characters ξ' appearing in $\psi_i|_A$. By the Second Orthogonality Relation, $(1_A + \sum \xi)(x) = 0$ for all $x \in A^*$, and it follows that

$$\zeta_i(x) = \beta - \alpha + \epsilon \psi_i(x), \forall x \in A^*, 1 \leq i \leq n.$$

Thus $\zeta_i(x) = \epsilon \psi_i(x) + z$, for some integer z , and all $x \in A^*$. We then have

$$\begin{aligned} \sum_{x \in A^*} |\zeta_i(x)|^2 &= \sum_{x \in A^*} (\epsilon \psi_i(x) + z)(\epsilon \psi_i(x^{-1}) + z) \\ &= \sum_{x \in A^*} |\psi_i(x)|^2 + \epsilon z \sum_{x \in A^*} (\psi_i(x) + \psi_i(x^{-1})) + (m-1)z^2 \\ &= me - e^2 - 2\epsilon e z + z^2(m-1). \end{aligned}$$

(We have used the fact that $\sum_{x \in A^*} \psi_i(x) = -\psi_i(1) = -e$, because the restriction of ψ_i to A is a sum of nontrivial linear characters of A .) It follows that

$$\sum_{x \in A^*} |\xi_i(x)|^2 \geq e(m-e),$$

since $m-1=en$, and $z^2n-2ez \geq 0$ for $n \geq 2$ and any integer z . This completes the proof of the proposition.

Remark. The proofs of parts (iv)–(vi) are especially interesting, in that they use information about multiplicities to derive character values.

Proof of Suzuki's CA-group Theorem 14.14. We assume that G is a non-abelian simple CA-group. Then each maximal abelian subgroup of G is a special abelian subgroup, as we have remarked earlier. We have already used the fact that if A and B are two SA-subgroups such that $A \cap B \neq 1$, then both A and B are contained in the centralizer of any non-identity element of their intersection, and hence coincide. Thus each non-identity element of G lies in exactly one maximal abelian subgroup of G . These maximal abelian subgroups, in turn, may be partitioned into classes of conjugate SA-subgroups, with representatives $\{A_1, \dots, A_t\}$. We set $H_i = N_G(A_i)$, and let

$$|A_i| = m_i, |H_i : A_i| = e_i, 1 \leq i \leq t.$$

Then $n_i = (m_i - 1)/e_i$ is an integer, for each i .

We wish to show that $|G|$ is even, so suppose instead that $|G|$ is odd. From this assumption, it follows that each n_i is even, since $n_i e_i = m_i - 1$ is even and e_i is odd. Thus $n_i \geq 2$ for each i , and the results of the preceding two propositions can be applied to each of the subgroups $\{A_1, \dots, A_t\}$.

By (14.17), there exist exactly n_i exceptional characters associated with each subgroup A_i , and by (14.19ii), exceptional characters for A_i are non-exceptional for A_j , if $i \neq j$. Hence we have $\sum_{i=1}^t n_i$ distinct nontrivial irreducible characters of G which are exceptional for the various subgroups $\{A_i\}$. On the other hand, the sets $\{A_j\}$ form a partition of the conjugacy classes of G ; since each set A_j^* is a disjoint union of n_j special classes, it follows that G has $1 + \sum_{i=1}^t n_i$ distinct conjugacy classes. By (3.37), it follows that every nontrivial irreducible character of G is exceptional for some subgroup A_i , $1 \leq i \leq t$.

Now let us choose the notation so that m_i is the smallest integer among the $\{m_i\}$, and set

$$m_t = m, e_t = e, n_t = n.$$

We may assume also, by (14.19i) and (14.19iv), that the common degree d of the exceptional characters for A_i satisfies

$$m_i | d, 1 \leq i \leq u, m_i \nmid d, u+1 \leq i \leq t.$$

Finally let $\Gamma_i = (1_A - \psi_i)^G$, where the $\{\psi_i\}$ are characters of H_t of degree e , as in (14.17iii); then we may write

$$\Gamma_i = 1 - e\xi_i + a \sum_{k=1}^n \xi_k + \sum_j c_j \theta_j, \quad 1 \leq i \leq n.$$

Now the non-exceptional characters $\{\theta_j\}$ for A_t fall into sets of exceptional characters $\{\xi_j^h\}_{1 \leq j \leq n_h}$ for the other subgroups A_h ; the characters in each such set have the same degree by (14.19i) and hence appear in Γ_i with the same multiplicity by (14.19iv). We may therefore rewrite each Γ_i in the form

$$\Gamma_i = 1 - e\xi_i + a \sum_{k=1}^n \xi_k + \sum_{h=1}^{t-1} c_h \left(\sum_{j=1}^{n_h} \xi_j^h \right).$$

Moreover, by (14.17iv), each Γ_i will vanish on the set $A_1^* \cup \dots \cup A_{t-1}^*$.

Suppose now that for some $h_0 \leq u$, the multiplicity c_{h_0} equals zero. Then by (14.19iv), for all $x \in A_{h_0}^*$ we have

$$\xi_k(x) = 0, \quad 1 \leq k \leq n; \quad \xi_j^h(x) = y_h \in \mathbb{Z} \quad \text{for } 1 \leq j \leq n_h, \text{ for all } h \neq h_0.$$

The equation $\Gamma_i(x) = 0$ for $x \in A_{h_0}^*$ then implies that

$$0 = 1 + \sum_{h \neq h_0} c_h n_h y_h,$$

which is impossible since $\{c_h\}$, $\{n_h\}$ and $\{y_h\}$ are integers, and the $\{n_h\}$ are all even. Hence $c_h \neq 0$ for $1 \leq h \leq u$. On the other hand, by (14.19iii) we have

$$e = a^2(n-1) + (a-e)^2 + \sum_h c_h^2 n_h \geq 1 + \sum_{h=1}^u c_h^2 n_h.$$

Hence we have proved

$$(14.20) \quad e - 1 \geq \sum_{h=1}^u c_h^2 n_h, \quad \text{where each } c_h \neq 0.$$

We next obtain an inequality for the order g of G . Setting $\xi = \xi_k$ for some k , $1 \leq k \leq n$, we have

$$g = \sum_{x \in G} |\xi(x)|^2 = d^2 + \sum_{i=1}^t (g/m_i e_i) \sum_{x \in A_i^*} |\xi(x)|^2,$$

since there are $|G : H_i| = g/m_i e_i$ distinct conjugates of each subgroup A_i , $1 \leq i \leq t$. For each i with $u < i < t$, $\xi(x)$ is a nonzero rational integer for all

$x \in A_i^*$, by (14.19iv). Hence

$$\sum_{x \in A_i^*} |\zeta(x)|^2 \geq m_i - 1, \quad i = u+1, \dots, t-1.$$

In case $i = t$, we have by (14.19vi):

$$\sum_{x \in A_t^*} |\zeta(x)|^2 \geq e(m-e).$$

Combining these results, we obtain

$$(14.21) \quad g \geq d^2 + \left\{ \sum_{i=u+1}^{t-1} \frac{g}{m_i e_i} (m_i - 1) \right\} + \frac{g}{m} (m-e).$$

On the other hand, every element of G is conjugate to some element of $A_1 \cup \dots \cup A_t$, so

$$g = 1 + \sum_{i=1}^t \frac{g}{m_i e_i} (m_i - 1).$$

This formula and (14.21) imply

$$1 + \left\{ \sum_{i=1}^u \frac{g}{m_i e_i} (m_i - 1) \right\} + \frac{g}{m e} (m-1) \geq d^2 + \frac{g}{m} (m-e).$$

Since

$$\frac{1}{me} (m-1) - \frac{1}{m} (m-e) = \frac{m-1+e^2}{me} - 1,$$

the above formula simplifies to

$$(*) \quad \left\{ \sum_{i=1}^u \frac{m_i - 1}{m_i e_i} \right\} + \frac{m-1+e^2}{me} \geq 1 + \frac{d^2 - 1}{g}.$$

Now $(m_i - 1)/e_i = n_i$, and $m_i \geq m$ for $1 \leq i \leq t$, so we obtain

$$\left(\sum_{i=1}^u m_i \right) / m \geq \sum_{i=1}^u \frac{m_i - 1}{m_i e_i}.$$

By (14.20), we have $e-1 \geq \sum_{i=1}^u n_i$, so the inequality (*) implies

$$\frac{e-1}{m} + \frac{m-1+e^2}{me} \geq 1 + \frac{d^2 - 1}{g}.$$

Since we have assumed that d is the degree of a nontrivial irreducible character of a non-abelian simple group, we have $d > 1$. Therefore we obtain a strict inequality

$$\frac{e-1}{m} + \frac{m-1+e^2}{me} > 1.$$

From this we deduce, since $m-1 = ne$,

$$e-1+n+e > ne+1, \text{ so } 2(e-1)+n(1-e) > 0,$$

and therefore

$$(e-1)(2-n) > 0.$$

The last inequality is impossible because $e \geq 1$ and $n \geq 2$, and the proof of the theorem is completed!

§14D. Characters of A_5 . Examples of Exceptional Characters

Let G be the alternating group A_5 . Using the Sylow theorems, it can be shown that G is the unique simple non-abelian group of order 60. From this result, or by a direct argument based on Sylow's theorems, it can also be verified that

$$G \cong SL_2(4) \cong PSL_2(5).$$

As an illustration of the methods of the preceding section, we shall determine the characters of G in the field K of complex numbers, leaving a number of details to be checked by the reader. The group G is also an example of a simple CA -group.

There are 5 conjugacy classes in G , which we label by the orders of their elements:

$$1, 2, 3, 5_1, 5_2.$$

The orders of the corresponding centralizers are

$$60, 4, 3, 5, 5.$$

Let A be a Sylow 5-subgroup of G . Then A is a cyclic SA -subgroup generated by a 5-cycle, and $N_G(A) = H$ is easily shown to be dihedral of order 10. We apply (14.17) to find the exceptional characters associated with the subgroup A . In this case we have, following the notation of §14C,

$$m = |A| = 5, e = |H : A| = 2, n = (m-1)/e = 2.$$

Thus there are two exceptional characters having the same degree, by (14.19i).

The dihedral group $H=N_G(A)$ has exactly two non-linear irreducible characters ψ_1, ψ_2 of degree 2; these are induced characters

$$\psi_1 = \lambda_1^H, \quad \psi_2 = \lambda_2^H,$$

where λ_1, λ_2 are non-trivial linear characters of A (see (10.11)). For $i=1, 2$, the values of ψ_i are given in (10.11), using the fact that $\psi_i|_A = \lambda_i + \bar{\lambda}_i$. Part of the character table of H involving ψ_1 and ψ_2 is as follows:

	5_1	5_2
ψ_1	α	β
ψ_2	β	α

where

$$\alpha = \epsilon + \bar{\epsilon}, \quad \beta = \epsilon^2 + \bar{\epsilon}^2,$$

and ϵ is a primitive 5-th root of 1.

By (14.17iv) we have

$$(\psi_1 - \psi_2)^G = \xi_1 - \xi_2,$$

where ξ_1 and ξ_2 are the exceptional characters associated with the subgroup A ; in this case, the sign ϵ in (14.17) can be chosen equal to 1.

We shall apply Theorem 14.11 to determine the values of ξ_1, ξ_2 on the special classes 5_1 and 5_2 . Changing the notation of §14B, we have

$$\text{Irr } H = \{\psi_0 (= 1_H), \psi_1, \psi_2, \psi_3\},$$

where ψ_3 is the nontrivial linear character. Also

$$\text{Irr } G = \{\xi_0 (= 1_G), \xi_1, \xi_2, \xi_3, \xi_4\},$$

where ξ_3 and ξ_4 are the nontrivial non-exceptional characters of G . For a basis of $W(\mathfrak{S})$ as in (14.6), we may choose

$$\lambda_1 = \psi_1 - \psi_2, \quad \lambda_2 = 1_A^H - \psi_1 = 1_H + \psi_3 - \psi_1.$$

Then by (14.17iv),

$$\lambda_1^G = \xi_1 - \xi_2, \quad \lambda_2^G = 1_G - \xi_1 + a(\xi_1 + \xi_2) + c_3\xi_3 + c_4\xi_4.$$

The relation (14.19iii) gives

$$e = a^2(n-1) + (a-\epsilon)^2 + \sum c_j^2.$$

Since $\epsilon = \pm 1$, this yields as possibilities

$$a=0, \{c_3, c_4\} = \{\pm 1, 0\}, \text{ or else } a=1, \{c_3, c_4\} = \{\pm 1, 0\}.$$

In the first case, it follows immediately from Theorem 14.11 that the exceptional characters ξ_1 and ξ_2 take the same values as ψ_1 and ψ_2 on the special classes. In the second case, we interchange ξ_1 and ξ_2 , making $\epsilon = -1$, and again obtain $a=0$; thus in this case the values of ξ_1 and ξ_2 differ in sign from those of ψ_1 and ψ_2 . This ambiguity will be removed later. Let B denote a Sylow 2-subgroup of G , of order 4.

The permutation representations of G on the cosets $G/N_G(B)$ and $G/N_G(A)$ are both doubly transitive, of degrees 5 and 6, respectively. If θ_3 and θ_4 are the permutation characters, then by Exercise 10.3, $\xi_3 = \theta_3 - 1$ and $\xi_4 = \theta_4 - 1$ are irreducible, of degrees 4 and 5, respectively. Since the sum of the squares of the degrees of all irreducible representations is 60, it follows that ξ_3 and ξ_4 are the non-exceptional characters, and the exceptional characters ξ_1 and ξ_2 both have degree 3. The values of ξ_3 and ξ_4 are easily found from the values of θ_3 and θ_4 . Note that the multiplicity of ξ_4 in λ_2^G is zero by (14.19iv), since $\xi_4(1) = 5 = m$. We then obtain for the character table of G :

	1	2	3	ξ_1	ξ_2
ξ_0	1	1	1	1	1
ξ_1	3	x	y	$\pm\alpha$	$\pm\beta$
ξ_2	3	x	y	$\pm\beta$	$\pm\alpha$
ξ_3	4	0	1	-1	-1
ξ_4	5	1	-1	0	0

By the Second Orthogonality Relation, we obtain $x = -1$, $y = 0$. It then follows from the second orthogonality relation that α and β appear with the sign +1 in all occurrences, since $\{\alpha, \beta\} = \left\{ \frac{1}{2}(1 \pm \sqrt{5}) \right\}$.

There are several noteworthy features of this example, for which we should be alert in more general situations. The first is the remarkable fact that the part of the table involving the irrational entries $\{\alpha, \beta\}$ is simply lifted from the character table of a much easier group $H = D_5$, using the theory of exceptional characters. The non-exceptional characters are formed in this case from doubly transitive permutation representations. Later, in §20C, we shall indicate how to get more information about non-exceptional characters by using the theory of modular representations.

It is also possible to find the characters of A_5 from the method of §9F, by calculating the structure constants c_{ijk} for the center of the group algebra (see Frobenius [96] or McKay [79]). One may also use the method of induced characters (see Isaacs [76; p. 84]).

§14E. The Brauer-Suzuki Theorem on Generalized Quaternion Sylow 2-Groups

In this subsection, we shall apply the theory of special classes to another important minimal situation in the classification of finite simple groups. This time, we shall focus on the possible structures for a Sylow 2-subgroup of a finite simple group. In §13C we proved, using Burnside's Transfer Theorem, that a Sylow 2-subgroup of a non-abelian simple group cannot be cyclic of order greater than 1. The Brauer-Suzuki theorem, proved in this subsection, shows that there cannot be a simple finite group whose Sylow 2-subgroup is generalized quaternion of order ≥ 16 . Using the theory of blocks, Brauer-Suzuki [59] also showed that the quaternion group of order 8 cannot appear as the Sylow 2-subgroup of a simple group. Another proof of this result, independent of block theory, and based instead on a delicate refinement of the discussion to follow, was found by Glauberman [74].

On the other hand, dihedral groups may appear as Sylow 2-subgroups of simple groups, and the classification of such simple groups was historically an important step towards the determinations of all simple groups whose structure is minimal in some sense. In this connection, Gorenstein-Walter [65] proved that a simple group with dihedral Sylow 2-subgroup must be either A_7 or $\mathrm{PSL}_2(q)$, q odd.

We recall from §1B that a generalized quaternion 2-group S has a presentation

$$S = \langle x, y : x^{2^n} = 1, y^2 = x^{2^{n-1}}, x^y = x^{-1} \rangle.$$

We shall assume $|S| \geq 16$, so $n \geq 3$. It is easily shown that such a group S has a unique involution (=element of order 2), namely y^2 ($=x^{2^{n-1}}$).

(14.23) Theorem. *Let G be a finite group whose Sylow 2-subgroups are generalized quaternion of order ≥ 16 . Then $G/O(G)$ contains a nontrivial cyclic normal 2-subgroup (where $O(G)$ denotes the unique maximal normal subgroup of G of odd order).*

The theorem is due to Brauer-Suzuki [59]. Our proof follows closely the presentation by Gorenstein ([68], Chapter 12).

Proof. Let S be a Sylow 2-subgroup of G , with generators and relations as above. We set

$$X = \langle x \rangle, T = \langle x^2 \rangle, R = \langle x^4 \rangle, C = C_G(T), N = N_G(T).$$

Step 1. We claim that there exists a subgroup $H \trianglelefteq N$ such that

$$N = H \rtimes S, |H| \text{ is odd, and } C = H \rtimes X.$$

To prove this, we note first that T is the derived group S' of S , so S normalizes T and is contained in N . Also, since $n \geq 3$, S does not centralize T , so $S \cap C = X$. Since $C \trianglelefteq N$, X is a Sylow 2-subgroup of C , and is cyclic, so C has a normal 2-complement H , by Corollary 13.22. Then $H = O(C)$, the largest normal subgroup of C of odd order, and H is characteristic in C . Since $C \trianglelefteq N$, we have $H \trianglelefteq N$. By the proof of (13.22), the automorphism group of the cyclic 2-group T is a 2-group, so each element of odd order in N acts trivially on T . Hence the elements in N of odd order lie in C , and thus clearly belong to H . Therefore N/H is a 2-group, and we have $N = H \rtimes S$, $C = H \rtimes X$, proving the claim made above.

Step 2. Let $A = C - RH$. We assert that A is a T.I. set in G (see (14.16)) with normalizer N , and hence defines a set of special classes in N , by the proof of (14.17ii). We first note that since $C = XH$ by Step 1, we have

$$\langle a^2 \rangle H = TH \text{ or } \langle a \rangle H = TH$$

for each $a \in A$. Moreover, $TH \cong T \times H$ by Step 1, so for each $a \in A$, $T = \langle a^m \rangle$ for some integer m . Therefore if $a \in A \cap A^z$ for some $z \in G$, we have $\langle a^m \rangle = T = T^z$, so $z \in N$. On the other hand, N normalizes both $C = XH$ and RH , since R is a characteristic subgroup of the cyclic group X . Then N normalizes A . Finally, if $\langle a' \rangle = \langle a \rangle$ for some $a' \in C$ and $a \in A$, then clearly $a' \in A$, completing the proof that A is a T.I. set with normalizer N , and that A defines a set of special classes in N .

Step 3. There exists a linear character λ of C such that $\ker \lambda = RH$, $\lambda^N \in \text{Irr } N$, and $\lambda^N(1) = 2$. Set $\theta = 1_C|_N - \lambda^N$. Then the following statements hold:

- (i) $(\theta, \theta)_N = 3$;
- (ii) $\theta(1) = 0$, and θ vanishes on $N - A$.

Since $C/RH \cong X/R$ is cyclic of order 4, there does exist a linear character λ of C whose kernel is RH . For any such λ , $\gamma\lambda \neq \lambda$ for all γ such that $N = \langle C, \gamma \rangle$, by Step 1. By (10.25), λ^N is irreducible, of degree two. Now $1_C|_N$ is the character of the regular representation of N/C , by Exercise 10.8. Since $|N/C| = 2$, $1_C|_N = 1_N + \mu$ where μ is a non-trivial linear character of N with kernel C . Then clearly 1_N , μ and λ^N are the three distinct irreducible characters appearing with nonzero multiplicity in θ , and we have $(\theta, \theta) = 3$ by the orthogonality relations, proving (i). It is also clear that $\theta(1) = 0$ and that θ vanishes on $N - A$, by the definition of induced characters.

Step 4. Let $\theta = 1_C|_N - \lambda^N$, as in Step 3. We claim there exist distinct nontrivial irreducible characters ξ_1 and ξ_2 of G such that

$$\theta^G = 1_G + \xi_1 - \xi_2, \text{ and } \xi_2(1) = \xi_1(1) + 1.$$

By Steps 2 and 3 and (14.9), we have

$$(\theta^G, \theta^G) = (\theta, \theta)_N = 3.$$

Moreover, $(1_G, \theta^G) = (1_N, \theta) = 1$ by Frobenius Reciprocity. Then

$$\theta^G = 1_G \pm \xi_1 \pm \xi_2$$

for some nontrivial irreducible characters ξ_1 and ξ_2 . Since $\theta^G(1) = 0$, we may assume the signs chosen so that $\theta^G = 1_G + \xi_1 - \xi_2$; then

$$0 = \theta^G(1) = 1 + \xi_1(1) - \xi_2(1),$$

as required.

Step 5. If u is an involution or an element of odd order in G , then $\theta^G(u) = 0$ and $\xi_2(u) = 1 + \xi_1(u)$. These assertions hold because, by Step 2, A contains no involutions or elements of odd order. Thus u is conjugate to no element of A , so $\theta(u) = 0$ by Step 3, part (ii). By (14.9), $\theta^G(u) = \theta(u) = 0$, hence $\xi_2(u) = 1 + \xi_1(u)$ by Step 4.

Step 6. We assert that G contains a single conjugacy class of involutions, with a representative which we denote by u . [This is clear by Sylow's Theorem, since every involution must be conjugate to the unique involution in S .] Next, if c_{uuw} is the number of ordered pairs of involutions whose product is w , for $w \in G$, we claim that $c_{uuw} = 0$ if w has even order. For suppose that u and v are involutions such that $uv = w$, with w of even order $2s$. By an easy computation, both u and v invert w , so $\langle u, v \rangle$ is a dihedral group of order $4s$. Then w^s is a central involution in $\langle u, v \rangle$, and $\langle u, w^s \rangle \cong \mathbb{Z}_2 \times \mathbb{Z}_2$. This contradicts Sylow's theorem, since S has no subgroup isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$, and the assertion on c_{uuw} is now proved.

Step 7. By (9.28), the integer c_{uuw} in Step 6 is a structure constant of the center of the group algebra of G . We have, by (9.33),

$$c_{uuw^{-1}} = |G| |C_G(u)|^{-2} \sum_{m=1}^s z_m^{-1} (\xi^m(u))^2 \xi^m(w),$$

where $\text{Irr } G = \{\xi^1, \dots, \xi^s\}$ and $z_m = \xi^m(1)$, $1 \leq m \leq s$. Keeping the involution u fixed, we set $\gamma(w) = c_{uuw^{-1}}$, for $w \in G$; then γ is an integer-valued class function on G , which vanishes on elements of even order by Step 6.

Step 8. We now show that for each involution $u \in G$,

$$1 + \frac{\xi_1(u)^2}{\xi_1(1)} - \frac{\xi_2(u)^2}{\xi_2(1)} = 0,$$

where ξ_1 and ξ_2 are defined as in Step 4. To prove this, let γ be the class function defined in Step 7; then $(\gamma, \theta^G) = 0$, since γ vanishes on elements of even order, and θ^G vanishes on elements of odd order by Step 5. Since $\theta^G = 1_G + \xi_1 - \xi_2$ by Step 4, and

$$\gamma = |G| |C_G(u)|^{-2} \sum_{m=1}^s z_m^{-1} (\xi^m(u))^2 \xi^m$$

by Step 7, the Orthogonality Relations imply

$$1 + \frac{\xi_1(u)^2}{\xi_1(1)} (\xi_1, \xi_1) - \frac{\xi_2(u)^2}{\xi_2(1)} (\xi_2, \xi_2) = 0,$$

as required.

Step 9. We show next that the kernel of ξ_2 contains every involution of G , and is consequently a normal subgroup of G of even order. By Steps 4, 5 and 8, we have

$$1 + \frac{(\xi_2(u)-1)^2}{\xi_2(1)-1} - \frac{\xi_2(u)^2}{\xi_2(1)} = 0.$$

This readily implies that

$$(\xi_2(u)-\xi_2(1))^2 = 0.$$

Then $u \in \ker \xi_2$ by (9.27), which proves the assertion above, since by Step 6, there is only one class of involutions in G .

Step 10. We are now in position to complete the proof. Let U be the subgroup of G generated by the involutions. Then $U \trianglelefteq G$, and the subgroup $V = S \cap U$ is a Sylow 2-subgroup of U . We prove that V is cyclic. Suppose this is not the case; then V is also generalized quaternion, and contains yx^i for some i . Since $V \trianglelefteq S$, V contains also

$$(yx^i)^x = x^{-1}yx^{i+1} = yx^{i+2},$$

using the fact that $x^{-1}y = yx$ by the defining relations for S . Thus V contains x^2 , and so S/V is abelian. We now set $G_1 = SU$. Applying Steps 1–9 to G_1 , we conclude that G_1 has a non-linear irreducible character ζ whose kernel contains U . Then $G_1/\ker \zeta$ is a homomorphic image of

$$G_1/U \cong SU/U \cong S/U \cap S = S/V,$$

which is abelian. This is contrary to the existence of a non-linear irreducible character of $G_1/\ker \zeta$. Therefore V must be cyclic, as we wished to prove.

Finally, since U has a cyclic Sylow 2-subgroup of order greater than 1, U has a normal 2-complement L by Corollary 13.22. Then L is a characteristic subgroup of U , and since $U \trianglelefteq G$, we have $L \trianglelefteq G$, and so $L \trianglelefteq O(G)$. Then $U/L \trianglelefteq G/L$, and U/L is a cyclic 2-group. Hence $G/O(G)$ contains a nontrivial cyclic normal 2-subgroup, completing the proof.

Remarks. (i) If G has a generalized quaternion Sylow 2-subgroup S as above, then it follows from the preceding theorem that $G/O(G)$ has a central subgroup of order 2. The inverse image Z of this subgroup is a normal subgroup of G whose order is twice an odd number. It follows that a Sylow 2-subgroup of G/Z is isomorphic to $SZ/Z \cong S/Z \cap S$, which is a dihedral group. From the Gorenstein-Walter [65] classification of groups with dihedral Sylow 2-subgroups, it can be proved that $G/O(G)$ is either a 2-group, or an extension of A_7 by a group of order 2, or else contains a normal subgroup isomorphic to $\mathrm{PSL}_2(q)$, for q odd.

(ii) The following result can be viewed as a far-reaching extension of the Brauer-Suzuki Theorem.

Glauberman's Z^* -Theorem. *Let G be a finite group with Sylow 2-subgroup S , and let u be an involution in S . Suppose the only conjugate of u lying in S is u itself. Then*

$$uO(G) \in \text{center of } (G/O(G)).$$

Indeed a generalized quaternion group contains a unique involution; we see thus that the Brauer-Suzuki Theorem is a special case of Glauberman's Theorem. The Z^* -theorem can be proved using the theory of blocks (see Chapter 9).

§14F. Centralizers of Involutions and Special Classes

Our final application of special classes (in §14) is to the problem of determining the structure of a finite group G containing an involution u whose centralizer $C_G(u)$ in G has some known structure.

This problem arises in the following way. Consider a known finite simple group G_0 , and let $u_0 \in G_0$ be an involution whose centralizer $H_0 = C_{G_0}(u_0)$ can be determined from our knowledge of the structure of G_0 . We then consider an arbitrary finite simple group G containing an involution u such that $H = C_G(u)$ is isomorphic to H_0 , and ask whether G is isomorphic to G_0 , and if not, what other possibilities are there for G ? This method is of basic importance for the general classification theory of simple groups, because it yields workable characterizations of most of the known simple groups, and has led (in exactly the way indicated above) to the discovery of several of the sporadic simple groups. The underlying principle is a result of Brauer (see

Brauer-Fowler [55]), which asserts that there exist at most finitely many non-isomorphic simple groups containing an involution whose centralizer has a given structure.

Our presentation follows G. Higman [68], whose choice of an example and explanation of the method seem particularly illuminating.

We begin with the consideration of the finite simple group $G_0 = SL_3(3)$, of order 5616. The group G_0 is a finite group of Lie type, of rank 2 as a BN -pair. The structure of such groups will be considered in greater detail in Chapter 7. It is easily checked that the centralizer in G_0 of the involution

$$\begin{bmatrix} -1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

is isomorphic to the group $GL_2(3)$ of order 48.

(14.24) Theorem. *Let G be a finite simple group containing an involution t whose centralizer is isomorphic to $GL_2(3)$. Then the order of G is 5616 or 7920.*

We remark that the second possibility in (14.24) also corresponds to a finite simple group, the Mathieu group M_{11} . This provides an illustration of how multiple solutions of the classification problems, in terms of centralizers of involutions, may yield sporadic simple groups.

We shall present a sketch of the proof of the above theorem, concentrating on how the theory of special classes is used, and omitting a number of details.

We first require the character table of $H = GL_2(3)$. It is given below with $\text{Irr}(H) = \{\varphi^1, \dots, \varphi^8\}$. The conjugacy classes $\{\mathfrak{C}_1, \dots, \mathfrak{C}_8\}$ of H are represented by matrices in $GL_2(3)$, which may be chosen as follows:

$$1_H = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad t = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \quad u = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad u' = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix},$$

$$v = \begin{pmatrix} -1 & 0 \\ -1 & -1 \end{pmatrix}, \quad v' = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad w_1 = \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix}, \quad w_2 = \begin{pmatrix} -1 & 1 \\ -1 & -1 \end{pmatrix}.$$

Note that t is the unique central involution in H . It will be seen later that the representatives

$$\{t, u, v, w_1, w_2\}$$

correspond to special classes in H , where we view H as the centralizer (in G) of some involution in an unknown simple group G . In addition to the character table of H given below, we also need the orders of the centralizers in H of the 8 conjugacy class representatives listed above. These orders are (respectively):

$$48, 48, 8, 6, 6, 4, 8, 8.$$

The character table of H is as follows:

	1_H	t	u	u'	v	v'	w_1	w_2
φ^1	1	1	1	1	1	1	1	1
φ^2	1	1	1	1	1	-1	-1	-1
φ^3	2	2	2	-1	-1	0	0	0
φ^4	3	3	-1	0	0	1	-1	-1
φ^5	3	3	-1	0	0	-1	1	1
φ^6	2	-2	0	-1	1	0	$\sqrt{2} i$	$-\sqrt{2} i$
φ^7	2	-2	0	-1	1	0	$-\sqrt{2} i$	$\sqrt{2} i$
φ^8	4	-4	0	1	-1	0	0	0

We now view H as a subgroup of G , and identify H with the centralizer of the involution t . We first note that the elements $\{t, u, v, w_1, w_2\}$ are indeed representatives of a set of special classes in H . These are representatives of all classes in H containing elements h such that $t \in \langle h \rangle$. With this observation, it is easy to check that the axioms (14.5) are satisfied. For example, let h_1 and h_2 be representatives of two of the above classes, and assume $xh_1x^{-1} = h_2$ for some $x \in G$. Then $x\langle h_1 \rangle x^{-1} = \langle h_2 \rangle$, and hence $xtx^{-1} = t$, since t is the unique involution contained in both $\langle h_1 \rangle$ and $\langle h_2 \rangle$. Thus $x \in H$, and we have proved (14.5ii).

A \mathbb{Z} -basis for the set of virtual characters of H vanishing off the special classes consists of the virtual characters

$$\begin{aligned}\lambda_1 &= \varphi^1 + \varphi^3 - \varphi^4, \quad \lambda_2 = \varphi^2 + \varphi^3 - \varphi^5, \\ \lambda_3 &= \varphi^3 - \varphi^6, \quad \lambda_4 = \varphi^3 - \varphi^7, \quad \lambda_5 = \varphi^1 + \varphi^2 + \varphi^3 - \varphi^8.\end{aligned}$$

We thus have determined the matrix $\mathbf{A} = (a_{ij})$ in Lemma 14.10, and now attempt to determine the possibilities for a matrix $\mathbf{B} = (b_{ij})$ as in (14.10), using the fact that

$$\mathbf{B} \cdot {}^t \mathbf{B} = \mathbf{A} \cdot {}^t \mathbf{A},$$

by (14.10ii). In this effort, we are reassured by the fact that $\sum_k b_{ik}^2 = \sum_k a_{ik}^2$ for each i , so there are only finitely many choices for \mathbf{B} .

The matrix \mathbf{A} expressing the $\{\lambda_i\}$ in terms of the $\{\varphi^j\}$ is

	φ^1	φ^2	φ^3	φ^4	φ^5	φ^6	φ^7	φ^8
λ_1	1		1	-1				
λ_2		1	1		-1			
λ_3			1			-1		
λ_4				1			-1	
λ_5	1	1	1					-1

with zeros except as indicated. Then we have

$$(14.26) \quad \mathbf{A} \cdot {}^t \mathbf{A} = \begin{pmatrix} 3 & 1 & 1 & 1 & 2 \\ 1 & 3 & 1 & 1 & 2 \\ 1 & 1 & 2 & 1 & 1 \\ 1 & 1 & 1 & 2 & 1 \\ 2 & 2 & 1 & 1 & 4 \end{pmatrix}.$$

Now let $\mathbf{B} = (b_{ij})$ be the matrix such that

$$\lambda_i^G = \sum_{j=1}^s b_{ij} \xi^j, \quad 1 \leq i \leq 5,$$

where $\text{Irr } G = \{\xi^1, \xi^2, \dots, \xi^s\}$. Then \mathbf{B} is a $5 \times s$ matrix, whose rows we shall denote by $\{\mathbf{r}_1, \mathbf{r}_2, \dots, \mathbf{r}_5\}$. Letting $\mathbf{r}_i \cdot \mathbf{r}_j$ denote the usual dot product of s -tuples, we see at once that the condition $\mathbf{B} \cdot {}^t \mathbf{B} = \mathbf{A} \cdot {}^t \mathbf{A}$ is equivalent to the condition that

$$\mathbf{r}_i \cdot \mathbf{r}_j = (i, j)\text{-entry of } \mathbf{A} \cdot {}^t \mathbf{A}.$$

We are going to show that, up to sign and rearrangement of the nontrivial characters $\{\xi^2, \dots, \xi^s\}$, the values of $\{\xi^2, \dots, \xi^s\}$ on the special classes agree with the values of $\{\varphi^1, \dots, \varphi^8\}$ on these classes in H . By Theorem 14.11, it is sufficient to prove that up to a rearrangement of the columns after the first, and up to changes of sign in the columns, the matrix \mathbf{B} coincides with the matrix \mathbf{A} given in (14.25) (with additional columns of zeros added as necessary.) This procedure is valid because the values of the characters $\{\xi^i\}$ will be used only in the class number equation (9.33), where an ambiguity of sign has no effect.

By (14.26), we have $\mathbf{r}_1 \cdot \mathbf{r}_1 = 3$, so for the first row of \mathbf{B} we may take

$$\mathbf{r}_1 = \langle 1, 0, 1, -1, 0, 0, \dots \rangle,$$

taking into account the remarks in the preceding paragraph. Now $b_{21} = (\lambda_2^G, 1_G) = a_{21} = 0$ by (14.10), and $\mathbf{r}_2 \cdot \mathbf{r}_1 = 1$, $\mathbf{r}_2 \cdot \mathbf{r}_2 = 3$, so we may choose

$$\mathbf{r}_2 = \langle 0, 1, 1, 0, -1, 0, \dots \rangle,$$

because the other possibilities

$$\langle 0, 1, \pm 1, \pm 1, 0, \dots \rangle \text{ or } \langle 0, 1, -1, 0, -1, 0, \dots \rangle$$

are easily ruled out. Next

$$\mathbf{r}_3 \cdot \mathbf{r}_3 = 2, \quad \mathbf{r}_3 \cdot \mathbf{r}_1 = \mathbf{r}_3 \cdot \mathbf{r}_2 = 1 \text{ and } b_{31} = 0.$$

Thus \mathbf{r}_3 has exactly one ± 1 in positions corresponding to the nonzero entries

of \mathbf{r}_1 and \mathbf{r}_2 . Then for \mathbf{r}_3 we obtain

$$\mathbf{r}_3 = \langle 0, 0, 1, 0, 0, -1, 0, \dots \rangle,$$

since all other possibilities can be ruled out by using the additional relations

$$\mathbf{r}_4 \cdot \mathbf{r}_4 = 2, \mathbf{r}_4 \cdot \mathbf{r}_3 = \mathbf{r}_4 \cdot \mathbf{r}_2 = \mathbf{r}_4 \cdot \mathbf{r}_1 = 1.$$

Continuing in this way, we obtain

$$\mathbf{r}_4 = \langle 0, 0, 1, 0, 0, 0, -1, 0, \dots \rangle$$

and

$$\mathbf{r}_5 = \langle 1, 1, 1, 0, 0, 0, 0, -1, 0, \dots \rangle,$$

as required.

Now consider the characters $\{\xi^1, \dots, \xi^8\}$ in $\text{Irr } G$, whose values on the special classes are determined up to sign by the matrix \mathbf{B} calculated above. Let $x_i = \xi^i(1)$, $1 \leq i \leq 8$. Then these “virtual degrees” are also determined only up to sign. With these ambiguities, we obtain the following fragment of the character table of G :

	1	t	u	v	w_1	w_2
ξ^1	x_1	1	1	1	1	1
ξ^2	x_2	1	1	1	-1	-1
ξ^3	x_3	2	2	-1	0	0
ξ^4	x_4	3	-1	0	-1	-1
ξ^5	x_5	3	-1	0	1	1
ξ^6	x_6	-2	0	1	$\sqrt{2}i$	$-\sqrt{2}i$
ξ^7	x_7	-2	0	1	$-\sqrt{2}i$	$\sqrt{2}i$
ξ^8	x_8	-4	0	-1	0	0

By Theorem 14.11, the characters $\xi^i \in \text{Irr } G$, such that $i \notin [1, 8]$, vanish on the special classes. Thus we may apply the Second Orthogonality Relation to the above fragment to obtain information about the “virtual degrees” $\{x_i\}$:

$$x_1 = 1$$

$$1 + x_2 + 2x_3 + 3x_4 + 3x_5 - 2x_6 - 2x_7 - 4x_8 = 0$$

$$1 + x_2 + 2x_3 - x_4 - x_5 = 0$$

$$1 + x_2 - x_3 \quad + x_6 + x_7 - x_8 = 0$$

$$1 - x_2 \quad - x_4 + x_5 \quad + \sqrt{2} ix_6 - \sqrt{2} ix_7 = 0$$

$$1 - x_2 \quad - x_4 + x_5 \quad - \sqrt{2} ix_6 + \sqrt{2} ix_7 = 0.$$

From these relations, we obtain easily

$$x_6 = x_7, x_4 + x_5 = x_6 + x_8 = 1 + x_2 + 2x_3,$$

$$x_6 = x_3, x_4 = 1 + x_3, x_4 - x_5 = 1 - x_2.$$

Therefore, putting $x_2 = x$ and $x_3 = y$, the virtual degrees $\{x_1, x_2, \dots, x_8\}$ are given by

$$(14.28) \quad \{1, x, y, y+1, x+y, y, y, x+y+1\}.$$

We now proceed to apply to (14.27) and (14.28) the class number formula (9.33), which asserts that

$$c_{abd} = |G| |C_G(a)|^{-1} |C_G(b)|^{-1} \sum_{m=1}^s \xi^m(1)^{-1} \xi^m(a) \xi^m(b) \xi^m(d^{-1}),$$

where a, b, d are class representatives. We note that the irreducible characters $\{\xi^1, \dots, \xi^8\}$ vanish on the special classes, and that the right hand side of the formula is independent of the sign ambiguities discussed previously. In order to compute the numbers c_{abd} for representatives of the special classes, we may use the character table of H . To see this, suppose that

$$t^x t^y = h \in H, x, y \in G,$$

where h is a representative of one of the special classes; then

$$(t^x)^{-1} h t^x = t^y t^x = h^{-1},$$

and hence $(t^x)^{-1} \langle h \rangle t^x = \langle h \rangle$, so $t^x \in C_G(t) = H$. There are two possibilities for the class intersection number c_{ttd} below, depending on whether we have:

$$\text{Case I: } t = {}_G \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

or

$$\text{Case II: } t \neq {}_G \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

With these preparations, we obtain the following table.

	Case I	Case II
$c_{uu} = \frac{ G }{(48)^2} \left\{ 1 + \frac{1}{x} - \frac{8}{y} + \frac{27}{y+1} + \frac{27}{x+y} - \frac{64}{x+y+1} \right\} =$	12	0
$c_{uu} = \frac{ G }{(48)^2} \left\{ 1 + \frac{1}{x} + \frac{8}{y} - \frac{9}{y+1} - \frac{9}{x+y} \right\} =$	4	0
$c_{uv} = \frac{ G }{(48)^2} \left\{ 1 + \frac{1}{x} - \frac{16}{x+y+1} \right\} =$	6	0
$c_{uw_1} = \frac{ G }{(48)^2} \left\{ 1 - \frac{1}{x} - \frac{9}{y+1} + \frac{9}{x+y} \right\} =$	0	0.

In Case II, it follows that $y=2$. In that case $t \in \ker \zeta^3$, contrary to the assumption that G is a simple group. Thus we have only Case I to consider. It is then easy to check that the following formula holds:

$$|G| = \frac{2(48)^2 y(y+1)}{(y-2)^2}.$$

We then obtain $(y-2)|48$, and

$$x = \frac{-y(y+1)}{y-8}.$$

Continuing in this manner (see Higman [68]) or Dornhoff ([71], I, §28)), we find that the possible solutions are:

$$y=26, x=-39, |G|=5616,$$

or

$$y=10, x=-55, |G|=7920,$$

completing the proof.

§14. Exercise

- Let F be a finite field, and let G be the set of all maps $\theta: F \rightarrow F$, given by

$$\theta(x) = ax + b, x \in F,$$

where $a, b \in F$, and $a \neq 0$. Prove that G is a group under composition of maps. Then prove that G is a Frobenius group, and find the Frobenius kernel and a Frobenius complement. Then find $\text{Irr}_C G$, using (14.4).

§15. THE ARTIN AND BRAUER INDUCTION THEOREMS

Let H be a subgroup of a finite group G , and let R be a commutative ring. The connections between RH -modules and RG -modules defined by the induction and restriction maps were discussed in §§10–12, and in §13 for tensor induction. It is not surprising that significant new information is obtained when several subgroups are brought into the picture simultaneously. This section contains powerful results in this direction, due to Artin in case R is the rational field, and to Brauer in case R is the field of complex numbers.

There is no doubt that Brauer's Theorem has played a central role in character theory since its discovery. One of the first applications, due to Brauer himself, was to prove a long-standing conjecture that the cyclotomic field of n -th roots of unity is always a splitting field for a finite group G of order n . Another application was Brauer's characterization of virtual characters, which has been used to prove a wide variety of theorems. These applications and others, as well as a converse of Brauer's Theorem due to Green, are all included in the latter part of this section.

§15A. Artin's Induction Theorem Revisited

Let G be a finite group. A \mathbb{Q} -character φ of G , or a *rational character* of G , is a character afforded by a $\mathbb{Q}G$ -module. Permutation characters $\{1_H^G\}$ arising from subgroups H of G are examples of rational characters. Artin's Induction Theorem asserts that every rational character φ of G can be expressed in the form

$$(15.1) \quad \varphi = |G|^{-1} \sum a_C 1_C^G,$$

where the sum is taken over all cyclic subgroups C of G , and the coefficients a_C are rational integers. For a proof and discussion of this result, see CR §39.

Our objective here is to give Brauer's [51] proof and refinement of the theorem, in which the coefficients a_C are given explicitly. Brauer was interested in these formulas in connection with calculations of class numbers in algebraic number fields (see [51]). We present them here partly because such formulas do not seem to be known for two other induction theorems with which we shall be concerned: the Brauer Induction Theorem (§15B or CR §40), and the Berman-Witt Theorem ((21.6) or CR §42).

For the proof of Brauer's Theorem we require first the fact that if φ is a rational character of G , then

$$(15.2) \quad \varphi(x) = \varphi(y) \text{ whenever } \langle x \rangle = \langle y \rangle.$$

For a proof see Exercise 15.3.

We shall also use the Möbius μ -function, defined by

$$\mu(n) = \begin{cases} 1 & \text{if } n=1, \\ 0 & \text{if } a^2|n \text{ for some } a>1, \\ (-1)^r & \text{if } n=p_1 p_2 \cdots p_r, p_i \text{ distinct primes.} \end{cases}$$

Then $\mu(n_1 n_2) = \mu(n_1)\mu(n_2)$ if $(n_1, n_2) = 1$, and we have

$$(15.3) \quad \sum_{d|n} \mu(d) = \begin{cases} 1 & \text{if } n=1, \\ 0 & \text{if } n>1. \end{cases}$$

(see Niven and Zuckerman ([80], §4.3) for (15.3) and further discussion of the Möbius function.)

We now have:

(15.4) Artin Induction Theorem. *Each rational character φ of G can be expressed in the form*

$$\varphi = \sum a_C 1_C^G,$$

where the sum is taken over all cyclic subgroups $\{C\}$ of G , and the coefficients are given by

$$a_C = \frac{1}{|G:C|} \sum_{C^* \geq C} \mu(|C^*:C|) \varphi(z^*),$$

where $\{C^*\}$ ranges over all cyclic subgroups containing C , and z^* is a generator of C^* .

Proof (Brauer). From (15.2), we know that the value $\varphi(z^*)$ is independent of the choice of the generator of C^* . Let

$$\varphi^* = \sum a_C 1_C^G,$$

where the coefficients a_C are given as in the statement of the theorem. We have to prove that $\varphi^* = \varphi$.

Let $x \in G$; then from (10.3) we have

$$1_C^G(x) = \frac{1}{|C|} \sum_{y \in G} i_C(yxy^{-1}),$$

which is zero unless $yxy^{-1} \in C$ for some $y \in G$. In case $1_C^G(x) \neq 0$, we may assume that $x \in C$, since 1_C^G is a class function. If $y \in N_G(\langle x \rangle)$, then certainly $yxy^{-1} \in C$; the converse also holds, since if $yxy^{-1} \in C$ then yxy^{-1} is a power

of x , because the elements yxy^{-1} and x of the cyclic group C have the same order. Therefore

$$\mathbf{1}_C^G(x) = \begin{cases} 0 & \text{if } yxy^{-1} \notin C \text{ for all } y \in G, \\ |N_G(\langle x \rangle)|/|C| & \text{if } yxy^{-1} \in C \text{ for some } y \in G. \end{cases}$$

Using this result, we have

$$\varphi^*(x) = \frac{|N_G(\langle x \rangle)|}{|G|} \sum'_{C} \sum_{C^* \geq C} \mu(|C^*:C|) \varphi(z^*),$$

where the sum Σ' is taken over cyclic subgroups C containing a conjugate of x . Now G contains exactly $|G : N_G(\langle x \rangle)|$ cyclic groups conjugate to $\langle x \rangle$, and an arbitrary cyclic subgroup C contains at most one of these conjugates. Therefore the expression for $\varphi^*(x)$ simplifies to

$$\varphi^*(x) = \sum''_{C \ni x} \sum_{C^* \geq C} \mu(|C^*:C|) \varphi(z^*),$$

where the sum Σ'' is taken over those cyclic subgroups C which contain x . Rearranging the sums, we obtain

$$\varphi^*(x) = \sum_{C^* \ni x} \varphi(z^*) \sum_C \mu(|C^*:C|),$$

where the outer sum is over cyclic subgroups C^* containing x , and the inner sum over subgroups C satisfying $C^* \geq C \geq \langle x \rangle$. For each fixed subgroup C^* of order m , the inner sum can be expressed as

$$\sum_{d|(m/t)} \mu(d),$$

where $|\langle x \rangle| = t$. By (15.3), this sum is zero unless $m/t = 1$, that is, unless $C^* = \langle x \rangle$. In that case, x is a generator of C^* , and by (15.2) we have $\varphi^*(x) = \varphi(x)$, completing the proof.

In Chapter 6, we shall give Conlon's generalization of the Artin Induction Theorem, dealing with permutation representations of G over a field K of characteristic $p \geq 0$. Conlon's Theorem gives an equality of the type (15.1), valid in the representation algebra of KG rather than in its character ring. In this formula, the subgroup C of G must be allowed to range over all semidirect products $P \rtimes E$, in which P is any p -group and E any cyclic p' -group.

§15B. Character Rings and the Brauer Induction Theorem

Throughout this section G denotes a finite group, and K the field of complex numbers. The Brauer Induction Theorem states that every K -character of G is a \mathbb{Z} -linear combination of induced linear characters from certain subgroups of G , called elementary subgroups, which have a relatively simple structure.

After the appearance of Brauer's original proof [47b] of his theorem, new proofs were found by Roquette [52] and by Brauer and Tate [55]. These made it clear that the key to the proof of the induction theorem was the consideration of certain ideals in the commutative ring $\text{ch}(KG)$ of virtual K -characters of G (see §9C). The Brauer-Tate proof of the induction theorem was given in CR §40. Here we give a new proof, due to Goldschmidt and Isaacs [75], which has some interesting features. These include an induction theorem for permutation characters (due to L. Solomon), which will be used to achieve a preliminary reduction of the problem. From this point on, the Goldschmidt-Isaacs approach is quite constructive and explicit.

We begin with a basic lemma concerning induction of class functions. A module-theoretic version was proved earlier in Corollary 10.20.

(15.5) Lemma. *Let H be a subgroup of G , and let $\xi \in \text{cf}_K(G)$ and $\psi \in \text{cf}_K(H)$. Then*

$$\xi \cdot \psi^G = (\xi|_H \cdot \psi)^G.$$

Proof. Let $x \in G$. Then

$$\begin{aligned} (\xi \cdot \psi^G)(x) &= \xi(x) \left(|H|^{-1} \sum_{y \in G} \psi(yxy^{-1}) \right) = |H|^{-1} \sum_{y \in G} \xi(yxy^{-1}) \psi(yxy^{-1}) \\ &= |H|^{-1} \sum_{y \in G} \xi|_H(yxy^{-1}) \psi(yxy^{-1}) = (\xi|_H \cdot \psi)^G(x), \end{aligned}$$

as required.

Now let us recall from §9C the definition of $\text{ch}(KG)$, the ring of virtual K -characters of G . This ring consists of all \mathbb{Z} -linear combinations of K -characters of G , with operations of pointwise addition and multiplication. An element $\xi \in \text{cf}_K(G)$ belongs to $\text{ch}(KG)$ if and only if the multiplicities $(\xi, \xi^{(i)})$ lie in \mathbb{Z} , for a basic set $\{\xi^{(1)}, \dots, \xi^{(s)}\}$ of irreducible K -characters of G . Thus $\xi \in \text{ch}(KG)$ if and only if ξ can be expressed as

$$\xi = \sum_{i=1}^s a_i \xi^{(i)}, a_i \in \mathbb{Z}.$$

(15.6) Definition. Let \mathcal{H} be a family of subgroups of G . We define

$$v(\mathcal{H}, G) = \sum_{H \in \mathcal{H}} \sum_{\psi \in \text{ch}(KH)} \mathbb{Z}\psi^G.$$

We may express $v(\mathcal{H}, G)$ more concisely as

$$v(\mathcal{H}, G) = \sum_{H \in \mathcal{H}} \{\text{ch}(KH)\}^G,$$

because of the additivity of the induction map $\psi \rightarrow \psi^G$.

From Lemma 15.5, it follows at once that $v(\mathcal{H}, G)$ is an ideal in the commutative ring $\text{ch}(KG)$, for an arbitrary family of subgroups \mathcal{H} . Brauer's Theorem is mainly the assertion that $v(\mathcal{H}, G) = \text{ch}(KG)$ when \mathcal{H} is the family of elementary subgroups of G .

(15.7) Definition. A subgroup H of G is called *p-elementary* for a prime p , if H is the direct product of a p -group and a cyclic group of order prime to p . The family of *elementary subgroups* \mathcal{E} consists of all such subgroups, each of which is p -elementary for some prime p .

The Primary Decomposition Theorem implies that a cyclic group is p -elementary for every prime p , and thus every element of G is contained in some elementary subgroup. The same result also shows that a direct product of a p -group and an arbitrary cyclic group is p -elementary. Finally we note that elementary groups are nilpotent, and that subgroups of elementary groups are elementary (because a nilpotent group is the direct product of its p -Sylow subgroups).

Another family of subgroups which will be important for our considerations is the family of *hyper-elementary groups* \mathcal{H} , defined as follows: A group H is *hyper-elementary* if there exists a cyclic normal subgroup $\langle x \rangle$ of H of order prime to p , such that $H/\langle x \rangle$ is a p -group; in other words, H has a cyclic normal p -complement. Equivalently, H is a semidirect product $\langle x \rangle \rtimes P$ of a cyclic p' -group $\langle x \rangle$ and a p -group P , for some prime p . It follows from the homomorphism theorems that subgroups of hyper-elementary groups are hyper-elementary. We also observe that elementary groups are hyper-elementary, so that $\mathcal{E} \subseteq \mathcal{H}$.

We can now state the main results of this section:

(15.8) Theorem. Let \mathcal{E} be the family of elementary subgroups of G . Then $v(\mathcal{E}, G) = \text{ch}(KG)$.

(15.9) Brauer Induction Theorem. Every virtual character of G is a \mathbb{Z} -linear combination of induced linear characters from elementary subgroups of G . In

other words, for each $\zeta \in \text{ch}(KG)$ there exist linear characters $\{\lambda_i\}$ of elementary subgroups $\{H_i\}$ and integers $\{a_i\}$, depending on ζ , such that

$$\zeta = \sum a_i \lambda_i^G.$$

(15.10) **Theorem (L. Solomon).** *There exist rational integers $\{c_i\}$ such that*

$$1_G = \sum c_i (1_{H_i})^G,$$

for some hyper-elementary subgroups $\{H_i\}$ of G .

We shall first prove theorem 15.10, and will then show how theorems 15.8 and 15.9 follow from it.

This approach to Brauer's Theorem is due to Goldschmidt and Isaacs [75] (see also Isaacs [76], Chapter 8). The idea is to use Solomon's Theorem 15.10 to prove that $1_G \in v(\mathcal{E}, G)$. It will then follow that $v(\mathcal{E}, G) = \text{ch}(KG)$ because by Lemma 15.5, $v(\mathcal{E}, T)$ is an ideal in $\text{ch}(KG)$.

To begin the proof of Theorem 15.10, let $P(\mathcal{H}, G)$ be the additive group of \mathbb{Z} -linear combinations of permutation characters $\{1_H^G : H \in \mathcal{H}\}$. If H and H' are subgroups of G , then by the Tensor Product Theorem 10.18 we have

$$(1_H)^G \cdot (1_{H'})^G = \sum_x (1_{xH \cap H'})^G$$

for certain elements $x \in G$. Since subgroups of hyper-elementary groups are hyper-elementary, it follows that $P(\mathcal{H}, G)$ is a ring of \mathbb{Z} -valued functions on G , under pointwise addition and multiplication. We have to prove that $1_G \in P(\mathcal{H}, G)$. For this purpose, we use a special case of a result due to Banaschewski [63, §1]:

(15.11) **Lemma.** *Let A be a ring* of \mathbb{Z} -valued functions on a finite set X , under pointwise addition and multiplication. Let 1_X be the constant function, all of whose values are equal to 1. If 1_X does not belong to A , then there exists an $x \in X$ and a prime p such that $p \mid f(x)$ for all $f \in A$.*

Proof. For each $x \in X$, let $I_x = \{f(x) : f \in A\}$. Then I_x is a subring* of \mathbb{Z} ; if $I_x \neq \mathbb{Z}$, then $I_x \subseteq (p)$ for some prime p , and hence $p \mid f(x)$ for all $f \in A$. To prove the lemma, we have to show that if $I_x = \mathbb{Z}$ for all $x \in X$, then $1_X \in A$. Assuming that $1 \in I_x$ for each $x \in X$, we may choose $f_x \in A$ with $f_x(x) = 1$. Then

$$\prod_{x \in X} (1_X - f_x) = 0.$$

*In this lemma, rings are not assumed to have identity elements.

Expanding this product, we see that 1_X is a \mathbb{Z} -linear combination of products of the functions $\{f_x\}$, and hence $1_X \in A$, as required.

We can now complete the proof of (15.10). By Lemma 15.11, it is sufficient to show that given $x \in G$ and a prime p , there exists a hyper-elementary subgroup H such that $p \nmid (1_H^G)(x)$. Let C be the p -complement in $\langle x \rangle$, and let $N = N_G(C)$; let H/C be a Sylow p -subgroup of N/C . Then H is hyper-elementary, with cyclic p -complement C .

Now $1_H^G(x)$ is equal to the number of left cosets $\{gH\}$ fixed by x . If $xgH = gH$, then $x^g \in H$, whence $C^g \leq \langle x \rangle^g \leq H$. Since C is the unique subgroup in H of its order, we have $C^g = C$, and $g \in N_G(C) = N$. Noting that x also lies in N , we have shown that

$$1_H^G(x) = 1_H^N(x).$$

Next, $C \trianglelefteq N$ and $C \trianglelefteq H$, which imply that C acts trivially on the cosets of H in N . Moreover, $\langle x \rangle/C$ is a p -group, so that the number of elements in each non-trivial orbit of $\langle x \rangle$ acting on N/H is divisible by p . The total number of cosets being permuted is $|N:H|$, whence the number of fixed cosets under the action of x is congruent to $|N:H| \pmod{p}$. We have thus shown that

$$1_H^N(x) \equiv |N:H| \pmod{p}.$$

But $|N:H|$ is prime to p , so that $p \nmid (1_H^N)(x)$, as required. This completes the proof of (15.10).

We next prove that Theorem 15.10 implies Theorem 15.8. Because $v(\mathcal{E}, G)$ is an ideal in $\text{ch}(KG)$ by Lemma 15.5, it suffices to prove that $1_G \in v(\mathcal{E}, G)$. By (15.10) and transitivity of induction, we may assume that G is hyper-elementary. Using induction on $|G|$, it thus suffices to prove that if G is hyper-elementary but not elementary, then 1_G is a \mathbb{Z} -linear combination of characters induced from proper subgroups of G . This can be established quite explicitly, as follows:

We have $G = C \times P$, where C is a cyclic p' -group and P is a p -group, for some prime p . Let Z be the centralizer in C of the subgroup P ; then $Z < C$ since we are assuming that G is not elementary. Put $H = Z \times P$, so $H < G$; we shall prove

$$(15.12) \quad 1_H^G = 1_G + \sum \xi_i,$$

where the $\{\xi_i\}$ are irreducible characters of G which are induced from proper subgroups of G . This will imply that 1_G is itself a \mathbb{Z} -linear combination of characters induced from proper subgroups, and so the proof of (15.8) will be finished.

Since $G = HC$, we have

$$(1_H^G)|_C = (1_{C \cap H})^C = 1_Z^C$$

by the Subgroup Theorem 10.13. Let (15.12) be the decomposition of 1_H^G as a sum of irreducible complex characters. Restricting to C , we obtain

$$(15.13) \quad 1_Z^C = 1_C + \sum \xi_i|_C.$$

By Frobenius Reciprocity we deduce that $(\xi_i|_Z, 1_Z) \neq 0$ for each i ; further, $\xi_i|_C \neq 1_C$ for each i , since 1_C occurs with multiplicity 1 in 1_Z^C . Since C is a cyclic normal subgroup of G , it now follows from (11.4) that for each i , ξ_i is a component of λ^G for some linear character $\lambda \neq 1$ of C , and furthermore $Z \leq \ker \lambda$. However, (11.5iii) gives the decomposition of λ^G into irreducible characters, each of which is induced from a character of the stabilizer G_λ . If we can show that $G_\lambda < G$, it will thus follow that each ξ_i occurring in (15.12) is induced from a proper subgroup of G , and we will have proved Theorem 15.8. We need only use the following (see Isaacs [76, Lemma 8.11]):

(15.14) Lemma. *Let G be a finite group such that $G = N \rtimes P$, where N is a p' -group and P is a p -group for some prime p . Let λ be a linear character of N whose stabilizer G_λ coincides with G , and is such that $Z \leq \ker \lambda$, where $Z = C_N(P)$. Then $\lambda = 1_N$.*

Proof. Let $L = \ker \lambda$. Since λ is linear, λ takes distinct constant values on the cosets of L in N . For $y \in P$, ${}^y\lambda = \lambda$ by hypothesis; the preceding remark then shows that each coset nL of L in N is fixed under conjugation by y . Now P is a p -group, so the length of each nontrivial orbit of L under the action of P is a multiple of p . Since the number of elements in nL is prime to p , there must be at least one trivial orbit. Hence some element of nL lies in the centralizer Z of P in N . Since $Z \leq L$ by hypothesis, this shows that each coset nL coincides with L , and therefore $L = N$. We have thus proved that $\lambda = 1_N$, as required.

Finally, we show that Theorem 15.8 implies the Brauer Induction Theorem 15.9. By Theorem 15.8, it suffices to prove that each irreducible character of an elementary group H is induced from a linear character of some elementary subgroup H_0 of H . We have already pointed out that subgroups of elementary groups are elementary, and that elementary groups are nilpotent. Thus the desired result follows from Theorem 11.3, and the proof of (15.9) is finished.

§15C. Applications of the Brauer Induction Theorem

Let us keep the notation of §15B. In particular, K is the complex field, $\text{ch}(KG)$ the ring of virtual K -characters of G , and \mathcal{E} denotes the family of all elementary subgroups of G .

(15.15) Brauer's Criterion for Virtual Characters. A class function $\varphi \in cf_K(G)$ belongs to $ch(KG)$ if and only if for all elementary subgroups $H \leq G$, we have $\varphi|_H \in ch(KH)$.

Proof. One way is clear. For the other part, let $\varphi \in cf_K(G)$ be such that $\varphi|_H \in ch(KH)$ for all subgroups $H \in \mathcal{E}$. From (15.9), we may write

$$1_G = \sum a_i \lambda_i^G, \quad a_i \in \mathbb{Z}, \quad \lambda_i \in ch(KH_i), \quad H_i \in \mathcal{E}.$$

Then by (15.5),

$$\varphi = \varphi \cdot 1_G = \sum a_i (\varphi \cdot \lambda_i^G) = \sum a_i [(\varphi|_{H_i}) \lambda_i] ^G \in ch(KG),$$

as required. (The last step follows from the hypothesis and the fact that the product of two virtual characters of H_i is a virtual character).

The above result has been one of the most useful theorems for constructing character tables of finite groups. For a given finite group, it is often possible to guess at some class functions, and then use (15.15) to prove that they are virtual characters. One then obtains irreducible characters from the observation that if φ is a virtual character for which $(\varphi, \varphi) = 1$, then $\pm \varphi \in Irr(G)$.

The next result settles an old problem considered by Burnside, Maschke and Schur. Evidently the value of the irreducible complex characters of G belong to the cyclotomic field $\mathbb{Q}(\omega_n)$, where $n = |G|$ and ω_n is a primitive n -th root of 1 (see §4H). The question is whether $\mathbb{Q}(\omega_n)$ is a splitting field for G .

(15.16) Brauer's Splitting Field Theorem. Let G be a finite group of order n . The cyclotomic field $\mathbb{Q}(\omega_n)$, generated by a primitive n -th root of 1, is a splitting field for G .

Proof (Feit). By Proposition 7.14, it is sufficient to prove that every irreducible K -representation of G can be realized in $\mathbb{Q}(\omega_n)$. Referring to (15.9), it is clear that the linear representations λ of elementary subgroups of G are $\mathbb{Q}(\omega_n)$ -representations, and hence each induced representation λ^G is also a $\mathbb{Q}(\omega_n)$ -representation. Now let T be an irreducible K -representation of G with character τ . By (15.9) we have

$$\tau = \sum a_i \lambda_i^G, \quad a_i \in \mathbb{Z},$$

where the $\{\lambda_i^G\}$ are characters of $\mathbb{Q}(\omega_n)$ -representations of G . If all the coefficients $\{a_i\}$ are positive then τ is afforded by a $\mathbb{Q}(\omega_n)$ -representation, and there is nothing left to prove. If some coefficients $\{a_i\}$ are negative, then by rearranging terms we have

$$(15.17) \quad \tau_2 = \tau + \tau_1,$$

where τ_1 and τ_2 are characters of $\mathbb{Q}(\omega_n)$ -representations T_1 and T_2 respectively, and we have

$$T_2^K \cong T_1^K \oplus T.$$

But then T can be realized in $\mathbb{Q}(\omega_n)$, by Exercise 15.6, which completes the proof.

(15.18) Corollary. *Let F be a field of characteristic 0, G a finite group of exponent* n , and ω a primitive n -th root of 1 over \mathbb{Q} . Then every field E containing $F(\omega)$ is a splitting field for G and all of its subgroups.*

Proof. The proof of Theorem 15.16 shows in fact that $\mathbb{Q}(\omega)$ is a splitting field for G . Since $E \supseteq F(\omega) \supseteq \mathbb{Q}(\omega)$, and extensions of splitting fields are also splitting fields, it follows that E is a splitting field for G . The corresponding statement for subgroups of G is then obvious.

Our next result is an interesting criterion, due to Gallagher [66], for the vanishing of irreducible characters of G on certain types of elements. The reader will note that many occurrences of zeros in the character tables constructed in the exercises in §§9–11, for example, are accounted for by Gallagher’s Theorem. Gallagher’s result should be compared with the classical result of Burnside that every irreducible non-linear C-character of G has at least one zero (see CR Exercise 31.3).

We first introduce some terminology. Let Π be a set of rational primes. A positive integer m is a Π -number if each prime factor of m belongs to Π , and a Π' -number if no prime factor of m belongs to Π . Each m can be written uniquely as $m = m_\Pi m_{\Pi'}$, where m_Π is the Π -part of m and is a Π -number, and $m_{\Pi'}$ is the Π' -part and is a Π' -number. A finite group G is a Π -group if $|G|$ is a Π -number. Similarly, we define Π' -groups, and Π - and Π' -elements of G . Extending the terminology used for a single prime, an element $x \in G$ is called Π -regular if x is a Π -element, and Π -irregular otherwise. Thus, x is Π -irregular if and only if the order of x has a prime factor from Π .

(15.19) Theorem (Gallagher [66]). *Let G be a finite group and Π a set of primes. Let ζ be an irreducible complex character of G whose degree is divisible by $|G|_\Pi$. Then ζ vanishes on all Π -irregular elements of G .*

Remark. By Proposition 9.32, the degree of ζ divides $|G|$, so the hypothesis is equivalent to the statement that $|G|/\deg \zeta$ is a Π' -number, or equivalently, that $|G|_\Pi = \zeta(1)_\Pi$. It should also be noted that the Theorem follows at once from (18.28) below.

Proof. Throughout the proof, all characters of G and its subgroups are taken in the complex field K . Here is the idea of the proof. Define a class function φ

*The exponent of G is the L.C.M. of the orders of the elements of G .

on G by setting,

$$\varphi(x) = \begin{cases} \zeta(x) & \text{if } x \text{ is } \Pi\text{-regular,} \\ 0 & \text{if } x \text{ is } \Pi\text{-irregular.} \end{cases}$$

We shall use Brauer's Criterion 15.15 to show that $\varphi \in \text{ch}(KG)$. Once this is done, from the inequalities $0 < (\varphi, \varphi) \leq (\zeta, \zeta) = 1$ we obtain $(\varphi, \varphi) = 1$. Then $(\varphi, \zeta) = (\varphi, \varphi) = 1$, so $(\varphi - \zeta, \varphi - \zeta) = 0$, whence $\varphi = \zeta$, and the theorem is proved.

In order to use Brauer's Criterion, we must show that $\varphi|_H \in \text{ch}(KH)$ for each $H \in \mathcal{E}$, where \mathcal{E} is the family of elementary subgroups of G . Equivalently, we must show that $(\varphi|_H, \lambda)_H \in \mathbb{Z}$ for all K -characters λ of H , and all $H \in \mathcal{E}$. Given $H \in \mathcal{E}$, we may write $H = A \times B$, where A is a Π' -subgroup and B a Π -subgroup. Using the definition of φ and the factorization of H , we obtain for each λ :

$$\begin{aligned} (\varphi|_H, \lambda)_H &= |H|^{-1} \sum_{x \in H} \varphi(x) \overline{\lambda(x)} = |H|^{-1} \sum_{x \in A} \varphi(x) \overline{\lambda(x)} \\ &= |A| |H|^{-1} (\zeta_A, \lambda_A)_A = |B|^{-1} (\zeta_A, \lambda_A)_A. \end{aligned}$$

We shall prove below that $|B|^{-1} \zeta(x) \in \text{alg. int. } \{K\}$ for each $x \in A$. Taking this for granted for the moment, let $m = (\zeta_A, \lambda_A)_A$, so $m \in \mathbb{Z}$ because ζ_A, λ_A are K -characters of A . Then

$$m|A|/|B| = |A|(|B|^{-1} \zeta_A, \lambda_A)_A \in \text{alg. int. } \{K\},$$

so $|B|$ divides $m|A|$. Since $|B|$ is relatively prime to $|A|$, this shows that $|B|$ divides m , whence $(\varphi|_H, \lambda_H)_H \in \mathbb{Z}$ as desired.

To complete the proof, let $x \in A$ and let us show that $|B|^{-1} \zeta(x)$ is an algebraic integer. We have

$$\zeta(x) \cdot |G : C_G(x)| / \zeta(1) \in \text{alg. int. } \{K\}$$

by (9.29) and (9.31). But $C_G(x) \geq B$, so $|G : C_G(x)| |C_G(x) : B| = |G : B|$. Moreover $\zeta(1)_\Pi = |G|_\Pi$ by hypothesis. Using the fact that

$$|G : C_G(x)|_\Pi = |G|_\Pi |B|_\Pi^{-1} |C_G(x) : B|_\Pi^{-1},$$

we obtain

$$\begin{aligned} \frac{\zeta(x) |G : C_G(x)|}{\zeta(1)} &= \frac{\zeta(x) |G : C_G(x)|_\Pi |G : C_G(x)|_{\Pi'}}{\zeta(1)_\Pi \zeta(1)_{\Pi'}} \\ &= \frac{\zeta(x) |G|_\Pi |G : C_G(x)|_{\Pi'}}{\zeta(1)_\Pi \zeta(1)_{\Pi'} |B|_\Pi |C_G(x) : B|_\Pi} = \frac{\zeta(x) |G : C_G(x)|_{\Pi'}}{\zeta(1)_{\Pi'} |B|_\Pi |C_G(x) : B|_\Pi}. \end{aligned}$$

Therefore,

$$\frac{\xi(x)|G:C_G(x)|_{\Pi'}}{|B|} \in \text{alg. int. } \{K\}.$$

But $|G:C_G(x)|_{\Pi'}$ is invertible modulo the Π -number $|B|$, so the above implies that $|B|^{-1}\xi(x) \in \text{alg. int. } \{K\}$. This completes the proof.

§15D. Extensions of Invariant Characters

We continue with another application of Brauer's Theorem, to the question of when an irreducible character ψ of a normal subgroup can be extended to its stabilizer. We shall give several criteria for such extensions to exist; each criterion, when combined with Proposition 11.5, gives an explicit construction of the irreducible components of ψ^G . All the results in this section are contained in Gallagher's paper [62b].

We begin with some preliminary remarks. We shall be concerned throughout exclusively with K -characters of a finite group G and its subgroups, where $K=C$. Let $N \trianglelefteq G$, and let $\psi \in \text{Irr}_K(N)$. We call ψ an *invariant* character if its stabilizer G_ψ coincides with G (see §11B). A K -character ξ of G *extends* ψ (or is an *extension* of ψ) if $\xi|_N = \psi$; such an extension, if it exists, is automatically irreducible. Let ξ_1 be a fixed extension of ψ ; then from (11.7) we know that any other extension ξ can be expressed in the form $\xi = \xi_1\omega$ for a uniquely determined linear character ω of G/N .

For a character μ of G , irreducible or not, we shall write $\mu \in \psi^G$ to indicate that either $\psi^G = \mu$ or that $\psi^G = \mu + \mu'$ for some other character μ' . Next, we note that if \mathbf{M} is a K -representation of G with character μ , then $\det \mathbf{M}$ is a linear representation of G , which depends only on the equivalence class of \mathbf{M} . We denote the character of $\det \mathbf{M}$ by $\det \mu$, so

$$(\det \mu)(x) = \det \mathbf{M}(x), \quad x \in G.$$

(See §13B for connections between $\det \mu$ and the transfer map.) For each linear character ω of G , we have

$$(15.20) \quad \det(\omega\mu) = \omega^{\deg \mu} \det \mu.$$

Our first result is an application of the results in §11B:

(15.21) Proposition. *Let N be a normal subgroup of prime index p in G . Then each invariant irreducible character ψ of N extends to a character of G .*

Proof. Let $\xi \in \text{Irr}(G)$ be such that $(\xi, \psi^G) > 0$. By Proposition 11.4, $\xi|_N = a\psi$ for some positive integer a , because ψ is invariant. The factor group G/N is cyclic of order p , and for each linear character ω of G/N , we have $\omega\xi \in \text{Irr}_K(G)$

and $\omega\zeta|_N = a\psi$. The characters $\{\omega\zeta : \omega \in \text{Irr}_K(G/N)\}$ are distinct. In fact, if $\omega\zeta = \omega'\zeta$ for $\omega \neq \omega'$, then $\zeta = 0$ off N , and we have,

$$a^2 = (\zeta|_N, \zeta|_N)_N = p(\zeta, \zeta)_G = p,$$

which is impossible. Therefore, by Frobenius Reciprocity,

$$\sum_{\omega} a \cdot \omega\zeta \in \psi^G.$$

Since

$$(\psi^G, \psi^G)_G = (\psi^G|_N, \psi)_N = p$$

because ψ is invariant, we conclude that $a = 1$, and hence ζ extends ψ , as required.

The next result gives a criterion for extensions to exist, which depends on Brauer's Theorem.

(15.22) Proposition. *Let $N \trianglelefteq G$, and let ψ be an irreducible invariant character of N . Suppose that for each intermediate subgroup H for which H/N is elementary, ψ can be extended to a character ψ_H of H . Assume further that the extensions $\{\psi_H\}$ satisfy the following two conditions:*

$$(i) \quad {}^x(\psi_H) = \psi_{xH}, \quad \forall x \in G,$$

$$(ii) \quad \psi_{H'} = \psi_{H''}|_{H'} \text{ if } H' \leq H''.$$

Then ψ can be extended to a character of G .

Proof. Let $1_{G/N}$ denote the trivial character of G/N , lifted to a trivial character of G . Then by Brauer's Theorem 15.9, we may write

$$1_{G/N} = \sum a_i \lambda_i^G, \quad a_i \in \mathbb{Z},$$

where $\{\lambda_i\}$ ranges over linear characters of subgroups $\{H_i\}$, with $H_i \geq N$, H_i/N elementary, and $N \leq \ker \lambda_i$. Define

$$\zeta = \sum a_i (\lambda_i \psi_{H_i})^G.$$

Then $\zeta \in \text{ch}(KG)$. Moreover, by an easy calculation using (10.3), we have

$$(\lambda_i \psi_{H_i})^G(n) = \lambda_i^G(n) \psi_{H_i}(n), \quad \forall n \in N,$$

and it follows that $\zeta|_N = \psi$.

To complete the proof, we must show that $\xi \in \text{Irr}_K(G)$, and for this it suffices to prove that $(\xi, \xi)_G = 1$. Indeed, the latter implies that $\pm \xi \in \text{Irr}_K(G)$, and then $\xi \in \text{Irr}_K(G)$ because $\xi(1) = \psi(1) > 0$. We have

$$1 = (1_{G/N}, 1_{G/N})_G = \sum_{i,j} a_i a_j (\lambda_i^G, \lambda_j^G)_G,$$

and

$$(\xi, \xi) = \sum_{i,j} a_i a_j ((\lambda_i \psi_{H_i})^G, (\lambda_j \psi_{H_j})^G)_G.$$

In order to prove that $(\xi, \xi) = 1$, it is sufficient to show that corresponding terms in the sums are equal. We have, by the Intertwining Number Theorem,

$$((\lambda_i \psi_{H_i})^G, (\lambda_j \psi_{H_j})^G)_G = \sum_x (^x(\lambda_i \psi_{H_i}), (\lambda_j \psi_{H_j}))_{^x H_i \cap H_j},$$

where the sum is taken over representatives $\{x\}$ of (H_i, H_j) double cosets in G . The subgroups ${}^x H_i \cap H_j$ contain N , and the factor groups $({}^x H_i \cap H_j)/N$ are elementary. By hypotheses (i) and (ii) of the proposition, we have

$$({}^x(\lambda_i \psi_{H_i}), \lambda_j \psi_{H_j})_{^x H_i \cap H_j} = (^x \lambda_i \psi_{^x H_i \cap H_j}, \lambda_j \psi_{^x H_i \cap H_j}).$$

From the remarks at the beginning of this section, the above scalar product is 1 or 0, according as the linear characters ${}^x \lambda_i$ and λ_j coincide on ${}^x H_i \cap H_j$ or not. Therefore the above product is equal to $({}^x \lambda_i, \lambda_j)_{^x H_i \cap H_j}$, and we conclude that $(\xi, \xi)_G = 1$, as required.

In order to state the main result of this section, we recall one more bit of terminology from finite group theory. A subgroup H of G is called a *Hall subgroup* if the order $|H|$ and the index $|G: H|$ are relatively prime. The main result* can then be stated as follows:

(15.23) Theorem (Gallagher). *Every invariant irreducible character of ψ of a normal Hall subgroup N of G extends to a character of G .*

The proof depends on one more preliminary result, which is of independent interest:

(15.24) Proposition. *Let $N \trianglelefteq G$, and let ψ be an irreducible invariant character of N , such that the following conditions hold:*

- (i) $\det \psi$ extends to a character ξ of G ;
- (ii) $\deg \psi$ is prime to $|G: N|$.

*The same result holds for representations over an arbitrary field; see Isaacs [81].

Then there is a unique irreducible character ξ of G such that $\xi|_N = \psi$ and $\det \xi = \xi$.

Proof. We first show that if ψ extends to a character of G , there is a unique extension ξ such that $\det \xi = \xi$. In fact, from the preliminary remarks of this section, all extensions are given by $\omega \xi_1$, where ξ_1 is any one fixed extension, and ω ranges over the linear characters of G/N . Since $\xi(\det \xi_1)^{-1}$ is a linear character of G/N and $\deg \psi$ is prime to $|G:N|$, there is a unique element ω of the finite abelian group of linear characters of G/N such that

$$\omega^{\deg \psi} = \xi(\det \xi_1)^{-1}.$$

For this character ω we have, by (15.20),

$$\det(\omega \xi_1) = \omega^{\deg \psi} \det \xi_1 = \xi,$$

as required.

To prove the existence of an extension, suppose first that G/N is supersolvable (see Exercise 11.1). If $G=N$, put $\xi=\psi$. If $G\neq N$, let H/N be a normal subgroup of prime order of G/N . Since ψ is invariant under H , Proposition 15.21 implies that ψ extends to a character of H . By the preceding paragraph, ψ has a unique extension ψ_1 such that $\det \psi_1 = \xi|_H$. For each $x \in G$, ${}^x \psi_1$ is an extension of ψ to H such that $\xi({}^x \psi_1) = \xi|_H$. Then ${}^x \psi_1 = \psi_1$ by uniqueness, and ψ_1 is invariant. By induction, ψ_1 extends to a character of G .

To complete the proof in the general case, we note that elementary groups are nilpotent, hence supersolvable. Hence there are unique extensions ψ_H of ψ to the groups $H \geq N$ such that H/N is elementary, and these satisfy $\det \psi_H = \xi|_H$. Properties (i) and (ii) of Proposition 15.22 follow from the uniqueness and the invariance of ξ under conjugation. We can then apply Proposition 15.22 to conclude that an extension exists, completing the proof of Proposition 15.24.

Proof of Theorem 15.23. Let ψ be an invariant character of N , as in the Theorem. Then $\deg \psi$ divides $|N|$, by Proposition 9.32, and hence $\deg \psi$ and $|G:N|$ are relatively prime since N is a Hall subgroup. Moreover, by Schur's Theorem 8.35, there exists a subgroup H of G such that

$$G = NH, \quad N \cap H = \{1\}.$$

Since $\det \psi$ is a linear character of N , and is invariant because of the invariance of ψ , the construction used in part (ii) of Proposition 11.8 shows at once that $\det \psi$ can be extended to a character of G . We then apply Proposition 15.24 to conclude that ψ extends to a character of G , which completes the proof of Gallagher's Theorem 15.23.

§15E. A Criterion for Existence of Normal Complements

We give one more application of Brauer's Theorem, this time to group theory. We say that a subgroup S of a finite group G has a *normal complement* if there exists a normal subgroup N of G such that G is the semidirect product, $G = N \rtimes S$. Burnside's Transfer Theorem 13.20 gives a criterion for Sylow p -subgroups to have normal complements. Another criterion for the existence of normal complements is provided by Frobenius' Theorem 14.2. The main result of this subsection, due to Brauer [64b] and Suzuki [63], includes both of the above results as special cases. The proof is based on Brauer's Criterion for Virtual Characters 15.15. Our presentation follows Isaacs [76] (see also Huppert [67; Chapter 5, (19.12)]) for a proof of Frobenius' Theorem by the same method).

Before stating the result, we recall from §15D that a subgroup S of G is a *Hall subgroup* if its order $|S|$ and index $|G : S|$ are relatively prime.

(15.25) Theorem. *Let S be a Hall subgroup of G , which satisfies both of the following conditions:*

- (i) *If $x, y \in S$ are conjugate in G , then they are conjugate in S ;*
- (ii) *Each elementary subgroup H of G , whose order divides $|S|$, is conjugate to a subgroup of S .*

Then S has a normal complement in G .

Proof. Let Π be the set of primes which divide $|S|$, and let us adopt the terminology “ Π -element”, “ Π -subgroup”, etc., as in the discussion preceding (15.19). For each $x \in G$, we may apply the Primary Decomposition Theorem to the cyclic group $\langle x \rangle$, and conclude that x is uniquely expressible in the form

$$x = x_{\Pi} x_{\Pi'}, \text{ where } x_{\Pi} = \Pi\text{-element}, x_{\Pi'} = \Pi'\text{-element},$$

and where x_{Π} commutes with $x_{\Pi'}$. (Indeed, both x_{Π} and $x_{\Pi'}$ are suitable powers of x .) We now proceed in a series of steps.

Step 1. Let $\varphi \in \text{ch } KS$, where $K = C$. We define a class function $\tilde{\varphi}$ on G as follows. Let $x \in G$; then $\langle x_{\Pi} \rangle$ is an elementary subgroup whose order divides $|S|$. By part (ii) of the hypothesis, x_{Π} is conjugate to an element $s \in S$, and we set

$$\tilde{\varphi}(x) = \varphi(s).$$

By part (i) of the hypothesis, it follows that $\tilde{\varphi}$ is a well-defined class function on G .

Now let $\{s_1, \dots, s_t\}$ be representatives of the conjugacy classes of S , and for each i , $1 \leq i \leq t$, let m_i be the number of elements $x \in G$ such that $x_{\Pi} = {}_G s_i$.

Then for all virtual K -characters φ and ψ of S , we have

$$(15.26) \quad (\tilde{\varphi}, \tilde{\psi})_G = |G|^{-1} \sum_{i=1}^t m_i \varphi(s_i) \psi(s_i^{-1}).$$

Step 2. We prove that if $\varphi \in \text{ch } KS$, then $\tilde{\varphi} \in \text{ch } KG$. By (15.15), it suffices to prove that for all elementary subgroups H of G , we have $\tilde{\varphi}_H \in \text{ch } KH$. The elementary subgroup H of G may be written as $H = A \times B$, where A is a Π -subgroup and B a Π' -subgroup. By hypothesis (ii), we may assume that $A \leq S$. For all $a \in A, b \in B$, we have $(ab)_\Pi = a$, and hence $\tilde{\varphi}_H(ab) = \varphi(a)$. Now let $\varphi_A = \sum c_i \xi_i$, where $\xi_i \in \text{Irr } A$, $c_i \in \mathbb{Z}$. Let $\xi_i \otimes 1_B$ denote the character of $A \times B$ which is the product of ξ_i and the trivial character 1_B of B . Then for all $a \in A, b \in B$, we have

$$\tilde{\varphi}_H(ab) = \varphi(a) = \sum c_i \xi_i(a) = \sum c_i (\xi_i \otimes 1_B)(ab).$$

Thus $\tilde{\varphi}_H = \sum c_i (\xi_i \otimes 1_B) \in \text{ch } KH$, and by Brauer's Criterion 15.15 it follows that $\tilde{\varphi} \in \text{ch } KG$, as desired.

Step 3. Next we prove that for all virtual characters $\varphi, \psi \in \text{ch } KS$, we have

$$(\tilde{\varphi}, \tilde{\psi})_G = (\varphi, \psi)_S.$$

We first require some preliminary remarks. Let $R = \mathbb{Z}[\omega]$, where ω is a primitive $|G|$ -th root of 1. Then R is a ring of algebraic integers in the complex field K . We set $\text{ch}_R KG = R \otimes_{\mathbb{Z}} \text{ch } KG$; since the characters in $\text{Irr } G$ are a \mathbb{Z} -basis of $\text{ch } KG$, they are also an R -basis of $\text{ch}_R KG$. Therefore, $\text{ch}_R KG$ can be identified with the set of R -linear combinations of the elements of $\text{ch } KG$. Similar remarks apply to $\text{ch}_R KS$. It follows at once from Step 2 that if $\mu \in \text{ch}_R KS$, and $\tilde{\mu}$ is defined as above, then $\tilde{\mu} \in \text{ch}_R KG$; indeed, if we write $\mu = \sum a_i \varphi_i$, with $\varphi_i \in \text{Irr}_K S$, $a_i \in R$, then $\tilde{\mu} = \sum a_i \tilde{\varphi}_i \in \text{ch}_R KG$.

Now consider the class functions $\{\gamma_i : 1 \leq i \leq t\}$ defined by

$$\gamma_i = \sum_{\varphi \in \text{Irr } S} \varphi(s_i^{-1}) \varphi \in \text{cf}_K(S), \quad 1 \leq i \leq t,$$

where $\{s_1, \dots, s_t\}$ are representatives of the conjugacy classes in S , as in Step 1. Using the Second Orthogonality Relation 9.26, we have

$$\gamma_i(s_j) = \begin{cases} |C_S(s_i)|, & j=i, \\ 0, & j \neq i, \end{cases}$$

where i and j range from 1 to t . Since each coefficient $\varphi(s_i^{-1})$ lies in R , we have $\gamma_i \in \text{ch}_R KS$, and hence $\tilde{\gamma}_i \in \text{ch}_R KG$ by the preceding remarks and Step 2.

Let us show that $m_i = |G : C_S(s_i)|$ for each i , $1 \leq i \leq t$. By (15.26) we have

$$(\tilde{\gamma}_i, 1_G) = |G|^{-1} \sum_{j=1}^t m_j \gamma_i(s_j) = |G|^{-1} \cdot m_i \cdot |C_S(s_i)| \in R \cap Q,$$

and so $|G|^{-1} \cdot m_i \cdot |C_S(s_i)| \in Z$, $1 \leq i \leq t$. Therefore $m_i \geq |G : C_S(s_i)|$ for each i , and we obtain

$$|G| = \sum_{i=1}^t m_i \geq \sum_{i=1}^t |G : C_S(s_i)| = |G : S| \cdot \sum_{i=1}^t |S : C_S(s_i)|.$$

But $|S : C_S(s_i)|$ is the number of distinct conjugates of s_i in S , so $\sum |S : C_S(s_i)| = |S|$, and we have

$$|G| = \sum m_i \geq |G : S| \cdot |S| = |G|.$$

Thus we must have equality, and therefore $m_i = |G : C_S(s_i)|$ for each i .

To conclude this step, we use (15.26) once more, to obtain

$$\begin{aligned} (\tilde{\varphi}, \tilde{\psi})_G &= |G|^{-1} \sum_{i=1}^t |G : C_S(s_i)| \varphi(s_i) \psi(s_i^{-1}) \\ &= |S|^{-1} \sum_{i=1}^t |S : C_S(s_i)| \varphi(s_i) \psi(s_i^{-1}) = (\varphi, \psi)_S, \end{aligned}$$

as required.

Step 4. We can now complete the proof. Suppose $\varphi \in \text{Irr } S$. Then $\tilde{\varphi} \in \text{ch } KG$ by Step 2, and $(\tilde{\varphi}, \tilde{\varphi})_G = (\varphi, \varphi)_S = 1$ by Step 3. Therefore $\pm \tilde{\varphi} \in \text{Irr } G$, and since $\tilde{\varphi}(1) > 0$, we have $\tilde{\varphi} \in \text{Irr } G$ for all $\varphi \in \text{Irr } S$. Now define

$$N = \bigcap_{\varphi \in \text{Irr } S} \ker \tilde{\varphi}.$$

Then $N \trianglelefteq G$. If $s \in S \cap N$, then for all $\varphi \in \text{Irr } S$ we have $\varphi(s) = \tilde{\varphi}(s) = \tilde{\varphi}(1) = \varphi(1)$, so $s = 1$ by Exercise 9.5. Moreover, let p be any prime which divides $|G|$ but not $|S|$, and let P be a Sylow p -subgroup of G . Then for all $\varphi \in \text{Irr } S$ and all $u \in P$, we have

$$\tilde{\varphi}(u) = \tilde{\varphi}(1) = \varphi(1),$$

since $u \in \ker \tilde{\varphi}$, and hence $P \leq N$. It follows that $G = N \rtimes S$, completing the proof.

As a corollary, we give a second proof of Burnside's Transfer Theorem 13.20.

(15.27) Corollary. *Let S be a Sylow p -subgroup of a finite group G , such that S is contained in the center of its normalizer. Then G has a normal p -complement.*

Proof. If $H \leq G$ is a p -group, then H is conjugate to a subgroup of S , by the Sylow Theorems, so hypothesis (ii) of (15.25) is satisfied. In order to verify hypothesis (i), we must show that if s and t are elements of S which are conjugate in G , then they are conjugate in S , (and hence equal, because S is abelian). We have $s = t^x$ for some $x \in G$. Since S is abelian, we obtain $S \leq C_G(s)$, and $S^x \leq C_G(t^x) = C_G(s)$. By Sylow's Theorem, applied to $C_G(s)$, we have $S^{xz} = S$ for some $z \in C_G(s)$. Then $xz \in N_G(S)$, and by the hypothesis of the corollary, we have

$$t = t^{xz} = s^z = s,$$

completing the proof of (i). The corollary now follows from (15.25).

§15F. A Converse to Brauer's Theorem

In (15.8) we proved that $v(\mathcal{E}, G) = \text{ch}(KG)$, where $\mathcal{E} = \{H_i\}_{i \in I}$ is the set of elementary subgroups of G . This equality means that

$$(15.28) \quad \text{ch}(KG) = \sum_{i \in I} \{\text{ch}(KH_i)\}^G,$$

where $\{\text{ch}(KH_i)\}^G$ is the set of all virtual characters of G of the form φ^G , with $\varphi \in \text{ch}(KH_i)$. We shall prove a theorem of Green [55a], which asserts that for any family of subgroups $\mathcal{F} = \{F_j\}_{j \in J}$ such that $\text{ch}(KG) = \sum_j \{\text{ch}(KF_j)\}^G$, each elementary subgroup of G is contained in some conjugate of some subgroup F_j . Thus the family of elementary subgroups is, in this sense, the smallest family for which (15.28) holds.

(15.29) Lemma. *Let $R = \mathbb{Z}[\omega]$, where ω is a primitive $|G|$ -th root of 1, and let p be prime. Consider the p -elementary group $\langle x \rangle P$, where x is a p' -element of G and P a Sylow p -subgroup of $C_G(x)$. Let H be a subgroup of G which does not contain any conjugate of $\langle x \rangle P$, and let $\psi \in \text{ch}_K(H)$ have values in R . Then*

$$\psi^G(x) \in pR.$$

Proof. Let \mathfrak{C} be the conjugacy class of G containing x . From Exercise 10.5, we have

$$\psi^G(x) = \frac{|C_G(x)|}{|H|} \sum_{y \in \mathfrak{C} \cap H} \psi(y).$$

Let $\{\mathfrak{D}_1, \dots, \mathfrak{D}_t\}$ be the distinct H -conjugacy classes contained in $\mathfrak{C} \cap H$ (this

intersection may be empty!), and let $h_i \in \mathfrak{D}_i$, $1 \leq i \leq t$. The number of conjugates of h_i in H equals

$$|\mathfrak{D}_i| = |H : H \cap C_G(h_i)|.$$

Therefore

$$\psi^G(x) = \frac{|C_G(x)|}{|H|} \sum_{i=1}^t |\mathfrak{D}_i| \psi(h_i) = \sum_{i=1}^t a_i \psi(h_i),$$

where

$$a_i = |C_G(h_i)| / |H \cap C_G(h_i)|, \quad 1 \leq i \leq t.$$

(We have used the fact that each h_i is G -conjugate to x .) Thus each $a_i \in \mathbb{Z}$, and we need only show that p divides each a_i .

Suppose that $p \nmid a_i$ for some i , and let $x = h_i^z$, $z \in G$. Since $p \nmid a_i$, $|C_G(h_i)|$ and $|H \cap C_G(h_i)|$ have the same p -part, so a Sylow p -subgroup P_i of $H \cap C_G(h_i)$ is also a Sylow p -subgroup of $C_G(h_i)$. We have $\langle h_i \rangle P_i \leq H$, and $h_i^z = x$, $\langle h_i \rangle^z = \langle x \rangle$; further, P_i^z is a Sylow p -subgroup of $C_G(h_i^z)$, hence of $C_G(x)$. But P is also a Sylow p -subgroup of $C_G(x)$, hence is conjugate to P_i^z in $C_G(x)$. Therefore $\langle x \rangle P_i^z$ and $\langle x \rangle P$ are conjugate. But

$$\{\langle h_i \rangle P_i\}^z = \langle x \rangle P_i^z,$$

so H contains a conjugate of $\langle x \rangle P$. This is contrary to our hypotheses, and so each a_i is a multiple of p . Hence $\psi^G(x) \in pR$, as claimed.

(15.30) Theorem (Green). *Let \mathcal{F} be a family of subgroups of G such that $v(\mathcal{F}, G) = \text{ch}(KG)$. Then each elementary subgroup of G is contained in some conjugate of some subgroup belonging to \mathcal{F} .*

Proof. Let $\langle x \rangle P$ be a p -elementary subgroup of G , for a p' -element x and a p -group P . If $\langle x \rangle P$ is contained in no conjugate of a subgroup belonging to \mathcal{F} , then the preceding lemma implies that $\varphi(x) \in pR$ for all $\varphi \in v(\mathcal{F}, G)$. In particular, this would imply $1_G(x) \in pR$, which is impossible, and the theorem is proved.

For further reading, see Lorenz [75].

§15G. The Aramata-Brauer Induction Theorem

We prove next the Aramata-Brauer Theorem, discovered originally by Aramata [31], [33], and proved independently at a later date by Brauer [47a]. Both authors used this theorem to prove that if E is a finite Galois extension

of an algebraic number field K , then the Dedekind zeta function $\zeta_K(s)$ is a divisor of $\zeta_E(s)$. Using this result, together with earlier work by Landau and Siegel, Brauer obtained the following remarkable consequence:

Let K range over all algebraic number fields of a fixed degree n . Let d be the discriminant of K (over Q), h the ideal class number of K , and R the regulator of K . Then as $|d| \rightarrow \infty$.

$$\log hR \sim \frac{1}{2} \log |d|.$$

Let us now prove the Aramata-Brauer Theorem. We shall use the notation in (9.25), and work throughout with complex characters.

(15.31) Theorem. *Let G be a finite group of order n , where $n > 1$, and let ρ be the regular character of G . Then there exist nontrivial linear characters ω_i of cyclic subgroups of G , such that*

$$\rho - 1 = \sum_i a_i (\omega_i)^G$$

with each a_i a positive rational number with denominator n .

Remark. Artin's Theorem 15.4 guarantees that $\rho - 1$ is expressible as above with rational coefficients $\{a_i\}$. The significance of the present theorem is the fact that these $\{a_i\}$ may be chosen positive.

Proof. Let C be a nontrivial cyclic subgroup of G of order m , and let x range over all $\varphi(m)$ generators of C . Put $\text{Irr}(C) = \{\psi^1, \dots, \psi^m\}$, where $\psi^1 = 1$, and define

$$u_i = \varphi(m) - \sum_x \psi^i(x), \quad 1 \leq i \leq m.$$

Let us write $C = \langle c \rangle$, $\psi^i(c) = \omega = m\text{-th root of } 1$. Then $x = c^r$, where r ranges between 1 and m , and $(r, m) = 1$. We have $\psi^i(x) = \omega^r$, so $\sum_x \psi^i(x)$ is unchanged by all automorphisms of $Q(\omega)$ over Q . Thus each $u_i \in Q$, and since u_i is an algebraic integer, we have $u_i \in Z$. Further, $|\psi^i(x)| = 1$ for each s , so $u_i > 0$ for $i \neq 1$. Clearly $u_1 = 0$. We obtain at once from the orthogonality relations, for $y \in C$,

$$\sum_{i=1}^m u_i \overline{\psi^i(y)} = \begin{cases} m\varphi(m) & \text{for } y = 1, \\ 0 & \text{for } y \neq 1 \text{ and } C \neq \langle y \rangle, \\ -m & \text{if } C = \langle y \rangle. \end{cases}$$

Taking complex conjugates, we obtain exactly the same formulas for $\sum u_i \psi^i(y)$.

Now let $\text{Irr}(G) = \{\xi^1, \dots, \xi^s\}$, $\xi^1 = 1$, $z_i = \xi^i(1)$, so $\rho - 1 = \sum_{i>1} z_i \xi^i$. By §9C we have for each i ,

$$\xi^i|_C = \sum_{j=1}^m h_{ij} \psi^j, \text{ where } h_{ij} = (\psi^j, \xi^i)_C \text{ for } 1 \leq j \leq m.$$

The $\{h_{ij}\}$ are nonnegative integers, and h_{ij} is the multiplicity of ψ^j in $\xi^i|_C$. By Frobenius Reciprocity, we obtain

$$(\psi^j)^G = \sum_{i=1}^s h_{ij} \xi^i = \sum_{i=1}^s (\psi^j, \xi^i)_C \xi^i.$$

For each C as above, set

$$\begin{aligned} S(C) &= \sum_{j=1}^m u_j (\psi^j)^G = \sum_{i,j} u_j (\psi^j, \xi^i)_C \xi^i \\ &= \sum_i \left(\sum_j u_j \psi^j, \xi^i \right)_C \xi^i. \end{aligned}$$

Since the values of $\sum_j u_j \psi^j$ on C have already been calculated above, we find easily that

$$S(C) = \sum_{i=2}^s \left(z_i \varphi(m) - \sum_x \xi^i(x) \right) \xi^i,$$

where x ranges over all generators of C .

We sum the above equality over all nontrivial cyclic subgroups C of G . Then x ranges over $G - \{1\}$, so

$$\sum_C \sum_x \xi^i(x) = -\xi^i(1) = -z_i.$$

Further, $\sum_C \varphi(m) = n - 1$, and therefore we obtain

$$\sum_C S(C) = \sum_{i=2}^s \{z_i(n-1) + z_i\} \xi^i = \sum_{i=2}^s n z_i \xi^i = n(\rho - 1).$$

Therefore

$$\rho - 1 = n^{-1} \sum_C S(C) = \sum_C \sum_j (u_j/n) (\psi^j)^G.$$

This gives the desired result, since for each C , the coefficient u_1/n of $(\psi^1)^G$ is zero.

§15. Exercises

1. Let $H = C \times P$ be a p -elementary group, where C is a cyclic p' -group, and P a p -group. Prove that H is nilpotent, and that each subgroup of H is p -elementary. Prove also that C is the set of all p' -elements in H , and that P is the set of all p -elements in H .
2. Prove that subgroups of hyper-elementary groups are hyper-elementary.
3. Let M be a $\mathbb{Q}G$ -module, with character μ . Let $x, y \in G$, and assume $\langle x \rangle =_G \langle y \rangle$. Prove that $\mu(x) = \mu(y)$. (See (14.8)).

[Hint: Since μ is a class function, we may assume that $\langle x \rangle = \langle y \rangle$. Then $y = x^a$, for some integer a relatively prime to n , where n is the order of x . Let $\{\xi_i\}$ be the eigenvalues of $\mathbf{M}(x)$; then each $\{\xi_i\}$ is an n -th root of 1, and we have

$$\mu(x) = \sum \xi_i, \quad \mu(y) = \sum \xi_i^a.$$

Let ω be a primitive n -th root of 1. Show that there exists a \mathbb{Q} -automorphism σ of the field $\mathbb{Q}(\omega)$ such that $\sigma(\omega) = \omega^a$, and deduce that $\sigma(\mu(x)) = \mu(y)$. See also §21.]

4. Let $\{C_1, \dots, C_m\}$ be a full set of non-conjugate cyclic subgroups of a finite group G . From the Artin Induction Theorem, it follows that every rational character φ of G can be expressed in the form

$$\varphi = \sum_{i=1}^m \frac{a_i}{|G|} (1_{C_i})^G, \quad a_i \in \mathbb{Z}.$$

Prove that the number of isomorphism classes of simple $\mathbb{Q}G$ -modules is m .

[Hint: Use Exercise 3 to show that each rational character μ is determined by its values on generators of C_1, \dots, C_m , so there are at most m non-isomorphic simple $\mathbb{Q}G$ -modules. On the other hand, for each cyclic subgroup C of G , let

$$t_C = \sum_{C' \leq C} \frac{1}{|C:C'|} \mu(|C:C'|)(1_{C'})^C.$$

Using the proof of Artin's Theorem, show that for each $x \in C$,

$$t_C(x) = \begin{cases} 1, & C = \langle x \rangle, \\ 0, & \text{otherwise.} \end{cases}$$

Then show that $\{t_{C_1}^G, \dots, t_{C_m}^G\}$ are linearly independent. (See also Theorem 21.5).]

5. Let $P(G)$ be the set of \mathbb{Z} -linear combinations of induced characters $\{1_H^G : H \leq G\}$. As in §15B, let $P(\mathcal{H}, G)$ be the set of \mathbb{Z} -linear combinations of induced characters $\{1_H^G : H \in \mathcal{H}\}$, where \mathcal{H} is the family of hyper-elementary groups. Prove that $P(G)$ is a ring under pointwise addition and multiplication. Then prove that $P(G) = P(\mathcal{H}, G)$.

[Hint: First prove that $P(\mathcal{H}, G)$ is an ideal in $P(G)$, and then use (15.10).]

6. Let A be any f.d. semisimple K -algebra, let E be an extension field of K , and suppose that

$$V \oplus X^E \cong Y^E,$$

where V is an A^E -module, and X, Y are A -modules. Show that $V \cong W^E$ for some A -module W .

[Hint: Write $X = X_0 \oplus U$, $Y = Y_0 \oplus U$, where X_0 and Y_0 have no common direct summand. Then

$$V \oplus X_0^E \cong Y_0^E, \text{ and } \text{Hom}_A(Y_0, X_0) = 0.$$

Therefore $\text{Hom}(Y_0^E, X_0^E) = 0$, so $V \cong Y_0^E$.]

7. Keeping the above notation, assume that $\dim_K E$ is finite, but drop the hypothesis that A be semisimple. Prove the result in this case.

[Hint: We now have $V \oplus X_0^E \cong Y_0^E$, where X_0 and Y_0 have no common indecomposable direct summand. If $\dim_K E = n$, then

$$V|_A \oplus X_0^{(n)} \cong Y_0^{(n)}$$

which contradicts the K-S-A Theorem unless $X_0 = 0$.]

Introduction to Modular Representations

This chapter contains an introduction to Brauer's theory of modular representations, to be followed in Chapter 9 by an account of the theory of blocks. Let G be a finite group, and p a rational prime number dividing the order of G . The p -local structure of G is the family of p -subgroups of G , together with their normalizers. The p -local structures of G , for various primes p , determine the structure of G to a considerable extent, and have played a central role in the problem of classifying finite simple groups.

A main objective of Brauer's theory has been to relate the character theory of G over the complex field to the p -local structures of G for primes p dividing $|G|$. The theory began with Brauer's work on representations of a finite group G over a modular field k of characteristic p . In its present form, it is the study of the representation theories of G over three rings R , K , and k , and their interrelationships. Here, the ring R is a discrete valuation ring (d.v.r.) with quotient field K , maximal ideal \mathfrak{p} and residue class field $k=R/\mathfrak{p}$ of characteristic p . Given an RG -lattice M , we form the KG -module $KM=K\otimes_R M$, and the kG -module $\bar{M}=M/\mathfrak{p}M$, and study the connections among M , KM , and \bar{M} . The most important situation is that where K is an algebraic number field which is a splitting field for G . We can then relate KG -modules and their characters to the structure of RG -lattices and kG -modules, and to the p -local structure of G .

The study of RG -lattices and kG -modules offers many new challenges. The behavior of RG -lattices, studied in this chapter by the methods of Brauer and Green, provides a useful introduction to the general theory of integral representations, to be considered in greater detail in Chapters 3 and 4. On the other hand, since kG -modules need not be semisimple, the machinery of semisimple rings and modules cannot be applied directly to the investigation of kG -modules. Instead, we shall use the theory of artinian rings with radical, and our results will often be stated in terms of Grothendieck groups and Brauer characters.

§16. THE DECOMPOSITION MAP

We begin in §16A with a glossary of notation and terminology, to be in force throughout the entire chapter. In §16B we give a brief introduction to Grothendieck groups; these will be studied more extensively in Chapter 10. Finally, and most important, §16C gives the definition and elementary properties of the decomposition map, which assigns to each RG -lattice M the kG -module $\bar{M} = M/\mathfrak{p}M$, and induces a homomorphism $G_0(KG) \rightarrow G_0(kG)$ of Grothendieck groups.

§16A. Notation and Terminology

All modules are assumed to be finitely generated, unless specifically stated otherwise. Let p be 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 . (Here, π is a prime element of the d.v.r. R .) Usually K will be assumed to have characteristic 0, but we shall not impose this restriction in advance.

For example, a p -modular system arises from an algebraic number field K by choosing some non-archimedean \mathfrak{p} -adic valuation on K , and letting R be its valuation ring, and k the residue class field R/\mathfrak{p} . We may also choose K to be the \mathfrak{p} -adic completion of such an algebraic number field, and then its valuation ring R is complete in the \mathfrak{p} -adic topology (see §4C).

Throughout this section, G denotes a finite group of order $|G|$. As in §10D, an RG -lattice is a left RG -module having a finite free R -basis. (Note that since R is a P.I.D., every f.g. projective R -module is necessarily R -free.) For each RG -lattice M , we set

$$\bar{M} = M/\mathfrak{p}M,$$

so \bar{M} is a f.g. kG -module. Let bars denote “reduction mod \mathfrak{p} ”, so the element $m \in M$ maps onto the element $\bar{m} \in \bar{M}$ under the natural map $M \rightarrow \bar{M}$. Likewise, we shall occasionally write

$$\bar{R} = R/\mathfrak{p} = k,$$

and denote the image of $a \in R$, under the natural map $R \rightarrow \bar{R}$, by \bar{a} . Further (see §4D), we identify the RG -lattice M with its image $1 \otimes M$ in $K \otimes_R M$, so that $K \otimes_R M$ can be written in abbreviated form as KM , and viewed as the set of K -linear combinations of the elements of M .

An element $x \in G$ is called p -regular if its order is a p' -number (that is, its order is relatively prime to p), and p -irregular otherwise. Sometimes we will call a p -regular element a p' -element of G . We call $x \in G$ a p -element if the order of x is a power of p . The identity element 1_G is the only p -element which is p -regular. As we have seen in §1B, every $x \in G$ is uniquely expressible in the

form

$$x = x'x'', \text{ with } x' \text{ } p\text{-regular, } x'' \text{ a } p\text{-element, and } x'x'' = x''x'.$$

We call x' the *p-regular part* of x , and x'' the *p-part* of x . Finally, let

$$G_{p'} = \{\text{all } p\text{-regular elements of } G\}.$$

§16B. Grothendieck Groups

Let A be an arbitrary ring, and let \mathcal{C} be some category of left A -modules. A *short exact sequence* (ses) is an exact sequence of A -modules

$$(16.1) \quad 0 \rightarrow L \rightarrow M \rightarrow N \rightarrow 0.$$

If each module belongs to \mathcal{C} , we call (16.1) a ses from \mathcal{C} . We assume always that $0 \in \mathcal{C}$, and that if $M, M' \in \mathcal{C}$ then also $M \oplus M' \in \mathcal{C}$. We assume further that the collection of isomorphism classes of modules in \mathcal{C} forms a set. For example, \mathcal{C} may be chosen as one of the following categories:

$${}_A\mathfrak{M} = \text{category of all left } A\text{-modules,}$$

$${}_A\text{mod} = \text{category of all f.g. left } A\text{-modules,}$$

$$\mathcal{P}(A) = \text{category of all f.g. projective left } A\text{-modules.}$$

In considering invariants of modules, one often constructs a map $h: \mathcal{C} \rightarrow T$, which assigns to each module $M \in \mathcal{C}$ an element $h(M)$ in some fixed abelian group T . The map h is usually additive on ses's from \mathcal{C} , that is,

$$(16.2) \quad h(M) = h(L) + h(N)$$

for each ses (16.1) from \mathcal{C} . In particular, this implies that $h(M)$ depends only upon the isomorphism class of the module M . For example, let \mathcal{C} be the category of all f.g. CG -modules, and for each $M \in \mathcal{C}$, let $h(M)$ be the character μ afforded by M . Then h maps \mathcal{C} into the additive group $\text{ch}CG$ of virtual characters of G . Clearly h is additive on ses's from \mathcal{C} in this case.

Returning to the general case, let $h: \mathcal{C} \rightarrow T$ be a map which is additive on ses's from \mathcal{C} . We wish to extend h so as to obtain an additive homomorphism into T . Grothendieck groups provide the framework for such extensions. We may think of this procedure as generalizing the passage from ordinary characters to virtual characters.

(16.3) Definition. Let \mathcal{C} be a category of A -modules. Let \mathbf{F} be the free abelian group generated by symbols (M) , one for each isomorphism class of modules M in \mathcal{C} . Let \mathbf{F}_0 be the subgroup of \mathbf{F} generated by all expressions

$$(M) - (L) - (N)$$

arising from all ses's (16.1) in \mathcal{C} . The *Grothendieck group* $K_0(\mathcal{C})$ of the category \mathcal{C} is defined by

$$K_0(\mathcal{C}) = \mathbf{F}/\mathbf{F}_0,$$

an abelian additive group. For $M \in \mathcal{C}$, let $[M]$ denote its image in $K_0(\mathcal{C})$.

Each $x \in K_0(\mathcal{C})$ is expressible as a difference $[M] - [N]$ with $M, N \in \mathcal{C}$, though not in a unique manner. Furthermore, it may occur that $x = 0$ even though M is not isomorphic to N .

From the definition of $K_0(\mathcal{C})$, we have at once:

(16.4) Proposition. *Let T be some fixed abelian group, and let $h: \mathcal{C} \rightarrow T$ be a map which is additive on ses's from \mathcal{C} . Then there is a uniquely determined well defined additive homomorphism*

$$g: K_0(\mathcal{C}) \rightarrow T$$

which extends h , and is given by the formula

$$g([M] - [N]) = h(M) - h(N) \text{ for all } M, N \in \mathcal{C}.$$

We postpone until Chapter 10 a more thorough investigation of such Grothendieck groups, and concentrate here on those cases needed in our discussion of modular representation theory.

(16.5) Definition. The *Grothendieck group* $G_0(A)$ of the ring A is defined by

$$G_0(A) = K_0(A\text{-mod}).$$

Thus, $G_0(A)$ is 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 $0 \rightarrow M' \rightarrow M \rightarrow M'' \rightarrow 0$ of f.g. left A -modules.

The *projective class group* $K_0(A)$ of the ring A is defined by

$$K_0(A) = K_0(\mathcal{P}(A)).$$

Thus, $K_0(A)$ is generated by expressions $[P]$, one for each isomorphism class (P) of f.g. projective left A -modules P , with relations

$$[P \oplus P'] = [P] + [P'] \text{ for all } P, P' \in \mathcal{P}(A).$$

(Note that each ses $0 \rightarrow P' \rightarrow P \rightarrow P'' \rightarrow 0$ of modules from $\mathcal{P}(A)$ must split, because P'' is A -projective. Hence, the defining relations for $K_0(A)$ can be expressed in the simpler form involving direct sums, rather than exact sequences from $\mathcal{P}(A)$.)

Given a p -modular system (K, R, k) and a finite group G , we shall be concerned mainly with the Grothendieck groups $G_0(KG)$ and $G_0(kG)$, and with the projective class groups $K_0(RG)$ and $K_0(kG)$. It should be remarked that each module $P \in \mathcal{P}(RG)$ is necessarily a f.g. projective R -module, and is therefore an RG -lattice. Of course, not every RG -lattice need be RG -projective.

We shall show below that if $\text{char } K = 0$, then $G_0(KG)$ is our old friend $\text{ch } KG$, the ring of virtual characters of KG -modules. As a first step in this direction, we prove

(16.6) Proposition. *Let A be a left artinian ring, and let $\{V_1, \dots, V_s\}$ be a basic set of simple left A -modules. Then*

$$G_0(A) = \bigoplus_{i=1}^s \mathbf{Z}[V_i],$$

a free abelian group with basis $\{[V_1], \dots, [V_s]\}$.

Proof. (All modules are assumed to be f.g. left A -modules.) Each A -module U has a composition series

$$U = U_0 \supset U_1 \supset \cdots \supset U_{t+1} = 0,$$

and the composition factors $\{U_j/U_{j+1}\}$ are simple A -modules. Since the sequence

$$0 \rightarrow U_{j+1} \rightarrow U_j \rightarrow U_j/U_{j+1} \rightarrow 0$$

is exact for each j , it follows from the definition of $G_0(A)$ that

$$[U] = \sum_{j=0}^t [U_j/U_{j+1}] \text{ in } G_0(A).$$

Hence we may write

$$[U] = \sum_{i=1}^s r_i(U)[V_i] \text{ in } G_0(A),$$

where for each i , $r_i(U)$ is the multiplicity of V_i as composition factor of U . Note that $r_i(U)$ is well-defined, by the Jordan-Hölder Theorem. Clearly, r_i is additive on ses's of A -modules. Thus by (16.4) there is a well-defined additive homomorphism*

$$g : G_0(A) \rightarrow \mathbf{Z}^{(s)},$$

given by

$$g[U] = (r_1(U), \dots, r_s(U)), \quad U = A\text{-module}.$$

It is clear that g is surjective.

* $\mathbf{Z}^{(n)}$ denotes the free abelian group on n generators.

On the other hand, there is an obvious homomorphism $f: \mathbf{Z}^{(s)} \rightarrow G_0(A)$, defined by

$$f(r_1, \dots, r_s) = \sum r_i [V_i], \quad r_i \in \mathbf{Z}.$$

We have $gf=1$, so f and g are isomorphisms, and are inverses of one another. This completes the proof that $[V_1], \dots, [V_s]$ form a free \mathbf{Z} -basis of $G_0(A)$. An analogous argument will be used in the proof of Proposition 16.7 below.

Our next task is to determine the additive structure of $K_0(A)$ for the case where A is a semiperfect ring. Recall from §6C that the ring A is *semiperfect* if it has the following two properties:

- (i) $A/\text{rad } A$ is a semisimple artinian ring.
- (ii) Every idempotent in $A/\text{rad } A$ can be lifted to an idempotent in A .

The semiperfect rings with which we shall be mainly concerned are the rings RG and kG , where (K, R, k) is a p -modular system. We proved in §6 that RG is semiperfect provided that R is complete in the \wp -adic topology, and that kG is semiperfect for an arbitrary field k . We should remark that RG is also semiperfect whenever K is a splitting field for G , whether or not the d.v.r. R is complete; this follows at once from (5.22) and Exercise 6.16.

(16.7) Proposition. *Let A be a semiperfect ring, and let $\{P_1, \dots, P_r\}$ be a basic* set of f.g. indecomposable projective left A -modules. Then*

$$K_0(A) = \bigoplus_{i=1}^r \mathbf{Z}[P_i],$$

a free abelian group with basis $\{[P_1], \dots, [P_r]\}$.

Proof. All modules considered here are assumed f.g. For the purposes of this proof, let $\bar{A}=A/N$, where $N=\text{rad } A$. In §6C (see especially (6.25)) we proved that the isomorphism classes of projective left A -modules P correspond bijectively to the classes of projective \bar{A} -modules, the correspondence being given by $P \leftrightarrow P/NP$. The indecomposable projective A -modules then correspond to the simple \bar{A} -modules. Since each \bar{A} -module is expressible as a finite direct sum of simple \bar{A} -modules with uniquely determined multiplicities, it follows that each projective A -module P can be expressed as a direct sum

$$P \cong \coprod_{i=1}^r (P_i)^{(n_i)}$$

with uniquely determined multiplicities $\{n_i\}$. It follows as in the proof of

*This means that every f.g. indecomposable projective left A -module is isomorphic to exactly one of the $\{P_i\}$.

(16.6) that there is a well defined additive map $g: K_0(A) \rightarrow \mathbf{Z}^{(r)}$, given by

$$g[P] = (n_1, \dots, n_r).$$

Then g is surjective, and is an isomorphism because it has an inverse f given by

$$f(n_1, \dots, n_r) = \sum_{i=1}^r n_i [P_i], n_i \in \mathbf{Z}.$$

This completes the proof.

Remark. The vital point of the preceding proof is that the K-S-A Theorem is valid for f.g. projective modules over a semiperfect ring A . The hypothesis that A be semiperfect was needed only to insure the validity of this theorem. Thus, the assertions in (16.7) remain true for any ring A , semiperfect or not, as long as the K-S-A Theorem holds for f.g. projective A -modules.

Now let K be an arbitrary field, G a finite group, and let us show that the Grothendieck group $G_0(KG)$ can be made into a commutative ring, with multiplication corresponding to (inner) tensor products of KG -modules. For M and N a pair of f.g. left KG -modules, let $M \otimes_K N$ be their usual inner tensor product, which is again a KG -module. We intend to define multiplication in $G_0(KG)$ by starting with the formula

$$(16.8) \quad [M][N] = [M \otimes_K N],$$

and then extending the definition in an obvious manner to products of the form $(\sum a_i[M_i])(\sum b_j[N_j])$, $a_i, b_j \in \mathbf{Z}$. The difficulty lies in showing that multiplication is then well defined. We may overcome this difficulty as follows. As in Definition 16.5, we may write

$$G_0(KG) = \mathbf{F}/\mathbf{F}_0,$$

where \mathbf{F} is the free abelian group generated by symbols (M) , one for each isomorphism class of f.g. KG -modules M , and \mathbf{F}_0 is the subgroup of \mathbf{F} generated by all expressions

$$(M) - (L) - (N)$$

arising from ses's

$$0 \rightarrow L \rightarrow M \rightarrow N \rightarrow 0$$

of f.g. KG -modules. Since \mathbf{F} is a free abelian group, we may define multiplication in \mathbf{F} unambiguously by specifying how its generators multiply. Specifically, we put

$$(16.9) \quad (M)(N) = (M \otimes_K N)$$

for each pair of KG -modules M and N . Then \mathbf{F} becomes a commutative associative ring with identity element. To insure that this multiplication carries over to $G_0(KG)$, it suffices to verify that \mathbf{F}_0 is an *ideal* of \mathbf{F} . Now let (16.1) be an exact sequence of KG -modules; it is obviously split as a sequence of K -modules. But then for any KG -module X , the sequence of KG -modules

$$0 \rightarrow X \otimes_K L \rightarrow X \otimes_K M \rightarrow X \otimes_K N \rightarrow 0$$

is exact (and split over K). Therefore

$$(X)\{(M)-(L)-(N)\} = (X \otimes M) - (X \otimes L) - (X \otimes N) \text{ in } \mathbf{F},$$

which lies in \mathbf{F}_0 , so \mathbf{F}_0 is an ideal in \mathbf{F} . Therefore $G_0(KG)$ is indeed a commutative ring with identity element. Notice that (16.8) automatically holds true in $G_0(KG)$, by virtue of formula (16.9) used to make F into a ring.

We are now ready to establish the connection between our Grothendieck ring $G_0(KG)$ and the ring of virtual characters $\text{ch } KG$ defined in §9C.

(16.10) Proposition. *Let K be a field of characteristic 0, and G a finite group. Then there is an isomorphism of rings*

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

obtained by assigning to each f.g. KG -module M the character μ of G afforded by M .

Proof. Define $\psi: G_0(KG) \rightarrow \text{ch } KG$ by $\psi[M] = \mu$. Since ψ is additive on ses's of KG -modules, it is clear from (16.4) that ψ is well defined on $G_0(KG)$. Since $G_0(KG)$ is Z -free on the simple KG -modules by (16.6), while $\text{ch } KG$ is Z -free on the irreducible K -characters of G , it is clear that ψ is an isomorphism of additive groups. Moreover, if N is a KG -module with character ν , then $M \otimes_K N$ affords the character $\mu\nu$. This implies at once that ψ is a ring isomorphism, as claimed.

For a p -modular system (K, R, k) and a finite group G , we expect the Grothendieck ring $G_0(kG)$ to serve as an object of investigation, rather than the character ring $\text{ch } kG$. Indeed, a kG -module is *never* uniquely determined by its character. In addition, we shall be using the projective class group $K_0(RG)$, which also has a ring structure, as we shall see later on.

§16C. Reduction mod \mathfrak{p} and the Decomposition Map

Let (K, R, k) be a p -modular system, and G any finite group. Thus R is a d.v.r. with quotient field K , maximal ideal \mathfrak{p} , and residue class field k of characteristic p . We shall obtain the first of several important connections

among KG -modules, RG -modules, and kG -modules. The construction begins with a left KG -module V . We shall show that V contains a full left RG -lattice M . Then $\bar{M} = M/\mathfrak{p}M$ is a kG -module, which we shall say is obtained from M by “reduction mod \mathfrak{p} ”. For a fixed KG -module V , there are in general many choices for the full RG -lattice M in V , and the KG -modules \bar{M} thus obtained need not be isomorphic to one another. Nevertheless, we shall prove that the above construction yields a well-defined homomorphism $G_0(KG) \rightarrow G_0(kG)$, called the *decomposition homomorphism*. This observation is the starting point of the theory of modular representations. In later sections, we shall interpret the decomposition map in terms of Brauer characters, and relate it to $K_0(RG)$ and $K_0(kG)$.

As in §10D and §16A, an RG -lattice is a left RG -module having a finite free R -basis. Since R is a P.I.D., the structure theorem for R -modules shows that a f.g. RG -module M is an RG -lattice if and only if M is R -torsionfree. Therefore, submodules of RG -lattices are necessarily sublattices.

(16.11) Definition. Let V be a f.g. left KG -module. A *full RG-lattice* M in V is an RG -lattice M contained in V , such that $KM = V$.

We remark that for each full RG -lattice M in V , we have

$$K \otimes_R M \cong KM$$

as KG -modules. Indeed, the obvious surjection $K \otimes_R M \rightarrow KM$ is a KG -homomorphism. On the other hand, it is a K -isomorphism because of the fact that M is R -torsionfree. For further discussion of this matter, see §4D and (23.13).

(16.12) Lemma. Let V be any f.g. left KG -module. An RG -submodule M of V is a full RG -lattice in V if and only if M satisfies the conditions:

- (i) M has a finite R -basis, and
- (ii) $KM = V$.

Proof. If M is a full RG -lattice in V , then (i) and (ii) clearly hold. Conversely, if M is an RG -submodule of V satisfying (i), then M is an RG -lattice, and (ii) shows that M is full in V .

We remark that if M is a full RG -lattice in V , then for each R -basis $\{m_1, \dots, m_d\}$ of M , the elements $\{1 \otimes m_1, \dots, 1 \otimes m_d\}$ form a K -basis of $K \otimes_R M$. After the usual identification of M with $1 \otimes M$, we may conclude:

(16.13) Corollary. If M is a full RG -lattice in V , then every R -basis of M is also a K -basis of V .

Since equivalence (over K) of K -representations of G is the result of change of K -basis in a KG -module, the following remark is an immediate consequence of (16.13) (see also (23.16)):

(16.14) Corollary. *Every K -representation of G is equivalent (over K) to an R -representation of G , that is, a representation by matrices with entries in R .*

If R is an arbitrary Dedekind domain with quotient field K , rather than a d.v.r., then it is not necessarily true that every K -representation of G is K -equivalent to an R -representation (see §23 for a full discussion of this situation). Another subtlety is that two R -representations of G which are K -equivalent need not be R -equivalent (see Exercise 16.3 and §23).

We now turn to the question of *existence* of full RG -lattices in KG -modules. For the rest of the section, (K, R, k) continues to denote a p -modular system. The next result is a special case of a general statement about R -orders in K -algebras (see (23.15)).

(16.15) Proposition. *Every f.g. left KG -module V contains full RG -lattices.*

Proof. We have $V = \sum_{i=1}^d Kv_i$ for some K -basis $\{v_i\}$ of V . Put

$$M = \sum_{i=1}^d RGv_i.$$

Then M is f.g./ R , and is R -torsionfree, hence is an RG -lattice in V . Clearly $KM = V$, so M is a full RG -lattice, as required.

Now let $a \mapsto \bar{a}$, $a \in R$, denote the natural map $R \rightarrow R/\mathfrak{p} = k$. Let M be a full RG -lattice in a KG -module V . Then $\bar{M} = M/\mathfrak{p}M$ is an RG -module annihilated by \mathfrak{p} , and hence can be made into a kG -module, with the action of kG given by

$$\left(\sum_{x \in G} \bar{a}_x x \right) \bar{m} = \sum_{x \in G} \overline{a_x x m}, \quad a_x \in R, m \in M.$$

We call \bar{M} the kG -module obtained from M by *reduction mod \mathfrak{p}* .

This construction can be reformulated in various ways. First, every K -representation of G is equivalent to an R -representation of G , by (16.14). Let $\mathbf{T}: G \rightarrow GL_d(R)$ be an R -representation of G , given by

$$\mathbf{T}(x) = (a_{ij}(x)), \quad a_{ij}(x) \in R, \quad x \in G.$$

Then define $\bar{\mathbf{T}}: G \rightarrow GL_d(k)$ by

$$\bar{\mathbf{T}}(x) = (\overline{a_{ij}(x)}), \quad x \in G.$$

Clearly $\bar{\mathbf{T}}$ is a k -representation of G . If \mathbf{T} is the R -representation of G afforded by a full RG -lattice M in V , with respect to an R -basis $\{m_1, \dots, m_d\}$ of M , then $\{\bar{m}_1, \dots, \bar{m}_d\}$ is a k -basis of \bar{M} , and $\bar{\mathbf{T}}$ is the k -representation of G afforded by \bar{M} with respect to the basis $\{\bar{m}_1, \dots, \bar{m}_d\}$.

A second interpretation of \bar{M} is given by the formula

$$\bar{M} \cong k \otimes_R M.$$

To prove this, we apply $* \otimes M$ to the exact sequence

$$0 \rightarrow \mathfrak{p} \rightarrow R \rightarrow k \rightarrow 0,$$

so we obtain an exact sequence

$$\mathfrak{p} \otimes M \rightarrow R \otimes M \rightarrow k \otimes M \rightarrow 0,$$

where \otimes means \otimes_R . Identifying $R \otimes M$ with M , the image of $\mathfrak{p} \otimes M$ is identified with $\mathfrak{p}M$, and we have $M/\mathfrak{p}M \cong k \otimes M$, as claimed.

As we pointed out at the beginning of the subsection, two full RG -lattices M and N in V may yield non-isomorphic kG -modules \bar{M} and \bar{N} . Some order is restored to the situation, however, if we work with Grothendieck groups. We remark that two matrix-theoretic proofs of the next result, due to Brauer-Nesbitt [37], are given in CR §82.

(16.16) Proposition. *Let M and N be a pair of full RG -lattices in a KG -module V . Then $[\bar{M}] = [\bar{N}]$ in $G_0(kG)$, or equivalently, the kG -modules \bar{M} and \bar{N} have the same composition factors.*

Proof. By Lemma 16.12, the sum $M+N$ is a full RG -lattice in V containing both M and N . Therefore it is sufficient to prove the result for full RG -lattices L and M in V such that $L \subseteq M$. We may further assume, because M is a noetherian RG -module, that L is a maximal submodule of M . We claim that $\mathfrak{p}M \subseteq L$. Otherwise, $L + \mathfrak{p}M$ is an RG -lattice in M properly containing L , so that $L + \mathfrak{p}M = M$ by maximality of L . This implies that $L = M$, by Nakayama's Lemma 5.7, contrary to assumption. Thus $\mathfrak{p}M \subseteq L$, and we have

$$\mathfrak{p}L \subseteq \mathfrak{p}M \subseteq L \subseteq M.$$

Now by (16.6), $[\bar{L}] = [\bar{M}]$ in $G_0(kG)$ if and only if \bar{L} and \bar{M} have the same composition factors, so we have to prove that the composition factors of $M/\mathfrak{p}M$ and $L/\mathfrak{p}L$ are the same (up to order of occurrence). These kG -modules have the composition factors of $L/\mathfrak{p}M$ in common, so it suffices to prove that M/L and $\mathfrak{p}M/\mathfrak{p}L$ have the same composition factors. But \mathfrak{p} is a principal ideal πR , so that $\mathfrak{p}M = \pi M$, $\mathfrak{p}L = \pi L$, and

$$\mathfrak{p}M/\mathfrak{p}L = \pi M/\pi L.$$

Hence $M/L \cong \mathfrak{p}M/\mathfrak{p}L$ as RG -modules, with the isomorphism given by multiplication by π . Thus the kG -modules $\mathfrak{p}M/\mathfrak{p}L$ and M/L are isomorphic over kG , and the proof is complete.

(16.17) Proposition. *There exists a homomorphism of abelian groups*

$$d: G_0(KG) \rightarrow G_0(kG).$$

For a f.g. left KG -module V , the map assigns to $[V]$ in $G_0(KG)$ the element $[\bar{M}]$ in $G_0(kG)$, where M is any full RG -lattice in V .

Proof. We propose to define d by setting $d[V] = [\bar{M}]$, where M is a full RG -lattice in V . By (16.16), the image $[\bar{M}]$ is independent of the choice of M in V . We have to prove that d is additive on short exact sequences (ses's). Given a ses of KG -modules

$$0 \rightarrow V_1 \rightarrow V_2 \xrightarrow{\varphi} V_3 \rightarrow 0,$$

let M_2 be a full RG -lattice in V_2 , and set $M_3 = \varphi(M_2)$. Then M_3 is an RG -lattice in V_3 , and

$$KM_3 = K\varphi(M_2) = \varphi(KM_2) = V_3,$$

so M_3 is full in V_3 . Letting $V_1 \rightarrow V_2$ be the inclusion map, we set $M_1 = M_2 \cap V_1$, and obtain a ses of RG -modules

$$(16.18) \quad 0 \rightarrow M_1 \rightarrow M_2 \xrightarrow{\varphi} M_3 \rightarrow 0.$$

Then $0 \rightarrow KM_1 \rightarrow KM_2 \rightarrow KM_3 \rightarrow 0$ is exact, whence $KM_1 = V_1$, and M_1 is full in V_1 . Since M_3 is R -projective, the sequence (16.18) is split as a sequence of R -modules. Hence, tensoring it with k over R preserves exactness. But $k \otimes M_i \cong \bar{M}_i$, as we observed in the remarks following the definition of \bar{M} . We therefore have an exact sequence of kG -modules

$$0 \rightarrow \bar{M}_1 \rightarrow \bar{M}_2 \rightarrow \bar{M}_3 \rightarrow 0.$$

Hence $[\bar{M}_2] = [\bar{M}_1] + [\bar{M}_3]$ in $G_0(kG)$, so that $d[V_2] = d[V_1] + d[V_3]$, completing the proof.

By Proposition 16.6, $G_0(KG)$ and $G_0(kG)$ have \mathbb{Z} -bases $\{[Z_1], \dots, [Z_s]\}$ and $\{[F_1], \dots, [F_r]\}$, respectively, where $\{Z_i\}_{1 \leq i \leq s}$ and $\{F_j\}_{1 \leq j \leq r}$ are basic sets of simple modules over the group algebras KG and kG , respectively. Then

$$(16.19) \quad d[Z_i] = \sum_{j=1}^r d_{ij} [F_j], \quad 1 \leq i \leq s,$$

where d_{ij} is the multiplicity of F_j as a composition factor of the kG -module obtained by reduction mod \mathfrak{p} of a full RG -lattice in Z_i , $1 \leq i \leq s$. The $s \times r$ matrix (d_{ij}) , whose entries are defined by (16.19), is the transpose of the matrix of d with respect to the ordered bases $\{[Z_i]\}$ of $G_0(KG)$ and $\{[F_j]\}$ of $G_0(kG)$, respectively.

(16.20) Definition. The homomorphism of abelian groups

$$d: G_0(KG) \rightarrow G_0(kG),$$

defined in (16.17), is called the *decomposition map* (or *decomposition homomorphism*) associated with the p -modular system (K, R, k) and the finite group G . The $s \times r$ matrix $\mathbf{D} = (d_{ij})$, defined by (16.19), is called the *decomposition matrix*.

Examples. (i) $G = S_3$, $p = 2$, and the p -modular system is (\mathbb{Q}, R, k) , where \mathbb{Q} is the rational field, R is the ring of 2-adic integers in \mathbb{Q} , $\mathfrak{p} = 2R$, and $k = R/\mathfrak{p} = \mathbb{Z}/2\mathbb{Z}$. In this case there are three simple $\mathbb{Q}G$ -modules Z_1, Z_2, Z_3 , affording the trivial representation, the sign representation, and the simple module of dimension 2, respectively. There are two simple kG -modules F_1 and F_2 , affording the trivial representation, and the 2-dimensional representation obtained by reduction mod 2 from Z_3 , respectively. We leave it to the reader to verify this fact, and that the decomposition matrix is

$$\mathbf{D} = \begin{bmatrix} 1 & 0 \\ 1 & 0 \\ 0 & 1 \end{bmatrix}.$$

(ii) Let $G = S_4$, $p = 2$, and let (\mathbb{Q}, R, k) be the 2-modular system defined in Example (i). There are 5 simple $\mathbb{Q}G$ -modules $\{Z_1, \dots, Z_5\}$ of dimensions 1, 1, 2, 3, 3, respectively. Let H be the elementary abelian normal 2-subgroup of G generated by products of commuting transpositions. Then $G/H \cong S_3$, and Z_1, Z_2, Z_3 are the simple modules of G on which H acts trivially, and correspond to the simple modules in Example (i). The representation of G on $\{1, 2, 3, 4\}$ is 2-transitive, hence by Exercise 10.3 it can be expressed as the direct sum of the trivial representation and an irreducible representation of degree 3, which is realized in the rational field \mathbb{Q} . The other 3-dimensional representation arises by tensoring the first one with the sign representation. By (17.16), the normal 2-subgroup H acts trivially on each simple kG -module, and hence there are 2 simple kG -modules F_1 and F_2 , which arise from those of S_3 described in example (i). The decomposition matrix is

$$\mathbf{D} = \begin{bmatrix} 1 & 0 \\ 1 & 0 \\ 0 & 1 \\ 1 & 1 \\ 1 & 1 \end{bmatrix}.$$



§16D. Behavior of Grothendieck Groups under Extension of Ground Field

Let (K, R, k) be a p -modular system, where $\text{char } K=0$, and let K' be a finite extension field of K . We wish to find a p -modular system (K', R', k') which extends the original system (K, R, k) . This can always be done, by the following result:

(16.21) Proposition. *Let (K, R, k) be a p -modular system, where R is a d.v.r. with maximal ideal \mathfrak{p} and residue class field $k=R/\mathfrak{p}$. Let v denote the discrete valuation on K whose valuation ring is R . Then for each field K' which is a finite extension of K , the valuation v can be extended to a discrete valuation v' on K' . Let R' be the valuation ring of v' , \mathfrak{p}' the maximal ideal of R' , and set $k'=R'/\mathfrak{p}'$. Then*

$$R' \cap K = R, \quad \mathfrak{p}' \cap K = \mathfrak{p},$$

and k' is a finite extension of the field k , in a natural manner.

Proof. This is a standard result in algebraic number theory; see, for example, Weiss [63, section 2-4], as well as the discussion in §4C and in §30B below, or MO §12. Here, we shall give a brief summary of the relevant facts, omitting proofs.

The d.v.r. R is the valuation ring associated with some discrete (rank 1) valuation v on K , and we have

$$R = \{x \in K : v(x) \geq 0\}, \quad \mathfrak{p} = \{x \in K : v(x) > 0\}.$$

Let \hat{K} be the p -adic completion of K (see §4C); the valuation v extends to a discrete valuation \hat{v} on \hat{K} . Let Ω be some algebraic closure of \hat{K} . Then \hat{v} extends to a valuation w on Ω , defined by

$$w(x) = \frac{1}{n} \hat{v}(Nx), \quad n = \dim_{\hat{K}} \hat{K}(x), \quad x \in \Omega,$$

where Nx denotes the norm of x from $\hat{K}(x)$ to \hat{K} . For each field E such that $\hat{K} \subseteq E \subseteq \Omega$, with $\dim_{\hat{K}} E$ finite, the restriction of w to E yields a discrete valuation w_E on E , and w_E is the unique extension of \hat{v} from \hat{K} to E .

Now Ω is an algebraically closed field containing K . Let $\theta_i : K' \rightarrow \Omega$, $1 \leq i \leq m$, be the distinct embeddings of K' into Ω . Then the discrete valuation v on K has precisely m distinct extensions v_1, \dots, v_m to K' , and these are given by the formula

$$v_i(a) = w(\theta_i a), \quad a \in K', \quad 1 \leq i \leq m.$$

Keep i fixed; then v_i is a discrete valuation on K' , with valuation ring R' and maximal ideal \mathfrak{p}' , where

$$R' = \{a \in K' : v_i(a) \geq 0\}, \quad \mathfrak{p}' = \{a \in K' : v_i(a) > 0\}.$$

The composite map $R \rightarrow R' \rightarrow k'$ has kernel $R \cap \mathfrak{p}'$. This intersection is \mathfrak{p} , so we obtain a natural embedding of k in k' , as desired.

For convenience, we will call the above p -modular system (K', R', k') a *finite extension* of the p -modular system (K, R, k) . We are going to investigate the behavior of $G_0(KG)$, $K_0(kG)$ and $G_0(kG)$, under ground field extension.

(16.22) Proposition. *Let (K', R', k') be a finite extension of the p -modular system (K, R, k) . Then there are additive homomorphisms*

$$G_0(KG) \rightarrow G_0(K'G), K_0(kG) \rightarrow K_0(k'G), G_0(kG) \rightarrow G_0(k'G),$$

defined by tensoring with K' , k' and k' , respectively. All three maps are injections. Further, both of the maps

$$K_0(kG) \rightarrow K_0(k'G), G_0(kG) \rightarrow G_0(k'G),$$

are split injections, that is, the embeddings identify $K_0(kG)$ and $G_0(kG)$ as \mathbb{Z} -direct summands of $K_0(k'G)$ and $G_0(k'G)$, respectively.

Proof. Let $\{V_1, \dots, V_s\}$ be a basic set of simple KG -modules. Since $\text{char } K = 0$, $\{V_1^{K'}, \dots, V_s^{K'}\}$ are semisimple $K'G$ -modules, no two of which have a simple submodule in common, by Exercise 7.9. It then follows from (16.6) and the fact that tensoring with K' preserves ses's, that there exists an injection of \mathbb{Z} -modules $G_0(KG) \rightarrow G_0(K'G)$, which takes the element $[V_i]$ in $G_0(KG)$ onto $[V_i^{K'}]$ in $G_0(K'G)$.

Now let $\{F_1, \dots, F_r\}$ be a basic set of simple kG -modules. By Proposition 7.11, each module $F_i^{k'}$ is a direct sum of simple $k'G$ -modules, no two of which are isomorphic. By Exercise 7.9, the modules $F_i^{k'}$ and $F_j^{k'}$ have no simple submodules in common, if $i \neq j$. It is then clear, using (16.6) again, that the map given by $[F_i] \rightarrow [F_i^{k'}]$, $1 \leq i \leq r$, defines an injection $G_0(kG) \rightarrow G_0(k'G)$. This injection identifies $G_0(kG)$ with a \mathbb{Z} -direct summand of $G_0(k'G)$.

Finally, tensoring with k' is easily seen to define an homomorphism of \mathbb{Z} -modules $K_0(kG) \rightarrow K_0(k'G)$. By (16.7), $K_0(kG)$ has a \mathbb{Z} -basis $\{[P_1], \dots, [P_r]\}$, where $\{P_1, \dots, P_r\}$ are a basic set of f.g. indecomposable projective kG -modules. From §6C, each module P_i is the projective cover of the simple kG -module $P_i/\text{rad } P_i$. It is easily checked that $P_i^{k'}$ is the projective cover of $(P_i/\text{rad } P_i)^{k'}$. By (16.7) and the uniqueness of projective covers, the fact that $K_0(kG) \rightarrow K_0(k'G)$ is a split injection follows from the corresponding result about the map $G_0(kG) \rightarrow G_0(k'G)$, and the proof is complete.

Examples show that the map $G_0(KG) \rightarrow G_0(K'G)$ is not always a split injection (see Exercise 16.8).

(16.23) Proposition. *Let (K', R', k') be a finite extension of the p -modular system (K, R, k) . Then there exists a commutative diagram*

$$\begin{array}{ccc} G_0(KG) & \longrightarrow & G_0(K'G) \\ d \downarrow & & d \downarrow \\ G_0(kG) & \longrightarrow & G_0(k'G), \end{array}$$

where the vertical maps are decomposition homomorphisms (see (16.20)), and the horizontal maps are the injections defined in (16.22).

The proof is left as an exercise for the reader.

§16. Exercises

- Verify the statements made in Examples (i) and (ii) at the end of §16C. Note in particular that if M is a full RG -lattice in either of the simple modules Z_4 or Z_5 in Example (ii), then \bar{M} is not a simple kG -module.
- Find the decomposition matrix for the groups S_3 and S_4 considered in Exercise 1, in case $p=3$ and the p -modular system is (\mathbb{Q}, R, k) , where R is the ring of 3-adic integers in \mathbb{Q} and $k=\mathbb{Z}/3\mathbb{Z}$.
- Find an example of a p -modular system (K, R, k) , a finite group G , and two full RG -lattices M_1 and M_2 in a simple KG -module V , such that \bar{M}_1 and \bar{M}_2 are not kG -isomorphic.
- Let A be an arbitrary ring. Show that each element x of the projective class group $K_0(A)$ can be expressed in the form

$$x = [P] - [A^{(n)}]$$

for some $P \in \mathcal{P}(A)$ and some non-negative integer n . Show also that x may be expressed as

$$x = [A^{(m)}] - [P']$$

for some $m \geq 0$ and some $P' \in \mathcal{P}(A)$.

[Hint: Write $x = [P_1] - [P_2]$ with each $P_i \in \mathcal{P}(A)$, and choose $Q \in \mathcal{P}(A)$ such that $P_2 \oplus Q \cong A^{(n)}$ for some $n \geq 0$. Then

$$x = [P_1 \oplus Q] - [P_2 \oplus Q] = [P_1 \oplus Q] - [A^{(n)}],$$

as desired.]

- If A is a semisimple ring, show that $K_0(A) = G_0(A)$.

6. Let A be a f.d. separable K -algebra, and let E be an extension field of K . Set $A^E = E \otimes_K A$. Show that the map

$$\beta: G_0(A) \rightarrow G_0(A^E),$$

given by $\beta[V] = [V^E]$ for each A -module V , is a monomorphism.

[Hint: Let $\{V_1, \dots, V_s\}$ be a basic set of simple left A -modules. Then

$$G_0(A) = \bigoplus_{i=1}^s \mathbb{Z}[V_i].$$

For each i , we may write

$$V_i^E \cong \prod_{j=1}^{n_i} W_{ij}^{(m_{ij})},$$

where the $\{W_{ij}\}$ are simple A^E -modules. By (7.9ii), the modules $\{W_{ij} : 1 \leq j \leq n_i, 1 \leq i \leq s\}$ are a basic set of simple A^E -modules. Since

$$G_0(A^E) = \bigoplus_{i,j} \mathbb{Z}[W_{ij}],$$

it is clear that β is monic.]

7. Let G be a finite group, and let R be a d.v.r. with quotient field K . Let V be a simple KG -module. Show that every full RG -lattice M in V is indecomposable, and in fact, that M contains no nonzero RG -submodules of smaller R -rank.

8. Let G be the quaternion group of order 8, and K a splitting field for G of finite dimension over the rational field \mathbb{Q} . Let $M = \mathbb{Q} \oplus \mathbb{Q}i \oplus \mathbb{Q}j \oplus \mathbb{Q}k$ be the simple QG -module consisting of rational quaternions (see Example 10.36). Show that

$$[M^K] = 2[W] \text{ in } G_0(KG),$$

where W is the simple KG -module such that $\dim_K W = 2$. Deduce that the image of $G_0(QG)$ in $G_0(KG)$ is not a \mathbb{Z} -direct summand of $G_0(KG)$.

§17. BRAUER CHARACTERS

In this section, we interpret the decomposition map (defined in §16C) in terms of characters.

§17A. Splitting Fields

Let G be a finite group of exponent m ; by definition, m is the L.C.M. of the orders of the elements of G . Following Serre [77], we say that a field E is *sufficiently large (relative to G)* if E contains all the m -th roots of unity. Let

(K, R, k) be a p -modular system. In this subsection, we shall prove that if K is sufficiently large relative to G , then so is k , and of more importance, both K and k are splitting fields for G and all of its subgroups.

If $\text{char } E=0$, then E is sufficiently large relative to G if and only if E contains the cyclotomic field of m -th roots of unity. On the other hand, if $\text{char } E=p>0$, write $m=p^a m'$, where $p \nmid m'$ (so m' is the p' -part of m). Then in $E[X]$ we have

$$X^m - 1 = (X^{m'} - 1)^{p^a},$$

and thus E contains the m -th roots of 1 if and only if E contains the m' -th roots of 1. The polynomial $X^{m'} - 1$ is separable over E , and its roots form a cyclic group $\langle \omega \rangle$ of order m' , generated by a primitive m' -th root of unity ω .

(17.1) Theorem. *If the field E is sufficiently large relative to the finite group G , then E is a splitting field for G and all its subgroups.*

Proof. If E is sufficiently large for G , then clearly it is also sufficiently large for each subgroup of G , so it suffices to prove the theorem for G itself. If $\text{char } E=0$, the result follows from Corollary 15.18. For the rest of the proof, we need only consider the case where $\text{char } E=p>0$. Let us write $m=p^a m'$ as above, where m is the exponent of G , and m' is its p' -part. Then by hypothesis, E contains a primitive m' -th root of unity ω . Set $E_0 = \mathbb{F}_p$, and let $k=E_0(\omega) \subseteq E$. Then k is a finite field, and by remark (iv) following Definition 7.12, it is sufficient to prove that k is a splitting field for G .

By Proposition 7.13, there exists a finite extension F of k which is a splitting field for G . Then F is a finite field, and is thus a Galois extension of k . Let \mathfrak{G} denote the Galois group of F relative to k . Suppose now that U is a simple kG -module; we have to prove that U is absolutely simple, and for this, it suffices (by (3.43)) to show that $\text{End}_{kG} U = k \cdot 1_U$. Let $U^F = F \otimes_k U$; then by Proposition 7.18, U^F is a direct sum of algebraic conjugates of a simple FG -module M , all occurring with the same multiplicity. By Proposition 7.11, this common multiplicity is equal to 1. If M affords the F -character μ , then for each $\sigma \in \mathfrak{G}$, the algebraic conjugate module ${}^\sigma M$ affords the character ${}^\sigma \mu$. Moreover, $M \cong {}^\sigma M$ if and only if ${}^\sigma \mu = \mu$, by the Frobenius-Schur Theorem 3.41, which may be applied since F is a splitting field for G . On the other hand, all of the character values $\{\mu(x) : x \in G\}$ lie in k , since k contains all m -th roots of 1. Hence ${}^\sigma \mu = \mu$ for all $\sigma \in \mathfrak{G}$. Then ${}^\sigma M \cong M$ for all σ , and since the multiplicity of M as a summand of U^F is 1, we have $U^F \cong M$. Then $\text{End}_{FG} M = F \cdot 1_M$, and it follows that $\text{End}_{kG} U = k \cdot 1_U$, completing the proof.

(17.2) Corollary. *Let (K, R, k) be a p -modular system and assume $\text{char } K=0$. If K is sufficiently large relative to the finite group G , then k is also sufficiently large, and both K and k are splitting fields for G and all of its subgroups.*

Proof. Let m be the exponent of G , $m=p^a m'$, where $p \nmid m'$, and let ω be a primitive m -th root of 1 in K . Then $\omega \in R$, since the equation $\omega^m - 1 = 0$ shows that $\omega \in \text{alg. int.}\{K\} \subseteq R$. We have

$$X^m - 1 = \prod_{i=0}^{m-1} (X - \omega^i) \text{ in } R[X].$$

If bars denote passage to the residue class field $k (=R/\mathfrak{p})$, we have

$$(X^{m'} - \bar{1})^{p^a} = X^m - \bar{1} = \prod_{i=0}^{m-1} (X - \bar{\omega}^i) \text{ in } k[X].$$

Therefore the powers $\{\bar{\omega}^i : 0 \leq i \leq m-1\}$ give all the m' -th roots of 1, each with multiplicity p^a . Each $\bar{\omega}^i$ lies in k , since $\omega^i \in R$, so k contains all the m' -th (and m -th) roots of 1. The result now follows from (17.1).

The ideas used in establishing Theorem 17.1 can also be used to prove:

(17.3) Theorem. *For E an arbitrary field, and G a finite group, the characters afforded by a basic set of simple EG -modules are linearly independent over E .*

Proof. Let $\{M_1, \dots, M_d\}$ be a basic set of simple EG -modules, affording the characters $\{\mu_1, \dots, \mu_d\}$, respectively. For the case where $\text{char } E=0$, see (9.20). Another proof may be found in CR (30.12).

Now let $\text{char } E=p>0$. From §7, there exists an extension field F of E which is a splitting field for G . Let $\{W_1, \dots, W_e\}$ be a basic set of simple FG -modules affording the characters $\{\omega_1, \dots, \omega_e\}$, respectively. By (7.11), each module M_i^F is a sum of simple modules $\{W_{i,j}\}$, no two of which are isomorphic. By Exercise 2.7, no simple module appears as a common summand of M_i^F and M_j^F if $i \neq j$. The characters $\{\omega_1, \dots, \omega_e\}$ are linearly independent over F by the Frobenius-Schur Theorem 3.41. We leave to the reader the easy exercise of combining these remarks to deduce that $\{\mu_1, \dots, \mu_d\}$ are linearly independent over E , and the proof is complete.

§17B. Brauer Characters

We come now to some fundamental ideas due to Brauer. Let (K, R, k) be a p -modular system such that $\text{char } K=0$, and let G be a finite group. By (17.3), the characters of a basic set of simple kG -modules are linearly independent. The simplest examples show, however, that two kG -modules can have the same k -character without being isomorphic or even having the same set of composition factors. (For example, take the direct sum of p copies and of $2p$ copies of the trivial representation of G , where $p=\text{char } k$; the characters of both representations are zero for all elements of G .) The usefulness of

characters in fields of characteristic zero, for investigations of finite groups, provides strong motivation for seeking a satisfactory way of handling characters of kG -modules without losing too much information. Brauer found an ingenious way out of this dilemma by associating with each kG -module L a K -valued function λ , defined on the set $G_{p'}$ of p -regular elements of G . As we shall see, these functions yield most of the desired information.

Throughout this subsection, we fix the following notation:

(K, R, k) , a p -modular system such that $\text{char } K = 0$, with K sufficiently large relative to a given finite group G ;

$m = \text{exponent of } G$, $m = p^a m'$, $p \nmid m'$;

$\omega = \text{primitive } m'\text{-th root of 1 in } K$;

$f: R \rightarrow k$ ($= R/\mathfrak{p}$) the natural homomorphism, also denoted by $\xi \mapsto \bar{\xi}$, $\xi \in R$.

By Corollary 17.2, k is sufficiently large relative to G , and both K and k are splitting fields for G and all its subgroups. By the proof of Corollary 17.2, $\bar{\omega}$ is a primitive m' -th root of 1 in k , and $f: \langle \omega \rangle \rightarrow \langle \bar{\omega} \rangle$ is an isomorphism from the cyclic group of m' -th roots of 1 in K onto the corresponding cyclic group in k .

Let L be a left kG -module (always assumed f.g.). For each p -regular element $x \in G_{p'}$, all the eigenvalues $\{\xi_1, \dots, \xi_d\}$ of x_L on L are m' -th roots of 1, and hence can be expressed as powers of $\bar{\omega}$, say $\{\bar{\omega}^{t_1}, \dots, \bar{\omega}^{t_d}\}$, where $d = \dim_k L$. Then define

$$\lambda(x) = \omega^{t_1} + \cdots + \omega^{t_d},$$

or, in terms of the eigenvalues $\{\xi_i\}$ of x_L ,

$$\lambda(x) = \sum_{i=1}^d f^{-1}(\xi_i).$$

It is clear from the definition that $\lambda: G_{p'} \rightarrow K$ is a well-defined K -valued function on $G_{p'}$. Note also that once the p -modular system (K, R, k) is fixed, there is no ambiguity in the definition of λ ; the isomorphism $f: \langle \omega \rangle \cong \langle \bar{\omega} \rangle$ arises from the canonical map $R \rightarrow R/\mathfrak{p} = k$.

(17.4) Definition. For each left kG -module L , the K -valued function $\lambda: G_{p'} \rightarrow K$ defined above is called the *Brauer character** of G afforded by L . The trace function

$$x \mapsto \text{Tr}(x, L), x \in G,$$

is called the *k-character* of L .

*Brauer called λ a “modular character” of G .

We now collect some elementary facts about Brauer characters.

(17.5) Proposition. (i) *The Brauer character λ afforded by a left kG -module L is a class function on the p -regular classes of G .*

(ii) *A Brauer character λ afforded by a kG -module L takes values in R , and we have*

$$\overline{\lambda(x)} = \text{Tr}(x, L), \quad x \in G_{p'}$$

(iii) *Let $L_0 \supset L_1 \supset 0$ be kG -modules. Let χ be the Brauer character afforded by L_0/L_1 , χ_1 the Brauer character afforded by L_1 and χ_0 the Brauer character of L_0 . Then $\chi_0 = \chi + \chi_1$.*

(iv) *Let V be a KG -module with K -character χ . Then for each full RG -lattice M in V , the restriction $\chi|_{G_{p'}}$ of χ to $G_{p'}$ is the Brauer character of the kG -module $\bar{M} (= M/\mathfrak{p}M)$.*

Proof. (i) and (iii) are left as exercises for the reader. (ii) is immediate, since $\lambda(x)$ is a sum of roots of 1, hence in R , and $\overline{\lambda(x)}$ is the sum of the eigenvalues of the left multiplication x_L on L , so $\lambda(x) = \text{Tr}(x, L)$.

(iv) Let \mathbf{M} be the matrix representation of G afforded by V , with respect to an R -basis of the full RG -lattice M in V . For $x \in G_{p'}$, the eigenvalues $\{\xi_i\}_{1 \leq i \leq d}$ of $\mathbf{M}(x)$ belong to R , and

$$\chi(x) = \xi_1 + \cdots + \xi_d.$$

The result will follow if we can show that $\{\bar{\xi}_1, \dots, \bar{\xi}_d\}$ are the eigenvalues of $\bar{\mathbf{M}}(x)$, since $\bar{\mathbf{M}}$ is a matrix representation afforded by the kG -module \bar{M} . The matrix $\mathbf{M}(x)$ has entries in R , so $\text{char. pol. } \mathbf{M}(x) \in R[X]$, and

$$\text{char. pol. } \mathbf{M}(x) = \prod_{i=1}^d (X - \xi_i) \text{ in } R[X].$$

The polynomial obtained from $\text{char. pol. } \mathbf{M}(x)$, by reducing coefficients mod \mathfrak{p} , is $\text{char. pol. } \bar{\mathbf{M}}(x)$. Therefore

$$\text{char. pol. } \bar{\mathbf{M}}(x) = \prod_{i=1}^d (X - \bar{\xi}_i) \text{ in } k[X].$$

It follows that $\{\bar{\xi}_i\}_{1 \leq i \leq d}$ are the eigenvalues of $\bar{\mathbf{M}}(x)$, and (iv) is proved.

The following notation will be fixed, and extends the character table data given in (9.25):

$$(17.6) \quad \left\{ \begin{array}{l} \text{cf}_K(G_{p'}), \text{ the } K\text{-valued class functions on } G_{p'}. \\ \{F_1 = 1_G, F_2, \dots, F_r\}, \text{ a basic set of simple } kG\text{-modules.} \\ \{\varphi^1, \varphi^2, \dots, \varphi^r\}, \text{ the Brauer characters afforded by } \{F_1, \dots, F_r\}, \\ \text{ called the } \textit{irreducible Brauer characters}. \\ \{U_1, U_2, \dots, U_r\}, \text{ a basic set of indecomposable projective } kG\text{-mod-} \\ \text{ules, such that } U_i \text{ is a projective cover of } F_i, 1 \leq i \leq r. \\ \{\eta^1, \eta^2, \dots, \eta^r\}, \text{ the Brauer characters afforded by the } \{U_i\}, \text{ the} \\ \text{ principal (or projective) indecomposable Brauer characters}. \end{array} \right.$$

Letting ξ^i be the K -character afforded by Z_i as in (9.25), for $1 \leq i \leq s$, the decomposition map (see §16C) is given in terms of Brauer characters by

$$(17.7) \quad \xi^i|_{G_{p'}} = \sum_{j=1}^r d_{ij} \varphi^j \text{ on } G_{p'},$$

where $\mathbf{D} = (d_{ij})$ is the decomposition matrix ((16.20)). The proof of (17.7) is an application of Proposition 17.5, and is left as an exercise for the reader.

Our next objective is to prove, following Serre [77], that the irreducible Brauer characters $\{\varphi^1, \dots, \varphi^r\}$ are linearly independent over K . Since k is sufficiently large, we already know by the Frobenius-Schur Theorem that the k -characters afforded by the modules $\{F_1, \dots, F_r\}$ are linearly independent over k .

(17.8) Lemma. *Let $\mathbf{M}: G \rightarrow GL_n(k)$ be a matrix representation of G over k . Let $x \in G$, and let $x = su$ be its decomposition into a p -regular part s and a p -part u . Then the matrices $\mathbf{M}(x)$ and $\mathbf{M}(s)$ have the same set of eigenvalues, counted with multiplicities.*

Proof. We have $\mathbf{M}(x) = \mathbf{M}(s)\mathbf{M}(u)$, and the matrices $\mathbf{M}(s)$ and $\mathbf{M}(u)$ commute with each other. Therefore the eigenvalues of $\mathbf{M}(x)$ are the pairwise products of suitably ordered sets of eigenvalues of $\mathbf{M}(s)$ and $\mathbf{M}(u)$. Since u is a p -element, and k has characteristic p , it follows that a p -power of $\mathbf{M}(u)$ is equal to the identity, and therefore all the eigenvalues of $\mathbf{M}(u)$ are equal to 1. Therefore the eigenvalues of $\mathbf{M}(x)$ coincide with those of $\mathbf{M}(s)$, as required.

