

---

# **REPRESENTATION THEORY OF FINITE GROUPS AND ASSOCIATIVE ALGEBRAS**

**CHARLES W. CURTIS**

UNIVERSITY OF OREGON

**IRVING REINER**

UNIVERSITY OF ILLINOIS

---

**INTERSCIENCE PUBLISHERS**

a division of John Wiley & Sons, NEW YORK • LONDON • SYDNEY

10 9 8 7 6

Copyright © 1962 by JOHN WILEY & SONS, INC.

ALL RIGHTS RESERVED—Reproduction in whole or in part for any purpose  
of the United States Government will be per-  
mitted.

Library of Congress Catalog Card Number 62-16994

ISBN 0 470 18975 4

## Preface

Representation theory is the study of concrete realizations of the axiomatic systems of abstract algebra. It originated in the study of permutation groups, and algebras of matrices. The theory of group representations was developed in an astonishingly complete and useful form by Frobenius in the last two decades of the nineteenth century. Both Frobenius and Burnside realized that group representations were sure to play an important part in the theory of abstract finite groups. The first book to give a systematic account of representation theory appeared in 1911 (Burnside [4]) and contained many results on abstract groups which were proved using group characters. Perhaps the most famous of these is Burnside's theorem that a finite group whose order has at most two distinct prime divisors must be solvable. Recently, a purely group-theoretic proof of Burnside's theorem has been obtained by Thompson. The new proof is of course important for the structure theory of groups, but it is at least as complicated as the original proof by group characters.

The second stage in the development of representation theory, initiated by E. Noether [1] in 1929, resulted in the absorption of the theory into the study of modules over rings and algebras. The representation theory of rings and algebras has led to new insights in the classical theory of semi-simple rings and to new investigations of rings with minimum condition centering around Nakayama's theory of Frobenius algebras and quasi-Frobenius rings.

Another major development in representation theory is R. Brauer's work on modular representations of finite groups. Like the original work of Frobenius, Brauer's theory has many significant applications to the theory of finite groups. At the same time it draws on the representation theory of algebras and suggests new problems on modules and rings with minimum condition. It also emphasizes the fundamental importance of number-theoretical questions in group theory and representation theory.

During the past decade there has been increased emphasis on integral representations of groups and rings, motivated to some extent by questions arising from homological algebra. This theory of integral representations has been a fruitful source of problems

and conjectures both in homological algebra and in the arithmetic of non-commutative rings.

The purpose of this book is to give, in as self-contained a manner as possible, an up-to-date account of the representation theory of finite groups and associative rings and algebras. This book is not intended to be encyclopedic in nature, nor is it a historical listing of the entire theory. We have instead concentrated on what seem to us to be the most important and fruitful results and have included as much preliminary material as necessary for their proofs.

In addition to the classical work given in Burnside's book [4], we have paid particular attention to the theory of induced characters and induced representations, quasi-Frobenius rings and Frobenius algebras, integral representations, and the theory of modular representations. Much of this material has heretofore been available only in research articles. We have concentrated here on general methods and have built the theory solidly on the study of modules over rings with minimum condition. Enough examples and problems have been included, however, to help the research worker who needs to compute explicit representations for particular groups. We have included some applications of group representations to the structure theory of finite groups, but a definitive account of these applications lies outside the scope of this book. In Section 92 we have given a survey of the present literature dealing with these applications and have included in this book all the representation-theoretic prerequisites needed for reading this literature, though not all the purely group-theoretic background which might be necessary.

No attempt has been made to orient the reader toward physical applications. For these we may refer the reader to recent books and articles dealing with that part of group theory relevant to physics, and in particular to Wigner [1], Gelfand-Sapiro [1], Lomont [1], and Boerner [1].

It has also been necessary to omit the vast literature on representations of the symmetric group. Fortunately the reader is now able to consult the excellent book on this topic by Robinson [1].

Many of the results on group representations have been generalized to infinite groups and also to infinite-dimensional representations of topological groups. We have felt that these generalizations do not properly fall within the scope of this book and, in fact, would require a lengthy separate presentation.

The book has been written in the form of a textbook; a preliminary

version has been used in several courses. We have assumed that the reader is familiar with the following topics, which are usually treated in a "standard" first-year graduate course in algebra: elementary group theory, commutative rings, elementary number theory, rudiments of Galois theory, vector spaces, and linear transformations.

We are confident that the expert as well as the student will find something of interest in this book. We offer no apology, however, for writing to be understood by a reader unfamiliar with the subject. In keeping with this objective, we have not always presented results in their greatest generality, and we have included details which will sometimes seem tedious to the experienced reader. After serious deliberation, we decided not to introduce the full machinery of homological algebra. Although it would have simplified several sections of the book, we felt that many readers were not likely to be well-grounded in homological algebra, and this book was not intended to be a first course in the subject.

The first three chapters are written at the level of a first-year graduate course and include introductory material as well as background for later chapters. Much of this material may be skimmed rapidly or omitted entirely at a first reading, though Sections 9-13 should be read with care.

Chapters IV-VII form a unit containing the structure theory of semi-simple rings with minimum condition, and the applications of this theory to group representations and characters.

Chapters IV, VIII, IX, and X form a unit on rings with minimum condition and finite-dimensional algebras. Chapter IV develops the theory of the radical and semi-simplicity by the perhaps old-fashioned method of calculations with idempotents, because idempotents furnish the main tool in the study of non-semi-simple rings and algebras in Chapters VIII and IX.

Chapters III and XI form a more or less self-contained account of algebraic number theory and integral representations of groups. Some knowledge of earlier chapters is needed, especially in Sections 77-78.

Chapter XII is devoted to the theory of modular representations and requires a knowledge of parts of all the preceding chapters. The exact prerequisites for reading Chapter XII are given at the beginning of the chapter.

For the reader whose main interest is in representations of finite groups, we may suggest the following sections for a first brief reading: 9-13, 23-27, 30-34, 38-40, 43-46, 49-50, 54-55, 61, 82-92.

These sections are to some extent self-contained, provided that the reader is willing to postpone to the second reading the proofs of some of the results needed from other sections.

Exercises are included at the end of almost every section. Some provide easy checks on the reader's comprehension of the text; others are intended to challenge his abilities. Many are important results in their own right and may occasionally be referred to when needed in later sections.

Sections are numbered consecutively throughout the book. A cross reference to (a.b) refers to Section a and to the bth numbered item in that section.

There is a fairly large bibliography of works which are either directly relevant to the text or offer supplementary material of interest. An attempt has been made to give credit for some of the major methods and theorems, but we have stopped far short of trying to trace each theorem to its source.

We are indebted to many persons and organizations for assisting us with this work. Our students, friends, colleagues, and families have listened to us lecture on these subjects, read portions of the manuscript and proof sheets, made suggestions and corrections, and given us encouragement. We are deeply appreciative of their kind help. Our interest in this subject was stimulated by a seminar conducted at the Institute for Advanced Study in 1954-1955. We are indebted to the participants in that seminar for their help and to the Institute for making possible the preparation of mimeographed seminar notes. It is a pleasure to acknowledge the generous support we have received for the work on this book from the Office of Naval Research. Finally we are grateful to Interscience Publishers for publishing it and giving us their patient and friendly cooperation.

Charles W. Curtis  
Irving Reiner

June 1962

# Contents

<b>Notation .....</b>	xiii
<b>I. Background from Group Theory .....</b>	1
1. Permutation Groups and Orbit.....	1
2. Subgroups and Factor Groups .....	3
3. Conjugate Classes .....	8
4. Abelian Groups .....	10
5. Solvable and Nilpotent Groups .....	14
6. Sylow Subgroups.....	17
7. Semi-direct Products .....	21
<b>II. Representations and Modules .....</b>	25
8. Linear Transformations .....	26
9. Definitions and Examples of Representations .....	30
10. Representations of Groups and Algebras .....	38
11. Modules .....	50
12. Tensor Products .....	59
13. Composition Series.....	76
14. Indecomposable Modules .....	81
15. Completely Reducible Modules .....	86
<b>III. Algebraic Number Theory .....</b>	91
16. Modules over Principal Ideal Domains .....	91
17. Algebraic Integers .....	102
18. Ideals .....	107
19. Valuations; $P$ -adic Numbers .....	115
20. Norms of Ideals; Ideal Classes .....	123
21. Cyclotomic Fields .....	135
22. Modules over Dedekind Domains .....	144
<b>IV. Semi-simple Rings and Group Algebras .....</b>	157
23. Preliminary Remarks .....	157
24. The Radical of a Ring with Minimum Condition .....	159
25. Semi-simple Rings and Completely Reducible Modules .....	163
26. The Structure of Simple Rings .....	173
27. Theorems of Burnside, Frobenius, and Schur .....	179
28. Irreducible Representations of the Symmetric Group ..	190

29. Extension of the Ground Field .....	198
<b>V. Group Characters .....</b>	<b>207</b>
30. Introduction .....	207
31. Orthogonality Relations .....	217
32. Simple Applications of the Orthogonality Relations....	224
33. Central Idempotents .....	233
34. Burnside's Criterion for Solvable Groups .....	239
35. The Frobenius-Wielandt theorem on the Existence of Normal Subgroups in a Group .....	241
36. Theorems of Jordan, Burnside, and Schur on Linear Groups.....	250
37. Units in a Group Ring.....	262
<b>VI. Induced Characters .....</b>	<b>265</b>
38. Introduction .....	265
39. Rational Characters .....	279
40. Brauer's Theorem on Induced Characters .....	283
41. Applications .....	292
42. The Generalized Induction Theorem .....	301
<b>VII. Induced Representations .....</b>	<b>313</b>
43. Induced Representations and Modules .....	314
44. The Tensor Product Theorem and the Intertwining Number Theorem .....	323
45. Irreducibility and Equivalence of Induced Modules ....	328
46. Examples: The Tetrahedral and Octahedral Groups ..	329
47. Applications: Representations of Metacyclic Groups ..	333
48. A Second Application: Multiplicity-free Representations .....	340
49. The Restriction of Irreducible Modules to Normal Subgroups .....	342
50. Imprimitive Modules.....	346
51. Projective Representations .....	348
52. Applications .....	355
53. Schur's Theory of Projective Representations .....	358
<b>VIII. Non-Semi-Simple Rings .....</b>	<b>367</b>
54. Principal Indecomposable Modules .....	367
55. The Classification of the Principal Indecomposable Modules into Blocks .....	377
56. Projective Modules.....	380

57. Injective Modules .....	384
58. Quasi-Frobenius Rings .....	393
59. Modules over Quasi-Frobenius Rings .....	403
<b>IX. Frobenius Algebras .....</b>	<b>409</b>
60. Injective Modules for a Finite-Dimensional Algebra ..	409
61. Frobenius and Quasi-Frobenius Algebras .....	413
62. Projective and Injective Modules for a Frobenius Algebra .....	420
63. Relative Projective and Injective Modules .....	426
64. Group Algebras of Finite Representation Type.....	431
65. The Vertex and Source of an Indecomposable Module	435
66. Centralizers of Modules over Symmetric Algebras ....	440
67. Irreducible Tensor Representations of $GL(V)$ .....	449
<b>X. Splitting Fields and Separable Algebras .....</b>	<b>453</b>
68. Splitting Fields for Simple Algebras and Division Algebras .....	453
69. Separable Extensions of the Base Field .....	459
70. The Schur Index.....	463
71. Separable Algebras.....	480
72. The Wedderburn-Malcev Theorem .....	485
<b>XI. Integral Representations.....</b>	<b>493</b>
73. Introduction .....	494
74. The Cyclic Group of Prime Order .....	506
75. Modules over Orders.....	515
76. $P$ -Integral Equivalence .....	531
77. Projective Modules: Local Theory.....	542
78. Projective Modules: Global Theory .....	550
79. The Jordan-Zassenhaus Theorem .....	558
80. Order Ideals .....	563
81. Genus .....	567
<b>XII. Modular Representations .....</b>	<b>583</b>
82. Introduction .....	584
83. Cartan Invariants and Decomposition Numbers .....	590
84. Orthogonality Relations .....	598
85. Blocks .....	604
86. The Defect of a Block .....	611
87. Defect Groups .....	618
88. Block Theory for Groups with Normal $P$ -Subgroups ..	627

89.	Block Distribution of Classes.....	635
90.	Miscellaneous Topics.....	638
	A. Generalized Decomposition Numbers .....	638
	B. Conjugate Characters .....	641
	C. The Number of Characters Belonging to a Block..	643
	D. Numerical Bounds .....	645
91.	Examples .....	646
92.	Literature on Applications to Group Theory .....	650
	A. Groups of a Given Order .....	651
	B. Characterizations of Simple Groups .....	652
	C. Criteria for Existence of Normal Subgroups .....	654
<b>Bibliography .....</b>		655
<b>Index.....</b>		673

## Notation

$Z$	= ring of rational integers
$Q$	= rational field
$a b$	: $a$ divides $b$ where $a, b \in Z$
$a \nmid b$	: $a$ does not divide $b$ , ( $a, b \in Z$ )
$p^n a$	: $p^n a$ but $p^{n+1} \nmid a$ where $p$ is prime and $a \in Z$
G.C.D.	: greatest common divisor
L.C.M.	: least common multiple

### Group theory notation

$[G : 1]$	= number of elements in $G$
$[G : H]$	= number of distinct left cosets of $H$ in $G$
$H \triangle G$	: $H$ is a normal subgroup of $G$
$[x]$	= cyclic group generated by $x$
$S_n$	= symmetric group on $n$ symbols
$P(X)$	= group of all permutations of a set $X$
$C(G)$	= center of the group $G$
$C(x)$	= centralizer of $x$ in $G$
$C_G(H)$	= centralizer of $H$ in $G$
$N(H)$	= normalizer $H$ in $G$
$A(G)$	= group of automorphisms of $G$
$I(G)$	= group of inner automorphisms of $G$
$G_1 \times G_2$	= direct product of $G_1$ and $G_2$
$a_L$	: denotes the left multiplication: $x \rightarrow ax$
$G_1 \cong G_2$	: $G_1$ is isomorphic to $G_2$
$[G, G]$	= commutator subgroup of $G$

### Notations from field theory

$\text{char } K$	= characteristic of the field $K$
$\text{Irr } (\alpha, K)$	= minimal polynomial of $\alpha$ over $K$
$\text{alg. int. } \{K\}$	= ring of all algebraic integers in $K$

### Notations from module theory and linear algebra

${}_R R$	= left regular $R$ -module
$M + N$	: external direct sum

$M \oplus N$	: internal direct sum
$\Sigma \oplus M_i$	: direct sum
A.C.C.	: ascending chain condition
D.C.C.	: descending chain condition
$f N$	: restriction of $f$ to the subset $N$ of the domain of $f$
$\text{Hom}_R(M, N)$	= additive group of $R$ -homomorphisms of $M$ into $N$
$D_n$	= ring of all $n \times n$ matrices with entries in $D$
$(M:K)$	= dimension of $M$ over $K$
${}^t X$	= transpose of the matrix $X$
$ X $	= $\det X$ = determinant of the matrix $X$
$0$	= zero matrix
$I$	= identity matrix
$\text{diag}\{a_1, \dots, a_n\}$	= diagonal matrix with diagonal entries $a_1, \dots, a_n$
$GL_n(K)$	= group of invertible matrices in $K_n$ , $K$ = field
$GL(M)$	= group of invertible elements in $\text{Hom}_K(M, M)$ , $M$ = vector space over field $K$
$M \otimes_R N$	= tensor product of right $R$ -module $M$ and left $R$ -module $N$
$T \times U$	= Kronecker product of matrices
$M^g$	= induced module
$T^g$	= induced representation

## CHAPTER I

### Background from Group Theory

We presuppose a knowledge of elementary group theory, such as that which may be obtained from reading introductory material in any of the following references: M. Hall [2], Kurosh [1], Ledermann [1], or Speiser [2]. In this chapter, some purely group-theoretical results are collected which will serve to motivate the later discussion, to suggest problems which the theory of group representations might hope to solve, and to develop concepts and theorems needed for the later chapters.

#### § 1. Permutation Groups and Orbits

A *permutation* of a set  $X$  is a one-to-one mapping of  $X$  onto itself. As is well known, the set of all permutations of  $X$  forms a group  $P(X)$ , in which the product  $\sigma\tau$  of a pair of permutations  $\sigma, \tau$  is defined by

$$(\sigma\tau)x = \sigma(\tau x), \quad x \in X.$$

If  $X$  contains more than two elements,  $P(X)$  is not commutative. Any subgroup of  $P(X)$  is called a *permutation group on  $X$* , or a group of permutations of  $X$ . We shall say that the permutations in  $P(X)$  *act* or *operate* on the elements of  $X$ .

A permutation group  $G$  on  $X$  gives rise to a partitioning of  $X$  into disjoint subsets. The importance of this simple idea for mathematics can scarcely be overstated. We begin by defining an equivalence relation in  $X$  as follows: We say that  $x$  is  *$G$ -equivalent* to  $y$  and write  $x \sim y$ , provided that

$$\sigma x = y \quad \text{for some } \sigma \in G.$$

It is easily verified that  $G$ -equivalence is indeed an equivalence relation. The equivalence classes of  $X$  under this relation are called the *orbits* in  $X$  relative to  $G$ . These orbits are disjoint subsets of  $X$  whose union is  $X$ . Thus  $x$  and  $y$  belong to the same orbit if

and only if  $\sigma x = y$  for some  $\sigma \in G$ . If there is only one orbit in  $X$  relative to  $G$ , we say that  $G$  is *transitive* on  $X$ . Clearly,  $P(X)$  acts transitively on  $X$ ; it is easy to see by an example that proper subgroups of  $P(X)$  may also act transitively on  $X$ .

To get some geometric examples of orbits, the reader may consider the set  $X$  of all points in the complex plane. If, on the one hand,  $G$  is the group of all rotations about the origin, the orbits in  $X$  relative to  $G$  are the concentric circles about the origin. If, on the other hand,  $u_0$  is a fixed non-zero vector and  $G$  is taken to be the set of all translations

$$x \rightarrow x + au_0, \quad a \text{ real},$$

the orbit containing a complex number  $x$  consists of all points on the line through  $x$  parallel to  $u_0$ .

Given a permutation group  $G$  on  $X$ , an equally important concept is that of *invariance* relative to  $G$ . A subset  $Y$  of  $X$  is called *invariant* relative to  $G$  if, for each  $\sigma \in G$ ,  $\sigma(Y) \subset Y$ . An element  $x \in X$  is invariant relative to  $G$  if and only if the orbit of  $x$  contains only  $x$ ; an orbit consisting of a single element is called *trivial*.

As a first application of the concept of orbits, consider the symmetric group  $S_n$  defined as the group of all permutations of the set  $X = \{1, 2, \dots, n\}$ . Let  $[\pi]$  denote the cyclic group generated by an element  $\pi \in S_n$ . We call  $\pi$  a *cycle* if  $X$  has only one non-trivial orbit relative to  $[\pi]$ . Each cycle  $\pi$  cyclically permutes the elements in its non-trivial orbit; hence it may be written as

$$\pi = (y \ \pi y \ \pi^2 y \cdots \pi^{q-1} y)$$

where  $q$  is the smallest positive integer such that  $\pi^q = 1$ .