(17.9) Theorem. *The irreducible Brauer characters $\{\varphi^1, \dots, \varphi^r\}$ form a K -basis of the space of K -valued class functions $\text{cf}_K(G_{p'})$.*

Proof. We first prove that $\{\varphi^1, \dots, \varphi^r\}$ are linearly independent over K . Suppose not, and consider a nontrivial relation of linear dependence with

coefficients in K . Since K is the quotient field of R , we can clear denominators, and obtain such a relation with coefficients in R . Every nonunit in R is divisible by a power of π , so we can divide by some appropriate power of π , to arrive at a relation

$$\sum_{i=1}^r a_i \varphi^i(s) = 0 \quad \forall s \in G_{p'},$$

where the $a_i \in R$, and some $a_{i_0} \notin \mathfrak{p}$. Reducing mod \mathfrak{p} , we obtain

$$\sum_{i=1}^r \overline{a_i} \overline{\varphi^i(s)} = 0 \quad \forall s \in G_{p'},$$

with at least one coefficient $\overline{a_{i_0}} \neq 0$ in k . By (17.5ii), we can rewrite this relation as

$$\sum_{i=1}^r \overline{a_i} \operatorname{Tr}(s, F_i) = 0 \quad \forall s \in G_{p'}.$$

But for $x \in G$, $\operatorname{Tr}(x, F_i)$ is the sum of the eigenvalues of x_i on F_i ; it follows from (17.8) that

$$\sum_{i=1}^r \overline{a_i} \operatorname{Tr}(x, F_i) = 0, \quad \forall x \in G.$$

Since $\overline{a_{i_0}} \neq 0$, we have obtained a nontrivial relation of linear dependence among the k -characters of the simple kG -modules $\{F_i\}$, contrary to the Frobenius-Schur Theorem (see also (17.3)). Thus $\{\varphi^1, \dots, \varphi^r\}$ are linearly independent over K .

Now let $\xi \in \operatorname{cf}_K(G_{p'})$ be an arbitrary K -valued class function on $G_{p'}$. Then ξ can be extended to a class function $\xi^\#$ on G , for example by setting $\xi^\#(x) = 0$ for $x \notin G_{p'}$. From §9C, this extension $\xi^\#$ is a K -linear combination of the characters $\{\zeta^1, \dots, \zeta^s\}$ in $\operatorname{Irr}_K G$. Then

$$\xi^\#(x) = \sum_j \alpha_j \zeta^j(x) \quad \forall x \in G,$$

for some coefficients $\{\alpha_j\}$ in K . Restricting to $x \in G_{p'}$, we have

$$\xi = \sum_j \alpha_j \zeta^j|_{G_{p'}}.$$

By (17.7), $\zeta^j|_{G_{p'}}$ is a K -linear combination of the irreducible Brauer characters $\{\varphi^1, \dots, \varphi^r\}$, and hence the same is true for ξ . This completes the proof of the theorem.

There are a number of important corollaries of the preceding theorem. The first answers the question of how two kG -modules with the same Brauer character are related. They are not necessarily isomorphic, but at least they determine the same element of the Grothendieck group $G_0(kG)$.

(17.10) Corollary. *Let L and M be kG -modules with Brauer characters λ and μ , respectively. If $\lambda = \mu$, then L and M have the same sets of composition factors, and hence $[L] = [M]$ in $G_0(kG)$.*

Proof. Suppose L and M have composition series such that the simple module F_j appears a_j times in L and b_j times in M . By (17.5iii), it follows that

$$\lambda = \sum_{j=1}^r a_j \varphi^j, \quad \mu = \sum_{j=1}^r b_j \varphi^j.$$

Then, by Theorem 17.9, $\lambda = \mu$ implies $a_j = b_j$, $1 \leq j \leq r$, and the result follows.

The next corollary settles the important problem of determining the number of simple kG -modules in a basic set. Another proof of this fundamental result (due to Brauer), which does not involve Brauer characters, and is of independent interest, can be found in CR §83B.

(17.11) Corollary. *The number of absolutely simple EG -modules, for a splitting field E of characteristic p , is equal to the number of p -regular conjugacy classes of G .*

Proof. We first show that it is sufficient to prove the result for kG -modules, where k is part of our p -modular system (K, R, k) . Indeed, there exists a composite field extension of E and k . Hence by §7, the number of simple EG -modules coincides with the number of simple kG -modules. Thus we have to prove that the number of simple kG -modules is equal to the number of conjugacy classes of G contained in G_p . But this is clear by Theorem 17.9, since the Brauer characters $\{\varphi^1, \dots, \varphi^r\}$ form a K -basis for the space of K -valued class functions on G_p .

We shall now interpret the decomposition map in terms of Brauer characters.

(17.12) Definition. A virtual Brauer character on G is a \mathbb{Z} -linear combination of Brauer characters of kG -modules. The set of virtual Brauer characters of G is denoted by $\text{Bch } kG$, or simply $\text{Bch } G$.

(17.13) Lemma. *Let L and M be kG -modules, affording the Brauer characters λ and μ , respectively. Then $\lambda\mu$ is the Brauer character of the kG -module $L \otimes_k M$.*

Proof. Let $x \in G_{p'}$. Then x_i is a semisimple linear transformation on L and M . By choosing bases of eigenvectors for x_i in L and M , and a basis of $L \otimes_k M$ consisting of tensor products of these basis elements, it follows that the eigenvalues of x_i on $L \otimes_k M$ are the products of eigenvalues of x_i on L with the eigenvalues of x_i on M . Since the Brauer character is defined in terms of eigenvalues, we obtain the result of the Lemma.

(17.14) Proposition. *The set of virtual Brauer characters $\text{Bch } kG$ is a ring under addition and multiplication of functions. The map, which assigns to an element $t \in G_0(kG)$ the virtual Brauer character τ associated with it, defines an isomorphism of \mathbb{Z} -algebras:*

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

Proof. Let us first explain what is meant by the virtual Brauer character associated with an element $t \in G_0(kG)$. By (16.6), $\{[F_1], \dots, [F_r]\}$ is a \mathbb{Z} -basis of $G_0(kG)$, so we can write

$$t = \sum_{i=1}^r a_i [F_i],$$

with uniquely determined coefficients $\{a_i\}$ in \mathbb{Z} . The virtual Brauer character τ corresponding to t is then defined by

$$\tau = \sum_{i=1}^r a_i \varphi^i.$$

We next observe that by Theorem 17.9, $\{\varphi^1, \dots, \varphi^r\}$ forms a \mathbb{Z} -basis of $\text{Bch } kG$. Therefore the above map $t \mapsto \tau$ is an isomorphism of free \mathbb{Z} -modules. By Lemma 17.13 and (16.8), it follows that the map is an isomorphism of \mathbb{Z} -algebras, completing the proof.

(17.15) Proposition. *There is a commutative diagram*

$$\begin{array}{ccc} G_0(KG) & \longrightarrow & \text{ch } KG \\ d \downarrow & & \downarrow d' \\ G_0(kG) & \longrightarrow & \text{Bch } kG, \end{array}$$

where the horizontal maps are the isomorphisms defined in (16.10) and (17.14). The vertical map d is the decomposition map, and d' is the restriction map $\psi \mapsto \psi|_{G_p}$ of a virtual character $\psi \in \text{ch } KG$ to G_p .

Proof. By (17.7), the diagram commutes when we compute the image of each element $[Z_i]$ in $G_0(KG)$ corresponding to a simple KG -module Z_i . Since these elements form a \mathbb{Z} -basis of $G_0(KG)$, the result follows.

We conclude this section with some additional remarks about Proposition 5.26:

(17.16) Proposition. *Let D be a normal p -subgroup of G , and let (K, R, k) be an arbitrary p -modular system. Then*

(i) *D acts trivially on every simple kG -module V , and therefore the simple kG -modules coincide with the simple $k(G/D)$ -modules.*

(ii) *The natural surjection $\tau: RG \rightarrow R(G/D)$ has the property that $\ker \tau$ is nilpotent mod $\mathfrak{p}G$, and hence $\ker \tau \subseteq \text{rad } RG$.*

Proof. If I is the augmentation ideal of kD , then $I \cdot kG = kG \cdot I$, and thus $I \cdot V$ is a kG -submodule of V . Since $I \cdot V \neq V$ because I is nilpotent, we deduce that $I \cdot V = 0$, and thus D acts trivially on V .

Alternatively, we may note that by Clifford's Theorem 11.1, V_D is a semisimple kD -module, and hence is D -trivial by (5.24).

The remainder of the proof is as in (5.26).

(17.17) Example. Let $G = SL_2(p)$ for an odd prime p . Let (K, R, k) be a p -modular system with $\text{char } K = 0$ and K sufficiently large relative to G . By definition, G is the group of 2×2 matrices of determinant 1 with entries in the prime field \mathbf{F}_p . Using linear algebra, the reader can show as an exercise that the conjugacy class of a p -regular element of G is determined by its characteristic equation, and that there are exactly p p -regular conjugacy classes. By (17.11), there are exactly p simple kG -modules. Here is their construction. For each d , $0 \leq d \leq p-1$, let M_d be the k -space of homogeneous polynomials of degree d in two indeterminates X and Y . The group G acts on $k[X, Y]$ as a group of automorphisms, where for $g = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in G$, we let

$$gX = \alpha X + \beta Y, \quad gY = \gamma X + \delta Y.$$

The subspaces $\{M_d\}_{0 \leq d \leq p-1}$ of $k[X, Y]$ are kG -submodules of dimensions 1, 2, ..., p , respectively. As an exercise, the reader should prove that in M_d , the elements

$$X^d, X^{d-1}Y, \dots, XY^{d-1}, Y^d$$

span non-isomorphic 1-dimensional kT -modules, where T is the subgroup of G consisting of diagonal matrices. A calculation, based on this fact, shows that M_d is a simple kG -module, for $0 \leq d \leq p-1$. Finally, by comparing $\dim_k M_d$ with $|G|$, the reader can show that dimensions of the simple kG -modules need not divide $|G|$.

§17. Exercises

1. Find the Brauer characters of the symmetric groups S_3 and S_4 for the 2-modular system defined in Examples (i) and (ii) at the end of §16.

2. Referring to Proposition 17.15, show that the kernel of the decomposition map $d: G_0(KG) \rightarrow G_0(kG)$ corresponds to the set of virtual characters

$$\{\psi \in \text{ch } KG : \psi|_{G_p} = 0\}.$$

3. Prove Corollary 17.2 without the assumption that $\text{char } K = 0$.

4. Show that for any field E , the ring $G_0(EG)$ has no nonzero nilpotent elements.

[Hint: Choose a field $E' \supseteq E$ which is sufficiently large. The map $\beta: G_0(EG) \rightarrow G_0(E'G)$, given by $[V] \mapsto [E' \otimes_E V]$ for each EG -module V , is a ring homomorphism. By Exercise 16.6, β is monic. Thus it suffices to prove that $G_0(E'G)$ has no nilpotent elements except 0. Let (K, R, k) be a p -modular system, with K sufficiently large and where $\text{char } K = 0$. Then $G_0(KG) \cong \text{ch } KG$, so $G_0(KG)$ has no nonzero nilpotent elements. Further, $G_0(kG) \cong \text{Bch } kG$, so $G_0(kG)$ has no nonzero nilpotent elements.]

5. Show that the number of p -regular conjugacy classes in a direct product $G \times H$ equals the product of the corresponding numbers for G and H . This result can be used (see §10E) to complete the proof that for k sufficiently large, every simple $k(G \times H)$ -module can be expressed as an outer tensor product of simple kG - and kH -modules.

6. Determine the Brauer characters of the simple kG -modules, for a finite abelian group G , with respect to a p -modular system such that p divides $|G|$.

§18. THE CARTAN-BRAUER TRIANGLE

In §16, we defined the decomposition map $d: G_0(KG) \rightarrow G_0(kG)$ for an arbitrary p -modular system (K, R, k) . In this section we assume that RG is a semiperfect ring (see §6C). Let $K_0(RG)$ denote the Grothendieck group associated with the category $\mathcal{P}(RG)$ of f.g. projective RG -modules, and let $K_0(kG)$ be the Grothendieck group of the category $\mathcal{P}(kG)$. We prove first that there is a natural isomorphism

$$K_0(RG) \cong K_0(kG)$$

obtained by reduction mod \mathfrak{p} . We then prove that there exists a commutative diagram called the *Cartan-Brauer Triangle*,

$$\begin{array}{ccc} G_0(KG) & \xrightarrow{d} & G_0(kG) \\ e \swarrow & & \searrow c \\ K_0(kG), & & \end{array}$$

where d is the decomposition map and c the Cartan homomorphism (see (18.4)). In §18B, the properties of the Cartan-Brauer Triangle are derived when K is sufficiently large (§17A), and are then applied to derive orthogonality relations for the Brauer characters of the simple kG -modules and their projective covers. The point of view taken in this section is due to Swan ([60], [63]; see also Serre [77]). Extensions of the results in various directions will appear in §§21, 32, and Chapters 10 and 11 below.

§18A. The Cartan Map and the Cartan-Brauer Triangle

Throughout this section, (K, R, k) denotes a p -modular system such that RG is a semiperfect ring (see §6C). We do not assume, in this subsection, that K is sufficiently large or of characteristic zero.

The hypothesis that RG be semiperfect holds whenever R is complete in the p -adic topology, by §6B. In particular, this is the case whenever K is the completion of some algebraic number field with respect to a discrete valuation, and R is the valuation ring in K . The condition on RG also holds for a d.v.r. R in an arbitrary field K , provided that K is a sufficiently large field such that $\text{char } K \nmid |G|$ (see Exercise 6.16).

For the convenience of the reader, we begin with a brief summary of results from §§5, 6 concerning the structure of RG , kG and their modules.

Let $N = \text{rad } RG$, $\mathfrak{p}G = \mathfrak{p} \cdot (RG)$, and recall from (5.22) that $\mathfrak{p}G \subseteq N$ and $RG/N \cong kG/\text{rad } kG$. The latter isomorphism implies that simple kG -modules can be identified with simple RG -modules.

As in §16, we shall denote $RG/\mathfrak{p}G$ by \overline{RG} or by kG ; we let $a \rightarrow \bar{a}$ denote the natural map from R to k , or from RG to kG . For a left RG -module M , we let \overline{M} stand for the kG -module $M/\mathfrak{p}M$. The decomposition map $d: G_0(KG) \rightarrow G_0(kG)$ (see (16.20)) assigns to each element $[V]$ in $G_0(KG)$ corresponding to a KG -module V , the element $[\overline{M}]$ in $G_0(kG)$, where M is any full RG -lattice in V .

The condition that RG is semiperfect means that RG/N is artinian, and that every idempotent in RG/N is the image of an idempotent in RG . By §6B, the ring kG is always semiperfect. From the theory of projective covers in §6C, f.g. projective modules over RG and kG , respectively, decompose into indecomposable summands, which are unique up to isomorphism and order of occurrence.

(18.1) Summary. Let (K, R, k) be a p -modular system such that RG is a semiperfect ring.

(i) Let $\{F_1, \dots, F_r\}$ be a basic set of simple kG -modules. Each module F_i has an indecomposable projective cover U_i , which is isomorphic to a left ideal in kG generated by a primitive idempotent. Each indecomposable projective module U_i has a unique maximal submodule $\text{rad } U_i$, and $U_i/\text{rad } U_i \cong F_i$ for each i . Note that $\text{rad } U_i = (\text{rad } kG)U_i$ by (5.29).

- (ii) *Each f.g. projective kG -module U can be expressed as an external direct sum*

$$U \cong \coprod U_i^{(n_i)},$$

with uniquely determined multiplicities $\{n_i\}$.

- (iii) *By means of the isomorphism $RG/N \cong kG/\text{rad } kG$, the simple modules $\{F_1, \dots, F_r\}$ can be identified with a basic set of simple RG -modules. Each simple RG -module F_i has an indecomposable projective cover $P_i \in \mathcal{P}(RG)$ such that $\bar{P}_i \cong U_i$, $1 \leq i \leq r$. The module P_i can be taken to be a left ideal RGe_i , where e_i is a primitive idempotent in RG such that \bar{e}_i is primitive in kG , and $kGe_i \cong U_i$.*

- (iv) *Every f.g. projective RG -module M can be expressed as an external direct sum*

$$M \cong \coprod P_i^{(m_i)}$$

with uniquely determined multiplicities $\{m_i\}$. Two modules M and M' in $\mathcal{P}(RG)$ are isomorphic if and only if $\bar{M} \cong \bar{M}'$. A module $M \in \mathcal{P}(RG)$ is indecomposable if and only if \bar{M} is indecomposable.

- (v) *Each module $M \in \mathcal{P}(RG)$ is the projective cover of the semisimple module $M/\text{rad } M$. The module $M \in \mathcal{P}(RG)$ is indecomposable if and only if $M/\text{rad } M$ is simple, and in that case, $\text{rad } M$ is the unique maximal submodule of M .*

- (vi) *Each U_i has a unique minimal submodule $\text{soc } U_i$ (its socle), and*

$$\text{soc } U_i \cong F_i, \quad 1 \leq i \leq r.$$

Further, U_i is the injective hull of F_i .

References for the proofs of the results summarized in (18.1) are as follows. Radicals of modules are discussed in §5A. Statement (i) follows from (6.8) and (6.9). A module $U \in \mathcal{P}(kG)$ is f.g., hence a direct sum of indecomposable modules. The summands are projective because U is projective. The uniqueness statement in (ii) follows from the K-S-A Theorem.

The existence and uniqueness of projective covers of simple RG -modules is proved in (6.23). The fact that $\bar{P}_i \cong U_i$ follows because \bar{P}_i is projective (as a direct summand of \bar{RG}), and both \bar{P}_i and U_i are projective covers of F_i , for $1 \leq i \leq r$. The last statement in (iii) is left as an exercise for the reader.

The first part of (iv) follows by the same argument used to prove (ii). The last part of (iv) and all of (v) are immediate from the theory of projective covers (see (6.17), (6.23) and (6.25)). Finally, (vi) follows from (9.12).

We recall from §16 the notation $K_0(kG)$ for the Grothendieck group of the category $\mathcal{P}(kG)$ of f.g. projective kG -modules, and $K_0(RG)$ for the Grothendieck group of $\mathcal{P}(RG)$. Note that each ses $0 \rightarrow P' \rightarrow P \rightarrow P'' \rightarrow 0$ of modules from $\mathcal{P}(RG)$ must split, because P'' is projective. Thus the defining relations of $K_0(RG)$ can be expressed in the simpler form

$$[P' \oplus P''] = [P'] + [P''], P', P'' \in \mathcal{P}(RG).$$

Similar remarks apply to $\mathcal{P}(kG)$.

By (16.7), $K_0(RG)$ and $K_0(kG)$ are free abelian groups, with bases $\{[P_1], \dots, [P_r]\}$ and $\{[U_1], \dots, [U_r]\}$ corresponding to basic sets of indecomposable projective modules in $\mathcal{P}(RG)$ and $\mathcal{P}(kG)$, respectively. By (18.1iii), these bases can be chosen so that $[\bar{P}_i] = [U_i]$ for $1 \leq i \leq r$. We now have

(18.2) Theorem. *The map $[M] \rightarrow [\bar{M}]$, for $M \in \mathcal{P}(RG)$, defines an isomorphism of abelian groups:*

$$K_0(RG) \cong K_0(kG).$$

Proof. By the preceding remarks, there is an isomorphism of abelian groups $K_0(RG) \cong K_0(kG)$, given by

$$\sum_{i=1}^r a_i [P_i] \rightarrow \sum_{i=1}^r a_i [\bar{P}_i], a_i \in \mathbb{Z}.$$

We need only check that this map carries $[M]$ onto $[\bar{M}]$ for all $M \in \mathcal{P}(RG)$. By (18.1iv), we have

$$M \cong \coprod_{i=1}^r P_i^{(m_i)} \text{ for some non-negative integers } \{m_i\}.$$

Since the relations in $K_0(RG)$ are given by direct sum decompositions, we obtain

$$[M] = \sum_{i=1}^r m_i [P_i] \text{ in } K_0(RG).$$

On the other hand, the decomposition of M yields

$$\bar{M} \cong \coprod_{i=1}^r \bar{P}_i^{(m_i)},$$

and hence

$$[\bar{M}] = \sum_{i=1}^r m_i [\bar{P}_i] \text{ in } K_0(kG).$$

Thus $[M]$ goes to $[\bar{M}]$ under the isomorphism, and the proof is complete.

It is easily checked that the map

$$P \rightarrow K \otimes_R P, P \in \mathcal{P}(RG),$$

defines a homomorphism of abelian groups from $K_0(RG)$ to $G_0(KG)$. Composing this map with the isomorphism $K_0(kG) \rightarrow K_0(RG)$ given in (18.2), we obtain a homomorphism of abelian groups:

$$(18.3) \quad e: K_0(kG) \rightarrow G_0(KG).$$

Next, let $U \in \mathcal{P}(kG)$, and let $c_i(U)$ be the uniquely determined multiplicity of the simple module F_i as a composition factor of U . By (16.4) and (16.6), there exists an additive homomorphism

$$c: K_0(kG) \rightarrow G_0(kG),$$

given by

$$c[U] = [U] = \sum_{i=1}^r c_i(U)[F_i] \text{ for each } U \text{ in } \mathcal{P}(kG).$$

(18.4) Definition. The homomorphism

$$c: K_0(kG) \rightarrow G_0(kG)$$

defined above is called the *Cartan homomorphism*. The $r \times r$ *Cartan matrix* $\mathbf{C} = (c_{ij})$ of kG is defined by

$$c[U_i] = \sum_{j=1}^r c_{ij}[F_j], 1 \leq i \leq r.$$

Thus the Cartan matrix is the transpose of the matrix of c with respect to the ordered bases $\{[U_i]\}$ and $\{[F_j]\}$ of $K_0(kG)$ and $G_0(kG)$, respectively.

(18.5) Proposition. *The Cartan-Brauer triangle*

$$\begin{array}{ccc} G_0(KG) & \xrightarrow{d} & G_0(kG) \\ e \swarrow & & \searrow c \\ K_0(kG) & & \end{array}$$

where d is the decomposition map, c is the Cartan homomorphism, and e is defined by (18.3), is a commutative diagram of additive groups and additive homomorphisms.

Proof. We have to prove that $d(e[U])=c[U]$ for each $U \in \mathcal{P}(kG)$. From (18.1), it follows that there exists $P \in \mathcal{P}(RG)$ such that $\bar{P}=U$. Then by the definition of e , $e[U]=[K \otimes_R P]$. Evidently P is a full RG -lattice in $K \otimes_R P$, so by (16.17) we have

$$d(e[U]) = [\bar{P}] = [U] \text{ in } G_0(kG).$$

On the other hand, the element $[U] \in G_0(kG)$ is the image $c[U]$ of the element $[U] \in K_0(kG)$, and hence $d(e[U])=c[U]$, as required.

By (19.4), it follows that $K_0(kG)$ is a ring*. It is then clear that the maps $\{c, d, e\}$ in (18.5) are homomorphisms of rings.

§18B. Properties of the Cartan-Brauer Triangle (K Sufficiently Large)

In this subsection, we continue to require that (K, R, k) be a p -modular system such that RG is a semiperfect ring. We shall assume furthermore that K is sufficiently large, and that $\text{char } K=0$. As pointed out in §18A, these assumptions on K guarantee that RG is semiperfect for each d.v.r. R . Further, by §17A we know that both K and k are splitting fields for G and all of its subgroups.

The properties of the Cartan-Brauer Triangle in this situation are fundamental for deeper investigations of Brauer characters, and are equivalent, for the most part, to properties of the Cartan matrix C and the decomposition matrix D . Most of the results are due to Brauer-Nesbitt [41], whose approach was presented in CR §§82–84. As we noted in the introduction to §18, our treatment here follows Swan ([60], [63]) and Serre [77].

As in §9, let $\{Z_1, \dots, Z_s\}$ denote the simple KG -modules, and $\{\zeta^1, \dots, \zeta^s\}$ the K -characters afforded by them. We let

$$(18.6) \quad (\zeta, \zeta') = |G|^{-1} \sum_{x \in G} \zeta(x) \zeta'(x^{-1}),$$

for K -characters ζ and ζ' . Since K is a splitting field, the irreducible characters $\{\zeta^1, \zeta^2, \dots, \zeta^s\}$ form an orthonormal basis for $\text{cf}_K(G)$ with respect to the bilinear form (ζ, ζ') , by Proposition 9.21 and the discussion in §9C. Moreover, by (9.24) we have

$$(18.7) \quad (\zeta, \zeta') = i(M, M'),$$

for KG -modules M and M' affording the characters ζ and ζ' , respectively. Here $i(M, M')$ is the *intertwining number* defined by

$$i(M, M') = \dim_K \text{Hom}_{KG}(M, M').$$

* $K_0(kG)$ need not have an identity element, however.

Since $G_0(KG) \cong \text{ch } KG$ by (16.10), we may define a \mathbb{Z} -bilinear form

$$i_K: G_0(KG) \times G_0(KG) \rightarrow \mathbb{Z}$$

corresponding to the bilinear form on $\text{ch } KG$ defined by (18.6). Using (18.7), the form i_K is defined by

$$i_K([M], [M']) = i(M, M') = (\xi, \xi')$$

for f.g. KG -modules M and M' affording the K -characters ξ and ξ' , respectively. By the orthogonality relations (see (9.24)), we have

$$i_K([Z_i], [Z_j]) = \delta_{ij}, \quad 1 \leq i, j \leq s.$$

Turning to the residue field k , we have:

(18.8) Proposition. *Let k be a splitting field for G . There exists a bilinear map*

$$i_k: K_0(kG) \times G_0(kG) \rightarrow \mathbb{Z}$$

such that

$$(*) \quad i_k([U], [M]) = \dim_k(\text{Hom}_{kG}(U, M))$$

for all modules $U \in \mathcal{P}(kG)$ and $M \in {}_{kG}\text{mod.}^{\dagger}$. Moreover, letting $\{U_1, \dots, U_r\}$ and $\{F_1, \dots, F_r\}$ denote corresponding basic sets of indecomposable projective and simple kG -modules, respectively, we have

$$i_k([U_i], [F_j]) = \delta_{ij}, \quad 1 \leq i, j \leq r.$$

Proof. We first define i_k by $(*)$ above, and then extend by linearity to a map

$$i_k: K_0(kG) \times G_0(kG) \rightarrow \mathbb{Z}.$$

We have to show that i_k is well defined. First, let

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

be a ses of kG -modules, and let $U \in \mathcal{P}(kG)$. Then the sequence

$$0 \rightarrow \text{Hom}_{kG}(U, M') \rightarrow \text{Hom}_{kG}(U, M) \rightarrow \text{Hom}_{kG}(U, M'') \rightarrow 0$$

is exact. This follows from (2.22), since the functor $\text{Hom}(U, \cdot)$ is exact whenever U is projective. On the other hand, if

$$0 \rightarrow U' \rightarrow U \rightarrow U'' \rightarrow 0$$

[†] ${}_{kG}\text{mod}$ denotes the category of f.g. left kG -modules.

is a ses in $\mathcal{P}(kG)$, then $U \cong U' \dot{+} U''$, and hence

$$\text{Hom}_{kG}(U, M) \cong \text{Hom}_{kG}(U', M) \dot{+} \text{Hom}_{kG}(U'', M)$$

for all f.g. kG -modules M . From these remarks, it follows that i_k is a well defined bilinear map on the Grothendieck groups.

To prove the second statement, let us assume that the $\{U_i\}$ and $\{F_j\}$ correspond to each other as in §18A. Then by (18.1), $\text{rad } U_i$ is the unique maximal submodule of U_i , and $U_i/\text{rad } U_i \cong F_i$, $1 \leq i \leq r$. Since k is a splitting field, its follows that

$$\dim_k(\text{Hom}_{kG}(U_i, F_j)) = \delta_{ij}, \quad 1 \leq i, j \leq r,$$

completing the proof.

(18.9) Theorem. *The decomposition map*

$$d: G_0(KG) \rightarrow G_0(kG),$$

and the map

$$e: K_0(kG) \rightarrow G_0(KG) \quad (\text{defined by (18.3)}),$$

are transposes of one another with respect to the bilinear forms i_k and i_K . More precisely, we have

$$i_k(u, dz) = i_K(eu, z) \quad \forall u \in K_0(kG), z \in G_0(KG).$$

Proof. It is sufficient to prove the result for generators of $K_0(kG)$ and $G_0(KG)$, so we let $u = [U]$ and $z = [Z]$, for modules $U \in \mathcal{P}(kG)$ and $Z \in {}_{KG}\text{mod}$. Since RG is semiperfect, we may apply Theorem 18.2 to obtain an element $P \in \mathcal{P}(RG)$ such that $\bar{P} = U$; then $e[U] = K \otimes_R P$. On the other hand, let L be a full RG -lattice in Z ; then $d[Z] = [\bar{L}]$ in $G_0(kG)$. By the Change of Rings Theorem 2.38,

$$K \otimes_R \text{Hom}_{RG}(P, L) \cong \text{Hom}_{KG}(K \otimes_R P, K \otimes_R L).$$

But also $\text{Hom}_{RG}(RG, L) \cong L$ as RG -modules, and therefore

$$\overline{\text{Hom}_{RG}(RG, L)} \cong \bar{L} \cong \text{Hom}_{kG}(kG, \bar{L}).$$

Since P is projective and Hom is additive, the above result implies that

$$\overline{\text{Hom}_{RG}(P, L)} \cong \text{Hom}_{kG}(\bar{P}, \bar{L}).$$

Combining these observations, we obtain

$$\begin{aligned} i_K(e[U], [Z]) &= \dim_K(\text{Hom}_{KG}(K \otimes_R P, K \otimes_R L)) \\ &= \dim_k(\text{Hom}_{kG}(\bar{P}, \bar{L})) = \dim_k(\text{Hom}_{kG}(U, \bar{L})) = i_k([U], d[Z]), \end{aligned}$$

as required.

(18.10) Corollary. *Let \mathbf{C} be the Cartan matrix and \mathbf{D} the decomposition matrix of G , for the p -modular system (K, R, k) . Then \mathbf{C} is a symmetric matrix, and we have*

$$\mathbf{C} = {}^t \mathbf{D} \mathbf{D}.$$

Proof. Let ${}^t \mathbf{E}$ be the matrix of the map $e: K_0(kG) \rightarrow G_0(KG)$, with respect to the bases $\{[U_i]\}_{1 \leq i \leq r}$ and $\{[Z_j]\}_{1 \leq j \leq s}$. By the preceding theorem, we have $\mathbf{E} = {}^t \mathbf{D}$. On the other hand, $c = d \circ e$, by Proposition 18.5. Using the definition of the matrices \mathbf{C} and \mathbf{D} , we obtain

$$\mathbf{C} = \mathbf{E} \cdot \mathbf{D} = {}^t \mathbf{D} \mathbf{D}.$$

Thus ${}^t \mathbf{C} = \mathbf{C}$, and the proof is complete.

For another version of this proof, in different notation, see CR (83.9).

(18.11) Corollary. *Assume that $p \nmid |G|$. Then $G = G_{p'}$, $r = s$, \mathbf{C} is the identity matrix, and \mathbf{D} is a permutation matrix. Every Brauer character of a kG -module coincides with the K -character of a KG -module.*

The proof is immediate from Corollary 18.10, since in this case kG is a split semisimple k -algebra, and the number of simple kG -modules equals the number of conjugacy classes of G , by (3.37). For a direct proof of this corollary, see Exercise 18.4.

The next result is the source of several other properties of the Cartan-Brauer triangle, and is of independent interest.

(18.12) Theorem (The Brauer lift). *Let λ be the Brauer character of a left kG -module L , and extend λ to a class function $\hat{\lambda}$ on G by setting*

$$\hat{\lambda}(x) = \lambda(s), \quad x \in G,$$

where s is the p' -part of x . Then $\hat{\lambda}$ is a virtual K -character of G .

Proof. It is clear that $\hat{\lambda} \in \text{cf}_K(G)$. By Brauer's criterion for virtual characters (15.15), it is sufficient to prove that $\hat{\lambda}_H \in \text{ch } KH$ for every elementary subgroup H of G . Such a subgroup can be expressed as a direct product

$H = A \times B$, where A is a p' -group and B is a p -group. The restriction L_H is a kH -module whose Brauer character is λ_H , and $\hat{\lambda}_H$ has the same relation to λ_H as in the general case. Thus it is sufficient to prove the theorem for an elementary group $H = A \times B$, and a kH -module L with Brauer character λ , and where $\hat{\lambda}$ is defined as in the statement of the theorem. Now λ_A is the Brauer character of the kH -module L_A . Since A is a p' -group, we can apply Corollary 18.11 to find a KA -module M whose K -character coincides with λ_A . Then the outer tensor product $M \# 1_B$ of M with the trivial KB -module 1_B is a KH -module whose character clearly coincides with $\hat{\lambda}$, and the proof is finished.

(18.13) Definition. The virtual K -character $\hat{\lambda}$, associated with a Brauer character λ of G as in (18.12), is called the *Brauer lift* of λ .

The Brauer lift was first defined by Green [55b], and played a fundamental role in his determination of the irreducible complex-valued characters of the general linear groups over finite fields.

(18.14) Corollary. *The decomposition map*

$$d: G_0(KG) \rightarrow G_0(kG)$$

is surjective.

Proof. By (17.15), it is sufficient to prove that each Brauer character λ is the restriction $\hat{\lambda}_{G_p}$ of its Brauer lift $\hat{\lambda}$, and this is clear from the definition.

(18.15) Corollary. *The map $e: K_0(kG) \rightarrow G_0(KG)$ is injective.*

Proof. Let $u \in \ker e$. By (18.9), it follows that $i_k(u, dz) = 0$ for all $z \in G_0(KG)$, and so $i_k(u, v) = 0$ for all $v \in G_0(kG)$ because d is surjective. By (18.8), $K_0(kG)$ and $G_0(kG)$ admit dual bases with respect to the form i_k ; hence $u = 0$, which proves that e is injective.

An immediate consequence of (18.15) is the following interesting result:

(18.16) Corollary. *Suppose P and $P' \in \mathcal{P}(RG)$ are such that the KG -modules $K \otimes_R P$ and $K \otimes_R P'$ are isomorphic. Then $P \cong P'$ as RG -modules.*

This result can also be obtained as a special case of Hattori's Theorem 32.5. A second proof of (18.16), using the invertibility of the Cartan matrix, is given in Exercise 18.14; see also (21.21).

A final corollary provides some number-theoretic information about the decomposition matrix.

(18.17) Corollary. *The invariant factors of the $s \times r$ matrix \mathbf{D} are $\{1, 1, \dots, 1\}$ (r times). For $1 \leq h \leq r$, the G.C.D. of the h -rowed minors of \mathbf{D} is equal to 1. The matrix \mathbf{D} has rank r over the field k .*

Proof. The decomposition matrix $\mathbf{D} = (d_{ij})$ is the transpose of the matrix of the decomposition map $d: G_0(KG) \rightarrow G_0(kG)$ with respect to the bases $\{[Z_i]\}_{1 \leq i \leq s}$ and $\{[F_j]\}_{1 \leq j \leq r}$. Thus

$$d[Z_i] = \sum_{j=1}^r d_{ij}[F_j], \quad 1 \leq i \leq s.$$

By the Invariant Factor Theorem (CR (16.8)) applied to the pair of \mathbb{Z} -modules $d(G_0(KG)) \subseteq G_0(kG)$, we can find a \mathbb{Z} -basis $\{f_1, \dots, f_r\}$ of $G_0(kG)$, and positive integers $\delta_1, \dots, \delta_t$ for some $t \leq r$, such that $\{\delta_1 f_1, \dots, \delta_t f_t\}$ is a \mathbb{Z} -basis for $d(G_0(KG))$, and $\delta_i | \delta_{i+1}$ for each i . These $\{\delta_i\}$ are the *invariant factors* of \mathbf{D} . From CR §16, this corresponds to finding \mathbb{Z} -unimodular matrices $\mathbf{X}^{s \times s}$ and $\mathbf{Y}^{r \times r}$ such that

$$\mathbf{X}\mathbf{D}\mathbf{Y} = \begin{bmatrix} \delta_1 & & & \\ & \ddots & & \\ & & \delta_t & \\ & & & 0 \\ & & & & \ddots \\ & & & & & 0 \end{bmatrix}.$$

Since d is surjective by (18.14), we deduce that $t=r$, and each of the invariant factors $\{\delta_i\}_{1 \leq i \leq r}$ is equal to 1. From CR §16, this implies that the G.C.D. of the h -rowed minors of \mathbf{D} is equal to 1, for $1 \leq h \leq r$. Finally, since $\bar{\mathbf{X}}$ and $\bar{\mathbf{Y}}$ are invertible matrices over k , and

$$\bar{\mathbf{X}}\bar{\mathbf{D}}\bar{\mathbf{Y}} = \begin{bmatrix} 1 & & \\ & \ddots & \\ & & 1 \end{bmatrix},$$

it follows that $\bar{\mathbf{D}}$ has rank r , and the proof is completed.

§18C. Orthogonality Relations for Brauer Characters

We keep the notation and assumptions of §18B, that is, (K, R, k) is a p -modular system with $\text{char } K = 0$, such that K is sufficiently large relative to G , and RG is a semiperfect ring.

We first extend the character table data (9.25) to encompass Brauer characters. Recall from (17.11) that the number of simple kG -modules is equal to the number r of p -regular classes in G . See also (17.6).

(18.18) Brauer Character Table Data. $\{Z_i\}, \{\zeta^i\}$, $z_i = \deg \zeta^i$, $\{\mathfrak{C}_i\}$, $h_i = |\mathfrak{C}_i|$, ζ_j^i, ζ_{j*}^i as in (9.25), for $1 \leq i, j \leq s$. (We write ζ^i instead of $\zeta^{(i)}$, for convenience.)

$\{\mathfrak{C}_1 = \{1\}, \mathfrak{C}_2, \dots, \mathfrak{C}_r\}$ = p -regular conjugacy classes in G .

$\{F_1 = 1_G, \dots, F_r\}$ = basic set of simple kG -modules.

$\{\varphi^1, \dots, \varphi^r\}$ = Brauer characters afforded by F_1, \dots, F_r .

$\{U_1, \dots, U_r\}$ = indecomposable projective modules, with U_i the projective cover of F_i , $1 \leq i \leq r$. The $\{U_i\}$ are also called *principal indecomposable modules*.

$\{\eta^1, \dots, \eta^r\}$ = Brauer characters of $\{U_1, \dots, U_r\}$.

$\{P_1, \dots, P_r\}$ = basic set of indecomposable projective RG -modules, with $P_i = U_i$, $1 \leq i \leq r$.

$\varphi_j^i, \varphi_{j*}^i, \eta_j^i, \eta_{j*}^i$, $1 \leq i, j \leq n$, values of the Brauer characters φ^i, η^i on the classes $\mathfrak{C}_j, \mathfrak{C}_{j*}$, respectively.

$\mathbf{C} = (c_{ij})$ = Cartan matrix.

$\mathbf{D} = (d_{ij})$ = decomposition matrix.

$\Phi = (\varphi_j^i)^{r \times r}$, $H = (\eta_j^i)^{r \times r}$, $Z = (\zeta_j^i)^{s \times r}$.

By (17.15) and (17.10), we have

$$(18.19) \quad \zeta' \Big|_{G_p} = \sum_{j=1}^r d_{ij} \varphi^j, \quad 1 \leq i \leq s,$$

$$(18.20) \quad \eta^i = \sum_{j=1}^r c_{ij} \varphi^j, \quad 1 \leq i \leq r.$$

From these results, we obtain,

$$(18.21) \quad Z = D\Phi, \quad H = C\Phi$$

(18.22) Lemma. (i) Φ is unimodular over R .

(ii) $\det \mathbf{C} \neq 0$.

Proof. By (17.2), k is a splitting field for G , so by (17.3) the k -characters of $\{F_1, \dots, F_r\}$ are linearly independent over k . These characters are determined by the rows of the matrix Φ , by (17.5ii) and thus $\det \Phi \neq 0$ in k . Since R is a local ring with residue field k , $\det \Phi$ is a unit in R , proving (i).

In order to prove (ii), we first apply the Second Orthogonality Relation (9.26) to obtain

$$\sum_{m=1}^s \xi_i^m \xi_j^m = (|G| h_i^{-1} \delta_{ij})^{r \times r}$$

and hence $\det {}^t \mathbf{Z} \mathbf{Z} \neq 0$. By (18.21) and (18.10) we have

$${}^t \mathbf{Z} \mathbf{Z} = {}^t \Phi {}^t \mathbf{D} \mathbf{D} \Phi = {}^t \Phi \mathbf{C} \Phi.$$

Since $\det {}^t \mathbf{Z} \mathbf{Z} \neq 0$ and Φ is unimodular by part (i), we obtain $\det \mathbf{C} \neq 0$, and the lemma is proved.

(18.23) Theorem (Orthogonality relations for Brauer characters).

$$(i) \quad \sum_{j=1}^r h_j \varphi_j^i \eta_{j*}^k = |G| \delta_{ik}.$$

$$(ii) \quad \sum_{j=1}^r h_j \varphi_j^i \varphi_{j*}^k = |G| \gamma_{ik}, \text{ where } \mathbf{C}^{-1} = (\gamma_{ij}).$$

$$(iii) \quad \sum_{j=1}^r h_j \eta_j^i \eta_{j*}^k = |G| c_{ik}.$$

Proof. We first note that \mathbf{C} is invertible by Lemma 18.22, so that \mathbf{C}^{-1} is defined. From the proof of (18.22), (18.21) and (18.10), we have:

$${}^t \mathbf{Z} \mathbf{Z} = \mathbf{Y}, \quad \mathbf{Z} = \mathbf{D} \Phi, \quad \mathbf{H} = \mathbf{C} \Phi = {}^t \mathbf{D} \mathbf{Z},$$

where

$$\mathbf{Y} = (|G| h_i^{-1} \delta_{ij*}).$$

From these we obtain

$$\Phi \mathbf{Y}^{-1} {}^t \Phi = \mathbf{C}^{-1}, \quad \Phi \mathbf{Y}^{-1} {}^t \mathbf{H} = \mathbf{I}, \quad \text{and } \mathbf{H} \mathbf{Y}^{-1} {}^t \mathbf{H} = \mathbf{C}.$$

These formulas in turn imply (ii), (i), and (iii) above, completing the proof.

Before obtaining some interesting consequences, we need a variation on the Brauer lift (18.12), as follows:

(18.24) Lemma. Let $|G| = p^a m$, with $p \nmid m$. Let λ be a Brauer character of a kG -module L . Define

$$\theta(x) = \begin{cases} p^a \lambda(x), & x \in G_{p'}, \\ 0, & x \notin G_{p'}. \end{cases}$$

Then θ is a virtual character of G .

Proof. By Brauer's criterion (15.15), we have to prove that $\theta|_H$ is a virtual character of H for every elementary subgroup H . As in the proof of (18.12), we can express H in the form $H = A \times B$, for a p' -subgroup A and a p -group B of order p^t , where $t \leq a$. Let ρ_B be the regular character of B , and define a K -valued function ψ on H by

$$\psi(ab) = \lambda(a)\rho_B(b), \quad a \in A, b \in B.$$

From the proof of Theorem 18.12, $\lambda|_A$ is a K -character of A , and hence ψ is a K -character of H . For $x \in H_{p'}$, we have $x \in A$, and

$$\psi(x) = |B|\lambda(x) = p^t\lambda(x) = p^{t-a}\theta(x).$$

Then $\theta(x) = p^{a-t}\psi(x)$. The same formula holds for p -irregular x in H , since ρ_B vanishes on the elements in $B - \{1\}$. Thus $\theta \in \text{ch } KH$ for every elementary subgroup H , so $\theta \in \text{ch } KG$, as required.

(18.25) Theorem. $\det \mathbf{C} = p^l$, for some nonnegative integer l .

Proof. Let $|G| = p^a m$ as in (18.24) and let $\theta_i \in \text{ch } KG$ be the virtual character defined in (18.24) corresponding to the irreducible Brauer character φ^i , for $1 \leq i \leq r$. Let $\theta_i = \sum_{j=1}^r a_{ij} \zeta^j$, where $a_{ij} \in \mathbb{Z}$, for $1 \leq i \leq r$. Then from (9.24), we have

$$\begin{aligned} a_{ij} &= (\theta_i, \zeta^j) = |G|^{-1} \sum_{x \in G} \theta_i(x^{-1}) \zeta^j(x) \\ &= p^a |G|^{-1} \sum_{x \in G_{p'}} \varphi^i(x^{-1}) \zeta^j(x) = p^a |G|^{-1} \sum_{x \in G_{p'}} \varphi^i(x^{-1}) \sum_{k=1}^r d_{jk} \varphi^k(x) \\ &= p^a \sum_{k=1}^r d_{jk} \left\{ |G|^{-1} \sum_{x \in G_{p'}} \varphi^i(x^{-1}) \varphi^k(x) \right\} = p^a \sum_{k=1}^r d_{jk} \gamma_{ki}, \end{aligned}$$

where $\mathbf{C}^{-1} = (\gamma_{ij})$, by (18.23ii). But \mathbf{C}^{-1} is a symmetric matrix, and $\mathbf{A} = (a_{ij})$ satisfies the equation

$$\mathbf{A} = p^a \mathbf{C}^{-1 \top} \mathbf{D}.$$

Then, by (18.10),

$$\mathbf{A} \cdot {}^\top \mathbf{A} = p^{2a} \mathbf{C}^{-1 \top} \mathbf{D} \mathbf{D}^\top \mathbf{C}^{-1} = p^{2a} \mathbf{C}^{-1}.$$

Thus

$$(\det \mathbf{C})(\det(\mathbf{A} \cdot {}^\top \mathbf{A})) = \text{power of } p,$$

completing the proof. For a more conceptual proof, see (21.22) and (21.24) below.

(18.26) Theorem. Let $\{P_1, \dots, P_r\}$ be a basic set of indecomposable projective RG -modules, as in (18.18), and let τ_i be the K -character afforded by the KG -module $K \otimes_R P_i$, $1 \leq i \leq r$. Then the following statements hold:

$$(i) \quad \tau_i = \sum_{j=1}^s d_{ji} \xi^j, \quad 1 \leq i \leq r.$$

$$(ii) \quad \tau_i(x) = 0 \text{ for all } p\text{-irregular } x \in G.$$

(iii) $\{\tau_1, \dots, \tau_r\}$ form a \mathbb{Z} -basis for the set of virtual K -characters of G which vanish on the p -irregular elements of G .

Proof. Fix i between 1 and r . By Proposition 17.5(iv), $\tau_i|_{G_p} = \eta^i$ since $\overline{P}_i = U_i$. By (18.9) and (18.8), we have

$$\begin{aligned} i_K([K \otimes_R P_i], [Z_j]) &= i_k([U_i], [\overline{Z_j}]) \\ &= i_k\left([U_i], \sum_{h=1}^r d_{jh} [F_h]\right) = d_{ji}. \end{aligned}$$

Since τ_i is the character afforded by $K \otimes_R P_i$, we have $(\tau_i, \xi^j) = d_{ji}$ by the definition of the bilinear form i_K ; hence

$$\tau_i = \sum_{j=1}^s d_{ji} \xi^j,$$

proving (i). This also shows that the $\{\tau_i\}$ are linearly independent, by (18.17).

We next prove that each character τ_i vanishes on the p -irregular classes of G . From the orthogonality relations for the $\{\xi^i\}$ and (18.10), we obtain

$$|G|^{-1} \sum_{x \in G} |\tau_i(x)|^2 = \sum_{j=1}^s d_{ji}^2 = c_{ii}.$$

On the other hand, from (18.23) we have

$$|G|^{-1} \sum_{y \in G_p} |\tau_i(y)|^2 = |G|^{-1} \sum_{j=1}^r h_j \eta_j^i \eta_{j*}^i = c_{ii}.$$

Comparing these results, we see that $\tau_i(x) = 0$ for all $x \notin G_p$, and (ii) is established.

Finally, to prove (iii), we have to show that if $\theta \in \text{ch } KG$ is a virtual character vanishing on the p -irregular classes, then θ is a \mathbb{Z} -linear combination of the $\{\tau_i\}$. We put

$$\theta = \sum a_i \tau_i,$$

and try to solve for coefficients $\{a_i\}$ in \mathbf{Z} . The problem is to solve the equations

$$\theta(x_i) = \sum_{j=1}^r a_j \tau_j(x_i) = \sum_{j=1}^r a_j \eta'_i, \text{ where } x_i \in \mathfrak{C}_i, 1 \leq i \leq r.$$

The coefficient matrix is $\mathbf{H} = \mathbf{C}\Phi$, and is invertible since both \mathbf{C} and Φ are invertible. It remains to show that the solutions $\{a_i\}$ are integers. By Theorem 18.23, we have

$$a_j = |G|^{-1} \sum_{i=1}^r h_i \theta(x_i) \varphi_{i*}^j.$$

Since the decomposition map is surjective by (18.14), we may write

$$\varphi_{i*}^j = \sum_{k=1}^s m_{jk} \xi_{i*}^k$$

for some integers $\{m_{jk}\}$. Since θ' is a virtual character vanishing on the p -irregular classes, we obtain

$$a_j = |G|^{-1} \sum_{i=1}^r \sum_{k=1}^s h_i \theta(x_i) m_{jk} \xi_{i*}^k = \sum_{k=1}^s m_{jk} (\theta, \xi^k) \in \mathbf{Z},$$

completing the proof. For another proof of (ii), see Theorem 32.15.

We can now state the following additional properties of the Cartan-Brauer Triangle (18.5):

(18.27) Proposition. (i) *The Cartan homomorphism $c: K_0(kG) \rightarrow G_0(kG)$ is injective, and $\text{cok } c (= G_0(kG)/\text{im } c)$ is a finite group of order a power of p .*

(ii) *$\text{im } e$ consists of all $a \in G_0(KG)$ whose virtual character α (see (16.10)) vanishes on the p -irregular classes.*

(iii) *The map $e: K_0(kG) \rightarrow G_0(KG)$ is a split injection, that is, e is injective and $\text{im } e$ is a \mathbf{Z} -direct summand of $G_0(KG)$.*

Proof. Assertion (i) is a restatement of (18.25), while (ii) is a direct consequence of the definition of e and (18.26iii). Further, e is injective by (18.15). Finally, by assertion (ii) we can identify $\text{im } e$ with the \mathbf{Z} -submodule of $\text{ch } KG$ consisting of all virtual characters which vanish outside $G_{p'}$. Therefore $\text{im } e$ is a \mathbf{Z} -pure submodule of $\text{ch } KG$, and hence (see §4D) is a direct summand of $\text{ch } KG$. This completes the proof.

Another proof of (18.27ii) is given in Steps 1 and 2 of the proof of (32.16) below. See also (21.20).

We conclude this section with a number of interesting examples, and begin with:

(i) *Characters of defect zero.* The p -defect (or simply *defect*) of $\xi \in \text{Irr } G$ is the exponent to which p divides $|G|/\xi(1)$. Thus ξ is of *defect zero* if $|G|_p$ divides $\xi(1)$ (see CR §86).

(18.28) Proposition. *Let $\xi \in \text{Irr } G$ be a character of defect zero. Then $\xi = \tau_i$ for some character τ_i , $1 \leq i \leq r$, afforded by KP_i , where P_i is a projective indecomposable RG-module. Moreover, \bar{P}_i is a simple kG-module, and is also a projective kG-module.*

Proof. Let Z be a simple KG -module affording ξ . Since ξ has defect zero, the central primitive idempotent ϵ corresponding to ξ belongs to RG , by (9.21ii). For some indecomposable projective RG -module P_i , Z is a composition factor of $KP_i (= K \otimes_R P_i)$. Then $\epsilon P_i \neq 0$. If $\epsilon P_i \neq P_i$, then since ϵ is a central idempotent of RG , the formula $P_i = \epsilon P_i \oplus (1 - \epsilon)P_i$ gives an RG -decomposition of P_i , which is impossible. Therefore $\epsilon P_i = P_i$, which implies at once that $\tau_i = a\xi$ for some positive integer a .

It now follows from (18.26ii) that ξ vanishes on all p -irregular elements of G . Hence by (18.26iii), ξ is expressible as a \mathbb{Z} -linear combination of the $\{\tau_j\}_{1 \leq j \leq n}$. Since $\xi = a^{-1}\tau_i$, this proves that $a = 1$, and that furthermore the index i is uniquely determined by ξ .

We deduce that exactly one of the decomposition numbers $\{d_{ji}\}$ in (18.26i) is nonzero, and must equal 1. Since $\mathbf{C} = {}^t \mathbf{D} \mathbf{D}$, this implies that \bar{P}_i is simple. Thus we have $\bar{P}_i = U_i = F_i$, completing the proof. (Gallagher's Theorem 15.19 is an easy consequence of this Theorem.)

Our next example shows how characters of defect zero may arise:

(ii) *The Steinberg character of $SL_2(q)$.* Let $G = SL_2(q)$, the group of 2×2 matrices of determinant 1 over a finite field \mathbf{F}_q of q elements, and let p be the characteristic of \mathbf{F}_q . Let B be the subgroup of G consisting of all upper triangular matrices. As an exercise, we ask the reader to show that

$$G = B \cup (BxB),$$

for some $x \notin B$. From Exercise 10.3 it follows that the permutation character $\theta = 1_B|_G$ satisfies $(\theta, \theta) = 2$, and hence $\theta = 1_G + \xi$ for an irreducible character ξ of degree $|G : B| - 1$. Since $|G| = q(q^2 - 1)$ and $|B| = q(q-1)$, we have $|G : B| = q+1$, and $\xi(1) = q$. Then ξ is an irreducible character of p -defect zero, and satisfies all the conditions of Proposition 18.28. The character ξ is called the

Steinberg character of G . In Chapter 7 we shall prove that all finite groups with BN -pairs have a Steinberg character which behaves according to (18.28), and plays a special role in the representation theory of G . (See Steinberg [56], [57] for the construction of a representation affording the Steinberg characters of Chevalley groups, and Curtis [66] for a construction of the character for finite groups with a BN -pair.)

As a final example, we continue the discussion of Example (ii) following (16.20). Let $G = S_4$, $p = 2$, and let (Q, R, k) be the 2-modular system in which R is the ring of 2-adic integers in the rational field Q , and $k = R/2R \cong \mathbb{Z}/2\mathbb{Z}$. The character table of S_4 is given at the end of §9D. The reader should verify that the Brauer character table is given by

	x_1	x_3
φ^1	1	1
φ^2	2	-1

where $x_1 = 1$, $x_3 = (123)$. The formula $C = {}^t D D$ gives

$$C = \begin{pmatrix} 4 & 2 \\ 2 & 3 \end{pmatrix}.$$

Further, the characters of G afforded by the indecomposable projective RG -modules are

$$\tau_1 = \sum d_{j1} \zeta^j = \zeta^1 + \zeta^2 + \zeta^4 + \zeta^5$$

$$\tau_2 = \sum d_{j2} \zeta^j = \zeta^3 + \zeta^4 + \zeta^5,$$

and both of these vanish on the 2-irregular classes. There are two indecomposable projective kG -modules U_1, U_2 , both of k -dimension 8.

The reader should now carry out a similar calculation for the case where $p = 3$. In this situation, the characters ζ^4 and ζ^5 have defect zero.

§18. Exercises

- Using the notation of (18.8), show that

$$\dim_k \text{Hom}_{kG}(U_i, U_j) = c_{ij}, \quad 1 \leq i, j \leq r.$$

[Hint: The left hand expression equals $i_k([U_i], [U_j])$, and $[U_j] = \sum_m c_{jm} [F_m]$ in $G_0(kG)$.]

- Let G be a p -group, k a field of characteristic p . Show that kG has a unique minimal left ideal, given by $k \cdot s$, where

$$s = \sum_{\sigma \in G} \sigma.$$

3. Let k be a field of characteristic p , E a finite Galois extension of k whose Galois group G is a p -group. Let $T: E \rightarrow k$ be the trace map, and let $\alpha \in E$ be such that $T(\alpha) \neq 0$. Prove that α generates a normal basis for E over k , that is,

$$E = \bigoplus_{\sigma \in G} k \cdot \sigma(\alpha).$$

Show further that such elements α exist.

[Hint: (Childs-Orzech [81]). It suffices to show that the elements $\{\sigma(\alpha) : \sigma \in G\}$ are linearly independent over k . Suppose not, so $\xi_0 \alpha = 0$ for some nonzero $\xi_0 \in kG$. Then

$$\{\xi \in kG : \xi \alpha = 0\}$$

is a nonzero ideal of kG , and therefore contains $\sum_{\sigma \in G} \sigma$ by the preceding Exercise. Thus $\left(\sum_{\sigma} \sigma \right) \alpha = 0$, that is, $T(\alpha) = 0$.

To prove the existence of elements of E of nonzero trace, use the fact that E is separable over k ; see §7A and Exercise 7.12.]

4. Let (K, R, k) be a p -modular system such that RG is a semiperfect ring, where G is a finite p' -group. Show that

- (a) The simple left kG -modules $\{F_i : 1 \leq i \leq r\}$ coincide with the projective indecomposable modules $\{U_i : 1 \leq i \leq r\}$.
- (b) For each i , $1 \leq i \leq r$, there exists a projective RG -lattice P_i such that $\bar{P}_i = F_i$, where bar denotes reduction mod \mathfrak{p} .
- (c) For each i , $KP_i (= K \otimes_R P_i)$ is a simple left KG -module such that $d[KP_i] = [F_i]$, where d is the decomposition map defined in (16.17).
- (d) The modules $\{KP_i : 1 \leq i \leq r\}$ are a basic set of simple left KG -modules.

[Hint: Both KG and kG are semisimple, since $|G| \neq 0$ in both K and k . Then $RG/\text{rad } RG \cong kG$, $\text{rad } kG = 0$, so (a) and (b) follows from (18.1). By definition of d , we have $d[KP_i] = F_i$ and KP_i is therefore simple. Finally, KG is a direct sum of copies of the $\{KP_i\}$, since RG is a direct sum of copies of the lattices $\{P_i\}$; this implies that (d) is valid.]

Another proof of these assertions is given in (18.11), using the formula for the Cartan matrix in terms of the decomposition matrix. A related result is given in (30.16) below; see also Exercise 19.3.

As pointed out at the beginning of §18A, the ring RG will be semiperfect whenever K is sufficiently large relative to G , and also whenever R is a complete d.v.r. Without such a restriction on RG , assertion (b) above need not be valid, since idempotents in kG need not come from idempotents in RG . For example, let R be the 2-adic valuation ring in the rational field \mathbb{Q} , and let G be a cyclic group of order 7. Then $k = \mathbb{Z}/2\mathbb{Z}$, and G has 3 irreducible representations over k , since $x^7 - 1 = (x-1)f(x)g(x)$ in $k[x]$, with $f(x), g(x)$ distinct irreducible polynomials of degree 3. On the other hand, G has only 2 irreducible representations over \mathbb{Q} , since $x^7 - 1 = (x-1)\Phi_7(x)$ in $\mathbb{Q}[x]$, where $\Phi_7(x)$ is the cyclotomic polynomial of order 7 and degree 6.]

In the remaining exercises, G denotes a finite group, and (K, R, k) a p -modular system such that K is sufficiently large relative to G .

5. For each i , $1 \leq i \leq r$, let η^i denote the Brauer character of the indecomposable projective kG -module U_i . Prove that the degree $\eta^i(1)$ is a multiple of $|G|_p$.

[Hint: Let S be a Sylow p -subgroup of G . Then kG is a free left kS -module. Deduce from this that the restriction $(U_i)_S$ is a projective left kS -module, and hence a free left kS -module, since kS is a local ring (see (5.24)). Also see Example (i) following (19.16).]

6. Prove that the diagonal entry c_{ii} of the Cartan matrix is ≥ 2 unless the corresponding module U_i is a simple kG -module.

[Hint: Apply (18.1vi).]

7. Let G be an elementary group (see Definition 15.7). Prove that the image of the Cartan map $c: K_0(kG) \rightarrow G_0(kG)$ is $|G|_p \cdot G_0(kG)$.

[Hint: Write G in the form $H \times S$, where H is a p' -group and S is a p -group, so $|S|=|G|_p$. Then $kH = \bigoplus V_i$, where the $\{V_i\}$ are simple left kH -modules, not necessarily distinct. Since $kG \cong kH \otimes_k kS$ as k -algebras, it follows that

$$kG = \bigoplus_i (V_i \# kS),$$

where $V_i \# kS$ is an outer tensor product. This gives the decomposition of kG into indecomposable projective summands. Since the trivial S -module k occurs with multiplicity $|S|$ as composition factor of kS , it follows that

$$c[V_i \# kS] = |S|[V_i] \text{ in } G_0(kG).$$

Another approach is as follows: By Exercise 9.6,

$$\mathrm{Irr}_K G = \{\lambda\mu : \lambda \in \mathrm{Irr}_K H, \mu \in \mathrm{Irr}_K S\}.$$

Extend each λ to a character λ^* on G which is trivial on S . By (17.11) and (18.11), the λ 's are the irreducible Brauer characters of H , and the λ^* 's those of G . Now compute the decomposition matrix of $d: G_0(KG) \rightarrow G_0(kG)$ from the formula

$$\lambda\mu|_{G_p} = \lambda^*,$$

and then use (18.10) to find the Cartan matrix of G .]

8. (Gustafson). Prove that every simple kG -module is one-dimensional if and only if $G = S \rtimes A$, where A is abelian and S is a Sylow p -subgroup of G .

9. For $H \leq G$, prove that there is a commutative diagram of additive groups and homomorphisms:

$$\begin{array}{ccccc} G_0(KG) & \xrightarrow{d} & G_0(kG) & \xrightarrow{c} & K_0(kG) \\ \mathrm{ind}_H^G \uparrow & & \mathrm{ind}_H^G \uparrow & & \mathrm{ind}_H^G \uparrow \\ G_0(KH) & \xrightarrow{d} & G_0(kH) & \xrightarrow{c} & K_0(kH). \end{array}$$

Here, the d 's and c 's are decomposition maps and Cartan maps, respectively, and maps ind_H^G are given by

$$\text{ind}_H^G[M] = [M^G],$$

where M is either a KH - or a kH -module.

[Hint: See §21B if need be.]

10. Let $H \leq G$, and let L be a kH -module with Brauer character λ . Define a class function λ^G on $G_{p'}$ by the formula

$$\lambda^G(x) = |H|^{-1} \sum_{y \in G} \lambda(yxy^{-1}), \quad x \in G_{p'},$$

as in (10.3). Prove that λ^G is the Brauer character of the induced kG -module L^G .

[Hint: By (18.12), there exists a virtual character $\tilde{\lambda}$ of H such that $\tilde{\lambda}|_{H_p} = \lambda$. Then $\tilde{\lambda} = \mu - \nu$, where μ and ν are K -characters of H afforded by KH -modules M and N , respectively. We have $d([M] - [N]) = [L]$ in $G_0(kH)$, by (17.5iv) and (17.15). By Exercise 9, we obtain

$$d([M^G] - [N^G]) = [L^G] \text{ in } G_0(kG).$$

Again using (17.5iv) and (17.15), it follows that the Brauer character of L^G is $(\mu - \nu)^G|_{G_{p'}}$, and this restriction is λ^G . (For a different proof, see Brauer-Nesbitt [41, p. 580].)

11. Let $H \leq G$, and let $\{\varphi^i, \eta^j\}$ be defined as in (18.18) for G , and let the corresponding types of Brauer characters for H be given by $\{\hat{\varphi}^i, \hat{\eta}^j\}$. Prove the formulas of Nakayama (see Brauer-Nesbitt [41, §26]), which are as follows:

There exists non-negative integers $\{a_{ij}\}$ and $\{b_{ij}\}$ such that

$$(\hat{\eta}^i)^G = \sum_j a_{ij} \eta^j \text{ on } G_{p'}, \quad \varphi^j|_{H_{p'}} = \sum_i a_{ij} \hat{\varphi}^i \text{ on } H_{p'},$$

$$(\hat{\varphi}^i)^G = \sum_j b_{ij} \varphi^j \text{ on } G_{p'}, \quad \eta^j|_{H_{p'}} = \sum_i b_{ij} \hat{\eta}^i \text{ on } H_{p'}.$$

[Hint: For each indecomposable projective kH -module \hat{U}_l , the induced module $(\hat{U}_l)^G$ is kG -projective, so that the desired equation holds for $(\hat{\eta}^i)^G$ for some choice of $\{a_{ij}\}$. Then

$$a_{ij} = |G|^{-1} \sum_{x \in G_{p'}} (\hat{\eta}^i)^G(x) \varphi^j(x^{-1})$$

by (18.23i). The method of proof of the Frobenius Reciprocity Formula 10.9 then gives

$$a_{ij} = |H|^{-1} \sum_{y \in H_{p'}} \hat{\eta}^i(y) \varphi^j(y^{-1}),$$

which implies the desired formula for $\varphi^j|_{H_{p'}}$, by (18.23i). The other formulas are proved similarly.]

12. Let $H \leq G$, and let $\xi \in \text{Bch } kG$, $\xi \in \text{Bch } kH$. Prove that

$$(\xi|_{H_p})\xi \in \text{Bch } kH, \quad \xi \cdot \xi^G \in \text{Bch } kG,$$

and then show that

$$\xi \cdot \xi^G = \{(\xi|_{H_p})\xi\}^G \text{ in } \text{Bch } kG.$$

[Hint: This result is the analogue of (15.5) for Brauer characters. To prove it, use (17.13) and Exercise 10, and the method of proof of (15.5).]

13. Brauer Induction Theorem for Brauer Characters.

Prove that

$$\text{Bch } kG = \sum_{H \in \mathcal{E}} (\text{Bch } kH)^G,$$

where \mathcal{E} is the family of elementary subgroups of G , and $(\text{Bch } kH)^G$ is the set of all virtual Brauer characters λ^G , for $\lambda \in \text{Bch } kH$.

[Hint: By the Brauer Induction Theorem 15.9, we have

$$1_G = \sum a_i \lambda_i^G, \text{ where } a_i \in \mathbb{Z}, \lambda_i \in \text{ch } KH_i, H_i \in \mathcal{E}.$$

Then on G_p we have $1_G = \sum a_i (\lambda_i^G)_{G_p}$. Using (17.5iv), show that for each i ,

$$\lambda_i|_{(H_i)_{p'}} \in \text{Bch } kH_i, \text{ and } (\lambda_i^G)_{G_p} = \text{ind}_{H_i}^G \lambda_i|_{(H_i)_{p'}}.$$

Then use Exercise 10 to show that the Brauer character 1_G is a \mathbb{Z} -linear combination of Brauer characters in $(\text{Bch } kH_i)^G$, for $H_i \in \mathcal{E}$. Finally, use the idea of the proof of (15.9), together with Exercise 12, to complete the proof.]

14. Prove (18.16) as follows: Since $K \otimes_R P \cong K \otimes_R P'$, the kG -modules \bar{P}, \bar{P}' have the same composition factors. Therefore $\bar{P} \cong \bar{P}'$ since C is non-singular. This implies that $P \cong P'$ by (6.6).

§19. VERTICES AND SOURCES

Let (K, R, k) be a p -modular system, and let V be a simple KG -module, for a finite group G . Let M be a full RG -lattice in V . By Exercise 16.7, M is an indecomposable RG -lattice. Thus the classification of indecomposable RG -lattices is closely connected with the investigation of simple KG -modules and their characters. In §§19 and 20 we present an introduction to Green's work on indecomposable RG -lattices. It is here, for the first time, that we see the deep relationships between representation theory and the p -local structure of G , described in the introduction to the chapter. Green's work also provides powerful methods for understanding Brauer's theory of blocks (Chapter 9).

§19A. Relative Projective and Injective Modules over Group Rings

The theory of vertices and sources (Green [59], [62]) is based on the results of Gaschütz [52] on relative projective and injective modules over group rings. For remarks on the background, and extensions to ring theory, see CR §§62 and 63.

Throughout §19A, R denotes an arbitrary commutative ring, and (G, H) a pair consisting of a finite group G and a subgroup H of G . All RG -modules are assumed to be f.g./ R as usual. In this section and the next, we use the notation

$$M|N$$

to indicate that the RG -module M is isomorphic to a direct summand of an RG -module N .

(19.1) Definitions. A f.g. RG -module M is (G, H) -projective if every ses (short exact sequence) of RG -modules

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

for which the ses of restrictions to H

$$0 \rightarrow M'_H \rightarrow M''_H \rightarrow M_H \rightarrow 0$$

is RH -split, is necessarily RG -split. A f.g. RG -module M is (G, H) -injective if every ses of RG -modules

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

for which the ses of RH -modules

$$0 \rightarrow M_H \rightarrow M'_H \rightarrow M''_H \rightarrow 0$$

is RH -split, is necessarily RG -split.

Let us consider two extreme cases of the definition. When $H = G$, the condition “ (G, G) -projective” places no restriction at all on the RG -module M . On the other hand, taking $H = 1$, it is clear that every RG -projective module M is $(G, 1)$ -projective. The converse is not necessarily true, because ses's of R -modules do not always split. However, the conditions “ RG -projective” and “ $(G, 1)$ -projective” are equivalent if R is a field. They are also equivalent for an RG -lattice M when R is a Dedekind domain, since in that case every RG -exact sequence $0 \rightarrow M' \rightarrow M'' \rightarrow M \rightarrow 0$ is necessarily split over R .

(19.2) Theorem (Gaschütz [52]). *Let M be a f.g. RG -module, and let H be a subgroup of G . The following statements are equivalent:*

- (i) M is (G, H) -projective.
- (ii) M is (G, H) -injective.
- (iii) Let $G = \cup_{i=1}^n g_i H$. Then there exists $\gamma \in \text{End}_{RH}(M_H)$ such that
$$\sum_{i=1}^n g_i \gamma g_i^{-1} = 1_M.$$
- (iv) $M \mid M_H^G$.
- (v) $M \mid L^G$ for some RH -module L .

The ideas in this result arise naturally from the proof of Maschke's Theorem 3.14. We first require the following:

(19.3) Lemma. *Let M be a f.g. RG -module, L a f.g. RH -module, and let $G = \cup_{i=1}^n g_i H$, with $g_1 = 1$. Then*

- (a) *The formula*

$$L^G = (1 \otimes L) \oplus \left(\bigoplus_{i=2}^n g_i \otimes L \right)$$

gives an RH -direct sum decomposition of L^G . In particular, $M_H \mid (M_H^G)_H$.

- (b) *The map*

$$\psi: M_H^G \rightarrow M,$$

given by $\psi(\sum g_i \otimes m_i) = \sum g_i m_i$, is an RG -surjection. The map ψ is split by the RH -homomorphism $\lambda: M \rightarrow M_H^G$ defined by $\lambda(m) = 1 \otimes m$, $m \in M$.

The proof is immediate from the properties of induced modules discussed in §10, and is left as an exercise for the reader. By Lemma 19.3, (i) \Rightarrow (iv) and (ii) \Rightarrow (iv). We complete the proof of Theorem 19.2 by showing, in order, that (v) \Rightarrow (iii), (iii) \Rightarrow (ii), (iii) \Rightarrow (i), and (iv) \Rightarrow (v).

(v) \Rightarrow (iii): We assume that $M \mid L^G$ for some RH -module L . Without loss of generality, we may suppose that $M \subseteq L^G$, so there exists an RG -projection $\pi: L^G \rightarrow M$ such that $\pi = 1$ on M . Let $\gamma^* \in \text{End}_{RH}(L^G)$ be defined by

$$\gamma^*(\sum g_j \otimes l_j) = 1 \otimes l_1,$$

where $g_1 = 1$ as usual. It is easily verified that $\sum g_i \gamma^* g_i^{-1}$ acts as 1 on L^G . We set

$$\gamma = \pi \cdot \gamma^*|_M \in \text{End}_{RH} M.$$

Then for $m \in M$,

$$\sum_{i=1}^n g_i \gamma g_i^{-1} m = \pi(\sum g_i \gamma^* g_i^{-1} m) = \pi(m) = m,$$

which establishes (iii).

(iii) \Rightarrow (ii): Assuming (iii), suppose that M and M' are RG -modules such that $M \subseteq M'$ and M is an RH -direct summand of M' . Then there exists an RH -projection π of M' onto M . Now define

$$\pi' = \sum_{i=1}^n g_i \gamma \pi g_i^{-1},$$

where γ is the map occurring in (iii). It is easily checked that $\pi' \in \text{End}_{RG} M'$ and that π' is a projection of M' onto M . Thus M is an RG -direct summand of M' , so we have proved that M is RG -injective, and (ii) is established.

(iii) \Rightarrow (i): Let $\varphi: M' \rightarrow M$ be a surjection of RG -modules, and let $\xi: M_H \rightarrow M'_H$ be an RH -homomorphism which splits φ , that is, $\varphi \xi = 1_M$. Assuming (iii), set $\xi' = \sum g_i \xi \gamma g_i^{-1}$. Then, as in the preceding proof, one checks that $\xi' \in \text{Hom}_{RG}(M, M')$ and that $\varphi \xi' = 1_M$. Thus φ is RG -split, and we have proved that M is (G, H) -projective, as required.

Finally, it is immediate that (iv) \Rightarrow (v), which completes the proof of the theorem.

As a first application, we prove:

(19.4) Corollary. *Let R be a Dedekind domain, and let M and P be f.g. RG -lattices with $P \in \mathcal{P}(RG)$. Then $M \otimes_R P \in \mathcal{P}(RG)$.*

Proof. We have already noted that since $P \in \mathcal{P}(RG)$, P is $(G, 1)$ -projective. By Theorem 19.2(iii), there exists $\gamma \in \text{End}_R P$ such that

$$\sum_{g \in G} g \gamma g^{-1} = 1_P.$$

Then $1 \otimes \gamma \in \text{End}_R(M \otimes_R P)$, and we clearly have

$$\sum_{g \in G} g(1 \otimes \gamma)g^{-1} = 1 \text{ on } M \otimes_R P.$$

By Theorem 19.2 again, it follows that $M \otimes_R P$ is $(G, 1)$ -projective. Since R is a Dedekind domain, and M and P are R -lattices, it follows from §4 that $M \otimes_R P$ is R -projective. Combining these results, we conclude that $M \otimes_R P \in \mathcal{P}(RG)$, as required.

We conclude this section with a list of other corollaries and observations which will be basic for the theory of vertices and sources. A number of facts about induced modules, and conjugates $\{ {}^xL : x \in G \}$ of RH -modules L , will be noted (see §10). For $H_1, H_2 \leq G$, we shall write $H_1 \leq_G H_2$ to mean that ${}^xH_1 \leq H_2$ for some $x \in G$, and $H_1 =_G H_2$ to mean that ${}^xH_1 = H_2$ for some $x \in G$.

(19.5) Proposition. *Let R be an arbitrary commutative ring, and H a subgroup of G .*

- (i) *Direct summands of RG -lattices are RG -lattices.*
- (ii) *If L is an RH -lattice, then L^G is an RG -lattice.*
- (iii) *An RH -lattice L is indecomposable if and only if for each $a \in G$, the conjugate $R \cdot {}^aH$ -lattice aL is indecomposable.*
- (iv) *$({}^aL)^G \cong L^G$ for each RH -lattice L and each $a \in G$.*
- (v) *Let M be an RG -lattice, and let $M = M_1 \oplus M_2$ for RG -lattices M_1 and M_2 . Then M is (G, H) -projective if and only if both M_1 and M_2 are (G, H) -projective.*
- (vi) *If M is a (G, H) -projective RG -lattice, then M is also $(G, {}^aH)$ -projective for all $a \in G$.*
- (vii) *An RG -lattice M is (G, H) -projective if and only if it is (G, H') -projective for all $H' \geq_G H$.*
- (viii) *If M is an RG -lattice, and $M \mid L^G$ for an (H, H_0) -projective RH -lattice L , where $H_0 \leq H$, then M is (G, H_0) -projective.*
- (ix) *Let H be a subgroup of G whose index $|G : H|$ is a unit in R . Then every RG -module M is (G, H) -projective, and $M \mid M_{H^G}$.*

Proof. (i)–(v) are left as exercises (most of them have been proved elsewhere).

- (vi) By Theorem 19.2, $M \mid L^G$ for some RH -lattice L . By (iv), $L^G \cong ({}^aL)^G$, and aL is an $R \cdot {}^aH$ -lattice. By (19.2) again, M is $(G, {}^aH)$ -projective.
- (vii) Assume $M \mid L^G$ for some RH -lattice L , and let $H' \geq_G H$, so ${}^xH \leq H'$ for some $x \in G$. Then xL is an $R \cdot {}^xH$ -module, $({}^xL)^{H'}$ is an RH' -module, and $M \mid (({}^xL)^{H'})^G$, since $(({}^xL)^{H'})^G \cong ({}^xL)^G \cong L^G$, by transitivity of induction. By (19.2), M is RH' -projective. The converse is clear.

(viii) By (19.2) we have $L \mid L_0^H$ for some RH_0 -module L_0 . Since $M \mid L^G$ by assumption, we have $M \mid (L_0^H)^G$ by the additive property of tensor products. Then $M \mid L_0^G$ by transitivity of induction, and hence M is (G, H_0) -projective by (19.2).

(ix) Let $G = \cup_{i=1}^n g_i H$, and define $\gamma \in \text{End}_{RH}(M_H)$ by $\gamma(m) = |G:H|^{-1}m$, $m \in M$. Then $\sum g_i \gamma g_i^{-1} = 1_M$, and M is (G, H) -projective by Theorem 19.2.

Remarks. Most of the results in (19.5) hold for arbitrary f.g. RG -modules. They are stated for RG -lattices because in §19B we shall be concerned entirely with the classification of RG -lattices. It is therefore important to note that the module operations of taking direct summands, conjugates, induced modules, etc., carry lattices to lattices.

It will also be noted from the proof of (19.5) that, among the equivalent conditions for (G, H) -projectivity stated in Theorem 19.2, perhaps the most useful one is (v), which asserts that $M \mid L^G$ for an RH -module L . In the next section, we shall use this condition as our working definition of (G, H) -projectivity.

Finally, we remark that (19.5ix) will be used several times in Chapter 4, especially in the proof of (33.4) and the calculations in §34E.

§19B. Vertices and Sources of Indecomposable Lattices

All the results in the rest of this section, and in §20A as well, are due to Green ([59], [62], and [64]), with some reorganization and alternate proofs by other authors.

The basic set-up consists of a finite group G , a prime p , and a commutative ring R such that either of the following two conditions hold:

(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} , such that the residue field $\bar{R} = R/\mathfrak{p}$ has characteristic p , and R is complete in the \mathfrak{p} -adic topology.

In the context of a p -modular system (K, R, k) , the results will be applied both to RG -modules and kG -modules (assuming the completeness hypothesis is satisfied). In case K is sufficiently large, of characteristic zero, the results will also apply to RG -modules without the completeness assumption.

We shall be concerned only with RG -lattices, that is, f.g. RG -modules which are R -projective. In case R is a field of characteristic p , every f.g. RG -module is of course an RG -lattice. It will be convenient to use the following notation, which will be in force throughout §§19–20.

$\text{Ind } RG = \text{set of all indecomposable } RG\text{-lattices.}$

Because of the hypothesis on R , the K-S-A Theorem holds for all RG -lattices M , and asserts that every such M can be expressed as a direct sum

$$M = \bigoplus_{i=1}^m U_i, \quad U_i \in \text{Ind } RG,$$

where the indecomposable summands $\{U_i\}$ are uniquely determined up to isomorphism and order of occurrence. The K-S-A Theorem was proved in §6B for RG -lattices, with commutative rings R satisfying conditions (A) or (B) above. In case R is a d.v.r. which is not necessarily complete, we shall show in (30.18) that the K-S-A Theorem is valid for RG -lattices, provided that K is sufficiently large and $\text{char } K = 0$.

Besides the K-S-A Theorem, we shall also make heavy use of the results in §19A, and the Subgroup Theorem 10.13, which we restate for the reader's convenience as follows:

(19.6) Subgroup Theorem. *Let B and C be subgroups of G , and let L be an RB -lattice. Then*

$$(L^G)_C = \bigoplus_{CaB} (^aL_{aB \cap C})^C,$$

where the sum is taken over the double cosets $C \setminus G / B$, and the summands are independent of the choice of representatives $\{a\}$.

The objective of the theory of vertices and sources is to determine the structure of indecomposable RG -lattices in terms of certain p -subgroups of G and indecomposable lattices associated with these subgroups.

(19.7) Definition. Let M be an RG -lattice. We denote by $\mathcal{V}(M)$ the set of all subgroups H of G such that M is (G, H) -projective. We view $\mathcal{V}(M)$ as a partially ordered set under the relation \leq_G .

Remark. For each RG -lattice M , $\mathcal{V}(M)$ is nonempty, because M is (G, G) -projective. We also note that if $H \in \mathcal{V}(M)$, and $H' \geq_G H$, then $H' \in \mathcal{V}(M)$, by (19.5vii).

(19.8) Theorem. *Let $M \in \text{Ind } RG$. There exists a subgroup $D \in \mathcal{V}(M)$ such that $D \leq_G H$ for all $H \in \mathcal{V}(M)$.*

The proof depends on two lemmas.

(19.9) Lemma. *Let D and H be subgroups of G , and let $M = RG$ -lattice, $L = RD$ -lattice, and assume $M \mid L^G$. Let $U \mid M_H$ for some $U \in \text{Ind } RH$. Then there exists $a \in G$ such that $U \mid (^aL_{aD \cap H})^H$, and U is $(H, ^aD \cap H)$ -projective.*

Proof. By the Subgroup Theorem 19.6 we have

$$(L^G)_H = \bigoplus_{HaD} (^aL_{aD \cap H})^H.$$

Then $M|L^G$ implies $M_H|(L^G)_H$. Since $U|M_H$ and $U \in \text{Ind } RH$, the K-S-A Theorem implies that $U|(^aL_{aD \cap H})^H$ for some $a \in G$. By (19.2v), U is $(H, {}^aD \cap H)$ -projective, as required.

(19.10) Lemma. *Let $M \in \text{Ind } RG$, and assume conditions (i)–(iii):*

- (i) D is a minimal element of $\mathcal{V}(M)$ with respect to the order relation \leq_G ,
- (ii) $M|L^G$ where $L \in \text{Ind } RD$, and
- (iii) H is an arbitrary member of $\mathcal{V}(M)$.

Then there exists $U \in \text{Ind } RH$ such that

$$U|M_H, M|U^G,$$

and for such a lattice U , there exists an $a \in G$ satisfying

$${}^aD \leq H \text{ and } U|({}^aL)^H, \text{ where } (^aL)^H = \text{ind}_{^aD}^H({}^aL).$$

Proof. Since M is (G, H) -projective, $M|M_H^G$, by (19.2iv). By the K-S-A Theorem, it follows that there exists $U \in \text{Ind } RH$ such that

$$M|U^G \text{ and } U|M_H.$$

For such a lattice U , by Lemma 19.9 $U|({}^aL_{aD \cap H})^H$ and U is $(H, {}^aD \cap H)$ -projective, for some $a \in G$. By (19.5viii), M is $(G, {}^aD \cap H)$ -projective. But ${}^aD \cap H \leq_G D$, so by minimality of D in $\mathcal{V}(M)$, ${}^aD \cap H =_G D$, whence ${}^aD \leq H$ (otherwise $|{}^aD \cap H| < |D|$). Then the condition $U|({}^aL_{aD \cap H})^H$ becomes $U|({}^aL)^H$ in this case, and the proof is complete.

Proof of Theorem 19.8. Let D be a minimal member of $\mathcal{V}(M)$, and let $H \in \mathcal{V}(M)$. By Lemma 19.10, $D \leq_G H$, and the theorem is proved.

(19.11) Definition. Let $M \in \text{Ind } RG$, and let D be a subgroup in $\mathcal{V}(M)$ such that $D \leq_G H$ for all subgroups $H \in \mathcal{V}(M)$, as in Theorem 19.8. Such a subgroup D is called a *vertex* of M . The set of all vertices of M is denoted by $\text{vtx } M$. If D is a vertex of M , and $L \in \text{Ind } RD$ is a module such that $M|L^G$, then L is called a *source* of M .

(19.12) Remarks. By Theorem 19.8, each $M \in \text{Ind } RG$ has a vertex. Moreover the set of all vertices of M forms a single conjugacy class of subgroups of

G , by (19.5vi) and the properties of the partial order relation \leq_G . Now let $D \in \text{vtx } M$, so M is (G, D) -projective, and $M|X^G$ for some RD -lattice X . By the K-S-A Theorem, $M|L^G$ for some $L \in \text{Ind } RD$ such that $L|X$. Thus for each $D \in \text{vtx } M$, there exists an $L \in \text{Ind } RD$ which is a source of M .

(19.13) Proposition. *Let $M \in \text{Ind } RG$. Then:*

- (i) *vtx M is a single conjugacy class of p -subgroups of G .*
- (ii) *If $D \in \text{vtx } M$, and both L and L' are indecomposable RD -lattices which are sources of M , then $L' \cong {}^x L$ for some $x \in N_G(D)$.*

Proof. (i) Let $D \in \text{vtx } M$; we have already shown in (19.12) that $\text{vtx } M$ consists of all conjugates of D . Now let S be a Sylow p -subgroup of G . Then the integer $|G:S|$ is prime to p , and hence is a unit in R , by hypothesis (A) or (B) above. By (19.5ix) it follows that M is (G, S) -projective. Therefore $D \leq_G S$ by (19.11), which shows that D is a p -subgroup.

(ii) We first apply Lemma 19.10 to M, D, L , with $H = D$. By the lemma, there exists a module $U \in \text{Ind } RD$ such that $U|({}^a L)^D$ and ${}^a D \leq D$, where the choice of U is independent of L . Then $a \in N_G(D)$, and $U \cong {}^a L$. Applying the lemma a second time, with L' in place of L , we obtain $U \cong {}^{a'} L'$, for some $a' \in N_G(D)$. It follows that $L' \cong {}^x L$, with $x = (a')^{-1}a \in N_G(D)$, completing the proof.

The organization of Green's results in the rest of this subsection was influenced by Burry [79].

(19.14) Theorem. *Let H be an arbitrary subgroup of G , let $M \in \text{Ind } RG$, $U \in \text{Ind } RH$, and let $D_M \in \text{vtx } M$ and $D_U \in \text{vtx } U$. Then we have:*

- (i) $U|M_H \Rightarrow D_U \leq_G D_M$,
- (ii) $M|U^G \Rightarrow D_M \leq_G D_U$.

Proof. (i) Since $D_M \in \text{vtx } M$, we have $M|L^G$ for some $L \in \text{Ind } RD_M$. Then $U|M_H$ implies by (19.9) that U is $(H, {}^a D_M \cap H)$ -projective for some $a \in G$. Therefore the vertex D_U of U satisfies the condition

$$D_U \leq_H ({}^a D_M \cap H),$$

by Theorem 19.8. Since ${}^a D \cap H \leq_G D$, for any D , we have $D_U \leq_G D_M$, and (i) is proved.

(ii) Since $M|U^G$, and U is (H, D_U) -projective, it follows that M is (G, D_U) -projective by (19.5viii). Then $D_M \leq_G D_U$ by (19.11), completing the proof.

The next result is a kind of *going-down theorem*, in which we begin with a subgroup H of G and a lattice $M \in \text{Ind } RG$, and construct lattices $U \in \text{Ind } RH$ satisfying various conditions, such as having a common vertex and source with M .

(19.15) Theorem. *Let $M \in \text{Ind } RG$, and let H be a subgroup of G such that $H \in \mathcal{V}(M)$. Then the set \mathfrak{D} of all vertices of M contained in H is nonempty, and \mathfrak{D} may be expressed as a disjoint union*

$$\mathfrak{D} = \mathfrak{D}_1 \cup \cdots \cup \mathfrak{D}_m$$

of H -conjugacy classes of subgroups of H . Moreover, the following statements hold:

- (i) *There exists $U \in \text{Ind } RH$ such that $M \mid U^G$ and $U \mid M_H$. For any such U , we have $\text{vtx } U = \mathfrak{D}_i$ for some class $\mathfrak{D}_i \subseteq \mathfrak{D}$.*
- (ii) *Given a fixed class $\mathfrak{D}_i \subseteq \mathfrak{D}$, there exists $U \in \text{Ind } RH$ such that $U \mid M_H$ and $\text{vtx } U = \mathfrak{D}_i$.*
- (iii) *Given a fixed class $\mathfrak{D}_j \subseteq \mathfrak{D}$, there exists $W \in \text{Ind } RH$ such that $M \mid W^G$ and $\text{vtx } W = \mathfrak{D}_j$.*
- (iv) *For any $U \in \text{Ind } RH$ such that $U \mid M_H$ and $\text{vtx } U \subseteq \mathfrak{D}$, the lattices U and M have a common vertex and a common source.*

Remark. Before starting the proof, we remark that there is no reason to expect that (ii) and (iii) can be satisfied by the same indecomposable RH -lattice, for a given class $\mathfrak{D}_i \subseteq \mathfrak{D}$. See §20, however, for further discussion of this point.

Proof. The condition $H \in \mathcal{V}(M)$ implies that $D \leq_G H$ for $D \in \text{vtx } M$, so there exist vertices of M contained in H . By (19.13i), $\text{vtx } M$ is a single conjugacy class of subgroups of G , so clearly the collection \mathfrak{D} of subgroups $D \in \text{vtx } M$ such that $D \leq H$ can be expressed as a union of H -conjugacy classes of subgroups. We now prove the assertions (i)–(iv) in order.

(i) Since $H \in \mathcal{V}(M)$, M is (G, H) -projective, so $M \mid M_H^G$ by Theorem 19.2. Then $M \mid U^G$ for some U in $\text{Ind } RH$ such that $U \mid M_H$, by the K-S-A Theorem. For any such U , let $D \in \text{vtx } U$; then $D \in \text{vtx } M$ by Theorem 19.14, and it follows that $\text{vtx } U = \mathfrak{D}_i$ for some $\mathfrak{D}_i \subseteq \mathfrak{D}$.

(ii) Let $D \in \mathfrak{D}_i$ for a fixed class $\mathfrak{D}_i \subseteq \mathfrak{D}$. Then $D \in \text{vtx } M$, so $D \in \mathcal{V}(M)$, and we can apply part (i) to D instead of H . In this case, D is the unique vertex of M contained in D . We thus obtain an $L \in \text{Ind } RD$ such that $L \mid M_D$ and $D \in \text{vtx } L$. Since $D \leq H \leq G$, it follows from the K-S-A Theorem that there exists $U \in \text{Ind } RH$ such that $L \mid U_D$ and $U \mid M_H$. Applying (19.14i) to the

situation $L|U_D$ and the pair of groups D and H , we obtain $D \in \text{vtx } U$, so the class \mathfrak{D}_j containing D coincides with $\text{vtx } U$, as required.

(iii) Let $D \in \mathfrak{D}_j$, for fixed \mathfrak{D}_j , and apply (i) again to obtain an $L \in \text{Ind } RD$ such that $M|L^G$ and $D \in \text{vtx } L$. Then $M|W^G$, for some $W \in \text{Ind } RH$ such that $W|L^H$, by the K-S-A Theorem. Let $D' \in \text{vtx } W$; then by (19.14ii) applied to the situation $W|L^H$, we have $D' \leq_H D$. On the other hand $M|W^G$ and $D \in \text{vtx } M$ together imply that $D \leq_G D'$, by (19.14ii) again. It follows that $D' =_H D$, hence $D \in \text{vtx } W$, and $\text{vtx } W = \mathfrak{D}_j$, completing the proof of (iii).

(iv) By the hypothesis of (iv), $\text{vtx } U \subseteq \text{vtx } M$, and the problem is to find a common source. Let $D \in \text{vtx } U$, and let $L \in \text{Ind } RD$ be a source of M . By Lemma 19.9, there exists $a \in G$ such that

$$U | (^a L {}_{aD \cap H})^H,$$

and therefore U is $(H, {}^a D \cap H)$ -projective. Then ${}^a D \subseteq H$, because otherwise U has a vertex contained in ${}^a D \cap H$ of smaller order than D , which contradicts Theorem 19.8 since $D \in \text{vtx } U$. Since ${}^a D \subseteq H$, the same reasoning shows that ${}^a D \in \text{vtx } U$. Then ${}^a L$ is an indecomposable $R({}^a D)$ -lattice, and we have $M|({}^a L)^G$ and $U|({}^a L)^H$. Thus ${}^a L \in \text{Ind } R({}^a D)$ is a common source of M and U , and the theorem is proved.

Our final result is a *going-up theorem*:

(19.16) Theorem. *Let H be a subgroup of G , and let $U \in \text{Ind } RH$. Then there exists an $M \in \text{Ind } RG$ such that $M|U^G$ and $U|M_H$. For any such M , the modules M and U have a vertex and source in common.*

Proof. Applying Lemma 19.3a to U , we have $U|(U^G)_H$. By the K-S-A Theorem, it follows that there exists $M \in \text{Ind } RG$ such that $M|U^G$ and $U|M_H$. The rest of the theorem follows from (19.15i) and (19.15iv).

Examples. (i) *Indecomposable projective RG -lattices.* Let P be an indecomposable projective RG -lattice. Then P is $(G, 1)$ -projective, hence $\text{vtx } P$ consists of the trivial subgroup $\{1\}$, and $P|1_{\{1\}}^G$. Now $1_{\{1\}}^G \cong RG$ as left RG -modules, whence $P|RG$. Let S be a Sylow p -subgroup of G , and let $U \in \text{Ind } RS$ be a lattice such that $U|P_S$. By Theorem 19.14, $\text{vtx } U \subseteq \text{vtx } P = \{1\}$, hence each such U is $(S, 1)$ -projective. Since each summand U of P_S is also R -projective, each summand U of P_S belongs to $\mathcal{P}(RS)$, whence* $P_S \in \mathcal{P}(RS)$. Since RS is a local R -algebra by (5.25), projective RS -modules are free (Exercise 6.9), and it follows that P_S is a free RS -module. In particular, the R -rank of P is

*This is obvious anyway, since for any $P \in \mathcal{P}(RG)$ and any $H \leq G$, the restriction P_H lies in $\mathcal{P}(RH)$.

divisible by $|G|_p$; we showed this in §18 in the case where R is a d.v.r. with a sufficiently large quotient field.

(ii) *Blocks of RG .* The direct product $G \times G$ acts on the group ring RG according to the rule

$$(x, y) \cdot a = x a y^{-1}, \quad x, y \in G, a \in RG.$$

Then RG is an $R(G \times G)$ -lattice. The indecomposable $R(G \times G)$ -direct summands of RG are called the *p-blocks* of RG . Clearly the *p-blocks* are indecomposable two-sided ideals in RG whose direct sum is RG . Let G_0 be the diagonal subgroup of $G \times G$.

(19.17) Proposition. *Each p-block B of RG is $(G \times G, G_0)$ -projective.*

Proof. By (19.2), it is sufficient to prove that

$$RG \cong 1_{G_0}^{G \times G},$$

where 1_{G_0} is the trivial R -representation of G_0 . We first notice that the elements of G are permuted among themselves by the action of $G \times G$ on RG . It is clear that the action of $G \times G$ is transitive, and that the stabilizer in $G \times G$ of the identity element of RG is G_0 . The above isomorphism follows from these remarks.

(19.18) Corollary. *The vertex of each p-block B of RG is isomorphic to a p-subgroup of G .*

Proof. By (19.17), (19.8) and (19.13), any vertex of B is a *p*-subgroup of $G \times G$ isomorphic to a subgroup of G_0 . Since $G_0 \cong G$, the result follows.

Definition. A *p*-subgroup of G corresponding to a vertex of a *p*-block B of RG (as in (19.18)) is called a *defect group of the block B*.

The *p*-blocks and their defect groups were first defined by Brauer, from a different point of view (see CR Chapter 12). The study of blocks, and of their applications to character theory and finite group theory, constitutes the central part of Brauer's theory of modular representations, and will be taken up in Chapter 9.

§19C. The Green Indecomposability Theorem

Many of the deeper results on vertices and sources, and their applications to block theory, depend on a result of Green [59], which asserts that under certain circumstances, induction from an indecomposable RH -lattice produces an indecomposable RG -lattice, for normal subgroups H of G . The main

results will be stated precisely later in this subsection. We begin with an analysis, similar to that in §11C for simple modules, of the endomorphism algebra $\text{End}_{RG}(L^G)$, where L is an absolutely indecomposable RH -lattice and H is a normal subgroup of G . The proof of the main result is an adaptation of the work of Conlon, Ward and Tucker (see §11C for references, and also Broué [76] for a related result).

Throughout this subsection, R denotes a commutative ring satisfying either of the following two conditions involving a prime p (see §19B):

(A) R is a perfect field of characteristic p , or

(B) R is a d.v.r. with maximal ideal \mathfrak{p} , such that the residue field $\bar{R} = R/\mathfrak{p}$ is a perfect field of characteristic p , and R is complete in the \mathfrak{p} -adic topology.

The additional hypothesis that \bar{R} is perfect certainly holds true if \bar{R} is a finite field or is algebraically closed. In case (A), we take $\mathfrak{p} = 0$ and identify R with \bar{R} in the discussion to follow. The additional assumption that \bar{R} be perfect is needed because, later in this subsection, we require Theorem 30.29; this theorem asserts that an RH -lattice L is absolutely indecomposable if and only if

$$\text{End}_{RH} L / \text{rad}(\text{End}_{RH} L) \cong \bar{R},$$

provided that the field \bar{R} is perfect.

For the first main result, we start with a finite group S , and an R -algebra A f.g./ R as module, such that A has an S -graded Clifford system in the sense of Definition 11.12. We recall that in this situation we have $A = \bigoplus_{s \in S} A_s$, where the $\{A_s\}$ are R -submodules of A satisfying the conditions:

$$A_s A_t = A_{st}, A_s = A_1 a_s = a_s A_1 \text{ for some units } a_s \in A,$$

and $1 \in A_1$. Then A_1 is an R -subalgebra of A . If L is a left A_1 -module and M a left A -module, we denote by L^A the induced A -module $A \otimes_{A_1} L$, and by M_{A_1} the A_1 -module obtained by restriction of scalars from A to A_1 . From §11C we have

$$L^A = \bigoplus_{s \in S} a_s \otimes L,$$

and each $a_s \otimes L$ is an A_1 -submodule of L^A . The endomorphism ring $E = \text{End}_A(L^A)$ will be viewed as a ring of right operators on L^A . We shall make constant use of (11.14), which established the following:

(i) Letting $E_s = \{f \in E : (1 \otimes L)f \subseteq a_s \otimes L\}$, $s \in S$, we have for all $s, t \in S$:

$$A_s(a_t \otimes L) = a_{st} \otimes L, (a_s \otimes L)E_t \subseteq a_{st} \otimes L,$$

$$E_s E_t \subseteq E_{st}, 1 \in E_1, E = \bigoplus_{s \in S} E_s.$$

(ii) For $s \in S$, let $U_s = \text{Hom}_{A_1}(1 \otimes L, a_s \otimes L)$. Then each $\varphi \in U_s$ extends uniquely to an element $\hat{\varphi} \in E_s$ such that

$$(a \otimes l)\hat{\varphi} = a((1 \otimes l)\varphi) \text{ for } l \in L, a \in A.$$

The map $\varphi \rightarrow \hat{\varphi}$ gives an isomorphism of R -modules

$$U_s \cong E_s, s \in S.$$

In particular, $E_1 \cong \text{End}_{A_1} L$ as R -algebras.

(19.19) Theorem. *Let A be an S -graded R -algebra as above, and let L be an indecomposable A_1 -module. Keeping the above notation, set*

$$\tilde{E}_1 = E_1 / \text{rad } E_1, E = \text{End}_A L^A,$$

and assume that $\tilde{E}_1 \cong \bar{R}$. Let

$$T = \{s \in S : 1 \otimes L \cong a_s \otimes L \text{ as } A_1\text{-modules}\}.$$

Then T is a subgroup of S . Moreover, there exists a two-sided ideal J of E such that

$$\mathfrak{p} E \subseteq J \subseteq \text{rad } E, J = \bigoplus_{s \in S} (J \cap E_s),$$

and E/J is a T -graded \bar{R} -algebra, whose grading is given by

$$E/J = \bigoplus_{t \in T} E_t / (E_t \cap J).$$

Each submodule $E_t / (E_t \cap J)$ is a one-dimensional \bar{R} -subspace of E/J .

Proof. Since L is an indecomposable A_1 -lattice, so are its conjugates $\{a_s \otimes L : s \in S\}$, and the formula

$$L^A = \bigoplus_{s \in S} a_s \otimes L$$

gives the direct sum decomposition of L^A into indecomposable A_1 -submodules. Let $\{\mu_s\}$ and $\{\pi_s\}$ be the associated injections and projections, respectively, where for $s \in S$,

$$a_s \otimes L \xrightleftharpoons[\pi_s]{\mu_s} L^A.$$

Let us put $E' = \text{End}_{A_1}(L^A)$, so E is a subring of E' . Each $f \in E'$ can then be represented as a matrix

$$f = (f_{rs})_{r, s \in S}, \text{ where } f_{rs} = \mu_r f \pi_s \in \text{Hom}_{A_1}(a_r \otimes L, a_s \otimes L), r, s \in S,$$

remembering that E and E' act from the right on L^A . Composition of f 's corresponds to multiplication of matrices. We now proceed in a series of steps.

Step 1. Let us set

$$J = E \cap \text{rad } E', \text{ where } E' = \text{End}_{A_1} L^A.$$

Clearly J is a two-sided ideal of E . Since $(\text{rad } E')^m \subseteq \mathfrak{p} E'$ for some integer m , we have $J^m \subseteq (\mathfrak{p} E' \cap E)$. It is easily verified that $\mathfrak{p} E' \cap E = \mathfrak{p} E$, since L^A is an R -lattice. Therefore $J^m \subseteq \mathfrak{p} E$, so $J \subseteq \text{rad } E$ by Exercise 5.3. On the other hand, $\text{rad } E' \supseteq \mathfrak{p} E'$ by (5.22), so $J \supseteq \mathfrak{p} E$ as desired.

Our next task is to give another description of the ideal J , using the following result of independent interest:

Lemma. *Let B be an R -algebra f.g./ R , where R is as above, and let $\{L_i : 1 \leq i \leq n\}$ be a set of f.g. indecomposable B -modules. Put $L = L_1 \oplus \cdots \oplus L_n$, and let $E' = \text{End}_B L$, viewed as ring of right operators on L . Each $f \in E'$ may be written as a matrix*

$$f = (f_{ij})^{n \times n}, \text{ where } f_{ij} \in \text{Hom}_B(L_i, L_j).$$

Then $\text{rad } E'$ coincides with the set J' of all matrices (f_{ij}) all of whose entries are non-isomorphisms.

Proof. Changing notation, we may write

$$L = \coprod_{i=1}^d L_i^{(n_i)},$$

where $\{L_1, \dots, L_d\}$ are non-isomorphic indecomposable B -modules. Each $f \in E'$ is thus represented by a $d \times d$ array

$$f = (F_{rs})^{d \times d}, \text{ where } F_{rs} \in \text{Hom}_B(L_r^{(n_r)}, L_s^{(n_s)}) \text{ for } 1 \leq r, s \leq d.$$

For $r \neq s$, L_r is not isomorphic to L_s , so each entry of F_{rs} is a non-isomorphism. On the other hand, the ring $\text{End}_B L_r$ is local, so the set of non-automorphisms of L_r in this ring coincides with $\text{rad}(\text{End } L_r)$. Therefore J' consists of all $d \times d$ arrays $(F_{rs})^{d \times d}$ with arbitrary off-diagonal blocks, and with diagonal blocks F_{rr} having entries in $\text{rad}(\text{End } L_r)$, $1 \leq r \leq d$.

It is easily checked that J' is a two-sided ideal of E' , by using two obvious facts:

- (i) If $\alpha, \beta \in \text{End } L_r$, with either α or β not an automorphism, then $\alpha\beta$ is not an automorphism.

(ii) If $\alpha \in \text{Hom}(L_r, L_s)$ and $\beta \in \text{Hom}(L_s, L_r)$, where $r \neq s$, then $\beta\alpha$ is not an automorphism of L_s (since otherwise $L_s | L_r$).

Clearly,

$$E'/J' \cong \prod_{r=1}^d M_n((\text{End } L_r)/(\text{rad End } L_r)),$$

so E'/J' is semisimple by (5.14). We need only show that $J' \subseteq \text{rad } E'$. Since $\mathfrak{p}E' \subseteq J'$, it suffices to prove that $\bar{J}' \subseteq \text{rad } \bar{E}'$, where bars denote reduction mod \mathfrak{p} . By (5.22), for large enough k we have

$$\{\text{rad}(\text{End } L_r)\}^k \subseteq \mathfrak{p} \cdot \text{End } L_r, \quad 1 \leq r \leq d,$$

so each diagonal block in every matrix in \bar{J}' is nilpotent. Further, every triangular matrix in \bar{J}' , with zero diagonal blocks, is also nilpotent. Hence \bar{J}' is nilpotent by Wedderburn's Theorem (see Exercise 19.4), and $\bar{J}' \subseteq \text{rad } \bar{E}'$, which completes the proof that $J' = \text{rad } E'$ and establishes the lemma.

Step 2. Each $f \in E$ can be represented by a matrix $(f_{rs})_{r,s \in S}$, whose first row is determined by the restriction of f to $1 \otimes L$. Conversely, given the elements $\{f_{1s} : s \in S\}$, we know the action of f on $1 \otimes L$, and hence also on $a_r \otimes L$ for each $r \in S$. Thus we have

$$f = \sum_{s \in S} \hat{f}_{1s},$$

and this is precisely the formula which arises from the decomposition $E = \bigoplus_{s \in S} E_s$.

By Step 1, we have

$$J = \{f \in E : f_{rs} \text{ is not an isomorphism for each } r, s \in S\}.$$

But for $f \in E$, if f_{1s} is not an isomorphism, then $f_{t,ts}$ is not an isomorphism for any $t \in S$. It follows at once that we have a decomposition

$$J = \bigoplus_{s \in S} (J \cap E_s),$$

induced from the decomposition of E . Further, the preceding argument shows that

$$J \cap E_1 \cong \text{rad } E_1,$$

the isomorphism being given by restriction of $f \in J \cap E_1$ to the module $1 \otimes L$. It remains for us to establish the T -graded Clifford structure on E/J .

Now let $T = \{s \in S : 1 \otimes L \cong a_s \otimes L\}$. For each $s \in S - T$, there are no isomorphisms from $1 \otimes L$ onto $a_s \otimes L$. It follows at once that $E_s \subseteq J$, that is,

$$J \cap E_s = E_s \text{ for } s \in S, s \notin T.$$

This implies that

$$E/J = \bigoplus_{t \in T} E_t / (E_t \cap J),$$

as claimed. Note that E/J is an \bar{R} -space, since $J \supseteq \mathfrak{p} E$.

Step 3. Finally, we prove that E/J has a T -graded Clifford system. Given $t \in T$, there exists an A_1 -isomorphism

$$\psi : 1 \otimes L \cong a_t \otimes L,$$

whose extension $\hat{\psi}$ to L^A gives an element of E_t . Then $\hat{\psi} \notin J$ since $\hat{\psi}_{1,t}$ is an A_1 -isomorphism. For each $s \in S$, we have

$$(a_s \otimes L) \hat{\psi} = a_s ((1 \otimes L) \hat{\psi}) = a_s (a_t \otimes L) = a_{st} \otimes L,$$

which shows that $\hat{\psi}$ is surjective, and hence $\hat{\psi} \in \text{Aut}_A L^A$. Now for any $f \in E_t$ we have $f \hat{\psi}^{-1} \in E_1$, and $f \in J$ if and only if $f \hat{\psi}^{-1} \in \text{rad } E_1$. But $E/\text{rad } E_1 \cong \bar{R}$ by the hypothesis of the theorem, so for each $f \in E_t$ lying outside J , we have

$$f \equiv \beta \hat{\psi} \pmod{J \cap E_t}$$

for some $\beta \in R$. We have therefore shown that for each $t \in T$, $E_t / (J \cap E_t)$ is a one-dimensional \bar{R} -space (with basis element $\hat{\psi}$, a unit in E/J).

Set $\bar{E}_t = E_t / (J \cap E_t)$, $t \in T$. The above remarks imply that T is a group (see proof of (11.15)), and $\bar{E}_s \bar{E}_t = \bar{E}_{st}$ for $s, t \in T$. Thus E/J is indeed a T -graded Clifford system, with the grading induced from the S -grading of E by means of the natural surjection $E \rightarrow E/J$. This completes the proof of the theorem.

(19.20) Theorem. *Keeping the notation and hypotheses of Theorem 19.19, let*

$$B = \bigoplus_{t \in T} A_t, \quad E_T = \bigoplus_{t \in T} E_t.$$

Let $L^B = B \otimes_{A_1} L = \bigoplus_{i=1}^m U_i$ be the decomposition of L^B into indecomposable B -modules $\{U_i\}$. Then

$$L^A = A \otimes_{A_1} L = \bigoplus_{i=1}^m U_i^A, \text{ where } U_i^A = A \otimes_B U_i,$$

gives the decomposition of L^A into indecomposable A -modules $\{U_i^A\}$. Moreover, $U_i \cong U_j$ as B -modules if and only if $U_i^A \cong U_j^A$ as A -modules.

Proof. By Exercise 11.8, the restriction map

$$\text{res} : E_T \rightarrow \text{End}_B L^B,$$

obtained by restricting each $f \in E$ to the module L^B , is an isomorphism of R -algebras. Now let

$$J_T = \{f \in E_T : f_{tu} \text{ is not an isomorphism for each } t, u \in T\}.$$

Then by the identification $E_T \cong \text{End}_B L^B$, we have

$$J_T = \text{End}_B(L^B) \cap \text{rad}(\text{End}_{A_1} L^B)$$

as in Theorem 19.19, and clearly $J \cap E_T \subseteq J_T$. To prove equality, by Theorem 19.19 it suffices to show that

$$J \cap E_t = J_T \cap E_t \text{ for all } t \in T,$$

and we have already pointed out the inclusion $J \cap E_t \subseteq J_T \cap E_t$. But by the last step of the proof of (19.19), both $J \cap E_t$ and $J_T \cap E_t$ are maximal submodules of E_t , and so they coincide. This completes the proof that $J \cap E_T = J_T$, and it now follows easily from (19.19) that there is an isomorphism of \bar{R} -algebras

$$E/J \cong E_T/J_T.$$

The theorem is now proved as follows. By (6.3), a decomposition $L^B = \bigoplus U_i$ into indecomposable summands corresponds to a decomposition of E_T into indecomposable left ideals, with isomorphisms between direct summands of L^B corresponding to isomorphisms between left ideals. By (6.8), since $J_T \subseteq \text{rad } E_t$, a decomposition of E_T into indecomposable left ideals corresponds to such a decomposition of E_T/J_T , with isomorphism between summands preserved. By (6.3) and (6.8), the same statements apply to decompositions of $L^A = (L^B)^A$ into indecomposable summands, and decompositions of E , and of E/J , into indecomposable left ideals. Since $E/J \cong E_T/J_T$, we conclude in particular that the $\{U_i^A\}$ are indecomposable summands of L^A , since otherwise they would split up further, contradicting the fact that L^A and L^B have the same number of indecomposable summands. We also have $U_i \cong U_j$ if and only if $U_i^A \cong U_j^A$ by the preceding discussion, and the theorem is proved.

The preceding theorem reduces the decomposition problem for L^A to the stable case, and this is now easily handled by the following important result of Conlon (see also Tucker, Ward, loc. cit.):

(19.21) Theorem. *Keep the hypotheses of (19.19), and assume also that L is a stable A_1 -module relative to A , that is, the groups S and T coincide. Then each*

decomposition $L^A = \bigoplus W_i$ into indecomposable summands corresponds to a decomposition of E/J into indecomposable left ideals, with preservation of isomorphisms between summands. Moreover, E/J is isomorphic to a twisted group algebra of S over the residue field \bar{R} .

Proof. Since $S=T$, we know by (19.19) that E/J is an S -graded Clifford system over \bar{R} . By Example (b) following (11.12) and the subsequent discussion, it follows that E/J is a twisted group algebra $(\bar{R}S)_\alpha$ over \bar{R} , for some factor set $\alpha: S \times S \rightarrow \bar{R}$. The correspondence between decompositions of L^A and E/J follows easily from (6.3) and (6.8), as explained in the proof of (19.20). This completes the proof of (19.21).

We now come to a main result of this section. To understand the proof, it will be necessary for the reader to become familiar with §30B, on absolutely indecomposability of Λ -lattices. In particular, we require Theorem 30.29, which asserts that a f.g. indecomposable Λ -module is absolutely indecomposable if and only if $\tilde{E}(M) \cong \bar{R}$, provided that \bar{R} is a perfect field (recall that $\tilde{E}(M) = E(M)/\text{rad } E(M)$, and $E(M) = \text{End}_\Lambda M$).

(19.22) The Green Indecomposability Theorem (Green [59]). *Let L be an absolutely indecomposable RH -module, where H is a normal subgroup of G such that $|G:H|=p$. Then the induced module L^G is absolutely indecomposable.*

Proof. By Example (a) of §11C, RG is an S -graded Clifford system, with $A=RG$, $A_1=RH$, and $S=G/H$. By Theorem 30.29 we have $\tilde{E}(L)=\bar{R}$, so the hypothesis of (19.19) is satisfied. Since S has order p , there are only two cases that can occur.

Case (i). The subgroup T in (19.19) is trivial. In this case $B=A_1 \cong RH$, and by (19.20),

$$E/J \cong E_T/J_T \cong \bar{R}.$$

By (19.20), it follows that L^G is indecomposable, and that $\tilde{E}(L^G) \cong \bar{R}$, where $\tilde{E}(L^G) \cong \text{End}_{RG}(L^G)/\text{rad}(\text{End}_{RG}(L^G))$. Then L^G is absolutely indecomposable by (30.29), and the theorem is proved in this case.

Case (ii). The subgroup T in (19.19) coincides with S , and has order p . In this case, we apply (19.21) to conclude that a decomposition of L^G corresponds to a decomposition of E/J into left ideals. Moreover, it follows from (6.3) that corresponding summands of L^G and E/J have the same endomorphism algebras. By (19.21), E/J is isomorphic to a twisted group algebra $(\bar{R}S)_\alpha$ of S over the perfect field \bar{R} , for some factor set $\alpha: S \times S \rightarrow \bar{R}$. Since S is a p -group and \bar{R} is a perfect field of characteristic p , we can apply the remark following Lemma 11.38, and conclude that α is a principal factor set. It follows that E/J is isomorphic to the group algebra $\bar{R}S$. By (5.24), $\bar{R}S$ is an indecomposable left ideal, whose endomorphism algebra is $\bar{R}S$. Since

$\bar{R}S/\text{rad } \bar{R}S \cong \bar{R}$ by (5.24), it follows that L^G is indecomposable and $\tilde{E}(L^G) \cong \bar{R}$. Thus L^G is absolutely indecomposable by (30.29), and the theorem is proved.

There are three corollaries to the Green Indecomposability Theorem, which extend its scope considerably:

(19.23) Corollary. *Suppose that $H \trianglelefteq G$, and G/H is a p -group. If L is an absolutely indecomposable RH -module, then L^G is an absolutely indecomposable RG -module.*

The proof is immediate from (19.22), using transitivity of induction and the fact that every p -group is solvable.

(19.24) Corollary. *Suppose that G is a p -group, and H is an arbitrary subgroup (not necessarily normal). If L is an absolutely indecomposable RH -module then L^G is an absolutely indecomposable RG -module.*

Proof. Since G is a p -group, any subgroup is properly contained in its normalizer (see §1B). It follows that there is a normal series between H and G whose factors are cyclic of order p . The result then follows from (19.22), using transitivity of induction.

(19.25) Corollary. *Let G be a p -group, and let M be a transitive permutation module over RG , that is, M has a free R -basis X which is a transitive G -set. Then M is an absolutely indecomposable RG -module*

Proof. Let $x_0 \in X$ and let $H = \text{Stab}_G x_0$. Then X affords the induced permutation representation 1_H^G , so $M = L^G$, where L affords the trivial R -representation of H . Then L^G is absolutely indecomposable by Corollary 19.24. (For a generalization of this result, see (32.14) below.)

We conclude this section with two applications of the Green Indecomposability Theorem. The first is a generalization of Example (i) following (19.16).

(19.26) Theorem. *Let M be an indecomposable RG -lattice, let $D \in \text{vtx } M$, and let H be a Sylow p -subgroup of G containing D . Then the R -rank of M is divisible by the index $|H : D|$.*

Proof. We show first that it suffices to consider the case where G is a p -group. By (19.14), each indecomposable RH -summand of M_H has vertex $D_U \leq_G D$. Therefore, if we know the result for the p -subgroup H and modules $U \in \text{Ind } RH$, then the result also holds for the RG -module M .

For the rest of the proof, we may assume that G is a p -group. We shall treat the case where R is a d.v.r. as in (B) above, leaving to the reader the easier case where R is a perfect field. Let $M \in \text{Ind } RG$, and let $D \in \text{vtx } M$. By

Lemma 19.10, $M|L^G$ for some $L \in \text{Ind } RD$. If L is absolutely indecomposable, then so is L^G by (19.24), and it follows that $M \cong L^G$. But then

$$\text{R-rank of } M = |G:D| \cdot (\text{R-rank of } L),$$

which gives the desired result.

We now show how to reduce the general situation to the absolutely indecomposable case. By (30.31), there exists a complete d.v.r. S which is an extension of R with perfect residue class field \bar{S} , such that $SM = \bigoplus N_i$, where each N_i is an absolutely indecomposable SG -lattice for which $\tilde{E}(N_i) \cong \bar{S}$. If $D \in \text{vtx } M$, then clearly each N_i is (G, D) -projective, so $D \in \text{vtx } N_i$ for each i . By the previous discussion, the S -rank of each N_i is a multiple of $|G:D|$. Therefore the S -rank of SM is a multiple of $|G:D|$. But the S -rank of SM equals the R -rank of M , which completes the proof.

The final result is an application of (19.22) to character theory, and illustrates the kind of result about complex characters which can be obtained from the theory of modular representations. The following theorem is of interest in its own right, and is essential for block theory (Chapter 9).

(19.27) Green's Theorem on Zeros of Characters (Green [62]). *Let R be a complete d.v.r. with quotient field K , and perfect residue class field \bar{R} of characteristic p . Let M be an RG -lattice which is (G, D) -projective, for some p -subgroup D of G . Let $x \in G$ be an element whose p -part u is not conjugate to an element of D . Then the trace map on M vanishes at x , that is,*

$$\text{Tr}(x, M) = 0.$$

In other words, the K -character of G afforded by $K \otimes_R M$ vanishes at x .

Proof. Let u be the p -part of x ; then $u \notin D$, so $u \neq 1$. Set $X = \langle x \rangle$, $Y = \langle x^p \rangle$. Then $|X:Y|=p$ because $u \neq 1$. Since $u \notin {}^aD$ for all $a \in G$, we have

$${}^aD \cap X \leq Y \text{ for all } a \in G.$$

Now M is (G, D) -projective, so $M|L^G$ for some $L \in \text{Ind } RD$. Then $M_X|(L^G)_X$, and by Mackey's Theorem 19.6, we have

$$(L^G)_X = \bigoplus_a (L_{{}^aD \cap X})^X = \bigoplus_a (L_{{}^aD \cap X})^Y)^X,$$

since $Y \leq X$. We may write

$$(L_{{}^aD \cap X})^Y = \bigoplus N_j,$$

for certain indecomposable RY -lattices N_j . By (30.31), we may assume, after a suitable extension of R (which does not affect the trace function), that the $\{N_j\}$ are absolutely indecomposable RY -lattices. By the Green Indecomposability Theorem 19.22, each module N_j^X is an indecomposable RX -lattice. By

the K-S-A Theorem, it follows that M_x is isomorphic to a direct sum of some of the modules $\{N_j^X\}$. Since X is abelian, and $x \notin Y$, we have

$$\mathrm{Tr}(x, N_j^X) = 0 \text{ for each } j.$$

Therefore $\mathrm{Tr}(x, M) = 0$ and the proof is complete.

§19 Exercises

1. Let H be a Sylow p -subgroup of the finite group G , and let $\mathrm{char} k = p$. Let $|\mathrm{Ind} kH|$ denote the number of isomorphism classes of indecomposable kH -modules (always assumed f.g.).

(i) Show that

$$|\mathrm{Ind} kG| < \infty \Leftrightarrow |\mathrm{Ind} kH| < \infty.$$

(ii) Prove that if $H = \langle x \rangle$ is a cyclic group of order p^n , then $\mathrm{Ind} kH$ consists of the indecomposable modules

$$M_d = k[x]/(1-x)^d k[x], \quad 1 \leq d \leq p^n.$$

(iii) Prove that $|\mathrm{Ind} kH|$ is infinite when H is not cyclic.

[Hint: (These results are due to D. G. Higman [54]): For (i), use (19.2) and (19.3). For (ii), see (20.13) below. A proof of (iii) is given in CR §64; the result also follows as a special case of Dade's Theorem 33.8 below.]

2. Let (K, R, k) be a p -modular system. Show that for each projective RG -lattice M , the R -rank of M is a multiple of $|G|_p$.

3. Let R be any commutative ring, and let G be a finite group whose order is a unit in R . Show that every RG -lattice M is a projective RG -module.

[Hint: M is RG -projective if and only if M is $(G, 1)$ -projective, since M is a lattice. Now use (19.5) with $H = \{1\}$. For related results, see (30.16) below.]

4. Prove **Wedderburn's Theorem**. Let A be a f.d. algebra over a field K , and let B be a left ideal of A which has a K -basis $\{b_i\}$ consisting of nilpotent elements. Then B is a nilpotent ideal of A , and therefore $B \subseteq \mathrm{rad} A$.

[Hint: After extending the ground field, we may assume that K is algebraically closed. Let $N = \mathrm{rad} A$, and set

$$\bar{A} = A/N, \quad \bar{B} = (B + N)/N.$$

Then \bar{B} is a left ideal of the split semisimple K -algebra \bar{A} , and \bar{B} also has a K -basis $\{\bar{b}_i\}$ consisting of nilpotent elements. It suffices to prove that $\bar{B} = 0$. If $\bar{B} \neq 0$, then \bar{B} contains a minimal left ideal $\bar{A}e$ of \bar{A} , where e is some primitive idempotent of \bar{A} . We may represent e as a matrix $\mathrm{diag}(1, 0, \dots, 0)$, and then $\mathrm{Trace}(e) = 1$. On the other hand, $e = \sum \beta_i \bar{b}_i$, $\beta_i \in K$, with each \bar{b}_i nilpotent, so $\mathrm{Trace}(e) = 0$.]

§20. THE GREEN CORRESPONDENCE. APPLICATIONS TO CHARACTER THEORY

In this section, we prove several fundamental results of Green [64], which establish further connections between indecomposable RG -lattices and indecomposable RH -lattices, for certain subgroups H of G . The idea is to achieve a *group-theoretical reduction*, which transfers the study of indecomposable lattices from G to proper subgroups of G . More precisely, let D be a fixed p -subgroup of G , and let $H \geq N_G(D)$. We shall show that there is a certain family \mathcal{Q} of subgroups of D , including D itself, for which there exists a bijection between the set of indecomposable RG -lattices $\{M\}$ with vertices in \mathcal{Q} , and the set of indecomposable RH -lattices $\{N\}$ with vertices in \mathcal{Q} , such that corresponding lattices have the same vertex. This bijection is called the Green Correspondence.

When applied to blocks (see §19B and Chapter 9), the Green correspondence provides an interpretation of some of the main theorems of Brauer.

In §20B, we give Thompson's application of the theory of vertices and sources, and the Green correspondence, to the character theory of certain groups involving Frobenius groups as subgroups. This application, in turn, will be crucial for the theory of blocks in Chapter 9.

§20A. The Green Correspondence

Throughout this section, the hypotheses and notation established in §19B remain in force. Thus, $\text{Ind } RG$ denotes the set of indecomposable RG -lattices, where R is either a field of characteristic p or a d.v.r. with residue field $\bar{R} = R/\mathfrak{p}$ of characteristic p , such that the K-S-A Theorem holds for RG -lattices. As in §19B, $\text{vtx } M$ denotes the set of vertices of $M \in \text{Ind } RG$. By (19.13), $\text{vtx } M$ is a single conjugacy class of p -subgroups of G . It will be convenient to add to our terminology as follows:

(20.1) Definitions. Let \mathcal{Z} be a family of subgroups of G . An RG -lattice M is said to be (G, \mathcal{Z}) -projective if $M = \bigoplus M_i$, where for each i , M_i is a (G, Z_i) -projective RG -lattice for some subgroup $Z_i \in \mathcal{Z}$. Using a notation borrowed from analysis, we write

$$M = O(\mathcal{Z})$$

to denote a (G, \mathcal{Z}) -projective RG -lattice M . We shall write $Z \leq_G \mathcal{Z}$ to indicate that $Z \leq_G Z'$ for some subgroup $Z' \in \mathcal{Z}$. We also write

$$M = L \oplus O(\mathcal{Z})$$

whenever $M = L \oplus N$ with $N = O(\mathcal{Z})$.

We first require two preliminary results.

(20.2) Lemma. *Let \mathcal{Z} be a family of subgroups of G . Then direct sums, and summands, of (G, \mathcal{Z}) -projective RG -lattices are (G, \mathcal{Z}) -projective.*

Proof. Direct sums of (G, \mathcal{Z}) -projective RG -lattices are clearly (G, \mathcal{Z}) -projective by definition (see (20.1)). Now let $M = O(\mathcal{Z})$, and let N be an RG -lattice such that $N|M$. By the first part of the proof, it is sufficient to prove that the indecomposable direct summands of N are $O(\mathcal{Z})$, so we may assume that N is indecomposable. By (20.1), $M = \bigoplus M_i$, where each summand M_i is (G, Z_i) -projective for some subgroup $Z_i \in \mathcal{Z}$. Since $N|M$ and $N \in \text{Ind } RG$, the K-S-A Theorem implies that $N|M_i$ for some i , and so N is (G, Z_i) -projective by (19.5v). This completes the proof of the lemma.

(20.3) Lemma. *Let \mathcal{Z} be a family of subgroups of G . Let M be an indecomposable RG -lattice with vertex D^* . Then $M = O(\mathcal{Z})$ if and only if $D^* \leq_G \mathcal{Z}$.*

Proof. If $D^* \leq_G \mathcal{Z}$ then $D^* \leq_G Z_i$ for some $Z_i \in \mathcal{Z}$. Then M is (G, Z_i) -projective by (19.5vii), and so $M = O(\mathcal{Z})$. Conversely, if $M = O(\mathcal{Z})$, then M is (G, Z_i) -projective for some subgroup $Z_i \in \mathcal{Z}$, and we have $D^* \leq_G Z_i$ by Theorem 19.8.

(20.4) Definition. An *admissible triple* (G, H, D) for the Green correspondence consists of a finite group G , a p -subgroup D of G , and a subgroup H containing $N_G(D)$. For each such triple, we define families of subgroups:

$$(20.5) \quad \begin{cases} \mathcal{X} = \mathcal{X}(D, H) = \{ {}^x D \cap D : x \in G - H \} \\ \mathcal{Y} = \mathcal{Y}(D, H) = \{ {}^x D \cap H : x \in G - H \} \\ \mathcal{Q} = \mathcal{Q}(D, H) = \{ D^* \leq D : D^* \not\leq_G \mathcal{X} \}. \end{cases}$$

We recall that $D^* \not\leq_G \mathcal{X}$ means $D^* \not\leq_G X$ for all subgroups $X \in \mathcal{X}$. We also note that $D \in \mathcal{Q}$, so that \mathcal{Q} is nonempty.

The main result is as follows:

(20.6) Theorem. *Let (G, H, D) be an admissible triple of groups as in (20.4), and let $\mathcal{Q}, \mathcal{X}, \mathcal{Y}$ be the families of subgroups defined in (20.5). Then there exists a bijection*

$$g : [M] \leftrightarrow [N]$$

from the set of isomorphism classes of indecomposable RG -lattices M with vertex in \mathcal{Q} to the set of isomorphism classes of indecomposable RH -lattices N with vertex in \mathcal{Y} . A lattice $M \in \text{Ind } RG$ with vertex in \mathcal{Q} corresponds to an indecomposable RH -lattice N with the same vertex if and only if either of the following equivalent conditions holds:

$$(i) \quad M_H = N \oplus O(\mathcal{Y})$$

or

$$(ii) \quad N^G = M \oplus O(\mathcal{Y}).$$

Furthermore, corresponding modules have the same source as well as the same vertex.

(20.7) Definition. The bijection g defined in Theorem 20.6 is called the *Green correspondence* (associated with the triple (G, H, D)).

Before proving the theorem, it may be helpful to state a corollary which is a less general version of the Green correspondence, but is perhaps easier to understand.

(20.8) Corollary. Let D be a p -subgroup of G , and let $H \geq N_G(D)$. Then there is a bijection $g: [M] \leftrightarrow [N]$ between isomorphism classes of indecomposable RG -lattices M with vertex D , and 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 $M | N^G$ or $N | M_H$.

The proof of Theorem 20.5 will be given in several steps, some of which are of interest in themselves.

Step 1. Let N be an (H, D) -projective RH -lattice. We assert that

$$(N^G)_H = N \oplus O(\mathcal{Y}).$$

We have already noted several times that $N | (N^G)_H$; see (19.3a) or the Subgroup Theorem 19.6. Therefore $(N^G)_H = N \oplus N'$ for some RH -lattice N' . We have to prove that $N' = O(\mathcal{Y})$. Since N is (H, D) -projective, by (19.2v) we have

$$L^H = N \oplus U$$

for some RD -lattice L and some RH -lattice U . Then $U | (U^G)_H$, so we may write $(U^G)_H = U \oplus U'$. This gives

$$N \oplus N' \oplus U \oplus U' = (N^G)_H \oplus (U^G)_H \cong ((L^H)^G)_H \cong (L^G)_H.$$

By the Subgroup Theorem, we obtain

$$(L^G)_H = L^H \oplus \left(\bigoplus_{x \notin H} ({^x}L_{{^x}D \cap H})^H \right) \cong N \oplus U \oplus \left(\bigoplus_{x \notin H} ({^x}L_{{^x}D \cap H})^H \right)$$

By the cancellation theorem (Corollary 6.15), we conclude that

$$N' \oplus U' \cong \bigoplus_{x \notin H} ({^x}L_{{^x}D \cap H})^H = O(\mathcal{Y}).$$

By Lemma 20.2, it follows that $N' = O(\mathcal{Y})$, and the proof is completed.

Step 2. Let $D^* \leq D$, and let \mathcal{X} and \mathcal{Y} be the families of subgroups defined in (20.5). Then

$$D^* \leq_G \mathcal{X} \Leftrightarrow D^* \leq_H \mathcal{X} \Leftrightarrow D^* \leq_H \mathcal{Y}.$$

The proof is left as an exercise.

Step 3. Let $M \in \text{Ind } RG$, and suppose there exists $D^* \in \text{vtx } M$ such that $D^* \leq D$. The following statements hold:

- (i) If $M = O(\mathcal{X})$, then $M_H = O(\mathcal{Y})$.
- (ii) If $M \neq O(\mathcal{X})$, then $M_H = N \oplus O(\mathcal{Y})$

for some indecomposable RH -lattice N with vertex D^* , such that $N \neq O(\mathcal{Y})$.

We first prove (i). By (19.15iii), there exists $W \in \text{Ind } RH$ such that $M | W^G$ and $D^* \in \text{vtx } W$. Since $D^* \leq D$, W is (H, D) -projective, so

$$(W^G)_H = W \oplus O(\mathcal{Y})$$

by Step 1. But $M_H | (W^G)_H$, and $M = O(\mathcal{X})$ by hypothesis, so $D^* \leq_G \mathcal{X}$ by Lemma 20.3. Therefore $D^* \leq_H \mathcal{Y}$ by Step 2. Since $D^* \in \text{vtx } W$, we can apply (20.3) to W , to obtain $W = O(\mathcal{Y})$. Thus $(W^G)_H = O(\mathcal{Y})$, so $M_H = O(\mathcal{Y})$ by Lemma 20.2.

To prove (ii), we apply (19.15iii) again, to obtain $N \in \text{Ind } RH$ such that $M | N^G$ and $D^* \in \text{vtx } N$. By Step 1, $(N^G)_H = N \oplus O(\mathcal{Y})$. Since $M \neq O(\mathcal{X})$, $D^* \not\leq_G \mathcal{X}$ by (20.3), so $D^* \not\leq_H \mathcal{Y}$. By (20.3) again, N is the unique indecomposable summand of $(N^G)_H$ which is not $O(\mathcal{Y})$. By (19.15ii), M_H has an indecomposable summand with vertex D^* . Since $M_H | (N^G)_H$ and $(N^G)_H = N \oplus O(\mathcal{Y})$, this summand must be N . It follows that $M_H = N \oplus O(\mathcal{Y})$, completing the proof of (ii).

The significant feature of Step 3 is that, in case (ii), N is the *unique* indecomposable summand of M_H not in $O(\mathcal{Y})$. This phenomenon is the key to the proof of Theorem 20.6. The next result shows that the same thing happens in the opposite direction.

Step 4. Let N be an indecomposable RH -lattice with vertex $D^* \leq D$. The following statements hold:

- (i) If $N = O(\mathcal{X})$, then also $N^G = O(\mathcal{X})$.
- (ii) If $N \neq O(\mathcal{X})$, then $N^G = M \oplus O(\mathcal{X})$

for some lattice $M \in \text{Ind } RG$ such that $N | M_H$, and $D^* \in \text{vtx } M$.

We first prove (i). Since $D^* \in \text{vtx } N$, N is (H, D^*) -projective, and hence $N | (N_{D^*})^H$ by Theorem 19.2. Then $N^G | (N_{D^*})^G$ by transitivity of induction, and so N^G is (G, D^*) -projective. Since $D^* \leq_G \mathcal{X}$ by Lemma 20.3, it follows that $N^G = O(\mathcal{X})$, completing the proof of (i).

The proof of (ii) is more difficult. We first write

$$N^G = M_1 \oplus \cdots \oplus M_l, \text{ with } M_i \in \text{Ind } RG, 1 \leq i \leq l.$$

From the proof of part (i) and (19.5v), each module M_i is (G, D^*) -projective, and hence each M_i has a vertex D_i such that

$$D_i \leq_G D^* \leq D.$$

By Step 3, for each i , $1 \leq i \leq l$, we have either:

(a) $M_i = O(\mathcal{X})$ and $(M_i)_H = O(\mathcal{Y})$,

or

(b) $M_i \neq O(\mathcal{X})$ and $(M_i)_H$ has exactly one indecomposable direct summand which is $\neq O(\mathcal{Y})$.

By Step 1 we also have

(c) $(N^G)_H = N \oplus O(\mathcal{Y})$.

By the hypothesis of (ii), $N \neq O(\mathcal{X})$, and hence $D^* \not\leq_H \mathcal{X}$ by Lemma 20.3. Then $D^* \not\leq_H \mathcal{Y}$ by Step 2, and $N \neq O(\mathcal{Y})$, by (20.3) again. From (a)–(c) above, it follows that there is a unique indecomposable summand M_{i_0} of N^G such that $M_{i_0} \neq O(\mathcal{X})$. Moreover, N is the unique indecomposable summand of $(M_{i_0})_H$ which is $\neq O(\mathcal{Y})$, according to (b). Finally, M_{i_0} has vertex D^* , by (19.16), completing the proof.

Step 5. It is now easy to assemble a proof of (20.6). Let $M \in \text{Ind } RG$, with $D^* \in \text{vtx } M$ for some subgroup D^* in \mathcal{Q} . Then $D^* \not\leq_G \mathcal{X}$ by (20.5), so $M \neq O(\mathcal{X})$ by (20.3), and M_H has a uniquely determined indecomposable summand $N \neq O(\mathcal{Y})$, where N has vertex D^* . Thus we have a well-defined map of isomorphism classes

$$g : [M] \rightarrow [N],$$

as in (20.6). By Step 4, the map g is surjective. To prove it is injective, suppose that $N \mid M_H$ where $N \in \text{Ind } RH$ and $M \in \text{Ind } RG$ both have vertex D^* in \mathcal{Q} . We have to prove that the isomorphism class of M is uniquely determined by these conditions, and for that, it is sufficient by Step 4 to prove that $M \mid N^G$. (Notice that this is closely related to the question as to whether both conditions (ii) and (iii) of Theorem 19.15 can be satisfied with the same module.) By (19.15i), there exists $U \in \text{Ind } RH$ with vertex G -conjugate to D^* , such that $U \mid M_H$ and $M \mid U^G$. It follows from Step 2 and (20.3) that $U \neq O(\mathcal{Y})$, so $U \cong N$ by Step 3, and $M \mid N^G$ as required. This completes the proof that g is a bijection of isomorphism classes.

The second statement of (20.6) is immediate from Steps 3 and 4, and the final remark follows from (19.15iv).

§20B. Applications to Character Theory

In this subsection, we shall apply the results of §19 and §20A to character theory. Our presentation is based mainly on Thompson's paper [67]. The first part is devoted to general results on characters afforded by RG -modules, with reference to questions about projectivity and reduction mod \mathfrak{p} . The discussion then focuses on the character theory of a group G with a cyclic self-centralizing Sylow p -subgroup D , which is a T.I. set. Examples will be given to show that this configuration occurs frequently among simple groups which are minimal in some sense. Such a subgroup D is a special abelian subgroup. This situation was studied previously in §14C, and the results on exceptional and non-exceptional characters relative to such a subgroup can be applied (see Propositions 14.17 and 14.19). The main point of the discussion below is that with the help of modular representations, we can obtain much sharper versions of the results of §14C. The summarized version (20.23) shows how, in this case, a remarkable amount of information about the characters of G can be lifted from the character theory of a p -local subgroup of G . In Chapter 9, these sharper results will be applied to the study of blocks with cyclic defect groups. One result along the way, of independent interest, is the determination of all indecomposable kG -modules for certain Frobenius groups which occur as normalizers of p -groups D as above (see (20.11) and (20.13)).

Throughout this subsection, G denotes 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 RG is a semiperfect ring. In this situation, all of the results of §§18, 19 and 20A are valid, and we shall frequently use the notation and results established in those sections.

If M is any RG -lattice, by the K -character of G afforded by M we shall always mean the K -character μ of G afforded by the KG -module $K \otimes_R M$. The values $\{\mu(x) : x \in G\}$ can be computed from an R -representation of G relative to an R -basis of M , without passing to $K \otimes_R M$.

Suppose now that U and V are KG -modules affording characters μ, ν , respectively. As in §19A, we shall write $\mu|\nu$ to indicate that $U|V$ (that is, U is isomorphic to a KG -direct summand of V).

As preparation for the following discussion, the reader may wish to review the properties of R -pure sublattices of RG -lattices, as described in §4D.

Our first result asserts that summands of the character afforded by an indecomposable projective lattice M can be "taken off the top" of M .

(20.9) Proposition. *Let P be an indecomposable projective RG -lattice, affording the K -character τ , and let μ be a K -character of G such that $\mu|\tau$. Then there exists an R -pure RG -sublattice N of P such that P/N affords μ , and $\overline{P/N}$ is an indecomposable kG -module.*

Proof. Let $V = K \otimes_R P$, so V is a semisimple KG -module, and write $\tau = \mu + \nu$ for some character ν . Then correspondingly $V = U \oplus W$, where U, W afford

μ, ν , respectively. Setting $N = W \cap P$, we obtain an exact sequence of RG -lattices

$$0 \rightarrow N \rightarrow P \rightarrow P/N \rightarrow 0,$$

since N is R -pure in P (see (4.12)). Clearly P/N affords μ . (This part of the argument does not depend on P being an indecomposable projective module, and is a special case of (23.15) below.)

In order to prove that $\overline{P/N}$ (and hence also P/N) is indecomposable, we note that the RG -homomorphism

$$\varphi: P \rightarrow P/N \rightarrow \overline{P/N},$$

defined by composition of maps, has the property that $\mathfrak{p}P \subseteq \ker \varphi$. Therefore $\overline{P/N}$ is a homomorphic image of the indecomposable projective kG -module \overline{P} , and is therefore indecomposable, since \overline{P} has a unique maximal submodule, by (18.1). This completes the proof.

(20.10) Proposition. *Let M be an RG -lattice such that $\overline{M} = N_1 \oplus P_1$, where P_1 is a projective kG -module. Then there exist an RG -lattice N and a projective RG -lattice P such that*

$$M \cong N \oplus P, \quad \overline{N} \cong N_1, \quad \overline{P} \cong P_1.$$

Proof. By (18.1) $P_1 \cong \overline{P} = P/\mathfrak{p}P$ for some projective RG -lattice P . Likewise, we may write $\overline{M} = M/\mathfrak{p}M$. Consider the diagram

$$\begin{array}{ccc} P & & M \\ \alpha \downarrow & & \beta \downarrow \\ \overline{P} & \xrightleftharpoons{i} & \overline{M}, \\ & j \uparrow & \end{array}$$

where α, β are natural maps, and i, j arise from the direct sum decomposition $\overline{M} \cong \overline{P} \oplus N_1$. Thus, $ji = 1$ on \overline{P} .

Since P is RG -projective, we can find a map $f \in \text{Hom}_{RG}(P, M)$ such that $\beta f = i\alpha$ on P . Likewise, since M is R -projective, we can find a map $g \in \text{Hom}_R(M, P)$ such that $\alpha g = j\beta$ on M . Then

$$\alpha g f = j\beta f = ji\alpha = \alpha,$$

and consequently

$$P = \mathfrak{p}P + (gf)P.$$

This implies that $P = (gf)P$ by Nakayama's Lemma, since P is a f.g. R -module.

It follows now that f is a monomorphism, and the exact sequence of RG -modules

$$(*) \quad 0 \rightarrow P \xrightarrow{f} M \rightarrow M/P \rightarrow 0$$

is split by the R -homomorphism $g: M \rightarrow P$. In particular, M/P is also a RG -lattice.

Since P is RG -projective, P is also $(G, 1)$ -projective in the sense of (19.1). But then P is $(G, 1)$ -injective by (19.2). Since the sequence $(*)$ is split over R , it follows that it is also split over RG . Thus

$$M \cong P \oplus (M/P)$$

as RG -modules, which completes the proof.

As a special case of (20.10), it follows that if \overline{M} is kG -projective, then M is RG -projective. In this connection, see (30.11).

For the rest of this subsection, we shall assume that the finite group G has a cyclic Sylow p -subgroup D of order p^d . Our main interest centers on the case where the following holds:

$$D = C_G(D), \text{ and } D^* \text{ is a T.I. set,}$$

(see (14.16)), where $D^* = D - \{1\}$. We put $H = N_G(D)$.

It is clear from the conditions on D that $D = C_G(x)$ for all $x \in D^*$, so D is a special abelian subgroup of G (see (14.15)). Then by (14.17i), H is a Frobenius group with Frobenius kernel D . A further simplification is that each p -irregular element is a p -element. Here are some examples of the above situation:

$$G = PSL_2(p), D = \text{Sylow } p\text{-subgroup of } G, p \text{ odd};$$

$$G = A_5, p = 3, 5; G = A_6 \cong PSL_2(9), p = 5;$$

$$G = PSL_2(7) \cong GL_3(2), p = 3, 5; G = SL_2(8), p = 7;$$

$$G = PSL_2(11), p = 5, 11; G = M_{11}, p = 5, 11.$$

The results obtained below are helpful in determining the character tables of all of the groups listed above.

Our first step is the determination of all indecomposable kH -modules, the key fact being that H has a cyclic normal Sylow p -subgroup D . We showed in CR (64.6) that there are at most $|H|$ distinct indecomposable kH -modules, and that this maximum is achieved if and only if H/D is abelian, and k is sufficiently large relative to H/D . We shall need a more detailed version of this result for the case where D satisfies the restrictive hypotheses described earlier. However, since this same situation arises in many other contexts, we

shall begin with a more general discussion of indecomposable kH -modules. The following result occurs frequently in the literature (see, for example, Srinivasan [60], O'Reilly [65], Berman [66], Lam-Reiner [69]):

(20.11) Proposition. *Let D be a cyclic normal Sylow p -subgroup of a finite group H , and let k be any field of characteristic p , not necessarily a splitting field for H . Let $\{U_i : 1 \leq i \leq s\}$ be a basic set of projective indecomposable kH -modules, and let*

$$D = \langle x : x^{p^d} = 1 \rangle, N = \text{rad } kD = (x - 1)kD,$$

so N is nilpotent of exponent p^d . Put

$$M_{ij} = U_i / N^j U_i, 1 \leq j \leq p^d, 1 \leq i \leq s.$$

Then the $s \cdot p^d$ modules $\{M_{ij}\}$ are a full set of non-isomorphic indecomposable kH -modules.

Proof. For each $a \in H$ we have $aNa^{-1} = N$ since $D \trianglelefteq H$, and therefore $N^j U_i$ is a kH -submodule of U_i , for each i and j . Furthermore, by (18.1) the projective indecomposable kH -module U_i has a unique maximal submodule $(\text{rad } kH)U_i$, with simple quotient

$$F_i = U_i / (\text{rad } kH)U_i, 1 \leq i \leq s,$$

and these $\{F_i\}$ are a basic set of simple kH -modules. Since $N \cdot kH = kH \cdot N$ and N is nilpotent, it is clear that $N \subseteq \text{rad } kH$, and thus $N^j U_i \subseteq (\text{rad } kH)U_i$ for each i and j . Therefore each M_{ij} has a unique maximal submodule $(\text{rad } kH)U_i / N^j U_i$, with simple quotient F_i . This shows that each M_{ij} is indecomposable, and that $M_{ij} \cong M_{i'j'}$ implies $i = i'$.

Next, since each U_i is kH -projective, it follows that its restriction $U_i|_D$ is kD -projective, and is therefore free as kD -module by (5.24). This implies that

$$\dim_k M_{ij} = j \cdot \dim_k M_{i1},$$

so no two of the modules $\{M_{ij} : 1 \leq j \leq p^d\}$ can be isomorphic. We have therefore constructed $s \cdot p^d$ indecomposable kH -modules $\{M_{ij} : 1 \leq j \leq p^d, 1 \leq i \leq s\}$, and it remains to prove that there are no others.

By linear algebra, there are exactly p^d indecomposable kD -modules, given by

$$T_j \cong k[x] / (1 - x)^j k[x] = kD / N^j, 1 \leq j \leq p^d,$$

and $\dim_k T_j = j$ for each j . Since D is a Sylow p -subgroup of H , each

$M \in \text{Ind } kH$ is (H, D) -projective by (19.5ix), and hence $M|T_j^H$ for some j . But

$$T_j^H = kH \otimes_{kD} (kD/N^j) \cong kH/N^j kH, \quad 1 \leq j \leq p^d.$$

Since kH is expressible as a direct sum of U_i 's with various multiplicities, say

$$kH \cong \coprod_{i=1}^s U_i^{(n_i)},$$

it follows that

$$T_j^H \cong \coprod_{i=1}^s (M_{ij})^{(n_i)}, \quad 1 \leq j \leq p^d.$$

This completes the proof that the $\{M_{ij}\}$ are a full set of indecomposable kH -modules, and establishes the proposition. Furthermore, since kH is a free left kD -module on $e = |H : D|$ generators, it follows that $T_j^H|_D \cong T_j^{(e)}$ (this can also be deduced from the Subgroup Theorem), and therefore for each i , the restriction $M_{ij}|_D$ is isomorphic to a sum of copies of T_j .

(20.12) Remarks. (i) Since D is a Sylow p -subgroup of H , the Schur-Zassenhaus Theorem tells us that $H = D \rtimes A$ for some subgroup A of H . We have not used this fact anywhere in the above proof. Furthermore, the fact that D is a Sylow group was only used to deduce that every kH -module is (H, D) -projective. Thus, the above proof yields the following more general statement, which will be needed in Chapter 6, in our discussion of relative Grothendieck rings.

Let D be a cyclic normal p -subgroup of H . Then the modules $\{M_{ij}\}$ constructed above are a full set of non-isomorphic indecomposable (H, D) -projective kH -modules, and every (H, D) -projective kH -module is uniquely expressible as a direct sum of M_{ij} 's.

(ii) An analogous calculation, in which we determine all indecomposable representations of H over the ring of p -adic integers, is given in the paragraphs following (34.44) below.

We now resume the main current of our discussion, and prove:

(20.13) Proposition. *Let H be a Frobenius group whose Frobenius kernel D is cyclic of order p^d , and let k be a field of characteristic p which is sufficiently large relative to H . Let A be a Frobenius complement in H . Then A is an abelian group, whose order e divides $p - 1$, and we have:*

- (i) *For each simple kH -module F , $\dim_k F = 1$.*

- (ii) There are exactly $|H|$ non-isomorphic indecomposable kH -modules $\{M_{ij} : 1 \leq i \leq e, 1 \leq j \leq p^d\}$, and $\dim M_{ij} = j$ for all i, j .
- (iii) If $M \in \text{Ind } kH$, then $M_D \in \text{Ind } kD$.
- (iv) All submodules of an indecomposable kD -module are indecomposable.

Proof. From §14A, we may write $H = D \rtimes A$, and A acts on D without fixed points, since $C_H(D) = D$. Then A is isomorphic to a subgroup of $\text{Aut } D$, so A is abelian of order e , where e divides $\varphi(p^d) = p^{d-1}(p-1)$. Since $|A|$ and $|D|$ are relatively prime because D is a Sylow p -subgroup of H , it follows that $e|(p-1)$, as claimed.

Now A is abelian group whose order e is prime to p , and k is a sufficiently large field of characteristic p , so the algebra kA is a split semisimple k -algebra. Let $\{\delta_1, \dots, \delta_e\}$ be the primitive idempotents in the commutative algebra kA ; then the simple kA -modules are $\{kA \cdot \delta_i : 1 \leq i \leq e\}$, and

$$kA = \bigoplus_{i=1}^e kA \cdot \delta_i = \bigoplus_{i=1}^e k\delta_i,$$

with $\dim_k k\delta_i = 1$ for each i . We have therefore

$$kH \cong kH \otimes_{kA} kA = \bigoplus_{i=1}^e kH \cdot \delta_i = \bigoplus_{i=1}^e kD \cdot \delta_i.$$

Since $kD \cdot \delta_i$ is a homomorphic image of kD , comparing dimensions of both sides of the above shows that

$$\dim_k kH \cdot \delta_i = p^d, \quad 1 \leq i \leq e,$$

and $kH \cdot \delta_i$ is isomorphic to kD as kD -module. Setting

$$U_i = kH \cdot \delta_i = kD \cdot \delta_i, \quad 1 \leq i \leq e,$$

it follows that the $\{U_i\}$ are indecomposable projective kH -modules. Further, by (5.24) and Clifford's Theorem, we know that D acts trivially on each simple kH -module, so the simple kH -modules can be identified with the simple kA -modules $\{k\delta_i : 1 \leq i \leq e\}$. By (18.1), it follows that the $\{U_i : 1 \leq i \leq e\}$ are a basic set of projective indecomposable kH -modules.

We now apply the Proposition 20.11. Since $kH = \bigoplus_{i=1}^e U_i$, it follows that

$$T_j^H \cong \coprod_{i=1}^e M_{ij},$$

using the notation of the proof of (20.11). Comparing dimensions of both

sides, we conclude that $\dim M_{ij} = \dim T_j = j$, and that $M_{ij}|_D \cong T_j$. This completes the proof of (i)–(iii), while (iv) is obvious from the formula for T_j , so Proposition 20.13 is established.

(20.14) Proposition. *Let H be as in (20.13), and let (K, R, k) be a p -modular system such that K is sufficiently large, of characteristic zero, and RH is semiperfect. Let M be an indecomposable RH -lattice such that \bar{M} is indecomposable, and let μ be the K -character of H afforded by M . Then $(\mu_D, \varphi) \leq 1$ for all linear characters φ of D .*

Proof. From (17.2), k is sufficiently large relative to H , so we may apply (20.13) to conclude that \bar{M}_D and each of its submodules is indecomposable. Therefore every R -pure RD -submodule of M is indecomposable, since it remains indecomposable after reduction mod \mathfrak{p} .

Now let φ be a linear K -character of D , and define

$$M_\varphi = \{m \in M : (x - \varphi(x))m = 0 \text{ } \forall x \in D\}.$$

Then $M_\varphi = (KM_\varphi) \cap M$, so M_φ is a pure R -sublattice of M , by (4.12). It is also clear that M_φ is an RD -submodule of M_D , and hence $M_\varphi \in \text{Ind } RD$.

We next show that

$$\text{rank}_R M_\varphi = (\mu_D, \varphi)_D.$$

Let $V = KM$; then V affords μ , and $(\mu_D, \varphi)_D$ is the K -dimension of the homogeneous component V_φ of V_D affording a multiple of φ . Now V_D is a semisimple KD -module, and since φ is a linear character of the abelian group D , we have

$$V_\varphi = \{v \in V : (x - \varphi(x))v = 0 \text{ } \forall x \in D\}.$$

Then $M_\varphi = V_\varphi \cap M$, and $V_\varphi = KM_\varphi$, so $\text{rank}_R M_\varphi = (\mu_D, \varphi)_D$, as claimed.

Finally, since $M_\varphi \in \text{Ind } RD$, it follows that the R -rank of M_φ is ≤ 1 , because any R -decomposition of M_φ is an RD -decomposition, by the preceding step. This completes the proof of (20.14).

We shall now apply the preceding results, along with the Green correspondence (20.6), to the character theory of a finite group G containing the configuration of (20.13).

(20.15) Proposition. *Let D be a cyclic self-centralizing Sylow p -subgroup of G which is a T.I. set, and let $H = N_G(D)$, so H is a Frobenius group with Frobenius kernel D , as in (20.13). Let (K, R, k) be a p -modular system with K sufficiently large. Then for every indecomposable non-projective RG -lattice M for which \bar{M} is also indecomposable, there exists an indecomposable non-projective RH -lattice L*

such that

$$M \mid L^G, \bar{L} \in \text{Ind } kH, \text{ and } M_H = L \oplus Q \text{ for some } Q \in \mathcal{P}(RH).$$

Proof. By (14.17i), H is indeed a Frobenius group with Frobenius kernel D , as in (20.13). We shall apply the Green Correspondence 20.6, to the admissible triple of group (G, H, D) . The families of subgroups \mathcal{X} and \mathcal{Q} in (20.5) then become

$$\mathcal{X} = \{ {}^x D \cap D : x \in G - H \} = \{ 1 \}$$

(since D is a T.I. set), and

$$\mathcal{Q} = \{ D^* \leq D : D^* \not\leq_G \mathcal{X} \} = \text{set of all non-trivial subgroups of } D.$$

Therefore an RG -lattice M is $O(\mathcal{X})$ if and only if M is $(G, 1)$ -projective, that is (see §19A), if and only if M is RG -projective. Further, by (20.3), \mathcal{Q} contains a vertex of M if and only if M is not RG -projective.

By Theorem 20.6 and the above remarks, there exists a bijection

$$[M] \leftrightarrow [g[M]] = [L]$$

from isomorphism classes of RG -lattices M such that $M \in \text{Ind } RG$ and $M \notin \mathcal{P}(RG)$, to isomorphism classes of RH -lattices $L = g(M)$, such that $L \in \text{Ind } RH$ and $L \notin \mathcal{P}(RH)$. Moreover, if the original RG -lattice M corresponds to $g(M) = L$, then we have

$$M \mid L^G, \text{ and } M_H \cong L \oplus Q, \text{ with } Q \in \mathcal{P}(RH).$$

By hypothesis, $\bar{M} \in \text{Ind } kG$; further, $\bar{M} \notin \mathcal{P}(kG)$ by (20.10) (with $N_1 = 0$). We may then apply Green's Theorem 20.6 to \bar{M} , to obtain an indecomposable kH -module L_1 such that $L_1 \notin \mathcal{P}(kH)$, and

$$\bar{M} \mid L_1^G, \text{ and } \bar{M}_H \cong L_1 \oplus Q_1 \text{ for some } Q_1 \in \mathcal{P}(kH).$$

Then

$$\bar{L} \oplus \bar{Q} \cong L_1 \oplus Q_1,$$

and both $\bar{Q}, Q_1 \in \mathcal{P}(kH)$. Thus L_1 is the unique non-projective indecomposable summand of \bar{L} . Then necessarily $\bar{L} \cong L_1$, since otherwise \bar{L} would have a non-trivial projective summand, and would therefore be decomposable by (20.10). This completes the proof of (20.15).

We can now combine the preceding results to obtain the following proposition, which will yield new information about the exceptional characters associated with the subgroup D .

(20.16) Proposition. Let G satisfy the hypotheses of (20.15), and let μ be a K -character of G such that $\mu|\tau$, where τ is the K -character afforded by some indecomposable projective RG -lattice P (as in (20.9)). Define

$$h(\mu) = \max_{\varphi, \varphi' \in \text{Irr } D} \{ |(\mu_D, \varphi) - (\mu_D, \varphi')| \}.$$

Then $h(\mu) \leq 1$.

Proof. By (20.9), there exists an R -pure RG -sublattice N of P such that $M = P/N$ affords μ , and $M \in \text{Ind } kG$. There are two cases to consider:

Case (i). Suppose M is projective. Then $M = P/N$ implies $M|P$, and hence $M \cong P$, since P is indecomposable. Then $\mu = \tau$, and for each linear character φ of D , we have

$$(\tau_D, \varphi) = |D|^{-1} \sum_{x \in D} \tau(x)\varphi(x^{-1}) = |D|^{-1}\tau(1)$$

by (18.26), since 1 is the only p' -element in D . In this case clearly $h(\mu) = 0$.

Case (ii). We now assume M is not projective, and apply Proposition 20.15. Then

$$M_H = L \oplus Q, \text{ with } L \in \text{Ind } RH, Q \in \mathcal{P}(RH),$$

and we have

$$\mu_H = \lambda + \eta,$$

where λ and η are the K -characters of H afforded by L and Q , respectively. Now $Q \in \mathcal{P}(RH)$, so

$$(\eta_D, \varphi) - (\eta_D, \varphi') = 0$$

for all $\varphi \in \text{Irr } D$, by Case (i). By (20.15), it follows that L satisfies the hypotheses of (20.14), and by (20.14) we have

$$0 \leq (\lambda_D, \varphi) \leq 1 \quad \forall \varphi \in \text{Irr } D.$$

Then, for all linear characters φ and φ' of D , we obtain

$$\begin{aligned} |(\mu_D, \varphi) - (\mu_D, \varphi')| &= |(\lambda_D, \varphi) - (\lambda_D, \varphi') + (\eta_D, \varphi) - (\eta_D, \varphi')| \\ &= |(\lambda_D, \varphi) - (\lambda_D, \varphi')| \leq 1, \end{aligned}$$

as required.

We now return to the study of the exceptional characters associated with the subgroup D , where D is a cyclic self-centralizing Sylow p -subgroup of G , and D is a T.I. set. By (20.15), $H=N_G(D)$ is a Frobenius group with Frobenius kernel D . Letting $D^*=D-\{1\}$, we have $C_G(d)=D$ for all $d \in D^*$, so D is a special abelian subgroup in the sense of §14C.

We first recall some of the information contained in Propositions 14.17 and 14.19. We set

$$m=|D|=p^d, e=|H:D|, n=(m-1)/e,$$

as in (14.17). For the rest of the discussion, we shall assume that $n \geq 2$. By (14.17), the set D^* is the union of a set of exactly n special classes in H .

It is easily checked that D is the derived group of H , so H has e linear characters, and, by (14.17iii), H has exactly n distinct irreducible non-linear characters $\{\psi_1, \dots, \psi_n\}$, all of degree e , which are induced from non-trivial irreducible characters φ 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

$$l_D^H - \psi_i, \quad 1 \leq i \leq n.$$

Then by (14.17iv) there exist non-trivial irreducible characters

$$\{\xi_1, \dots, \xi_n; \theta_1, \dots, \theta_f; \chi_1, \dots, \chi_h\}$$

of G , which, together with the trivial character l_G , constitute all characters in $\text{Irr } G$. There also exists a sign $\epsilon = \pm 1$, and multiplicities a , and $c_j \neq 0$, $1 \leq j \leq f$, such that

$$(20.17) \quad \lambda_i^G = (\psi_i - \psi_n)^G = \epsilon(\xi_i - \xi_n), \quad 1 \leq i \leq n-1,$$

and

$$(20.18) \quad \Gamma_i = (l_D^H - \psi_i)^G = l_G - \epsilon \xi_i + a \sum_{i=1}^n \xi_i + \sum_{j=1}^f c_j \theta_j, \quad 1 \leq i \leq n.$$

The constants ϵ , a and $\{c_j\}$ are independent of i , $1 \leq i \leq n$, and are related by the formula (see (14.19iii)).

$$(20.19) \quad e = a^2(n-1) + (a-\epsilon)^2 + \sum_{j=1}^f c_j^2.$$

The characters $\{\xi_1, \dots, \xi_n\}$ are called *exceptional characters* (relative to D); the characters $\{\theta_1, \dots, \theta_f; \chi_1, \dots, \chi_h\}$ are called *non-exceptional*, and are arranged so that the first f characters $\{\theta_j\}$ appear with non-zero multiplicities $\{c_j\}$ in the virtual characters Γ_i , $1 \leq i \leq n$, and the remaining h non-exceptional characters $\{\chi_j\}$ appear with zero multiplicity in all the $\{\Gamma_i\}$.

Various other facts, from §14C, about the values of ξ_i and θ_i and χ_j , will be quoted when we need them. We can now state the main result of this subsection.

(20.20) Theorem. *Let G , D , $H=N_G(D)$, etc., be as in (20.15), and assume that $n=(m-1)/e \geq 2$. Then the following statements hold:*

- (i) *The exceptional characters $\{\xi_i\}$ have the same degree, which is prime to p . The non-exceptional characters $\{\theta_j : 1 \leq j \leq f\}$ have degrees satisfying $\theta_j(1) \equiv \pm 1 \pmod{p}$. The degrees of the characters $\{\chi_j : 1 \leq j \leq h\}$ are all divisible by $|D|$.*
- (ii) *Up to sign, the values of the $\{\xi_i : 1 \leq i \leq n\}$ agree with the values of the $\{\psi_i\}$ on the special classes. More precisely, we have*

$$\xi_i|_{D^*} = \epsilon \psi_i|_{D^*}, \quad 1 \leq i \leq n.$$

The values of the non-exceptional characters $\{\theta_j : 1 \leq j \leq f\}$ on the elements of D^ are all ± 1 . The non-exceptional characters $\{\chi_j : 1 \leq j \leq h\}$ vanish on D^* .*

- (iii) *The exceptional characters agree on the elements of $G_{p'}$:*

$$\xi_i(x) = \xi_j(x), \quad \forall x \in G_{p'}, \quad 1 \leq i, j \leq n.$$

The values of the nonexceptional characters $\{\theta_j\}$ on $G_{p'}$ are related to the values of $\{\xi_i\}$ as follows:

$$\delta \xi_1(x) = 1 + \sum_{i=1}^f \delta_i \theta_i(x), \quad \forall x \in G_{p'},$$

where $\{\delta, \delta_1, \dots, \delta_f\}$ are all ± 1 , and are independent of $x \in G_{p'}$.

- (iv) *The number f of non-exceptional characters $\{\theta_j\}$ is given by $f=e-1$.*

(v) *The decomposition numbers $\{d_{i,j}\}$ (see (16.20)) are 0 or 1 for all irreducible characters of G .*

We first prove a crucial preliminary result:

(20.21) Lemma. *Let*

$$\Gamma_i = 1_G - \epsilon \xi_i + a \sum_{i=1}^n \xi_i + \sum_{j=1}^f c_j \theta_j, \quad 1 \leq i \leq n,$$

as in (20.18). Then $a=0$ or $\epsilon, |c_j|=1$ for $1 \leq j \leq f$, and $f=e-1$.

Proof. We first observe that since RG is projective, the regular character of G is a sum of characters afforded by the indecomposable projective RG -modules. Hence every irreducible character ζ of G satisfies the condition $\zeta|\tau$, for some character τ afforded by an indecomposable projective RG -module, as in (20.16). We first apply (20.16) to a non-exceptional character θ_i , $1 \leq i \leq f$, and obtain

$$\begin{aligned} 1 \geq h(\theta_i) &= \max_{\varphi, \varphi' \in \text{Irr } D} \{ |(\varphi, (\theta_i)_D) - (\varphi', (\theta_i)_D)| \} \\ &= \max_{\varphi, \varphi'} \{ |(\varphi - \varphi', (\theta_i)_D)| \} = \max_{\varphi, \varphi'} \{ |((\varphi - \varphi')^G, \theta_i)| \} \\ &= \max \left\{ \left| ((1_D - \psi_j)^G, \theta_i) \right|, \left| ((\psi_j - \psi_{j'})^G, \theta_i) \right| \right\} = \max \{ |c_i|, 0 \} = |c_i| \end{aligned}$$

by (20.17) and (20.18), and the definition of the characters $\{\psi_i\}$. Since $c_i \neq 0$ for $1 \leq i \leq f$ by definition, we have $|c_i|=1$.

We next compute $h(\xi_i)$ for an exceptional character. Following the calculation above, we note that for all $\varphi, \varphi' \in \text{Irr } D$, $(\varphi - \varphi')^G$ is either $1_D^G - \psi_i^G = \Gamma_i$, $1 \leq i \leq n$, or $(\psi_i - \psi_j)^G$. Moreover, by (20.17) and (20.18), we have

$$((\psi_i - \psi_j)^G, \xi_i) = \epsilon, \quad ((\psi_j - \psi_l)^G, \xi_i) = 0 \text{ if } i \neq j, l,$$

$$(\Gamma_j, \xi_i) = a \text{ (if } i \neq j) \text{ or } a - \epsilon \text{ (if } i = j).$$

Hence

$$1 \geq h(\xi_i) = \max \{ |\epsilon|, |a - \epsilon|, |a| \},$$

and we conclude that $a=0$ or ϵ .

We now apply this information to the formula (20.19), which becomes either

$$e = 1 + f \text{ if } a = 0, \text{ or } e = (n - 1) + f \text{ if } a = \epsilon.$$

It therefore suffices to prove that, in the second case, we have $n=2$. For this purpose, we prove that if $(\xi_i, \tau) \neq 0$ for some projective indecomposable

character τ , then $(\sum_{i=1}^n \xi_i, \tau) \neq 0$. We have, for $j \neq i$,

$$\begin{aligned} (\xi_i - \xi_j, \tau) &= \epsilon((\psi_i - \psi_j)^G, \tau) \\ &= \epsilon((\xi_i - \xi_j)^G, \tau) = \epsilon(\xi_i - \xi_j, \tau_D), \end{aligned}$$

where ξ_i and ξ_j are linear characters of D such that $\psi_i = \xi_i^H$ and $\psi_j = \xi_j^H$. Then, by (18.26), we clearly have $(\xi_i - \xi_j, \tau) = 0$, since τ vanishes on D^* , and $\xi_i(1) = \xi_j(1)$. Therefore $(\sum_{i=1}^n \xi_i, \tau) \neq 0$. We now assume $a = \epsilon$, and obtain, for a linear character ξ of D such that $\xi^G = \psi_1$,

$$\left(l_D - \xi, \sum_{i=1}^n \xi_i \right)_D = \left(\Gamma_1, \sum_{i=1}^n \xi_i \right) = \epsilon(n-1),$$

by Frobenius Reciprocity. By (20.16), it follows that

$$|\epsilon(n-1)| \leq h \left(\sum_{i=1}^n \xi_i \right) \leq 1,$$

and therefore $n=2$, completing the proof.

(20.22) Corollary. *The multiplicity a in (20.18) is zero unless $n=2$. In that case $a=0$ or ϵ , and in the latter case, we may interchange ξ_1 and ξ_2 , to obtain the formulas (20.17) and (20.18), with ϵ replaced by $-\epsilon$, and $a=0$.*

Proof. By the proof of Lemma 20.21, it suffices to consider the case $n=2$. In that case, the formula (20.17) holds (initially) for $\epsilon=1$, and (20.17) and (20.18) become:

$$\begin{aligned} (\psi_1 - \psi_2)^G &= \xi_1 - \xi_2, \\ \Gamma_1 &= l_G + \xi_2 + \sum c_j \theta_j, \quad \Gamma_2 = l_G + \xi_2 + \sum c_j \theta_j. \end{aligned}$$

We then put $\xi'_1 = \xi_2$, $\xi'_2 = \xi_1$, and obtain, for $\epsilon = -1$,

$$\begin{aligned} (\psi_1 - \psi_2)^G &= \epsilon(\xi'_1 - \xi'_2), \\ \Gamma_1 &= l_G - \epsilon \xi'_1 + \sum c_j \theta_j, \quad \Gamma_2 = l_G - \epsilon \xi'_2 + \sum c_j \theta_j, \end{aligned}$$

as required.

Proof of Theorem 20.20. (i) By (20.21), the multiplicities $\{c_j\}$ are all ± 1 , so the degrees $\theta_j(1) \equiv \pm 1 \pmod{p^d}$, because of (14.19iv). By (20.21) and (20.22),

we may assume that $a=0$, and that

$$\Gamma_1 = 1_G - \epsilon \zeta_1 + \sum_{j=1}^{e-1} c_j \theta_j.$$

Then $\Gamma_1 = (1_D^H - \varphi_1)^G$ vanishes at the identity, and we obtain

$$0 = 1 - \epsilon \zeta_1(1) + \sum_{j=1}^{e-1} c_j \theta_j(1).$$

By (14.19iv) again, $\theta_j(1) \equiv c_j \pmod{p}$ and taking congruences mod p , we have, since $|c_j| = 1$ for $1 \leq j \leq e-1$,

$$0 \equiv 1 - \epsilon \zeta_1(1) + e - 1 \pmod{p},$$

so $\zeta_1(1) \equiv \epsilon e \pmod{p}$. Since $e = |H:D|$ is prime to p , and all the exceptional characters have the same degree by (14.19i), it follows that the degrees $\{\zeta_i(1)\}$ are all prime to p .

Now let $\chi \in \text{Irr } G$ be distinct from $\{1_G, \zeta_1, \dots, \zeta_n, \theta_1, \dots, \theta_{e-1}\}$. Then by (20.18) we have $(\Gamma_i, \chi) = 0$, and hence $(1_D^H - \psi_i, \chi_H) = 0$, $1 \leq i \leq n$. It follows that $(1_D - \xi, \chi_D) = 0$ for all non-trivial characters ξ of D , by the definition of the characters $\{\psi_i\}$. Therefore χ_D is a multiple of the regular character of D , and we have $\chi(1) \equiv 0 \pmod{|D|}$, completing the proof of (i).

(For another proof of the last step, see (14.19iv).)

(ii) By (20.22) we may assume that $a=0$ in formula (20.18). Now $\{\lambda_1, \dots, \lambda_{n-1}, 1_D^H - \psi_1\}$ form a \mathbb{Z} -basis for the elements of $\text{ch } KH$ vanishing off D^* , and we have

$$(1_D^H - \psi_1)^G = 1_G - \epsilon \zeta_1 + \sum c_j \theta_j.$$

We therefore have, for the matrices (a_{ij}) and (b_{ij}) in Theorem 14.11, $b_{ij} = \epsilon a_{ij}$, $1 \leq i \leq n$, where the indices j correspond to the characters $\{\zeta_1, \dots, \zeta_n\}$ and $\{\psi_1, \dots, \psi_n\}$, respectively. By Theorem 14.11, we then obtain $\zeta_i|_{D^*} = \epsilon \psi_i|_{D^*}$, $1 \leq i \leq n$, as required in part (ii).

We have $\theta_j(x) = \pm 1$ for all $x \in D^*$ and $1 \leq j \leq e-1$, by (14.19iv), and the fact that all the multiplicities $\{c_j\}$ are ± 1 . Finally, the characters $\{\chi_j : 1 \leq j \leq h\}$ all satisfy the condition $\chi_j(1) \equiv 0 \pmod{|G|_p}$ by part (i), and hence vanish on D^* by (15.19) (see also (18.28)).

(iii) The first statement follows since

$$\zeta_i - \zeta_j = \epsilon (\psi_i - \psi_j)^G,$$

and hence vanishes off D^* , for all i and j . For the second statement, we know that Γ_1 also vanishes off D^* , so that for all $x \in G_p$, we have

$$0 = \Gamma_1(x) = 1 - \epsilon \zeta_1(x) + \sum_{j=1}^{e-1} c_j \theta_j(x),$$

(since $a=0$). This completes the proof of (iii), since $|c_j|=1$ for all j .

(iv) has been proved in (20.21).

(v) We have already shown in the proof of (20.21) that if χ is any one of the characters $\{1, \sum_i^n \zeta_i, \theta_1, \dots, \theta_{e-1}\}$, then χ appears with positive multiplicity in some indecomposable projective character τ . We assert that for any such character χ , we have $h(\chi) \geq 1$. This follows at once from the formulas,

$$(1_D - \xi, 1_D) = (\Gamma_1, 1_G) = 1,$$

$$(1_D - \xi, (\sum_i^n \zeta_i)_D) = (\Gamma_1, \sum_i^n \zeta_i) = -\epsilon,$$

$$(1_D - \xi, (\theta_j)_D) = c_j = \pm 1,$$

where $\xi \in \text{Irr } D$ and $\xi^H = \psi_1$, and $\Gamma_1 = 1_G - \epsilon \zeta_1 + \sum c_j \theta_j$, since we have $a=0$. By (20.16), we then have $h(2\chi) \geq 2$ for any character χ as above, and hence $(2\chi, \tau_i) = 0$ for all indecomposable projective characters τ_i . By (18.26), we have $\tau_i = \sum_{j=1}^e d_{ji} \zeta^j$. Thus the decomposition numbers corresponding to 1_G or $\{\theta_j : 1 \leq j \leq e-1\}$ are 0 or 1. On the other hand, by the proof of Lemma 20.21, the multiplicity of any exceptional character $\{\zeta_j : 1 \leq j \leq n\}$ in one of the $\{\tau_i\}$ is the same as the multiplicity of $\sum_i^n \zeta_i$, and hence is less than 2. Finally, for the non-exceptional characters $\{\chi_j : 1 \leq j \leq h\}$ of defect zero (see (18.18) and part (i)), the corresponding decomposition numbers are equal to one or zero, by (18.28), completing the proof of the theorem.

(20.23) Interpretation of Theorem 20.20. The information in Theorem 20.20 can be summarized conveniently in terms of the character tables of H and G . (For a numerical illustration, see the character table of A_5 , for $p=5$, discussed in §13D.)

In the character table of H , the entries in the matrix \mathbf{A} can be found, in any particular case, from the definition of the $\{\psi_i\}$ as induced characters. The matrix \mathbf{B} has all entries equal to 1. Note also that there are exactly $e-1$ non-trivial linear characters of H , since D is the derived group of H and $|H:D|=e$.

		Character Table of H	
		1	Classes of p -elements
		1	Classes of p' -elements
	1_H	1	
Nonlinear characters	ψ_1	e	
	\vdots	\vdots	
	ψ_n	e	\mathbf{A}
			*
Nontrivial linear characters	μ_1	1	
	\vdots	\vdots	
	μ_{e-1}	1	\mathbf{B}
			*

		Character Table of G	
		1	Classes of p -elements
		1	Classes of p' -elements
	1_G	1	
	ξ_1	$\pm e(p)$	
	\vdots	\vdots	
	ξ_n	$\pm e(p)$	$\epsilon \mathbf{A}$
			↑ constant values on each class ↓
	θ_1	$\pm 1(p)$	
	\vdots	\vdots	
	θ_{e-1}	$\pm 1(p)$	\mathbf{B}'
	χ_1	$\equiv 0(D)$	*
	\vdots	\vdots	
	χ_h	$\equiv 0(D)$	$\mathbf{0}$
			*

In the table for G , the degrees of the characters are described by congruences mod p , or mod $|D|$, where $|D|=p^d$. We note first that the characters $\{1_G, \xi_1, \dots, \xi_n, \theta_1, \dots, \theta_{e-1}\}$ constitute all characters of G whose degrees are prime to p . Later, in Chapter 9, we shall see that these characters form the principal block of G .

The values of these characters on the p -elements are almost lifted from the part of the character table of H corresponding to the p -elements. Thus, the values of the $\{\xi_i\}$ differ by the sign ϵ from the values of the $\{\psi_i\}$ on the p -classes. The number of non-exceptional characters $\{\theta_i\}$ is equal to the number of nontrivial linear characters of H , and their values on the p -elements are given by the matrix \mathbf{B}' whose i -th row is the constant vector (c_i, \dots, c_i) ,

where $c_i = (\theta_i, \Gamma_1)$, $1 \leq i \leq e-1$, and Γ_1 is given by (20.18). Since $|c_i| = 1$ for all i , the matrix \mathbf{B}' is obtained from the corresponding matrix \mathbf{B} in the table for H , by changing (at most) the signs of the rows. Finally, the other non-exceptional characters $\{\chi_i\}$ vanish on the p -classes.

§21. THE INDUCTION THEOREM FOR ARBITRARY FIELDS

Let (K, R, k) be a p -modular system. The properties of the Cartan-Brauer triangle

$$\begin{array}{ccc} G_0(KG) & \xrightarrow{d} & G_0(kG) \\ & \swarrow e & \searrow c \\ & K_0(kG) & \end{array}$$

were derived in §18 under the assumption that K is sufficiently large relative to G . Several of these properties, for example, the facts that the decomposition map d is surjective, and that the determinant of c is a p -power, used the Brauer Induction Theorem and Brauer's criterion for virtual characters. In this section we prove corresponding facts about the triangle for an arbitrary p -modular system, without the hypothesis that K be large.

In order to accomplish this objective, we need an extension of the Brauer Induction Theorem, due to Berman [56a] and Witt [52] (see CR §42 and Serre ([77], 12.6]). This result, of importance in many other connections as well, is first proved for an arbitrary field of characteristic zero, and then extended to fields of characteristic p by using properties of the decomposition map (§16).

Our presentation in §21 follows Serre ([77], Chapters 12 and 17) and CR §42.

§21A. The Witt-Berman Induction Theorem

We recall from §17A that a field K of characteristic zero is said to be *sufficiently large* relative to G provided that K contains the m -th roots of 1, where m is the exponent of G . The Brauer Induction Theorem 15.8 asserts that

$$\operatorname{ch} KG = \sum_{H \in \mathcal{E}} (\operatorname{ch} KH)^G,$$

where \mathcal{E} is the set of elementary subgroups of G , and K is sufficiently large. For arbitrary fields K of characteristic zero, the right hand side is, in general, properly contained in $\operatorname{ch} KG$ (see Exercise 21.6). Equality can be restored by enlarging the family of subgroups \mathcal{E} . In §21B, we shall obtain a similar result for fields of characteristic $p > 0$.

Until further notice, let K denote an arbitrary field of characteristic zero, G a finite group, m the exponent of G , and set $F=K(\omega)$, where ω is a primitive m -th root of 1. By Corollary 15.18, F is a splitting field for G and all subgroups of G . Moreover, F is a Galois extension of K , whose Galois group we denote by \mathfrak{G} . Each automorphism $\sigma \in \mathfrak{G}$ is uniquely determined by its action on ω , and is given by $\sigma(\omega) = \omega^t$, where t is an integer uniquely determined modulo m . Thus t corresponds to a unit in $\mathbb{Z}/m\mathbb{Z}$, and there is a monomorphism $\mathfrak{G} \rightarrow (\mathbb{Z}/m\mathbb{Z})^\times$, given by $\sigma \mapsto t$. We write σ_t for the element of \mathfrak{G} corresponding to $t+m\mathbb{Z}$ in $(\mathbb{Z}/m\mathbb{Z})^\times$, and denote the image of \mathfrak{G} in $(\mathbb{Z}/m\mathbb{Z})^\times$ by $I_m(K)$.

For $t \in I_m(K)$ and $x \in G$, the element $x^t \in G$ is well defined since $x^m = 1$. Hence $I_m(K)$ acts on G , with $t \in I_m(K)$ sending x to x^t .

We also have an action of \mathfrak{G} on $\text{cf}_F G$, the vector space of F -valued class functions on G , given by

$$(\sigma f)(x) = \sigma(f(x)), \quad f \in \text{cf}_F G, \quad \sigma \in \mathfrak{G}, \quad x \in G.$$

If ξ is an F -character of G , afforded by an FG -module Z , then for each $t \in I_m(K)$ we have

$$(21.1) \quad \sigma_t(\xi)(x) = \xi(x^t), \quad x \in G.$$

Indeed, as we have shown before, $\xi(x)$ is the sum of the eigenvalues of x acting on Z , while $\xi(x^t)$ is the sum of the t -th powers of these eigenvalues, and is therefore the same as $\sigma_t(\xi)(x)$.

We recall that for x and y in G , we write $x =_G y$ if x and y are conjugate in G . We now define x and y to be K -conjugate provided that

$$x =_G y^t \text{ for some } t \in I_m(K).$$

The relation of K -conjugacy is an equivalence relation on G , and the equivalence classes are called K -conjugacy classes.

A subgroup $H \leq G$ is called a K -elementary subgroup for a prime p provided that H is a semidirect product

$$H = \langle x \rangle \rtimes D$$

of a cyclic p' -group $\langle x \rangle$ and a p -group D acting on $\langle x \rangle$, such that for each $u \in D$, $uxu^{-1} = x^t$ for some $t \in I_m(K)$. Evidently, two elements of $\langle x \rangle$ are conjugate in H if and only if they are K -conjugate in H .

If K contains ω , then $I_m(K) = 1$, and K -conjugacy becomes ordinary conjugacy in G . In this case, the K -elementary subgroups are the elementary subgroups considered in §15 (see (15.7)). At the other extreme, if $K = \mathbb{Q}$, the K -elementary groups are the hyperelementary groups, used in the Goldschmidt-Isaacs proof of the Brauer Induction Theorem in §15.

We now introduce some additional notation which will be used throughout the rest of this subsection:

$\mathcal{E}_K = \mathcal{E}_K(G)$: the set of all K -elementary subgroups of G .

$R = \mathbb{Z}[\omega]$: a ring of algebraic integers in F , where $F = K(\omega)$.

$\text{ch } KG, \text{ ch } FG$: the rings of virtual K -characters and F -characters of G , respectively.

$$\text{Irr}_F G = \{\zeta^1 = 1_G, \zeta^2, \dots, \zeta^s\}.$$

$$v(\mathcal{E}_K, G) = \sum_{H \in \mathcal{E}_K} (\text{ch } KH)^G.$$

$$\text{ch}_R KG = R \otimes_{\mathbb{Z}} \text{ch } KG, \quad \text{ch}_K KG = K \otimes_{\mathbb{Z}} \text{ch } KG.$$

$$\text{ch}_F KG = F \otimes_{\mathbb{Z}} \text{ch } KG, \quad \text{ch}_F FG = F \otimes_{\mathbb{Z}} \text{ch } FG.$$

$$v_R(\mathcal{E}_K, G) = R \otimes_{\mathbb{Z}} v(\mathcal{E}_K, G).$$

Since $\text{ch } KG$ is a free \mathbb{Z} -module with finite basis, the ring $\text{ch}_R KG$ consists simply of all R -linear combinations of the elements of $\text{ch } KG$, and can be viewed as a subring of $\text{cf}_F G$. Similar remarks apply to the rings $\text{ch}_K KG, \text{ch}_R FG$, etc.. The Galois group \mathfrak{G} acts on $\text{cf}_F G$ as shown above, and hence acts also on each of these subrings.

(21.2) Proposition. *A class function $\psi \in \text{cf}_F G$ belongs to $\text{ch}_K FG$ if and only if*

$$\sigma_t(\psi(x)) = \psi(x') \text{ for all } t \in I_m(K) \text{ and all } x \in G.$$

Proof. The formula holds for F -characters of G , by (21.1), and hence for class functions $\psi \in \text{ch}_K FG$, since σ_t fixes elements of K , for all $t \in I_m(K)$.

Conversely, suppose the condition holds for some $\psi \in \text{cf}_F G$, and write

$$\psi = \sum a_i \zeta^i, \quad a_i \in F,$$

where $a_i = (\psi, \zeta^i)$. We have to show that each $a_i \in K$, that is, $\sigma_t(a_i) = a_i$ for all $t \in I_m(K)$. By definition of the inner product, we have

$$(\psi, \zeta^i) = |G|^{-1} \sum_{x \in G} \psi(x) \zeta^i(x^{-1}).$$

For each $t \in I_m(K)$, it follows from the assumption on ψ that

$$\begin{aligned}\sigma_t(\psi, \xi^t) &= |G|^{-1} \sum_{x \in G} \sigma_t(\psi(x)) \sigma_t(\xi^t(x^{-1})) \\ &= |G|^{-1} \sum_{x \in G} \psi(x^t) \xi^t(x^{-t}) = (\psi, \xi^t),\end{aligned}$$

as required.

(21.3) Corollary. *A class function $\psi \in \text{cf}_K G$ belongs to $\text{ch}_K KG$ if and only if ψ is constant on the K -conjugacy classes of G .*

Proof. Each $\psi \in \text{ch}_K KG$ takes values in K , so is fixed by σ_t for all $t \in I_m(K)$. Therefore

$$(21.4) \quad \psi(x) = \psi(x') \text{ for all } x \in G \text{ and all } t \in I_m(K)$$

by (21.2), since $\text{ch}_K KG \subseteq \text{ch}_K FG$. Thus ψ is constant on the K -conjugacy classes.

Conversely, let $\psi \in \text{cf}_K G$, and write

$$\psi = \sum_{i=1}^s a_i \xi^i, \quad a_i \in K.$$

If ψ is constant on the K -conjugacy classes, then (21.4) holds; hence $\sigma_t \psi = \psi$ for all $t \in I_m(K)$. Since the coefficients a_i lie in K , and are thus fixed under the action of \mathfrak{G} , it follows that the coefficients are constant on the \mathfrak{G} -orbits in $\text{Irr}_F G$. The sum of characters in such an orbit is a rational multiple of a K -character of G , by Exercise 9.14. Hence $\psi \in \text{ch}_K KG$, completing the proof.

From these results we obtain easily:

(21.5) Theorem. *The characters $\{\theta^1, \dots, \theta^n\}$ of a basic set of simple KG -modules form a basis of the K -space consisting of all functions in $\text{cf}_K G$ which are constant on the K -conjugacy classes. In particular, the number of distinct simple KG -modules is equal to the number of K -conjugacy classes.*

Proof. Each character θ^i is a multiple of a sum of characters $\{\xi^j\} \subseteq \text{Irr}_F G$ corresponding to a \mathfrak{G} -orbit in $\text{Irr}_F G$, by Exercise 9.14. Therefore the $\{\theta^i\}$ are linearly independent, because of the linear independence of the $\{\xi^j\}$, and the fact that the orbits corresponding to θ_i and θ_j are disjoint if $i \neq j$. By Corollary 21.3, every class function in $\text{cf}_K G$ which is constant on the K -conjugacy classes is a K -linear combination of the $\{\theta^i\}$, and the result follows. The Theorem is due to Witt [52] and Berman [56b].

The main result of the section is as follows:

(21.6) Witt-Berman Theorem. *Let K be an arbitrary field of characteristic zero. Then*

$$\mathrm{ch} \, KG = v(\mathcal{E}_K, G),$$

that is, every K -character ξ of G can be expressed as a \mathbb{Z} -linear combination of induced characters of the form μ^G , where μ is a K -character of a K -elementary subgroup of G .

We have remarked that in case K is sufficiently large, the K -elementary subgroups coincide with the elementary subgroups defined in §15. Thus the Witt-Berman Theorem, in this case, includes the Brauer Induction Theorem 15.8. The proof of the Witt-Berman Theorem, when specialized to the case of a sufficiently large field K , offers a quite different approach to the proof of the Brauer Induction Theorem from that given in §15.

Now let K be arbitrary. We note first that $v(\mathcal{E}_K, G)$ is an ideal in $\mathrm{ch}(KG)$ by (15.5); hence the theorem will be proved once we show that the trivial character ξ^1 belongs to $v(\mathcal{E}_K, G)$. As the first lemma shows, it is sufficient to prove the weaker result that $\xi^1 \in v_R(\mathcal{E}_K, G)$, where $R = \mathbb{Z}[\omega]$.

(21.7) Lemma. *If $\xi^1 \in v_R(\mathcal{E}_K, G)$, then $\xi^1 \in v(\mathcal{E}_K, G)$.*

Proof. We first observe that R/\mathbb{Z} is a torsionfree \mathbb{Z} -module, since if $q\alpha \in \mathbb{Z}$ for $\alpha \in R$, $q \in \mathbb{Z}$, then $\alpha \in \mathbb{Q} \cap R = \mathbb{Z}$. It follows that \mathbb{Z} is a direct summand of R , so we may write $R = \bigoplus_1^d \mathbb{Z} r_i$, with $r_1 = 1$. Now let $N = v(\mathcal{E}_K, G)$, $M = \mathrm{ch} \, KG$. Then $N \subseteq M$, and we have $\xi^1 \in M$, and by hypothesis $1 \otimes \xi^1 \in R \otimes_{\mathbb{Z}} N$. We must prove that $1 \otimes \xi^1 \in 1 \otimes N$. Identify N with $1 \otimes N$, M with $1 \otimes M$. Then $R \otimes N = \bigoplus_1^d r_i \otimes N$, $R \otimes M = \bigoplus_1^d r_i \otimes M$, and

$$\xi^1 = 1 \otimes \xi^1 = \sum_{i=1}^d r_i \otimes n_i, \quad n_i \in N,$$

so

$$1 \otimes \xi^1 - 1 \otimes n_1 = \sum_{i=2}^d r_i \otimes n_i \in \bigoplus_{i=2}^d r_i \otimes M.$$

The left side is in $1 \otimes M$, so we obtain $\xi^1 = n_1 \in N$ as required.

We next prove several interesting lemmas about K -characters of K -elementary subgroups of G . As in §15C, we shall write $|G|_p$ and $|G|_{p'}$ for the p -part and p' -part, respectively, of the order of a group G .

(21.8) Lemma. *Let $H = \langle x \rangle D$ be a K -elementary subgroup of G , with $\langle x \rangle$ a p' -group and D a p -group, for some prime p . Then the restriction map $\text{res}_{\langle x \rangle}^H : \text{ch } KH \rightarrow \text{ch } K\langle x \rangle$ is surjective. In fact, every K -character of $\langle x \rangle$ is the restriction to $\langle x \rangle$ of some K -character of H .*

Proof. If x has order c , then

$$K\langle x \rangle \cong K[X]/(X^c - 1) \cong \prod_{i=1}^q K[X]/(f_i(X)) \cong \prod_{i=1}^q K_i,$$

where X is an indeterminate, and the $\{K_i\}$ are subfields of F containing K which correspond to the irreducible factors $\{f_i(X)\}$ of $X^c - 1$. The fields $\{K_i\}$ are a basic set of simple $K\langle x \rangle$ -modules, with x acting on K_i as multiplication by a zero θ_i of $f_i(X)$ in K_i .

We shall prove that for each fixed i , the action of $\langle x \rangle$ on K_i can be extended to an action of H on K_i . For $y \in D$, we may write

$$yxy^{-1} = x^t, \text{ where } t \in I_m(K).$$

The map $y \mapsto t$, $y \in D$, is a homomorphism from D into $I_m(K)$, and $I_m(K)$ is, in turn, isomorphic to the Galois group \mathfrak{G} of F/K , consisting of the automorphisms $\{\sigma_t : t \in I_m(K)\}$. Moreover, each $\sigma_t \in \mathfrak{G}$ carries K_i onto itself, since K_i is a Galois extension of K . Therefore D acts on K_i , with $y \in D$ operating as the corresponding automorphism σ_t . We now have to prove that the separate actions of $\langle x \rangle$ and D on K_i define a K -representation of H .

For each $t \in I_m(K)$, the automorphism $\sigma_t|_{K_i}$ carries c -th roots of 1 onto their t -th powers, since c divides m . Hence $\sigma_t(\theta_i) = \theta_i^t$. In order to prove that the separate actions of D and $\langle x \rangle$ on K_i define a representation of H , it is sufficient to check that

$$\sigma_t \theta_i \sigma_t^{-1} = \theta_i^t$$

as left operators on K_i . For this, it suffices to calculate their action on the powers $\{\theta_i\}$, since $K_i = K(\theta_i)$. But

$$(\sigma_t \theta_i \sigma_t^{-1}) \theta_i^t = \sigma_t(\theta_i) \sigma_t(\theta_i^{-1} \theta_i^t) = \theta_i^t \theta_i^t,$$

as desired, and the proof is complete.

(21.9) Lemma. *Let p be a prime, and let $x \in G$ be a p' -element of order c . Set*

$$N_{(K)}(x) = \{y \in G : yxy^{-1} = x^t \text{ for some } t \in I_m(K)\}.$$

Let D be a Sylow p -subgroup of $N_{(K)}(x)$. Then $H = \langle x \rangle D$ is a K -elementary

subgroup of G , and there exists an element $\xi \in \text{ch}_R KH$ such that

$$(*) \quad \xi(x^j) = \begin{cases} c & \text{if } j \in I_m(K), \\ 0 & \text{otherwise.} \end{cases}$$

Proof. It is immediate from the definition that N is a group, and that H is a K -elementary subgroup. Let $\{\chi_1, \dots, \chi_c\}$ be a basic set of irreducible F -characters of $\langle x \rangle$; they are all linear characters since $\omega \in F$. Define $\xi_1 : \langle x \rangle \rightarrow \mathbb{Z}$ by the formula $(*)$ above; then $\xi_1 \in \text{cf}_F \langle x \rangle$. Hence

$$(21.10) \quad \xi_1 = \sum_{i=1}^c a_i \chi_i, \quad a_i \in F,$$

where the coefficients a_i are given by the orthogonality relations:

$$a_i = c^{-1} \sum_{j=1}^c \xi_1(x^j) \chi_i(x^{-j}) = \sum_{j \in I_m(K)} \chi_i(x^{-j}), \quad 1 \leq i \leq c.$$

Thus each $a_i \in R$, and since a_i is a sum of \mathfrak{G} -conjugate elements of F , we have also $a_i \in K$ for all i . Since a_i is fixed by all automorphisms in \mathfrak{G} , it follows from the above formula that the coefficients a_i in (21.10) are constant on \mathfrak{G} -orbits of characters $\{\chi_i\}$. It is easily shown, using the first part of the proof of Lemma 21.8 (or Exercise 9.14), that the sums of the F -characters $\{\chi_i\}$ in different \mathfrak{G} -orbits coincide with the irreducible K -characters of $\langle x \rangle$. Thus we have shown that ξ_1 is an R -linear combination of K -characters of $\langle x \rangle$. By Lemma 21.8, each K -character on $\langle x \rangle$ can be lifted to a K -character of H , so we can define an R -linear combination ξ of K -characters of H whose restriction to $\langle x \rangle$ agrees with ξ_1 , completing the proof.

(21.11) Lemma. *Keep the notation of (21.9), and let $\psi = \xi^G$, where $\xi \in \text{ch}_R KH$ is the class function constructed in (21.9). Then $\psi \in v_R(\mathfrak{E}_K, G)$, and satisfies the conditions:*

$$\psi(x) = |N_{(K)}(x)|_{p'},$$

and

$$\psi(s) = 0$$

for each $s \in G_{p'}$ such that s is not K -conjugate to x .

Proof. It is clear from the definition of ψ that $\psi \in v_R(\mathfrak{E}_K, G)$. Let $s \in G_{p'}$, and suppose $\psi(s) \neq 0$. By (10.3), $ysy^{-1} \in H$ and $\xi(ysy^{-1}) \neq 0$, for some $y \in G$. Then $ysy^{-1} \in G_{p'} \cap H$, and so $ysy^{-1} \in \langle x \rangle$; since $\xi(ysy^{-1}) \neq 0$, we have $ysy^{-1} = x^t$ for some $t \in I_m(K)$. Thus if $s \in G_{p'}$ is such that $\psi(s) \neq 0$, then s is K -conjugate to x .

Now let $S = \{x' : t \in I_m(K)\}$. Then by (10.3),

$$\psi(x) = |H|^{-1} \sum_{\substack{y \in G \\ yxy^{-1} \in S}} c = |H|^{-1} |N_{(K)}(x)|_p c = |N_{(K)}(x)|_p,$$

since $c = |\langle x \rangle|$ and $|H| = c |N_{(K)}(x)|_p$. This completes the proof.

We require one more preliminary result.

(21.12) Lemma. *Let p be a prime, and let P be a prime ideal in R containing p . Then for all $\varphi \in \text{ch}_R KG$, we have $\varphi(x) \equiv \varphi(y) \pmod{P}$, for any two elements $x, y \in G$ whose p' -parts are K -conjugate to each other.*

Proof. By Corollary 21.3, φ is constant on K -conjugacy classes. Hence it suffices to show that $\varphi(x) \equiv \varphi(y) \pmod{P}$ if x is the p' -part of y . Both x, y lie in $\langle y \rangle$, and by restriction to $\langle y \rangle$ and extension of the ground ring R , it is sufficient to prove the result for an irreducible, hence linear, F -character μ of $\langle y \rangle$. Let $y = xu$, where u is the p -part of y . Then $\mu(y) = \mu(x)\mu(u)$. Moreover, $\mu(u)^{p^d} = 1$ for some integer d , so $(\mu(u) - 1)^{p^d} \equiv 0 \pmod{P}$. Since P is a prime ideal, we obtain $\mu(u) \equiv 1 \pmod{P}$ and $\mu(y) \equiv \mu(x) \pmod{P}$, as required.

Proof of the Witt-Berman Theorem 21.6. By Lemma 21.7, it is sufficient to prove that $\xi^1 \in v_R(\mathcal{E}_K, G)$. Since the integers $\{|G|_p : p \text{ prime}, p \mid |G|\}$ are relatively prime, it suffices to prove, for a fixed prime p dividing $|G|$, that $|G|_p \xi^1 \in v_R(\mathcal{E}_K, G)$. Let $\{x_j\}_{j \in J}$ be a set of representatives of the p -regular K -conjugacy classes of G , and let $\{P_i\}_{i \in I}$ be the set of prime ideals in R containing the rational prime p . Now $R = \mathbb{Z}[\omega]$ is a Dedekind domain (see (CR (21.13))). From this result, or from the elementary fact that R/pR is an artinian ring, we know that the prime ideals $\{P_i\}$ are maximal ideals, finite in number. Further, since $\cap_{i \in I} P_i$ maps onto $\text{rad}(R/pR)$, we obtain*

$$\left(\prod_{i \in I} P_i \right)^h \subseteq \left(\bigcap_{i \in I} P_i \right)^h \subseteq pR$$

for some positive integer h , by the results of §5. We shall keep the above notation throughout the remaining steps of the proof.

Step 1. We shall show that there exists an $\eta \in v_R(\mathcal{E}_K, G)$ such that

$$\eta(x) \equiv 1 \pmod{P_i} \quad x \in G, i \in I.$$

For each p -regular class representative x_j , $j \in J$, let $\psi_j \in v_R(\mathcal{E}_K, G)$ be the

*From Theorem 4.40, it follows readily that, in fact, $(\prod_{i \in I} P_i)^h = pR$ for some h . However, this stronger result will not be needed in the present proof.

function defined in Lemma 21.11; it satisfies the conditions

$$\psi_j(x_j) = |N_{(K)}(x_j)|_{p'}, \quad \psi_j(x_{j'}) = 0, \quad j' \neq j.$$

For each j , let a_j be a rational integer such that $a_j |N_{(K)}(x_j)|_{p'} \equiv 1 \pmod{p}$, and define

$$\eta = \sum_{j \in J} a_j \psi_j.$$

Now let $x \in G$, and $i \in I$. By Lemma 21.12, we have $\eta(x) \equiv \eta(x_{j_0}) \pmod{P_i}$, for some $j_0 \in J$; hence

$$\eta(x) \equiv \eta(x_{j_0}) \equiv \sum_j a_j \psi_j(x_{j_0}) \equiv a_{j_0} \psi_{j_0}(x_{j_0}) \equiv 1 \pmod{P_i},$$

as required.

Step 2. There exists a positive integer q such that the function η defined in Step 1 satisfies the condition:

$$\eta(x)^q \equiv 1 \pmod{|G|_p R} \text{ for all } x \in G.$$

The proof of this assertion is an easy consequence of Step 1 and the remarks preceding Step 1, and is left to the reader as an exercise.

Now consider the function

$$\varphi = |G|_{p'} (\xi^1 - \eta^q) \in \text{ch}_R KG.$$

By Step 2,

$$\varphi(x) = |G|_{p'} (1 - \eta(x)^q) \equiv 0 \pmod{|G|_p R}$$

for all $x \in G$. If we can prove that such a function φ belongs to $v_R(\mathcal{E}_K, G)$, then we will have the desired conclusion:

$$|G|_p \xi^1 = \varphi + |G|_{p'} \eta^q \in v_R(\mathcal{E}_K, G),$$

since $\eta^q \in v_R(\mathcal{E}_K, G)$ by Step 1. The last step is handled as follows:

Step 3. The proof of (21.9) shows that for each $x \in G$ (not necessarily a p' -element), we can find an element $\xi \in \text{ch}_R K\langle x \rangle$ such that

$$\xi(x^j) = \begin{cases} \text{order of } x, & \text{if } j \in I_m(K), \\ 0, & \text{otherwise.} \end{cases}$$

The proof of (21.11) shows that

$$\xi^G(y) = \begin{cases} |N_{(K)}(x)| & \text{if } y \text{ is } K\text{-conjugate to } x, \\ 0 & \text{otherwise.} \end{cases}$$

Since $\langle x \rangle$ is obviously a K -elementary subgroup of G , it follows that $\xi^G \in v_R(\mathfrak{S}_K, G)$.

Now let $\{x_1, \dots, x_t\}$ represent the K -conjugacy classes of G , and for each x_i , construct an element ξ_i as above. Then for the function φ defined in Step 2, we have

$$\varphi = \sum_{i=1}^t \frac{\varphi(x_i)}{|N_{(K)}(x_i)|} \xi_i^G.$$

This follows at once from the fact that both sides are constant on K -conjugacy classes of G , and agree at each x_i , $1 \leq i \leq t$. Finally, each coefficient $\varphi(x_i)/|N_{(K)}(x_i)|$ lies in R , so $\varphi \in v_R(\mathfrak{S}_K, G)$. This completes the proof of the Witt-Berman Theorem for fields of characteristic zero.

§21B. The Induction Theorem over Fields of Characteristic $p > 0$

Let (K, R, k) be a p -modular system, with K a field of characteristic zero. We shall first reformulate the Witt-Berman Theorem so that it makes sense for kG -modules. By Proposition 16.10, there is an isomorphism of rings: $\text{ch } KG \cong G_0(KG)$. Moreover, for each subgroup H of G , the induction map $\text{ind}_H^G : \text{ch } KH \rightarrow \text{ch } KG$ is part of a commutative diagram

$$\begin{array}{ccc} \text{ch } KH & \xrightarrow{\text{ind}_H^G} & \text{ch } KG \\ \downarrow & & \downarrow \\ G_0(KH) & \xrightarrow{\text{ind}_H^G} & G_0(KG), \end{array}$$

where the vertical maps are defined as in Proposition 16.10. The map $\text{ind}_H^G : G_0(KH) \rightarrow G_0(KG)$, also called *induction*, is defined by the formula $\text{ind}_H^G [L] = [L^G]$ for each isomorphism class $[L]$ of KH -modules. The Witt-Berman Theorem 21.6 thus becomes, in the language of Grothendieck groups,

$$(21.13) \quad G_0(KG) = \sum_{H \in \mathfrak{S}_K} \text{ind}_H^G G_0(KH),$$

where \mathfrak{S}_K is the family of K -elementary subgroups of G . We shall prove a result analogous to (21.13), with K replaced by k .

When K is sufficiently large, \mathcal{E}_K is the family of elementary subgroups of G , and by Exercise 18.13 we have

$$\mathrm{Bch} kG = \sum_{H \in \mathcal{E}} (\mathrm{Bch} kH)^G,$$

where Bch denotes the ring of virtual Brauer characters. Since $\mathrm{Bch} kG \cong G_0(kG)$ by (17.14), the above formula becomes

$$G_0(kG) = \sum_{H \in \mathcal{E}} \mathrm{ind}_H^G G_0(kH),$$

which is the desired analogue of (21.13) when K is sufficiently large.

With these remarks as motivation, we consider an arbitrary p -modular system (K, R, k) , with $\mathrm{char} K=0$. For each subgroup $H \leq G$, the restriction map $M \rightarrow M_H$ carries any ses of kG -modules to a ses of kH -modules, and hence defines a \mathbb{Z} -homomorphism

$$\mathrm{res}_H^G: G_0(kG) \rightarrow G_0(kH)$$

such that $\mathrm{res}_H^G[M] = [M_H]$ for a kG -module M . It is easily checked that the restriction map commutes with the decomposition map $d: G_0(KG) \rightarrow G_0(kG)$, defined in (16.17), in the sense that there exists a commutative diagram

$$\begin{array}{ccc} G_0(KG) & \xrightarrow{\mathrm{res}_H^G} & G_0(KH) \\ d \downarrow & & \downarrow d \\ G_0(kG) & \xrightarrow{\mathrm{res}_H^G} & G_0(kH). \end{array}$$

Similar remarks apply to induction. If L is a kH -module, then $L^G = kG \otimes_{kH} L$ is a kG -module. Moreover, kG is a free right kH -module, so each ses

$$0 \rightarrow L' \rightarrow L \rightarrow L'' \rightarrow 0$$

of kH -modules yields, by (2.28), a ses of kG -modules:

$$0 \rightarrow L'^G \rightarrow L^G \rightarrow L''^G \rightarrow 0.$$

Therefore the map $\mathrm{ind}_H^G: G_0(kH) \rightarrow G_0(kG)$, defined by $\mathrm{ind}_H^G[L] = [L^G]$, is a \mathbb{Z} -homomorphism.

We next show that, as in the case of restriction, the operation ind_H^G commutes with the decomposition map. We have to prove that the diagram

$$\begin{array}{ccc} G_0(H) & \xrightarrow{\text{ind}_H^G} & G_0(KG) \\ d \downarrow & & \downarrow d \\ G_0(kH) & \xrightarrow{\text{ind}_H^G} & G_0(kG) \end{array}$$

commutes. For this, it suffices to show that $\overline{M}^G \cong \overline{M^G}$ for each RH -lattice M , where bars denotes reduction mod \mathfrak{p} . To accomplish this objective, we note that \overline{M} is defined by a ses of RH -modules:

$$0 \rightarrow M \xrightarrow{\pi} M \rightarrow \overline{M} \rightarrow 0,$$

where π denotes multiplication by a generator π of \mathfrak{p} . As we have noted above, we then have a ses of RG -modules

$$0 \rightarrow M^G \xrightarrow{\pi} M^G \rightarrow \overline{M}^G \rightarrow 0.$$

Thus $\overline{M^G} = M^G / \pi M^G \cong \overline{M}^G$, as required.

We next require a version of Lemma 15.5 for Grothendieck rings (see also Exercise 18.12). We recall that for an arbitrary field E , multiplication in $G_0(EG)$ is given by the formula $[M][N] = [M \otimes_E N]$ (see (16.8)).

(21.14) Lemma. *Let E be an arbitrary field, and let H be a subgroup of G . Then for all $u \in G_0(EH)$, $v \in G_0(EG)$, we have*

$$(\text{ind}_H^G u) \cdot v = \text{ind}_H^G(u \cdot \text{res}_H^G v).$$

Proof. By our preceding remarks, it is sufficient to prove that if L is a left EH -module, and M a left EG -module, then there is an isomorphism of EG -modules

$$L^G \otimes_E M \cong (L \otimes_E M_H)^G.$$

But this result was proved in (10.20) by using the Tensor Product Theorem.

Now we come to the main result of this subsection.

(21.15) Theorem. *Let (K, R, k) be an arbitrary p -modular system, with $\text{char } K = 0$. Then*

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

where \mathcal{E}_K is the family of K -elementary subgroups of G .

Proof. Using Lemma 21.14 with $E=k$, it follows that the right hand side is an ideal in the ring $G_0(kG)$. Thus it is sufficient to prove that the identity element of $G_0(kG)$ belongs to the sum on the right hand side. The identity element of $G_0(KG)$ is $[1_G]$, where 1_G affords the trivial character of G ; also, $d[1_G]$ is the identity element of $G_0(kG)$, where $d: G_0(KG) \rightarrow G_0(kG)$ is the decomposition map. By the Witt-Berman Theorem 21.6 (or by (21.13)) we have

$$[1_G] = \sum_{H \in \mathcal{E}_K} a_H \text{ind}_H^G(u_H), \text{ where } a_H \in \mathbb{Z}, u_H \in G_0(KH) \text{ for each } H \in \mathcal{E}_K,$$

and \mathcal{E}_K is the family of K -elementary subgroups of G . Applying the decomposition map d to both sides of this formula, we obtain

$$d[1_G] = \sum_H a_H d(\text{ind}_H^G u_H) = \sum_H a_H \text{ind}_H^G(d(u_H)),$$

using the fact that the decomposition map commutes with induction. Since $d(u_H) \in G_0(kH)$ for each subgroup $H \in \mathcal{E}_K$, the proof is complete.

§21C. The Cartan-Brauer Triangle (General Case)

Throughout this subsection, G denotes a finite group, and (K, R, k) a p -modular system such that $\text{char } K=0$, and R is complete in the p -adic topology. It is not assumed that either K or k are splitting fields. In this setting, we shall establish most of the properties of the Cartan-Brauer Triangle which were previously proved in §18 under the additional assumption that K is sufficiently large. This part of our discussion is based on the treatment in Serre [77]. We also include a proof of a theorem, due to Witt and Berman, on the number of simple EG -modules, for an arbitrary field E of characteristic $p > 0$ (see (21.5) for fields of characteristic zero).

As we have shown in §18, the hypothesis that R is complete implies that RG is semiperfect, and that there is an isomorphism of \mathbb{Z} -modules, $K_0(RG) \cong K_0(kG)$, given by reduction mod p . The first main result is that the decomposition map $d: G_0(KG) \rightarrow G_0(kG)$ is surjective. The simplest examples show that the decomposition map need not be surjective, in case R is not assumed to be complete. Thus, further generalizations are not always possible (see Exercise 21.4).

(21.16) Theorem. *Let (K, R, k) be a p -modular system such that R is complete, and $\text{char } K=0$. Then the decomposition map $d: G_0(KG) \rightarrow G_0(kG)$ is surjective.*

Proof. By (21.13) and (21.15), we have

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

and

$$G_0(kG) = \sum_{H \in \mathfrak{S}_K} \text{ind}_H^G G_0(kH).$$

Here, in both cases, \mathfrak{S}_K is the family of K -elementary subgroups of G . Since d commutes with the operation ind_H^G (see §21B), we have

$$d(G_0(KG)) = \sum_{H \in \mathfrak{S}_K} \text{ind}_H^G d(G_0(KH)).$$

By virtue of formula (*) above, it therefore suffices to prove that

$$(21.17) \quad d(G_0(KH)) = G_0(kH)$$

for each K -elementary subgroup H of G . Thus the proof of (21.16) will be complete once we establish the following more general version of (21.17):

(21.18) Proposition. *Let (K, R, k) be a p -modular system with $\text{char } K=0$ and R complete in the p -adic topology. Let H be a group which is a semi-direct product $A \rtimes D$ of a cyclic q' -group $A=\langle a \rangle$ and a q -group D , for some prime q . Then every simple kH -module F can be lifted to a simple KH -module Z , that is, there exists a full RH -lattice M in Z such that $M/\mathfrak{p}M \cong F$.*

Before beginning the proof, we remark that any group H satisfying the above hypotheses is an example of a p -solvable group (see §1B). Thus, in case K is sufficiently large, the above proposition is a special case of the Fong-Swan-Rukolaine Theorem proved in §22. In the situation occurring in (21.18), the stronger hypotheses on H allow us to lift simple kH -modules, without having to assume that K is sufficiently large.

Proof of (21.18). We shall use induction on $|H|$. First suppose that $q \neq p$, and let S be the Sylow p -subgroup of A . Then S is a normal p -subgroup of H , and acts trivially on the given simple kH -module F , by (17.16). If we set $\bar{H}=H/S$, then \bar{H} is a p' -group, and F is a simple $k\bar{H}$ -module. Therefore $F \in \mathcal{P}(k\bar{H})$, and since R is complete, F can be lifted to a projective $R\bar{H}$ -lattice by (18.1); this lattice is then an RH -lattice, whose reduction mod \mathfrak{p} is F , and the result is proved in this case where $q \neq p$.

Now assume that $q=p$, and let L be a simple kA -submodule of F_A . If the kA -module L is not H -stable, then let $H_1 = \text{Stab}_H L$, a proper subgroup of H . By Theorem 11.1, we have $F \cong (L_1)^H$ for some simple kH_1 -module L_1 . Since the group H_1 also satisfies the hypotheses of (21.18), we can apply the induction hypothesis to lift L_1 to a simple KH_1 -module. It is then easily checked that $(L_1)^H$ can be lifted to a KH -module, and the result is established in this case.

Thus we may now assume that L is H -stable, and that F_A is a direct sum of copies of L . Using the notation of Exercise 21.5, we may decompose kA and KA into direct sums of fields: $kA = \coprod_i k_i$, $KA = \coprod_i K_i$. To fix the notation, suppose that

$$L \cong k_1 = k[y]/(f_1(y)) = k[\bar{\omega}], R_1 = R[y]/(g_1(y)) = R[\omega],$$

where $\bar{g}_1 = f_1$, and where $g_1(\omega) = 0$, $f_1(\bar{\omega}) = 0$. We may assume that a acts on k_1 as multiplication by $\bar{\omega}$, and on R_1 as multiplication by ω .

Let us now consider the action of D on F . Since D is a p -group, and $\text{char } k = p$, it follows from (5.24) that D acts trivially on the socle of F_D . Therefore F contains a nonzero element u such that $xu = u$ for all $x \in D$. Then $(kA)u$ is a kH -submodule of F , since $x(kA)x^{-1} = kA$ for all $x \in D$, because $A \trianglelefteq H$. Therefore $F = (kA)u$, and so F_A is a cyclic kA -module. Since kA has no repeated summands as kA -module, it follows that $F_A \cong L$, that is, $F \cong k_1$ as kA -modules.

For each $x \in D$, a acts on the conjugate module xL in the same way that xax^{-1} acts on L . Writing $xax^{-1} = a^t$ for some integer t , it follows that xax^{-1} acts as $\bar{\omega}'$ on k_1 . But L is H -stable, and therefore $\bar{\omega}'$ must be a zero of the polynomial $f_1(y)$ used to define k_1 . This shows that the map $\bar{\omega} \rightarrow \bar{\omega}'$ gives an element $\sigma_x \in \mathfrak{G}$, where \mathfrak{G} is the Galois group

$$(21.19) \quad \mathfrak{G} = \text{Gal}(k_1/k) \cong \text{Gal}(R_1/R).$$

The map $x \rightarrow \sigma_x$, $x \in D$, is a homomorphism of D into \mathfrak{G} , and allows us to view k_1 as a kH -module, on which a acts as $\bar{\omega}$ and $x \in D$ acts as σ_x . Then $F \cong k_1$ as kH -modules.

In view of the isomorphism, we can make R_1 into an RH -lattice by letting a act as ω , and $x \in D$ act as σ_x (that is, $x \cdot \omega = \omega'$, in terms of the above notation). Clearly $R_1 \cong k_1$ as kH -modules, so F has now been lifted to an RH -lattice R_1 , and this completes the proof of Proposition 21.18, as well as the proof of Theorem 21.16.

We remark that the structure of the simple module F in the stable case, as in the preceding proof, was described by Theorem 11.17, but not in a sufficiently precise way to accomplish the lifting, without the help of the Galois theory of local fields.

We now consider the Cartan-Brauer Triangle

$$\begin{array}{ccc} G_0(KG) & \xrightarrow{d} & G_0(kG) \\ e \swarrow & & \searrow c \\ & K_0(kG), & \end{array}$$

defined in §18A whether or not the field K is sufficiently large. The next two

theorems will use the facts established in §18B for the splitting field case, together with some results on ground field extensions proved in §16D.

(21.20) Theorem. *The map $e: K_0(kG) \rightarrow G_0(KG)$ is a split injection, for any p -modular system (K, R, k) with $\text{char } K = 0$ and R complete in the p -adic topology.*

Proof. The result holds if K is sufficiently large, by (18.27). For the general case, by §17A there exists a finite extension (K', R', k') of (K, R, k) , in which K' is sufficiently large. Now consider the commutative diagram

$$\begin{array}{ccc} K_0(k'G) & \xrightarrow{e'} & G_0(K'G) \\ \alpha \uparrow & & \beta \uparrow \\ K_0(kG) & \xrightarrow{e} & G_0(KG), \end{array}$$

where e and e' are defined by (18.3), and α, β arise from ground field extensions. Then e' is a split injection by (18.27), so $\gamma e' = 1$ for some γ as shown below:

$$\begin{array}{ccc} K_0(k'G) & \xrightleftharpoons[\gamma]{e'} & G_0(K'G) \\ \alpha \uparrow \downarrow \delta & & \beta \uparrow \\ K_0(kG) & \xrightarrow{e} & G_0(KG). \end{array}$$

By (16.22), both α and β are injections, and therefore so is e , because e' is an injection. Further, by (16.22) there exists a map δ such that $\delta\alpha = 1$. It follows at once that

$$\delta\gamma\beta e = \delta\gamma e'\alpha = \delta\alpha = 1,$$

so $\delta\gamma\beta$ is the desired splitting of e .

Keeping the hypotheses of (21.20), we obtain the following extension of (18.16):

(21.21) Corollary. *Let P and $P' \in \mathcal{P}(RG)$ be such that $K \otimes_R P \cong K \otimes_R P'$ as KG -modules. Then $P \cong P'$ as RG -modules.*

The next result is a reformulation and generalization of (18.25), and we shall prove it without the use of Brauer characters.

(21.22) Theorem. Let (K, R, k) be a p -modular system, with R complete and $\text{char } K = 0$. The Cartan homomorphism

$$c : K_0(kG) \rightarrow G_0(kG)$$

is injective, $\text{cok } c$ is finite, and $|G|_p \cdot \text{cok } c = 0$.

Proof. Since $K_0(kG)$ and $G_0(kG)$ are \mathbb{Z} -free of the same rank, by §18A, it follows that c is injective if and only if $\text{cok } c$ is a finite \mathbb{Z} -module.

We first give a new proof of the result in case K is sufficiently large (see (18.25) and (18.27)), this time using the induction theorem (21.15) instead of the theory of Brauer characters.

If K is sufficiently large, the family of K -elementary subgroups of G coincides with the family \mathcal{E} of elementary subgroups, and in this case (21.15) gives

$$G_0(kG) = \sum_{H \in \mathcal{E}} \text{ind}_H^G G_0(kH).$$

We must prove that $|G|_p u \in \text{im } c$ for every $u \in G_0(kG)$. Since $|G|_p \geq |H|_p$ for all $H \in \mathcal{E}$, and since the Cartan map obviously commutes with induction (see Exercise 18.9), it is clearly sufficient to prove that $|H|_p$ annihilates $G_0(kH)/c\{K_0(kH)\}$. But for such a group, $\text{im } c = |H|_p \cdot G_0(kH)$ by Exercise 18.7, which completes the proof of the theorem in the case where K is sufficiently large.

Turning to the general case, let (K', R', k') be a finite extension of (K, R, k) , with K' sufficiently large. Then there is a commutative diagram

$$\begin{array}{ccccccc} 0 & \longrightarrow & K_0(kG) & \xrightarrow{\alpha} & K_0(k'G) & \longrightarrow & X \longrightarrow 0 \\ & & c \downarrow & & c' \downarrow & & f \downarrow \\ 0 & \longrightarrow & G_0(kG) & \xrightarrow{\beta} & G_0(k'G) & \longrightarrow & Y \longrightarrow 0, \end{array}$$

where α and β are the injections defined in (16.22), c and c' are Cartan homomorphisms, $X = \text{cok } \alpha$, $Y = \text{cok } \beta$, and f is the homomorphism induced on X by c' . By the Snake Lemma, there is an exact sequence of abelian groups

$$0 \rightarrow \ker c \rightarrow \ker c' \rightarrow \ker f \rightarrow \text{cok } c \rightarrow \text{cok } c'.$$

By the first part of the proof, $\ker c' = 0$ and $|G|_p \cdot \text{cok } c' = 0$. Therefore $\ker c = 0$, and so $\text{cok } c$ is finite, by the remark at the beginning of the proof. On the other hand, α is a split injection by (16.22), so X is \mathbb{Z} -free. Therefore $\ker f$ is

also \mathbf{Z} -free. From the exact sequence

$$0 \rightarrow \ker f \rightarrow \text{cok } c \rightarrow \text{cok } c',$$

and the fact that $\text{cok } c$ is finite, we conclude that $\ker f = 0$. Therefore $\text{cok } c$ is embedded in $\text{cok } c'$, and so $|G|_p \cdot \text{cok } c = 0$, which finishes the proof of the theorem.

As an immediate consequence of Theorem 21.22, we obtain the following corollaries, valid for an arbitrary p -modular system (K, R, k) in which $\text{char } K = 0$ and R is complete:

(21.23) Corollary. *Two f.g. projective kG -modules are isomorphic if and only if they have the same composition factors (counted with multiplicity).*

(21.24) Corollary. *The determinant of the Cartan matrix is a power of p .*

It should be pointed out that for an arbitrary p -modular system (K, R, k) as above, we do not obtain the equation $\mathbf{C} = {}^t \mathbf{D} \mathbf{D}$, nor even that \mathbf{C} is symmetric. For further discussion, see CR §83A.

In §32C, we give a detailed study of the image of the map $K_0(RG) \rightarrow G_0(KG)$ in the global case, where R is a Dedekind domain with quotient field K of characteristic 0.

For the rest of this subsection, E denotes an arbitrary field of characteristic $p > 0$, and G a finite group. We shall prove a result due to Witt [52] and Berman [56a], on the number of simple EG -modules. The corresponding result for a field of characteristic zero is given in Theorem 21.5. The Witt-Berman result has been extended to twisted group algebras by Reynolds [71]. Our proof follows Reiner [64], and is based on the theory of Brauer characters.

Let m be the exponent of G , and write $m = p^a m'$, where $p \nmid m'$. Then the polynomial $X^{m'} - 1$ is separable over E , and the field F generated over E by the zeros of $X^{m'} - 1$ is a Galois extension of E , and is a splitting field for G , by Theorem 17.1. We have $F = E(\tilde{\omega})$, where $\tilde{\omega}$ is a primitive m' -th root of 1 over E .

As in §21A, let \mathfrak{G} be the Galois group of F over E , and define a monomorphism $\sigma \rightarrow t$ from \mathfrak{G} into a subgroup $I_m(E)$ of $(\mathbf{Z}/m'\mathbf{Z})^\times$. If $\sigma_i \in \mathfrak{G}$ corresponds to $t \in I_m(E)$, then $\sigma_i(\tilde{\omega}) = \tilde{\omega}^t$.

Two elements $x, y \in G$ are called E -conjugate if $x = {}_G y^t$ for some $t \in I_m(E)$. Then E -conjugacy is an equivalence relation, and the equivalence classes are the E -conjugacy classes. The E -conjugacy classes contained in G_p are called p -regular E -conjugacy classes.

The Witt-Berman Theorem can now be stated as follows:

(21.25) Theorem. *Let G be a finite group, and let E be an arbitrary field of characteristic $p > 0$. Then the number of isomorphism classes of simple EG -modules is equal to the number of p -regular E -conjugacy classes of G .*

We first have to extend some of the results on Brauer characters from §17, in order to handle EG -modules. In §17, Brauer characters were defined for kG -modules, when k is part of a p -modular system, and k is sufficiently large. For the more general case of EG -modules, we make the following definition:

(21.26) Definition. Let E be an arbitrary field of characteristic $p > 0$, and let G be a finite group of exponent $m = p^a m'$, where $(p, m') = 1$. Let

$$k_0 = \text{prime field of } E, k = k_0(\tilde{\omega}) \subseteq E(\tilde{\omega}) = F,$$

where $\tilde{\omega}$ is a primitive m' -th root of unity over E . Then k is sufficiently large relative to G , and is part of a p -modular system (K, R, k) in which K is sufficiently large relative to G , and where R contains a primitive m' -th root of unity ω such that $\bar{\omega} = \tilde{\omega}$, where bars denote reduction mod \mathfrak{p} .

Now let L be a left EG -module. For each $x \in G_{p'}$, the eigenvalues of the left multiplication x_L on L are powers of $\tilde{\omega}$, and lie in k . We then define the *Brauer character* λ of G afforded by L exactly as in (17.4). The resulting function λ is a K -valued class function defined on $G_{p'}$. It is easily checked that statements (i)–(iii) of (17.5) hold true for Brauer characters afforded by EG -modules.

The preceding definition of Brauer characters clearly generalizes that given in (17.4). It will be useful to have another interpretation of Brauer characters afforded by EG -modules. Let $\{M_i : 1 \leq i \leq r\}$ be a basic set of simple kG -modules, and let μ_i be the Brauer character of G afforded by M_i , $1 \leq i \leq r$. Since k is sufficiently large relative to G , the FG -modules $\{F \otimes_k M_i\}$ are a basic set of simple FG -modules, and the Brauer character afforded by $F \otimes_k M_i$ is precisely μ_i , $1 \leq i \leq r$. On the other hand, starting with the EG -module L with Brauer character λ , we may form the FG -module $F \otimes_E L$, whose Brauer character is also equal to λ . By (17.5iii), the Brauer character of the module $F \otimes_F L$ depends only on the composition factors of the module. If $F \otimes_k M_i$ occurs with multiplicity a_i as composition factor of $F \otimes_E L$, for $1 \leq i \leq r$, then clearly we have

$$(21.27) \quad \lambda = \sum_{i=1}^r a_i \mu_i$$

as class functions on $G_{p'}$. The key idea in this discussion is the fact that Brauer characters, as defined in (21.26), are unchanged by ground field extension.

We need in addition the following fact:

(21.28) Lemma. Let $H \leq G$, and let L be an EH -module affording the Brauer character λ of H . Then the induced EG -module L^G has Brauer character λ^G , where λ^G is the class function defined on $G_{p'}$, as in (10.3).

Proof. The result is an extension of Exercise 18.10. Let $\{N_i\}$ be a basic set of simple kH -modules, and let N_i afford the Brauer character ν_i of H . By (21.27) we obtain

$$\lambda^G = \sum_i a_i \nu_i^G$$

as class functions on $G_{p'}$. By Exercise 18.10, ν_i^G is the Brauer character of G afforded by N_i^G , and hence also by $F \otimes_k N_i^G$. However, $F \otimes_E L^G$ is isomorphic to $(F \otimes_E L)^G$, and therefore has the same FG -composition factors as $\prod_{i=1}^r (F \otimes_k N_i^G)^{(a_i)}$. It follows at once that the Brauer character of G afforded by $F \otimes_E L^G$ is precisely $\sum a_i \nu_i^G$. This shows that L^G affords the Brauer character λ^G , and the proof is completed.

We are now ready to proceed with the proof of (21.25).

Step 1. Let $\{X_i : 1 \leq i \leq u\}$ be a basic set of simple EG -modules, and let χ_i be the Brauer character of G afforded by X_i , $1 \leq i \leq u$. These $\{\chi_i\}$ are K -valued class functions on $G_{p'}$, and we shall prove that they are linearly independent over K . As in (21.27), let $\{\mu_j\}$ be a basic set of irreducible Brauer characters of G . Then the $\{\mu_j\}$ are linearly independent over K by (17.9), since k is sufficiently large relative to G . Now each χ_i is expressible as a Z -linear combination of the $\{\mu_j\}$ by (21.27). Further, a given μ_j cannot occur in both χ_i and $\chi_{i'}$, where $i \neq i'$, since by Exercise 7.9 the FG -modules $F \otimes_E X_i$ and $F \otimes_E X_{i'}$ have no common composition factor. This shows that the Brauer characters $\{\chi_i : 1 \leq i \leq u\}$ can be expressed as non-overlapping sums of the $\{\mu_j\}$. Since the $\{\mu_j\}$ are linearly independent over K , so are the $\{\chi_i\}$, as claimed.

Step 2. We show next that Brauer characters afforded by EG -modules are constant on E -conjugacy classes in $G_{p'}$. Let χ be the Brauer character of G afforded by an EG -module X , and suppose that $a, b \in G_{p'}$ are E -conjugate. Then we may write $gag^{-1} = b^t$ for some $g \in G$ and $t \in I_m(E)$. If $\mathbf{X} : G \rightarrow M_d(E)$ is a matrix representation afforded by X , then $\mathbf{X}(a)$ and $\mathbf{X}(b^t)$ have the same sets of eigenvalues, and the eigenvalues of $\mathbf{X}(b^t)$ are the t -th powers of those of $\mathbf{X}(b)$. However, since $\mathbf{X}(b)$ has entries in E , the map $\tilde{\omega} \rightarrow \tilde{\omega}^t$ defines an automorphism of E which leaves $\mathbf{X}(b)$ fixed. It follows that $\mathbf{X}(b)$ and $\mathbf{X}(b^t)$ have the same sets of eigenvalues, and hence $\chi(a) = \chi(b^t) = \chi(b)$, as required.

Step 3. Let $a \in G_{p'}$, and let A be the cyclic p' -group generated by a . Define a class function $\theta : A \rightarrow K$ by setting

$$\theta(a^t) = \begin{cases} |A|, & t \in I_m(E), \\ 0, & \text{otherwise.} \end{cases}$$

Let us show that θ is expressible as a K -linear combination of Brauer

characters of A afforded by EA -modules. Since A is a p' -group and F is sufficiently large, we have $\text{Bch } FA = \text{ch } KA$ by (18.11). Now the Galois group \mathfrak{G} of F relative to E permutes the set of simple FA -modules, and the direct sum over each orbit is the extension $F \otimes_E L$ of some simple EA -module L ; this follows from the proof of Exercise 21.5, and also from (7.11) and (7.19). Consequently, the Brauer character of A afforded by L is the sum over a \mathfrak{G} -orbit of the Brauer characters afforded by simple FA -modules.

By the first part of the proof of (21.9), the above function θ is a K -linear combination of irreducible characters afforded by simple KA -modules, or equivalently, of irreducible Brauer characters afforded by simple FA -modules. Further, the coefficients are constant on the \mathfrak{G} -orbits of such FA -modules. This implies at once that θ is a K -linear combination of Brauer characters afforded by EA -modules, as claimed.

Step 4. We can now complete the proof of the Witt-Berman Theorem (21.25). Let $\{a_j : 1 \leq j \leq v\}$ be representatives of the p -regular E -conjugacy classes of G , and let $\{\chi_i : 1 \leq i \leq u\}$ be a basic set of irreducible Brauer characters of G , as in Step 1. Then the $\{\chi_i\}$ are linearly independent over K by Step 1, and they are constant on the E -conjugacy classes of G by Step 2. It follows that $u \leq v$.

Conversely, for each a_j , $1 \leq j \leq v$, let θ_j be the function constructed in Step 3 for the cyclic group $\langle a_j \rangle$. Since θ_j is a K -linear combination of Brauer characters afforded by $E\langle a_j \rangle$ -modules, it follows from (21.28) that the induced class function θ_j^G is a K -linear combination of Brauer characters of EG -modules. Hence each θ_j^G is a K -linear combination of the $\{\chi_i\}$. Once we show that the class functions $\{\theta_j^G : 1 \leq j \leq v\}$ are linearly independent over K , it will then follow immediately that $v \leq u$. From Step 2, the characters $\{\theta_j^G\}$ are constant on E -conjugacy classes of G . It is easily checked that $\theta_j^G(a_j) \neq 0$, while $\theta_j^G(a_l) = 0$ if $l \neq j$. This implies that the $\{\theta_j^G\}$ are linearly independent over K , and so $v \leq u$. This completes the proof of the theorem.

§21. Exercises

- Let $G = \langle x : x^n = 1 \rangle$ be a cyclic group of order n . For each d dividing n , let $\Phi_d(X)$ be the cyclotomic polynomial of order d , and let ζ_d be a primitive d -th root of 1 over the rational field \mathbb{Q} . Show that the Wedderburn decomposition of $\mathbb{Q}G$ into simple components is given by

$$\mathbb{Q}G \cong \coprod_{d|n} \mathbb{Q}[X]/(\Phi_d(X)) \cong \coprod_{d|n} \mathbb{Q}(\zeta_d).$$

[Hint: As in the proof of (21.8), we have

$$\mathbb{Q}G \cong \mathbb{Q}[X]/(X^n - 1), \quad X^n - 1 = \prod_{d|n} \Phi_d(X).$$

Now use the results in §4H.]

2. Let G be as above, and let K be any field such that $\text{char } K$ does not divide $|G|$. Find the Wedderburn decomposition of KG , and relate this to the results in (21.5) and (21.26).

3. Generalize Exercises 1 and 2 to the case where G is a finite abelian group.

4. Prove that the decomposition map $d: G_0(KG) \rightarrow G_0(kG)$ need not be surjective, if (K, R, k) is a p -modular system in which R is not complete.

[Hint: Let $p=5$, $K=0$, R the ring of 5-adic integers in \mathbb{Q} , and $k=\mathbb{Z}/5\mathbb{Z}$. Take G to be the cyclic group of order 4. For another example, see the hint for Exercise 18.4.]

5. Let (K, R, k) be a p -modular system in which $\text{char } K=0$ and R is complete. Let $A=\langle a: a^m=1 \rangle$ be cyclic, where $p \nmid m$. Show that the Wedderburn decomposition of the semisimple ring

$$kA = \coprod_i k_i, \quad k_i = \text{field},$$

lifts to a decomposition of R -algebras

$$RA = \coprod_i R_i, \quad \text{where } R_i/\mathfrak{p} R_i \cong k_i.$$

Further, if K_i is the quotient field of R_i , show that K_i is a Galois unramified extension of K with valuation ring R_i , and that

$$\text{Gal}(K_i/K) \cong \text{Gal}(k_i/k) \text{ for each } i.$$

[Hint: We have (since $p \nmid m$)

$$kA \cong k[y]/(y^m - 1) \cong \coprod_i k_i, \quad \text{where } k_i = k[y]/(f_i(y)),$$

and where

$$y^m - 1 = \prod_i f_i(y), \quad f_i(y) \in k[y], \quad f_i(y) \text{ irreducible.}$$

By Hensel's Lemma, this factorization lifts to a factorization

$$y^m - 1 = \prod_i g_i(y), \quad g_i(y) \in R[y], \quad g_i(y) \text{ irreducible,}$$

with $\bar{g}_i = f_i$ for each i .

Keep i fixed, and let ω range over those m -th roots of 1 (in an algebraic closure of K) which are zeros of $g_i(x)$. Then $K_i = K(\omega)$ is unramified over K , and $R_i = R[\omega]$ is its valuation ring. Further, $R_i/\mathfrak{p} R_i \cong \bar{R}[\bar{\omega}] = k(\bar{\omega}) = k_i$, and $\bar{\omega}$ ranges over the zeros of $f_i(y)$. The correspondence $\omega \leftrightarrow \bar{\omega}$ gives the desired isomorphism of Galois groups. (For more details, see Weiss [63, section 3-2].)

6. (Serre [77]). Show that $\sum_{H \in \mathcal{E}} (\text{ch } KH)^G$ is properly contained in $\text{ch } KG$, in case $G = S_3$, $K = \mathbb{R}$, and \mathcal{E} is the family of elementary subgroups of G .

§22. MODULAR REPRESENTATIONS OF p -SOLVABLE GROUPS

Let (K, R, k) be a p -modular system, with K sufficiently large relative to some given finite group G . The main result of this section is that if G is a *solvable* group, then every simple kG -module F is obtained from some simple KG -module by reduction mod \mathfrak{p} . This is clearly a considerable strengthening of our earlier result that the decomposition map $d: G_0(KG) \rightarrow G_0(kG)$ is surjective (see (18.4)). The restriction that G be solvable cannot be omitted, in general, as will be clear from Corollary 22.5 below. On the other hand, the main result is valid for a wider class of groups, consisting of all p -solvable groups. This version of the main result is due to Fong, Swan ([63]; Theorem 6, using Fong [61]), and Rukolaine [62].

Let p be any prime. We recall from §1B that a finite group G is *p -solvable* if G has a normal series each of whose factors is either a p -group or a p' -group. We say that G is p -solvable of *height* m if m is the minimal number of factors in such a normal series. Evidently, a solvable group is p -solvable for every prime p .

Throughout this section, G denotes a finite p -solvable group, and (K, R, k) a p -modular system, with K sufficiently large, and $\text{char } K=0$. The main result is as follows:

(22.1) Fong-Swan-Rukolaine Theorem. *Let F be a simple kG -module, where G is a finite p -solvable group. Then there exists a simple KG -module Z such that $F \cong Z_0 / \mathfrak{p}Z_0$ for each full RG -lattice Z_0 in Z .*

Besides the original sources of the theorem, there is a new and elegant proof due to Serre ([77], §17.4), which was reproduced in Dornhoff ([72], Part B, §72). We shall give a leisurely account of Serre's proof, pointing out, as we go along, connections with Clifford theory and projective representations.

Proof of (22.1). Step 1. Let bars denote reduction mod \mathfrak{p} . If Z_0 and Z_1 are a pair of full RG -lattices in a KG -module Z , then by (16.16) \bar{Z}_0 and \bar{Z}_1 have the same composition factors. Therefore if $\bar{Z}_0 \cong F$, then also $\bar{Z}_1 \cong F$, so it suffices to find a single RG -lattice Z_0 with the desired property.

Now let (K', R', k') be another p -modular system, with K' a finite extension field of K , $R' \cap K = R$, and k' a finite extension of k . Suppose the result is known for the p -modular system (K', R', k') . We assert that it also holds for (K, R, k) . Let F be a simple kG -module; then $F' = k' \otimes_k F$ is a simple $k'G$ -module, since k is a splitting field by (17.2). By hypothesis, there exists a simple $K'G$ -module Y , and a full $R'G$ -lattice Y_0 in Y , such that $Y_0 / \mathfrak{p}'Y_0 \cong F'$. By (16.16), the same result holds for any other full $R'G$ -lattice in Y , because F' is simple. Since K is a splitting field for G , we have $Y = K' \otimes_K Z$ for some simple KG -module Z , by (7.15iii). Let Z_0 be a full RG -lattice in Z . Then



$Y'_0 = R' \otimes_R Z_0$ is a full $R'G$ -lattice in Y , and we have

$$(R' \otimes_R Z_0) / \mathfrak{p}'(R' \otimes_R Z_0) \cong (R' / \mathfrak{p}'R') \otimes_k (Z_0 / \mathfrak{p}Z_0) \cong k' \otimes_k \bar{Z}_0,$$

where $\bar{Z}_0 = Z_0 / \mathfrak{p}Z_0$. Then by the preceding remarks, we have $k' \otimes_k \bar{Z}_0 \cong F' \cong k' \otimes_k F$, and hence $\bar{Z}_0 \cong F$ by the Noether-Deuring Theorem (Exercise 6.6).

Step 2. We shall prove (22.1) by using induction on the height m of G , and for groups of the same height, by induction on the order of G . We note that if G has height 1, then G is either a p -group or a p' -group, and the result follows from (5.24) or Exercise 18.4. Therefore, we may assume that $m \geq 2$. In that case, G contains either a normal p -subgroup D , or a normal p' -subgroup H , such that the height of the quotient group is at most $m-1$. In the former case, D acts trivially on each simple kG -module F , by (17.16). Therefore, each simple kG -module F can be viewed as a simple $k(G/D)$ -module, and hence can be lifted to a simple KG -module, by the induction hypothesis. Thus the theorem holds when G contains such a subgroup D .

Step 3. From now on, we may assume that G has height $m \geq 2$, and contains a normal p' -subgroup H for which G/H has height $m-1$. Given a simple kG -module F , its restriction F_H is a direct sum of simple KH -modules, by Clifford's Theorem 11.1. If L is one such summand, let T be the stabilizer of L , that is, $T = \{x \in G : {}^x L \cong L\}$. Then by (11.1iv), $F \cong \text{ind}_T^G F_1$ for some simple kT -module F_1 . If $T \neq G$, then we can use the induction hypothesis to lift F_1 to a KT -module, and hence lift F ($\cong \text{ind}_T^G F_1$) to a KG -module. (Of course, we are using the fact that T has height $\leq m$.)

Step 4. By Step 3, it remains to consider the case where G has height $m \geq 2$, H is a normal p' -subgroup of G , and F_H has a stable simple submodule L . By Clifford's Theorem 11.20, we have

$$F \cong L \otimes_k I,$$

where L affords a projective representation U of G , with factor set $\alpha : G \times G \rightarrow k$, say, and I affords a projective representation V of G/H , with factor set α^{-1} . In this Step 4, we shall lift U to a projective R -representation of G . Later we shall lift V , and shall then glue together the resulting projective R -representations of G to obtain the desired R -representation of G .

Since L is a simple kH -module, and H is a p' -group, there exists an RH -lattice M such that KM is absolutely simple and $\bar{M} \cong L$, by (18.11). Further, for each $x \in G$ we have ${}^x \bar{M} \cong {}^x M \cong \bar{M}$, since L is a stable kH -module. We may now *apply Theorem 30.16, using the fact that $|H|$ is a unit in R , to conclude that for each $x \in G$, there is an isomorphism of RH -lattices $M \cong {}^x M$. It follows that for each $x \in G$, there exists an R -automorphism $S(x)$ of M

*We could instead use Exercise 19.3 and (18.1iv).

such that

$$(22.2) \quad S(h)m = hm, \text{ and } hS(x)m = S(x)h^x m \text{ for all } m \in M, h \in H, x \in G.$$

An easy computation shows that for all $x, y \in G$, we have $S(y)^{-1}S(x)^{-1}S(xy) \in \text{End}_{RH}(M)$. Since KM is absolutely simple, it follows that for $x, y \in G$, there exists a unit $\beta(x, y) \in R$ such that

$$(22.3) \quad S(x)S(y) = \beta(x, y)S(xy),$$

and hence $S: G \rightarrow GL(M)$ is a projective R -representation of G . Moreover, for each $x \in G$, there exists a k -automorphism $\bar{S}(x)$ of \bar{M} corresponding to $S(x)$, with the following properties:

$$\begin{cases} \bar{S}(h)\bar{m} = h\bar{m}, h\bar{S}(x)\bar{m} = \bar{S}(x)h^x\bar{m}, \\ \bar{S}(x)\bar{S}(y) = \bar{\beta}(x, y)\bar{S}(xy), \text{ for all } x, y \in G, h \in H, \bar{m} \in \bar{M}. \end{cases}$$

By the remarks following (11.20) it follows that the projective k -representation \bar{S} of G is equivalent to U , and we have lifted U to a projective R -representation of G , completing the proof of Step 4. By replacing V by an equivalent representation, we may identify U with \bar{S} .

Step 5. In order to lift the projective k -representation V to a projective R -representation of G , we have to use the induction hypothesis, which does not work smoothly for projective representations. Therefore we shall first apply the methods of §11 to construct a central extension E of G to which the k -representations U and V , and the R -representation S , can all be lifted.

Let $b \in H^2(G, R)$ be the equivalence class of the factor set $\beta: G \times G \rightarrow R$ which occurs in (22.3). We shall now prove that b has finite order e , where $p \nmid e$, when b is viewed as an element of the multiplicative group $H^2(G, R)$. Let us put

$$d = R\text{-rank of } M = \dim_K KM.$$

Then d divides $|H|$ by (9.32), since KM is an absolutely simple KH -module. Therefore d is relatively prime to p , because H is a p' -group. Relative to some R -basis of M , each $S(x)$ can be represented by a matrix $\mathbf{S}(x) \in GL_d(R)$, $x \in G$. We set $g(x) = \det \mathbf{S}(x) \in R$, $x \in G$. Taking determinants in (22.3), we obtain

$$g(x)g(y) = \{\beta(x, y)\}^d g(xy) \text{ for all } x, y \in G.$$

This implies that $b^d = 1$ in $H^2(G, R)$, and completes the proof that the order e of b is finite, and that $p \nmid e$. (See Exercise 11.9.)

Since $b^e = 1$ in $H^2(G, R)$, there exists a map $h: G \rightarrow R$ such that

$$h(x)h(y) = \{\beta(x, y)\}^e h(xy) \text{ for all } x, y \in G.$$

Now let K' be the field obtained from K by adjoining all e -th roots of all of the elements $\{h(x) : x \in G\}$; it should be noted that K already contains all the e -th roots of 1, since e divides $|G|$ and K is sufficiently large relative to G . Let R' be a valuation ring in K' which corresponds to some extension of the p -adic valuation from K to K' . Then K' is a finite (Galois) extension of K , and R' contains the e -th roots $\{h(x)^{1/e} : x \in G\}$, since each $h(x) \in R$. As in the proof of (11.38), we can then obtain a new factor set $\beta' : G \times G \rightarrow (R')$ such that β' takes values which are e -th roots of 1, and such that β' is equivalent to β (when β is viewed as a factor set with values in (R') , by virtue of the inclusion $R' \subseteq (R')$).

Let (K', R', k') be the p -modular system just defined. By Step 1, it suffices to prove that the $k'G$ -module $k' \otimes_k F$ can be lifted to a simple $K'G$ -module. Changing notation, we may therefore suppose that the p -modular system (K, R, k) is such that the factor set $\beta : G \times G \rightarrow R$ takes values which are e -th roots of 1 in R . We may then write the values of the factor set β occurring in (22.3) in the form

$$(22.4) \quad \beta(x, y) = \omega^{n(x, y)}, \quad x, y \in G,$$

where ω is a primitive e -th root of 1 in R , and where each $n(x, y)$ is an integer such that $0 \leq n(x, y) < e$.

Now let $B = \langle b \rangle$ be a cyclic group of order e . As in the proof of (11.40), we define $f : G \times G \rightarrow B$ by

$$f(x, y) = b^{n(x, y)}, \quad x, y \in G,$$

so f is a factor set from $G \times G$ to B .

By the discussion in §8C, we can then construct a central extension

$$1 \rightarrow B \rightarrow E \xrightarrow{\pi} G \rightarrow 1,$$

such that $\{f(x, y)\}$ is the factor set associated with some π -section $x \mapsto u_x$, $x \in G$. Then every element of E can be expressed uniquely in the form $\{b^i u_x : 0 \leq i < e, x \in G\}$, and we have

$$u_x u_y = f(x, y) u_{xy}, \quad x, y \in G.$$

Now let $\psi : B \rightarrow R$ be the linear character of B defined by $\psi(b) = \omega$. Using (22.4), it follows that the map $\tilde{S} : E \rightarrow GL(M)$ defined by

$$\tilde{S}(b^i u_x) = \psi(b^i) S(x), \quad i \in \mathbb{Z}, \quad x \in G,$$

is an R -representation of E . Moreover, the map $x \mapsto \tilde{S}(u_x)$, $x \in G$, is the original projective representation S of G constructed in Step 4. In other words, we have lifted the projective k -representation U of G to a projective R -representation S of G , and to an ordinary R -representation \tilde{S} of E .

Now let $\bar{\psi}: B \rightarrow k$ be the linear k -representation of B given by $\bar{\psi}(b) = \bar{\omega}$, where $\bar{\omega}$ is the image of ω in k . It is clear that the same construction, using $\bar{\psi}$ instead of ψ , defines a k -representation $U^*: E \rightarrow GL(\bar{M})$, given by

$$U^*(b^i u_x) = \bar{\psi}(b^i) U^*(x), \quad i \in \mathbb{Z}, \quad x \in G.$$

Then the map $x \rightarrow U^*(u_x)$, $x \in G$, coincides with the original projective representation $x \rightarrow U(x)$ of G on M .

Step 6. We now consider the projective k -representation V of G/H on I , and will lift it to an ordinary R -representation of E . If $\alpha: G \times G \rightarrow k$ is the factor set associated with U , then α^{-1} is the factor set associated with V . We can therefore apply the construction in the last paragraph of Step 5 to lift V to an ordinary k -representation V^* of E , using the homomorphism $\bar{\psi}^{-1}: B \rightarrow k$ instead of $\bar{\psi}$. From the definition of V (see the proof of (11.20)), it is clear that H is contained in the kernel of V^* . It follows that $H \trianglelefteq E$, and $H \cap B = 1$, since $\bar{\psi}^{-1}$ is a faithful representation of B . Letting $\bar{E} = E/H$, we now have a central extension

$$1 \rightarrow B \rightarrow \bar{E} \rightarrow G/H \rightarrow 1.$$

We shall apply the induction hypothesis to lift V^* to an R -representation of \bar{E} , and hence to E .

By assumption, G/H is p -solvable of height $\leq m-1$, where m is the height of G , and $m \geq 2$. Thus \bar{E} contains a normal subgroup $D \geq B$ such that $E/D \cong (\bar{E}/B)/(D/B)$ has height $\leq m-2$, and D/B is either a p -group or a p' -group. If D/B is a p -group, then $D \cong P \times B$ for some p -group P , since B is central. Then $P \trianglelefteq \bar{E}$, and $P \leq \ker V^*$, by (17.16). Then \bar{E}/P is p -solvable of height $\leq m-1$, and V^* can be lifted to an R -representation of \bar{E}/P , and hence to an R -representation T of E , by the induction hypothesis.

On the other hand, if D/B is a p' -group, then D is a normal p' -subgroup of \bar{E} , so the height of \bar{E} is $\leq m-1$. By induction, we can then lift V^* to an R -representation of E , which we again denote by T .

Step 7. We can now complete the proof of the theorem as follows. By Step 4, the simple kG -module F affords a k -representation of the form $U \otimes_k V$, where U and V are projective k -representations, whose factor sets are inverses of one another. In Steps 5 and 6, these projective representations were lifted to ordinary k -representations U^* and V^* of E , where E is the central extension of G with cyclic kernel B of order prime to p , as in Step 4. Then $U^* \otimes_k V^*$ is a k -representation of E , whose kernel contains B , because of the way U^* and V^* were defined, using $\bar{\psi}$ and $\bar{\psi}^{-1}$ on B , etc. Then $U^* \otimes_k V^*$ defines a k -representation of $G = E/B$, and by the previous discussion, this is a k -representation of G afforded by F .

In Steps 4–6, the k -representations U^* and V^* were lifted to R -representations S and T of E . Then $S \otimes_R T$ is an R -representation of E , such

that $\overline{S \otimes_R T}$ is a k -representation equivalent to $U^* \otimes_k V^*$, (where $\overline{S \otimes_R T}$ denotes the representation of E obtained by reduction mod \mathfrak{p} of $S \otimes_R T$.)

Finally, there is the question as to whether $S \otimes_R T$ defines a representation of G . Since B is a p' -group, which is contained in the kernel of $\overline{S \otimes_R T}$ it follows by (18.11) that B is also contained in the kernel of $S \otimes_R T$. Therefore $S \otimes_R T$ defines an R -representation of G whose reduction mod \mathfrak{p} is the k -representation afforded by F . This completes the proof of the Fong-Swan-Rukolaine Theorem.

(22.5) Corollary. *The degree of each irreducible k -representation of a p -solvable group G coincides with the degree of some irreducible K -representation, and hence divides the order of G .*

In an example at the end of §17, it was shown that the degrees of the irreducible k -representations of $SL_2(p)$, where $p = \text{char } k$, need not divide the order of $SL_2(p)$. By Corollary 22.5, it follows that, in general, the conclusion of Theorem 22.1 does not hold for the groups $\{SL_2(p)\}$.

(22.6) Corollary. *Let φ be an irreducible Brauer character of a finite p -solvable group G , afforded by a simple kG -module, where $\text{char } k = p$. Then there exists an irreducible K -character ξ of G such that $\xi_{G_{p'}} = \varphi$, where $\xi_{G_{p'}}$ denotes the restriction of ξ to the p' -elements of G .*

(22.7) Corollary. *The decomposition numbers $\{d_{ij}\}$ (see (16.20)) associated with a p -solvable group G and a p -modular system (K, R, k) as above, are either 0 or 1.*

For other results on modular representations of p -solvable groups, see Fong [62], Cliff [75], [77], and Isaacs [74], [78]. In Isaacs [74], there is another proof of the Fong-Swan-Rukolaine Theorem, using some of Gallagher's results on extending invariant characters from normal subgroups (see §15C), instead of the theory of projective representations. Isaacs also points out that the character ξ in (22.6) is not uniquely determined.

We conclude by summarizing without proof the main result of Isaacs [74]. A K -character ξ of G is called p -rational if for each $x \in G$, the character value $\xi(x)$ can be expressed as a sum of roots of unity of orders prime to p . Isaacs shows that if G is a p -solvable group with $p \neq 2$, then every irreducible Brauer character φ of G can be lifted to a character $\xi \in \text{Irr } G$ such that

(i) ξ is p -rational, and

(ii) If $H \trianglelefteq G$, and ψ is any irreducible character of H occurring in ξ_H , then ψ is p -rational and its restriction ψ_{H_p} is an irreducible Brauer character of H .

Furthermore, these properties (i) and (ii) uniquely determine the character ξ lifting φ .

§22 Exercise

1. Let G be a finite group with a normal p -complement H , and let (K, R, k) be a p -modular system with K sufficiently large. Prove that each indecomposable projective Brauer character η^i can be expressed in the form λ^G , for some $\lambda \in \text{Irr}_K H$. (For extensions of this result to general p -solvable groups, see Fong [62, Theorem 2D].)

Integral Representations: Orders and Lattices

This is the first of several chapters on integral representation theory, and it may be worthwhile to begin with a broad description of this theory. We may think of it as a refinement of ordinary and modular representation theory, as well as a generalization of certain parts of algebraic number theory. Many of the key results are obtained by applying number-theoretic techniques to problems in ordinary representation theory. At the same time, concepts and methods from homological algebra play a significant role in the theory. In a rough sense, we may regard integral representation theory as a central core which connects various topics in ordinary and modular representation theory, algebraic number theory, and algebraic K -theory.

The deeper aspects of the study of algebraic number fields depend on knowledge of the *rings* of integers in these fields. Basic results from field theory thus appear as rough versions of deeper facts about rings of integers. For example, let $R = \text{alg. int. } \{K\}$, where K is an algebraic number field. Let E be a finite extension field of K of degree n , and $S = \text{alg. int. } \{K\}$. Then the trivial result that E has a K -basis of n elements is a consequence of the deeper fact that S is isomorphic (as R -module) to an external direct sum of n ideals of R .

We have already observed in Chapter 2 that if (K, R, k) is a p -modular system, and G is a finite group, then the RG -lattices play an intermediate role in the passage from KG -modules to kG -modules. Thus, given a f.g. KG -module V , we choose an RG -lattice M whose elements span V , and then form the kG -module $\bar{M} = M/PM$, where P is the maximal ideal* of the d.v.r. R . This procedure allows us to define the decomposition map, which is the starting point of modular representation theory.

In another sense, the study of KG -modules and kG -modules is just a first approximation to the investigation of RG -lattices. Indeed, given an RG -lattice M , we first consider the KG -module KM spanned by M . Once this is known,

*In Chapters 3 and 4, we revert to the notation used in §4, and denote a maximal ideal of R by P rather than \mathfrak{p} .

we may then turn to more delicate questions, such as those involving the connections between M and the modules $M/P'M$, $t \geq 1$. For example, it turns out that M is projective RG -lattice if and only if M/PM is a projective kG -module, and that in this case the isomorphism class of M is determined by that of M/PM . On the other hand, a non-projective lattice M is determined by its behavior mod P' for some sufficiently large t .

The general framework of integral representation theory is as follows. Given a KG -module V , we first consider all RG -lattices M in V . By the Jordan-Zassenhaus Theorem, there are finitely many isomorphism classes of such lattices. In the case where $R = \text{alg. int. } \{K\}$, these isomorphism classes are then partitioned into genera by means of congruence properties. Specifically, two RG -lattices M, N spanning V are placed in the same *genus* if for every maximal ideal P of R , the P -adic completions M_P and N_P are $R_P G$ -isomorphic. Equivalently, this occurs if for each P , the lattices M and N mod P' are isomorphic for large enough t . The concept of genus is central to the entire theory, since it leads to a natural generalization of the ideal class group occurring in algebraic number theory. This new class group $\text{Cl } RG$ turns out to be intimately connected with the K -theory of RG , and has important applications to topology, since certain topological invariants have values in this class group.

Next, we note that any KG -submodule W of a KG -module V must be a direct summand of V . The analogous statement fails for RG -lattices, just as it fails for kG -modules if k is a field and $\text{char } k$ divides $|G|$. In studying sublattices L of an RG -lattice M , one often begins by picking out those L 's for which the quotient M/L is also a *lattice* (rather than an arbitrary RG -module). Assuming that both L and M/L are known, it then becomes necessary to study the group $\text{Ext}_{RG}^1(M/L, L)$ which classifies extensions of M/L by L . We shall give a number of examples in which these extension groups are calculated and used to determine all RG -lattices.

Just as the theory of KG -modules depends on the more general theory of modules over semisimple artinian rings, the theory of RG -lattices depends on the more general investigation of lattices over R -orders. Certain R -orders, especially the maximal orders, have special properties which make them easier to handle. One technique, used repeatedly in integral representation theory, is to embed a given R -order Λ in a maximal order Λ' , and then to study Λ -lattices M by first investigating the corresponding Λ' -lattice $\Lambda' M$ spanned by M . This procedure is a refinement of the step from M to KM , and often yields useful information.

The first section of this chapter introduces the concepts of orders acting on lattices, and the following section is devoted to the fundamental Jordan-Zassenhaus Theorem. In Section 25, we consider the technique of forming extensions of one lattice by another, and here the discussion of Ext in §8A will play a basic role. Section 26 deals with maximal orders in separable algebras. In Sections 27 and 28, we concentrate on properties of integral

group rings and their twisted analogues. The chapter concludes with a discussion of projective endomorphisms and annihilators of Ext of a pair of lattices.

In keeping with the spirit of this book, we shall concentrate on general results rather than detailed calculations, although numerous illustrative examples will be given. This chapter inevitably overlaps parts of CR and of “Maximal Orders” (Reiner [75]), and it is not feasible to duplicate here any large part of these earlier works. We shall occasionally list results from these books without proof. These books will hereafter be cited simply as CR and MO, respectively.

§23. LATTICES AND ORDERS

Throughout this section, R denotes a commutative ring (with 1). We shall be primarily interested in the case where R is an integral domain, though much of the discussion below does not require this restriction on R . As in §10D, an R -lattice is a f.g. projective R -module. This terminology is suggested by a geometric example: let $M = \{(a, b) : a, b \in \mathbb{Z}\}$, the set of integral lattice points in the plane; then M is a \mathbb{Z} -lattice relative to componentwise addition of ordered pairs.

Suppose for the time being that R is an integral domain. The torsion submodule of an arbitrary R -module M is defined to be

$$\{m \in M : rm = 0 \text{ for some nonzero } r \in R\}.$$

Call M *torsionfree* if its torsion submodule is 0. Some authors use the terminology “ R -lattice” to mean a f.g. torsionfree R -module. However, we shall keep to our original definition throughout this book.

When R is an integral domain, every free R -module is torsionfree, and therefore every R -lattice is also torsionfree. The converse is not true in general: torsionfree modules need not be lattices. However, for certain types of rings R , a f.g. R -module M is an R -lattice if and only if M is torsionfree. This is the case whenever R is a P.I.D., for example, since then every f.g. torsionfree R -module must have a finite R -basis.

More generally, let R be a Dedekind domain. Then (see §4D) a f.g. R -module is torsionfree if and only if it is R -projective. Thus, when R is a Dedekind domain, every R -lattice is a f.g. torsionfree R -module, and conversely. Since submodules of f.g. torsionfree R -modules are necessarily f.g. torsionfree, it follows (in this case) that submodules of R -lattices are necessarily R -lattices. However, factor modules of lattices need not be lattices, since they may fail to be torsionfree.

Our next task is to motivate the definition of “order” given below. Let R be an arbitrary integral domain, and let Λ be an R -algebra (see §1A). Every Λ -module, including Λ itself, may then be viewed as an R -module, using the

homomorphism from R into the center of Λ . We always take this point of view hereafter, without further comment. Now let M be any left Λ -module, and suppose that as R -module, M is an R -lattice. Let us put

$$I = \{x \in \Lambda : xM = 0\} = \text{annihilator of } M.$$

Define $\bar{\Lambda} = \Lambda/I$, which is obviously an R -algebra acting on M . Indeed, $\bar{\Lambda}$ acts faithfully on M (that is, the $\bar{\Lambda}$ -annihilator of M is 0). For $x \in \Lambda$, let \bar{x} be its image in $\bar{\Lambda}$, and let $\bar{x}_l : M \rightarrow M$ be left multiplication by \bar{x} on M . Since the elements of R commute with those of $\bar{\Lambda}$, it follows that each $\bar{x}_l \in \text{End}_R M$. Furthermore, $\bar{x}_l = 0$ if and only if $\bar{x} = 0$, since $\bar{\Lambda}$ acts faithfully on M . We thus obtain a monomorphism of R -algebras

$$\bar{\Lambda} \rightarrow \text{End}_R M,$$

given by mapping $\bar{x} \in \bar{\Lambda}$ onto \bar{x}_l . Further, since M is R -torsionfree, the ring homomorphism $R \rightarrow$ center of $\bar{\Lambda}$ must be a monomorphism, and thus R is embedded in $\bar{\Lambda}$. Instead of studying the Λ -structure of M , we may equally well study its $\bar{\Lambda}$ -structure.

We may derive some important consequences from the embedding of $\bar{\Lambda}$ into $\text{End}_R M$, and begin by analyzing the R -structure of the latter ring. Since M is an R -lattice, there is an R -isomorphism

$$M \oplus M' \cong R^{(k)}$$

for some k and some R -module M' . Put $E = \text{End}_R R^{(k)} \cong M_k(R)$, and let $e : R^{(k)} \rightarrow M$ be the idempotent projection (see §2A) associated with the above decomposition of $R^{(k)}$. Then there is a *Pierce decomposition*

$$E = eEe \oplus eE(1-e) \oplus (1-e)Ee \oplus (1-e)E(1-e),$$

and we may identify $\text{End}_R M$ with eEe . This shows that $\text{End}_R M$ is (as R -module) a direct summand of the free R -module $M_k(R)$, and therefore $\text{End}_R M$ is an R -lattice.

Suppose now that R is a Dedekind domain. Since $\bar{\Lambda}$ is an R -submodule of $\text{End}_R M$, it follows that $\bar{\Lambda}$ is also an R -lattice. Hence in studying lattices over R -algebras, where R is a Dedekind domain, there is no loss of generality in considering only those R -algebras which are themselves R -lattices, with R embedded in their center.

We now make the following definition:

(23.1) Definition. Let R be a Dedekind domain with field of quotients K . An R -order is a ring Λ whose center contains R , and such that Λ is an R -lattice. (This means that Λ is f.g./ R and R -projective, relative to the action of R on Λ induced by the inclusion of R in the center of Λ .)

Now let Λ be an R -order, where R is a Dedekind domain. Then there is an embedding $\Lambda \rightarrow K \otimes_R \Lambda$, given by $x \mapsto 1 \otimes x$, $x \in \Lambda$. We always identify Λ with its image $1 \otimes \Lambda$ in $K \otimes \Lambda$; this tensor product can then be written as $K \cdot \Lambda$, the K -space spanned by the elements of Λ . Set $A = K \otimes_R \Lambda$; then A is a f.d. K -algebra, and Λ is a subring of A containing a K -basis of A . We call Λ an R -order in A , in accordance with the following:

(23.2) Definition. Let A be a f.d. K -algebra, and let R be a Dedekind domain with field of quotients K . An R -order in A is a subring Λ of A satisfying all of the conditions:

- (i) The center of Λ contains R ,
- (ii) Λ is f.g. as R -module,
- (iii) $K \cdot \Lambda = A$.

(23.3) Examples of R -orders. (i) Let G be a finite group, and let

$$A = KG, \quad \Lambda = RG = \text{integral group ring of } G \text{ over } R.$$

Then Λ is an R -order in A .

(ii) Let L be a finite separable field extension of K , and let R' be the integral closure of R in L . Then by (4.4) R' is an R -order in the K -algebra L . In particular, if L is an algebraic number field, then the ring alg. int. $\{L\}$ is a \mathbb{Z} -order in the \mathbb{Q} -algebra L .

(iii) Let \mathfrak{b} be an ideal of R , and set $A = M_2(K)$, and

$$\Lambda = \begin{pmatrix} R & \mathfrak{b} \\ R & R \end{pmatrix} = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a, c \in R, b, d \in \mathfrak{b} \right\}.$$

Then Λ is an R -order in A .

(iv) Let A be any f.d. K -algebra, and let $\alpha \in A$ be integral over R (see §1A). Then the ring $R[\alpha]$ is an R -order in the commutative K -algebra $K[\alpha]$.

(23.4) Definition. Let Λ be an R -order in a K -algebra A . A Λ -lattice is a (left) Λ -module which is an R -lattice, that is, f.g. and projective as R -module.

Let M be a Λ -lattice, where Λ is an R -order. If M is R -free with a finite R -basis $\{m_1, \dots, m_d\}$, then relative to this basis M affords a matrix representation \mathbf{M} of Λ . For $x \in \Lambda$, let

$$(23.5) \quad xm_j = \sum_{i=1}^d \alpha_{ij} m_i, \quad \alpha_{ij} \in R, \quad 1 \leq j \leq d,$$

and put $\mathbf{M}(x) = (\alpha_{ij}) \in M_d(R)$. The map $x \rightarrow \mathbf{M}(x)$, $x \in \Lambda$, is then a representation of Λ by means of matrices with entries in R . We call \mathbf{M} an *integral representation* or *R-representation* of Λ .

In order to describe how a change of R -basis of M affects the matrix representation \mathbf{M} , it is convenient to write the R -basis $\{m_i\}$ as a formal row vector $\mathbf{m} = (m_1, \dots, m_d)$. Then (23.5) may be rewritten as

$$x\mathbf{m} = \mathbf{m}\mathbf{M}(x), \quad x \in \Lambda.$$

Let $\{m'_1, \dots, m'_d\}$ be another free R -basis for M , and put $\mathbf{m}' = (m'_1, \dots, m'_d)$. We may write $\mathbf{m}' = \mathbf{m}\mathbf{P}$ for some matrix $\mathbf{P} \in GL_d(R)$. For $x \in \Lambda$, we have

$$x\mathbf{m}' = x\mathbf{m}\mathbf{P} = \mathbf{m}\mathbf{M}(x)\mathbf{P} = \mathbf{m}' \cdot \mathbf{P}^{-1}\mathbf{M}(x)\mathbf{P}.$$

Thus, change of R -basis of M has the effect of replacing \mathbf{M} by the *equivalent representation* $\mathbf{P}^{-1}\mathbf{M}\mathbf{P}$.

We may equally well start with an R -representation \mathbf{M} of an R -order Λ ; by definition, \mathbf{M} is an R -algebra homomorphism of Λ into a matrix ring $M_d(R)$, and d is called the *degree* of the representation. Let M be the free R -module consisting of all $d \times 1$ column vectors over R ; then M affords the representation \mathbf{M} of Λ , relative to the basis $\{m_1, \dots, m_d\}$, where m_i is the column vector with 1 at position i , and zeros elsewhere.

(23.6) Example. Let

$$G = \langle a, b : a^4 = 1, b^2 = 1, bab^{-1} = a^{-1} \rangle$$

be the dihedral group of order 8, and let $\Lambda = \mathbb{Z}G$ be its integral group ring. Then Λ is a \mathbb{Z} -order in the \mathbb{Q} -algebra $\mathbb{Q}G$. Let \mathbf{M}_i ($i = 1, 2$) be the \mathbb{Z} -representation of Λ defined by setting

$$\mathbf{M}_1(a) = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad \mathbf{M}_1(b) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix};$$

$$\mathbf{M}_2(a) = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad \mathbf{M}_2(b) = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

It is easily checked that

$$\mathbf{M}_i(a)^4 = 1, \quad \mathbf{M}_i(b)^2 = 1, \quad \mathbf{M}_i(bab^{-1}) = \mathbf{M}_i(a^{-1}), \quad i = 1, 2,$$

so \mathbf{M}_1 and \mathbf{M}_2 are \mathbb{Z} -representations of Λ (and of the group G). However, \mathbf{M}_1 is not \mathbb{Z} -equivalent to \mathbf{M}_2 , since there is no matrix $\mathbf{P} \in GL_2(\mathbb{Z})$ for which

$$\mathbf{P}^{-1}\mathbf{M}_1(a)\mathbf{P} = \mathbf{M}_2(a), \quad \mathbf{P}^{-1}\mathbf{M}_1(b)\mathbf{P} = \mathbf{M}_2(b).$$

As in (23.2), let Λ be an R -order in a K -algebra A , and let M be any Λ -lattice. Then as in §4D, we may embed M in the finite dimensional K -space $K \otimes_R M$. We may denote this space by KM , after the usual identification of M with $1 \otimes M$. Then KM is a f.g. left A -module. In practice, we usually have a great deal of information about the A -module KM , and the difficulty arises in trying to classify the full Λ -lattices contained in KM . (Recall that a *full* Λ -lattice in an A -module V is a Λ -lattice M in V such that $KM = V$.)

We wish to set up a correspondence between A -submodules of the f.g. A -module V and the sublattices of a full Λ -lattice M in V . Just as in §4D, the key concept is that of *purity*. A Λ -sublattice L of M is called R -*pure* in M if M/L is R -torsionfree, or equivalently, if L is an R -direct summand of M . As in (4.12), we have:

(23.7) Proposition. *Let R be a Dedekind domain with field of quotients K , and let Λ be an R -order in the f.d. K -algebra A . Let M be a full Λ -lattice in the left A -module V . There is an inclusion-preserving bijection $N \leftrightarrow W$, where N ranges over all R -pure Λ -sublattices of M , and W ranges over all A -submodules of V . The bijection is given explicitly by*

$$N = M \cap W, \quad W = KN.$$

Further, for each such W , the quotient $M/(M \cap W)$ is a full Λ -lattice in the A -module V/W .

The existence of the desired bijection follows readily from (4.12). Furthermore, for each W the Λ -sublattice $M \cap W$ is R -pure in M , whence $M/(M \cap W)$ is R -torsionfree, and is therefore a Λ -lattice. Clearly

$$K \otimes_R \{M/(M \cap W)\} \cong KM/K(M \cap W) = V/W,$$

as asserted. In the discussion below, we shall deduce this proposition, as well as (4.12), as a special case of a more general result which is of interest in itself, and will be useful later.

Let R be an arbitrary commutative ring, and S any multiplicative subset of R (see §4A). Let $S^{-1}R$ denote the ring of quotients of R with respect to S . Likewise, for each R -module M we may form the module of quotients $S^{-1}M$, which we always identify with $S^{-1}R \otimes_R M$ (as in §4A). There is then an R -homomorphism

$$(23.8) \quad i: M \rightarrow S^{-1}R \otimes_R M = S^{-1}M,$$

given by $m \mapsto 1 \otimes m = m/1$, $m \in M$. The kernel of i is precisely the S -torsion submodule of M .

We wish to establish a connection between the R -submodules of M and the $S^{-1}R$ -submodules of $S^{-1}M$, and begin with a definition which generalizes the earlier concept of purity:

(23.9) Definition. Let S be a multiplicative subset of the commutative ring R , and let $L \subseteq M$ be an inclusion of R -modules. Call L an S -saturated submodule of M if M/L is S -torsionfree, or equivalently, if

$$sm \in L, s \in S, m \in M \Rightarrow m \in L.$$

(23.10) Proposition. Let M be an R -module, and let $i: M \rightarrow S^{-1}M$ be the canonical R -homomorphism defined in (23.8). Then there is an inclusion-preserving bijection $L \leftrightarrow X$ between the set of S -saturated R -submodules L of M , and the set of $S^{-1}R$ -submodules X of $S^{-1}M$, given by

$$X = S^{-1}L, L = i^{-1}(X).$$

Proof. Starting with any S -saturated $L \subseteq M$, put $X = S^{-1}L$, an $S^{-1}R$ -submodule of $S^{-1}M$. Clearly, $L \subseteq i^{-1}(X)$, and we must prove equality. If $m \in M$ is such that $i(m) \in X$, then we may write

$$m/l = l/s \text{ for some } l \in L, s \in S.$$

Hence $s'sm = s'l$ for some $s' \in S$, so $s'sm \in L$. Since L is S -saturated in M , it follows that $m \in L$. This completes the proof that $L = i^{-1}(S^{-1}L)$.

Conversely, given an $S^{-1}R$ -submodule X of $S^{-1}M$, define $L = i^{-1}(X)$. Then L is an R -submodule of M , and clearly $S^{-1}L \subseteq X$. We claim that equality holds; indeed, given $x \in X$ we may write $x = m/s$, $m \in M$, $s \in S$. Then also $m/1 \in X$, whence $m \in L$, so $x \in S^{-1}L$. This shows that $S^{-1}L = X$. Finally, we verify that L is S -saturated in M . If $sm \in L$, where $s \in S$ and $m \in M$, then $sm/1 \in X$. Therefore $m/1 \in X$, so $m \in L$, as desired. This completes the proof.

(23.11) Corollary. Keep the above notation. If M is a noetherian R -module, then $S^{-1}M$ is a noetherian $S^{-1}R$ -module. If R is a noetherian ring, so is $S^{-1}R$. The corresponding results hold when “noetherian” is replaced by “artinian”.

Suppose now that Λ is an R -algebra, where R is any commutative ring, and let S be a multiplicative subset of R . Define

$$S^{-1}\Lambda = S^{-1}R \otimes_R \Lambda,$$

which is clearly an $S^{-1}R$ -algebra. Each left Λ -module M gives rise to an $S^{-1}\Lambda$ -module $S^{-1}M$, and clearly

$$S^{-1}M = S^{-1}R \otimes_R M \cong S^{-1}\Lambda \otimes_{\Lambda} M.$$

If M is f.g./ R , then $S^{-1}M$ is f.g./ $S^{-1}R$. If M is R -projective, then $S^{-1}M$ is $(S^{-1}R)$ -projective; this follows at once from the fact that if M is R -free, then $S^{-1}M$ is $S^{-1}R$ -free. In particular, if M is any Λ -lattice then $S^{-1}M$ is an $S^{-1}\Lambda$ -lattice.

As an immediate consequence of (23.10), we obtain:

(23.12) Proposition. *Let S be a multiplicative subset of the commutative ring R , and let Λ be any R -algebra. Let M be a left Λ -module. Then there is an inclusion-preserving bijection $L \leftrightarrow X$ between the set of S -saturated Λ -submodules L of M , and the set of $S^{-1}\Lambda$ -submodules X of $S^{-1}M$. This bijection is given by*

$$X = S^{-1}L, L = i^{-1}(X) = \{m \in M : m/1 \in X\}.$$

We have seen above that each Λ -module M gives rise to an $S^{-1}\Lambda$ -module $S^{-1}M$. We may ask, conversely, whether every $S^{-1}\Lambda$ -module can be obtained in this way. For our purposes, it will suffice to restrict our attention to f.g. modules. The following result, extremely useful in practice, settles the above question completely:

(23.13) Proposition. *Let S be a multiplicative subset of the commutative ring R , and let Λ be any R -algebra. Then each f.g. left $S^{-1}\Lambda$ -module X contains a f.g. left Λ -module M such that*

$$S^{-1}\Lambda \otimes_{\Lambda} M \cong S^{-1}R \otimes_R M \cong (S^{-1}R) \cdot M = X,$$

where $(S^{-1}R) \cdot M$ is computed inside X .

Proof. The canonical ring homomorphism $\Lambda \rightarrow S^{-1}\Lambda$ is not necessarily an injection, but it nevertheless allows us to view each $S^{-1}\Lambda$ -module X as a Λ -module. Each $x \in X$ then generates a Λ -submodule Λx of X . Now let $X = \sum_{i=1}^k S^{-1}\Lambda x_i$, and choose $M = \sum \Lambda x_i \subseteq X$. Clearly $X = (S^{-1}R) \cdot M$, and we need only show that the surjection

$$f: S^{-1}R \otimes_R M \rightarrow (S^{-1}R) \cdot M$$

is injective. For this purpose, it suffices to define a map $g: (S^{-1}R)M \rightarrow S^{-1}R \otimes_R M$ for which gf is the identity map. In order to define g , we note that each element $y \in (S^{-1}R)M$ is of the form $y = s^{-1}m$ with $s \in S$, $m \in M$. Let us set

$$g(y) = s^{-1} \otimes m \in S^{-1}R \otimes_R M.$$

If also $y = t^{-1}n$ with $t \in S$, $n \in M$, then $s^{-1}m = t^{-1}n$ in X . Therefore $tm = sn$ in M , and so

$$s^{-1} \otimes m = (st)^{-1}t \otimes m = (st)^{-1} \otimes tm = (st)^{-1} \otimes sn = t^{-1} \otimes n.$$

This proves that g is well defined, and it is obvious that gf is the identity map, so the proof is complete.

Let us apply this machinery to the study of orders. Suppose now that R is a Dedekind domain with quotient field K , and let Λ be an R -order in A . Given a multiplicative subset S of R , we may form the $S^{-1}R$ -algebra $S^{-1}\Lambda$. Clearly

$$K \otimes_{S^{-1}R} S^{-1}\Lambda = K \otimes_{S^{-1}R} (S^{-1}R \otimes_R \Lambda) \cong K \otimes_R \Lambda = A,$$

so $S^{-1}\Lambda$ is a subring of A which spans A over K . Further, $S^{-1}\Lambda$ is f.g./ $S^{-1}R$, and $S^{-1}R$ is contained in the center of $S^{-1}\Lambda$. Thus, $S^{-1}\Lambda$ is an $S^{-1}R$ -order in A . We note that the canonical map $\Lambda \rightarrow S^{-1}\Lambda$ is an injection, since Λ is S -torsionfree. Each Λ -module M gives rise to an $S^{-1}\Lambda$ -module $S^{-1}M$. The remarks preceding (23.12) show that if M is a Λ -lattice, then $S^{-1}M$ is an $S^{-1}\Lambda$ -lattice.

In the special case where $S=R-\{0\}$, we note that a Λ -sublattice L of a Λ -lattice M is S -saturated in M if and only if L is an R -pure submodule of M . It follows at once that (23.7) is a special case of Proposition 23.12. Furthermore, from (23.13) we obtain:

(23.14) Corollary. *Let Λ be an R -order, where R is a Dedekind domain with quotient field K , and let S be any multiplicative subset of R . Then each $S^{-1}\Lambda$ -lattice X contains a Λ -lattice M such that*

$$S^{-1}M \cong (S^{-1}\Lambda) \cdot M = X.$$

Proof. The $S^{-1}\Lambda$ -lattice X is $S^{-1}R$ -torsionfree, hence certainly R -torsionfree. The Λ -module M constructed in the proof of (23.13) is f.g. and torsionfree as R -module, and is therefore a Λ -lattice, as desired.

Even the special case of the above, in which $S=R-\{0\}$, is extremely useful. From (23.7) and (23.14), we obtain:

(23.15) Corollary. *Let Λ be an R -order in the K -algebra A . Then every f.g. left A -module V is of the form $V = K \cdot M$ for some full Λ -lattice M in V . Further, for each A -submodule W of V , $M/(M \cap W)$ is a full Λ -lattice in V/W .*

Let us derive several important consequences of this rather simple result. We begin with:

(23.16) Proposition. *Let R be a P.I.D. with field of quotients K , and let Λ be an R -order in a K -algebra A . Let V be a f.g. left A -module. Then V has a K -basis, relative to which each $x \in \Lambda$ is represented by a matrix over R . In short, every K -representation of Λ is equivalent to an R -representation of Λ .*

Proof. We may write $V = K \cdot M \cong K \otimes_R M$ for some full Λ -lattice M in V . Since R is a P.I.D., M has a free R -basis $\{m_1, \dots, m_d\}$. This is also a K -basis of V . Relative to this basis, we obtain an R -representation of Λ as in (23.5). This completes the proof.

Even when R is not a principal ideal domain, it is sometimes possible to choose an R -free Λ -lattice spanning a given A -module. In order to determine whether a given Λ -lattice M is R -free, we can use Steinitz's Theorem 4.13 on the structure of R -lattices. Specifically, we may express M as an external direct sum of (nonzero) ideals of R , say $M = \coprod_{i=1}^d J_i$. Then M is R -free if and only if the product $J_1 \cdots J_d$ is a *principal ideal* (that is, an ideal of the form Rx for some nonzero $x \in K$.) If M is not R -free, we may let J be an arbitrary ideal of R , and form the Λ -lattice JM . Clearly

$$JM = \coprod_{i=1}^d JJ_i,$$

and JM will be R -free if and only if $\prod_{i=1}^d JJ_i$ is a principal ideal, that is, if and only if the ideal $J^d \cdot \prod_{i=1}^d J_i$ is principal. We use this to prove a beautiful theorem due to Schur, which generalizes the preceding proposition.

(23.17) Theorem (Schur). *Let R be a Dedekind domain with field of quotients K , and suppose that the ideal class number h of R is finite. Let Λ be an R -order in a K -algebra A , and let V be a f.g. left A -module with $\dim_K V = d$. Assume that d is relatively prime to h . Then V contains an R -free full Λ -lattice M . If $\{m_1, \dots, m_d\}$ is a free R -basis for M , it is also a K -basis of V . Relative to this basis, V affords an R -representation of Λ .*

Proof. By (23.15), V contains a full Λ -lattice M . As pointed out in the discussion preceding the theorem, we may write $M = \coprod_{i=1}^d J_i$, and it suffices to find an R -ideal J such that $J^d \cdot \prod_{i=1}^d J_i$ is principal. But $(d, h) = 1$, so as J ranges over a full set of ideal class representatives, so does J^d . Hence we can choose J so that $J^d \cdot \prod_{i=1}^d J_i$ is a principal ideal, and the proof is finished.

Let us show by example that we cannot omit the hypothesis that $(h, d) = 1$. Let R be a Dedekind domain whose class number h is greater than 1, and let $V \cong K^{(h)}$, $A = \text{End}_K(V)$, so we view V as an (A, K) -bimodule. Pick any full R -lattice M in V , and let $\Lambda = \text{End}_R(M)$. Then M is a (Λ, R) -bimodule, and is a full Λ -lattice in V . Let us show that for any other full Λ -lattice N in V , we have $N = Ma$ for some nonzero R -ideal a in K .

Let P range over the maximal ideals of R , and let the subscript P denote localization. Then $\Lambda_P = \text{End}_{R_P}(M_P)$, and M_P is R_P -free on h generators. Hence Λ_P is a maximal R_P -order in A (see MO, (8.7)). But then $M_P \cong N_P$ as Λ_P -lattices by MO (18.7), and this isomorphism extends to an A -automorphism of V . However, $\text{End}_A(V) \cong K$, so there exists a nonzero element $\alpha_P \in K$ such that $N_P = M_P \alpha_P$. Further $N_P = M_P$ a.e., so we may choose $\alpha_P = 1$ a.e. We now let a be the R -ideal of K for which $a_P = R_P \alpha_P$ for each P ; explicitly, choose $a = \bigcap_P R_P \alpha_P$, an ideal with the desired properties

by (4.21vii). Then $M\alpha$ is a left Λ -lattice in V such that $(M\alpha)_P = N_P$ for all P , whence $M\alpha = N$ by (4.21vi).

Now let M be chosen so that M is *not* R -free; for example, let $V = \bigoplus_1^h Kv_i$ and pick

$$M = \bigoplus_1^{h-1} Rv_i \oplus qv_h,$$

where q is some non-principal ideal of R . Then we claim that V does not contain full R -free Λ -lattices. Indeed, any Λ -lattice N in V is of the form $N = M\alpha$, with α an R -ideal in K . The Steinitz class of N is the ideal class of $\alpha^h q$; but α^h is principal, since h is the ideal class number of R . Hence the Steinitz class of N is not the principal class, and so N cannot be R -free. Thus we see that if $\Lambda = \text{End}_R(M)$, where M is any non- R -free lattice, then the A -module V cannot contain an R -free Λ -lattice N for which $K \cdot N = V$.

The preceding example shows that when Λ is an R -order, where R is *not* a P.I.D., then there exist K -representations of Λ which are not K -equivalent to R -representations. There are several ways of overcoming this difficulty, in practice. One procedure, followed in Chapter 2, is to work over d.v.r.'s rather than arbitrary Dedekind domains. This is an especially useful approach, since a d.v.r. is even easier to handle than an arbitrary P.I.D. A second procedure, used repeatedly in integral representation theory, is to study a Λ -lattice M by investigating its localizations M_P , with P ranging over the maximal ideals of R . Since R_P is a d.v.r., every Λ_P -lattice necessarily has an R_P -basis.

To conclude this section, we consider yet another approach, that of ground ring extension. Let Λ be an R -order, where R is an arbitrary Dedekind domain. We hope to find an extension field K' of K , with ring of integers R' , such that every K -representation of Λ is K' -equivalent to an R' -representation of Λ . This can always be done when R has finite class number, as we now show:

(23.18) Theorem. *Let R be a Dedekind domain whose class number h is finite, and let K be its field of quotients. Then there exists an extension field K' of K with $\dim_K K' \leq h$, such that for each R -order Λ , every K -representation of Λ is K' -equivalent to an R' -representation of Λ , where R' is the integral closure of R in K' .*

Proof. Let $A = K\Lambda$, and let V be a f.g. A -module affording a K -representation of Λ . If V happens to contain an R -free full Λ -lattice, then of course the K -representation of Λ is K -equivalent to an R -representation. However, V need not contain such a Λ -lattice, so instead we consider the K' -representation of Λ afforded by the K' -space $K' \otimes_K V$. Denote this space by $K'V$, after the obvious identification of V with $1 \otimes V$. We must show that (with suitably chosen K'), the space $K'V$ contains an R' -free Λ -module.

To begin with, we may choose K' so that $\dim_K K' \leq h$, and such that each R -ideal α of K generates a principal R' -ideal of K' (that is, $R'\alpha = R'\alpha$ for some $\alpha \in R'$); this is proved in CR(20.14), and we shall not repeat the proof here. Note that K' is chosen once and for all, independently of the order Λ . Now let M be a full Λ -lattice in V (see (23.15)). By Steinitz's Theorem 4.13, we have

$$M = \bigoplus_{i=1}^n \alpha_i m_i, \quad n = \dim_K V,$$

where each α_i is an R -ideal in K , and each $m_i \in M$. Then in $K'V$ we have

$$R' \otimes_R M = \bigoplus_{i=1}^n (R'\alpha_i)m_i = \bigoplus_{i=1}^n (R'\alpha_i)m_i$$

for some elements $\{\alpha_i\}$ of K' . Thus $K'V$ contains an R' -free Λ -module. Relative to the basis $\{\alpha_1 m_1, \dots, \alpha_n m_n\}$, $K'V$ affords an R' -representation of Λ . This completes the proof.

Remark. If K is an algebraic number field, it is known from class field theory that there exists a finite Galois extension K' of K , whose Galois group is isomorphic to the ideal class group of R (and hence is abelian), such that every ideal of R generates a principal ideal of R' . For this abelian extension K' of K , we have $\dim_K K' = h$. The above proof shows that every representation of Λ by matrices over K is K' -equivalent to a representation by matrices over R' .

§23. Exercises

Throughout, let R be a Dedekind domain with field of quotients K , and let A be a f.d. K -algebra.

- Let Λ be an R -order in a semisimple K -algebra A , and let M be a left Λ -lattice. Show that M can be embedded in a free left Λ -module with a finite basis.

[Hint: The left A -module KM is a direct summand of a free module $A^{(k)}$ for some finite k , since A is semisimple. There are embeddings $M \rightarrow KM$, $KM \rightarrow A^{(k)}$. Hence there is an embedding $M \rightarrow K \cdot \Lambda^{(k)}$, and then $\alpha M \subseteq \Lambda^{(k)}$ for some nonzero $\alpha \in R$.]

- Let $\Lambda \subseteq \Gamma$ be R -orders in A . Each Γ -lattice is also a Λ -lattice. Show that for any Γ -lattices M and N ,

$$\text{Hom}_\Gamma(M, N) = \{f \in \text{Hom}_A(KM, KN) : f(M) \subseteq N\} = \text{Hom}_\Lambda(M, N).$$

Deduce that $M \cong N$ as Γ -lattices if and only if $M \cong N$ as Λ -lattices. Show that M is indecomposable as Γ -lattice if and only if M is indecomposable as Λ -lattice.

3. Let Λ be an R -order in A , and M a full left Λ -lattice in a f.g. left A -module V . Given an A -composition series for V :

$$V = V_0 \supset V_1 \supset \cdots \supset V_n = 0,$$

put $M_i = M \cap V_i$, $0 \leq i \leq n$. Using (23.15), show that the decreasing chain of Λ -lattices

$$M = M_0 \supset M_1 \supset \cdots \supset M_n = 0$$

has the following properties:

(i) For each i , M_i is a full Λ -lattice in V_i .

(ii) For each i , the factor module M_{i-1}/M_i is a full Λ -lattice in the A -module V_{i-1}/V_i .

4. Keep the above notation; the factor modules $\{M_{i-1}/M_i : 1 \leq i \leq n\}$ are called the R -composition factors of the lattice M . Show that when R is not a field, these are *never* composition factors of the Λ -module M in the usual sense. Show further that the R -composition factors of M are not necessarily uniquely determined up to isomorphism and order of occurrence.

[Hint: See CR (73.28).]

5. Let Λ be an R -order in A , and suppose that for each simple A -module V , all full Λ -lattices in V are mutually isomorphic. (This condition is satisfied, for instance, when R is a d.v.r. and Λ is a maximal R -order in a f.d. separable K -algebra A ; see MO (18.10).) Show that for each Λ -lattice M , the R -composition factors of M are uniquely determined (up to isomorphism and order of occurrence).

6. Let V be a f.g. left A -module with no repeated A -composition factors, and let M be a full Λ -lattice in V . Let $\{N_1, \dots, N_i\}$ and $\{N'_1, \dots, N'_i\}$ be two sets of R -composition factors of M , and assume that $KN_i \cong KN'_i$ for each i . Show that $N_i \cong N'_i$ for each i .

[Hint: See CR (73.13).]

7. Let $\Lambda \subset \Gamma$ be any pair of R -orders in a f.d. K -algebra A . Show that the map $\Gamma \otimes_{\Lambda} \Gamma \rightarrow \Gamma$, given by $x \otimes y \mapsto xy$, need not be a monomorphism. This provides an example of a left Λ -lattice M for which $\Gamma \otimes_{\Lambda} M$ is not isomorphic to the product ΓM computed inside KM .

[Hint: Let I be a two-sided Γ -ideal in Λ such that $K \cdot I = A$, and set $\bar{\Lambda} = \Lambda/I$, $\bar{\Gamma} = \Gamma/I$. There is a left Λ -homomorphism $\theta: \Gamma \otimes_{\Lambda} \Gamma \rightarrow \bar{\Gamma} \otimes_{\bar{\Lambda}} (\Gamma/\Lambda)$, given by $x \otimes y \mapsto \bar{x} \otimes \bar{y}$. For $x \in \Gamma - \Lambda$ we have

$$\theta(1 \otimes x - x \otimes 1) = \bar{1} \otimes \bar{x} - \bar{x} \otimes \bar{1} = \bar{1} \otimes \bar{x},$$

since $\bar{x} \otimes \bar{1} = 0$ in Γ/Λ because $1 \in \Lambda$. But $1 \otimes x - x \otimes 1 \in \Gamma \otimes \Gamma$ is an element with image 0 in Γ , so it suffices to choose $x \in \Gamma - \Lambda$ with $\bar{1} \otimes \bar{x} \neq 0$ in $\bar{\Gamma} \otimes_{\bar{\Lambda}} (\Gamma/\Lambda)$. Now the map $\bar{\Lambda} \otimes (\Gamma/\Lambda) \rightarrow \bar{\Gamma} \otimes (\Gamma/\Lambda)$ is monic whenever Γ/Λ is $\bar{\Lambda}$ -flat, and in this case any

$x \in \Gamma - \Lambda$ will work. Thus, it suffices to give an example where $\bar{\Lambda}$ is a field. Take $\Gamma = \mathbb{Z}[a]$, $\Lambda = \mathbb{Z}[2a]$, $I = 2\Gamma$ where $a = \sqrt{3}$. Then $\bar{\Lambda} = \Lambda/I = (\mathbb{Z} \oplus 2a\mathbb{Z})/(2\mathbb{Z} \oplus 2a\mathbb{Z}) \cong \mathbb{Z}/2\mathbb{Z}$. This exercise is due to J. Rotman.]

8. Keep the notation of Exercise 7, and let M be a Λ -lattice. Let

$$\mu: \Gamma \otimes_{\Lambda} M \rightarrow \Gamma M$$

be the Γ -homomorphism defined by $\gamma \otimes m \mapsto \gamma m \in \Gamma M$, where ΓM is calculated inside KM . Find $\ker \mu$.

[Hint: There is an exact sequence $0 \rightarrow \Gamma \rightarrow A \rightarrow T \rightarrow 0$, with T an R -torsion Λ -module. Then

$$\text{Tor}(A, M) \xrightarrow{\varphi} \text{Tor}(T, M) \rightarrow \Gamma \otimes M \xrightarrow{\psi} A \otimes M$$

is exact, where Tor is Tor_1^{Λ} and \otimes is \otimes_{Λ} . We have $\text{im } \psi = \text{im } \mu$, and $\text{im } \varphi = 0$ since $\text{Tor}(A, M)$ is divisible whereas $\text{Tor}(T, M)$ is an R -torsion module. Thus $\ker \mu \cong \text{Tor}(T, M)$.]

9. Let L be a finite separable extension of K , and let S be the integral closure of R in L . Let Λ be an S -order in a f.d. L -algebra A . Then Λ is also an R -order in A . Show that Λ -lattices relative to S are also Λ -lattices relative to R , and conversely.

[Hint: It suffices to show that an R -torsionfree Λ -module M is necessarily S -torsionfree. Suppose that $s \in S$, $m \in M$, and that $sm = 0$ but $s \neq 0$. By Exercise 1.2, we may choose $s' \in S$ so that $s's = N_{L/K}(s)$. Then $s's \in R$, $s's \neq 0$, and $s'sm = 0$, which implies that $m = 0$ since M is R -torsionfree.]

§24. JORDAN-ZASSENHAUS THEOREM

Throughout this section, let R be a Dedekind domain with quotient field K . If K is a global field (either an algebraic number field or a function field, as described in §4F), then the number of classes of R -ideals in K is finite. The Jordan-Zassenhaus Theorem stated below is a strong generalization of this fact, and it is proved by arguments analogous to those used for global fields. Instead of R -ideals in K , we consider full Λ -lattices in some given f.g. left A -module. Here, Λ is an R -order in a semisimple f.d. K -algebra A . Further, instead of ideal classes we consider isomorphism classes of Λ -lattices. The fundamental result is as follows:

(24.1) Jordan-Zassenhaus Theorem. *Let R be a Dedekind ring whose field of quotients K is a global field. Let A be a finite dimensional semisimple K -algebra, and let Λ be an R -order in A . Then for each f.g. left A -module V , there are only a finite number of isomorphism classes of left Λ -lattices M such that $KM \cong V$.*

We shall omit the proof, which is given in detail in MO §26. Another version of the proof is given in CR §79 for the special case where K is an algebraic number field.

It is often useful to state (24.1) in a somewhat different form. If $KM \cong V$, we may replace M by its isomorphic image in V ; it thus suffices to consider full Λ -lattices lying in a given f.g. A -module V . Recall from §4D that the dimension $\dim_K KM$ is called the *R-rank* of M . Let $t > 0$. Since A is semisimple (by hypothesis), there are only finitely many isomorphism classes of A -modules V such that $\dim_K V \leq t$. Thus we have the following equivalent formulation of (24.1):

(24.2) Theorem. *Keep the notation and hypotheses of (24.1). Then for each $t > 0$, there are only finitely many isomorphism classes of left Λ -lattices whose R-rank is at most t .*

We are going to prove that if A is *not* semisimple, and if $R \neq K$, then for each R -order Λ in A there are infinitely many non-isomorphic full left Λ -lattices in A . Thus (assuming that R is not a field), the hypothesis that A be semisimple cannot be omitted from the statement of the Jordan-Zassenhaus Theorem.

By way of preparation, let us give a definition which will be useful in other contexts as well.

(24.3) Definition. Let M be a full R -lattice in a f.d. K -algebra A . The *left order* of M is defined as

$$O_l(M) = \{x \in A : xM \subseteq M\}.$$

The *right order* of M is defined as

$$O_r(M) = \{x \in A : Mx \subseteq M\}.$$

(Some authors call $O_l(M)$ the *left multiplier ring* of M .)

Clearly $O_l(M)$ is an R -module, and is a subring of A whose center contains R . To show that $O_l(M)$ is an R -order in A , we must check that $O_l(M)$ is a full R -lattice in A . For each $x \in A$, xM is an R -lattice in A (though not necessarily a full lattice in A); hence there exists a nonzero $r \in R$ such that $r \cdot xM \subseteq M$. Thus $rx \in O_l(M)$, which proves that $K \cdot O_l(M) = A$. Next, there exists a nonzero $s \in R$ such that $s \cdot 1_A \in M$, where 1_A is the identity element of A . Then $O_l(M) \cdot (s \cdot 1_A) \subseteq M$, so $O_l(M) \subseteq s^{-1}M$. Since R is noetherian and $s^{-1}M$ is f.g./ R , it follows that $O_l(M)$ is also f.g./ R . Thus $O_l(M)$ is a full R -lattice in A , and is therefore an R -order in A . Likewise, $O_r(M)$ is an R -order in A .

In particular, if Λ is an R -order in A , then by Exercise 24.4

$$O_t(\Lambda) = O_r(\Lambda) = \Lambda.$$

These concepts play a crucial role in the following result of Faddeev [65a] (see also Roggenkamp and Huber-Dyson [70, pp. 201–202]):

(24.4) Proposition. *Let A be a non-semisimple f.d. K -algebra. Let Λ be an R -order in A , where R is a Dedekind domain but not a field. Then there exists a strictly increasing infinite chain of full left Λ -lattices in A , no two of which are isomorphic.*

Proof. Since A is (left) artinian and not semisimple, it follows from (5.15) and (5.18) that $\text{rad } A$ is a nonzero nilpotent ideal of A . Hence there exists an integer $n \geq 1$ such that

$$(\text{rad } A)^n \neq 0, (\text{rad } A)^{n+1} = 0.$$

Since $R \neq K$, there exists a nonzero element $r \in R$ such that $r^{-1} \notin R$. We now put

$$L_i = \Lambda \cap (\text{rad } A)^i, i \geq 1.$$

Then each L_i is an R -pure Λ -sublattice of Λ , by (23.7). We now define

$$\Lambda_t = \Lambda + r^{-t}L_1 + r^{-2t}L_2 + \cdots + r^{-nt}L_n, t \geq 1.$$

From the fact that $L_i L_j \subseteq L_{i+j}$, for $i, j \geq 1$, it follows readily that each Λ_t is an R -order in A . Further, since $L_i \subseteq r^{-1}L_i$ for each i , we obtain an increasing sequence

$$(24.5) \quad \Lambda = \Lambda_0 \subseteq \Lambda_1 \subseteq \Lambda_2 \subseteq \cdots.$$

We prove next that each inclusion is strict. Suppose to the contrary that $\Lambda_t = \Lambda_{t+1}$ for some t . Multiplying by $r^{(t+1)n}$, we find that $L_n \subseteq r^t \Lambda$. Therefore

$$L_n \subseteq r^t \Lambda \cap (\text{rad } A)^n = r^t (\Lambda \cap (\text{rad } A)^n) = r^t L_n.$$

Thus $L_n = r^t L_n$, which is impossible since r^t is a nonunit of R and L_n is an R -lattice (see Exercise 24.3). Thus the chain of Λ_t 's is strictly increasing, as claimed.

We have shown that each Λ_t is an R -order in A , and is hence a full Λ -lattice in A . We claim that no two of the $\{\Lambda_t\}$ are Λ -isomorphic. Indeed, if $\Lambda_i \cong \Lambda_j$ as left Λ -modules, then by (2.39) this isomorphism extends to an isomorphism $A \cong A$ as left A -modules. Such an isomorphism must be given by right multiplication by some unit $x \in A$, and so $\Lambda_i = \Lambda_j x$. But then (see

Exercise 24.4)

$$\Lambda_i = O_t(\Lambda_i) = O_t(\Lambda_j x) = \Lambda_j,$$

so $i=j$. Thus (24.5) is the desired chain of full Λ -lattices in A , no two of which are isomorphic.

(24.6) Corollary. *Keep the hypotheses of (24.4). Then every R -order Λ is strictly contained in a larger R -order in A .*

Proof. Use the notation of the proof of (24.4). We have shown that $\Lambda \subset \Lambda_1$, and that Λ_1 is also an R -order in A .

There is also a local version of the Jordan-Zassenhaus Theorem, as follows:

(24.7) Theorem. *Let R be a complete d.v.r. whose field of quotients K is the completion of a global field with respect to some non-archimedean valuation. Let Λ be an R -order in a semisimple f.d. K -algebra A . Then for each $t > 0$, there are only finitely many isomorphism classes of left Λ -lattices whose R -rank is at most t .*

This result can be proved in exactly the same manner as the global version (24.1). Indeed, the local result is somewhat simpler, and follows from MO §26 or CR §79 by slightly modifying the proofs given in these references. It should also be observed that the result follows directly from Maranda's Thoerem 30.14, assuming that A is a separable K -algebra (see Remark (ii) of 30.15).

Notes. (1) For a proof of (24.1) when K is a function field, see also Higman-MacLaughlin [59].

(2) If K is not a global field, the Jordan-Zassenhaus Theorem need not hold for Λ -lattices. Even when R is a complete d.v.r., there exist counterexamples in case R has infinite residue class field. For example, see Roggenkamp [70].

(3) Plesken [77] considers the number of classes of full RG -lattices in an absolutely simple KG -module V , in the case where K is arbitrary and $\text{char } K \nmid |G|$. He proves that this number is finite if and only if R has finite class number.

§24. Exercises

- Let Λ be an R -order in a semisimple K -algebra A . Show that the left class number of Λ equals the right class number of Λ . In other words, let \mathcal{L} be the set of “fractional” left ideals of Λ , that is, the set of all full left Λ -lattices in A . Let \mathcal{R} be the set of all fractional right ideals. Then show that there is a bijection between the set of Λ -isomorphism classes in \mathcal{L} and the corresponding set for \mathcal{R} .

[Hint: For each $L \in \mathcal{L}$, let $L^* = \text{Hom}_R(L, R)$, viewed as right Λ -lattice. Then $K \otimes_R L^* = \text{Hom}_K(A, K)$, and

$$\text{Hom}_K(A, K) \cong A_A$$

since A is a Frobenius algebra over K (see (9.8)). Thus we may identify L^* with a full right Λ -lattice in A . Since $L \cong (L^*)^*$, the correspondence $L \in \mathcal{L} \leftrightarrow L^* \in \mathcal{R}$ gives the desired bijection.]

2. Let M be an R -lattice as in (24.3), S a Dedekind domain containing R . Prove that

$$O_l(S \otimes_R M) = S \otimes_R O_l(M).$$

[Hint: Use (2.39).]

3. Let α be a nonunit of the Dedekind domain R , and let L be an R -lattice such that $L = \alpha L$. Show that L must equal 0.

[Hint: Choose a maximal ideal P of R containing α , and let the subscript P indicate localization at P . Then $L_P = \alpha L_P$ gives $L_P = PL_P$, whence $L_P = 0$ by Nakayama's Lemma. Therefore $P + \text{ann}_R L = R$ by Exercise 4.5, a contradiction since L is R -torsionfree. This same argument works for R any commutative ring, and L any f.g. torsionfree R -module.]

4. Let Λ be an R -order in a f.d. K -algebra A , and let $x \in A$. Prove that

$$O_l(\Lambda x) = \Lambda.$$

[Hint: Let $y \in A$. Then

$$y \in O_l(\Lambda x) \Leftrightarrow y\Lambda x \subseteq \Lambda x \Leftrightarrow y\Lambda \subseteq \Lambda \Leftrightarrow y \in \Lambda.$$

§25. EXTENSIONS OF LATTICES

Throughout this section, let R be a commutative ring, and let Λ be an R -algebra. Our main interest is in the case where R is a Dedekind domain with quotient field K , and Λ is an R -order in a f.d. K -algebra A . In this situation, let L be some full Λ -lattice in a f.g. left A -module V , so $V = K \cdot L$. We hope to use our knowledge of V and its submodules to obtain information about L . If we start with an A -composition series for V (see Exercise 23.3) and intersect its terms with L , we obtain a strictly decreasing chain of Λ -sublattices of L . In particular, suppose V contains a nonzero proper A -submodule W . Setting $M = L \cap W$, it follows from (23.15) that M is a full Λ -lattice in W , and that the factor module L/M is (isomorphic to) a full Λ -lattice in V/W . Thus, the A -exact sequence

$$0 \rightarrow W \rightarrow V \rightarrow V/W \rightarrow 0$$

gives rise to an exact sequence of Λ -lattices*:

$$0 \rightarrow M \rightarrow L \rightarrow N \rightarrow 0, \text{ where } N = L/M.$$

The sequence is necessarily R -split since N is R -projective, and thus $L \cong M \oplus N$ as R -modules, though this need not be a Λ -isomorphism.

In practice, our aim is to construct the Λ -module L from the pair of Λ -modules M and N . We shall discuss this question in terms of the R -module $\text{Ext}_\Lambda^1(N, M)$, whose elements correspond to equivalence classes of extensions of N by M (see §8A, and especially the paragraphs following (8.11)). Then we shall treat the same question from the standpoint of derivations, and shall later sketch a matrix approach to such calculations. For the most part, R may be any commutative ring. The restriction to Dedekind domains is needed mainly in (25.5), (25.6), (25.15) and (25.16).

Let Λ be an R -algebra, where R is any commutative ring. Recall that a Λ -lattice is a left Λ -module which is f.g. and projective as R -module. Later we shall restrict our attention to Λ -lattices, but for the time being we work with Λ -modules. Given a pair of Λ -modules M and N , an *extension* of N by M is a Λ -exact sequence

$$(25.1) \quad 0 \rightarrow M \rightarrow X \rightarrow N \rightarrow 0.$$

(Often, the module X itself is called an extension of N by M .) As noted earlier, if N is a Λ -lattice, the sequence (25.1) is R -split, and $X \cong M \oplus N$ as R -modules. Hence if M and N are Λ -lattices, then so is X .

Now let

$$\xi_i : 0 \rightarrow M \rightarrow X_i \rightarrow N \rightarrow 0, \quad i = 1, 2,$$

be a pair of extensions of N by M . As in §8A, we call these extensions *equivalent* if there exists a commutative diagram

$$\begin{array}{ccccccc} \xi_1 : 0 & \longrightarrow & M & \longrightarrow & X_1 & \longrightarrow & N \longrightarrow 0 \\ & & \downarrow 1 & & \downarrow \varphi & & \downarrow 1 \\ \xi_2 : 0 & \longrightarrow & M & \longrightarrow & X_2 & \longrightarrow & N \longrightarrow 0. \end{array}$$

(The Λ -homomorphism φ occurring here is necessarily an isomorphism.) These equivalence classes of extensions then form an R -module $\text{Ext}_\Lambda^1(M, N)$. We caution the reader that there exist cases where $X_1 \cong X_2$ even though $\xi_1 \neq \xi_2$ in $\text{Ext}_\Lambda^1(N, M)$.

*The fact that N is a Λ -lattice, rather than an arbitrary f.g. Λ -module, will be extremely important in our later discussion.

We have described in §8A one method of calculating $\text{Ext}_{\Lambda}^1(N, M)$, which goes as follows. Let us start with an exact sequence of Λ -lattices

$$0 \rightarrow Q \xrightarrow{i} P \rightarrow N \rightarrow 0, \quad P \text{ projective.}$$

Then

$$(25.2) \quad \text{Ext}_{\Lambda}^1(N, M) \cong \text{Hom}_{\Lambda}(Q, M) / i^* \{ \text{Hom}_{\Lambda}(P, M) \},$$

and we have given this isomorphism explicitly in the remarks following (8.12). We shall give below some examples illustrating how to use (25.2) to calculate $\text{Ext}(N, M)$, but before doing so, let us derive a number of basic facts about such Ext groups.

Suppose for the moment that Λ is an R -order in a f.d. K -algebra A , where R is a Dedekind domain with quotient field K .

It follows as a special case of (8.11) that for any pair of Λ -lattices M and N , the group $\text{Ext}_{\Lambda}^1(N, M)$ is a f.g. R -module. (Indeed, it is also a f.g. Λ -module whenever Λ is commutative.) Let S be any multiplicative subset of R ; by (8.18) we have

$$(25.3) \quad S^{-1}R \otimes_R \text{Ext}_{\Lambda}^1(N, M) \cong \text{Ext}_{S^{-1}\Lambda}^1(S^{-1}N, S^{-1}M)$$

as $S^{-1}R$ -modules. For the special case where $S = R - \{0\}$, this gives

$$(25.4) \quad K \otimes_R \text{Ext}_{\Lambda}^1(N, M) \cong \text{Ext}_A^1(KN, KM).$$

We use this to show:

(25.5) Proposition. *Let M and N be Λ -lattices, where Λ is an R -order in a semisimple f.d. K -algebra A . Then $\text{Ext}_{\Lambda}^1(N, M)$ is a f.g. torsion R -module, that is, each element thereof is annihilated by some nonzero element of R .*

Proof. We have already remarked that $\text{Ext}_{\Lambda}^1(N, M)$ is f.g./ R . Next, since A is semisimple, every A -module is projective, so the right hand side of (25.4) is zero. But then $\text{Ext}_{\Lambda}^1(N, M)$ is an R -torsion R -module, by §4A.

(25.6) Corollary. *Keep the above hypotheses, let P range over all maximal ideals of R , and let the subscript P denote localization at P . Then*

$$\text{Ext}_{\Lambda}^1(N, M) \cong \coprod_P \text{Ext}_{\Lambda_P}^1(N_P, M_P),$$

and $\text{Ext}_{\Lambda_P}^1(N_P, M_P) = 0$ a.e.* (See also (29.7).)

*“a.e.” means “almost everywhere”, that is, for all but a finite number of P ’s.

Proof. For each P , we have

$$R_P \otimes_R \text{Ext}_\Lambda^1(N, M) \cong \text{Ext}_{\Lambda_P}^1(N_P, M_P)$$

by (25.3). Since $\text{Ext}_\Lambda^1(N, M)$ is a f.g. torsion R -module, the desired result follows at once from the Primary Decomposition Theorem 4.31. The result is due to deLeeuw [53]; see also Nunke [59], Reiner [59].

Returning to the case where R is any commutative ring and Λ is an R -algebra, we proceed to interpret $\text{Ext}_\Lambda^1(N, M)$ in terms of derivations. This will yield additional information about Ext, and will give another method for calculating it. Let us begin with some definitions. Let T be a (Λ, Λ) -bimodule, and suppose that T is *centralized* by R , that is,

$$\alpha t = t\alpha \text{ for all } \alpha \in R, t \in T.$$

A *derivation* $F: \Lambda \rightarrow T$ is an R -homomorphism satisfying

$$(25.7) \quad F_{\lambda' \lambda} = \lambda' F_\lambda + F_{\lambda'} \lambda \text{ for all } \lambda, \lambda' \in \Lambda.$$

Let $\text{Der}(\Lambda, T)$ be the R -module consisting of all derivations from Λ into T . For each $\theta \in T$, the map

$$(25.8) \quad \lambda \mapsto \theta\lambda - \lambda\theta, \lambda \in \Lambda,$$

is a derivation, called an *inner* or *principal derivation*. The set of all inner derivations is then an R -submodule of $\text{Der}(\Lambda, T)$. We now define

$$(25.9) \quad H^1(\Lambda, T) = \text{Der}(\Lambda, T)/\text{inner derivations}.$$

Then $H^1(\Lambda, T)$ is an R -module, called the *first cohomology group* of Λ with respect to T .

Now let M and N be left Λ -modules. As in §2A, $\text{Hom}_R(N, M)$ has a natural structure as a (Λ, Λ) -bimodule centralized by R . Explicitly, we have

$$(\lambda f)n = \lambda \cdot f(n), (f\lambda)n = f(\lambda n) \text{ for all } \lambda \in \Lambda, n \in N, f \in \text{Hom}_R(N, M).$$

We shall establish

(25.10) Proposition. *There exists an R -isomorphism*

$$\text{Ext}_\Lambda^1(N, M) \cong H^1(\Lambda, \text{Hom}_R(N, M))$$

whenever N is a Λ -lattice, and M any Λ -module.

Before proving (25.10), we require some further discussion of derivations. Suppose we are given an extension (25.1) in which N is any R -lattice, and let

us view M as a submodule of X . Since N is R -projective, the sequence

$$0 \rightarrow M \rightarrow X \xrightarrow{f} N \rightarrow 0$$

is R -split. Thus by (2.3) there exists an R -homomorphism $h: N \rightarrow X$ such that $f \circ h = 1$ on N . For each $\lambda \in \Lambda$, let

$$F_\lambda(n) = h(\lambda n) - \lambda h(n), \quad n \in N.$$

Since f is a Λ -homomorphism, we have $f(F_\lambda(n)) = 0$ for each n , so $F_\lambda(n) \in M$. The functions $F_\lambda: N \rightarrow M$ evidently measure the extent to which the map $h: N \rightarrow X$ fails to be a Λ -homomorphism. Clearly the map

$$F: \Lambda \rightarrow \text{Hom}_R(N, M), \text{ defined by } \lambda \mapsto F_\lambda, \lambda \in \Lambda,$$

is an R -homomorphism. In fact, F is a derivation because for all $\lambda, \lambda' \in \Lambda$ we have (for all $n \in N$):

$$\begin{aligned} F_{\lambda\lambda'}(n) &= h((\lambda\lambda')n) - (\lambda\lambda')h(n) = h(\lambda(\lambda'n)) - \lambda(\lambda'h(n)) \\ &= F_\lambda(\lambda'n) + \lambda h(\lambda'n) - \lambda(F_\lambda(n)) = F_\lambda(\lambda'n) + \lambda F_{\lambda'}(n), \end{aligned}$$

using the fact that M and N are Λ -modules.

It will be somewhat more convenient for us to work with ordered pairs. We may write $X = M \oplus N$ as R -modules, where M is viewed as a Λ -submodule of X . Each $x \in X$ may then be uniquely expressed as an ordered pair (m, n) from $M \oplus N$. The Λ -action on X defining the extension is given by

$$(25.11) \quad \lambda(m, 0) = (\lambda m, 0), \quad \lambda(0, n) = (F_\lambda(n), \lambda n) \text{ for all } m \in M, n \in N, \lambda \in \Lambda,$$

for some element $F_\lambda(n)$ in M . Here, λm is computed inside the Λ -module M , and λn inside the Λ -lattice $N \cong X/M$. The map $\lambda \mapsto F_\lambda$, $\lambda \in \Lambda$, gives an R -homomorphism

$$F: \Lambda \rightarrow \text{Hom}_R(N, M).$$

Then the condition

$$(\lambda\lambda')(m, n) = \lambda(\lambda'(m, n)) \text{ for all } \lambda, \lambda' \in \Lambda, m \in M, n \in N,$$

is satisfied if and only if (25.7) holds true, that is, if and only if F is a derivation from Λ into the (Λ, Λ) -bimodule $\text{Hom}_R(N, M)$. Conversely, each derivation F allows us to make $M \oplus N$ into a Λ -module, with the action of Λ given by (25.11); this module is then an extension of N by M .

We must still determine the effect on the derivation F if we use a different R -splitting $N \rightarrow X$ of (25.1). We must also decide under which conditions

another extension $0 \rightarrow M \rightarrow X' \rightarrow N \rightarrow 0$, with derivation F' , is equivalent to the original extension in (25.1). Both questions can be answered by the same calculation, as follows: the two extensions are equivalent if and only if there is a commutative diagram

$$\begin{array}{ccccccc} 0 & \longrightarrow & M & \longrightarrow & X & \longrightarrow & N & \longrightarrow 0 \\ & & 1 \downarrow & & \varphi \downarrow & & 1 \downarrow & \\ 0 & \longrightarrow & M & \longrightarrow & X' & \longrightarrow & N & \longrightarrow 0 \end{array}$$

in which $\varphi: X \cong X'$ is a Λ -isomorphism. The map φ must then be given by

$$\varphi(m, n) = (m + \theta(n), n) \text{ for all } m \in M, n \in N,$$

where $\theta \in \text{Hom}_R(N, M)$. For each $\lambda \in \Lambda$, we then have

$$\varphi\lambda(m, n) = \varphi(\lambda m + F_\lambda(n), \lambda n) = (\lambda m + F_\lambda(n) + \theta(\lambda n), \lambda n),$$

$$\lambda\varphi(m, n) = \lambda(m + \theta(n), n) = (\lambda m + F'_\lambda(n) + \lambda\theta(n), \lambda n).$$

Therefore

$$F'_\lambda = F_\lambda + \theta\lambda - \lambda\theta \text{ for all } \lambda \in \Lambda,$$

so $F' - F$ is an inner derivation. The process is reversible, and it follows readily that change of R -splitting of (25.1) changes the derivation F by adding an inner derivation. Likewise, two derivations F and F' yield equivalent extensions if and only if $F' - F$ is inner. We have therefore established the isomorphism asserted in (25.10). Note that it holds when N is any Λ -lattice and M an arbitrary Λ -module. However, (25.10) need not be valid when both M and N are arbitrary Λ -modules.

We shall now prove a fundamental result, which may be regarded as a generalization of Maschke's Theorem 3.14, and is in fact a special case of Theorem 8.43:

(25.12) Theorem. *Let G be a finite group, and let $\Lambda = RG$ be its group ring over a commutative ring R . Let T be any (Λ, Λ) -bimodule centralized by the elements of R . Then*

$$|G| \cdot H^1(\Lambda, T) = 0.$$

In particular,

$$(25.13) \quad |G| \cdot \text{Ext}_{RG}^1(N, M) = 0$$

for every RG -lattice N and RG -module M .

Proof. Let $F: \Lambda \rightarrow T$ be a derivation. Then for all $x, y \in G$ we have

$$(25.14) \quad F_{xy} = xF_y + F_x y.$$

Multiplying on the right by y^{-1} , and summing over all $y \in G$, we obtain

$$\sum_y F_{xy} y^{-1} = x \cdot S + |G| \cdot F_x \text{ for all } x \in G,$$

where $S = \sum_y F_y \cdot y^{-1}$. But

$$\sum_y F_{xy} y^{-1} = \sum_y F_{xy} (xy)^{-1} \cdot x = Sx.$$

Therefore

$$|G| F_x = Sx - xS \text{ for all } x \in G.$$

Since F is R -linear, we then obtain

$$|G| F_\lambda = S\lambda - \lambda S \text{ for all } \lambda \in \Lambda,$$

so $|G| \cdot F$ is an inner derivation, and the proof is complete. (For the connection between this theorem and (8.43), see Exercise 25.3.)