Two cycles  $\pi_1, \pi_2 \in S_n$  are called *disjoint* if their non-trivial orbits are disjoint. It is easily seen that disjoint cycles commute with each other. Using this fact, we show

(1.1) **THEOREM.** *Every permutation  $\sigma \in S_n$ ,  $\sigma \neq 1$ , is expressible as a product of disjoint cycles. This expression is unique up to order of occurrence of the factors.*

**PROOF.** Let  $X_1, \dots, X_m$  be the distinct orbits of  $[\sigma]$ . Define for each  $i$ ,  $1 \leq i \leq m$ , a cycle  $\pi_i$  which acts in the same way as  $\sigma$  on  $X_i$  and as the identity on the rest of  $X$ . (We must agree to set  $\pi_i = 1$  if  $X_i$  consists of a single element, and still refer to  $\pi_i$  as a cycle.) We find at once that

$$\sigma = \pi_1 \cdots \pi_m,$$

a product of disjoint cycles.

To prove the uniqueness, suppose also that  $\sigma = \tau_1 \cdots \tau_q$  is a product of disjoint cycles, and let  $X'_i$  be the non-trivial orbit of  $\tau_i$ . Then the  $\{X'_i\}$  give the orbits of  $\sigma$ ; hence they are just a rearrangement of the  $\{X_i\}$ . Permuting the  $\{\tau_i\}$ , we may assume  $X'_1 = X_1, \dots, X'_m = X_m, q = m$ . Then, for each  $i$ ,  $1 \leq i \leq m$ ,  $\tau_i$  and  $\pi_i$  both act as  $\sigma$  on  $X_i$ , and each is the identity on the complement of  $X_i$  in  $X$ . Hence  $\tau_i = \pi_i$  for each  $i$ .

We remark finally that  $\pi\rho$  means “first  $\rho$ ; then  $\pi$ ,” so that, for example,

$$(432)(412)(51)(123)(531) = (14).$$

## § 2. Subgroups and Factor Groups

We apply the principles of orbit decomposition and invariance to the case where the set upon which the permutations act is itself a group  $G$ . We shall single out various subgroups of the full permutation group  $P(G)$  and study orbits and invariance relative to these subgroups.

For any element  $a \in G$ , let  $a_L \in P(G)$  be the mapping

$$a_L: x \rightarrow ax, \quad x \in G.$$

Call this map a *left multiplication* of  $G$ ; the set of all left multiplications forms a subgroup  $G_L$  of  $P(G)$ , by virtue of

$$a_L b_L = (ab)_L, \quad a_L^{-1} = (a^{-1})_L, \quad a, b \in G.$$

Cayley's theorem asserts that the map  $a \rightarrow a_L, a \in G$ , is an isomorphism of  $G$  onto  $G_L$ .

Analogously, define for  $a \in G$  the map

$$a_R: x \rightarrow xa, \quad x \in G.$$

Then  $a \rightarrow a_R, a \in G$ , gives an anti-isomorphism of  $G$  onto the subgroup  $G_R$  of  $P(G)$ . We note also that

$$a_L b_R = b_R a_L, \quad a, b \in G.$$

Now let  $H$  be a subgroup of  $G$ , and let  $H_L$  and  $H_R$  be the sets of left and right multiplications determined by the elements of  $H$ .

(2.1) DEFINITION. The orbits of  $G$  relative to  $H_L$  are called *right cosets* of  $H$  in  $G$ , those relative to  $H_R$ , *left cosets*.

In order to determine the cosets more explicitly, it is convenient

to define multiplication of subsets  $A$  and  $B$  of  $G$  by

$$AB = \{ab : a \in A, b \in B\}.$$

Likewise, define

$$A^{-1} = \{a^{-1} : a \in A\}.$$

Now let  $x \in G$ ; the orbit of  $G$  relative to  $H_R$  containing  $x$  is then  $xH$ . Similarly, the right coset containing  $x$  is  $Hx$ . Since cosets are orbits, any two left cosets either are disjoint or coincide. If  $xH$  and  $yH$  are left cosets, the equation

$$(yx^{-1})_L xH = yH$$

shows that  $xH$  and  $yH$  have the same cardinal number. If  $G$  is a finite group, we can decompose  $G$  into a union of disjoint left cosets, say,

$$(2.2) \quad G = x_1 H \cup x_2 H \cup \cdots \cup x_r H.$$

The number  $r$  of distinct left cosets of  $H$  in  $G$  is called the *index of  $H$  in  $G$*  and is denoted by  $[G : H]$ . In keeping with this notation, we use  $[G : 1]$  to denote the number of elements in  $G$ . From (2.2) we deduce Lagrange's theorem:

$$(2.3) \quad [G : 1] = [G : H][H : 1].$$

The one-to-one mapping  $g \rightarrow g^{-1}$ ,  $g \in G$ , carries the left coset  $xH$  onto the right coset  $Hx^{-1}$  and effects a one-to-one transformation of the collection of left cosets onto the collection of right cosets. Therefore  $[G : H]$  is also the number of distinct right cosets of  $H$  in  $G$ .

More generally, let  $H$  and  $K$  be a pair of subgroups of  $G$ . Because

$$h_L k_R = k_R h_L, \quad h \in H, k \in K,$$

it follows that  $H_L K_R$  is a subgroup of  $P(G)$ . The orbits of  $G$  relative to  $H_L K_R$  are called the  $(H, K)$ -double cosets in  $G$ . Being orbits, distinct double cosets are disjoint. The  $(H, K)$ -double coset containing  $x$  is just  $HxK$ . A finite group  $G$  also has a decomposition into disjoint double cosets, say,

$$G = Hx_1 K \cup \cdots \cup Hx_s K.$$

However, as we shall see, different double cosets may have different cardinal numbers. For example, let

$$G = S_3, \quad H = \{1, (12)\}, \quad K = \{1, (13)\}.$$

Then the  $(H, K)$ -double cosets in  $G$  are

$$H \cdot 1 \cdot K = \{1, (12), (13), (132)\},$$

$$H \cdot (23) \cdot K = \{(23), (123)\}.$$

In general, the number of double cosets need not divide  $[G:1]$ .

As our next application of orbits and invariance, we shall consider the automorphisms of a group  $G$ . An *automorphism* of  $G$  is an element  $\alpha \in P(G)$  such that

$$\alpha(xy) = \alpha(x)\alpha(y), \quad x, y \in G.$$

Thus  $\alpha$  is an isomorphism of  $G$  onto  $G$ . The set of all automorphisms forms a subgroup  $A(G)$  of  $P(G)$ . Contained in  $A(G)$  are the inner automorphisms  $\{i_a, a \in G\}$ , defined by

$$i_a: x \rightarrow axa^{-1}, \quad x \in G.$$

We have

$$i_a i_b = i_{ab}, \quad i_a^{-1} = i_{a^{-1}}, \quad a, b \in G,$$

which shows that the set  $I(G)$  of all inner automorphisms of  $G$  is a subgroup of  $A(G)$ .

(2.4) DEFINITION. A subgroup  $H$  of  $G$  which is invariant relative to  $I(G)$  is called a *normal subgroup* of  $G$  (notation:  $H \triangle G$ ).

In other words;  $H$  is normal in  $G$  if and only if

$$aHa^{-1} \subset H \quad \text{for all } a \in G.$$

This assertion is easily seen to be equivalent to the statement

$$aHa^{-1} = H, \quad a \in G,$$

and this, in turn, to the important relation

$$aH = Ha, \quad a \in G.$$

Thus  $H$  is normal in  $G$  if and only if every right coset is a left coset, and vice versa.

If  $H$  is a normal subgroup of  $G$ , we have

$$(xH)(yH) = xyH, \quad x, y \in G,$$

and it follows that, relative to set multiplication, the cosets of  $H$  in  $G$  form a group. This group is called the *factor group* of  $G$  over  $H$  and is denoted by  $G/H$ . If  $G/H$  is a finite group, the number of elements in it is  $[G:H]$ , the index of  $H$  in  $G$ . If  $G$  is a finite group we have at once from (2.3)

$$[G/H : 1] = [G : H] = [G : 1]/[H : 1].$$

We recall that a *homomorphism* of a group  $G$  into a group  $G'$  is a mapping  $f: G \rightarrow G'$  such that

$$f(xy) = f(x)f(y), \quad x, y \in G.$$

Because of the manner in which multiplication in a factor group  $G/H$  is defined, it is clear that the mapping  $x \mapsto xH$  of  $G$  onto  $G/H$  is a homomorphism, called the *natural* or *canonical homomorphism* of  $G$  onto  $G/H$ , and that the normal subgroup  $H$  can be characterized as the set of all elements of  $G$  mapped onto the identity element of  $G/H$  under this homomorphism.

The next theorem asserts, among other things, that every homomorphism arises in this way.

(2.5) **THEOREM (Fundamental Theorem on Homomorphisms).** *Let  $f: G \rightarrow G'$  be a homomorphism of  $G$  onto a group  $G'$ . Then*

$$H = \{x \in G : f(x) = 1\}$$

*is a normal subgroup of  $G$  called the kernel of  $f$ . The mapping*

$$xH \rightarrow f(x)$$

*is an isomorphism of  $G/H$  onto  $G'$ . There is a one-to-one inclusion-preserving correspondence between the set of all subgroups  $K'$  of  $G'$  and the subgroups  $K$  of  $G$  containing  $H$ , given by*

$$K \rightarrow f(K) = K', \quad K = f^{-1}(K').$$

*Moreover,  $K \triangle G$  if and only if  $K' \triangle G'$ . If  $K \triangle G$ , we have*

$$(2.6) \quad G/K \cong G'/K' \cong (G/H)/(K/H).$$

We assume that this result is familiar to the reader and omit the proof.

(2.7) **DEFINITION.** The *center* of the group  $G$  is the subgroup

$$C(G) = \{x \in G : xa = ax \text{ for all } a \in G\}.$$

As an immediate application of this definition, we may observe that the mapping

$$a \rightarrow i_a, \quad a \in G,$$

is a homomorphism of  $G$  onto  $I(G)$ , with kernel  $C(G)$ . From the fundamental homomorphism theorem, we have

$$G/C(G) \cong I(G).$$

Now let  $H$  be a normal subgroup of  $G$ , and let  $K$  be any subgroup of  $G$ . Since, for  $h \in H$  and  $k \in K$ ,

$$kh = h'k \quad \text{for some } h' \in H,$$

it follows that  $HK$  is also a subgroup of  $G$ . (Indeed, if also  $K \triangle G$ , then  $HK \triangle G$ .) The mapping

$$k \rightarrow kh$$

is a homomorphism of  $K$  onto  $HK/H$  with kernel  $K \cap H$ , and so

$$(2.8) \quad K/(K \cap H) \cong HK/H.$$

We shall use this basic isomorphism theorem repeatedly.

### Exercises

1. For  $\alpha \in A(G)$  and  $a \in G$ , prove that

$$\alpha \cdot i_a \cdot \alpha^{-1} = i_{\alpha a}.$$

Deduce from this that  $I(G) \triangle A(G)$ .

In Exercises 2.2 to 2.4,  $G$  is a transitive permutation group on the set  $X = \{x_1, \dots, x_n\}$  and

$$H = \{g \in G; gx_1 = x_1\}.$$

2. Prove the existence of elements  $g_1, \dots, g_n \in G$  such that  $g_i(x_1) = x_i$ ,  $1 \leq i \leq n$ , and such that

$$G = g_1H \cup \dots \cup g_nH$$

gives a coset decomposition of  $G$ .

3. The subgroup  $H$  also acts on the set  $X$ . Show that the number of orbits of  $X$  under  $H$  is the same as the number of  $(H, H)$ -double cosets in  $G$ . [Hint: Suppose that  $x_i$  and  $x_j$  are in the same orbit with respect to  $H$ ; then  $x_j = hx_i$  for some  $h \in H$  and  $g_j^{-1}hg_i : x_1 \rightarrow x_1$  where the  $\{g_k\}$  are as in Exercise 2.2. Then  $g_j^{-1}hg_i \in H$ , and so  $Hg_iH = Hg_jH$ . The argument is reversible. Finally, every  $(H, H)$ -double coset in  $G$  is of the form  $Hg_iH$  for some  $i$ .]

4. Assume that  $G$  is doubly transitive on  $X$ , so that, for each two pairs  $\{x_i, x_j\}$  ( $i \neq j$ ) and  $\{x_k, x_l\}$  ( $k \neq l$ ), there exists an element  $g \in G$  such that  $gx_i = x_k$ ,  $gx_j = x_l$ . Prove that  $H$  acts transitively on  $\{x_2, \dots, x_n\}$ .

5. Let  $H \triangle G$ , and set  $i = [G: H]$ ,  $j = [H: 1]$ . If  $i$  and  $j$  are relatively prime, show that  $H$  is the only subgroup of  $G$  of order  $j$ . [Hint: Let  $S$  be a subgroup of  $G$  of order  $j$ . Then  $HS/H$  is a subgroup of  $G/H$  whose order divides  $i$ . Also  $HS/H \cong S/(S \cap H)$  implies that the order of  $HS/H$  divides  $j$ . Therefore  $HS = H$ .]

6. A characteristic subgroup  $H$  of  $G$  is a subgroup for which  $\alpha H = H$

for each  $\alpha \in A(G)$ . Show that every characteristic subgroup of  $G$  is a normal subgroup of  $G$ . More generally, show that  $H$  characteristic in  $E$  and  $E \triangle G$  together imply  $H \triangle G$ .

7. Let  $n$  be fixed, and set  $S = \{x \in G : x^n = 1\}$ . If  $S$  is a subgroup of  $G$ , then  $S$  is a characteristic subgroup of  $G$ .

### § 3. Conjugate Classes

Still another important application of the orbit concept is the following, where  $I(G)$  again denotes the group of inner automorphisms of the group  $G$ :

(3.1) **DEFINITION.** The orbits of  $G$  relative to  $I(G)$  are called the *conjugate classes* of  $G$ . Elements in the same conjugate class are called *conjugates* of one another. Being orbits, two conjugate classes either are disjoint or coincide.

In order to determine the number of elements in the conjugate class containing  $x$ , we first introduce

(3.2) **DEFINITION.** The *centralizer of  $x$  in  $G$*  is the subgroup

$$C(x) = \{a \in G : axa^{-1} = x\}.$$

Of course  $x \in C(x)$ .

Now we note that  $axa^{-1} = bxb^{-1}$  if and only if  $a \in b \cdot C(x)$ . Thus, the number of distinct conjugates of  $x$  is the same as the number of left cosets of  $C(x)$  in  $G$ . Hence

(3.3) *If  $x \in G$ , there are  $[G : C(x)]$  elements in the conjugate class containing  $x$ .*

In particular,  $x$  coincides with all its conjugates if and only if  $x \in C(G)$ . Since every element of  $G$  lies in exactly one conjugate class, we may write the *class equation*

$$(3.4) \quad [G : 1] = [C(G) : 1] + \sum_x [G : C(x)]$$

where  $\sum_x$  extends over a set of representatives  $\{x\}$  of the conjugate classes of  $G$  having more than one element.

Let  $p$  be a prime. Call  $G$  a  *$p$ -group* if  $[G : 1]$  is a positive power of  $p$ . We may use the class equation to prove

(3.5) **THEOREM.** *The center of a  $p$ -group contains more than one element.*

**PROOF.** Let  $[G : 1] = p^n$ ,  $n \geq 1$ . If the conjugate class of  $x$  con-

tains more than one element, then  $C(x) \neq G$  and so  $p \nmid [G : C(x)]$ . The class equation then implies that  $p \mid [C(G) : 1]$ .

An example that is of importance to us is the determination of the conjugate classes of  $S_n$ . If

$$\sigma = (y \ \sigma y \ \sigma^2 y \cdots \sigma^{q-1} y)$$

is a cycle in  $S_n$ , we leave it as an exercise to the reader to show that, for any  $\pi \in S_n$ ,

$$\pi\sigma\pi^{-1} = (\pi y \ \pi(\sigma y) \ \pi(\sigma^2 y) \cdots \pi(\sigma^{q-1} y))$$

is also a cycle in  $S_n$  of the same length as  $\sigma$ . Now let  $\tau \in S_n$  be written as a product of disjoint cycles

$$(3.6) \quad \tau = \sigma_1 \cdots \sigma_r$$

where we put in “cycles” of length 1. Then

$$\pi\tau\pi^{-1} = (\pi\sigma_1\pi^{-1}) \cdots (\pi\sigma_r\pi^{-1})$$

gives the analogous decomposition of  $\pi\tau\pi^{-1}$ . This establishes

(3.7) *The cycle factorization of  $\pi\tau\pi^{-1}$  is gotten from that of  $\tau$  by letting  $\pi$  act on the digits in the cycle representation of  $\tau$ .*

For example, if

$$\tau = (123)(45) \quad \text{and} \quad \pi = (12)(34),$$

then

$$\pi\tau\pi^{-1} = (214)(35).$$

A *partition* of  $n$  is an ordered set of integers  $\{m_i\}$  satisfying

$$m_1 + m_2 + \cdots + m_r = n, \quad m_1 \geq m_2 \geq \cdots \geq m_r > 0.$$

Each  $\tau \in S_n$  gives rise to a partition of  $n$  as follows: write  $\tau$  in the form of (3.6) in which the  $\{\sigma_i\}$  are disjoint cycles of lengths  $m_1, m_2, \dots, m_r$ , arranged in order of decreasing length. Then (3.7) shows that each conjugate of  $\tau$  yields the same partition of  $n$  as  $\tau$  does.

Conversely, let

$$\tau' = \sigma'_1 \cdots \sigma'_r$$

yield the same partition of  $n$  as  $\tau$  does. Then, for each  $i$ ,  $\sigma_i$  and  $\sigma'_i$  have the same length, say

$$\sigma_i = (y_1 y_2 \cdots y_{m_i}), \quad \sigma'_i = (z_1 z_2 \cdots z_{m_i}).$$

For each  $i$ , define  $\pi$  on the orbit of  $[\sigma_i]$  by  $\pi(y_1) = z_1, \dots, \pi(y_{m_i}) = z_{m_i}$ .

Then  $\pi \in S_n$ , and  $\pi\tau\pi^{-1} = \tau'$ . Consequently,

(3.8) *There is a one-to-one correspondence between conjugate classes in  $S_n$  and partitions of  $n$ .*

As an analogue of (3.1), we have

(3.9) **DEFINITION.** Let  $H$  be a subgroup of  $G$ , and let  $a \in G$ . We call the subgroup  $aHa^{-1}$  a *conjugate of  $H$* . Define the *normalizer of  $H$  in  $G$*  by

$$N(H) = \{a \in G : aHa^{-1} = H\}.$$

This concept of conjugates does not arise from orbits, and so it is possible that distinct conjugates of  $H$  will overlap; this is indeed certain to occur since all conjugates of  $H$  contain 1. However, we note that the number of distinct conjugates of  $H$  is given by the index  $[G : N(H)]$ . Further,  $H \triangle G$  if and only if  $G = N(H)$  and, in particular,  $H \triangle N(H)$ .

It is also convenient to generalize the concept of centralizer as follows:

(3.10) **DEFINITION.** Let  $H$  be a subgroup of  $G$ . Define the *centralizer of  $H$  in  $G$*  by

$$C_G(H) = \{a \in G : aha^{-1} = h \text{ for all } h \in H\}.$$

Thus  $C_G(H)$  is just the center of  $G$ .