A number of important refinements of (25.13) will be given later; see especially §29.

We are now in a position to sharpen the results of (25.6) in the special case where Λ is an integral group ring. The following result will be used repeatedly in later sections:

(25.15) Theorem. *Let R be a Dedekind domain, G a finite group of order n , and suppose that $n \neq 0$ in R . Let M and N be a pair of RG -lattices. Then n annihilates $\mathrm{Ext}_{RG}^1(N, M)$, and there is an R -isomorphism*

$$\mathrm{Ext}_{RG}^1(N, M) \cong \coprod_{P \ni n} \mathrm{Ext}_{R_P G}^1(N_P, M_P),$$

the direct sum extending over all maximal ideals P of R which contain n . (There are finitely many such P 's.)

Proof. Write Ext instead of Ext_{RG}^1 , etc., for brevity. Then $n \cdot \mathrm{Ext}(N, M) = 0$ by (25.13). Hence $\{\mathrm{Ext}(N, M)\}_P = 0$ whenever P does not contain n , by Exercise 4.5. The above isomorphism thus follows from (25.6) and its proof.

(25.16) Corollary. *Keep the above notation. An RG -lattice N is RG -projective if and only if N_P is $R_P G$ -projective for each P containing $|G|$.*

Remarks. (i) Compare this result with (8.19).

(ii) In the special case where $R=K$, (25.15) says that if $\text{char } K \nmid |G|$, then $\text{Ext}_{KG}^1(N, M)=0$ for each pair of f.g. left KG -modules M and N . Thus every short exact sequence of f.g. KG -modules must split, which implies that the group algebra KG is semisimple. Hence we obtain Maschke's Theorem as a special case of (25.15). This is hardly surprising, however, since (25.12) is proved by exactly the same calculation occurring in the proof of Maschke's Theorem 3.14.

We shall now describe another approach to the calculation of Ext of a pair of Λ -lattices, which does not use any of the machinery of homological algebra, but is instead based on the isomorphism (25.10). We restrict our attention to the case where R is a Dedekind domain with quotient field K , and Λ is an R -order in a f.d. semisimple K -algebra A . Set

$$T = \text{Hom}_R(N, M), \quad KT = \text{Hom}_K(KN, KM).$$

Then T is a (Λ, Λ) -bimodule, and is an R -lattice. The injection $T \rightarrow K \otimes_R T$ allows us to write $K \otimes_R T$ as KT , and the above expression for KT is then a consequence of (4.1). Thus, T is a full R -lattice in the (A, A) -bimodule KT . Since A is semisimple, we have (using (25.10))

$$0 = \text{Ext}_A^1(KN, KM) \cong H^1(A, KT).$$

Thus, every derivation $F: \Lambda \rightarrow T$ extends to an inner derivation $F^*: A \rightarrow KT$, that is, there exists an element $\theta \in KT$ such that

$$F^*(a) = a\theta - \theta a \text{ for all } a \in A.$$

(We write $F^*(a)$ instead of F_a^* for convenience of notation.) It follows that

$$(25.17) \quad F(\lambda) = \lambda\theta - \theta\lambda \text{ for all } \lambda \in \Lambda.$$

The condition $F(\lambda)N \subseteq M$ for all $\lambda \in \Lambda$ may be written thus:

$$(25.18) \quad (\lambda\theta - \theta\lambda)N \subseteq M \text{ for all } \lambda \in \Lambda.$$

Conversely, starting with any $\theta \in KT$ satisfying (25.18), formula (25.17) defines a derivation $F: \Lambda \rightarrow T$. Furthermore, F is inner if and only if there exists an element $\theta_0 \in T$ such that

$$\lambda\theta - \theta\lambda = \lambda\theta_0 - \theta_0\lambda \text{ for all } \lambda \in \Lambda,$$

that is, if and only if $\theta - \theta_0 \in \text{Hom}_A(KN, KM)$.

Let us set

$$\Omega = \{\theta \in \text{Hom}_K(KN, KM) : (\lambda\theta - \theta\lambda)N \subseteq M \text{ for all } \lambda \in \Lambda\},$$

and let

$$\Omega_0 = \text{Hom}_R(N, M) + \text{Hom}_A(KN, KM).$$

We have thus established R -isomorphisms

$$(25.19) \quad \Omega/\Omega_0 \cong H^1(\Lambda, \text{Hom}_R(N, M)) \cong \text{Ext}_\Lambda^1(N, M),$$

the first of which is induced by the map which carries each $\theta \in \Omega$ onto the derivation F defined by (25.17).

In practice, to calculate Ω we must find all elements $\theta \in KT$ for which condition (25.18) is satisfied. In verifying (25.18), it obviously suffices to let λ range over a set of R -generators for Λ . Further, it is easily verified that if (25.18) holds for λ and λ' , it also holds for $\lambda\lambda'$. This leads to the following simpler description of Ω , in the special case where Λ is an integral group ring RG , and $G = \langle g_1, \dots, g_n \rangle$:

$$(25.20) \quad \Omega = \{\theta \in \text{Hom}_K(KN, KM) : (g_i\theta - \theta g_i)N \subseteq M, 1 \leq i \leq n\}.$$

We shall illustrate the calculation of $\text{Ext}_{RG}^1(N, M)$ by means of (25.19) and (25.20), in Example 25.24 below.

Next, let us give a matrix formulation of the problem of calculating extensions of lattices. We consider here the case where R is a P.I.D. with quotient field K , and Λ is an R -order in a f.d. K -algebra A . Every Λ -lattice then has a finite R -basis. In particular, let $0 \rightarrow M \rightarrow L \rightarrow N \rightarrow 0$ be a short exact sequence of Λ -lattices, and choose R -bases so that

$$L = \bigoplus_{i=1}^d Rx_i, \quad M = \bigoplus_{i=1}^k Rx_i, \quad N = L/M = \bigoplus_{i=k+1}^d R\bar{x}_i,$$

where \bar{x}_i is the image of x_i in L/M . For each $\lambda \in \Lambda$, we write

$$\lambda x_j = \sum_{i=1}^d \alpha_{ij} x_i, \quad \alpha_{ij} \in R, \quad 1 \leq j \leq d,$$

and let $\mathbf{L}(\lambda) = (\alpha_{ij})_{1 \leq i, j \leq d}$. Thus L affords the matrix representation \mathbf{L} of Λ , and we find at once that

$$(25.21) \quad \mathbf{L}(\lambda) = \begin{pmatrix} \mathbf{M}(\lambda) & \mathbf{T}(\lambda) \\ \mathbf{0} & \mathbf{N}(\lambda) \end{pmatrix}, \quad \lambda \in \Lambda,$$

where M and N afford the representations \mathbf{M} and \mathbf{N} , respectively. The identity

$$\mathbf{L}(\lambda\lambda') = \mathbf{L}(\lambda)\mathbf{L}(\lambda') \text{ for all } \lambda, \lambda' \in \Lambda$$

yields the condition

$$\mathbf{T}(\lambda\lambda') = \mathbf{M}(\lambda)\mathbf{T}(\lambda') + \mathbf{T}(\lambda)\mathbf{N}(\lambda') \text{ for all } \lambda, \lambda' \in \Lambda.$$

It follows at once that \mathbf{T} is a derivation from Λ into the bimodule of $k \times (d-k)$ matrices over R . The element $\lambda \in \Lambda$ acts from the left on this bimodule as multiplication by $\mathbf{M}(\lambda)$, and on the right as $\mathbf{N}(\lambda)$. (This derivation \mathbf{T} is also called a *binding system* for the pair of matrix representations \mathbf{M} and \mathbf{N} ; see CR(73.14), for instance.)

Suppose now that

$$\begin{pmatrix} \mathbf{M} & \mathbf{T} \\ \mathbf{0} & \mathbf{N} \end{pmatrix} \text{ and } \begin{pmatrix} \mathbf{M}' & \mathbf{T}' \\ \mathbf{0} & \mathbf{N} \end{pmatrix}$$

are a pair of R -representations of Λ . The matrix analogue of equivalence of extensions is as follows: the two matrix representations above are called *equivalent** if there exists a matrix \mathbf{C} with entries in R , such that

$$\begin{pmatrix} \mathbf{M}(\lambda) & \mathbf{T}'(\lambda) \\ \mathbf{0} & \mathbf{N}(\lambda) \end{pmatrix} = \begin{pmatrix} \mathbf{I} & \mathbf{C} \\ \mathbf{0} & \mathbf{I} \end{pmatrix}^{-1} \begin{pmatrix} \mathbf{M}(\lambda) & \mathbf{T}(\lambda) \\ \mathbf{0} & \mathbf{N}(\lambda) \end{pmatrix} \begin{pmatrix} \mathbf{I} & \mathbf{C} \\ \mathbf{0} & \mathbf{I} \end{pmatrix}$$

for each $\lambda \in \Lambda$. This gives

$$(25.22) \quad \mathbf{T}'(\lambda) = \mathbf{T}(\lambda) + \mathbf{M}(\lambda)\mathbf{C} - \mathbf{C}\mathbf{N}(\lambda) \text{ for all } \lambda \in \Lambda,$$

so $\mathbf{T}' - \mathbf{T}$ is an inner derivation.

(25.23) Example. Let $\Lambda = \mathbb{Z}G$, $A = \mathbb{Q}G$, where

$$G = \langle a, b : a^4 = 1, b^2 = 1, bab^{-1} = a^{-1} \rangle,$$

the dihedral group of order 8. Let \mathbf{M} be the \mathbb{Z} -representation of G defined by

$$\mathbf{M}(a) = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad \mathbf{M}(b) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

Thus, \mathbf{M} is the representation \mathbf{M}_1 of Example 23.6. Let \mathbf{N} denote the representation \mathbf{M}_2 of that example, so we have

$$\mathbf{N}(a) = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad \mathbf{N}(b) = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Let $M = \mathbb{Z} \oplus \mathbb{Z}$ be the $\mathbb{Z}G$ -module affording \mathbf{M} , and let $N = \mathbb{Z} \oplus \mathbb{Z}$ afford \mathbf{N} . We

*Some authors refer to this as “strong equivalence”.

shall calculate $\text{Ext}_{\mathbb{Z}G}^1(N, M)$ by using (25.19) and (25.20). We have

$$\begin{aligned}\Omega &= \left\{ \mathbf{X} \in M_2(\mathbb{Q}) : \mathbf{M}(g)\mathbf{X} - \mathbf{X}\mathbf{N}(g) \in M_2(\mathbb{Z}) \text{ for } g = a, b \right\} \\ &= \left\{ \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in M_2(\mathbb{Q}) : \alpha - \gamma, \delta - \alpha, \beta + \delta \in \mathbb{Z} \right\}.\end{aligned}$$

Next, to find Ω_0 we note first that

$$\begin{aligned}\text{Hom}_A(\mathbb{Q}N, \mathbb{Q}M) &= \left\{ \mathbf{X} \in M_2(\mathbb{Q}) : \mathbf{M}(g)\mathbf{X} - \mathbf{X}\mathbf{N}(g) = \mathbf{0} \text{ for } g = a, b \right\} \\ &= \left\{ \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in M_2(\mathbb{Q}) : \alpha - \gamma = \delta - \alpha = \beta + \gamma = 0 \right\} \\ &= \{\alpha P : \alpha \in \mathbb{Q}\}, \text{ where } \mathbf{P} = \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix}.\end{aligned}$$

Thus

$$\Omega_0 = M_2(\mathbb{Z}) + \{\alpha P : \alpha \in \mathbb{Q}\}.$$

We may now calculate Ω/Ω_0 ; let $\mathbf{X} = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \Omega$. Then working modulo Ω_0 , we have

$$\mathbf{X} = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \equiv \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} - \alpha \mathbf{P} = \begin{pmatrix} 0 & \alpha + \beta \\ \gamma - \alpha & \delta - \alpha \end{pmatrix} \equiv 0,$$

the last step because $\alpha - \gamma, \delta - \alpha$ and $\alpha + \beta$ all lie in \mathbb{Z} . This shows that $\text{Ext}_{\mathbb{Z}G}^1(N, M) = 0$.

On the other hand, we may calculate $\text{Ext}_{\mathbb{Z}G}^1(M, M)$ in the same way, obtaining for this case

$$\Omega = \left\{ \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in M_2(\mathbb{Q}) : \beta \pm \gamma, \alpha - \gamma \in \mathbb{Z} \right\},$$

$$\Omega_0 = M_2(\mathbb{Z}) + \{\alpha \mathbf{I} : \alpha \in \mathbb{Q}\}.$$

If $\mathbf{X} = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \Omega$, then mod Ω_0 we obtain

$$\mathbf{X} \equiv \begin{pmatrix} \alpha - \delta & \beta \\ \gamma & 0 \end{pmatrix} \equiv \begin{pmatrix} 0 & \beta \\ \gamma & 0 \end{pmatrix},$$

and $\beta \pm \gamma \in \mathbb{Z}$. Hence Ω/Ω_0 is a \mathbb{Z} -module with 2 elements, generated by

$$\mathbf{X} = \begin{bmatrix} 0 & -\frac{1}{2} \\ \frac{1}{2} & 0 \end{bmatrix}.$$

The derivation \mathbf{T} corresponding to \mathbf{X} is given by

$$\mathbf{T}(g) = \mathbf{M}(g)\mathbf{X} - \mathbf{X}\mathbf{M}(g), g \in G,$$

and we obtain

$$\mathbf{T}(a) = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \quad \mathbf{T}(b) = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Thus

$$g \rightarrow \begin{pmatrix} \mathbf{M}(g) & \mathbf{T}(g) \\ \mathbf{0} & \mathbf{M}(g) \end{pmatrix}, g \in G,$$

gives a \mathbb{Z} -representation of G which is a nonsplit extension of the factor representation \mathbf{M} (lower right hand corner) by the sub-representation \mathbf{M} (upper left hand corner).

(For another matrix calculation, see Exercise 25.10.)

A further comment on matrix representations may be useful. Let Λ be an R -order in a f.d. K -algebra A , where R is a P.I.D. with quotient field K . Let M be a Λ -lattice, and let

$$M = M_0 \supset M_1 \supset \cdots \supset M_n = 0$$

be a chain of sublattices, such that each M_{i-1}/M_i is a Λ -lattice (see Exercise 23.3). Choose an R -basis for M so that the first batch of elements form a basis for M_{n-1} , the first two batches a basis for M_{n-2} , and so on. Relative to this basis, M affords a matrix representation

$$(25.24) \quad \mathbf{M}(\lambda) = \begin{bmatrix} \mathbf{U}_{11}(\lambda) & \mathbf{U}_{12}(\lambda) & \cdots & \mathbf{U}_{1n}(\lambda) \\ \mathbf{0} & \mathbf{U}_{22}(\lambda) & \cdots & \mathbf{U}_{2n}(\lambda) \\ \vdots & \vdots & \ddots & \vdots \\ \mathbf{0} & \mathbf{0} & \cdots & \mathbf{U}_{nn}(\lambda) \end{bmatrix}, \quad \lambda \in \Lambda.$$

Here, \mathbf{U}_{ii} is the R -representation of Λ afforded by the R -composition factor M_{n-i}/M_{n-i+1} of M . For each i , $\mathbf{U}_{i,i+1}$ is a derivation of Λ relative to the pair \mathbf{U}_{ii} , $\mathbf{U}_{i+1,i+1}$. However, \mathbf{U}_{13} , $\mathbf{U}_{14}, \dots, \mathbf{U}_{24}, \dots$, are *not* derivations (generally speaking), and their calculation is precisely the problem of finding successive extensions of modules. There is no neat solution to this problem in most cases. (See Exercise 25.9.)

We shall conclude this section with an example in which we use the homological algebra approach in (25.2) to calculate Ext of a pair of $\mathbb{Z}G$ -lattices, where G is a finite cyclic group of order g . The result plays a key role in the later discussion of integral group representations. For each positive integer n ,

let ω_n be a primitive n -th root of 1 over \mathbb{Q} . Then (see (4.5)) we put

$$K_n = \mathbb{Q}(\omega_n), R_n = \mathbb{Z}[\omega_n] = \text{alg. int. } \{K_n\}.$$

Now $\min.\text{pol.}_{\mathbb{Q}}(\omega_n) = \Phi_n(x)$, the cyclotomic polynomial of order n and degree $\varphi(n)$, where φ is the Euler φ -function. Hence we have $R_n \cong \mathbb{Z}[x]/(\Phi_n(x))$. We shall identify the group ring $\mathbb{Z}G$ with the ring

$$\Lambda = \mathbb{Z}[x]/(x^g - 1),$$

by identifying x with a generator of G . Since

$$x^g - 1 = \prod_{n|g} \Phi_n(x),$$

it follows that there is a ring isomorphism

$$(25.25) \quad R_n \cong \Lambda / \Phi_n(x) \Lambda \text{ whenever } n \text{ divides } g.$$

For each divisor n of g , the surjection $\Lambda \rightarrow R_n$ permits us to view every R_n -module as a Λ -module. In particular, R_n is itself a left Λ -lattice. Our aim here is to calculate $\text{Ext}_{\mathbb{Z}G}^1(R_n, R_m)$ when m and n divide g . The result stated below is due to Diederichsen [40]; we shall give the simplified proof by Reiner [79b]. Calculations of this nature may also be found in Berman-Gudivok [64]; see also Berman [64].

(25.26) Theorem. *Let G be a cyclic group of order g , and let m and n be divisors of g . Let $R_n = \text{alg. int. } \{K_n\}$, where K_n is the cyclotomic field $\mathbb{Q}(\omega_n)$, with ω_n a primitive n -th root of 1 over \mathbb{Q} . Define R_m analogously, and view R_m and R_n as $\mathbb{Z}G$ -lattices. Then*

- (i) $\text{Ext}_{\mathbb{Z}G}^1(R_n, R_m) = 0$ unless $m/n = p^t$ for some prime p and some nonzero integer t , possibly negative.
- (ii) If $m/n = p^t$ for some prime p and some nonzero $t \in \mathbb{Z}$, then there is a $\mathbb{Z}G$ -isomorphism*

$$\text{Ext}_{\mathbb{Z}G}^1(R_n, R_m) \cong R_l/pR_l, \text{ where } l = \min(m, n).$$

Proof. Step 1. Let Λ be an arbitrary ring, and let $a \in \Lambda$, $\bar{\Lambda} = \Lambda/\Lambda a$, so $\bar{\Lambda}$ is a left Λ -module. Put

$$J = \text{ann}_{\Lambda}(a) = \{b \in \Lambda : ba = 0\}.$$

*Diederichsen proved that $\text{Ext}(R_n, R_m)$ is isomorphic to the direct sum of $\varphi(l)$ copies of $\mathbb{Z}/p\mathbb{Z}$, where $l = \min(m, n)$. The stated isomorphism is a stronger result, and implies that of Diederichsen, since R_l has a free \mathbb{Z} -basis of $\varphi(l)$ elements.

For each left Λ -module M , let

$$M' = \{m \in M : Jm = 0\}.$$

Then we have

$$(25.27) \quad \mathrm{Ext}_{\Lambda}^1(\bar{\Lambda}, M) \cong M'/aM,$$

by Exercise 25.7.

Step 2. Now let $\Lambda = \mathbb{Z}G$, where G is cyclic of order g , and let $n|g$. We show at once that

$$\mathrm{Ext}_{\mathbb{Z}G}^1(R_n, R_n) = 0.$$

Let Φ_n be the cyclotomic polynomial of order n , where we write Φ_n instead of $\Phi_n(x)$ for convenience. Consider any $\mathbb{Z}G$ -exact sequence

$$0 \rightarrow R_n \rightarrow M \rightarrow R_n \rightarrow 0$$

in which M is a $\mathbb{Z}G$ -module. Then $\Phi_n \cdot M \subseteq R_n$, so $\Phi_n^2 \cdot M = 0$; clearly also $(x^g - 1)M = 0$. Since Φ_n is irreducible and $x^g - 1$ has no repeated factors, their G.C.D. in $\mathbb{Q}[x]$ is Φ_n . It follows that there exists polynomials $p(x), g(x) \in \mathbb{Z}[x]$, and a nonzero $a \in \mathbb{Z}$, such that

$$a\Phi_n = p(x)\Phi_n^2 + q(x)(x^g - 1).$$

Then $a\Phi_n M = 0$, and so $\Phi_n M = 0$ because M is \mathbb{Z} -torsionfree. Therefore M may be viewed as an R_n -module. But then the sequence is R_n -split by (2.22)), and so the sequence is also $\mathbb{Z}G$ -split. This completes the proof that $\mathrm{Ext}_{\mathbb{Z}G}^1(R_n, R_n) = 0$.

Step 3. We assume that $m \neq n$ from now on, and write Ext in place of $\mathrm{Ext}_{\mathbb{Z}G}^1$ for brevity. Let $\Psi_n(x) \in \mathbb{Z}[x]$ be defined by the equation $\Phi_n \Psi_n = x^g - 1$. Then $\Psi_n \cdot \mathbb{Z}G$ is the annihilator of Φ_n in $\mathbb{Z}G$. Since Φ_m is a factor of Ψ_n , it follows that $\Psi_n \cdot R_m = 0$. Applying (25.27) with $A = \Lambda$, $a = \Phi_n$, $M = R_m$, we obtain

$$\mathrm{Ext}(R_n, R_m) \cong R_m / \Phi_n(x)R_m.$$

Using (25.25), this becomes

$$(25.28) \quad \mathrm{Ext}(R_n, R_m) \cong \mathbb{Z}[x]/(\Phi_n, \Phi_m) \text{ if } m \neq n.$$

This implies that $\mathrm{Ext}(R_n, R_m) \cong \mathrm{Ext}(R_m, R_n)$. We could have predicted this in advance by a general argument about contragredients of $\mathbb{Z}G$ -lattices (see Exercise 10.22).

It is rather complicated to compute $\text{Ext}(R_n, R_m)$ directly from (25.28), and indeed Diederichsen's proof involves intricate (though elementary) manipulations with roots of unity. Instead, we use (25.15) to express $\text{Ext}(R_n, R_m)$ as a direct sum of its p -primary components, with p ranging over all rational primes dividing g . We have

$$(25.29) \quad \text{Ext}_{\mathbb{Z}G}(R_n, R_m) \cong \coprod_{p|g} \text{Ext}_{\mathbb{Z}_p G}((R_n)_p, (R_m)_p),$$

where the subscript p denotes localization at p . From (25.28) we obtain

$$(25.30) \quad \text{Ext}_{\mathbb{Z}_p G}((R_n)_p, (R_m)_p) \cong \mathbb{Z}_p[x]/(\Phi_n, \Phi_m).$$

Before proceeding to the next step, we make some comments about the isomorphisms occurring in (25.26ii), (25.28)–(25.30). Since the ring $\mathbb{Z}G$ is commutative, the remarks following (8.10) show that each of the modules $\text{Ext}_{\mathbb{Z}G}$, $\text{Hom}_{\mathbb{Z}G}$, etc., may be viewed in a natural manner as a $\mathbb{Z}G$ -module. (An analogous statement holds with \mathbb{Z} replaced by \mathbb{Z}_p .) But then it is easily verified that (25.26ii), (25.28) and (25.29) give $\mathbb{Z}G$ -isomorphisms, while (25.30) is a \mathbb{Z}_p -isomorphism. This fact will play a crucial role in Step 5 below.

Step 4. Keep p fixed, and write $m=p^a r$, $n=p^b s$, where $p \nmid rs$. Let $\bar{\mathbb{Z}}=\mathbb{Z}/p\mathbb{Z}$, and let bars denote images mod p . By (4.40) we have

$$(25.31) \quad \bar{\Phi}_m = (\bar{\Phi}_r)^{\varphi(p^a)}, \quad \bar{\Phi}_n = (\bar{\Phi}_s)^{\varphi(p^b)} \text{ in } \bar{\mathbb{Z}}[x].$$

Using this fact, we now show that for $m \neq n$,

$$(25.32)$$

$$\text{Ext}_{\mathbb{Z}_p G}((R_n)_p, (R_m)_p) = 0 \text{ except when } m/n = p^t \text{ for some nonzero } t \in \mathbb{Z}.$$

If m/n is not a power of p , then $r \neq s$. Hence $(\bar{\Phi}_r, \bar{\Phi}_s) = 1$ in $\bar{\mathbb{Z}}[x]$, since every zero of $\bar{\Phi}_r$ is a primitive r -th root of 1 over $\bar{\mathbb{Z}}$, while every zero of $\bar{\Phi}_s$ is a primitive s -th root of 1 (see (4.34)). Hence $(\bar{\Phi}_m, \bar{\Phi}_n) = 1$ in $\bar{\mathbb{Z}}[x]$ by (25.31). Now let Ω be the *resultant* of Φ_m and Φ_n in $\mathbb{Z}[x]$; by definition,

$$\Omega = \prod_{j, k} (\alpha_j - \beta_k) \in \mathbb{Z},$$

where α_j ranges over the zeros of Φ_m , and β_k ranges over the zeros of Φ_n . Since Φ_m and Φ_n are monic polynomials in $\mathbb{Z}[x]$, each α_j and β_k is an algebraic integer, whence so is Ω . On the other hand, Ω is unchanged by all automorphisms in the Galois group of the splitting field of $\Phi_m \cdot \Phi_n$ over \mathbb{Q} , and therefore $\Omega \in \mathbb{Q}$. Thus $\Omega \in \mathbb{Z}$ as claimed above.

Let bars denote images in the splitting field of $\bar{\Phi}_m \cdot \bar{\Phi}_n$ over $\bar{\mathbb{Z}}$; then we have

$$\bar{\Omega} = \prod_{j, k} (\bar{\alpha}_j - \bar{\beta}_k) \in \bar{\mathbb{Z}}.$$

Since $(\bar{\Phi}_m, \bar{\Phi}_n) = 1$, each of the above factors $\bar{\alpha}_j - \bar{\beta}_k$ is nonzero, so $\bar{\Omega} \neq 0$. Therefore Ω is a unit in the localization \mathbb{Z}_p . On the other hand (see van der Waerden [64]), the resultant Ω lies in the ideal (Φ_m, Φ_n) of $\mathbb{Z}[x]$. Hence in $\mathbb{Z}_p[x]$ we have $(\Phi_m, \Phi_n) = \mathbb{Z}_p[x]$, and (25.32) is then an immediate consequence of (25.30).

Step 5. Suppose finally that $m \neq n$ but $m/n = p^t$ for some nonzero $t \in \mathbb{Z}$. Then we have $m = p^a s$, $n = p^b s$, where $p \nmid s$. By (25.28), there is no loss of generality in assuming that $m < n$, so $a < b$. We show first that p lies in the ideal (Φ_n, Φ_m) of $\mathbb{Z}[x]$. Put

$$y = x^{s \cdot p^{b-1}} \in G.$$

Since x acts as ω_m on R_m , it follows that y acts as 1 on R_m . On the other hand, x acts as ω_n on R_n , so y acts on R_n as multiplication by a primitive p -th root of 1. Therefore $1 + y + y^2 + \cdots + y^{p-1}$ annihilates R_n .

Now $\text{Ext}_{\mathbb{Z}G}(R_n, R_m)$ is a $\mathbb{Z}G$ -bimodule, since $\mathbb{Z}G$ is commutative (see the last paragraph of Step 3). The right action of $\mathbb{Z}G$ on $\text{Ext}(R_n, R_m)$ arises from the left action of $\mathbb{Z}G$ on the first variable R_n , since Ext is contravariant in the first variable (see Remark (8.4iv)). Likewise, the left action of $\mathbb{Z}G$ on $\text{Ext}(R_n, R_m)$ arises from the left action of $\mathbb{Z}G$ on the second variable R_m , since Ext is covariant in the second variable. Further, the two actions of $\mathbb{Z}G$ on Ext are identical: $\gamma\xi = \xi\gamma$ for all $\gamma \in \mathbb{Z}G$, $\xi \in \text{Ext}$. This is clear from the fact that for any pair of $\mathbb{Z}G$ -modules M and N , the two actions of $\mathbb{Z}G$ on $\text{Hom}_{\mathbb{Z}G}(M, N)$ coincide.

By the preceding remarks, we see that $1 + y + \cdots + y^{p-1}$ acts on $\text{Ext}(R_n, R_m)$ as the zero map (from the right), and as multiplication by p (from the left). Therefore $p \cdot \text{Ext}(R_n, R_m) = 0$, and so $p \in (\Phi_n, \Phi_m)$ by (25.28). But then

$$\text{Ext}(R_n, R_m) \cong \mathbb{Z}[x]/(\Phi_n, \Phi_m, p) \cong \bar{\mathbb{Z}}[x]/(\bar{\Phi}_n, \bar{\Phi}_m).$$

But when $m < n$ and $r = s$, $\bar{\Phi}_n$ is a power of $\bar{\Phi}_m$ by (25.31). Thus we obtain

$$\text{Ext}(R_n, R_m) \cong \bar{\mathbb{Z}}[x]/(\bar{\Phi}_m) = \mathbb{Z}[x]/(p, \Phi_m(x)) \cong R_m/pR_m.$$

The same argument holds with \mathbb{Z} replaced by \mathbb{Z}_p , since $\mathbb{Z}_p/p\mathbb{Z}_p \cong \bar{\mathbb{Z}}$. We have thus established assertion (ii) of our theorem, as well as the fact that

$$\text{Ext}_{\mathbb{Z}_p G}((R_n)_p, (R_m)_p) \cong R_l/pR_l, l = \min(m, n),$$

if $m/n = p^t$ for nonzero $t \in \mathbb{Z}$.

We are now ready to finish the proof of our theorem. Step 2 shows that $\text{Ext}(R_n, R_n) = 0$, so now let $m \neq n$. We consider the quotients m/n and n/m ; if neither one is a prime power, then $\text{Ext}(R_n, R_m) = 0$ by (25.29) and (25.32). On the other hand, if $m/n = p^t$ for some prime p and some nonzero $t \in \mathbb{Z}$, then we have already proved the desired result (ii) in Step 5. This completes the proof of the theorem.

For some other calculations of Ext , see §34E.

§25. Exercises

Throughout these exercises, R is a commutative ring and G an arbitrary group.

- Let M and N be RG -modules. Make $\text{Hom}_R(N, M)$ into a *left* RG -module by defining

$$x * f = xfx^{-1} \text{ for all } x \in G, f \in \text{Hom}_R(N, M),$$

and extending the action to all of RG by linearity. Show that the G -trivial submodule of $\text{Hom}_R(N, M)$ is precisely $\text{Hom}_{RG}(N, M)$.

[Hint: See the proof of (10.31)]

- Let $\Lambda = RG$, and let T be a (Λ, Λ) -bimodule centralized by R . Turn T into a *left* Λ -module, denoted by T' , by specifying that for $x \in G$ and $t \in T$,

$$x * t \text{ (computed in } T') = xtx^{-1} \text{ (computed in } T),$$

and extending to a Λ -action on T' by linearity. Show that each derivation $F: \Lambda \rightarrow T$ yields a derivation $F': \Lambda \rightarrow T'$ (in the sense of (8.23)), by setting

$$F'_x = F_x \cdot x^{-1}, \quad x \in G,$$

and extending by linearity. Prove that the map $F \mapsto F'$ gives an R -isomorphism $\text{Der}(\Lambda, T) \cong \text{Der}(\Lambda, T')$, and that

$$H^1(RG, T) \cong H^1(G, T').$$

- When G is a finite group, deduce (25.12) from (8.43) by using the preceding exercise.

- Let M be an RG -module whose G -trivial submodule is 0. Show that if G is a finite group, then

$$\left(\sum_{x \in G} x \right) M = 0.$$

- (Diederichsen [40]). Let $H \trianglelefteq G$, where G is a finite group. Let N be an RG -lattice on which H acts trivially. Let M be any RG -module whose H -trivial submodule

$\text{inv}_H M$ is 0 (see §10D). Show that

$$|H| \cdot \text{Ext}_{RG}^1(N, M) = 0$$

if R is an integral domain of characteristic 0.

[Hint: Use (25.10), and let $F: G \rightarrow \text{Hom}_R(N, M)$ be a derivation. We must prove that $|H|F$ is inner. Deduce from (25.14) that

$$(*) \quad F_x = F_{xy}(xy)^{-1}x - xF_yy^{-1}, \forall x, y \in G.$$

Sum over $x \in H$; use Exercise 25.4, and the hypothesis that N is H -trivial, to obtain

$$\sum_{x \in H} F_x x^{-1} = \sum_{z \in Hy} F_z z^{-1} = T \text{ (say), for all } y \in G.$$

Thus T is independent of y , and

$$T = \sum_{z \in yH} F_z z^{-1} \text{ for all } y \in G,$$

since $yH = Hy$. Keep $x \in G$ fixed, and sum $(*)$ over $y \in H$. This gives

$$|H| \cdot F_x = \sum_{y \in H} F_{xy}(xy)^{-1}x - x \sum_{y \in H} F_y y^{-1} = Tx - xT,$$

so $|H|F$ is an inner derivation.

A fancier proof uses the Hochschild-Serre-Lyndon *spectral sequence*, which we now describe. Let $H \trianglelefteq G$, $\bar{G} = G/H$, and let X be any RG -module. Then $\text{inv}_H X$ is an $R\bar{G}$ -module. The spectral sequence is the following exact sequence (see Babakhanian [72, p. 193] or Rotman [79, p. 355]):

$$0 \rightarrow H^1(\bar{G}, \text{inv}_H X) \rightarrow H^1(G, X) \rightarrow \text{inv}_{\bar{G}} H^1(H, X) \rightarrow H^2(\bar{G}, \text{inv}_H X) \rightarrow H^2(G, X).$$

(There is a natural action of \bar{G} on $H^1(H, X)$, so $\text{inv}_{\bar{G}} H^1(H, X)$ is meaningful.)

If now $\text{inv}_H X = 0$, then $H^1(G, X)$ is embedded in the \bar{G} -trivial submodule of $H^1(H, X)$, whence

$$|H| \cdot H^1(G, X) = 0.$$

In the case above, take $X = \text{Hom}_R(N, M)$, so $\text{inv}_H X = \text{Hom}_{RH}(N, M)$. Show that the latter is 0 because N is H -trivial, while $\text{inv}_H M = 0$. Thus $|H| \cdot H^1(G, \text{Hom}_R(N, M)) = 0$, and now use Exercise 25.2 and (25.10).]

6. Let G be a finite group of order n , acting trivially on \mathbb{Z} . Put

$$\sigma = \sum_{x \in G} x \in \mathbb{Z}G,$$

and let $J = \mathbb{Z}G/\mathbb{Z}\sigma = \text{left } \mathbb{Z}G\text{-lattice}$. Prove that

$$\text{Ext}_{\mathbb{Z}G}^1(J, \mathbb{Z}) \cong \mathbb{Z}/n\mathbb{Z}.$$

[Hint: $0 \rightarrow \mathbb{Z} \xrightarrow{\sigma} \mathbb{Z}G \rightarrow J \rightarrow 0$ is $\mathbb{Z}G$ -exact. Now use (25.2).]

7. Let Λ be an arbitrary ring, let $a \in \Lambda$, and set $\bar{\Lambda} = \Lambda/\Lambda a =$ left Λ -module. Put

$$T = \text{ann}_\Lambda a = \{b \in \Lambda : ba = 0\}.$$

For each left Λ -module M , define

$$M' = \{m \in M : T \cdot m = 0\}.$$

Prove that

$$\text{Ext}_\Lambda^1(\bar{\Lambda}, M) \cong M'/aM$$

as additive groups.

[Hint: From the exact sequence $0 \rightarrow \Lambda a \xrightarrow{i} \Lambda \rightarrow \bar{\Lambda} \rightarrow 0$, where i is the inclusion map, we obtain

$$\text{Ext}^1(\bar{\Lambda}, M) \cong \text{Hom}(\Lambda a, M)/i^*(\text{Hom}(\Lambda, M)),$$

where we omit the subscript Λ from Ext and Hom for convenience. Each $f \in \text{Hom}(\Lambda a, M)$ is determined by the image $f(a) \in M$, which may be chosen arbitrarily in M , subject to the condition that

$$(\text{ann}_\Lambda a) \cdot f(a) = 0.$$

Thus $\text{Hom}(\Lambda a, M) \cong M'$. Since $\text{Hom}(\Lambda, M) \cong M$ by (2.6), we obtain

$$i^*(\text{Hom}(\Lambda, M)) \cong aM,$$

and the result is proved.]

8. Let G be a finite group of order n , R an integral domain of characteristic 0, and let M and N be RG -lattices. Let $F: G \rightarrow \text{Hom}_R(N, M)$ be a derivation such that $F \equiv 0 \pmod{n}$, that is,

$$F_x \in n \cdot \text{Hom}_R(N, M) \text{ for all } x \in G.$$

Show that F is an inner derivation.

[Hint: Put $F_1 = n^{-1}F$, and show that F is a derivation. Then use (25.12).]

9. In terms of the notation (25.24), show that

$$\begin{bmatrix} U_{13} \\ U_{23} \end{bmatrix}$$

is a derivation of Λ relative to the pair

$$\begin{bmatrix} U_{11} & U_{12} \\ \mathbf{0} & U_{22} \end{bmatrix}, [U_{33}].$$

Generalize!

10. Let $G = \langle x \rangle$ be a cyclic group of order g , and K any field. Let M and N be f.g. left KG -modules such that $\text{Hom}_{KG}(N, M) = 0$, and let $m = \dim_K M$, $n = \dim_K N$. Suppose that M and N afford the matrix representations \mathbf{M} and \mathbf{N} , respectively. Show that for every $m \times n$ matrix \mathbf{T} over K , the map

$$x \mapsto \begin{pmatrix} \mathbf{M}(x) & \mathbf{T} \\ \mathbf{0} & \mathbf{N}(x) \end{pmatrix}$$

defines a K -representation of G .

[Hint: It suffices to show that $\mathbf{T} = \mathbf{M}(x)\mathbf{W} - \mathbf{W}\mathbf{N}(x)$ for some $\mathbf{W} \in K^{m \times n}$, since then

$$\begin{pmatrix} \mathbf{M}(x) & \mathbf{T} \\ \mathbf{0} & \mathbf{N}(x) \end{pmatrix} = \begin{pmatrix} \mathbf{I} & \mathbf{W} \\ \mathbf{0} & \mathbf{I} \end{pmatrix}^{-1} \begin{pmatrix} \mathbf{M}(x) & \mathbf{0} \\ \mathbf{0} & \mathbf{N}(x) \end{pmatrix} \begin{pmatrix} \mathbf{I} & \mathbf{W} \\ \mathbf{0} & \mathbf{I} \end{pmatrix}.$$

Consider the K -endomorphism φ of $K^{m \times n}$ defined by

$$\varphi(\mathbf{W}) = \mathbf{M}(x)\mathbf{W} - \mathbf{W}\mathbf{N}(x), \quad \mathbf{W} \in K^{m \times n}.$$

Then $\varphi(\mathbf{W}) = \mathbf{0}$ if and only if $\mathbf{W} \in \text{Hom}_{KG}(N, M)$, whence φ is an injection. Hence φ is surjective, so every $\mathbf{T} \in K^{m \times n}$ lies in $\text{im}(\varphi)$.]

11. Let Λ be an R -order in a K -algebra A , and let U, V be f.g. left A -modules. Let $e \in \Lambda$ be a central idempotent of A such that e acts as 1 on each composition factor of U , and e annihilates each composition factor of V . Show that $\text{Ext}_\Lambda^1(M, N) = 0$ for each pair of Λ -lattices M, N such that $KM = U, KN = V$.

[Hint: By Exercise 3.16, $eV = 0$ and $(e-1)U = 0$. Thus e acts as 1 on M and as 0 on N . Since e is central in Λ , e acts on $\text{Ext}_\Lambda^1(M, N)$ by its action on M or on N , and these two actions of e are identical. Thus $\text{Ext}_\Lambda^1(M, N) = 0$.]

12. Let $E = G \times H$ be a direct product of finite groups, R a Dedekind domain, and T an RH -lattice. Given any RG -lattice M , we may form the outer tensor product $M \# T = M \otimes_R T$, an RE -lattice. Show that for any RG -lattices M and N , there is a monomorphism

$$\text{Ext}_{RG}^1(M, N) \rightarrow \text{Ext}_{RE}^1(M \# T, N \# T),$$

obtained by applying $* \# T$ to exact sequences of RG -lattices.

[Hint: The result is due to Reiner [67]. It suffices to prove the result with R_P in place of R , where P ranges over the maximal ideals of R . Changing notation, let R be a P.I.D. and let $T = \bigoplus_1^n R t_i$. Given an exact sequence of RG -lattices $0 \rightarrow N \rightarrow X \xrightarrow{\mu} M \rightarrow 0$, suppose that

$$0 \rightarrow N \# T \rightarrow X \# T \xrightarrow{\mu \otimes 1} M \# T \rightarrow 0$$

is RE -split, and let $\rho: M \# T \rightarrow X \# T$ split $\mu \otimes 1$. Write

$$\rho(m \otimes t_i) = \sum_{j=1}^n f_{ij}(m) \otimes t_j, \quad m \in M, 1 \leq i \leq n,$$

where each $f_{ij} \in \text{Hom}_{RG}(M, X)$. Then for each i , $(\mu \otimes 1)\rho(m \otimes t_i) = m \otimes t_i$ implies that $\mu f_{ii} = 1_M$, so f_{ii} splits μ .]

13. Let R be a Dedekind domain, G_1 and G_2 arbitrary groups, and let M_i and M'_i be RG_i -lattices, $i=1, 2$. Set $\Gamma_i = RG_i$, $\Gamma = RG$, where $G = G_1 \times G_2$. Prove the following results of Jones [63b]:

$$\text{Ext}_\Gamma^1(M_1 \# M_2, M'_1 \# M'_2) \cong \text{Hom}_{\Gamma_1}(M_1, M'_1) \otimes_R \text{Ext}_{\Gamma_2}^1(M_2, M'_2)$$

$$\oplus \text{Ext}_{\Gamma_1}^1(M_1, M'_1) \otimes_R \text{Hom}_{\Gamma_2}(M_2, M'_2),$$

$$\text{Hom}_\Gamma(M_1 \# M_2, M'_1 \# M'_2) \cong \text{Hom}_{\Gamma_1}(M_1, M'_1) \otimes_R \text{Hom}_{\Gamma_2}(M_2, M'_2).$$

[Hint: Let \otimes denote \otimes_R . Suppose the complex X' with derivation d_i is a projective resolution of M_i , $i=1, 2$. All the modules of X' can be assumed Γ_i -free, and f.g. as Γ_i -modules. Consider now the complex $X^1 \# X^2$, where

$$(X^1 \# X^2)_m = \sum_{j+k=m} X_j^1 \# X_k^2,$$

and where the derivation on $X_j^1 \# X_k^2$ is $d_1 \otimes 1 + (-1)^j \otimes d_2$. The modules of $X^1 \# X^2$ are Γ -free, and for $m > 0$,

$$H_m(X^1 \otimes X^2) = \text{Tor}_R^m(M_1, M_2) = 0.$$

It follows that $X^1 \# X^2$ is a projective resolution of $M_1 \# M_2$.

Therefore

$$\text{Ext}_\Gamma(M_1 \# M_2, M'_1 \# M'_2) \cong H(\text{Hom}_\Gamma(X^1 \# X^2, M'_1 \# M'_2)).$$

Now observe that

$$\text{Hom}_\Gamma(\Gamma, M'_1 \# M'_2) \cong M'_1 \# M'_2 \cong \text{Hom}_{\Gamma_1}(\Gamma_1, M'_1) \otimes \text{Hom}_{\Gamma_2}(\Gamma_2, M'_2).$$

Therefore since the modules of X' are Γ_i -free and finitely generated, it follows that

$$\text{Hom}_\Gamma(X^1 \# X^2, M'_1 \# M'_2) \cong \text{Hom}_{\Gamma_1}(X^1, M'_1) \otimes \text{Hom}_{\Gamma_2}(X^2, M'_2).$$

Next observe that $\text{Hom}_{\Gamma_i}(\Gamma_i, M'_i) \cong M'_i$ is an R -lattice, so the modules of $\text{Hom}_{\Gamma_i}(X^i, M'_i)$ are R -lattices. Then from Künneth's Theorem we get

$$H_m(\text{Hom}_{\Gamma_1}(X^1, M'_1) \otimes \text{Hom}_{\Gamma_2}(X^2, M'_2))$$

$$\cong \sum_{j+k=m} H_j(\text{Hom}_{\Gamma_1}(X^1, M'_1)) \otimes H_k(\text{Hom}_{\Gamma_2}(X^2, M'_2))$$

$$\oplus \sum_{j+k=m-1} \text{Tor}_1^R(H_j(\text{Hom}_{\Gamma_1}(X^1, M'_1)), H_k(\text{Hom}_{\Gamma_2}(X^2, M'_2))).$$

From this, taking $m=1$ and observing that

$$\text{Tor}_1^R(\text{Hom}_{\Gamma_1}(M_1, M'_1), \text{Hom}_{\Gamma_2}(M_2, M'_2)) = 0,$$

we obtain the formula for Ext_Γ^1 . Similarly, with $m=0$, the formula for Hom_Γ follows.]

§26. MAXIMAL AND HEREDITARY ORDERS

Throughout this section, R is a Dedekind domain with quotient field K , and A is a f.d. K -algebra. A *maximal R -order* in A is an R -order in A which is not properly contained in any larger R -order in A . For example, when K is an algebraic number field, the ring alg. int. $\{K\}$ is a maximal \mathbf{Z} -order in K . As is evident from Dedekind's theory of ideals, rings of algebraic integers enjoy special properties which make them easier to handle than their subrings. These properties also account for the widespread usefulness of such rings in many branches of algebra and number theory.

Recall that a ring is (left) hereditary if each of its (left) ideals is a projective module. One of the most useful facts is that every Dedekind domain R is hereditary. (Indeed, this property characterizes Dedekind domains; see (4.6)). More generally, it will turn out that every maximal order is hereditary, although the converse is false for the noncommutative case.

In §26A we derive some elementary facts about maximal orders, including the basic result that when A is a separable K -algebra, then every order can be embedded in a maximal order. In §26B we give a self-contained (but complicated) proof that maximal orders are hereditary. The proof includes as a special case the result that hereditary domains possess a classical ideal theory. Finally, §26C lists (without proofs) the basic structure theorems for maximal and hereditary orders. Much of the global theory of a Dedekind domain can be obtained from a study of its localizations and completions. In an analogous manner, many of the properties of maximal and hereditary orders can be deduced from the knowledge of their completions. This information can be given in a remarkably explicit form, as will be evident from the structure theorems given in §26C.

§26A. Existence of Maximal Orders in Separable Algebras

As in (23.1), an R -order in A is a subring Λ of A such that

$$R \subseteq \Lambda, \quad \Lambda \text{ is f.g./}R \text{ as module, } K \cdot \Lambda = A.$$

The embedding of R into the center of Λ allows us to view all Λ -modules (and Λ itself) as R -modules, and we do so with no further comment hereafter.

In this subsection, we shall need some facts about reduced norms and reduced traces; these are described in the early part of §7D. We shall also

make use of order ideals of R -modules, and the relation between discriminants and order ideals (see §§4D, E).

Our first result shows that an R -order may be considered to be a “noncommutative ring of integers”.

(26.1) Proposition. *Let Λ be an R -order in the K -algebra A . Then every element $x \in \Lambda$ is integral over R . Furthermore,*

$$\min. \text{pol.}_K(x) \in R[X], \text{char. pol.}_{A/K}(x) \in R[X],$$

where X is an indeterminate. Therefore

$$N_{A/K}(x) \in R, T_{A/K}(x) \in R,$$

where N and T are the usual norm and trace maps from A to K .

Proof. The Dedekind domain R is integrally closed, and Λ is f.g./ R , so the result follows from (1.8) and (1.9).

(26.2) Corollary. *Let Λ be an R -order in the separable K -algebra A . Then*

$$\text{red. char. pol.}_{A/K}(x) \in R[X] \text{ for all } x \in \Lambda.$$

Therefore

$$\text{nr}_{A/K}(x) \in R, \text{tr}_{A/K}(x) \in R,$$

where nr and tr are the reduced norm and reduced trace maps from A to K .

Proof. By §7D, $\text{red. char. pol.}(x)$ and $\text{char. pol.}(x)$ have the same irreducible factors, apart from multiplicities. Since $\text{char. pol.}(x) \in R[X]$ by (26.1), each irreducible factor of $\text{char. pol.}(x)$ also lies in $R[X]$ by Gauss's Lemma 1.7. Thus $\text{red. char. pol.}(x) \in R[X]$, whence $\text{nr}(x), \text{tr}(x) \in R$.

Suppose now that Λ is an R -order in a separable K -algebra A , and let $m = \dim_K A$. By §7D, there is a nondegenerate symmetric K -bilinear reduced trace form

$$\text{tr}: A \times A \rightarrow K, \text{ given by } (a, b) \mapsto \text{tr}_{A/K}(ab) \text{ for all } a, b \in A.$$

We now define the *discriminant* $d(\Lambda)$ of the order Λ to be the ideal of R generated by all elements

$$\det[\text{tr}(x_i x_j)]_{1 \leq i, j \leq m} \text{ with } x_1, \dots, x_m \in \Lambda.$$

These $\{x_i\}$ need not be chosen to be a K -basis for A ; however, whenever the

$\{x_i\}$ are linearly dependent over K , so are the rows of the $m \times m$ matrix $[\text{tr}(x_i x_j)]_{1 \leq i, j \leq m}$, and then the determinant equals 0. On the other hand, this determinant is nonzero when the $\{x_i\}$ are linearly independent over K , since the trace form is nondegenerate. Further, each entry $\text{tr}(x_i x_j) \in R$ by (26.2), and therefore the discriminant $d(\Lambda)$ is a nonzero ideal of R . Finally, if it happens that Λ has a free R -basis $\{x_1, \dots, x_m\}$, then it is easily seen that $d(\Lambda)$ is the principal ideal generated by $\det[\text{tr}(x_i x_j)]$.

Let us collect a number of remarks about discriminants:

(26.3) **Proposition.** *Let A be a separable K -algebra of dimension m . Let P range over the maximal ideals of R , and let the subscript P denote localization at P .*

(i) *If Λ is an R -order in A , then Λ_P is an R_P -order in A . Furthermore,*

$$\Lambda = \bigcap_P \Lambda_P \text{ (intersection within } A\text{).}$$

(ii) *For each P , $\{d(\Lambda)\}_P = d(\Lambda_P)$.*

(iii) *Let $\Lambda \subseteq \Lambda'$, where Λ and Λ' are R -orders in A , and let $\text{ord}(\Lambda'/\Lambda)$ be the order ideal of the R -torsion R -module Λ'/Λ . Then*

$$(26.4) \quad d(\Lambda) = \{\text{ord}(\Lambda'/\Lambda)\}^2 d(\Lambda').$$

Therefore $d(\Lambda) \subseteq d(\Lambda')$, with equality if and only if $\Lambda = \Lambda'$.

Proof. Since $\Lambda_P = R_P \otimes_R \Lambda$, the discussion following (23.11) shows that, for each P , Λ_P is an R_P -order in A . The second assertion in part (i) follows from (4.21vi). We leave (ii) as exercise for the reader. Formula (26.4) has already been established in (4.26), and clearly implies the remaining part of (iii).

The preceding proposition, though elementary in nature, has the following important consequence:

(26.5) **Theorem.** *Any R -order Λ in a separable K -algebra A is contained in at least one maximal R -order in A .*

Proof. Consider any strictly increasing chain of R -orders in A which begins with Λ , say

$$\Lambda \subset \Lambda_1 \subset \Lambda_2 \subset \cdots.$$

By (26.3), this chain gives rise to a strictly increasing chain of ideals of R :

$$d(\Lambda) \subset d(\Lambda_1) \subset d(\Lambda_2) \subset \cdots.$$

This latter chain must terminate, since R is noetherian. Hence the chain of orders must also terminate, that is, for some t the order Λ_t must be a maximal order. This completes the proof.

The above proof depends heavily on the existence of a nondegenerate bilinear form from $A \times A$ to K . For a separable K -algebra A , the reduced trace map furnishes such a bilinear form. However, when $\text{char } K=0$ and A is semisimple, the ordinary trace form $T_{A/K}$ is also nondegenerate. One can thus prove the preceding theorem by using the ordinary trace form, in the special case where A is a semisimple algebra over a field of characteristic 0. However, even in this case there are advantages to using the reduced trace (see, for example, the proof of Jacobinski's Theorem in §27).

We shall deduce from (26.5) the existence of maximal orders in separable algebras. For this purpose, we need only show that every f.d. K -algebra A contains at least one R -order Λ . Now every f.d. K -space contains a full R -lattice (by §4D, or (23.15)). Hence A itself contains a full R -lattice M . The discussion following (24.3) shows that $O_l(M)$ is an R -order in A . If A is separable over K , then by (26.5) it follows that $O_l(M)$ is contained in a maximal R -order in A . This establishes:

(26.6) Corollary. *Every separable K -algebra A contains at least one maximal R -order.*

We are going to show that a commutative separable K -algebra contains a unique maximal order. To prove this, however, we need some way of deciding when a ring of integers is actually an order. The key result in this direction is as follows:

(26.7) Proposition. *Let A be a separable K -algebra, and let Λ be a subring of A containing R , such that $K \cdot \Lambda = A$. If every element of Λ is integral over R , then Λ is an R -order in A .*

Proof. We need only show that Λ is f.g. as R -module. Since $K \cdot \Lambda = A$, we may find elements $x_1, \dots, x_m \in \Lambda$ such that $A = \bigoplus_{i=1}^m Kx_i$. Let

$$\alpha = \det [\text{tr}(x_i x_j)]_{1 \leq i, j \leq m},$$

where tr is the reduced trace form from A to K . Then $\alpha \neq 0$ since tr is nondegenerate, while $\alpha \in R$ since each product $x_i x_j$ lies in Λ and hence is integral over R .

We claim that

$$(26.8) \quad \Lambda \subseteq \alpha^{-1} \cdot \bigoplus_{i=1}^m Rx_i.$$

Once this is proved, it is clear that Λ is necessarily f.g./ R , and the proposition is established. To prove the claim, let $y \in \Lambda$; we may write $y = \sum_1^m r_i x_i$ with each $r_i \in K$. Then

$$\text{tr}(yx_j) = \sum_{i=1}^m r_i \text{tr}(x_i x_j), \quad 1 \leq j \leq m.$$

Further, $yx_j \in \Lambda$ for each j , whence $\text{tr}(yx_j) \in R$ by (26.2). Solving the above equations for the $\{r_i\}$ by Cramer's Rule, we obtain

$$r_i = (\text{element of } R)/\alpha, \quad 1 \leq i \leq m.$$

Therefore $\alpha y = \sum \alpha r_i x_i \in \bigoplus Rx_i$. This establishes (26.8), and finishes the proof.

(26.9) Corollary. *Let A be a separable K -algebra, and let Γ be a subring of A containing R . If Γ is f.g./ R , then Γ lies in some maximal R -order in A .*

Proof. Let M be any full R -lattice in A , and set $L = \Gamma \cdot M$. Then L is also a full R -lattice in A ; we set $\Lambda = O_f(L)$, the left order of L (see (24.3)). Then Λ is an R -order in A , hence is contained in a maximal R -order in A , by (26.5). But $\Gamma \subseteq \Lambda$, so Γ also lies in some maximal order.

We are now ready to prove:

(26.10) Proposition. *Let A be a commutative separable K -algebra. Then there is a unique maximal R -order in A , namely the integral closure Λ of R in A .*

Proof. By definition, Λ consists of all elements $a \in A$ which are integral over R . Clearly $R \subseteq \Lambda$, and (by (1.4)) Λ is closed under addition and multiplication, since A is commutative. To check that $A = K \cdot \Lambda$, let $b \in A$. Then b satisfies a polynomial equation

$$\alpha_0 b^n + \alpha_1 b^{n-1} + \cdots + \alpha_n = 0, \quad \alpha_i \in R, \quad \alpha_0 \neq 0,$$

for some n . Multiplying by α_0^{n-1} , we find at once that $\alpha_0 b$ is integral over R , so $\alpha_0 b \in \Lambda$. This shows that $A = K \cdot \Lambda$, so Λ is an R -order in A , by (26.7). Finally, Λ contains every R -order in A , by virtue of (26.1). Thus, Λ is the unique maximal R -order in A , as asserted.

Let us consider briefly the situation where A is *not* a separable K -algebra. In this case, maximal orders may or may not exist, as is shown by the following two examples.

(26.11) Examples. (i) Let k be a field, $\text{char } k = p \neq 0$. Let $K = k(x)$ be a transcendental extension of k , and let $R = k[x]$, a P.I.D. with field of

quotients K . Let

$$A = K(y), \Lambda = R[y], \text{ where } y^p = x.$$

Then $\Lambda = k[x, y] = k[y]$, $A = k(x, y) = k(y)$, so Λ is also a P.I.D., with field of quotients A . Thus Λ is integrally closed in A . Every $z \in A$ which is integral over R is also integral over Λ , hence lies in Λ . This shows that Λ is the integral closure of R in A , and is the unique maximal R -order in A . Note that this occurs in a situation where A is inseparable over K .

(ii) Suppose that $R \neq K$, and let A be a f.d. K -algebra with nonzero radical. Given any R -order Λ in A , we showed in the proof of (24.4) that there exists an infinite ascending chain (24.5) of R -orders in A , starting with Λ . In particular, *every* order is properly contained in a larger order, *so there are no maximal orders in A in this case*.

We conclude this subsection by mentioning some examples of maximal orders:

- (i) If K is an algebraic number field, then alg. int. $\{K\}$ is a maximal \mathbb{Z} -order in K , by (26.10).
- (ii) For G a finite group, the integral group ring RG is a maximal order in KG if and only if $|G|$ is a unit of R (see (27.1)).
- (iii) The matrix ring $M_n(R)$ is always a maximal order in the matrix algebra $M_n(K)$, by Exercise 26.10. Hence for each $\mathbf{X} \in GL_n(K)$, the ring $\mathbf{X} \cdot M_n(R) \cdot \mathbf{X}^{-1}$ is also a maximal R -order in $M_n(K)$. Thus, when $n > 1$, there are many possible maximal orders in the matrix algebra $M_n(K)$.
- (iv) Let L be a finite Galois extension of K with Galois group G , and let S be the integral closure of R in L . The *twisted group ring* $S \circ G$ is defined as the free S -module with basis $\{u_\sigma : \sigma \in G\}$, with multiplication defined by the formulas

$$u_\sigma u_\tau = u_{\sigma\tau}, \quad u_\sigma a = \sigma(a)u_\sigma, \quad \sigma, \tau \in G, a \in S.$$

Then $S \circ G$ is a maximal R -order in the twisted group algebra $L \circ G$ if and only if S is unramified over R . The result is due to Auslander-Goldman [60b]; see (28.5).

(v) Let L be any full R -lattice in a f.d. K -space V . Then $\text{End}_R L$ is a maximal R -order in $\text{End}_K V$, by §26C. This result is a generalization of (iii) above.

§26B. Maximal Orders Are Hereditary

Let Λ be an R -order in a f.d. K -algebra A . We call Λ *left hereditary* if every left ideal of Λ is projective as Λ -module. As pointed out in (4.6), an integral domain is hereditary if and only if it is a Dedekind domain. This result has a beautiful and useful generalization: every maximal order in a semisimple algebra is both left and right hereditary. (The converse is false, however! There exist hereditary orders which are not maximal; see §26C.)

One way of getting information about an R -order Λ and its representation theory, is to embed Λ in a maximal R -order Λ' , and then use properties of Λ' (see §33, for example). In this approach, the fact that Λ' is hereditary is often of great importance.

The result that maximal orders are hereditary is an almost trivial corollary of the structure theorems listed in §26C; see MO, Theorem 21.4. This subsection may therefore be skipped in a first reading, if desired. However, it seems worthwhile to include here a self-contained proof of the result, which avoids the use of the structure theorems, and instead follows closely one of the standard proofs that every ideal in a Dedekind domain factors uniquely into a product of prime ideals. Indeed, this latter fact is merely a special case of the theorem proved below. In any case, it is fascinating to see how the usual proof for the commutative case can be modified to deal with noncommutative arithmetic. Our proof depends upon elementary manipulations with ideals in maximal orders, and at the end, benefits from some simplifications given in Swan-Evans [70].

The main result is as follows:

(26.12) Theorem. *Let Λ be a maximal R -order in a f.d. semisimple K -algebra A . Then:*

- (i) *The ring Λ is left and right hereditary, that is, every one-sided ideal of Λ is projective as Λ -module.*
- (ii) *Every left (or right) Λ -lattice is Λ -projective.*
- (iii) *A left Λ -lattice M is indecomposable if and only if KM is a simple left A -module.*

The difficulty lies in proving Λ left hereditary; the other assertions are then easily established. Let us show first that the problem can be reduced to the study of full left Λ -lattices in A . Let M be any left ideal of Λ . Then KM is a left ideal of the semisimple ring A , so $A = KM \oplus W$ for some left ideal W in A . We now set $L = \Lambda \cap W$, so by (23.7) L is a left ideal of Λ such that

$$K(M \oplus L) = KM \oplus KL = KM \oplus W = A.$$

If we can prove that the left ideal $M \oplus L$ of Λ is Λ -projective, then M is also projective by §2D. Now $M \oplus L$ is a *full* left Λ -lattice in A , that is, $K(M \oplus L) = A$. Thus, in order to prove that Λ is left hereditary, it suffices to show that every full left Λ -lattice in A is Λ -projective.

For the remainder of this subsection, the word “ideal” will mean a one-sided (or two-sided) ideal M of Λ such that $KM = A$. Keeping this in mind from now on, we make the following definition:

(26.13) Definition. A *prime ideal* of the R -order Λ is a proper two-sided ideal \mathfrak{p} of Λ , such that for each pair of two-sided ideals I and J ,

$$I \cdot J \subseteq \mathfrak{p} \Rightarrow I \subseteq \mathfrak{p} \text{ or } J \subseteq \mathfrak{p}.$$

Evidently, the maximal two-sided ideals of Λ are prime ideals. It can be shown in this case (where Λ is an order) that the converse is also true (see Exercise 26.4).

In order to prove Theorem 26.12, we shall make use of the following theorem*, which is of interest in itself:

(26.14) Theorem. Let Λ be a maximal R -order in a f.d. semisimple K -algebra A . Then the set of full two-sided Λ -sublattices of A is a free abelian group with the prime ideals of Λ as generators.

Proof. Step 1. We show first that every two-sided ideal of Λ must contain a finite product of prime ideals (where the “empty” product is interpreted as Λ itself). If the result is false, there is a maximal counterexample J_0 , since Λ is noetherian by (3.4). Since J_0 is not a prime ideal (obviously), there exist two-sided ideals I and J , neither contained in J_0 , such that $IJ \subseteq J_0$. But then $I+J_0$ and $J+J_0$ both properly contain J_0 , hence are not counterexamples, and thus each contains a product of prime ideals. But then so does J_0 , since $J_0 \supseteq (I+J_0)(J+J_0)$. This contradiction shows that every two-sided ideal contains a product of prime ideals.

We now define “inverses” of ideals as follows: given any full R -lattice L in A , let

$$(26.15) \quad L^{-1} = \{x \in A : L \cdot x \cdot L \subseteq L\}$$

$$= \{x \in A : Lx \subseteq O_L(L)\} = \{x \in A : xL \subseteq O_R(L)\},$$

where the left order $O_L(L)$ of L , and the right order $O_R(L)$, are defined as in

*Compare with Exercise 35.11. Another proof of Theorem 26.14, based on the structure theorems in §26C, is given in MO, Theorem 22.10.

(24.3). There are obvious inclusions

$$(26.16) \quad O_l(L^{-1}) \supseteq O_r(L), \quad O_r(L^{-1}) \supseteq O_l(L).$$

Furthermore, $L \supseteq M$ implies that $L^{-1} \subseteq M^{-1}$ for any pair of full R -lattices L and M in A which have the same left order. We do *not* know at this point that $(L^{-1})^{-1} = L$, though indeed this formula turns out to be true when L is a Λ -lattice for a maximal order Λ (see Exercise 26.6).

Step 2. Let J be a proper two-sided ideal of the maximal order Λ . It is clear that $J^{-1} \supseteq \Lambda$. We now show that $J^{-1} \supset \Lambda$, by assuming that $J^{-1} = \Lambda$ and obtaining a contradiction. We may choose a prime ideal \mathfrak{p} of Λ with $J \subseteq \mathfrak{p} \subset \Lambda$; then $\mathfrak{p}^{-1} \subseteq J^{-1} = \Lambda$ whence $\mathfrak{p}^{-1} = \Lambda$. To show that this is impossible, note first that $K\mathfrak{p} = A$, so $1_A = \lambda x$ for some $\lambda \in K$ and $x \in \mathfrak{p}$. Clearing the denominator, we obtain a nonzero element $\alpha \in R \cap \mathfrak{p}$. By Step 1, $\alpha\Lambda$ contains a product of prime ideals, and so we may write

$$\mathfrak{p} \supseteq \alpha\Lambda \supseteq \mathfrak{p}_1 \cdots \mathfrak{p}_r,$$

with the $\{\mathfrak{p}_i\}$ prime ideals, and where r is minimal for this α . Since $\mathfrak{p} \supseteq \mathfrak{p}_1 \cdots \mathfrak{p}_r$, it follows that $\mathfrak{p} \supseteq \mathfrak{p}_j$ for some j , whence $\mathfrak{p} = \mathfrak{p}_j$. Thus we may rewrite the above display as

$$\mathfrak{p} \supseteq \alpha\Lambda \supseteq B \cdot \mathfrak{p} \cdot C$$

where BC is a product of $r-1$ prime ideals of Λ . Using the fact that Λ is a maximal order, we then obtain:

$$\begin{aligned} \alpha^{-1}B\mathfrak{p}C \subseteq \Lambda &\Rightarrow \alpha^{-1}B\mathfrak{p}C \cdot B \subseteq B \Rightarrow \alpha^{-1}\mathfrak{p}CB \subseteq O_r(B) = \Lambda \\ &\Rightarrow \alpha^{-1}CB \subseteq \mathfrak{p}^{-1} = \Lambda \Rightarrow \alpha\Lambda \supseteq BC, \end{aligned}$$

contradicting the minimality of r . This completes the proof that $J^{-1} \supset \Lambda$.

Step 3. Let L be a full R -lattice in A such that $O_l(L)$ is maximal; we claim that

$$(26.17) \quad L \cdot L^{-1} = O_l(L).$$

Indeed, let $\Gamma = O_l(L)$, $J = L \cdot L^{-1}$, so J is a two-sided ideal in the maximal order Γ . Then

$$JJ^{-1} \subseteq \Gamma \Rightarrow LL^{-1} \cdot J^{-1} \subseteq \Gamma \Rightarrow L^{-1}J^{-1} \subseteq J^{-1} \Rightarrow J^{-1} \subseteq O_r(L^{-1}).$$

But $O_r(L^{-1}) \supseteq \Gamma$ by (26.16), so $O_r(L^{-1}) = \Gamma$ (since Γ is maximal), and thus $J^{-1} \subseteq \Gamma$. Hence $J = \Gamma$ by Step 2, and (26.17) is proved. In the same manner it

follows that if N is a full R -lattice in A whose right order $O_r(N)$ is maximal, then $N^{-1}N = O_r(N)$.

Consequently, for every two-sided ideal J of the maximal order Λ , we have

$$(26.18) \quad JJ^{-1} = J^{-1}J = \Lambda.$$

Further, we may choose a nonzero $\beta \in R$ such that $\beta J^{-1} \subseteq \Lambda$; then by the above,

$$(\beta J^{-1})(\beta J^{-1})^{-1} = \Lambda, \text{ that is, } (J^{-1})(J^{-1})^{-1} = \Lambda.$$

This proves that

$$(J^{-1})^{-1} = J.$$

Let us deduce from this that every two-sided ideal J of Λ is uniquely expressible as a finite product of prime ideals, and that multiplication of such ideals is commutative. (If $J = \Lambda$, write J as an “empty” product of prime ideals!) Suppose the result false, and let J be a maximal counterexample. Then J is not prime, so there exists a prime ideal \mathfrak{p} with $J \subset \mathfrak{p} \subset \Lambda$, whence

$$J \subseteq J\mathfrak{p}^{-1} \subseteq \Lambda.$$

If $J = J\mathfrak{p}^{-1}$ then $\mathfrak{p}^{-1} \subseteq O_r(J) = \Lambda$, which is impossible by Step 2. Hence $J\mathfrak{p}^{-1} \supsetneq J$, and so $J\mathfrak{p}^{-1}$ is a product $\mathfrak{p}_1 \cdots \mathfrak{p}_k$ of primes; but then $J = J\mathfrak{p}^{-1} \cdot \mathfrak{p} = \mathfrak{p}_1 \cdots \mathfrak{p}_k \mathfrak{p}$, a contradiction. This shows that every two-sided ideal of Λ is expressible as a product of prime ideals.

Now let $\mathfrak{p}, \mathfrak{q}$ be distinct primes; then

$$\mathfrak{p}^{-1}\mathfrak{q}\mathfrak{p} \subseteq \mathfrak{p}^{-1} \cdot \Lambda \cdot \mathfrak{p} \subseteq \Lambda,$$

and

$$\mathfrak{p}(\mathfrak{p}^{-1}\mathfrak{q}\mathfrak{p}) = \mathfrak{q}\mathfrak{p} \subseteq \mathfrak{q}.$$

Thus \mathfrak{q} contains the product of \mathfrak{p} and $\mathfrak{p}^{-1}\mathfrak{q}\mathfrak{p}$, a pair of two-sided ideals of Λ . Since \mathfrak{q} is prime, this gives $\mathfrak{q} \supseteq \mathfrak{p}^{-1}\mathfrak{q}\mathfrak{p}$, so $\mathfrak{p}\mathfrak{q} \supseteq \mathfrak{q}\mathfrak{p}$. The reverse inclusion holds by symmetry, and thus $\mathfrak{p}\mathfrak{q} = \mathfrak{q}\mathfrak{p}$.

Now suppose that the $\{\mathfrak{p}_i\}$, $\{\mathfrak{q}_j\}$ are prime ideals for which

$$\mathfrak{p}_1 \cdots \mathfrak{p}_r = \mathfrak{q}_1 \cdots \mathfrak{q}_s.$$

Then $\mathfrak{p}_1 \supseteq \mathfrak{q}_1$, so $\mathfrak{p}_1 = \mathfrak{q}_1$ for some I . Multiply by \mathfrak{p}_1^{-1} and repeat the argument, so as to deduce eventually that the $\{\mathfrak{p}_i\}$ are just a rearrangement of the $\{\mathfrak{q}_j\}$. This shows that every two-sided ideal of Λ is uniquely expressible as a finite product of prime ideals (apart from order of occurrence), and that multiplication of such ideals is commutative.

To complete the proof of (26.14), it suffices to show that every full two-sided Λ -lattice J in A can be expressed as a product of prime ideals and inverses of prime ideals. But $\alpha J \subseteq \Lambda$ for some nonzero $\alpha \in R$, and $J = (\alpha\Lambda)^{-1} \cdot \alpha J$. If we write $\alpha\Lambda = \prod p_i$, and $\alpha J = \prod q_j$, then we obtain $J = \{\prod p_i^{-1}\} \{\prod q_j\}$, as desired. This establishes (26.14).

(We should point out an important special case of (26.14). Let E be an algebraic number field, and let $S = \text{alg. int. } \{E\}$. Then S is the integral closure of \mathbb{Z} in E , so S is a maximal \mathbb{Z} -order in E by (26.10). It then follows from (26.14) that every nonzero ideal of S is uniquely expressible as a product of maximal ideals of S , and that the group of fractional S -ideals of E is the free abelian group generated by these maximal ideals.)

Let us continue with our main objective: the proof of Theorem 26.12. We show next that every two-sided ideal J of Λ is both left and right Λ -projective. Since $J^{-1}J = \Lambda$ by (26.18), we may write

$$1 = \sum_{i=1}^n x_i m_i, \quad x_i \in J^{-1}, \quad m_i \in J,$$

for some choices of elements $\{x_i\}$, $\{m_i\}$. Now define

$$\varphi: \Lambda^{(n)} \rightarrow J \text{ by } \varphi(a_1, \dots, a_n) = \sum a_i m_i, \quad a_i \in \Lambda,$$

$$\psi: J \rightarrow \Lambda^{(n)} \text{ by } \psi(m) = (mx_1, \dots, mx_n), \quad m \in J.$$

Then φ and ψ are left Λ -homomorphisms such that $\varphi\psi$ is the identity map on J . Therefore J is a direct summand of Λ (as left Λ -module), and hence J is left Λ -projective. Likewise, J is projective as right Λ -module. (Compare this argument with the proof of the Dual Basis Lemma 3.46.)

To complete the proof of (26.12i), we shall use some elementary facts about the *homological dimension* $\text{hd}(T)$ of a left Λ -module T . (This approach saves two pages of manipulation!) By definition, $\text{hd}(T)$ is the smallest integer k (if such exists) such that

$$\text{Ext}_{\Lambda}^n(T, *) = 0 \text{ for all } n > k.$$

(Write $\text{hd}(T) = \infty$ if no such k exists.) We now prove that

$$(26.19) \quad \text{hd}(T) \leq 1 \text{ for every f.g. } R\text{-torsion } \Lambda\text{-module } T.$$

(In the above, T is a f.g. left Λ -module which is a torsion R -module.) Taking this for granted for the moment, let M be any full left ideal of Λ . Then there is an exact sequence of left Λ -modules:

$$0 \rightarrow M \rightarrow \Lambda \rightarrow T \rightarrow 0.$$

Since $K \cdot M = K \cdot \Lambda$, it follows that T is a f.g. R -torsion Λ -module, whence $\text{Ext}_{\Lambda}^2(T, *) = 0$. But

$$\text{Ext}_{\Lambda}^1(\Lambda, *) \rightarrow \text{Ext}_{\Lambda}^1(M, *) \rightarrow \text{Ext}_{\Lambda}^2(T, *)$$

is exact by (8.6), and $\text{Ext}_{\Lambda}^1(\Lambda, *) = 0$ by (8.4v). Hence we obtain $\text{Ext}_{\Lambda}^1(M, *) = 0$, so M is Λ -projective by (8.4v). Thus, every full left ideal of Λ is projective. It follows from Step 1 that Λ is left hereditary, as claimed.

We shall now prove (26.19). We have $\beta T = 0$ for some nonzero $\beta \in R$, so T may be viewed as a f.g. module over the ring $R/\beta R$. But $R/\beta R$ is artinian and noetherian, whence so is the $(R/\beta R)$ -module T , by §3A. Since every Λ -submodule of T is automatically an R -submodule of T , it follows that T is both artinian and noetherian as left Λ -module. Therefore T has a Λ -composition series by (3.8). We shall prove (26.19) by induction on the Λ -composition length $l(T)$ of the Λ -module T .

Consider first the case where $l(T) = 1$, so T is a simple left Λ -module, and $\beta T = 0$ for some nonzero $\beta \in R$. By (26.14), we may write

$$\beta\Lambda = \prod_{i=1}^r \mathfrak{p}_i^{e_i},$$

with the $\{\mathfrak{p}_i\}$ distinct prime ideals of Λ . For each i , $\mathfrak{p}_i T$ is a Λ -submodule of the simple module T , and thus $\mathfrak{p}_i T$ is either 0 or T . If $\mathfrak{p}_i T = T$ for each i , then $\beta T = T$, which is impossible. Hence there exists an index i such that $\mathfrak{p}_i T = 0$. Then T is also a simple left $\bar{\Lambda}$ -module, where $\bar{\Lambda} = \Lambda/\mathfrak{p}_i$. Now $\bar{\Lambda}$ is a simple artinian ring by Exercise 26.4, so T is isomorphic to a direct summand of $\bar{\Lambda}$ (as left $\bar{\Lambda}$ -module). But then T is also isomorphic to a direct summand of $\bar{\Lambda}$ as left Λ -module, whence by (8.4iv) we have $\text{hd}_{\Lambda}(T) \leq \text{hd}_{\Lambda}(\bar{\Lambda})$. But

$$0 \rightarrow \mathfrak{p}_i \rightarrow \Lambda \rightarrow \bar{\Lambda} \rightarrow 0$$

is an exact sequence of left Λ -modules, and \mathfrak{p}_i is left Λ -projective by the earlier discussion. Hence $\text{hd}_{\Lambda}(\bar{\Lambda}) \leq 1$ by (8.6), so also $\text{hd}_{\Lambda}(T) \leq 1$, which proves (26.19) whenever T is a simple Λ -module.

Suppose now that $l(T) = d > 1$, and that $\text{hd}(T') \leq 1$ for all f.g. R -torsion left Λ -modules T' with $l(T') = d - 1$. Let T_0 be any simple Λ -submodule of T . Then there is an exact sequence

$$0 \rightarrow T_0 \rightarrow T \rightarrow T' \rightarrow 0,$$

where $l(T') = d - 1$. Then $\text{hd}(T_0) \leq 1$, $\text{hd}(T') \leq 1$, whence also $\text{hd}(T) \leq 1$ by (8.6). This completes the proof of (26.19).

We have now completed the proof that Λ is left hereditary. To prove that Λ is also right hereditary, we may use either of two arguments. On the one hand, the desired result follows from a theorem of M. Auslander: *If the ring Λ*

is left and right noetherian, then Λ is left hereditary if and only if Λ is right hereditary. (For a proof, see Rotman [79, Cor. 9.23].)

A second approach is as follows: let Λ° denote the opposite ring of Λ . Then Λ° is a maximal R -order in the semisimple K -algebra A° , so Λ° is left hereditary by the previous steps. Every right Λ -module may be viewed as left Λ° -module, and vice versa. Hence Λ is right hereditary, as claimed.

Assertion (ii) of Theorem 26.12 follows at once from Exercise 23.1 and Proposition 4.3. Finally, let M be any left Λ -lattice. If M is decomposable, then so is KM , whence KM is not a simple A -module. Conversely, suppose that W is a nonzero proper submodule of KM , and set $L = W \cap M$. By (23.15) there is then an exact sequence of Λ -lattices:

$$0 \rightarrow L \rightarrow M \rightarrow M/L \rightarrow 0.$$

But M/L is Λ -projective by (26.12ii), whence the sequence splits: $M \cong L \oplus (M/L)$ as Λ -modules. We have thus shown that M is decomposable if and only if KM is not simple, which completes the proof of assertion (iii), and establishes the theorem.

Remark. There exist left hereditary rings which are not right hereditary; for example (see L. Small [66]), the ring

$$\left\{ \begin{pmatrix} a & 0 \\ b & c \end{pmatrix} : a \in \mathbb{Z}, b, c \in \mathbb{Q} \right\}$$

is left but not right hereditary.

§26C. Structure Theorems for Maximal and Hereditary Orders

Throughout this subsection, let R be a Dedekind domain with quotient field K . We shall summarize without proof a number of basic facts about maximal and hereditary orders. Detailed proofs may be found in MO, and we shall not repeat them here. Of course, we already know from §26B that every maximal order is hereditary, so we may expect that theorems about the structure of maximal orders will generalize to the case of hereditary orders.

The first part of the discussion shows that for both maximal and hereditary orders, the problem of determining their structure can be reduced to the case of orders in simple algebras over local fields. There is a further reduction to the case of orders in division algebras over local fields, in which case we have extremely explicit information. We conclude with a discussion of the behavior of maximal and hereditary orders under ground ring extension.

To begin with, we quote a result showing that the study of maximal and hereditary orders can be reduced to the case of central simple algebras.

(26.20) Theorem. *Let A be a separable f.d. K -algebra, and write*

$$A = A_1 \oplus \cdots \oplus A_t, \quad 1 = e_1 + \cdots + e_t, \quad e_i \in A_i,$$

where the $\{A_i\}$ are the Wedderburn components of A , and the $\{e_i\}$ the corresponding central primitive idempotents. For each i , let K_i be the center of A_i , and R_i the integral closure of R in K_i . Then:

- (i) For each maximal R -order Λ in A , we have $\Lambda = \bigoplus_{i=1}^t \Lambda e_i$, and for each i , Λe_i is a maximal R -order in A_i .
- (ii) Conversely, if Λ_i is a maximal R -order in A_i for each i , then $\bigoplus \Lambda_i$ is a maximal R -order in A .
- (iii) An R -order Λ_i in A_i is a maximal R -order in A_i if and only if Λ_i is a maximal R_i -order in A_i .
- (iv) In the special case where R is a complete d.v.r., the above assertions remain true whenever A is a semisimple algebra, whether or not separable over K .

(26.20a) Theorem. The preceding Theorem 26.20 remains true if “maximal” is replaced by “hereditary” throughout.

For the proof of (26.20), see MO (10.5); for (26.20a), see MO (10.8), (10.9) and (40.7). The proofs are rather straightforward.

Our next results show the connection between the global and local cases. Let P range over all maximal ideals of R , and let R_P denote localization at P , and \hat{R}_P P -adic completion. If Λ is any R -order in a f.d. K -algebra A , then Λ_P is an R_P -order in A , and $\hat{\Lambda}_P$ is an \hat{R}_P -order in \hat{A}_P . We have:

(26.21) Theorem. (i) For any R -order Λ in a f.d. K -algebra A , we have

$$\Lambda = \bigcap_P \Lambda_P = \bigcap_P (\hat{\Lambda}_P \cap A).$$

(ii) Λ is a maximal R -order in A if and only if for each P , Λ_P is a maximal R_P -order in A .

(iii) Let P be fixed, and let Δ be an R_P -order in A . Then Δ is a maximal R_P -order in A if and only if its P -adic completion $\hat{\Delta}_P$ is a maximal \hat{R}_P -order in \hat{A}_P .

(26.21a) Theorem. The preceding Theorem 26.21 remains true if “maximal” is replaced by “hereditary” throughout.

Assertion (26.21i) is clear from (4.21), and is restated here for convenience. For (26.21ii) see MO (11.2), and MO (11.5) for (26.21iii). For the proof of (26.21a), see MO (3.24), (2.22) and (2.39).

The theorems above show that the study of maximal (and hereditary) orders can be reduced to the study of such orders in central simple algebras over local fields. The key to the latter situation is the fact that if D is a division algebra over a complete local field K , and R the d.v.r. in K , then D has a unique maximal R -order Δ . This order Δ is the integral closure of R in D , and behaves in every way like a d.v.r., except for the fact that multiplication is not commutative. If R has a finite residue class field \bar{R} , as is the case most often encountered, even stronger results are available. Finally, the passage from D to a matrix algebra over D is accomplished by use of the Morita Theorems.

The main facts concerning maximal orders in division rings are summarized in the following theorem; for proofs, see MO (12.8), (13.2), (13.3) and (14.3).

(26.22) Theorem. *Let R be a complete d.v.r. with exponential valuation* v , prime element π , field of quotients K , and residue class field $\bar{R} = R/\pi R$. Let D be a skewfield with center K , and let $\dim_K D = m^2$, m finite.*

(i) Define

$$w(a) = \frac{1}{m^2} v(N_{D/K} a), \quad a \in D,$$

where $N_{D/K}$ is the usual norm from D to K . Then w is a discrete valuation on D which extends v . The valuation ring of w is given by

$$\Delta = \{a \in D : w(a) \geq 0\} = \{a \in D : N_{D/K} a \in R\}.$$

This ring Δ is the integral closure of R in D , and is the unique maximal R -order in D .

(ii) Let π_D be a prime element of Δ , that is, an element for which $w(\pi_D) = 1$. Set $\mathfrak{p} = \pi_D \Delta$, $\bar{\Delta} = \Delta/\mathfrak{p}$. Then \mathfrak{p} is a two-sided ideal of Δ , and every nonzero two-sided ideal of Δ is a power of \mathfrak{p} . Further

$$\mathfrak{p}^k = \pi_D^k \Delta = \Delta \pi_D^k = \{a \in \Delta : w(a) \geq k\}.$$

Every one-sided ideal of Δ is a two-sided ideal.

(iii) The residue class ring $\bar{\Delta}$ is a skewfield whose center contains \bar{R} , and

$$f = \dim_{\bar{R}} \bar{\Delta} = \text{inertial degree of } D \text{ over } K$$

is finite. We have

$$\dim_K D = m^2 = ef, \text{ where } e = w(\pi) = \text{ramification index of } D \text{ over } K.$$

*See §4C.

(iv) If the field \bar{R} is finite, then

$$e=f=m=\sqrt{\dim_K D}.$$

Using the Morita Theorems to extend the above to the classification of maximal orders in a full matrix algebra $M_r(D)$, we obtain (see MO (17.3), (17.4)):

(26.23) Theorem. *Keep the above notation, and let $A = M_r(D)$.*

(i) *Let $\Lambda = M_r(\Delta)$. Then Λ is a maximal R -order in A , and its unique maximal two-sided ideal is $\pi_D \Lambda$. Every nonzero two-sided ideal of Λ is of the form*

$$(\pi_D \Lambda)^k = \pi_D^k \Lambda = M_r(\pi_D^k \Delta), k=0,1,2,\dots.$$

We have $\text{rad } \Lambda = \pi_D \Lambda$, and

$$\Lambda / \text{rad } \Lambda \cong M_r(\bar{\Delta}), \text{ where } \bar{\Delta} = \Delta / \pi_D \Delta.$$

(ii) *The maximal R -orders in A are precisely the rings $u\Lambda u^{-1}$, with u a unit of A .*

(iii) *Let $A = \text{End}_D V$, where V is a right D -space of dimension r . Let Γ be any maximal R -order in A ; then there exists a full right Δ -lattice M in V , which is free of rank r as Δ -module, such that $\Gamma = \text{End}_\Delta M$. Conversely, each such endomorphism ring is a maximal order.*

This result readily carries over to the case where the d.v.r. R is not necessarily complete (see MO (18.3), (18.7), and (18.10)):

(26.24) Theorem. *Let R be a d.v.r. with maximal ideal P , and let \hat{R} be its P -adic completion, and \hat{K} the P -adic completion of K . Let A be a central simple K -algebra.*

(i) *The maximal R -orders Λ in A are of the form $\Lambda = A \cap \hat{\Lambda}$, with $\hat{\Lambda}$ ranging over the maximal \hat{R} -orders in \hat{A} . Further, $\hat{\Lambda}$ is the completion of Λ . If $\text{rad } \hat{\Lambda}$ denotes the unique maximal two-sided ideal of $\hat{\Lambda}$, then*

$$\text{rad } \Lambda = \Lambda \cap \text{rad } \hat{\Lambda} = \text{unique maximal two-sided ideal of } \Lambda.$$

Further, $\text{rad } \hat{\Lambda}$ is the completion of $\text{rad } \Lambda$, and

$$\Lambda / \text{rad } \Lambda \cong \hat{\Lambda} / \text{rad } \hat{\Lambda}.$$

(ii) Let $\hat{A} \cong M_r(D)$, where D is a skewfield. Then D has center \hat{K} , and has a unique maximal \hat{R} -order Δ (as in (26.22)). We have

$$\Lambda / \text{rad } \Lambda \cong \hat{\Lambda} / \text{rad } \hat{\Lambda} \cong M_r(\bar{\Delta}),$$

where $\bar{\Delta} = \Delta / \pi_D \Delta$ is a skewfield of finite dimension f over \bar{R} . Further,

$$P\Lambda = (\text{rad } \Lambda)^e, \text{ where } ef = \dim_{\hat{K}} D.$$

If \bar{R} is finite, then

$$e = f = \sqrt{\dim_{\hat{K}} D} .$$

(iii) Every one-sided ideal of Λ is a principal ideal. More generally*, let M and N be a pair of left Λ -lattices. Then $M \cong N \Leftrightarrow KM \cong KN$ as A -modules $\Leftrightarrow M$ and N have the same R -rank.

Returning to the global case, we may combine the results of Theorems 26.21 and 26.23 to obtain:

(26.25) Theorem. Let R be any Dedekind domain, with quotient field K . Let D be a f.d. division algebra over its center K . Let V be a f.d. right vector space over D , and let $A = \text{End}_D V$, a central simple K -algebra.

(i) Let Δ be some fixed maximal R -order in D . Then for every full right Δ -lattice M in V , the ring $\text{End}_{\Delta} M$ is a maximal R -order in A .

(ii) Let Δ be as above. Then each maximal R -order Γ in A is of the form $\Gamma = \text{End}_{\Delta} N$ for some full right Δ -lattice N in V .

(iii) The maximal order Δ is not necessarily unique. However, any two maximal orders in D must be Morita equivalent. Therefore each pair of maximal orders in A must be Morita equivalent.

(The proofs are given in MO (21.6), (21.7) and MO Exercise 22.11. Also see Exercise 26.10 below.)

It is extremely useful to know whether maximal orders remain maximal after ground ring extension. As above, the problem reduces to the case of simple algebras over local fields, and for this case the question is completely settled by:

*The result for lattices implies the assertion about ideals. Indeed, if M is a left ideal of Λ , then KM is a left ideal of A . Therefore $KM = Ax = K \cdot \Lambda x$ for some $x \in A$, and so $M \cong \Lambda x$.

(26.26) Theorem (Janusz [79]). Let R be a complete d.v.r. with quotient field K . For $i = 1, 2$, let A_i be a central simple E_i -algebra, where E_i is a finite separable extension of K , and let S_i be the integral closure of R in E_i . Let Λ_i be a maximal R -order in A_i , $i = 1, 2$. Then $\Lambda_1 \otimes_R \Lambda_2$ is a maximal R -order in the semisimple K -algebra $A_1 \otimes_K A_2$ if and only if one of the orders, say Λ_1 , satisfies the following two conditions:*

(i) $\Lambda_1 \cong M_n(S_1)$ and S_1 is unramified over R ,

(ii) $\text{G.C.D.}(f_1, f_2m) = \text{G.C.D.}(f_1, f_2)$, where

$m = \text{index of } A_2, f_i = \text{residue class degree of } S_i \text{ relative to } R$ ($i = 1, 2$).

We omit the proof, which is based on calculations of discriminants. Janusz also showed that if $\Lambda_1 \otimes \Lambda_2$ is a maximal order, then Λ_1 and Λ_2 must both be maximal. As a special case of the above theorem, we have:

(26.27) Corollary. Keep the above notation, and let $\Lambda_1 = S_1$, $A_1 = E_1$. Then $S_1 \otimes_R \Lambda_2$ is a maximal S_1 -order in $E_1 \otimes_K A_2$ whenever S_1 is unramified over R and

$$\text{G.C.D.}(f_1, f_2m) = \text{G.C.D.}(f_1, f_2).$$

Turning next to hereditary orders, we shall give an analogue of Theorem 26.23 which describes the structure of hereditary orders in simple algebras over local fields. Some notation will be helpful. Let $\{\alpha_{ij} : 1 \leq i, j \leq r\}$ be a set of ideals in a ring Γ . Then the expression

$$\begin{bmatrix} (\alpha_{11}) & (\alpha_{12}) & \cdots & (\alpha_{1r}) \\ (\alpha_{21}) & (\alpha_{22}) & \cdots & (\alpha_{2r}) \\ \vdots & \vdots & \ddots & \vdots \\ (\alpha_{r1}) & (\alpha_{r2}) & \cdots & (\alpha_{rr}) \end{bmatrix}^{\{n_1, \dots, n_r\}}$$

denotes the set of all matrices

$$\begin{bmatrix} \mathbf{T}_{11} & \mathbf{T}_{12} & \cdots & \mathbf{T}_{1r} \\ \mathbf{T}_{21} & \mathbf{T}_{22} & \cdots & \mathbf{T}_{2r} \\ \vdots & \vdots & \ddots & \vdots \\ \mathbf{T}_{r1} & \mathbf{T}_{r2} & \cdots & \mathbf{T}_{rr} \end{bmatrix}$$

where for each pair (i, j) , the matrix \mathbf{T}_{ij} ranges over all $n_i \times n_j$ matrices with entries in the ideal α_{ij} .

We are now ready to state the main result, whose proof is given in MO (39.14), (39.23) and (39.24):

*See §4B for the definitions of “unramified” and of f_i . The index of A_2 is defined as in (7.46).

(26.28) Theorem. Let R be a complete d.v.r. with quotient field K , D a f.d. division algebra over its center K , Δ the integral closure of R in D , and $\mathfrak{p} = \text{rad } \Delta$ (as in (26.22)). Let $A = M_n(D)$, and let Λ be a hereditary R -order in A . Then we have:

(i) After a similarity transformation $\Lambda \rightarrow \mathbf{X} \Lambda \mathbf{X}^{-1}$, for some $\mathbf{X} \in GL_n(D)$, we may write

$$\Lambda = \begin{bmatrix} (\Delta) & (\mathfrak{p}) & (\mathfrak{p}) & \cdots & (\mathfrak{p}) \\ (\Delta) & (\Delta) & (\mathfrak{p}) & \cdots & (\mathfrak{p}) \\ (\Delta) & (\Delta) & (\Delta) & \cdots & (\mathfrak{p}) \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ (\Delta) & (\Delta) & (\Delta) & \cdots & (\Delta) \end{bmatrix}^{\{n_1, \dots, n_r\}}$$

for some positive integers $\{n_i\}$ with sum n .

(ii) $\text{rad } \Lambda$ is obtained from the above display by replacing each (Δ) on the main diagonal by (\mathfrak{p}) . Therefore

$$\Lambda / \text{rad } \Lambda \cong \coprod_{i=1}^r M_{n_i}(\bar{\Delta}), \text{ where } \bar{\Delta} = \Delta / \mathfrak{p}.$$

(iii) The isomorphism invariants of the hereditary order Λ are its type r and the cycle $\{n_1, \dots, n_r\}$. These determine Λ up to similarity.

(iv) Let M be the space of $n \times 1$ column vectors over Δ . Then

$$\{(\text{rad } \Lambda)^i M : 0 \leq i \leq r-1\}$$

is a full set of nonisomorphic indecomposable Λ -lattices. For each i , $(\text{rad } \Lambda)^i M$ consists of all column vectors whose first $n_1 + \dots + n_i$ entries lie in \mathfrak{p} , and whose remaining entries are arbitrary elements of Δ .

(v) There are precisely r maximal orders containing Λ , and Λ is their intersection.

To conclude this section, we record without proof the analogue of (26.26):

(26.29) Theorem (Janusz [79]). Let R be a complete d.v.r. with quotient field K , and let Λ_1 and Λ_2 be R -orders in f.d. simple separable K -algebras. Then $\Lambda_1 \otimes_R \Lambda_2$ is a hereditary R -order if and only if both Λ_1 and Λ_2 are hereditary, and one of them is a full matrix ring over a d.v.r. which is unramified over R .

As a special case, we obtain

(26.30) Corollary. Hereditary orders remain hereditary under unramified extensions of the ground ring.

§26. Exercises

1. Let Λ be an R -order in the K -algebra A , and let T be the ordinary trace map from A to K . Suppose that $\Lambda = Rx_1 \oplus \cdots \oplus Rx_m$, and that

$$\alpha = \det [T(x_i, x_j)]_{1 \leq i, j \leq m}$$

is a nonzero element of R . Show that the localization Λ_P is a maximal R_P -order in A for every maximal ideal P of R such that $\alpha \notin P$.

[Hint: Let Λ' be an R -order in A containing Λ . As in the proof of (26.8), we have $\Lambda' \subseteq \alpha^{-1}\Lambda$. Therefore $\Lambda'_P = \Lambda_P$ whenever $\alpha \notin P$.]

2. Let G be a finite group, and suppose $|G|$ is a unit in R . Deduce from Exercise 1 that RG is a maximal R -order in KG .

3. Prove that a non-maximal order cannot be a principal ideal ring.

[Hint: Let $\Lambda \subset \Lambda'$ be R -orders, and choose a nonzero $\alpha \in R$ such that $\alpha\Lambda' \subset \Lambda$, so $\alpha\Lambda'$ is a left ideal of Λ . If $\alpha\Lambda' = \Lambda x$ for some $x \in A$, then $\Lambda' = \Lambda y$ for some y . Hence $\Lambda' = \Lambda'y$, so $y \in u(\Lambda')$. Therefore $\Lambda' = \Lambda'y^{-1} = (\Lambda y)y^{-1} = \Lambda$, a contradiction.]

4. Let Λ be an R -order in a K -algebra A , and let J be a two-sided ideal in Λ such that $K \cdot J = A$. Show that J is a prime ideal if and only if J is a maximal two-sided ideal.

[Hint: Let J be maximal, and let $S \cdot T \subseteq J$ where S, T are two-sided ideals. If $S \not\subseteq J$ and $T \not\subseteq J$, then $S+J = T+J = \Lambda$. But then

$$J \supseteq (S+J)(T+J) = \Lambda,$$

a contradiction.

Conversely, let J be prime, and set $P = J \cap R$, a prime ideal of R . Note that $P \neq 0$ since $K \cdot J = A$. Let $\bar{\Lambda} = \Lambda/J$, $\bar{R} = R/P$; then $\bar{\Lambda}$ is a f.d. \bar{R} -algebra. If $\text{rad } \bar{\Lambda} \neq 0$, its inverse image in Λ is a two-sided ideal S containing J such that $S^k \subseteq J$ for some k , whence $S \subseteq J$, which is impossible. Thus $\text{rad } \bar{\Lambda} = 0$, so $\bar{\Lambda}$ is semisimple. If $\bar{\Lambda}$ is not simple, then there exist two-sided ideals S, T in Λ such that $\bar{S} \cdot \bar{T} = 0$, $\bar{S} \neq 0$, $\bar{T} \neq 0$; then $S \cdot T \subseteq J$, a contradiction. Thus $\bar{\Lambda}$ is a simple artinian ring, hence has no nontrivial two-sided ideals. Thus J is maximal.]

5. Let Λ be a maximal R -order in a central simple K -algebra. Show that there is a bijection between the set of maximal ideals P of R and the set of prime ideals \mathfrak{p} of Λ , given by

$$P = R \cap \mathfrak{p}, \mathfrak{p} = \Lambda \cap \text{rad } \Lambda_P.$$

Further, if $P \leftrightarrow \mathfrak{p}$, Then $P\Lambda = \mathfrak{p}^e$ for some e .

[Hint: Given any prime ideal \mathfrak{p} , we put $P = R \cap \mathfrak{p}$, $\bar{\Lambda} = \Lambda/\mathfrak{p}$, $\bar{R} = R/P$. Then $\bar{\Lambda}$ is a simple artinian \bar{R} -algebra, and P is a maximal ideal of R . We have

$$\bar{\Lambda} \cong R_P \otimes_R \bar{\Lambda} \cong \Lambda_P / \mathfrak{p} \Lambda_P,$$

since the elements of $R - P$ act invertibly on $\bar{\Lambda}$. Since $\bar{\Lambda}$ is simple, we have $\mathfrak{p}\Lambda_P \supseteq \text{rad } \Lambda_P$. To prove equality, suppose that

$$P\Lambda_P = \prod_{i=1}^g \mathfrak{p}_i^{e_i}$$

where $g > 1$. Choose sequences $\{x_n\}, \{y_n\}$ of elements of Λ , such that

$$x_n \equiv 1 \pmod{\mathfrak{p}_1^n}, \quad x_n \equiv 0 \pmod{(\mathfrak{p}_2 \cdots \mathfrak{p}_g)^n},$$

$$y_n \equiv 1 \pmod{\mathfrak{p}_g^n}, \quad y_n \equiv 0 \pmod{(\mathfrak{p}_1 \cdots \mathfrak{p}_{g-1})^n}.$$

If \hat{A}_P denotes the P -adic completion of A , then $x_n \rightarrow x, y_n \rightarrow y$, with x, y idempotents in \hat{A}_P . Clearly $xy = 0$, and furthermore x and y are in the center of \hat{A}_P , since for all $a \in A$ and all n ,

$$ax_n \equiv x_n a, \quad ay_n \equiv y_n a \pmod{(\mathfrak{p}_1 \cdots \mathfrak{p}_g)^n}.$$

This is impossible, since \hat{A}_P is a central simple \hat{K}_P -algebra. Therefore $g = 1$ so $P\Lambda_P = (\mathfrak{p}\Lambda_P)^e$ for some e . It thus follows that $\mathfrak{p}\Lambda_P = \text{rad } \Lambda_P$.

For any maximal ideal Q of R with $Q \neq P$, we have $R_Q \otimes_R \bar{\Lambda} = 0$, whence $\Lambda_Q = \mathfrak{p}_Q$. But then $\mathfrak{p} = \mathfrak{p}_P \cap \left(\bigcap_Q \mathfrak{p}_Q \right) = \mathfrak{p}_P \cap \Lambda = \text{rad } \Lambda_P \cap \Lambda$.

Conversely, given \mathfrak{p} we choose any prime ideal \mathfrak{p} of Λ with $P\Lambda \subseteq \mathfrak{p}$. Then $P = R \cap \mathfrak{p}$, so by the above discussion $\mathfrak{p} = \Lambda \cap \text{rad } \Lambda_P$. This proves the existence of a bijection $P \leftrightarrow \mathfrak{p}$. Finally, if \mathfrak{q} is any prime ideal of Λ occurring in the factorization of $P\Lambda$, then (as above) $\mathfrak{q} = \Lambda \cap \text{rad } \Lambda_P$, whence $\mathfrak{q} = \mathfrak{p}$.]

6. Let M be a full left Λ -lattice in A , where Λ is a maximal R -order in the K -algebra A . Show that $O_r(M)$ is also a maximal R -order in A , and that

$$M^{-1}M = O_r(M), \quad MM^{-1} = \Lambda.$$

Prove also that $(M^{-1})^{-1} = M$.

[Hint: Put $\Gamma = O_r(M) \cong \text{End}_\Lambda M$. Since M is left Λ -projective by (26.12), it follows that

$$\text{Hom}_\Lambda(M, \Lambda) \otimes_\Lambda M \rightarrow \Gamma$$

is surjective. But

$$\text{Hom}_\Lambda(M, \Lambda) \cong \{x \in A : Mx \subseteq \Lambda\} = M^{-1},$$

which implies that $M^{-1}M = \Gamma$.

On the other hand, $MM^{-1} = \Lambda$ by (26.17). If $\Gamma \subseteq \Gamma'$, where Γ' is an R -order in A , then $M\Gamma'M^{-1} \supseteq M\Gamma M^{-1} = MM^{-1} = \Lambda$, so $M\Gamma'M^{-1}$ is an R -order containing Λ . Therefore $M\Gamma'M^{-1} = \Lambda$, whence $\Gamma' = M^{-1}\Lambda M = \Gamma$. Thus Γ is maximal.

Finally, $(M^{-1})^{-1}M^{-1} = \Lambda$ implies that $(M^{-1})^{-1} = M$.]

7. Let M be a left Λ -lattice, where Λ is a maximal R -order in the K -algebra A . Show that $\text{End}_\Lambda M$ is a maximal R -order in $\text{End}_A KM$.

[Hint: First pass to P -adic completions, and then use the fact that when A is a central simple K -algebra, then $M \cong \Delta^{(k)}$ for some k (in the notation of (26.23).)]

8. Let Λ be an R -order in a f.d. semisimple K -algebra A . Show that Λ is left hereditary if and only if $\text{Ext}_\Lambda^1(I, J) = 0$ for each pair of left ideals I, J of Λ .

[Hint: Assume $\text{Ext}_\Lambda^1(I, J) = 0$ for all I and J . By Exercise 23.1, every left Λ -lattice L can be embedded in a free Λ -lattice $\Lambda^{(k)}$ for some k . We now use induction on k to show that $\text{Ext}_\Lambda^1(I, L) = 0$ for all I . For $k = 1$, the result follows from the hypothesis. Now let $k > 1$; as in the proof of (4.3), there exists a Λ -exact sequence

$$0 \rightarrow L_0 \rightarrow L \rightarrow I_0 \rightarrow 0,$$

with I_0 an ideal of Λ and L_0 a sublattice of $\Lambda^{(k-1)}$. Thence the result at $k - 1$ implies it at k , and so $\text{Ext}_\Lambda^1(I, L) = 0$ for every Λ -lattice L and for all left ideals I of Λ .

Given I , there exists a Λ -exact sequence

$$0 \rightarrow L \rightarrow \Lambda^{(r)} \rightarrow I \rightarrow 0$$

for some r . From $\text{Ext}_\Lambda^1(I, L) = 0$ we obtain $\Lambda^{(r)} \cong L \oplus I$, so I is Λ -projective.]

9. Given $K = \text{algebraic number field}$, $R = \text{alg. int. } \{K\}$, $G = \langle x : x^n = 1 \rangle$ a cyclic group, $S = R[\omega_n]$, where ω_n is a primitive n -th root of 1. Show that if $S \neq \text{alg. int. } \{K(\omega_n)\}$, then there exist ideals I, J of S such that $\text{Ext}_{RG}^1(I, J) \neq 0$. Here, x acts on S and its ideals as multiplication by ω_n .

[Hint: (Gudivok [67]). The proof of (25.26, Step 2) shows that $\text{Ext}_{RG}^1(I, J) = \text{Ext}_S^1(I, J)$. If $S \neq \text{alg. int. } \{K(\omega_n)\}$, then S is not hereditary, since

$$S \text{ hereditary} \Rightarrow S = \text{Dedekind domain}$$

$$\Rightarrow S \text{ integrally closed in } K(\omega_n) \Rightarrow S = \text{alg. int. } \{K(\omega_n)\}.$$

Now use Exercise 8. An analogous result holds when K is a P -adic field. Further, there are examples where $R[\omega_n] \neq \text{alg. int. } \{K(\omega_n)\}$. Find one!]

10. Prove directly the following special case of (26.25): Let $A = \text{End}_K(V)$ where V is an n -dimensional K -space. Then every maximal R -order in A is of the form $\text{End}_R(M)$ for some full R -lattice M in V , and every such order is maximal. In particular, if R is a P.I.D., then every maximal R -order in $M_n(K)$ is conjugate to $M_n(R)$.

[Hint: Let Λ be a maximal R -order in A , and let M be a full Λ -lattice in V . Then $\Lambda \subseteq \text{End}_R(M) = R$ -order in A , whence $\Lambda = \text{End}_R(M)$. On the other hand, for any full R -lattice M in V , we show that $\text{End}_R(M)$ is maximal. By (26.21), it suffices to treat the case where R is local; assume thus that R is a P.I.D. For any R -order Γ containing $M_n(R)$, let $\mathbf{X} = (\alpha_{ij}) \in \Gamma$ with each $\alpha_{ij} \in K$. For fixed i, j , we have $e_{ii}\mathbf{X}e_{jj} = \text{diag}(\alpha_{ii}, 0, \dots, 0) \in \Gamma$. This diagonal matrix is integral over R , so $\alpha_{ii} \in R$. Thus $\Gamma = M_n(R)$.]

11. Let R be a d.v.r. with quotient field K , and let Λ be a maximal R -order in a separable K -algebra A . Let M and N be left Λ -lattices such that $KM \cong KN$ as left A -modules. Show that $M \cong N$ as Λ -modules.

[Hint: Let P be the maximal ideal of R , and let \hat{M} denote the P -adic completion of M . It suffices to prove that $\hat{M} \cong \hat{N}$ (see (30.17)). Changing notation, let R be a complete d.v.r. By (26.20), Λ decomposes into a direct sum of maximal orders in the Wedderburn components of A . Each Λ -lattice has a corresponding decomposition, so it suffices to prove the result for the case where A is a simple algebra whose center F is a finite separable field extension of K . Let S be the integral closure of R in F , so Λ is a maximal S -order in the central simple F -algebra A by (26.20).]

Let M be any left Λ -lattice, so M is Λ -projective by (26.12), and therefore $M = \bigoplus M_i$ where the $\{M_i\}$ are indecomposable projective Λ -lattices. Let $J = \text{rad } \Lambda$; by (6.9), each M_i/JM_i is a simple left (Λ/J) -module. But Λ/J is a simple artinian ring, by Exercises 4 and 5. Thus the $\{M_i/JM_i\}$ are mutually isomorphic, whence so are the $\{M_i\}$. It follows at once that the isomorphism class of M is completely determined by the R -rank of M .]

12. Let A be a commutative separable K -algebra, and let Λ be its maximal R -order. Let L be a finite separable unramified extension of K , and let S be the integral closure of R in L . Show that $S \otimes_R \Lambda$ is a maximal R -order in $L \otimes_K A$. This is a special case of (26.27).

[Hint: Use (4.26a)].

§27. GROUP RINGS AND MAXIMAL ORDERS

In this section, R denotes a Dedekind domain with quotient field K , and Λ is an R -order in a f.d. K -algebra A . We saw in §26 that a great deal of detailed information is available about maximal orders and their ideal theory. We hope to use these facts to study the representation theory of an arbitrary order Λ , and begin by embedding Λ in a maximal order Γ in A . If we have enough information about the relation between Λ and Γ we can derive significant results about the representations of Λ . For example, if Λ is a commutative order in a separable K -algebra A , then we can decide whether the number of isomorphism classes of indecomposable Λ -lattices is finite or not, merely by computing the minimal number of generators of the Λ -modules Γ/Λ and $\text{rad}(\Gamma/\Lambda)$ (see §33C).

In the general case, we may also measure the relation between Λ and Γ by means of the *conductor*

$$(\Gamma : \Lambda) = \{x \in A : x\Gamma \subseteq \Lambda\},$$

which is the largest right Γ -module contained in Λ . We have already seen in §25 the importance of the groups $\text{Ext}_\Lambda^1(M, N)$, where M and N are Λ -lattices. It will be shown in (29.4) that if α lies in the center of A , and is such that

$\alpha\Gamma \subseteq \Lambda$, then

$$\alpha \cdot \text{Ext}_{\Lambda}^1(M, N) = 0$$

for all lattices M and N . This gives some idea of the importance of being able to determine the conductor $(\Gamma : \Lambda)$.

Our main result in this section is Jacobinski's explicit formula for the conductor $(\Gamma : RG)$, where Γ is a maximal R -order in KG containing the integral group ring RG of a finite group G . This formula depends on the use of the reduced trace from KG to K , and the reader may wish to review the first half of §7D before proceeding.

(A given order Λ can usually be embedded in more than one maximal order Γ . Of course, when A is a commutative separable K -algebra, there is a unique maximal R -order in A , by (26.10). In the noncommutative case, however, there are usually many distinct maximal orders in A (see Example (iii) after (26.11)). In studying a hereditary order Λ , it is vital to know which maximal orders contain Λ . For further details about this question, see MO (39.23) and (40.8).)

Our first result gives a simple but useful relation between an integral group ring RG and any R -order in KG containing RG .

(27.1) Proposition. *Let G be a finite group of order n , and suppose that $\text{char } K \nmid n$. Let Λ' be any R -order containing RG . Then*

$$RG \subseteq \Lambda' \subseteq n^{-1} \cdot RG.$$

The group ring RG is a maximal order in KG if and only if $n^{-1} \in R$.

Proof. Let T be the ordinary trace map from KG to K . Using the elements of G as K -basis for KG , we have

$$T(x) = \begin{cases} n, & x = 1, \\ 0, & x \in G - \{1\}. \end{cases}$$

Now let $\lambda \in \Lambda'$, and write $\lambda = \sum_{y \in G} \alpha_y y$, with each $\alpha_y \in K$. For any $x \in G$ we have $\lambda x^{-1} \in \Lambda'$, so $T(\lambda x^{-1}) \in R$ by (26.1). But

$$T(\lambda x^{-1}) = \sum_y \alpha_y T(yx^{-1}) = n\alpha_x, \quad x \in G.$$

Thus each $\alpha_x \in n^{-1}R$, so $\lambda = \sum \alpha_x x \in n^{-1} \cdot RG$. This establishes the desired inclusion, and shows that RG is maximal whenever $n^{-1} \in R$.

On the other hand, let RG be a maximal order, and let

$$e = n^{-1} \sum_{x \in G} x.$$

Then e is a central idempotent of KG , and $ye = e$ for all $y \in G$. It follows at once that $RG + Re$ is also an R -order in KG , whence $e \in RG$ (since RG is assumed maximal). But $e \in RG$ implies $n^{-1} \in R$, completing the proof.

Our aim is to prove Jacobinski's refinement of this result (see (27.8)), which is obtained by using reduced trace instead of ordinary trace. We begin with the following:

(27.2) Definition. Let $\Lambda \subseteq \Gamma$ be a pair of rings. We define

$$\begin{aligned} \text{left conductor of } \Gamma \text{ into } \Lambda &= (\Gamma : \Lambda)_l = \{x \in \Gamma : x\Gamma \subseteq \Lambda\} \\ &= \text{largest right } \Gamma\text{-module in } \Lambda, \end{aligned}$$

$$\begin{aligned} \text{right conductor of } \Gamma \text{ into } \Lambda &= (\Gamma : \Lambda)_r = \{x \in \Gamma : \Gamma x \subseteq \Lambda\} \\ &= \text{largest left } \Gamma\text{-module in } \Lambda. \end{aligned}$$

Now let $\Lambda = RG$, where G is a finite group of order n , and where we assume that $\text{char } K \nmid n$. Let $\Lambda \subseteq \Gamma$, where Γ is a maximal R -order in KG . We shall compute the conductors of Γ into Λ . For this purpose, it is first necessary to introduce some notation. The group algebra $A = KG$ is a separable K -algebra, and we may write

$$(27.3) \quad A = KG = A_1 \oplus \cdots \oplus A_t,$$

where the $\{A_i\}$ are the simple components of A . If K_i is the center of A_i , then K_i is a finite extension field of K , and we have (by (7.22))

$$(27.4) \quad \dim_{K_i} A_i = n_i^2, \quad 1 \leq i \leq t,$$

for some integers $\{n_i\}$. Let R_i denote the integral closure of R in K_i . By (26.20) we may write

$$(27.5) \quad \Gamma = \Gamma_1 \oplus \cdots \oplus \Gamma_t, \quad \text{where } \Gamma_i \text{ is a maximal } R_i\text{-order in } A_i, \quad 1 \leq i \leq t.$$

For each i , let tr_i denote the reduced trace form A_i to K . By (7.36) we have

$$(27.6) \quad \text{tr}_i = T_{K_i/K} \circ \text{tr}_{A_i/K_i},$$

where $T_{K_i/K}$ is the ordinary trace from K_i to K , and tr_{A_i/K_i} is the reduced trace from A_i to K_i . Since each A_i is a simple algebra of dimension n_i^2 over its center, it follows from (7.35) that the ordinary trace $T_{A_i/K}$ is equal to $n_i \text{tr}_i$. Therefore we obtain

$$(27.7) \quad T_{A/K}(x) = \sum_{i=1}^t n_i \text{tr}_i(x_i), \quad \text{where } x = \sum x_i, \quad x_i \in A_i.$$

Next, Proposition 7.41 asserts that the reduced trace form $\text{tr}_i: A_i \times A_i \rightarrow K$ is a nondegenerate symmetric bilinear form. We can therefore consider duality relative to this form, as in §4E. With each full left Γ_i -lattice L in A_i , we can associate a dual right Γ_i -lattice \tilde{L} defined by

$$\tilde{L} = \{x \in A_i : \text{tr}_i(xL) \subseteq R\}.$$

In particular, applying this construction to the two-sided Γ_i -lattice Γ_i , we obtain a two-sided Γ_i -lattice $\tilde{\Gamma}_i$ containing Γ_i , called the *inverse different* of Γ_i with respect to the reduced trace form tr_i . For later use, we remark that, by (26.14), the set of full two-sided Γ_i -lattices in A_i is an abelian multiplicative group. Thus we may write $\tilde{\Gamma}_i = \mathfrak{D}_i^{-1}$, where \mathfrak{D}_i is a two-sided ideal of Γ_i . We call \mathfrak{D}_i the *different* of Γ_i with respect to tr_i .

We are now ready to prove:

(27.8) Theorem (Jacobinski [66]). *Let Γ be a maximal R -order containing the group ring RG . Keeping the notation above, we have*

$$(\Gamma : RG)_l = (\Gamma : RG)_r = \bigoplus_{i=1}^t (n/n_i) \mathfrak{D}_i^{-1}.$$

Proof. Let $T: A \times A \rightarrow K$ be the ordinary trace form, and let $G = \{x_1, \dots, x_n\}$. These $\{x_i\}$ form a K -basis of A , so by virtue of the formula for T given in the proof of (27.1), the dual basis is precisely $\{n^{-1}x_1, \dots, n^{-1}x_n\}$. Let $\Lambda = RG$, and let $\tilde{\Lambda}$ denote the dual of Λ with respect to this trace form T , so

$$\tilde{\Lambda} = \{y \in A : T(y\Lambda) \subseteq R\}.$$

Since $\Lambda = \bigoplus_1^n Rx_i$, we have

$$\tilde{\Lambda} = \bigoplus_{i=1}^n R(n^{-1}x_i) = n^{-1}\Lambda.$$

Next, let $M = (\Gamma : \Lambda)$; then M is the largest left Γ -lattice in Λ , so its dual \tilde{M} (with respect to T) is the smallest right Γ -lattice containing $\tilde{\Lambda}$. But then

$$\tilde{M} = \tilde{\Lambda} \cdot \Gamma = n^{-1}\Lambda \cdot \Gamma = n^{-1}\Gamma,$$

so

$$M = \tilde{M} = \text{dual of } n^{-1}\Gamma = n\tilde{\Gamma}.$$

On the other hand, we may compute $\tilde{\Gamma}$ by working in each simple component, so that $\tilde{\Gamma} = \bigoplus \tilde{\Gamma}_i$, where $\tilde{\Gamma}_i$ is the inverse different of Γ_i with respect to the trace

form $T_{A_i/K}$. Using (27.7), we obtain

$$\begin{aligned}\widetilde{\Gamma} &= \bigoplus_{i=1}^t \widetilde{\Gamma}_i = \bigoplus_{i=1}^t n_i^{-1} \cdot (\text{dual of } \Gamma_i \text{ with respect to } \text{tr}_i) \\ &= \bigoplus_{i=1}^t n_i^{-1} \mathfrak{D}_i^{-1}.\end{aligned}$$

Hence we obtain

$$(\Gamma : \Lambda)_r = M = n\widetilde{\Gamma} = \bigoplus_{i=1}^t (n/n_i) \mathfrak{D}_i^{-1},$$

which establishes the theorem, since a similar argument works for $(\Gamma : \Lambda)_l$.

This theorem gives a surprisingly explicit expression for the largest Γ -ideal inside Λ . The fact that the left and right conductors coincide is also of interest, and will be needed in §29B. As an illustration of the strength of Jacobinski's Theorem, we shall deduce a number of important consequences.

For the rest of this discussion, we restrict our attention to the case where K is an algebraic number field, and $R = \text{alg. int. } \{K\}$. For each i , $1 \leq i \leq t$, we have

$$n/n_i \in (n/n_i) \mathfrak{D}_i^{-1} \subseteq (\Gamma : \Lambda)_r \subseteq \Lambda,$$

since $\mathfrak{D}_i^{-1} \supseteq \Gamma_i$. But $\Lambda = RG$, so we obtain

$$(27.9) \quad n_i \text{ divides } n, \quad 1 \leq i \leq t.$$

This result contains significant information about Schur indices and the degrees of the absolutely irreducible complex representations of G , as we shall now explain.

For each i , $1 \leq i \leq t$, we may write

$$(27.10) \quad A_i = M_{k_i}(D_i), \quad D_i = \text{division algebra with center } K_i, \quad \dim_{K_i} D_i = m_i^2.$$

We call m_i the *index* of D_i , and note that $n_i = m_i k_i$. If V_i is the simple left A -module corresponding to a simple left ideal in A_i , then m_i is called the *Schur index* of V_i relative to K (see Chapter 6). From (27.9) we obtain at once:

(27.11) Theorem. *For each i , $m_i k_i$ is a divisor of $|G|$. In particular, the Schur indices of the simple KG -modules are divisors of $|G|$.*

We also obtain another proof of the basic result (9.32) about dimensions of absolutely simple modules:

(27.12) Theorem. *The degrees of the absolutely irreducible complex representations of G are divisors of $|G|$.*

Proof. In the preceding discussion, choose K to be a splitting field for G . Then for each i , $1 \leq i \leq t$, we have

$$A_i \cong M_{n_i}(K), k_i = n_i, m_i = 1.$$

The integers $\{n_i\}$ are precisely the degrees of the absolutely irreducible complex representations of G , and $n_i | n$ by (27.11), so the theorem is proved.

To conclude this section, let us derive Jacobinski's formula for the central conductor of the maximal order Γ into the integral group ring $\Lambda = RG$. We assume throughout that $R = \text{alg. int. } \{K\}$. Let C denote the integral closure of R in the center of KG , so we may write

$$C = R_1 \oplus \cdots \oplus R_t, \quad R_i = \text{integral closure of } R \text{ in } K_i.$$

Then C is the unique maximal R -order in the center of KG , and is contained in Γ (since otherwise $C\Gamma$ is a larger R -order in KG). We define the *central conductor* of Γ into Λ as follows:

$$\text{central conductor} = C \cap (\Gamma : \Lambda)_i = \{c \in C : c\Gamma \subseteq \Lambda\}.$$

As a consequence of (27.8), we now prove:

(27.13) Theorem. *Let $R = \text{alg. int. } \{K\}$, $\Lambda = RG$, Γ a maximal R -order in KG containing Λ .*

(i) *The central conductor F of Γ into Λ is given by*

$$F = \bigoplus_{i=1}^t (n/n_i) \mathfrak{D}^{-1}(R_i/R),$$

where

$$\mathfrak{D}^{-1}(R_i/R) = \left\{ x \in K_i : T_{K_i/K}(xR_i) \subseteq R \right\},$$

which is (by definition) the inverse different of R_i relative to R (see §4B).

(ii) *We have*

$$R \cap F = \bigcap_{i=1}^t (n/n_i) \{ K \cap \mathfrak{D}^{-1}(R_i/R) \}.$$

Proof. For each i , $1 \leq i \leq t$, we set

$$d_i^{-1} = \left\{ x \in A_i : \text{tr}_{A_i/K_i}(x\Gamma_i) \subseteq R_i \right\},$$

the inverse different of Γ_i with respect to tr_{A_i/K_i} . For convenience of notation,

let

$$\delta_i^{-1} = \mathfrak{D}_i^{-1}(R_i/R),$$

so δ_i is an ideal of R_i . Let us begin by deducing from (27.6) that

$$\mathfrak{D}_i^{-1} = d_i^{-1} \delta_i^{-1}.$$

Indeed, for $x \in A$, we have

$$\begin{aligned} x \in \mathfrak{D}_i^{-1} &\Leftrightarrow \text{tr}_i(x\Gamma_i) \subseteq R_i \Leftrightarrow T_{K_i/K}(\text{tr}_{A_i/K_i}(x\Gamma_i)) \subseteq R \\ &\Leftrightarrow T_{K_i/K}(\text{tr}_{A_i/K_i}(xR_i\Gamma_i)) \subseteq R \Leftrightarrow T_{K_i/K}(R_i \cdot \text{tr}_{A_i/K_i}(x\Gamma_i)) \subseteq R \\ &\Leftrightarrow \text{tr}_{A_i/K_i}(x\Gamma_i) \subseteq \delta_i^{-1} \Leftrightarrow \text{tr}_{A_i/K_i}(x\delta_i\Gamma_i) \subseteq R_i \\ &\Leftrightarrow x\delta_i \subseteq d_i^{-1} \Leftrightarrow x \in d_i^{-1}\delta_i^{-1}. \end{aligned}$$

From the definition of the central conductor F , we have

$$F = C \cap (\Gamma : \Lambda)_I = \bigoplus_{i=1}^t (R_i \cap (n/n_i)\mathfrak{D}_i^{-1}).$$

To prove assertion (i), it therefore must be shown that

$$(27.14) \quad R_i \cap (n/n_i)\mathfrak{D}_i^{-1} = (n/n_i)\delta_i^{-1}$$

for each i , where $\delta_i = \mathfrak{D}_i(R_i/R)$. Let $y \in R_i$. Then

$$\begin{aligned} y \in (n/n_i)\mathfrak{D}_i^{-1} &\Leftrightarrow y \in (n/n_i)d_i^{-1}\delta_i^{-1} \\ &\Leftrightarrow y\delta_i \subseteq (n/n_i)d_i^{-1} \Leftrightarrow y\delta_i \subseteq (n/n_i)(K_i \cap d_i^{-1}). \end{aligned}$$

We may write $K_i \cap d_i^{-1} = \alpha^{-1}$, where α is an ideal in R_i . We shall show that $\alpha = R_i$. If $\alpha \neq R_i$, let P be a maximal ideal of R_i containing α , and let \mathfrak{p} be the prime ideal of Γ_i which corresponds to P (see Exercise 26.5). Then the power of \mathfrak{p} which occurs in the factorization of the different d_i into the prime ideals of Γ_i is precisely \mathfrak{p}^{e-1} , where $P\Gamma_i = \mathfrak{p}^e$ (see MO (25.7)). Then

$$P \supseteq \alpha \Rightarrow P^{-1} \subseteq \alpha^{-1} \Rightarrow P^{-1} \subseteq d_i^{-1} \Rightarrow P\Gamma_i \supseteq d_i \Rightarrow P\Gamma_i \supseteq \mathfrak{p}^{e-1},$$

a contradiction. This proves that $K_i \cap d_i^{-1} = R_i$, and so

$$R_i \cap (n/n_i)\mathfrak{D}_i^{-1} \subseteq (n/n_i)\delta_i^{-1}.$$

To prove the reverse inclusion, we note that

$$(n/n_i)\delta_i^{-1} \subseteq (n/n_i)\mathfrak{D}_i^{-1} \subseteq \Lambda,$$

so each element of $(n/n_i)\delta_i^{-1}$ is integral over R , and therefore lies in R_i . This proves (27.14), and establishes assertion (i).

Finally, we have just verified that $(n/n_i)\delta_i^{-1} \subseteq R_i$. Since $K \cap R_i = R$, we obtain

$$R \cap F = (R \cap C) \cap (\Gamma : \Lambda)_l = \bigoplus_{i=1}^t (R \cap (n/n_i)\delta_i^{-1}).$$

But for each i ,

$$R \cap (n/n_i)\delta_i^{-1} = K \cap (n/n_i)\delta_i^{-1} = (n/n_i)(K \cap \delta_i^{-1}).$$

This proves assertion (ii), and the theorem is established.

§28. TWISTED GROUP RINGS AND CROSSED-PRODUCT ORDERS

The twisted group ring $S \circ G$ of a finite group G , over some commutative ring S , is a natural generalization of the ordinary group ring SG . In the case of twisted group rings, we assume that G acts as a group of automorphisms of S , and then “twist” the multiplication in $S \circ G$ according to this action. Specifically, suppose that $a \rightarrow \sigma(a)$, $a \in S$, is the automorphism of S which corresponds to the element $\sigma \in G$. We then define multiplication in $S \circ G$ according to the rule

$$\sigma \cdot a = \sigma(a)\sigma \text{ for all } \sigma \in G, a \in S.$$

If each $\sigma \in G$ acts as the identity automorphism of S , then of course we obtain the ordinary group ring SG once more.

We have already seen, in Example 7.39, that twisted group algebras may arise as Wedderburn components of ordinary group algebras. In the same way, problems about integral representations of groups often lead to questions about lattices over twisted group rings. In practice, G is the Galois group of some finite Galois extension L of a field K , R is a Dedekind domain with quotient field K , and S is the integral closure of R in L . Then we can form the twisted group algebra $L \circ G$, which will turn out to be a full matrix algebra over K . This algebra contains the twisted group ring $S \circ G$, which is an R -order in $L \circ G$.

As we shall see, the properties of the twisted group ring $S \circ G$ depend strongly upon the arithmetic nature of the inclusion $R \subseteq S$. The first basic

result below is that $S \circ G$ is a maximal R -order if and only if $d(S/R) = R$, where $d(S/R)$ denotes the discriminant ideal of S relative to R (see end of §4B). The second important fact is that $S \circ G$ is a hereditary ring if and only if $T_{L/K}(S) = R$. As we shall see, the conditions that $d(S/R) = R$, or that $T_{L/K}(S) = R$, are equivalent to assertions about the behavior of maximal ideals of R in the larger ring S .

We will then work out an example where it is possible to classify completely all $(S \circ G)$ -lattices. This example will be used in §34E, where it will play a vital role in the determination of integral representations of a dihedral group of order $2p$, or more generally, of certain metacyclic groups.

The section concludes with a brief discussion of orders in crossed-product algebras. Twisted group algebras are special cases of crossed-product algebras, and some of our results have natural extensions to orders in such algebras.

The material in this section is quite important from the standpoint of classifying integral representations of groups in certain specific cases. However, unlike the earlier sections of this chapter, the present section does not play as crucial a role in the treatment in Chapter 4 of integral representation theory. Some readers may therefore wish to concentrate on the examples and statements of theorems, and return later to the details of the proofs.

We begin by defining the *twisted group ring** $S \circ G$ of a finite group G , where S is a commutative ring on which G acts as a group of automorphisms. We set

$$(28.1) \quad S \circ G = \bigoplus_{\sigma \in G} Su_{\sigma},$$

where the symbols $\{u_{\sigma} : \sigma \in G\}$ form a S -basis for $S \circ G$, and multiplication is defined by

$$(28.2) \quad (au_{\sigma})(bu_{\tau}) = a\sigma(b)u_{\sigma\tau} \text{ for all } a, b \in S, \sigma, \tau \in G.$$

(28.3) Example. Let R be a Dedekind domain with quotient field K , and let S be the integral closure of R in a finite Galois extension L of K , with Galois group G . Each $\sigma \in G$ determines a K -automorphism of L , inducing an R -automorphism of S , and we may form the rings

$$A = \bigoplus L u_{\sigma}, \quad \Lambda = \bigoplus S u_{\sigma}.$$

Then u_1 is the identity element of A , and we leave it as an exercise for the reader to check that:

$$\text{center of } A = Ku_1, \text{ center of } \Lambda = Ru_1.$$

*Another kind of twisted group algebra was introduced in (8.33ii), and was used in §11C and §19C.

Thus, A is a K -algebra (but not an L -algebra, if $L \neq K!$), and Λ is an R -order in $L \circ G$.

Let us show at once that there is an isomorphism of K -algebras:

$$A \cong M_n(K), \text{ where } n = \dim_K L = |G|.$$

We define a map $\psi: A \rightarrow \text{End}_K L$ by

$$a \mapsto a_1, u_\sigma \mapsto \sigma, \text{ for } a \in L, \sigma \in G.$$

Since

$$(a, \sigma)(b, \tau) = a_1 \sigma(b)_1 \sigma \tau = (a \sigma(b))_1 \sigma \tau$$

for $a, b \in L$, $\sigma, \tau \in G$, it follows at once that ψ is a homomorphism of K -algebras. Let us show that ψ is a monomorphism, by proving that A has no nontrivial two-sided ideals. Indeed, if X is a nonzero two-sided ideal of A , let

$$x = a_{\sigma_1} u_{\sigma_1} + \cdots + a_{\sigma_r} u_{\sigma_r} \in X, x \neq 0,$$

with r minimal. If $r > 1$, choose $b \in L$ with $\sigma_1(b) \neq \sigma_2(b)$. Then $x - \sigma_1(b)^{-1} x b$ is a nonzero element of X with a shorter expression. This contradicts our choice of x , so necessarily $r = 1$, and then X contains a unit $a_{\sigma_1} u_{\sigma_1}$ of A . Therefore $X = A$, as desired. This completes the proof* that ψ is an algebra monomorphism. Since A and $\text{End}_K L$ both have K -dimension n^2 , it follows that ψ is an isomorphism. Of course, $\text{End}_K L \cong M_n(K)$ since $\dim_K L = n$.

For later use, we note that the map ψ enables us to view L as a left A -module, and then obviously L is a simple left A -module. The action of A on L is given explicitly by

$$(au_\sigma)x = a\sigma(x), \quad a, x \in L, \sigma \in G.$$

This construction was used in the proof of (21.18).

(28.4) Example. As a second example of a twisted group ring, let

$$H = \langle x, y : x^n = 1, y^2 = 1, yxy^{-1} = x^{-1} \rangle, \quad G = \langle y \rangle, \quad C = \langle x \rangle,$$

and let R be any commutative ring. We let G act as a group of automorphisms on the ordinary group ring RC by defining

$${}^y\xi = y\xi y^{-1} \text{ for all } \xi \in RC,$$

where the product $y\xi y^{-1}$ is computed inside the ordinary group ring RH . We may form the twisted group ring $(RC) \circ G$, and obtain an isomorphism of

*Compare this proof with the Hint in Exercise 7.11.

R -algebras

$$RH \cong (RC) \circ G.$$

For $\xi \in RH$, we have $y\xi = {}^y\xi y$.

Now let ω be a primitive n -th root of 1 over \mathbb{Q} , and let $\Phi(X)$ be the cyclotomic polynomial of order n . Then $\Phi(X) = \min. \text{ pol.}_\mathbb{Q}(\omega)$, and ω^{-1} is also a zero of $\Phi(X)$. It follows that

$$X^{\varphi(n)} \Phi(X^{-1}) = \pm \Phi(X).$$

Since

$${}^y\{\Phi(x)\} = y\Phi(x)y^{-1} = \Phi(x^{-1}) \text{ in } \mathbb{Z}H,$$

it follows that $\Phi(x)\mathbb{Z}H$ is a two-sided ideal in $\mathbb{Z}H$. There are ring isomorphisms

$$\mathbb{Z}H/\Phi(x)\mathbb{Z}H \cong \{\mathbb{Z}C/\Phi(x)\mathbb{Z}C\} \circ G \cong \mathbb{Z}[\omega] \circ G,$$

and here $\mathbb{Z}[\omega] = \text{alg. int. } \{\mathbb{Q}(\omega)\}$ (see §4H). Since $xyx^{-1} = x^{-1}$, and the map $\mathbb{Z}H \rightarrow \mathbb{Z}[\omega]$ carries x onto ω , it follows that ${}^y\omega = \omega^{-1} = \bar{\omega}$ in the twisted group ring $\mathbb{Z}[\omega] \circ G$. Thus

$${}^y\xi = \bar{\xi}, \quad \xi \in \mathbb{Z}[\omega],$$

where bar denotes complex conjugation. Thus, twisted group rings appear naturally as factor rings of ordinary group rings. The same argument shows that the twisted group algebra $\mathbb{Q}(\omega) \circ G$ is a simple component of the ordinary group algebra $\mathbb{Q}H$.

Until further notice, we shall adopt the notation and hypotheses of Example 28.3, so let L be a finite Galois extension of K with Galois group G , and let S be the integral closure of R in L . The first major result, due to Auslander-Goldman [60b], is as follows:

(28.5) Theorem. *The twisted group ring $S \circ G$ is a maximal R -order in $L \circ G$ if and only if the discriminant ideal $d(S/R)$ coincides with R .*

Proof. For each maximal ideal P of R , let the subscript P denote localization at P . We have

$$(S \circ G)_P = S_P \circ G,$$

and by (26.21), $S \circ G$ is maximal if and only if $S_P \circ G$ is a maximal R_P -order

for each P . Further,

$$d(S_P/R_P) = \{d(S/R)\}_P$$

by §4C. Hence it suffices to prove the result when R is replaced by R_P . Changing notation, we may assume for the rest of the proof that R is a d.v.r.

Let us put $A = L \circ G$, $\Lambda = S \circ G$. As in §26A, the discriminant ideal $d(\Lambda)$ is computed by using the reduced trace tr from A to K , while the discriminant ideal $d(S/R)$ is computed by using the ordinary trace T from L to K . Let us show first that

$$(*) \quad d(\Lambda) = \{d(S/R)\}^n,$$

where $n = \dim_K L = |G|$. Let $S = \bigoplus_{i=1}^n R s_i$, $G = \{\sigma_1, \dots, \sigma_n\}$; then Λ has an R -basis $\{s_i u_{\sigma_j} : 1 \leq i, j \leq n\}$, and by (7.36) we have:

$$\text{tr}\{(s_i u_{\sigma_j})(s_k u_{\sigma_l})\} = \text{tr}\{s_i \sigma_j(s_k) u_{\sigma_j} u_{\sigma_l}\} = \begin{cases} T(s_i \sigma_j(s_k)), & \text{if } \sigma_j = \sigma_l^{-1}, \\ 0, & \text{otherwise.} \end{cases}$$

It follows that

$$d(\Lambda) = R \cdot \prod_{j=1}^n \det[T(s_i \sigma_j(s_k))]_{1 \leq i, k \leq n}.$$

However,

$$\det[T(s_i \sigma_j(s_k))]_{1 \leq i, k \leq n} = \pm \det[T(s_i s_k)]_{1 \leq i, k \leq n}.$$

Furthermore,

$$d(S/R) = R \cdot \det[T(s_i s_k)]_{1 \leq i, k \leq n},$$

and so we obtain $(*)$ at once.

We are now ready to complete the proof of the theorem. If $d(S/R) = R$, then $d(\Lambda) = R$, and therefore Λ is a maximal R -order by (26.3iii). Conversely, suppose that Λ is a maximal R -order in A . Since $A \cong M_n(K)$ by (28.3), it follows that $\Lambda \cong M_n(R)$ (see Exercise 26.10). We shall use this fact to show that $d(\Lambda) = R$. When an element $\lambda \in \Lambda$ is represented by a matrix in $M_n(R)$, its reduced trace $\text{tr}(\lambda)$ is precisely the trace of this matrix. Let $\{e_{ij} : 1 \leq i, j \leq n\}$ be the matrix units in $M_n(R)$, so e_{ij} is the matrix with entry 1 at position (i, j) and zeros elsewhere. These n^2 matrix units form an R -basis for $M_n(R)$, and we have

$$\text{tr}(e_{ij} e_{kl}) = \delta_{jk} \delta_{il},$$

where i, j, k, l range from 1 to n . It follows that the discriminant ideal of the

R -order $M_n(R)$ is equal to R . Thus $d(\Lambda) = R$ as claimed. But then $d(S/R) = R$ by (*), and the proof is finished.

Remarks. (i) By §4B, we know that $d(S/R) = R$ if and only if S is unramified over R . This means that for each maximal ideal P of R , we may write PS as a product $\prod P_i$ of distinct prime ideals, and that S/P_i is separable over R/P for each i .

(ii) The preceding proof shows that for any Dedekind domain R , not necessarily a P.I.D., the relation $d(\Lambda) = \{d(S/R)\}^n$ is valid.

(28.6) Example. Let $\Lambda = S \circ G$, where $S = \mathbb{Z}[\omega]$, using the notation of (28.4). Let

$$L = \mathbb{Q}(\omega), K = \mathbb{Q}(\omega + \bar{\omega}), R = \mathbb{Z}[\omega + \bar{\omega}],$$

so $G = \text{Gal}(L/K)$, $R = \text{alg. int. } \{K\}$, and S is the integral closure of R in L . If we assume that n is odd, then the rational prime 2 is unramified in the extension L/\mathbb{Q} by (4.34). It follows at once that S_2 is unramified over the ring R_2 , where the subscript 2 denotes localization. (Note that R_2 is a semilocal Dedekind domain.) Then

$$S_2 = \mathbb{Z}_2 \otimes_{\mathbb{Z}} S = \mathbb{Z}_2[\omega], R_2 = \mathbb{Z}_2 \otimes_{\mathbb{Z}} R = \mathbb{Z}_2[\omega + \bar{\omega}].$$

By the Auslander-Goldman Theorem 28.4, we may conclude that the twisted group ring $S_2 \circ G$ is a maximal R_2 -order in $L \circ G$. However, $S \circ G$ is *not* a maximal R -order in $L \circ G$ (if $n > 1$), since S is not unramified over R .

We turn next to the more complicated question as to when a twisted group ring $S \circ G$ is a hereditary R -order, and again we use the notation and hypotheses of (28.3). Our second main result, due to Auslander-Rim [63, page 578], is as follows:

(28.7) Theorem. *The twisted group ring $S \circ G$ is a hereditary R -order if and only if $T_{L/K}(S) = R$, or equivalently, if and only if $T_{L/K}(s_0) = 1$ for some $s_0 \in S$.*

Proof. Set $\Lambda = S \circ G$, and suppose that there exists an element $s_0 \in S$ such that $\sum_{\sigma \in G} \sigma(s_0) = 1$. We must show that every left ideal M of Λ is projective as Λ -module. The map $s \mapsto s u_1$, $s \in S$, embeds S in Λ . Thus every Λ -module is also an S -module. Since M is an S -submodule of the S -lattice Λ , it follows that M is S -projective. Now let $\theta: X \rightarrow M$ be a Λ -surjection of the Λ -module X onto M . Then there exists $\psi \in \text{Hom}_S(M, X)$ which splits θ , that is, $\theta \psi = 1_M$. Put

$$\psi' = \sum_{\sigma} u_{\sigma} \cdot s_0 \psi \cdot u_{\sigma}^{-1} \in \text{Hom}_{\Lambda}(M, X).$$

Then

$$\theta\psi' = \sum \theta u_\sigma s_0 \psi u_\sigma^{-1} = \sum u_\sigma s_0 \theta \psi u_\sigma^{-1} = \sum u_\sigma s_0 u_\sigma^{-1} = \sum \sigma(s_0) = 1.$$

Hence ψ' splits θ , which shows that M is Λ -projective. (Compare this argument with that in Exercise 4.15 and the proof of (19.2).)

We have now shown that Λ is left hereditary if $T_{L/K}(S)=R$. A similar argument proves that Λ is right hereditary in this case. We could also have used the final part of the proof of Theorem 26.12, where we showed that an order Λ is left hereditary if and only if Λ is right hereditary.

Turning to the converse, assume now that Λ is left hereditary and let $y = \sum u_\sigma \in \Lambda$. There is a left Λ -surjection $\varphi: \Lambda \rightarrow \Lambda y$, given by right multiplication by y . Since Λy is a left ideal of Λ , and hence is Λ -projective, there exists a map $\theta \in \text{Hom}(\Lambda y, \Lambda)$ such that $\varphi\theta=1$ on Λy . Let us set

$$\theta(y) = \sum_{\sigma \in G} a_\sigma u_\sigma, \quad a_\sigma \in S.$$

Since $u_\tau y = y$ for all $\tau \in G$, we obtain

$$\sum a_\sigma u_\sigma = \theta(y) = \theta(u_\tau y) = u_\tau \theta(y) = u_\tau \cdot \sum a_\sigma u_\sigma$$

for each τ . This readily implies that $a_\sigma = \sigma(a_1)$ for each $\sigma \in G$. But then

$$y = (\varphi\theta)(y) = \left(\sum_\sigma a_\sigma u_\sigma \right) y = \left(\sum_\sigma \sigma(a_1) \right) y,$$

whence $\sum_\sigma \sigma(a_1) = 1$. Hence $T_{L/K}(S)=R$, and the theorem is established.

Remark. We saw in Theorem 28.5 that $S \circ G$ is a maximal R -order if and only if S is unramified over R . It is natural to ask whether there is some condition on ramification which will guarantee that $S \circ G$ is hereditary R -order. We shall show now, using results from §4, that $S \circ G$ is a hereditary if and only if S is tamely ramified over R . Indeed, we need only show that $T_{L/K}(S)=R$ if and only if S is tamely ramified over R . We have already proved this in Exercise 4.13, and the remarks which follow are merely intended to summarize some results and definitions concerning ramification.

To start with, let L be any separable extension of K , not necessarily a Galois extension. Let P range over the maximal ideals of R , and write

$$PS = \prod_{i=1}^g P_i^{e_i}, \quad e_i > 0,$$

where the $\{P_i\}$ are distinct maximal ideals of S . As in §4B, call P_i *unramified* over R if $e_i=1$ and S/P_i is a separable extension of R/P ; (this latter condition is automatically satisfied when K is a global field, for then R/P is a finite field.) Call P_i *ramified* over R if either $e_i > 1$ or S/P_i is inseparable over

R/P . By §4B (see also MO (4.37)), P_i is ramified over R if and only if P_i divides the different $D(S/R)$.

We call S/R *unramified* if each maximal ideal P_i of S is unramified over R ; this occurs if and only if $D(S/R)=S$, or equivalently if and only if the discriminant ideal $d(S/R)$ coincides with R .

The concept of tame ramification plays a basic role in the question as to whether $T_{L/K}(S)=R$. Call P_i *tamely ramified* over R if its ramification index e_i is not zero in S/P_i , and S/P_i is separable over R/P . We call S *tamely ramified* over R if for each maximal ideal P of R , there exists at least one P_i containing P which is tamely ramified over R . Then by Exercise 4.13, S/R is tamely ramified if and only if $T_{L/K}(S)=R$.

The preceding discussion simplifies somewhat when L is a Galois extension of K , which we now assume. For each P_i and each $\sigma \in G$, the conjugate ideal P_i^σ is also a maximal ideal of S . By CR §20, we know that PS factors as a product of distinct conjugates of P_1 , all factors occurring with the same ramification index. Likewise, the residue class fields S/P_i^σ are mutually isomorphic over R/P . Thus, if P_i is unramified over R , then so is each of its conjugates P_i^σ , $\sigma \in G$. Likewise, if P_i is tamely ramified over R , then so is each P_i^σ . Hence, when L is a Galois extension of K , we see that S/R is tamely ramified if and only if each P_i is tamely ramified over R .

Finally, $T_{L/K}(S)$ is a nonzero ideal of R , and by Exercise 4.13 it coincides with R if and only if S is tamely ramified over R .

(28.8) Example. Let p be an odd prime, and take $n=p$ in (28.6). By §4H, there is a unique maximal ideal P_1 of S which ramifies over R , namely, the ideal P_1 such that $pS=P_1^{p-1}$. The ramification index of P_1 relative to R is 2, so P_1 is tamely ramified over R . Thus S/R is tame, and we conclude that $S \circ G$ is a hereditary R -order.

We shall next consider the general problem of classifying all Λ -lattices, where Λ is a twisted group ring $S \circ G$, with S tamely ramified over R . This problem arises frequently in specific cases when we try to classify integral representations of groups. For example, the results below will be needed in §34E, where we consider representations of certain metacyclic groups.

Suppose now that $\Lambda=S \circ G$ is a hereditary R -order in the K -algebra $A=L \circ G$. As in the proof of (26.14), we know that a left Λ -lattice M is indecomposable if and only if KM is a simple left A -module. Apart from isomorphism, there is a unique simple A -module, which may be chosen as the field L itself, according to the proof of (28.3). Since every Λ -lattice can be expressed as a finite direct sum of indecomposable lattices, our first task is to investigate the full Λ -lattices in L .

Let M be a full Λ -lattice in the left A -module L . Then M is a fractional S -ideal in the field L (see §4B) such that

$$\sigma(M)=M \text{ for every } \sigma \in G.$$

Such ideals are called *ambiguous* ideals. For example, $S\alpha$ is an ambiguous ideal for every fractional R -ideal α in K . We may easily decide whether two ambiguous S -ideals M and N are isomorphic as Λ -lattices. Indeed, each $f \in \text{Hom}_\Lambda(M, N)$ extends to an element of $\text{Hom}_A(L, L)$, and is therefore given by right multiplication by some $x \in K^\times$. Therefore $M \cong N$ if and only if $M = Nx$ for some $x \in K^\times$.

We are now ready to determine all ambiguous S -ideals \mathfrak{A} in L . If P_1 is a maximal ideal of S which occurs to the exponent n in \mathfrak{A} , then since $\sigma(\mathfrak{A}) = \mathfrak{A}$ for all $\sigma \in G$, it follows that each of the R -conjugates P_1^σ of P_1 must also occur to the exponent n . Given any maximal ideal P of R , we may write

$$PS = \tau(P)^e, \text{ where } \tau(P) = P_1 \cdots P_g,$$

and the $\{P_i\}$ are the distinct R -conjugates of the maximal ideal P_1 of S . The exponent $e = e(P, S/R)$ is the ramification index of P (in the extension L/K), and equals 1 for almost all P . Clearly $\tau(P)$ is an ambiguous ideal of S , and is the largest ambiguous ideal in S in which P_1 occurs as a factor. It follows at once that every ambiguous S -ideal \mathfrak{A} in L is uniquely expressible in the form

$$\mathfrak{A} = \left\{ \prod_P \tau(P)^{k_p} \right\} \alpha = \mathfrak{Q} \alpha, \text{ say,}$$

where α is an R -ideal in K , P ranges over the maximal ideals of R ramified in S , and for each P , $0 \leq k_p \leq e(P, S/R) - 1$. The G -invariant submodule of \mathfrak{A} is given by

$$\mathfrak{A} \cap K = \alpha (\mathfrak{Q} \cap K) = \alpha \cdot \prod_{k_p > 0} P = \alpha \psi(\mathfrak{Q}), \text{ say.}$$

Suppose now that the Λ -lattice M is expressed as an external direct sum $M = \prod_{i=1}^n \mathfrak{Q}_i \alpha_i$, with each $\mathfrak{Q}_i \alpha_i$ as above. The G -invariant submodule of M , which is determined up to isomorphism by the isomorphism class of M , is then equal to $\prod_i \alpha_i \psi(\mathfrak{Q}_i)$, where $\psi(\mathfrak{Q}_i)$ is defined as above. Thus, the

R -isomorphism class of the R -lattice $\prod_{i=1}^n \alpha_i \psi(\mathfrak{Q}_i)$ is an invariant of the Λ -isomorphism class of M . Of course, the R -lattice $\prod_{i=1}^n \alpha_i \psi(\mathfrak{Q}_i)$ is determined up to isomorphism by its rank n and its Steinitz class, namely, the R -ideal class of $\prod_i \alpha_i \psi(\mathfrak{Q}_i)$.

We show next that (with the same notation as above) there is always a Λ -isomorphism

$$(28.9) \quad \mathfrak{Q}_i \alpha_i \oplus \mathfrak{Q}_j \alpha_j \cong \mathfrak{Q}_j \oplus \mathfrak{Q}_i \alpha_i \alpha_j.$$

Thus, in a direct sum $\prod_i \mathfrak{Q}_i \alpha_i$, we may move the factors α_i from one term to another, without affecting the isomorphism class of the direct sum. In order

to prove (28.9), we note that for each $x \in K$, the Λ -lattices $\mathfrak{Q}\alpha$ and $\mathfrak{Q}\alpha x$ are isomorphic. We may choose x so that αx is an ideal of R which is coprime to each $P \in \mathcal{S}$, where \mathcal{S} is the finite set of all maximal ideals P of R which ramify in S (see Exercise 31.13 or CR (18.20)). Hence in proving (28.9) we may assume that both α , and α , are ideals of R which are coprime to each $P \in \mathcal{S}$. Therefore

$$(28.10) \quad (R/\alpha_i)_P = 0 \text{ for each } P \in \mathcal{S},$$

where the subscript P indicates localization.

Now let \mathfrak{Q} be any ambiguous S -ideal in L , and consider the R -torsion Λ -module $\mathfrak{Q}/\alpha_i \mathfrak{Q}$. By the Primary Decomposition Theorem 4.31, we may express $\mathfrak{Q}/\alpha_i \mathfrak{Q}$ as a direct sum of its localizations. Further, the localization at each $P \in \mathcal{S}$ is zero, by (28.10). Now let $P \notin \mathcal{S}$, so $e(P, S/R) = 1$ and $\tau(P) = PS$. If $\tau(P)$ occurs with exponent k in \mathfrak{Q} , then we have $\mathfrak{Q}_P = P^k S_P$. Using the fact that $P^k/\alpha_i P^k \cong R/\alpha_i$, as R -modules (see CR (18.24)), we obtain Λ -isomorphisms:

$$\begin{aligned} (\mathfrak{Q}/\alpha_i \mathfrak{Q})_P &\cong P^k S_P / \alpha_i P^k S_P \cong S_P \otimes_{R_P} (P^k/\alpha_i P^k) \\ &\cong S_P \otimes_{R_P} (R/\alpha_i) \cong S_P / \alpha_i S_P. \end{aligned}$$

This shows that the isomorphism class of the Λ -module $\mathfrak{Q}/\alpha_i \mathfrak{Q}$ is independent of \mathfrak{Q} . Hence we obtain Λ -isomorphisms

$$\mathfrak{Q}_j \otimes_R (\alpha_j/\alpha_i \alpha_j) \cong \mathfrak{Q}_j \otimes_R (R/\alpha_i) \cong \mathfrak{Q}_j \otimes_R (R/\alpha_i).$$

We may apply Schanuel's Lemma to the pair of exact sequences of Λ -modules

$$\begin{aligned} 0 \rightarrow \mathfrak{Q}_j \alpha_i \rightarrow \mathfrak{Q}_j \rightarrow \mathfrak{Q}_j \otimes_R (R/\alpha_i) \rightarrow 0, \\ 0 \rightarrow \mathfrak{Q}_j \alpha_i \alpha_j \rightarrow \mathfrak{Q}_j \alpha_j \rightarrow \mathfrak{Q}_j \otimes_R (\alpha_j/\alpha_i \alpha_j) \rightarrow 0, \end{aligned}$$

since the Λ -lattices \mathfrak{Q}_j and $\mathfrak{Q}_j \alpha_j$ are Λ -projective. This gives (28.9) at once.

Let us illustrate the usefulness of the preceding results in a special case which arises in classifying integral representations of metacyclic groups (see §34E). Suppose that there is a unique maximal ideal P_0 of R which ramifies in S , and suppose further that P_0 is *completely ramified* in S , that is

$$P_0 S = P^n, n = \dim_K L = |G|,$$

where P now denotes a maximal ideal of S . Suppose finally that $\bar{n} \neq 0$ in R/P_0 , so S is tamely ramified over R , and $\Lambda = S \circ G$ is a hereditary R -order in the simple K -algebra $A = L \circ G$. Each ambiguous S -ideal \mathfrak{A} in L is uniquely expressible in the form $\mathfrak{A} = P^k \alpha$, where $0 \leq k \leq n-1$ and α is a fractional

R -ideal in K . Further

$$\begin{aligned} P^k \alpha_i &\cong P' \beta_i \Leftrightarrow P^k \alpha_i = P' \beta_i x \text{ for some } x \in K \\ &\Leftrightarrow k = l \text{ and } \alpha_i = \beta_i x, \end{aligned}$$

assuming that $0 \leq l \leq n-1$ and that $\beta_i = R$ -ideal in K . Hence, a full set of non-isomorphic indecomposable Λ -lattices is given by

$$\{P^k \alpha_i : 0 \leq k \leq n-1, 1 \leq i \leq h\},$$

where α_i ranges over a full set of representatives of the h ideal classes of R . (Assume h finite, for simplicity).

We shall now decide when two direct sums of indecomposable Λ -lattices are isomorphic; the results are due to Rosen [63]. Let \hat{R} , $\hat{\Lambda}$ and so on, denote P_0 -adic completions. Since $P_0 S = P^n$, the P -adic completion \hat{S} of S coincides with its P_0 -adic completion. Clearly,

$$\hat{R} \otimes_R P^k \alpha_i \cong \hat{P}^k \hat{\alpha}_i \cong \hat{P}^k,$$

since $\hat{\alpha}_i$ is an ideal of the d.v.r. \hat{R} . Now consider a Λ -lattice

$$(28.11) \quad M = \coprod_{k=0}^{n-1} P^k N_k,$$

where N_k is an R -lattice of R -rank r_k . Then \hat{N}_k is a free \hat{R} -lattice of \hat{R} -rank r_k , so we have

$$\hat{M} \cong \coprod_{k=0}^{n-1} (\hat{P}^k)^{(r_k)}.$$

On the other hand (see §4C), \hat{P}_0 is completely ramified in the extension \hat{L}/\hat{K} , and $\hat{P}_0 \hat{S} = \hat{P}^n$, $n = \dim_{\hat{K}} \hat{L}$. It follows from the preceding paragraph that for k, l distinct, $0 \leq k, l \leq n-1$, the $\hat{\Lambda}$ -modules \hat{P}^k and \hat{P}^l are not isomorphic. However, the K-S-A Theorem holds for $\hat{\Lambda}$ -lattices (see §6B). It follows that the integers $\{r_0, \dots, r_{n-1}\}$ are invariants of the isomorphism class of \hat{M} , and are therefore also isomorphism invariants of M .

Finally, each R -lattice N_k is determined (up to isomorphism) by its R -rank r_k and its Steinitz class $[\alpha_k]$, where α_k is an R -ideal in K . By virtue of (28.9), we can choose all but one of the N_k 's to be a free R -module, and can collect all the α_k 's into a single summand of M . Hence (assuming $r_0 \geq 1$ for simplicity) we have

$$M \cong \left\{ S \cdot \prod_{k=0}^{n-1} \alpha_k \right\} \oplus S^{(r_0-1)} \oplus \coprod_{k=1}^{n-1} (P^k)^{(r_k)}.$$

On the other hand, by computing the G -invariant submodule of M according to the earlier part of this discussion, we see that the ideal class of $\prod \alpha_k$ is an isomorphism invariant of M . We therefore conclude that, in the present case, a *full set of isomorphism invariants* of the Λ -lattice M given in (28.11) consists of

- (i) The integers $\{r_0, \dots, r_{n-1}\}$, where $r_k = R\text{-rank of } N_k$, and
- (ii) The R -ideal class of the product of the Steinitz classes of the R -lattices N_0, \dots, N_{n-1} .

We conclude this section with a number of remarks about possible generalizations and refinements of our results above. By MO (40.8), a given hereditary order Λ can be embedded in only finitely many maximal orders, and the number of such maximal orders is intimately related to the structure of Λ . We shall see that in some cases, this number can be determined quite explicitly. Since the problem can always be reduced to the local case (see MO §40), we begin by assuming that the ground ring R is a d.v.r., and we recall some definitions from algebraic number theory.

Let R be a d.v.r. with maximal ideal P and residue class field \bar{R} . Let $\{P_i\}$ be the set of maximal ideals of S which contain P , and put $\bar{S} = S/P_1$. We now let

$$D = \{\sigma \in G : \sigma(P_1) = P_1\}, \quad I = \{\sigma \in D : \bar{\sigma} = 1 \text{ on } \bar{S}\},$$

where $\sigma \in G$ induces $\bar{\sigma} \in \text{Gal}(\bar{S}/\bar{R})$. Then D is the *decomposition group* of P_1 (relative to R), and I the *inertia group* of P_1 . It is easily verified that $D/I \cong \text{Gal}(\bar{S}/\bar{R})$; see Weiss [63, Ch. 4, §10].

Suppose now that S is tamely ramified over the d.v.r. R , so $T_{L/K}(S) = R$, and let Λ be the twisted group ring $S \circ G$. Then Λ is a hereditary order in $L \circ G$. As shown in MO §39, there are finitely many maximal orders in $L \circ G$ which contain Λ , and Λ is their intersection. Further, the number of such maximal orders coincides with the number of maximal two-sided ideals of Λ , which in turn equals the number of simple components of the semisimple \bar{R} -algebra $\Lambda/\text{rad } \Lambda$. According to the results of Williamson [63], this number is precisely the order of the inertia group I defined above.

We turn next to the generalization of the concept of a twisted group algebra and a twisted group ring. As before, let L be a finite Galois extension of K with Galois group G , and let $f: G \times G \rightarrow L^\times$ be a factor set on G with values in the multiplicative group L^\times of nonzero elements of L (see (8.26)). We may then form the *crossed-product algebra*

$$A = (L/K, f) = \bigoplus_{\sigma \in G} Lu_\sigma,$$

having an S -basis consisting of symbols $\{u_\sigma : \sigma \in G\}$, with multiplication in A defined by the formulas

$$u_\sigma a = \sigma(a)u_\sigma, \quad u_\sigma u_\tau = f(\sigma, \tau)u_{\sigma\tau}$$

for all $\sigma, \tau \in G$, $a \in L$. The condition that f be a factor set is precisely the condition that A be an associative algebra. The crossed-product algebra $A = (L/K, f)$ has already been encountered in (8.33). As shown in MO (29.6), A is a central simple K -algebra with $\dim_K A = n^2$, where $n = |G| = \dim_K L$. The K -isomorphism class of A depends only upon the cohomology class of f in $H^2(G, L)$. When f is the trivial factor set (all of whose values are 1), the crossed-product algebra A is just a full matrix algebra $M_n(K)$, as we showed in (28.3).

Now let S be the integral closure of R in L , where R is a Dedekind domain with quotient field K . In order to form the analogue of the twisted group ring $S \circ G$, we assume that $f: G \times G \rightarrow S^\times$ is a factor set whose values are units in S . Then

$$\Lambda = \bigoplus_{\sigma \in G} Su_\sigma$$

is an R -order in the crossed-product algebra $A = (L/K, f)$, and we quote without proof the following generalization of (28.7) due to Williamson [63] (see also Harada [64] and Merklen [78] for further results):

(28.12) Theorem. *The crossed-product order Λ (defined above) is a hereditary R -order in the crossed-product algebra $(L/K, f)$ if and only if $T_{L/K}(S) = R$, or equivalently, if and only if S is tamely ramified over R .*

It is known that a hereditary order Λ is contained in only finitely many maximal orders (see MO (40.8)), and it is of interest to determine all such maximal orders for a given order Λ of the type occurring in (28.12). We give without proof some results of Janusz [80]. Let $\Lambda = \bigoplus Su_\sigma$ be a hereditary R -order in the crossed-product algebra $A = (L/K, f)$. Janusz showed that the number of maximal R -orders in A containing Λ is precisely

$$\prod e(P)/m(P),$$

where P ranges over all maximal ideals of R . Here, $e(P)$ is the ramification index (over R) of any maximal ideal of S containing P . The integer $m(P)$ denotes the local index of A at P , defined as follows: the P -adic completion of A can be written as a full matrix algebra over a skewfield, and $m(P)$ is the index of this skewfield. Both $e(P)$ and $m(P)$ are equal to 1 for almost all P . Janusz showed further that the maximal orders containing Λ have the form $O_I(J\Lambda e)$, with J some ambiguous ideal of S , and e some primitive idempotent in A .

§28. Exercises

- Let L be a f.d. semisimple commutative K -algebra, where K is a field, and let G be a finite group of K -automorphisms of L . Suppose that the subalgebra of L invariant under G is K itself. Prove that the twisted group algebra $L \circ G$ is a central simple

K -algebra. (The result was pointed out by Merklen [78]; for G cyclic, it is due to Albert [39, p. 93, Th. 1].)

2. Let L be a Galois extension of K with finite Galois group $G = \{g_1, \dots, g_n\}$. Let

$$U(g) = [\delta_{g_i, gg_j}]_{1 \leq i, j \leq n}, \quad g \in G,$$

where for $g, h \in G$, $\delta_{gh} = 1$ if $g = h$, and 0 otherwise (see §10). For $a \in L$, let

$$a^* = \text{diag}(g_1^{-1}a, \dots, g_n^{-1}a) \in M_n(L).$$

Show that

$$U(g)a^* = (ga)^*U(g), \quad \text{for all } a \in L, g \in G.$$

Deduce that the map defined by

$$a \rightarrow a^*, \quad g \rightarrow U(G),$$

yields an n -th degree representation of $L \circ G$ over the field L .

3. Keep the above notation. Show that for $a_i \in L$,

$$\text{nr}_{(L \circ G)/K} \left(\sum_{i=1}^n a_i g_i \right) = \det \left(\sum_{i=1}^n a_i^* U(g_i) \right).$$

4. Prove the following generalization of Maschke's Theorem: Let K be a field, and $f: G \times G \rightarrow K$ a factor set from a finite group G into K . Let

$$A = \bigoplus_{x \in G} Ku_x, \quad \text{where } u_x u_y = f(x, y) u_{xy} \text{ for } x, y \in G,$$

and where the elements $\{u_x\}$ commute with those of K . Prove that A is a separable K -algebra if and only if $\text{char } K \nmid |G|$.

[Hint (Williamson [63], Harada [64]): The argument works for any commutative ring K , and a factor set $f: G \times G \rightarrow u(K)$. Changing the K -basis of A , we may assume that f is *normalized*, that is,

$$f(x, 1) = f(1, x) = 1, \quad x \in G,$$

and therefore u_1 is the unity element of A . Let \otimes be \otimes_K , and let $A^e = A \otimes A^\circ$, where A° is the opposite ring of A . Then (see MO, Exercise 7.9) A is K -separable if and only if A is projective as left A^e -module. Let μ be the A^e -surjection given by

$$\mu: A \otimes A^\circ \rightarrow A, \quad \mu(a \otimes b^\circ) = ab \text{ for } a, b \in A.$$

Then A is A^e -projective if and only if there exists a left A^e -homomorphism $\nu: A \rightarrow A^e$ which splits μ .

If $|G| \in u(K)$, the desired map ν is given by

$$\nu(a) = |G|^{-1} \sum_{x \in G} au_x \otimes u_x^{-1}, \quad a \in A.$$

Conversely, if ν splits μ , set

$$\nu(1) = \sum_{x, y \in G} \alpha_{x,y} (u_x \otimes u_y) \in A^e, \quad \alpha_{x,y} \in K.$$

Then

$$1 = \mu\nu(1) = \sum_{x \in G} \alpha_{x,x^{-1}} = |G| \alpha_{11},$$

since the condition

$$(u_z \otimes 1)\nu(1) = \nu(u_z) = (1 \otimes u_z)\nu(1) \text{ for } z \in G$$

implies that $\alpha_{x,x^{-1}} = \alpha_{11}$ for all $x \in G$.]

5. Let R be a d.v.r. with maximal ideal P and residue class field \bar{R} . Let $\Lambda = S \circ G$ be a twisted group ring as in (28.3), and set

$$PS = (P_1 \cdots P_g)^e, \quad J = P_1 \cdots P_g,$$

where the $\{P_i\}$ are the distinct G -conjugates of the maximal ideal P_1 of S . Let $\hat{\Lambda}$ denote the P -adic completion of Λ . Assume that $|G|$ is a unit in R , and that each S/P_i is a separable extension of \bar{R} . Prove that

$$\text{rad } \Lambda = J\Lambda, \quad \text{rad } \hat{\Lambda} = J\hat{\Lambda}.$$

[Hint (Williamson [63]; this proof was supplied to the authors by Janusz): Since $\sigma(J) = J$ for all $\sigma \in G$, $J\Lambda$ is a two-sided ideal of Λ . Further, $(J\Lambda)^e = P\Lambda \subseteq \text{rad } \Lambda$, so $J\Lambda \subseteq \text{rad } \Lambda$. Put

$$\bar{\Lambda} = \Lambda / J\Lambda = \bigoplus_{\sigma \in G} (S/J)u_{\sigma},$$

with G acting as a group of automorphisms of S/J . But

$$S/J \cong \coprod_{i=1}^g \bar{S}_i, \quad \text{where } \bar{S}_i = S/P_i.$$

If $\varphi_i: S \rightarrow \bar{S}_i$ is the natural surjection, and T is the ordinary trace from $\bar{\Lambda}$ to \bar{R} , then for $s \in S$ and $\sigma \in G$ we have

$$T(\bar{s}u_{\sigma}) = \begin{cases} |G| \cdot \sum_{i=1}^g T_i(\varphi_i s), & \sigma = 1, \\ 0, & \sigma \neq 1. \end{cases}$$

Here, T_i is the trace from \bar{S}_i to \bar{R} . Then $T: \bar{\Lambda} \times \bar{\Lambda} \rightarrow \bar{R}$ is a nondegenerate trace form, so $\bar{\Lambda}$ is a semisimple \bar{R} -algebra, and $\text{rad } \Lambda = J\Lambda$. Now use Exercise 5.7 to find $\text{rad } \bar{\Lambda}$.]

6. Prove Artin's Theorem (see Exercise 7.11) by using (28.3).

§29. ANNIHILATOR OF EXT

In §25 we saw the importance of the R -module $\mathrm{Ext}_\Lambda^1(M, N)$, where M and N are a pair of lattices for the R -order Λ . When $\Lambda = RG$, with G a finite group, the fact that $|G| \cdot \mathrm{Ext}(M, N) = 0$ for all such M and N , can be viewed as a useful generalization of Maschke's Theorem. We need an analogous result when Λ is an arbitrary R -order. If Λ is an R -order in a f.d. semisimple K -algebra A , then $\mathrm{Ext}(M, N)$ is a f.g. R -torsion R -module, by (25.5). The significant question is whether we can find nonzero elements $a \in R$, depending only on Λ , such that $a \cdot \mathrm{Ext}(M, N) = 0$ for all Λ -lattices M and N . Further, can we do better by considering those $a \in R$ such that for a given M , $a \cdot \mathrm{Ext}(M, N) = 0$ for all N ? We devote this section to answering such questions.

§29A. Annihilator of Ext; Higman Ideal

There are two main results from this section which will play a vital role in Chapter 4. Suppose that Λ is an R -order in a separable K -algebra A , and let Λ' be a maximal R -order in A containing Λ . Then there exist nonzero elements $a \in R$ such that $a\Lambda' \subseteq \Lambda$ (this is obvious), and for such $a \in R$ we will show that

$$a \cdot \mathrm{Ext}_\Lambda^1(M, N) = 0$$

for all Λ -lattices M and all Λ -modules N . The second major result is a consequence of the first one, namely,

$$\mathrm{Ext}_\Lambda^1(M, N) \cong \coprod_P \mathrm{Ext}_{\Lambda_P}^1(M_P, N_P)$$

for M, N as above, where P ranges over the finite set of maximal ideals of R for which $\Lambda_P \neq \Lambda'_P$.

There are two rather different approaches to the problem of determining which elements of R annihilate $\mathrm{Ext}(M, N)$ for all M and N . One method is to embed the given R -order Λ in a maximal order Λ' in A , and then use the fact that every Λ' -lattice is Λ' -projective (see (26.12)). This usually yields stronger results than the second method, due to D. G. Higman, in which one constructs an ideal $i(\Lambda)$ of R such that

$$(29.1) \quad i(\Lambda) \cdot H^1(\Lambda, T) = 0 \text{ for every } (\Lambda, \Lambda)\text{-bimodule } T.$$

By (25.10) we have $\mathrm{Ext}_\Lambda^1(M, N) \cong H^1(\Lambda, \mathrm{Hom}_R(M, N))$ whenever M and N are Λ -lattices, and hence

$$(29.2) \quad i(\Lambda) \cdot \mathrm{Ext}_\Lambda^1(M, N) = 0 \text{ for all } \Lambda\text{-lattices } M \text{ and } N.$$

However, even though the *Higman ideal* $i(\Lambda)$ is the largest ideal of R for

which (29.1) holds, it is not necessarily the largest ideal such that (29.2) is valid.

Let A be a f.d. separable K -algebra, and let R be a Dedekind domain with quotient field K . Let C denote the integral closure of R in the center of A . By (26.10), C is the unique maximal R -order in this center. Furthermore, every maximal R -order Λ' in A must contain C , since otherwise $C\Lambda'$ is a larger order. The following concept was first introduced in §27:

(29.3) Definition. Let Λ be an R -order in A , and let $\Lambda \subseteq \Lambda'$, where Λ' is a maximal R -order in A . The *central conductor* of Λ' into Λ is defined to be

$$F = \{c \in C : c\Lambda' \subseteq \Lambda\}.$$

Now $\alpha\Lambda' \subseteq \Lambda$ for some nonzero $\alpha \in R$, so $\alpha \in F$, and therefore also $\alpha C \subseteq F$. Thus F is an ideal of C such that $K \cdot F = K \cdot C =$ center of A . Further, $F \subseteq \Lambda$ since $1 \in \Lambda'$.

We now prove the following basic result due to Jacobinski [66]:

(29.4) Theorem. Let Λ be an R -order in a semisimple K -algebra A , and let F be the central conductor of Λ' into Λ , where Λ' is a maximal R -order in A containing Λ . Then:

$$F \cdot \text{Ext}_\Lambda^1(M, N) = 0 \text{ for all } \Lambda\text{-lattices } M \text{ and all } \Lambda\text{-modules } N.$$

Proof. We write Ext in place of Ext_Λ^1 , and Hom in place of Hom_Λ , for convenience. Given a Λ -lattice M , let

$$0 \rightarrow X \xrightarrow{i} Y \rightarrow M \rightarrow 0$$

be a Λ -exact sequence with $Y = \Lambda^{(k)} \subseteq A^{(k)}$, and i the inclusion map. Then for any Λ -module N , (8.9iii) gives

$$\text{Ext}(M, N) \cong \text{Hom}(X, N) / i^*(\text{Hom}(Y, N)).$$

We need only show that for each $f \in \text{Hom}(X, N)$ and each $c \in F$, the element cf lies in the image of i^* . Note that cf is a Λ -homomorphism since c lies in the center of Λ .

We set $Y' = \Lambda'Y$ (computed inside $A^{(k)}$), so $Y' = \Lambda'^{(k)}$. Let $X_1 = KX \cap Y'$, an R -pure Λ' -sublattice of Y' by (23.15); then Y'/X_1 is a Λ' -lattice, hence is Λ' -projective by (26.12). Therefore the exact sequence

$$0 \rightarrow X_1 \rightarrow Y' \rightarrow Y'/X_1 \rightarrow 0$$

is Λ' -split, so there exists a map $j \in \text{Hom}_{\Lambda'}(Y', X_1)$ which splits the inclusion $X_1 \subseteq Y'$; in other words, j restricted to X_1 is the identity map.

Now let f and c be given, so $c\Lambda' \subseteq \Lambda$, and hence $cY' \subseteq Y$. Since $Y/X \cong M$ and M is a Λ -lattice, it follows that X is R -pure in Y , and thus $X = KX \cap Y \subseteq X_1$. Therefore

$$cX_1 = c(KX \cap Y') \subseteq KX \cap cY' \subseteq KX \cap Y = X.$$

We may thus define $f_1 \in \text{Hom}_\Lambda(X_1, N)$ by setting $f_1(x_1) = f(cx_1)$, $x_1 \in X_1$. Then f_1 extends the map $cf: X \rightarrow N$.

Consider the commutative diagram

$$\begin{array}{ccc} X \subseteq X_1 & \xrightleftharpoons{i} & Y' \\ cf \downarrow & \swarrow f_1 & \\ N & & \end{array}$$

in which each map is a Λ -homomorphism. Let g be the restriction of $f_1 j$ to the Λ -submodule Y of Y' . Then $g \in \text{Hom}(Y, N)$ and $i^*(g) = cf$. We have thus shown that cf extends to a homomorphism from Y to N , that is, $cf \in \text{im}(i^*)$, which completes the proof.

Keep the above notation; let $\alpha \in R$ be a nonzero element such that $\alpha\Lambda' \subseteq \Lambda$; then $\alpha \in R \cap F$, which shows at once that $R \cap F$ is a nonzero ideal of R . Consequently, we obtain:

(29.5) Corollary. *Let Λ be any R -order in a separable K -algebra A . Then there exists a nonzero ideal c of R such that*

$$c \cdot \text{Ext}_\Lambda^1(M, N) = 0 \text{ for every } \Lambda\text{-lattice } M \text{ and every } \Lambda\text{-module } N.$$

Proof. By (26.5), Λ is contained in some maximal R -order Λ' in A , and it suffices to choose $c = R \cap F$, where F is the central conductor of Λ' into Λ .

Remarks. (i) The proof of (29.4) carries over unchanged to the case where Λ' is any *hereditary* order, whether maximal or not. We could thus have chosen the ideal c in (29.5) to be the ideal of R generated by all elements in $R \cap F$, with F ranging over all central conductors of hereditary orders (above Λ) into Λ .

(ii) For a fixed order Λ , the central conductor of Λ' into Λ may well depend on the choice of the maximal order Λ' containing Λ .

(29.6) Corollary. *Let Λ , M and N be as in (29.4), and let $e \in C$ be idempotent. Let M and N be Λ -lattices such that either $eM = M$ or $eN = N$. Then*

$$\{\alpha \in R : \alpha e \in F\} \text{ annihilates } \text{Ext}_\Lambda^1(M, N).$$

Proof. Let $\alpha \in R$ be such that $\alpha e \in F$; then $\alpha e \cdot \text{Ext}(M, N) = 0$ by (29.4). But αe and α act in the same way on $\text{Ext}(M, N)$, since the hypothesis implies that e acts as the identity map on either M or N .

To conclude this part of the discussion, we present an improvement of (25.6), which may in turn be viewed as a generalization of (25.15):

(29.7) Proposition. *Let Λ be an R -order in a separable K -algebra A , and let*

$$S(\Lambda) = \{P : P = \text{maximal ideal of } R, \Lambda_P \neq \text{maximal } R_P\text{-order in } A\}.$$

Let M and N be left Λ -lattices. Then

$$\text{Ext}_\Lambda^1(M, N) \cong \coprod_{P \in S(\Lambda)} \text{Ext}_{\Lambda_P}^1(M_P, N_P).$$

Proof. If $P \notin S(\Lambda)$ then Λ_P is a maximal R_P -order, and M_P is a Λ_P -lattice. Then M_P is Λ_P -projective since Λ_P is hereditary (see (26.12)), so $\text{Ext}_{\Lambda_P}^1(M_P, *) = 0$ by §8. The result now follows from (25.6).

We now restrict our attention to the special case where $\Lambda = RG$ and $A = KG$, with K an algebraic number field and G a finite group. In (27.13) we determined the central conductor F of a maximal R -order Γ into Λ , namely

$$F = \prod_{i=1}^t (n/n_i) \mathfrak{D}^{-1}(R_i/R).$$

Here, $\prod_{i=1}^t R_i$ is the integral closure of R in the center of KG , and $\mathfrak{D}^{-1}(R_i/R)$ is the inverse different of R_i with respect to R . Further, $n = |G|$, and the $\{n_i\}$ are the integers defined in (27.4). Let

$$1 = e_1 + \cdots + e_t$$

be the decomposition of 1 into central primitive idempotents in A . Then the ideals $\{Ae_i\}$ are the Wedderburn components of A , and the center of Ae_i is just K_i , the quotient field of R_i . By definition,

$$n_i^2 = \dim_{K_i} A_i, \quad 1 \leq i \leq t.$$

Let e be a central idempotent in A , so that e is a sum of a subset of $\{e_1, \dots, e_t\}$. For $\alpha \in R$, we have $\alpha e \in F$ if and only if $\alpha \in (n/n_i) \mathfrak{D}^{-1}(R_i/R)$ for each e_i occurring in e . As shown in the proof of (27.13), where $\mathfrak{D}^{-1}(R_i/R)$ was denoted by δ_i^{-1} , we have

$$R \cap (n/n_i) \mathfrak{D}^{-1}(R_i/R) = (n/n_i)(K \cap \mathfrak{D}^{-1}(R_i/R)) = (n/n_i) \delta_i^{-1},$$

where

$$(29.8) \quad \mathfrak{d}_i^{-1} = K \cap \mathfrak{D}^{-1}(R_i/R) \supseteq R.$$

Note that \mathfrak{d}_i^{-1} is a fractional R -ideal in K , and its inverse \mathfrak{d}_i is an ideal of R . From (29.6) and the above discussion, we obtain:

(29.9) Theorem (Jacobinski [66]). *Let M and N be RG-lattices, and let*

$$I = \{i : 1 \leq i \leq t, e_i M \neq 0\}.$$

Then

$$\bigcap_{i \in I} (n/n_i) \mathfrak{d}_i^{-1} \text{ annihilates } \mathrm{Ext}_{RG}^1(M, N).$$

In particular,

$$\bigcap_{i=1}^t (n/n_i) \mathfrak{d}_i^{-1} \text{ annihilates } \mathrm{Ext}(M, N)$$

for any RG-lattices M and N .

(29.10) Corollary. *Let M and N be RG-lattices*, such that either $e_i M = M$ or $e_i N = N$. Then*

$$(n/n_i) \mathfrak{d}_i^{-1} \cdot \mathrm{Ext}(M, N) = 0.$$

If the A -module KM is absolutely simple, then $\mathrm{End}_A(KM) \cong K$; this implies that $K_i = K$, $R_i = R$, and $\mathfrak{d}_i^{-1} = R$. Further, in this case $n_i = \dim_K KM$, and we obtain:

(29.11) Corollary. *Let M and N be RG-lattices, where KM is an absolutely simple A -module. Let $n_i = \dim_K KM$. Then*

$$(n/n_i) \mathrm{Ext}(M, N) = 0 \text{ for all } N.$$

An analogous result holds when KN is absolutely simple.

This corollary is due to Reiner [63]. In the next subsection, we shall show that the result is best possible (see (29.19)). We shall also discuss the question of determining the largest ideal of R which annihilates $\mathrm{Ext}(M, N)$ for fixed M and all N .

*It suffices to assume M an RG-lattice, and N may be any RG-module.

We conclude with a brief discussion of the Higman ideal. Let Λ be an arbitrary R -order in a K -algebra A . By definition, the *Higman ideal* $i(\Lambda)$ is the largest ideal of R such that (29.1) holds true. As shown in CR (75.11), $i(\Lambda) \neq 0$ if and only if A is a separable K -algebra. Further,

$$i(S^{-1}\Lambda) = S^{-1} \cdot i(\Lambda)$$

for every multiplicative subset S of R . In particular,

$$i(\dot{\Lambda}_P) = \{i(\Lambda)\}_P$$

for each maximal ideal P of R .

Suppose now that we are given a nondegenerate associative bilinear form $f: A \times A \rightarrow K$. We may use f to calculate $i(\Lambda)$, as follows: Let $A = \bigoplus_{i=1}^n Ka_i$, and let $\{b_j\}$ be a dual K -basis of A , chosen so that $f(a_i, b_j) = \delta_{ij}$, $1 \leq i, j \leq n$. For $x \in A$, let

$$(29.12) \quad c(x) = \sum_{i=1}^n b_i x a_i.$$

Then (see CR §71) c is a well defined map from A into its center, and does not depend on the choice of bases. Let $c(A) = \{c(x) : x \in A\}$; then $c(A)$ coincides with the center of A if and only if A is a separable K -algebra (see CR (71.6); the result is due to D. G. Higman [55b]).

We now define the *inverse different* $\mathfrak{D}^{-1}(\Lambda/R)$ and the *different* $\mathfrak{D}(\Lambda/R)$ by the formulas

$$\mathfrak{D}^{-1}(\Lambda/R) = \{a \in A : f(\Lambda, a) \subseteq R\},$$

$$\mathfrak{D}(\Lambda/R) = \{x \in A : \mathfrak{D}^{-1} \cdot x \subseteq \Lambda\}.$$

Then D. G. Higman's formula for $i(\Lambda)$ is as follows (see CR (75.14)):

$$i(\Lambda) = R \cap c(\mathfrak{D}(\Lambda/R)),$$

where c is defined as in (29.12). Further, $i(\Lambda) \neq 0$ if and only if A is a separable K -algebra. When $\Lambda = RG$, we have $i(\Lambda) = |G|R$ (CR, §75, p. 528).

Let us now assume that A is a separable K -algebra, and let $\text{tr}_{A/K}$ be the reduced trace from A to K . Then we obtain a nondegenerate associative symmetric bilinear form f by setting $f(a, b) = \text{tr}_{A/K}(ab)$ for $a, b \in A$ (see §7D, or MO (9.26)). In that case, \mathfrak{D} is the usual different computed relative to reduced trace. In particular, suppose that A is commutative; then one verifies (Exercise 29.1) that $c(x) = x$ for each $x \in A$, and hence

$$i(\Lambda) = R \cap \mathfrak{D}(\Lambda/R).$$

When Λ' is a maximal order, we obtain

$$i(\Lambda') = R \cap \mathfrak{D}(\Lambda'/R).$$

Now it may well happen that $i(\Lambda') \subset R$; for example, let Λ' be the integral closure S of R in a finite separable field extension L of K . If some prime P of R ramifies in S , then $P_1 \supseteq \mathfrak{D}(S/R)$ for some prime P_1 of S containing R . Then $P = R \cap P_1 \supseteq R \cap \mathfrak{D}(S/R)$. Hence every prime of R ramified in S is a divisor of the Higman ideal $i(S)$ relative to R . However, $\text{Ext}_S^1(M, N) = 0$ for every S -lattice M and every S -module N , so (29.4) and (29.5) are stronger results than (29.2)! Note that in this example, the central conductor differs from the Higman ideal.

§29B. Projective Endomorphisms

Let M and N be left Λ -modules, where Λ is any ring. In §8 we saw that $\text{End}_{\Lambda} M$ acts from the right on $\text{Ext}_{\Lambda}^1(M, N)$. Let us review this situation, interpreting elements of $\text{Ext}(M, N)$ as equivalence classes of extensions of N by M . Let $\xi \in \text{Ext}(M, N)$ correspond to the class of the short exact sequence of Λ -modules

$$\xi: 0 \rightarrow N \rightarrow X \xrightarrow{\mu} M \rightarrow 0.$$

Given any $\varphi \in \text{End } M$, the class of $\xi\varphi$ corresponds to a sequence

$$0 \rightarrow N \rightarrow X_1 \rightarrow M \rightarrow 0,$$

where X_1 is the pullback of the pair of maps μ, φ (see §2A). There is thus a commutative diagram

$$(29.13) \quad \begin{array}{ccccccc} \xi: & 0 & \longrightarrow & N & \longrightarrow & X & \xrightarrow{\mu} M \longrightarrow 0 \\ & & & \uparrow 1 & & \uparrow \varphi_1 & \\ \xi\varphi: & 0 & \longrightarrow & N & \longrightarrow & X_1 & \xrightarrow{\mu_1} M \longrightarrow 0. \end{array}$$

We may identify X_1 with $\{(x, m) \in X + M : \mu(x) = \varphi(m)\}$, and then

$$\mu_1(x, m) = m, \quad \varphi_1(x, m) = x, \quad \text{for } (x, m) \in X_1.$$

(29.14) Definition. A *projective endomorphism* of M is an element $\varphi \in \text{End}_{\Lambda} M$ such that φ annihilates $\text{Ext}_{\Lambda}^1(M, N)$ for each N .

Thus, in particular, M is Λ -projective if and only if the identity map 1_M is a projective endomorphism of M . In general, φ is a projective endomorphism if and only if for each sequence ξ in (29.13), the sequence $\xi\varphi$ is split exact.

We now characterize projective endomorphisms in another way. Given a left Λ -module M , we may form its *dual* $\text{Hom}_\Lambda(M, \Lambda)$, consisting of all left Λ -homomorphisms from M into Λ . Since Λ is a (Λ, Λ) -bimodule, the dual can be made into a right Λ -module in a natural way. Explicitly, for $f \in \text{Hom}_\Lambda(M, \Lambda)$ and $\lambda \in \Lambda$, we define $f\lambda$ by

$$(f\lambda)(m) = f(m)\lambda, m \in M.$$

(The fact that $f\lambda \in \text{Hom}_\Lambda(M, \Lambda)$ is easily checked. It also follows from general principles, if we recall from §2 that the right action of Λ on the bimodule ${}_\Lambda\Lambda_\Lambda$ produces a right action of Λ on $\text{Hom}_\Lambda(M, \Lambda)$.)

(29.15) Proposition. *Let M be a f.g. left Λ -module. Define*

$$\tau : \text{Hom}_\Lambda(M, \Lambda) \otimes_\Lambda M \rightarrow \text{End}_\Lambda M$$

by

$$\tau(f \otimes m) : m' \mapsto f(m')m, m' \in M, f \in \text{Hom}_\Lambda(M, \Lambda), m \in M,$$

extended by linearity. Then the image of τ coincides with the set of projective endomorphisms of M .

Proof. It is easily checked that τ is a well defined two-sided $\text{End}_\Lambda(M)$ -homomorphism, if we view $\text{End}_\Lambda M$ as acting from the right on M (see §3D).

We may choose a Λ -exact sequence $0 \rightarrow M' \rightarrow F \rightarrow M \rightarrow 0$, in which $F = \bigoplus_{i=1}^n \Lambda x_i$ is a free Λ -module on N generators $\{x_i\}$. If $\varphi \in \text{End}_\Lambda M$ is a projective homomorphism, consider the commutative diagram with exact rows:

$$\begin{array}{ccccccc} \xi : 0 & \longrightarrow & M' & \longrightarrow & F & \xrightarrow{\mu} & M \longrightarrow 0 \\ & & \downarrow 1 & & \downarrow \varphi_1 & & \downarrow \varphi \\ \xi\varphi : 0 & \longrightarrow & M' & \longrightarrow & F_1 & \xrightarrow{\mu_1} & M \longrightarrow 0. \end{array}$$

Since φ is a projective endomorphism, there exists a map $\rho : M \rightarrow F_1$ which splits μ_1 , that is, $\mu_1 \rho = 1_M$. Write

$$(\varphi_1 \rho)(m) = \sum_{i=1}^n f_i(m)x_i,$$

with each $f_i \in \text{Hom}_\Lambda(M, \Lambda)$ (as is easily verified). Then

$$\varphi(m) = (\varphi \mu_1 \rho)(m) = (\mu \varphi_1 \rho)(m) = \mu \{ \sum f_i(m)x_i \} = \sum f_i(m)\mu(x_i).$$

It follows that

$$\varphi = \tau \left\{ \sum_{i=1}^n f_i \otimes \mu(x_i) \right\} \in \text{im } \tau,$$

as claimed.

Let us show conversely that every $\varphi \in \text{im } \tau$ is a projective endomorphism of M . Suppose that

$$\varphi = \tau \left\{ \sum_{i=1}^k f_i \otimes m_i \right\}, \quad f_i \in \text{Hom}_{\Lambda}(M, \Lambda), \quad m_i \in M.$$

Then

$$\varphi(m) = \sum f_i(m) m_i, \quad m \in M.$$

Consider the diagram (29.13), and choose $x_i \in X$ with $\mu(x_i) = m_i$, $1 \leq i \leq k$. Now let

$$\rho(m) = (\sum f_i(m)x_i, m) \in X + M \text{ for } m \in M.$$

Since

$$\mu(\sum f_i(m)x_i) = \varphi(m) \text{ for } m \in M,$$

it follows that $\rho \in \text{Hom}_{\Lambda}(M, X_1)$. Further, $\mu_1 \rho(m) = m$ for $m \in M$, so ρ is a splitting of μ_1 . Thus, for each $\xi \in \text{Ext}_{\Lambda}^1(M, N)$, the class of sequences corresponding to $\xi \varphi$ are split exact. This proves that φ is a projective endomorphism, and establishes the proposition.

(29.16) Corollary. *Let R be a Dedekind domain, Λ an R -algebra, M a f.g. left Λ -module, and $\varphi \in \text{End}_{\Lambda} M$. Then φ is a projective endomorphism of M if and only if for each maximal ideal P of R , the localization φ_P is a projective endomorphism of M_P .*

Proof. This follows at once from (29.15) and (4.2).

In order to apply (29.15) to the case where Λ is an integral group ring RG , we need another characterization of the dual $\text{Hom}_{RG}(M, RG)$ of a left RG -module M .

(29.17) Lemma. *Let $\Lambda = RG$, where G is a finite group and R is any commutative ring. Let M be any left Λ -module. Then there is an isomorphism of right Λ -modules*

$$\theta : \text{Hom}_R(M, R) \cong \text{Hom}_{\Lambda}(M, \Lambda),$$

given by

$$\theta(h) : m \mapsto \sum_{x \in G} h(x^{-1}m)x, \quad m \in M.$$

In other words, $\theta(h) = \sum_x xhx^{-1}$.

Proof. We have already seen in Proposition 10.21 that θ is an R -isomorphism, so it suffices to verify that

$$\theta(hy) = \theta(h)y \text{ for all } h \in \text{Hom}_R(M, R), y \in G.$$

For $m \in M$, we have

$$\begin{aligned} \{\theta(hy)\}m &= \sum_x (hy)(x^{-1}m) \cdot x = \sum_x (h(yx^{-1}m)) \cdot x \\ &= \sum_{z \in G} h(z^{-1}m) \cdot zy = \{\theta(h)m\}y = \{\theta(h)y\}m, \end{aligned}$$

as desired. This completes the proof. Note that $\text{Hom}_R(M, R)$ has been made into a right Λ -module by using the (Λ, R) -bimodule structure of M .

We shall combine this lemma with (29.15) to obtain a useful description of the projective endomorphisms of an RG -lattice. The result is due to D. G. Higman [57]; for a direct proof, see also Reiner [63].

(29.18) Theorem. Let $\Lambda = RG$ with G a finite group and R an arbitrary commutative ring. Let M be a left Λ -lattice (that is, a left Λ -module f.g. and projective over R). Let $\varphi \in \text{End}_\Lambda M$; then φ is a projective endomorphism of M if and only if

$$\varphi = \sum_{x \in G} xhx^{-1} \text{ for some } h \in \text{End}_R M.$$

Proof. Let $\sigma : \text{End}_R(M) \rightarrow \text{End}_\Lambda(M)$ be the additive R -homomorphism defined by

$$\sigma(h) = \sum_{x \in G} xhx^{-1}, \quad h \in \text{End}_R(M).$$

Let $\tau_0 : \text{Hom}_R(M, R) \otimes_R M \rightarrow \text{End}_R(M)$ be defined as in (29.15), using $\Lambda = R$ in the definition. Then τ_0 is surjective, since M is R -projective.

It is easily verified that the following diagram is commutative, where θ is defined as in (29.17):

$$\begin{array}{ccc} \text{Hom}_R(M, R) \otimes_R M & \xrightarrow{\tau_0} & \text{End}_R(M) \\ \theta \otimes 1 \downarrow & & \downarrow \sigma \\ \text{Hom}_\Lambda(M, \Lambda) \otimes_\Lambda M & \xrightarrow{\tau} & \text{End}_\Lambda(M). \end{array}$$

Since both τ_0 and $\theta \otimes 1$ are surjective, it follows at once that $\text{im } \tau = \text{im } \sigma$. This implies the desired result, by (29.15). (A related result is given in (19.2iii).)

(29.19) Corollary (Reiner [63]). *Let G be a finite group of order n , and R a Dedekind domain with quotient field K , where $\text{char } K \nmid n$. Let M be an RG -lattice such that KM is an absolutely simple KG -module, and let $d = \dim_K KM$. Then $d \mid n$, and for any $a \in R$ we have*

$$a \cdot \text{Ext}_{RG}^1(M, *) = 0 \text{ if and only if } a \in (n/d)R.$$

Proof. The ring $\text{End}_\Lambda M$ is an R -order in $\text{End}_{KG}(KM)$. But $\text{End}_{KG}(KM) \cong K$ since KM is absolutely simple, and thus it follows that $\text{End}_\Lambda(M) \cong R$. Hence $a \cdot \text{Ext}_{RG}^1(M, *) = 0$ if and only if a_l is a projective endomorphism of M , where a_l denotes left multiplication by a on M . By (29.18), this occurs precisely when

$$(29.20) \quad a_l = \sum_{x \in G} xhx^{-1} \text{ for some } h \in \text{End}_R(M).$$

Thus, we must prove that (29.20) holds if and only if $a \in (n/d)R$.

For each $h \in \text{End}_R(M)$, let $T(h)$ denote the trace of the K -linear transformation of KM induced by h ; then $T(h) \in R$ by (26.1). Further, $T(xhx^{-1}) = T(h)$ for each $x \in G$. Finally, for each h the expression $\sum xhx^{-1}$ gives an element of $\text{End}_{RG}(M)$, hence equals a_l for some $a \in R$. Taking traces on both sides, we obtain the equation

$$d \cdot a = nT(h).$$

In particular, choosing h so that $T(h) = 1$, we see that $n/d \in R$, whence also* $n/d \in \mathbb{Z}$, so $d \mid n$. Secondly, for arbitrary h we obtain $a = (n/d)T(h) \in (n/d)R$ whenever (29.20) holds. This completes the proof. The result strengthens that of (29.11).

To conclude this subsection, we present Roggenkamp's [71] partial converse of Theorem 29.9. Let $A = KG$, $\Lambda = RG$, where R is a Dedekind domain whose quotient field K is an algebraic number field. Let Λ' be a maximal R -order in A such that $\Lambda' \supseteq \Lambda$, and let $(\Lambda': \Lambda)_l$ be the left conductor of Λ' into Λ (see (27.2)). Let e be a central idempotent of A , and view $\Lambda'e$ as left Λ -module. Then each $f \in \text{Hom}(\Lambda'e, \Lambda)$ is given by right multiplication a_r for some $a \in A$ such that $ae \in (\Lambda': \Lambda)_l$. Since $a_r = (ae)_r$, we thus have an identification $\text{Hom}_\Lambda(\Lambda'e, \Lambda) \cong Ae \cap (\Lambda': \Lambda)_l$. Both Ae and $(\Lambda': \Lambda)_l$ are two-sided Λ' -modules (see (27.8)), whence so is their intersection.



*Since n/d lies in every R , it belongs to $\mathbb{Q} \cap \text{alg. int.}\{K\}$ (assuming K is an algebraic number field), and so $n/d \in \mathbb{Z}$. This also holds for arbitrary K , by (9.32) and Exercise 18.4.

Let

$$\tau : \text{Hom}(\Lambda'e, \Lambda) \otimes_{\Lambda} \Lambda'e \rightarrow \text{End}_{\Lambda} \Lambda'e$$

be the map defined as in (29.15). Identifying $\text{End}_{\Lambda} \Lambda'e$ with $\Lambda'e$, we see that we may also identify the image of τ with

$$\{Ae \cap (\Lambda' : \Lambda)_l\} \cdot \Lambda'e = Ae \cap (\Lambda' : \Lambda)_l.$$

Thus, the projective endomorphisms of the left Λ -lattice $\Lambda'e$ are given by right multiplications by elements of $Ae \cap (\Lambda' : \Lambda)_l$. In particular, for $\alpha \in R$ we have (see (29.10)):

(29.21)

$$\begin{cases} \alpha \cdot \text{Ext}_{\Lambda}^1(\Lambda'e, *) = 0 \\ \text{if and only if } \alpha \in (n/n_i)\delta_i^{-1} \text{ for each idempotent summand } e_i \text{ of } e. \end{cases}$$

From this result we obtain:

(29.22) Theorem (Roggenkamp [71]). *Let $\alpha \in R$. Then*

(i) $\alpha \cdot \text{Ext}_{\Lambda}^1(M, N) = 0$ for all Λ -lattices M and N if and only if

$$\alpha \in \bigcap_{i=1}^t (n/n_i)\delta_i^{-1},$$

using the notation of (29.9).

(ii) *For each central idempotent e of A , there exists a Λ -lattice M (namely $\Lambda'e$) such that $eM = M$, and such that*

$$\alpha \cdot \text{Ext}_{\Lambda}^1(M, *) = 0 \text{ if and only if } \alpha \in \bigcap_{e_i|e} (n/n_i)\delta_i^{-1},$$

where the intersection is over all indices i for which the central primitive idempotent e_i occurs as a summand of e .

(iii) *For each central primitive idempotent e_i of A , there exists a Λ -lattice M (namely $\Lambda'e_i$) such that $e_iM = M$, and such that*

$$(29.23) \quad \alpha \cdot \text{Ext}_{\Lambda}^1(M, *) = 0 \text{ if and only if } \alpha \in (n/n_i)\delta_i^{-1}.$$

Note that we have not proved a complete converse to (29.9) and (29.10). For example, we have not settled the following question: let M be a Λ -lattice such that KM is simple, and let e_i be the central idempotent such that

$e_i M = M$. Does (29.23) hold true in this case? Reiner's Theorem 29.19 shows that it holds whenever KM is absolutely simple, but there is still a gap for the case where KM is simple but not absolutely simple. Further results on this problem may be found in Plesken [78].

(29.24) Notes. (i) Let G be a finite group having a normal cyclic Sylow p -subgroup H , and let \hat{Z} , \hat{Q} , etc., denote p -adic completions. Let M and N be $\hat{Z}G$ -lattices such that $\hat{Q}M \cong \hat{Q}N$, and $\hat{Q}M$ is simple. Berman [66] proved that

$$\mathrm{Ext}_{\hat{Z}G}^1(\hat{M}, \hat{N}) = 0.$$

Gudivok observed that the analogous statement fails when \hat{Z} is replaced by some larger P -adic ring. Indeed, the results in Exercise 26.9 lead to a counterexample.

(ii) Let $R = \text{alg. int. } \{K\}$, and let V and W be f.g. left KG -modules. Put

$$\sigma(V) = \{M : M = \text{full } RG\text{-lattice in } V\}.$$

Several authors have considered the question as to whether

$$\mathrm{Ext}_{RG}^1(M, N) = 0 \text{ for all } M \in \sigma(V), N \in \sigma(W),$$

and obtained *sufficient* conditions in certain special cases. See the work of Berman-Lichtman [65], generalized by Reiner [67]. Also see Plesken [78].

§29. Exercises

1. Let L be a finite separable field extension of K , and let $T: L \rightarrow K$ be the trace map. Let $f: L \times L \rightarrow K$ be the bilinear trace form given by $f(a, b) = T(ab)$ for $a, b \in L$. If $\{a_i\}$ and $\{b_j\}$ are dual bases of L over K relative to f , show that

$$\sum a_i b_i = 1.$$

[Hint: Let $L = \bigoplus_{i=1}^n Ka_i$, $T(a_i b_j) = \delta_{ij}$, $1 \leq i, j \leq n$. For $x \in L$, write

$$xa_i = \sum_{j=1}^n \alpha_{ij} a_j, \quad \alpha_{ij} \in K, \quad 1 \leq i \leq n.$$

Then

$$\sum_i T(xa_i b_i) = \sum_{i,j} \alpha_{ij} T(a_j b_i) = \sum_i \alpha_{ii} = T(x).$$

Hence

$$f\left(x, 1 - \sum_i a_i b_i\right) = 0 \text{ for all } x \in L,$$

and so $\sum a_i b_i = 1$.]

2. Prove the analogous result when L is a commutative separable K -algebra. Can the hypothesis of commutativity be omitted?

3. Let Λ be any ring. Show that the set of projective endomorphisms of a left Λ -module M is a two-sided ideal of $\text{End}_{\Lambda}(M)$.

4. Let M and N be RG -lattices, and keep the notation of (29.9). Show that $n/\text{G.C.D. } (n_1, \dots, n_t)$ annihilates $\text{Ext}_{RG}^1(M, N)$.

5. Let R be a commutative ring, G a finite group, H a subgroup of G , and M a left RG -module. Suppose there exists an $h \in \text{End}_{RH}(M)$ such that $\sum_{i=1}^n x_i h x_i^{-1} = 1_M$,

where $G = \bigcup_{i=1}^n x_i H$. Show that every exact sequence of RG -modules

$$0 \rightarrow X \rightarrow Y \rightarrow M \rightarrow 0$$

which splits over RH also splits over RG . (See also §19A.)

6. Use Theorem 29.18 to give another proof of Exercise 4.15.

[Hint: Let $s_0 \in S$ be such that $T_{L/K}(s_0) = 1$. In (29.18) let h be left multiplication by s_0 on S . Then $\sum_{x \in G} x h x^{-1} = T_{L/K}(s_0) = 1$, so the identity map on S is a projective endomorphism. Therefore S is RG -projective.]

Local and Global Theory of Integral Representations

In these introductory remarks, let Λ be an R -order in a f.d. separable K -algebra A , where R is a Dedekind domain with quotient field K . In Chapter 3, the basic idea was to study a Λ -lattice M by relating it to the A -module KM which it generates. This led naturally to the problem of describing M as an extension of a Λ -lattice N by another Λ -lattice L . The extension problem was treated by introducing the R -module $\mathrm{Ext}_\Lambda^1(N, L)$, which could be calculated from the behavior of the localizations $\{N_P\}$ and $\{L_P\}$ at some finite set of maximal ideals P of R .

The preceding remark suggests that the knowledge of the localizations $\{M_P\}$ of a Λ -lattice M will provide more information about M than does the A -module KM . We also expect that some finite set of P 's will play a basic role in the relationship between M and the $\{M_P\}$, and it is the study of this relationship which is the central theme of Chapter 4.

As a first step in this program, §30 is devoted to a closer look at the local situation, where R is a d.v.r. with maximal ideal P . Parts of the discussion in Chapter 2, where Λ is the group ring RG of a finite group G , anticipate some of the results of §30. In general, however, the point of view here is considerably different from that in Chapter 2, and we are interested in Λ -lattices themselves, rather than merely in using them as an intermediate tool for relating ordinary and modular representations of G . We shall continue to use the notation of Chapter 3, denoting a maximal ideal of R by P , rather than \mathfrak{p} as in Chapter 2. Further, k will now be used as an index, rather than for the residue class field of R .

Section 30 begins with a review of relevant material from the Introduction, especially §§5–6. We then consider properties of a Λ -lattice M , where Λ is an arbitrary R -order. For example, we shall see that projective Λ -lattices are completely determined by their behavior mod P . Maranda's Theorems generalize this fact to show that an arbitrary Λ -lattice M is determined by its behavior mod P^k , for some sufficiently large k which depends on Λ , but not on M .

In §30B we introduce the technique of extension of the ground ring. This is a natural idea, in view of the importance of ground field extension and

splitting fields in the theory of representations of algebras. The results of §30B were already needed in Chapter 2, and will be used again later in this Chapter.

Section 31 introduces the concept of genus, which is of decisive importance for all further discussion of integral representations. If Λ is an R -order, where R is a Dedekind domain, we place two Λ -lattices M and N in the same genus if they are locally isomorphic (that is, $M_P \cong N_P$ as Λ_P -lattices, for each P). Only finitely many P 's are of significance in this definition. Many properties of a Λ -lattice M , especially those relating to decomposability and direct sums, depend only on the genus of M , rather than the Λ -isomorphism class of M . This circle of ideas leads naturally to the concept of the locally free class group $\text{Cl } \Lambda$ of an order Λ . We interpret this class group in terms of idèles, and postpone until Chapter 11 the deeper study of this class group.

In §32 we prove Swan's celebrated theorem that every projective $\mathbb{Z}G$ -lattice is in the same genus as a free $\mathbb{Z}G$ -lattice.

We call an order Λ of *finite representation type* if the number of isomorphism classes of indecomposable Λ -lattices is finite. In §33, we begin by proving Jones' Theorem, which tells us that the question, as to whether Λ has finite representation type, can always be reduced to the case in which the ground ring R is a complete d.v.r. We then sketch a proof of the Jacobinski, Drozd-Roiter Theorem which gives necessary and sufficient conditions that a commutative order have finite representation type.

Section 34 is devoted to calculations of indecomposable representations of various groups and orders. Here we use much of the machinery developed in §§25, 28. The remaining sections of this chapter are of interest in themselves, but they will be used infrequently in later chapters. In §35 we prove the beautiful theorem of Dade-Taussky-Zassenhaus, using a surprising result due to Fröhlich. Section 36 is devoted to a discussion as to whether the K-S-A Theorem holds for Λ -lattices, where Λ is an order over a non-complete d.v.r. As we shall see, this is the case in certain very special situations, but counterexamples are known in many other cases.

Finally, §37 contains an introduction to the theory of Bass and Gorenstein orders. This theory may be viewed as a generalization of the theory of hereditary orders. Since every integral group ring is a Gorenstein order (=weakly self-injective order), the ideas in §37 are sometimes helpful. They form the cornerstone of the Drozd-Roiter approach to the problem of finite representation type.

§30. LOCAL THEORY

The local theory deals with representations of groups and orders over some commutative local ring R . Usually, R will be a d.v.r., and in many cases we impose the further requirement that R be complete. A particularly important local result is that the K-S-A Theorem holds for Λ -lattices, where Λ is an

R -order, with R complete. This fact, as well as other basic facts proved in the introductory sections §§5–6, is reviewed at the beginning of this section.

In §30A, we prove Maranda's Theorems and related results. Let Λ be an R -order, where R is a d.v.r. with maximal ideal P and residue class field $\bar{R} = R/P$. (This represents a change from the notation in Chapter 2.) The first main result is that a Λ -lattice M is projective if and only if M/PM is $(\Lambda/P\Lambda)$ -projective. Furthermore, if M and N are projective Λ -lattices, then $M \cong N$ if and only if $M/PM \cong N/PN$. Maranda's Theorems generalize these facts, and show that an arbitrary Λ -lattice is determined, as to isomorphism, decomposability, etc., by its behavior mod P^k for some sufficiently large k , depending on Λ but not on M . This result on decomposability may be viewed as a generalization of Hensel's Lemma (see Exercise 6.11), or of the Theorem on Lifting Idempotents 6.7.

Section 30B takes up the technique of ground ring extension. If $R \subseteq S$ are complete d.v.r.'s, with quotient fields K and L , respectively, then each Λ -lattice M gives to an $S\Lambda$ -lattice SM . We prove the Reiner-Zassenhaus Theorem, which says that SM determines M up to isomorphism. We next investigate the decomposition of SM into indecomposable $S\Lambda$ -modules, and show how this is related to the decomposition of

$$\bar{S} \otimes_{\bar{R}} \{E(M)/\text{rad } E(M)\},$$

where \bar{R} and \bar{S} are the residue class fields of R and S , respectively, and $E(M) = \text{End } M$. This enables us to decide whether the Λ -lattice M is absolutely indecomposable. It also implies that for each M , we can find an S such that SM is a direct sum of absolutely indecomposable lattices. Indeed, we can find an S which works for all M 's simultaneously, provided we permit $\dim_K L$ to be infinite.

In §30C, we give a brief introduction to the theory of representations of orders by matrices with entries in R/P^k . This theory is rather undeveloped, and is surprisingly difficult.

We fix the following notation for the entire section:

$$(30.1) \quad \left\{ \begin{array}{l} R = \text{commutative local noetherian ring} \\ P = \text{unique maximal ideal of } R \\ \bar{R} = R/P = \text{residue class field of } R \\ \Lambda = R\text{-algebra, f.g. as } R\text{-module} \\ \mathcal{P}(\Lambda) = \text{set of f.g. projective left } \Lambda\text{-modules} \\ \hat{R} = P\text{-adic completion of } R, \quad \hat{\Lambda} = \hat{R} \otimes_R \Lambda \end{array} \right.$$

In most of the main results in §30, the ring R is assumed to be a d.v.r. (discrete valuation ring), with prime element π and quotient field K . However, we shall first give a review of basic material in the more general setting (30.1), and then afterward shall restrict our attention to the case where R is a d.v.r.

In §§5–6 we have already developed some of the basic machinery needed to study representations of groups and orders over a local ring R . For convenience, we list here some of the major earlier results. At the end of the listing, we shall give cross-references to where these results are established in §§5–6. Most of the results will be vital for this section, and were also used extensively in §§17–18 of Chapter 2.

(30.2) Nakayama's Lemma. *Let M be a f.g. R -module, with R as in (30.1). Let L be an R -submodule of M such that $L+PM=M$. Then $L=M$.*

(30.3) Proposition. *We set $\bar{\Lambda}=\Lambda/P\Lambda$, a f.d. \bar{R} -algebra. Then*

- (i) $(\text{rad } \Lambda)^k \subseteq P\Lambda \subseteq \text{rad } \Lambda$ for some $k \geq 1$.
- (ii) $\Lambda/\text{rad } \Lambda \cong \bar{\Lambda}/\text{rad } \bar{\Lambda} = \text{semisimple artinian ring}$.
- (iii) $\hat{\Lambda}/\text{rad } \hat{\Lambda} \cong \Lambda/\text{rad } \Lambda$, $\text{rad } \hat{\Lambda} = \hat{R} \otimes_R \text{rad } \Lambda$, and $\text{rad } \Lambda = \Lambda \cap \text{rad } \hat{\Lambda}$.

(30.4) Theorem. *Let R be a complete local ring, and let $\bar{\Lambda}=\Lambda/N$, where N is any two-sided ideal of Λ contained in $\text{rad } \Lambda$. Then the following statements hold:*

- (i) *Each decomposition $\Lambda=\bigoplus_{i=1}^n \Lambda e_i$ into indecomposable left ideals generated by idempotents $\{e_i\}$, yields a corresponding decomposition $\bar{\Lambda}=\bigoplus_{i=1}^n \bar{\Lambda} e_i$ into indecomposable left ideals. Conversely, every such decomposition of $\bar{\Lambda}$ arises in this way from a decomposition of Λ .*
- (ii) *In (i), $\bar{\Lambda} e_i$ is the projective cover of $\bar{\Lambda} e_i$ for each i , and $\Lambda e_i \cong \Lambda e_j$ if and only if $\bar{\Lambda} e_i \cong \bar{\Lambda} e_j$.*

(30.5) Proposition. *Let R be a complete local ring, and let M be a f.g. left Λ -module. Then M is indecomposable if and only if $\text{End}_\Lambda M$ is a local ring.*

(30.6) K-S-A Theorem (Krull-Schmidt-Azumaya). *Let R be a complete local ring, and let M be a f.g. left Λ -module. Then M is expressible as a finite direct sum of indecomposable Λ -modules, with the summands unique up to isomorphism and order of occurrence.*

(30.7) Corollary. *Keep the above hypotheses, and let L , M and N be f.g. left Λ -modules. Then for each $k \geq 1$,*

$$L^{(k)} \cong M^{(k)} \Rightarrow L \cong M, \quad L \oplus M \cong L \oplus N \Rightarrow M \cong N.$$

(30.8) Proposition. *For $M, N \in \mathcal{P}(\Lambda)$, we have*

$$M \cong N \Leftrightarrow M/PM \cong N/PN.$$

(30.9) Proposition. Let R be a d.v.r. with prime element π and field of quotients K , and let \hat{R} , \hat{K} , etc., denote P -adic completions. Let M be a f.g. R -module. Then:

(i) The map $M \rightarrow \hat{M}$ is an embedding, and M is dense in \hat{M} in the P -adic topology of \hat{M} .

(ii) $M/P^k M \cong \hat{M}/P^k \hat{M}$ for $k \geq 1$.

(iii) For each $M \in \mathcal{P}(R)$ we have $M = KM \cap \hat{M}$, where we write KM for $K \otimes_R M$, after identifying M with $1 \otimes M$.

(iv) Let V be a K -space, \hat{V} its completion. There is a bijection $M \leftrightarrow T$, given by

$$M = V \cap T, \quad T = \hat{M},$$

between the set of full R -lattices M in V and the set of full R -lattices T in \hat{V} .

(30.10) Corollary. Let R be a d.v.r. with quotient field K , and let Λ be an R -order in a f.d. K -algebra A . Let M be a left Λ -lattice, and let \hat{M} , $\hat{\Lambda}$, etc., denote P -adic completions. Then:

(i) The map $M \rightarrow \hat{M}$ embeds M into the $\hat{\Lambda}$ -lattice \hat{M} , and $M = KM \cap \hat{M}$.

(ii) Let V be a f.g. A -module, $\hat{V} = \hat{K} \otimes_K V$ its P -adic completion. There is a bijection $M \leftrightarrow T$, given by

$$M = V \cap T, \quad T = \hat{M},$$

between the set of full Λ -lattices M in V and the set of full $\hat{\Lambda}$ -lattices T in \hat{V} .

Cross-references. For (30.2), see (5.7). For (30.3), see (5.22) and Exercise 5.7. For (30.4), see (6.8) and (6.26ii). Prop. 30.5 is given in (6.10), and (30.6) is deduced from it in (6.12). Cor. 30.7 follows easily; see (6.15) and Exercise 6.1. For (30.8), see (6.6) or (6.17iv). Swan [60] gives a special case of this result. Proposition 30.9 is given in (4.21) and §4D. Finally, (30.10) is an immediate consequence of (30.9). See §23 for the definitions of “ Λ -lattice”, “full”, etc. The result (30.10) was pointed out by Heller [61a].

§30A. Reduction mod P^k

We now proceed toward the Maranda Theorems. As usual, the notation $M|N$ means that M is isomorphic to a direct summand of N . We begin with:

(30.11) Theorem (Reiner [56]). Let R be a d.v.r. with prime element π , and let Λ be an R -order, and M a f.g. left Λ -lattice. Put $\bar{R} = R/P$, $\bar{\Lambda} = \Lambda/P\Lambda$,

$\bar{M} = M/PM$. Then

$$M \text{ is } \Lambda\text{-projective} \Leftrightarrow \bar{M} \text{ is } \bar{\Lambda}\text{-projective}.$$

Proof. If $M|\Lambda^{(k)}$ then $\bar{M}|\bar{\Lambda}^{(k)}$; hence if M is Λ -projective, it is clear that \bar{M} is $\bar{\Lambda}$ -projective. We give two proofs of the converse.

(I) Assume \bar{M} is $\bar{\Lambda}$ -projective, say $\bar{M}|F$ where $F=\Lambda^{(k)}$. Consider the commutative diagram

$$\begin{array}{ccccccc} 0 & \longrightarrow & F & \xrightarrow{\pi} & F & \longrightarrow & \bar{F} \longrightarrow 0 \\ & & & \downarrow \theta & & & \downarrow \bar{\theta} \\ 0 & \longrightarrow & M & \xrightarrow{\pi} & M & \longrightarrow & \bar{M} \longrightarrow 0, \end{array}$$

where $\xrightarrow{\pi}$ means multiplication by π , and the map $\bar{\theta}$ is surjective. The rows are exact, since F and M are R -torsionfree. Now F is Λ -free, so the surjection $\bar{\theta}$ lifts to a Λ -homomorphism $\theta: F \rightarrow M$. Then $\theta(F) + \pi M = M$, so $\theta(F) = M$ by Nakayama's Lemma 30.2. Let $N = \ker \theta$; then we obtain a commutative diagram

$$\begin{array}{ccccccc} 0 & \longrightarrow & N & \xrightarrow{\rho} & F & \xrightarrow{\theta} & M \longrightarrow 0 \\ & & \downarrow & & \downarrow & & \downarrow \\ 0 & \longrightarrow & \bar{N} & \xrightarrow{\bar{\rho}} & \bar{F} & \xrightarrow{\bar{\theta}} & \bar{M} \longrightarrow 0, \end{array}$$

in which ρ is the inclusion map, and the top row is exact. Since the top row is R -split, applying $\bar{R} \otimes_R *$ to it yields the exactness of the bottom row (see Exercise 30.1).

Now \bar{M} is $\bar{\Lambda}$ -projective, so we can find a map $\psi: \bar{F} \rightarrow \bar{N}$ such that $\psi \bar{\rho} = 1$ on \bar{N} . Lifting ψ to a Λ -map $\psi': F \rightarrow N$, we obtain a commutative diagram

$$\begin{array}{ccc} N & \xrightleftharpoons[\psi']{\rho} & F \\ \downarrow & & \downarrow \\ \bar{N} & \xrightleftharpoons[\psi]{\bar{\rho}} & \bar{F} \end{array}$$

with $\psi' \rho \in \text{End}_\Lambda(N)$. Since $\psi' \rho \equiv 1 \pmod{P}$, it follows from Exercise 5.8 that $\psi' \rho \in \text{Aut}_\Lambda(N)$, whence the inclusion ρ is split by the map $(\psi' \rho)^{-1} \psi'$. But then M is a direct summand of F , so M is Λ -projective.

(II) Assume \bar{M} is $\bar{\Lambda}$ -projective, say $\bar{M}|\bar{\Lambda}^{(k)}$. Since

$$0 \rightarrow \Lambda \xrightarrow{\pi} \Lambda \rightarrow \bar{\Lambda} \rightarrow 0$$

is exact, we obtain

$$\mathrm{Ext}_{\Lambda}^2(\bar{\Lambda}, *) = 0$$

by §8A, whence also $\mathrm{Ext}_{\Lambda}^2(\bar{M}, *) = 0$ by (8.4iv). Now let X be any f.g. left Λ -module, so $\mathrm{Ext}_{\Lambda}^1(M, X)$ is f.g./ R . From the Λ -exact sequence $0 \rightarrow M \xrightarrow{\pi} M \rightarrow \bar{M} \rightarrow 0$ we obtain an exact sequence

$$\mathrm{Ext}_{\Lambda}^1(M, X) \xrightarrow{\pi} \mathrm{Ext}_{\Lambda}^1(M, X) \rightarrow \mathrm{Ext}_{\Lambda}^2(\bar{M}, X)$$

(see (8.6)). Thus, multiplication by π is a surjective endomorphism of the f.g. R -module $\mathrm{Ext}_{\Lambda}^1(M, X)$, so this module must equal 0 by Nakayama's Lemma.

In particular, consider a surjection $F: \Lambda^{(n)} \rightarrow M$, and set $X = \ker f$. Then X is f.g./ Λ , and the exact sequence

$$0 \rightarrow X \rightarrow \Lambda^{(n)} \rightarrow M \rightarrow 0$$

is Λ -split because $\mathrm{Ext}_{\Lambda}^1(M, X) = 0$. Therefore $M|\Lambda^{(n)}$, so M is projective as claimed.

Nakayama [57, remarks at end of §3] proved the result for the special case of group rings. There is also a proof via binding homomorphisms in CR (77.1). For the case of group rings, the result also follows from (20.10).

The preceding result shows the close connection between a Λ -lattice M and the $\bar{\Lambda}$ -module \bar{M} , where bars denote reduction mod P . We saw further (in (30.8)) that for $M, N \in \mathcal{P}(\Lambda)$, $M \cong N$ if and only if $\bar{M} \cong \bar{N}$. We shall now discuss the Maranda Theorems, which establish analogous relations between M and $M/P^k M$, even when M is not Λ -projective. For these theorems, it will be necessary to restrict our attention to the case where R is a discrete valuation ring, and Λ is an R -order in a separable algebra. We fix the following notation, to be used for the remainder of this subsection unless otherwise specified:

$$(30.12) \quad \begin{cases} R = \text{d.v.r. with prime element } \pi, P = \pi R \\ K = \text{quotient field of } R \\ A = \text{f.d. separable } K\text{-algebra} \\ \Lambda = R\text{-order in } A \\ \hat{R}, \hat{K}, \hat{A}, \hat{\Lambda}, \text{ etc., denote } P\text{-adic completions} \end{cases}$$

The reader should keep in mind the case where $\Lambda = RG$, $A = KG$, with G a finite group such that $\text{char } K \nmid |G|$. As shown in (25.12), we then have

$$|G| \cdot \text{Ext}_{\Lambda}^1(M, N) = 0 \text{ for all } \Lambda\text{-lattices } M \text{ and } N.$$

For the general case where A is any separable K -algebra, we proved in (29.5) that there exists a nonzero ideal c of R such that

$$c \cdot \text{Ext}_{\Lambda}^1(M, N) = 0 \text{ for all } \Lambda\text{-lattices } M \text{ and } N.$$

Indeed, by (26.5) the order Λ is contained in some maximal R -order Λ' in A . We may then choose a nonzero $\alpha \in R$ such that $\alpha\Lambda' \subseteq \Lambda$, and then by (29.4) we obtain

$$\alpha \cdot \text{Ext}_{\Lambda}^1(M, N) = 0 \text{ for all } \Lambda\text{-lattices } M \text{ and } N.$$

The above discussion shows that under hypotheses (30.12), there exists a nonnegative integer k_0 such that

$$(30.13) \quad \pi^{k_0} \text{Ext}_{\Lambda}^1(M, N) = 0 \text{ for all } \Lambda\text{-lattices } M \text{ and } N.$$

Further, when $\Lambda = RG$ we may choose k_0 so that $\pi^{k_0} \parallel |G|$ in R , that is, k_0 is the largest k such that $|G| \in \pi^k R$. In particular, we pick $k_0 = 0$ whenever $|G|$ is a unit of R .

Keeping the above notation, we prove a result due to Maranda, as generalized by D. G. Higman [60]:

(30.14) Theorem (Maranda [53]). *Let M and N be Λ -lattices, and let $k \geq 0$. Define $\Lambda_k = \Lambda/\pi^k \Lambda$, $M_k = M/\pi^k M$, and so on; thus, M_k is an R_k -free Λ_k -module. Then:*

- (i) *If $M \cong N$ as Λ -modules, then $M_k \cong N_k$ as Λ_k -modules for each $k \geq 0$.*
- (ii) *If $M_k \cong N_k$ for some $k \geq k_0 + 1$, then $M \cong N$.*

Proof. Assertion (i) is obvious. For (ii), let k be fixed, $k \geq k_0 + 1$, and assume that $\varphi: M_k \cong N_k$ is a Λ_k -isomorphism. In the diagram

$$\begin{array}{ccc} M & & N \\ \downarrow & & \downarrow \\ M_k & \xrightarrow{\varphi} & N_k \end{array}$$

we can lift φ to some $f \in \text{Hom}_R(M, N)$, since M is R -projective. Likewise, we can lift φ^{-1} to some $g \in \text{Hom}_R(N, M)$. Then $gf \in \text{End}_R(M)$ is such that

$gf \equiv 1 \pmod{\pi^k}$, that is,

$$(gf)(m) - m \in \pi^k M \text{ for all } m \in M.$$

Since f lifts φ , we have

$$(xf - fx)M \subseteq \pi^k N \text{ for all } x \in \Lambda.$$

We may therefore define a map $F_x \in \text{Hom}_R(M, N)$ for each $x \in \Lambda$, by setting

$$xf - fx = \pi^k F_x, \quad x \in \Lambda.$$

Each F_x is well defined since N is R -torsionfree. We obtain at once

$$\pi^k(F_{xy} - xF_y - F_xy) = 0 \text{ for all } x, y \in \Lambda,$$

and we may cancel the factor π^k since $\text{Hom}_R(M, N)$ is R -torsionfree. But then the map $F \in \text{Hom}_R(\Lambda, \text{Hom}_R(M, N))$, defined by $x \mapsto F_x$, $x \in \Lambda$, is a derivation from Λ into $\text{Hom}_R(M, N)$ (see §25A). Thus F determines an element of $\text{Ext}_\Lambda^1(M, N)$. It follows from (30.13) that $\pi^{k_0} F$ is an inner derivation, that is, there exists an $h \in \text{Hom}_R(M, N)$ such that

$$\pi^{k_0} F_x = xh - hx, \quad x \in \Lambda.$$

Multiplying by π^{k_1} , where $k_1 = k - k_0 \geq 1$, we obtain

$$xf - fx = \pi^{k_1}(xh - hx), \quad x \in \Lambda.$$

Therefore $f - \pi^{k_1} h$ commutes with each $x \in \Lambda$, and is thus an element of $\text{Hom}_\Lambda(M, N)$. Since f is an R -isomorphism of M onto N , so is $f - \pi^{k_1} h$ by Exercise 5.8. Thus $f - \pi^{k_1} h$ is a Λ -isomorphism of M onto N , and the theorem is proved.

(30.15) Remarks. (i) If one drops the hypothesis that A be separable, one obtains the following modification of (30.14), due to Reiner [79a]:

$$M_k \cong N_k \text{ for each } k \geq 1 \Rightarrow M \cong N.$$

To prove this, consider the R -module \mathfrak{D} of all derivations from Λ into $\text{Hom}_R(M, N)$; clearly \mathfrak{D} is f.g./ R . For each $k \geq 1$, let φ_k be a Λ_k -isomorphism of M_k onto N_k . As in the preceding proof, we can find an R -isomorphism $\theta_k: M \cong N$ such that

$$(\theta_k x - x\theta_k)M \subseteq \pi^k N \text{ for all } x \in \Lambda.$$

Set

$$\theta_k x - x\theta_k = \pi^k D_k(x), \quad x \in \Lambda, \quad k \geq 1.$$

Then $D_k \in \mathfrak{D}$ for each k .

Now let \mathfrak{D}_0 be the R -submodule of \mathfrak{D} generated by D_1, D_2, \dots . Since \mathfrak{D} is f.g./ R and R is noetherian, it follows that \mathfrak{D}_0 is also f.g./ R . Hence there exists a positive integer k such that

$$D_k = \alpha_1 D_1 + \cdots + \alpha_{k-1} D_{k-1} \text{ for some } \alpha_1, \dots, \alpha_{k-1} \in R.$$

Then

$$\pi^{-k}(\theta_k x - x\theta_k) = \sum_{i=1}^{k-1} \alpha_i \pi^{-i} (\theta_i x - x\theta_i) \text{ for } x \in \Lambda.$$

Setting

$$\theta' = \theta_k - \sum_{i=1}^{k-1} \alpha_i \pi^{k-i} \theta_i,$$

we obtain $\theta'x = x\theta'$ for all $x \in \Lambda$. Thus θ' is a Λ -homomorphism from M into N . But $\theta' \equiv \theta_k \pmod{\pi}$, so θ' is an R -isomorphism $M \cong N$ by Exercise 5.8. Hence $M \cong N$ as Λ -modules, as claimed.

(ii) Keep the hypotheses (30.12), and assume further that the field \bar{R} is finite. Then for $k = k_0 + 1$, the ring R_k is also finite, and so there are only a finite number of Λ_k -modules of given R_k -rank. Hence by (30.14), we obtain the important result that there are only a finite number of isomorphism classes of Λ -lattices of given R -rank. (See also (24.7).)

The following frequently used result is closely related to Maranda's Theorem:

(30.16) Theorem. *Let R be a d.v.r. with quotient field K , and let bars denote reduction mod π . Let G be a finite group such that $|G|$ is invertible in R , and let M and N be RG -lattices. Then M and N are projective RG -lattices, and*

$$KM \cong KN \Leftrightarrow M \cong N \Leftrightarrow \bar{M} \cong \bar{N}.$$

Proof. The second equivalence follows from Maranda's Theorem, since by (25.12) we may choose $k_0 = 0$ in this case. However, it is not necessary to use Maranda's Theorem for the proof, and instead we may proceed as follows. The hypothesis implies that $\bar{R}G$ is a semisimple \bar{R} -algebra. If $KM \cong KN$, then \bar{M} and \bar{N} have the same composition factors (see (16.16)), and therefore

$\overline{M} \cong \overline{N}$. Further, \overline{M} is $\overline{R}G$ -projective, whence M is RG -projective by (30.11). But then $\overline{M} \cong \overline{N}$ implies $M \cong N$ by (30.8). This completes the proof. (See also Exercises 18.4 and 19.3.)

Returning to the general case, we establish a fundamental relation between Λ -modules and their completions:

(30.17) Proposition. *Let R be a d.v.r. with prime element π , and let Λ be any R -algebra, f.g./ R as module. Let M and N be f.g. left Λ -modules, and let $\hat{\Lambda}$, \hat{M} , etc., denote P -adic completions. Then*

$$M \cong N \text{ as } \Lambda\text{-modules} \Leftrightarrow \hat{M} \cong \hat{N} \text{ as } \hat{\Lambda}\text{-modules}.$$

Proof. In the special case where Λ is an R -order in a separable K -algebra, and M , N are Λ -lattices, the result follows from Maranda's Theorem. Choose $k = k_0 + 1$, and use the fact (see (30.9)) that

$$M/P^k M \cong \hat{M}/P^k \hat{M}.$$

Then, applying Maranda's Theorem to both Λ and $\hat{\Lambda}$, we obtain

$$M \cong N \Leftrightarrow M/P^k M \cong N/P^k N \Leftrightarrow \hat{M}/P^k \hat{M} \cong \hat{N}/P^k \hat{N} \Leftrightarrow \hat{M} \cong \hat{N}.$$

In the general case where Λ is an R -algebra, we have (by (2.38))

$$\hat{R} \otimes_R \text{Hom}_\Lambda(M, N) \cong \text{Hom}_{\hat{\Lambda}}(\hat{M}, \hat{N}),$$

and $\text{Hom}_\Lambda(M, N)$ is dense in $\text{Hom}_{\hat{\Lambda}}(\hat{M}, \hat{N})$ in the P -adic topology. Now let $f_1 : \hat{M} \cong \hat{N}$ be a $\hat{\Lambda}$ -isomorphism, and let $g_1 = (f_1)^{-1}$. We may choose $f \in \text{Hom}_\Lambda(M, N)$ such that $f \equiv f_1 \pmod{\pi}$, that is, $(f - f_1)(M) \subseteq \pi \hat{N}$. Likewise, we may choose $g \in \text{Hom}_\Lambda(N, M)$ with $g \equiv g_1 \pmod{\pi}$. Then $gf \in \text{End}_\Lambda(M)$ satisfies $gf \equiv 1 \pmod{\pi}$, so

$$(gf)(m) - m \in \pi \hat{M} \text{ for all } m \in M.$$

But $M \cap \pi \hat{M} = \pi M$ by (30.9), whence $M = (gf)M + \pi M$. Thus $gf \in \text{Aut}_\Lambda(M)$. Likewise $fg \in \text{Aut}_\Lambda(N)$, so $f : M \cong N$ as desired.

Let us continue our investigation of the connections between Λ -modules and $\hat{\Lambda}$ -modules. We may ask whether indecomposable Λ -lattices yield indecomposable $\hat{\Lambda}$ -lattices, and also whether every $\hat{\Lambda}$ -lattice is the completion of some Λ -lattice. Simple examples show that these questions may have a negative answer. For instance, let R be a d.v.r., and let $f(X) \in R[X]$ be a monic irreducible polynomial, such that in $\hat{R}[X]$ there is a factorization $f(X) = \prod_i f_i(X)$ into at least two distinct irreducible factors. Let

$\Lambda = R[X]/(f(X))$; then Λ is an R -order in the field $K[X]/(f(X))$, and

$$\hat{\Lambda} = \hat{R}[X]/(f(X)) = \hat{R}[X]/(\prod f_i(X)).$$

However, the ring $\hat{R}[X]/(f_i(X))$ is a $\hat{\Lambda}$ -lattice which is not the completion of any Λ -lattice, as is clear from a consideration of ranks. Furthermore, if we choose $f(X)$ so that for $i \neq j$, the ideal $(f_i(X), f_j(X))$ of $\hat{R}[X]$ coincides with $\hat{R}[X]$, then

$$\hat{\Lambda} \cong \coprod R[X]/(f_i(X)).$$

Thus, $\hat{\Lambda}$ is decomposable even though Λ is indecomposable.

There is, however, one important case where such behavior cannot occur. We shall prove:

(30.18) Theorem (Heller [61a]). *Let R be a d.v.r. with quotient field K , and let Λ be an R -order in a semisimple K -algebra. Let $\hat{\Lambda}$, \hat{A} , etc., denote P -adic completions. Suppose that for each simple left A -module S , the \hat{A} -module \hat{S} is also simple*. Then:*

- (i) *Every $\hat{\Lambda}$ -lattice is isomorphic to the completion of a Λ -lattice.*
- (ii) *A Λ -lattice M is indecomposable if and only if its completion \hat{M} is indecomposable as $\hat{\Lambda}$ -lattice.*
- (iii) *The K-S-A Theorem is valid for Λ -lattices.*

Proof. Since $A = \bigoplus S_i$ is a direct sum of simple A -modules S_i , we have $\hat{A} = \bigoplus \hat{S}_i$, a direct sum of simple \hat{A} -modules; thus \hat{A} is a semisimple \hat{K} -algebra. Each f.g. left \hat{A} -module is then isomorphic to a direct sum $\coprod \hat{S}_i^{(n_i)}$, hence is isomorphic to the completion of some A -module (namely $\coprod S_i^{(n_i)}$).

Now let T be any left $\hat{\Lambda}$ -lattice, and form the \hat{A} -module $\hat{K}T$. Then $\hat{K}T \cong \hat{K}V$ for some f.g. A -module V , where

$$\hat{K}T = \hat{K} \otimes_{\hat{R}} T, \quad \hat{K}V = \hat{K} \otimes_K V.$$

Replacing T by its isomorphic image in $\hat{K}V$, we may assume that $\hat{K}T = \hat{K}V$, so T is a full $\hat{\Lambda}$ -lattice in $\hat{K}V$. If we set $M = V \cap T$, then by (30.10) M is a full Λ -lattice in V such that $\hat{M} = T$. Thus, the hypotheses imply that every $\hat{\Lambda}$ -lattice is the completion of a Λ -lattice.

Suppose now that M is an indecomposable Λ -lattice, and that $\hat{M} = T_1 \oplus T_2$, where the $\{T_i\}$ are nonzero $\hat{\Lambda}$ -lattices. Then we may write $T_i = \hat{M}_i$ for some Λ -lattice M_i , $i = 1, 2$. Therefore $\hat{M} \cong \hat{M}_1 \oplus \hat{M}_2$, whence $M \cong M_1 \oplus M_2$ by (30.17). This is a contradiction, and establishes (ii).

*This hypothesis certainly holds whenever K is a splitting field for A (see (7.12)).

Finally, let M be an arbitrary Λ -lattice, and let $M = \coprod M_i$ with each M_i indecomposable. Then $\hat{M} = \coprod \hat{M}_i$ gives a decomposition of \hat{M} into indecomposable Λ -lattices $\{\hat{M}_i\}$. By the K-S-A Theorem, the $\{\hat{M}_i\}$ are uniquely determined up to isomorphism and order of occurrence. Hence the same holds true for the $\{M_i\}$ by (30.17), and the theorem is proved.

Let us give an illustration of Heller's Theorem. Let R be the localization of \mathbb{Z} at the prime p , and let G be a cyclic group of order p^n . Then (see Exercise 21.1):

$$\mathbb{Q}G \cong \coprod_{r=0}^n K_r, \text{ where } K_r = \mathbb{Q}[x]/(\Phi_{p^r}(x)),$$

and $\Phi_{p^r}(x)$ is the cyclotomic polynomial of order p^r and degree $\varphi(p^r)$. If $\hat{\mathbb{Q}}$ denotes the p -adic completion of \mathbb{Q} , then the proof of CR (21.13) shows that each $\Phi_{p^r}(x)$ is irreducible over $\hat{\mathbb{Q}}$. Hence

$$\hat{\mathbb{Q}}G \cong \coprod_{r=0}^n \hat{\mathbb{Q}} \otimes_{\mathbb{Q}} K_r, \quad \hat{\mathbb{Q}} \otimes K_r = \hat{\mathbb{Q}}[x]/(\Phi_{p^r}(x)),$$

so each simple $\mathbb{Q}G$ -module K_r yields a simple $\hat{\mathbb{Q}}G$ -module \hat{K}_r . By Heller's Theorem, we may conclude that every $\hat{\mathbb{Q}}G$ -lattice is the completion of an RG -lattice, and that indecomposability is preserved in passing to completions. Further, the K-S-A Theorem holds for RG -lattices.

For Jones' generalization of this result, and for further remarks about the K-S-A Theorem, see §36, especially (36.1).

Let us return to the situation in (30.14) where Λ is an R -order in a separable K -algebra. As we saw there, the isomorphism class of M is completely determined by the structure of $M \bmod \pi^{k_0+1}$. There are two further results of this nature, valid when R is assumed to be a complete d.v.r. The first result is due to Maranda [53]; here, we present Heller's [61a] simplification and strengthening of the result, as follows:

(30.19) Theorem. *Let Λ be an R -order in a separable K -algebra, where R is a complete d.v.r. Let $k_0 \geq 0$ be such that (30.13) holds, and let M be a Λ -lattice such that $M/\pi^k M$ is decomposable for some $k \geq k_0 + 1$. Then M is also decomposable.*

Proof. Put $M_k = M/\pi^k M$; since M_k is decomposable, there exists a nontrivial idempotent $\varphi \in \text{End}_{\Lambda} M_k$. As in the proof of (30.14), we can find a map $f \in \text{End}_{\Lambda} M$ such that f and φ coincide mod π^{k_1} , where $k_1 = k - k_0 \geq 1$. Then

$$(30.20) \quad (f^2 - f)M \subseteq \pi^{k_1} M \subseteq \pi M,$$

so we may write $f^2 - f = \pi f_1$ for some $f_1 \in \text{End}_{\Lambda} M$. Put

$$(30.21) \quad E = \text{End}_{\Lambda} M, \quad \bar{E} = E/\pi E,$$

and let bars denote images mod π . Then $\bar{f}^2 = \bar{f}$ in \bar{E} , and we claim that $\bar{f} \neq 0, 1$. Indeed, if $\bar{f} = 0$ then $f \in \pi E$, whence $f(M) \subseteq \pi M$; this implies that $\varphi(M_k) \subseteq \pi M_k$, and so

$$(30.22) \quad \varphi(M_k) = \varphi^2(M_k) = \varphi^3(M_k) = \cdots = 0,$$

a contradiction. Thus $\bar{f} \neq 0$; a similar argument (using $1 - \varphi$ in place of φ) shows that $\bar{f} \neq 1$.

We have thus obtained a non-trivial idempotent $\bar{f} \in \bar{E}$. Since R is complete by hypothesis, we can apply the Theorem on Lifting Idempotents (6.7) to find a non-trivial idempotent in E which lifts \bar{f} . But $E = \text{End}_\Lambda(M)$, so M must be decomposable, as claimed.

As in Remark 30.15i, we may drop the hypothesis that A be separable. We obtain (see Reiner [79a]): *Let Λ be any R -order, where R is a complete d.v.r., and let M be a Λ -lattice such that $M/\pi^k M$ is decomposable (as $(\Lambda/\pi^k \Lambda)$ -module) for each $k > 0$. Then M is also decomposable.*

Maranda [53] also established the following result (see CR (76.11) for a proof):

(30.23) Theorem. *Let Λ be an R -order in a separable K -algebra, where R is a complete d.v.r., and let k_0 be as in (30.13). Let $k > 2k_0$, and let $R_k = R/\pi^k R$, $\Lambda_k = \Lambda/\pi^k \Lambda$ and so on. Let M be a Λ -lattice such that M_k contains a Λ_k -sublattice X which is an R_k -direct summand of M_k . Then M contains a Λ -sublattice L which is an R -direct summand of M , and is such that L and X are isomorphic mod π^{k-k_0} .*

The Maranda Theorems reduce the problem of studying R -representations of an R -order Λ to the problem of studying the R_k -free Λ_k -modules, where $R_k = R/\pi^k R$ and k is sufficiently large. Unfortunately, in many cases this latter problem is at least as difficult as the original one. The case $k=1$ leads to the subject of modular representation theory, which is of course well developed. However, relatively little is known about the cases where $k > 1$, and so Maranda's Theorems have not turned out to be of great practical value in the study of integral representations over a local ring. For a discussion of known results when $k > 1$, see §30C.

(30.24) Notes. (1) Let R be a complete d.v.r. with prime element π , and let Λ, Λ' be R -orders in separable K -algebras. Then $\Lambda \cong \Lambda'$ as R -orders if and only if

$$\Lambda/\pi^k \Lambda \cong \Lambda'/\pi^k \Lambda' \text{ as } R\text{-algebras}$$

for some sufficiently large value of k . This result, due to D. G. Higman [59], follows from the type of reasoning used to prove (30.17). For further results of this nature, see D. G. Higman [60].

(2) A variant of Maranda's Theorem 30.14 is given in Nazarova-Roiter [67a].

§30B. Extension of the Ground Ring

Suppose first that R is an arbitrary Dedekind domain, contained in a larger Dedekind domain S . Given an R -order Λ , we may form the S -order $S \otimes_R \Lambda$, which we write as $S\Lambda$ after identifying Λ with its image $1 \otimes \Lambda$ in $S \otimes_R \Lambda$. Each Λ -lattice M determines an $S\Lambda$ -lattice $SM (= S \otimes_R M)$, whose isomorphism type is uniquely determined by that of M , since an isomorphism $f: M \cong N$ of Λ -lattices induces an $S\Lambda$ -isomorphism $1 \otimes f: S \otimes M \cong S \otimes N$. We shall consider here the converse question: does the isomorphism class of SM determine that of M ? We shall also study the decomposition of SM into indecomposable summands.

Let us begin with a simple example, where we choose $\Lambda = R$. If a and b are nonzero ideals in R , then $a \cong b$ as R -modules if and only if a and b lie in the same ideal class (see §4F). Further, $S \otimes_R a \cong Sa$, and $Sa \cong Sb$ if and only if the S -ideals Sa and Sb lie in the same ideal class of S . It may well happen that Sa and Sb lie in the same class, even though a and b do not. For example (see the proof of (23.18)), we can choose S so that *each* ideal a of R generates a principal ideal Sa of S . Thus, the isomorphism $Sa \cong Sb$ need not imply that $a \cong b$, in general. Even when R is a P.I.D., one can give examples of an R -order Λ , and Λ -lattices M and N , such that (for suitable S) $SM \cong SN$ as $S\Lambda$ -lattices, but M is not Λ -isomorphic to N (see Berman-Gudivok [62], Jacobinski [68a]).

This situation changes drastically when R and S are d.v.r.'s, which we shall assume from now on. Specifically, let R be the valuation ring of a discrete valuation v on K , let $P = \pi R$ be the maximal ideal of R , and \bar{R} its residue class field. Let L denote an extension field of K , where $\dim_K L$ may possibly be infinite, and suppose that the valuation v can be extended to a discrete valuation w on L . Let S be its valuation ring, P_1 the maximal ideal of S , and $\bar{S} = S/P_1$. We shall call the d.v.r. S an *extension* of the d.v.r. R in this case. Clearly

$$R = K \cap S, P = R \cap P_1,$$

and \bar{S} is an extension field of \bar{R} .

Our first result, due to Reiner-Zassenhaus [61], is as follows:

(30.25) Theorem. *Let R and S be d.v.r.'s, with S an extension of R . Let M and N be Λ -lattices, where Λ is an R -order in a f.d. K -algebra A . Then $M \cong N$ if and only if $S \otimes_R M \cong S \otimes_R N$ as $(S \otimes_R \Lambda)$ -lattices.*

Proof. Step 1. Assume to begin with that $\dim_K L$ is finite. The following argument is valid for the more general situation in which Λ is any R -algebra, f.g./ R as module, and where M and N are any f.g. left Λ -modules (not necessarily lattices).

Put

$$M_1 = S \otimes_R M, N_1 = S \otimes_R N,$$

and let \hat{R} , \hat{M} , $\hat{\Lambda}$ denote P -adic completions, and \hat{S} , \hat{M}_1 , etc., P_1 -adic completions. Then \hat{S} is a free \hat{R} -module of finite rank, since $\dim_K L$ is finite. Suppose that \hat{S} is \hat{R} -free on n generators. We have

$$\hat{M}_1 = \hat{S} \otimes_S M_1 \cong \hat{S} \otimes_R M \cong \hat{S} \otimes_{\hat{R}} (\hat{R} \otimes_R M) \cong \hat{S} \otimes_{\hat{R}} \hat{M},$$

so $\hat{M}_1 \cong \hat{M}^{(n)}$ as left $\hat{\Lambda}$ -modules. If $M_1 \cong N_1$, then $\hat{M}_1 \cong \hat{N}_1$, and so $\hat{M}^{(n)} \cong \hat{N}^{(n)}$ as $\hat{\Lambda}$ -modules. Therefore $\hat{M} \cong \hat{N}$ by (30.7), so $M \cong N$ by (30.17), and we have shown that $M \cong N$ if and only if $M_1 \cong N_1$.

Step 2. Assume now that M and N are Λ -lattices, where Λ is an R -order, and set $\bar{R} = R/P$, $\bar{S} = S/P_1$, so \bar{S} is an extension field of \bar{R} . We shall imitate the proof of the Noether-Deuring Theorem given in Exercises 6.4–6.6. We may write SM for $S \otimes_R M$, after the usual identification of M with $1 \otimes M$. If we assume that $SM \cong SN$, then M and N have the same R -rank, which we denote by n . Each element of $\text{Hom}_R(M, N)$ can then be represented by an $n \times n$ matrix over R . Let $\mathbf{X}_1, \dots, \mathbf{X}_r$ be an R -basis for $\text{Hom}_{\Lambda}(M, N)$. Since

$$S \otimes_R \text{Hom}_{\Lambda}(M, N) \cong \text{Hom}_{S\Lambda}(SM, SN),$$

these matrices $\{\mathbf{X}_i\}$ are also an S -basis for $\text{Hom}_{S\Lambda}(SM, SN)$. Define

$$f(t_1, \dots, t_r) = \det(t_1 \mathbf{X}_1 + \dots + t_r \mathbf{X}_r) \in R[t_1, \dots, t_r],$$

as in Exercise 6.4. Since $SM \cong SN$, there exist elements $\alpha_i \in S$ with $f(\alpha_1, \dots, \alpha_r)$ a unit in S . Let \bar{f} be the polynomial obtained from f by reducing each coefficient mod P . If $\alpha_i \in S$ maps onto $\bar{\alpha}_i \in \bar{S}$, the above discussion shows that

$$\bar{f}(\bar{\alpha}_1, \dots, \bar{\alpha}_r) \neq 0,$$

and therefore \bar{f} is not the zero polynomial in $\bar{R}[t_1, \dots, t_r]$. Clearly \bar{f} has degree at most n .

If $\text{card } \bar{R} > n$, there exist elements $\beta_1, \dots, \beta_r \in R$ such that $\bar{f}(\bar{\beta}_1, \dots, \bar{\beta}_n) \neq 0$, and then $\sum \beta_i \mathbf{X}_i$ is the desired Λ -isomorphism of M onto N . On the other hand, if $\text{card } \bar{R} \leq n$ we may choose a finite extension field K' of K , with a valuation ring R' containing R , such that the residue class field of R' has more than n elements (see Weiss [63, Prop. 3-2-12] or MO (5.8), for the case where R is a complete d.v.r.; for the general case, use the fact that passage to completions does not affect residue class fields.) We can then find elements $\gamma_i \in R'$ for which $f(\gamma_1, \dots, \gamma_r)$ is a unit in R' , and therefore $R' M \cong R' N$ as $R'\Lambda$ -lattices. But then $M \cong N$ as Λ -lattices by Step 1, completing the proof.

For the remainder of this subsection, we shall assume that R and S are complete d.v.r.'s, with S an extension of R . For each R -module M , the map $M \rightarrow S \otimes_R M$ is an embedding (see Exercise 8.2), and we always identify M with $1 \otimes M$, so $S \otimes_R M$ may be written as SM . Now let Λ be any R -algebra, f.g./ R as module, and let M be a f.g. left Λ -module. We wish to study the decomposition of the $S\Lambda$ -module SM into a direct sum of indecomposable submodules. The entire discussion depends on the relationship given in (6.3) between decompositions of a module and decompositions of its endomorphism ring. We follow the treatment in Reiner [66].

Given the f.g. left Λ -module M , set

$$(30.26) \quad E = E(M) = \text{End}_\Lambda M, \quad \tilde{E} = \tilde{E}(M) = E(M)/\text{rad } E(M).$$

Then E is an R -algebra, f.g./ R as module, and \tilde{E} is a f.d. semisimple R -algebra, by (5.22). View M as a bimodule ${}_A M_E$, with E acting on the right. By (6.3), each decomposition $M = \bigoplus M_i$ into indecomposable submodules gives rise to a decomposition $E = \bigoplus L_i$ into indecomposable left ideals. If $\pi_i: M \rightarrow M_i$ is the idempotent in E given by the projection of M onto its i -th summand M_i , then again by (6.3) we have (for each i)

$$M_i = M\pi_i = ML_i, \quad L_i = E\pi_i,$$

$$\text{End}_\Lambda M_i \cong \text{End}_E L_i \cong \pi_i E \pi_i.$$

Further, $M_i \cong M_j$ if and only if $L_i \cong L_j$.

On the other hand, let J be any two-sided ideal of E contained in $\text{rad } E$, and let $E' = E/J$, $L'_i = \text{image of } L_i$ in E' . By (6.17) the decomposition $E = \bigoplus L_i$ corresponds to a decomposition $E' = \bigoplus L'_i$ into indecomposable left ideals L'_i of E' , with $L_i \cong L_j$ if and only if $L'_i \cong L'_j$. Further, since

$$E/\text{rad } E \cong E'/\text{rad } E',$$

it follows readily from (5.14) that for each i ,

$$\tilde{E}(L_i) \cong \tilde{E}(L'_i),$$

where $\tilde{E}(L_i) = \text{End}_E(L_i)/\text{rad End}_E(L_i)$, and $\tilde{E}(L'_i)$ is defined analogously.

We shall apply this machinery to the $S\Lambda$ -module SM , rather than to M itself, in order to prove the following basic result:

(30.27) Theorem. *Let R and S be complete d.v.r.'s, with S an extension of R , and let Λ be an R -algebra, f.g./ R as module. For each f.g. left Λ -module M , define $\tilde{E}(M)$ by (30.26), and form the \bar{S} -algebra*

$$\bar{S} \otimes_{\bar{R}} E(M).$$

Then:

- (i) *Each decomposition of the $S\Lambda$ -module $SM = \bigoplus N_j$ as a direct sum of indecomposable submodules corresponds to a decomposition*

$$\bar{S} \otimes_{\bar{R}} E(M) = \bigoplus L_j$$

into indecomposable left ideals.

- (ii) *Further, $N_i \cong N_j$ if and only if $L_i \cong L_j$. For each i , we have*

$$\tilde{E}(N_j) \cong \tilde{E}(L_j).$$

- (iii) *In particular, if $\tilde{E}(M) \cong \bar{R}$ then SM is indecomposable for every S , and $\tilde{E}(SM) \cong \bar{S}$.*

Proof. We have

$$E(SM) = \text{End}_{S\Lambda}(SM) \cong S \otimes_R E(M)$$

by (2.38). We choose

$$J = P_1 E(SM) + S \otimes \text{rad } E, \text{ where } E = E(M).$$

Then J is a two-sided ideal of $E(SM)$ contained in $\text{rad } E(SM)$, so $E(SM)$ decomposes into indecomposable left ideals in the same way as the factor ring $E(SM)/J$. But

$$E(SM)/J \cong (S \otimes_R E(M))/J \cong \bar{S} \otimes_{\bar{R}} \tilde{E}(M).$$

Assertions (i)–(iii) are then immediate consequences of the discussion preceding the theorem.

In (6.10) we showed that the Λ -module M is indecomposable if and only if $E(M)$ is a local ring, or equivalently, if and only if $\tilde{E}(M)$ is a division algebra over \bar{R} . We have just seen that if M is an indecomposable Λ -module for which $\tilde{E}(M) = \bar{R}$, then M remains indecomposable under ground ring extension; that is, $S \otimes_R M$ is an indecomposable $(S \otimes_R \Lambda)$ -module for each complete d.v.r. S which is an extension of R . Let us make the following definition:

(30.28) Definition. Let R be a complete d.v.r., and let Λ be any R -algebra f.g./ R as module. An indecomposable f.g. left Λ -module M is called *absolutely indecomposable* if SM is an indecomposable $S\Lambda$ -module, for each complete d.v.r. S which is an extension of R .

We have thus shown that M is absolutely indecomposable whenever $\tilde{E}(M) \cong \bar{R}$. The reader should compare this fact with (3.43), which is in fact a special case of the theorem above. It may well happen, however, that M is absolutely indecomposable even when $\tilde{E}(M) \neq \bar{R}$. This phenomenon is related to questions of inseparability (see (30.34) below), and to bypass this difficulty let us restrict our attention to the case where the field \bar{R} is perfect. (This is the situation which arises most frequently in practice, since \bar{R} is usually a finite field. See §19C, for example, where these results are used to prove indecomposability of induced modules in certain situations.)

We are now ready to prove:

(30.29) Theorem. *Let \bar{R} be a perfect field, and let M be a f.g. indecomposable Λ -module. Then M is absolutely indecomposable if and only if $\tilde{E}(M) \cong \bar{R}$.*

Proof. We need only show that if $\tilde{E}(M) \neq \bar{R}$, then SM is decomposable for some choice of S . Now $\tilde{E}(M)$ is a division algebra whose center contains \bar{R} , and thus $\tilde{E}(M)$ is a separable \bar{R} -algebra, because \bar{R} is perfect (see §7A). We can therefore find a finite extension field F of \bar{R} such that $F \otimes_{\bar{R}} \tilde{E}(M)$ is a split semisimple F -algebra, by (7.2). But any such algebra has a nontrivial decomposition into simple left ideals, except when the algebra coincides with F itself. This latter case cannot arise because $\tilde{E}(M) \supset \bar{R}$. Thus, as soon as we find a complete d.v.r. S for which $\bar{S} = F$, then SM is decomposable by (30.27), and the theorem is proved.

To complete the proof, we need only make use of the following result, which holds whether or not \bar{R} is perfect:

(30.30) Proposition. *Let R be a complete d.v.r. with quotient field K and residue class field \bar{R} , and let K' be an algebraic closure of K . Then there is a one-to-one inclusion-preserving correspondence $L \leftrightarrow F$ between the set of fields L such that*

$$K \subseteq L \subseteq K', \quad L = \text{finite unramified extension of } K,$$

and the set of fields F which are finite separable over \bar{R} . If S is the valuation ring in L obtained by extending the valuation from K to L , then S is a complete d.v.r. and the residue class field of S equals F .

For a proof, see Weiss [63, Th. 3-2-11] or Serre [62, Ch. III, §5]. If π denotes a prime element of R , then the condition that L be unramified over K means that π is also a prime element of S , and that \bar{S} is separable over \bar{R} (this latter condition holds automatically when \bar{R} is perfect). For further discussion of ramification, see §4B.

Let us record an important consequence of the above reasoning, already used in §19.

(30.31) Corollary. *Let \bar{R} be a perfect field, and let M be any f.g. left Λ -module. Then there exists a complete d.v.r. S , whose quotient field L is a finite unramified extension of K , such that $SM = \bigoplus N_i$, where each N_i is an absolutely indecomposable $S\Lambda$ -module, and where $\tilde{E}(N_i) \cong \bar{S}$ for each i .*

Proof. The \bar{R} -algebra $\tilde{E}(M)$ is separable over \bar{R} , so by (7.2) and (30.30) we can find S , as in the statement of (30.31), for which $\bar{S} \otimes_{\bar{R}} \tilde{E}(M)$ is a split semisimple \bar{S} -algebra. This algebra is then a direct sum of absolutely simple left ideals $\{L_i\}$, and we have $\tilde{E}(L_i) = E(L_i) \cong \bar{S}$. (By (30.27), there is a corresponding decomposition $SM = \bigoplus N_i$ into indecomposable $S\Lambda$ -modules, with $\tilde{E}(N_i) \cong \tilde{E}(L_i)$.) Each N_i is absolutely indecomposable as $S\Lambda$ -module, by (30.29), and the proof is complete.

It is often convenient to find a complete d.v.r. S such that for every f.g. indecomposable Λ -module M , the $S\Lambda$ -module SM splits into a direct sum of absolutely indecomposable submodules. Given an M , we can always choose an S depending on M by (30.31). The following discussion is an adaptation of the results given in (30.30). Let R be a complete d.v.r. with perfect residue class field \bar{R} , and let Ω denote an algebraic closure of \bar{R} , and K' an algebraic closure of K . By (30.30), each finite extension F of \bar{R} in Ω is the residue class field \bar{S} of a d.v.r. S in some finite unramified extension L of K in K' . Let K_0 be the union of all of these L 's. The P -adic valuation v on K extends uniquely to K_0 (and indeed to K'), and the valuation ring R_0 of K_0 is then a d.v.r. with prime element π , where $P = \pi R$. The residue class field $\bar{R}_0 = R_0/\pi R_0$ is the union of all of the fields F , and coincides with Ω . (The field K_0 is called the *maximal unramified extension* of K .) Then K_0 is algebraic over K , and each subfield L of K_0 finite over K is an unramified extension of K . If the residue class field \bar{R} is finite, then K_0 can be obtained from K by adjoining all m -th roots of unity, where m ranges over all integers not divisible by $\text{char } R$.)

It may occur, however, that the d.v.r. R_0 is not complete, and usually $\dim_K K_0 = \infty$. Let S_0 denote the π -adic completion of R_0 , and L_0 the quotient field of S_0 . Then S_0 is a complete d.v.r. for which

$$\bar{S}_0 = S_0/\pi S_0 \cong R_0/\pi R_0 \cong \Omega,$$

and S_0 is an extension of the d.v.r. R . Of course, S_0 need not be a f.g. R -module.

We are now ready to prove

(30.32) Proposition. *Let \bar{R} be perfect, and let S_0 be the complete d.v.r. defined above. Then for each f.g. indecomposable Λ -module, the $S_0\Lambda$ -module $S_0 M$ is a direct sum of absolutely indecomposable submodules.*

Proof. For each M , choose S as in (30.31) so that SM is a direct sum of absolutely indecomposable $S\Lambda$ -modules. Since S_0 contains S , the result is

clear from the identifications

$$S_0\Lambda \cong S_0(S\Lambda), S_0M \cong S_0(SM).$$

The results so far obtained may be viewed as generalizations of the theorems in §7 concerning the behavior of modules under ground field extensions. Indeed, many of the proofs in §7 can be obtained from those given here, by choosing $R = \bar{R} = K$, $S = \bar{S} = L$, in the proofs in this section.

In particular, our earlier result (7.11) has the following interesting analogue in integral representation theory:

(30.33) Theorem (Reiner [66]). *Let R and S be complete d.v.r.'s with S an extension of R , and suppose that \bar{R} is a finite field. Then for each indecomposable f.g. Λ -module M , the $S\Lambda$ -module SM is a direct sum of non-isomorphic indecomposable submodules.*

Proof. Since M is indecomposable, $\tilde{E}(M)$ must be a division algebra over \bar{R} . Since \bar{R} is finite, so is $\tilde{E}(M)$, and therefore $\tilde{E}(M)$ is a field by Wedderburn's Theorem (see CR (68.9)). Then $\bar{S} \otimes_{\bar{R}} \tilde{E}(M)$ is a commutative algebra, and is semisimple by (7.8). It is therefore a direct sum of fields, no two of which are isomorphic as ideals of $\bar{S} \otimes \tilde{E}(M)$. The desired result now follows from (30.27).

In case \bar{R} is not assumed perfect, we have the following result (see Reiner [66] for proof):

(30.34) Theorem. *Let M be any f.g. left Λ -module. Then M is absolutely indecomposable if and only if $\tilde{E}(M)$ is a field which is purely inseparable over \bar{R} .*

For further results concerning behavior of modules under ground ring extensions, see Bialnicki-Birula [70], Roggenkamp [72], Huppert [75].

§30C. Representations mod P^k

Let Λ be an R -order in a K -algebra A , where for the moment R is an arbitrary Dedekind domain. Given a nonzero ideal $\alpha = \prod P^{e(P)}$ in R , we wish to consider representations of Λ by matrices with entries in the residue class ring R/α . This is equivalent to studying f.g. Λ -modules which are free as (R/α) -modules. For each such module M , we may decompose M into its P -primary parts $\{M_P\}$ with P ranging over the prime ideal divisors of α . Thus, the problem of classifying M reduces to the case in which α is a power of a prime ideal. (Of course, if each M_P is known, then we can find an (R/α) -free module M with prescribed P -primary parts $\{M_P\}$, provided that the number of elements in a free $(R/P^{e(P)})$ -basis of M_P is independent of P .)

Further, in finding representations of Λ over R/P^e , there is no harm in replacing R by its localizations R_P , since this does not affect the residue class ring. Changing notation, we may now assume that R is a d.v.r. with maximal ideal P . For $k \geq 1$, set

$$R_k = R/P^k, \quad \Lambda_k = \Lambda/P^k\Lambda.$$

By a Λ_k -lattice we mean a f.g. left Λ_k -module which is R_k -free. Every exact sequence of Λ_k -lattices is split over R_k . Further, the ring R_k is self-injective (see Exercise 2.13), so every Λ_k -lattice is injective as R_k -module. It follows that if $N \subseteq M$ are Λ_k -lattices, then so is M/N . We note also that any direct summand of a Λ_k -lattice is R_k -projective, hence R_k -free since R_k is local. Thus, direct summands of Λ_k -lattices are again Λ_k -lattices.

Suppose now that $\Lambda = RG$, where G is a finite group of order n , with n a unit in R . Then every exact sequence of Λ_k -lattices

$$0 \rightarrow L \rightarrow M \rightarrow N \rightarrow 0$$

is Λ_k -split, since it is R_k -split, and we can mimic the proof of Maschke's Theorem. Therefore every Λ_k -lattice is Λ_k -projective. It follows from (30.4) and (30.8) that the correspondence $M \mapsto \bar{M} = M/PM$ gives an isomorphism-preserving bijection between the set of Λ_k -lattices M and the set of f.g. projective $\bar{\Lambda}$ -modules \bar{M} , where $\bar{\Lambda} = \Lambda/P\Lambda$. Further, since the K-S-A Theorem holds for Λ_k -lattices, each such lattice is uniquely a direct sum of copies of lattices $\{M_1, \dots, M_r\}$, where these are a full set of non-isomorphic indecomposable projective Λ_k -lattices.

The case where $n \in P$ is much more interesting and difficult, assuming that $k > 1$. (The case $k = 1$ is the usual one of finding all modular representations of G .) We shall describe the results of Drobotenko-Drobotenko-Zhilinskaya-Pogoril'yak [65], as simplified by Hannula [68], which deal with the case in which G is cyclic of prime order p . Here, R may be any d.v.r. in which p is a prime element. Let $k > 1$, and assume p odd for simplicity. Given a Λ_k -lattice M , put $\bar{M} = M/pM$, viewed as a $\bar{\Lambda}$ -module. Let

$$S_i = \bar{R}[\lambda]/(\lambda^i), \quad 1 \leq i \leq p,$$

where $\lambda = 1 - x$, and x is a generator of G . These $\{S_i\}$ give all of the indecomposable $\bar{\Lambda}$ -modules, and \bar{M} is a direct sum of copies of these $\{S_i\}$.

Let us show at once that \bar{M} is a sum of types S_1 , S_{p-1} and S_p , and no others. Indeed, suppose $p > 3$ and $S_t \mid \bar{M}$, where $2 \leq t \leq p-2$. Choose $m \in M$ so that

$$\{\bar{m}, \lambda\bar{m}, \dots, \lambda^{t-1}\bar{m}\} = \bar{R}\text{-basis of } S_t.$$

Then $\{m, \lambda m, \dots, \lambda^{t-1}m\}$ is part of an R_k -basis for M (see Exercise 6.9). We

have $\lambda \bar{m} \notin \lambda^2 \bar{M}$. But

$$\lambda^p m = \lambda^2 \cdot \lambda^{p-2} m \in p\lambda^2 M$$

since $t \leq p-2$. Then

$$0 = (x^p - 1)m = ((1-\lambda)^p - 1)m = (-\lambda^p + p\lambda^{p-1} - \cdots - p\lambda)m,$$

which implies that $p\lambda m \in p\lambda^2 M$, and therefore (since $k > 1$) $\lambda \bar{m} \in \lambda^2 \bar{M}$, a contradiction.

If \bar{M} is a sum of copies of S_1 , we say M has type i . If M has type p , then $\bar{M} \cong \bar{\Lambda}^{(n)}$ for some n , so \bar{M} is $\bar{\Lambda}$ -projective. As in (30.11) it follows that M is Λ -projective, and indeed $M \cong \Lambda^{(n)}$.

Now let M be any Λ_k -lattice, and let $S_p \mid \bar{M}$; then M contains the Λ_k -lattice N as direct summand, where

$$N = \bigoplus_{i=0}^{p-1} R_k \lambda^i m, \text{ and } S_p = \bar{\Lambda} \bar{m}.$$

Thus $N \cong \Lambda_k$; but then the exact sequence of Λ_k -lattices

$$0 \rightarrow N \rightarrow M \rightarrow M/N \rightarrow 0$$

is R_k -split, hence also Λ_k -split. (To see this, let $M^* = \text{Hom}_{R_k}(M, R_k)$ be the contragredient of M . Then $M^{**} \cong M$, and also $\Lambda_k^* \cong \Lambda_k$. The sequence

$$0 \rightarrow (M/N)^* \rightarrow M^* \rightarrow N^* \rightarrow 0$$

is then Λ_k -split, whence so is the original one, by taking contragredients once more. See Exercise 10.22.)

We therefore have a Λ_k -decomposition

$$M = M' \oplus M'',$$

where M' is Λ_k -free, and \bar{M}'' is a sum of copies of S_1 and S_{p-1} . A computation involving successive basis changes then shows that

$$M'' = M_1 \oplus M_{p-1}, \quad M_i = \Lambda_k\text{-module of type } i, \quad i = 1, p-1.$$

(We omit the details.)

The structure of the Λ_k -lattice M_1 is easily described. If t is minimal such that $\lambda M_1 \subseteq p'M_1$, then from the fact that $(\lambda + 1)^p - 1$ annihilates M_1 , we find that $t = k-1$. Thus, M_1 affords a matrix representation

$$x \rightarrow \mathbf{I} + p^{k-1} \mathbf{B},$$

where \mathbf{B} may be viewed as a matrix over \bar{R} . The isomorphism class of M_1

determines the similarity class of \mathbf{B} over \bar{R} , and conversely. The indecomposable M_1 's thus correspond to matrices \mathbf{B} which are companion matrices of polynomials $f(X)^e$, with $f(X)$ irreducible in $\bar{R}[X]$ and $e \geq 1$.

Finally, the Λ_k -lattices M_{p-1} of type $p-1$ can be classified as follows. The augmentation ideal of the group ring Λ_k is $\lambda \cdot \Lambda_k$, and every Λ_k -lattice M of type $p-1$ can be written as an inner tensor product

$$M \cong (\lambda \cdot \Lambda_k) \otimes_{R_k} N,$$

with N a Λ_k -lattice of type 1. (Conversely, each such tensor product is of type $p-1$.) The isomorphism class of M determines that of N , and conversely. The proof is not difficult, but we omit it.

The above results show how to classify all R_kG -lattices when G is cyclic of order p , with p odd. Analogous results hold for $p=2$. For cyclic groups of order p^n , $n > 1$, partial results have been obtained by Thévenaz [81a, b]. His work also deals with arbitrary finite groups. However, the general classification problem for R_kG -lattices is of wild type (see Chapter 8) whenever $k \geq 2$ and G is a p -group (cyclic or not) of order greater than p . This result is due to Bondarenko [76]; see also Gudivok [78b].

For further reading: Drobotenko-Gudivok-Lichtman [64], Drobotenko-Lichtman [60], Hannula [68], Nazarova-Roiter [67a], [69], Levy [81].

Note. Nazarova-Roiter [69] determine *all* finite $\mathbb{Z}G$ -modules, where G is cyclic of prime order p . Each such module M decomposes into a sum of q -primary components, with q ranging over all rational primes. The case where $q \neq p$ is easily handled, since then \mathbb{Z}_qG is a direct sum of local Dedekind rings. The only problem occurs when $q=p$.

Here they use the fibre product diagram

$$\begin{array}{ccc} \Lambda & \longrightarrow & R = \hat{\mathbb{Z}}_p[\varepsilon], \quad \varepsilon = \text{primitive } p\text{-th root of 1} \\ \downarrow & & \downarrow \\ \hat{\mathbb{Z}}_p & \longrightarrow & \bar{\mathbb{Z}} = \mathbb{Z}/p\mathbb{Z}. \end{array}$$

They call Λ a *dyad*.

The general dyad problem is this: let R_1, R_2 be a pair of local Dedekind rings with common residue class field k , and let

$$\begin{array}{ccc} \Lambda & \longrightarrow & R_1 \\ \downarrow & & \downarrow \\ R_2 & \longrightarrow & k \end{array}$$

be a fibre product; call Λ a *dyad*. Each f.g. Λ -module M determines a pair of

matrices \mathbf{A}, \mathbf{B} over k , whose rows are weighted in a certain way. Certain permissible operations are performed on these rows (and also on the columns), and the resulting canonical forms yield a complete classification of all indecomposable f.g. Λ -modules M . The procedure generalizes Nazarova [67].

The authors use their results to describe all finite groups having an abelian normal subgroup of index p . This extends the work of V. S. Drobotenko [66]. See also Nazarova-Roiter-Sergeičuk-Bondarenko [72], and Levy [81].

§30. Exercises

1. Let I be an ideal of the commutative ring R , and let M be any left R -module. Show that there is an R -isomorphism

$$(R/I) \otimes_R M \cong M/IM.$$

[Hint: The sequence

$$I \otimes M \rightarrow R \otimes M \rightarrow (R/I) \otimes M \rightarrow 0$$

is exact.]

2. Let R be a d.v.r. with prime element π , and let Λ be an R -order in a semisimple K -algebra A . Let bars denote reduction mod π , and let M and N be Λ -lattices. Show that

$$\text{Hom}_\Lambda(\bar{M}, \bar{N}) \cong \text{Ext}_\Lambda^1(\bar{M}, N),$$

and that

$$\text{Hom}_\Lambda(\bar{M}, \bar{N}) = 0 \Rightarrow \text{Ext}_\Lambda^1(M, N) = 0.$$

[Hint: The exact sequence $0 \rightarrow N \xrightarrow{\pi} N \rightarrow \bar{N} \rightarrow 0$ gives an exact sequence

$$\text{Hom}(\bar{M}, N) \rightarrow \text{Hom}(\bar{M}, \bar{N}) \rightarrow \text{Ext}(\bar{M}, N) \xrightarrow{\pi} \text{Ext}(\bar{M}, N)$$

But $\text{Hom}(\bar{M}, N) = 0$ since N is R -torsionfree; also, $\pi \cdot \text{Ext}(\bar{M}, N) = 0$ since $\pi \bar{M} = 0$. Thus $\text{Hom}(\bar{M}, \bar{N}) \cong \text{Ext}(\bar{M}, N)$. If $\text{Hom}(\bar{M}, \bar{N}) = 0$, then the exact sequence

$$\text{Ext}^1(\bar{M}, N) \rightarrow \text{Ext}^1(M, N) \xrightarrow{\pi} \text{Ext}^1(M, N)$$

shows that π gives a monomorphism of $\text{Ext}(M, N)$ into itself. This implies that $\text{Ext}(M, N) = 0$, since $\text{Ext}(M, N)$ is a f.g. torsion R -module.]

3. Keep the notation of (30.17). Prove that $M|N$ if and only if $\hat{M}|\hat{N}$.

[Hint: If $\hat{M}|\hat{N}$, there exist $\hat{\Lambda}$ -homomorphisms $f_1: \hat{M} \rightarrow \hat{N}$, and $g_1: \hat{N} \rightarrow \hat{M}$, such that $g_1 f_1 = 1$. As in the proof of (30.17), there exists Λ -maps $f: M \rightarrow N$, $g: N \rightarrow M$, which lift f_1 and g_1 , respectively, and such that $gf \in \text{Aut}_\Lambda M$. Therefore $M|N$.]

4. Keep the notation of (30.27), but assume further that S has an R -basis of k elements. Show that SM and SN have a common indecomposable direct summand if and only if the same holds true for M and N .

[Hint: It suffices to treat the case where M and N are indecomposable. Then use the fact that $S \otimes_R M \cong M^{(k)}$ as Λ -modules.]

5. Keep the notation of (30.27). Let S be a totally ramified extension of R , that is, an extension for which $\bar{S} = \bar{R}$. Show that for each f.g. indecomposable Λ -module M , the $S\Lambda$ -module SM is also indecomposable.

6. Let Λ be an R -order, where R is a Dedekind domain. An R -algebra S is called *faithfully flat* if S is a flat R -module with the property that for each R -module M , $S \otimes_R M = 0$ implies $M = 0$. Assuming S faithfully flat, show that for f.g. left Λ -modules M and N satisfying $S \otimes_R M \cong S \otimes_R N$ as $(S \otimes_R \Lambda)$ -modules, it need not follow that $M \cong N$.

[Hint: Take $\Lambda = R$, $S = \coprod_P (R_P)$, where P ranges over all maximal ideals of R , and R_P denotes the P -adic completion of R . Choose $N = R$, $M =$ nonprincipal ideal of R . Then $S \otimes M \cong S \otimes N$ but $M \not\cong N$.]

§31. GENUS

Throughout this section, R denotes a Dedekind domain with quotient field K , and Λ is an R -order in a separable f.d. K -algebra A . To avoid trivial cases, we assume always that $R \neq K$. Let P range over the maximal ideals of R , and let R_P denote the localization of R at P , and \hat{R}_P the P -adic completion of R (or of R_P).

By (26.5), there exists a maximal R -order Λ' in A which contains Λ . Then for each P , $\Lambda_P \subseteq \Lambda'_P$ and Λ'_P is a maximal R_P -order in A . Thus Λ_P fails to be a maximal R_P -order precisely when $\Lambda_P \neq \Lambda'_P$. We put

$$(31.1) \quad S(\Lambda) = \{P : \Lambda_P \neq \text{maximal } R_P\text{-order in } A\} = \{P : \Lambda_P \neq \Lambda'_P\}.$$

Then $S(\Lambda)$ is a finite set of maximal ideals P of R , by Exercise 4.7, and $S(\Lambda) = \emptyset$ if and only if Λ is a maximal order (see (26.21)). For example, when $\Lambda = RG$ where $\text{char } K \nmid |G|$, the set $S(\Lambda)$ is given by $\{P : P \text{ contains } |G|\}$, by (27.1).

Two Λ -lattices M and N are placed in the same *genus* (notation: $M \vee N$) if $M_P \cong N_P$ as Λ_P -lattices for each P . As we shall see, it suffices to impose this condition when $P \in S(\Lambda)$. Further, it is often convenient to use Roiter's Lemma: $M \vee N$ if and only if for each nonzero ideal I of R , there is a Λ -exact sequence

$$0 \rightarrow M \rightarrow N \rightarrow T \rightarrow 0,$$

with $I + \text{ann}_R T = R$.

Instead of working with localizations, we could equally well use P -adic completions.

The first basic fact about genera is that if $N_P|M_P$ for each $P \in S(\Lambda)$ (assuming $S(\Lambda) \neq \emptyset$), then there exists a Λ -lattice N' in the genus of N such that $N'|M$. Thus, decomposability is a property of genus. An important consequence of this result is that one can “add” lattices within a genus, that is, if L , M and N are in the same genus, then

$$L \oplus M \cong N \oplus N'$$

for some lattice N' in the genus. This formula leads to the concept of the locally free class group $\text{Cl } \Lambda$ of an order. This class group also arises naturally in algebraic K -theory, when one studies $K_0(\mathbb{Z}G)$ (see Chapter 10). We shall give an idèle-theoretic version of $\text{Cl } \Lambda$ in this section, reserving the deeper discussion of the subject for Chapter 11.

The section concludes with a beautiful and powerful result due to Roiter (and, in another form, to Jacobinski): *Let M and N be Λ -lattices in the same genus, and let F be any faithful* Λ -lattice. Then N is a direct summand of $M \oplus F$.* As a consequence of this theorem, it follows that if L is a Λ -lattice such that $L_P|M_P$ for each $P \in S(\Lambda)$, and if every A -composition factor of KL occurs more often in KM than in KL , then L is a direct summand of M .

§31A. Basic Properties

For M and N Λ -lattices, we write $M \vee N$ if $M_P \cong N_P$ for each P . We say that M and N are in the same *genus*, or are *locally isomorphic*. By (30.17), $M \vee N$ if and only if $\hat{M}_P \cong \hat{N}_P$ for each P . Put

$$\Gamma_M = \{N : N = \Lambda\text{-lattice}, N \vee M\},$$

the *genus* of M .

Our first result shows that the genus of M is determined by the behavior of M at the primes in the set $S(\Lambda)$ defined in (31.1). We have:

(31.2) Proposition. *Let M and N be Λ -lattices, and let $S(\Lambda)$ be defined as in (31.1). Then*

- (i) *$M \vee N$ implies $KM \cong KN$ as A -modules.*
- (ii) *If $S(\Lambda) \neq \emptyset$, then $M \vee N$ if and only if $M_P \cong N_P$ for all $P \in S(\Lambda)$.*
- (iii) *If Λ is a maximal order, then $M \vee N$ if and only if $KM \cong KN$.*

Proof. If $M \vee N$, then $M_P \cong N_P$ for each P . However, if this isomorphism holds for even one choice of P , then we obtain $KM_P \cong KN_P$, whence $KM \cong KN$.

*This means that $\text{ann}_\Lambda F = 0$.

This establishes (i) and part of (iii). Suppose now that $KM \cong KN$; if Λ_P is a maximal R_P -order, then the Λ_P -lattices M_P and N_P have the property that $KM_P \cong KN_P$, whence $M_P \cong N_P$ by Exercise 26.11. This completes the proof of (iii). Finally, suppose $S(\Lambda) \neq \emptyset$; by the first step in the proof, we deduce that $KM \cong KN$, whence as above $M_P \cong N_P$ whenever $P \notin S(\Lambda)$. But this proves (ii), and establishes the proposition.

(31.3) Corollary. *Let L , M and N be Λ -lattices.*

- (i) *A Λ -exact sequence $0 \rightarrow L \rightarrow M \rightarrow N \rightarrow 0$ is split if and only if for each $P \in S(\Lambda)$, the Λ_P -exact sequence $0 \rightarrow L_P \rightarrow M_P \rightarrow N_P \rightarrow 0$ is split.*
- (ii) *N is Λ -projective if and only if N_P is Λ_P -projective for all $P \in S(\Lambda)$.*
- (iii) *If G is a finite group with $\text{char } K \nmid |G|$, then an RG -lattice N is RG -projective if and only if N_P is $R_P G$ -projective for each P dividing $|G|$.*

Proof. For (i), we note that the original sequence splits if and only if it splits at each P . But for $P \notin S(\Lambda)$, N_P is a lattice over the maximal R_P -order Λ_P , and is therefore Λ_P -projective by (26.12). This establishes (i), and then (ii), (iii) are obvious consequences.

We shall next derive Roiter's criterion for two lattices to lie in the same genus, and we begin with preliminary result which is used often. This result involves simultaneous approximation of some collection of homomorphisms; for later applications, we need the version dealing with completions rather than localizations.

(31.4) Lemma. *Let S_0 be some finite non-empty collection of maximal ideals of R , and let M and N be Λ -lattices. Suppose that for each $P \in S_0$, there exist $\hat{\Lambda}_P$ -homomorphisms*

$$f_P: \hat{M}_P \rightarrow \hat{N}_P, \quad g_P: \hat{N}_P \rightarrow \hat{M}_P,$$

such that $f_P g_P = 1$ on \hat{N}_P . Then there exist Λ -homomorphisms

$$u: M \rightarrow N, \quad v: N \rightarrow M,$$

such that for each $P \in S_0$, $uv \in \text{Aut } \hat{N}_P$.

Proof. For each $P \in S_0$, the completion \hat{R}_P is a flat R -module, by (2.34). Using (2.38), we obtain

$$(31.5) \quad \hat{R}_P \otimes_R \text{Hom}_{\Lambda}(M, N) \cong \text{Hom}_{\hat{\Lambda}_P}(\hat{M}_P, \hat{N}_P).$$

Let us treat this isomorphism as an identification, so by (4.21) we see that

$\text{Hom}(M, N)$ is densely embedded in $\text{Hom}(\hat{M}_P, \hat{N}_P)$ in the P -adic topology. For each $P \in S_0$, we may choose $u_P \in \text{Hom}(M, N)$ such that

$$(u_P - f_P) \hat{M}_P \subseteq P \hat{N}_P.$$

By (4.7) or (4.8), we can find elements $\{\alpha_P : P \in S_0\}$ in R , such that for each $P \in S_0$,

$$\alpha_P \equiv 1 \pmod{P}, \quad \alpha_P \equiv 0 \pmod{P'} \text{ for all } P' \in S_0 - \{P\}.$$

Set $u = \sum_{P \in S_0} \alpha_P u_P$; then $u \in \text{Hom}_{\Lambda}(M, N)$, and

$$(u - f_P) \hat{M}_P \subseteq P \hat{N}_P \text{ for all } P \in S_0.$$

Likewise, we may find a map $v \in \text{Hom}_{\Lambda}(N, M)$ such that

$$(v - g_P) \hat{N}_P \subseteq P \hat{M}_P \text{ for all } P \in S_0.$$

Then for $P \in S_0$ we have

$$\hat{N}_P = f_P g_P \hat{N}_P = uv \hat{N}_P + P \hat{N}_P.$$

Therefore $\hat{N}_P = uv \hat{N}_P$ by Nakayama's Lemma, whence $uv \in \text{Aut}(\hat{N}_P)$ by (5.8). This completes the proof.

We shall use this lemma repeatedly. As its first important application, we derive the following criterion for two lattices to lie in the same genus:

(31.6) Roiter's Lemma. *Let M and N be Λ -lattices. Then $M \vee N$ if and only if for each nonzero ideal I of R , there exists a Λ -exact sequence*

$$0 \rightarrow M \rightarrow N \rightarrow T \rightarrow 0$$

for some Λ -module T such that $I + \text{ann}_R T = R$.

Proof. If the criterion holds, then for each P there is such an exact sequence for which $P + \text{ann}_R T = R$. Then $T_P = 0$ by Exercise 4.5, whence $M_P \cong N_P$ because $0 \rightarrow M_P \rightarrow N_P \rightarrow T_P \rightarrow 0$ is exact by §4A. Hence $M \vee N$, as claimed.

Conversely, suppose that $M \vee N$, so there exists an A -isomorphism $\varphi: KM \cong KN$. If the ideal I coincides with R , we proceed as follows: choose a nonzero element $a \in R$ such that $a \cdot \varphi(M) \subseteq N$. Then there is an exact sequence

$$0 \rightarrow M \xrightarrow{a\varphi} N \rightarrow T \rightarrow 0,$$

in which $I + \text{ann} T = R$, as desired.

We are now left with the case where $I \subset R$, and we choose S_0 to be the non-empty set of all maximal ideals of R which contain I . Since we are assuming that $M \vee N$, it follows that for each $P \in S_0$ we can find $\hat{\Lambda}_P$ -isomorphisms

$$f_P: \hat{M}_P \cong \hat{N}_P \text{ and } g_P: \hat{N}_P \cong \hat{M}_P.$$

Hence by (31.4) we can find maps $u \in \text{Hom}_{\Lambda}(M, N)$, $v \in \text{Hom}_{\Lambda}(N, M)$, such that for each $P \in S_0$, $vu \in \text{Aut}_{\hat{\Lambda}_P}(\hat{M}_P)$ and $uv \in \text{Aut}_{\hat{\Lambda}_P}(\hat{N}_P)$. Let us now consider the Λ -exact sequence

$$0 \rightarrow \ker u \rightarrow M \xrightarrow{u} N.$$

By (4.2) we have $(\ker u)_P = \ker u_P = 0$ for $P \in S_0$. Thus $\ker u$ is a torsion R -module annihilated by some element of the multiplicative set $R - P$. But $\ker u \subseteq M$, so $\ker u$ is R -torsionfree. This gives $\ker u = 0$, so we obtain a Λ -exact sequence

$$0 \rightarrow M \xrightarrow{u} N \rightarrow T \rightarrow 0, \text{ where } T = \text{cok } u.$$

For each $P \in S_0$, the map u gives rise to an isomorphism $u_P: \hat{M}_P \cong \hat{N}_P$. Therefore $\hat{T}_P = 0$, so $T_P = 0$ by (4.2iiii), and thus $P + \text{ann}_R T = R$. Since this holds for each P dividing I , we obtain $I + \text{ann}_R T = R$ as desired, completing the proof.

As an application of the above, we show how to “add” lattices in the same genus:

(31.7) Corollary. *Let L , M and N be Λ -lattices in the same genus. Then there exists a Λ -lattice L' in the genus such that*

$$M \oplus N \cong L \oplus L'.$$

Proof. By Roiter’s Lemma, there exists Λ -exact sequences

$$0 \rightarrow M \xrightarrow{f} L \rightarrow T \rightarrow 0, \quad 0 \rightarrow N \xrightarrow{f} L \rightarrow U \rightarrow 0,$$

with T and U R -torsion Λ -modules such that

$$\text{ann}_R T + \text{ann}_R U = R.$$

Thus for each maximal ideal P of R , either $T_P = 0$ or $U_P = 0$, that is, either f_P or g_P is an isomorphism.

Now consider the sequence

$$0 \rightarrow L' \rightarrow M \oplus N \xrightarrow{(f, g)} L \rightarrow 0,$$

where $L' = \ker(f, g)$, and where $(f, g)(m+n) = f(m) + g(n)$, $m \in M$, $n \in N$. The map (f, g) is surjective by (4.2), since for each P it induces a surjection $M_P \oplus N_P \rightarrow L_P$. Thus the sequence is exact. By (4.2) the sequence is Λ -split, since it splits at each P . Thus we have $M \oplus N \cong L \oplus L'$. Finally, at each P we obtain

$$\hat{M}_P \oplus \hat{N}_P \cong \hat{L}_P \oplus \hat{L}'_P, \quad \hat{M}_P \cong \hat{L}_P,$$

whence by (30.7) we obtain $\hat{N}_P \cong \hat{L}'_P$. Thus $L' \vee N$, as desired.

In §31B, we shall return to this idea of “addition” of lattices in a given genus, but first let us continue with consequences of the preceding lemmas. The following striking result, an analogue of Schanuel’s Lemma (see §2), is due to Roiter [66a]:

(31.8) Proposition. *Let L , L' , M and M' be Λ -lattices, and let T be an R -torsion Λ -module such that $T_P = 0$ for all $P \in S(\Lambda)$. Suppose that there exist a pair of Λ -exact sequences*

$$0 \rightarrow L' \rightarrow L \xrightarrow{f} T \rightarrow 0, \quad 0 \rightarrow M' \rightarrow M \xrightarrow{g} T \rightarrow 0.$$

Then there is a Λ -isomorphism

$$L \oplus M' \cong L' \oplus M.$$

Proof. Let W be the pullback of the pair of maps f, g (see §2). Then we obtain a commutative diagram of Λ -modules and Λ -homomorphisms, with exact rows and columns:

$$\begin{array}{ccccccc} & & 0 & & 0 & & \\ & & \downarrow & & \downarrow & & \\ & & L' & \xrightarrow{1} & L' & & \\ & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & M' & \longrightarrow & W & \longrightarrow & L \longrightarrow 0 \\ & & \downarrow 1 & & \downarrow & & \downarrow f \\ 0 & \longrightarrow & M' & \longrightarrow & M & \xrightarrow{g} & T \longrightarrow 0 \\ & & \downarrow & & \downarrow & & \downarrow \\ & & 0 & & 0 & & \end{array}$$

At each $P \in S(\Lambda)$ we have $T_P = 0$ by hypothesis. Further, the process of localization at P preserves exactness and commutativity. It follows that both

of the Λ -exact sequences

$$0 \rightarrow M' \rightarrow W \rightarrow L \rightarrow 0, \quad 0 \rightarrow L' \rightarrow W \rightarrow M \rightarrow 0,$$

are split at each $P \in S(\Lambda)$. Hence they are split over Λ by (31.3). Therefore

$$W \cong M' \oplus L, \quad W \cong L' \oplus M,$$

which proves the result.

From this result we may derive formulas (31.10) and (31.11) below, which demonstrate the failure of the K-S-A Theorem in the global case. Let M and N be Λ -lattices, and let X be an extension of N by M , so there is a Λ -exact sequence

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

Each $\varphi \in \text{End}_\Lambda(M)$ determines another extension ${}_\varphi X$ of N by M , namely, we choose ${}_\varphi X$ to be the pushout of φ and the above map $M \rightarrow X$. We obtain a commutative diagram with exact rows:

$$\begin{array}{ccccccc} 0 & \longrightarrow & M & \longrightarrow & X & \longrightarrow & N & \longrightarrow 0 \\ & & \varphi \downarrow & & \theta \downarrow & & 1 \downarrow & \\ 0 & \longrightarrow & M & \longrightarrow & {}_\varphi X & \longrightarrow & N & \longrightarrow 0. \end{array}$$

(Indeed, if X corresponds to an extension class $\xi \in \text{Ext}_\Lambda^1(N, M)$, then ${}_\varphi X$ corresponds to the class $\varphi\xi$ (see §8)). From the Snake Lemma (Exercise 2.5), we obtain

$$\ker \varphi \cong \ker \theta, \quad \text{cok } \varphi \cong \text{cok } \theta.$$

Suppose now that φ satisfies the condition

$$(31.9) \quad \varphi_P \in \text{Aut}_{\Lambda_P}(M_P) \text{ for all } P \in S(\Lambda),$$

where $S(\Lambda) \neq \emptyset$. Then $\ker \varphi_P = 0$, that is, $(\ker \varphi)_P = 0$ for each $P \in S(\Lambda)$; since $\ker \varphi$ is R -torsionfree, we see that $\ker \varphi = 0$, whence also $\ker \theta = 0$. Further,

$$(\text{cok } \theta)_P \cong (\text{cok } \varphi)_P = \text{cok } \varphi_P = 0, \quad P \in S(\Lambda).$$

We thus obtain Λ -exact sequences

$$0 \rightarrow X \xrightarrow{\theta} {}_\varphi X \rightarrow \text{cok } \varphi \rightarrow 0, \quad 0 \rightarrow M \xrightarrow{\varphi} M \rightarrow \text{cok } \varphi \rightarrow 0.$$

From (31.8) we then obtain the following “Absorption Formula”, due to

Reiner [78]:

$$(31.10) \quad {}_{\varphi} X \oplus M \cong X \oplus M.$$

In a similar manner, if Y is another extension of N by M , we obtain an exact sequence

$$0 \rightarrow Y \rightarrow {}_{\varphi} Y \rightarrow \text{cok } \varphi \rightarrow 0,$$

and hence we deduce the ‘‘Exchange Formula’’

$$(31.11) \quad X \oplus {}_{\varphi} Y \cong {}_{\varphi} X \oplus Y,$$

also due to Reiner [78]. We emphasize that these formulas depend strongly on the hypothesis (31.9).

We show next that decomposability of a Λ -lattice M depends only upon the local behavior of M .

(31.12) Theorem. *Let M and N be Λ -lattices such that $\hat{N}_P \mid \hat{M}_P$ for each $P \in S(\Lambda)$. (If $S(\Lambda) = \emptyset$, assume instead that $KN \mid KM$.) Then there exists a Λ -lattice $N' \in \Gamma_N$ such that $N' \mid M$.*

Proof. Assume first that $S(\Lambda) \neq \emptyset$; the hypothesis implies that for each $P \in S(\Lambda)$, there exist maps f_P, g_P as in (31.4). Hence we can find maps u, v with

$$M \xrightarrow[u]{v} N, \quad uv \in \text{Aut}(\hat{N}_P) \text{ for all } P \in S(\Lambda).$$

Put $L = u(M)$, a Λ -sublattice of N . Then for $P \in S(\Lambda)$ we have

$$\hat{N}_P = u(\hat{M}_P) = \hat{L}_P,$$

so $N \vee L$ by (31.2). Furthermore, at each $P \in S(\Lambda)$ the surjection $u: \hat{M}_P \rightarrow \hat{L}_P$ is split by the map $v: \hat{L}_P \rightarrow \hat{M}_P$. Hence the Λ -exact sequence

$$0 \rightarrow \ker u \rightarrow M \rightarrow L \rightarrow 0$$

splits at each $P \in S(\Lambda)$, whence it splits globally*. Thus $M \cong L \oplus \ker u$, and the result is proved for the case where $S(\Lambda) \neq \emptyset$. For the proof when $S(\Lambda) = \emptyset$, see Exercise 31.2.

*This follows from (4.2) and the fact that a sequence of Λ_P -lattices splits if and only if the corresponding sequence of $\hat{\Lambda}_P$ -lattices is split (see Exercise 31.1).

(31.13) Corollary. *Let L, M and N be Λ -lattices such that $L \vee (M \oplus N)$. Then there exist Λ -lattices M', N' with*

$$L \cong M' \oplus N', M' \vee M, N' \vee N.$$

(31.14) Corollary. *Let L and M be Λ -lattices such that $L \vee M^{(r)}$. Then there exists a Λ -lattice M' in the genus of M such that*

$$L \cong M^{(r-1)} \oplus M'.$$

Proof. From (31.13), we obtain

$$L \cong M_1 \oplus \cdots \oplus M_r,$$

where each $M_i \vee M$. Now use (31.7) repeatedly:

$$M_1 \oplus M_2 \cong M \oplus M'_2, \text{ where } M'_2 \vee M,$$

$$M'_2 \oplus M_3 \cong M \oplus M'_3, \text{ where } M'_3 \vee M,$$

and so on.

In (31.12) we saw that if M and N are Λ -lattices such that N is a local direct summand of M , then some N' in the genus of N is a global direct summand of M . We shall see in §31C that, *under suitable hypotheses*, a much deeper result holds: if N is a local direct summand of M , then N is also a global direct summand of M .

To conclude this subsection, we remark that genus can also be studied by using semilocal rings. Let $S(\Lambda) \neq \emptyset$, and set

$$\tilde{R} = \bigcap_{P \in S(\Lambda)} R_P,$$

so \tilde{R} is the ring of quotients $S^{-1}R$, where S is the multiplicative set

$$S = R - \bigcup_{P \in S(\Lambda)} P.$$

The maximal ideals of \tilde{R} are $\{P\tilde{R} : P \in S(\Lambda)\}$, and \tilde{R} is semilocal. Put $\tilde{\Lambda} = \tilde{R}\Lambda$, an \tilde{R} -order in A ; each Λ -lattice M gives rise to a $\tilde{\Lambda}$ -lattice $\tilde{M} = \tilde{R}M$.

(31.15) Proposition. *Two Λ -lattices M and N are in the same genus if and only if $\tilde{M} \cong \tilde{N}$ as $\tilde{\Lambda}$ -modules.*

Proof. For each $P \in S(\Lambda)$, $M_P \cong (\tilde{M})_{P\tilde{R}}$ by transitivity of the construction of modules of quotients. Hence if $\tilde{M} \cong \tilde{N}$, then $M_P \cong N_P$ for each $P \in S(\Lambda)$, and therefore $M \vee N$. Conversely, if $M \vee N$ then $\tilde{M} \vee \tilde{N}$ as $\tilde{\Lambda}$ -lattices. By Roiter's

Lemma we can then find a $\tilde{\Lambda}$ -exact sequence

$$0 \rightarrow \tilde{M} \rightarrow \tilde{N} \rightarrow T \rightarrow 0$$

in which T is an \tilde{R} -torsion module for which $\text{ann}_{\tilde{R}} T$ is coprime to each of the ideals $\{P\tilde{R} : P \in S(\Lambda)\}$. This implies that $T=0$, so $\tilde{M} \cong \tilde{N}$, as desired.

By (23.14), every $\tilde{\Lambda}$ -lattice is expressible as \tilde{M} for some Λ -lattice M . The preceding result shows that the study of genera of Λ -lattices is equivalent to the study of $\tilde{\Lambda}$ -lattices. For V a f.g. left A -module, let

$$\sigma(V) \cong \{M : M \cong \text{full left } \Lambda\text{-lattice in } V\},$$

and let $g(V)$ be the number of genera in $\sigma(V)$. Then $g(V)$ is precisely the number of $\tilde{\Lambda}$ -isomorphism classes in the set $\sigma(V)$. We have shown above that each $\tilde{\Lambda}$ -lattice X is determined up to isomorphism by the isomorphism classes $\{X_P : P \in S(\Lambda)\}$. If $h_P(V)$ denotes the number of Λ_P -isomorphism classes in the set $\sigma(V)$, the above discussion yields the formula

$$g(V) = \prod_{P \in S(\Lambda)} h_P(V),$$

due to Maranda [55] and Takahashi [59]. Note that $g(V)$ is finite whenever K is a global field. (If Λ is a maximal order, we find readily that $g(V)=1$ for each V .)

In practice, the use of $\tilde{\Lambda}$ -lattices for working with genera produces some simplifications in proofs (see, for example, Lee [64] and Pu [65]). However, the method does not seem to be of major significance. We may remark also that the K-S-A Theorem need not be valid for $\tilde{\Lambda}$ -lattices (see §36).

§31B. Idèles and Class Groups

In this subsection only, we change notation, and use the subscript P to denote P -adic completion, rather than localization at P . As usual, let R be a Dedekind domain with quotient field K . Let Γ be an R -order in a f.d. separable K -algebra B , and let M be a left Γ -lattice. We put

$$A = \text{End}_B KM, \quad \Lambda = \text{End}_\Gamma M,$$

where these endomorphism rings are viewed as acting on the opposite side from scalars. Then Λ is an R -order in the f.d. K -algebra A , and by Exercise 7.13, A is a separable K -algebra. We view M as a bimodule ${}_R M_\Lambda$. Our aim is to establish the relationship between Γ -lattices in the genus of M , and left ideals of Λ .

For any Γ -lattice N in the genus of M , we have $KN \cong KM$ as B -modules, by (31.2). Replacing N by an isomorphic copy, if need be, we may assume that N

is a full Γ -lattice in KM . Thus, in studying Γ -lattices in the genus of M , we may restrict our attention to the full Γ -lattices in KM .

Given any full Γ -lattice N in KM , we note that each $\varphi \in \text{Hom}_\Gamma(N, M)$ extends to an element of $\text{Hom}_B(KN, KM)$, and is therefore given by right multiplication by an element of A . Therefore

$$(31.16) \quad N \cong M \text{ as } \Gamma\text{-lattices} \Leftrightarrow N = Mx \text{ for some } x \in A^\circ,$$

where A° is the group of units of A . Furthermore, for each maximal ideal P of R , the completion N_P is a full Γ_P -lattice in $K_P M_P$. We have $N \vee M$ if and only if $N_P \cong M_P$ for each P , that is, if and only if for each P , $N_P = M_P \alpha_P$ for some $\alpha_P \in (A_P)^\circ$. Furthermore, since $M_P = N_P$ a.e. (see Exercise 4.7), we may choose $\alpha_P \in (\Lambda_P)^\circ$ a.e. (or even $\alpha_P = 1$ a.e., if desired).

By §4 we have

$$N = KM \cap \left(\bigcap_P N_P \right) = KM \cap \left(\bigcap_P M_P \alpha_P \right).$$

This suggests that we should introduce the *idèle group* $J(A)$ relative to R , defined by

$$(31.17) \quad J(A) = \left\{ (\alpha_P) \in \prod_P (A_P)^\circ : \alpha_P \in (\Lambda_P)^\circ \text{ a.e.} \right\}.$$

We note at once that $J(A)$ does not depend on the choice of the R -order Λ in A , since if Λ' is another R -order in A , then $\Lambda_P = \Lambda'_P$ a.e. Thus, up to isomorphism, every Γ -lattice N in the genus of M is given by

$$N = KM \cap \left(\bigcap_P M_P \alpha_P \right), \text{ where } (\alpha_P) \in J(A).$$

For each $\alpha = (\alpha_P) \in J(A)$, we define

$$\Lambda\alpha = A \cap \left\{ \bigcap_P \Lambda_P \alpha_P \right\} = \bigcap_P \{A \cap \Lambda_P \alpha_P\}.$$

By (4.21), $\Lambda\alpha$ is a full left Λ -lattice in A such that $(\Lambda\alpha)_P = \Lambda_P \alpha_P$ for each P . Thus $\Lambda\alpha$ is isomorphic to a left ideal of Λ , and $\Lambda\alpha$ is in the same genus as Λ (as Λ -lattices). We shall call $\Lambda\alpha$ a *locally free (rank 1) Λ -lattice*, or a *locally free fractional Λ -ideal in A* .

We note next that $N = M \cdot \Lambda\alpha$, for $\alpha \in J(A)$ as above, since for each P we have

$$N_P = M_P \alpha_P = M_P \Lambda_P \alpha_P = M_P \cdot (\Lambda\alpha)_P = (M \cdot \Lambda\alpha)_P.$$

Thus, each full Γ -lattice N in KM , such that $N \vee M$, is of the form $N = M \cdot \Lambda\alpha$.

for some $\alpha \in J(A)$. Conversely, every $M \cdot \Lambda\alpha$ is such an N . We remark that

$$\Lambda\alpha = \text{Hom}_\Gamma(M, N),$$

since these two expressions are R -lattices in A having the same completion at each P :

$$\begin{aligned} (\Lambda\alpha)_P &= \Lambda_P\alpha_P, \quad \{\text{Hom}_\Gamma(M, N)\}_P = \text{Hom}_{\Gamma_P}(M_P, M_P\alpha_P) \\ &= \text{End}_{\Gamma_P}(M_P) \cdot \alpha_P = \Lambda_P\alpha_P. \end{aligned}$$

(Remark: $N \vee M$ implies by (31.7) that $N \mid M^{(2)}$. By (6.3), the summands of $M^{(2)}$ correspond bijectively with the summands of $\Lambda^{(2)}$, with

$$N \leftrightarrow \text{Hom}_\Gamma(M, N), \quad N = M \otimes_\Lambda \text{Hom}_\Gamma(M, N).$$

We have just encountered a special case of this correspondence.)

Now let $\alpha, \beta \in J(A)$, and form the left Γ -lattices $M \cdot \Lambda\alpha, M \cdot \Lambda\beta$. These are Λ -isomorphic if and only if

$$M \cdot \Lambda\beta = M \cdot \Lambda\alpha \cdot x \text{ for some } x \in A^\circ.$$

This latter condition is equivalent to the assertion that for some $x \in A^\circ$,

$$M_P\beta_P = M_P\alpha_P x \text{ for all } P,$$

that is, for all P we have

$$\beta_P = u_P\alpha_P x \text{ for some } u_P \in (\Lambda_P)^\circ.$$

We introduce two subgroups of the idèle group $J(A)$. The image of A° in $J(A)$ is the group of *principal idèles*, denoted by $u(A)$. (A principal idèle is an idèle of the form (x) , having P -th component x for all P , where $x \in A^\circ$.) Next, let $U(\Lambda)$ be the group of *unit idèles*, defined by

$$U(\Lambda) = \prod_P (\Lambda_P)^\circ \subseteq J(A).$$

We have just shown that $M \cdot \Lambda\beta \cong M \cdot \Lambda\alpha$ if and only if $\beta \in U(\Lambda) \cdot \alpha \cdot u(A)$. We collect our results in the following result, due to Takahashi [59] and Fröhlich [75] (see also Drozd [69a] and Faddeev [65a]):

(31.18) Theorem. *Let Γ be an R -order, M a left Γ -lattice, and let $\Lambda = \text{End}_\Gamma(M)$, $A = K\Lambda$, where M is viewed as bimodule ${}_\Gamma M_\Lambda$. Then there is a bijection between the set of isomorphism classes of left Γ -lattices in the genus of M , and the set of double cosets $U(\Lambda) \cdot \alpha \cdot u(A)$ of the idèle group $J(A)$. The*

double coset containing an idèle α corresponds to the isomorphism class of the Γ -lattice

$$M \cdot \Lambda\alpha = KM \cap \left\{ \bigcap_P M_P \alpha_P \right\}, \text{ where } \alpha = (\alpha_P) \in J(A).$$

We are now ready to take up once more the methods of “addition” of lattices in the same genus, and we can now give a much more enlightening version of (31.7). In the notation of this subsection, let $\alpha, \beta \in J(A)$, and consider the locally free fractional Λ -ideals $\Lambda\alpha, \Lambda\beta$ defined above. Then $\Lambda\alpha$ and $\Lambda\beta$ are left Λ -lattices in the genus of Λ , so by (31.7) we know that

$$\Lambda\alpha \oplus \Lambda\beta \cong \Lambda \oplus \Lambda\gamma \text{ for some } \gamma \in J(A).$$

Our problem is to determine γ in terms of α and β . The analogy with Steinitz’s Theorem 4.13 may be useful here; this theorem tells us that if I and J are nonzero fractional R -ideals of K , then

$$I \oplus J \cong R \oplus IJ \text{ as } R\text{-lattices.}$$

This suggests that there should be some multiplicative version of (31.7). Indeed, we shall now prove the following result, due to Fröhlich [75]; his proof used properties of reduced norms, and the more direct proof given here is due to Reiner (see Reiner-Roggenkamp [79]):

(31.19) Theorem. *For α and $\beta \in J(A)$, we have*

$$\Lambda\alpha \oplus \Lambda\beta \cong \Lambda \oplus \Lambda\alpha\beta.$$

Proof. We shall begin by replacing α by $ru\alpha$, and β by βx , for suitably chosen elements $r \in R$ ($r \neq 0$), $u \in U(\Lambda)$, and $x \in u(A)$. These changes will not affect the isomorphism classes of the Λ -lattices $\Lambda\alpha, \Lambda\beta$ and $\Lambda\alpha\beta$. First choose r so that $r\alpha$ is an *integral idèle*, that is, $r\alpha_P \in \Lambda_P$ for each P . Then pick u so that $ru_P\alpha_P = 1$ a.e. Changing notation, we assume from now on that $\alpha_P \in \Lambda_P$ for each P , and that $\alpha_P = 1$ a.e.

Now let $S_0 = \{P : \alpha_P \neq 1\}$; if $S_0 = \emptyset$, then $\alpha = 1$ and the result is obvious for this case. We may therefore consider the case where the finite set S_0 is non-empty. Let t be a positive integer, to be chosen later; the choice will depend on α , but not on β . For each $P \in S_0$, A is dense in the P -adic completion A_P . Therefore by the Strong Approximation Theorem 4.8, we can find an element $x \in u(A)$ such that

$$\beta_P x \equiv 1 \pmod{P^t \Lambda_P} \text{ for each } P \in S_0,$$

and such that βx is an integral idèle. Replacing β by βx and changing

notation, we may hereafter assume that β is an integral idèle for which

$$\beta_P \equiv 1 \pmod{P' \Lambda_P} \text{ for each } P \in S_0.$$

Some preliminary comments may be useful before we describe how to choose t . We wish to consider the commutator $\beta\alpha\beta^{-1}\alpha^{-1}$, and to make its P -th component

$$\beta_P \alpha_P \beta_P^{-1} \alpha_P^{-1}$$

close to 1 (in Λ_P) for each $P \in S_0$. This will guarantee that the above P -th component lies in (Λ_P) for each $P \in S_0$. For fixed α_P , the above expression is a continuous function of β_P relative to the P -adic topology. Hence if we take β_P sufficiently close to 1, we can make the above expression near $1 \cdot \alpha_P \cdot 1 \cdot \alpha_P^{-1}$, that is, it will also be close to 1.

To be explicit, we first choose a positive integer k such that for each $P \in S_0$, we have $\alpha_P^{-1} \in P^{-k} \Lambda_P$. Note that for each P , both α_P and β_P lie in Λ_P , since α and β are integral idèles. We now take $t = k + 1$. Then for $P \in S_0$ we may write

$$\beta_P = 1 + \lambda \pi'$$

for some $\lambda \in \Lambda_P$, where π is a prime element of R_P . But then

$$\beta_P^{-1} = (1 + \lambda \pi')^{-1} = 1 - \lambda \pi' + \lambda^2 \pi'^{2t} - \dots = 1 + \lambda_1 \pi'$$

for some $\lambda_1 \in \Lambda_P$. We therefore obtain

$$\begin{aligned} \beta_P \alpha_P \beta_P^{-1} \alpha_P^{-1} &= (1 + \lambda \pi') \alpha_P (1 + \lambda_1 \pi') \alpha_P^{-1} \\ &= (\alpha_P + \lambda \alpha_P \pi') (\alpha_P^{-1} + \lambda_2 \pi'^{-k}) \end{aligned}$$

for some $\lambda_2 \in \Lambda_P$ (note that we have used the fact that $\alpha_P^{-1} \in \pi^{-k} \Lambda_P$). Multiplying, we have

$$\beta_P \alpha_P \beta_P^{-1} \alpha_P^{-1} = 1 + \lambda_3 \pi'^{-k} = 1 + \pi \lambda_3$$

for some $\lambda_3 \in \Lambda_P$. Since $\pi \Lambda_P \subseteq \text{rad } \Lambda_P$ by §5, it follows that the commutator $\beta_P \alpha_P \beta_P^{-1} \alpha_P^{-1} \in (\Lambda_P)$. This holds for each $P \in S_0$, and therefore

$$(31.20) \quad \Lambda_P \beta_P \alpha_P = \Lambda_P \alpha_P \beta_P \text{ for each } P \in S_0,$$

a result which is crucial in the rest of the proof.

Since α and β are integral idèles, both $\Lambda\alpha$ and $\Lambda\beta$ are left ideals of Λ , and therefore $\Lambda\alpha + \Lambda\beta \subseteq \Lambda$. We shall show that indeed $\Lambda\alpha + \Lambda\beta = \Lambda$; by §4, it

suffices to show that

$$\Lambda_P \alpha_P + \Lambda_P \beta_P = \Lambda_P \text{ for each } P.$$

This surely holds for $P \notin S_0$, for then $\alpha_P = 1$; but it also holds when $P \in S_0$, since then $\beta_P \equiv 1 \pmod{P\Lambda_P}$, so $\beta_P \in (\Lambda_P)^\circ$. We have thus shown that $\Lambda\alpha + \Lambda\beta = \Lambda$, so there is a surjection $f: \Lambda\alpha + \Lambda\beta \rightarrow \Lambda$ of the external direct sum $\Lambda\alpha + \Lambda\beta$ onto Λ , where f is defined by using the inclusions $\Lambda\alpha \subseteq \Lambda$, $\Lambda\beta \subseteq \Lambda$. Setting $L = \ker f$, we obtain an exact sequence of Λ -lattices

$$(31.21) \quad 0 \rightarrow L \rightarrow \Lambda\alpha + \Lambda\beta \xrightarrow{f} \Lambda \rightarrow 0.$$

If $(a, b) \in \ker f$, we have $a = -b$; therefore

$$L \cong \Lambda\alpha \cap \Lambda\beta = \cap (\Lambda \cap \Lambda_P \alpha_P \cap \Lambda_P \beta_P).$$

We claim that $\Lambda\alpha \cap \Lambda\beta = \Lambda\alpha\beta$, that is,

$$\Lambda_P \alpha_P \cap \Lambda_P \beta_P = \Lambda_P \alpha_P \beta_P \text{ for all } P.$$

For $P \in S_0$ we have $\beta_P \in (\Lambda_P)^\circ$, so

$$\Lambda_P \alpha_P \cap \Lambda_P \beta_P = \Lambda_P \alpha_P = \Lambda_P \beta_P \alpha_P = \Lambda_P \alpha_P \beta_P$$

by (31.20). For $P \notin S_0$ we have $\alpha_P = 1$, so

$$\Lambda_P \alpha_P \cap \Lambda_P \beta_P = \Lambda_P \beta_P = \Lambda_P \alpha_P \beta_P.$$

This proves that $L \cong \Lambda\alpha\beta$, as claimed. But (31.21) splits, so $\Lambda\alpha \oplus \Lambda\beta \cong \Lambda \oplus \Lambda\alpha\beta$, and the theorem is proved.

(31.22) Corollary. *For $\alpha, \beta \in J(A)$,*

$$\Lambda \oplus \Lambda\alpha\beta \cong \Lambda \oplus \Lambda\beta\alpha.$$

We may now obtain the formula for “addition” within a genus as an immediate consequence of (31.19). Let M be a left Γ -lattice, and let L, N be Γ -lattices in the genus of M . Using the notation of (31.18), we may write

$$L = M \cdot \Lambda\alpha, N = M \cdot \Lambda\beta \text{ for some } \alpha, \beta \in J(A).$$

Now there is a surjection of Γ -lattices:

$$M \otimes_{\Lambda} \Lambda\alpha \rightarrow L, \text{ given by } m \otimes \xi \mapsto m\xi, \text{ for } m \in M, \xi \in \Lambda\alpha.$$

This map is injective, since it is injective at each P . Thus we have

$$M \otimes_{\Lambda} \Lambda\alpha \cong M \cdot \Lambda\alpha = L.$$

From (31.19) we obtain

$$(M \otimes \Lambda\alpha) \oplus (M \otimes \Lambda\beta) \cong (M \otimes \Lambda) \oplus (M \otimes \Lambda\alpha\beta),$$

where \otimes is \otimes_{Λ} . From this result, we obtain

$$L \oplus N \cong M \oplus M \cdot \Lambda\alpha\beta,$$

which proves (31.7) in a stronger form:

$$(31.23) \quad M \cdot \Lambda\alpha \oplus M \cdot \Lambda\beta \cong M \oplus M \cdot \Lambda\alpha\beta, \quad \alpha, \beta \in J(A).$$

It should be remarked that the above proof is in the same spirit as the proof of the isomorphism $I \oplus J \cong R \oplus IJ$ in Steinitz's Theorem, given in CR §22, p. 150.

(31.24) Example. Let us consider the idèle group $J(K)$ relative to the Dedekind domain R . By definition,

$$J(K) = \left\{ (\alpha_P) \in \prod_P (K_P) : \alpha_P \in (R_P) \text{ a.e.} \right\}.$$

Here, $(K_P)^\circ$ is just the multiplicative group consisting of all nonzero elements of the P -adic field K_P . Then the *group of unit idèles* is given by

$$U(R) = \prod_P (R_P)^\circ,$$

and $u(K)$ is the group of principal idèles. Since $J(K)$ is a commutative group, the double cosets $U(R) \cdot \alpha \cdot u(K)$ in $J(K)$ coincide with the cosets of $J(K)$ relative to the subgroup $U(R) \cdot u(K)$. Hence by (31.18), applied to the special case where $\Gamma = \Lambda = R$, $M = R$, we obtain a bijection between the set of ideal classes in R and the set of cosets of $J(K)$ relative to $U(R) \cdot u(K)$. Indeed, (31.23) asserts that there is an isomorphism

$$(31.25) \quad J(K) / (U(R) \cdot u(K)) \cong \text{Cl}(R),$$

where $\text{Cl}(R)$ denotes the ideal class group of R . This isomorphism carries the coset $\alpha \cdot U(R) \cdot u(K)$ containing the element $\alpha \in J(K)$ onto the ideal class $[R\alpha]$, where

$$R\alpha = \bigcap_P (K \cap R_P \alpha_P).$$

In short, $R\alpha$ is the fractional R -ideal in K whose P -th component is $R_P \alpha_P$ for each P . If we set

$$R_P \alpha_P = \pi_P^{n(P)} R_P, \text{ where } \pi_P = \text{prime element of } R_P,$$

then $n(P)=0$ a.e., and

$$R\alpha = \prod_P P^{n(P)}.$$

(Of course, the isomorphism (31.25) is well known, and is the starting point for the idèle-theoretic treatment of ideal theory and class field theory for global fields.)

As a direct consequence of (31.18) and the above example, we obtain the following result of Maranda [55] (see also Takahashi [59]):

(31.26) Theorem. *Let R be a Dedekind domain whose quotient field K is a global field. Let Γ be an R -order in a separable K -algebra B , and let M be a full left Γ -lattice in the left B -module V . Suppose that V is absolutely simple, that is, $\text{End}_B V \cong K$. Then the number of Γ -isomorphism classes in the genus of M equals the class number of R , that is, the order of the class group $\text{Cl}(R)$.*

Proof. In the notation of (31.18), we have $A = K$. Since Λ is an R -order in A , we obtain $\Lambda = R$. Therefore each Γ -lattice N in KM in the genus of M may be written as $N = M \cdot R\alpha$ for some $\alpha \in J(K)$. In fact, $R\alpha$ is a fractional R -ideal α in K , so $N = M\alpha$. By (31.18), for $\alpha, \beta \in J(K)$,

$$M \cdot R\alpha \cong M \cdot R\beta \Leftrightarrow \beta \in U(\Lambda) \cdot \alpha \cdot u(K) \Leftrightarrow R\alpha = R\beta.$$

Thus, the number of isomorphism classes of N 's equals the number of ideal classes of R .

Suppose now that Λ is an arbitrary R -order in a separable K -algebra A . By analogy with Example 31.24 above, we wish to introduce a *locally free class group* $\text{Cl}(\Lambda)$, whose elements are “classes” of locally free fractional Λ -ideals. Thus, $\text{Cl}(\Lambda)$ consists of classes $[\Lambda\alpha]$, $\alpha \in J(A)$, with “addition” of classes given by the formula

$$[\Lambda\alpha] + [\Lambda\beta] = [\Lambda\alpha\beta] \text{ for } \alpha, \beta \in J(A).$$

(For the case $\Lambda = R$, we get the usual ideal class group $\text{Cl}(R)$ in this way.) In the proof of Steinitz's Theorem, one of the crucial steps is the use of exterior powers to show that the Steinitz class of an R -lattice is indeed an isomorphism invariant of the R -lattice (see (34.30)). Unfortunately, this technique is no longer available when the order Λ is not commutative, and the isomorphism classes of $\Lambda\alpha$ and $\Lambda\beta$ do *not* (generally speaking) determine the isomorphism class of $\Lambda\alpha\beta$. Indeed, from Theorem 31.19 we know that the isomorphism classes of $\Lambda\alpha$ and $\Lambda\beta$ determine the isomorphism class of $\Lambda \oplus \Lambda\alpha\beta$. However, an example due to Swan [62] (see Chapter 11) shows that

one may have

$$\Lambda \oplus \Lambda\gamma \cong \Lambda \oplus \Lambda\gamma', \quad \Lambda\gamma \neq \Lambda\gamma',$$

for suitable choice of Λ , and of $\gamma, \gamma' \in J(A)$.