### *Exercises*

1. Let  $H \triangle G$ , and let  $C$  be a conjugate class in  $G$ . Prove that, if  $C \cap H \neq \emptyset$ , then  $C \subset H$ .
2. Prove that  $C_G(H) \triangle N(H)$ .
3. Let  $H, K$  be subgroups of  $G$ . The subgroups  $H$  and  $kHk^{-1}, k \in K$ , are called *K-conjugates*. Prove that the number of distinct *K-conjugates* of  $H$  is exactly

$$[K : K \cap N(H)].$$

### **§ 4. Abelian Groups**

Valuable insight toward most problems in group theory comes by testing these problems on finite abelian groups. This step may be essential for groups which, although they fail to be abelian, are built up in some simple way from abelian groups. In this section we recall some of the fundamental properties of finite abelian groups.

For the most part, these properties are special cases of theorems on  $\mathbb{Z}$ -modules which we shall prove at the beginning of Chapter III.

Let  $H_1, \dots, H_m$  be a finite collection of groups. By the (external) *direct product*  $H_1 \times \dots \times H_m$  is meant the group consisting of all  $m$ -tuples  $(h_1, \dots, h_m)$ ,  $h_1 \in H_1, \dots, h_m \in H_m$ , with multiplication defined by

$$(h_1, \dots, h_m) \cdot (h'_1, \dots, h'_m) = (h_1 h'_1, \dots, h_m h'_m).$$

[If the groups are written additively, we refer instead to the (external) *direct sum*  $H_1 + \dots + H_m$ .]

Suppose  $H$  and  $K$  are both subgroups of some group  $G$  such that  $hk = kh$  for all  $h \in H$  and  $k \in K$ . Then, setting

$$HK = \{hk: h \in H, k \in K\},$$

we see that  $HK$  is also a subgroup of  $G$ . If furthermore  $H \cap K = \{1\}$ , it follows that

$$HK \cong H \times K.$$

We shall then call  $HK$  the (internal) *direct product* of  $H$  and  $K$  in  $G$ .

For example, suppose  $H$  and  $K$  are subgroups such that every element of  $H$  commutes with every element of  $K$ . Suppose also that the orders  $[H: 1]$  and  $[K: 1]$  are relatively prime. Then  $H \cap K = \{1\}$  since the order of any element in  $H \cap K$  must divide both  $[H: 1]$  and  $[K: 1]$ . By the preceding remarks, we have

$$HK \cong H \times K.$$

We give an immediate application of this fact. Let  $G$  be a finite abelian group of order  $g$ . For each prime  $p$ , let  $G_p$  be the set of elements in  $G$  whose orders are powers of  $p$ . (Of course  $G_p = \{1\}$ , if  $p \nmid g$ ). Then  $G_p$  is a subgroup of  $G$ , called the  *$p$ -primary component* of  $G$ . We conclude at once that

$$(4.1) \quad G = \prod_{p \mid g} G_p \quad (\text{direct product}).$$

We also note that  $[G_p: 1] = \text{power of } p \text{ occurring in } g$ . The decomposition (4.1) is absolutely unique in the sense that, if also

$$G = \prod H_p,$$

a direct product of a finite number of subgroups  $H_p$  whose orders are distinct prime powers, then the  $\{H_p\}$  are the  $p$ -primary components of  $G$ .

For many purposes we require a finer decomposition of finite abelian groups. We first recall that a group  $G$  is *indecomposable* if it admits no non-trivial decomposition  $G = G_1 \times G_2$ . We now state without proof

(4.2) ELEMENTARY DIVISOR THEOREM. (i) *A finite abelian group is indecomposable if and only if it is cyclic of prime power order.*

(ii) *Every finite abelian group  $G \neq \{1\}$  is a direct product of indecomposable groups*

$$(4.3) \quad G = G_1 \times G_2 \times \cdots \times G_m$$

where each  $G_i$  is cyclic of prime power order  $a_i$ ,  $a_i > 0$ . The collection of orders  $\{p_1^{a_1}, \dots, p_m^{a_m}\}$  constitutes the elementary divisors of the decomposition (4.3).†

(iii) *Any two decompositions of  $G$  into indecomposable groups have the same set of elementary divisors.*

By (iii) we are entitled to speak of the *elementary divisors* of  $G$ . Clearly, two finite abelian groups are isomorphic if and only if they have the same set of elementary divisors.

We next require the following lemma:

(4.4) LEMMA. *A direct product  $H_1 \times \cdots \times H_r$  of cyclic groups, whose orders  $\{h_i\}$  are powers of distinct primes, is cyclic. Conversely, any cyclic group is so expressible.*

PROOF. We need only use the fact that, if  $x$  and  $y$  commute, the order of  $xy$  is the L.C.M. (least common multiple) of the order of  $x$  and the order of  $y$ .

We now state the second main result on finite abelian groups.

(4.5) INVARIANT FACTOR THEOREM. *Every finite abelian group  $G$  is a direct product*

$$(4.6) \quad G = H_1 \times H_2 \times \cdots \times H_r$$

of non-trivial cyclic groups  $\{H_i\}$ , whose orders  $\{h_i\}$  have the property that  $h_i | h_{i+1}$ ,  $1 \leq i \leq r-1$ . If also  $G = K_1 \times \cdots \times K_s$ , where the  $\{K_i\}$  are non-trivial cyclic groups of orders  $\{k_i\}$  such that  $k_i | k_{i+1}$ ,  $1 \leq i \leq s-1$ , then  $r = s$  and  $h_i = k_i$ ,  $1 \leq i \leq r$ .

We shall prove in this section only that Theorems 4.2 and 4.5 are equivalent. A proof of Theorem 4.5 will be given in §16.

Start with the decomposition (4.3). For each prime  $p_i$  dividing  $[G:1]$ , let  $p_i^{e_i}$  be the highest power of  $p_i$  which occurs among the

† The primes  $\{p_i\}$  are not necessarily distinct.

elementary divisors of  $G$ . Then, for each  $i$ , some one of the groups on the right-hand side of (4.3) has the order  $p_i^{a_i}$ , say, the group  $G_{m_i}$ . Set

$$H_r = \prod_i G_{m_i}.$$

By (4.4),  $H_r$  is cyclic of order  $\prod p_i^{a_i}$ . Apply the same construction to the remaining  $\{G_j\}$ , obtaining a cyclic direct factor  $H_{r-1}$  of order  $h_{r-1}$ , with  $h_{r-1} | h_r$ . Continuing in this way, we arrive at the decomposition (4.6).

To prove uniqueness, we note that by (4.4) each  $K_i$  is a direct product of cyclic groups whose orders are powers of distinct primes. By the elementary divisor theorem, the collection of all such prime powers (over all indices  $i$ ) are the elementary divisors of  $G$ . Because  $k_i | k_{i+1}$ , it follows that  $k_s$  is the L. C. M. of the elementary divisors,  $k_{s-1}$  is the L. C. M. of the remaining ones after the highest power of each prime is removed, and so on. This proves that Theorem 4.2 implies Theorem 4.5.

The proof that Theorem 4.5 implies Theorem 4.2 is straightforward and will be left to the reader.

### Exercises

1. Let  $G(n)$  be the multiplicative group consisting of those residue classes in  $Z/nZ$  whose elements are relatively prime to  $n$ . Show that  $[G(n):1] = \varphi(n)$  where  $\varphi$  is the Euler  $\varphi$ -function. Further, if  $n = \prod p_i^{a_i}$  where the  $\{p_i\}$  are distinct primes, then

$$G(n) \cong \prod_i G(p_i^{a_i}) \quad (\text{direct product}).$$

For  $p$  an odd prime,  $G(p^a)$  is cyclic, and

$$G(p^a) \cong G_1 \times G_2, \quad [G_1:1] = p - 1, \quad [G_2:1] = p^{a-1}.$$

On the other hand,  $G(2^a)$  is not cyclic for  $a > 2$ , and

$$G(2^a) \cong G_3 \times G_4, \quad [G_3:1] = 2, \quad [G_4:1] = 2^{a-2},$$

where  $G_4$  is cyclic. (See Hecke [1].)

2. Let  $A$  and  $B$  be groups whose orders are relatively prime. Prove that every subgroup of  $A \times B$  is of the form  $A_1 \times B_1$  for some subgroups  $A_1$  of  $A$  and  $B_1$  of  $B$ . [Hint: Let  $H$  be a subgroup of  $A \times B$ , and write  $h \in H$  as  $h = ab$ . Then  $(ab)^{[B:1]} \in H$  implies that  $a^{[B:1]} \in H$ . Since also  $a^{[A:1]} \in H$ , we have  $a \in H$ . Thus  $ab \in H$  if and only if both  $a$  and  $b$  belong to  $H$ .]

### § 5. Solvable and Nilpotent Groups

For no other general class of groups do we have structure theorems as definitive as those just stated for commutative groups. There are nevertheless important classes of groups more general than the commutative ones, about which our knowledge is more penetrating than in the general case.

We begin with

(5.1) **DEFINITION.** A *normal series* for a group  $G$  is a chain of subgroups

$$(5.2) \quad G = G_1 \supset G_2 \supset \cdots \supset G_r = \{1\}$$

in which  $G_{i+1} \triangleleft G_i$ ,  $1 \leq i \leq r - 1$ . The *factors of the normal series* are the factor groups  $G_1/G_2, \dots, G_{r-1}/G_r$ . We say that  $G$  is *solvable* if  $G$  has a normal series in which all of the factor groups are abelian.

Some basic properties of solvable groups are given in the following, which we state without proof:

- (5.3) **THEOREM** (i) *Subgroups of solvable groups are solvable.*
- (ii) *Homomorphic images of solvable groups are solvable.*
- (iii) *If  $H \triangleleft G$  is such that both  $H$  and  $G/H$  are solvable, then  $G$  is also solvable.*

For example, the alternating group  $A_n$  is not solvable when  $n \geq 5$ . On the other hand, every abelian group is solvable. Let us show, by induction on the order of  $G$ , that every  $p$ -group  $G$  is solvable. By (3.5), the center  $C(G)$  of  $G$  is non-trivial. If  $C(G) = G$ , then  $G$  is abelian and hence solvable. If not, then  $C(G)$  and  $G/C(G)$  are  $p$ -groups of orders less than  $[G:1]$  and so are solvable by the induction hypothesis. From (iii) of Theorem 5.3, we conclude that  $G$  is also solvable.

Burnside proved that if  $[G:1] = p^\alpha q^\beta$ , where  $p$  and  $q$  are primes, then  $G$  is solvable. In Chapter V we shall give a fairly simple proof of this based on the theory of group characters. A purely group-theoretical, but more complicated, proof has recently been found by Thompson for the case where  $p$  and  $q$  are both odd.

Let  $H \triangleleft G$ ; we call  $H$  a *maximal normal subgroup* of  $G$  if  $H$  is a proper subgroup of  $G$  not properly contained in any proper normal subgroup of  $G$ . A *composition series* for  $G$  is a series (5.2) in which for  $1 \leq i \leq r - 1$ ,  $G_{i+1}$  is a maximal normal subgroup of  $G_i$ . If  $G$  is a finite group, it is well known that every normal series without

repetitions can be “refined” into a composition series by inserting additional groups at strategic places. The factors of a composition series are called the *composition factors* of  $G$ . Of basic importance is

(5.4) **THEOREM (Jordan-Hölder Theorem).** *Any two composition series of a finite group  $G$  have the same length, and the composition factors obtained from the two series are the same (up to order of occurrence and isomorphism).*

This permits us to speak of the composition factors of  $G$  in an unambiguous manner. In particular, we find that a finite group  $G$  is solvable if and only if the composition factors of  $G$  are cyclic of prime order.

Before going into a further discussion of  $p$ -groups, we shall introduce some additional concepts.

(5.5) **DEFINITION.** The (*ascending*) *central series* of a finite group  $G$  is the sequence of subgroups

$$\{1\} = Z_0 \subset Z_1 \subset Z_2 \subset \dots$$

where  $Z_{i+1}$  is the uniquely determined normal subgroup of  $G$  such that  $Z_{i+1}/Z_i$  is the center of  $G/Z_i$ . We call  $G$  *nilpotent* if  $G = Z_n$  for some  $n$ .

It follows at once from (3.5) that

(5.6) *Every  $p$ -group is nilpotent.*

The suspicion that solvability and nilpotency are not independent concepts is not unfounded. The link between the two is the important notion of commutator groups.

If  $x$  and  $y$  are elements of a group  $G$ , their *commutator*  $[x, y]$  is defined by

$$[x, y] = xyx^{-1}y^{-1}.$$

It measures the extent to which  $xy$  differs from  $yx$ ; in fact,

$$(5.7) \quad xy = [x, y]yx.$$

(5.8) **DEFINITION.** The subgroup of  $G$  generated by all commutators  $[x, y]$ ,  $x, y \in G$ , is called the *commutator subgroup* of  $G$  and is denoted by  $[G, G]$ .

If  $\eta$  is any endomorphism of  $G$ , then

$$\eta[x, y] = [\eta x, \eta y].$$

In particular, each inner automorphism of  $G$  maps commutators onto

commutators, and therefore  $[G, G] \triangle G$ . The *factor commutator group of  $G$*  is defined as  $G/[G, G]$ ; in view of (5.7), this factor commutator group is abelian. Conversely, it also follows from (5.7) that, if  $H \triangle G$  is such that  $G/H$  is abelian, then  $H \supset [G, G]$ .

(5.9) DEFINITION. Let  $G' = [G, G]$ ,  $G'' = [G', G']$ , and so on. The sequence

$$G \supset G' \supset G'' \supset \dots$$

is called *the derived series of  $G$* .

(5.10) THEOREM. A group  $G$  is solvable if and only if  $G^{(n)} = \{1\}$  for some  $n$ .

PROOF. If  $G^{(n)} = \{1\}$ , then

$$G \supset G' \supset G'' \supset \dots \supset G^{(n)} = \{1\}$$

is a normal series for  $G$  with abelian factors, and so  $G$  is solvable. Conversely, let  $G$  be solvable, and let

$$G = G_1 \supset G_2 \supset \dots \supset G_r = \{1\}$$

be a normal series with abelian factors. A simple induction argument establishes that  $G^{(i)} \subset G_{i+1}$  for each  $i$ , whence  $G^{(r-1)} = \{1\}$ .

(5.11) THEOREM. Every nilpotent group is solvable.

PROOF. Let  $G$  be nilpotent, and let

$$\{1\} = Z_0 \subset Z_1 \subset \dots \subset Z_n = G$$

be a central series terminating in  $G$ . Since  $Z_n/Z_{n-1}$  is the center of  $G/Z_{n-1}$ , it follows that  $G/Z_{n-1}$  is abelian and  $G' \subset Z_{n-1}$ . An induction argument yields  $G^{(i)} \subset Z_{n-i}$  for each  $i$ , and hence  $G^{(n)} = \{1\}$ . From (5.10), it follows that  $G$  is solvable.

The converse of the above theorem is false. For example, the symmetric group  $S_8$  is solvable, but its central series never reaches past the subgroup  $\{1\}$ . This example also shows that the analogue of (iii) of Theorem 5.3 is false for nilpotent groups. Specifically, if  $H \triangle G$  is such that  $H$  and  $G/H$  are both nilpotent, it is false, in general, to conclude that  $G$  is nilpotent. However, it is true that subgroups and factor groups of nilpotent groups are nilpotent, though we shall not prove these facts here.

### Exercises

1. If  $A, B$  are normal subgroups of a finite group  $G$  such that  $[A:1]$  and

$[B:1]$  are relatively prime, show that  $A \cap B = \{1\}$ . If  $a \in A$  and  $b \in B$ , prove that  $aba^{-1}b^{-1} \in A \cap B$  and hence that  $ab=ba$ ,  $a \in A$ ,  $b \in B$ . Consequently  $AB \cong A \times B$ .

2. Let  $H$  be a normal subgroup of a finite group  $G$ . The set of composition factors of  $G$  is the union of the set of composition factors of  $H$  with that of  $G/H$ .

## § 6. Sylow Subgroups

In § 4 we saw that, for each prime  $p$  dividing the order of a commutative group  $G$ , there exists a subgroup  $G_p$  of  $G$  whose index is prime to  $p$ . Sylow's remarkable theorem, proved in 1873, asserts that this result is true for arbitrary finite groups. To prove the theorem, we begin with a preliminary result.

(6.1) *Let  $G$  be an abelian group of order  $g$ , and let  $p \mid g$ ,  $p$  prime. Then  $G$  contains an element of order  $p$ .*

PROOF. Let  $G_p$  be the  $p$ -primary component of  $G$ . Since  $[G_p:1]$  is the power of  $p$  occurring in  $g$ , we conclude that  $G_p$  contains an element  $x \neq 1$ . If the order of  $x$  is  $p^n$ ,  $n \geq 1$ , then  $x^{p^{n-1}}$  is an element of order  $p$  in  $G$ .

(6.2) DEFINITION. Let  $G$  be a finite group and  $p$  a prime. A subgroup  $P$  of  $G$  is a  $p$ -Sylow subgroup of  $G$  if  $P$  is a  $p$ -group such that  $p \nmid [G:P]$ . Alternately,  $P$  is a  $p$ -Sylow subgroup of  $G$  if and only if the order of  $P$  is the exact power of  $p$  which divides  $[G:1]$ .

We shall now prove the first of Sylow's theorems.

(6.3) THEOREM. *Let  $G$  be a finite group and  $p$  a prime. Then  $G$  contains a  $p$ -Sylow subgroup.*

PROOF. Use induction on the order of  $G$ , and suppose  $p^a \mid [G:1]$ . If  $G$  contains a proper subgroup  $H$  whose index is prime to  $p$ , then also  $p^a \mid [H:1]$ . By the induction hypothesis,  $H$  has a subgroup  $P$  of order  $p^a$ , and then  $P$  is also a  $p$ -Sylow subgroup of  $G$ .

For the remainder of the proof, we may assume that  $p \mid [G:H]$  for each proper subgroup  $H$  of  $G$ . Now consider the class equation (3.4)

$$[G:1] = [C(G):1] + \sum_{O(x) \neq G} [G:C(x)]$$

where  $x$  ranges over the representatives of the conjugate classes having more than one element. Then  $p$  divides each summand in

the summation and also  $p \mid [G: 1]$  (otherwise the result is trivial), so that  $p \mid [C(G): 1]$ . By (6.1), it follows that  $C(G)$  contains an element  $x$  of order  $p$ . The cyclic subgroup  $[x]$  is normal in  $G$ , and, by the induction hypothesis,  $G/[x]$  has a  $p$ -Sylow subgroup. From (2.5) we conclude that  $G$  contains a subgroup  $P$  (containing  $[x]$ ) such that the order of  $P/[x]$  is  $p^{a-1}$ . But  $P$  then has order  $p^a$  and is a  $p$ -Sylow subgroup of  $G$ .

In order to establish further properties of Sylow groups, we have to look in a more sophisticated way at the ideas used in the development of the class equation of  $G$ . Let  $P$  be a  $p$ -Sylow subgroup of  $G$  where  $p^a \mid \mid [G: 1]$ ,  $a \geq 1$ . If  $H$  is any  $p$ -subgroup of  $G$  (not necessarily a Sylow subgroup of  $G$ ), we call the subgroups  $P$  and  $hPh^{-1}$ ,  $h \in H$ ,  $H$ -conjugates of one another (see Exercise 3.3). If  $N(P)$  denotes, as usual, the normalizer of  $P$  in  $G$ , there are  $[H: H \cap N(P)]$  distinct  $H$ -conjugates of  $P$ . We now show

(6.4) LEMMA.  $H \cap N(P) = H \cap P$ .

PROOF. Since  $P \subset N(P)$ , we have  $(H \cap P) \subset (H \cap N(P))$ . To prove the converse, let  $H_1 = H \cap N(P)$ . Since  $H_1$  is a subgroup of the  $p$ -group  $H$ , also  $H_1$  is a  $p$ -group. But, on the other hand,  $P \triangle N(P)$ , and  $H_1$  is a subgroup of  $N(P)$ , so that, by (2.8), we have

$$[H_1P: P] = [H_1: H_1 \cap P] = \text{power of } p,$$

the latter because  $H_1$  is a  $p$ -group. Hence  $H_1P$  is a  $p$ -group containing  $P$ , and, since  $P$  is a maximal  $p$ -subgroup of  $G$ ,  $H_1P = P$ . Therefore  $H_1 \subset (H \cap P)$ , which proves our lemma.

Now consider all the conjugate subgroups  $P_x = xPx^{-1}$  of  $P$ ,  $x \in G$ . All of them are  $p$ -Sylow subgroups of  $G$ , and their number is  $[G: N(P)]$  which is prime to  $p$ . Let  $H$  be a fixed  $p$ -subgroup of  $G$  and divide the conjugate subgroups  $\{P_x\}$  into classes of  $H$ -conjugates. The number of subgroups  $P_z$  which are  $H$ -conjugates of  $P_x$  is just [by Exercise 3.3 and (6.4)]

$$[H: H \cap N(P_x)] = [H: H \cap P_x].$$

Therefore we obtain a formula

$$(6.5) \quad [G: N(P)] = \sum_{P_x} [H: H \cap P_x]$$

where the sum extends over a set of representatives  $\{P_x\}$  of the classes of  $H$ -conjugates of  $P$ . Since  $H$  is a  $p$ -group, all the terms on the right-hand side of (6.5) are powers of  $p$ , whereas  $[G: N(P)]$  is prime to  $p$ . We conclude that, for some  $P_x$ ,

$$[H: H \cap P_x] = 1,$$

that is,  $H = H \cap P_x$ , and so  $H \subset P_x = xPx^{-1}$ . This shows

(6.6) *Every  $p$ -subgroup of  $G$  lies in some conjugate of the  $p$ -Sylow subgroup  $P$  of  $G$ .*

As an immediate consequence, we deduce

(6.7) **THEOREM.** *Any two  $p$ -Sylow subgroups of a finite group  $G$  are conjugate. The total number of distinct  $p$ -Sylow subgroups is  $[G: N(P)]$ , where  $P$  is any  $p$ -Sylow subgroup of  $G$ .*

If in (6.5) we put  $H = P$ , then  $[H: H \cap P_x]$  is a positive power of  $p$  except when  $x = 1$ . This establishes

(6.8) *The number of distinct  $p$ -Sylow subgroups of  $G$  is  $\equiv 1 \pmod{p}$ .*

From (6.7), it follows readily that  $P$  is the only  $p$ -Sylow subgroup in its normalizer  $N(P)$ . Now let  $x \in G$  satisfy  $xN(P)x^{-1} = N(P)$ ; then  $xPx^{-1}$  is a  $p$ -Sylow subgroup of  $N(P)$  and hence coincides with  $P$ . This shows that  $x \in N(P)$ . Thus

(6.9) *If  $P$  is a  $p$ -Sylow subgroup of  $G$ , the normalizer of  $N(P)$  coincides with  $N(P)$ .*

For later use we shall need

(6.10) *Each non-cyclic  $p$ -group  $G$  has a factor group of type  $A \times A$  where  $A$  is cyclic of order  $p$ .*

**PROOF.** We shall use induction on the order of  $G$  and remark first that the result is an immediate consequence of the elementary divisor theorem when  $G$  is abelian. Assume thus that the center  $C$  of  $G$  is different from  $G$ , and let  $y \rightarrow \bar{y}$  under the canonical homomorphism  $\varphi$  of  $G$  onto  $\bar{G} = G/C$ . If  $\bar{G}$  is non-cyclic, it contains a normal subgroup  $\bar{H}$  such that  $\bar{G}/\bar{H} \cong A \times A$ . Choosing  $H = \varphi^{-1}(\bar{H})$ , we have [using (2.6)]

$$G/H \cong \bar{G}/\bar{H} \cong A \times A.$$

Finally, if  $\bar{G} = [\bar{y}]$  is cyclic, every element of  $G$  is expressible as a power of  $y$  times an element of  $C$ , and it is immediate that  $G$  is abelian. The result is known in this case, and (6.10) is proved.

In § 4 we proved that a finite abelian group is the direct product of its  $p$ -Sylow subgroups (which are the  $p$ -primary components) for the different primes  $p$  dividing the group order. Although this statement is not true for arbitrary finite groups, it is true for nilpotent groups.

To show this, we need a preliminary result.

(6.11) *Let  $H$  be a proper subgroup of the nilpotent group  $G$ . Then  $H$  properly contained in its normalizer  $N(H)$ .*

PROOF. Let

$$\{1\} = Z_0 \subset Z_1 \subset \cdots \subset Z_n = G$$

be a central series for  $G$ , and let  $H$  be a proper subgroup of  $G$ . Then  $Z_0 \subset H$  but  $Z_n \not\subset H$ , so we may find an index  $i$  such that

$$Z_i \subset H, \quad Z_{i+1} \not\subset H.$$

Since  $Z_{i+1}/Z_i$  = center of  $G/Z_i$ , we have

$$gvg^{-1}v^{-1} \in Z_i \quad \text{for } v \in Z_{i+1}, g \in G.$$

In particular, setting  $g = h \in H$  and using the fact that  $Z_i \subset H$ , we have

$$vh^{-1}v^{-1} \in H \quad \text{for } v \in Z_{i+1}, h \in H.$$

Hence

$$Z_{i+1} \subset N(H),$$

so that surely  $H \neq N(H)$ .

We may now prove

(6.12) THEOREM. *Let  $G$  be a finite nilpotent group. Then each  $p$ -Sylow subgroup of  $G$  is normal in  $G$ , and  $G$  is the direct product of its Sylow subgroups.*

PROOF. Let  $P$  be a  $p$ -Sylow subgroup of  $G$ , and let  $N(P)$  be its normalizer. By (6.9),  $N(P)$  is its own normalizer, and from (6.11) it follows that  $N(P) = G$ . This shows that  $P \triangleleft G$ .

Now let  $P, R, \dots$  be the Sylow subgroups of  $G$  for the primes  $p, r, \dots$ , dividing the order of  $G$ . Since  $P, R, \dots$  are normal subgroups whose orders are relatively prime, it follows from Exercise 5.1 that

$$PR \cdots \cong P \times R \times \cdots.$$

Since  $PR \cdots$  has the same order as  $G$ , we have

$$G \cong P \times R \times \cdots.$$

The converse of Theorem 6.12 is also true; that is, a finite group  $G$  which is a direct product of its Sylow subgroups is nilpotent. This holds since every  $p$ -group is nilpotent and a direct product of nilpotent groups is nilpotent.

*Exercises*

- Let  $G$  be a  $p$ -group such that  $G/[G, G]$  is cyclic. Then  $G$  is cyclic.
- Let  $H$  be a subgroup of a  $p$ -group  $G$  such that  $[G: H] = p$ . Prove that  $H \triangle G$ .

**§ 7. Semi-direct Products**

When a finite group is constructed in a simple way from some of its subgroups, information about the group can frequently be obtained from a knowledge of properties of the subgroups by the use of some inductive principle to transfer the information to the whole group. As the standard example of this procedure, we cite the theorems which state that, if two groups  $A$  and  $B$  have a certain property, so does their direct product. A less simple but interesting and useful method of building a new group from a pair of groups is by use of the semi-direct product, which we shall now define.

(7.1) **DEFINITION.** Let  $A$  and  $B$  be groups, and suppose there exists a homomorphism  $b \rightarrow \hat{b}$  of  $B$  into the group of automorphism of  $A$ . The set of all ordered pairs  $\{(a, b) : a \in A, b \in B\}$  can be made into a group if we define products by

$$(a, b)(a_1, b_1) = (a \cdot \hat{b}(a_1), bb_1).$$

This group is called the *semi-direct product* of  $A$  and  $B$ , relative to the homomorphism  $b \rightarrow \hat{b}$ . If  $\hat{b} = 1$  for all  $b \in B$ , we obtain just the usual direct product.

If we set

$$A' = \{(a, 1) : a \in A\}, \quad B' = \{(1, b) : b \in B\},$$

then  $A'$  and  $B'$  are subgroups of the semi-direct product  $G$  which are isomorphic to  $A$  and  $B$ , respectively, and will be identified with  $A$  and  $B$  in what follows. We then have  $G = AB$ ,  $A \cap B = \{1\}$ , and

$$ba = \hat{b}(a) \cdot b, \quad a \in A, b \in B.$$

These facts show that  $A \triangle G$  and that  $G/A \cong B$ .

(7.2) **THEOREM.** Let  $G$  be a group with subgroups  $A$  and  $B$ , and suppose there is a mapping  $b \rightarrow \hat{b}$  of  $B$  into the set of mappings of  $A$  into itself such that

- (i)  $G = AB$ ,
- (ii)  $A \cap B = \{1\}$ ,
- (iii)  $ba = \hat{b}(a) \cdot b, \quad a \in A, b \in B$ .

Then  $b \rightarrow \hat{b}$  is a homomorphism of  $B$  into the group of automorphisms of  $A$ , and  $G$  is isomorphic to a semi-direct product of  $A$  and  $B$  (relative to this homomorphism).

We shall omit the details of the proof. When the hypotheses of the theorem are satisfied, we shall refer to  $G$  as the semi-direct product of its subgroups  $A$  and  $B$ .

As our first illustration of the concept of the semi-direct product, let  $H$  be a group,  $A(H)$  its group of automorphisms, and  $H_L$  the set of left multiplications by elements of  $H$ . Both  $A(H)$  and  $H_L$  are subgroups of the group  $P(H)$  of all permutations of  $H$ . We call the subgroup  $K$  of  $P(H)$  generated by  $A(H)$  and  $H_L$  the *holomorph* of  $H$ . Let us show that  $H_L$  and  $A(H)$  satisfy the conditions of Theorem 7.2. First,

$$(7.3) \quad \alpha \cdot a_L = (\alpha a)_L \cdot \alpha, \quad a \in H, \alpha \in A(H).$$

Thus, every finite product of elements of  $H_L$  and  $A(H)$  can be written as a single product of an element of  $H_L$  and an element of  $A(H)$ . Hence (i) is satisfied; that is,  $K = H_L \cdot A(H)$ . It is obvious that  $H_L \cap A(H) = \{1\}$ . Finally,  $A(H)$  is already a group of automorphisms of  $H_L$ , provided that we identify  $H$  and  $H_L$ . Thus  $K$  is a semi-direct product of  $H_L$  and  $A(H)$ .

In some cases,  $A(H)$  is known explicitly, and the multiplication table of the holomorph  $K$  of  $H$  can be given with ease. For example, let  $H = [a]$ , a finite cyclic group generated by an element  $a$  of order  $m$ . Then the automorphisms of  $H$  are given by the  $\varphi(m)$  mappings

$$\alpha_i: a \rightarrow a^i, \quad 1 \leq i \leq m, (i, m) = 1.$$

The subscripts on the  $\alpha$ 's are taken mod  $m$ , and we have

$$\alpha_i \alpha_j = \alpha_{ij},$$

so that  $A(H)$  is isomorphic to the multiplicative group of residue classes mod  $m$  relatively prime to  $m$ . The elements of  $K$  are  $\{a^r \alpha_i : 0 \leq r \leq m-1, 1 \leq i \leq m, (i, m) = 1\}$ , multiplied by means of

$$(a^r \alpha_i)(a^s \alpha_j) = a^{r+s} \alpha_{ij}.$$

In this case  $K$  is solvable.

If, in particular,  $H$  is the cyclic group of order 4, its holomorph is a group of order 8 which is isomorphic to the group of symmetries of the square.

As our next illustration, we consider the *dihedral* group  $D_m$  of order  $2m$ , defined for each positive integer  $m$  as a semi-direct product

of a cyclic group  $A$  of order  $m$  with a cyclic group  $B$  of order 2. If  $b$  is a generator of  $B$ , then  $\hat{b}$  is the automorphism of  $A$  given by

$$\hat{b}(a) = a^{-1}, \quad a \in A.$$

In particular, suppose  $A = [a]$ ; then  $D_m$  consists of all elements  $\{a^i b^j : 0 \leq i \leq m-1, j = 1, 2\}$  which satisfy the relations

$$a^m = 1, \quad b^2 = 1, \quad ba = a^{-1}b.$$

Geometrically,  $D_m$  arises as the group of symmetries (distance-preserving permutations of the vertices) of the  $m$ -sided regular polygon, where  $a$  represents a rotation which cyclically advances the vertices one step and  $b$  is a reflection with respect to a line of symmetry.

Finally, we consider the *generalized quaternion groups*. The simplest such group is the one of order 8 whose elements are the quaternions  $\pm 1, \pm i, \pm j, \pm k$ . For each positive integer  $t$ , the generalized quaternion group  $Q_t$  is a group of order  $4t$  with two generators  $x, y$  satisfying

$$x^t = y^2, \quad yxy^{-1} = x^{-1}.$$

The second relation yields

$$yx^t y^{-1} = x^{-t}$$

which implies

$$y^4 = x^{2t} = 1.$$

Any element  $w \in Q$  can be expressed uniquely in the form

$$w = x^i y^j, \quad 0 \leq i \leq 2t-1, j = 0, 1.$$

The group  $A = [x]$  is an abelian normal subgroup of  $Q_t$  of index 2, and so  $Q_t$  is solvable. It is impossible for  $Q_t$  to be the semi-direct product of  $A$  and any other subgroup since  $Q_t$  has only one element  $y^2$  of order 2 and  $y^2 \in A$ .

It is instructive to look at the above examples from the point of view of the following general concept:

(7.4) DEFINITION. A group  $U$  is called an *extension of a group  $G$  by a group  $H$*  if there exists a homomorphism  $\varphi$  of  $U$  onto  $G$  with kernel  $H$ . The extension is called a *split extension* if there exists a homomorphism  $\psi$  of  $G$  into  $U$  such that  $\varphi\psi = 1$ .

It follows easily from (7.1) that a semi-direct product of  $A$  and  $B$  is a split extension of  $B$  with kernel  $A$ . Conversely, let  $U$  be a split extension of  $G$  by  $H$ , and let  $G' = \varphi(G)$ . Then  $\varphi$  maps  $G'$

isomorphically onto  $G$ , and hence  $G' \cap H = \{1\}$  since  $H$  is the kernel of  $\varphi$ . If  $u \in U$ , then  $\varphi(u) = \varphi(g')$  for some  $g' \in G'$ , and so  $u(g')^{-1} \in H$ , which shows that  $U = G'H$ . Because  $H \triangle U$ , we have  $G'H = HG'$ . From Theorem 7.2, we conclude that  $U$  is isomorphic to a semi-direct product of  $G$  and  $H$ .

The example of the generalized quaternion groups shows that even when  $G$  and  $H$  are commutative, not every extension of  $G$  by  $H$  need be a split extension. However, there is one important case in which we know that an extension must split. We state without proof:

(7.5) THEOREM (Schur). *Let  $H \triangle G$ ,  $i = [G: H]$ ,  $j = [H: 1]$ , and assume that  $i$  and  $j$  are relatively prime. Then  $G$  contains a subgroup  $S$  of order  $i$ , and  $G$  is a semi-direct product of  $S$  and  $H$ .*

For the proof the reader may consult M. Hall [2, p. 224], Kurosh [1, vol. II, pp. 201 and 202], or Zassenhaus [3, p. 132].

## Representations and Modules

The theory of group representations is concerned with the problem of classifying the homomorphisms of an abstract finite group into groups of matrices or linear transformations. The importance of this idea for the study of abstract groups was clearly recognized by Frobenius and Burnside and seems to depend on the fact that group-theoretical calculations are easier to carry out in groups of matrices than in abstract groups.

This chapter begins with the concrete notions of representations of groups by linear transformations and by matrices. From these ideas we are led in a natural way to representations of algebras and, finally, to modules over algebras and rings. Almost all the main theorems in this book are stated and proved in the language of modules because we believe that the conceptual difficulties involved in the deeper results are best overcome in this setting. As we shall show in the first few sections, it is possible to translate all statements concerning modules into equivalent statements about representations; although we do not dwell on this fact at all times, the reader will find that he will reach a better understanding of the subject if he frequently performs this translation for himself.

The rest of the chapter contains the standard theorems concerning modules over rings and algebras which are essential for our purposes. Much of this material may already be familiar to the reader, and in that case he should begin by reading Chapter IV, referring back to Chapters II and III when it becomes necessary. A possibly unfamiliar note is the rather general discussion of tensor products of modules. This approach gives quick access to the usual results on tensor products of vector spaces over fields and is needed in its full generality throughout Chapter VII on induced representations.

### § 8. Linear Transformations

Let  $M$  and  $N$  be commutative groups, written additively, and let

$$\text{Hom}(M, N)$$

denote the set of all homomorphisms of  $M$  into  $N$ . If we define the sum of two homomorphisms  $f$  and  $g$  by the rule

$$(8.1) \quad (f + g)m = f(m) + g(m), \quad m \in M,$$

then  $\text{Hom}(M, N)$  becomes a commutative group.

The additive group  $\text{Hom}(M, M)$  becomes a ring with an identity element if we define multiplication of homomorphisms by composition, namely

$$(8.2) \quad (fg)m = f(g(m)), \quad m \in M.$$

Now let  $M$  and  $N$  be vector spaces over a field  $K$ . Then

$$\text{Hom}_K(M, N)$$

denotes the subgroup of  $\text{Hom}(M, N)$  consisting of all mappings  $f \in \text{Hom}(M, N)$  such that

$$f(\alpha m) = \alpha f(m), \quad \alpha \in K, m \in M.$$

The mappings in  $\text{Hom}_K(M, N)$  are called *linear transformations* or sometimes  *$K$ -homomorphisms* or  *$K$ -linear transformations*. The group  $\text{Hom}_K(M, N)$  becomes a vector space over  $K$  if we define for each  $\alpha \in K$  and each  $f \in \text{Hom}_K(M, N)$ ,

$$(\alpha f)m = \alpha f(m), \quad m \in M.$$

In particular,  $\text{Hom}_K(M, M)$  is simultaneously a ring and a vector space over  $K$ , with the ring multiplication and the scalar multiplication linked by the relation

$$\alpha(fg) = (\alpha f)g = f(\alpha g), \quad f, g \in \text{Hom}_K(M, M), \alpha \in K.$$

Now let  $M$  be a finite-dimensional space, and let  $B = \{m_1, \dots, m_n\}$  be a basis of  $M$  over  $K$ . We shall usually denote the linear transformations of  $M$  by  $T, U, \dots$ . For  $T \in \text{Hom}_K(M, M)$ , let

$$(8.3) \quad Tm_i = \alpha_{1i}m_1 + \cdots + \alpha_{ni}m_n = \sum_{j=1}^n \alpha_{ji}m_j, \quad 1 \leq i \leq n,$$

where the  $\{\alpha_{ji}\}$  are elements of  $K$  which are uniquely determined

by  $T$  and the basis  $B$ . Let  $\mathbf{T}$  denote the  $n \times n$  matrix whose  $(j, i)$  entry is  $\alpha_{ji}$ , where in general the  $(r, s)$  entry of a matrix means the element appearing in the  $r$ th row and  $s$ th column. Then the constants  $\{\alpha_{ki}, 1 \leq k \leq n\}$  given in (8.3) form the  $i$ th column of  $\mathbf{T}$ . For example, let

$$\begin{aligned} Tm_1 &= 3m_1 - m_2, \\ Tm_2 &= m_2 + 2m_3, \\ Tm_3 &= -m_1 + m_3; \end{aligned}$$

then the matrix  $\mathbf{T}$  of  $T$  with respect to the basis  $\{m_1, m_2, m_3\}$  is

$$\mathbf{T} = \begin{bmatrix} 3 & 0 & -1 \\ -1 & 1 & 0 \\ 0 & 2 & 1 \end{bmatrix}.$$

The action of the linear transformation  $T$  on any vector  $m \in M$  is completely determined by the matrix  $\mathbf{T}$ ; for, letting  $m = \sum \xi_i m_i$ ,  $\xi_i \in K$ , we have

$$Tm = \sum_{i=1}^n \xi_i Tm_i = \sum_{i=1}^n \xi_i \sum_{j=1}^n \alpha_{ji} m_j = \sum_{j=1}^n \sum_{i=1}^n \xi_i \alpha_{ji} m_j.$$

We call  $\mathbf{T}$  the *matrix of  $T$  with respect to the basis  $B$* .