To overcome this difficulty, it is customary to introduce the concept of stable isomorphism: two projective Λ -lattices M and N are called *stably isomorphic* if

$$M \oplus \Lambda^{(k)} \cong N \oplus \Lambda^{(k)}$$

for some k . (We shall see later that when K is an algebraic number field, this occurs if and only if $M \oplus \Lambda \cong N \oplus \Lambda$; see Chapter 10). Each $\Lambda\alpha$ is locally free, hence Λ -projective by (8.19). We now let $[\Lambda\alpha]$ denote the stable isomorphism class of $\Lambda\alpha$. (By Exercise 31.3, we know that any projective Λ -lattice M which is stably isomorphic to some $\Lambda\alpha$ must lie in the genus of Λ ; thus $M \cong \Lambda\beta$ for some β .)

(31.27) Definition. Let Λ be an R -order in a separable K -algebra A , and let $J(A)$ be the idèle group of A relative to R . For each $\alpha \in J(A)$, let $\Lambda\alpha$ be the locally free fractional Λ -ideal in A which corresponds to α , and let $[\Lambda\alpha]$ denote its stable isomorphism class. The *locally free ideal class group* of Λ , denoted by $\text{Cl}(\Lambda)$, consists of all classes $[\Lambda\alpha]$, $\alpha \in J(A)$, with addition defined by

$$[\Lambda\alpha] + [\Lambda\beta] = [\Lambda\alpha\beta], \quad \alpha, \beta \in J(A).$$

The zero element is $[\Lambda]$, and the negative of $[\Lambda\alpha]$ is $[\Lambda\alpha^{-1}]$. Thus, $\text{Cl}(\Lambda)$ is an additive abelian group.

The order of $\text{Cl}(\Lambda)$ equals the number of stable isomorphism classes $[\Lambda\alpha]$, and is therefore at most equal to the number of ordinary isomorphism classes of full left Λ -lattices in A . If K is a global field, this latter number is finite by the Jordan-Zassenhaus Theorem. This shows that $\text{Cl}(\Lambda)$ is a finite group whenever K is a global field. We shall return to the question of calculating $\text{Cl}(\Lambda)$ explicitly in Chapter 11.

§31C. Roiter's Theorem on Genera

Throughout this subsection, let K be a global field, and Λ an R -order in a separable K -algebra A . In this situation, we know that the Jordan-Zassenhaus Theorem is valid (see §24). Furthermore, for each maximal ideal P of R , the residue class field R/P is finite. This is proved in CR §20 when K is an algebraic number field; for the function field case, see Weiss [63, Chapter 5].

We return here to our earlier convention of using the subscript P to denote *localization* at P , rather than completion. If L, M and N are left Λ -lattices in

the same genus, then we saw in (31.7) that L is a direct summand of $M \oplus N$. In this subsection we shall present a deep generalization of this result, due to Roiter [66a]. The result can also be obtained from Jacobinski's theory of genera, to be developed later (see Chapter 11).

Recall that a Λ -lattice F is called *faithful* if for $\lambda \in \Lambda$, $\lambda F = 0$ implies $\lambda = 0$. Roiter's elegant result is as follows:

(31.28) Theorem. *Let M and N be Λ -lattices in the same genus, and let F be any faithful Λ -lattice. Then $N|(M \oplus F)$, and indeed*

$$M \oplus F \cong N \oplus F'$$

for some Λ -lattice F' such that $F' \vee F$.

All of the difficulty lies in proving that $N|(M \oplus F)$, since the second assertion is then an easy consequence of this fact (see Exercise 31.3). Since Λ is itself a faithful Λ -lattice, the theorem implies that

$$N \vee M \Rightarrow N|(M \oplus \Lambda)$$

(compare with Exercise 31.4, and Theorem 31.32 below).

The proof of Roiter's Theorem is based on several lemmas. We follow the treatment in Swan-Evans [70].

(31.29) Lemma. *Let M and N be Λ -lattices in the same genus, and let a be a nonzero ideal of R . Then there exists a Λ -exact sequence*

$$0 \rightarrow M \rightarrow N \rightarrow T \rightarrow 0,$$

where T is an R -torsion Λ -module such that:

(i) $a + \text{ann } T = R$, and

(ii) $T \cong \coprod_{i=1}^k T_i$ for some finite collection of simple Λ -modules $\{T_i\}$, such that

$$\text{ann } T_i + \text{ann } T_j = R \text{ for } i \neq j, 1 \leq i, j \leq k.$$

Here, ann means ann_R .

Proof. Let $n = \dim_K KM$ be the R -rank of M . By the Jordan-Zassenhaus Theorem, there are finitely many isomorphism classes of Λ -lattices of rank n ; let $\{M_i : 1 \leq i \leq q\}$ be representatives of these classes.

Let S be any simple left Λ -module; then $PS = 0$ for some maximal ideal P of R . For if this is not the case, then $PS = S$ for each P , whence $P \cdot S_P = S_P$, so $S_P = 0$ for each P by Nakayama's Lemma; this implies that $S = 0$, a contradiction.

We now consider all embeddings of M_i into M_j , such that the factor module is a simple Λ -module. Each such embedding corresponds to an exact sequence

$$(31.30) \quad 0 \rightarrow M_i \xrightarrow{f} M_j \rightarrow S_f \rightarrow 0,$$

where S_f is a simple left Λ -module, and the subscript f is merely an index to show that S_f depends on f . Here, i and j range independently from 1 to q , including the cases where $i=j$.

For a given ordered pair of indices (i, j) , we consider all possible sequences of the form (31.30). We shall call (i, j) a *good* pair if the set of ideals

$$\{\operatorname{ann} S_f : \text{all } f\}$$

is infinite; otherwise, we call the pair (i, j) *bad*. For each bad pair (i, j) there are only finitely many ideals in the set $\{\operatorname{ann} S_f\}$, and each of these is a maximal ideal of R by the earlier comments. We now put

$$\mathfrak{b} = \prod_{(i, j) \text{bad}} \left\{ \prod_f \operatorname{ann} S_f \right\}, \text{ a nonzero ideal of } R.$$

In the inner product, $\operatorname{ann} S_f$ ranges over the distinct prime ideals of R which occur as annihilators of simple factor modules $S_f = M_j/f(M_i)$.

Since $M \vee N$, by Roiter's Lemma there exists a Λ -exact sequence

$$0 \rightarrow M \rightarrow N \xrightarrow{\varphi} Y \rightarrow 0,$$

with Y an R -torsion Λ -module such that

$$\mathfrak{a}\mathfrak{b} + \operatorname{ann} Y = R.$$

Since Y is a *finite* Λ -module*, it has a Λ -composition series:

$$Y = Y_0 \supset Y_1 \supset \cdots \supset Y_r = 0.$$

Put $N_l = \varphi^{-1}(Y_l)$, $0 \leq l \leq r$. Then we obtain a chain

$$N = N_0 \supset N_1 \supset \cdots \supset N_r = M, N_l / N_{l+1} = \text{simple } \Lambda\text{-module}.$$

Consider the sequence $0 \rightarrow N_1 \rightarrow N_0 \rightarrow N_0 / N_1 \rightarrow 0$; we have $N_1 \cong M_i$, $N_0 \cong M_j$ for some pair (i, j) , and thus we have an exact sequence of the form (31.30), with $S = N_0 / N_1$. But S is a composition factor of Y , so $\operatorname{ann} S + \mathfrak{b} = R$; this implies at once that (i, j) is a good pair! But then there exist embeddings $N_1 \rightarrow N_0$ such that $\operatorname{ann}(N_0 / N_1)$ ranges over an infinite set of primes. In particular, we

*The finiteness of Y follows from the fact that K is a global field, so R/\mathfrak{a} is finite for each nonzero ideal \mathfrak{a} of R (see introductory remarks for this subsection).

may find an exact sequence

$$0 \rightarrow N_1 \rightarrow N_0 \rightarrow T_1 \rightarrow 0,$$

where T_1 is a simple Λ -module such that

$$\text{ann } T_1 + \alpha = R.$$

Repeating this argument for the pair N_1 and N_2 , we obtain an exact sequence

$$0 \rightarrow N_2 \rightarrow N_1 \rightarrow T_2 \rightarrow 0,$$

with

$$\text{ann } T_2 + \alpha \cdot \text{ann } T_1 = R, \quad T_2 \text{ simple.}$$

Continuing in this manner, we arrive at an exact sequence

$$0 \rightarrow M \rightarrow N \rightarrow T \rightarrow 0$$

with T an R -torsion Λ -module, such that the Λ -composition factors of T are $\{T_1, T_2, \dots, T_r\}$, and where

$$\text{ann } T_i + \text{ann } T_j = R, \quad \text{ann } T_i + \alpha = R, \quad 1 \leq i, j \leq r, \quad i \neq j.$$

But then the Primary Decomposition Theorem 4.31 gives $T \cong \coprod_{i=1}^r T_i$, which completes the proof of the lemma.

(31.31) Lemma. *Let Λ be an R -order in A , and let $\alpha \in R$ be a nonzero element such that $\alpha\Lambda' \subseteq \Lambda \subseteq \Lambda'$, where Λ' is a maximal R -order in A . Let*

$$T = \coprod_1^r T_i, \quad T_i = \text{simple } \Lambda\text{-module},$$

where

$$\text{ann } T_i + \text{ann } T_j = R, \quad \text{ann } T_i + R\alpha = R, \quad 1 \leq i, j \leq r, \quad i \neq j.$$

Then for each faithful Λ -lattice F , there exists a surjection of F onto T .

Proof. We shall find surjections $\varphi_i : F \rightarrow T_i$, $1 \leq i \leq r$. Then $\sum_{i=1}^r \varphi_i$ yields a map $F \rightarrow T$ which is surjective at each maximal ideal P of R , and hence is surjective (by §4), as desired.

Changing notation, let T be a simple Λ -module such that $\text{ann } T = P$, where P is a maximal ideal of R such that $P + \alpha R = R$. Then $P + \text{ann}(\Lambda'/\Lambda) = R$, whence $\Lambda'_P = \Lambda_P$, so Λ_P is a maximal order. Since F is a faithful Λ -module, it follows that KF is a faithful A -module, whence $A|(KF)^{(m)}$ for some m . Then $\Lambda_P | F_P^{(m)}$ by Exercise 31.2. But T is a factor module of $\Lambda_P / P\Lambda_P$, since $P \cdot T = 0$ and T is simple. Hence T is also a factor module of $F_P^{(m)} / PF_P^{(m)}$. This latter quotient is isomorphic to $F^{(m)} / PF^{(m)}$, so there exists a surjection $\psi: F^{(m)} \rightarrow T$. Then ψ must map at least one of the m summands of $F^{(m)}$ onto T , since T is simple. Hence there is a surjection of F onto T , as claimed.

We may now prove Roiter's Theorem 31.28. Let M and N be Λ -lattices in the same genus, and let $\alpha \in R$ be a nonzero element such that $\alpha\Lambda' \subseteq \Lambda \subseteq \Lambda'$ as in (31.31). By (31.29), there exists a Λ -exact sequence

$$0 \rightarrow M \rightarrow N \rightarrow T \rightarrow 0$$

where

$$\text{ann } T + \alpha R = R, \quad T \cong \coprod_1^r T_i \text{ as in (31.29ii).}$$

By (31.31), we can find an exact sequence

$$0 \rightarrow F' \rightarrow F \xrightarrow{\varphi} T \rightarrow 0, \text{ where } F' = \ker \varphi.$$

If $\Lambda = \Lambda'$, then N is Λ -projective, and then $M \oplus F \cong N \oplus F'$ by Schanuel's Lemma. If $\Lambda \neq \Lambda'$, then for each P such that $\Lambda_P \neq \Lambda'_P$ we have $\alpha \in P$, so $\text{ann } T + P = R$ and therefore $T_P = 0$. The desired isomorphism now follows from (31.8), which completes the proof of Roiter's Theorem.

To illustrate the power of Roiter's Theorem, let us derive two important and beautiful consequences, which were proved independently by Roiter [66a] and Jacobinski [68b]:

(31.32) Theorem. *Let M and N be Λ -lattices, and suppose that $N_P | M_P$ for each $P \in S(\Lambda)$, where $S(\Lambda)$ is defined by (31.1). Assume that every A -composition factor of KN occurs strictly more often in KM than in KN . Then $N | M$ as Λ -lattices.*

Proof. By (31.12), $M = N' \oplus L$ for some Λ -lattice N' in the genus of N , and some Λ -lattice L . Let $I = \text{ann}_\Lambda M$; then I is a two-sided ideal of Λ , and $\Lambda_1 = \Lambda / I$ is an R -order which acts faithfully on M (see §23). We claim that L is also a faithful Λ_1 -lattice. Indeed, we have

$$KM = KN' \oplus KL \cong KN \oplus KL.$$

Since A is semisimple, each of the above modules is isomorphic to the direct sum of its composition factors. By hypothesis, every composition factor of KN is also a composition factor of KL . Hence for $y \in K\Lambda_1$,

$$y \cdot KL = 0 \Rightarrow y \cdot KN = 0 \Rightarrow y \cdot KM = 0 \Rightarrow y = 0,$$

which shows that KL is a faithful $K\Lambda_1$ -module. This implies at once that L is a faithful Λ_1 -lattice.

Applying (31.28) to the order Λ_1 in place of Λ , we obtain

$$N' \oplus L \cong N \oplus L'$$

for some Λ_1 -lattice L' in the genus of L . Therefore $M \cong N \oplus L'$ as Λ -lattices, and the proof is complete.

Let Γ_M denote the genus of a Λ -lattice M , and let $g(M)$ be the number of Λ -isomorphism classes in Γ_M . Under our hypothesis that K is a global field, it follows at once from the Jordan-Zassenhaus Theorem that $g(M)$ is finite for each M . We shall now show that there exists a constant g_0 , depending on Λ but not on M , such that $g(M) \leq g_0$ for each M . The result is due to Roiter [66a] and Jacobinski [68b], and we give Roiter's proof below. (There is also a proof by Drozd [69a] which uses adèles; see also Platonov [69].)

Let M_1, \dots, M_g be a full set of non-isomorphic Λ -lattices in the genus Γ_M of a given Λ -lattice M . We choose a nonzero $\alpha \in R$ such that $\alpha\Lambda' \subseteq \Lambda \subseteq \Lambda'$, where Λ' is a maximal R -order in A containing Λ . We may view each M_i as embedded in M , and we can find Λ -exact sequences

$$0 \rightarrow M_i \rightarrow M \rightarrow U_i \rightarrow 0, \quad 1 \leq i \leq g,$$

such that

$$\text{ann } U_i + \text{ann } U_j = R, \quad \text{ann } U_i + R\alpha = R \text{ for } 1 \leq i, j \leq g, i \neq j,$$

and such that for each i , U_i is a finite direct sum of simple Λ -modules $\{T_{il}\}$, with

$$\text{ann } T_{ij} + \text{ann } T_{lk} = R \text{ for } j \neq k,$$

(see the proof of (31.29)). Now put $N = M_1 \cap \cdots \cap M_g \subseteq M$. Then there is a Λ -monomorphism

$$\psi: M/N \rightarrow \coprod_{i=1}^g (M/M_i),$$

and we claim ψ is an isomorphism. It suffices to show that ψ_P is surjective for each P , where the subscript denotes localization at the maximal ideal P of R . If $(M/M_i)_P = 0$ for each i , then surely ψ_P is surjective. On the other hand, if (say) $(M/M_1)_P \neq 0$, then $P \mid \text{ann } U_1$, whence $P + \text{ann } U_j = R$ for $j > 1$, and then

$(M/M_j)_P = 0$ for $j > 1$. Thus we have

$$N_P = (M_1)_P \cap \cdots \cap (M_g)_P = (M_1)_P,$$

so ψ_P is surjective, as desired. This completes the proof that

$$M/N \cong \prod (M/M_i).$$

We thus have a Λ -exact sequence

$$0 \rightarrow N \rightarrow M \rightarrow \coprod_{i=1}^g U_i \rightarrow 0.$$

We note also that $N \vee M$, since $N_P = M_P$ whenever $P + R\alpha = R$.

On the other hand, by (31.31) there is also a Λ -exact sequence

$$0 \rightarrow L_0 \rightarrow \Lambda \rightarrow \coprod_{i=1}^g U_i \rightarrow 0,$$

so we can find a Λ -homomorphism θ for which the following diagram commutes:

$$\begin{array}{ccccccc} 0 & \longrightarrow & L_0 & \longrightarrow & \Lambda & \longrightarrow & \coprod U_i & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \theta \downarrow & & \downarrow 1 \\ 0 & \longrightarrow & N & \longrightarrow & M & \longrightarrow & \coprod U_i & \longrightarrow & 0. \end{array}$$

Let $L = M \cap K \cdot \theta(\Lambda)$; then L is an R -pure Λ -sublattice of M , and

$$\operatorname{rank}_R L \leq \operatorname{rank}_R \Lambda = \dim_K A.$$

From the above diagram we obtain $M = N + \theta(\Lambda) = N + L$, since $L \supseteq \theta(\Lambda)$. Therefore $M/L \cong N/(L \cap N)$, so there is an exact sequence of Λ -lattices

$$(\xi) \quad 0 \rightarrow L \cap N \xrightarrow{h} N \rightarrow M/L \rightarrow 0.$$

Here, $\xi \in \operatorname{Ext}(M/L, L \cap N)$, where Ext means $\operatorname{Ext}_\Lambda^1$. For each i , $1 \leq i \leq g$, there is an inclusion map $\mu_i : N \rightarrow M_i$, and then $M = N + L = M_i + L$. We obtain a commutative diagram with exact rows:

$$\begin{array}{ccccccc} (\xi) \quad 0 & \longrightarrow & L \cap N & \xrightarrow{h} & N & \longrightarrow & M/L & \longrightarrow & 0 \\ & & f_i \downarrow & & \mu_i \downarrow & & 1 \downarrow & & \\ (\xi_i) \quad 0 & \longrightarrow & L \cap M_i & \longrightarrow & M_i & \longrightarrow & M/L & \longrightarrow & 0. \end{array}$$

Here, $\xi_i \in \text{Ext}(M/L, L \cap M_i)$; the commutativity of the diagram gives $\xi_i = f_i \xi$ by §8A.

Applying $\text{Hom}_\Lambda(*, L \cap M_i)$ to the exact sequence (ξ) , we obtain a long exact sequence

$$\cdots \rightarrow \text{Hom}(N, L \cap M_i) \xrightarrow{h^*} \text{Hom}(L \cap N, L \cap M_i) \xrightarrow{\partial} \text{Ext}(M/L, L \cap M_i) \rightarrow \cdots.$$

By §8A we have $\xi_i = \partial(f_i)$, so the isomorphism class of M_i is determined by the isomorphism class of $L \cap M_i$ and by the choice of f_i . Since $(\mu_i)_P$ is an isomorphism whenever $P + R\alpha = R$, so is $(f_i)_P$, and therefore $(L \cap M_i) \vee (L \cap N)$ for each i . The number of possible isomorphism classes of $L \cap M_i$, as i varies, is therefore $\leq g(L \cap N)$. Since

$$(31.33) \quad \text{rank}_R(L \cap N) \leq \text{rank}_R L \leq \dim_K A,$$

it follows from the Jordan-Zassenhaus Theorem that there exists a constant g_1 , independent of N , for which $g(L \cap N) \leq g_1$ for all N . Therefore $g(M) \leq g_1 g_2$, where g_2 is an upper bound for the order of the image of ∂ in $\text{Ext}(M/L, L \cap M_i)$.

Let \tilde{R} be as in the proof of (31.15). Then f_i induces an isomorphism $\tilde{L} \cap \tilde{N} \cong \tilde{L} \cap \tilde{M}_i$, and by (29.7) we obtain a commutative diagram

$$\begin{array}{ccc} \text{Hom}(\tilde{L} \cap \tilde{N}, \tilde{L} \cap \tilde{N}) & \xrightarrow{\tilde{\partial}} & \text{Ext}(M/L, L \cap N) \\ \downarrow & & \downarrow \\ \text{Hom}(\tilde{L} \cap \tilde{N}, \tilde{L} \cap \tilde{M}_i) & \xrightarrow{\partial'} & \text{Ext}(M/L, L \cap M_i), \end{array}$$

in which the vertical maps are isomorphisms. Thus $|\text{im } \partial| = |\text{im } \partial'| = |\text{im } \tilde{\partial}|$. Since $\alpha \cdot \text{im } \tilde{\partial} = 0$ by (29.5), we have

$$|\text{im } \tilde{\partial}| \leq |\text{End}(\tilde{L} \cap \tilde{N}) : \alpha \cdot \text{End}(\tilde{L} \cap \tilde{N})|.$$

This index is finite, bounded independently of N because of (31.33). If g_2 is an upper bound, then we have $g(M) \leq g_1 g_2$, and we have thus proved:

(31.34) Theorem. *Let K be a global field, A a separable K -algebra, and Λ any R -order in A . Let $g(M)$ denote the number of Λ -isomorphism classes in the genus of a given Λ -lattice M . Then there exists a positive integer g_0 , depending on Λ but not on M , such that $g(M) \leq g_0$ for all M .*

(31.35) Remarks. (i) We may improve our bound g_2 above, as follows: let $D = L \cap N$, and put $\tilde{D} = \tilde{R} \otimes_R D$. By (34.5), the isomorphism class of the extension of M/L by $L \cap M_i$ corresponding to f_i is unchanged if we replace \tilde{f}_i by $\tilde{f}_i \theta$, with $\theta \in \text{Aut}_\Lambda D$. We may therefore choose g_2 to be an upper bound for

the index of the image of $\text{Aut}_\Lambda D$ in the group of units of the ring $\text{End}(\tilde{D})/\alpha \cdot \text{End}(\tilde{D})$. This procedure is needed in §34D, for example.

(ii) Roiter conjectured that $g(M) \leq g(\Lambda)$ for all M . The Drozd-Turčin example in §34D shows that this conjecture is false. Roggenkamp also gave a counterexample, based on Swan's counterexample to "cancellation" of lattices.

(iii) Roiter raised the following question: given a Λ -lattice M , is every lattice in the genus of M isomorphic to a maximal sublattice? This question was answered by Drozd [69b] and Jacobinski [70]. It is easy to find counterexamples when the K -algebra A has more than one simple component, so we may restrict our attention to the case where A is simple. Drozd and Jacobinski proved that the answer is affirmative in this case, under the hypothesis that M is an Eichler lattice (see the discussion following (34.12) below). We shall treat this question in detail in Chapter 11.

(iv) Let M be a left Γ -lattice, where Γ is an R -order in a f.d. K -algebra B which need not be semisimple. Drozd [71] investigated the number $g(M)$ of Γ -isomorphism classes in the genus of M . Set

$$\Lambda = \text{End}_\Gamma M, A = K\Lambda, \bar{A} = A/\text{rad } A, \bar{\Lambda} = \Lambda / (\Lambda \cap \text{rad } A),$$

so $\bar{\Lambda}$ is an R -order in the semisimple K -algebra \bar{A} . Theorem 31.18 carries over unchanged, as does the relation between Γ -lattices in the genus of M and locally free left ideals of Λ .

Each locally free left ideal L of Λ gives rise to a locally free ideal \bar{L} of $\bar{\Lambda}$, namely, $\bar{L} = L / (\Lambda \cap \text{rad } A)L$. The correspondence $L \leftrightarrow \bar{L}$ is a bijection from the genus of Λ to the genus of $\bar{\Lambda}$.

Assume now that K is an algebraic number field, so $g(\bar{\Lambda})$ is finite. It follows that $g(\Lambda)$ is finite, and therefore so is $g(M)$. Drozd gave an example to show that there need not be a uniform upper bound on $g(M)$, where M ranges over all Γ -lattices. Thus, the analogue of (31.34) need not be valid for orders in non-semisimple algebras.

§31. Exercises

- Let R be a d.v.r., \hat{R} its completion, and let Λ be an R -order. Show that an exact sequence of Λ -lattices

$$(ξ) \quad 0 \rightarrow L \rightarrow M \xrightarrow{f} N \rightarrow 0$$

is split if and only if the corresponding sequence of $\hat{\Lambda}$ -lattices

$$(ξ̂) \quad 0 \rightarrow \hat{L} \rightarrow \hat{M} \xrightarrow{\hat{f}} \hat{N} \rightarrow 0$$

is split.

[Hint: If the latter sequence is split, then by (31.3) we can find $v: N \rightarrow M$ such that $\hat{f}\hat{v} \in \text{Aut } \hat{N}$. This implies that $f v \in \text{Aut } N$, so v is the desired splitting of f .

Another proof is as follows: From (8.16) we have

$$\hat{R} \otimes_R \text{Ext}_\Lambda^1(N, M) \cong \text{Ext}_\Lambda^1(\hat{N}, \hat{M}),$$

and in the embedding $\text{Ext}_\Lambda^1(N, M) \rightarrow \text{Ext}_\Lambda^1(\hat{N}, \hat{M})$, the sequence (ξ) maps onto the sequence $(\hat{\xi})$. Hence $(\xi) = 0$ if and only if $(\hat{\xi}) = 0$.]

2. Let Λ be a maximal order, and let M and N be Λ -lattices such that $KN|KM$. Show that there exists a Λ -lattice N' with $N' \vee N$ and $N'|M$.

[Hint: We may write $KM \cong K(N \oplus L)$ for some Λ -lattice L , by (23.15). Then $M_P \cong N_P \oplus L_P$ for every P , by Exercise 26.11. Now use the proof of (31.12).]

3. Let L, L', M and M' be Λ -lattices such that

$$L \oplus M \cong L' \oplus M', L \vee L'.$$

Prove that $M \vee M'$.

4. Let \mathfrak{a} be a nonprincipal ideal of the Dedekind domain R . Show that \mathfrak{a} is a local direct summand of R (that is, $\mathfrak{a}_P|R_P$ for each maximal ideal R of R), but that \mathfrak{a} is not a direct summand of R . Prove that $\mathfrak{a}|R^{(2)}$, however.

5. Let M_1 and M_2 be Λ -lattices such that every A -composition factor of KM_2 is also a composition factor of KM_1 . Let $g(M)$ denote the number of Λ -isomorphism classes in the genus of the Λ -lattice M . Prove that

$$g(M_1 \oplus M_2) \leq g(M_1).$$

[Hint: Let $N \vee (M_1 \oplus M_2)$, so M_2 is a local summand of N . By (31.32) we obtain $N \cong M'_1 \oplus M_2$ for some $M'_1 \vee M_1$, which implies the result.]

6. Let \hat{R} be the completion of a d.v.r. R , and let M and N be Λ -lattices, where Λ is an R -order. Show that if $\hat{N}|\hat{M}$, then $N|M$.

[Hint: Use (31.5). See also Exercise 30.3.]

7. Let $0 \rightarrow L \rightarrow M \rightarrow N \rightarrow 0$ be an exact sequence of Λ -lattices, and let $M' \in \Gamma_M$. Show that there exist lattices $L' \in \Gamma_L$, $N' \in \Gamma_N$, and a commutative diagram with exact rows

$$\begin{array}{ccccccc} 0 & \longrightarrow & L & \longrightarrow & M & \longrightarrow & N & \longrightarrow 0 \\ & & \alpha \uparrow & & \beta \uparrow & & \gamma \uparrow & \\ 0 & \longrightarrow & L' & \longrightarrow & M' & \longrightarrow & N' & \longrightarrow 0, \end{array}$$

such that

(i) α, β, γ are Λ -monomorphisms with R -torsion cokernels, and

(ii) For each $P \in S(\Lambda)$, the maps α_P, β_P and γ_P are Λ_P -isomorphisms.

[Hint: If $S(\Lambda) \neq \emptyset$, then (ii) implies (i), since if α_P is an isomorphism for even one choice of P , then

$$(\ker \alpha)_P = 0, (\text{cok } \alpha)_P = 0,$$

whence $\ker \alpha = 0$ and $\text{cok } \alpha$ is an R -torsion Λ -module. Now let $S_0 = S(\Lambda)$ if $S(\Lambda) \neq \emptyset$, and let $S_0 = \{P_0\}$ for some maximal ideal P_0 of R when $S(\Lambda) = \emptyset$. It suffices to prove (ii) with $S(\Lambda)$ replaced by S_0 . By (31.6), there exists a Λ -monomorphism β with β_P an isomorphism for each $P \in S_0$. Put $N' = (\varphi\beta)(M') \subseteq N$, and let γ be the inclusion map. There is then an induced map $\alpha: L' \rightarrow L$ giving rise to the above commutative diagram. For each $P \in S_0$, α_P and γ_P are isomorphisms, which implies that $L' \vee L, N' \vee N$.]

8. Let $0 \rightarrow L \rightarrow M \rightarrow N \rightarrow 0$ be an exact sequence of Λ -lattices, and let $M' \in \Gamma_M$. Show that there exist lattices $L' \in \Gamma_L$, $N' \in \Gamma_N$, and a commutative diagram with exact rows

$$\begin{array}{ccccccc} 0 & \longrightarrow & L & \longrightarrow & M & \longrightarrow & N & \longrightarrow 0 \\ & & \downarrow \lambda & & \downarrow \mu & & \downarrow \nu & \\ 0 & \longrightarrow & L' & \longrightarrow & M' & \longrightarrow & N' & \longrightarrow 0 \end{array}$$

such that

(i) λ, μ, ν are Λ -monomorphisms with R -torsion cokernels, and

(ii) For each $P \in S(\Lambda)$, the maps λ_P, μ_P and ν_P are Λ_P -isomorphisms.

[Hint: Let S_0 be as in Exercise 7, and choose a monomorphism μ such that μ_P is an isomorphism for each $P \in S_0$. Replacing M' by an isomorphic copy if need be, we may assume that $KM = KM'$ and that $M_P = M'_P$ for each $P \in S_0$. Define $L' = KL \cap M'$, an R -pure sublattice of M' , and let $N' = M'/L'$. The map μ induces maps λ, ν , with λ_P and ν_P isomorphisms for $P \in S_0$. This implies that (i) holds as well as (ii).]

9. Keep the notation of the preceding exercise. Show that if $M \cong L \oplus N$ then $M' \cong L' \oplus N'$. This gives a slightly different proof of (31.13).

10. Let L and M be Λ -lattices in the same genus, and let Λ' be any R -order in A containing Λ . Prove that

$$M \oplus (\Lambda' \otimes_{\Lambda} L) \cong L \oplus (\Lambda' \otimes_{\Lambda} M)$$

as Λ -modules.

[Hint: There is an exact sequence of two-sided Λ -modules $0 \rightarrow \Lambda \rightarrow \Lambda' \rightarrow U \rightarrow 0$, with U an R -torsion module. Let $0 \rightarrow L \rightarrow M \rightarrow T \rightarrow 0$ be a Λ -exact sequence such that $T_P = 0$ whenever $P \in S(\Lambda)$ or whenever $U_P \neq 0$. In the Λ -exact sequence

$$\Lambda \otimes T \xrightarrow{\varphi} \Lambda' \otimes T \rightarrow U \otimes T \rightarrow 0$$

we have $\ker \varphi_P = 0$, $(U \otimes T)_P = 0$ for all P , whence $\Lambda' \otimes T \cong T$. Then

$$\Lambda' \otimes L \xrightarrow{\psi} \Lambda' \otimes M \rightarrow T \rightarrow 0$$

is exact, and $\ker \psi_P = 0$ for all P , so ψ is monic. Now use (31.8).]

11. Keep the above notation. Show that the kernel of the surjection $\Lambda' \otimes L \rightarrow \Lambda' L$ is precisely the R -torsion submodule of $\Lambda' \otimes L$. Deduce that

$$M \oplus \Lambda' L \cong L \oplus \Lambda' M.$$

[Hint: Use Exercise 23.8 and the fact that isomorphisms preserve R -torsion submodules.]

12. Let Λ be an R -order in a separable K -algebra A , and let Λ' be a maximal R -order in A containing Λ . Let X be a Λ' -lattice such that $KX \cong A^{(r)}$. Show that there exists a projective Λ -lattice M for which

$$\Lambda' \otimes_{\Lambda} M \cong X, KM \cong A^{(r)}.$$

[Hint: We may assume that $\Lambda' \neq \Lambda$, so $S(\Lambda) \neq \emptyset$. By (31.2), $X \vee (\Lambda')^{(r)}$; hence by Roiter's Lemma there is a Λ' -lattice Y isomorphic to X , such that $Y_P = (\Lambda'_P)^{(r)}$ for each $P \in S(\Lambda)$, with $Y \subseteq A^{(r)}$. Choosing $M = Y \cap \Lambda^{(r)}$, we have

$$M_P = Y_P \cap \Lambda_P^{(r)} = \Lambda_P^{(r)}$$

for each $P \in S(\Lambda)$. Then M is a projective Λ -lattice by (31.3), and has the desired properties.]

13. Let R be a Dedekind domain with quotient field K , and let I be a fractional R -ideal in K . Let $\{P_1, \dots, P_n\}$ be some given set of distinct maximal ideals of R . Show that there exists an $x \in K^*$ such that Ix is an ideal in R which is coprime to each P_j .

[Hint: The R -module I is in the same genus as R , so by Roiter's Lemma 31.6 there exists an exact sequence of R -modules

$$0 \rightarrow I \xrightarrow{\theta} R \rightarrow T \rightarrow 0,$$

in which T is an R -torsion module such that

$$\text{ann}_R T + P_j = R, 1 \leq j \leq n.$$

Then θ is right multiplication by some $x \in K^*$, and Ix has the desired properties.

The above result asserts that every ideal class of R contains an integral ideal coprime to any preassigned finite collection of maximal ideals of R . The proof given in CR (18.20) is essentially a special case of the proof of Roiter's Lemma. Likewise, the proof of Steinitz's identity $I \oplus J \cong R \oplus IJ$, for I and J fractional ideals (see (4.13) above), is a special case of (31.8) and (31.19).]

§32. PROJECTIVE LATTICES OVER GROUP RINGS; SWAN'S THEOREM

Throughout this section, let G denote a finite group of order n , and let R be a Dedekind domain with quotient field K . Our aim here is to prove a remarkable result due to Swan [60], stating that under certain mild hypotheses, every

f.g. projective RG -module is locally free (that is, lies in the same genus as a free module). This result is of basic importance in the applications of integral representation theory to topological questions (see Milnor [71]). We shall begin with a study of the local case, where R is a discrete valuation ring; all of the difficulty of the proof is concentrated in this case. Then we shall apply the local results to obtain information about the global case.

§32A. Local Case

In this subsection, let R be a d.v.r. with maximal ideal $P=\pi R$, quotient field K , and residue class field $\bar{R}=R/P$. We wish to study f.g. projective RG -modules, where G is a finite group. Each such module is of course R -torsionfree and R -projective, and we shall therefore call such modules *projective (left) RG-lattices*. The key result is as follows:

(32.1) Theorem. *Let M and N be projective RG-lattices such that $KM \cong KN$ as KG -modules. Then $M \cong N$ as RG -modules.*

Swan's original proof depended on the non-singularity of the Cartan matrix (see §§18, 21), and this version of it may be found in §21; see also Exercise 18.14 or CR(77.14). Here we shall follow another approach, due to Hattori [65], in which (32.1) is established in a much more general situation. We begin with a trivial lemma about group rings, after introducing some notation. For Λ any R -order, we set

$$(32.2) \quad \begin{cases} [\Lambda, \Lambda] = \left\{ \sum_{i=1}^k (a_i b_i - b_i a_i), \text{ where } a_i, b_i \in \Lambda, k \geq 1 \right\} \\ \Lambda^* = \Lambda / [\Lambda, \Lambda]. \end{cases}$$

Clearly Λ^* is an R -module, and we have:

(32.3) Lemma. *Let $\Lambda = RG$ be the integral group ring of a finite group G over any commutative ring R . Then Λ^* is R -torsionfree.*

Proof. Let x range over a full set of non-conjugate elements of G , and let C_x be the class sum (in RG) of all conjugates of x . If $y = txt^{-1}$ with $t \in G$, then $y - x \in [\Lambda, \Lambda]$, and hence the image x^* (of x in Λ^*) depends only on the conjugacy class of x .

Let $c(\Lambda)$ be the center of Λ , so

$$c(\Lambda) = \bigoplus_x RC_x.$$

Define $\varphi \in \text{Hom}_R(c(\Lambda), \Lambda^*)$ by $\varphi(C_x) = x^*$ for each x . Next, define $\psi \in \text{Hom}_R(\Lambda, c(\Lambda))$ by $\psi(y) = C_y$, $y \in G$. Every element of $[\Lambda, \Lambda]$ is an

R -linear combination of expressions of the form $yz - zy$, with $y, z \in G$; since yz and zy are conjugate, it follows that $\psi[\Lambda, \Lambda] = 0$, so ψ induces an R -map $\varphi: \Lambda^* \rightarrow c(\Lambda)$. Clearly φ and ψ are inverses of one another, so $\Lambda^* \cong c(\Lambda)$ as R -modules, and thus Λ^* is R -free.

Our next lemma concerns the structure of $RG/\text{rad } RG$ for the case where R is local:

(32.4) Lemma. *Let R be a d.v.r. with residue class field \bar{R} , and let G be a finite group. Then $RG/\text{rad } RG$ is a separable algebra over the field \bar{R} .*

Proof. Let $\Lambda = RG$, and set $\bar{\Lambda} = \Lambda/P = \bar{R}G$. Then by (30.3) we have

$$\Lambda/\text{rad } \Lambda \cong \bar{\Lambda}/\text{rad } \bar{\Lambda}.$$

But the latter expression is a separable \bar{R} -algebra by (7.10), so we are done.

We are now ready to prove (32.1), and amazingly enough, the proof requires only the two properties of the group ring RG given in the lemmas above. We shall prove the following more general version of (32.1), due to Hattori [65]:

(32.5) Theorem. *Let R be a d.v.r., and let Λ be any R -order in a K -algebra A , satisfying the conditions:*

- (i) Λ^* is R -torsionfree, where Λ^* is defined as in (32.2), and
- (ii) $\bar{\Lambda}/\text{rad } \bar{\Lambda}$ is a separable \bar{R} -algebra (where bars denote reduction mod P).

Then for any pair of projective left Λ -lattices M and N ,

$$KM \cong KN \text{ as } A\text{-modules} \Leftrightarrow M \cong N \text{ as } \Lambda\text{-modules}.$$

Proof. Step 1. Let \hat{R} be the P -adic completion of R , and let $\hat{\Lambda}$, \hat{M} , etc., denote P -adic completions. We find at once that

$$(\hat{\Lambda})^* \cong \hat{R} \otimes_R \Lambda^*, \quad \hat{\Lambda}/\text{rad } \hat{\Lambda} \cong \Lambda/\text{rad } \Lambda, \quad \hat{R}/P\hat{R} \cong \bar{R}$$

(see Exercise 5.7). Thus $\hat{\Lambda}$ satisfies the same hypotheses as Λ . Further, \hat{M} and \hat{N} are projective $\hat{\Lambda}$ -lattices, and from $KM \cong KN$ we obtain $\hat{K}\hat{M} \cong \hat{K}\hat{N}$. If we can deduce from this that $\hat{M} \cong \hat{N}$, then using (30.17) we obtain $M \cong N$, as desired. Hence it suffices to prove the result when R is replaced by \hat{R} . Changing notation, we assume for the rest of the proof that R is a complete d.v.r.

Our next step will be to replace R by a larger d.v.r. S in some finite unramified extension L of K . Set

$$\Lambda_1 = S \otimes_R \Lambda, M_1 = S \otimes_R M, N_1 = S \otimes_R N,$$

so M_1 and N_1 are projective Λ_1 -lattices, and Λ_1 is an S -order in the L -algebra $L \otimes_K A$. The proof of (30.27) shows at once that

$$\overline{\Lambda}_1 / \text{rad } \overline{\Lambda}_1 \cong \bar{S} \otimes_{\bar{R}} (\overline{\Lambda} / \text{rad } \overline{\Lambda}),$$

using (30.3) and the hypothesis that $\overline{\Lambda} / \text{rad } \overline{\Lambda}$ is a separable \bar{R} -algebra.

As in the proof of (30.31), we may choose \bar{S} to be a splitting field for $\overline{\Lambda} / \text{rad } \overline{\Lambda}$ over \bar{R} , and \bar{S} can be realized as the residue class field of some d.v.r. S . Thus $\Lambda_1 / \text{rad } \Lambda_1$ is a split semisimple \bar{S} -algebra. From $KM \cong KN$ we obtain $LM_1 \cong LN_1$. If we can deduce from this that $M_1 \cong N_1$, then we obtain the desired isomorphism $M \cong N$, by (30.25). Changing notation once more, we may assume from here on that $\Lambda / \text{rad } \Lambda$ is a split semisimple \bar{R} -algebra.

Step 2. In this step, Λ is an arbitrary ring, and M is a f.g. projective left Λ -module. We put $E(M) = \text{End } M$, and view M as a $(\Lambda, E(M))$ -bimodule. Set $M' = \text{Hom}_{\Lambda}(M, \Lambda)$, a right Λ -module. By §3D (see also (29.15)), there is a two-sided $E(M)$ -homomorphism $\mu: M' \otimes_{\Lambda} M \rightarrow E(M)$, given by

$$\mu(f \otimes x) = [f, x], \text{ where } y[f, x] = f(y)x \text{ for all } x, y \in M, f \in M'.$$

The map μ is an isomorphism by Morita's Theorem 3.54, since M is a f.g. projective Λ -module.

We would like to define a map

$$\alpha: M' \otimes_{\Lambda} M \rightarrow \Lambda$$

by setting $\alpha(f \otimes m) = f(m)$ for $f \in M'$, $m \in M$. However, for $\lambda \in \Lambda$ we have

$$\alpha(f\lambda \otimes m) = (f\lambda)(m) = f(m)\lambda, \quad \alpha(f \otimes \lambda m) = f(\lambda m) = \lambda f(m),$$

so α is not well defined on $M' \otimes_{\Lambda} M$ unless Λ is commutative. But the above computation shows that there is a well defined map

$$\alpha: M' \otimes_{\Lambda} M \rightarrow \Lambda^*, \text{ given by } \alpha(f \otimes m) = \{f(m)\}^*,$$

where $*$ denotes images in Λ^* , and $\Lambda^* = \Lambda / [\Lambda, \Lambda]$ as in (32.2). There is thus a *trace map*

$$(32.6) \quad T: E(M) \xrightarrow{\mu^{-1}} M' \otimes_{\Lambda} M \xrightarrow{\alpha} \Lambda^*.$$

It is easily verified that for each f.g. projective Λ -module M , the trace map T (defined above) is additive and symmetric, and is indeed an R -homomorphism in our case. Furthermore, T behaves properly under change of rings, in the following sense: let $\varphi: \Lambda \rightarrow \Gamma$ be a ring homomorphism. Then $\Gamma \otimes_{\Lambda} M$ is a f.g. projective Γ -module, and there is a map $E(M) \rightarrow E(\Gamma \otimes M)$, given by $\theta \in E(M) \mapsto 1 \otimes \theta \in E(\Gamma \otimes M)$. On the other hand, φ induces an additive map $\varphi^*: \Lambda^* \rightarrow \Gamma^*$. Then the following diagram commutes

$$(32.7) \quad \begin{array}{ccc} E(M) & \longrightarrow & E(\Gamma \otimes_{\Lambda} M) \\ T \downarrow & & \downarrow T' \\ \Lambda^* & \xrightarrow{\varphi^*} & \Gamma^*, \end{array}$$

where T' is the trace map on $E(\Gamma \otimes M)$.

As shown in Exercise 32.1, the trace map T agrees with the usual definition when M is Λ -free and Λ is commutative. Further, for each idempotent $e \in \Lambda$, we may form the projective Λ -module $M = \Lambda e$. Each $\theta \in E(M)$ is then given by right multiplication by an element $\theta(e) \in e\Lambda e$, and (see Exercise 32.1) we have

$$(32.8) \quad T(\theta) = \theta(e)^* \in \Lambda^*.$$

We now define the *rank element* of the projective left Λ -module M as

$$r_{\Lambda}(M) = T(1_M) \in \Lambda^*,$$

where 1_M is the identity map on M . The reader will easily verify that

$$(32.9) \quad \begin{cases} r_{\Lambda}(M_1 \otimes M_2) = r_{\Lambda}(M_1) + r_{\Lambda}(M_2), \\ r_{\Lambda}(\Lambda e) = e^*, \\ r_{\Gamma}(\Gamma \otimes_{\Lambda} M) = 1 \otimes r_{\Lambda}(M) \in \Gamma^*, \end{cases}$$

where $\varphi: \Lambda \rightarrow \Gamma$ is any ring homomorphism.

Step 3. Returning to our original problem, we assume now that M and N are projective Λ -lattices such that $KM \cong KN$, and that Λ satisfies the conditions:

- (a) Λ^* is R -torsionfree, and
- (b) $\Lambda/\text{rad } \Lambda$ is a split semisimple \bar{R} -algebra.

Clearly KM and KN are f.g. projective left A -modules, so their rank elements $r_A(KM)$ and $r_A(KN)$ are defined as in Step 2. Since $KM \cong KN$ we have $r_A(KM) = r_A(KN)$. Therefore $r_{\Lambda}(M)$ and $r_{\Lambda}(N)$ have the same image in A^* ,

under the map $\Lambda^* \rightarrow K \otimes_R \Lambda^* = A^*$. Condition (a) then implies that $r_\Lambda(M) = r_\Lambda(N)$ in Λ^* .

Now let $\Lambda = \bigoplus \Lambda e_i$ be a decomposition of Λ into indecomposable left ideals, numbered so that $\Lambda e_1, \dots, \Lambda e_r$ are a full set of non-isomorphic summands. Let $\tilde{\Lambda} = \Lambda / \text{rad } \Lambda = \bigoplus \tilde{\Lambda} e_i$; this gives a decomposition of the split semisimple \bar{R} -algebra $\tilde{\Lambda}$ into simple left $\tilde{\Lambda}$ -modules, and $\tilde{\Lambda} \tilde{e}_1, \dots, \tilde{\Lambda} \tilde{e}_r$ are a basic set of simple modules (see (6.8)). Since R is now assumed to be a complete d.v.r., the K-S-A Theorem holds for Λ -lattices. But $M \mid \Lambda^{(k)}$ for some k , and therefore, for some integers $\{m_i\}$ and $\{n_i\}$,

$$M \cong \coprod_{i=1}^r (\Lambda e_i)^{(m_i)}, N \cong \coprod_{i=1}^r (\Lambda e_i)^{(n_i)}.$$

If M and N have a common summand, say Λe_1 , then we may delete it and obtain a new pair of projective Λ -lattices M' and N' such that $KM' \cong KN'$. If we can prove that $M' \cong N'$, then it will follow that $M \cong N$. Hence for the rest of the proof, we may assume that for each i , either $m_i = 0$ or $n_i = 0$. Furthermore, if $d = \text{G.C.D. } \{m_1 - n_1, \dots, m_r - n_r\}$, then $d \mid m_i$ and $d \mid n_i$ for each i , so we may write $M = M_0^{(d)}$, $N = N_0^{(d)}$, with M_0 and N_0 projective and $KM_0 \cong KN_0$. It would thus suffice to show that $M_0 \cong N_0$. Changing notation, we may hereafter assume that $d = 1$; consequently, some $\bar{m}_i - \bar{n}_i \neq 0$ in \bar{R} . To fix the notation, suppose that $\bar{m}_1 - \bar{n}_1 \neq 0$ in \bar{R} .

We now have

$$r_\Lambda(M) = \sum_{i=1}^r m_i e_i^*, \quad r_\Lambda(N) = \sum_{i=1}^r n_i e_i^*.$$

Since $r_\Lambda(M) = r_\Lambda(N)$, this gives $\sum (m_i - n_i) e_i^* = 0$ in Λ^* . The ring homomorphism $\Lambda \rightarrow \tilde{\Lambda}$ induces a map $\Lambda^* \rightarrow \tilde{\Lambda}^*$, whence $\sum (\bar{m}_i - \bar{n}_i) \tilde{e}_i^* = 0$ in $\tilde{\Lambda}^*$. Therefore we obtain

$$(32.10) \quad \sum_{i=1}^r (\bar{m}_i - \bar{n}_i) \tilde{e}_i \in [\tilde{\Lambda}, \tilde{\Lambda}].$$

But $\tilde{\Lambda} \cong \coprod_{i=1}^r M_{k_i}(\bar{R})$ by condition (b), so $[\tilde{\Lambda}, \tilde{\Lambda}]$ correspondingly decomposes into a direct sum of r subspaces. From (32.10) we deduce that

$$(\bar{m}_1 - \bar{n}_1) \tilde{e}_1 \in [M_{k_1}(\bar{R}), M_{k_1}(\bar{R})],$$

whence $(\bar{m}_1 - \bar{n}_1) \tilde{e}_1$ has zero trace. This is impossible since $\bar{m}_1 - \bar{n}_1 \neq 0$ in \bar{R} , and since the primitive idempotent $\tilde{e}_1 \in M_{k_1}(\bar{R})$ looks like $\text{diag}(1, 0, \dots, 0)$ relative to a suitable \bar{R} -basis of $M_{k_1}(\bar{R})$. This is a contradiction, and shows that the above defined M' and N' are 0. This completes the proof of Hattori's Theorem 32.5, and also of its special case (32.1) where $\Lambda = RG$.

Remark. Another proof of (32.1), in case K is sufficiently large, is given in (18.16). For the general case, a proof of (32.1) is given in (21.20) (see also CR (77.14)).

§32B. Global Case

We are now ready to state and prove the fundamental result of Swan [60]:

(32.11) Theorem. *Let R be a Dedekind domain whose quotient field K has characteristic 0. Let G be a finite group of order n , and assume that no prime divisor of n is a unit in R . Set $\Lambda = RG$, $A = KG$. Then every f.g. projective left Λ -module M is locally free, that is, M_P is Λ_P -free for each maximal ideal P of R , where the subscript denotes either localization at P or P -adic completion. Further, KM is A -free, and M/PM is $(\Lambda/P\Lambda)$ -free for each P .*

Proof. Step 1. Let M be any projective Λ -lattice; then for each P , the localization Λ_P is a projective Λ_P -lattice. Once we prove that $KM \cong A^{(t)}$ for some t , then we have

$$K \cdot M_P \cong K \cdot \Lambda_P^{(t)},$$

which implies by (32.1) that $M_P \cong \Lambda_P^{(t)}$. Further,

$$M/PM \cong M_P/PM_P \cong (\Lambda_P/P\Lambda_P)^{(t)} \cong (\Lambda/P\Lambda)^{(t)},$$

so the theorem will be established (including the fact that we can equally well use P -adic completions instead of localizations at P .) Thus, it suffices for us to prove that KM is A -free.

Step 2. Let the A -module KM afford the character μ of G . If we can show that $\mu(x) = 0$ for all $x \in G - \{1\}$, then the inner product $(\mu, 1_G)_G$ of μ with the trivial character 1_G of G will be equal to $\mu(1)/n$, where $n = |G|$. Since this inner product lies in \mathbb{Z} , we then obtain $\mu(1) = nt$ for some $t \in \mathbb{Z}$. But then $\mu = t\rho$, where ρ is the character of G afforded by the regular left module $_A A$. Since $\text{char } K = 0$, the equality $\mu = t\rho$ implies the desired isomorphism $KM \cong A^{(t)}$.

Let $x \in G - \{1\}$, and let $H = \langle x \rangle$. Then M_H is RH -projective (since Λ_H is RH -free!), and we can calculate $\mu(x)$ by letting x act on the KH -module KM_H . Thus, if the theorem is established for the case of cyclic groups, then we will have $\mu(x) = 0$ as desired, and therefore the theorem also holds for arbitrary groups.

Changing notation, suppose for the rest of the proof that $G = \langle x : x^n = 1 \rangle$ is cyclic of order n , where $n > 1$. We may write x as a product of commuting elements, each of prime power order. Hence for some rational prime p dividing n , we may write $x = yz$, where $yz = zy$, and where y has order p^k , $k > 0$, while z has order prime to p . Therefore $G = H \times E$, where $H = \langle y \rangle$ is a nontrivial p -group, and where $E = \langle z \rangle$ has order prime to p .

Now let $K' = K(\sqrt[p]{1})$; then by (15.18) K' is a splitting field for G . Let R' be the integral closure of R in K' . Since p is not a unit in R by hypothesis, there exists a maximal ideal P' of R' containing p . Let $S = (R')_{P'}$ be the localization of R' at P' ; then S is a d.v.r. whose residue class field \bar{S} has characteristic p .

The projective RG -lattice M gives rise to a projective SG -lattice $S \otimes_R M$, and we may compute $\mu(x)$ by letting x act on an S -basis of $S \otimes M$, where \otimes means \otimes_R . Let $\{e_i\}$ be a full set of primitive orthogonal idempotents of the group algebra $K'E$. Since $|E|$ is a unit in S , and E is commutative, it follows from (9.21) that each $e_i \in SE$, where SE is the integral group ring of E over S . Therefore

$$S \otimes M = \bigoplus_i e_i(S \otimes M),$$

and each summand $e_i(S \otimes M)$ is also a projective SG -module. (We are using strongly the fact that G is abelian, so each $e_i(S \otimes M)$ is indeed an SG -module.)

Now $E = \langle z \rangle$, and for each i we have $ze_i = \omega_i e_i$ for some root of unity ω_i in S . On the other hand, we may view each $e_i(S \otimes M)$ as a left SH -module, and let it afford the character ρ_i of H (over the field K'). Since $x = yz$, we obtain

$$\mu(x) = \sum_i \rho_i(y) \omega_i,$$

using the fact that z acts on $e_i(S \otimes M)$ as multiplication by ω_i . To complete the proof, we need only show that each $\rho_i(y) = 0$. But for each i , $e_i(S \otimes M)$ is a projective SH -module, and H is a p -group. Hence by (5.25) SH is a local ring, so every projective SH -module is SH -free. But then $\rho_i(y) = 0$ since $y \neq 1$. This completes the proof that $\mu(x) = 0$ for $x \in G - \{1\}$, and establishes the theorem. (The authors wish to thank Janusz for pointing out this simplified version of Step 2.)

The following corollary is an immediate consequence of Swan's Theorem and the results in §31 on genus:

(32.12) Corollary. *Keeping the notation and hypotheses of (32.11), let M be any projective left Λ -lattice. Then M lies in the genus of a free Λ -module $\Lambda^{(r)}$ for some integer r . Further,*

$$M \cong \Lambda^{(r-1)} \oplus M_0$$

for some left ideal M_0 in the genus of Λ .

Proof. Using (31.14), we obtain a decomposition of M as above, with M_0 in the genus of Λ . Then $KM_0 \cong K\Lambda$, so we may identify M_0 with a left ideal of Λ .

Swan's Theorem also implies that the ring RG cannot be decomposed into a direct sum of left ideals, since each summand would be RG -projective, and hence its R -rank would be a multiple of n . Thus RG contains no idempotent elements except 1. In this connection we prove a result due to Coleman [66]:

(32.13) Theorem. *Let R be any integral domain of characteristic 0, and let $n=|G|$. Then RG contains an idempotent $e \neq 1$ if and only if some rational prime divisor of n is a unit in R .*

Proof. If $p|n$ and $p^{-1} \in R$, let $x \in G$ have order p . Then

$$p^{-1}(1+x+\cdots+x^{p-1})$$

is an idempotent in RG distinct from 1. Conversely, let $e = \sum_{y \in G} \alpha_y y \in RG$ be idempotent, with each $\alpha_y \in R$ and where $e \neq 1$. The left regular module ${}_{RG}(RG)$ affords a matrix representation \mathbf{M} of RG . Since $e^2 = e$, the eigenvalues of the matrix $\mathbf{M}(e)$ are 0's and 1's; thus $\mathbf{M}(e)$ has trace q , where $q \in \mathbb{Z}$, $0 \leq q \leq n$. If $q=n$, then all eigenvalues of $\mathbf{M}(e)$ are 1, so $\mathbf{M}(e)$ is nonsingular. But $\{\mathbf{M}(e)\}^2 = \mathbf{M}(e^2) = \mathbf{M}(e)$, so $\mathbf{M}(e)$ is the identity matrix. Since RG acts faithfully on the left regular module, this gives $e=1$, a contradiction. Thus $q < n$, and a similar argument with $1-e$ in place of e shows that $q > 0$.

On the other hand,

$$\text{Trace of } \mathbf{M}(e) = \sum \alpha_y \cdot \text{Trace of } \mathbf{M}(y) = n\alpha_1.$$

Thus $q = n\alpha_1$ for some $\alpha_1 \in R$, so $q/n \in R$, and we have $0 < q < n$. Hence some rational prime divisor of n must be a unit in R , as claimed. The theorem also holds when $\text{char } R \neq 0$, using a slight modification of the above argument.

The preceding results on indecomposability are generalized nicely in the following result of Berman [63, Th. 5], [65], and Dress [70]:

(32.14) Theorem. *Keeping the hypotheses of (32.11), let $H \leq G$ and let R_H denote the RH -module R on which H acts trivially. Then the induced RG -module $(R_H)^G$ is indecomposable.*

Proof. When $H=1$, we have $(R_H)^G = RG$, and the result follows from Swan's Theorem. For general H , let $N|(R_H)^G$; we shall show that $|G:H|$ divides $\text{rank}_R N$, which implies the desired result. It suffices to show that for each prime p dividing $|G|$, the p -part of $|G:H|$ divides $\text{rank}_R N$. Let P be a maximal ideal of R containing p , so $\bar{R} = R/P$ has characteristic p , and let bars denote reduction mod P . Let V and W be Sylow p -subgroups of G and H , respectively, with $W \subseteq V$.

Since $N|(R_H)^G$, we have $\bar{N}|(\bar{R}_H)^G$. But $\bar{R}_H|(\bar{R}_W)^H$, so $\bar{N}|(\bar{R}_W)^G$. Therefore \bar{N}_V is a direct summand of $(\bar{R}_W)^G|_V$. By Mackey's Subgroup Theorem, the latter module is a direct sum of modules of the form $(\bar{R}_T)^V$, where T ranges over certain subgroups of V of the form ${}^xW \cap V$. Since \bar{R}_T is absolutely indecomposable and V is a p -group, Green's Theorem 19.24 shows that $(\bar{R}_T)^V$ is indecomposable. But \bar{N}_V is then a direct sum of such induced modules, and since

$$\dim_{\bar{R}} (\bar{R}_T)^V = |V:T| = |V:{}^xW \cap V|,$$

it follows that $\dim_{\bar{R}} \bar{N}_V$ is a multiple of $|V:W|$. But this dimension equals the R -rank of N , while $|V:W|$ is the p -part of $|G:H|$, so the proof is completed.

The same argument establishes Berman's result:

Let $H \leq G$, and let χ be a linear character from H into the complex field. Let $R = \mathbb{Z}[\chi]$ be the ring obtained by adjoining to \mathbb{Z} all of the character values $\{\chi(h) : h \in H\}$, and view R as RH -module with $h \in H$ acting as $\chi(h)$. Then the induced RG -module $RG \otimes_{RH} R$ is indecomposable. Indeed, the generalized permutation representation of G , afforded by this induced module, is indecomposable over every ring of algebraic integers.

§32C. Characters Afforded by Projective Lattices

Throughout this subsection, let R be a Dedekind domain whose quotient field K has characteristic 0, and let G be a finite group of order n . We shall call an element $x \in G$ *R-singular* if the order of x is not a unit in R . Our aim is to investigate the relationship between RG -lattices M and the values of their characters on R -singular elements of G . The results below are due to Swan [63].

We begin with an easy generalization of (32.11), as follows:

(32.15) Theorem. *Let μ be the character of G afforded by a projective RG -lattice M . Then $\mu(x) = 0$ for every R -singular element $x \in G$.*

Proof. Let $x \in G$ be R -singular. Then some rational prime p dividing the order of x is a non-unit in R , and p is contained in some maximal ideal P of R . Then M_P is $R_P G$ -projective, and also affords μ . Further, x is R_P -singular. Hence it suffices to prove the result when R is replaced by its localization R_P . Changing notation, assume hereafter that M is RG -projective and x is R -singular, where R is a d.v.r.

Now choose $H = \langle x \rangle$. Then the argument in Step 2 of the proof of (32.11) carries over unchanged to the present situation, and shows that $\mu(x) = 0$. This completes the proof.

In (18.26) we proved a special case of the above theorem by a different method. We showed there that if (K, R, k) is a p -modular system, with K a sufficiently large field of characteristic 0, then the K -characters afforded by projective RG -modules vanish on p -irregular elements.

We may rephrase Theorem 32.15 in terms of Grothendieck groups and projective class groups, using the terminology of §16A. Let $K_0(RG)$ be the projective class group generated by projective RG -lattices, with relations arising from direct sums. As usual*, we identify $K_0(KG)$ with the ring $\text{ch } KG$ of virtual characters of KG -modules. Then there is a homomorphism of additive groups

$$\tau: K_0(RG) \rightarrow K_0(KG) = \text{ch } KG,$$

which takes each projective RG -lattice M onto the character of G afforded by M (or, more precisely, by KM). Since each element of $K_0(RG)$ is of the form $[M] - [N]$, with M and N projective RG -lattices, Theorem 32.15 is equivalent to the assertion that for each virtual character $\chi \in \text{im } \tau$, χ vanishes at each R -singular $x \in G$.

Our next step is to show that this property characterizes the image of τ . Let $e: K_0(kG) \rightarrow G_0(KG)$ be the map defined in (18.3), and remember that $G_0(KG) = K_0(KG)$. In (18.27iii) we proved that if (K, R, k) is a p -modular system, with K a sufficiently large field of characteristic 0, then the image of e corresponds to the set of all virtual characters in $\text{ch } KG$ which vanish on the p -irregular elements of G . The main result of this subsection is a far-reaching generalization of that fact, and is as follows:

(32.16) Theorem. *The image of τ consists precisely of all $\chi \in K_0(KG)$ such that $\chi(x) = 0$ for every R -singular $x \in G$.*

Proof. Step 1. Suppose first that R is a d.v.r., K is a splitting field for G and all of its subgroups, and G is of the form $G = H \times E$, where H is a p -group and E is a p' -group, with p a non-unit in R . Then every irreducible K -character θ of G can be expressed as $\theta = \varphi\psi$ with $\varphi \in \text{Irr}(H)$, $\psi \in \text{Irr}(E)$, that is,

$$\theta(x, y) = \varphi(x)\psi(y) \text{ for } x \in H, y \in E.$$

(See Exercise 9.6.) If the KH -module V affords φ , and the KE -module W affords ψ , then the outer tensor product $V \# W$ affords θ .

Now let $\chi \in \text{ch } KG$ vanish on all R -singular elements of G ; this means in our case that $\chi(xy) = 0$ for all $x \in H - \{1\}$ and all $y \in E$. Let us express χ in the form

$$\chi = \sum \varphi_i \psi_i, \quad \varphi_i \in \text{ch } KH, \quad \psi_i \in \text{Irr } KE,$$

*Since the ring KG is semisimple, the projective class group $K_0(KG)$ coincides with the Grothendieck group $G_0(KG)$. (See §16B and Exercise 16.5.)

which is possible by virtue of the earlier remarks. Then for $x \in H - \{1\}$,

$$\sum \varphi_i(x) \psi_i = 0 \text{ in } \text{ch } KE.$$

But the $\{\psi_i\}$ are linearly independent over K , by (3.41). This shows that for each i , φ_i vanishes on $H - \{1\}$, so by Step 2 of the proof of (32.11) we see that $\varphi_i = b_i \rho$ for some $b_i \in \mathbb{Z}$, where ρ is the regular character of H . But then $\chi = \rho \psi$ for some $\psi \in \text{ch } KE$. We may write $\psi = \nu_1 - \nu_2$, where ν_i is the character of E afforded by the RE -lattice N_i , $i = 1, 2$. But N_i is RE -projective by (25.16), since $|E|$ is a unit in R . Then τ maps the element

$$[RH \# N_1] - [RH \# N_2] \in K_0(RG)$$

onto χ , which completes the proof of the theorem for this special case.

Step 2. Let R and K be as above, but let G be arbitrary. By Brauer's Induction Theorem 15.9, there exist elementary subgroups $\{H_i\}$ of G , and elements $\xi_i \in \text{ch } KH_i$, such that

$$1 = \sum \xi_i^G \text{ in } \text{ch } KG.$$

Suppose $\chi \in \text{ch } KG$ vanishes on all R -singular elements of G ; then its restriction $\chi|_{H_i}$ vanishes on all R -singular elements of H_i . However,

$$\chi = \sum \chi \cdot \xi_i^G = \sum (\chi|_{H_i} \cdot \xi_i)^G,$$

by (15.5). Since $\chi|_{H_i} \cdot \xi_i$ vanishes on all R -singular elements of H_i , and since each elementary group is of the form described in Step 1, it follows that for each i ,

$$\chi|_{H_i} \cdot \xi_i \in \text{im } \tau_i, \text{ where } \tau_i: K_0(RH_i) \rightarrow \text{ch } KH_i.$$

But then $\chi \in \text{im } \tau$, since the following diagram is commutative:

$$\begin{array}{ccc} K_0(RH_i) & \xrightarrow{\tau_i} & \text{ch } KH_i \\ \text{ind}_{H_i}^G \downarrow & & \downarrow \text{ind}_H^G \\ K_0(RG) & \xrightarrow{\tau} & \text{ch } KG. \end{array}$$

This completes the proof of the theorem in the special case where K is a splitting field for G and its subgroups, and R is a d.v.r. Another proof, for this special case, is given in (18.27ii).

Step 3. We assume next that R is a d.v.r., but drop the hypothesis that K be a splitting field. Let \hat{R} , \hat{K} , etc., be completions. The ring inclusions $R \rightarrow \hat{R}$, $K \rightarrow \hat{K}$, give rise to a commutative diagram

$$\begin{array}{ccc} K_0(RG) & \xrightarrow{\tau} & K_0(KG) \\ \downarrow & & \downarrow \\ K_0(\hat{R}G) & \xrightarrow{\hat{\tau}} & K_0(\hat{K}G). \end{array}$$

Suppose that the elements $a \in K_0(KG)$ and $b \in K_0(\hat{R}G)$ have the same image in $K_0(\hat{K}G)$. Using Exercise 16.4 twice, we may write

$$a = [V] - [(KG)^{(r)}], \quad b = [X] - [(\hat{R}G)^{(r)}],$$

for some KG -module V and some projective $\hat{R}G$ -lattice X , with the same choice of r for both a and b . Then

$$[\hat{K}V] = [\hat{K}X] \text{ in } K_0(\hat{K}G),$$

so $\hat{K}V \cong \hat{K}X$. By (30.10), there exists an RG -lattice M for which $X \cong M$. By virtue of (30.11), M is RG -projective, and so both a and b are images of the element $[M] - [(RG)^{(r)}] \in K_0(RG)$.

Now let $\chi \in \text{ch } KG$ vanish on all R -singular elements of G . Then its image $\hat{\chi} \in \text{ch } \hat{K}G$ has the same property, so if the theorem is known to be true for the case of complete d.v.r.'s, it follows that $\hat{\chi} \in \text{im } \hat{\tau}$. But then $\chi \in \text{im } \tau$ by the preceding remarks.

For the rest of this Step, we may assume that R is a complete d.v.r. As in Step 2 of the proof of (32.11), we can choose a splitting field K' containing K , with a d.v.r. S whose residue class field \bar{S} contains the residue class field \bar{R} of R . There is a commutative diagram

$$\begin{array}{ccc} K_0(RG) & \xrightarrow{\tau} & \text{ch } KG \\ \alpha \downarrow & & \downarrow \beta \\ K_0(SG) & \xrightarrow{\tau'} & \text{ch } K'G, \end{array}$$

and by Step 2 we have $\beta(\chi) = \tau'(\xi')$ for some $\xi' \in K_0(SG)$.

Next, by (16.10) we have $\text{ch } KG \cong G_0(KG)$, and therefore the map β is monic by Exercise 16.6. We show next that the map α is a split monomorphism, and so the image of α is a \mathbb{Z} -pure submodule of $K_0(SG)$. To prove that

α is a split monomorphism, let us consider the diagram

$$\begin{array}{ccccc} K_0(RG) & \longrightarrow & K_0(\bar{R}G) & \longrightarrow & K_0(\bar{R}G/\text{rad } \bar{R}G) \\ \alpha \downarrow & & \downarrow & & \bar{\alpha} \downarrow \\ K_0(SG) & \longrightarrow & K_0(\bar{S}G) & \longrightarrow & K_0(\bar{S}G/\text{rad } \bar{S}G). \end{array}$$

Each horizontal map is an isomorphism, by (30.3). Further, $\bar{\alpha}$ is a split monomorphism by (16.22). Hence α is also split, as claimed. Therefore $\text{im } \alpha$ is \mathbb{Z} -pure in $K_0(SG)$, by §4D.

Now let $\rho: K_0(SG) \rightarrow K_0(RG)$, $\sigma: \text{ch } K'G \rightarrow \text{ch } KG$, be the restriction maps. It is easily verified that $\tau\rho = \sigma\tau'$, since these maps agree on SG , and hence on any summand of a free SG -module. Put $\xi = \rho(\xi') \in K_0(RG)$. Then

$$\tau'\alpha(\xi) = \beta\tau(\rho\xi') = \beta\sigma\tau'(\xi') = \beta\sigma\beta(\chi) = m\beta(\chi) = \tau'(m\xi'),$$

where $m = \dim_K K'$. But then $\alpha(\xi) = m\xi'$, since τ' is monic by Hattori's Theorem 32.5. Therefore $m\xi' \in \text{im } \alpha$, and so also $\xi' \in \text{im } \alpha$, because $\text{im } \alpha$ is \mathbb{Z} -pure in $K_0(SG)$. Writing $\xi' = \alpha(\eta)$, we obtain

$$\beta\tau(\eta) = \tau'\alpha(\eta) = \tau'(\xi') = \beta(\chi),$$

so $\chi = \tau(\eta)$. This completes the proof of the theorem for the case where R is any d.v.r.

Step 4. It remains for us to show how to pass from the local case to the general case. Let $\chi \in \text{ch } KG$ vanish on all R -singular elements of G , where now R is an arbitrary Dedekind domain. Let $\{P_1, \dots, P_t\}$ be the set of maximal ideals of R which contain $|G|$. The previous step shows that for each i , $1 \leq i \leq t$, there exists a projective $(R_{P_i}G)$ -lattice M_i such that

$$\tau_i \left\{ [M_i] - \left[(R_{P_i}G)^{(q)} \right] \right\} = \chi,$$

with q independent of i . Here, τ_i maps $K_0(R_{P_i}G)$ into $K_0(KG)$. The KG -modules $\{KM_i : 1 \leq i \leq t\}$ all have the same character, so they are mutually isomorphic. By (4.21), we can find an RG -lattice M such that

$$M_{P_i} \cong M_i, \quad 1 \leq i \leq t.$$

Then M is RG -projective by (25.16), and τ maps $[M] - [(RG)^{(q)}]$ onto χ . This proves the theorem.

We shall next sharpen Theorem 32.16 so that it deals with ordinary characters rather than virtual characters. Let $\text{ch}^+ KG$ be the semigroup

consisting of all characters of G afforded by KG -modules, and let $K_0^+(RG)$ be the semigroup consisting of all classes $[M]$, where M ranges over all projective RG -lattices. We might expect that each $\chi \in \text{ch}^+ KG$, which vanishes at all R -singular elements of G , is of the form $\chi = \tau[M]$ for some M . However, this need not be the case even when R is a complete d.v.r. (see Exercise 32.2).

When the group G is suitably restricted, however, the hoped-for result is true. The following theorem is due to Swan [63]:

(32.17) Theorem. *Suppose that the group G is p -solvable for each prime factor p of n which is a non-unit in R . Then for each KG -module V whose character χ vanishes on all R -singular elements of G , there exists a projective RG -lattice M such that $V \cong KM$.*

Proof. Let us first treat the case where R is a complete d.v.r. in which p is a non-unit, and K is a splitting field for G and its subgroups. Using the notation of (17.6), let $\{\eta^1, \dots, \eta^r\}$ be the principal indecomposable Brauer characters of G . Then

$$\chi = \sum_{i=1}^r m_i \eta^i$$

for some integers $m_i \in \mathbb{Z}$, by (32.16). On the other hand, since G is p -solvable, each decomposition number d_{ij} is 0 or 1 (see (22.7)). Thus for each i , $1 \leq i \leq r$, some irreducible K -character ζ^j occurs with multiplicity 1 in η^i , and does not occur in any η^l for $l \neq i$. But then $m_i \geq 0$, since otherwise ζ^j would occur with negative multiplicity in the character χ . It follows that

$$V \cong KM, \text{ where } M = \coprod_{i=1}^r U_i^{(m_i)},$$

which completes the proof in this case.

Still assuming R complete, we drop the hypothesis that K be a splitting field. Choose a finite extension field K' of K , with d.v.r. R' , such that K' is a splitting field. The previous discussion shows that

$$K'V \cong K'M' \text{ for some projective } R'G\text{-lattice } M'.$$

Let $M = M'|_{RG}$, so $M \in \mathcal{P}(RG)$, and $KM = KM' = KR'M' = K'M'$, with the last equality true because $KR' = K'$. This gives

$$V^{(m)} \cong KM \text{ as } KG\text{-modules, where } m = \dim_K K'.$$

On the other hand, (32.16) gives

$$[V] = [KN_1] - [KN_2] \text{ in } \text{ch } KG,$$

with $N_1, N_2 \in \mathcal{P}(RG)$. Therefore

$$KM \oplus KN_2^{(m)} \cong KN_1^{(m)},$$

so by Hattori's Theorem, $M \oplus N_2^{(m)} \cong N_1^{(m)}$. The K-S-A Theorem then yields $M \cong L^{(m)}$ for some $L \in \mathcal{P}(RG)$, and therefore $V \cong KL$. This completes the proof for R any complete d.v.r.

If R is any d.v.r., not necessarily complete, let \hat{R} be its completion. Then $\hat{V} \cong \hat{K}X$ for some $X \in \mathcal{P}(\hat{R}G)$, so by (30.10), $V \cong KM$ where M is an RG -lattice for which $\hat{M} \cong X$. Thus $M \in \mathcal{P}(RG)$, and again we are through.

Finally, the case of arbitrary Dedekind domains is treated just as in Step 4 of the proof of (32.16), and so we have established Theorem 32.17.

§32. Exercises

1. Let $\mathcal{P}(\Lambda)$ be the category of f.g. projective left Λ -modules over an arbitrary ring Λ , and let Λ^* be defined as in (32.2). For each $M \in \mathcal{P}(\Lambda)$, let

$$E(M) = \text{End}_\Lambda(M), M' = \text{Hom}_\Lambda(M, \Lambda) = \text{right } \Lambda\text{-module},$$

where $E(M)$ acts from the right on M . Let

$$\mu: M' \otimes_\Lambda M \rightarrow E(M)$$

be the two-sided $E(M)$ -isomorphism defined as in §3D, or in Step 2 of the proof of (32.5). Let

$$T: E(M) \xrightarrow{\mu^{-1}} M' \otimes_\Lambda M \xrightarrow{\alpha} \Lambda^*$$

be the trace map defined by composition, where $\alpha(f \otimes m) = f(m)^*$.

- (i) Suppose that $M = \bigoplus_{i=1}^k \Lambda m_i$ is Λ -free. For $\theta \in E(M)$, let

$$m_i \theta = \sum_{j=1}^k a_{ij} m_j, a_{ij} \in \Lambda.$$

Show that $T(\theta) = (\sum a_{jj})^* \in \Lambda^*$. Thus T is the usual trace map when Λ is commutative.

- (ii) Let $e \in \Lambda$ be idempotent, and let $M = \Lambda e \in \mathcal{P}(\Lambda)$. Show that each $\theta \in E(M)$ is given by right multiplication by some element $\theta(e) \in e\Lambda e$, and that $T(\theta) = \{\theta(e)\}^*$.

- (iii) Let $M \in \mathcal{P}(\Lambda)$, and choose $N \in \mathcal{P}(\Lambda)$ so that $M \oplus N \cong \Lambda^{(r)}$ for some r . Each $\theta \in E(M)$ extends to an element $\theta_1 \in \text{End}_\Lambda(\Lambda^{(r)})$ by letting θ_1 vanish on N . Represent θ_1 as an $r \times r$ matrix over Λ , and show that $T(\theta)$ is precisely the trace of this matrix, viewed as element of Λ^* .

[Hint: In (i), we have (using notation of §3D)

$$m\theta = \sum (m, f_j)m_j$$

for some elements $f_j \in M'$, so $a_{ij} = (m_i, f_j)$ for each i . Then

$$m_i \theta = \sum_j (m_i, f_j) m_j = m_i \Sigma [f_j, m_j]$$

implies that $\theta = \mu\{\Sigma f_j \otimes m_j\}$. Therefore

$$T(\theta) = (\alpha \mu^{-1})(\theta) = \alpha \{\Sigma f_j \otimes m_j\} = \Sigma (m_j, f_j)^* = \Sigma a_{jj}^*.$$

For (ii), define $f \in M'$ by $(m, f) = m\theta(e)$, $m \in M$. Then $\mu(f \otimes e) = \theta$, so

$$T(\theta) = \alpha(f \otimes e) = (e, f)^* = \{e\theta(e)\}^* = \{\theta(e)\}^*.$$

2. Show that the conclusion of Theorem 32.17 does not hold for the case where R is the ring \hat{Z}_5 of 5-adic integers and $G = S_5$, which is *not* 5-solvable.

[Hint: Suppose the conclusion does hold, and let $x = (12345) \in G$. Then τ maps $K_0^+(RG)$ onto the semigroup

$$T = \{\chi \in \text{ch}^+ KG : \chi(x) = 0\}.$$

Since $K_0^+(RG)$ is a free semigroup on 7 generators and τ is monic, the image T is also free. Write $\chi = \sum_{i=1}^7 a_i \xi^i$, $a_i \in \mathbb{Z}^+$, where the $\{\xi^i\}$ are the irreducible \mathbb{Q} -characters of G (see §9D). Then

$$\chi(x) = 0 \text{ if and only if } a_1 + a_2 + a_7 = a_3 + a_4.$$

Thus $T = \{(a_1, \dots, a_7) \in (\mathbb{Z}^+)^7 : a_1 + a_2 + a_7 = a_3 + a_4\}$. But T requires at least 8 generators, which gives a contradiction.]

§33. FINITE REPRESENTATION TYPE

Throughout this section, Λ denotes an R -order in a separable K -algebra A , where K is a global field or the completion of a global field, and R is a Dedekind domain with quotient field K . As usual, we assume that $R \neq K$. These hypotheses imply that R/\mathfrak{a} is finite for every nonzero ideal \mathfrak{a} of R , and that the Jordan-Zassenhaus Theorem holds for Λ -lattices (see introduction to §31A). Let $n(\Lambda)$ denote the number of isomorphism classes of indecomposable left Λ -lattices. We say that Λ has *finite representation type* if $n(\Lambda)$ is finite, and *infinite representation type* otherwise. Given an R -order Λ , one would like to know all indecomposable Λ -lattices (up to isomorphism), since every Λ -lattice is expressible as a finite direct sum of indecomposable lattices. As a first approximation to solving this problem, we may try to check whether $n(\Lambda)$ is finite. Once this is done, there remains the more difficult problem of finding a full set of indecomposable Λ -lattices. We devote this section to a discussion of the first of these questions.

(Let us comment briefly about our restrictions on the field K and the algebra A . These hypotheses are imposed in order to guarantee that the Jordan-Zassenhaus Theorem hold true for Λ -lattices (see §24). In more general situations, where K is not a global field or where A is not a separable K -algebra, it may happen that the Jordan-Zassenhaus Theorem is not valid for Λ -lattices. In such cases, it is easily seen that $n(\Lambda)$ must be infinite. To prove this, suppose that $n(\Lambda)$ is finite. A Λ -lattice M of R -rank t is a direct sum of at most t indecomposable summands. If $n(\Lambda)$ is finite, there are finitely many isomorphism classes of such indecomposable summands, and hence only finitely many classes of M 's. Thus, if the Jordan-Zassenhaus Theorem fails for Λ -lattices, then $n(\Lambda)$ is necessarily infinite. Therefore, in investigating whether $n(\Lambda)$ is finite, it is reasonable to restrict our attention to those cases where we know in advance that the Jordan-Zassenhaus Theorem is valid.)

§33A. Jones' Theorem. Jacobinski's Criterion for Group Rings

In this subsection we shall show that the question, as to whether Λ has finite representation type, can be decided by answering the local question at some finite set of primes P of R . For each maximal ideal P of R , let the subscript P denote *completion*, rather than localization. As in (31.1), let

$$S(\Lambda) = \{P : \Lambda_P \neq \text{maximal } R_P\text{-order in } A_P\},$$

so $S(\Lambda)$ is a finite set. Further, $S(\Lambda) = \emptyset$ if and only if Λ is a maximal order. This latter case is completely settled by:

(33.1) Proposition. *Let Λ be any hereditary or maximal order. Then the number $n(\Lambda)$ of non-isomorphic indecomposable Λ -lattices is finite, and equals the number of isomorphism classes of full Λ -lattices in simple A -modules.*

Proof. This follows from (26.12) and the Jordan-Zassenhaus Theorem.

For the rest of the discussion, we may assume that $S(\Lambda) \neq \emptyset$. Our main result, due to Jones [63a], is as follows:

(33.2) Theorem. *Let Λ be an R -order in a f.d. separable K -algebra A , where K is a global field. Let $n(\Lambda)$ be the number of non-isomorphic indecomposable left Λ -lattices, and let $S(\Lambda)$ be as above. Then*

$$n(\Lambda) < \infty \Leftrightarrow n(\Lambda_P) < \infty \text{ for each } P \in S(\Lambda).$$

Proof. Step 1. If $n(\Lambda) < \infty$, let $\{M_i : 1 \leq i \leq n\}$ be a full set of non-isomorphic indecomposable left Λ -lattices. Let P be any maximal ideal of R , and let X be an indecomposable Λ_P -lattice. We shall show that $X | (M_i)_P$ for

some i , whence $n(\Lambda_P) < \infty$ by the K-S-A Theorem. To prove our assertion, first choose an A_P -module Y_0 such that $K_P X \oplus Y_0$ is A_P -free, say equal to F_P for some f.g. free A -module F . By (23.15) we may write $Y_0 = K_P Y$ for some full Λ_P -lattice Y in Y_0 . Therefore

$$K_P(X \oplus Y) \cong K_P F \text{ as } A_P\text{-modules.}$$

Let us treat this isomorphism as an identification, and now set $L = (X \oplus Y) \cap F$. Then L is a lattice over the localization of Λ at P , and $L_P = X \oplus Y$ by the proof of Heller's Theorem 30.18. But this L is the localization of some Λ -lattice M , by (23.14), and thus we have $X \oplus Y \cong M_P$. Since M is a direct sum of M_i 's with various multiplicities, we deduce from (6.16) that $X|(M_i)_P$ for some i . This completes the proof that if $n(\Lambda) < \infty$, then $n(\Lambda_P) < \infty$ for each P .

Step 2. Suppose now that $n(\Lambda_P) = n_P < \infty$ for each $P \in S(\Lambda)$. As pointed above, $n(\Lambda) < \infty$ if $S(\Lambda)$ is empty, so assume for the rest of the proof that $S(\Lambda)$ is not empty. For each $P \in S(\Lambda)$, let $\{X_1^P, \dots, X_{n_P}^P\}$ be a full set of non-isomorphic indecomposable Λ_P -lattices, and let $n = \sum_{P \in S(\Lambda)} n_P$. Let C denote the additive semigroup of n -tuples of non-negative integers, and partially order C by writing $(a_i) \leq (b_i)$ in C if $a_i \leq b_i$ for $1 \leq i \leq n$. We shall show in Step 3 that relative to this partial order, every non-empty subset of C has only a finite number of minimal elements. Let us take this for granted for the moment, and proceed with the argument.

Let M be a Λ -lattice, and let $r(j, P)$ denote the multiplicity of X_j^P as a direct summand of M_P , for $1 \leq j \leq n_P$ and all $P \in S(\Lambda)$. Let $\theta(M)$ denote the ordered n -tuple in C whose entries are the non-negative integers $\{r(j, P)\}$. Let C' be the subsemigroup of C consisting of all elements $\theta(M)$, where M ranges over all Λ -lattices, and partially order C' according to the ordering on C . If N is a Λ -lattice such that $N|M$, then clearly $\theta(N) \leq \theta(M)$, with equality if and only if $M \vee N$. Conversely, let N be a Λ -lattice such that $\theta(N) < \theta(M)$. By (31.12) we have $M \cong N \oplus L$ for some N' in the genus of N , and some Λ -lattice L . Note that $\theta(N') = \theta(N)$, and thus $\theta(M) = \theta(N) + \theta(L)$.

It follows at once that a Λ -lattice M is indecomposable if and only if $\theta(M)$ is a minimal element of the partially ordered semigroup C' . In Step 3, we shall show that there are only finitely many such minimal elements. Further, given such an element $\theta_0 \in C'$, the condition that $\theta(M) = \theta_0$ places an upper bound on the R -rank of M ; hence by the Jordan-Zassenhaus Theorem, the number of non-isomorphic M 's with $\theta(M) = \theta_0$ is finite. Once we know that the number of minimal element θ_0 in C' is finite, we will have shown that

$$n(\Lambda_P) < \infty \text{ for all } P \in S(\Lambda) \Rightarrow n(\Lambda) < \infty,$$

as desired.

Step 3. Let us prove finally that each non-empty subset D of C has a finite number of minimal elements, relative to the ordering introduced above. We use induction on n , where $n = \sum n_p$ as above. The result is obvious when $n = 1$, so let $n > 1$, and assume the result true at $n - 1$. Let (d_1, \dots, d_n) be some fixed element of D . Put

$$D(m, i) = \{(a_1, \dots, a_n) \in D : a_i = m\}, \quad 1 \leq i \leq n, \quad m \in \mathbb{Z}, \quad m \geq 0.$$

For each m and i , the partially ordered set $D(m, i)$ has finitely many minimal elements by the induction hypothesis (except that possibly $D(m, i)$ may be empty). Let

$$\mathfrak{M} = \bigcup_{i=1}^n \bigcup_{m=0}^{d_i} \{\text{set of all minimal elements of } D(m, i)\},$$

so \mathfrak{M} is a finite set. We claim that \mathfrak{M} contains every minimal element (b_1, \dots, b_n) of D . Surely it is false that

$$(d_1, \dots, d_n) < (b_1, \dots, b_n),$$

and therefore $b_i \leq d_i$ for some i , $1 \leq i \leq n$. But then $(b_1, \dots, b_n) \in D(b_i, i)$ for that choice of i , and so (b_1, \dots, b_n) is a minimal element in $D(b_i, i)$. Since $0 \leq b_i \leq d_i$, this shows that $(b_1, \dots, b_n) \in \mathfrak{M}$, as claimed, and the proof is finished.

As special cases of Jones' Theorem, we have:

(33.3) Corollary. *Let R be a d.v.r. in a global field K , and let \hat{R} be its P -adic completion, where P is the maximal ideal of R . Let Λ be an R -order in a separable K -algebra. Then Λ has finite representation type if and only if $\hat{R} \otimes_R \Lambda$ has finite representation type.*

(33.3a) Corollary. *Let G be a finite group, and let R be any Dedekind domain with quotient field K , where $\text{char } K \nmid |G|$. Then $n(RG) < \infty$ if and only if $n(R_P G) < \infty$ for each P containing $|G|$.*

For the case where R is local, the problem as to whether $n(RG) < \infty$ can always be reduced to the situation in which G is a p -group. This follows from an easy result:

(33.4) Proposition. *Let R be a complete d.v.r., and let $H \leq G$ be finite groups such that $|G : H|$ is a unit in R . Then $n(RG) < \infty$ if and only if $n(RH) < \infty$. In particular, this conclusion holds whenever H is a Sylow p -subgroup of G , where p is a non-unit in R .*

Proof. For any RH -lattice M , we have $M|(M^G)_H$, since

$$M^G = 1 \otimes M \oplus \{g_2 \otimes M \oplus \cdots \oplus g_n \otimes M\},$$

where $G = \dot{\cup}_{i=1}^n g_i H$, $g_1 = 1$. (This does not require the hypothesis that $n \in R$.)

On the other hand, for any RG -lattice L we claim that

$$(33.5) \quad L|(L_H)^G \text{ if } |G:H| \in R.$$

Indeed, $(L_H)^G = \oplus(g_i \otimes L)$, and we define R -linear maps φ, ψ by

$$\begin{aligned} \varphi: (L_H)^G &\rightarrow L, \quad \varphi(\xi \otimes x) = \xi x, \quad \xi \in RG, \quad x \in L, \\ \psi: L &\rightarrow (L_H)^G, \quad \psi(x) = n^{-1} \sum_{i=1}^n g_i \otimes g_i^{-1} x, \quad x \in L. \end{aligned}$$

It is easily checked that ψ is independent of the choice of representatives of the cosets of H in G , and that φ, ψ are RG -homomorphisms such that $\varphi\psi$ is the identity map on L . This establishes (33.5). (Analogous results were given in (19.3a) and (19.5ix).)

Now let R be a complete d.v.r., so the K-S-A Theorem holds for RG - and RH -lattices, and assume that $|G:H| \in R$. If $n(RH) < \infty$, then also $n(RG) < \infty$ by (33.5). The converse holds by the first paragraph of the proof, and the proposition is established.

Suppose next that H is a p -group, and R is a complete d.v.r. in which p is a non-unit. The finiteness of $n(RH)$ depends on the nature of R as well as on the structure of H . If H is non-cyclic, or cyclic of order greater than p^2 , then for every R we have $n(RH) = \infty$. This follows from the work of Heller-Reiner [63] and Berman-Gudivok [64]. It is also a consequence of a more general result due to Dade (see §33B), which applies to arbitrary orders, which are not necessarily integral group rings.

It remains to investigate the case where H is cyclic of order p or p^2 , and here the answer depends on R . For the ring of p -adic integers R , we shall prove in (34.31) and (34.32) that

$$\begin{aligned} n(RH) &= 3 \text{ if } H \text{ is cyclic of order } p, \\ n(RH) &= 4p + 1 \text{ if } H \text{ is cyclic of order } p^2, \end{aligned}$$

and indeed we shall find all indecomposable RH -lattices in both cases. These results are due to Heller-Reiner [62] and Berman-Gudivok [64], independently. Combining all of the above facts with Jones' Theorem, we obtain:

(33.6) Theorem. *Let G be a finite group. Then $\mathbb{Z}G$ has finite representation type if and only if for each prime p dividing $|G|$, the Sylow p -subgroups of G are cyclic of order p or p^2 .*

Proof. For $\Lambda = \mathbb{Z}G$, the set $S(\Lambda)$ consists of all p 's which divide $|G|$. By Jones' Theorem, $n(\Lambda)$ is finite if and only if $n(\Lambda_p)$ is finite for each $p \in S(\Lambda)$. Here, $\Lambda_p = \mathbb{Z}_p G$ where \mathbb{Z}_p is the ring of p -adic integers. If H is a Sylow p -subgroup of G , then by (33.4) $n(\Lambda_p)$ is finite if and only if $n(\mathbb{Z}_p H)$ is finite. The theorem therefore follows from the above remarks. (Berman [66] gave another proof, somewhat more complicated, which did not use Jones' Theorem.)

To conclude, we state without proof a general result due to Jacobinski [67]:

(33.7) Theorem. *Let $R = \text{alg. int. } \{K\}$, where K is an algebraic number field. For each prime p dividing $|G|$, let P range over all maximal ideals of R containing p , and let $e(P)$ denote the ramification index of P for the extension K/\mathbb{Q} (see §4B). Let S_p be a Sylow p -subgroup of G . Then RG has finite representation type if and only if for each P , one of the following conditions is satisfied:*

- (i) $e(P) = 1$, and S_p is cyclic of order p or p^2 .
- (ii) $e(P) \leq 2$, $p > 3$, and S_p is cyclic of order p .
- (iii) $e(P) \leq 3$, $p = 3$, and S_p is cyclic of order p .

Many partial results of this nature were obtained earlier by various authors; see especially Gudivok [67] and Kneser [66].

§33B. Dade's Theorem

Let Λ be an R -order in a f.d. K -algebra A . We shall show that Λ has infinite representation type if A splits into a direct sum of at least four two-sided ideals, but the order Λ itself does not decompose into proper two-sided ideals. This result will imply, for example, that an integral group ring $\mathbb{Z}G$ of a p -group G has infinite representation type if G is non-cyclic, or cyclic of order $>p^2$.

The main result of this subsection is as follows:

(33.8) Theorem (Dade [63]). *Let Λ be an R -order in a f.d. K -algebra A and let $A = A_1 \oplus A_2 \oplus A_3 \oplus A_4$, where each A_i is a nonzero two-sided ideal of A . Suppose that for some maximal ideal P of R , the ring $\Lambda/P\Lambda$ is local. Then there are infinitely many non-isomorphic indecomposable left Λ -lattices, and indeed there exists a set of such lattices whose R -ranks tend toward infinity.*

Proof. Step 1. Replacing R by its localization R_P does not affect the hypotheses. Suppose that the theorem holds true in this local case, so $n(\Lambda_P) = \infty$. Each indecomposable Λ_P -lattice is the localization at P of some

indecomposable Λ -lattice by (23.14), whence $n(\Lambda) = \infty$. Further, for each indecomposable Λ -lattice M , the R -rank of M equals the R_P -rank of M_P . Hence it suffices to establish the theorem in the local case. Changing notation, assume from now on that R is a d.v.r. with maximal ideal P . Set

$$\bar{R} = R/P, \bar{\Lambda} = \Lambda/P\Lambda, D = \bar{\Lambda}/\text{rad } \bar{\Lambda}.$$

Then $\bar{\Lambda}$ is a f.d. \bar{R} -algebra, and D is a skewfield since $\bar{\Lambda}$ is by hypothesis a local ring (see (5.21)). Let $J = \text{rad } \Lambda$; from (30.3) we have

$$(33.9) \quad \Lambda/J \cong D, J^m \subseteq P\Lambda \subseteq J \subseteq \Lambda$$

for some $m \geq 1$.

Step 2. Let $A = \bigoplus_{i=1}^4 A_i$, and let $\pi_i: A \rightarrow A_i$ be the i -th projection map, so π_i is a K -algebra homomorphism. We put

$$\Lambda' = \bigoplus_{i=1}^4 \pi_i(\Lambda), J' = \bigoplus_{i=1}^4 \pi_i(J), \Lambda_0 = \Lambda + J'.$$

Clearly $\Lambda \subseteq \Lambda'$, and Λ_0 is an R -order in A such that $\Lambda \subseteq \Lambda_0 \subseteq \Lambda'$. We shall show that Λ_0 has infinite representation type, and indeed that there exist indecomposable Λ_0 -lattices of arbitrarily large R -rank. The same will then hold true for Λ , since every Λ_0 -lattice is also a Λ -lattice, and since for each pair M and N of Λ -lattices we have

$$\text{Hom}_{\Lambda_0}(M, N) = \text{Hom}_{\Lambda}(M, N)$$

(see Exercise 23.2). Hence, non-isomorphic indecomposable Λ_0 -lattices are also non-isomorphic indecomposable Λ -lattices.

Now J' is a Λ' -lattice containing J , and $J' \cap \Lambda$ is a two-sided ideal of Λ containing J . Thus $J' \cap \Lambda$ is either J or Λ , and the latter alternative is impossible since $1 \notin J'$. Thus $J' \cap \Lambda = J$, so

$$\Lambda_0/J' = (\Lambda + J')/J' \cong \Lambda/J \cong D.$$

Further

$$\Lambda_0/J' \subseteq \Lambda'/J' = \bigoplus_{i=1}^4 \pi_i(\Lambda)/\pi_i(J) \cong D^{(4)}.$$

Note that $\pi_i(\Lambda)/\pi_i(J)$ is a nonzero homomorphic image of Λ/J , hence equals D . The embedding of Λ_0/J' in Λ'/J' is just the diagonal map $D \rightarrow D^{(4)}$, given by $d \in D \mapsto (d, d, d, d) \in D^{(4)}$, once we identify Λ_0/J' with D , and Λ'/J' with $D^{(4)}$.

Step 3. For an arbitrary positive integer n , set $V=D[x]/(x^n)$, an n -dimensional left D -space on which x acts so that $x^n=0$, and x commutes with the elements of D . We form the $4n$ -dimensional D -space

$$V^{(4)} = D^{(4)}[x]/(x^n),$$

viewed as left Λ' -module by means of the ring homomorphism $\Lambda' \rightarrow \Lambda'/J' \cong D^{(4)}$. We now define

$$W = \{v \in V^{(4)} : v = (a, b, a+b, a+xb) \text{ for some } a, b \in V\}.$$

Then the map $\Lambda_0 \rightarrow \Lambda_0/J' \cong D$ makes W into a left Λ_0 -module, and W is a Λ_0 -submodule of $V^{(4)}$ such that $\Lambda' \cdot W = V^{(4)}$. Let M' be the free Λ' -module defined by $M' = \Lambda'[x]/(x^n)$; then there is a Λ' -homomorphism

$$\varphi: M' \rightarrow M'/J'M' = V^{(4)}.$$

We set $M = \varphi^{-1}(W)$, so M is a Λ_0 -sublattice of the Λ' -lattice M' . From $\Lambda' \cdot W = V^{(4)}$ we obtain

$$M' = \Lambda' M + J' M'.$$

Now Λ'/J' is semisimple, and $(J')^m \subseteq PJ'$ by (33.9), so $J' = \text{rad } \Lambda'$. Therefore $M' = \Lambda' M$ by Nakayama's Lemma. Thus we have diagrams

$$\begin{array}{ccc} \Lambda_0 \subseteq \Lambda' & & M \subseteq M' = \Lambda' \cdot M \\ \downarrow & & \downarrow \varphi \\ D \subseteq D^{(4)}, & & W \subseteq V^{(4)} = D^{(4)}W, \end{array}$$

where the vertical arrows are reduction mod J' .

We shall show that for each n , the Λ_0 -lattice M is indecomposable. Since

$$R\text{-rank of } M = \dim_K KM = n \cdot \dim_K A,$$

it will then follow that Λ_0 has indecomposables of arbitrarily large rank, which will imply the theorem. To prove M indecomposable, suppose to the contrary that there is a non-trivial Λ_0 -decomposition of M . This gives rise to a non-trivial decomposition of $\Lambda' M$, and thence (after an easy calculation) to non-trivial decompositions of W and $V^{(4)}$ which are consistent with the embedding of W into $V^{(4)}$.

Suppose now that \bar{f} is a non-trivial idempotent endomorphism of $V^{(4)}$ as $D^{(4)}$ -module, such that $\bar{f}(W) \subseteq W$. We may write

$$\bar{f} = (f_1, f_2, f_3, f_4), \text{ with each } f_i \in \text{End}_D(V),$$

noting that the off-diagonal terms are zero since \bar{f} commutes with the action

of $D^{(4)}$. Let $a, b \in V$; from $\bar{f}(W) \subseteq W$ we obtain

$$\bar{f}(a, 0, a, a) = (f_1 a, 0, f_3 a, f_4 a) \in W,$$

so

$$f_1 = f_3 = f_4.$$

Also

$$\bar{f}(0, b, b, xb) = (0, f_2 b, f_3 b, f_4(xb)) \in W,$$

so

$$f_2 = f_3, f_4(xb) = xf_2(b).$$

Hence

$$\bar{f} = (h, h, h, h), \text{ where } h \in \text{End}_{D[x]}(V), \text{ and } h^2 = h$$

(because $\bar{f}^2 = \bar{f}$). Since $V = D[x]/(x^n)$, its $D[x]$ -endomorphism ring is precisely the local ring $D[x]/(x^n)$. Thus $h=0$ or 1, which contradicts the hypothesis that $\bar{f} \neq 0$ or 1. This completes the proof of Dade's Theorem.

As a consequence of the theorem, we deduce the following corollary, first proved by other methods by Heller-Reiner [63] and Berman-Gudivok [64]:

(33.10) Corollary. *Let p be prime, and let G be a p -group. Then the integral group ring $\mathbb{Z}G$ is of infinite representation type if G is non-cyclic, or if G is cyclic and $|G| > p^2$.*

Proof. Let $\Lambda = \mathbb{Z}G$, $A = QG$, so $\Lambda/p\Lambda$ is local by (5.25). If G is cyclic of order p^k , then A splits into a direct sum of $k+1$ Wedderburn components, by Exercise 21.1. Hence if $k > 2$, there are at least 4 simple components of A , so Λ has infinite representation type by Dade's Theorem.

On the other hand, if G is a non-cyclic p -group, it is easily shown that G has a homomorphic image \bar{G} of type (p, p) , that is, \bar{G} is the direct product of two cyclic groups of order p . Since every $\mathbb{Z}\bar{G}$ -lattice is also a $\mathbb{Z}G$ -lattice, it suffices to prove $\mathbb{Z}\bar{G}$ of infinite representation type. But $\mathbb{Z}\bar{G}/p \cdot \mathbb{Z}\bar{G}$ is local, and $Q\bar{G}$ has at least 4 simple components, so we can again use Dade's Theorem.

In the above, we can replace \mathbb{Z} by any Dedekind domain R of characteristic 0, such that p is a non-unit of R . Dade's Theorem has been generalized by a number of authors: Jacobinski [67; see correction in Math. Reviews 35 #2876], Drozd-Roiter [67, §2], Drozd [74], Green-Reiner [78].

To conclude, we state without proof two results of Drozd [74]:

(33.11) Proposition. *Let R be a d.v.r., and let Λ be an R -order in a separable K -algebra A . If there exists an indecomposable projective left Λ -lattice M such that the composition length of the A -module KM is ≥ 4 , then Λ has infinite representation type.*

This follows from a stronger result due to Drozd:

(33.12) Theorem. *Let R be a d.v.r., and let Λ be an R -order in a separable K -algebra A . Suppose that Λ is a local ring, and set $D = \Lambda/\text{rad } \Lambda$ (a skewfield). Let Γ be an R -order in A containing Λ , and suppose that J is a two-sided ideal of Γ for which*

$$\text{rad } \Lambda \subseteq J \subseteq \text{rad } \Gamma.$$

Let m be the dimension over D of the D -space Γ/J . Then

- (i) *Λ has infinite representation type if $m \geq 4$.*
- (ii) *If Γ is itself a local order, and if $(\text{rad } \Gamma)^2 \subseteq J$, then Λ has infinite representation type whenever $m \geq 3$.*

This result plays a vital role in the work of Drozd-Kirichenko [73]; also see the remarks in §33C.

§33C. Commutative Orders

Throughout this section, let Λ denote an R -order in a separable K -algebra A , where K is a global field or its completion, and R is a Dedekind domain with quotient field K . In this section we shall again consider the question as to when $n(\Lambda) < \infty$, where $n(\Lambda)$ is the number of isomorphism classes of indecomposable left Λ -lattices. By Jones' Theorem, $n(\Lambda) < \infty$ if and only if $n(\Lambda_P) < \infty$ for each maximal ideal P of R such that Λ_P is not a maximal order, where the subscript P denotes P -adic completion. As we shall see, the results of Jacobinski and Drozd-Roiter give a complete solution to the question as to when $n(\Lambda) < \infty$, in case the order Λ is commutative. There are many partial results for the non-commutative case, of which the Drozd-Kirichenko Theorem seems to be the best so far.

Let Λ be commutative from now on, unless specifically stated otherwise, and let Λ' be the unique* maximal R -order in the commutative separable K -algebra A . Jacobinski [67] gave necessary and sufficient conditions that $n(\Lambda)$ be finite. Another version of these results was given by Drozd-Roiter

*See (26.10).

[67]; their proof is independent of Jacobinski's approach. A recent investigation by Green-Reiner [78] also treats this question, and we shall follow their approach.

The Drozd-Roiter criteria for finite representation type are somewhat easier to state than those of Jacobinski, and we shall phrase the main theorem as in Drozd-Roiter. These criteria involve a comparison of Λ with the maximal order Λ' containing it. We begin with a few general remarks about generators of modules.

Let Γ be an arbitrary ring, X a f.g. left Γ -module; denote by $\mu_\Gamma(X)$, or just $\mu(X)$ if there is no danger of confusion, the minimal number of generators of X as Γ -module. Put $N = \text{rad } \Gamma$, and let $\bar{\Gamma} = \Gamma/N$, $\bar{X} = X/NX$. Each surjection $\psi: \Gamma^{(n)} \rightarrow X$ yields a surjection $\bar{\psi}: \bar{\Gamma}^{(n)} \rightarrow \bar{X}$. Conversely, every surjection $\bar{\psi}$ lifts to a map ψ , which must be surjective by Nakayama's Lemma. From these remarks we have

$$(33.13) \quad \mu_\Gamma(X) = \mu_{\bar{\Gamma}}(\bar{X})$$

for every f.g. Γ -module X . We remark also that if $\bar{\Gamma}$ is a semisimple artinian ring, then

$$\text{rad } X = (\text{rad } \Gamma)X$$

by (5.29). Furthermore, if Γ is a local ring, then $\bar{\Gamma}$ is a skewfield by (5.21); in this case, we have

$$\mu_{\bar{\Gamma}}(\bar{X}) = \dim_{\bar{\Gamma}} \bar{X}.$$

Suppose now that Γ is an R -algebra, f.g./ R as module, where R is a Dedekind domain, and let X be a f.g. R -torsion Γ -module. Let $a \in R$ be a nonzero element with $aX = 0$, so we may view X as a $(\Gamma/a\Gamma)$ -module. Express $\Gamma/a\Gamma$ and X as direct sums of P -primary components (see (4.31)):

$$\Gamma/a\Gamma \cong \coprod \Gamma_P/a\Gamma_P, \quad X \cong \coprod X_P,$$

where P ranges over all maximal ideals of R dividing Ra , and the subscript P denotes P -adic completion. Clearly

$$\mu_\Gamma(X) = \max_{P \mid Ra} \mu_{\Gamma_P}(X_P) = \max_{\text{all } P} \mu_{\Gamma_P}(X_P).$$

We remark also that if Γ is a finite direct sum of rings $\Gamma = \coprod \Gamma_i$, then each Γ -module X decomposes as $X = \coprod X_i$, with X_i a Γ_i -module. We have

$$\mu_\Gamma(X) = \max_i \mu_{\Gamma_i}(X_i).$$

Now let Λ be a commutative R -order in A , and form the R -torsion Λ -module Λ'/Λ , where Λ' is the maximal R -order in A . The basic result, due to Jacobinski [67] and (in this version) to Drozd-Roiter [67], is as follows:

(33.14) Theorem. *Let A be a separable commutative K -algebra, where K is a global field or its completion. Let Λ be an R -order in A , and Λ' the maximal order in A . Then Λ has finite representation type if and only if*

$$(33.15) \quad \mu_{\Lambda}(\Lambda'/\Lambda) \leq 2 \text{ and } \mu_{\Lambda}(\text{rad}_{\Lambda}(\Lambda'/\Lambda)) \leq 1.$$

Here, $\text{rad}_{\Lambda}(\Lambda'/\Lambda)$ denotes the radical of the Λ -module Λ'/Λ . Both of the μ 's in (33.15) can be computed once they are known locally. Further, the number $n(\Lambda)$ of indecomposable Λ -lattices is finite if and only if $n(\Lambda_P) < \infty$ for each P at which $\Lambda_P \neq \Lambda'_P$, by Jones' Theorem. Hence it suffices to prove the theorem for the local case.

For the rest of this proof, we assume that R is a complete d.v.r. with prime element π and finite residue class field $\bar{R} = R/\pi R$. Both $\Lambda/\text{rad } \Lambda$ and $\Lambda'/\text{rad } \Lambda'$ are direct sums of field extensions of R , and for later calculations we would like all these fields to coincide with \bar{R} . We shall accomplish this by replacing R by a larger ring S which is unramified over R , making use of the following interesting result due to Jacobinski [67]:

(33.16) Proposition. *Let L be a finite unramified extension of K with valuation ring S . Then $n(\Lambda) < \infty$ if and only if $n(S \otimes_R \Lambda) < \infty$.*

Proof. If $n(S \otimes \Lambda) < \infty$, let $\{L_1, \dots, L_t\}$ be a full set of indecomposable $(S \otimes \Lambda)$ -lattices. For each indecomposable Λ -lattice M , $S \otimes M$ is a direct sum of copies of the L_i 's; but $S \otimes M \cong M^{(n)}$ as Λ -lattices, where $n = R$ -rank of S . Hence M is a Λ -direct summand of $S \otimes M$, and therefore M is a summand of $L_i|_{\Lambda}$ for some i . This shows that $n(\Lambda) < \infty$. The argument does not depend on L/K being unramified.

To prove the converse, we start with an $(S \otimes \Lambda)$ -lattice X , and form the Λ -lattice X_{Λ} by restriction of operators. Then $S \otimes_R X_{\Lambda}$ is an $(S \otimes \Lambda)$ -lattice, and we wish to compare it with the original lattice X . Note that the S -rank of $S \otimes X$ is n times the S -rank of X . We must use the fact that L/K is a Galois extension with Galois group G , where $G \cong \bar{G} = \text{Gal}(\bar{S}/\bar{R})$. Here $\bar{S} = S/\pi S$ is the residue class field of S . Indeed, since L/K is unramified, we have

$$(33.17) \quad L = K[x]/(f(x)), \quad S = R[x]/(f(x)), \quad \bar{S} = \bar{R}[x]/(\bar{f}(x)),$$

where $f(x) \in R[x]$ is a monic irreducible polynomial whose image $\bar{f}(x)$ is also irreducible (see Weiss [63; §3-2]). Then \bar{S} is a Galois extension of the finite field \bar{R} , so $\bar{f}(x)$ splits into distinct linear factors in $\bar{S}[x]$. By Hensel's Lemma, $f(x)$ splits into linear factors in $S[x]$, and so L/K is a Galois extension. The correspondence between factorizations easily yields the desired isomorphism $G \cong \bar{G}$.

Now let X be an $(S \otimes \Lambda)$ -lattice, on which both S and Λ act by means of the embeddings $S \rightarrow S \otimes \Lambda$, $\Lambda \rightarrow S \otimes \Lambda$. For each $\sigma \in G$, we define a conjugate $(S \otimes \Lambda)$ -lattice X^σ , whose elements are symbols $\{x_\sigma : x \in X\}$ which are added according to the rule $(x+y)_\sigma = x_\sigma + y_\sigma$. The action of $S \otimes \Lambda$ on X^σ is given by

$$(s \otimes \lambda)x_\sigma = (s^\sigma \lambda x)_\sigma \text{ for all } s \in S, \lambda \in \Lambda, x \in X.$$

We shall prove*

$$(33.18) \quad S \otimes_R X_\Lambda \cong \coprod_{\sigma \in G} X^\sigma \text{ as } (S \otimes \Lambda)\text{-lattices,}$$

and begin by defining a map $T: S \otimes X \rightarrow \coprod X^\sigma$ as follows:

$$T(s \otimes x) = \coprod (s^\sigma x)_\sigma, \quad s \in S, x \in X.$$

We show first that T is an $(S \otimes \Lambda)$ -homomorphism; for if $t \in S$ and $\lambda \in \Lambda$, then

$$\begin{aligned} T((t \otimes \lambda)(s \otimes x)) &= T(ts \otimes \lambda x) = \coprod ((ts)^\sigma \lambda x)_\sigma = \coprod (t^\sigma s^\sigma \lambda x)_\sigma \\ &= (t \otimes \lambda) \coprod (s^\sigma x)_\sigma = (t \otimes \lambda)T(s \otimes x). \end{aligned}$$

Now let $S = \bigoplus_{i=1}^n R s_i$, $G = \{\sigma_1, \dots, \sigma_n\}$. Then $S \otimes X = \bigoplus (s_i \otimes X)$, so to show that T is an isomorphism, we must prove that given any elements $x_1, \dots, x_n \in X$, there are uniquely determined elements $y_1, \dots, y_n \in X$ such that

$$T\left(\sum_{i=1}^n s_i \otimes y_i\right) = \coprod_{\sigma \in G} (x_j), \text{ where } x_j \in X^\sigma.$$

This condition gives

$$\sum_{i=1}^n s_i^\sigma y_i = x_j, \quad 1 \leq j \leq n.$$

But $\det(s_i^\sigma)_{1 \leq i, j \leq n}$ is a unit in S , since the square of this determinant generates the discriminant ideal $d(S/R)$, which equals R because S/R is unramified. Hence we can solve the above equations uniquely for the $\{y_i\}$, which completes the proof of (33.18).

Now let $n(\Lambda) < \infty$, and let $\{M_1, \dots, M_k\}$ be a full set of indecomposable Λ -lattices. Each $(S \otimes \Lambda)$ -lattice X is an $(S \otimes \Lambda)$ -direct summand of $S \otimes X_\Lambda$ by (33.18), and X_Λ is a sum of M 's. Hence if X is indecomposable then

*This result is analogous to that in (7.18).

$X|(S \otimes M_i)$ for some i , which proves that $n(S \otimes \Lambda) < \infty$. This completes the proof of the Proposition.

(If S/R is ramified, the assertion in (33.16) may fail; see Exercise 33.1.)

Keeping the above notation, we investigate the effect of this change of ground ring on the μ 's in (33.15). Now $S \otimes \Lambda$ is an S -order in the separable commutative L -algebra $L \otimes A$, and $S \otimes \Lambda'$ is the maximal S -order in $L \otimes A$; this is an immediate consequence of (4.26a), since Λ' is a direct sum of valuation rings in finite extension fields of K . For convenience, let $\Gamma = S \otimes \Lambda$ and $\Gamma' = S \otimes \Lambda'$. As in the beginning of the proof of (32.5), we have

$$\Gamma / \text{rad } \Gamma \cong \bar{S} \otimes_{\bar{R}} (\Lambda / \text{rad } \Lambda), \quad \text{rad } \Gamma = S \otimes_R \text{rad } \Lambda.$$

A corresponding formula holds with Λ, Γ replaced by Λ', Γ' , respectively.

Let us now choose an extension field \bar{S} , finite over \bar{R} , which is a splitting field for both $\Lambda / \text{rad } \Lambda$ and $\Lambda' / \text{rad } \Lambda'$. We then use (30.30) to obtain an unramified extension L of K with the residue class field \bar{S} . Then $\Gamma / \text{rad } \Gamma$ and $\Gamma' / \text{rad } \Gamma'$ are direct sums of copies of \bar{S} , and we have already shown that $n(\Lambda) < \infty$ if and only if $n(\Gamma) < \infty$. It remains for us to check that

$$\mu_\Gamma(\Gamma' / \Gamma) = \mu_\Lambda(\Lambda' / \Lambda),$$

and likewise for the μ 's involving radicals. But, by (5.29),

$$\Gamma' / \Gamma \cong S \otimes (\Lambda' / \Lambda), \quad \text{and } \text{rad}(\Gamma' / \Gamma) = (\text{rad } \Gamma) \cdot (\Gamma' / \Gamma) \cong S \otimes \text{rad}(\Lambda' / \Lambda).$$

Hence we need only show that for any f.g. Λ -module Y ,

$$\mu_\Lambda(Y) = \mu_\Gamma(S \otimes Y).$$

If bars denote reduction modulo the radical, we have $\mu_\Lambda(Y) = \mu_{\bar{\Lambda}}(\bar{Y})$. Also, $\bar{\Gamma} = \bar{S} \otimes \bar{\Lambda}$, and $\bar{S} \otimes \bar{Y} = \bar{S} \otimes \bar{Y}$, so we need to prove that

$$\mu_{\bar{\Lambda}}(\bar{Y}) = \mu_{\bar{S} \otimes \bar{\Lambda}}(\bar{S} \otimes \bar{Y}).$$

Now \bar{Y} is a $\bar{\Lambda}$ -module, and $\bar{\Lambda}$ is a direct sum of fields. It therefore suffices to treat the case where $\bar{\Lambda}$ is a field and \bar{Y} is a vector space over $\bar{\Lambda}$; but the formula is obvious in this case.

We have now shown that replacing the ground ring R by a unramified extension ring S does not alter the representation type of Λ nor the expressions occurring in (33.15). Hence, for the remainder of the proof we may assume that $\Lambda / \text{rad } \Lambda$ and $\Lambda' / \text{rad } \Lambda'$ are direct sums of copies of \bar{R} . One further reduction is needed. If $\Lambda = \coprod \Lambda_i$ is a direct sum of R -orders Λ_i , then correspondingly $\Lambda' = \coprod \Lambda'_i$ with each Λ'_i a maximal order. Clearly, $\mu(\Lambda' / \Lambda) = \max \mu(\Lambda'_i / \Lambda_i)$, etc., and $n(\Lambda) < \infty$ if and only if $n(\Lambda_i) < \infty$ for each i . Hence

it suffices to prove the result when the commutative ring Λ is indecomposable, that is, when $\Lambda/\text{rad } \Lambda$ is a field. Thus, we may assume hereafter that Λ is a local order, with $\Lambda/\text{rad } \Lambda \cong \bar{R}$. Unfortunately, the theorem is still quite difficult to prove, despite these many reduction steps, and all of the known proofs are rather computational. We shall give some of the details of the Green-Reiner version, which is in the same spirit as Jacobinski's original proof, and which corrects some minor errors in that proof. The Drozd-Roiter approach may be found in their original article, or else in the detailed exposition in Roggenkamp [70].

Continuing with the proof, let $J = \text{rad } \Lambda$, and let bars denote reduction mod J . Applying $\bar{\Lambda} \otimes_{\Lambda} *$ to the Λ -exact sequence $0 \rightarrow \Lambda \rightarrow \Lambda' \rightarrow \Lambda'/\Lambda \rightarrow 0$, we obtain a $\bar{\Lambda}$ -exact sequence

$$\bar{\Lambda} \xrightarrow{\psi} \overline{\Lambda'} \rightarrow \overline{\Lambda'/\Lambda} \rightarrow 0,$$

in which $\psi(1) = 1$. Now $\psi(1) \neq 0$, since otherwise we obtain $\Lambda' = J\Lambda'$, which is impossible by Nakayama's Lemma. Since $\bar{\Lambda} \cong \bar{R}$, this shows that ψ is monic, and hence

$$1 + \dim \overline{\Lambda'/\Lambda} = \dim \overline{\Lambda'},$$

where \dim is \bar{R} -dimension. Since $\mu_{\Lambda}(\Lambda'/\Lambda) = \mu_{\bar{\Lambda}}(\overline{\Lambda'/\Lambda})$, we obtain

$$(33.19) \quad \mu_{\Lambda}(\Lambda'/\Lambda) = \dim \overline{\Lambda'} - 1.$$

Likewise we have $\text{rad}(\Lambda'/\Lambda) = J(\Lambda'/\Lambda) = (J\Lambda' + \Lambda)/\Lambda$, so

$$\mu_{\Lambda}(\text{rad}(\Lambda'/\Lambda)) = \dim \{ \text{rad}(\Lambda'/\Lambda)/J \cdot \text{rad}(\Lambda'/\Lambda) \} = \dim(J\Lambda' + \Lambda)/(J^2\Lambda' + \Lambda)$$

Hence conditions (33.15) may be rewritten as

$$(33.20) \quad \dim \Lambda'/J\Lambda' \leq 3, \quad \dim(J\Lambda' + \Lambda)/(J^2\Lambda' + \Lambda) \leq 1.$$

These conditions say that Λ is, in some sense, not too far removed from the maximal order Λ' .

The next step reduces the study of Λ -lattices to the study of pairs of modules over artinian rings. Let I be any proper Λ' -ideal in Λ such that $K \cdot I = A$, and set

$$\Delta = \Lambda/I, \quad \Delta' = \Lambda'/I,$$

so Δ and Δ' are nonzero R -torsion R -algebras, and hence are artinian rings. Of course, $\Delta'/\Delta \cong \Lambda'/\Lambda$ and

$$\mu_{\Lambda}(\Lambda'/\Lambda) = \mu_{\Delta}(\Delta'/\Delta), \quad \mu_{\Lambda}(\text{rad}(\Lambda'/\Lambda)) = \mu_{\Delta}(\text{rad}(\Delta'/\Delta)).$$

Since Λ is local, we have $I \subseteq J \subseteq J\Lambda' \subseteq \text{rad } \Lambda'$, the last inclusion resulting from the fact that $(J\Lambda')^m \subseteq \pi\Lambda'$ for some m . If $N = \text{rad } \Delta$, then we obtain

$$N = J/I, \quad \Delta/N \cong \Lambda/J \cong \bar{R},$$

$$\text{rad } \Delta' = (\text{rad } \Lambda')/I, \quad \Delta'/\text{rad } \Delta' \cong \Lambda'/\text{rad } \Lambda' \cong \bar{R}.$$

Thus, the rings Δ, Δ' satisfy the same hypotheses as Λ, Λ' , and conditions (33.20) may be rewritten as

$$(33.21) \quad \dim \Delta'/N\Delta' \leq 3, \quad \dim(N\Delta' + \Delta)/(N^2\Delta' + \Delta) \leq 1.$$

Let $\mathcal{P}(\Lambda)$ denote the set of f.g. projective Λ -modules. Given any Λ -lattice M , we may form $M' = \Lambda'M$ computed inside KM , so $M' \in \mathcal{P}(\Lambda')$ since Λ' is hereditary. We have $IM' = I\Lambda'M = IM$, and so there is an inclusion

$$M/IM \subseteq M'/IM = Y \text{ (say)},$$

and $Y \in \mathcal{P}(\Delta')$ since $M' \in \mathcal{P}(\Lambda')$.

Now every f.g. Δ -module has a projective cover (see §6C), unique up to isomorphism. If X is a projective cover of the Δ -module M/IM , then there is a Δ -surjection $X \rightarrow M/IM$ whose kernel lies in NX . Let $f \in \text{Hom}_\Delta(X, Y)$ be defined by composition of maps

$$X \rightarrow M/IM \rightarrow M'/IM' = Y.$$

Then we have $X \in \mathcal{P}(\Delta)$, $Y \in \mathcal{P}(\Delta')$, and

$$(33.22) \quad Y = \Delta' \cdot f(X), \quad \ker f \subseteq NX, \quad \text{where } N = \text{rad } \Delta.$$

Now let $\mathcal{Q} = \mathcal{Q}(\Delta, \Delta')$ be the category whose objects are triples (X, Y, f) , where $X \in \mathcal{P}(\Delta)$, $Y \in \mathcal{P}(\Delta')$, and $f \in \text{Hom}_\Delta(X, Y)$ satisfies (33.22). A morphism

$$(\alpha, \beta) : (X_1, Y_1, f_1) \rightarrow (X_2, Y_2, f_2)$$

in \mathcal{Q} is (by definition) a pair of maps $\alpha \in \text{Hom}_\Delta(X_1, X_2)$, $\beta \in \text{Hom}_{\Delta'}(Y_1, Y_2)$, such that $f_2 \alpha = \beta f_1$. Each Λ -lattice M thus gives rise to an object $F(M) = (X, Y, f)$ in \mathcal{Q} , defined as above. Furthermore, each $\mu \in \text{Hom}_\Lambda(M_1, M_2)$ gives rise to a commutative diagram

$$\begin{array}{ccccc} X_1 & & M_1/IM_1 & & M'_1/IM'_1 \\ \mu_0 \downarrow & & \mu_1 \downarrow & & \mu_2 \downarrow \\ X_2 & \xrightarrow{\hspace{1cm}} & M_2/IM_2 & \xrightarrow{\hspace{1cm}} & M'_2/IM'_2, \end{array}$$

where μ induces μ_1 and μ_2 . The map μ_1 lifts to a map μ_0 of projective

covers, and so μ gives rise to a morphism $F(\mu) = (\mu_0, \mu_2)$, where $(\mu_0, \mu_2) : F(M_1) \rightarrow F(M_2)$. However, F is *not* a functor from the category $\mathcal{L}(\Lambda)$ of Λ -lattices to the category \mathcal{Q} , since F need not preserve compositions of maps. Nevertheless, if μ is an isomorphism, then so is $F(\mu)$. Furthermore, $F(M_1 \oplus M_2) \cong F(M_1) \oplus F(M_2)$, since projective covers are “additive” (see (6.25)).

We wish to obtain information about Λ -lattices by studying the category \mathcal{Q} , which is easier to handle because Δ and Δ' are artinian rings. This “reduction to the artinian case” occurs in one form or another in many calculations with lattices, and is implicit in Jacobinski’s technique of working modulo the conductor of Λ' in Λ . It was made explicit in Green-Reiner [78]; other consequences of this reduction may be found in Ringel-Roggenkamp [79]. We shall show that the categories $\mathcal{L}(\Lambda)$ and \mathcal{Q} are *representation equivalent*, that is, there is a bijection between the sets of isomorphism classes of indecomposable objects in the two categories. For this purpose, we must construct a map $G : \mathcal{Q} \rightarrow \mathcal{L}(\Lambda)$.

Starting with a triple (X, Y, f) in \mathcal{Q} , there is a surjection $f : X \rightarrow f(X) \subseteq Y$, and we have $Y = \Delta' \cdot f(X)$. Since $\ker f \subseteq (\text{rad } \Delta)X$, the map $X \rightarrow f(X)$ gives a Δ -projective cover of $f(X)$. On the other hand, $I \subseteq J \subseteq J\Delta' \subseteq \text{rad } \Delta'$, so by (6.8) we have $Y \cong M'/IM'$ for some $M' \in \mathcal{P}(\Lambda')$. We now define the Λ -module M as a pullback:

$$\begin{array}{ccc} M & \dashrightarrow & M' \\ \downarrow & & \downarrow \\ f(X) & \longrightarrow & M'/IM' = Y. \end{array}$$

The inclusion $M \subseteq M'$ shows that M is a Λ -lattice. Further, from $Y = \Delta' \cdot f(X)$ we obtain $M' = \Lambda' M + IM'$, and so $M' = \Lambda' M$ since $I \subseteq \text{rad } \Lambda'$. Since $IM' = IM$, it follows that $f(X) \cong M/IM$. If we put $G(X, Y, f) = M$, then it is obvious that $F(M) \cong (X, Y, f)$. Conversely, starting with any Λ -lattice M , we obtain $GF(M) \cong M$.

Finally, we show that any morphism $(\alpha, \beta) : (X_1, Y_1, f_1) \rightarrow (X_2, Y_2, f_2)$ in \mathcal{Q} gives rise to a morphism in $\mathcal{L}(\Lambda)$. Since $\beta f_1 = f_2 \alpha$, we have $\beta f_1(X_1) \subseteq f_2(X_2)$, so there is a commutative diagram

$$\begin{array}{ccccc} X_1 & \xrightarrow{\quad} & f(X_1) & \xrightarrow{\quad} & Y_1 \\ \alpha \downarrow & & \downarrow & & \beta \downarrow \\ X_2 & \xrightarrow{\quad} & f(X_2) & \xrightarrow{\quad} & Y_2. \end{array}$$

The map β lifts to a Λ' -map $M'_1 \rightarrow M'_2$, where $Y_j = M'_j / IM'_j$, $j = 1, 2$. We then obtain an induced map $M_1 \rightarrow M_2$ on pullbacks, so G carries each morphism in \mathcal{Q} onto a morphism in $\mathcal{L}(\Lambda)$. However, G is not a functor since it need not preserve compositions. Nevertheless, G preserves isomorphisms and direct

sums. We have thus shown that F and G give a representation equivalence between the categories $\mathcal{L}(\Lambda)$ and \mathcal{Q} , so Λ has finite representation type if and only if the same is true for the category $\mathcal{Q} = \mathcal{Q}(\Delta, \Delta')$. (For further results of this nature, see Exercises 33.4–33.7.)

In order to prove the main theorem, we must show that the category \mathcal{Q} has finitely many isomorphism classes of indecomposable objects if and only if conditions (33.21) are satisfied. We may write

$$\Lambda = \coprod_{i=1}^t K_i, \quad \Lambda' = \coprod_{i=1}^t S_i, \quad \text{rad } \Lambda' = \coprod_{i=1}^t P_i,$$

where for each i , S_i is the integral closure of R in a finite separable extension K_i of R . Then S_i is also a complete d.v.r., and $S_i/P_i \cong \bar{R}$ since $\Lambda'/\text{rad } \Lambda' \cong \coprod \bar{R}$. Thus, S_i is completely ramified over R .

If $t \geq 4$, then by Dade's Theorem, the order Λ and the category \mathcal{Q} have infinite representation type. Moreover,

$$\dim \Lambda'/J\Lambda' \geq \dim \Lambda'/\text{rad } \Lambda' = t \geq 4,$$

since $J\Lambda' \subseteq \text{rad } \Lambda'$. Thus for the rest of the proof, we may assume that $t \leq 3$ (it will turn out that the *hardest* case is that where $t=1$).

(33.23) Lemma. *The category \mathcal{Q} has infinite representation type whenever $\dim \Lambda'/J\Lambda' > 3$.*

Proof. We apply Exercise 33.5 with $I_0 = N$, $J_0 = N\Delta'$, $\Gamma = \Delta'$, so $\Delta/I_0 \cong \bar{R}$ and $\Gamma/J_0 = \Delta'/N\Delta' \cong \Lambda'/J\Lambda' = \Omega$, say. The category $\bar{\mathcal{Q}}$ consists of triples (X, Y, f) with $X \in \mathcal{P}(\bar{R})$, $Y \in \mathcal{P}(\Omega)$ and $f \in \text{Hom}_{\bar{R}}(X, Y)$ satisfying

$$Y = \Omega \cdot f(X), \quad \ker f = 0,$$

(since $\ker f \subseteq (\text{rad } \bar{R})X$, and $\text{rad } \bar{R} = 0$). We may write

$$\Omega = \coprod_{i=1}^t S_i/P_i^{n_i}, \quad n_i \geq 1 \text{ for each } i,$$

and then

$$\dim \Lambda'/J\Lambda' = \dim \Omega = \sum_{i=1}^t n_i.$$

We shall show that $\bar{\mathcal{Q}}$ has infinite representation type whenever $\sum n_i > 3$, so then the same holds for \mathcal{Q} by Exercise 33.5. As remarked earlier, we are restricting our attention to the case where $t \leq 3$.

Suppose first that two of the $\{n_i\}$ are ≥ 2 , say $n_1 \geq 2$ and $n_2 \geq 2$. Again using Exercise 33.5, with

$$I_0 = 0, J_0 = P_1^2/P_1^{n_1} \oplus P_2^2/P_2^{n_2} \oplus \coprod_{i>2} S_i/P_i^{n_i},$$

we may now assume $t=2$ and $n_1=n_2=2$. For convenience of notation, put $k=\bar{R}$. Then Ω has a k -basis $\{y_i : 1 \leq i \leq 4\}$ with $y_1=1$, and $\text{rad } \Omega = ky_3 + ky_4$. As in Step 3 in the proof of Dade's Theorem, let $V=k[x]/(x^n)$ be a local ring of k -dimension n . Define $G(V) \in \bar{\mathcal{A}}$ by

$$G(V) = (V \oplus V, \Omega \otimes_k V, \psi),$$

where

$$\psi(v, v') = 1 \otimes v + y_3 \otimes v' + y_4 \otimes \theta v', \quad v, v' \in V,$$

and where $\theta(v') = xv'$, $v' \in V$. (It is easily verified that $G(V) \in \bar{\mathcal{A}}$.) The \mathcal{Q} -endomorphism ring of $G(V)$ consists of all pairs (α, β) such that

$$\alpha \in \text{End}_k(V \oplus V), \beta \in \text{End}_{\Omega}(\Omega \otimes V), \psi\alpha = \beta\psi.$$

Since $\Omega \otimes_k V = \coprod_1^4 y_i \otimes V$, we may write

$$\beta(1 \otimes v) = \sum_1^4 y_i \otimes \beta_i v, \quad \beta_i \in \text{End}_k V.$$

Note that $y_3^2 = y_3 y_4 = y_4^2 = 0$ since $(\text{rad } \Omega)^2 = 0$. For $v \in V$, the condition $\psi\alpha(v, 0) = \beta\psi(v, 0)$ becomes (writing $\alpha = (\alpha_{ij})^{2 \times 2}$),

$$1 \otimes \alpha_{11} v + y_3 \otimes \alpha_{21} v + y_4 \otimes \theta \alpha_{21} v = 1 \otimes \beta_1 v + y_2 \otimes \beta_2 v + y_3 \otimes \beta_3 v + y_4 \otimes \beta_4 v,$$

whence

$$\beta_1 = \alpha_{11}, \beta_2 = 0, \beta_3 = \alpha_{21}, \beta_4 = \theta \alpha_{21}.$$

Likewise, from the condition $\psi\alpha(0, v) = \beta\psi(0, v)$, $v \in V$, we obtain

$$\beta_1 = \alpha_{22}, \beta_1 \theta = \theta \alpha_{22}, \alpha_{12} = 0.$$

Thus

$$\alpha = \begin{pmatrix} \alpha_{11} & 0 \\ \alpha_{21} & \alpha_{11} \end{pmatrix}, \quad \alpha_{11}\theta = \theta \alpha_{11}.$$

If (α, β) is idempotent, then $\alpha_{11}^2 = \alpha_{11}$. Surely $\alpha_{11} \neq 0$, since if $\alpha_{11} = 0$ then from $\alpha^2 = \alpha$ we obtain $\alpha_{21} = 0$, and therefore $(\alpha, \beta) = 0$. Thus α_{11} is an

idempotent element of the local ring $\text{End}_{k[x]}V$, which shows that $\alpha_{11}=1$. This implies that $\alpha_{21}=0$ and $\beta=1$, so $(\alpha, \beta)=1$. We have therefore proved that the $\bar{\mathcal{Q}}$ -endomorphism ring of $G(V)$ has no nontrivial idempotents, so $G(V)$ is indecomposable. Therefore $\bar{\mathcal{Q}}$ has infinite representation type, as claimed.

We are thus left with the case where at most one $n_i > 1$. If each $n_i = 1$, then $\dim \Lambda'/J\Lambda' = t$, contradicting our underlying hypothesis that $t \leq 3$. Thus we may assume that $n_1 \geq 2$, $n_i = 1$ for $i > 1$. Since $t \leq 3$ and $\sum n_i > 3$, the only possibilities for Ω are as follows:

$$\begin{aligned}\Omega &= S_1/P_1^{n_1} \oplus k \oplus k, \quad n_1 \geq 2; \\ \Omega &= S_1/P_1^{n_1} \oplus k, \quad n_1 \geq 3; \quad \Omega = S_1/P_1^{n_1}, \quad n_1 \geq 4.\end{aligned}$$

In each case, a construction of the above type shows that $\bar{\mathcal{Q}}$ has infinite representation type; see Green-Reiner [78; pp. 69–70] for details. This completes the proof of the lemma.

Continuing with the proof of the main theorem, suppose now that

$$\dim \Delta'/N\Delta' \leq 3, \quad \dim(N\Delta' + \Delta)/(N^2\Delta' + \Delta) > 1,$$

and again let us show that $\bar{\mathcal{Q}}$ has infinite representation type. Using Exercise 33.5 once more, with $I_0 = N^2$, $J_0 = N^2\Delta$, $\bar{\Delta} = \Delta/I_0$, $\bar{\Delta}' = \Delta'/J_0$, the problem is reduced to a new pair of rings. Changing notation, we may then assume that $N^2 = 0$ and $\dim N\Delta'/N \geq 2$. Since $\dim \Delta'/N\Delta' \leq 3$, we find readily that the only possible situations are as follows:

$$\Delta' = \coprod_{i=1}^3 S_i/P_i^{n_i}, \quad N\Delta' = \coprod_{i=1}^3 P_i/P_i^{n_i}, \quad n_1 = n_2 = n_3 = 2;$$

$$\Delta' = \coprod_{i=1}^2 S_i/P_i^{n_i}, \quad N\Delta' = P_1^2/P_1^{n_1} \oplus P_2/P_2^{n_2}, \quad n_1 = 4, \quad n_2 = 2;$$

$$\Delta' = S_1/P_1^{n_1}, \quad N\Delta' = P_1^3/P_1^{n_1}, \quad n_1 = 6.$$

Again, in each case, a construction of the above type shows that $\bar{\mathcal{Q}}$ has infinite representation type (see Green-Reiner [78, pp. 70–71]). This completes the proof that conditions (33.21) are *necessary* for Λ to have finite representation type.

We turn next to the harder part of the proof of the main theorem, namely, the proof that conditions (33.21) are *sufficient* for finite representation type. After using Exercise 33.7 to replace Δ and Δ' by Δ/I_0 and Δ'/I_0 , respectively, where I_0 is the largest (two-sided) Δ' -ideal in Δ , and then changing notation, we may assume that Δ contains no nonzero (two-sided) Δ' -ideal. Suppose that (33.21) holds. It is then easily verified (see Green-Reiner [78, pp. 71–72]) that

the problem of finite representation type can be reduced to the following three test cases:

(I) $\Delta' = S_1/P_1^{n_1}$, and there exist elements $x, y \in N$ such that

$$\Delta'x = P_1^3\Delta', \Delta'y = P_1^4\Delta' \text{ or } P_1^5\Delta'.$$

(II) $\Delta' = S_1/P_1^{n_1} \oplus S_2/P_2^{n_2}$, and there exist $x, y \in N$ such that

$$\Delta'x = (P_1 \oplus P_2^2)\Delta', \Delta'y = P_2^2\Delta' \text{ or } P_2^3\Delta'.$$

(III) $\Delta' = \coprod_{i=1}^3 S_i/P_i^{n_i}$, and there exist $x, y \in N$ such that

$$\Delta'x = (P_1 \oplus P_2^b)\Delta', \Delta'y = (P_2 \oplus P_3)\Delta',$$

where $b=0$ or 1.

By way of illustration, let us show that \mathcal{Q} has finite representation type in Case (II), under the assumption that $\Delta'y = P_2^2\Delta'$. Let $\Gamma_i = S_i/P_i^{n_i}$, $i=1, 2$, so $\Delta' = \Gamma_1 \oplus \Gamma_2$. Each $X \in \mathcal{P}(\Delta)$ has a free Δ -basis $\{x_1, \dots, x_m\}$, and each $Y \in \mathcal{P}(\Delta')$ is of the form $Y = Y_1 \oplus Y_2$, with Y_i a free Γ_i -module. If $(X, Y, \psi) \in \mathcal{Q}$, then expressing the elements $\{\psi(x_1), \dots, \psi(x_m)\}$ in terms of a Γ_i -basis of Y_i , $i=1, 2$, we can represent ψ by a matrix

$$\mathbf{F} = \begin{pmatrix} \mathbf{A} \\ \mathbf{B} \end{pmatrix},$$

where \mathbf{A} is a matrix over Γ_1 with m columns, and \mathbf{B} is a matrix over Γ_2 with m columns. Basis changes in X and Y yield the equivalence relation

$$\left(\begin{array}{c} \mathbf{A} \\ \mathbf{B} \end{array} \right) \sim \left[\begin{array}{c} \mathbf{P}_1 \mathbf{A} \mathbf{T} \\ \mathbf{P}_2 \mathbf{A} \mathbf{T} \end{array} \right], \quad \mathbf{P}_i \in GL(\Gamma_i), \mathbf{T} \in GL(\Delta).$$

The triple (X, Y, ψ) is indecomposable in \mathcal{Q} if and only if the matrix \mathbf{F} is indecomposable under such an equivalence.

We shall now find canonical forms for indecomposable \mathbf{F} 's. For convenience, set $k = \bar{R} \cong S_i/P_i$, $P_i = \pi_i S_i$, $i=1, 2$. If bars denote passage to k , then since $Y = \Delta' \cdot \psi(X)$, we see at once that the rows of $\bar{\mathbf{A}}$ are linearly independent over k , and the same holds for $\bar{\mathbf{B}}$. We have

$$\Delta/N \cong \Gamma_i/P_i \Gamma_i \cong k, i=1, 2.$$

Consider the step $\mathbf{A} \rightarrow \mathbf{P}_1 \mathbf{A} \mathbf{T}$. We may choose $\mathbf{P}_1 \in GL(\Gamma_1)$, $\mathbf{T} \in GL(\Delta)$, such

that

$$\bar{\mathbf{P}}_1 \bar{\mathbf{A}} \bar{\mathbf{T}} = \begin{bmatrix} \bar{\mathbf{I}} & \bar{\mathbf{0}} \end{bmatrix} \text{ over the field } k.$$

(Note that $\bar{\mathbf{A}}$ has rank $\leq m$, and the rows of $\bar{\mathbf{A}}$ are linearly independent.) Therefore we have

$$\mathbf{A} \sim \begin{bmatrix} \mathbf{I} + \pi_1 \mathbf{F}_1 & \pi_1 \mathbf{F}_2 \end{bmatrix}$$

for some matrices $\mathbf{F}_1, \mathbf{F}_2$ over Γ_1 . Since $\mathbf{I} + \pi_1 \mathbf{F}_1 \in GL(\Gamma_1)$, we obtain

$$\mathbf{A} \sim (\mathbf{I} + \pi_1 \mathbf{F}_1)^{-1} \begin{bmatrix} \mathbf{I} + \pi_1 \mathbf{F}_1 & \pi_1 \mathbf{F}_2 \end{bmatrix} = \begin{bmatrix} \mathbf{I} & \pi_1 \mathbf{F}_3 \end{bmatrix}$$

for some matrix \mathbf{F}_3 .

Let us now use the hypothesis that Δ contains an element x such that $x\Gamma_1 = \pi_1\Gamma_1$. Since $\Delta/N \cong \Gamma_1/P_1 \cong k$, we can subtract x multiples of the first set of columns of the new \mathbf{A} from the last set of columns, so as to change $\pi_1 \mathbf{F}_3$ to a new matrix $\pi_1^2 \mathbf{F}_4$. We then use x^2 multiples to bring $\pi_1^2 \mathbf{F}_4$ to the form $\pi_1^3 \mathbf{F}_5$, and so on, until we eventually obtain $\mathbf{A} \sim [\mathbf{I} \ \mathbf{0}]$. We then have

$$\left(\begin{array}{c} \mathbf{A} \\ \mathbf{B} \end{array} \right) \sim \left(\begin{array}{c} \mathbf{I} & \mathbf{0} \\ \mathbf{B}_1 & \mathbf{B}_2 \end{array} \right).$$

We now proceed with a further set of equivalence transformations, which preserve the form $[\mathbf{I} \ \mathbf{0}]$ of the top row. For example, we can add Δ -multiples of the last set of columns to the first set of columns. Note also that

$$\mathbf{F} = \left(\begin{array}{c} \mathbf{I} & \mathbf{0} \\ \mathbf{B}_1 & \mathbf{B}_2 \end{array} \right) \sim \left(\begin{array}{cc} \mathbf{I} & \mathbf{0} \\ \mathbf{P}_2 \mathbf{B}_1 \mathbf{T}_1 & \mathbf{P}_2 \mathbf{B}_2 \mathbf{T}_2 \end{array} \right),$$

where $\mathbf{P}_2 \in GL(\Gamma_2)$, $\mathbf{T}_2 \in GL(\Delta)$ is arbitrary, and $\mathbf{T}_1 \in GL(\Delta)$ is chosen so that $\mathbf{P}_1 \mathbf{T}_1 = \mathbf{I}$ for some $\mathbf{P}_1 \in GL(\Gamma_1)$. Under the equivalence $\mathbf{B}_2 \rightarrow \mathbf{P}_2 \mathbf{B}_2 \mathbf{T}_2$, we can bring \mathbf{B}_2 into the form

$$\left(\begin{array}{cc} \mathbf{I} & \pi_2 \mathbf{B}_{13} \\ \mathbf{0} & \pi_2 \mathbf{B}_{23} \end{array} \right),$$

and now

$$\mathbf{F} \sim \left[\begin{array}{ccc} \mathbf{I} & \mathbf{0} & \mathbf{0} \\ \mathbf{B}_{11} & \mathbf{I} & \pi_2 \mathbf{B}_{13} \\ \mathbf{B}_{21} & \mathbf{0} & \pi_2 \mathbf{B}_{23} \end{array} \right].$$

After subtracting Δ -multiples of the second set of columns from the first set,

we can replace \mathbf{B}_{11} by $\pi_2 \mathbf{B}'_{11}$ (say). Since the rank of $\bar{\mathbf{B}}$ equals the number of rows of \mathbf{B} , it follows that the rank of $\bar{\mathbf{B}}_{21}$ is equal to the number of rows of \mathbf{B}_{21} . We can then use further equivalence transformations to bring \mathbf{B}_{21} into the form $[\mathbf{I} \ \pi_2 \mathbf{C}]$ for some \mathbf{C} , and thus

$$\mathbf{F} \sim \left[\begin{array}{cc|cc} \mathbf{I} & & \mathbf{0} & \\ \hline \pi_2 \mathbf{D}_1 & \pi_2 \mathbf{D}_2 & \mathbf{I} & \pi_2 \mathbf{B}_{13} \\ \mathbf{I} & \pi_2 \mathbf{D}_4 & \mathbf{0} & \pi_2 \mathbf{B}_{23} \end{array} \right].$$

We next work on $\pi_2 \mathbf{B}_{23}$, bringing it into the form

$$\begin{pmatrix} \pi_2 \mathbf{C}_1 & \pi_2^2 \mathbf{C}_2 \\ \pi_2^2 \mathbf{C}_3 & \pi_2^2 \mathbf{C}_4 \end{pmatrix},$$

and so on. This process eventually terminates (see Green-Reiner [78, p. 79]), and yields the following list of indecomposables for \mathbf{F} :

$$\left(\begin{array}{c} * \\ 1 \end{array} \right), \left(\begin{array}{c} 1 \\ * \end{array} \right), \left(\begin{array}{c} 1 \\ 1 \end{array} \right), \left(\begin{array}{c} * \\ 1 - \pi^n \end{array} \right), \left(\begin{array}{cc} 1 & 0 \\ 1 & \pi^n \end{array} \right), \left(\begin{array}{cc} 1 & 0 \\ \pi^n & 1 \end{array} \right), \left(\begin{array}{cc} 1 & 0 \\ 0 & 1 \end{array} \right),$$

where $n=1, 3, 5, \dots, q$, with q the least odd integer such that $\pi_2^q \in N$. The asterisk indicates a matrix with no rows.

The matrix $\left(\begin{array}{c} * \\ 1 \end{array} \right)$ corresponds to the case

$$X = \Delta, Y = \Gamma_2, \psi : \Delta \rightarrow \Gamma_2, \psi(1) = 1.$$

The Λ -lattice M is a corresponding pullback:

$$\begin{array}{ccc} M & \longrightarrow & S_2 = \Lambda' e_2 \\ \downarrow & & \downarrow \\ \Delta & \xrightarrow{\psi} & S_2 / P_2^{n_2}, \end{array}$$

where e_1, e_2 are the primitive idempotents of Λ' . Thus in this case $M \cong \Lambda e_2$, since $\text{im } \psi = \text{image of } \Lambda e_2$ in $S_2 / P_2^{n_2}$. Likewise, the matrix $\left(\begin{array}{c} 1 \\ * \end{array} \right)$ yields the indecomposable Λ -lattice Λe_1 , and the matrix $\left(\begin{array}{c} 1 \\ 1 \end{array} \right)$ gives $M = \Lambda$.

Consider next the matrix $\left(\begin{array}{c} * \\ 1 - \pi^n \end{array} \right)$, which corresponds to the case

$$X = \Delta x_1 \oplus \Delta x_2, Y = \Gamma_2 y, \psi(x_1) = y, \psi(x_2) = \pi^n y.$$

This case gives

$$M = (\Lambda + \Lambda\pi_2'')e_2.$$

In the same way, the last three \mathbf{F} 's yield the indecomposable Λ -lattices

$$\Lambda + \pi_2''\Lambda e_2, \Lambda(e_1 + \pi_2''e_2) + \Lambda e_2,$$

and

$$\Lambda(u_1 + u_2) + \Lambda(v_1 + \pi_2'''u_2),$$

the last viewed as sublattice of the direct sum $S_1u_1 \oplus S_1u_2 \oplus S_2v_1$ of two copies of S_1 and one copy of S_2 .

Analogous calculations can be performed for the other cases in (I)–(III) above, and in each case one can give a complete list of indecomposable lattices. Case I turns out to be the most complicated, and many steps are required to decompose a given matrix \mathbf{F} into a direct sum of indecomposable submatrices.

The calculations in Jacobinski [67] and Drozd-Roiter [67] are also quite formidable, and a neater proof of the main theorem has yet to be found.

For R a ring of algebraic integers, the question as to whether $n(RG) < \infty$ can always be reduced to the case where R is replaced by a complete d.v.r., and G by one of its Sylow p -subgroups H . Further, $n(RH) = \infty$ if H is non-cyclic (see (33.10)), so we need only study the case in which H is cyclic. In this case, the order RH is of course commutative, so in dealing with representations of groups, it suffices to consider only commutative orders.

However, there is the obvious question of generalizing the Jacobinski, Drozd-Roiter Theorem to the case of non-commutative orders. Many authors have obtained partial generalizations, in which the given non-commutative order is subjected to various restrictive hypotheses. Part of the difficulty seems to arise from the fact that $\Lambda \subseteq \Lambda'$ need not imply that $\text{rad } \Lambda \subseteq \text{rad } \Lambda'$, in the non-commutative case.

The best result obtained so far, for the general case, is the following theorem of Drozd-Kirichenko [73]:

(33.24) Theorem. *Let Λ be a \mathbb{Z} -order in a f.d. semisimple \mathbb{Q} -algebra A , not necessarily commutative, and let C be the center of Λ . Suppose that for each prime ideal P of C , the localization Λ_P is primary (that is, $\Lambda_P/\text{rad } \Lambda_P$ is a simple artinian ring.) Let $\tilde{\Lambda}$ be the intersection of all maximal \mathbb{Z} -orders in A which contains Λ .*

Then Λ is of finite representation type if and only if:

(i) $\tilde{\Lambda}$ is a hereditary ring, and

(ii) $\mu_{\Lambda}(\tilde{\Lambda}/\Lambda) \leq 2$ and $\mu_{\Lambda}(\text{rad } (\tilde{\Lambda}/\Lambda)) \leq 1$.

The proof is complicated, and uses strongly the theory of Bass and Gorenstein orders (see §37).

§33. Exercises

1. Let $p \geq 5$ be prime, $R = \text{ring of } p\text{-adic integers}$, $S = R[\zeta]$ where ζ is a primitive p -th root of 1, and let G be a cyclic group of order p . Show that $n(RG) < \infty$ but $n(S \otimes_R RG)$ is infinite. Thus, finite representation type need not be preserved under ramified extensions.
2. Let R be a complete d.v.r. with maximal ideal P , and let $\Lambda' = M_n(R)$. Let $\Lambda = \{(\alpha_{ij})^{n \times n} \in \Lambda' : \alpha_{ij} \in P \text{ for } 1 \leq i < j \leq n\}$. Show that Λ is a hereditary order, and that $P\Lambda'$ is a left ideal of Λ for which $\mu_\Lambda(P\Lambda') = n$.
3. Let A be a simple artinian ring, S a simple left A -module, and let $_A A \cong S^{(n)}$. For a f.g. left A -module X , let $l(X)$ denote its composition length, so $l(A) = n$. Show that

$$\mu_\Lambda(X) = 1 \text{ if } 1 \leq l(X) \leq n, \mu_\Lambda(X) = 2 \text{ if } n+1 \leq l(X) \leq 2n,$$

and so on.

4. A left artinian ring Δ is said to have *finite representation type* if there are only finitely many non-isomorphic f.g. indecomposable left Δ -modules. Let $\bar{\Delta} = \Delta/I_0$, where I_0 is a two-sided ideal of Δ . Show that if $\bar{\Delta}$ has infinite representation type, then so does Δ .
5. Let $\varphi: \Delta \rightarrow \Gamma$ be a ring homomorphism of left artinian rings such that $\varphi(I_0) \subseteq J_0$, where I_0 and J_0 are two-sided ideals of Δ and Γ , respectively. Set $\bar{\Delta} = \Delta/I_0$, $\bar{\Gamma} = \Gamma/J_0$, so φ induces a ring homomorphism $\bar{\varphi}: \bar{\Delta} \rightarrow \bar{\Gamma}$. Let \mathcal{Q} be the category whose objects are triples (X, Y, f) with $X \in \mathcal{P}(\Delta)$, $Y \in \mathcal{P}(\Gamma)$, and $f \in \text{Hom}(X, Y)$ any map such that

$$\Gamma \cdot f(X) = Y, \ker f \subseteq (\text{rad } \Delta) X.$$

(The map φ allows us to view each Δ -module as a Γ -module.) Define $\bar{\mathcal{Q}}$ analogously for the rings $\bar{\Delta}$, $\bar{\Gamma}$. Show that if $\bar{\mathcal{Q}}$ has infinite representation type, then so does \mathcal{Q} .

[Hint (Green-Reiner [78]): Given $\bar{A} = (\bar{X}, \bar{Y}, \bar{f}) \in \bar{\mathcal{Q}}$, let $\rho: Y \rightarrow \bar{Y}$ give a Γ -projective cover of \bar{Y} , so $\ker \rho \subseteq (\text{rad } \Gamma) Y$. If $\bar{W} = \bar{f}(\bar{X}) \subseteq \bar{Y}$, then $\bar{Y} = \bar{\Gamma} \bar{W}$. Let $W = \rho^{-1}(\bar{W})$, and let X be a Δ -projective cover of W . Then there is a commutative diagram

$$\begin{array}{ccccc} X & \xrightarrow{f} & W & \xrightarrow{\psi} & Y \\ \downarrow & & \sigma \downarrow & & \rho \downarrow \\ \bar{X} & \xrightarrow{\bar{f}} & \bar{W} & \longrightarrow & \bar{Y}, \end{array}$$

and the triple $(X, Y, f) \in \mathcal{Q}$. Set $H(\bar{A}) = (X, Y, \psi f)$, so each $\bar{A} \in \bar{\mathcal{Q}}$ determines an object $H(\bar{A}) \in \mathcal{Q}$. As in the discussion on page 33.24, an isomorphism $H(\bar{A}) \cong H(\bar{B})$ induces

an isomorphism $\bar{A} \cong \bar{B}$. Finally, each decomposition of $H(\bar{A})$ induces a decomposition of \bar{A} , since if

$$H(\bar{A}) = (X_1, Y_1, f_1) \oplus (X_2, Y_2, f_2) \text{ in } \mathcal{Q},$$

then there are corresponding decompositions of X , Y , \bar{W} , and \bar{Y} , and hence also a decomposition of \bar{A} .]

6. Let $\varphi: \Delta \rightarrow \Gamma$ be a homomorphism of artinian rings, and let $I_0 = \ker \varphi$, $J_0 = 0$. Show that the categories \mathcal{Q} and $\bar{\mathcal{Q}}$, defined in Exercise 5, are representation equivalent.

7. Let $\Delta \subseteq \Gamma$ be an inclusion of artinian rings, and let J_0 be a two-sided Γ -ideal contained in Δ . Choosing $I_0 = J_0$, show that the categories \mathcal{Q} and $\bar{\mathcal{Q}}$ above are representation equivalent.

8. Let $R = \hat{\mathbb{Z}}_p$ be the ring of p -adic integers, $G = \langle x \rangle$ a cyclic group of order p^2 . Let $\Lambda = RG$, $\Lambda' = \text{maximal } R\text{-order in } \hat{\mathbb{Q}}_p G$. Verify that

$$\mu_{\Lambda}(\Lambda'/\Lambda) = 2 \text{ and } \mu_{\Lambda}(\text{rad}(\Lambda'/\Lambda)) = 1,$$

so Λ has finite representation type. (See also §34C.)

§34. EXAMPLES OF INTEGRAL REPRESENTATIONS

Throughout this section, Λ denotes an R -order in a f.d. separable K -algebra A , where R is a Dedekind domain with quotient field K . In §25, we showed how arbitrary Λ -lattices could be built up as extensions of simpler lattices. In practice, this technique has yielded many of the results so far obtained about integral representations of specific groups and orders. This section is devoted to detailed investigations of a number of special cases.

In §34A, we show that for a given central idempotent e , each Λ -lattice M can be represented as an extension ξ of a lattice N on which e acts as 1, by a lattice L on which e acts on 0. The lattice M is determined up to isomorphism by the isomorphism classes of N and L and by the orbit of ξ in $\text{Ext}(N, L)$ under the actions of $\text{Aut } N$ and $\text{Aut } L$. We show further that, under suitable hypotheses, these orbits depend only on the genera of N and L .

This machinery is applied in §34B to a discussion of integral representations of cyclic p -groups. Of course, a complete classification of such representations cannot be expected for cyclic groups G of order p^κ , $\kappa \geq 3$, since by Dade's Theorem, $\mathbb{Z}G$ is of infinite representation type (see (33.10)). The special case $\kappa = 2$ is considered in §34C, and here we obtain a complete list of indecomposable $\mathbb{Z}G$ -lattices.

In §34D, we give the Drozd-Turčin example of a Λ -lattice M whose genus contains more isomorphism classes than does the genus of Λ itself.

Finally, in §34E, we consider representations of certain metacyclic and dihedral groups. Here, the results in §28 on twisted group rings play a

fundamental role, and permit a fairly complete classification of all indecomposable integral representations of such groups.

§34A. Extensions of Lattices

We shall now consider in more detail the problem of classifying Λ -lattices by means of extensions, and we shall use the earlier results of §25 freely. Let M be a full Λ -lattice in a f.g. left A -module V . Given a submodule W of V , we obtain an exact sequence of Λ -lattices

$$0 \rightarrow L \rightarrow M \rightarrow N \rightarrow 0, \quad L = M \cap W, \quad N = M/L.$$

In particular, let e be a central idempotent of A , and let $W = (1-e)V$. Then the sublattice

$$L = \{m \in M : em = 0\}$$

is a *characteristic* sublattice of M (that is, $\varphi(L) \subseteq L$ for every $\varphi \in \text{End}_\Lambda M$). If we put

$$(34.1) \quad \Lambda_1 = \Lambda / (\Lambda \cap Ae), \quad \Lambda_2 = \Lambda / (\Lambda \cap A(1-e)),$$

then L is a Λ_1 -lattice and N is a Λ_2 -lattice. Note that Λ_1 is an R -order in the K -algebra A/Ae , and Λ_2 in $A/A(1-e)$. Thus, to find all Λ -lattices M , we first classify all Λ_i -lattices ($i=1, 2$), and then find all extensions of a Λ_2 -lattice by a Λ_1 -lattice. We remark that in our case, $\text{Hom}_\Lambda(L, N) = 0$ since e acts as 0 on L and as 1 on N .

The purpose of the above procedure is to analyze a Λ -lattice M , such that KM involves more than one type of simple A -module, as an extension of Λ -lattices corresponding to single types of simple A -modules. In our first example below, this procedure is carried out in a somewhat disguised form.

(34.2) Example. Let $G = \langle x : x^n = 1 \rangle$, $\Lambda = RG$, where $\text{char } R = 0$. We identify Λ with $R[x]/(x^n - 1)$. Suppose that $x^n - 1 = f(x)g(x)$ in $R[x]$. Given a Λ -lattice M , put

$$L = \{m \in M : f(x)m = 0\}, \quad \Lambda_1 = R[x]/(f(x)), \quad \Lambda_2 = R[x]/(g(x)).$$

Then Λ_1 and Λ_2 are R -orders, L is a Λ_1 -lattice, and M/L is a Λ_2 -lattice. As above, $\text{Hom}_\Lambda(L, N) = 0$.

Let us explain how this example fits into the general procedure described above. The point here is that $K[x]/(x^n - 1)$ is a separable K -algebra, so for any factorization $x^n - 1 = f(x)g(x)$ in $R[x]$, the quotients $K[x]/(f(x))$ and $K[x]/(g(x))$ correspond to complementary Wedderburn components of $K[x]/(x^n - 1)$, and hence to central idempotents e and $1-e$, as above.

Our next example, which will also be needed later, is of a somewhat different nature.

(34.3) Example. Let $\Lambda' = M_2(\mathbb{Z})$, $A = M_2(\mathbb{Q})$, $\mathbf{I} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, and let $\bar{\mathbb{Z}} = \mathbb{Z}/p\mathbb{Z}$, where p is a rational prime. Setting

$$\Lambda = \mathbb{Z} \cdot \mathbf{I} + p\Lambda',$$

we see that Λ is a \mathbb{Z} -order in A , and $p\Lambda' \subset \Lambda \subset \Lambda'$. Given a Λ -lattice M , let

$$M_0 = p\Lambda' \cdot M \subseteq M,$$

so M_0 is a Λ -sublattice of M . For each $\varphi \in \text{End}_\Lambda M$, we have

$$\varphi(M_0) = \varphi(p\Lambda' \cdot M) = p\Lambda' \varphi(M) \subseteq M_0,$$

so M_0 is a characteristic sublattice of M . Then

$$N = M/M_0 = M/p\Lambda' M$$

is a $(\Lambda/p\Lambda')$ -module, but of course N is not a lattice in this case. Next,

$$\Lambda/p\Lambda' = (\mathbb{Z} \cdot \mathbf{I} + p\Lambda')/p\Lambda' \cong \mathbb{Z}/p\mathbb{Z} = \bar{\mathbb{Z}},$$

so N is a vector space over $\bar{\mathbb{Z}}$.

Now M_0 is a lattice over the maximal order Λ' . Setting

$$L = \left\{ \begin{pmatrix} a \\ b \end{pmatrix} : a, b \in \mathbb{Z} \right\},$$

we see that L is a left Λ' -lattice, and QL is a simple left A -module. Let us show that $M_0 \cong L^{(r)}$ for some r . If L' is any left Λ' -lattice in QL , then L' is in the same genus as L by (26.24), and therefore $L' \cong L$ by (31.26). (The same conclusion can also be obtained from the discussion following the proof of (23.16).) Finally, we use (26.12) to conclude from the above that $M_0 \cong L^{(r)}$ for some r . Further, $N \cong \bar{\mathbb{Z}}^{(s)}$ for some s , and there is a Λ -exact sequence

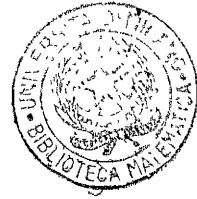
$$0 \rightarrow L^{(r)} \rightarrow M \rightarrow \bar{\mathbb{Z}}^{(s)} \rightarrow 0,$$

in which $L^{(r)}$ is characteristic in M . To find all M 's, we must therefore classify all extensions of $\bar{\mathbb{Z}}^{(s)}$ by $L^{(r)}$. We shall return to this problem in §34D.

Now let L and N be arbitrary Λ -lattices, and let M be an extension of N by L , corresponding to an element $\xi \in \text{Ext}_\Lambda^1(N, L)$. We indicate this fact by writing an exact sequence

(ξ)

$$0 \rightarrow L \rightarrow M \rightarrow N \rightarrow 0,$$



and using the notation

$$(34.3a) \quad M = (N, L; \xi).$$

Of course, ξ determines a family of mutually isomorphic extensions.

We shall now consider the problem as to when two extensions of N by L are isomorphic. Each $\xi \in \text{Ext}_\Lambda^1(N, L)$ determines a family of mutually isomorphic extensions. It often happens, however, that two different extension classes ξ, ξ' will yield isomorphic extensions. The following useful result is due to Heller-Reiner [62]:

(34.4) Proposition. *Let L, L', N and N' be Λ -lattices such that $\text{Hom}_\Lambda(L, N') = \text{Hom}_\Lambda(L', N) = 0$. Let $\xi \in \text{Ext}_\Lambda^1(N, L)$ determine a Λ -lattice M as an extension of N by L , and let $\xi' \in \text{Ext}_\Lambda^1(N', L')$ determine M' . Then $M \cong M'$ if and only if:*

$$(34.4a) \quad \lambda \xi = \xi' \nu \text{ in } \text{Ext}_\Lambda^1(N, L') \text{ for some isomorphisms } \lambda: L \cong L', \nu: N \cong N'.$$

Proof. For convenience, write Ext and Hom in place of Ext_Λ^1 and Hom_Λ . Given any isomorphism $\varphi: M \cong M'$, consider the diagram

$$\begin{array}{ccccccc} (\xi) & 0 & \longrightarrow & L & \xrightarrow{\alpha} & M & \longrightarrow & N & \longrightarrow 0 \\ & & & & & \downarrow \varphi & & & \\ (\xi') & 0 & \longrightarrow & L' & \xrightarrow{\alpha'} & M' & \xrightarrow{\beta'} & N' & \longrightarrow 0 \end{array}$$

with exact rows, and where α, α' are viewed as inclusions. Since $\beta' \varphi \alpha \in \text{Hom}(L, N') = 0$, it follows that φ induces Λ -homomorphisms $\lambda: L \rightarrow L'$ and $\nu: N \rightarrow N'$, and one obtains a commutative diagram. Likewise, φ^{-1} induces maps $\lambda': L' \rightarrow L$ and $\nu': N' \rightarrow N$. Since $\varphi^{-1} \varphi = 1$, we have $\lambda' \lambda = 1$, $\nu' \nu = 1$. Analogously we obtain $\lambda \lambda' = 1$, $\nu \nu' = 1$, so λ and ν are isomorphisms. Conversely, given a commutative diagram in which λ and ν are isomorphisms, the map φ' is also an isomorphism.

Suppose now that we have a commutative diagram $(\lambda, \varphi, \nu): (\xi) \rightarrow (\xi')$. By Exercise 2.12, there exists a commutative diagram with exact rows:

$$\begin{array}{ccccccccc} (\xi) & 0 & \longrightarrow & L & \xrightarrow{\alpha} & M & \longrightarrow & N & \longrightarrow 0 \\ & & \downarrow \lambda & & \downarrow & \downarrow 1 & & \downarrow 1 & \\ (\eta_1) & 0 & \longrightarrow & L' & \longrightarrow & M_1 & \longrightarrow & N & \longrightarrow 0 \\ & & \downarrow 1 & & \downarrow & & \downarrow 1 & & \\ (\eta_2) & 0 & \longrightarrow & L' & \longrightarrow & M_2 & \longrightarrow & N & \longrightarrow 0 \\ & & \downarrow 1 & & \downarrow & & & \downarrow \nu & \\ (\xi') & 0 & \longrightarrow & L' & \longrightarrow & M' & \xrightarrow{\beta'} & N' & \longrightarrow 0. \end{array}$$

Here, M_1 is the pushout of the pair of maps $\{\alpha, \lambda\}$, and M_2 is the pullback of the pair $\{\beta', \nu\}$. Since $\text{Hom}(L, L')$ acts from the left on $\text{Ext}(N, L)$, and $\text{Hom}(N, N')$ acts from the right, the discussion in §8A shows that

$$\eta_1 = \lambda \xi, \quad \eta_2 = \xi' \nu.$$

But the extensions $(\eta_1), (\eta_2)$ are equivalent, so $\eta_1 = \eta_2$ in $\text{Ext}(N, L')$ and (34.4a) is established.

Conversely, if (34.4a) holds, define $\eta_1 = \lambda \xi$, $\eta_2 = \xi' \nu$, as above. Then the extensions (η_1) and (η_2) are equivalent, so there exists a map $M_1 \rightarrow M_2$ making the above diagram commutative. Composition of maps then yields the desired isomorphism $M \cong M'$, which completes the proof of the proposition.

(34.5) Corollary. *Let L and N be arbitrary Λ -lattices such that $\text{Hom}_\Lambda(L, N) = 0$, and let M_1 and M_2 be a pair of extensions of N by L , corresponding to elements $\xi_1, \xi_2 \in \text{Ext}_\Lambda^1(N, L)$, respectively. Then $M_1 \cong M_2$ if and only if*

$$(34.6) \quad \lambda \xi_1 = \xi_2 \nu \text{ in } \text{Ext}_\Lambda^1(N, L) \text{ for some } \lambda \in \text{Aut } L, \nu \in \text{Aut } N.$$

In other words, the isomorphism classes of extensions of N by L are in bijection with the orbits of $\text{Ext}_\Lambda^1(N, L)$ under the action of $(\text{Aut } L) \times (\text{Aut } N)$.

(34.7) Remark. One procedure for classifying Λ -lattices M is now as follows. Let $e \in A$ be a central idempotent, and express M as an extension of a Λ_2 -lattice N by a Λ_1 -lattice L , using the notation of (34.1). Then $\text{Hom}(L, N) = 0$, and likewise if M' is an extension of L' by N' , then also $\text{Hom}(L, N') = 0$. The hypotheses of Proposition 34.4 and its corollary are then satisfied, so M determines L and N up to isomorphism. The preceding discussion shows that a full set of isomorphism invariants of M consists of:

- (i) The isomorphism classes of L and N , and
- (ii) The orbit of the element (ξ) in $\text{Ext}_\Lambda^1(N, L)$ under the actions of $\text{Aut}_\Lambda L$ and $\text{Aut}_\Lambda N$, where (ξ) is the class of the extension M of N by L .

Now let L and N be arbitrary Λ -lattices, not necessarily related to some idempotent $e \in A$ as above. As in §31, we write $L' \vee L$ to indicate that the Λ -lattice L' is in the genus Γ_L of L . By (29.7) and (31.2), there exists an R -isomorphism

$$\text{Ext}_\Lambda^1(N', L') \cong \text{Ext}_\Lambda^1(N, L) \text{ for } N' \vee N, L' \vee L.$$

It seems reasonable to expect that there should be a bijection between the set of $(\text{Aut } L, \text{Aut } N)$ -orbits of $\text{Ext}(N, L)$, and the $(\text{Aut } L', \text{Aut } N')$ -orbits of $\text{Ext}(N', L')$. The remainder of this subsection is devoted to establishing this result under suitable hypotheses. The result is quite useful in later calculations (see §34B, C).

As in (31.1), let $S(\Lambda)$ denote the set of all maximal ideals P in R for which the localization Λ_P is not a maximal order. If Λ is a maximal order, then $S(\Lambda) = \emptyset$, and to avoid distinguishing this case from the case where $S(\Lambda)$ is non-empty, we pick any maximal ideal P_0 of R , and define

$$(34.8) \quad S_0 = \begin{cases} S(\Lambda) & \text{if } S(\Lambda) \neq \emptyset, \\ \{P_0\} & \text{if } S(\Lambda) = \emptyset. \end{cases}$$

By Roiter's Lemma 31.6, there exist Λ -exact sequences

$$0 \rightarrow L \xrightarrow{f} L' \rightarrow T \rightarrow 0, \quad 0 \rightarrow N' \xrightarrow{g} N \rightarrow U \rightarrow 0,$$

where T and U are R -torsion Λ -modules such that $T_P = 0$ and $U_P = 0$ for all $P \in S_0$. As we shall see in a moment, the pair (f, g) determines an R -isomorphism

$$(34.9) \quad t : \mathrm{Ext}(N, L) \cong \mathrm{Ext}(N', L'),$$

where Ext means Ext_Λ^1 . We shall call t the *standard* isomorphism associated with the pair (f, g) .

We proceed to describe t explicitly, using the discussion in §8A. Suppose that $\xi \in \mathrm{Ext}(N, L)$ determines a Λ -lattice M , so there is an exact sequence

$$(\xi) \quad 0 \rightarrow L \xrightarrow{\alpha} M \rightarrow N \rightarrow 0.$$

Then define $f\xi \in \mathrm{Ext}(N, L')$ by the commutative diagram

$$\begin{array}{ccccccc} (\xi) & 0 & \longrightarrow & L & \xrightarrow{\alpha} & M & \longrightarrow & N & \longrightarrow 0 \\ & & & f \downarrow & & \downarrow & & 1 \downarrow & \\ (f\xi) & 0 & \longrightarrow & L' & \longrightarrow & M_0 & \longrightarrow & N & \longrightarrow 0, \end{array}$$

where M_0 is the pushout of the pair of maps $\{\alpha, f\}$. Then $t(\xi) = (f\xi)g$, where $(f\xi)g$ is defined by the commutative diagram

$$\begin{array}{ccccccc} (f\xi) & 0 & \longrightarrow & L' & \longrightarrow & M_0 & \xrightarrow{\beta} & N & \longrightarrow 0 \\ & & & 1 \uparrow & & \uparrow & & g \uparrow & \\ (f\xi)g & 0 & \longrightarrow & L' & \longrightarrow & M' & \longrightarrow & N' & \longrightarrow 0, \end{array}$$

in which M' is the pullback of the pair $\{\beta, g\}$.

For each $P \in S_0$, both f_P and g_P are isomorphisms, and therefore so is t_P . It follows at once from (29.7) that t is an isomorphism, and (34.9) is established.

Furthermore, we have $M' \vee M$ since $(M')_P \cong M_P$ for each $P \in S_0$. We caution the reader that it is usually possible to find other isomorphisms of Ext 's which need not arise from “change of variable” maps. Nevertheless, we have:

(34.10) Lemma. *The inverse of a standard isomorphism is also a standard isomorphism.*

Proof. Choose a nonzero ideal α of R , all of whose prime factors lie in S_0 , such that $\alpha \cdot \text{Ext}(N, L) = 0$. Then for any $h \in \text{End } N$ such that $h \equiv 1 \pmod{\alpha}$ (that is, $h - 1 \in \alpha \cdot \text{End } N$), h induces the identity map on $\text{Ext}(N, L)$.

Now let t be a standard isomorphism as in (34.9), associated with the pair (f, g) , where $f: L \rightarrow L'$, $g: N' \rightarrow N$. Since f_P is an isomorphism for each $P \in S_0$, we may form its inverse $f_P^{-1}: (L')_P \rightarrow L_P$ for each such P . Then choose $h \in \text{Hom}(L', L)$ such that h approximates f_P^{-1} at each $P \in S_0$. Specifically, we can choose h so that

$$hf \equiv 1 \pmod{\alpha \cdot \text{End } L}.$$

Since $\ker h_P = 0$ for $P \in S_0$, it follows that h is a monomorphism, and hf acts as 1 on $\text{Ext}(L, N)$. Likewise, there exists a monomorphism $j: N \rightarrow N'$ such that $gj \equiv 1 \pmod{\alpha \cdot \text{End } N}$, and then gj acts as 1 on $\text{Ext}(L, N)$. The pair (h, j) induces a standard isomorphism

$$t': \text{Ext}(N', L') \cong \text{Ext}(N, L),$$

and clearly $t't = 1$ on $\text{Ext}(N, L)$. But then $t' = t^{-1}$, and the lemma is proved.

Since each $\xi \in \text{Ext}(N, L)$ determines a class of equivalent extensions of N by L , we obtain (see also Exercises 31.7, 31.8):

(34.11) Corollary. *Let $L' \vee L$, $N' \vee N$, and let $t: \text{Ext}(N, L) \cong \text{Ext}(N', L')$ be a standard isomorphism. Then t gives a bijection between the set of equivalence classes of extensions of N by L , and the corresponding set for N' , L' .*

We have *not* shown above that there is a bijection between *isomorphism* classes of extensions. As we have seen in (34.7), for instance, a given isomorphism class may be a union of many equivalence classes. To overcome this difficulty, we shall need to impose the extra hypothesis that “cancellation” is possible in certain cases. Let us begin with:

(34.12) Definition. We say that *cancellation* is valid in the genus Γ of left Λ -lattices if for all $L, M, N \in \Gamma$,

$$L \oplus M \cong L \oplus N \Rightarrow M \cong N.$$

As we shall see in Chapter 11, cancellation is valid for most cases, but *not* for all cases. In order to state Jacobinski's *sufficiency* conditions for cancellation, some terminology is needed. Let $M \in \Gamma$, and consider the K -algebra $B = \text{End}_A KM$. We call M an *Eichler lattice* if B satisfies the Eichler condition relative to R (see MO (38.1)). In the special case where K is an algebraic number field and $R = \text{alg. int. } \{K\}$, this condition means that no Wedderburn component of B is a totally definite quaternion algebra. (If B is a central simple K -algebra, we call B a *totally definite quaternion algebra* if each infinite prime P of K is a real prime, and for each such P , the P -adic completion of B is isomorphic to the algebra of real quaternions (see Example 7.40)). Thus, the K -algebra B certainly satisfies the Eichler condition whenever B is a split semisimple algebra; the condition is also satisfied if K has at least one complex prime.

In Chapter 11, we shall prove the deep result:

(34.13) Jacobinski Cancellation Theorem. *Let K be a global field, and let M be an Eichler Λ -lattice. Then cancellation is valid in the genus Γ_M of M .*

We are now ready to resume our discussion of extensions of lattices. Using the theorem above, we now establish:

(34.14) Theorem (Reiner [78]). *Let L and N be left Λ -lattices such that $L \oplus N$ is an Eichler lattice, and let $L' \vee L$, $N' \vee N$. Let $t: \text{Ext}(N, L) \cong \text{Ext}(N', L')$ be a standard isomorphism as in (34.9). Then t induces a bijection between the set of isomorphism classes of extensions of N by L , and the set of isomorphism classes of extensions of N' by L' .*

Proof. Let M be an extension of N by L , corresponding to the element $\xi \in \text{Ext}(N, L)$; all M 's belonging to the same ξ are isomorphic to one another. Let $\xi' = t(\xi) \in \text{Ext}(N', L')$, and let ξ' determine the Λ -lattice M' as an extension of N' by L' ; then* $M' \vee M$. Now let $\xi_1 \in \text{Ext}(N, L)$ determine the extension M_1 , and let $t(\xi_1)$ determine M'_1 . We must prove that $M \cong M_1$ if and only if $M' \cong M'_1$.

It suffices to prove the result in one direction, since by (34.10), the inverse of a standard isomorphism is also standard. Furthermore, every standard isomorphism can be expressed as a product of two standard isomorphisms, each of which involves a change of only one of the “variables” L and N . It is therefore sufficient to prove the result when there is a change in only one variable, say L . Thus, we start with an exact sequence

$$0 \rightarrow L \xrightarrow{f} L' \rightarrow T \rightarrow 0, \text{ where } T_P = 0 \text{ for } P \in S_0.$$

*See the discussion which precedes (34.10).

Given any $\xi \in \text{Ext}(N, L)$, we have a commutative diagram with exact rows

$$\begin{array}{ccccccc} (\xi) & 0 & \longrightarrow & L & \longrightarrow & M & \longrightarrow & N & \longrightarrow 0 \\ & & f \downarrow & & g \downarrow & & 1 \downarrow & & \\ (f\xi) & 0 & \longrightarrow & L' & \longrightarrow & M' & \longrightarrow & N & \longrightarrow 0, \end{array}$$

so by the Snake Lemma we obtain an exact sequence

$$0 \rightarrow M \rightarrow M' \rightarrow \text{cok } f \rightarrow 0, \quad \text{cok } f = L'/f(L),$$

with $(\text{cok } f)_P = 0$ for $P \in S_0$. If $\xi_1 \in \text{Ext}(N, L)$ gives rise to M_1 , then in the same way we obtain another exact sequence

$$0 \rightarrow M_1 \rightarrow M'_1 \rightarrow \text{cok } f \rightarrow 0.$$

Comparing these two exact sequences and using (31.8), we get

$$M \oplus M'_1 \cong M_1 \oplus M'$$

(this is just the assertion in (31.11)). But now $M \vee M'$, $M_1 \vee M'_1$. If $M \cong M_1$, then all of the lattices M , M' , M_1 , M'_1 lie in the same genus. We have $KM \cong K(L \oplus N)$, and since $L \oplus N$ is an Eichler lattice by hypothesis, so is M . The Jacobinski Cancellation Theorem can now be applied, and we conclude that $M'_1 \cong M'$, as desired. This completes the proof.

It seems likely that the above theorem holds true without the hypothesis that $L \oplus N$ be an Eichler lattice. In any case, we have the following consequence of (34.5) and (34.14):

(34.15) Corollary. *Let L and N be Λ -lattices such that $\text{Hom}(L, N) = 0$, and such that $L \oplus N$ is an Eichler lattice. Let $L' \vee L$, $N' \vee N$. Then each standard isomorphism $t : \text{Ext}(N, L) \cong \text{Ext}(N', L')$ gives a bijection between the set of orbits of $\text{Ext}(N, L)$ under the actions of $\text{Aut } L$ and $\text{Aut } N$, and the corresponding set of orbits for the pair N', L' .*

§34B. Cyclic p -Groups

We shall apply the machinery of §34A to the problem of classifying Λ -lattices, where Λ is the integral group ring $\mathbb{Z}G$ of a cyclic group $G = \langle x \rangle$ of order p^κ , with p prime and $\kappa \geq 1$. A complete classification cannot be obtained for $\kappa > 2$, so we shall give some partial results in this subsection, and then use them in §34C to handle the case when $\kappa = 2$.

Throughout this subsection, we fix the following notation:

R^\times = group of units of a ring R

$\Lambda_\kappa = \mathbb{Z}[x]/(x^{p^\kappa} - 1)$

$\hat{\mathbb{Q}}, \hat{\mathbb{Z}}$, etc. = p -adic completions

$\Phi_i(x) =$ cyclotomic polynomial* of order p^i and degree $\varphi(p^i)$

$$\Phi_i(x) = \sum_{j=0}^{p-1} x^{j \cdot p^{i-1}} \text{ if } i \geq 1, \quad \Phi_0(x) = x - 1$$

ω_i = primitive p^i -th root of 1 over \mathbb{Q}

$K_i = \mathbb{Q}(\omega_i)$, $R_i = \text{alg. int. } \{K_i\} = \mathbb{Z}[\omega_i] \cong \mathbb{Z}[x]/(\Phi_i(x))$

$\hat{K}_i = \hat{\mathbb{Q}}(\omega_i)$, $R_i = \hat{\mathbb{Z}}[\omega_i] \cong \hat{\mathbb{Z}}[x]/(\Phi_i(x))$.

In the above, i ranges from 0 to κ . For $i \geq 1$, $P_i = (1 - \omega_i)R_i$ is the unique maximal ideal of R_i containing p , and p is completely ramified in K_i . We have

$$pR_i = P_i^{\varphi(p^i)}, \quad R_i/P_i \cong \mathbb{Z}/p\mathbb{Z} = \bar{\mathbb{Z}}.$$

Further, the P_i -adic completion \hat{K}_i of K_i coincides with its p -adic completion, and $\Phi_i(x)$ is irreducible in $\mathbb{Z}[x]$ and in $\hat{\mathbb{Z}}[x]$. The unique maximal ideal of \hat{R}_i is $\hat{P}_i = (1 - \omega_i)\hat{R}_i$.

We identify $\mathbb{Z}G$ with Λ_κ , and omit the subscript κ when there is no danger of confusion. Since G is a p -group, two Λ -lattices M_1 and M_2 lie in the same genus if and only if $\hat{M}_1 \cong \hat{M}_2$.

(34.16) Lemma. *Let M be a Λ -lattice. Then M is indecomposable if and only if \hat{M} is indecomposable.*

Proof. By Exercise 21.1, we have

$$\mathbb{Q}G = \mathbb{Q}[x]/(x^{p^\kappa} - 1) \cong \coprod_{i=0}^{\kappa} K_i, \quad \hat{\mathbb{Q}}G \cong \coprod_{i=0}^{\kappa} \hat{K}_i.$$

Since the completion \hat{K}_i of K_i is a field, each simple left $\mathbb{Q}G$ -module remains simple under passage to the p -adic completion. It follows from Heller's

*See CR(21.9) or Exercise 21.1.

Theorem 30.18 that every $\hat{\Lambda}$ -lattice is the completion of some $\tilde{\Lambda}$ -lattice, where $\tilde{\Lambda}$ is the localization of Λ at p . But every $\tilde{\Lambda}$ -lattice is the localization of some Λ -lattice, by (23.14). Therefore every $\hat{\Lambda}$ -lattice is the completion of a Λ -lattice. Hence if M is decomposable, so is M , by (31.13). This completes the proof. (The proof of (36.1) shows that the result holds for every p -group, not necessarily cyclic, when $p > 2$.)

Now let M be a Λ -lattice, and set

$$L = \{m \in M : (x^{p^{\kappa-1}} - 1)m = 0\}.$$

By (34.2), L is a characteristic sublattice of M , and there is an exact sequence of Λ -lattices

$$0 \rightarrow L \rightarrow M \rightarrow N \rightarrow 0, \quad N = M/L,$$

in which L is a $\Lambda_{\kappa-1}$ -lattice, and N is an R_κ -lattice. (Technically, N is a f.g. left R_κ -module which is \mathbb{Z} -torsionfree. It follows at once from Exercise 23.9 that N is also R_κ -torsionfree, and is therefore an R_κ -lattice.) Analogously, every $\hat{\Lambda}$ -lattice is an extension of an \hat{R}_κ -lattice by a $\hat{\Lambda}_{\kappa-1}$ -lattice.

The problem of classifying all Λ_κ -lattices is thus reduced to the following:

- (i) Classify all $\Lambda_{\kappa-1}$ -lattices L and all R_κ -lattices N .
- (ii) Classify the isomorphism classes of extensions of N by L .

Since R_κ is a Dedekind domain, it follows that we may write

$$N \cong \coprod_{k=1}^s \mathfrak{c}_k, \quad \text{so } N \vee R_\kappa^{(s)},$$

where the $\{\mathfrak{c}_k\}$ are R_κ -ideals in K_κ . The isomorphism invariants of N are its rank s , and its Steinitz class (see (4.13)). Of course, the problem of finding all $\Lambda_{\kappa-1}$ -lattices is the same as our original problem, except that κ has decreased by 1. Further, by (34.7), problem (ii) is equivalent to determining the $(\text{Aut } N, \text{Aut } L)$ -orbits of $\text{Ext}(N, L)$. By (34.15), in this determination we may replace L by L' , N by N' , where $L' \vee L$ and $N' \vee N$.

The same discussion shows that the genus of M is completely determined by the genus of L , the rank s of N , and an $(\text{Aut } \hat{N}, \text{Aut } \hat{L})$ -orbit in $\text{Ext}(\hat{N}, \hat{L})$.

In the special case where $\kappa=1$, we have $\Lambda_{\kappa-1}=\mathbb{Z}$, and L is just a \mathbb{Z} -lattice. We may treat a slightly more general version of this situation, as follows. Let $\kappa \geq 1$, and let $E = \mathbb{Z}[x]/(h(x))$, where $h(x)$ is a non-constant monic factor of $x^{p^{\kappa-1}} - 1$ in $\mathbb{Z}[x]$. Then E is an indecomposable \mathbb{Z} -order which is a factor ring of $\Lambda_{\kappa-1}$ (see Exercise 34.5). We shall treat the case in which L is a locally free E -lattice, that is, $L \vee E^{(r)}$ for some r . Our aim is to classify all Λ -lattices M which are extensions of an R_κ -lattice N by a locally free E -lattice L .

Suppose now that L and N are given as above. Since $L \vee E^{(r)}$ and $N \vee R_{\kappa}^{(s)}$ for some s , we have

$$\mathrm{Ext}(N, L) \cong \{\mathrm{Ext}(R_{\kappa}, E)\}^{r \times s},$$

where $\{\Omega\}^{r \times s}$ means the set of $r \times s$ matrices with entries in Ω . Since $(x^{p^{\kappa}-1} - 1)E = 0$, Step 3 of the proof of (25.26) shows that

$$\mathrm{Ext}(R_{\kappa}, E) \cong E/\Phi_{\kappa}(x)E = E/pE = \bar{E},$$

where bar denotes reduction mod p . Thus

$$\mathrm{Ext}(N, L) \cong \bar{E}^{r \times s}, \bar{E} \cong \bar{\mathbb{Z}}[x]/(\bar{h}(x)) = \bar{\mathbb{Z}}[x]/(x-1)^d \bar{\mathbb{Z}}[x],$$

where d is the degree of the polynomial $h(x)$. Since Λ is commutative, $\mathrm{Ext}(N, L)$ is naturally a Λ -module, by virtue of the action of Λ on either N or L . The above isomorphisms are easily seen to be Λ -isomorphisms.

In addition, when $N = R_{\kappa}^{(s)}$ and $L = E^{(r)}$, we have

$$\mathrm{Aut}_{\Lambda} N = \mathrm{Aut}_{R_{\kappa}} N \cong GL_s(R_{\kappa}), \mathrm{Aut}_{\Lambda} L = \mathrm{Aut}_E L \cong GL_r(E).$$

We therefore obtain:

(34.17) Proposition. *Let N be an R_{κ} -lattice of rank s , and L a locally free E -lattice such that $L \vee E^{(r)}$. Then there is a bijection between the set of orbits of $\mathrm{Ext}_{\Lambda}^1(N, L)$ under the actions of $\mathrm{Aut}(N)$ and $\mathrm{Aut}(L)$, and the set of orbits of $(\bar{E})^{r \times s}$ under the actions of $GL_r(E)$ and $GL_s(R)$.*

We note that there is a surjection $E \rightarrow E/pE = \bar{E}$, and also surjections

$$R_{\kappa} \rightarrow R_{\kappa}/pR_{\kappa} \cong \bar{\mathbb{Z}}[x]/((x-1)^{\varphi(p^{\kappa})}) \rightarrow \bar{E},$$

since $d = \deg h(x) \leq p^{\kappa-1} \leq \varphi(p^{\kappa})$. By virtue of these surjections, $GL_r(E)$ and $GL_s(R)$ act on $(\bar{E})^{r \times s}$, and this agrees with the action arising from their actions on L and N , respectively. Furthermore, we observe that \bar{E} is a local principal ideal ring, whose ideals are powers of $(x-1)\bar{E}$. In this situation we can describe the orbits of $\bar{E}^{r \times s}$ explicitly, following the treatment in Reiner [78].

Changing notation, let Γ and Δ be a pair of commutative rings, and let $\varphi: \Gamma \rightarrow \bar{\Gamma}$, $\psi: \Delta \rightarrow \bar{\Gamma}$, be a pair of ring surjections. We assume that $\bar{\Gamma}$ is a local principal ideal ring, whose distinct ideals are given by

$$\{\lambda^k \bar{\Gamma} : 0 \leq k \leq e\}, \text{ where } \lambda^e \bar{\Gamma} = 0.$$

Let $\bar{\Gamma}^{r \times s}$ be the $\bar{\Gamma}$ -module consisting of all $r \times s$ matrices over $\bar{\Gamma}$. We shall find

the $(GL_r(\Gamma), GL_s(\Delta))$ -orbits of $\bar{\Gamma}^{r \times s}$. Given $\xi_1, \xi_2 \in \bar{\Gamma}^{r \times s}$, we write $\xi_1 \approx \xi_2$, and call them *globally equivalent*, if

$$\xi_2 = \alpha \xi_1 \beta \text{ for some } \alpha \in GL_r(\Gamma), \beta \in GL_s(\Delta).$$

Note that α acts as $\varphi_*(\alpha)$, where φ induces the group homomorphism $\varphi_*: GL(\Gamma) \rightarrow GL(\bar{\Gamma})$; likewise, β acts as $\psi_*(\beta)$, where $\psi_*: GL(\Delta) \rightarrow GL(\bar{\Gamma})$.

If $\xi_2 \approx \xi_1$, then of course $\xi_2 = \mu \xi_1 \nu$ for some $\mu, \nu \in GL(\bar{\Gamma})$, so the matrices ξ_1 and ξ_2 are equivalent in the usual (weaker) sense. We can then use the machinery of elementary divisors over $\bar{\Gamma}$; each elementary divisor may be chosen to be a power of the prime element λ of $\bar{\Gamma}$. We put

$$\text{el. div. } (\xi) = \text{set of elementary divisors of } \xi,$$

where $\xi \in \bar{\Gamma}^{r \times s}$. Clearly, for $\xi_1, \xi_2 \in \bar{\Gamma}^{r \times s}$,

$$(34.18) \quad \xi_1 \approx \xi_2 \Rightarrow \text{el. div. } (\xi_1) = \text{el. div. } (\xi_2).$$

We need some easy facts about global equivalence of matrices over $\bar{\Gamma}$. Letting $\bar{\Gamma}^\times$ denote the group of units of $\bar{\Gamma}$, we have:

(34.19) Lemma. *For $u \in \bar{\Gamma}^\times$, let D_u denote a diagonal matrix in $GL_r(\bar{\Gamma})$ with diagonal entries $u, u^{-1}, 1, \dots, 1$, arranged in any order. Let D_u^* denote an analogous matrix in $GL_s(\bar{\Gamma})$. Then for any $\xi \in \bar{\Gamma}^{r \times s}$, we have*

$$\xi \approx D_u \xi, \quad \xi \approx \xi D_u^*.$$

Proof. In $GL_2(\bar{\Gamma})$, there is an identity

$$(34.20) \quad \begin{pmatrix} u & 0 \\ 0 & u^{-1} \end{pmatrix} = \begin{pmatrix} 1 & u^{-1} \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & u^{-1}-1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ -u & 1 \end{pmatrix}.$$

Hence D_u is expressible as a product of elementary* matrices in $GL_r(\bar{\Gamma})$. But each factor is the image of an elementary matrix over Γ , and therefore $\xi \approx D_u \xi$. Likewise we obtain $\xi \approx \xi D_u^*$.

(34.21) Proposition. (i) *If $r \leq s$, then each $\xi \in \bar{\Gamma}^{r \times s}$ is globally equivalent to a matrix $[\mathbf{D} \ \mathbf{0}]$, where*

$$(34.22) \quad \mathbf{D} = \text{diag}(\lambda^{k_1} u_1, \dots, \lambda^{k_r} u_r), \quad 0 \leq k_1 \leq \dots \leq k_r \leq e, \quad u_i \in \bar{\Gamma}.$$

(ii) *If $r \geq s$, then $\xi \approx \begin{bmatrix} \mathbf{D}^* \\ \mathbf{0} \end{bmatrix}$, where \mathbf{D}^* is a diagonal $s \times s$ matrix of the above type.*

*An *elementary* matrix is one obtained from the identity matrix by replacing exactly one off-diagonal zero entry by some element of the ring.

(iii) Let $\xi_1, \xi_2 \in \bar{\Gamma}^{r \times s}$, where $r \neq s$. Then

$$\xi_1 \approx \xi_2 \text{ if and only if } \text{el. div.}(\xi_1) = \text{el. div.}(\xi_2).$$

Proof. For (i), let $\xi \in \bar{\Gamma}^{r \times s}$, where $r \leq s$. Since $\bar{\Gamma}$ is a local principal ideal ring, we can bring ξ into the form $[\mathbf{D} \ 0]$, with \mathbf{D} as in (34.22), by a sequence of left and right multiplications by elementary matrices over $\bar{\Gamma}$. Each such elementary matrix is the image of a corresponding elementary matrix over Γ or Δ , and therefore $\xi \approx [\mathbf{D} \ 0]$ as claimed. An analogous argument gives (ii).

Suppose now that $\xi \approx [\mathbf{D} \ 0]$, with \mathbf{D} as in (34.22). Then

$$\text{el. div.}(\xi) = \{\lambda^{k_1}, \dots, \lambda^{k_r}\}.$$

We have already shown that $\text{el. div.}(\xi)$ is an invariant of the global equivalence class of ξ . Hence, to prove (iii), we may assume that $r < s$ and that $\text{el. div.}(\xi_1) = \text{el. div.}(\xi_2)$; we need to show that $\xi_1 \approx \xi_2$ in this case. Since $\xi_1 \approx [\mathbf{D} \ 0]$ for some \mathbf{D} as above, we have by (34.19)

$$\begin{aligned} \xi_1 &\approx [\mathbf{D} \ 0] \cdot \text{diag} \left(u_1^{-1}, u_2^{-1}, \dots, u_r^{-1}, \underbrace{u_1 \cdots u_r, 1, \dots, 1}_{s-r} \right) \\ &\approx [\mathbf{D}_1 \ 0], \text{ where } \mathbf{D}_1 = \text{diag}(\lambda^{k_1}, \dots, \lambda^{k_r}). \end{aligned}$$

Since $\text{el. div.}(\xi_1) = \text{el. div.}(\xi_2)$, we obtain $\xi_1 \approx \xi_2$, which completes the proof of the proposition.

The preceding result shows that when $r \neq s$, the set $\text{el. div.}(\xi)$ completely determines the global equivalence class of an element $\xi \in \bar{\Gamma}^{r \times s}$. The case where $r = s$ is considerably more interesting and difficult, and some additional notation is required in order to state the main result.

Suppose that $\xi \in \bar{\Gamma}^{r \times r}$ has elementary divisors $\lambda^{k_1}, \dots, \lambda^{k_r}$, and let

$$\xi \approx \mathbf{D} = \text{diag}(\lambda^{k_1} u_1, \dots, \lambda^{k_r} u_r),$$

as in (34.22). Let

$$(34.23) \quad \Omega_\xi = (\Gamma')^\circ / (\Gamma^* \Delta^*), \text{ where } \Gamma' = \Gamma / \lambda^{e-k_r} \Gamma \cong \bar{\Gamma} / \lambda^{e-k_r} \bar{\Gamma},$$

and where Γ^* and Δ^* denote the images of Γ' and Δ' , respectively, in the group of units $(\Gamma')^\circ$. Note that the ring Γ' and the group Ω_ξ depend only upon $\text{el. div.}(\xi)$. We now set

$$w(\xi) = \text{image of } u_1 u_2 \cdots u_r \text{ in } \Omega_\xi,$$

assuming $\xi \approx \mathbf{D}$ as above. Our main result, due to Reiner [78], is as follows:

(34.24) **Theorem.** Let $\xi_1, \xi_2 \in \bar{\Gamma}^{r \times r}$. Then $\xi_1 \approx \xi_2$ if and only if

$$\text{el. div.}(\xi_1) = \text{el. div.}(\xi_2), \text{ and } w(\xi_1) = w(\xi_2) \text{ in } \Omega_\xi.$$

Proof. Step 1. Supposing the conditions satisfied, let $\xi_1 \approx \mathbf{D}$ as above, and let

$$\xi_2 \approx \text{diag}(\lambda^{k_1} u'_1, \dots, \lambda^{k_r} u'_r), u'_i \in \bar{\Gamma}.$$

Setting $u = u_1 \cdots u_r$ and $u' = u'_1 \cdots u'_r$, it follows from (34.19) that

$$(34.25) \quad \xi_1 \approx \text{diag}(\lambda^{k_1}, \dots, \lambda^{k_{r-1}}, \lambda^{k_r} u), \quad \xi_2 \approx \text{diag}(\lambda^{k_1}, \dots, \lambda^{k_{r-1}}, \lambda^{k_r} u').$$

The condition $w(\xi_1) = w(\xi_2)$ means that $u' \equiv \gamma u \delta$ in Γ' for some $\gamma \in \Gamma^*$, $\delta \in \Delta^*$. But then $\lambda^{k_r} u' = \gamma \cdot \lambda^{k_r} u \cdot \delta$ in $\bar{\Gamma}$, and therefore

$$\text{diag}(1, \dots, 1, \gamma) \cdot \text{diag}(\lambda^{k_1}, \dots, \lambda^{k_r} u) \cdot \text{diag}(1, \dots, 1, \delta) = \text{diag}(\lambda^{k_1}, \dots, \lambda^{k_r} u').$$

This implies that $\xi_1 \approx \xi_2$, as desired.

Step 2. Assume conversely that $\xi_1 \approx \xi_2$, so then $\text{el. div.}(\xi_1) = \text{el. div.}(\xi_2)$, and we may assume that ξ_1 and ξ_2 are equal to the diagonal matrices given in (34.25). The hypotheses imply that $\gamma \xi_1 = \xi_2 \delta$ for some $\gamma \in GL_r(\Gamma)$, $\delta \in GL_s(\Delta)$. Our aim is to use determinants to show that $(\det \gamma) u = u' (\det \delta)$ in the ring Γ' defined in (34.23). Set $\mathbf{D}_0 = \text{diag}(\lambda^{k_1}, \dots, \lambda^{k_r})$. The equality $\gamma \xi_1 = \xi_2 \delta$ can be rewritten as

$$\mu \mathbf{D}_0 = \mathbf{D}_0 \nu, \text{ where } \mu = \gamma \cdot \text{diag}(1, \dots, 1, u), \nu = \text{diag}(1, \dots, 1, u') \cdot \delta.$$

As we shall show in our next step, the above implies that

$$(\det \mu) \cdot \lambda^{k_r} = (\det \nu) \cdot \lambda^{k_r} \text{ in } \bar{\Gamma}.$$

Since

$$\det \mu = u \cdot \det \gamma \in u \cdot \Gamma^*, \quad \det \nu = u' \cdot \det \delta \in u' \cdot \Delta^*,$$

this implies that the images of u and u' in (Γ') differ by factors from Γ^* and Δ^* . Hence $w(\xi_1) = w(\xi_2)$, as claimed.

Step 3. To complete the proof, it suffices to establish the following interesting result about determinants:

(34.26) **Lemma.** Let R be an arbitrary commutative ring, and let $\mathbf{D} = \text{diag}(d_1, \dots, d_m)$ be a matrix with entries in R , such that

$$r_1 d_1 = \cdots = r_{m-1} d_{m-1} = d_m$$

for some elements $r_i \in R$. Let \mathbf{X} and \mathbf{Y} be $m \times m$ matrices over R such that $\mathbf{XD} = \mathbf{DY}$. Then

$$(\det \mathbf{X}) d_m = (\det \mathbf{Y}) d_m \text{ in } R.$$

Proof. Write $\mathbf{X} = (x_{ij})$, $\mathbf{Y} = (y_{ij})$. From $\mathbf{XD} = \mathbf{DY}$ we obtain

$$x_{ij}d_j = d_i y_{ij}, \text{ for } 1 \leq i, j \leq m.$$

Let $\pi: \{1, \dots, m\} \rightarrow \{i_1, \dots, i_m\}$ be any permutation of the symbols $1, \dots, m$. A typical term in the expansion of $\det \mathbf{X}$ is of the form

$$\pm x_{1i_1} \cdots x_{mi_m} d_m,$$

so we need only verify that for each π , we have

$$(34.27) \quad x_{1i_1} \cdots x_{mi_m} d_m = y_{1i_1} \cdots y_{mi_m} d_m.$$

Write π as a product of disjoint cycles, and suppose (by way of illustration) that (a, b, c) is a 3-cycle occurring as a factor of π . Then

$$\begin{aligned} x_{ab}x_{bc}x_{ca}d_m &= r_a x_{ab}x_{bc}x_{ca}d_a = r_a x_{ab}x_{bc}d_c y_{ca} \\ &= r_a x_{ab} \cdot d_b y_{bc} \cdot y_{ca} = r_a d_a y_{ab} y_{bc} y_{ca} = d_m \cdot y_{ab} y_{bc} y_{ca}. \end{aligned}$$

The same procedure applies to each of the cycles occurring as a factor of π . This establishes (34.27), and completes the proof of the lemma, as well as the proof of Theorem 34.24.

We now return to the situation described in Proposition 34.17, since we can use the results of Theorem 34.24 to classify the orbits of $\bar{E}^{r \times s}$ under the actions of $GL_r(E)$ and $GL_s(R_\kappa)$. Since each orbit contains a diagonalized matrix, it follows that there are exactly three kinds of indecomposable Λ -lattices M which are extensions of an R_κ -lattice N by a locally free E -lattice L . Furthermore, all extensions M can be completely classified, up to isomorphism. We summarize our results in the following:

(34.28) Theorem (Reiner [78]). Let $\kappa \geq 1$, and set

$$\Lambda = \mathbb{Z}[x]/(x^{p^\kappa} - 1), E = \mathbb{Z}[x]/(h(x)), R_\kappa = \mathbb{Z}[x]/(\Phi_\kappa(x)),$$

where $h(x)$ is a monic factor of $x^{p^{\kappa-1}} - 1$ in $\mathbb{Z}[x]$ of degree d , and $\Phi_\kappa(x)$ is the cyclotomic polynomial of order p^κ and degree $\varphi(p^\kappa)$. Let

$$\bar{E} = E/pE \cong \bar{\mathbb{Z}}[\lambda]/(\lambda^d), \text{ where } \lambda = x - 1.$$

Let \mathfrak{b} range over the R_κ -ideals in the cyclotomic field $K_\kappa = \mathbb{Q}[x]/(\Phi_\kappa(x))$, and let

\mathfrak{c} range over all locally free ideals of E (that is, all ideals in the genus of E). There is an isomorphism of Λ -modules

$$\mathrm{Ext}_{\Lambda}^1(\mathfrak{b}, \mathfrak{c}) \cong \bar{E},$$

which we treat as an identification.

(i) Let M be an indecomposable Λ -lattice which is an extension of an R_{κ} -lattice by a locally free E -lattice. Then M is isomorphic to exactly one of the following: \mathfrak{b} , \mathfrak{c} , and $(\mathfrak{b}, \mathfrak{c}; \lambda^k u)$, where \mathfrak{b} ranges over a full set of ideal class representatives of R_{κ} , \mathfrak{c} ranges over a full set of isomorphism class representatives of locally free ideals of E , and where $(\mathfrak{b}, \mathfrak{c}; \lambda^k u)$ denotes a non-split extension of \mathfrak{b} by \mathfrak{c} , corresponding to the extension class $\lambda^k u \in \bar{E} \cong \mathrm{Ext}(\mathfrak{b}, \mathfrak{c})$. Here, $0 \leq k < d$ and $u \in \bar{E}$. Further, the isomorphism class of $(\mathfrak{b}, \mathfrak{c}; \lambda^k u)$ is completely determined by the classes of \mathfrak{b} and \mathfrak{c} , the integer k , and the image of u in the group

$$\Omega_k = (E')/(E^* R_{\kappa}^*), \text{ where } E' = \bar{E}/(\lambda^{d-k}) \cong \bar{\mathbb{Z}}[\lambda]/(\lambda^{d-k}).$$

Here, E^* and R_{κ}^* denote the images of E and R_{κ} , respectively, in (E') .

(ii) Let M be an arbitrary Λ -lattice which is an extension of an R_{κ} -lattice N by a locally free E -lattice L . Then we may express M as a direct sum of indecomposable Λ -lattices:

$$(34.29) \quad M \cong \coprod_{i=1}^a (\mathfrak{b}_i, \mathfrak{c}_i; \lambda^{k_i} u_i) \oplus \coprod_{j=a+1}^{a+b} \mathfrak{b}_j \oplus \coprod_{k=a+1}^{a+c} \mathfrak{c}_k,$$

where $0 \leq k_i < d$, $u_i \in \bar{E}$ for each i . For this M , we have

$$N \cong \coprod_{i=1}^{a+b} \mathfrak{b}_i, \quad L \cong \coprod_{j=1}^{a+c} \mathfrak{c}_j.$$

(iii) The genus of the lattice M in (34.29) is completely determined by the following invariants:

$$\begin{cases} a+b = R_{\kappa}\text{-rank of } N; \\ a+c = E\text{-rank of } L; \\ \text{the set of exponents } k_1, \dots, k_a. \end{cases}$$

(iv) For M as in (34.29), the additional invariants of the isomorphism class of M , needed to determine this isomorphism class, once the genus invariants are given as in (iii), are as follows:

(I) The isomorphism class of $\coprod_{i=1}^{a+b} \mathfrak{b}_i$, that is, the Steinitz class of N .

(II) The isomorphism class of $\coprod_{i=1}^{a+c} \mathfrak{c}_i$, that is, the “Steinitz class” of L .

(III) Only for the case where $b=c=0$, the image of $u_1 \cdots u_a$ in the multiplicative group $W=W_M$, defined by

$$W = (E')/(E^* R_\kappa^*),$$

where

$$m = \text{Max}(k_1, \dots, k_a), E' = \bar{E}/(\lambda^{d-m}) \cong \bar{\mathbb{Z}}[\lambda]/(\lambda^{d-m}).$$

Proof. Let M be an extension of N by L , corresponding to an extension class $\xi \in \text{Ext}_\Lambda^1(N, L)$. We identify $\text{Ext}_\Lambda^1(N, L)$ with $\bar{E}^{r \times s}$, as in the discussion preceding (34.17). The lattice M is then determined up to isomorphism by the isomorphism classes of N and L , and the $(GL_r(E), GL_s(R_\kappa))$ -orbit of ξ in $\bar{E}^{r \times s}$. Since the orbit of ξ contains a diagonalized matrix, with diagonal entries of the form $\lambda^k u$, $0 \leq k < d$, $u \in \bar{E}$, the only possible indecomposable M 's are those given in (i). The assertion in (i), as to the isomorphism invariants of $(b, c; \lambda^k u)$, is a direct consequence of (34.24).

Now let M be expressed as in (34.29), in which case the expressions given for N and L are obvious. The extension class ξ determined by M is given by the matrix

$$\xi = \begin{bmatrix} \lambda^{k_1} u_1 & & & & & 0 \\ & \ddots & & & & \vdots \\ & & \lambda^{k_a} u_a & & & \vdots \\ & & & \ddots & & \vdots \\ 0 & \cdots & \cdots & \cdots & & 0 \end{bmatrix}^{(a+c) \times (a+b)}.$$

Since $\{k_1, \dots, k_a\}$ are the genus invariants associated with ξ , assertion (iii) follows once from our earlier remarks.

It remains for us to list the isomorphism invariants of M . By Steinitz's Theorem, N is determined by its R_κ -rank and Steinitz class. We shall show below that a corresponding statement is true for L . The only remaining invariant is that needed to characterize the orbit of ξ , once the exponents $\{k_i\}$ are specified. But by (34.21), there is no additional invariant needed except when $b=c=0$, and in that case we obtain the asserted result by use of (34.24). This completes the proof of the theorem, except for the assertion about the classification of locally free E -lattices. This assertion is a consequence of a result which is of independent interest:

(34.30) Proposition. Let E be a commutative order, and let $L = \prod_{i=1}^r \mathfrak{c}_i$ where the $\{\mathfrak{c}_i\}$ are locally free ideals of E . A full set of isomorphism invariants of L consists of its E -rank r , and the E -isomorphism class of the product $\prod_{i=1}^r \mathfrak{c}_i$ (called the Steinitz class of L).

Proof. Since each c_i lies in the genus of E , by (31.14) we obtain

$$L = \prod_{i=1}^r c_i \cong E^{(r-1)} \oplus c'$$

for some $c' \vee E$. We shall prove that $c' \cong \prod_{i=1}^r c_i$. Let $\wedge^k(L)$ denote the k -th exterior power of the E -module L over the commutative ring E (see §12A). It is easily verified that

$$\wedge^r \left(\prod_{i=1}^r c_i \right) \cong \prod_{i=1}^r c_i, \quad \wedge^r(E^{(r-1)} \oplus c') \cong c',$$

which establishes the proposition. This also completes the proof of Theorem 34.28.

Let us apply this machinery to the special case where $\kappa=1$, so G is a cyclic group of order p , and $\Lambda_{\kappa-1}=\mathbb{Z}$. As we have seen earlier, every Λ -lattice M is an extension of an R -lattice N by a \mathbb{Z} -lattice L , where

$$R = \mathbb{Z}[\omega], \quad \omega = \text{primitive } p\text{-th root of 1 over } \mathbb{Q}.$$

Keeping this notation, we obtain the result of Diederichsen [40], as extended by Reiner [57]:

(34.31) Theorem. *Let b range over a full set of representatives of the R -ideal classes in the cyclotomic field $\mathbb{Q}(\omega)$. Then every $\mathbb{Z}G$ -lattice M is expressible as a direct sum of indecomposable lattices*

$$M \cong \coprod_{i=1}^a (b_i, \mathbb{Z}; 1) \oplus \coprod_{j=a+1}^{a+b} b_j \oplus \mathbb{Z}^{(c)},$$

where $(b_i, \mathbb{Z}; 1)$ is a non-split extension of b_i by \mathbb{Z} .

The genus invariants of M are the integers a, b , and c . The only additional invariant needed to determine the isomorphism class of M is the ideal class of the product $\prod_{i=1}^{a+b} b_i$.

Proof. We use (34.28) with $\kappa=1$, $E=\mathbb{Z}=\mathbb{Z}[x]/(x-1)$, $d=1$, $\bar{E}=\bar{\mathbb{Z}}=\mathbb{Z}/p\mathbb{Z}$, $R_\kappa=R$. Each c_i in (34.28) may be replaced by \mathbb{Z} , and since $d=1$, the non-split extensions $(b_i, c_i; \lambda^k u)$ mentioned above are just $(b_i, \mathbb{Z}; u)$, with $u \in \bar{\mathbb{Z}}$. To complete the proof, it suffices to show that

$$(b_i, \mathbb{Z}; u) \cong (b_i, \mathbb{Z}; 1) \text{ for } u \in \bar{\mathbb{Z}}.$$

But this follows at once from (34.28i), as soon as we show that the surjection

$$R \rightarrow R/(1-\omega)R \cong \bar{\mathbb{Z}}$$

gives a surjection $R \rightarrow \bar{\mathbb{Z}}$.

To prove this last assertion, let $n \in \mathbb{Z}$ be relatively prime to p . Then ω is expressible as a power of ω^n , and so

$$(1 - \omega^n)/(1 - \omega) \in R \text{ and } (1 - \omega)/(1 - \omega^n) \in R.$$

Thus $u = (1 - \omega^n)/(1 - \omega) \in R$, and we shall show that the image of u in $\bar{\mathbf{Z}}$ is precisely \bar{n} . Indeed, setting $\lambda = 1 - \omega$, we have

$$u = ((1 + \lambda)^n - 1)/\lambda \equiv n \pmod{\lambda},$$

so $\bar{u} = \bar{n}$ in $\bar{\mathbf{Z}}$. This completes the proof of the theorem. For a more direct proof, see CR(74.3).

We remark finally that Theorem 34.28 can be used to classify all $\mathbf{Z}[x]/((x - 1)\Phi_\kappa(x))$ -lattices, for $\kappa \geq 1$. In fact, each such lattice is an extension of an R_κ -lattice by a free \mathbf{Z} -lattice.

As another application of the theorem, let $\Delta = \mathbf{Z}H$, where H is a cyclic group of order g . Let ζ_m denote a primitive m -th root of 1 over \mathbf{Q} , and set $S_m = \mathbf{Z}[\zeta_m]$. If m and n are divisors of g , then S_m and S_n are Δ -modules. Diederichsen's formula (25.26) gives

$$\mathrm{Ext}_\Delta^1(S_n, S_m) \cong S_m/pS_m = \bar{S}_m,$$

if $n = p^t m$ for some prime p and some $t \geq 1$. Then \bar{S}_m is a semilocal ring, and the proofs of (34.21) and (34.28) carry over readily to this case. We can then classify all Δ -lattices which are extensions of an S_n -lattice by an S_m -lattice. For details, see Reiner [79b]. Some partial results of this nature are also to be found in Berman [64].

§34C. Cyclic Groups of Order p^2

Keeping the notation of §34B, we concentrate here on the case where G is cyclic of order p^2 , in which case we can completely classify all $\mathbf{Z}G$ -lattices. Let $\Lambda = \mathbf{Z}G$, and let $\hat{\Lambda} = \hat{\mathbf{Z}}G$ be its p -adic completion. By (34.16), a Λ -lattice M is indecomposable if and only if the $\hat{\Lambda}$ -lattice \hat{M} is indecomposable. We shall first find all indecomposable $\hat{\Lambda}$ -lattices \hat{M} (of which there are only finite many isomorphism classes; see Exercise 33.8). Then we shall determine all M 's which correspond to a given \hat{M} , and shall list a full set of isomorphism invariants for a direct sum of indecomposable Λ -lattices.

A historical account may be of interest. In his fundamental work on integral representations of cyclic groups, Diederichsen [40] considered the question as to whether Λ has finite representation type, and gave an example to show that Λ is of infinite type when $p = 2$. This example was incorrect, however, as pointed out independently by Roiter [60] and Troy [61]. Both of them gave a full list of indecomposable Λ -lattices for this case, and indeed the

number $n(\Lambda)$ of isomorphism classes of such lattices turned out to be 9. Soon after, Heller-Reiner [62] and Berman-Gudivok [64] independently proved that for arbitrary p , $n(\hat{\Lambda})=4p+1$, and therefore $n(\Lambda)<\infty$ by (34.16) and the Jordan-Zassenhaus Theorem. (The earlier announcement by Berman-Gudivok [62] contains some errors.)

We shall follow the Heller-Reiner proof that $n(\hat{\Lambda})=4p+1$; a completely different approach has recently been given by Butler [75] (see also Wiedemann [80]). We shall set

$$E = \mathbb{Z}[x]/(x^p - 1),$$

a factor ring of Λ , so every E -lattice is also a Λ -lattice. Theorem 34.31 gives a complete classification of E -lattices. Now let M be any Λ -lattice, and set

$$L = \{m \in M : (x^p - 1)m = 0\}.$$

The discussion at the beginning of §34B shows that there is an exact sequence of Λ -lattices

$$(\xi) \quad 0 \rightarrow L \rightarrow M \rightarrow N \rightarrow 0$$

in which N is an R_2 -lattice, L an E -lattice, and for which $\text{Hom}_\Lambda(L, N) = 0$. A full set of isomorphism invariants of M consists of the isomorphism class invariants of N and L , together with the invariants describing the $(\text{Aut } N, \text{Aut } L)$ -orbit of ξ in $\text{Ext}(N, L)$. As in (34.3a), we shall write $M = (N, L; \xi)$.

Let us first determine all indecomposable $\hat{\Lambda}$ -lattices \hat{M} ; each such \hat{M} is an extension of an \hat{R}_2 -lattice \hat{N} by an \hat{E} -lattice \hat{L} . By (34.31), we may write $\hat{N} \cong \hat{R}_2^{(s)}$ and

$$\hat{L} \cong \hat{\mathbb{Z}}^{(a)} \oplus \hat{R}_1^{(b)} \oplus \hat{E}^{(c)}.$$

The integer s determines \hat{N} up to isomorphism, while the triple $\{a, b, c\}$ is a full set of isomorphism invariants of \hat{L} . If bars denote reduction mod p , then, as shown in §34B,

$$\begin{aligned} \text{Ext}_\Lambda^1(\hat{N}, \hat{L}) &\cong \{\text{Ext}(\hat{R}_2, \hat{L})\}^{(s)} \cong \bar{L}^{(s)} \\ &\cong \bar{\mathbb{Z}}^{a \times s} \oplus \bar{R}_1^{b \times s} \oplus \bar{E}^{c \times s}. \end{aligned}$$

We have

$$\bar{R}_1 \cong \bar{\mathbb{Z}}[\lambda]/(\lambda^{p-1}), \quad \bar{E} \cong \bar{\mathbb{Z}}[\lambda]/(\lambda^p), \text{ where } \lambda = 1 - x.$$

Clearly $\text{Aut } \hat{N} \cong GL_s(\hat{R}_2)$, which acts on the expression for $\text{Ext}(\hat{N}, \hat{L})$ by means of the ring surjections of \hat{R}_2 onto $\bar{\mathbb{Z}}$, \bar{R}_1 and \bar{E} . These surjections induce surjections of groups of units $(\hat{R}_2)^\times \rightarrow \bar{\mathbb{Z}}^\times$, etc.

Each $\hat{\Lambda}$ -lattice \hat{M} , indecomposable or not, is thus completely determined by the non-negative integers s, a, b , and c , and by the matrix

$$\xi = \begin{bmatrix} \mathbf{F}_0 \\ \mathbf{F}_1 \\ \mathbf{F}_2 \end{bmatrix}, \quad \mathbf{F}_0 \in \bar{\mathbb{Z}}^{a \times s}, \quad \mathbf{F}_1 \in \bar{R}_1^{b \times s}, \quad \mathbf{F}_2 \in \bar{E}^{c \times s}.$$

If \hat{M} is indecomposable, and if $s=0$, then the choices for \hat{M} are precisely $\hat{\mathbb{Z}}$, \hat{R}_1 or \hat{E} . For the remainder of this argument, let us assume that $s>0$ and that \hat{M} is indecomposable.

To proceed, we need to calculate $\text{End}_{\hat{\Lambda}} L$. We have

$$\text{Hom}(\hat{\mathbb{Z}}, \hat{R}_1) = \text{Hom}(\hat{R}_1, \hat{\mathbb{Z}}) = 0, \quad \text{End } \hat{\mathbb{Z}} \cong \hat{\mathbb{Z}}, \quad \text{End } \hat{R}_1 \cong \hat{R}_1, \quad \text{End } \hat{E} \cong \hat{E},$$

$$\text{Hom}(\hat{\mathbb{Z}}, \hat{E}) \cong \Phi_1(x)\hat{E}, \quad \text{Hom}(\hat{R}_1, \hat{E}) \cong \lambda\hat{E}, \quad \text{Hom}(\hat{E}, \hat{\mathbb{Z}}) \cong \hat{\mathbb{Z}}, \quad \text{Hom}(\hat{E}, \hat{R}_1) \cong \hat{R}_1$$

(Note that each $\varphi \in \text{Hom}(\hat{E}, \hat{\mathbb{Z}})$ is given by $\varphi(u) = ur$, $u \in \hat{E}$, where $r \in \hat{\mathbb{Z}}$ is arbitrary, and where the action of u on r arises from the surjection $\hat{E} \rightarrow \hat{\mathbb{Z}}$. On the other hand, each $\psi \in \text{Hom}(\hat{\mathbb{Z}}, \hat{E})$ is given by $\psi(v) = vs$, $v \in \hat{\mathbb{Z}}$, where $s \in \hat{E}$ is subject to the restriction that $(1-x)s=0$, or equivalently, that $s \in \Phi_1(x)\hat{E}$. Analogous remarks hold for the other cases.)

It follows that $\text{End}_{\hat{\Lambda}} L$ consists of all matrices

$$f = \begin{bmatrix} \mathbf{A}_0 & \mathbf{0} & \mathbf{A}_{02} \\ \mathbf{0} & \mathbf{A}_1 & \mathbf{A}_{12} \\ \Phi_1(x)\mathbf{A}_{20} & \lambda\mathbf{A}_{21} & \mathbf{A}_2 \end{bmatrix}, \quad \mathbf{A}_0 \in \hat{\mathbb{Z}}^{a \times a}, \quad \mathbf{A}_1 \in \hat{R}_1^{b \times b}, \quad \mathbf{A}_2 \in \hat{E}^{c \times c},$$

where the rows have entries in $\hat{\mathbb{Z}}$, \hat{R}_1 and \hat{E} , respectively. The orbit of ξ in $\text{Ext}(\hat{N}, \hat{L})$ thus consists of all matrices $f\xi g$, with f an invertible matrix, and with $g \in GL_s(\hat{R}_2)$. We write $\xi \approx f\xi g$, and call ξ *equivalent* to $f\xi g$. Thus we have

$$\begin{bmatrix} \mathbf{F}_0 \\ \mathbf{F}_1 \\ \mathbf{F}_2 \end{bmatrix} \approx \begin{bmatrix} \mathbf{A}_0 & \mathbf{0} & \mathbf{A}_{02} \\ \mathbf{0} & \mathbf{A}_1 & \mathbf{A}_{12} \\ \Phi_1(x)\mathbf{A}_{20} & \lambda\mathbf{A}_{21} & \mathbf{A}_2 \end{bmatrix} \begin{bmatrix} \mathbf{F}_0 \\ \mathbf{F}_1 \\ \mathbf{F}_2 \end{bmatrix} \cdot \mathbf{T},$$

with $\mathbf{A}_0, \mathbf{A}_1, \mathbf{A}_2$ and \mathbf{T} invertible over $\hat{\mathbb{Z}}, \hat{R}_1, \hat{E}$ and \hat{R}_2 , respectively.

This equivalence allows us to replace \mathbf{F}_0 by $\mathbf{A}_0\mathbf{F}_0\mathbf{T}$. Since there are ring surjections $\hat{\mathbb{Z}} \rightarrow \bar{\mathbb{Z}}, \hat{R}_2 \rightarrow \bar{\mathbb{Z}}$, which induce surjections of groups of units, we can diagonalize \mathbf{F}_0 and can bring it into the form

$$\mathbf{F}_0 = \begin{pmatrix} \mathbf{I} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} \end{pmatrix}^{a \times s},$$

where \mathbf{I} is a $w \times w$ identity matrix for some w , $0 \leq w \leq a$. If $w < a$, then the last

$a-w$ copies of \hat{Z} split off as a direct summand of \hat{M} , contradicting our assumption that $s > 0$ and \hat{M} is indecomposable. Therefore $w = a \leq s$, and we may write

$$\xi = \begin{bmatrix} \mathbf{F}_0 \\ \mathbf{F}_1 \\ \mathbf{F}_2 \end{bmatrix} = \begin{bmatrix} \mathbf{I} & \mathbf{0} \\ \mathbf{F}_{11} & \mathbf{F}_{12} \\ \mathbf{F}_{21} & \mathbf{F}_{22} \end{bmatrix} \begin{matrix} a \\ b \\ c \end{matrix}$$

$$a \quad s-a$$

where the letters a , b , etc., show the number of rows or columns in the various blocks of \mathbf{F}_0 , \mathbf{F}_1 and \mathbf{F}_2 .

If $\mathbf{F}_1 = \mathbf{0}$, then $\hat{R}_1^{(b)}$ is a summand of \hat{M} , and thus $\hat{M} = \hat{R}_1$, contradicting our assumption that $s > 0$. Likewise, $\mathbf{F}_2 \neq \mathbf{0}$. Each entry of \mathbf{F}_1 and \mathbf{F}_2 may be written in the form $u\lambda^k$, with u a unit and $k \geq 0$; call k the *exponent* of the element $u\lambda^k$. The remainder of the discussion splits into four cases, depending on the location of an element of smallest exponent among all of the entries of the matrices \mathbf{F}_{11} , \mathbf{F}_{12} , \mathbf{F}_{21} and \mathbf{F}_{22} .

Case 1. Suppose the smallest exponent k occurs for an entry in \mathbf{F}_{22} . We may partition \mathbf{T} as

$$\mathbf{T} = \begin{bmatrix} \mathbf{T}_1 & \mathbf{0} \\ \mathbf{T}_{21} & \mathbf{T}_2 \end{bmatrix}, \quad \mathbf{T}_1 \in GL_a(\hat{R}_2), \quad \mathbf{T}_2 \in GL_{s-a}(\hat{R}_2),$$

and thus after equivalence we may replace \mathbf{F}_{22} by $\mathbf{A}_2 \mathbf{F}_{22} \mathbf{T}_2$. Choosing \mathbf{A}_2 and \mathbf{T}_2 suitably, we may then assume that

$$\mathbf{F}_{22} = \begin{bmatrix} \lambda^k & \mathbf{0} \\ \mathbf{0} & * \end{bmatrix},$$

with k minimal as above.

In the equivalence $\xi \approx f\xi$, we choose f to be the matrix

$$\begin{bmatrix} \mathbf{I} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{I} & \mathbf{A}_{12} \\ \mathbf{0} & \mathbf{0} & \mathbf{I} \end{bmatrix}.$$

Since every entry of \mathbf{F}_{12} has exponent $\geq k$, further equivalence allows us to eliminate all entries of \mathbf{F}_{12} in its first column, by choosing \mathbf{A}_{12} properly. Likewise, using

$$\mathbf{T} = \begin{bmatrix} \mathbf{I} & \mathbf{0} \\ \mathbf{T}_{21} & \mathbf{I} \end{bmatrix}$$

with suitable \mathbf{T}_{21} , we can eliminate all entries in the first row of \mathbf{F}_{21} . Thus, we

obtain

$$\xi \approx \begin{bmatrix} \mathbf{I} & \mathbf{0} & \mathbf{0} \\ \mathbf{F}_{11} & \mathbf{0} & * \\ \mathbf{0} & \lambda^k & \mathbf{0} \\ * & \mathbf{0} & * \end{bmatrix}$$

so \hat{M} decomposes, and the extension of \hat{R}_2 by \hat{E} corresponding to the extension class $\lambda^k \in \text{Ext}(\hat{R}_2, \hat{E})$ splits off as a summand of \hat{M} . Denoting this extension by $(\hat{R}_2, \hat{E}; \lambda^k)$, we see that it coincides with \hat{M} , since \hat{M} is indecomposable. Since λ^k is an element of \bar{E} in this step, the exponent k has the range $0 \leq k < p$, and each such k gives an indecomposable extension. We obtain p non-isomorphic indecomposable extensions in this way.

Case 2. Suppose that the smallest exponent k occurs for an entry in \mathbf{F}_{21} , but not in \mathbf{F}_{22} . Since

$$\xi \approx \begin{bmatrix} \mathbf{A}_0 \mathbf{T}_1 & \mathbf{0} \\ * & * \\ \mathbf{A}_2 \mathbf{F}_{21} \mathbf{T}_1 & * \end{bmatrix},$$

we may choose invertible matrices \mathbf{A}_0 , \mathbf{A}_2 and \mathbf{T}_1 so that $\mathbf{A}_0 \mathbf{T}_1 = \mathbf{I}$ over $\bar{\mathbb{Z}}$, and \mathbf{F}_{21} has the form

$$\mathbf{F}_{21} = \begin{bmatrix} \lambda^k & \mathbf{0} \\ \mathbf{0} & * \end{bmatrix}.$$

The entries of the first row of \mathbf{F}_{22} have exponent $> k$, so right multiplication by

$$\mathbf{T} = \begin{bmatrix} \mathbf{I} & \lambda \mathbf{T}_{12} \\ \mathbf{0} & \mathbf{I} \end{bmatrix},$$

with suitably chosen \mathbf{T}_{12} , can be used to eliminate the first row of \mathbf{F}_{22} . Note that this procedure does not affect the top rows $[\mathbf{I} \ 0]$ of ξ , since $\mathbf{I} \cdot \lambda \mathbf{T}_{12} = \mathbf{0}$ over $\bar{\mathbb{Z}}$. This gives

$$\xi \approx \begin{bmatrix} 1 & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{I} & \mathbf{0} \\ \mathbf{0} & * & * \\ \lambda^k & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & * & * \end{bmatrix},$$

so again \hat{M} decomposes, and we obtain

$$\hat{M} \cong (\hat{R}_2, \hat{\mathbf{Z}} \oplus \hat{E}; 1 \oplus \lambda^k), \quad \text{where } 0 \leq k \leq p-1.$$

However, the extension for which $k=p-1$ is decomposable. Indeed, we may write $\Phi_1(x)=\lambda^{p-1}$ in \bar{E} . Upon subtracting a suitable $\Phi_1(x)$ -multiple of the first row of \mathbf{F}_0 from the first row of \mathbf{F}_2 (which is permitted under our definition of equivalence), the corner entry of \mathbf{F}_{21} becomes 0. In other words, we have

$$(\hat{R}_2, \hat{\mathbf{Z}} \oplus \hat{E}; 1 \oplus \lambda^{p-1}) \cong (\hat{R}_2, \hat{\mathbf{Z}}; 1) \oplus \hat{E}.$$

Analogously, we obtain

$$(\hat{R}_2, \hat{\mathbf{Z}} \oplus \hat{E}; 1 \oplus 1) \cong \hat{\mathbf{Z}} \oplus (\hat{R}_2, \hat{E}; 1).$$

It is easily verified that for $0 < k < p-1$, the classes

$$\xi = \begin{pmatrix} 1 \\ \lambda^k \end{pmatrix} \in \text{Ext}(\hat{R}_2, \hat{\mathbf{Z}} \oplus \hat{E})$$

yield indecomposable $\hat{\Lambda}$ -lattices, no two of which are isomorphic. This can be shown by considering

$$\begin{bmatrix} a_0 & b_0 \\ \Phi_1(x)b_2 & a_2 \end{bmatrix} \begin{bmatrix} 1 \\ \lambda^k \end{bmatrix} \cdot \alpha, \quad \text{where } a_0 \in \hat{\mathbf{Z}}, a_2 \in \hat{E}, \alpha \in (\hat{R}_2),$$

which can never be of the forms $\begin{pmatrix} 1 \\ 0 \end{pmatrix}$, $\begin{pmatrix} 0 \\ 1 \end{pmatrix}$, or $\begin{pmatrix} 1 \\ \lambda^l \end{pmatrix}$ with $l \neq k$.

Case 3. Suppose the smallest k occurs in \mathbf{F}_{12} , and not in \mathbf{F}_{21} or \mathbf{F}_{22} . Subtracting suitable multiples of the columns of \mathbf{F}_{12} from those of \mathbf{F}_{21} , and suitable λ -multiples of the rows of \mathbf{F}_{12} from those of \mathbf{F}_{22} , we eventually obtain

$$\hat{M} \cong (\hat{R}_2, \hat{R}_1; \lambda^k), \quad 0 \leq k \leq p-2,$$

which is indecomposable. (Since $\lambda^{p-1}=0$ in \bar{R}_1 , the upper limit for k must be $p-2$.)

Case 4. Suppose the smallest k occurs in \mathbf{F}_{11} , and not in \mathbf{F}_{12} , \mathbf{F}_{21} or \mathbf{F}_{22} . As in Case 2, we may bring \mathbf{F}_{11} into the form

$$\mathbf{F}_{11} = \begin{pmatrix} \lambda^k & \mathbf{0} \\ \mathbf{0} & * \end{pmatrix}.$$

We may then subtract λ -multiples of the first row of \mathbf{F}_{11} from the rows of \mathbf{F}_{21} , under our equivalence procedure. We may also subtract λ -multiples of the first column of \mathbf{F}_{11} from the columns of \mathbf{F}_{12} , noting that the top rows of ξ are not affected by this procedure because $\lambda \mathbf{I} = \mathbf{0}$ over $\bar{\mathbf{Z}}$. The matrix ξ then decomposes, and we obtain

$$\hat{M} \cong (\hat{R}_2, \hat{\mathbf{Z}} \oplus \hat{R}_1; 1 \oplus \lambda^k), \quad 0 \leq k \leq p-2.$$

We collect our results in the following:

(34.32) Theorem. *There are precisely $4p+1$ non-isomorphic indecomposable $\hat{\mathbb{Z}}G$ -lattices, where $\hat{\mathbb{Z}}$ is the ring of p -adic integers, and G is cyclic of order p^2 . These are given by**

$$\hat{\mathbb{Z}}, \hat{R}_1, \hat{E}, \hat{R}_2, (\hat{R}_2, \hat{\mathbb{Z}}; 1),$$

$$(\hat{R}_2, \hat{\mathbb{Z}} \oplus \hat{E}; \lambda^k), 0 \leq k \leq p-1,$$

$$(\hat{R}_2, \hat{\mathbb{Z}} \oplus \hat{E}; 1 \oplus \lambda^k), 1 \leq k \leq p-2,$$

$$(\hat{R}_2, \hat{R}_1; \lambda^k), 0 \leq k \leq p-2,$$

$$(\hat{R}_2, \hat{\mathbb{Z}} \oplus \hat{R}_1; 1 \oplus \lambda^k), 0 \leq k \leq p-2.$$

We may remark that all of these lattices can be embedded as ideals in $\hat{\Lambda}$, except for the lattices of the form $(\hat{R}_2, \hat{\mathbb{Z}} \oplus \hat{E}; 1 \oplus \lambda^k)$. The $\hat{\mathbb{Z}}$ -rank of these last-named extensions is $p^2 + 1$, so they cannot be ideals in the group ring $\hat{\mathbb{Z}}G$.

Berman-Gudivok [64] give explicit matrix representations of G afforded by these $4p+1$ indecomposable lattices. Butler [75] gives a completely different description of these lattices (see also Wiedemann [80]). Berman [63], [66] classifies all groups H whose indecomposable $\mathbb{Z}H$ -lattices are isomorphic to ideals of $\mathbb{Z}H$. Berman-Gudivok [64] also treat the case where G is cyclic of order p^κ , $\kappa \geq 2$, and classify all indecomposable $\hat{\mathbb{Z}}G$ -lattices which are annihilated by $(x-1)\Phi_i(x)\Phi_\kappa(x)$ for some fixed i , $0 < i < \kappa$. There are finitely many such indecomposable lattices.

Let us turn now to a consideration of $\mathbb{Z}G$ -lattices. The results given below are due to Reiner [78]. If M is an indecomposable $\mathbb{Z}G$ -lattice, then \hat{M} must be one of the indecomposable $\hat{\mathbb{Z}}G$ -lattices listed above. Given \hat{M} , we can find all possible M 's by replacing extension classes λ^k or $1 \oplus \lambda^k$ by expressions such as $\lambda^k u$, $u_0 \oplus \lambda^k u_1$, etc., where the u 's are units in rings such as $\bar{\mathbb{Z}}$, \bar{R}_1 , and \bar{E} . We then have the problem, already encountered in Theorem 34.28, of deciding when two indecomposable M 's are isomorphic, and of giving a full list of isomorphism invariants of a direct sum of indecomposable lattices.

Let us treat in detail the problem of finding all indecomposable M 's with given \hat{M} , for the most difficult case, that in which $\hat{M} = (\hat{R}_2, \hat{\mathbb{Z}} \oplus \hat{E}; 1 \oplus \lambda^k)$, where $1 \leq k \leq p-2$. Let b range over a full set of representatives of the h_1 ideal classes of R_1 , and c over a corresponding set for the h_2 ideal classes of R_2 . For each b , let $E(b)$ denote the locally free E -lattice which is a non-split extension of b by \mathbb{Z} ; in (34.31), we denoted $E(b)$ by $(b, \mathbb{Z}; 1)$. The discussion in §34B, and at the beginning of this subsection, shows at once that M must

*We follow the notation described in (34.3a), which differs from that in Reiner [78].

be (isomorphic to) an extension of \mathfrak{c} by $\mathbb{Z} \oplus E(\mathfrak{b})$, for some \mathfrak{b} and \mathfrak{c} , with extension class $\xi \in \text{Ext}(\mathfrak{c}, \mathbb{Z} \oplus E(\mathfrak{b}))$. Further, choosing some standard isomorphism

$$\text{Ext}(\mathfrak{c}, \mathbb{Z} \oplus E(\mathfrak{b})) \cong \text{Ext}(R_2, \mathbb{Z} \oplus E) \cong \bar{\mathbb{Z}} \oplus \bar{E},$$

where bars denote reduction mod p , we can represent ξ as a column vector

$$\xi = \begin{pmatrix} m \\ \lambda^k u \end{pmatrix}, m \in \bar{\mathbb{Z}}, u \in \bar{E}, 1 \leq k \leq p-2.$$

A full set of isomorphism invariants of M consists of the ideal classes of \mathfrak{b} and \mathfrak{c} , and the orbit of ξ under the actions of $\text{Aut}(\mathbb{Z} \oplus E)$ and $\text{Aut } R_2$.

The orbit of ξ consists of all column vectors $f\xi s$, with $f \in \text{Aut}(\mathbb{Z} \oplus E)$, $s \in R_2$. As shown in the proof of (34.31), R_2 maps onto $\bar{\mathbb{Z}}$, so we may find a new ξ in the same orbit for which $m=1$. Thus we may take

$$\xi = \begin{pmatrix} 1 \\ \lambda^k u \end{pmatrix}$$

from now on, and we must decide when two different ξ 's lie in the same orbit. The complete solution to this question is given by:

(34.33) Proposition. *Let*

$$\xi = \begin{pmatrix} 1 \\ \lambda^k u \end{pmatrix}, \xi' = \begin{pmatrix} 1 \\ \lambda^{k'} u' \end{pmatrix}, \text{ where } 1 \leq k, k' \leq p-2, \text{ and } u, u' \in \bar{E}.$$

Then ξ and ξ' lie in the same orbit if and only if

(i) $k=k'$,

(ii) u and u' have the same image in Ω_k , where

$$\Omega_k = (R')/\text{image of } R_1, \text{ with } R' = \bar{\mathbb{Z}}[\lambda]/(\lambda^{p-1-k}),$$

and (iii) For the case where $p \equiv 1 \pmod{4}$, the image of u/u' in $\bar{\mathbb{Z}}$ is a square.

Proof. There is a fibre product diagram

$$\begin{array}{ccc} E & \xrightarrow{\mu_0} & \mathbb{Z} \\ \downarrow \mu_1 & & \downarrow \\ R_1 & \longrightarrow & \bar{\mathbb{Z}} \end{array}$$

in which μ_0, μ_1 are canonical surjections. One important consequence of this

fact is the obvious result:

$$\mu_1\{E\} = \{r \in R_1 : r \equiv \pm 1 \pmod{\lambda}\},$$

where $\lambda = 1 - \omega_1$. We shall also need the fact (see Exercise 34.4) that under the canonical surjection $\theta: R_2 \rightarrow \bar{R}_1$, the image of R_2 is contained in the image of R_1 in (\bar{R}_1) .

As a special case of the discussion at the start of this subsection, we have

$$\text{End}(\mathbb{Z} \oplus E) = \left\{ f : f = \begin{pmatrix} a & b \\ \Phi_1(x)c & d \end{pmatrix}, a, b \in \mathbb{Z}, c, d \in E \right\}.$$

By Exercise 34.2, f induces the maps

$$f_0 = \begin{pmatrix} a & b \\ p\mu_0(c) & \mu_0(d) \end{pmatrix} \in \text{End}(\mathbb{Z} \oplus \mathbb{Z}), \quad f_1 = \mu_1(d) \in \text{End } R_1,$$

and $f \in \text{Aut}(\mathbb{Z} \oplus E)$ if and only if $f_0 \in GL_2(\mathbb{Z})$ and $\mu_1(d) \in R_1$. The condition that ξ and ξ' lie in the same orbit becomes

$$\begin{pmatrix} 1 \\ \lambda^{k'} u' \end{pmatrix} = \begin{pmatrix} a & b \\ \Phi_1(x)c & d \end{pmatrix} \begin{pmatrix} 1 \\ \lambda^k u \end{pmatrix} \cdot s$$

for some $f \in \text{Aut}(\mathbb{Z} \oplus E)$ and $s \in R_2$. This can be written as

$$(34.34) \quad as = 1 \text{ in } \bar{\mathbb{Z}}, \quad \lambda^{k'} u' = (\lambda^{p-1} c + d\lambda^k u)s \text{ in } \bar{E},$$

using the facts that $b\lambda^k = 0$ in $\bar{\mathbb{Z}}$ because $k \geq 1$, and that $\Phi_1(x) = \lambda^{p-1}$ in \bar{E} . Since $k' \leq p-2$, the second equation in (34.34) cannot hold true if $k \neq k'$, so for the rest of the proof we may assume that $k = k'$.

Suppose now that (34.34) holds for some $f \in \text{Aut}(\mathbb{Z} \oplus E)$ and some $s \in R_2$. Then in \bar{E} we have

$$ad \equiv a\mu_0(d) \equiv \pm 1 \pmod{\lambda}, \quad as \equiv 1 \pmod{\lambda},$$

and so

$$u' \equiv dus \equiv \pm a^{-2}u \pmod{\lambda}.$$

If $p \equiv 1 \pmod{4}$, then for each $a \in \mathbb{Z}$ prime to p , $\pm a^{-2}$ is always a square mod p , which shows that u/u' is a square in $\bar{\mathbb{Z}}$. Furthermore,

$$\lambda^k u' = \mu_1(d) \lambda^k u s \text{ in } \bar{R}_1.$$

Since $\bar{s} = \bar{r}$ in \bar{R}_1 for some $r \in R_1$ by Exercise 34.4, this shows that u' and u have the same image in the group Ω_k defined above. Therefore, if $\xi \approx \xi'$, then conditions (i)–(iii) are satisfied.

Assume conversely that these conditions hold. From (iii), we may write $u' \equiv q^2 u \pmod{\lambda}$ for some $q \in \mathbb{Z}$ prime to p . As in the proof of (34.31), we can then find $r \in R_1$, $s \in R_2$, such that $r \equiv s \equiv q \pmod{\lambda}$. But then we can choose $f \in \text{Aut}(\mathbb{Z} \oplus E)$ such that $\det f_0 = 1$ and $\mu_1(d) = r$. We then obtain $\xi \approx \xi''$, where

$$\xi'' = \begin{pmatrix} as \\ \lambda^k u'' \end{pmatrix}, \text{ and } \lambda^k u'' \equiv \lambda^k \cdot dus \pmod{\lambda^{p-1}}.$$

Then

$$as \equiv aq \equiv d^{-1}q \equiv r^{-1}q \equiv 1 \pmod{\lambda},$$

so $as = 1$ in $\bar{\mathbb{Z}}$. Further,

$$u'' \equiv dus \equiv q^2 u \equiv u' \pmod{\lambda},$$

and u'' and u' have the same image in Ω_k . It remains for us to prove that $\xi'' \approx \xi'$.

Since u'' and u' have the same image in Ω_k , it follows that

$$\lambda^k u'' \equiv \lambda^k u' r \pmod{\lambda^{p-1} \bar{E}}$$

for some $r \in R_1$. But $r \equiv 1 \pmod{\lambda}$ because $u'' \equiv u' \pmod{\lambda}$, and thus by our earlier comments, $r = \mu_1(d)$ for some $d \in E$. But then we can find $c \in E$ such that

$$\lambda^k u'' = \Phi_1(x)c + \lambda^k u'd \text{ in } \bar{E},$$

so now

$$\xi' \approx \begin{pmatrix} 1 & 0 \\ \Phi_1(x)c & d \end{pmatrix} \begin{pmatrix} 1 \\ \lambda^k u' \end{pmatrix} = \begin{pmatrix} 1 \\ \lambda^k u'' \end{pmatrix} = \xi'',$$

which completes the proof that $\xi \approx \xi'$, and establishes the proposition.

A similar discussion, considerably less complicated, can be carried out for each of the other choices of \hat{M} in (34.32). Indeed, in most of the cases the desired information is obtained as a special case of Theorem 34.28; for details, see Reiner [78]. The final result is as follows*:

(34.35) Theorem. *Let $R_i = \mathbb{Z}[\omega_i]$, $i = 1, 2$, where ω_i is a primitive p^i -th root of unity over \mathbb{Q} . Let b range over a full set of representatives of the h_1 ideal classes of R_1 , and c over the h_2 ideal classes of R_2 . For each b , let $E(b)$ be the non-split*

*We use the notation of (34.3a) rather than that in Reiner [78].

extension of \mathfrak{b} by \mathbf{Z} . Let n_0 be some fixed quadratic non-residue $(\text{mod } p)$, when $p \equiv 1 \pmod{4}$.

Let

$$(34.36) \quad \begin{cases} U_m = (\bar{\mathbf{Z}}[\lambda]/(\lambda^m)) / \text{image of } R_1, & 1 \leq m \leq p-1, \\ U_p = \bar{E} / \{ \text{image of } E \} \{ \text{image of } R_2 \}. \end{cases}$$

For each m , $1 \leq m \leq p$, let \tilde{U}_m denote a full set of representatives u , in (\bar{R}_1) or \bar{E} , of the elements of the factor group U_m , where these u 's are chosen so that $u \equiv 1 \pmod{\lambda}$.

Let $(\mathfrak{c}, \mathbf{Z}; 1)$ denote an extension of \mathfrak{c} by \mathbf{Z} with extension class 1, and $(\mathfrak{c}, \mathbf{Z} \oplus E(\mathfrak{b}); 1 \oplus \lambda^k u)$ an extension of \mathfrak{c} by $\mathbf{Z} \oplus E(\mathfrak{b})$ with extension class $1 \oplus \lambda^k u$, and so on.

Then a full list of non-isomorphic indecomposable $\mathbf{Z}G$ -lattices is as follows:

- (a) $(\mathfrak{c}, \mathfrak{b}, E(\mathfrak{b}), \mathfrak{c}, (\mathfrak{c}, \mathbf{Z}; 1))$.
- (b) $(\mathfrak{c}, E(\mathfrak{b}); \lambda^k u)$, $u \in \tilde{U}_{p-k}$, $0 \leq k \leq p-1$.
- (c) $(\mathfrak{c}, \mathbf{Z} \oplus E(\mathfrak{b}); 1 \oplus \lambda^k u)$, $u \in \tilde{U}_{p-1-k}$, $1 \leq k \leq p-2$.
- (d) If $p \equiv 1 \pmod{4}$, $(\mathfrak{c}, \mathbf{Z} \oplus E(\mathfrak{b}); 1 \oplus \lambda^k u n_0)$, $u \in \tilde{U}_{p-1-k}$, $1 \leq k \leq p-2$.
- (e) $(\mathfrak{c}, \mathfrak{b}; \lambda^k u)$, $u \in \tilde{U}_{p-1-k}$, $0 \leq k \leq p-2$.
- (f) $(\mathfrak{c}, \mathbf{Z} \oplus \mathfrak{b}; 1 \oplus \lambda^k u)$, $u \in \tilde{U}_{p-1-k}$, $0 \leq k \leq p-2$.

The groups U_m defined in (34.36) are extremely interesting, and measure to what extent units in the local ring $\bar{\mathbf{Z}}[\lambda]/(\lambda^m)$ can be lifted to global units in R_1 , R_2 and E . This same question arises in the determination of the locally free class group $\text{Cl}(\mathbf{Z}G)$, where G is a cyclic p -group (see Chapter 11). We have $U_1 = \{1\}$, since the proof of (34.31) shows that R_1 maps onto $\bar{\mathbf{Z}}$. Further, since $1 + \lambda = x \in E$, it follows at once that $U_2 = \{1\}$.

If we put

$$E' = \bar{\mathbf{Z}}[\lambda]/(\lambda^m), \text{ where } 1 \leq m \leq p,$$

then the group (E') can be written as a direct product

$$(E') \cong \bar{\mathbf{Z}} \times \langle 1 + \lambda \rangle \times \langle 1 + \lambda^2 \rangle \times \cdots \times \langle 1 + \lambda^{m-1} \rangle.$$

The preceding discussion shows that the images of R_1 or R_2 cover the factor $\bar{\mathbf{Z}}$, so U_m is always an elementary abelian p -group. This group has been studied in detail by Galovich [74], Kervaire-Murthy [77], and Ullom [77].

especially for the case where p is a regular odd prime. Let us summarize their results:

An odd prime p is *regular* if $p \nmid h_1$, where h_1 is the ideal class number of R_1 (see Borevich-Shafarevich [66]). If p is regular, then the image R_1^* of R_1 in (E') is given by

$$R_1^* = \bar{\mathbb{Z}} \times \langle 1 + \lambda \rangle \times \prod_{i=1}^{\lfloor (m-1)/2 \rfloor} \langle 1 + \lambda^{2i} + \alpha_i \lambda^{2i+1} \rangle$$

for some α 's in E' . Thus U_m is elementary abelian of order $p^{f(m)}$, where $f(m) = \lfloor (m-2)/2 \rfloor$ (interpreted as 0 if $m < 2$).

To test for regularity of p , one considers the Bernoulli numbers B_1, B_2, \dots . Let $\delta(k)$ be the number of B 's among B_1, \dots, B_k whose numerator is divisible by p . Then p is regular if and only if $\delta\left(\frac{p-3}{2}\right) = 0$. On the other hand, we call p *properly irregular* if $p \mid h_1$ but p does not divide the ideal class number of $\mathbb{Z}[\omega_1 + \bar{\omega}_1]$. For such p , one must omit from the formula for R_1^* all those factors for which $2i \leq p-3$ and the numerator of B_i is a multiple of p . Thus, for each properly irregular p , U_m is an elementary abelian p -group of order $p^{g(m)}$, where

$$g(m) = \begin{cases} \left[\frac{m-2}{2} \right] + \delta\left(\left[\frac{m-1}{2} \right]\right), & 0 \leq m \leq p-2, \\ \frac{p-3}{2} + \delta\left(\frac{p-3}{2}\right), & m = p-1, p. \end{cases}$$

As far as is now known, every odd prime is either regular or properly irregular. Thus, the groups U_m occurring in (34.35) may be regarded as known.

Let us conclude this subsection with some observations about direct sums of indecomposable $\mathbb{Z}G$ -lattices. Suppose that $1 \leq k \leq p-2$, and let $u \in E$ have image $\bar{u} \in \bar{E}$. We consider the exact sequences with indicated extension classes:

$$\begin{array}{ccccccc} 1 \oplus \lambda^k: & 0 & \longrightarrow & \mathbb{Z} \oplus E & \longrightarrow & M & \longrightarrow R_2 \longrightarrow 0, \\ & & & \downarrow (1, u) & & \downarrow & \downarrow 1 \\ 1 \oplus \lambda^k \bar{u}: & 0 & \longrightarrow & \mathbb{Z} \oplus E & \longrightarrow & M' & \longrightarrow R_2 \longrightarrow 0. \end{array}$$

The commutativity of the diagram gives rise to an exact sequence

$$0 \rightarrow (R_2, \mathbb{Z} \oplus E; 1 \oplus \lambda^k) \rightarrow (R_2, \mathbb{Z} \oplus E; 1 \oplus \lambda^k \bar{u}) \rightarrow E/uE \rightarrow 0.$$

But also

$$0 \rightarrow E \xrightarrow{u} E \rightarrow E/uE \rightarrow 0$$

is exact, so by (31.8) we obtain

$$(R_2, \mathbb{Z} \oplus E; 1 \oplus \lambda^k \bar{u}) \oplus E \cong (R_2, \mathbb{Z} \oplus E; 1 \oplus \lambda^k) \oplus E.$$

(Other formulas of this nature are given in (31.10) and (31.11)).

A systematic use of this procedure enables us to reduce a direct sum of indecomposable lattices to some sort of canonical form. In this manipulation, all of the ideals $\{\mathfrak{b}\}$ can be concentrated into a single summand, being replaced by R_1 in all other summands. The same holds for the \mathfrak{c} 's and the $E(\mathfrak{b})$'s. Further, all of the units $\{u\}$ can be eliminated, except possibly for a single summand. The end result, too complicated to state here, gives a full list of invariants for the isomorphism class of a direct sum of indecomposable $\mathbb{Z}G$ -lattices. For details, see Reiner [78]. This procedure has been generalized somewhat by Jones [80].

For the case where G is cyclic of order p^κ , $\kappa \geq 2$, Berman-Gudivok [64] obtained all indecomposable $\mathbb{Z}G$ -lattices \hat{M} for which $\hat{Q}\hat{M}$ has only three types of simple summands, namely \hat{Q} , $\hat{Q}(\omega_i)$ and $\hat{Q}(\omega_j)$, with $1 \leq i < j \leq \kappa$.

§34D. An Order in a Matrix Algebra

We devote this subsection to the Drozd-Turčin [67] example considered in (34.3) above, and keep the notation introduced there. We shall classify all indecomposable genera of Λ -lattices, and shall exhibit a Λ -lattice M such that $g(M) > g(\Lambda)$, where $g(M)$ denotes the number of isomorphism classes of Λ -lattices in the genus of M . This provides a negative answer to a question of Roiter (see (31.35ii)).

Starting with a prime p , we set

$$\Lambda = \mathbb{Z} \cdot \mathbf{I} + p\Lambda', \quad \Lambda' = M_2(\mathbb{Z}), \quad L = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a, b \in \mathbb{Z} \right\},$$

so L is a left Λ' -lattice for which QL is a simple $M_2(\mathbb{Q})$ -module. The ring isomorphism $\Lambda/p\Lambda' \cong \bar{\mathbb{Z}} = \mathbb{Z}/p\mathbb{Z}$ is given by

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} + p\Lambda' \rightarrow \bar{a} \in \bar{\mathbb{Z}}, \quad \text{for all } \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Lambda.$$

We showed in (34.3) that every Λ -lattice M is an extension

$$(ξ) \quad 0 \rightarrow L^{(r)} \rightarrow M \rightarrow \bar{\mathbb{Z}}^{(s)} \rightarrow 0,$$

and the isomorphism invariants of M are the integers r and s , and the orbit of $ξ$ in $\text{Ext}(\bar{\mathbb{Z}}^{(s)}, L^{(r)})$ under the actions of $\text{Aut } L^{(r)}$ and $\text{Aut } \bar{\mathbb{Z}}^{(s)}$. We note also that the genus of M is completely determined by the $\hat{\Lambda}$ -lattice \hat{M} , by (31.2), and that just as in (34.16), M is indecomposable if and only if \hat{M} is indecomposable.

Let us calculate $\text{Ext}(\bar{\mathbb{Z}}, L)$, where Ext means Ext_{Λ}^1 . The exact sequence $0 \rightarrow p\Lambda' \rightarrow \Lambda \rightarrow \bar{\mathbb{Z}} \rightarrow 0$ gives

$$\text{Ext}(\bar{\mathbb{Z}}, L) \cong \text{Hom}_{\Lambda}(p\Lambda', L)/\text{image of } \text{Hom}_{\Lambda}(\Lambda, L).$$

But by Exercise 23.2,

$$\text{Hom}_{\Lambda}(p\Lambda', L) = \text{Hom}_{\Lambda'}(p\Lambda', L) \cong L,$$

and under this isomorphism, the image of $\text{Hom}_{\Lambda}(\Lambda, L)$ is equal to pL . Therefore

$$\text{Ext}(\bar{\mathbb{Z}}, L) \cong L/pL \cong \bar{\mathbb{Z}} \oplus \bar{\mathbb{Z}}.$$

It follows at once that

$$\text{Ext}(\bar{\mathbb{Z}}^{(s)}, L^{(r)}) \cong (\bar{\mathbb{Z}} \oplus \bar{\mathbb{Z}})^{r \times s},$$

the $\bar{\mathbb{Z}}$ -vector space consisting of all $r \times s$ matrices over $\bar{\mathbb{Z}} \oplus \bar{\mathbb{Z}}$. Each $\xi \in \text{Ext}(\bar{\mathbb{Z}}^{(s)}, L^{(r)})$ is therefore expressible as $\xi = (\mathbf{F}_1, \mathbf{F}_2)$, where $\mathbf{F}_1, \mathbf{F}_2$ are a pair of $r \times s$ matrices over $\bar{\mathbb{Z}}$. In order to describe the actions of $\text{Aut } \bar{\mathbb{Z}}^{(s)}$ and $\text{Aut } L^{(r)}$ on ξ , we note that

$$\text{Aut}_{\Lambda} \bar{\mathbb{Z}}^{(s)} = \text{Aut}_{\bar{\mathbb{Z}}} \bar{\mathbb{Z}}^{(s)} \cong GL_s(\bar{\mathbb{Z}}),$$

$$\text{Aut}_{\Lambda} L^{(r)} = \text{Aut}_{\Lambda'} L^{(r)} \cong GL_r(\mathbb{Z}).$$

If $\xi' = (\mathbf{F}'_1, \mathbf{F}'_2)$, then ξ and ξ' lie in the same orbit (notation: $\xi \approx \xi'$) if and only if $\xi' = \mathbf{X}\xi\mathbf{Y}$ for some $\mathbf{X} \in GL_r(\mathbb{Z})$, $\mathbf{Y} \in GL_s(\bar{\mathbb{Z}})$, that is,

$$(34.37) \quad \mathbf{F}'_1 = \mathbf{X}\mathbf{F}_1\mathbf{Y}, \mathbf{F}'_2 = \mathbf{X}\mathbf{F}_2\mathbf{Y} \text{ for some } \mathbf{X} \in GL_r(\mathbb{Z}), \mathbf{Y} \in GL_s(\bar{\mathbb{Z}}).$$

The lattice M corresponding to ξ is decomposable if and only if we can write $\xi \approx \xi_1 \oplus \xi_2$ for some $\xi_1 = (\mathbf{G}_1, \mathbf{G}_2)$, $\xi_2 = (\mathbf{H}_1, \mathbf{H}_2)$, that is

$$(34.38) \quad (\mathbf{F}_1, \mathbf{F}_2) \approx \left(\begin{pmatrix} \mathbf{G}_1 & \mathbf{0} \\ \mathbf{0} & \mathbf{G}_2 \end{pmatrix}, \begin{pmatrix} \mathbf{H}_1 & \mathbf{0} \\ \mathbf{0} & \mathbf{H}_2 \end{pmatrix} \right).$$

The genus of M is determined by an analogous argument, the only difference being that in (34.37), we let $\mathbf{X} \in GL_r(\hat{\mathbb{Z}})$. Since the map $GL_j(\hat{\mathbb{Z}}) \rightarrow GL_j(\bar{\mathbb{Z}})$ is surjective for each j , it follows that the genus of M is determined by the orbit of $\xi \in (\bar{\mathbb{Z}} \oplus \bar{\mathbb{Z}})^{r \times s}$ under the actions of $GL_r(\bar{\mathbb{Z}})$ and $GL_s(\bar{\mathbb{Z}})$.

We are thus led to the well-known problem of classifying matrix pairs $(\mathbf{F}_1, \mathbf{F}_2)$ over a field $\bar{\mathbb{Z}}$, under the equivalence relation

$$(34.39) \quad (\mathbf{F}_1, \mathbf{F}_2) \approx (\mathbf{X}\mathbf{F}_1\mathbf{Y}, \mathbf{X}\mathbf{F}_2\mathbf{Y}) \text{ for } \mathbf{X} \in GL_r(\bar{\mathbb{Z}}), \mathbf{Y} \in GL_s(\bar{\mathbb{Z}}).$$

The indecomposable genera of Λ -lattices are in bijective correspondence with the indecomposable matrix pairs, where decomposability of a matrix pair is defined as in (34.38).

We shall now state the Kronecker-Weierstrass Theorem, which gives a complete list of inequivalent indecomposable matrix pairs over an arbitrary field K . Proofs may be found in Dieudonné [46] or Gantmacher [60, Chapter XII].

(34.40) Kronecker-Weierstrass Theorem. *Let $\mathbf{F}_1, \mathbf{F}_2$ be a pair of $r \times s$ matrices over a field K . Equivalence of pairs is defined by (34.39), and decomposability by (34.38). The following is a full list of inequivalent indecomposable pairs:*

(i) $\mathbf{F}_1 = \mathbf{I}$, $\mathbf{F}_2 = \text{companion matrix of } (h(x))^m$, where $h(x)$ ranges over all irreducible polynomials in $K[x]$, and m over all positive integers.

(ii) For each $m \geq 1$,

$$\mathbf{F}_1 = \begin{bmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \\ 0 & 0 & 0 & \cdots & 0 \end{bmatrix}^{m \times m}, \quad \mathbf{F}_2 = \mathbf{I}^{m \times m}.$$

(iii) For each $m \geq 1$,

$$\mathbf{F}_1 = [\mathbf{I} \quad \mathbf{0}]^{m \times (m+1)}, \quad \mathbf{F}_2 = [\mathbf{0} \quad \mathbf{I}]^{m \times (m+1)},$$

where $\mathbf{0}$ is an $m \times 1$ column vector of 0's.

(iv) For each $m \geq 1$,

$$\mathbf{F}_1 = \begin{bmatrix} \mathbf{I} \\ \mathbf{0} \end{bmatrix}^{(m+1) \times m}, \quad \mathbf{F}_2 = \begin{bmatrix} \mathbf{0} \\ \mathbf{I} \end{bmatrix}^{(m+1) \times m},$$

where $\mathbf{0}$ is a $1 \times m$ row vector of 0's.

Let us apply this theorem to the classification of Λ -lattices. Since $p\Lambda' \cong L^{(2)}$, the exactness of the sequence

$$0 \rightarrow p\Lambda' \rightarrow \Lambda \rightarrow \bar{\mathbb{Z}} \rightarrow 0$$

shows that the extension class of Λ corresponds to a pair of 2×1 matrices over $\bar{\mathbb{Z}}$. But Λ is indecomposable, since $\hat{\Lambda}/\text{rad } \hat{\Lambda} = \hat{\Lambda}/p\hat{\Lambda}' \cong \bar{\mathbb{Z}}$. The genus of Λ thus corresponds to the pair

$$\xi_0 = \left(\begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix} \right)$$

in the above list. Each Λ -lattice M in the genus of Λ thus yields a pair

$$\xi = \left(\begin{pmatrix} a \\ b \end{pmatrix}, \begin{pmatrix} c \\ d \end{pmatrix} \right)$$

with entries in $\bar{\mathbb{Z}}$, such that ξ is equivalent to ξ_0 over $\bar{\mathbb{Z}}$. (This occurs if and only if $ad - bc \neq 0$ in $\bar{\mathbb{Z}}$.) If $M' \vee \Lambda$ yields the pair

$$\xi' = \left(\begin{pmatrix} a' \\ b' \end{pmatrix}, \begin{pmatrix} c' \\ d' \end{pmatrix} \right),$$

then $M \cong M'$ if and only if $\xi \approx \xi'$, that is

$$\begin{pmatrix} a' \\ b' \end{pmatrix} = \mathbf{X} \begin{pmatrix} a \\ b \end{pmatrix} y, \quad \begin{pmatrix} c' \\ d' \end{pmatrix} = \mathbf{X} \begin{pmatrix} c \\ d \end{pmatrix} y \text{ for some } \mathbf{X} \in GL_2(\mathbb{Z}), y \in \bar{\mathbb{Z}}.$$

Hence $\xi \approx \xi'$ if and only if

$$(34.41) \quad \begin{pmatrix} a' & c' \\ b' & d' \end{pmatrix} = \mathbf{X} \begin{pmatrix} a & c \\ b & d \end{pmatrix} y \text{ for some } \mathbf{X} \in GL_2(\mathbb{Z}), y \in \bar{\mathbb{Z}}.$$

This equation yields

$$(34.42) \quad \begin{vmatrix} a' & c' \\ b' & d' \end{vmatrix} = \pm y^2 \cdot \begin{vmatrix} a & c \\ b & d \end{vmatrix}.$$

Conversely, it is easily verified that if (34.42) holds for some $y \in \bar{\mathbb{Z}}$, then (34.41) holds for some \mathbf{X} . It follows at once that the number $g(\Lambda)$ of isomorphism classes in the *principal genus* (that is, the genus of Λ) is given by the index

$$g(\Lambda) = |\bar{\mathbb{Z}} : \{ \pm q^2 : q \in \bar{\mathbb{Z}} \}|.$$

Therefore

$$g(\Lambda) = \begin{cases} 2, & p \equiv 1 \pmod{4}, \\ 1, & \text{otherwise}. \end{cases}$$

We shall now choose a Λ -lattice M for which $g(\Lambda) < g(M)$. Let $h(x) \in \bar{\mathbb{Z}}[x]$ be irreducible, and let \mathbf{F}_2 be the companion matrix of $(h(x))^m$. Let us write $n = md$, where d is the degree of $h(x)$. Then \mathbf{F}_2 is an $n \times n$ matrix over $\bar{\mathbb{Z}}$. Choose M to be the Λ -lattice corresponding to the extension class $\xi = (\mathbf{I}, \mathbf{F}_2)$. Each M' in the genus of M determines a class $\xi' = (\mathbf{G}_1, \mathbf{G}_2)$, and under the equivalence in (34.37) (which does not affect the isomorphism class of M'), we may assume that $\mathbf{G}_1 = \mathbf{I}$. The condition that $M' \vee \Lambda$ then is equivalent to the assertion that \mathbf{G}_2 is *similar* to \mathbf{F}_2 over the field $\bar{\mathbb{Z}}$. Thus, the Λ -lattices M' in the genus of M determine extension classes $\xi' = (\mathbf{I}, \mathbf{G})$, with \mathbf{G} similar to \mathbf{F}_2 over $\bar{\mathbb{Z}}$.

In order to calculate $g(M)$, we must decide when $(\mathbf{I}, \mathbf{G}) \approx (\mathbf{I}, \mathbf{G}')$ where both \mathbf{G}, \mathbf{G}' are similar to \mathbf{F}_2 over $\bar{\mathbb{Z}}$. The reader will easily verify that the image of $GL_n(\mathbb{Z})$ in $GL_n(\bar{\mathbb{Z}})$ is precisely the subgroup $\{\mathbf{T} \in GL_n(\bar{\mathbb{Z}}) : \det \mathbf{T} = \pm 1\}$. It follows from (34.37) that

$$(\mathbf{I}, \mathbf{G}) \approx (\mathbf{I}, \mathbf{G}') \Leftrightarrow \mathbf{G}' = \mathbf{T} \mathbf{G} \mathbf{T}^{-1} \text{ for some } \mathbf{T} \in GL_n(\bar{\mathbb{Z}}) \text{ such that } \det \mathbf{T} = \pm 1.$$

Now we may write

$$\mathbf{G} = \mathbf{B} \mathbf{F}_2 \mathbf{B}^{-1}, \quad \mathbf{G}' = \mathbf{B}' \mathbf{F}_2 \mathbf{B}'^{-1}, \text{ with } \mathbf{B}, \mathbf{B}' \in GL_n(\bar{\mathbb{Z}}).$$

The equation $\mathbf{G}' = \mathbf{T} \mathbf{G} \mathbf{T}^{-1}$ is equivalent to

$$\mathbf{T} \mathbf{B} = \mathbf{B}' \mathbf{S} \text{ for some } \mathbf{S} \text{ which commutes with } \mathbf{F}_2.$$

Let Γ be the subgroup of $GL_n(\bar{\mathbb{Z}})$ generated by $\{\mathbf{T} : \det \mathbf{T} = \pm 1\}$ and all $\mathbf{S} \in GL_n(\bar{\mathbb{Z}})$ which commute with \mathbf{F}_2 . Since the first of these groups is normal in $GL_n(\bar{\mathbb{Z}})$, we conclude at once that

$$(\mathbf{I}, \mathbf{G}) \approx (\mathbf{I}, \mathbf{G}') \text{ if and only if } \mathbf{B}' \in \mathbf{B}\Gamma.$$

Therefore we obtain

$$g(M) = |GL_n(\bar{\mathbb{Z}}) : \Gamma|,$$

and since Γ contains $SL_n(\bar{\mathbb{Z}})$, this gives

$$g(M) = |\bar{\mathbb{Z}} : \det \Gamma|, \text{ where } \det \Gamma = \langle \{\det \gamma : \gamma \in \Gamma\} \rangle.$$

We now calculate $\det \Gamma$, and for this purpose we must compute $\det \mathbf{S}$ for each $\mathbf{S} \in GL_n(\bar{\mathbb{Z}})$ which commutes with \mathbf{F}_2 . Since \mathbf{F}_2 is the companion matrix of $(h(x))^m$ with $h(x)$ irreducible, it follows from linear algebra that $\mathbf{S} = \theta(\mathbf{F}_2)$ for some polynomial $\theta(x) \in \mathbb{Z}[x]$. If $\{\alpha_1, \dots, \alpha_d\}$ are the zeros of $h(x)$ in some splitting field E over $\bar{\mathbb{Z}}$, then the eigenvalues of \mathbf{S} are the $\{\theta(\alpha_i)\}$, each with multiplicity m . Therefore

$$\det \mathbf{S} = \left\{ \prod_{i=1}^d \theta(\alpha_i) \right\}^m = \{N(\theta(\alpha_1))\}^m,$$

where $N: E \rightarrow \bar{\mathbb{Z}}$ is the norm map (see §4). But this norm map N is surjective (see MO, proof of Theorem 14.1, for example). Consequently

$$\det \Gamma = \{ \pm u^m : u \in \bar{\mathbb{Z}} \}.$$

Note that $g(M)$ depends only upon m , and not upon the choice of $h(x)$. We may now choose p and m so that $g(M)$ is large. For example, let p be a

large prime, and let m be some divisor of $(p-1)/2$. Then -1 is an m -th power in $\bar{\mathbb{Z}}$, since -1 is always a $(p-1)/2$ -th power. Therefore

$$g(M) = |\bar{\mathbb{Z}} : \{u^m : u \in \bar{\mathbb{Z}}\}| = (p-1)/m$$

in this case. In particular, $g(M) > g(\Lambda)$ in most circumstances. For instance, if $p=17$ and $m=2$, then $g(M)=8$ while $g(\Lambda)=2$.

To conclude this discussion, we remark that for odd p , $g(M) \leq (p-1)/2$ for all $m \geq 1$. Further, $g(M)=1$ for $p=2$ and all $m \geq 1$. The same estimates also hold for indecomposable Λ -lattices which correspond to other choices of indecomposable matrix pairs listed in the Kronecker-Weierstrass Theorem. For further reading on this topic, see Drozd-Kirichenko [67] and Kirichenko [70], as well as the original article by Drozd-Turčin [67].

§34E. Dihedral and Metacyclic Groups

Let G be the metacyclic group defined by

$$G = \langle x, y : x^p = 1, y^q = 1, yxy^{-1} = x^r \rangle,$$

where p and q are distinct primes, p odd, and where r is a primitive q -th root of $1 \pmod p$. Clearly $q|(p-1)$, and for the special case where $q=2$, G is the dihedral group of order $2p$. We shall find all indecomposable $\mathbb{Z}G$ -lattices, apart from questions involving units in rings of algebraic integers. The results are due to Pu [65]; the special case $q=2$ was treated earlier by Lee [64].

Let $R = \mathbb{Z}[\zeta]$, $K = \mathbb{Q}(\zeta)$, where ζ is a primitive p -th root of 1 over \mathbb{Q} . Define $\sigma \in \text{Aut}_{\mathbb{Q}} K$ by $\sigma(\zeta) = \zeta^r$, and let K_0 be the subfield of K fixed by σ . Then K is a Galois extension of K_0 of degree q , with Galois group $\langle \sigma \rangle$. We set $R_0 = R \cap K_0 = \text{alg. int. } \{K_0\}$. Now let $H = \langle y \rangle$ be cyclic of order q , and form the twisted group algebra $K \circ H$, with y acting as σ on K . By (28.3), $K \circ H \cong M_q(K_0)$. The rational prime p is completely ramified in K (see (4.38)), and we have

$$pR = P^{p-1}, \quad P = (1 - \zeta)R, \quad pR_0 = P_0^{(p-1)/q}, \quad P_0R = P^q,$$

where P_0 and P are prime ideals of R_0 and R , respectively. Thus P_0 is the *only* prime ideal of R_0 ramified in R (by (4.37)), and

$$R/P \cong R_0/P_0 \cong \mathbb{Z}/p\mathbb{Z} = \bar{\mathbb{Z}}.$$

Since $\dim_{K_0} K = q$, it follows that R is tamely ramified over R_0 (see Exercise 4.12), so by (28.7) and the discussion following it, $R \circ H$ is a hereditary R_0 -order in $K \circ H$.

Let the subscripts p and q denote *localization*. From the fibre product diagram

$$(34.43) \quad \begin{array}{ccc} \mathbf{Z}G & \longrightarrow & R \circ H \\ \downarrow & & \downarrow \\ \mathbf{Z}H & \longrightarrow & \bar{\mathbf{Z}}H, \end{array}$$

we have $\mathbf{Z}_q G \cong R_q \circ H \oplus \mathbf{Z}_q H$. Since R_q is unramified over $(R_0)_q$, it follows from §28 that the order $R_q \circ H$ is maximal, and hence* there is (up to isomorphism) a unique indecomposable $(R_q \circ H)$ -lattice, namely R_q itself. (Note that K is a simple $(K \circ H)$ -module.) Furthermore, $\mathbf{Z}_q H$ is a local ring, and by (34.31) its indecomposable lattices are \mathbf{Z}_q , S_q and $\mathbf{Z}_q H$, where $S = \mathbf{Z}[\theta]$ and θ is a primitive q -th root of 1 over \mathbf{Q} . A full list of indecomposable $(\mathbf{Z}_q G)$ -lattices is therefore given by

$$(34.44) \quad \mathbf{Z}_q, S_q, \mathbf{Z}_q H, R_q.$$

The study of $\mathbf{Z}_p G$ -lattices† is somewhat more difficult, and here we will find it more convenient to consider $\hat{\mathbf{Z}}G$ -lattices, where $\hat{\mathbf{Z}}$ is the p -adic completion of \mathbf{Z} . Since $\langle x \rangle$ is a Sylow p -subgroup of G , the proof of (33.4) shows that every indecomposable $\hat{\mathbf{Z}}G$ -lattice is a summand of X^G , for some indecomposable $\hat{\mathbf{Z}}[x]$ -lattice X . By (34.31), there are just three choices for X : $X = \hat{\mathbf{Z}}$ on which x acts as 1; $X = \hat{R} = \hat{\mathbf{Z}}[\xi]$ on which x acts as multiplication by ξ ; and $X = \hat{\mathbf{Z}}[x]$ itself. Now

$$\hat{\mathbf{Z}}^G = \hat{\mathbf{Z}}G \otimes_{\hat{\mathbf{Z}}[x]} \hat{\mathbf{Z}} \cong \hat{\mathbf{Z}}H,$$

where x acts as 1 on $\hat{\mathbf{Z}}H$. Since $x^{p-1} - 1$ splits into distinct linear factors over $\bar{\mathbf{Z}}$, it follows from Hensel's Lemma (Exercise 6.11) that $\hat{\mathbf{Z}}$ contains the $(p-1)$ -st roots of 1. Thus $\theta \in \hat{\mathbf{Z}}$, and since $|H| = q \in (\hat{\mathbf{Z}})$, we obtain a $\hat{\mathbf{Z}}G$ -isomorphism

$$\hat{\mathbf{Z}}H \cong \prod_{i=0}^{q-1} \hat{\mathbf{Z}}_i.$$

Here, x acts as 1 on each summand, while y acts as θ^i on $\hat{\mathbf{Z}}_i$. Furthermore, we may assume that θ was chosen originally to be that (unique) primitive q -th root of 1 for which $\theta \equiv r \pmod{p\hat{\mathbf{Z}}}$. In this case, we have $\bar{\theta} = \bar{r}$ in $\bar{\mathbf{Z}}$, a fact needed in the discussion below.

*This follows readily from (31.2) and the fact that $(R_0)_q$ is semilocal (see proof of (31.15), for example).

†The analogous problem of finding all $\bar{\mathbf{Z}}G$ -modules was treated in (20.11) and (20.13).

Turning next to the case where $X = \hat{R}$, we have $\hat{R}^G \cong \hat{R} \circ H$ as $\hat{\mathbb{Z}}G$ -modules, with $\hat{\mathbb{Z}}G$ acting on $\hat{R} \circ H$ by means of the surjection in (34.43). Now

$$(\hat{R} \circ H) / \text{rad}(\hat{R} \circ H) \cong (\hat{R} \circ H) / (\hat{P} \circ H) \cong \bar{\mathbb{Z}}H,$$

since $\hat{R}/\hat{P} \cong \bar{\mathbb{Z}}$ on which H acts trivially. However, $\bar{\mathbb{Z}}H \cong \coprod_{i=0}^{q-1} \bar{\mathbb{Z}}_i$, with $\bar{\mathbb{Z}}_i = \bar{\mathbb{Z}}$ and y acting as $\bar{\theta}^i$ on $\bar{\mathbb{Z}}_i$. It follows that the ring $\hat{R} \circ H$ must decompose into a direct sum of q non-isomorphic indecomposable projective modules. By the discussion in §28 following the proof of (28.9), the ambiguous ideals $\{\hat{P}^k : 0 \leq k \leq q-1\}$ are such a set of projective $(\hat{R} \circ H)$ -modules, and so we obtain

$$\hat{R} \circ H \cong \prod_{i=0}^{q-1} \hat{P}^i.$$

Note that for each i , \hat{P}^i is a $\hat{\mathbb{Z}}G$ -lattice on which x acts as multiplication by ξ_i , and y acts as the automorphism σ . Further, it easily is verified that $\hat{P}^i/(1-x)\hat{P}^i \cong \bar{\mathbb{Z}}_i$ as $\bar{\mathbb{Z}}H$ -modules. (This uses the fact that $\bar{\theta} = \bar{r}$ in $\bar{\mathbb{Z}}$.)

Finally we treat the case where $X = \hat{\mathbb{Z}}[x]$, so

$$X^G = \hat{\mathbb{Z}}G = \hat{\mathbb{Z}}G \otimes_{\hat{\mathbb{Z}}H} \hat{\mathbb{Z}}H \cong \prod_{i=0}^{q-1} \hat{\mathbb{Z}}_i^G.$$

Let us show that for each i , $0 \leq i \leq q-1$, the $\hat{\mathbb{Z}}G$ -module $\hat{\mathbb{Z}}_i^G$ is indecomposable, and is a non-split extension of the $\hat{\mathbb{Z}}G$ -lattice $\hat{\mathbb{Z}}_i$ by the $\hat{\mathbb{Z}}G$ -lattice \hat{P}^{i+1} . We start with the exact sequence of $\hat{\mathbb{Z}}G$ -lattices

$$0 \rightarrow (x-1)\hat{\mathbb{Z}}[x] \rightarrow \hat{\mathbb{Z}}[x] \rightarrow \hat{\mathbb{Z}} \rightarrow 0,$$

where y acts by conjugation on the first two lattices, and acts as 1 on $\hat{\mathbb{Z}}$. Now the cyclotomic polynomial $x^{p-1} + \dots + x + 1$ annihilates $(x-1)\hat{\mathbb{Z}}[x]$, so x acts as ξ on this lattice. Further, if we put $L = (x-1)\hat{\mathbb{Z}}[x]$, then y acts as $\bar{\theta}$ on $L/(x-1)L$. It follows that $L \cong \hat{P}$ as $\hat{\mathbb{Z}}G$ -lattices, and L is indecomposable. The above sequence can now be written as

$$(34.45) \quad 0 \rightarrow \hat{P} \rightarrow \hat{\mathbb{Z}}[x] \rightarrow \hat{\mathbb{Z}} \rightarrow 0,$$

and the sequence is non-split by (5.25). We now apply $* \otimes_{\hat{\mathbb{Z}}} \hat{\mathbb{Z}}_i$ to the above, obtaining a new exact sequence of inner tensor products of $\hat{\mathbb{Z}}G$ -lattices

$$0 \rightarrow \hat{P} \otimes \hat{\mathbb{Z}}_i \rightarrow \hat{\mathbb{Z}}[x] \otimes \hat{\mathbb{Z}}_i \rightarrow \hat{\mathbb{Z}}_i \rightarrow 0, \quad 0 \leq i \leq q-1.$$

It is easily verified that $\hat{P} \otimes \hat{\mathbb{Z}}_i \cong \hat{P}^{i+1}$ as $\hat{\mathbb{Z}}G$ -modules; this follows from checking the action of y on both sides. The sequence is non-split, since we can recover (34.45) from it by tensoring with $\hat{\mathbb{Z}}_{q-i}$. Further, $\hat{\mathbb{Z}}[x] \otimes \hat{\mathbb{Z}}_i \cong \hat{\mathbb{Z}}_i^G$ by

Frobenius Reciprocity, so we obtain non-split exact sequences of $\hat{\mathbf{Z}}G$ -lattices

$$(34.46) \quad 0 \rightarrow \hat{P}'^{+1} \rightarrow \hat{\mathbf{Z}}_i^G \rightarrow \hat{\mathbf{Z}}_i \rightarrow 0, \quad 0 \leq i \leq q-1.$$

The above remarks show that there are exactly $3q$ non-isomorphic indecomposable $\hat{\mathbf{Z}}G$ -lattices, namely the following:

$$(34.47) \quad \hat{\mathbf{Z}}_i, \hat{P}_i, \hat{\mathbf{Z}}_i^G, \quad 0 \leq i \leq q-1.$$

We are now ready to consider $\mathbf{Z}G$ -lattices M . For each M , let $L = \{m \in M : \Phi(x)m = 0\}$, where $\Phi(x)$ is the cyclotomic polynomial of order p . There is then an exact sequence of $\mathbf{Z}G$ -lattices

$$(\xi) \quad 0 \rightarrow L \rightarrow M \rightarrow N \rightarrow 0$$

in which L is an $(R \circ H)$ -lattice and N is a $\mathbf{Z}H$ -lattice. The isomorphism class of M is completely determined by those of L and N , and by the orbit of ξ in $\text{Ext}(N, L)$ under the actions of $\text{Aut } L$ and $\text{Aut } N$.

The lattice N is completely known by (34.31), namely, N is a direct sum of modules \mathbf{Z}, α , and non-split extensions of α by \mathbf{Z} , with α ranging over a full set of representatives of the h_S ideal classes of S , where $S = \mathbf{Z}[\theta]$ and θ is a primitive q -th root of 1. The discussion in §28, leading to the formula (28.11) and its list of isomorphism invariants, shows that the $(R \circ H)$ -lattice L may be expressed as

$$L \cong \coprod_{i=0}^{q-1} P^i X_i,$$

with X_i an R_0 -lattice of rank r_i . The isomorphism invariants of L are the ranks $\{r_0, \dots, r_{q-1}\}$ and the Steinitz class of the R_0 -lattice $\coprod X_i$.

In calculating orbits in $\text{Ext}(N, L)$, we may replace N and L by lattices in their respective genera, by virtue of (34.15). (The reader will easily verify that the Eichler condition holds for the lattices involved here.) Thus, we may take N to be a sum of copies of \mathbf{Z} , S and $\mathbf{Z}H$ with various multiplicities, and we may assume that L is a direct sum of P_i 's.

Let us now determine which $\mathbf{Z}G$ -lattices M are indecomposable, for the cases where L and N are nonzero. The sequence $0 \rightarrow L_q \rightarrow M_q \rightarrow N_q \rightarrow 0$ must split, since the only indecomposable $\mathbf{Z}_q G$ -lattices are those listed in (34.44). Therefore $M_q \cong L_q \oplus N_q$, and the decomposition of M_q into indecomposable summands is obtained by decomposing L_q and N_q . On the other hand, in considering decompositions after localizing at p , we may instead work with p -adic completions, by §30. By looking at the list (34.47) and the non-split sequences (34.46), and taking into account the formulas

$$\hat{\mathbf{Z}}H \cong \coprod_{i=0}^{q-1} \hat{\mathbf{Z}}_i, \quad \hat{S} \cong \coprod_{i=1}^{q-1} \hat{\mathbf{Z}}_i,$$

the reader will be convinced that the genera of indecomposable $\mathbf{Z}G$ -lattices are represented by the middle terms in the following three types of non-split exact sequences:

$$(34.48) \quad \begin{cases} (a) & 0 \rightarrow P \rightarrow V \rightarrow \mathbf{Z} \rightarrow 0 \\ (b) & 0 \rightarrow L_T \rightarrow X_T \rightarrow S \rightarrow 0 \\ (c) & 0 \rightarrow L_T \rightarrow Y_T \rightarrow \mathbf{Z}H \rightarrow 0. \end{cases}$$

Here, T is any non-empty subset of $\{0, 1, \dots, q-1\}$, and $L_T = \coprod_{t \in T} P^t$. However, in (b) we must always omit the summand P , since there is no non-split extension of $\hat{\mathbf{Z}}$ by \hat{P} for $j = 1, \dots, q-1$.

The preceding discussion shows that the indecomposable genera of $\mathbf{Z}G$ -lattices are represented by

$$P^i (0 \leq i \leq q-1), \mathbf{Z}, S, \mathbf{Z}H; \{X_T\}, \{Y_T\}, V.$$

Further, there is only one genus of each of these types, since the genus of M is determined by the isomorphism classes of M_q and \hat{M} , and we have

$$(34.49) \quad \hat{V} \cong (\hat{\mathbf{Z}}_0)^G, \hat{X}_T \cong \prod_{t \in T} (\hat{\mathbf{Z}}_{t-1})^G \oplus \prod_{t \notin T} \hat{\mathbf{Z}}_{t-1},$$

with an analogous formula for each Y_T . As T varies, we obtain $2^{q-1}-1$ choices for X_T , and 2^q-1 choices for Y_T . Thus there are

$$2^q + 2^{q-1} + q + 2$$

indecomposable genera of $\mathbf{Z}G$ -lattices.

It should be noted that a genus need not decompose uniquely into indecomposable genera. For example, let T_1, \dots, T_4 be non-empty subsets of $\{0, 2, 3, \dots, q-1\}$, such that

$$T_1 \cup T_2 = T_3 \cup T_4 \quad (\text{counting multiplicities}).$$

Then we have

$$(X_{T_1} \oplus X_{T_2}) \vee (X_{T_3} \oplus X_{T_4})$$

by virtue of (34.39).

We remark finally that the question of finding all $\mathbf{Z}G$ -lattices in a given indecomposable genus reduces to a problem on units, of the same nature as the questions on units in §34C.

Let us apply the above discussion to the special case in which G is a dihedral group of order $2p$, where p is an odd prime. We thus take $q=2$,

$r = -1$ in the preceding calculations. Here,

$$K_0 = \mathbb{Q}(\zeta + \zeta^{-1}), R_0 = \mathbb{Z}[\zeta + \zeta^{-1}], \theta = -1, S = \mathbb{Z}.$$

There are then 10 indecomposable genera of $\mathbb{Z}G$ -lattices, represented by the following list:

- (i) $R = \mathbb{Z}[\zeta]$, $P = (1 - \zeta)R$, on which x acts as multiplication by ζ , and y acts as complex conjugation.
- (ii) $\mathbb{Z}, \mathbb{Z}', \mathbb{Z}H$, on which x acts trivially, while y acts as $+1$ and -1 on \mathbb{Z} and \mathbb{Z}' , respectively.
- (iii) $V =$ non-split extension of \mathbb{Z} by P , so $V \cong \text{ind}_H^G \mathbb{Z}$.
- (iv) $X =$ non-split extension of \mathbb{Z}' by R , so $X \cong \text{ind}_H^G \mathbb{Z}'$.
- (v) Y_0, Y_1 , and Y_2 , non-split extensions as shown:

$$\begin{aligned} 0 \rightarrow R \rightarrow Y_0 \rightarrow \mathbb{Z}H \rightarrow 0, \quad 0 \rightarrow P \rightarrow Y_1 \rightarrow \mathbb{Z}H \rightarrow 0, \\ 0 \rightarrow R \oplus P \rightarrow Y_2 \rightarrow \mathbb{Z}H \rightarrow 0. \end{aligned}$$

We have $\hat{\mathbb{Z}}G$ -isomorphisms

$$\hat{Y}_0 \cong \hat{X} \oplus \hat{\mathbb{Z}}, \quad \hat{Y}_1 \cong \hat{V} \oplus \hat{\mathbb{Z}}', \quad \hat{Y}_2 \cong \hat{X} \oplus \hat{V},$$

and therefore

$$(34.50) \quad (Y_0 \oplus Y_1) \vee (Y_2 \oplus \mathbb{Z}H).$$

Since $\text{Ext}(\mathbb{Z}, P) \cong \bar{\mathbb{Z}}$ (see Exercise 34.7), and $\text{Aut } P$ maps onto $(\bar{\mathbb{Z}})$, there is only one orbit of $\text{Ext}(\mathbb{Z}, P)$, under the action of $(\text{Aut } \mathbb{Z}, \text{Aut } P)$, which contains the extension class of V . Similar remarks hold for X and each Y_i . Consequently we obtain:

(34.51) Theorem. *Let α range over a full set of representatives of the h_0 ideal classes of R_0 , where $R_0 = \mathbb{Z}[\zeta + \zeta^{-1}]$. Then there are precisely $7h_0 + 3$ isomorphism classes of indecomposable $\mathbb{Z}G$ -lattices, and these are represented by:*

$$R\alpha, P\alpha; \mathbb{Z}, \mathbb{Z}', \mathbb{Z}H;$$

and nonsplit extensions (compare with the list (i)–(v) above):

$$\begin{aligned} 0 \rightarrow P\alpha \rightarrow V_\alpha \rightarrow \mathbb{Z} \rightarrow 0, \quad 0 \rightarrow R\alpha \rightarrow X_\alpha \rightarrow \mathbb{Z}' \rightarrow 0 \\ 0 \rightarrow R\alpha \rightarrow (Y_0)_\alpha \rightarrow \mathbb{Z}H \rightarrow 0, \quad 0 \rightarrow P\alpha \rightarrow (Y_1)_\alpha \rightarrow \mathbb{Z}H \rightarrow 0 \\ 0 \rightarrow R\alpha \oplus P \rightarrow (Y_2)_\alpha \rightarrow \mathbb{Z}H \rightarrow 0. \end{aligned}$$

Using (34.50), it is not difficult to find all relations connecting direct sums of indecomposable $\mathbb{Z}G$ -lattices. For details, see Lee [64].

Notes. Some additional cases where integral representations have been calculated are as follows:

- (i) G cyclic of squarefree order: Knee [62], Oppenheim [62].
- (ii) Cubic \mathbb{Z} -rings (that is, \mathbb{Z} -orders in semisimple \mathbb{Q} -algebras A with $\dim_{\mathbb{Q}} A = 3$): Faddeev [65b], Drozd [67].
- (iii) G an abelian $(2, 2)$ -group: Nazarova [61], [67]; see also Nazarova-Roiter [69].
- (iv) $G = A_4$ (alternating group): Nazarova [63].
- (v) $G = S_n$ (symmetric group): Craig [76] finds all full $\mathbb{Z}G$ -lattices in a simple $\mathbb{Q}G$ -lattice of \mathbb{Q} -dimension $n - 1$.

§34. Exercises

1. Keep the notation of (34.3), and let M, M' be Λ -lattices. There are exact sequences

$$0 \rightarrow L^{(r)} \rightarrow M \rightarrow \bar{Z}^{(s)} \rightarrow 0, \quad 0 \rightarrow L^{(t)} \rightarrow M' \rightarrow \bar{Z}^{(u)} \rightarrow 0,$$

in which $L^{(r)}$ is a characteristic submodule of M , and $L^{(t)}$ of M' . Show that $M \cong M'$ if and only if $r = t$, $s = u$, and there exists a commutative diagram

$$\begin{array}{ccccccc} 0 & \longrightarrow & L^{(r)} & \longrightarrow & M & \longrightarrow & \bar{Z}^{(s)} & \longrightarrow 0 \\ & & \downarrow \lambda & & \downarrow \mu & & \downarrow \nu & \\ 0 & \longrightarrow & L^{(r)} & \longrightarrow & M' & \longrightarrow & \bar{Z}^{(s)} & \longrightarrow 0 \end{array}$$

in which λ and ν are isomorphisms.

[Hint: An isomorphism μ induces maps $\lambda: L^{(r)} \rightarrow L^{(t)}$, $\nu: \bar{Z}^{(s)} \rightarrow \bar{Z}^{(u)}$, with λ injective, ν surjective. Thus $r \leq t$, $s \geq u$. Now use μ^{-1} .]

2. Keep the notation of (34.33) and the discussion which follows it. Show that there is a fibre product diagram

$$\begin{array}{ccc} E & \xrightarrow{\mu_0} & \mathbb{Z} \\ \downarrow \mu_1 & & \downarrow \\ R_1 & \longrightarrow & \bar{Z}, \end{array}$$

and an exact sequence of E -modules

$$0 \rightarrow \mathbb{Z} \oplus \mathbb{Z} \xrightarrow{1 \oplus \Phi_1(x)} \mathbb{Z} \oplus E \rightarrow R_1 \rightarrow 0.$$

Show that each $f \in \text{End}(\mathbb{Z} \oplus E)$, given as in (34.33), induces maps f_0, f_1 as in (34.34), and that f is an automorphism if and only if both f_0 and f_1 are automorphisms.

3. Using the above notation, show

(i) For each $\alpha \in R_1$, there exists an $f \in \text{Aut}(\mathbb{Z} \oplus E)$ for which $\mu_1(d) = \alpha$.

(ii) For each matrix $\beta \in GL_2(\mathbb{Z})$ whose $(2, 1)$ -entry is a multiple of p , there exists an $f \in \text{Aut}(\mathbb{Z} \oplus E)$ for which $f_1 = \beta$.

4. Keep the notation of the preceding two exercises, and let $\bar{R}_1 = R_1/pR_1$. There is a ring surjection $\theta: R_2 \rightarrow \bar{R}_1$, defined by composition of maps:

$$R_2 \rightarrow R_2/pR_2 \cong \bar{\mathbb{Z}}[\lambda]/(\lambda^{p(p-1)}) \rightarrow \bar{\mathbb{Z}}[\lambda]/(\lambda^{p-1}) \cong \bar{R}_1,$$

where $\lambda = 1 - \omega_2$. Show that for each $s \in R_2$, there exists an $r \in R_1$ such that $\theta(s) = r$ in \bar{R}_1 .

[Hint: The result is trivial when $p=2$, so assume p odd. Write $s=f(\omega_2)$, where $f(X) \in \mathbb{Z}[X]$, and let $f(X) = \prod_{j=1}^n (X - \alpha_j)$ in some splitting field for $f(X)$ over $\mathbb{Q}(\omega_2)$. We choose $r=N(s) \in R_1$, where $N: R_2 \rightarrow R_1$ is the relative norm map. Then $r \in R_1$ since N is multiplicative. Further

$$r = N(f(\omega_2)) = \prod_{i=0}^{p-1} f(\omega_1^i \omega_2) = \prod_i f(\omega_1^i X) \Big|_{X=\omega_2}.$$

But

$$\begin{aligned} \prod_i f(\omega_1^i X) &= \prod_{i=0}^{p-1} \prod_{j=1}^n (\omega_1^i X - \alpha_j) = \prod_j (X^p - \alpha_j^p) \\ &\equiv \left\{ \prod_j (X - \alpha_j) \right\}^p = \{f(X)\}^p \equiv f(X^p) \pmod{p}. \end{aligned}$$

Therefore

$$r \equiv f(\omega_2^p) = f(\omega_1) = \theta(s) \pmod{pR_1},$$

as desired.]

5. Keep the notation of (34.28). Show that E does not decompose into a direct sum of ideals.

[Hint: If E decomposes, so does \bar{E} , where bars denote reduction mod p . But $\bar{E} \cong \bar{\mathbb{Z}}[\lambda]/(\lambda^d)$.]

6. Let $\bar{Z} = \mathbb{Z}/p\mathbb{Z}$. Show that the image of $GL_n(\mathbb{Z})$ in $GL_n(\bar{Z})$ consists of all matrices in $GL_n(\bar{Z})$ of determinant ± 1 .

7. Using the notation in §34E, prove that

$$\mathrm{Ext}_{\hat{\mathbb{Z}}G}^1(\hat{\mathbb{Z}}_i, \hat{P}^{i+1}) \cong \bar{\mathbb{Z}}, \quad 0 \leq i \leq q-1,$$

and that $\hat{P}^q \cong \hat{R}$ as $\hat{\mathbb{Z}}G$ -modules.

8. For $n \geq 2$, let ω be a primitive 2^n -th root of 1, and let $R = \mathbb{Z}[\omega]$. Let $\Lambda = R \circ H$ be the twisted group ring, where $H = \langle x : x^2 = 1 \rangle$, and where $x\alpha = \bar{\alpha}x$, $\alpha \in R$, with $\bar{\alpha}$ the complex conjugate of α . Show that $K = \mathbb{Q}(\omega)$ is the unique simple $(K \circ H)$ -module, where x acts as complex conjugation on K . Let α_i range over the h_0 representatives of the ideal classes of R_0 , where $R_0 = \mathbb{Z}[\omega + \bar{\omega}]$.

(i) Prove that a full set of non-isomorphic full Λ -lattices in K is given by $\{R\alpha_i : 1 \leq i \leq h_0\} \cup \{(1-\omega)R\alpha_i : 1 \leq i \leq h_0\}$.

(ii) Show that for $1 \leq i, j \leq h_0$,

$$\mathrm{Ext}_{\Lambda}^1(R\alpha_i, (1-\omega)R\alpha_j) = 0 = \mathrm{Ext}_{\Lambda}^1((1-\omega)R\alpha_i, R\alpha_j),$$

$$\mathrm{Ext}_{\Lambda}^1(R\alpha_i, R\alpha_j) \cong \bar{\mathbb{Z}} \cong \mathrm{Ext}_{\Lambda}^1((1-\omega)R\alpha_i, (1-\omega)R\alpha_j),$$

where $\bar{\mathbb{Z}} = \mathbb{Z}/2\mathbb{Z}$.

(iii) Show that there exist nonsplit exact sequences of Λ -lattices:

$$0 \rightarrow R \rightarrow \Lambda \rightarrow R \rightarrow 0, \quad 0 \rightarrow (1-\omega)R \rightarrow \Lambda \rightarrow (1-\omega)R \rightarrow 0.$$

(iv) Find all indecomposable Λ -lattices.

[Hint: See Theohari-Apostolidi [82].]

§35. INVERTIBLE IDEALS

In this section we shall be concerned mainly with the theory of invertible ideals in commutative rings. However, we begin our discussion with the more general concept of invertible bimodules over a pair of rings Λ, Δ , not necessarily commutative. This extra generality will be needed for our discussion of Picard groups in Chapter 11.

A (Λ, Δ) -bimodule ${}_{\Lambda}M_{\Delta}$ is called *invertible* if M gives rise to a Morita equivalence between the categories of Λ -modules and Δ -modules, according to Theorem 3.54. This occurs if all of the following conditions are satisfied:

- (i) $M \in \mathcal{P}(\Lambda)$, the category of f.g. projective Λ -modules,
- (ii) M is a generator for the category of left Λ -modules,
- (iii) $\Delta \cong \{\mathrm{End}_{\Lambda} M\}^{\circ}$.

On the other hand, given a left Λ -module M , define Δ as in (iii). Then there are bimodule maps

$$(35.1) \quad (\cdot, \cdot): M \otimes_{\Delta} \text{Hom}(M, \Lambda) \rightarrow \Lambda, [\cdot, \cdot]: \text{Hom}(M, \Lambda) \otimes_{\Lambda} M \rightarrow \Delta.$$

We showed that (\cdot, \cdot) is surjective if and only if M is a generator for the category of left Λ -modules, and that $[\cdot, \cdot]$ is surjective if and only if $M \in \mathcal{P}(\Lambda)$. In particular, if both maps are surjective, then both are isomorphisms.

We may restate (35.4) as follows: a bimodule ${}_{\Lambda}M_{\Delta}$ is invertible if and only if there exists a bimodule ${}_{\Delta}N_{\Lambda}$ and bimodule surjections

$$(35.2) \quad M \otimes_{\Delta} N \rightarrow \Lambda, N \otimes_{\Lambda} M \rightarrow \Delta,$$

for which the following diagrams commute:

$$(35.3) \quad \begin{array}{ccc} M \otimes_{\Delta} N \otimes_{\Lambda} M & \longrightarrow & \Lambda \otimes_{\Lambda} M \\ \downarrow & & \downarrow \\ M \otimes_{\Delta} \Delta & \longrightarrow & M, \end{array} \quad \begin{array}{ccc} N \otimes_{\Lambda} M \otimes_{\Delta} N & \longrightarrow & \Delta \otimes_{\Delta} N \\ \downarrow & & \downarrow \\ N \otimes_{\Lambda} \Lambda & \longrightarrow & N. \end{array}$$

When this occurs, the maps in (35.2) are isomorphisms.

For example, let A be a simple artinian ring, and let ${}_A X_A$ be an invertible bimodule. We claim that $X \cong A$ as left A -modules. Suppose that V is a simple left A -module, and set $D = \text{End}_A V$, so $A \cong \text{End}_D V$. Since X is invertible, we have $A \cong \{\text{End}_A({}_A X)\}^{\circ}$. Now $X \cong V^{(n)}$ for some n (as left A -modules), so

$$A^{\circ} \cong \text{End}_A(V^{(n)}) \cong M_n(D).$$

But then $n = \dim_D V$ and $X \cong V^{(n)} \cong A$ as left A -modules, as claimed. (We note, however, that X need not be isomorphic to A as (A, A) -bimodule; see Exercise 35.13.)

We show next that invertibility is a “local” property:

(35.4) Proposition. *Let R be a commutative noetherian ring, and let Λ and Δ be R -algebras, f.g./ R as modules. Let ${}_{\Lambda}M_{\Delta}$ be a bimodule f.g./ R . Let P range over all maximal ideals of R , and let M_P, Λ_P, Δ_P , etc., denote localizations at P . Then M is an invertible (Λ, Δ) -bimodule if and only if for each P , the (Λ_P, Δ_P) -bimodule M_P is invertible.*

Proof. For each P , we have maps

$$M_P \otimes \text{Hom}_{\Lambda_P}(M_P, \Lambda_P) \rightarrow \Lambda_P, \text{Hom}_{\Lambda_P}(M_P, \Lambda_P) \otimes M_P \rightarrow \Delta_P,$$

obtained by localizing the maps in (35.1). The desired result follows at once from (4.2). Note that

$$\{\text{End}_{\Lambda} M\}_P \cong \text{End}_{\Lambda_P} M_P \text{ for all } P.$$

Suppose now that Λ is a commutative ring, and let us agree to make each one-sided Λ -module M into a (Λ, Λ) -bimodule by setting $m\lambda = \lambda m$ for all $m \in M, \lambda \in \Lambda$. We shall call M an *invertible* Λ -module if M is invertible as bimodule. The discussion preceding (35.4) shows that if Λ is a direct sum of fields, then a Λ -module M is invertible if and only if $M \cong \Lambda$. We shall use this fact in proving that invertible modules are locally free:

(35.5) Theorem. *Let Λ be a commutative R -algebra, f.g./ R as module, where R is a commutative noetherian ring. Let M be any f.g. Λ -module. Then M is invertible if and only if $M_P \cong \Lambda_P$ for each maximal ideal P of R .*

Proof. If M is invertible, so is M_P , and we must show that $M_P \cong \Lambda_P$. Replacing R by R_P and changing notation, we may now assume that R is a local noetherian ring. Let $J = \text{rad } \Lambda$, and let bars denote reduction mod J . Since M is invertible, there exists a Λ -module N and maps as in (35.2) and (35.3), with Δ replaced by Λ . The corresponding situation then occurs for the Λ -modules \bar{M} and \bar{N} , which shows that \bar{M} is an invertible $\bar{\Lambda}$ -module. But $\bar{\Lambda}$ is a commutative semisimple ring by (5.22), and is therefore a direct sum of fields. Our previous discussion shows that $\bar{M} \cong \bar{\Lambda}$. Since $M \in \mathcal{P}(\Lambda)$, we obtain $M \cong \Lambda$ by (6.6).

Conversely, suppose that $M_P \cong \Lambda_P$ for each P , and let $\Delta = \text{End}_\Lambda(M)$. Then $\Lambda \subseteq \Delta$, and $\Lambda_P = \Delta_P$ for each P , whence $\Lambda = \Delta$ by (4.2). But then in the situation of (35.1) with Δ replaced by Λ , both maps are surjective at each P , whence they are surjective by (4.2). Hence M is an invertible Λ -module, as desired.

As a corollary, we obtain the following result of Faddeev [65a]:

(35.6) Corollary. *Let Λ be a commutative R -order, where R is a Dedekind domain, and let M be a Λ -lattice. Then M is invertible if and only if M lies in the genus of Λ . Each such M is isomorphic to a locally free ideal of Λ .*

A more general result of this nature, needed for our later discussion, is as follows:

(35.7) Proposition. *Let Λ be an R -order in a f.d. commutative K -algebra A , where R is a Dedekind domain with quotient field K , and let M be a Λ -lattice. Then we have an equivalence:*

$$\left. \begin{array}{l} M \text{ is } \Lambda\text{-projective} \\ KM \cong A^{(n)} \end{array} \right\} \Leftrightarrow M \vee \Lambda^{(n)}.$$

Proof. If $M \vee \Lambda^{(n)}$, then M is Λ -projective and $KM \cong A^{(n)}$, so we need only prove the converse. Replacing R by its P -adic completion, where P is an arbitrary maximal ideal of R , and changing notation, we must now show that if $M \in \mathcal{P}(\Lambda)$ and $KM \cong A^{(n)}$, then $M \cong \Lambda^{(n)}$.

Let $J = \text{rad } \Lambda$, so Λ/J is a direct sum of fields. Then we may write $\Lambda = \bigoplus_{i=1}^r \Lambda e_i$, where the $\{e_i\}$ are primitive orthogonal idempotents in Λ , and each $\Lambda e_i/J e_i$ is one of the fields occurring as a summand of Λ/J . Then $\Lambda e_i \cong \Lambda e_j$ if and only if $i=j$, and furthermore, the A -modules $A e_i$ and $A e_j$ have no common direct summand if $i \neq j$.

Now we may write

$$M \cong \coprod_{i=1}^r (\Lambda e_i)^{(m_i)},$$

whence

$$KM \cong \prod (A e_i)^{(m_i)}, A^{(n)} \cong \prod (A e_i)^{(n)}.$$

Thus each $m_i = n$, so $M \cong \Lambda^{(n)}$ as claimed.

Note. The same argument shows that if $M, N \in \mathcal{P}(\Lambda)$ and $KM \cong KN$, then $M \vee N$. See Exercise 35.9.

We now wish to relate the above concept of invertibility with the intuitively more appealing concept of invertibility of fractional ideals relative to some ring. Suppose from now on that R is a Dedekind domain with quotient field K , and let A be a f.d. *commutative* K -algebra, which we shall later assume to be separable over K . Let M be a full R -lattice in A , that is, M is a f.g. projective R -module such that $KM = A$. We may think of M as a “fractional ideal” in A . Let Λ be the (left) order of M as defined in (24.3), that is,

$$\Lambda = \{x \in A : xM \subseteq M\} = O(M).$$

Then Λ is an R -order in A , and M is a Λ -lattice. We define

$$M^{-1} = \{y \in A : yM \subseteq \Lambda\},$$

as in (26.15). Then M^{-1} is also a full R -lattice in A , and obviously $M^{-1} \cong \text{Hom}_{\Lambda}(M, \Lambda)$. If M is invertible, then the obvious map $M \otimes_{\Lambda} M^{-1} \rightarrow \Lambda$ is surjective, and therefore $M \cdot M^{-1} = \Lambda$.

Let M be a full R -lattice in A . We may observe that if M is an invertible Δ -module, where Δ is some R -order in A , then $M \cdot N = \Delta$ for some Δ -module N in A . (Indeed, if $MN = \Delta$ for some full R -lattice N in A , then also $M \cdot \Delta N = \Delta$, and ΔN is a Δ -module.) From the equality $M \cdot N = \Delta$ we find at once that $\Delta = O(M)$. Thus, the only case in which M can be an invertible Δ -module is that where $\Delta = O(M)$, and where M is invertible when considered as $O(M)$ -module. This motivates the following definition.

(35.8) Definition. A full R -lattice M in A is called *invertible* if M is an invertible Λ -module, where Λ is the order of M , defined as above.

Let M be a full R -lattice in a commutative separable K -algebra A . The powers M, M^2, \dots are also full lattices in A . If M is invertible, then obviously so is each power of M ; for if $MN = \Lambda$, where Λ is the order of M , then $M'N' = \Lambda$, which readily implies that Λ is the order of M' and that M' is invertible. It may happen, however, that some power of M is invertible even though M itself is not. In this section we shall prove the beautiful Dade-Taussky-Zassenhaus Theorem, which states that when A is an algebraic number field of degree n over the rational field \mathbb{Q} , then M^{n-1} is invertible for every full \mathbb{Z} -lattice M in A . Our proof will be based on the treatment given by Singer [73], which in turn depends on his simplified proof of a theorem of Fröhlich, interesting in its own light.

For the rest of this section, let A be a commutative f.d. separable K -algebra. Then A is just a finite direct sum of finite separable field extensions of K , by §7. Let Λ_0 be the integral closure of R in A , so by (26.10), Λ_0 is the unique maximal R -order in A . Let M and N be a pair of full R -lattices in an A -module V . We shall write $M \cong N$ if M and N are isomorphic Γ -lattices for some R -order Γ in A contained in both the order of M and the order of N ; by Exercise 23.2, this definition does not depend on the choice of Γ . Likewise, we say that M and N are in the same genus, and write $M \vee N$, if $M_P \cong N_P$ as Γ_P -lattices for each maximal ideal P of R . As pointed out in §30, $M_P \simeq N_P$ if and only if $\hat{M}_P \cong \hat{N}_P$, where $\hat{}$ indicates P -adic completion.

Now let J be a “fractional ideal” in A , that is, a full R -lattice in A . We have seen that J is invertible if and only if J is locally free (as $O(J)$ -lattice, where $O(J)$ is the order of J). We shall prove below the somewhat surprising result due to Fröhlich, which shows that J is invertible if and only if

$$\text{ord}_R(\Lambda_0 J/J) = \text{ord}_R(\Lambda_0 / O(J)),$$

where ord_R is the R -order ideal defined in §4D. In fact, we shall establish a more general result due to Fröhlich [65], as follows:

(35.9) Theorem. *Let A be a commutative separable K -algebra, Λ_0 its maximal R -order, and Λ any R -order in A . Let M be a full Λ -lattice in a free A -module $A^{(n)}$. Then*

$$(35.10) \quad \text{ord}_R(\Lambda_0 M/M) \text{ divides } \{\text{ord}_R(\Lambda_0 / \Lambda)\}^n,$$

and equality holds if and only if M is in the genus of $\Lambda^{(n)}$, or equivalently, if and only if M is Λ -projective.

Proof. We follow Dade's approach, as described in Fröhlich [65, Appendix B]. For each maximal ideal P of R , order ideals behave properly under passage to P -adic completions (see §4D). The hypotheses of the theorem carry over to the completions; since the conclusion of the theorem (that

$M \vee \Lambda^{(n)}$) is a local statement, it suffices to prove the result* when R is replaced by its completion. Changing notation, we assume for the rest of the proof that R is a complete d.v.r. with residue class field $\bar{R} = R/P$.

We suppose first that \bar{R} is an infinite field, and prove the theorem for this case. We may write

$$A \cong \coprod_{i=1}^t K_i, \quad \Lambda_0 \cong \coprod_{i=1}^t R_i, \quad R_i = \text{integral closure of } R \text{ in } K_i.$$

Here, each K_i is a finite separable extension field of K , and R_i is a d.v.r. with quotient field K_i . Let e_1, \dots, e_t be the primitive idempotents of A corresponding to the above decomposition, so $Ae_i \cong K_i$, $\Lambda_0 e_i \cong R_i$. Let $J_0 = \text{rad } \Lambda_0$; if P_i is the maximal ideal of R_i , then $J_0 \cong \coprod P_i$, and

$$\bar{\Lambda}_0 = \Lambda_0/J_0 = \bigoplus \Lambda_0 e_i / J_0 e_i \cong \coprod_{i=1}^t \bar{R}_i,$$

where $\bar{R}_i = R_i/P_i$ is a finite extension of the field \bar{R} .

Since $KM \cong A^{(n)}$, it is clear from (26.12ii), and the proof of (35.7), that the Λ_0 -lattice $\Lambda_0 M$ must be a free Λ_0 -module on n generators. (This also follows as a special case of Exercise 26.11.) We shall show that there exist elements $m_1, \dots, m_n \in M$ which form a free Λ_0 -basis for $\Lambda_0 M$, and we proceed to construct them inductively. We may write $\Lambda_0 M = \bigoplus_{i=1}^n \Lambda_0 a_i$, where the $\{a_i\}$ are a Λ_0 -basis for $\Lambda_0 M$. Then

$$\begin{aligned} \Lambda_0 M / J_0 M &= (\bigoplus \Lambda_0 a_i) / (\bigoplus J_0 a_i) = \bigoplus \bar{\Lambda}_0 \bar{a}_i \\ &\cong \bigoplus_{i=1}^n \bigoplus_{i=1}^t \bar{R}_i \bar{a}_i = \bigoplus_{i=1}^t X_i, \end{aligned}$$

where

$$X_i = \bigoplus_{i=1}^n \bar{R}_i \bar{a}_i \cong e_i \Lambda_0 M / e_i J_0 M, \quad 1 \leq i \leq t.$$

Thus, each X_i is an n -dimensional space over the field \bar{R}_i . The maps $M \rightarrow \Lambda_0 M \rightarrow \Lambda_0 M / J_0 M \rightarrow X_i$ induce an \bar{R} -homomorphism

$$\theta_i: M/PM \rightarrow X_i$$

for each i , $1 \leq i \leq t$, and $\theta_i(M/PM)$ spans X_i over \bar{R}_i .

Now let $0 \leq r < n$, and suppose that we have found elements $v_1, \dots, v_r \in M/PM$ such that

$\theta_i(v_1), \dots, \theta_i(v_r)$ are linearly independent over \bar{R}_i , for $1 \leq i \leq t$.

*Of course, we will prove that $M \cong \Lambda^{(n)}$ rather than $M \vee \Lambda^{(n)}$.

We wish to find an element $v_{r+1} \in M/PM$ so that the above property holds for the larger collection v_1, \dots, v_{r+1} . Let

$$W_i = \theta_i^{-1} \left\{ \bigoplus_{j=1}^r \bar{R}_i \theta_i(v_j) \right\}, \quad 1 \leq i \leq t.$$

(In the special case where $r=0$, let $W_i = \theta_i^{-1}(0) = \ker \theta_i$.) Each W_i is then a proper \bar{R} -subspace of M/PM , since $\theta(W_i)$ is an r -dimensional \bar{R}_i -space whereas $\theta_i(M/PM)$ spans the n -dimensional space X_i over \bar{R}_i . Now \bar{R} is assumed infinite, so by Exercise 35.6, the space M/PM cannot be the union of the proper subspaces W_1, \dots, W_t . Hence there exists an element $v_{r+1} \in M/PM$ which does not lie in any of W_1, \dots, W_t . But then v_{r+1} has the desired property.

We have now obtained (by induction) a set of n elements $v_1, \dots, v_n \in M/PM$ such that for each i , $1 \leq i \leq t$, their images $\theta_i(v_1), \dots, \theta_i(v_n)$ form a $\Lambda_0 \bar{e}_i$ -basis for X_i . Choose elements $m_j \in M$ representing the elements $\{v_j\}$. Then we obtain

$$\Lambda_0 M = \sum_{j=1}^n \Lambda_0 m_j + J_0 M,$$

so $\Lambda_0 M = \bigoplus \Lambda_0 m_j$ by Nakayama's Lemma. Therefore we obtain

$$\bigoplus_{j=1}^n \Lambda_0 m_j = \Lambda_0 M \supseteq M \supseteq \bigoplus_{j=1}^n \Lambda m_j,$$

and so

$$\text{ord}_R \Lambda_0 M / M \text{ divides } \text{ord}_R (\Lambda_0 M / \bigoplus \Lambda m_j),$$

with equality if and only if $M = \bigoplus \Lambda m_j$. But the latter order ideal is precisely $\{\text{ord}(\Lambda_0 / \Lambda)\}^n$, so we have established (35.10). Further, equality in (35.10) implies that $M \cong \Lambda^{(n)}$. Conversely, $M \cong \Lambda^{(n)}$ clearly gives equality in (35.10), so the theorem is proved in this case.

If the field \bar{R} is finite, we follow the procedure described in Exercises 35.1–35.5. Let $E = K(t)$ be a simple transcendental extension of K , and extend the valuation from K to E , getting a d.v.r. S in E with maximal ideal PS . Let \hat{S} be the completion of S , \hat{E} that of E , and let us set

$$\hat{S}\Lambda = \hat{S} \otimes_R \Lambda, \quad \hat{S}\Lambda_0 = \hat{S} \otimes_R \Lambda_0, \quad \hat{E}A = \hat{E} \otimes_K A,$$

and so on. By Exercise 35.5, $\hat{S}\Lambda$ is an \hat{S} -order in the commutative separable \hat{E} -algebra $\hat{E}A$, and $\hat{S}M$ is a full $\hat{S}\Lambda$ -lattice in $(\hat{E}A)^{(n)}$. Furthermore, \hat{S} has infinite residue class field. We may now apply the preceding argument to

deduce that

$$(35.11) \quad \text{ord}_{\hat{S}} \hat{S}\Lambda_0 M / \hat{S}M \text{ divides } \{\text{ord}_{\hat{S}} \hat{S}\Lambda_0 / \hat{S}\Lambda\}^n,$$

with equality if and only if $\hat{S}M \cong (\hat{S}\Lambda)^{(n)}$.