The set of all  $n \times n$  matrices with coefficients in  $K$  is a ring and a vector space over  $K$ , provided that we define addition, multiplication, and scalar multiplication by the familiar formulas

$$\begin{aligned} (\alpha_{ij}) + (\beta_{ij}) &= (\alpha_{ij} + \beta_{ij}), \\ (\alpha_{ij})(\beta_{ij}) &= (\gamma_{ij}), \quad \text{where } \gamma_{ij} = \sum_{k=1}^n \alpha_{ik} \beta_{kj}, \\ \xi(\alpha_{ij}) &= (\xi \alpha_{ij}), \quad \xi \in K. \end{aligned}$$

We denote this ring by  $K_n$  throughout this book, and shall sometimes speak of the matrices in  $K_n$  as *matrices over  $K$* .

The mapping  $T \rightarrow \mathbf{T}$  which assigns to each linear transformation  $T$  its matrix with respect to a fixed basis  $B$ , is easily seen to be a one-to-one mapping of  $\text{Hom}_K(M, M)$  onto  $K_n$ , which is both a ring isomorphism and a vector space isomorphism. We shall leave as an exercise the task of checking most of these assertions and shall work out in detail only the fact that the mapping preserves products, since this requirement dictated the original definition of the matrix of  $T$ . We have to show that if

$$(TU)m_i = \sum_{j=1}^n r_{ji}m_j ,$$

then the matrix  $(r_{ij}) = TU$ . Let

$$Tm_i = \sum \alpha_{ji}m_j \quad \text{and} \quad Um_i = \sum \beta_{ji}m_j ;$$

then

$$\begin{aligned} TUm_i &= T(Um_i) = T\left(\sum \beta_{ji}m_j\right) \\ &= \sum_{j=1}^n \beta_{ji}(Tm_j) = \sum_{j=1}^n \beta_{ji} \left( \sum_{k=1}^n \alpha_{kj}m_k \right) \\ &= \sum_{k=1}^n \sum_{j=1}^n \alpha_{kj}\beta_{ji}m_k . \end{aligned}$$

Then  $r_{ki} = \sum_{j=1}^n \alpha_{kj}\beta_{ji}$ , and our assertion is proved.

A *unit* in a ring  $R$  with 1 is any element  $x \in R$  which has a two-sided multiplicative inverse  $y$  in  $R$ . Thus  $x$  is a unit if and only if for some  $y \in R$ ,

$$xy = yx = 1 .$$

We also say that  $x$  is an *invertible* element of  $R$  in this case and write  $y = x^{-1}$ . The set of all units in  $R$  is obviously a multiplicative group.

The group of units in  $\text{Hom}_K(M, M)$  is called the *general linear group*  $GL(M)$ . Therefore an element  $T$  of  $\text{Hom}_K(M, M)$  is in  $GL(M)$  if and only if  $T$  is invertible; i.e., for some  $T^{-1} \in \text{Hom}_K(M, M)$ , we have

$$TT^{-1} = T^{-1}T = 1 ,$$

where 1 denotes the identity operator on  $M$ .

Let us fix a basis of  $M$ ; then, to each  $T \in \text{Hom}_K(M, M)$ , there corresponds a matrix  $T$ . The mapping  $T \rightarrow T$  maps  $GL(M)$  onto the group of units of  $K_n$ , which we denote by  $GL(n, K)$ .

It is necessary for us to determine what effect a change of basis in  $M$  has on the matrix  $T$  associated with a linear transformation  $T$ . Let  $T = (\alpha_{ij})$  and  $T' = (\alpha'_{ij})$  be the matrices of  $T$  with respect to the bases  $B = \{m_1, \dots, m_n\}$  and  $B' = \{m'_1, \dots, m'_n\}$ , respectively. We may write

$$(8.4) \quad m_i = \sum_{j=1}^n \sigma_{ji}m'_j ,$$

where  $S = (\sigma_{ij})$  is an invertible matrix in  $K_n$ . By (8.3) and (8.4),

we have for every  $i$ ,

$$\begin{aligned} Tm_i &= \sum_{j=1}^n \sigma_{ji}(Tm'_j) = \sum_{j=1}^n \sigma_{ji} \left( \sum_{k=1}^n \alpha_{kj} m'_k \right) \\ &= \sum_{k=1}^n \left( \sum_{j=1}^n \alpha_{kj} \sigma_{ji} \right) m'_k, \end{aligned}$$

whereas, on the other hand,

$$\begin{aligned} Tm_i &= \sum_{j=1}^n \alpha_{ji} m_j = \sum_{j=1}^n \alpha_{ji} \left( \sum_{k=1}^n \sigma_{kj} m'_k \right) \\ &= \sum_{k=1}^n \left( \sum_{j=1}^n \sigma_{kj} \alpha_{ji} \right) m'_k. \end{aligned}$$

We obtain by comparison  $T'S = ST$ , and therefore

$$(8.5) \quad T' = STS^{-1}.$$

Conversely, for any invertible matrix  $S = (\sigma_{ij})$  in  $K_n$ , we may define a new basis of  $M$  by (8.4). The matrix of  $T$  with respect to the new basis  $\{m'_1, \dots, m'_n\}$  is then  $STS^{-1}$ .

We can use the mapping  $T \rightarrow T'$  to define the determinant of a linear transformation  $T$ . If we set

$$|T| = |T'| = \det T,$$

the multiplication theorem for determinants applied to (8.5) guarantees that  $|T|$  is independent of the choice of the basis  $B$ . The determinant gives us a useful criterion for membership in  $GL(M)$ , namely,  $T \in GL(M)$  if and only if  $|T| \neq 0$ .

### Exercises

1. Define the *trace* of a matrix  $A = (\alpha_{ij})$  in  $K_n$  by  $\text{tr } A = \sum_{i=1}^n \alpha_{ii}$ . Prove that  $\text{tr } (AB) = \text{tr } (BA)$  for  $A, B$  in  $K_n$ . Hence prove that, if we define the trace of a linear transformation by

$$(8.6) \quad \text{tr } T = \text{tr } T',$$

the trace function is a well-defined additive map of  $\text{Hom}_K(M, M)$  into  $K$  such that  $\text{tr } (T_1 T_2) = \text{tr } (T_2 T_1)$ ,  $T_i \in \text{Hom}_K(M, M)$ .

2. Let  $T$  be the matrix of a linear transformation  $T$  in  $\text{Hom}_K(M, M)$ . Let  $\lambda$  be a transcendental element over  $K$ , and define the *characteristic polynomial* of  $T$  to be  $|\lambda I - T|$ , where  $I$  is the identity matrix in  $K_n$ . Show that the characteristic polynomial does not depend on the choice of a basis of  $M$ ;

that is, if  $\mathbf{T}'$  is the matrix of  $T$  relative to some other basis of  $M$ , then

$$|\lambda I - \mathbf{T}'| = |\lambda I - \mathbf{T}|.$$

Also prove that

$$|\lambda I - \mathbf{T}| = \lambda^n - (\text{tr } \mathbf{T})\lambda^{n-1} + \cdots + (-1)^n |\mathbf{T}|$$

for  $\mathbf{T} \in K_n$ .

### § 9. Definitions and Examples of Representations

In this section  $G$  will denote an arbitrary finite multiplicative group with identity element 1, and  $K$  a field. It is understood that all vector spaces considered are finite dimensional over  $K$ ; for a vector space  $M$ , we shall use the notation  $(M:K)$  to denote the dimension of  $M$  over  $K$ . We recall from §8 that  $GL(M)$  denotes the group of all invertible linear transformations of a vector space  $M$  onto itself, and that  $GL(n, K)$  stands for the group of invertible  $n \times n$  matrices over  $K$ .

(9.1) DEFINITION. Let  $G$  be a finite group and  $M$  a vector space over  $K$ . A *representation* of  $G$  with *representation space*  $M$  is a homomorphism  $T: g \rightarrow T(g)$  of  $G$  into  $GL(M)$ . Two representations  $T$  and  $T'$  with spaces  $M$  and  $M'$  are said to be *equivalent* if there exists a  $K$ -isomorphism  $S$  of  $M$  onto  $M'$  such that

$$T'(g)S = ST(g), \quad g \in G,$$

that is,

$$T'(g)Sm = ST(g)m$$

for all  $m \in M$  and  $g \in G$ . The dimension  $(M:K)$  of  $M$  over  $K$  is called the *degree* of  $T$  and will be denoted by  $\deg T$ .

Similarly, we have the concept of a matrix representation.

(9.2) DEFINITION. A *matrix representation* of  $G$  of *degree*  $n$  is a homomorphism  $\mathbf{T}: g \rightarrow \mathbf{T}(g)$  of  $G$  into  $GL(n, K)$ . Two matrix representations  $\mathbf{T}$  and  $\mathbf{T}'$  are *equivalent* if they have the same degree, say  $n$ , and if there exists a fixed matrix  $S$  in  $GL(n, K)$  such that

$$\mathbf{T}'(g) = S\mathbf{T}(g)S^{-1}, \quad g \in G.$$

If  $T$  is a representation of  $G$  with space  $M$ , then from the homomorphism property we have

$$\begin{aligned} T(ab) &= T(a)T(b), & a, b \in G, \\ T(a)^{-1} &= T(a^{-1}), \\ T(1) &= 1_M \end{aligned}$$

where  $1_M$  denotes the identity mapping on  $M$ . The corresponding statements hold, of course, for matrix representations.

Let  $T: G \rightarrow GL(M)$  be a representation of  $G$ , and let  $\{m_1, \dots, m_n\}$  be a basis of  $M$  over  $K$ . For each  $x \in G$ , the matrix  $T(x)$  of  $T(x)$  with respect to the basis  $\{m_1, \dots, m_n\}$  is in  $GL(n, K)$ , and

$$T: x \mapsto T(x)$$

defines a matrix representation of  $G$  called a *matrix representation afforded by  $T$*  (or by  $M$ ). The representation  $T$  affords other matrix representations obtained by selecting other bases of  $M$ , but (8.5) together with Definition 9.2 asserts that they are all equivalent.

Before introducing further concepts, we pause to lay firm hold on a number of important examples of representations. These are intended to serve as concrete illustrations upon which the reader should test the definitions and theorems to be developed in the rest of the chapter.

*Example 1. Permutation Representations.* Let  $S_n$  be the symmetric group on  $n$  symbols, and let

$$M = Km_1 \oplus \cdots \oplus Km_n$$

be an  $n$ -dimensional vector space over an arbitrary field  $K$ . For each  $\sigma \in S_n$ , let  $P(\sigma) \in \text{Hom}_K(M, M)$  be defined by

$$(9.3) \quad P(\sigma)m_i = m_{\sigma(i)}, \quad 1 \leq i \leq n.$$

For any  $\sigma, \tau \in S_n$  we have

$$P(\sigma\tau)m_i = m_{\sigma\tau(i)} = m_{\sigma(\tau(i))} = P(\sigma)P(\tau)m_i$$

for  $1 \leq i \leq n$ . Since the  $\{m_i\}$  are a  $K$ -basis of  $M$ , we conclude that

$$P(\sigma\tau) = P(\sigma)P(\tau), \quad \sigma, \tau \in S_n.$$

Moreover  $P(\sigma) = 1$  implies  $\sigma = 1$ , which shows that the mapping  $\sigma \rightarrow P(\sigma)$  is an isomorphism of  $S_n$  into  $GL(M)$ .

Let  $P(\sigma)$  be the matrix of  $P(\sigma)$  relative to the basis  $\{m_1, \dots, m_n\}$  of  $M$ . Then  $P(\sigma)$  is called a *permutation matrix* and is characterized by the property that in each row and each column there is just one non-zero entry, which is 1. The mapping  $\sigma \rightarrow P(\sigma)$  is an isomorphism

of  $S_n$  onto the subgroup of permutation matrices in  $GL(n, K)$ .

Now let  $G$  be an arbitrary group for which there exists a homomorphism  $\varphi : G \rightarrow S_n$  for some  $n$ . Then the composite mapping

$$T : x \rightarrow \varphi(x) \rightarrow P(\varphi(x))$$

of  $G$  into  $GL(M)$  is a representation of  $G$  with representation space  $M$ , and

$$T : x \rightarrow \varphi(x) \rightarrow P(\varphi(x))$$

is a matrix representation of  $G$  by permutation matrices.

In particular, let  $G$  be a group of order  $n$ . By Cayley's theorem (§ 2), there is an isomorphism  $\varphi : G \rightarrow S_n$  given by  $x \rightarrow x_L$ . Hence the mapping

$$R : x \rightarrow P(x_L), \quad x \in G,$$

is an isomorphism of  $G$  into  $GL(M)$ . We shall refer to  $R$  as the *regular representation* of  $G$ ; it is the most important example of a representation of a group. Let us describe this representation as explicitly as possible.

Suppose that  $G = \{x_1, \dots, x_n\}$  is a finite group of order  $n$ , and let  $M$  be an  $n$ -dimensional space with  $K$ -basis  $\{m_1, \dots, m_n\}$ . In order to determine  $R(x)$  for  $x \in G$ , we proceed as follows: For each  $i$ ,  $1 \leq i \leq n$ , there is a unique  $j$ ,  $1 \leq j \leq n$ , such that

$$(9.4) \quad xx_i = x_j.$$

Then we have

$$R(x)m_i = m_j$$

whenever  $i, j$  are related by (9.4). The matrix representation  $R$  afforded by  $M$  relative to the basis  $\{m_1, \dots, m_n\}$  is called the *regular matrix representation* of  $G$ . For each  $i$ ,  $1 \leq i \leq n$ , the  $i$ th column of  $R(x)$  consists of zeros except for an entry of 1 in the  $j$ th row, where  $i$  and  $j$  are related by (9.4). We note that, as a consequence of the preceding discussion, it is unnecessary to check that  $R$  is a representation of  $G$ .

As an illustration of this concept, let  $G = \{1, x, \dots, x^{n-1}\}$  be a cyclic group of order  $n$ . Then the regular matrix representation  $R$  of  $G$  maps  $x$  onto the matrix

$$\mathbf{R}(x) = \begin{pmatrix} 0 & 0 & \cdots & 0 & 1 \\ 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 \\ \cdot & \cdot & \cdots & \cdot & \cdot \\ 0 & 0 & \cdots & 1 & 0 \end{pmatrix},$$

and we have

$$\mathbf{R}(x^i) = \mathbf{R}(x)^i, \quad 1 \leq i \leq n - 1.$$

Evidently, in order to specify a matrix representation of an arbitrary group  $G$ , it is sufficient to give the matrices which correspond to a set of generators of  $G$ . For example, in order to give the regular matrix representation  $\mathbf{R}$  of the symmetric group

$$S_3 = \{1, (12), (13), (23), (123), (132)\},$$

it is enough to give  $\mathbf{R}((12))$  and  $\mathbf{R}((123))$ , since  $(12)$  and  $(123)$  generate the group. For them we have

$$\mathbf{R}((12)) = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \end{pmatrix},$$

$$\mathbf{R}((123)) = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}.$$

As a matter of fact, these matrices may be read off from a suitably arranged group table. We may observe that  $\mathbf{R}(x)$  has an entry 1 at position  $(j, i)$  if and only if  $x_j x_i^{-1} = x$ . Let us therefore construct a table the first column of which lists the elements  $x_1, \dots, x_n$  and the first row of which lists their inverses  $x_1^{-1}, \dots, x_n^{-1}$ . If the element at position  $(j, i)$  is  $x_j x_i^{-1}$ , the matrix  $\mathbf{R}(x)$  is gotten by putting a 1 wherever  $x$  occurs in this table and a zero elsewhere. For the group  $S_3$  we have

1	(12)	(13)	(23)	(132)	(123)
(12)	1	(132)	(123)	(13)	(23)
(13)	(123)	1	(132)	(23)	(12)
(23)	(132)	(123)	1	(12)	(13)
(123)	(13)	(23)	(12)	1	(132)
(132)	(23)	(12)	(13)	(123)	1.

From this, we may at once read off the matrices  $R((12))$  and  $R((123))$ . Conversely, knowledge of  $R$  enables us to reconstruct the group table.

*Example 2. The Cyclic Group.* Let  $G$  be a cyclic group generated by an element  $x$  of order  $n$ . A matrix representation of  $G$  is determined by the image  $X$  of  $x$ , and we observe that  $X$  may be chosen to be any square matrix satisfying

$$X^n = I \quad (I = \text{identity matrix}).$$

For example, let  $K$  be a field containing an  $n$ th root of unity  $\zeta$  (see § 21 on cyclotomic fields). Then

$$x \rightarrow (\zeta), \quad x^i \rightarrow (\zeta^i), \quad 1 \leq i \leq n,$$

defines a matrix representation of  $G$  of degree 1.

More generally suppose that  $K$  contains  $n$  distinct  $n$ th roots of unity, say  $\zeta_1, \dots, \zeta_n$ . (This will be the case only if the characteristic of  $K$  does not divide  $n$ .) Then the mapping

$$x \rightarrow T(x) = \text{diag} \{ \zeta_1^{-1}, \dots, \zeta_n^{-1} \}$$

defines a matrix representation of  $G$  of degree  $n$ . An easy computation shows, moreover, that

$$(9.5) \quad R(x)S = ST(x)$$

where  $R(x)$  is the matrix defined in Example 1 and

$$S = \begin{pmatrix} \zeta_1 & \cdots & \zeta_n \\ \zeta_1^2 & \cdots & \zeta_n^2 \\ \cdot & \cdots & \cdot \\ \zeta_1^n & \cdots & \zeta_n^n \end{pmatrix}.$$

Then  $|S|$  is a Van der Monde determinant, and we have

$$|S| = \pm \zeta_1 \cdots \zeta_n \prod_{1 \leq i < j \leq n} (\zeta_i - \zeta_j).$$

This is different from zero since the  $\{\zeta_i\}$  are distinct, and consequently

$S$  is invertible. The formula (9.5) asserts that the representation  $\mathbf{T}$  is equivalent to the regular matrix representation of  $G$ .

As another illustration, let  $G = [x]$  be a cyclic group of prime order  $p$ , and let  $K$  be a field of characteristic  $p$ . Then

$$\mathbf{X} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

has the property that  $\mathbf{X}^p = \mathbf{I}$ , and the mapping

$$(9.6) \quad x \rightarrow \mathbf{X}$$

defines a matrix representation of  $G$  of degree 2.