By (4.18),

$$\text{ord}_{\hat{S}} \hat{S}\Lambda_0 M / \hat{S}M = \hat{S} \otimes_R \text{ord}_R \Lambda_0 M / M, \quad \text{ord}_{\hat{S}} \hat{S}\Lambda_0 / \hat{S}\Lambda = \hat{S} \otimes_R \text{ord}_R \Lambda_0 / \Lambda,$$

so (35.11) implies (35.10). Further, equality holds in one case if and only if it holds in the other. But $\hat{S}M \cong (\hat{S}\Lambda)^{(n)}$ if and only if $M \cong \Lambda^{(n)}$ (see Exercise 35.5). The final assertion in the theorem follows from (35.7), and the theorem is established.

(35.12) Corollary. *Let J be a full R -lattice in A , and let $\Lambda = O(J)$ be its order. Then*

$$\text{ord } \Lambda_0 J / J \text{ divides } \text{ord } \Lambda_0 / \Lambda,$$

and equality holds if and only if $J \vee \Lambda$.

(35.13) Corollary. *Let M be a full R -lattice in $A^{(n)}$, and let J be any fractional ideal (that is, a full R -lattice in A). Then*

$$\text{ord } \Lambda_0 JM / JM \text{ divides both } (\text{ord } \Lambda_0 J / J)^n \text{ and } \text{ord}(\Lambda_0 M / M).$$

Further, $\text{ord } \Lambda_0 JM / JM = \text{ord } \Lambda_0 M / M$ if and only if $JM \vee M$.

Proof. We may assume that R is a complete d.v.r. with infinite residue class field, as in the proof of (35.9). We may write $\Lambda_0 M = \bigoplus \Lambda_0 m_i$, with each $m_i \in M$. Then

$$\Lambda_0 JM = \bigoplus \Lambda_0 Jm_i \supseteq JM \supseteq \bigoplus Jm_i.$$

Hence $\text{ord}(\Lambda_0 JM / JM)$ divides $\text{ord}(\bigoplus \Lambda_0 Jm_i / \bigoplus Jm_i)$, that is, it divides $(\text{ord } \Lambda_0 J / J)^n$. Equality holds if and only if $JM \cong J^{(n)}$.

Secondly, J is a full R -lattice in A , so using J in place of M in the proof of (35.9), it follows that $\Lambda_0 J = \Lambda_0 x$ for some $x \in J$. Clearly x is invertible in A , and $1 = xx^{-1} \in Jx^{-1}$, so we have

$$\Lambda_0 M = \Lambda_0 Jx^{-1} M \supseteq Jx^{-1} M \supseteq M.$$

Hence

$$\text{ord}(\Lambda_0 JM / JM) = \text{ord}(\Lambda_0 Jx^{-1} M / Jx^{-1} M),$$

and the latter divides $\text{ord } \Lambda_0 M / M$, with equality if and only if $Jx^{-1} M = M$,

that is, $M \cong JM$. This completes the proof. [This step does not require the hypothesis that $KM \cong A^{(n)}$.]

Taking $M=J$ above, we deduce that

$$\text{ord } \Lambda_0 J^2/J^2 \text{ divides } \text{ord } \Lambda_0 J/J,$$

with equality if and only if $J^2 \vee J$. Further, by Exercise 35.7, $J^2 \vee J$ if and only if J is an invertible ideal. Consider now the increasing sequence of ideals of R :

$$\text{ord } \Lambda_0 J/J \subseteq \text{ord } \Lambda_0 J^2/J^2 \subseteq \text{ord } \Lambda_0 J^3/J^3 \subseteq \dots.$$

This terminates, so for some $k \geq 1$ we have

$$\text{ord } \Lambda_0 J^{2k}/J^{2k} = \text{ord } \Lambda_0 J^k/J^k.$$

By the preceding remarks, this implies that J^k is invertible. We improve this result by establishing the following striking theorem, due to Dade-Taussky-Zassenhaus [62]:

(35.14) Theorem. *If $\dim_K A = n \geq 2$, then J^{n-1} is invertible for each fractional ideal J of A .*

Proof. If $\Lambda = O(J^{n-1})$, then J^{n-1} is invertible if and only if $J^{n-1} \vee \Lambda$. Hence it suffices to treat the case where R is a complete d.v.r. and to show that $J^{n-1} \cong \Lambda$. By (30.25), it suffices to prove this after extending the ground ring; hence we may assume that A is a split K -algebra. Finally, extending the ground ring from R to S as in the proof of (35.9), we may further assume that R has infinite residue class field. Replacing J by Jx^{-1} with suitable $x \in A$, as in the proof of (35.13), we may now assume that

$$1 \in J \subseteq \Lambda_0, \quad \Lambda_0 = \bigoplus_{i=1}^n Re_i, \quad A = \bigoplus_{i=1}^n Ke_i,$$

where the $\{e_i\}$ are the primitive idempotents of A . We shall show that $J^{n-1} = J^n$, whence $(J^{n-1})^2 = J^{n-1}$, so $\Lambda = J^{n-1}$, and J^{n-1} is invertible.

Since $1 \in J$, we have $J \subseteq J^2 \subseteq J^3 \subseteq \dots$. Let $\varphi_i: \Lambda_0 \rightarrow Re_i$ be the i -th projection map, so $\varphi_i(J) = Re_i$ since $1 \in J$. We proceed to construct R -bases of J , J^2 , etc., as follows: choose $w_1 \in J$ with $\varphi_1(w_1) = e_1$ (indeed, we may pick $w_1 = 1$). Then

$$J = R w_1 \oplus \{J \cap (Re_2 + \dots + Re_n)\},$$

and likewise (since $w_1 \in J^m$ for $m \geq 1$) we have

$$J^m = R w_1 \oplus \{J^m \cap (Re_2 + \dots + Re_n)\}.$$

Let us put

$$L_m = J^m \cap (Re_2 + \cdots + Re_n), m \geq 1.$$

Then $L_1 \subseteq L_2 \subseteq \cdots$, so $\varphi_2(L_1) \subseteq \varphi_2(L_2) \subseteq \cdots$, and we claim that in fact $\varphi_2(L_1) = \varphi_2(L_2) = \cdots$. Indeed, let $m \geq 2$ and suppose that $\varphi_2(L_{m-1}) = \varphi_2(L_1)$. For $x \in L_m$ we have $xe_1 = 0$ and $x \in J \cdot J^{m-1}$, so we may write

$$\begin{aligned} x &= \sum_i y_i (\beta_i w_1 + z_i) \text{ with } y_i \in J, \beta_i \in R, z_i \in L_{m-1} \\ &= yw_1 + \sum_i y_i z_i \text{ for some } y \in J. \end{aligned}$$

From $e_1 x = 0 = e_1 \cdot \sum y_i z_i$, we obtain $e_1 yw_1 = 0$, so $yw_1 \in L_1$. Therefore

$$\varphi_2(x) = \varphi_2(yw_1) + \sum \varphi_2(y_i) \varphi_2(z_i) \in \varphi_2(L_1).$$

This proves that $\varphi_2(L_m) = \varphi_2(L_1)$ for all $m \geq 1$, as claimed. We may therefore choose $w_2 \in L_1$ such that

$$\varphi_2(L_m) = \varphi_2(L_1) = R\varphi_2(w_2) \text{ for all } m \geq 1,$$

and hence we may write

$$J^m = R w_1 \oplus R w_2 \oplus (J^m \cap (Re_3 + \cdots + Re_n)), m \geq 1,$$

where $w_1, w_2 \in J$.

Now put

$$H_m = J^m \cap (Re_3 + \cdots + Re_n), m \geq 1,$$

so $\varphi_3(H_1) \subseteq \varphi_3(H_2) \subseteq \varphi_3(H_3) \subseteq \cdots$. We claim that the sequence is constant from $\varphi_3(H_2)$ on. Indeed, let $m \geq 3$ and suppose that $\varphi_3(H_{m-1}) = \varphi_3(H_2)$. For $x \in H_m$ we have $e_1 x = e_2 x = 0$, and we may write

$$\begin{aligned} x &= \sum_i y_i (\alpha_i w_1 + \beta_i w_2 + z_i) \text{ with } \alpha_i, \beta_i \in R, y_i \in J, z_i \in J^{m-1} \\ &= yw_1 + y'w_2 + \sum_i y_i z_i \text{ for some } y, y' \in J. \end{aligned}$$

Then

$$yw_1 + y'w_2 \in J^2 \cap (Re_3 + \cdots + Re_n) = H_2, \sum y_i z_i \in J \cdot H_{m-1}.$$

Hence $\varphi_3(x) \in \varphi_3(H_2) + \varphi_3(H_{m-1}) \subseteq \varphi_3(H_2)$, which proves that $\varphi_3(H_2) = \varphi_3(H_3) = \cdots$. Choose $w_3 \in H_2$ so that $\varphi_3(H_2) = R\varphi_3(w_3)$. We then have

$$J^m = R w_1 \oplus R w_2 \oplus R w_3 \oplus (J^m \cap (Re_4 + \cdots + Re_n)), m \geq 2,$$

where $w_1, w_2 \in J$ and $w_3 \in J^2$.

Thus, we may choose R -bases for the powers J, J^2, \dots , so that the first two basis elements w_1, w_2 can be used for each power, the first three w_1, w_2, w_3 for all powers from J^2 on, and so on. After $n-1$ steps, we find w_1, \dots, w_n which serve as R -basis for all powers from J^{n-1} on. Therefore $J^{n-1} = J^n$, and the theorem is proved.

Dade-Taussky-Zassenhaus [62] gave an example in which J^{n-2} is not invertible, so $n-1$ is in general best possible. This approach to the proof of the theorem is due to Singer [73]. In an earlier paper, Singer [70] showed that $n-1$ can be replaced by $d-1$, where d is the number of simple components of A , provided that we make the additional hypothesis that the order $O(J)$ of J maps onto the ring of integers in each component. He used this result to prove that if J is a full left $\mathbb{Z}G$ -lattice in QG , where G is a finite abelian group, then J^{t-1} is invertible. Here, $t = \text{Max}\{d(p) : p \text{ divides } |G|\}$, and $d(p)$ denotes the number of simple components of QG_p , where G_p is a Sylow p -subgroup of G .

Fröhlich's Theorem 35.9 does not generalize to the non-commutative case; see Ballew [70], [71].

For further results on invertible powers of ideals, see Bass [68], Dade [62], Dade-Taussky [65], Faddeev [64, 65a], Falk [76], Gorman [70].

§35. Exercises

- Let $E = K(t)$ be a simple transcendental extension of K , and let K' be a finite separable extension of K . Show that $E \otimes_K K'$ is a finite separable field extension of E , and that in fact $E \otimes_K K' \cong K'(t)$, a simple transcendental extension of K' .

[Hint: Let $K' = K[x]/(f(x))$, with $f(x) \in K[x]$ separable irreducible. Then $E \otimes_K K' \cong E[x]/(f(x))$; if $f = gh$ with $g, h \in E[x]$, then the coefficients of g and h are algebraic over K , and lie in E , hence belong to K . Thus $f(x)$ is irreducible in $E[x]$. The field $E \otimes_K K'$ contains $K'[t]$, hence coincides with $K'(t)$.]

- Keep the above notation, and let v be a discrete valuation on K' with complete valuation ring R' and prime element π' , where $v(\pi') = 1$. Let $R = K \cap R'$, the valuation ring of $v|_K$ in K . Each nonzero $\xi \in K'(t)$ is uniquely of the form $\xi = (\pi')^m f(t)/g(t)$, with $f(t), g(t) \in R'[t]$ primitive. (A polynomial is *primitive* if the G.C.D. of its coefficients is 1.) Now define a valuation v on $K'(t)$ by setting $v(\xi) = m$. Then v is a discrete valuation on $K'(t)$ extending the valuation v on K' . Find the valuation ring S' in $K'(t)$, and show that its residue class field $S'/\pi' S'$ is a simple transcendental extension $\bar{R}'(\bar{t})$, where $\bar{R}' = R'/\pi' R'$. Thus S' has infinite residue class field. Show further that $K'(t)$ is *never* complete in the v -adic valuation.

- Keep the above notation, and let S be the valuation ring of $v|_E$. Prove that $S' = S \otimes_R R'$.

[Hint: Clearly $S \otimes_R R' \subseteq S'$. For the reverse inclusion, let $\xi \in S'$. Since $\xi \in E \otimes_K K'$, we may write

$$\xi = (\pi')^m f(t)/g(t), \quad f(t), g(t) \in R'[t], \quad m \in \mathbb{Z},$$

where $f(t)$ and $g(t)$ are primitive. Then $m \geq 0$ since $\xi \in S'$, and $1/g(t) \in S$, so $\xi \in S \otimes_R R'$.]

4. Keep the above notation, and let Λ_0 be a maximal R -order in a f.d. commutative separable K -algebra A . Show that $S \otimes_R \Lambda_0$ is a maximal S -order in $E \otimes_K A$.

[Hint: It suffices to treat the case where $A = K'$ and $\Lambda_0 = R'$. But then $S \otimes_R R' = S'$, the integral closure of S in $E \otimes_K K'$.]

5. Keep the above notation, and let \hat{S} be the completion of S with respect to its valuation, and \hat{E} the corresponding completion of E . Show that

(i) \hat{S} is a complete d.v.r. with infinite residue class field.

(ii) $\hat{E} \otimes_K A$ is a f.d. commutative separable \hat{E} -algebra.

(iii) $\hat{S} \otimes_R \Lambda_0$ is a maximal \hat{S} -order in $\hat{E} \otimes_K A$.

(iv) If M and N are Λ -lattices, where Λ is any R -order in A , then $M \cong N$ if and only if

$$\hat{S} \otimes_R M \cong \hat{S} \otimes_R N \text{ as } (\hat{S} \otimes_R \Lambda)\text{-lattices.}$$

[Hint: (i) Since S is a d.v.r., its completion \hat{S} is also a d.v.r. with the same residue class field.

(ii) is clear from §7, while (iii) follows from Exercise 4 and (26.21). Finally, (iv) is a consequence of (30.25).]

6. Let Ω be an infinite field, and let V be an n -dimensional Ω -space. Show that V cannot be the union of a finite number of proper subspaces W_1, \dots, W_r .

[Hint: Use induction on r .]

7. Let J be a fractional ideal in A . Show that $J^2 \vee J$ if and only if J is invertible.

[Hint: If $J^2 \vee J$ then $J_P^2 = J_p x_p$ for each P , with $x_p = 1$ a.e. Then $\Lambda_P = J_p x_p^{-1}$ is an R_P -order, and $\Lambda = \bigcap_P \Lambda_P = \cap O(J_P) = O(J)$. We have $J \vee \Lambda$, so J is invertible.]

8. Let G be a cyclic p -group with generator x of order p^m , R the ring of p -adic integers, and let $J = \text{rad } RG = (x-1)RG + pRG$. Show that J^m is the smallest invertible power of J .

[Hint: See Singer [70].]

9. Let R be a d.v.r., Λ an R -order in a commutative separable K -algebra A , and let $M, N \in \mathcal{P}(\Lambda)$. Show that $M \cong N$ if and only if $KM \cong KN$.

[Hint: After passing to completions, we may assume R complete. Let $\{\epsilon_i\}$ be a full set of primitive idempotents in Λ , and $\{e_j\}$ in A . Each ϵ_i is a sum of e 's, with no overlap between different ϵ 's. If $M \cong \coprod (\Lambda \epsilon_i)^{(m_i)}$, the isomorphism class of KM determines the $\{m_i\}$.]

In the remaining Exercises, R denotes a Dedekind domain.

10. Let A be a f.d. K -algebra (not necessarily commutative), Λ any R -order in A , and M a (Λ, Λ) -bimodule. Show that M is invertible if and only if \hat{M}_P is invertible for each maximal ideal P of R . (Here, $\hat{M}_P = P$ -adic completion of M .)

11. Let A be a central simple K -algebra, Λ a hereditary R -order in A . For each P , let

$$M(P) = \Lambda \cap \text{rad } \hat{\Lambda}_P.$$

Show that $M(P)$ is an invertible two-sided ideal of Λ , and that

$$\hat{R}_P \otimes_R M(P) = \text{rad } \hat{\Lambda}_P, \quad \hat{R}_Q \otimes_R M(P) \cong \hat{\Lambda}_Q \text{ for } Q \neq P,$$

where Q denotes a maximal ideal of R .

[Hint: Use (26.28); see MO (39.1).]

12. Keep the notation above. Show that the set of invertible two-sided ideals of Λ is a free abelian group with generators $\{M(P)\}$.

[Hint: See MO, Exercise 39.6.]

13. Let A be any ring, and let f, g, h , etc., be automorphisms of A . By ${}_f A_g$ we denote the (A, A) -bimodule having the same elements as A , but with the action of A “twisted” by f and g , thus:

$$x(a)y = f(x)ag(y) \text{ for all } x, y, a \in A.$$

Here, $\{(a) : a \in A\}$ is the set of elements of ${}_f A_g$. Prove that there are (A, A) -bimodule isomorphisms:

$${}_f A_g \cong {}_{hf} A_{hg} \cong {}_1 A_{f^{-1}g} \cong {}_{g^{-1}f} A_1, \quad {}_f({}_f A_g)_{g'} \cong {}_{f'f} A_{gg'},$$

$${}_f A_g \otimes {}_{f'} A_{g'} \cong {}_f A_{gf'^{-1}g'}, \quad {}_1 A_g \otimes {}_1 A_{g'} \cong {}_1 A_{gg'},$$

$${}_1 A_f \otimes {}_f A_1 \cong A \cong {}_f A_1 \otimes {}_1 A_f,$$

where \otimes means \otimes_A . Show further that for each f , the bimodule ${}_1 A_f$ is invertible, and that ${}_1 A_f \cong A$ as bimodules if and only if f is an inner automorphism of A .

§36. THE KRULL-SCHMIDT-AZUMAYA THEOREM OVER DISCRETE VALUATION RINGS

Throughout this section, we abbreviate “Krull-Schmidt-Azumaya” as K-S-A. We say that the K-S-A Theorem is valid for a ring Λ if every f.g. Λ -module is expressible as a finite direct sum of indecomposable Λ -modules, with the summands uniquely determined up to isomorphism and order of occurrence. We saw in §6 that the K-S-A Theorem holds for every artinian ring Λ . It also

holds if Λ is an R -algebra f.g./ R as module, where R is a complete d.v.r. On the other hand, the K-S-A Theorem usually fails for R -orders when R is a Dedekind ring in a global field; this is already evident from Steinitz's Theorem, when R is not a P.I.D. As we shall see in this section, the K-S-A Theorem is usually not valid when R is a d.v.r. which is not complete. Furthermore, it is usually not valid when R is a semilocal ring.

Let us begin by giving a simple and useful example:

(36.0) Theorem. *Let G be a finite group of order n , and let R be a d.v.r. with quotient field K . If n is a unit in R , then the K-S-A Theorem is valid for RG -lattices.*

Proof. Set $\Lambda = RG$, $A = KG$. By Theorem 30.16, every (left) Λ -lattice M is projective as Λ -module. The last paragraph of the proof of (26.12), which is independent of the preceding part of the proof, then shows that we may write $M = \bigoplus M_i$, where each M_i is a Λ -lattice such that KM_i is a *simple* A -module. Since $KM = \bigoplus KM_i$, the summands $\{KM_i\}$ are the composition factors of the A -module KM , and are therefore uniquely determined by KM , up to isomorphism and order of occurrence. Using (30.16) once more, we conclude that the Λ -lattices $\{M_i\}$ are uniquely determined by M , up to isomorphism and order of occurrence. This completes the proof. (An alternate approach is as follows: By (27.1), Λ is a maximal R -order in A . We then obtain the desired result as a special case of Exercise 36.4. However, the latter ultimately depends on Theorem 26.12, which is a considerably deeper result than Theorem 30.16 used above.)

From now on, suppose that R is a discrete valuation ring (d.v.r.) with maximal ideal P and quotient field K , and let Λ be an R -order in a f.d. semisimple K -algebra A . Let \hat{R} , $\hat{\Lambda}$, \hat{A} , etc., denote P -adic completions. We showed in §30 that even when R is not complete, the K-S-A Theorem may be true for Λ -lattices. Specifically, if every simple left A -module S remains simple upon passing to P -adic completions, then the K-S-A Theorem holds for Λ -lattices by Heller's Theorem 30.18. It then also holds for all f.g. Λ -modules; see Exercise 36.1.

Let us write A as a direct sum of full matrix rings $M_n(D)$, where D is a division algebra whose center C is a finite extension of K . We have

$$\hat{K} \otimes_K M_n(D) \cong M_n((\hat{K} \otimes_K C) \otimes_C D).$$

The hypotheses of Heller's Theorem are satisfied if and only if $\hat{K} \otimes_K C$ is a field \hat{C} , and furthermore $\hat{C} \otimes_C D$ is a division algebra, for each summand $M_n(D)$ of A . Note that $\hat{K} \otimes_K C$ is a field if and only if the P -adic valuation on K has a unique extension to C . (See Exercise 36.3.)

In particular, if $A \cong \prod M_{n_i}(K_i)$ where each K_i is a field such that the P -adic valuation of K extends uniquely to K_i , then $\hat{A} \cong \prod M_{n_i}(\hat{K}_i)$, where \hat{K}_i is the

p -adic completion of K_i . Thus Heller's Theorem applies in this case, and shows that the K-S-A Theorem holds for Λ -lattices.

This situation arose in §34B, where $\Lambda = \mathbb{Z}_p G$ with \mathbb{Z}_p the localization of \mathbb{Z} at p , and G a cyclic p -group. Jones [65] (see also Jacobinski [68b]) proved the following more general result:

(36.1) Theorem. *Let G be a p -group, where p is an odd prime. Then the K-S-A Theorem holds for $\mathbb{Z}_p G$ -lattices.*

Proof. By Chapter 6, we have

$$\mathbb{Q}G \cong \coprod_{i=1}^s M_{n_i}(K_i), \text{ where } K_i = \mathbb{Q}(\omega_i),$$

where each ω_i is a root of 1 of order a power of p . But p is completely ramified in each K_i , so the p -adic valuation extends uniquely to K_i . The result now follows from our remarks above.

Jones [65] also proved:

(36.2) Theorem. *Let G be a nilpotent group of odd order, and suppose G has exponent qp^d , where p is prime, $p \nmid q$, and either $q=1$ or else p is a primitive root* mod q . Then the K-S-A Theorem holds for $\mathbb{Z}_p G$ -lattices.*

Proof. The cases where $q=1$ or $d=0$ are already settled by (36.0) and (36.1), but will be needed here as part of the argument below. Let $\hat{\mathbb{Z}}$, $\hat{\mathbb{Q}}$, etc., denote p -adic completions. It suffices to show that for each simple $\mathbb{Q}G$ -module V , the completion \hat{V} is a simple $\hat{\mathbb{Q}}G$ -module. We shall use the result from Chapter 6 that since G is a nilpotent group of odd order, the Schur index $m_{\mathbb{Q}}(V)$ equals 1. This means that for each extension field K of \mathbb{Q} , the KG -module $K \otimes_{\mathbb{Q}} V$ has no repeated summands. In particular, \hat{V} has this property.

Suppose first that $H = \langle x \rangle$ is a cyclic subgroup of G , and that $V = \mathbb{Q}[x]/(\Phi_m(x))$ is a simple $\mathbb{Q}H$ -module, where $\Phi_m(x)$ is the cyclotomic polynomial of order m . We shall show that the completion \hat{V} is a simple $\hat{\mathbb{Q}}H$ -module. Since q is odd, there exist primitive roots (mod q) if and only if q is a prime power (see Niven and Zuckerman [80, §2.9]). Therefore we may write $m = q'p^d$ where $q' \mid q$, $d' \leq d$, and where p is a primitive root (mod q') if $q' \neq 1$. Changing notation for convenience, suppose that $m = qp^d$. We have $\hat{V} = \hat{\mathbb{Q}}[x]/(\Phi_m(x))$ and we need only check that $\Phi_m(x)$ is irreducible in $\hat{\mathbb{Q}}[x]$. When $q=1$, this is clear from §4H. On the other hand, suppose $q > 1$. We may write

$$\bar{\Phi}_m(x) = (\bar{\Phi}_q(x))^{\varphi(p^d)},$$

*This means that $\varphi(q)$ is the least positive integer t such that $p^t \equiv 1 \pmod{q}$.

where bars denote reduction mod p . If θ is a primitive q -th root of 1 over \mathbb{Q} , then the zeros of $\Phi_q(x)$ are $\{\bar{\theta}^{ip}: 0 \leq i \leq \varphi(q)-1\}$. Their images $\{\bar{\theta}^{ip}\}$ are then the zeros of $\bar{\Phi}_q(x)$, and they are mutually conjugate over \mathbb{Z} . It follows that $\bar{\Phi}_q(x)$ is irreducible in $\bar{\mathbb{Z}}[x]$. An easy argument, left to the reader, then shows that \hat{V} is a simple $\hat{\mathbb{Q}}H$ -module. We have thus shown, under our hypotheses, that for each cyclic subgroup H of G , every simple $\hat{\mathbb{Q}}H$ -module is the completion of a simple $\mathbb{Q}H$ -module.

We are now ready to prove that for each simple $\mathbb{Q}G$ -module V , its completion \hat{V} is a simple $\hat{\mathbb{Q}}G$ -module. By the remarks at the beginning of the proof, we may write $\hat{V} \cong \coprod_{i=1}^r W_i$, where the $\{W_i\}$ are non-isomorphic simple $\hat{\mathbb{Q}}G$ -modules. Let i be fixed, $1 \leq i \leq r$. By the Artin Induction Theorem, there exist cyclic subgroups $\{H_j\}$ of G and $\hat{\mathbb{Q}}H_j$ -modules Y_j such that

$$W_i^{(n)} \oplus \coprod (Y_j)^G \cong \coprod (Y_k)^G,$$

where $n = |G|$. Since each Y_j is a direct sum of simple $\hat{\mathbb{Q}}H_j$ -modules, the preceding step shows that $Y_j \cong \hat{X}_j$ for some $\mathbb{Q}H_j$ -module X_j . Thus we obtain

$$W_i^{(n)} \oplus \coprod (\hat{X}_j)^G \cong \coprod (\hat{X}_k)^G.$$

But then (see Exercise 15.6) we have $W_i^{(n)} \cong \hat{T}_i$ for some $\mathbb{Q}G$ -module T_i . This gives $\hat{V}^{(n)} \cong \coprod_{i=1}^r \hat{T}_i$, so $V^{(n)} \cong \coprod_{i=1}^r T_i$ by the Noether-Deuring Theorem (Exercise 6.6). Therefore each T_i is a sum of copies of V , and consequently each W_i is a sum of copies of \hat{V} . This shows that $r=1$ and $W_1 = \hat{V}$, so \hat{V} is simple, and the theorem is established.

The converse of this result holds when G is abelian (Jones [65]):

(36.3) Proposition. *Let G be an abelian group of exponent qp^d , where $p \nmid q$. Then the K-S-A Theorem holds for \mathbb{Z}_pG -lattices if and only if either $q=1$ or p is a primitive root mod q .*

Proof. If the conditions hold, the preceding proof shows that the K-S-A Theorem holds for \mathbb{Z}_pG -lattices. Conversely, suppose that $q \neq 1$ and that p is not a primitive root mod q . Let $S = \mathbb{Z}_p[\theta]$, where θ is a primitive q -th root of 1 over \mathbb{Q} . Then S is the integral closure of \mathbb{Z}_p in $\mathbb{Q}(\theta)$, and $pS = P_1 \cdots P_g$, where $g = \varphi(q)/(\text{order of } p \text{ mod } q)$, so $g > 1$. Thus S is semilocal but not local.

Now G has a factor group H which is cyclic of order pq , and there is a surjection $\mathbb{Z}_pH \rightarrow S[x]/(x^p - 1) = \Gamma$ (say), obtained by mapping the generator of H of order q onto θ , and the generator of H of order p onto x . Then Γ is a homomorphic image of \mathbb{Z}_pG , and we need only verify that the K-S-A Theorem fails for Γ -lattices. However, Γ is indecomposable since the localization $(\Gamma)_P$ is indecomposable by (5.25). Further, $(\Gamma)_P$ is not a maximal order

for $i=1, 2, \dots, g$. The desired result now follows as a special case of (36.4) below.

The next result, due to Jacobinski, includes as special cases many of the examples where it has been shown that the K-S-A Theorem fails.

(36.4) Theorem. *Let R be a semilocal* Dedekind domain, and let Λ be an R -order which cannot be decomposed into a direct sum of two non-zero two-sided ideals. Suppose there are at least two maximal ideals P of R for which the localization Λ_P is not a maximal R_P -order in A . Then the K-S-A Theorem fails for Λ -lattices.*

Proof. Let Λ' be a maximal R -order in A containing Λ , and let $\{P_i : 1 \leq i \leq k\}$ be the set of maximal ideals of R for which $\Lambda_{P_i} \neq \Lambda'_{P_i}$. Then $k \geq 2$, by hypothesis.

For M a Λ -lattice, and P any maximal ideal of R , the localization M_P is clearly a Λ -lattice. We note that Λ'_P is an order containing Λ_P , and M_P may fail to be a Λ'_P -lattice, since $\Lambda'_P M_P$ (computed inside KM) need not be contained in M_P . We shall call the Λ -lattice M “good” at P if M_P is a Λ'_P -lattice, and otherwise “bad”. Thus, the Λ -lattice Λ itself is bad at P precisely for $P = P_1, \dots, P_k$.

For each i , $1 \leq i \leq k$, let X_i be a maximal element in the set of Λ'_{P_i} -direct summands of Λ_{P_i} . Then we may write

$$(36.5) \quad \Lambda_{P_i} = X_i \oplus Y_i,$$

where X_i is a Λ'_{P_i} -lattice, and where the Λ_{P_i} -lattice Y_i is nonzero, and Y_i has no Λ'_{P_i} -direct summand. Now define ϵ_i to be the sum of all central primitive idempotents e_j of A for which $e_j Y_i \neq 0$. Then $Y_i = \epsilon_i Y_i$, and since $\epsilon_i \in \Lambda'$ by (26.20), it follows from (36.5) that $\epsilon_i \in \Lambda_{P_i}$.

If $\epsilon_1 Y_i = 0$ for $i=2, \dots, k$, the same argument shows that $\epsilon_i \in \Lambda_{P_i}$ for each $i \geq 2$. Since $\Lambda = \cap_P \Lambda_P$, where P ranges over all maximal ideals of R , it follows that $\epsilon_1 \in \Lambda$. But Λ is assumed indecomposable, so $\epsilon_1 = 0$ or 1, and clearly both choices are impossible. Therefore $\epsilon_i Y_i \neq 0$ for some $i \geq 2$, so we may assume that $\epsilon_1 Y_2 \neq 0$. Therefore there exists a central primitive idempotent $e \in A$ for which $e Y_1 \neq 0$, $e Y_2 \neq 0$.

Now let N be an indecomposable Λ_{P_1} -direct summand of Y_1 such that $eN \neq 0$. From the way in which Y_1 was chosen, N is not a Λ'_{P_1} -lattice. By (4.21), we can now find a full Λ -lattice L_1 in KN such that $(L_1)_{P_1} = N$, and L_1 is “good” at all other maximal ideals P of R different from P_1 . Choose L_2 analogously, thus obtaining a pair of indecomposable Λ -lattices L_1 and L_2

*We depart here from our earlier assumption that R is a d.v.r., but we suppose that Λ is an R -order in a separable f.d. K -algebra A .

such that

$$eL_i \neq 0, L_i \text{ is good except at } P_i, \quad i = 1, 2.$$

Let $\{S_j\}$ be a basic set of simple left A -modules, and let

$$KL_1 \cong \coprod S_j^{(m_j)}, \quad KL_2 \cong \coprod S_j^{(n_j)}.$$

Since both eL_1 and eL_2 are nonzero, it follows that $\min(m_j, n_j) \neq 0$ for some j . We now define

$$V = \coprod S_j^{\max(m_j, n_j)}, \quad V' = \coprod S_j^{\min(m_j, n_j)},$$

so V and V' are nonzero A -modules, and $K(L_1 \oplus L_2) \cong V \oplus V'$. We may write

$$V = KL_1 \oplus W_1, \quad V' = KL_2 \oplus W_2,$$

for some A -modules W_1, W_2 . We now choose a full Λ -lattice M in V according to the conditions

- (i) $M_{P_1} = (L_1)_{P_1} \oplus (N_1)_{P_1}$, where N_1 is a full Λ' -lattice in W_1 ,
- (ii) $M_{P_2} = (L_2)_{P_2} \oplus (N_2)_{P_2}$, where N_2 is a full Λ' -lattice in W_2 ,
- (iii) M is good at all P 's different from P_1 and P_2 .

Then M is a Λ -direct summand of $L_1 \oplus L_2$, since this holds locally, and since R is semilocal (see the discussion at the end of §31A). Thus

$$L_1 \oplus L_2 \cong M \oplus M',$$

where M' is a full Λ' -lattice in V' . But this gives a counterexample to the K-S-A Theorem, since L_1 and L_2 are indecomposable, whereas each indecomposable summand of M' must be a Λ' -lattice. This completes the proof of (36.4).

Before giving further examples in which the K-S-A Theorem fails to hold, we prove an interesting result due to Roggenkamp [69]:

(36.6) Theorem. *Let Λ be an R -order in a commutative separable f.d. K -algebra A , where R is a d.v.r. with quotient field K . Then the K-S-A Theorem holds for projective Λ -lattices.*

Proof. If Λ decomposes as $\coprod \Lambda_i$, there is a corresponding decomposition for Λ -lattices. Hence it suffices to prove the result when Λ is indecomposable, which we assume from now on. Let $\hat{\Lambda}$, \hat{A} , etc., denote completions, and let $\{\epsilon_i\}$ be a full set of primitive idempotents in $\hat{\Lambda}$, $\{e_j\}$ a full set in \hat{A} , and $\{a_k\}$ a

full set in A , so each ϵ_i is a sum of e_j 's, with no overlaps. The same holds for each a_k .

In order to prove that the K-S-A Theorem holds for projective Λ -lattices, it suffices to show that the only indecomposable projective Λ -lattice is Λ itself. Let $M \in \mathcal{P}(\Lambda)$ be indecomposable, $M \neq 0$, and write

$$\hat{M} = \coprod_i (\hat{\Lambda}\epsilon_i)^{(m_i)}, \quad KM = \coprod_k (Aa_k)^{(r_k)}.$$

Suppose first that $KM \subseteq A$, whence $\hat{K}\hat{M} \subseteq \hat{A} = \coprod \hat{A}e_j$. It follows that each m_i is 0 or 1, say $m_1 = \dots = m_r = 1$, $m_i = 0$ for $i > r$. Let $N_0 = \coprod_i \hat{\Lambda}\epsilon_i$, so $\hat{M} \oplus N_0 = \hat{\Lambda}$.

We may choose an A -module X such that $KM \oplus X = \overset{i>r}{\hat{A}}$, and then $\hat{K}N_0 \cong \hat{K}X$. Identifying $\hat{K}N_0$ with $\hat{K}X$, and setting $N = X \cap N_0$, we see that N is a Λ -lattice such that $\hat{N} = N_0$. Thus $N \in \mathcal{P}(\Lambda)$, and we have $K(M \oplus N) = K\Lambda$; hence $M \oplus N = \Lambda$ by Exercise 35.9, whence $M = \Lambda$ since Λ is indecomposable.

On the other hand, if $KM \not\subseteq A$ then for some $r \geq 1$ we have $m_1 \geq 2, \dots, m_r \geq 2$, $m_i \leq 1$ for $i > r$. Thus $\hat{K}\hat{M}$ must also have repeated summands, whence so must KM . Indeed, if ϵ_i and a_k have a common summand e_j , then we have $m_i = r_k$. Hence we can assume (after renumbering the $\{r_i\}$ if need be) that $r_1 \geq 2, \dots, r_t \geq 2, r_i \leq 1$ for $i > t$. But then

$$\hat{K} \cdot \coprod_{i=1}^r (\hat{\Lambda}\epsilon_i)^{(m_i)} \cong \hat{K} \cdot \coprod_{k=1}^t (Aa_k)^{(r_k)},$$

which implies (by consideration of idempotents) that

$$\hat{K} \cdot \coprod_{i=1}^r \hat{\Lambda}\epsilon_i \cong \hat{K} \cdot \coprod_{k=1}^t Aa_k.$$

Thus there exists an $N \in \mathcal{P}(\Lambda)$ with $\hat{N} = \coprod_{i=1}^r \hat{\Lambda}\epsilon_i$. Therefore $\hat{N} \mid \hat{M}$, and so $N \mid M$ by Exercise 30.3. This contradicts the fact that M is indecomposable, and completes the proof.

To conclude this section, we give some more examples where the K-S-A Theorem fails. Returning to our original notation, let R be a d.v.r. with maximal ideal $P = \pi R$, quotient field K , and let Λ be an R -order in a separable K -algebra A . Let \hat{R} , $\hat{\Lambda}$, etc., denote P -adic completions.

(36.7) Example. Let L be a finite separable extension field of K , S the integral closure of R in L , and suppose that $PS = P_1P_2$, where P_1 and P_2 are distinct maximal ideals of the semilocal Dedekind domain S . Let $\pi_i S = P_i$, $i = 1, 2$, and let S_i be the P_i -adic completion of S , and L_i the quotient field of S_i . Then $\hat{L} \cong L_1 \oplus L_2$, $\hat{S} \cong S_1 \oplus S_2$.

We choose $A = M_2(L)$, and set

$$\Lambda = \begin{pmatrix} S & S \\ PS & S \end{pmatrix} = R\text{-order in } A = S\text{-order in the } L\text{-algebra } A.$$

Then

$$\hat{\Lambda} = \begin{pmatrix} S_1 & S_1 \\ \pi_1 S_1 & S_1 \end{pmatrix} \oplus \begin{pmatrix} S_2 & S_2 \\ \pi_2 S_2 & S_2 \end{pmatrix} = \Gamma_1 \oplus \Gamma_2, \text{ say.}$$

For $i = 1, 2$, we note that Γ_i is a hereditary S_i -order, and that $\Gamma_i/\text{rad } \Gamma_i \cong \bar{S}_i \oplus \bar{S}_i$, where $\bar{S}_i = S_i/\pi_i S_i$. Thus Γ_i has two non-isomorphic indecomposable projective modules $\Gamma_i e_0^{(i)}, \Gamma_i e_1^{(i)}$, where $e_0^{(i)} = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}, e_1^{(i)} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$. Since $\hat{\Lambda}$ is hereditary, it follows that Λ is also a hereditary order, and each Λ -lattice is projective.

Now define

$$M_{ab} = \begin{pmatrix} S \\ P_1^a P_2^b \end{pmatrix}, a=0,1, b=0,1,$$

so M_{ab} is an indecomposable Λ -lattice for which

$$\hat{M}_{ab} = \Gamma_1 e_a^{(1)} \oplus \Gamma_2 e_b^{(2)}.$$

Hence we obtain

$$M_{00} \oplus M_{11} \cong M_{01} \oplus M_{10}.$$

However, M_{00} is not isomorphic to M_{01} or M_{10} , since these lattices have different completions. The example is due to Roggenkamp [69], and shows that the K-S-A Theorem need not hold for projective Λ -lattices. For further examples of this nature, see Roggenkamp [70, p. 210].

Note that in the above paragraph, S is a semilocal ring and Λ is a hereditary S -order. Thus, the K-S-A Theorem also fails for projective lattices in the semilocal case. For other semilocal examples, see Reiner [62].

If R_0 is a d.v.r. in a field K_0 , we may sometimes find a finite extension K of K_0 , such that the integral closure R of R_0 in K is semilocal rather than local. Each R -order Λ is then also an R_0 -order*, and we can then proceed to find counterexamples to the K-S-A Theorem for this case. Thus, even though R_0 is a d.v.r., the K-S-A Theorem may fail for R_0 -orders. Of course, when R_0 is complete, then R is itself a d.v.r., and so this method of producing counterexamples no longer applies.

*See Exercise 23.9.

For more counterexamples, see Berman-Gudivok [62], Dress [70], Heller [61a], Kneser [66], Roggenkamp [70].

Jacobinski [75] obtains necessary and sufficient conditions for the validity of the K-S-A Theorem for lattices over an order, in the global case.

§36. Exercises

- Let Λ be an R -order in a K -algebra A , where R is a d.v.r. with completion \hat{R} . Suppose that for each simple A -module S , its completion \hat{S} is a simple \hat{A} -module. Prove that the K-S-A Theorem holds for all f.g. Λ -modules.

[Hint: By (30.18), each $\hat{\Lambda}$ -lattice is of the form \hat{L} for some Λ -lattice L . To prove the analogous statement for an arbitrary f.g. $\hat{\Lambda}$ -module X , we express X as an extension $0 \rightarrow T \rightarrow X \rightarrow Y \rightarrow 0$, with T the \hat{R} -torsion submodule of X , and Y a $\hat{\Lambda}$ -lattice. Then $T = \hat{U}$, $Y = \hat{L}$, for some R -torsion Λ -module U and some Λ -lattice L . But $\text{Ext}_{\hat{\Lambda}}^1(\hat{L}, \hat{U}) \cong \hat{R} \otimes_R \text{Ext}(L, U) \cong \text{Ext}_{\Lambda}^1(L, U)$, the last since $\text{Ext}_{\Lambda}^1(L, U)$ is an R -torsion module. Hence X is the completion of some Λ -extension of L by U .]

- Let Λ be any R -order, where R is a d.v.r. Does the K-S-A Theorem for Λ -lattices imply the K-S-A Theorem for f.g. Λ -modules?
- Let K be a global field, D a skewfield with index m and center C , where $\dim_K C < \infty$. Let D be expressed as a cyclic algebra $(L/C, \sigma, a)$, where L/C is a Galois extension with cyclic Galois group $\langle \sigma \rangle$ of order m , and where $a \in C^\times$ (here, $C^\times = C - \{0\}$). Let \hat{K} be the completion of K at some prime P of K . Show that $\hat{K} \otimes_K D$ is a skewfield if and only if the following two conditions hold:

(i) The P -adic valuation on K extends uniquely to a P' -adic valuation on L ,

(ii) If \hat{L} denotes the P' -adic completion of L , then m is the least positive integer t such that $a^t \in N_{\hat{L}/\hat{C}}(\hat{L}^\times)$, where N denotes the norm map.

[Hint: Use the results in MO §30. We have

$$\hat{K} \otimes_K D \cong (\hat{K} \otimes_K C) \otimes_C D,$$

so if $\hat{K} \otimes_K D$ is to be a skewfield, we must have $\hat{K} \otimes_K C = \hat{C} = \text{field}$. Further,

$$\hat{C} \otimes_C (L/C, \sigma, a) \sim (\hat{L}/\hat{C}, \sigma^k, a),$$

where \sim means equality in the Brauer group over \hat{C} . Here, $\langle \sigma^k \rangle = \text{Gal}(\hat{L}/\hat{C})$, where \hat{L} is some completion of L containing \hat{C} . If $\hat{C} \otimes_C D$ is to be a skewfield, we must have $k=1$, that is, $\dim_{\hat{C}} \hat{L} = \dim_C L$, and also condition (ii) must be satisfied.]

- Let Λ be a maximal R -order in a separable K -algebra, where R is a d.v.r. Show that the K-S-A Theorem holds for Λ -lattices.

[Hint: Use Exercise 26.11.]

§37. BASS AND GORENSTEIN ORDERS

Throughout this section, let A be a f.d. separable K -algebra, and R a Dedekind domain with quotient field K . An R -order Λ in A is called a *Gorenstein order* if every Λ -exact sequence:

$$0 \rightarrow \Lambda \rightarrow M \rightarrow N \rightarrow 0,$$

in which M and N are Λ -lattices, is necessarily split over Λ . If Λ has the additional property that every R -order in A containing Λ is also a Gorenstein order, we call Λ a *Bass order*. It is easily verified that there are inclusions

$$\begin{aligned} \{\text{maximal orders}\} &\subseteq \{\text{hereditary orders}\} \\ &\subseteq \{\text{Bass orders}\} \subseteq \{\text{Gorenstein orders}\}. \end{aligned}$$

Examples show that each inclusion is proper, generally speaking. Bass orders are a fundamental tool in the Drozd-Roiter and Drozd-Kirichenko approaches to the characterization of orders of finite representation type (see §33).

We shall consider the following properties* of an R -order Λ :

P_1 : $\mu_\Lambda(I) \leq 2$ for every left ideal I of Λ .

P_2 : Λ is a Bass order.

P_3 : Every indecomposable Λ -lattice is isomorphic to an ideal of Λ .

The main results of this section are the implications

$$P_1 \Rightarrow P_2 \Rightarrow P_3.$$

In general, P_3 does not imply P_1 . For example, every hereditary order is a Bass order (see below). However, by Exercise 33.2, one can find an ideal I in a suitable hereditary order Λ , for which $\mu_\Lambda(I) > 2$. Even for commutative orders, P_3 need not imply P_1 . As an example, we may take $\Lambda = RG$ where G is cyclic of order 4 and $R = \hat{\mathbb{Z}}_2$. Then P_3 holds for Λ by §34C, but $\mu_\Lambda(4\Lambda') = 3$ where Λ' is the maximal R -order containing Λ .

The final major result of this section is the following theorem due to Bass, which was historically the starting point of the development of the material in this section:

Let Λ be a commutative noetherian integral domain such that every f.g. indecomposable torsionfree Λ -module is isomorphic to an ideal of Λ . Then $\mu_\Lambda(I) \leq 2$ for every ideal I of Λ , so P_1 is equivalent to P_3 in this case.

*As usual, $\mu_\Lambda(X)$ denotes the minimal number of generators of a f.g. Λ -module X .

Now let A be a f.d. separable K -algebra. Given a f.g. left A -module V , set $B = (\text{End}_A V)^\circ$ and view V as (A, B) -bimodule. Set

$$V^* = \text{Hom}_K(V, K) = (B, A)\text{-bimodule},$$

the *dual* of V . Since A is a separable K -algebra, it is also a Frobenius algebra over K by (9.8), so $(A_A)^* \cong {}_A A$. Thus

$$(37.1) \quad V^* \cong \text{Hom}_K(A \otimes_A V, K) \cong \text{Hom}_A(V, \text{Hom}_K(A_A, K)) \cong \text{Hom}_A(V, A)$$

as (B, A) -bimodules, using the Adjointness Theorem 2.19.

Now let V be a faithful left A -module; then V is a progenerator for ${}_A \mathfrak{M}$ (and also for \mathfrak{M}_B), and there are bimodule isomorphisms

$$(37.2) \quad V^* \otimes_A V \cong B, \quad V \otimes_B V^* \cong A,$$

by virtue of (37.1) and §3D.

Assuming still that V is faithful, let M be a full R -lattice in V , and define its *left order* $O_l(M)$ and *right order* $O_r(M)$ by

$$O_l(M) = \{x \in A : xM \subseteq M\}, \quad O_r(M) = \{y \in B : My \subseteq M\}.$$

Then $O_l(M)$ is an R -order in A , and $O_r(M)$ in B . These definitions generalize those given in §24. Suppose further that N is a full R -lattice in V^* , so $O_l(N)$ is an R -order in B , and $O_r(N)$ in A . If we set

$$\Lambda = O_r(N) \cap O_l(M) \subseteq A, \quad \Gamma = O_l(N) \cap O_r(M) \subseteq B,$$

then Λ and Γ are orders in A and B , respectively. There are well-defined bimodule homomorphisms

$$(37.3) \quad N \otimes_{\Lambda} M \rightarrow B, \quad M \otimes_{\Gamma} N \rightarrow A,$$

consistent with the maps given in (37.2). We claim that there are bimodule isomorphisms

$$(37.4) \quad (N \otimes_{\Lambda} M)^* \cong \text{Hom}_{\Lambda}(N, M^*), \quad (M \otimes_{\Gamma} N)^* \cong \text{Hom}_{\Gamma}(M, N^*),$$

where $M^* = \text{Hom}_R(M, R)$ is the *dual* of M . Indeed, we have

$$\begin{aligned} (N \otimes_{\Lambda} M)^* &= \text{Hom}_R(N \otimes_{\Lambda} M, R) \\ &\cong \text{Hom}_{\Lambda}(N, \text{Hom}_R(M, R)) = \text{Hom}_{\Lambda}(N, M^*), \end{aligned}$$

and likewise for the other isomorphism in (37.4).

We caution the reader that the maps in (37.3) need not be monomorphisms (see Exercise 23.8), but their kernels are R -torsion modules, since

$K \otimes_R (N \otimes_{\Lambda} M) \cong KN \otimes_A KM \cong B$. Let NM denote the image of $N \otimes M$ in B , so the kernel of the map $N \otimes M \rightarrow NM$ is an R -torsion module. We then have

$$(N \otimes M)^* = \text{Hom}_R(N \otimes M, R) = \text{Hom}_R(NM, R) = (NM)^*,$$

so (37.4) yields

$$(37.5) \quad (NM)^* \cong \text{Hom}_{\Lambda}(N, M^*), \quad (MN)^* \cong \text{Hom}_{\Gamma}(M, N^*).$$

We note that all of the isomorphisms occurring above are natural ones.

Now let Λ be any R -order in A , and let M be a left Λ -lattice; its dual M^* is then a right Λ -lattice, and we have $M \cong M^{**}$ as left Λ -lattices (see (10.26)), the isomorphism being natural. Each exact sequence of Λ -lattices

$$(37.6) \quad 0 \rightarrow L \rightarrow M \rightarrow N \rightarrow 0$$

is R -split, hence yields a new exact sequence

$$(37.7) \quad 0 \rightarrow N^* \rightarrow M^* \rightarrow L^* \rightarrow 0$$

when we apply $\text{Hom}_R(\cdot, R)$. Conversely, this second sequence of right Λ -lattices dualizes to give the original sequence. It follows that the first sequence is Λ -split if and only if the second sequence is Λ -split.

We call a left Λ -lattice L *weakly injective* if every exact sequence (37.6) of left Λ -lattices is split over Λ . Then L is weakly injective if and only if its dual L^* is a projective right Λ -lattice. Equivalently, L is weakly injective if and only if $\text{Ext}_{\Lambda}^1(N, L) = 0$ for every left Λ -lattice N . It is obvious that weak injectivity is a local property, that is, L is weakly injective if and only if each localization L_P (or completion \hat{L}_P) is weakly injective, where P ranges over the maximal ideals of R .

If Λ is a hereditary order, then every Λ -lattice is projective, and consequently every Λ -lattice is weakly injective.

An arbitrary order Λ is called *weakly self-injective* if ${}_{\Lambda}\Lambda$ is weakly injective; such orders are also called (left) *Gorenstein orders*. Thus, Λ is left Gorenstein if and only if each exact sequence of Λ -lattices $0 \rightarrow \Lambda \rightarrow M \rightarrow N \rightarrow 0$ is necessarily split over Λ , or equivalently, if and only if $({}_{\Lambda}\Lambda)^*$ is projective as right Λ -lattice. By (3.51), this latter condition holds if and only if the map

$$\Lambda \otimes_{\Lambda} \text{Hom}(\Lambda^*, \Lambda) \rightarrow \text{End}_{\Lambda}(\Lambda^*)$$

is surjective. It follows at once that the property of being a Gorenstein order is a local property.

It is obvious that every hereditary order is a Gorenstein order. Our next step is to remove the asymmetry in our definition of Gorenstein orders:

(37.8) Proposition. *An R -order Λ is left Gorenstein if and only if it is right Gorenstein.*

Proof. It suffices to treat the case where R is a complete d.v.r. Assume Λ is left Gorenstein, so $(\Lambda\Lambda)^*$ is projective. Let $\{e_i\}_{i=1}^n$ be a basic set of primitive idempotents in Λ ; then by §6 there are precisely n non-isomorphic indecomposable projective left Λ -lattices $\{\Lambda e_i\}$ and right Λ -lattices $\{e_i \Lambda\}$. Since $(\Lambda\Lambda)^*$ is a direct sum of copies of some of the $\{e_i \Lambda\}$, it follows that $\Lambda\Lambda$ is a sum of their duals $\{(e_i \Lambda)^*\}$. Thus the modules $\{(e_i \Lambda)^*: 1 \leq i \leq n\}$ are a permutation of the modules $\{\Lambda e_i: 1 \leq i \leq n\}$. But then $(\Lambda\Lambda)^*$ is a sum of modules $\{(e_i \Lambda)^*\}$, and is therefore projective as left Λ -lattice. Therefore Λ is right Gorenstein, as desired.

From now on, we omit the adjectives “left” and “right” in referring to Gorenstein orders. Let us give some examples of Gorenstein orders:

(i) If G is a finite group, its integral group ring RG is a Gorenstein order by (10.29).

(ii) Every hereditary order is Gorenstein.

(iii) Let R be a complete d.v.r. with maximal ideal P , and let

$$\Lambda = \begin{pmatrix} R & R \\ P^2 & R \end{pmatrix} = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a, b, d \in R, c \in P^2 \right\}.$$

Let $e_1 = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$, $e_2 = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$, so

$$\Lambda e_1 = \begin{pmatrix} R \\ P^2 \end{pmatrix}, \quad \Lambda e_2 = \begin{pmatrix} R \\ R \end{pmatrix}.$$

Then

$$(\Lambda e_1)^* = \text{Hom}_R(\Lambda e_1, R) \cong (R \quad P^{-2})$$

as right Λ -modules, with the isomorphism arising from the formula

$$(R \quad P^{-2}) \begin{pmatrix} R \\ P^2 \end{pmatrix} = R.$$

But $(R \quad P^{-2}) \cong (P^2 \quad R) \cong e_2 \Lambda$, so $(\Lambda e_1)^*$ is right Λ -projective. Likewise so is $(\Lambda e_2)^*$, and Λ is a Gorenstein order.

As a consequence of the proof of (37.8), we have

(37.9) Corollary. *An R -order Λ is Gorenstein if and only if $(\Lambda\Lambda)^*$ is a generator for the category ${}_{\Lambda}\mathcal{M}$.*

Proof. It suffices to prove the result when R is a complete d.v.r. If Λ is Gorenstein, we have just shown that the $\{(e_i \Lambda)^*\}$ are a rearrangement of the

$\{\Lambda e_i\}$, using the notation of the proof of (37.8). But then each Λe_i is a summand of $(\Lambda_\Lambda)^*$, so $(\Lambda_\Lambda)^*$ is a generator for ${}_\Lambda \mathfrak{M}$. The argument works equally well in reverse: if $(\Lambda_\Lambda)^*$ is a generator, then each Λe_i is a summand of $(\Lambda_\Lambda)^*$, so the $\{\Lambda e_i\}$ are a permutation of the $\{(e_i \Lambda)^*\}$. Hence each $(\Lambda e_i)^*$ is projective, and therefore so is $(\Lambda_\Lambda)^*$.

By (3.49), the condition that $(\Lambda_\Lambda)^*$ be a generator for ${}_\Lambda \mathfrak{M}$ can be restated as follows: if $L = (\Lambda_\Lambda)^*$, the map

$$L \otimes_{\Gamma} \text{Hom}_{\Lambda}(L, \Lambda) \rightarrow \Lambda$$

should be surjective, where $\Gamma = \text{End}_{\Lambda}(L)$. This leads us to the concept introduced by Roiter [63], [65], of one module “covering” another.

For the moment, let Λ be any left noetherian ring, and let us restrict our attention to f.g. left Λ -modules. For two such modules L and M , we introduce the notation

$$(37.9a) \quad L \cdot \text{Hom}_{\Lambda}(L, M) = \sum_f f(L),$$

where f ranges over all elements of $\text{Hom}_{\Lambda}(L, M)$. Then $L \cdot \text{Hom}_{\Lambda}(L, M)$ is a left Λ -submodule of M . We shall say that L covers M , and write $L > M$, if $L \cdot \text{Hom}_{\Lambda}(L, M) = M$. (Roiter uses the term “divides” rather than “covers”, and writes $L | M$. This notation conflicts with our standard notation $X | Y$ indicating that X is a direct summand of Y , so we shall not use Roiter’s terminology here.)

(37.10) Lemma. (i) L covers every direct summand of each homomorphic image of L .

(ii) $>$ is transitive.

(iii) $\Lambda > M$ for all (f.g.) M .

(iv) For f.g. left Λ -modules L and M , where Λ is left noetherian, $L > M$ if and only if there is a surjection $L^{(n)} \rightarrow M$ for some n .

Proof. (i) and (ii) are clear. For (iv), let $\varphi: L^{(n)} \rightarrow M$ be a surjection, and let f_i be the restriction of φ to the i -th summand. Then $\sum_k f_i(L) = M$, so $L > M$. Conversely, if $L > M$, and $M = \sum_{i=1}^k \Lambda m_i$, choose $f_i \in \text{Hom}_{\Lambda}(L, M)$ with $m_i \in f_i(L)$, $1 \leq i \leq k$; then there is a surjection $\coprod f_i: L^{(k)} \rightarrow M$. Finally, (iv) implies (iii).

We remark also that the property of one module covering another is a local property. Further, (37.9) gives:

(37.11). Λ is a Gorenstein R-order if and only if $(\Lambda_\Lambda)^* \succ_\Lambda \Lambda$.

The following useful result is due to Faddeev [65a]:

(37.12) **Proposition.** Let Λ be an R-order, and let M be a faithful left Λ -lattice, where $\Lambda = O_I(M)$. Then $M^* \succ \Lambda^*$ as right Λ -lattices, and $M \succ \Lambda^*$ as left Λ -lattices.

Proof. Set $V = KM$, $A = K\Lambda$, so V is a faithful left A -module and $\Lambda = \{x \in A : xM \subseteq M\}$. Put $\Delta = (\text{End}_\Lambda M)^\circ$, so by (37.4) there is a two-sided Λ -isomorphism

$$M \otimes_\Delta M^* \cong \{\text{Hom}_\Delta(M, M)\}^*.$$

But $\text{Hom}_\Delta(M, M) = \{x \in A : xM \subseteq M\} = \Lambda$, so $M \otimes M^* \cong \Lambda^*$. If $M = \sum_{i=1}^n m_i \Delta$, then we obtain a right Δ -surjection $M^{*(n)} \rightarrow \Lambda^*$, so $M^* \succ \Lambda^*$ as claimed. A similar argument proves that $M \succ \Lambda^*$.

As an application of this proposition, we obtain:

(37.13) **Theorem.** Let Λ be a Gorenstein R-order, where R is a complete d.v.r. Then every nonprojective indecomposable left Λ -lattice M is a lattice relative to some strictly larger R-order in $K\Lambda$.

Proof. Suppose first that M is a faithful indecomposable Λ -lattice which is not a lattice relative to any larger order in $K\Lambda$. Then $\Lambda = O_I(M)$, so by (37.12) we have $M \succ \Lambda^*$ as left Λ -lattices. But $\Lambda^* \succ \Lambda$ since Λ is a Gorenstein order, and therefore we deduce that $M \succ \Lambda$. But then $\Lambda \mid M^{(k)}$ for some k , and so $\Lambda \cong M^{(l)}$ for some l , since M is indecomposable. However, this gives $M \mid \Lambda$, so M is projective.

Now let M be any nonprojective indecomposable Λ -lattice, not necessarily faithful. We may write $\text{ann}_A KM = Ae$, with $e \in A$ a central idempotent. Then $M = (1-e)M$, and M is a faithful $(1-e)\Lambda$ -lattice. Obviously M is indecomposable and nonprojective as $(1-e)\Lambda$ -lattice, and $(1-e)\Lambda$ is also a Gorenstein order. By the first part of the proof, M is then a left Γ -lattice for some R-order Γ in $(1-e)A$ properly containing $(1-e)\Lambda$. But then M is a $(e\Lambda \oplus \Gamma)$ -lattice, and $e\Lambda \oplus \Gamma$ is an R-order in A properly containing Λ . This completes the proof.

The preceding theorem begins to suggest the importance of Gorenstein orders. If Λ is a Gorenstein order over a complete d.v.r. R , then the indecomposable Λ -lattices consist of the indecomposable projectives, together with the indecomposable Λ' -lattices, where Λ' ranges over orders properly containing Λ . Usually, the larger the order, the easier it is to describe lattices relative to it.

We have already pointed out that every hereditary order Λ is a Gorenstein order. Further, if Λ is a hereditary order in A , then so is every larger order Λ' in A . Indeed, every Λ' -lattice is also a Λ -lattice. Therefore, every short exact sequence of Λ' -lattices is Λ -split, and hence also Λ' -split by Exercise 23.2. In the following discussion, a special role is played by those Gorenstein orders for which every larger order is also a Gorenstein order. These orders are called *Bass orders*, since their basic properties were first studied by Bass [62, 63] in the commutative case. As we mentioned in the introduction, there are inclusions

$$\begin{aligned} \{\text{maximal orders}\} &\subseteq \{\text{hereditary orders}\} \\ &\subseteq \{\text{Bass orders}\} \subseteq \{\text{Gorenstein orders}\}, \end{aligned}$$

and examples show each inclusion is proper.

Our first aim is to establish the implication $P_2 \Rightarrow P_3$, that is, every indecomposable lattice over a Bass order Λ is isomorphic to an ideal of Λ . We begin with an easy result:

(37.14) Lemma. *Let Λ be an R -order in A . Then Λ is a Bass order if and only if for all left Λ -lattices L and M ,*

$$L \succ M \text{ implies } L^* \succ M^*.$$

Proof. Suppose the condition satisfied, and let $\Lambda \subseteq \Gamma \subseteq A$, where Γ is an R -order. Then $\Gamma \succ \Gamma^*$ as Γ -lattices, hence also as Λ -lattices. But then $\Gamma^* \succ \Gamma$, so Γ is Gorenstein.

For the converse, it suffices to treat the case where R is a complete d.v.r., since the property of being a Bass order is a local property, as is the property of covering. Thus let Λ be a Bass order, and let $L \succ M$, that is, $L \cdot \text{Hom}_\Lambda(L, M) = M$. Write $\text{ann}_A KL = Ae$, where e is either a central idempotent of A or else $e=0$. Then KL is a faithful $(1-e)A$ -module, and we put

$$\Gamma = O_r(L) = \{a \in (1-e)A : aL \subseteq L\},$$

an R -order in $(1-e)A$. Then $\Lambda \subseteq (1-e)\Lambda \oplus e\Lambda \subseteq \Gamma \oplus e\Lambda$, and $\Gamma \oplus e\Lambda$ is an R -order in A . Since Λ is a Bass order, this means that $\Gamma \oplus e\Lambda$ is a Gorenstein order, whence so is Γ . But then by (37.11) and (37.12), $L^* \succ \Gamma^* \succ \Gamma$. But M is a Γ -module, since $M = L \cdot \text{Hom}_\Lambda(L, M)$ and L is a Γ -module (see Exercise 37.10). Then M^* is also a Γ -module, so $\Gamma \succ M^*$. Therefore $L^* \succ M^*$, which completes the proof.

We intend to prove that every indecomposable lattice over a Bass order Λ is isomorphic to an ideal of Λ . Unfortunately, this is not a local property, so we must in fact prove a slightly stronger property which is local. Some

additional notation is required: let $\{S_1, \dots, S_r\}$ be a basic set of simple left A -modules. For any left Λ -lattice M , its *signature* is defined by

$$\text{sig } M = \{m_1, \dots, m_r\}, \text{ where } KM \cong \coprod S_i^{(m_i)}.$$

Put

$$\text{sig } \Lambda = \{a_1, \dots, a_r\}, \text{ where } A \cong \coprod S_i^{(a_i)}.$$

Now let

$$(37.15) \quad I(M) = \coprod S_i^{\min(m_i, a_i)},$$

so $I(M)$ is a left ideal of A which depends only on KM , and is nonzero if $M \neq 0$. It is easily verified (Exercise 37.6) that for each P , $I(\hat{M}_P)$ is the P -adic completion of $I(M)$.

We are now ready to prove the fundamental result due to Drozd-Kirichenko-Roiter [67], generalizing earlier work of Bass [63]:

(37.16) Theorem. *Let Λ be a Bass R -order in a separable K -algebra A , and let M be any left Λ -lattice. Then there is a Λ -decomposition $M = M_0 \oplus M'$, where $KM_0 = I(M)$. Thus, M_0 is isomorphic to a left ideal of Λ .*

Proof. Step 1. We show first that the existence of such a decomposition of M is a local property. Let P range over the maximal ideals of R , and suppose that for each P we have

$$\hat{M}_P = L(P) \oplus N(P), \text{ where } \hat{K}_P \cdot L(P) = I(\hat{M}_P).$$

Since $I(\hat{M}_P)$ is the completion of $I(M)$, it follows from (4.21) and (23.14) that there exists a left Λ -lattice L such that $\hat{L}_P \cong L(P)$ for each P at which $\hat{\Lambda}_P$ is not a maximal order. By (31.12) there exists a Λ -lattice M_0 in the genus of L , such that $M_0 | M$. Clearly $KM_0 = I(M)$, since this holds at some P .

Step 2. By virtue of Step 1, we may assume from now on that R is a complete d.v.r., and attempt to prove the theorem for this case. Let L and M be left Λ -lattices; we call L “ M -injective” if given any diagram

$$\begin{array}{ccccc} 0 & \longrightarrow & M_1 & \longrightarrow & M \\ & & f \downarrow & & \\ & & L & & \end{array}$$

in which M_1 is a sublattice of M such that M/M_1 is also a lattice, there exists a homomorphism $g: M \rightarrow L$ extending f . Thus, for example, every weakly

injective Λ -lattice is M -injective for all M (see Exercise 37.1). We establish the following lemma, which is the key step in our induction argument:

Lemma. *Let Λ be a Bass R-order, where R is complete. Let L and M be left Λ -lattices such that $\text{Hom}_\Lambda(M, L) \neq 0$, and suppose that L is $M^{(k)}$ -injective for each k . Set $\text{sig } M = \{m_i\}$, $\text{sig } L = \{l_i\}$. Define* $Q = M \cdot \text{Hom}_\Lambda(M, L)$, a Λ -sublattice of L with signature $\{q_i\}$, where*

$$q_i = \begin{cases} l_i & \text{if } m_i \neq 0, \\ 0 & \text{if } m_i = 0. \end{cases}$$

Then there exist Λ -decompositions

$$M = I \oplus M_1, Q = I \oplus L_1,$$

where $I \neq 0$ and where L_1 is $M_1^{(k)}$ -injective for each k .

Proof. We note first that $Q \neq 0$ because $\text{Hom}_\Lambda(M, L) \neq 0$. The formula for $\text{sig } Q$ follows at once from the equality $KQ = KM \cdot \text{Hom}_\Lambda(KM, KL)$. Next, the hint in Exercise 37.2 shows that Q is $M^{(k)}$ -injective for each k . By definition of Q we have $M > Q$, so $M^* > Q^*$ by (37.14). By (37.10), there exists an exact sequence of right Λ -lattices

$$0 \rightarrow T \rightarrow M^{*(k)} \rightarrow Q^* \rightarrow 0$$

for some k . Taking duals, we obtain an exact sequence of left Λ -lattices

$$0 \rightarrow Q \xrightarrow{f} M^{(k)} \rightarrow T^* \rightarrow 0.$$

But since Q is $M^{(k)}$ -injective, the identity map on Q extends to a map $g: M^{(k)} \rightarrow Q$, so g splits f , and therefore $Q | M^{(k)}$. Therefore Q and M have a common nonzero summand I , so we may write $M = I \oplus M_1$, $Q = I \oplus L_1$ for some Λ -lattices M_1 and L_1 . Finally, by Exercise 37.3, L_1 is $M_1^{(k)}$ -injective for all k , which completes the proof of the lemma.

Step 3. We are now ready to prove the theorem. Given a (nonzero) left Λ -lattice M , put $Q = M \cdot \text{Hom}_\Lambda(M, \Lambda^*)$. Since Λ^* is weakly injective because Λ is a Bass order, it follows from Step 2 that there exist decompositions

$$M = I_1 \oplus M_1, Q = I_1 \oplus Q_1,$$

where $I_1 \neq 0$, Q_1 is $M_1^{(k)}$ -injective for each k , and $\text{sig } Q = \{q_i\}$, where

$$q_i = \begin{cases} a_i & \text{if } m_i \neq 0, \\ 0 & \text{if } m_i = 0. \end{cases}$$

*See (37.9a).

If $\text{sig } I_1 = \{\beta_i\}$, then

$$\text{sig } M_1 = \{m_i - \beta_i\}, \text{sig } Q_1 = \{q_i - \beta_i\}.$$

We now repeat the procedure with the pair M_1, Q_1 in place of M, Λ^* . Specifically, we set

$$Q'_1 = M_1 \cdot \text{Hom}_\Lambda(M_1, Q_1).$$

By Step 2, M_1 and Q'_1 have a common direct summand. If $Q'_1 = 0$, then KM_1 and KQ_1 have no common simple A -modules, so for each i we have:

$$\text{either } m_i - \beta_i = 0 \text{ and } q_i - \beta_i \geq 0, \text{ or } m_i - \beta_i \geq 0 \text{ and } q_i - \beta_i = 0.$$

In this case we find at once that $\beta_i = \min(a_i, m_i)$, and the decomposition $M = I_1 \oplus M_1$ is the desired one, since $KI_1 = I(M)$.

On the other hand, if $Q'_1 \neq 0$ then there is a decomposition

$$M_1 = I_2 \oplus M_2, Q'_1 = I_2 \oplus Q_2,$$

where $I_2 \neq 0$, Q_2 is $M_2^{(k)}$ -injective for each k , and

$$(\text{sig } Q'_1)_i = \begin{cases} q_i - \beta_i & \text{if } m_i - \beta_i \neq 0, \\ 0 & \text{if } m_i - \beta_i = 0. \end{cases}$$

Let $\text{sig } I_2 = \{\gamma_i\}$, so

$$\text{sig } M_2 = \{m_i - \beta_i - \gamma_i\}, \text{sig } Q_2 = \{q_i - \beta_i - \gamma_i\}.$$

We set $Q'_2 = M_2 \cdot \text{Hom}_\Lambda(M_2, Q_2)$. If $Q'_2 = 0$, then KM_2 and KQ_2 have no common simple A -module, so for each i we have:

$$\begin{aligned} &\text{either } m_i - \beta_i - \gamma_i = 0 \text{ and } q_i - \beta_i - \gamma_i \geq 0, \\ &\text{or } m_i - \beta_i - \gamma_i \geq 0 \text{ and } q_i - \beta_i - \gamma_i = 0. \end{aligned}$$

As above, we find that $\beta_i + \gamma_i = \min(a_i, m_i)$ for each i . Then $M = (I_1 \oplus I_2) \oplus M_2$ gives the desired decomposition, since $K(I_1 \oplus I_2) = I(M)$. On the other hand, if $Q'_2 \neq 0$ we can further decompose the modules involved:

$$M_2 = I_3 \oplus M_3, Q'_2 = I_3 \oplus Q_3,$$

and so on. This process must eventually terminate, and gives the desired decomposition $M = M_0 \oplus M'$ with $KM_0 = I(M)$. The theorem is thus established.

We next prove our second major result: $P_1 \Rightarrow P_2$. This is due to Roiter [66b], generalizing earlier work by Bass.

(37.17) Theorem. *Let Λ be an R -order such that $\mu_\Lambda(I) \leq 2$ for each left ideal I of Λ . Then Λ is a Bass order.*

Proof. Let P be a maximal ideal of R , and J any left ideal of $\hat{\Lambda}_P$. As in the first part of the proof of (33.2), J is a direct summand of the completion \hat{I}_P of some left ideal I of Λ . Since $\mu_\Lambda(I) \leq 2$, it follows that $\mu_{\hat{\Lambda}_P}(J) \leq 2$. We shall deduce from this that each $\hat{\Lambda}_P$ is a Bass order, whence so is Λ . For the rest of the proof, we may therefore take R to be a complete d.v.r.

The hypotheses imply that* $\mu_\Lambda(\Lambda') \leq 2$ for each R -order Λ' in A containing Λ . We shall deduce from this that $\Lambda^* \cong \Lambda$, so Λ is a Gorenstein order. But then for any order Γ containing Λ , we have $\mu_\Gamma(\Lambda') \leq \mu_\Lambda(\Lambda') \leq 2$ if $\Gamma \subseteq \Lambda'$, so $\Gamma^* \cong \Gamma$ and Γ is also Gorenstein. This implies that Λ is a Bass order, as desired.

So assume that $\mu_\Lambda(\Lambda') \leq 2$, and let $N = \text{rad } \Lambda$. Then Λ/N is a semisimple artinian ring, so we can find a collection of maximal two-sided ideals $\{W_1, \dots, W_r\}$ of Λ such that the factor rings Λ/W_i are precisely the Wedderburn components of Λ/N . Let U_i denote a simple right (Λ/W_i) -module. We have

$$\Lambda/N = \bigoplus \Lambda/W_i.$$

Now Λ^* is a two-sided Λ -module; let $\mu_I(\Lambda^*)$ be the minimal number of generators of Λ^* as left Λ -module, and define $\mu_r(\Lambda^*)$ analogously. Then

$$\mu_I(\Lambda^*) = \mu_I(\Lambda^*/N\Lambda^*) = \max_i \mu_I(\Lambda^*/W_i\Lambda^*).$$

Further, for each (Λ/W_i) -module X , the number of generators of X is completely determined by its composition length (see Exercise 33.3). By Exercise 37.11, it follows that

$$\mu_I(\Lambda^*/W_i\Lambda^*) = \mu_r((W_i\Lambda^*)^*/\Lambda).$$

However, (37.5) gives

$$(W_i\Lambda^*)^* = \text{Hom}_\Lambda(W_i, \Lambda) = \{x \in A : xW_i \subseteq \Lambda\} = T_i \text{ (say)}.$$

(We write equality rather than isomorphism, taking account of the canonical identification of A^{**} with A .) Thus

$$\mu_I(\Lambda^*) = \max_i \mu_r(T_i/\Lambda),$$

so we need only show that the right Λ -module T_i/Λ is cyclic for each i .

*Since $a\Lambda' \subseteq \Lambda$ for some nonzero $a \in R$, Λ' is isomorphic (as Λ -module) to a left ideal of Λ .

Let i be fixed, and suppose that T_i/Λ is not a cyclic right Λ -module. We show that in this case we have

$$T_i = O_i(W_i) = \{x \in A : xW_i \subseteq W_i\},$$

and for this it suffices to prove that $T_iW_i \subseteq W_i$. Now T_i/Λ is a right (Λ/W_i) -module, and Λ/W_i is a simple artinian ring with simple right module U_i . Thus T_i/Λ is a direct sum of copies of U_i , and so there exists a finite collection $\{V_\alpha\}$ of submodules of T_i such that

$$V_\alpha \supseteq \Lambda, V_\alpha/\Lambda \cong U_i \text{ for each } \alpha, \text{ and } T_i = \sum_{\alpha} V_\alpha.$$

To prove that $T_iW_i \subseteq W_i$, we need only show that $VW_i = W_i$, where V is any V_α . Surely $VW_i \supseteq W_i$, since $V \supseteq \Lambda$, so suppose that $VW_i \supsetneq W_i$. Let $l(\)$ denote Λ -composition length. Then

$$l(V/VW_i) \leq l(\Lambda/W_i),$$

since $VW_i \supsetneq W_i$ and $l(V/\Lambda) = 1$. On the other hand, if $j \neq i$ then $W_i + W_j = \Lambda$, and since $(V/\Lambda)W_i = 0$ we have $VW_i \subseteq \Lambda$, so

$$V = V(W_i + W_j) = \Lambda + VW_j,$$

whence

$$V/VW_j = (\Lambda + VW_j)/VW_j \cong \Lambda / (\Lambda \cap VW_j).$$

But $\Lambda \cap VW_j \supseteq W_j$, whence

$$l(V/VW_j) \leq l(\Lambda/W_j) \text{ for } j \neq i.$$

Therefore V/VW_j is a cyclic (Λ/W_j) -module for every j , including $j=i$. Therefore

$$\mu(V) = \max_j \mu(V/VW_j) = 1,$$

so V itself is a cyclic right Λ -module. Since V and Λ are full R -lattices in A , it follows that $V \cong \Lambda$. Letting $\Lambda/W_i \cong U_i^{(n)}$, we obtain Λ -exact sequences

$$0 \rightarrow W_i \rightarrow \Lambda \rightarrow U_i^{(n)} \rightarrow 0, \quad 0 \rightarrow \Lambda^{(n)} \rightarrow V^{(n)} \rightarrow U_i^{(n)} \rightarrow 0.$$

Thus $\Lambda \oplus V^{(n)} \cong \Lambda^{(n)} \oplus W_i$ by Schanuel's Lemma, whence $W_i \cong \Lambda$. We may write $W_i = y\Lambda$ for some invertible $y \in A$, and then $T_i = \Lambda y^{-1}$. From $T_i \Lambda = T_i$ we obtain $y^{-1}\Lambda = \Lambda y^{-1}$, so T_i is a cyclic right Λ -module, whence so is T_i/Λ , contrary to our assumption. This completes the proof that $T_i = O_i(W_i)$.

Continuing with the argument, we have $\mu_\Lambda(T_i) \leq 2$ since T_i is an R -order containing Λ . Therefore $l(T_i/T_iW_i) \leq 2n$, with n as above (see Exercise 33.3). But $T_iW_i = W_i$, so we have

$$l(T_i/\Lambda) + l(\Lambda/W_i) = l(T_i/W_i) = l(T_i/T_iW_i) \leq 2n,$$

whence $l(T_i/\Lambda) \leq n$. Therefore T_i/Λ is a cyclic (Λ/W_i) -module, hence also a cyclic Λ -module. This is again a contradiction, and completes the proof of the theorem.

We now prove Bass' Theorem that $P_3 \Rightarrow P_1$ under suitable circumstances:

(37.18) Theorem. *Let Λ be a commutative noetherian integral domain such that every indecomposable f.g. torsionfree Λ -module is isomorphic to an ideal of Λ . Then $\mu_\Lambda(I) \leq 2$ for every ideal I of Λ .*

Proof. Step 1. Throughout this proof, all Λ -modules considered are assumed f.g./ Λ . The rank of a torsionfree Λ -module X is (by definition) $\dim_K(K \otimes_\Lambda X)$, where K is the quotient field of Λ . Let \mathfrak{m} be any maximal ideal of Λ . Each torsionfree indecomposable $\Lambda_{\mathfrak{m}}$ -module is the localization of some torsionfree indecomposable Λ -module, and hence is an ideal of $\Lambda_{\mathfrak{m}}$. Thus $\Lambda_{\mathfrak{m}}$ has the same property as Λ , and we shall show that $\mu_{\Lambda_{\mathfrak{m}}}(I) \leq 2$ for each ideal I of $\Lambda_{\mathfrak{m}}$.

Changing notation for the moment, let Λ be a local domain with maximal ideal \mathfrak{m} , and suppose that every indecomposable torsionfree Λ -module is isomorphic to an ideal of Λ . Now suppose that there is an ideal I of Λ such that $\mu_\Lambda(I) = n \geq 3$, and let $F = \Lambda^{(n)}$ be free. Let $I = \sum_{i=1}^n \Lambda x_i$, and let $F \rightarrow I$ be the surjection given by $(a_1, \dots, a_n) \in F \rightarrow \sum a_i x_i \in I$. If $\xi = (x_1, \dots, x_n) \in F$, then I is generated by the images of the coordinates of ξ . This also holds if ξ is replaced by ξP , with $P \in GL_n(\Lambda)$. Now ξ cannot lie in any proper direct summand of F ; for any such summand would be projective, hence free, and so relative to some suitable new basis, ξ would be represented by an n -tuple ξ' with at least one zero entry. This would contradict the assumption that $\mu_\Lambda(I) = n$, because the images of the entries of ξ' generate I .

We now form the Λ -module $L = F \cap K\xi$, so F/L is a torsionfree Λ -module. From the exact sequence

$$0 \rightarrow L \rightarrow F \rightarrow M \rightarrow 0, \quad M = F/L,$$

we see that M has rank $n-1$, so M must decompose nontrivially. Suppose that $M = M_1 \oplus M_2$, where M_1, M_2 are nonzero. We have

$$\text{rank } M_1 + \text{rank } M_2 = \text{rank } M = n-1, \quad \mu(M_1) + \mu(M_2) = \mu(M) \leq n,$$

the latter because Λ is local (and thus μ is additive!). But $\text{rank } X \leq \mu(X)$ for

all Λ -modules X , with equality if and only if X is free. Now M cannot be free, since otherwise ξ lies in the direct summand L of F . Thus $\mu(M)=n$, and consequently $\text{rank } M_i = \mu(M_i)$ for exactly one i , say $i=1$. But then M_1 is Λ -free, and we obtain a surjection $\varphi: F \rightarrow M_1$ by composition of maps $F \rightarrow M \rightarrow M_1$. Since $\xi \in \ker \varphi$, we obtain a contradiction, which completes the proof that when Λ is local, $\mu_\Lambda(I) \leq 2$ for each ideal I of Λ .

Step 2. We now return to our original domain Λ . We may suppose that

$$(*) \quad \mu_{\Lambda_m}(I_m) \leq 2 \text{ for every ideal } I_m \text{ of } \Lambda_m, \text{ for every maximal ideal } m \text{ of } \Lambda.$$

We must show that $(*)$ implies $\mu_\Lambda(I) \leq 2$ for every ideal I of Λ . The key step in this proof is the fact that as a consequence of $(*)$, each nonzero ideal I of Λ is contained in only a finite number of maximal ideals of Λ . This follows from Cohen [50, Cor. 1 to Th. 10], and we shall omit the details of the proof. In the case where Λ is an R -order in some field, it is obvious that for nonzero I , the factor ring Λ/I is a f.g. R -torsion R -algebra, hence is semilocal and has finitely many maximal ideals. Thus, Cohen's Theorem is not needed for the case of orders.

Now let I be a nonzero ideal of Λ , and assume $(*)$ holds true. Let m_1, \dots, m_n be the distinct maximal ideals of Λ containing I . Using an obvious generalization of the Chinese Remainder Theorem, we can find an element $x \in I$ which is part of a minimal generating set for each I_{m_ν} , $1 \leq \nu \leq n$. Now let q_1, \dots, q_r be the maximal ideals of Λ which contain x . For each ρ , $1 \leq \rho \leq r$, we may choose an element $y_\rho \in I$ such that $\{x, y_\rho\}$ generate I_{q_ρ} as Λ_{q_ρ} -module. Indeed, if q_ρ is one of the m 's, such a choice is possible because of the way x was picked; on the other hand, if q_ρ is not one of the m 's, then $I_{q_\rho} = \Lambda_{q_\rho}$, so $y_\rho = 1$ will suffice. Now choose $y \in I$ so that $y \equiv y_\rho \pmod{q_\rho I}$, $1 \leq \rho \leq r$. It is then easily verified that $I = \Lambda x + \Lambda y$, so $\mu_\Lambda(I) \leq 2$ as desired. This completes the proof.

We discuss briefly some further results on these topics:

(a) (Borevich-Faddeev [65a, b]): Let A = commutative separable K -algebra, $\Lambda = R$ -order in A , Λ_0 = maximal R -order. Call Λ of *cyclic index* (in Λ_0) if $\Lambda_0 = \Lambda + \Lambda\omega$ for some ω . If Λ is of cyclic index, then:

(i) Every full Λ -lattice in A is invertible, or equivalently, locally free.

(ii) Every full Λ -lattice M in $A^{(s)}$ uniquely determines an ascending chain of R -orders in A : $\Lambda \subseteq \Lambda_1 \subseteq \cdots \subseteq \Lambda_s$, such that

$M \cong \coprod J_i$ as Λ -lattices, with J_i a full Λ -lattice in A such that $O_I(J_i) = \Lambda_i$.

(iii) The isomorphism invariants of M are the chain of orders $\{\Lambda_i\}$ and the ideal class of $\coprod J_i$ (as Λ_s -module). Further, we may choose $J_i = \Lambda_i$, $1 \leq i \leq s-1$, in the above.

(iv) Conversely, if every Λ -lattice is isomorphic to a direct sum of ideals of Λ , then Λ is an order of cyclic index.

(b) (Bass): Let Λ be an order in the *commutative* K -algebra A .

- (i) If A is a field, then $P_3 \Rightarrow P_1$. (Bass [62]).
- (ii) $P_2 \Rightarrow P_1$ always. (Bass [63, §7]).
- (iii) P_1 is a local property. (Bass [63, Lemma 7.4]).

(c) (Drozd-Kirichenko-Roiter [67]): Let $R = \text{complete d.v.r.}$, $A = D$ or $D_1 \oplus D_2$ or $M_2(D)$, where the D 's are f.d. division algebras over K . Let Λ be a local R -order in A . Then $P_3 \Rightarrow P_1$. Further, any local Bass order Λ must be an R -order in one of the algebras A of the type above.

(d) (Roiter [63a, b]): We give a brief discussion of normal decompositions of modules. By definition, a Λ -module L has a *normal decomposition* if $L = L_1 \oplus \cdots \oplus L_r$, $r > 1$, where the $\{L_i\}$ are nonzero submodules of L such that $L_i > L_j$ for $1 \leq i < j \leq r$. If no such decomposition exists, call L *normally indecomposable*.

The importance of this concept arises from its connection with the earlier concept of one module covering another. Let us establish:

(37.19) Proposition. *Let Λ be an R -order, where R is a complete d.v.r., and let L and M be left Λ -lattices such that $L > M$. Suppose that either L is normally indecomposable, or else that every idempotent in $\text{End}_\Lambda L$ is central. Then every Λ -surjection $M \rightarrow L$ is split.*

Proof. Let $\Gamma = \text{End}_\Lambda L$, acting from the left on L . Given a Λ -surjection $\varphi: M \rightarrow L$, put

$$T = \{\varphi\tau : \tau \in \text{Hom}_\Lambda(L, M)\} = \text{right ideal of } \Gamma.$$

Since $L > M$ and φ is surjective, we have $T \cdot L = L$. Now let

$$\bar{\Gamma} = \Gamma / \text{rad } \Gamma, \quad \bar{T} = (T + \text{rad } \Gamma) / \text{rad } \Gamma \subseteq \bar{\Gamma}.$$

Then \bar{T} is a right ideal of the semisimple ring $\bar{\Gamma}$. If $\bar{T} = 0$ then $T \subseteq \text{rad } \Gamma$, so $L = (\text{rad } \Gamma)L$, which is impossible by Nakayama's Lemma (we assume $L \neq 0$, of course). Thence $\bar{T} \neq 0$, so $\bar{T} = \bar{e}\bar{\Gamma}$ for some idempotent $e \in \Gamma$.

We now have $T \subseteq e\Gamma + \text{rad } \Gamma$, so

$$L = \Gamma L = \Gamma T L \subseteq \Gamma e L + (\text{rad } \Gamma)L \subseteq L,$$

and thus $L = \Gamma eL$. Since e centralizes Λ , there is a Λ -decomposition

$$L = eL \oplus (1-e)L.$$

For each $\gamma \in \Gamma$ we have $\gamma \in \text{Hom}_\Lambda(eL, L)$, whence (in the notation of (37.9a))

$$L \supseteq eL \cdot \text{Hom}_\Lambda(eL, L) \supseteq \Gamma eL = L.$$

This shows that $eL \succ L$ as left Λ -modules. But $L \succ (1-e)L$, and thus $eL \succ (1-e)L$. We therefore obtain a normal decomposition of L , except when $e=1$. Thus, if L is assumed normally indecomposable, then $e=1$ and $\overline{T}=\overline{\Gamma}$. But then T contains a unit of Γ , so $T=\Gamma$ and thus $1 \in T$. Hence $\varphi\tau=1$ for some $\tau \in \text{Hom}_\Lambda(L, M)$, and then τ is the desired splitting of φ . On the other hand, if we assume instead that each idempotent of Γ is central, then $L = \Gamma eL = e\Gamma L = eL$, so $e=1$ since Γ acts faithfully on L . This completes the proof.

For further results on normal decompositions of modules, see Brzezinski [78].

§37. Exercises

Throughout, Λ is an R -order in a f.d. separable K -algebra A .

- Let L be a left Λ -lattice, and consider all diagrams

$$\begin{array}{ccccccc} 0 & \longrightarrow & M_1 & \xrightarrow{\mu} & M & \longrightarrow & M_2 \longrightarrow 0 \\ & & f \downarrow & & & & \\ & & L & & & & \end{array}$$

with exact row of Λ -lattices. Show that L is weakly injective if and only if for each such diagram, f extends to a map $g: M \rightarrow L$.

[Hint: If each f extends, then every exact sequence of lattices

$$0 \rightarrow L \rightarrow M \rightarrow M_2 \rightarrow 0$$

must split, by taking $M_1 = L$, $f = 1$ above. Conversely, given such a diagram, let X be the pushout of $\{f, \mu\}$. Then there is an exact sequence $0 \rightarrow L \rightarrow X \rightarrow M_2 \rightarrow 0$. If L is weakly injective, the sequence splits, and from the splitting map $X \rightarrow L$ one easily obtains the desired $g: M \rightarrow L$.]

- Given L and M , suppose each diagram above, with fixed M , can be completed to a commutative diagram by means of a map $g: M \rightarrow L$. In this case, call L “ M -injective”. Show that if I is a weakly injective Λ -lattice, then $M \cdot \text{Hom}_\Lambda(M, I)$ is $M^{(n)}$ -injective for each n .

[Hint: Put $L = M \cdot \text{Hom}_\Lambda(M, I) = \Lambda$ -sublattice of I . Then, using the notation of (37.9a),

$$M^{(n)} \cdot \text{Hom}_\Lambda(M^{(n)}, I) = M \cdot \text{Hom}_\Lambda(M, I) = L.$$

Consider a diagram

$$\begin{array}{ccccccc} 0 & \longrightarrow & M_1 & \longrightarrow & M^{(n)} & \longrightarrow & M_2 & \longrightarrow 0 \\ & & f \downarrow & & \downarrow L & & & \\ & & i & & \downarrow & & & \\ & & & & I & & & \end{array}$$

with exact row of Λ -lattices, and i the inclusion map. Then there exists $g: M^{(n)} \rightarrow I$ extending if , and $g(M^{(n)}) \subseteq L$, so g extends f .]

3. Let L be $M^{(n)}$ -injective for each n , and set

$$L = P \oplus Q, M = P \oplus T.$$

Show that Q is $T^{(n)}$ -injective for each n .

[Hint: Starting with

$$\begin{array}{ccccccc} 0 & \longrightarrow & T_1 & \longrightarrow & T^{(n)} & \longrightarrow & T_2 & \longrightarrow 0, \\ & & f \downarrow & & & & & \\ & & Q & & & & & \end{array}$$

form the diagram

$$\begin{array}{ccccccc} 0 & \longrightarrow & T_1 \oplus P^{(n)} & \longrightarrow & T^{(n)} \oplus P^{(n)} & \longrightarrow & T_2 & \longrightarrow 0, \\ & & f' \downarrow & & \nearrow g' & & & \\ & & Q \oplus P & & & & & \end{array}$$

where f' coincides with f on T_1 and vanishes on $P^{(n)}$. Extend f' to g' , and then $g'|_{T^{(n)}}$ is the desired extension of f .]

4. Let G be a cyclic group of prime order. Show that ZG is a Bass order.

5. Let $L \subseteq M$ be left Λ -lattices. Call L *hypercharacteristic* in M if $L \cdot \text{Hom}_\Lambda(L, M) \subseteq L$, that is, $f(L) \subseteq L$ for each $f \in \text{Hom}_\Lambda(L, M)$. Show

- (i) For each order Γ containing Λ , Γ^* is a hypercharacteristic right Λ -sublattice of Λ^* .
- (ii) Each hypercharacteristic $M \subseteq \Lambda^*$ for which Λ^*/M is R -torsion, is some Γ^* .

(iii) The correspondence $\Gamma \leftrightarrow M$ is one-to-one inclusion-reversing.

[Hint: If $\Lambda \subseteq \Gamma$ then $\Gamma^* \subseteq \Lambda^*$, and

$$\text{Hom}_\Lambda(\Gamma^*, \Lambda^*) = (\Gamma^* \cdot \Lambda)^* \subseteq (\Gamma^* \cdot \Gamma)^* = \text{Hom}_\Lambda(\Gamma^*, \Gamma^*),$$

so Γ^* is hypercharacteristic in Λ^* . Conversely, given M as in (ii), put $L = M^* =$ left Λ -lattice containing Λ . Then

$$L = (L^* \cdot \Lambda)^* = \text{Hom}_\Lambda(L^*, \Lambda^*) = \text{Hom}_\Lambda(M, \Lambda^*) = \text{Hom}_\Lambda(M, M),$$

so L is an order. The result is due to Drozd-Kirichenko-Roiter [67].]

6. For a Λ -lattice M , define $I(M)$ as in (37.15). Show that for each P , $I(\hat{M}_P)$ is the P -adic completion of $I(M)$.

[Hint: Let $\hat{S}_i = \coprod_j S_{ij}^{(r_j)}$, where $\{S_{ij}\}$ is a basic set of simple left \hat{A} -modules. Then

$$\hat{A} \cong \coprod_{i,j} S_{ij}^{(r_j a_i)}, \quad \hat{K}\hat{M} \cong \coprod_{i,j} S_{ij}^{(r_j m_i)},$$

so

$$I(\hat{M}) = \coprod_{i,j} S_{ij}^{\min(r_j m_i, r_j a_i)} = \hat{K} \otimes I(M).$$

7. Let R be a complete d.v.r., and let Λ be a local Gorenstein R -order which is not a maximal order. Then there is a unique minimal overorder Λ' containing Λ , and indeed $\Lambda' = \text{End}_\Lambda(\text{rad } \Lambda)$.

[Hint: (Roiter [66b]). Let $N = \text{rad } \Lambda$. Since $\Lambda^* > \Lambda$ and Λ is indecomposable as module, we have $\Lambda^* \cong \Lambda$. Thus $N\Lambda^*$ is the unique maximal submodule of Λ^* . If $N\Lambda^* > \Lambda^*$, then $N\Lambda^* \cong \Lambda$, whence $N \cong \Lambda$. But then Λ is a hereditary order by MO (39.1), and is therefore a maximal order by (26.28). Thus $N\Lambda^*$ does not cover Λ^* , whence $N\Lambda^* \cdot \text{Hom}_\Lambda(N\Lambda^*, \Lambda^*) = N\Lambda^*$. Therefore $N\Lambda^*$ is hypercharacteristic in Λ^* . Now use Exercise 5.]

8. Show that Λ is a Gorenstein order if and only if every indecomposable lattice L can be embedded as a pure submodule of a free Λ -lattice. Show also that an R -order Λ is hereditary if and only if $M \otimes_\Lambda L$ is R -torsionfree for every right Λ -lattice M and left Λ -lattice L .

[Hint: See Gustafson [74].]

9. Let $\Lambda \subset \Gamma$ be R -orders in A , and let L and M be Γ -lattices. Show that if $L > M$ as Γ -lattices, then also $L > M$ as Λ -lattices.

10. Let $\Lambda \subset \Gamma$ as above, and let L be a Γ -lattice, M a Λ -lattice. Show that if $L > M$ as Λ -lattices, then M is necessarily a Γ -lattice.

[Hint: Choose a nonzero $a \in R$ such that $a\Gamma \subseteq \Lambda$. For each $f \in \text{Hom}_\Lambda(L, M)$, $f(a\Gamma \cdot L) = a\Gamma f(L)$. Hence

$$a\Gamma M = \sum_f f(a\Gamma L) = \sum_f f(aL) = a \sum_f f(L) = aM,$$

so $\Gamma M = M$.]

11. Let V be a f.g. left A -module, and set $V^* = \text{Hom}_K(V, K)$. For each full Λ -lattice M in V , let $M^* = \text{Hom}_R(M, R)$. Then M^* is a full Λ -lattice in the right A -module V^* . Prove that the bijection $M \leftrightarrow M^*$ is inclusion-reversing.

[Hint: Let $M \subset N$, where N is a full Λ -lattice in V , and put $T = N/M$. Now apply $\text{Hom}_R(\cdot, R)$ to the exact sequence

$$0 \rightarrow M \rightarrow N \rightarrow T \rightarrow 0.$$

Bibliography

References to articles on representation theory not discussed in this book may be found in the following publications:

- [74] *Reviews on finite groups*, D. Gorenstein, ed., Amer. Math. Soc., Providence, 1974.
- [71] *Representation theory of finite groups and related topics*, I. Reiner, ed., Proc. Symp. Pure Math., vol. 21, Amer. Math. Soc., Providence, 1971.
- [80] *The Santa Cruz conference on finite groups*, Proc. Symp. Pure Math., vol. 37, Amer. Math. Soc., Providence, 1980.

Albert, A. A.

- [39] *Structure of algebras*, Amer. Math. Soc., New York, 1939.

Alperin, J. L., Janusz, G. J.

- [73] Resolutions and periodicity, *Proc. Amer. Math. Soc.* 37 (1973), 403–406.

Alvis, D., Curtis, C. W., Dyke, T., Odutola, A.

- [81] Permutation-inversion groups for dimers: class structure and character table, *Molecular Physics*, to appear.

Anderson, F. W., Fuller, K. R.

- [73] *Rings and categories of modules*, Springer GTM 13, New York, 1973.

Aramata, H.

- [31] Über die Teilbarkeit der Dedekindschen Zetafunktionen, *Proc. Imp. Acad. Tokyo* 7 (1931), 334–336.
- [33] *Ibid.*, 9, (1933), 31–34.

Artin, E.

- [57] *Geometric algebra*, Wiley-Interscience, New York, 1957.

Auslander, M., Buchsbaum, D. A.

- [74] *Groups, rings, modules*, Harper and Row, New York, 1974.

Auslander, M., Goldman, O.

- [60a] Maximal orders, *Trans. Amer. Math. Soc.* 97 (1960), 1–24.
- [60b] The Brauer group of a commutative ring, *Trans. Amer. Math. Soc.* 97 (1960), 367–409.

Auslander, M., Rim, D. S.

- [63] Ramification index and multiplicity, *Illinois J. Math* **7** (1963), 566–581.

Ayoub, R. G., Ayoub, C.

- [69] On the group ring of a finite abelian group, *Bull. Austral. Math. Soc.* **1** (1969), 245–261.

Azumaya, G., Nakayama, T.

- [44] Über einfache distributive Systeme unendliche Ränge II, *Proc. Imp. Acad. Tokyo* **20** (1944), 348–352.

- [47] On irreducible rings, *Ann. of Math.* **48** (1947), 949–965.

Babakhanian, A.

- [72] *Cohomological methods in group theory*, Marcel Dekker, New York, 1972.

Bachmann, G.

- [64] *Introduction to p-adic numbers and valuation theory*, Academic Press, New York, 1964.

Ballew, D. W.

- [70] The module index and invertible ideals, *Trans. Amer. Math. Soc.* **148** (1970), 171–184.

- [71] Numerical invariants and projective modules, *J. Algebra* **17** (1971), 555–574.

Banaschewski, B.

- [63] On the character ring of finite groups, *Canad. J. Math.* **15** (1963), 605–612.

Bass, H.

- [62] Torsion free and projective modules, *Trans. Amer. Math. Soc.* **102** (1962), 319–327.

- [63] On the ubiquity of Gorenstein rings, *Math. Z.* **82** (1963), 8–28.

- [68] *Algebraic K-theory*, Math. Lecture Note Series, Benjamin, New York, 1968.

Behrens, E. -A.

- [72] *Ring theory*, Academic Press, New York, 1972.

Berger, T.

- [77] Hall-Higman type theorems V, *Pacific J. Math.* **73** (1977), 1–62.

Berman, S. D.

- [56a] p-adic ring of characters, *Dokl. Akad. Nauk SSSR* **106** (1956), 583–586.

- [56b] The number of irreducible representations of a finite group over an arbitrary field, *Dokl. Akad. Nauk SSSR* **106** (1956), 767–769.

- [63] Integral representations of finite groups, *Dokl. Akad. Nauk SSSR* **152** (1963), 1286–1287 = *Soviet Math. Dokl.* **4** (1963), 1533–1535. MR 27 #4854.

- [64] Integral representations of a cyclic group containing two irreducible rational components, *In Memoriam: N. G. Cebotarev*, Izdat. Kazan Univ., Kazan, 1964, pp. 18–29. (Russian) MR 33 #4154.

- [65] On integral monomial representations of finite groups, *Uspehi Mat. Nauk* **20** (1965), no. 4 (124), 133–134. (Russian) MR 33 #4155.

- [66] Representations of finite groups over an arbitrary field and over rings of integers, *Izv. Akad. Nauk SSSR Ser. Mat.* **30** (1966), 69–132; English transl., *Amer. Math. Soc. Transl. (2)* **64** (1967), 147–215. MR 33 #5747.

Berman, S. D., Gudivok, P. M.

- [62] Integral representations of finite groups, *Dokl. Akad. Nauk SSSR* **145** (1962), 1199–1201 = *Soviet Math. Dokl.* **3** (1962), 1172–1174. MR 25 #3095.
- [64] Indecomposable representations of finite groups over the ring of p -adic integers, *Izv. Akad. Nauk SSSR Ser. Mat.* **28** (1964), 875–910; English transl., *Amer. Math. Soc. Transl. (2)* **50** (1966), 77–113. MR 29 #3550.

Berman, S. D., Lichtman, A. I.

- [65] On integral representations of finite nilpotent groups, *Uspehi Mat. Nauk* **20** (1965), no. 5 (125), 186–188. (Russian) MR 34 #7673.

Bialnicki-Birula, A.

- [70] On the equivalence of integral representations of finite groups, *Proc. Amer. Math. Soc.* **26** (1970), 371–377.

Bondarenko, V. M.

- [76] The similarity of matrices over residue class rings, Math. Collection, Izdat “Nauk. Dumka,” Kiev (1976), 275–277. *Math Reviews* **56**, 12032.

Borevich, Z. I., Faddeev, D. K.

- [56] Theory of homology in groups, I, II, *Vestnik Leningrad. Univ.* **11** (1956), no. 7, 3–39; **14** (1959), no. 7, 72–87. (Russian) MR 18, 188; MR 21 #4968.
- [65a] Representations of orders with cyclic index, *Trudy Mat. Inst. Steklov.* **80** (1965), 51–65. *Proc. Steklov Inst. Math.* **80** (1965), 56–72. MR 34 #5805
- [65b] Remarks on orders with a cyclic index, *Dokl. Akad. Nauk SSSR* **164** (1965), 727–728 = *Soviet Math. Dokl.* **6** (1965), 1273–1274. MR 32 #7601.

Borevich, Z. I., Shafarevich, I. R.

- [66] *Number theory*, Academic Press, New York, 1966.

Bourbaki, N.

- [58] *Algèbre*, Ch. 8: Modules et anneaux semi-simples, Hermann, Paris, 1958.

Brauer, R.

- [47a] On the zeta-functions of algebraic number fields, *Amer. J. Math.* **69** (1947), 243–250.
- [47b] On Artin’s L -series with general group characters, *Ann. of Math.* **48** (1947), 502–514.
- [51] Beziehungen zwischen Klassenzahlen von Teilkörpern eines Galoisischen Körpers, *Math. Nachr.* **4** (1951), 158–174.
- [64a] A note on theorems of Burnside and Blitchfeldt, *Proc. Amer. Math. Soc.* **15** (1964), 31–34.
- [64b] On quotient groups of finite groups, *Math. Z.* **83** (1964), 72–84.

Brauer, R., Fowler, K. A.

- [55] On groups of even order, *Ann. of Math.* **62** (1955), 565–583.

- Brauer, R., Nesbitt, C.
- [37] *On the modular representations of finite groups*, Univ. of Toronto Studies Math. Ser. #4, 1937.
 - [41] On the modular characters of groups, *Ann. of Math.* **42** (1941), 556–590.
- Brauer, R., Suzuki, M.
- [59] On finite groups of even order whose 2-Sylow group is a quaternion group, *Proc. Nat. Acad. Sci. USA* **45** (1959), 1757–1759.
- Brauer, R., Suzuki, M., Wall, G. E.
- [58] A characterization of the one-dimensional unimodular projective groups over finite fields, *Illinois J. Math.* **2** (1958), 718–745.
- Brauer, R., Tate, J.
- [55] On the characters of finite groups, *Ann. of Math.* **62** (1955), 1–7.
- Broué, M.
- [75] Projectivité relative et groupes de Grothendieck, *C. R. Acad. Sci. Paris* **280** (1975), 1357–1360.
 - [76] Sur l’induction des modules indécomposables et la projectivité relative, *Math. Z.* **149** (1976), 227–245.
- Brzezinski, J.
- [78] Lattices of normally indecomposable modules, *Proc. Amer. Math. Soc.* **68** (1978), 271–276.
- Burnside, W.
- [11] *Theory of groups of finite order*, 2nd ed., Cambridge Univ. Press, Cambridge, 1911.
- Burry, D.
- [79] A strengthened theory of vertices and sources, *J. Algebra* **59** (1979), 330–344.
- Butler, M. C. R.
- [75] On the classification of local integral representations of finite abelian p -groups, Springer Lecture Notes 488, 1975, pp. 54–71.
- Childs, L. N., Orzech, M.
- [81] On modular group rings, normal bases and fixed points, *Amer. Math. Monthly* **88** (1981), 142–145.
- Cliff, G.
- [75] Vertices of representations of finite groups, Ph.D. thesis, Univ. of Illinois, 1975.
 - [77] On modular representations of p -solvable groups, *J. Algebra* **47** (1977), 129–137.
- Clifford, A. H.
- [37] Representations induced in an invariant subgroup, *Ann. of Math.* **38** (1937), 533–550.
- Cline, E.
- [72] Stable Clifford theory, *J. Algebra* **22** (1972), 350–364.

Cohen, I. S.

- [50] Commutative rings with restricted minimum condition, *Duke Math. J.* **17** (1950), 27–42.

Coleman, D. B.

- [66] Idempotents in group rings, *Proc. Amer. Math. Soc.* **17** (1966), 962.

Conlon, S. B.

- [64] Twisted group algebras and their representations, *J. Austral. Math. Soc.* **4** (1964), 152–173.

Craig, M.

- [76] A characterization of certain extreme forms, *Illinois J. Math.* **20** (1976), 706–717.

Curtis, C. W.

- [66] The Steinberg character of a finite group with a BN-pair, *J. Algebra.* **4** (1966), 433–441.

Curtis, C. W., Fossum, T. V.

- [68] On centralizer rings and characters of representations of finite groups, *Math. Z.* **107** (1968), 402–406.

Curtis, C. W., Reiner, I.

- [66] *Representation theory of finite groups and associative algebras*, Pure and Appl. Math., vol. 11, Interscience, New York, 1962; 2nd ed., 1966.

Dade, E. C.

- [62] Rings in which no fixed power of ideal classes becomes invertible, *Math. Ann.* **148** (1962), 65–66.
- [63] Some indecomposable group representations, *Ann. of Math.* (2) **77** (1963), 406–412.
- [70] Compounding Clifford's theory, *Ann. of Math.* (2) **91** (1970), 236–290.
- [71] Deux groupes finis distinct ayant la même algèbre de groupe sur tout corps, *Math. Z.* **119** (1971), 345–348.

Dade, E. C., Taussky, O.

- [65] Some new results connected with matrices of rational integers, *Symp. Pure Math.*, Amer. Math. Soc., vol. 8 (1965), pp. 78–88.

Dade, E. C., Taussky, O., Zassenhaus, H.

- [62] On the theory of orders, in particular on the semigroup of ideal classes and genera of an order in an algebraic number field, *Math. Ann.* **148** (1962), 31–64.

De Leeuw, K.

- [53] Some applications of cohomology to algebraic number theory and group representations, unpublished.

Diederichsen, F. E.

- [40] Über die Ausreduktion ganzzahliger Gruppendarstellungen bei arithmetischer Äquivalenz, *Abh. Math. Sem. Univ. Hamburg* **14** (1940), 357–412.

Dieudonné, J.

- [46] Sur la réduction canonique des couples de matrices, *Bull. Soc. Math. France* **74** (1946), 130–146.

Dornhoff, L.

- [71] *Group representation theory, Part A*, Dekker, New York, 1971.
- [72] *Group representation theory, Part B*, Dekker, New York, 1972.

Dress, A.

- [70] On the Krull-Schmidt theorem for integral group representations of rank 1, *Michigan Math. J.* **17** (1970), 273–277.
- [71] Operations in representation rings, Proc. Symp. Pure Math., Amer. Math. Soc., vol. 21 (1971), pp. 39–45.

Drobotenko, V. S.

- [66] Integral representations of primary abelian groups, *Algebra and Math. Logic: Studies in Algebra*, Izdat. Kiev Univ., Kiev, 1966, pp. 111–121. (Russian) MR 34 #4375.

Drobotenko, V. S., Drobotenko, E. S., Zhilinskaya, Z. P., Pogorilyak, E. Y.

- [65] Representations of the cyclic group of prime order p over residue classes mod p^s , *Ukrain. Mat. Z.* **17** (1965), no. 5, 28–42; English transl., *Amer. Math. Soc. Transl. (2)* **69** (1968), 241–256. MR 32 #5743.

Drobotenko, V. S., Gudivok, P. M., Lichtman, A. I.

- [64] On representations of finite groups over the ring of residue classes mod m , *Ukrain. Mat. Z.* **16** (1964), 82–89. (Russian) MR 29 #4810.

Drobotenko, V. S., Lichtman, A. I.

- [60] Representations of finite groups over the ring of residue classes mod p^s , *Dokl. Uzgorod Univ.* **3** (1960), 63. (Russian).

Drozd, Yu. A.

- [67] Representations of cubic Z-rings, *Dokl. Akad. Nauk SSSR* **174** (1967), 16–18 = *Soviet Math. Dokl.* **8** (1967), 572–574. MR 35 #6659.
- [69a] Adèles and integral representations, *Izv. Akad. Nauk SSSR Ser. Mat.* **33** (1969), 1080–1088 = *Math. USSR Izv.* **3** (1969), 1019–1026.
- [69b] On the distribution of maximal sublattices, *Mat. Zametki* **6** (1969), 19–24 = *Math. Notes* **6** (1969), 469–471.
- [71] The structure of genera of representations of nonsemisimple rings, *Mat. Zametki* **10** (1971), 63–67.
- [74] Generalization of a theorem of Dade, *Dopovidi Akad. Nauk RSR Ser. A*, **3** (1974), 204–207.

Drozd, Yu. A., Kirichenko, V. V.

- [67] Representations of rings in a second order matrix algebra, *Ukrain. Mat. Ž.* **19** (1967), no. 3, 107–112. (Russian) MR 35 #1632.
- [73] Primary orders with a finite number of indecomposable representations, *ibid.* **37** (1973), 715–736.

Drozd, Yu. A., Kirichenko, V. V., Roiter, A. V.

- [67] On hereditary and Bass orders, *Izv. Akad. Nauk SSSR Ser. Mat.* **31** (1967), 1415–1436 = *Math. USSR Izv.* **1** (1967), 1357–1376. MR 36 #2608.

Drozd, Yu. A., Roiter, A. V.

- [67] Commutative rings with a finite number of indecomposable integral representations, *Izv. Akad. Nauk SSSR Ser. Mat.* **31** (1967), 783–798 = *Math. USSR Izv.* **1** (1967), 757–772. MR 36 #3768.

Drozd, Yu. A., Turčin, V. M.

- [67] Number of representation modules in a genus for integral second order matrix rings, *Mat. Zametki* **2** (1967), 133–138 = *Math. Notes* **2** (1967), 564–566. MR 37 #5253.

Eilenberg, S., Nakayama, T.

- [55] On the dimensions of modules and algebras, II. (Frobenius algebras and quasi-Frobenius rings), *Nagoya Math. J.* **9** (1955), 1–16.

Evens, L.

- [63] A generalization of the transfer map in the cohomology of groups, *Trans. Amer. Math. Soc.* **108** (1963), 54–65.

Faddeev, D. K.

- [64] On the semigroup of genera in the theory of integer representations, *Izv. Akad. Nauk SSR Ser. Mat.* **28** (1964), 475–478; English transl., *Amer. Math. Soc. Transl.* (2) **64** (1967), 97–101. MR 28 #5089.

- [65a] An introduction to multiplicative theory of modules of integral representations, *Trudy Mat. Inst. Steklov.* **80** (1965), 145–182 = *Proc. Steklov Inst. Math.* **80** (1965), 164–210. MR 34 #5873.

- [65b] On the theory of cubic Z-rings, *Trudy Mat. Inst. Steklov.* **80** (1965), 183–187 = *Proc. Steklov Inst. Math.* **80** (1965), 211–215. MR 33 #4083.

- [66] Equivalence of systems of integer matrices, *Izv. Akad. Nauk SSSR Ser. Mat.* **30** (1966), 449–454; English transl., *Amer. Math. Soc. Transl.* (2) **71** (1968), 43–48. MR 33 #2642.

- [67] The number of classes of exact ideals for Z-rings, *Mat. Zametki* **1** (1967), 625–632 = *Math. Notes* **1** (1967), 415–419. MR 35 #5466.

Falk, D.

- [76] On the invertibility of ideals in orders, *J. Number Theory* **8** (1976), 308–312.

Feit, W.

- [67] *Characters of finite groups*, Benjamin, New York, 1967.

Feit, W., Hall, M., Thompson, J. G.

- [60] Finite groups in which the centralizer of any non-identity element is nilpotent, *Math. Z.* **74** (1960), 1–17.

Feit, W., Thompson, J. G.

- [63] Solvability of groups of odd order, *Pacific J. Math.* **13** (1963), 775–1029.

Fong, P.

- [61] On the characters of p -solvable groups, *Trans. Amer. Math. Soc.* **98** (1961), 263–284.
- [62] Solvable groups and modular representation theory, *Trans. Amer. Math. Soc.* **103** (1962), 484–494.

Foote, A.

- [67] Universal central extensions of groups, Ph.D. thesis, Wisconsin, 1967.

Frame, J. S.

- [41] The double cosets of a finite group, *Bull. Amer. Math. Soc.* **47** (1941), 458–467.

Frobenius, F. G.

- [96] Über Gruppencharaktere, *Sitzber. Preuss. Akad. Wiss.* (1896), 985–1021; *Gesammelte Abhandlungen*, III, Springer-Verlag, Berlin, 1968, pp. 1–37.

Fröhlich, A.

- [65] Invariants for modules over commutative separable orders, *Quart. J. Math. Oxford Ser. (2)* **16** (1965), 193–232.
- [75] Locally free modules over arithmetic orders, *J. Reine Angew. Math.* **274/275** (1975), 112–124.

Gallagher, P. X.

- [62a] Group characters and commutators, *Math. Z.* **79** (1962), 122–126.
- [62b] Group characters and normal Hall subgroups, *Nagoya Math. J.* **21** (1962), 223–230.
- [65] Determinants of representations of finite groups, *Hamb. Abh.* **28** (1965), 162–167.
- [66] Zeros of characters of finite groups, *J. Algebra* **4** (1966), 42–45.

Galovich, S.

- [74] The class group of a cyclic p -group, *J. Algebra* **30** (1974), 368–387.

Gantmacher, F. R.

- [60] *The theory of matrices*, Chelsea, New York, 1960.

Gaschütz, W.

- [52] Über den Fundamentalsatz von Maschke zur Darstellungstheorie der endlichen Gruppen, *Math. Z.* **56** (1952), 376–387.

Glauberman, G.

- [66] Central elements in core-free groups, *J. Algebra* **4** (1966), 403–420.
- [74] On groups with a quaternion Sylow 2-subgroup, *Illinois J. Math.* **18** (1974), 60–65.

Goldschmidt, D., Isaacs, I.

- [75] Schur indices in finite groups, *J. Algebra* **33** (1975), 191–199.

Gorenstein, D.

- [68] *Finite groups*, Harper and Row, New York, 1968.

Gorenstein, D., Walter, J.

- [65] The characterization of finite groups with dihedral Sylow 2-subgroups I–III, *J. Algebra* **2** (1965), 85–151, 218–270, 354–393.

Gorman, H.

- [70] Invertibility of modules over Prüfer rings, *Illinois J. Math.* **14** (1970), 283–298.

Green, E. L., Reiner, I.

- [78] Integral representations and diagrams, *Michigan Math. J.* **25** (1978), 53–84.

Green, J. A.

- [55a] On the converse to a theorem of R. Brauer, *Proc. Cambridge Phil. Soc.* **51** (1955), 237–239.
- [55b] The characters of the finite general linear groups, *Trans. Amer. Math. Soc.* **80** (1955), 402–447.
- [59] On the indecomposable representations of a finite group, *Math. Z.* **70** (1959), 430–445.
- [62] Blocks of modular representations, *Math. Z.* **79** (1962), 100–115.
- [64] A transfer theorem for modular representations. *J. Algebra* **1** (1964), 73–84.

Gruenberg, K.

- [70] *Cohomological topics in group theory*, Springer Lecture Notes 143, 1970.

Gruenberg, K., Roggenkamp, K. W.

- [75] Projective covers for augmentation ideals of finite groups, *J. Pure Appl. Algebra* **6** (1975), 165–176.

Gudivok, P. M.

- [67] Representations of finite groups over number rings, *Izv. Akad. Nauk SSSR Ser. Mat.* **31** (1967), 799–834 = *Math. USSR Izv.* **1** (1967), 773–805. MR 36 #1554.
- [74] On modular and integral representations of finite groups, *Dokl. Akad. Nauk SSSR* **214** (1974), 993–996.
- [78a] On representations of finite groups over complete discrete valuation rings, *Trudy Mat. Inst. Akad. Nauk SSSR* **148** (1978), 96–105.
- [78b] Integral representations of finite groups, *Educational Text*, Uzhgorod Univ., 1978.

Gustafson, W. H.

- [74] Torsionfree modules and classes of orders, *Bull. Austral. Math. Soc.* **11** (1974), 365–371.

Hall, M.

- [59] *The theory of groups*, Macmillan, New York, 1959.

Hannula, T.

- [68] The integral representation ring $a(R_kG)$, *Trans. Amer. Math. Soc.* **133** (1968), 553–559.

Harada, M.

- [64] Some criteria for hereditarity of crossed products, *Osaka J. Math.* **1** (1964), 69–80.

Hattori, A.

- [65] Rank element of a projective module, *Nagoya Math. J.* **25** (1965), 113–120.

Helgason, S.

- [62] *Differential geometry and symmetric spaces*, Academic Press, New York, 1962.

Heller, A.

- [61a] On group representations over a valuation ring, *Proc. Nat. Acad. Sci. USA* **47** (1961), 1194–1197.
- [61b] Indecomposable modules and the loop space operation, *Proc. Amer. Math. Soc.* **12** (1961), 640–643.

Heller, A., Reiner, I.

- [62] Representations of cyclic groups in rings of integers I, *Ann. of Math.* (2) **76** (1962), 73–92.
- [63] II, *ibid.* **77** (1963), 318–328.

Higman, D. G.

- [54] Indecomposable representations at characteristic p , *Duke Math. J.* **21** (1954), 377–381.
- [55a] Induced and produced modules, *Canad. J. Math.* **7** (1955), 490–508.
- [55b] On orders in separable algebras, *Canad. J. Math.* **7** (1955), 509–515.
- [57] Relative cohomology, *Canad. J. Math.* **9** (1957), 19–34.
- [59] On isomorphisms of orders, *Michigan Math. J.* **6** (1959), 255–258.
- [60] On representations of orders over Dedekind domains, *Canad. J. Math.* **12** (1960), 107–125.
- [64] Finite permutation groups of rank 3, *Math. Z.* **86** (1964), 145–156.
- [67] Intersection matrices for finite permutation groups, *J. Algebra* **6** (1967), 22–42.

Higman, D. G., McLaughlin, J. E.

- [59] Finiteness of class numbers of representations of algebras over function fields, *Michigan Math. J.* **6** (1959), 401–404.

Higman, G.

- [40] The units of group rings, *Proc. London Math. Soc.* (2) **46** (1940), 231–248.
- [68] *Odd characterizations of finite simple groups*, Lecture Notes, Univ. of Michigan, 1968.
- [71] Construction of simple groups from character tables, *Finite Simple Groups*, Academic Press, London, 1971, pp. 205–214.

Hochschild, G., Serre, J. P.

- [53] Cohomology of group extensions, *Trans. Amer. Math. Soc.* **74** (1953), 110–134.

Huppert, B.

- [67] *Endliche Gruppen*, I, Springer-Verlag, Berlin, 1967.
- [75] Bemerkungen zur modularen Darstellungstheorie I. Absolut unzerlegbare Moduln, *Archiv der Math.* **26** (1975), 242–249.

Isaacs, I. M.

- [74] Lifting Brauer characters of p -solvable groups, *Pacific J. Math.* **53** (1974), 171–188.
- [76] *Character theory of finite groups*, Academic Press, New York, 1976.
- [78] Lifting Brauer characters of p -solvable groups II, *J. Algebra* **51** (1978), 476–490.
- [81] Extensions of group representations over arbitrary fields, *J. Algebra* **68** (1981) 54–74.

Ito, N.

- [51] On the degrees of irreducible representations of a finite group, *Nagoya Math. J.* **3** (1951), 5–6.

Jacobson, N.

- [45a] The structure of simple rings without finiteness conditions, *Trans. Amer. Math. Soc.* **57** (1945), 228–245.
- [45b] The radical and semi-simplicity for arbitrary rings, *Amer. J. Math.* **67** (1945), 300–320.
- [56] *The structure of rings*, Amer. Math. Soc., Providence, 1956.

Jacobinski, H.

- [66] On extensions of lattices, *Michigan Math. J.* **13** (1966), 471–475.
- [67] Sur les ordres commutatifs avec un nombre fini de réseaux indécomposables, *Acta Math.* **118** (1967), 1–31.
- [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.
- [70] On embedding of lattices belonging to the same genus, *Proc. Amer. Math. Soc.* **24** (1970), 134–136.
- [75] Unique decomposition of lattices over orders, Springer Lecture Notes 488, 1975, pp. 168–175.

Janusz, G. J.

- [66] Primitive idempotents in group algebras, *Proc. Amer. Math. Soc.* **17** (1966), 520–523.
- [79] Tensor products of orders, *J. London Math. Soc.* (2) **20** (1979), 186–192.
- [80] Crossed product orders and the Schur index, *Comm. Algebra* **8** (1980), 697–706.

Jones, A.

- [63a] Groups with a finite number of indecomposable integral representations, *Michigan Math. J.* **10** (1963), 257–261.
- [63b] Integral representations of the direct product of groups, *Can. J. Math.* **15** (1963), 625–630.
- [65] On representations of finite groups over valuation rings, *Illinois J. Math.* **9** (1965), 297–303.
- [80] Integral representations of cyclic p -groups, *Trabalhos Dept. Mat.*, Univ. de São Paulo, 1980.

Kaplansky, I.

- [70] *Commutative Rings*, Allyn and Bacon, Boston, 1970.

Keller, G.

- [68] Concerning the degrees of irreducible characters, *Math. Z.* **107** (1968), 221–224.

Kerber, A.

- [68] Zur Darstellungstheorie von Kranzprodukten, *Canad. J. Math.* **20** (1968), 665–672.

Kervaire, M. A., Murthy, M. P.

- [77] On the projective class group of cyclic groups of prime power order, *Comment. Math. Helvetici* **52** (1977), 415–452.

Kirichenko, V. V.

- [70] Representations of third order matrix rings, *Mat. Zametki* **8** (1970), 235–244.

Knee, D. I.

- [62] The indecomposable integral representations of finite cyclic groups, Ph.D. thesis, M.I.T., Cambridge, Mass., 1962.

Kneser, M.

- [66] Einige Bemerkungen über ganzzahlige Darstellungen endlicher Gruppen, *Archiv der Math.* **17** (1966), 377–379.

Kodama, T.

- [56] On the commutator group of normal simple algebras, *Memoirs Fac. Sci. Kyushu Univ. Ser. A.* **10** (1956), 141–149.
- [60] *Ibid.* **40** (1960), 98–103.

Lam, T. Y., Reiner, I.

- [69] Relative Grothendieck groups, *J. Algebra* **11** (1969), 213–242.

Lang, S.

- [65] *Algebra*, Addison-Wesley, Reading, 1965.

Lee, M. P.

- [64] Integral representations of dihedral groups of order $2p$, *Trans. Amer. Math. Soc.* **110** (1964), 213–231.

Levy, L.

- [81] Mixed modules over ZG , G cyclic of prime order, and over related Dedekind pullbacks, *J. Algebra*, to appear.

Lorenz, F.

- [75] Die Umkehrung des Satzes von Brauer-Berman-Witt über induzierte Charaktere endlichen Gruppen, *Math. Z.* **142** (1975), 167–171.

Mackey, G. W.

- [51] On induced representations of groups, *Amer. J. Math.* **73** (1951), 576–592.
- [53] Symmetric and anti-symmetric Kronecker squares of induced representations of finite groups, *Amer. J. Math.* **75** (1953), 387–405.

Maranda, J. M.

- [53] On p -adic integral representations of finite groups, *Canad. J. Math.* **5** (1953), 344–355.
- [55] On the equivalence of representations of finite groups by groups of automorphisms of modules over Dedekind rings, *Canad. J. Math.* **7** (1955), 516–526.

McKay, J.

- [79] The non-abelian simple groups G , $|G| < 10^6$: character tables, *Comm. Algebra* **7** (1979), 1407–1445.

Merklen, H.

- [78] Hereditary crossed product orders, *Pacific J. Math.* **74** (1978), 391–406.

Milnor, J.

- [66] Whitehead torsion, *Bull. Amer. Math. Soc.* **72** (1966), 358–426.
- [71] *Introduction to algebraic K-theory*, Ann. of Math. Studies **72** (1971), Princeton, N.J.

Morita, K.

- [58] Duality for modules and its applications to the theory of rings with minimum condition, *Sci. Rep. Tokyo Kyoiku Daigaku, Section A*, **6**, no. 150, (1958), 83–142.

Nakayama, T.

- [57] On modules of trivial cohomology over a finite group, *Illinois J. Math.* **1** (1957), 36–43.

Nakayama, T., Matsushima, Y.

- [43] Über die multiplikative Gruppe einer p -adischen Divisionsalgebra, *Proc. Imp. Acad. Tokyo* **19** (1943), 622–628.

Nazarova, L. A.

- [61] Unimodular representations of the four group, *Dokl. Akad. Nauk SSSR* **140** (1961), 1011–1014 = *Soviet Math. Dokl.* **2** (1961), 1304–1307. MR 24 #770.
- [63] Unimodular representations of the alternating group of degree four, *Ukrain. Mat. Ž.* **15** (1963), 437–444. (Russian) MR 28 #2148.
- [67] Representations of a tetrad, *Izv. Akad. Nauk SSSR Ser. Mat.* **31** (1967), 1361–1378 = *Math. USSR Izv.* **1** (1967), 1305–1322. MR 36 #6400.

Nazarova, L. A., Roiter, A. V.

- [62] Integral representations of the symmetric group of third degree, *Ukrain. Mat. Ž.* **14** (1962), 271–288. (Russian) MR 26 #6273.
- [66] On irreducible representations of p -groups over $Z_p(\epsilon)$, *Ukrain. Mat. Ž.* **18** (1966), no. 1, 119–124. (Russian) MR 34 #254.
- [67a] On integral p -adic representations and representations over residue class rings, *Ukrain. Mat. Ž.* **19** (1967), no. 2, 125–126. (Russian) MR 35 #267.
- [67b] Refinement of a theorem of Bass, *Dokl. Akad. Nauk SSSR* **176** (1967), 266–268 = *Soviet Math. Dokl.* **8** (1967), 1089–1092. MR 37 #1402.
- [69] Finitely generated modules over a dyad of a pair of local Dedekind rings, and finite groups having an abelian normal subgroup of index p , *Izv. Akad. Nauk SSSR Ser. Mat.* **33** (1969), 65–89 = *Math. USSR Izv.* **3** (1969), 65–86.

Nazarova, L. A., Roiter, A. V., Sergeicuk, V. V., Bondarenko, V. M.

- [72] Applications of modules over dyads to the classification of finite p -groups that have an abelian subgroup of index p , and to the classification of pairs of mutually annihilating operators, *LOMI*, 1972, 69–92; *J. Soviet Math.* **3** (1975), 636–653.

Niven, I., Zuckerman, H. S.

- [80] *An introduction to the theory of numbers*, 4th ed., Wiley, New York, 1980.

Nunke, R. J.

- [59] Modules of extensions over Dedekind rings, *Illinois J. Math.* **3** (1959), 222–241.

Oppenheim, J.

- [62] Integral representations of cyclic groups of squarefree order, Ph.D. thesis, Univ. of Illinois, Urbana, Ill., 1962.

O'Reilly, M. F.

- [65] On the semisimplicity of the modular representation algebra of a finite group, *Illinois J. Math.* **9** (1965), 261–276.

Platonov, V. P.

- [69] Adèle groups and integral representations, *Izv. Akad. Nauk SSSR* **33** (1969), 155–162 = *Math. USSR Izv.* **3** (1969), 147–154.
- [75a] On the Tannaka-Artin problem, *Dokl. Akad. Nauk SSSR* **221** (1975), 1038–1041.
- [75b] The Tannaka-Artin problem and groups of projective conorm, *ibid.* **222** (1975), 1299–1302.
- [76] The Tannaka-Artin problem and reduced K -theory, *Izv. Acad. Nauk SSSR, Ser. Mat.* **40** (1976), 227–261 = *Math. USSR Izv.* **10** (1976), 211–243.

Plesken, W.

- [77] On absolutely irreducible representations of orders, *Number theory and algebra*, Academic Press, New York, 1977, pp. 241–262.
- [78] On reducible and decomposable representations of orders, *J. Reine Angew. Math.* **297** (1978), 188–210.

Pu, L. C.

- [65] Integral representations of non-abelian groups of order pq , *Michigan Math. J.* **12** (1965), 231–246.

Reiner, I.

- [56] Maschke modules over Dedekind rings, *Canad. J. Math.* **8** (1956), 329–334.
- [57] Integral representations of cyclic groups of prime order, *Proc. Amer. Math. Soc.* **8** (1957), 142–146.
- [59] On the class number of representations of an order, *Canad. J. Math.* **11** (1959), 660–672.
- [62] Failure of the Krull-Schmidt theorem for integral representations, *Michigan Math. J.* **9** (1962), 225–231.
- [63] Extensions of irreducible modules, *Michigan Math. J.* **10** (1963), 273–276.
- [64] On the number of irreducible modular representations of a finite group, *Proc. Amer. Math. Soc.* **15** (1964), 810–812.
- [66] Relations between integral and modular representations, *Michigan Math. J.* **13** (1966), 375–372.
- [67] Module extensions and blocks, *J. Algebra* **5** (1967), 157–163.
- [75] *Maximal orders*, Academic Press, London, 1975.
- [78] Invariants of integral representations, *Pacific J. Math.* **78** (1978), 467–501.
- [79a] Lifting isomorphisms of modules, *Canad. J. Math.* **31** (1979), 808–811.
- [79b] On Diederichsen's formula for extensions of lattices. *J. Algebra* **58** (1979), 238–246.

Reiner, I., Roggenkamp, K. W.

- [79] *Integral representations*, Springer Lecture Notes 744, Springer, Berlin, 1979.

Reiner, I., Zassenhaus, H.

- [61] Equivalence of representations under extensions of local ground rings, *Illinois J. Math.* **5** (1961), 409–411.

Reynolds, W. F.

- [71] Twisted group algebras over arbitrary fields, *Illinois J. Math.* **15** (1971), 91–103.

Ringel, C. M., Roggenkamp, K. W.

- [79] Diagrammatic methods in the representation theory of orders. *J. Algebra* **60** (1979), 11–42.

Roesler, F.

- [72] Darstellungstheorie von Schur-Algebren, *Math. Z.* **125** (1972), 32–58.

Roggenkamp, K. W.

- [69] Das Krull-Schmidt Theorem für projektive Gitter in Ordnungen über lokalen Ringen, *Math. Seminar Giessen*, 1969.
- [70] *Lattices over orders* II, Springer Lecture Notes 142, Springer, Berlin, 1970.
- [71] Projective homomorphisms and extensions of lattices, *J. Reine Angew. Math.* **246** (1971), 41–46.
- [72] An extension of the Noether-Deuring Theorem, *Proc. Amer. Math. Soc.* **31** (1972), 423–426.

Roggenkamp, K. W., Huber-Dyson, V.

- [70] *Lattices over orders* I, Springer Lecture Notes 115, Springer, Berlin, 1970.

Roiter, A. V.

- [60] On the representations of the cyclic group of fourth order by integral matrices, *Vestnik Leningrad. Univ.* **15** (1960), no. 19, 65–74. (Russian) MR 23 #A1730.
- [63a] Categories with division and integral representations, *Dokl. Akad. Nauk SSSR* **153** (1963), 46–48 = *Soviet Math. Dokl.* **4** (1963), 1621–1623. MR 33 #2704.
- [63b] On a category of representations, *Ukrain. Mat. Ž.* **15** (1963), 448–452.
- [65] Divisibility in the category of representations over a complete local Dedekind ring, *Ukrain. Mat. Ž.* **17** (1965), no. 4, 124–129. (Russian) MR 33 #5699.
- [66a] On integral representations belonging to a genus, *Izv. Akad. Nauk SSSR Ser. Mat.* **30** (1966), 1315–1324; English transl., *Amer. Math. Soc. Transl. (2)* **71** (1968), 49–59. MR 35 #4255.
- [66b] An analog of Bass' theorem for representation modules of non-commutative orders, *Dokl. Akad. Nauk SSSR* **168** (1966), 1261–1264 = *Soviet Math. Dokl.* **7** (1966), 830–833. MR 34 #2632.

Roquette, P.

- [52] Arithmetische Untersuchung des Charakterringes einer endlichen Gruppe, *J. Reine Angew. Math.* **190** (1952), 148–168.

Rosen, M.

- [63] Representations of twisted group rings, Ph.D. thesis, Princeton Univ., 1963.

Rotman, J.

- [79] *An introduction to homological algebra*, Academic Press, New York, 1979.

Rukolaine, A. V.

- [62] On the degrees of the modular representations of p -solvable groups, *Vestnik Leningrad. Univ.* **19** (1962) 41–48.
- [64] Some arithmetic properties of modular characters of p -solvable groups. *Izv. Akad. Nauk SSSR* **28** (1964), 571–582.

Schur, I.

- [04] Über die Darstellung der endlichen Gruppen durch gebrochene lineare Substitutionen, *J. Reine Angew. Math.* **127** (1904), 20–50.

Serre, J.-P.

- [62] *Corps Locaux*, Act. Sci. et Ind. 1296, Hermann, Paris, 1962.
- [77] *Linear representations of finite groups*, Springer-Verlag, New York, 1977.

Shimura, G.

- [71] *Introduction to the arithmetic theory of automorphic functions*, Princeton Univ. Press, Princeton, 1971.

Singer, M.

- [70] Invertible powers of ideals over orders in commutative separable algebras, *Proc. Cambridge Phil. Soc.* **67** (1970), 237–242.
- [71] A product theorem for lattices over orders, *Math. Scand.* **29** (1971), 50–54.
- [73] An elementary proof of the invertible powers theorem, *Proc. Cambridge Phil. Soc.* **73** (1973), 289–291.

Small, L.

- [66] Hereditary rings, *Proc. Nat. Acad. Sci. USA* **55** (1966), 25–27.

Srinivasan, B.

- [60] On the indecomposable representations of a certain class of groups, *Proc. London Math. Soc.* (3) **10** (1960), 497–513.

Steinberg, R.

- [56], [57] Prime power representations of finite linear groups I, II, *Canad. J. Math.* **8** (1956), 580–591; **9** (1957), 347–351.
- [62] Complete sets of representations of algebras, *Proc. Amer. Math. Soc.* **13** (1962), 746–747.

Suzuki, M.

- [57] The nonexistence of a certain type of simple group of odd order, *Proc. Amer. Math. Soc.* **8** (1957), 686–695.
- [59] Applications of group characters, *Proc. Symp. Pure Math.*, vol. 1 (*Finite Groups*), Providence, 1959, 88–99.
- [63] On the existence of a Hall normal subgroup, *J. Math. Soc. Japan* **15** (1963), 387–391.

Swan, R. G.

- [60] Induced representations and projective modules, *Ann. of Math.* **71** (1960), 552–578.
- [62] Projective modules over group rings and maximal orders, *Ann. of Math.* **76** (1962), 55–61.
- [63] The Grothendieck ring of a finite group, *Topology* **2** (1963), 85–110.
- [68] *Algebraic K-theory*, Springer Lecture Notes 76, Springer, Berlin, 1968.

Swan, R. G., Evans, E. G.

- [70] *K-theory of finite groups and orders*, Springer Lecture Notes 149, Springer, Berlin, 1970.

Takahashi, S.

- [59] Arithmetic of group representations, *Tôhoku Math. J.* (2) **11** (1959), 216–246.

Tamaschke, O.

- [60] Ring theoretische Behandlung einfach transitiver Permutationsgruppen, *Math. Z.* **73** (1960), 393–408.

- [64a] *S-Ringe und verallgemeinerte Charaktere auf endlichen Gruppen*, *Math. Z.* **84** (1964), 101–119.
- [64b] *S-rings and the irreducible representations of finite groups*, *J. Algebra* **1** (1964), 215–232.
- Theohari-Apostolidi, Th.
- [82] On integral representations of twisted group rings, *J. Algebra* (to appear).
- Thévenaz, J.
- [81a] Representations of finite groups in characteristic p^r , *J. Algebra* (to appear).
- [81b] Representations of groups of order ph in characteristic p^r , *J. Algebra* (to appear).
- Travis, D.
- [74] Spherical functions on finite groups, *J. Algebra* **29** (1974), 65–76.
- Troy, A.
- [61] Integral representations of cyclic groups of order p^2 , Ph.D. thesis, Univ. of Illinois, Urbana, Ill., 1961.
- Tucker, P.
- [62] On the reduction of induced representations of finite groups, *Amer. J. Math.* **84** (1962), 400–420.
- [63] Note on the reduction of induced representations, *Amer. J. Math.* **85** (1963), 53–58.
- [65a] Endomorphism ring of an induced module, *Michigan Math. J.* **12** (1965), 197–202.
- [65b] On the reduction of induced indecomposable representations, *Amer. J. Math.* **87** (1965), 798–806.
- Ullom, S.
- [77] Fine structure of class groups of cyclic p -groups, *J. Algebra* **49** (1977), 112–124.
- van der Waerden, B. L.
- [59] *Algebra II*, 4th ed., Springer, Berlin, 1959.
- [64] *Algebra I*, 6th ed., Springer, Berlin, 1964.
- Wang, S.
- [50] On the commutator group of a simple algebra, *Amer. J. Math.* **72** (1950), 323–334.
- Ward, H. N.
- [68] The analysis of representations induced from a normal subgroup, *Michigan Math. J.* **15** (1968), 417–428.
- Weiss, E.
- [63] *Algebraic number theory*, McGraw-Hill, New York, 1963.
- [69] *Cohomology of groups*, Academic Press, New York, 1969.
- Weyl, H.
- [46] *The classical groups*, 2nd ed., Princeton Univ. Press, Princeton, 1946.
- Wiedemann, A.
- [80] Auslander-Reiten-Graphen von Ordnungen und Blöcke mit zyklischem Defekt zwei, Thesis, Univ. of Stuttgart, 1980.

Wielandt, H.

- [64] *Finite permutation groups*, Academic Press, New York, 1964.

Williamson, S.

- [63] Crossed products and hereditary orders, *Nagoya Math. J.* **23** (1963), 103–120.

Witt, E.

- [52] Die algebraische Struktur des Gruppenringes einer endlichen Gruppe über einem Zahlenkörper, *J. Reine Angew. Math.* **190** (1952), 231–245.

Yamazaki, K.

- [64] On projective representations and ring extensions of finite groups, *J. Fac. Sci. Univ. Tokyo, Sect. I*, **10** (1964), 147–195.

Zassenhaus, H.

- [49] *The theory of groups*, Chelsea, New York, 1949.



INDEX

absolutely indecomposable, 466, 634
absolutely irreducible, 54
absolutely simple module, 54
absolute norm, 80
A. C. C. = ascending chain condition, 40
Adams operators, 316
additive functor, 27
Adjointness Theorem, 26
admissible triple for Green correspondence, 471
a. e. (= almost everywhere), 88
algebraic integer = alg. int., 3, 77
algebraic number field, 77, 92
algebra (over a ring), 1
 of polynomial functions, 328
 of polynomial invariants, 329
alternating group, 363
ambiguous ideal, 596
annihilator, 104, 198, 199
 of Ext, 603
Aramata-Brauer Theorem, 397
Artin Induction Theorem, 378
Artin's Theorem, 171, 602
artinian module, 41
artinian ring, 41
associative form, 196
augmentation ideal, 114, 115, 134, 189
augmentation map, 189
Auslander-Goldman Theorem, 591
Auslander-Rim Theorem, 593
Auslander's Theorem, 570, 571

balanced map, 24
basic set of indecomposable projective modules, 406, 422
basic set of irreducible characters, 202
basic set of simple modules, 52, 422

Bass orders, 776, 782
Bass' Theorem, 776, 783, 786, 788, 790
Berman-Gudivok Theorem, 736
Berman's Theorem, 678, 679
Berman-Witt Theorem, 491, 495, 508
bimodule, 15
binding system, 547
Blichfeldt's Criterion for Imprimitivity, 261
block, 459
Brauer characters, 420, 509
Brauer criterion for virtual characters, 385
Brauer Induction Theorem, 381, 448
Brauer lift, 435, 436
Brauer Splitting Field Theorem, 385
Brauer's Theorem, 265, 397
Brauer-Suzuki Theorem, 366, 392
Burnside ring, 242
Burnside's Theorem, 51, 217, 221
Burnside's Transfer Theorem, 342, 395

CA-group, 353
cancellation, 717, 718
Cartan-Brauer triangle, 427, 431, 505
Cartan homomorphism, 431, 507
Cartan matrix, 431
categorical, 56
categorical property, 71
category, 27
central conductor, 586, 604
central extension, 185, 292
central (primitive) idempotents, 71
central simple K -algebra, 67
centralize, 541
centralizer, 12, 50
 $\text{cf}_K(G)$, 209, 211
 $\text{ch } KG$, 408

- chain, 102
 Change of Rings Theorem, 36, 74, 178
 character, 202, 420, 509
 afforded by a module, 202, 420
 Brauer, 420, 509
 conjugate, 225, 236, 262
 degree of, 202
 exceptional, 357, 363, 485
 faithful, 217
 generalized, 208
 induced, 228, 447, 509
 invariant, 388
 irreducible, 202, 207, 422
 linear, 224
 non-exceptional, 357, 348
 ordinary, 208
 over K , 206, 475
 permutation, 254
 principal, 209
 principal indecomposable, 422
 projective indecomposable, 422
 rational, 377
 regular, 223
 ring, 209, 425
 table, 213, 220, 365, 372, 438, 490
 trivial, 209
 virtual, 208, 380, 385, 424
 characteristic polynomial = char. pol., 4
 characteristic sublattice, 712
 Chinese Remainder Theorem, 78
 class functions, 209
 class group, 658, 659
 class number, 92
 class sum, 53
 Clifford's Theorem, 259, 273, 278
 Clifford system, 267
 cohomology group, 180, 187, 541
 Coleman's Theorem, 678
 commutant, 50
 commutative diagram, 15
 complete (in N -adic topology), 122
 completely primary = local, 111
 completely ramified, 597
 completely reducible, 42
 completion, 83, 87
 complex prime, 83
 composition factors, 41
 composition series, 8, 41
 conductor, 583, 586, 604
 conjugacy class, 12, 492
 conjugate character, 225, 236, 262
 conjugate module, 152, 236
 Conlon's Theorem, 465
 connecting homomorphism, 174, 176
 contragredient character, 246
 contragredient module, 245
 contragredient representation, 246
 contravariant, 16, 27
 convolution, 280
 cosets (left, right, double), 11
 counting norm, 80
 covariant, 16, 27
 cover $>$, 780
 Criterion for Irreducibility of Induced Characters, 245
 crossed homomorphism, 181
 crossed-product algebra, 183, 599
 crossed-product order, 600
 cyclic index, 789
 cyclic module, 86
 cyclotomic field, 94
 cyclotomic polynomial, 94
 Dade's Theorem, 691
 Dade-Taussky-Zassenhaus Theorem, 763
 D. C. C. = descending chain condition, 41
 decomposition group, 599
 decomposition map, 413, 503
 decomposition matrix, 413
 Dedekind domain, 76-78
 defect, 443
 defect group, 459
 degree of a character, 202
 degree of a representation, 525
 deLeeuw's Theorem, 540, 541
 dense ring of linear transformations, 48
 Density Theorem, 48, 541
 derivation, 181, 541
 inner, 541
 principal, 181, 541
 derived group, 8
 derived series, 8
 determinant map, 338
 Diederichsen's Theorem, 550, 729
 Dieudonné determinant, 166
 different, 80, 584, 608
 dihedral characters, 234
 dihedral group, 13, 161, 234
 dimension shifting, 192
 direct sum, 19
 discrete valuation ring, 81
 discrete ring, 81
 discriminant, 80, 81
 discriminant ideal, 89, 560
 double centralizer property, 61
 doubly transitive, 255

- Dress' Theorem, 678
 Drozd-Kirichenko Theorem, 709
 Drozd-Kirichenko-Roiter Theorem, 783,
 790
 Drozd-Roiter Theorem, 697
 Drozd's Theorem, 695
 Drozd-Turčin Theorem, 742
 dual basis, 89, 203
 Dual Basis Lemma, 57
 dual lattices, 89, 245
 dual of lattice, 777
 dual of module, 89, 245, 610, 777
 d. v. r. = discrete valuation ring, 81
 dyad, 640
- Eichler condition, 718
 Eichler lattice, 718
 Eilenberg-Nakayama Theorem, 198
 elementary matrix, 166
 elementary subgroup, 381, 492
 elementary symmetric functions, 314
 equivalent categories, 56
 equivalent extensions, 175, 183
 equivalent representations, 525
 equivalent valuations, 81
 essential monomorphism, 134
 essential surjection, 131
 exact functor, 28
 exact sequence, 14
 exceptional character, 357, 363, 485
 Ext, 172
 extension of character, 388
 extension of groups, 7
 extension of modules, 175, 539
 exterior algebra, 310
 external direct product, 22
 external direct sum, 19
- factor set, 182, 277
 faithful, 50, 643, 660
 faithful character, 217
 faithfully, 523
 faithfully flat, 642
 f. g. = finitely generated, 1
 fibre product, 22
 finite extension of p -modular system, 415
 finite representation type, 686, 710
 finitely presented, 35
 first cohomology group, 541
 flat, 32, 74
 Fong-Swan-Rukolaine Theorem, 513
 fractional ideal, 78, 92
 free basis, 29
- free module, 29
 free resolution, 171
 Frobenius algebra, 197
 Frobenius automorphism, 95
 Frobenius complement, 344
 Frobenius group, 344, 479
 Frobenius kernel, 344
 Frobenius Reciprocity Theorem, 232, 233,
 243, 269
 Frobenius' Theorem, 345
 Frobenius-Schur Theorem, 54
 Fröhlich's Theorem, 759
 full lattice, 84
 function field, 92
 functor, 27
- G_0 , 404
 Gallagher's Theorem, 386, 390
 Gaschütz's Theorem, 449
 Gauss' Lemma, 4, 80
 Gaussian integers, 4
 generalized character, 208
 generalized quaternion group, 13, 163
 generator (of category), 56
 genus, 642, 643
 G -induced module, 191
 G -invariants, 248
 Glauberman's Z^* -Theorem, 370
 global field, 92
 Gorenstein orders, 776, 778
 graded algebra, 267, 309
 Green correspondence, 472
 Green Indecomposability Theorem, 466
 Green's Theorem, 396
 on Vertices, 457
 on Zeros of Characters, 468
 Grothendieck group, 404
 group:
 alternating, 363
 derived, 8
 dihedral, 13, 161, 234
 generalized quaternion, 13, 163
 hyper-octahedral, 304
 metacyclic, 747
 nilpotent, 8
 p -solvable, 9, 513, 684
 quaternion, 13, 251
 solvable, 8
 supersolvable, 9, 303
 symmetric, 9
 group algebra, 1
 group ring, 1, 2
 G -set, 10, 231

- Hall subgroup, 390, 392
 Hasse-Schilling-Maass Norm Theorem, 167
 Hattori's Theorem, 672
 Hecke algebra, 281
 height of p -solvable group, 513
 Heller-Reiner Theorem, 736
 Heller's Theorem, 628, 629
 Hensel's Lemma, 140
 hereditary, 76
 Higman ideal, 603, 608
 Hochschild-Serre-Lyndon spectral sequence, 294, 555
 homogeneous components, 47, 259
 homological dimension, 569
 homology groups, 189
 Hopkin's Theorem, 41, 111
 hyper-characteristic, 792
 hyper-elementary subgroups, 381
- ideal:**
 ambiguous, 596
 fractional, 78, 92
 integral, 78
 inverse, 92, 566
 invertible, 758
 prime, 566
 principal, 92
 ideal class, 85, 92
 ideal class group, 657
 ideal class number, 92
idèle:
 integral, 654
 principal, 653
 unit, 653
 idèle group, 652
 idempotent, 20, 44
 imprimitive, 261
 indecomposable, 127
 index, 167, 285, 585
 $\text{Ind } RG$, 453
 induced character, 228, 447, 509
 induced module, 191, 228, 268
 induction, 228, 333, 447
 Induction Theorems, § 15, § 21
 Aramata-Brauer, 397
 Artin, 378
 Brauer, 381, 448
 Berman-Witt, 491, 495
 Solomon, 382
 inertia group, 599
 inertial degree, 573
- infinite prime, 83
 infinite representation type, 686
 inflation, 294
 injective envelope, 134
 injective hull, 134
 injective module, 30
 injective resolution, 173
 inner automorphism, 11, 68
 inner derivation, 541
 inner tensor product, 239
 integral, 3, 77
 integral closure, 3, 77
 integral dependence, 3
 integral group ring, 2
 integral idèle, 64
 integral representation, 525
 integrally closed, 3, 78
 intersection matrix, 306
 intertwining number, 212, 319
 Intertwining Number Theorem, 244
 invariant character, 388
 Invariant Factor Theorem, 85
 invariant (G -), 184, 224, 248
 inverse different, 80, 584, 608
 inverse ideal, 92, 566
 invertible bimodule, 755
 invertible ideal, 758
 invertible module, 757
 $\text{inv}_G M = G\text{-invariants of } M$, 224, 248
 Irr, 202, 207
 irreducible character, 202, 207
 irreducible projective representation, 302
 isotypic components, 47
 Ito's Theorem, 290
- Jacobinski's Cancellation Theorem, 718
 Jacobinski's conductor formula, 584
 Jacobinski's Theorem, 604, 607, 663, 666, 691, 697, 769, 771
 Jacobson radical, 104
 Janusz's Theorem, 283, 576, 577, 600
 Jones' Theorem, 687, 689, 769, 770
 Jordan-Hölder Theorem, 8, 42
 Jordan-Zassenhaus Theorem, 534, 537
- K_0 , 404
 K -conjugacy class, 492
 K -elementary subgroup, 492
 kernel of a character, 215
 kernel of a representation, 215
 Kronecker-Weierstrass Theorem, 744

- Krull-Schmidt-Azumaya Theorem, 128, 620, 767
- lattice, 84, 245, 522, 524
- Lee's Theorem, 752
- left exact, 28
- left hereditary, 76, 565
- left multiplier ring, 535
- left order, 535, 777
- length of composition series, 41, 42
- lifting idempotents, 123
- lifting (of projective representations), 293
- linear character, 224
- linear representation, 256
- local capacity, 167
- local index, 167
- local ring, 75, 111
- localization, 75, 87
- locally free, 652
- locally free class group, 658, 659
- locally isomorphic, 643
- long exact sequence for Ext, 173
- long exact sequence for Tate cohomology groups, 191
- long exact sequence for Tor, 177
- lower central series, 8
- Mackey Subgroup Theorem, 237
- Mackey Tensor Product Theorem, 240
- Mackey's Theorem, 320
- Maranda's Theorem, 624, 629, 630, 658
- Maschke's Theorem, 42, 543, 601
- matrix coordinate functions, 53
- maximal condition, 40
- maximal order, 559
- maximal submodule, 101
- M -group, 262
- metacyclic group, 747
- method of little groups, 265
- minimal left ideal, 110
- minimal polynomial = min. pol., 4
- minimum condition, 41
- Möbius μ -function, 378
- module of quotients, 74
- Molien's Theorem, 329
- monic, 3
- monomial representation, 256, 262
- Morita context, 60
- Morita equivalence, 56
- Morita's Theorem, 60
- morphism, 27
- multiplicative subset, 73
- multiplicity, 211
- multiplier ring, 535
- N -adic topology, 122
- Nakayama formulas, 447
- Nakayama's Lemma, 105, 620
- Nakayama-Matsushima Theorem, 168
- natural, 18
- natural equivalence of functors, 55
- natural transformation, 55
- Newton's identities, 314
- nil ideal, 109
- nilpotent, 109
- nilpotent group, 8
- Noether-Deuring Theorem, 139
- noetherian module, 40
- noetherian ring, 40
- non-archimedean, 81
- non-exceptional character, 357, 485
- norm, 5, 79, 158
- normal complement, 392
- normal decomposition, 790
- normal p -complement, 9, 341
- normal series, 8
- normalized factor set, 601
- normalizer, 12
- normally indecomposable, 790
- $O_l(M)$, $O_r(M)$, 535
- orbit, 10
- order, 523, 524
- Bass, 776, 782
 - Gorenstein, 776, 778
 - hereditary, 565
 - left, 535, 777
 - maximal, 559
 - right, 535, 777
- order ideal, 86
- ordinary character, 208
- orthogonal idempotents, 20, 119
- orthogonality relations, 206, 209, 213, 288, 439
- outer tensor product, 239, 249
- P -adic completion, 83
- P -adic topology, 83
- P -adic valuation, 82
- p -element, Π -element, 9, 386, 402
- p' -element, Π' -element, 9, 386, 402
- p -irregular, Π -irregular, 386, 402
- p -local structure, 401
- p -modular system, 402, 414
- p -part, 386, 403

p -rational character, 518
 p -regular, Π -regular, 386, 402
 p -regular part, 403
 p -solvable group, 9, 513, 684
 permutation character, 10, 254
 permutation representation, 10
 Pierce decomposition, 140, 523
 power sums, 314
 Primary Decomposition Theorem, 93
 primary ring, 126
 primary submodule, 93
 prime ideal, 566
 prime of K , 81, 83
 primitive central idempotent, 71
 primitive idempotent, 71, 119
 primitive module, 261
 primitive root, 769
 principal character, 209
 principal derivation, 181
 principal factor set, 182
 principal ideal, 92
 principal idèle, 653
 progenitor, 60
 projection maps, 20
 projective class group, 404
 projective cover, 131
 projective endomorphism, 609
 projective general linear group, 292
 projective lifting property, 293
 projective module, 29
 projective representation, 277, 292
 projective resolution, 172
 properly irregular prime, 741
 pullback, 22
 pure, 84, 526
 purely inseparable, 156
 Pu's Theorem, 751
 pushout, 21

 quasi-Frobenius, 135, 199
 quaternion group, 13, 163, 251
 quaternions, 160

 radical of module, 102
 radical of ring, 104
 ramification index, 79, 573
 ramified, 79, 80, 167, 594

- tamely, 100, 101, 595

 rank, 84, 239

- rank element, 674

 rational character, 377

- Π

 R -composition factors, 533, 549

- Π

 real prime, 83

- Π

reduced characteristic polynomial, 159
 reduced norm, 159, 167
 reduced trace, 159
 Ree's Theorem, 284
 regular character, 223
 regular module, 6, 197
 regular prime, 741
 regular representation, 6
 Reiner's Theorem, 607, 613, 621, 635, 637, 718, 740
 Reiner-Zassenhaus Theorem, 631
 related extension, 134
 relative injective, 449
 relative projective, 449, 470
 relatively prime, 78
 representation equivalence of categories, 702
 representation group, 299
 residue class degree, 79
 restriction, 227, 228, 294
 resultant, 552
 RG -lattice, 245
 right exact, 28
 right order, 535, 777
 Rim's Theorem, 593
 ring of quotients, 74
 ring of virtual characters, 209
 R -lattice, 84, 245, 522
 Roggenkamp's Theorem, 614, 772
 Roiter's Lemma, 642, 645
 Roiter's Theorem, 660, 663, 666, 786
 R -representation, 525
 R -singular element, 679

 SA -group, 354
 saturated, 527
 saturated submodule, 527
 Schanuel's Lemma, 30
 Schur index, 585
 Schur's Lemma, 44
 Schur multiplier, 299
 Schur's Theorem, 530
 Schur-Zassenhaus Theorem, 185
 section, 182, 185
 self-congradient, 247
 self-injective, 135, 199
 semidirect product, 7
 semilocal, 115
 semiperfect ring, 132
 semisimple module, 42
 semisimple ring, 44, 111
 separable algebra, 142
 separable extension field, 143

separable module, 142
 short exact sequence, 14, 403
 signature, 783
 simple artinian ring (structure theorem),
 48, 50, 64
 simple K -algebra, 67
 simple module, 41
 simple ring, 47
 skew-symmetric tensor, 311, 319
 Skolem-Noether Theorem, 69
 Snake Lemma, 37
 socle, 136
 Solomon's Theorem, 382
 solvable group, 8
 source, 455
 special classes, 348
 spectral sequence, 294, 555
 split extension of groups, 7
 split semisimple K -algebra, 52
 split sequence, 14
 splitting field, 149, 155, 385
 stable isomorphism, 659
 stable module, 269
 stabilizer, 10, 259, 262
 standard basis elements, 286
 standard isomorphism, 716
 Steinberg character, 443
 S -rings (Schur algebras), 281
 Steinitz class, 85, 727, 728
 Steinitz' Theorem, 85
 Strong Approximation Theorem, 79
 subdegrees, 239, 285
 Subgroup Theorem, 237
 sufficiently large field, 417
 supersolvable group, 9, 303
 Suzuki's Theorem, 351, 353
 Swan's Theorem, 671, 676, 680, 684
 symmetric algebra, 198, 309
 symmetric form, 196
 symmetric tensor, 310, 319
 symmetry operator, 312
 tamely ramified, 100, 101, 595
 Tate cohomology group, 187, 188, 190
 tensor algebra, 309
 tensor induction, 333
 tensor product, 23, 239
 Tensor Product Theorem, 240, 249
 T. I. (trivial intersection) set, 354
 Tor, 177
 torsion module, 86, 93
 torsion submodule, 73, 74, 84
 torsionfree, 74, 84, 522
 totally definite quaternion algebra,
 718
 trace map, 5, 79, 158, 673
 transfer, 335, 336
 transgression, 294
 transitive, 10, 255
 Transitivity of Induction, 231
 trivial character, 209
 trivial G -module, 184
 trivial intersection set, 354
 trivial representation, 209
 trivial submodule, 184, 224
 twisted group algebra, 161, 183, 268, 589
 twisted group ring, 268, 589
 type (of hereditary order), 577
 unit, 106
 unit idèle, 653
 universal central extension, 293, 296
 unramified, 79, 81, 167, 594, 595
 upper central series, 8
 value group, 81
 valuation, 81
 valuation ring, 81
 vertex, 455
 virtual characters, 208, 380, 424, 493
 ring of, 209, 425, 493
 Wang-Platonov Theorem, 168
 weakly injective, 778, 791
 weakly self-injective, 779
 Wedderburn components, 48
 Wedderburn's Theorem (on nilpotent
 ideals), 469
 Wedderburn's Theorems (on simple and
 semisimple rings), 47, 48, 50, 64
 Williamson's Theorem, 600-602
 Witt-Berman Theorem, 491, 495,
 508
 wreath product, 305, 331