*Example 3.* Let  $G$  be the group of symmetries of the square, that is, the dihedral group of order 8. Then  $G$  has two generators  $a$  and  $b$  which satisfy the relations

$$a^4 = 1, \quad b^2 = 1, \quad bab^{-1} = a^{-1} \quad \text{or} \quad (ab)^2 = 1.$$

Because all other relations involving  $a$  and  $b$  are consequences of those we have listed, in order to specify a matrix representation of  $G$  it is sufficient to find matrices  $\mathbf{T}(a)$  and  $\mathbf{T}(b)$  such that

$$(9.7) \quad \mathbf{T}(a)^4 = 1, \quad \mathbf{T}(b)^2 = 1, \quad \text{and} \quad (\mathbf{T}(a)\mathbf{T}(b))^2 = 1.$$

It is a good exercise for the reader to convince himself that, if  $\mathbf{T}(a)$  and  $\mathbf{T}(b)$  do satisfy (9.7), then

$$a^i b^j \rightarrow \mathbf{T}(a)^i \mathbf{T}(b)^j$$

is a homomorphism of  $G$ . We list now some pairs of matrices which satisfy (9.7) and hence define representations of  $G$ .

$$\mathbf{T}(a) = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \quad \mathbf{T}(b) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix},$$

$$\mathbf{V}(a) = \begin{pmatrix} 0 & -1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & 1 & 0 \end{pmatrix}, \quad \mathbf{V}(b) = \begin{pmatrix} 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & -1 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}.$$

The reader may verify that there exists an invertible  $4 \times 4$  matrix  $S$  such that

$$S\mathbf{V}(a)S^{-1} = \begin{bmatrix} \mathbf{T}(a) & 0 \\ 0 & \mathbf{T}(a) \end{bmatrix},$$

and

$$SV(b)S^{-1} = \begin{bmatrix} T(b) & 0 \\ 0 & T(b) \end{bmatrix}.$$

The method used in Example 3 can be used to construct representations of any group for which we know the generators and a complete set of relations which the generators satisfy. The importance of knowing all the relations should be obvious to the reader; in fact, one can easily find matrices  $X$  and  $Y$  such that  $X^4 = Y^2 = 1$  but for which  $a \rightarrow X$ ,  $b \rightarrow Y$  cannot be extended to a representation of the group  $G$  of Example 3. Because questions concerning generators and relations can often be troublesome, the most fruitful approach to group representations, as we shall see, seems to be the analysis of the regular representation and representations constructed in some way from it.

*Example 4. One-Dimensional Representations.* Let  $G$  be a finite group with identity element 1, and let  $K$  be a field. We shall determine all one-dimensional  $K$ -representations of  $G$ , that is, all maps  $T: G \rightarrow K$  such that

$$(9.8) \quad T(xy) = T(x)T(y), \quad x, y \in G, \quad T(1) = 1.$$

For  $x \in G$ , we have at once  $T(x^{-1}) = T(x)^{-1}$ .

Now let  $G'$  be the commutator subgroup of  $G$ . Then  $G'$  is generated by the elements  $\{xyx^{-1}y^{-1} : x, y \in G\}$ , and  $G/G'$  is abelian. If  $T$  is any one-dimensional representation of  $G$ , then

$$T(xyx^{-1}y^{-1}) = T(x)T(y)\{T(x)\}^{-1}\{T(y)\}^{-1} = 1,$$

so that  $T$  maps every element of  $G'$  onto the unity element of  $K$ . Consequently,  $T$  induces a map  $\bar{T}: G/G' \rightarrow K$  by means of

$$(9.9) \quad \bar{T}(xG') = T(x), \quad x \in G.$$

Conversely, starting with a one-dimensional representation  $\bar{T}$  of  $G/G'$  in  $K$ , equation (9.9) serves to define such a representation  $T$  of  $G$ . Different  $T$ 's yield different  $\bar{T}$ 's, and conversely (see Exercise 9.1). Therefore there is a one-to-one correspondence, given by (9.9), between the distinct one-dimensional  $K$ -representations  $T$  of  $G$  and the distinct one-dimensional  $K$ -representations  $\bar{T}$  of  $G/G'$ .

We are thus faced with the following problem:

*Given a finite abelian group  $H$  of order  $h$  and a field  $K$  of characteristic  $p$ , determine all one-dimensional  $K$ -representations of  $H$ .*

To solve this problem, we use Theorem 4.2 on the structure

of finite abelian groups. We may write

$$H = H_1 \times \cdots \times H_m, \quad [H_i : 1] = h_i = p_i^{e_i}, \quad p_i \text{ prime,}$$

where each  $H_i$  is a cyclic group generated by an element  $x_i$  of order  $h_i$ ; clearly,  $h = h_1 \cdots h_m$ . Because of (9.8), the representation  $T$  is completely determined by the values  $T(x_1), \dots, T(x_m)$ . These values may be chosen independently of one another as long as they satisfy the relations

$$\{T(x_i)\}^{h_i} = 1.$$

Thus,  $T$  is completely determined by an  $m$ -tuple

$$\{\omega_1, \dots, \omega_m\}, \quad \omega_i \in K, \quad \omega_i^{h_i} = 1,$$

by setting  $T(x_i) = \omega_i$  for  $1 \leq i \leq m$ ; conversely, each such  $m$ -tuple gives a representation of  $H$  in  $K$ .

If the field  $K$  is such that the polynomial  $X^n - 1$  splits into linear factors in  $K$ , then  $K$  contains all  $n$ th roots of 1. We use the notation " $\sqrt[n]{1} \in K$ " to denote this fact. If  $p \nmid n$ , the equation  $X^n = 1$  has no repeated roots in  $K$ , and so if  $\sqrt[n]{1} \in K$ , then  $K$  contains precisely  $n$  distinct  $n$ th roots of 1.

Let  $q = \text{L.C.M.}(h_1, \dots, h_m)$ ; then  $q$  is the smallest positive integer such that  $x^q = 1$  for all  $x \in H$ , where 1 now denotes the identity element of  $H$ . We call  $q$  the *exponent* of  $H$ . Every  $q$ th root of 1 is expressible as a product of  $h_i$ th roots of 1 ( $i = 1, \dots, m$ ); on the other hand, every  $h_i$ th root of 1 is equal to some  $q$ th root of 1. Hence we see that  $\sqrt[q]{1} \in K$  if and only if each  $\sqrt[h_i]{1} \in K$ ,  $i = 1, \dots, m$ .

(9.10) THEOREM. Let  $H$  be a finite abelian group of exponent  $q$ , and let  $K$  have characteristic  $p$ , where  $p \nmid q$ . Then there are exactly  $[H : 1]$  distinct one-dimensional  $K$ -representations of  $H$  if  $\sqrt[q]{1} \in K$ . However, if  $\sqrt[q]{1} \notin K$ , there are fewer than  $[H : 1]$  such  $K$ -representations of  $H$ .

PROOF. Assume to begin with that  $\sqrt[q]{1} \in K$ . Then each  $\sqrt[h_i]{1} \in K$ , and so (using the previously defined notation) each  $\omega_i$  can take on  $h_i$  distinct possible values in  $K$ , namely, the  $h_i$  distinct roots of  $X^{h_i} = 1$ . There are thus  $\prod_i h_i$  one-dimensional  $K$ -representations of  $H$ , given by

$$T(x_1) = \omega_1, \quad \dots, \quad T(x_m) = \omega_m.$$

On the other hand,  $\sqrt[q]{1} \notin K$  implies that some equation  $X^{h_i} = 1$

does not have all its roots in  $K$ , and so some  $\omega_i$  is restricted to fewer than  $h_i$  possible values in  $K$ . Hence in this case there are fewer than  $\prod_i h_i$  one-dimensional  $K$ -representations of  $H$ . This completes the proof.

We may remark that, if  $p \mid q$ , then  $p \mid h_i$  for some  $i$ , and in this case  $X^{h_i} = 1$  has fewer than  $h_i$  distinct roots. Therefore, we have shown:

(9.11) COROLLARY. *If  $p \mid q$ , then  $H$  has fewer than  $[H:1]$  distinct one-dimensional representations in  $K$ .*

### *Exercise*

1. Prove that two one-dimensional representations are equivalent if and only if they are identical as mappings.

## § 10. Representations of Groups and Algebras

The notations introduced at the beginning of § 9 will also be used in this section. The basic method for the analysis of a representation  $T: G \rightarrow GL(M)$  is the study of those  $K$ -subspaces  $N$  of  $M$  such that

$$T(x)n \in N \quad \text{for all } x \in G \text{ and } n \in N.$$

Such a subspace will be called a  $G$ -subspace of  $M$ . If we define

$$(10.1) \quad T_1(x) = T(x) | N, \quad x \in G,$$

where  $T(x) | N$  denotes the restriction of  $T(x)$  to  $N$ , then  $T_1$  is a representation of  $G$  with representation space  $N$ .

By way of illustration, consider the representation space  $M$  for the symmetric group  $S_n$ , where

$$M = Km_1 \oplus \cdots \oplus Km_n$$

and where for each  $\sigma \in S_n$  we define a linear transformation  $P(\sigma)$  by

$$P(\sigma)m_i = m_{\sigma(i)}, \quad 1 \leq i \leq n.$$

(See § 9, Example 1). Then

$$N = K(m_1 + \cdots + m_n)$$

is an  $S_n$ -subspace of  $M$ , since

$$P(\sigma)(m_1 + \cdots + m_n) = m_1 + \cdots + m_n$$

for each  $\sigma \in S_n$ .

In terms of  $G$ -subspaces, we can now give some important definitions.

(10.2) DEFINITION. A representation  $T$  of  $G$  with non-zero representation space  $M$  is *irreducible* if the only  $G$ -subspaces of  $M$  are  $\{0\}$  and  $M$ ; otherwise  $T$  is called *reducible*. The representation  $T$  is *completely reducible* if for every  $G$ -subspace  $N$  of  $M$  there exists another  $G$ -subspace  $N'$  such that  $M = N \oplus N'$  (vector space direct sum). A  $G$ -subspace  $N$  of  $M$  is said to be *irreducible* or *completely reducible* according as the representation  $T_1$  defined in (10.1) is irreducible or completely reducible, respectively.

It should be remarked that a reducible representation need not be completely reducible. (See Exercise 10.3.)

Let us see what these definitions mean in terms of matrix representations. Let  $T: G \rightarrow GL(M)$  be a representation of  $G$ , and let  $N$  be a  $G$ -subspace of  $M$  such that  $N \neq \{0\}$  or  $M$ . Then we may choose bases so that

$$M = Km_1 \oplus \cdots \oplus Km_r, \quad N = Km_1 \oplus \cdots \oplus Km_s, \quad s < r.$$

Relative to these bases,  $M$  affords the matrix representation  $T$ , say, and  $N$  the matrix representation  $T_1$ ; we have, for each  $x \in G$ ,

$$(10.3) \quad T(x) = \begin{bmatrix} T_1(x) & V(x) \\ 0 & T_2(x) \end{bmatrix}.$$

In order to obtain some insight into the significance of  $T_2(x)$ ,  $x \in G$ , let us observe that there is a representation  $T_2: G \rightarrow GL(M/N)$  defined by

$$(10.4) \quad T_2(x)(m + N) = T(x)m + N, \quad x \in G,$$

where  $m + N$  ranges over all cosets in the factor space  $M/N$ . The mapping  $T_2(x)$  is a well-defined  $K$ -homomorphism of  $M/N$  into itself because  $N$  is a  $G$ -subspace of  $M$ . The cosets

$$\{m_{s+1} + N, \dots, m_r + N\}$$

form a basis for  $M/N$ , and clearly  $T_2$  affords the matrix representation  $T_2$  relative to this basis.

We shall postpone until much later (§ 73) our discussion of the significance of the matrices  $V(x)$ ,  $x \in G$ , and shall merely remark that these are certain rectangular matrices.

If  $U$  is any other matrix representation of  $G$  afforded by  $T$ ,

there exists a fixed matrix  $S \in GL(r, K)$  such that  $SU(x)S^{-1}$  has the form (10.3) for all  $x \in G$ .

Now suppose that  $M$  is completely reducible. Then we may write

$$M = N \oplus N', \quad N = Km_1 \oplus \cdots \oplus Km_s, \quad N' = Km_{s+1} \oplus \cdots \oplus Km_r,$$

and relative to the basis  $\{m_1, \dots, m_r\}$ ,  $T$  affords the matrix representation

$$(10.5) \quad U(x) = \begin{bmatrix} T_1(x) & 0 \\ 0 & T'_2(x) \end{bmatrix}, \quad x \in G.$$

It is easily verified from (10.4) that the matrix representations  $T_2$  and  $T'_2$  are equivalent. Thus, the complete reducibility of  $T$  implies that each matrix representation (10.3) is equivalent to one of the form (10.5).

With these calculations in mind, it is clear how to define the concepts of irreducible or completely reducible matrix representations. A matrix representation  $U: G \rightarrow GL(r, K)$  is *reducible* if  $U$  is equivalent to a representation  $T$  given by (10.3); if no such reduction exists, then  $U$  is an *irreducible matrix representation*. The representation  $U: G \rightarrow GL(r, K)$  is called a *completely reducible matrix representation* if, whenever  $U$  is equivalent to a matrix representation of the form (10.3),  $U$  is also equivalent to a representation (10.5).

We shall now prove two basic theorems which indicate clearly the direction in which the whole theory is to go, even though we shall not be able to exploit all their consequences until the end of Chapter IV.

(10.6) **LEMMA.** *A  $G$ -subspace of a completely reducible  $G$ -space  $M$  is completely reducible.*

**PROOF.** Let  $N$  be a  $G$ -subspace of  $M$ , and let  $N_1$  be a  $G$ -subspace of  $N$ . Then  $N_1$  is also a  $G$ -subspace of  $M$ , and there exists a  $G$ -subspace  $L$  of  $M$  such that  $M = N_1 \oplus L$ . Then  $L_1 = L \cap N$  is a  $G$ -subspace of  $N$ , and we have  $N = N_1 \oplus L_1$ , proving the lemma.

(10.7) **THEOREM.** *Let  $T: G \rightarrow GL(M)$  be a completely reducible representation of  $G$ . Then  $M$  is a direct sum of irreducible  $G$ -subspaces.*

**PROOF.** Select a  $G$ -subspace  $N \neq \{0\}$  of minimal dimension among all non-zero  $G$ -subspaces. Then  $N$  is irreducible, and we can find

a  $G$ -subspace  $L$  of  $M$  such that  $M = N \oplus L$ . If  $L = \{0\}$ , then  $M$  itself is irreducible, and there is nothing to prove. If  $L \neq \{0\}$ , then, by Lemma 10.6,  $L$  is completely reducible. Moreover  $(M : K) > (L : K)$ , so that we may conclude by an induction argument that  $L$  is a direct sum of irreducible  $G$ -subspaces. But a  $G$ -subspace of  $L$  is also a  $G$ -subspace of  $M$ . Therefore  $M$  is a direct sum of irreducible  $G$ -subspaces, and the theorem is proved.

(10.8) THEOREM. (*Maschke [1]*). *Let  $T: G \rightarrow GL(M)$  be a representation of a finite group  $G$  by linear transformations on a vector space  $M$  over a field  $K$ , and assume that*

$$p = \text{char}(K) \nmid [G : 1].$$

*Then  $T$  is completely reducible.*

PROOF. Let  $N \neq \{0\}$  be a  $G$ -subspace of  $M$ . We have to produce a  $G$ -subspace  $L$  of  $M$  such that  $M = N \oplus L$ . Because  $M$  is a vector space, we can at least find a  $K$ -subspace  $R$  such that

$$M = N \oplus R.$$

With such a decomposition is associated a  $K$ -linear map  $E: M \rightarrow N$  defined as follows: For  $m \in M$ , write

$$m = n + r, \quad n \in N, r \in R.$$

Then set

$$Em = n$$

so that  $E$  assigns to each  $m \in M$  its uniquely determined component in  $N$ . The linear transformation  $E$  is called a *projection* of  $M$  onto  $N$  and is characterized by the properties that

- (i)  $Em = m, m \in N,$
- (ii)  $EM \subset N.$

In fact, any  $F \in \text{Hom}_K(M, N)$  satisfying (i) and (ii) gives rise to a decomposition of  $M$  into  $K$ -subspaces:

$$M = FM \oplus (1 - F)M$$

where  $(1 - F)M = \{m - Fm : m \in M\}$ . We claim now that if

$$(10.9) \quad T(x)F = FT(x), \quad x \in G,$$

the subspaces  $FM$  and  $(1 - F)M$  are  $G$ -subspaces of  $M$ . For, if  $Fm$  is an element of  $FM$  and  $x$  is in  $G$ , then

$$T(x)Fm = FT(x)m \in FM,$$

which shows that  $FM$  is a  $G$ -subspace of  $M$ . A similar proof holds for  $(1 - F)M$ . Since  $FM = N$ , our theorem will be proved if we can construct from our given projection  $E$  a new projection  $F$  of  $M$  onto  $N$  satisfying (10.9). This is done by an “averaging” device; namely, we define  $F \in \text{Hom}_K(M, M)$  by

$$F = [G : 1]^{-1} \sum_{x \in G} T(x)ET(x)^{-1},$$

which is meaningful since  $[G : 1] \neq 0$  in  $K$ . Then for all  $y \in G$  we have

$$\begin{aligned} T(y)FT(y)^{-1} &= [G : 1]^{-1} \sum_{x \in G} T(y)T(x)ET(x)^{-1}T(y)^{-1} \\ &= [G : 1]^{-1} \sum_{x \in G} T(yx)ET(yx)^{-1} = F, \end{aligned}$$

and hence (10.9) holds.

Next we note that, for  $m \in M$  and  $x \in G$ , we have

$$T(x)ET(x)^{-1}m \in T(x)EM = T(x)N \subset N$$

since  $N$  is a  $G$ -subspace of  $M$ . Therefore

$$Fm = [G : 1]^{-1} \sum_{x \in G} T(x)ET(x)^{-1}m \in N$$

for all  $m \in M$ , which shows that  $F \in \text{Hom}_K(M, N)$ . For each  $n \in N$ , we have furthermore

$$ET(x)^{-1}n = T(x)^{-1}n, \quad x \in G,$$

since  $E|_N = 1$ ; therefore

$$Fn = [G : 1]^{-1} \sum_{x \in G} T(x)ET(x)^{-1}n = [G : 1]^{-1}[G : 1]n = n.$$

Thus  $F$  is a projection of  $M$  onto  $N$  for which (10.9) holds, and the theorem is proved.

Theorems (10.7) and (10.8) have the following consequence in terms of matrix representations:

(10.10) COROLLARY. *Let  $T: G \rightarrow GL(n, K)$  be a matrix representation of  $G$  by matrices with coefficients in a field  $K$  whose characteristic  $p \nmid [G : 1]$ . Then there exists a fixed matrix  $S \in GL(n, K)$  such that, for all  $x \in G$ ,*

$$ST(x)S^{-1} = \begin{pmatrix} T_1(x) & & & 0 \\ & T_2(x) & & \\ & & \ddots & \\ 0 & & & T_h(x) \end{pmatrix}$$

where the  $\{T_i\}$  are irreducible matrix representations.

The regular representation  $R$  of the cyclic group discussed in Example 2 of § 9 illustrates some of these ideas. If we view the representations  $R$  and  $T$  as having coefficients in an algebraically closed field of characteristic not dividing the order of the group, then (9.5) shows the splitting of the regular representation  $R$  as a direct sum of irreducible matrix representations. On the other hand, suppose  $G$  is cyclic of prime order  $p$ , and let  $K$  be the field of rational numbers. Then  $R$  contains an irreducible  $K$ -representation of degree  $p-1$  (see Exercise 10.9), and the formula (9.5) shows that an irreducible  $K$ -representation may split up into irreducible  $K'$ -representations of lower degree if we view the representation as a  $K'$ -representation instead, where  $K'$  is an extension field of  $K$ .

Let  $T: G \rightarrow GL(M)$  be a representation of  $G$ . It is often desirable to consider, instead of the linear transformations  $\{T(x)\}$  themselves, the  $K$ -subspace of  $\text{Hom}_K(M, M)$  spanned by all the  $\{T(x), x \in G\}$ . This space, called the *enveloping algebra* of  $T$ , consists of all linear combinations

$$\alpha_1 T(x_1) + \cdots + \alpha_r T(x_r), \quad x_i \in G, \alpha_i \in K.$$

Because  $T(xy) = T(x)T(y)$ , it follows that the enveloping algebra is a *subring* of  $\text{Hom}_K(M, M)$  as well as a subspace. It is also clear that the  $G$ -subspaces of  $M$  are identical with those subspaces  $N$  such that  $f(N) \subset N$  for all  $f$  belonging to the enveloping algebra of  $T$ . These remarks indicate that it is desirable to embed an abstract group  $G$  in some sort of a ring such that every element of the ring is a linear combination of the elements of  $G$  with coefficients in some field. Our next objective is to give this construction.

(10.11) DEFINITION. An *algebra*  $A$  over a field  $K$  is a ring  $A$  with an identity element which is at the same time a vector space over  $K$ . Moreover the scalar multiplication in the vector space and the ring multiplication are required to satisfy the axiom

$$\alpha(ab) = (\alpha a)b = a(\alpha b), \quad \alpha \in K, a, b \in A.$$

A subring of  $A$  which is also a  $K$ -subspace of  $A$  is called a *subalgebra* of  $A$ .

Now we come to the construction of the *group algebra* of an arbitrary finite group  $G$  with identity element  $e$ . We consider all formal sums

$$\sum \alpha_g \cdot g, \quad \alpha_g \in K,$$

two such expressions being regarded as equal if and only if they have the same coefficients. (The reader who finds formal sums unpalatable should note that a formal sum is simply a function on  $G$  to  $K$ , and that the coefficient  $\alpha_g$  gives the value of the function at the element  $g$  in  $G$ .) We then define operations on the formal sums by the rules

$$\sum \alpha_g g + \sum \beta_g g = \sum (\alpha_g + \beta_g) g$$

and

$$\begin{aligned} \left( \sum_{g \in G} \alpha_g g \right) \left( \sum_{h \in G} \beta_h h \right) &= \sum_{g, h \in G} \alpha_g \beta_h gh \\ &= \sum_{t \in G} r_t t, \end{aligned}$$

where

$$r_t = \sum_{g \in G} \alpha_g \beta_{g^{-1}t}.$$

In other words, we are defining addition of functions on  $G$  by

$$(f_1 + f_2)(g) = f_1(g) + f_2(g)$$

and multiplication by convolution:  $f_1 f_2 = f_3$  where

$$f_3(t) = \sum_{g \in G} f_1(g) f_2(g^{-1}t).$$

Finally, we define

$$\alpha(\sum \alpha_g g) = \sum \alpha \alpha_g g, \quad \alpha \in K.$$

With these definitions, it is easily checked that the set of all formal sums forms an algebra  $KG$ , called the *group algebra* of  $G$  over  $K$ . The formal sum  $1 \cdot e$ ,  $1 \in K$ ,  $e \in G$ , is the identity element of  $KG$ . The formal sums  $g^* = 1 \cdot g$ ,  $g \in G$ , which have all but one coefficient equal to zero, are linearly independent and form a basis of the algebra  $KG$  over  $K$ . The mapping  $g \rightarrow g^*$  is an isomorphism of  $G$  into  $KG$ , and we shall identify  $G$  with its image under this isomorphism. We can then view  $G$  as embedded in  $KG$  so that the elements of  $G$  form a  $K$ -basis for  $KG$ . The elements of  $KG$  are multiplied according to the distributive law and the multiplication defined for elements of  $G$ .

The same construction can be carried out with an arbitrary ring  $R$  with an identity in place of  $K$  and yields the *group ring*  $RG$  of  $G$  over  $R$ .

We have observed in § 8 that  $\text{Hom}_K(M, M)$  is an algebra over  $K$ . This leads to

(10.12) **DEFINITION.** Let  $A$  be a finite-dimensional algebra over a field  $K$  and  $M$  a finite-dimensional vector space over  $K$ . A *representation* of  $A$  with representation space  $M$  is an algebra homomorphism

$$T: A \rightarrow \text{Hom}_K(M, M),$$

that is, a mapping  $T$  which satisfies

$$\begin{aligned} T(a + b) &= T(a) + T(b), & T(ab) &= T(a)T(b), \\ T(\alpha a) &= \alpha T(a), & T(e) &= 1, \end{aligned} \quad a, b \in A, \alpha \in K,$$

where  $e$  is the identity element of  $A$ . Two representations  $T$  and  $T'$ , with representation spaces  $M$  and  $M'$ , are *equivalent* if there exists a vector space isomorphism

$$S: M \cong M'$$

such that

$$T'(a)S = ST(a) \quad \text{for all } a \in A.$$

Now let  $T$  be a representation of  $G$  with representation space  $M$ , where  $M$  is a vector space over the field  $K$ . Then there is a unique way to extend  $T$  to a representation  $T^*$  of  $KG$  with representation space  $M$ , namely

$$(10.13) \quad T^*(\sum \alpha_g g) = \sum \alpha_g T(g).$$

Conversely, every representation of  $KG$ , upon restriction to  $G$ , yields a representation of  $G$ . There is thus a one-to-one correspondence between  $K$ -representations of the *group*  $G$  and representations of the *group algebra*  $KG$ . Moreover, let  $T: G \rightarrow GL(M)$  be a representation of  $G$ , and let  $T^*: KG \rightarrow \text{Hom}_K(M, M)$  be the corresponding representation of  $KG$ . Let us call a  $K$ -subspace  $N$  of  $M$  a  *$KG$ -subspace* if

$$T^*(a)N \subset N \quad \text{for all } a \in KG.$$

It is then clear that a  $K$ -subspace  $N$  is a  $KG$ -subspace if and only if  $N$  is a  $G$ -subspace. Let us also remark that the set  $\{T^*(a) : a \in KG\}$  forms the enveloping algebra of the linear transformations  $\{T(g) : g \in G\}$ . Finally, we caution the reader that for  $a \in KG$  the linear transformation  $T^*(a)$  need not be invertible.

A *matrix representation of degree n* of a finite-dimensional algebra  $A$  is an algebra homomorphism of  $A$  into  $K_n$ . The remarks concerning the relation between representations by linear transformations and matrix representations of groups can be carried over verbatim to representations of algebras.

The final step in this process of abstraction was taken by Noether [1], who showed that the systematic use of modules over rings and algebras leads to simplifications in the terminology and conceptual framework of the theory of representations. As we have said before, the module-theoretic approach has been adopted in this book, and we proceed now to lay the foundations of this theory.

Let  $G$  be a group with identity element  $e$ , and let  $T: G \rightarrow GL(M)$  be a representation of  $G$ . For each  $m \in M$  and  $g \in G$ , we define a new element  $gm$  of  $M$  according to the rule

$$gm = T(g)m.$$

The “product”  $gm$  has the following properties:

$$(10.14) \quad \begin{cases} g(m + m') = gm + gm' \\ (gg')m = g(g'm), \quad em = m, \end{cases}$$

for  $g, g' \in G$ ,  $m, m' \in M$ . These are simply restatements of the formulas

$$\begin{aligned} T(g)(m + m') &= T(g)m + T(g)m', \\ T(gg')m &= T(g)T(g')m, \quad T(e)m = m. \end{aligned}$$

Thus each representation yields a  $G$ -module in the sense of

(10.15) **DEFINITION.** Let  $G$  be a group and  $M$  an additive abelian group. The group  $M$  is called a *left  $G$ -module* if, for each  $g \in G$  and  $m \in M$ , a product  $gm \in M$  is defined such that the relations (10.14) hold.

Similarly, let  $T: A \rightarrow \text{Hom}_K(M, M)$  be a representation of an algebra  $A$  over  $K$ . Then, for each  $a \in A$  and  $m \in M$ , we define

$$am = T(a)m$$

and observe that, because of the properties of the representation  $T$ , we have for all  $a, a' \in A$ ,  $m, m' \in M$ ,  $\alpha \in K$ ,

$$(10.16) \quad \begin{cases} a(m + m') = am + am', \quad (a + a')m = am + a'm, \\ (aa')m = a(a'm), \quad em = m, \\ (\alpha a)m = \alpha(am) = a(\alpha m), \end{cases}$$

where  $e$  is the identity element in  $A$ .

(10.17) DEFINITION. Let  $A$  be an algebra over  $K$ , and let  $M$  be a vector space over  $K$ . We say that  $M$  is a *left  $A$ -module* (or a module over  $A$ ) if for each  $a \in A$  and  $m \in M$ , a “product”  $am \in M$  is defined which satisfies the rules (10.16).

In this book all  $K$ -spaces which are modules over  $K$ -algebras are assumed to be finite-dimensional vector spaces over  $K$ .

The observation which led to the definition of module works equally well in reverse. For example, let  $M$  be a  $K$ -space which is a left  $A$ -module for an algebra  $A$  over  $K$ . For each  $a \in A$ , define a mapping  $T(a)$ :  $M \rightarrow M$  by setting

$$T(a)m = am, \quad a \in A, m \in M.$$

Then the formulas (10.16) assert that

$$T(a)(m + m') = T(a)m + T(a)m', \quad T(a)(\alpha m) = \alpha T(a)m,$$

so that  $T(a) \in \text{Hom}_K(M, M)$  for each  $a \in A$ . Moreover, we have

$$\begin{aligned} T(a_1 + a_2) &= T(a_1) + T(a_2), \\ T(a_1 a_2) &= T(a_1)T(a_2), \\ T(\alpha a) &= \alpha T(a), \\ T(e) &= 1, \end{aligned}$$

which shows that  $T$  is indeed a representation of  $A$ .

Let  $\{m_1, \dots, m_n\}$  be a basis of  $M$  over  $K$ . Then for each  $a \in A$  we have

$$am_i = \sum_{j=1}^n \alpha_{ji}(a)m_j, \quad 1 \leq i \leq n.$$

Let  $T(a)$  be the matrix  $(\alpha_{ij}(a))$ ; then our remarks show that  $T$  is a matrix representation of  $A$ , called a *matrix representation afforded by the  $A$ -module  $M$* .

(10.18) DEFINITION. Let  $M$  and  $M'$  be left  $A$ -modules where  $A$  is an algebra over the field  $K$ . The modules  $M$  and  $M'$  are said to be  *$A$ -isomorphic* if there exists a vector space isomorphism  $S$  of  $M$  onto  $M'$  such that for all  $a \in A$  and  $m \in M$  we have

$$a(Sm) = S(am).$$

Our definitions have been set up in such a way that two modules are  $A$ -isomorphic if and only if the representations afforded by them are equivalent.

The most important example of a left  $A$ -module over an algebra  $A$  is the vector space  $A$  itself, with the module product defined to be the ordinary ring multiplication in  $A$ . This module will be denoted by  ${}_A A$  and is called the *left regular module* of  $A$ .

(10.19) DEFINITION. Let  $M$  be a left  $A$ -module over a  $K$ -algebra  $A$  where  $K$  is a field. A  $K$ -subspace  $N$  of  $M$  is called a *submodule* if  $an \in N$  for all  $a \in A$  and  $n \in N$ .

For example, the submodules of the left regular module  ${}_A A$  are the *left ideals* of  $A$ .

Finally, let  $A = KG$  be the group algebra of a finite group  $G$  over a field  $K$ . From the results of this section, we see that there is a one-to-one correspondence between the  $K$ -representations of  $G$  and the left  $KG$ -modules  $M$ . For such a module  $M$ , the corresponding representation  $T: G \rightarrow GL(M)$  of  $G$  is given by

$$T(g)m = gm, \quad g \in G, m \in M.$$

The  $KG$ -submodules of  $M$  are precisely the  $G$ -subspaces of  $M$  introduced at the beginning of this section. Two left  $KG$ -modules are isomorphic if and only if the corresponding representations of  $G$  are equivalent.

### Exercises

- Let  $A$  be an algebra, and let the *center* of  $A$  be defined as

$$C = \{c \in A : ca = ac \text{ for all } a \in A\}.$$

Prove that  $C$  is a subalgebra of  $A$ .

- Let  $KG$  be the group algebra of a finite group. Show that  $\sum_{x \in G} x$  belongs to the center of  $KG$ . More generally, show that, if  $\mathfrak{C}$  is a fixed conjugate class in  $G$ , then  $\sum_{x \in \mathfrak{C}} x$  belongs to the center of  $KG$ .

- Let  $K$  be a field of characteristic  $p > 0$ , and let  $G$  be the cyclic group  $[x]$  of order  $p$ . Show that the matrix representation given in (9.6),

$$x \rightarrow \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix},$$

is reducible but not completely reducible. (Thus Theorem 10.8 is not true in general if  $p \mid [G : 1]$ .)

- Is the regular representation of a finite group  $G$  ever irreducible?
- Let  $KG$  be the group algebra of a finite group  $G$  over a field  $K$ . Show that the matrix representation of  $G$  afforded by the left  $KG$ -module  ${}_{KG}KG$  is equivalent to the regular representation of  $G$ .

The next two problems give another approach to Maschke's theorem for

representations over the fields of real or complex numbers. We begin with some definitions. A complex-valued function  $f$ , defined on pairs of vectors  $(m, n)$  belonging to a vector space  $M$  over the field of complex numbers, is called a *positive definite hermitian form* if for all vectors  $m, n, q$ ,

$$(10.20) \quad \begin{cases} f(m+n, q) = f(m, q) + f(n, q), & f(m, n+q) = f(m, n) + f(m, q), \\ f(\alpha m, n) = \bar{\alpha} f(m, n), & f(m, n) = \overline{f(n, m)}, \\ f(m, m) > 0 \text{ for } m \neq 0. \end{cases}$$

In this discussion  $\bar{\alpha}$  denotes the complex conjugate of  $\alpha$ . The assumption  $f(m, n) = \overline{f(n, m)}$  implies that  $f(m, m)$  is always a real number, so that the last condition makes sense. The standard example of such a form is given by

$$f(m, n) = \sum \alpha_i \bar{\beta}_i$$

where  $\{\alpha_i\}$  and  $\{\beta_i\}$  are the coefficients of  $m$  and  $n$  with respect to some fixed basis of  $M$ . For any form  $f$  satisfying (10.20), the set of all  $K$ -automorphisms  $U$  such that  $f(Um, Un) = f(m, n)$ ,  $m, n \in M$ , is a subgroup of  $GL(M)$  called the *unitary group* of  $M$  with respect to  $f$ , and its elements are called *unitary transformations*.

6. Let  $T: G \rightarrow GL(M)$  be an arbitrary representation of  $G$  by linear transformations of a complex vector space  $M$ . Prove that there exists a positive definite hermitian form  $f$  such that each linear transformation  $T(g)$  is a unitary transformation with respect to  $f$ . [Hint: Start with any positive definite hermitian form  $\varphi$  on  $M$ , and define

$$f(m, n) = \sum \varphi(T(x)m, T(x)n).$$

7. Let  $T: G \rightarrow GL(M)$  be a representation of a finite group  $G$ , by linear transformations of a complex vector space  $M$  such that each of the transformations  $\{T(g), g \in G\}$  is a unitary transformation with respect to a positive definite hermitian form  $f$ . Prove that  $T$  is completely reducible by showing that if  $N$  is a  $G$ -subspace of  $M$ , so is  $N^\perp = \{m \in M : f(N, m) = 0\}$ , and that  $M = N \oplus N^\perp$ .

8. Let  $T: G \rightarrow GL(M)$  be a representation of a possibly infinite group  $G$ , where  $M$  is a vector space over a field  $K$  of characteristic  $p$ . Suppose that  $G$  contains a subgroup  $H$  of finite index such that  $p \nmid [G : H]$  and for which  $T|H$  (the restriction of  $T$  to  $H$ ) is completely reducible. Prove that  $T$  is itself completely reducible. [The proof is almost the same as that of Maschke's theorem.]

9. Let  $G = [x]$  be a cyclic group of prime order  $p$ , and let  $K$  be the field of rational numbers. Let  $M$  be a  $p$ -dimensional vector space over  $K$  with basis  $\{m_0, m_1, \dots, m_{p-1}\}$ . Define  $R(x)$  by  $m_i \rightarrow m_{i+1}$ ,  $0 \leq i < p-1$ ,  $m_{p-1} \rightarrow m_0$ . Then  $R$  is the regular representation of  $G$ . Let  $u_0 = \sum_0^{p-1} m_i$ , and let  $u_i = m_i - m_{i-1}$ ,  $1 \leq i \leq p-1$ . Prove that  $N_1 = Ku_0$  and  $N_2 = \sum_1^{p-1} Ku_i$  are irreducible  $G$ -subspaces of  $M$ , and that  $M = N_1 \oplus N_2$ . (The proof uses the fact that the polynomial  $\lambda^{p-1} + \dots + \lambda + 1$  is irreducible in  $K[\lambda]$ .)

### § 11. Modules

We shall take a somewhat more general point of view than that introduced in § 10. In §§ 11-14,  $R$  will denote an arbitrary ring with a unity element 1.

(11.1) **DEFINITION.** An abelian group  $M$ , written additively, is called a *left  $R$ -module* if, for each  $r \in R$  and  $m \in M$ , a product  $rm \in M$  is defined such that

$$\begin{aligned} r(m_1 + m_2) &= rm_1 + rm_2, & (r_1 + r_2)m &= r_1m + r_2m, \\ (r_1r_2)m &= r_1(r_2m), & 1m &= m, \end{aligned}$$

for all  $r$  in  $R$ ,  $m$  in  $M$ . A subgroup  $M_1$  of  $M$  is called a *submodule* if  $rm_1 \in M_1$  for all  $r \in R$  and  $m_1 \in M_1$ . A one-to-one mapping  $f$  of a left  $R$ -module  $M$  onto a left  $R$ -module  $M'$  is called an  *$R$ -isomorphism* if  $f(m_1 + m_2) = f(m_1) + f(m_2)$  and  $f(rm) = rf(m)$  for all  $m \in M$ ,  $r \in R$ . When there exists an  $R$ -isomorphism between  $M$  and  $M'$ , we say that  $M$  and  $M'$  are  *$R$ -isomorphic* and write  $M \cong M'$ . (The group  $M$  is called a *right  $R$ -module* if there is a product  $mr$  defined such that  $mr \in M$  and

$$\begin{aligned} (m_1 + m_2)r &= m_1r + m_2r, & m(r_1 + r_2) &= mr_1 + mr_2, \\ m(r_1r_2) &= (mr_1)r_2, & m \cdot 1 &= m, \end{aligned}$$

for all  $r \in R$ ,  $m \in M$ . The concepts of submodule and isomorphism are defined for right modules in the obvious way.)

The *left regular module*  ${}_R R$  of a ring  $R$  is the left  $R$ -module whose underlying abelian group is the additive group of  $R$ , and the module product is given by the ring multiplication  $rm$  for  $r \in R$  and  $m \in {}_R R$ . The submodules of  ${}_R R$  are the *left ideals* of  $R$ . The *right regular module*  $R_R$  is defined similarly, and its submodules are the *right ideals* of  $R$ .

Included in the concept of module are vector spaces over fields and skewfields, as well as the modules over finite-dimensional algebras considered in the preceding section. In order to check that the present discussion does indeed include the theory of modules over algebras, let  $A$  be an algebra over  $K$  with unity element  $1^*$  and let  $M$  be a left  $A$ -module in the sense of Definition 11.1. We show that  $M$  is a vector space over  $K$  and that the last condition of (10.16) is satisfied. First, we define scalar multiplication on  $M$  by the rule

$$\alpha \cdot m = (\alpha 1^*)m, \quad \alpha \in K, m \in M;$$

then it is clear that with this definition,  $M$  is a vector space over  $K$  and that for all  $\alpha \in K$ ,  $a \in A$ ,  $m \in M$ ,

$$\alpha(am) = (\alpha a)m = a(\alpha m).$$

It is also clear that a submodule in the sense of Definition 11.1 is a subspace of the vector space  $M$  because of the definition of the scalar multiplication.

In the next three subsections, we develop some of the elementary notions of the theory of modules. In this discussion, “ $R$ -module” always means “left  $R$ -module”; it will be clear, however, that the entire discussion applies equally well to right modules.

### § 11A. Direct sums

If  $M_1$  and  $M_2$  are submodules of the  $R$ -module  $M$ , we define the *sum* of  $M_1$  and  $M_2$  by

$$M_1 + M_2 = \{m_1 + m_2 : m_1 \in M_1, m_2 \in M_2\}.$$

Then  $M_1 + M_2$  is again a submodule of  $M$  and is the smallest submodule which contains both  $M_1$  and  $M_2$ . The *intersection*  $M_1 \cap M_2$  is the largest submodule contained in both  $M_1$  and  $M_2$ .

Now let  $M_1, \dots, M_k$  be submodules of the  $R$ -module  $M$ . We write

$$M = M_1 \oplus \cdots \oplus M_k$$

and call  $M$  the (*internal*) *direct sum* of  $M_1, \dots, M_k$  if

- (i)  $M = M_1 + \cdots + M_k$  and
- (ii)  $m_1 + \cdots + m_k = 0$ ,  $m_i \in M_i$ , implies that each  $m_i = 0$ .

It is easily verified that if (i) holds then (ii) is equivalent to either of the following two conditions:

- (ii')  $M_i \cap (M_1 + \cdots + M_{i-1} + M_{i+1} + \cdots + M_k) = 0$  for each  $i$ ;
- (ii'') Every element  $m \in M$  can be expressed uniquely as a sum  $m = m_1 + m_2 + \cdots + m_k$ ,  $m_i \in M_i$ .

More generally, let  $\{M_i\}$  be a possibly infinite family of submodules of  $M$ . The sum  $\sum M_i$  of the family is the submodule of  $M$  whose elements are all possible finite sums of elements from the various submodules  $M_i$ . We say that  $M$  is the (*internal*) direct sum of the family  $\{M_i\}$  if

- (a)  $M = \sum M_i$  and
- (b) Every  $m \in M$  can be expressed uniquely as a sum

$$m = m_{i_1} + \cdots + m_{i_r}, \quad m_{i_j} \in M_{i_j}.$$

Now let  $M_1, \dots, M_k$  be a given set of  $R$ -modules, not necessarily

submodules of a common  $R$ -module. We define their *external direct sum*  $M^* = M_1 + \cdots + M_k$  to be the set of all  $k$ -tuples  $(m_1, \dots, m_k)$ ,  $m_i \in M_i$ , where addition is performed componentwise, and

$$r(m_1, \dots, m_k) = (rm_1, \dots, rm_k), \quad r \in R.$$

Then  $M^*$  is an  $R$ -module; if we set

$$M'_i = \{(0, \dots, 0, m_i, 0, \dots, 0) \mid m_i \in M_i\},$$

then  $M'_i$  is a submodule of  $M^*$ , and  $M'_i \cong M_i$ . Moreover we have

$$M_1 + \cdots + M_k = M'_1 \oplus \cdots \oplus M'_k.$$

(11.2) **DEFINITION.** Let  $\{m_\alpha\}$  be a possibly infinite set of elements of an  $R$ -module  $M$ , where  $\alpha$  ranges over some indexing set. The set  $\{m_\alpha\}$  is  *$R$ -free* if whenever

$$(11.3) \quad r_{\alpha_1}m_{\alpha_1} + \cdots + r_{\alpha_t}m_{\alpha_t} = 0, \quad r_{\alpha_i} \in R,$$

then necessarily each coefficient  $r_{\alpha_i} = 0$ .

(11.4) **DEFINITION.** A subset  $\{m_\alpha\}$  of an  $R$ -module  $M$  is called a *set of generators* of  $M$  if  $M = \sum_\alpha Rm_\alpha$ , that is, if every element of  $M$  is an  *$R$ -linear combination* of a finite number of the  $\{m_\alpha\}$ . A *finitely-generated* module is one having a finite set of generators. A *cyclic* module is a module with a single generator; thus  $M$  is a cyclic if and only if  $M = Rm$  for some  $m \in M$ .

(11.5) **DEFINITION.** A  $R$ -free set of generators of  $M$  is called an  *$R$ -basis* of  $M$ . Thus the set of elements  $\{m_\alpha\}$  is an  $R$ -basis of  $M$  if and only if every element of  $M$  can be expressed uniquely as a finite  $R$ -linear combination

$$\sum r_{\alpha_i}m_{\alpha_i}, \quad r_{\alpha_i} \in R, \quad m_{\alpha_i} \in \{m_\alpha\}.$$

Not all modules have bases; an  $R$ -module which has an  $R$ -basis is called a *free (left)  $R$ -module*. If  $\{m_\alpha\}$  is a basis of a free  $R$ -module  $M$ , each of the modules  $Rm_\alpha$  is isomorphic to the left regular module  ${}_R R$ . Conversely, any module which is a direct sum of submodules, each of which is isomorphic to  ${}_R R$ , is a free  $R$ -module.

(11.6) **DEFINITION.** An  $R$ -module  $M$  is  *$R$ -torsion-free* if  $rm = 0$ ,  $r \in R$ ,  $m \in M$ , implies that either  $r = 0$  or  $m = 0$ .

For example, a vector space  $V$  over a field  $K$  is a torsion-free  $K$ -module. On the other hand, an additive abelian group  $W$  is torsion-

free as  $Z$ -module if and only if  $W$  contains no elements of finite order.

### § 11B. Homomorphisms, submodules, and factor modules

Let  $M, N$  be  $R$ -modules. We use the notation  $\text{Hom}_R(M, N)$  to denote the set of all  $R$ -homomorphisms of  $M$  into  $N$ , that is, the set of all mappings  $f: M \rightarrow N$  such that

$$f(m_1 + m_2) = f(m_1) + f(m_2), \quad f(rm) = rf(m), \quad m_i \in M, r \in R.$$

The set  $\text{Hom}_R(M, N)$  forms a subgroup of  $\text{Hom}(M, N)$ , and  $\text{Hom}_R(M, M)$  forms a subring of  $\text{Hom}(M, M)$ . We call  $\text{Hom}_R(M, M)$  the *ring of  $R$ -endomorphisms* of  $M$ , or sometimes the *centralizer* of the  $R$ -module  $M$ , because the elements of  $\text{Hom}_R(M, M)$  are precisely those endomorphisms  $f$  of  $M$  which commute with all the endomorphisms of  $M$ .

$$r_L: m \rightarrow rm$$

determined by the elements of  $R$ .

If  $N$  is a submodule of  $M$ , the *factor module*  $M/N$  is the left  $R$ -module whose underlying commutative group is the totality of cosets  $\{m + N\}$  of  $N$  in  $M$ , and the module composition is defined by

$$(11.7) \quad r(m + N) = rm + N;$$

it is well defined because  $N$  is a submodule. The mapping  $\nu: m \rightarrow m + N$ , which maps  $m \in M$  onto the coset containing it, is by (11.7) an  $R$ -homomorphism of  $M$  onto  $M/N$ , called the *natural mapping* or *natural homomorphism* of  $M$  onto  $M/N$ .

We state without proof some straightforward analogues of the various homomorphism theorems for groups. The reader who is unfamiliar with modules will profit from working out detailed proofs of these results.

(11.8) *Let  $M, N$  be  $R$ -modules, and let  $f: M \rightarrow N$  be an  $R$ -homomorphism of  $M$  onto  $N$ . Let  $M_1 = f^{-1}(0)$  be the kernel of  $f$ ; then  $M_1$  is a submodule of  $M$ , and  $M/M_1 \cong N$ .*

More specifically, let  $\nu$  be the natural mapping of  $M$  onto  $M/M_1$ . Then

$$\bar{f}: \nu(m) \rightarrow f(m)$$

is the required isomorphism of  $M/M_1$  onto  $N$ .

(11.9) Let  $M, N$  be submodules of a common  $R$ -module. Then

$$(M + N)/M \cong N/(M \cap N).$$

(11.10) Let  $N$  be a submodule of the  $R$ -module  $M$ . There exists a one-to-one inclusion-preserving correspondence between the submodules of  $M$  which contain  $N$  and the submodules of  $M/N$ .

This correspondence is given as follows: let  $\nu: M \rightarrow M/N$  be the natural mapping. Then to each submodule  $L$  of  $M$  such that  $L \supset N$  corresponds the submodule  $\nu(L) = L/N$  of  $M/N$ ; conversely each submodule  $\bar{L}$  of  $M/N$  determines a unique submodule  $L$  of  $M$  such that  $L \supset N$ , namely,  $L = \nu^{-1}(\bar{L})$ . Furthermore, we have

$$(11.11) \quad M/L \cong (M/N)/(L/N)$$

whenever  $M \supset L \supset N$ .

(11.12) Let  $M$  be an  $R$ -module with submodules  $M_1, \dots, M_k$  such that

$$M = M_1 \oplus \cdots \oplus M_k.$$

For each  $i$ , let  $N_i$  be a submodule of  $M_i$ , and set

$$N = N_1 + \cdots + N_k = N_1 \oplus \cdots \oplus N_k.$$

(See Exercise 11.2.) Then

$$M/N \cong (M_1/N_1) \dot{+} \cdots \dot{+} (M_k/N_k).$$

A final remark concerns the familiar connection between direct sums and projections. Let  $M = M_1 \oplus \cdots \oplus M_k$ , and for each  $i$ ,  $1 \leq i \leq k$ , define a mapping  $\pi_i: M \rightarrow M_i$  by the rule

$$\pi_i(m_1 + \cdots + m_k) = m_i.$$

Then all the  $\{\pi_i\}$  are elements of  $\text{Hom}_R(M, M)$  and satisfy the conditions

$$\begin{aligned} 1 &= \pi_1 + \cdots + \pi_k, \\ \pi_i^2 &= \pi_i, \quad \pi_i \pi_j = \pi_j \pi_i = 0, \quad i \neq j. \end{aligned}$$

Conversely, given an  $R$ -module  $M$  and any set of  $R$ -endomorphisms  $\{\pi_i\}$  satisfying these relations, the sets  $\{\pi_i(M)\}$  are submodules of  $M$ , and  $M$  is their direct sum. The  $R$ -endomorphisms  $\{\pi_i\}$  are called the *projections* associated with the given direct sum decomposition, and a particular  $\pi_i$  is called the *projection* of  $M$  onto  $M_i$ . The reader will find it instructive to re-read the proof of Theorem 10.8 with these definitions in mind.

### § 11C. Finiteness conditions

For algebras and modules which are finite-dimensional vector spaces over fields, all the conditions discussed in this subsection will automatically be satisfied. The discussion in the general case, however, helps to clarify exactly what hypotheses are needed in order to prove the theorems on composition series and indecomposable modules in §§ 13 and 14.

(11.13) **DEFINITION.** Let  $M$  be an  $R$ -module. The submodules of  $M$  are said to satisfy the *descending chain condition* (D.C.C.) if every chain of submodules of  $M$

$$M_1 \supset M_2 \supset M_3 \supset \cdots$$

terminates, that is, if there exists an index  $j$  such that  $M_j = M_{j+1} = \cdots$ . Analogously, the submodules of  $M$  are said to satisfy the *ascending chain condition* (A.C.C.) if every chain of submodules of  $M$

$$M_1 \subset M_2 \subset M_3 \subset \cdots$$

terminates. If the submodules of  $M$  satisfy the A.C.C., we shall call  $M$  a *noetherian module*. A (left) *noetherian ring*  $R$  is one for which the left regular module  ${}_R R$  is a noetherian module; in other words,  $R$  is a noetherian ring if and only if its left ideals satisfy the A.C.C.

(11.14) **THEOREM.** *The following statements concerning the  $R$ -module  $M$  are equivalent:*

- (i) *The submodules of  $M$  satisfy the A.C.C.*
- (ii) *Every submodule of  $M$  is finitely generated.*
- (iii) *Every non-empty collection of submodules of  $M$  contains a maximal element, that is, a submodule which is not properly contained in any other submodule in the collection.*

**PROOF.** Statement (i) implies (ii): Suppose (ii) is false, and let  $M^*$  be a submodule of  $M$  which is not finitely generated. Then, by induction, we can construct an infinite sequence of elements  $a_1, a_2, \dots$  in  $M^*$  such that if  $M_k = Ra_1 + \cdots + Ra_k$ , then for every  $k$ ,  $M_k$  is properly contained in  $M_{k+1}$ . This contradicts (i), and the first implication is proved.

Statement (ii) implies (iii). Suppose (iii) is false. Then there exists a non-empty collection  $X$  of submodules which has no maximal element. By mathematical induction, we can find submodules  $M_1,$

$M_2, \dots$  in  $X$  such that for every  $k$ ,  $M_k$  is properly contained in  $M_{k+1}$ . The union  $\bigcup_{k=1}^{\infty} M_k = M^*$  is evidently a submodule of  $M$  although not necessarily a member of  $X$ . We prove that  $M^*$  is not finitely generated. Suppose the contrary, namely, that  $M^* = Rm_1 + \dots + Rm_s$  for some  $s$ . Then each  $m_i \in M_{k_i}$  for some  $k_i$ , and, choosing the largest of the modules  $M_{k_i}$ , we conclude that  $M^* = M_{k_i}$  for some index  $k_i$  and hence that  $M_{k_i+1} = M_{k_i}$ . But this contradicts the way the submodules  $M_k$  were constructed. To sum up, we have shown that if (iii) is false, then (ii) is false, and we can assert therefore that (ii) implies (iii).

Statement (iii) implies (i). Suppose (i) is false. Then there exists an infinite properly ascending chain of submodules, and it is clear that this collection of submodules can have no maximal element. This completes the proof of the theorem.<sup>†</sup>

By the same method of proof, we have

(11.15) THEOREM. *Let  $M$  be an  $R$ -module. Then the submodules of  $M$  satisfy the D.C.C. if and only if every non-empty collection of submodules of  $M$  has a minimal element, that is, a submodule which does not properly contain any other submodule in the collection.*

We have already discussed the fact that  $R$  itself may be regarded as a left  $R$ -module  ${}_R R$  and that the submodules of  ${}_R R$  are the left ideals of  $R$ . (Similarly, the submodules of the right module  $R_R$  are the right ideals of  $R$ .) By Theorem 11.14, we see that all the left ideals of  $R$  are finitely generated (as  $R$ -modules) if and only if  $R$  is a left noetherian ring in the sense of (11.13). We use this result in the course of the proof of the next theorem.

(11.16) THEOREM. *Let  $R$  be a left noetherian ring, and let  $M$  be a finitely generated  $R$ -module. Then every submodule of  $M$  is finitely generated.*

PROOF. Since  $M$  is finitely generated, there exist elements  $m_1, \dots, m_k$  in  $M$  such that

$$M = Rm_1 + \dots + Rm_k.$$

We prove the theorem by induction on  $k$ , the result being vacuously true if  $k = 0$ . Thus we may assume  $k \geq 1$ , and that every  $R$ -module which can be generated by fewer than  $k$  elements has the property that all its submodules are finitely generated.

---

<sup>†</sup> The proof of this theorem uses a disguised form of the Axiom of Choice; the theorem can also be proved using the Maximum Principle (§ 15 A).

Let  $N$  be a submodule of  $M$ . Every element  $n$  in  $N$  can be expressed, possibly in many ways, as an  $R$ -linear combination of the generators of  $M$ ,

$$(11.17) \quad n = r_1 m_1 + \cdots + r_k m_k, \quad r_i \in R.$$

For  $n \in N$ , let  $S(n)$  be the subset of  $R$  consisting of all elements  $r_1$  which occur as the coefficient of  $m_1$  in some expression for  $n$  such as (11.17). Let

$$S = \bigcup_{n \in N} S(n).$$

We shall prove that  $S$  is a left ideal in  $R$  (possibly the zero ideal). Let  $s, s' \in S$ ; then there exist elements

$$n = sm_1 + s_2 m_2 + \cdots + s_k m_k, \quad n' = s'm_1 + s'_2 m_2 + \cdots + s'_k m_k$$

in  $N$ . Then  $s - s'$  is the coefficient of  $m_1$  in some expression for  $n - n'$ , and  $s - s' \in S$ . Further,  $rn = rsm_1 + rs_2 m_2 + \cdots + rs_k m_k$ , and so  $rs \in S$  for all  $r \in R$ . Therefore  $S$  is a left ideal in  $R$ .

By Theorem 11.14 [see also the discussion preceding the statement of this theorem],  $S$  is a finitely generated  $R$ -module, and so there exist elements  $s_1, \dots, s_t$  in  $S$  such that

$$(11.18) \quad S = Rs_1 + \cdots + Rs_t.$$

For each  $i$ ,  $1 \leq i \leq t$ , there exists  $n_i \in N$  such that  $s_i \in S(n_i)$ . Now consider  $n \in N$  given by (11.17). We have  $r_i \in S$ , so by (11.18) we may write

$$r_i = x_1 s_1 + \cdots + x_t s_t, \quad x_i \in R.$$

Then we have

$$(11.19) \quad n - (x_1 n_1 + \cdots + x_t n_t) = y_2 m_2 + \cdots + y_k m_k$$

for some elements  $\{y_i\}$  in  $R$ .

Now let us set  $M' = Rm_2 + \cdots + Rm_k$ . Since the left side of (11.19) is in  $N$ , the right side is in  $M' \cap N$ , and it follows that

$$(11.20) \quad N = Rn_1 + \cdots + Rn_t + (M' \cap N).$$

The submodule  $M' \cap N$  is a submodule of  $M'$ , and  $M'$  is generated by  $k - 1$  elements. By our induction hypothesis,  $M' \cap N$  is finitely generated, and hence (11.20) implies that  $N$  is finitely generated. This completes the proof.

Another proof of this theorem can be obtained by a simple modification of Exercise 11.18 below.

*Exercises*

1. Let  $M_1, \dots, M_k$  be submodules of the  $R$ -module  $M$  such that  $M = M_1 \oplus \dots \oplus M_k$ . Show that every element of  $M$  is expressible in one and only one way as  $\sum_{i=1}^k m_i$ ,  $m_i \in M_i$ .

2. Let the  $R$ -module  $M$  be the direct sum of its submodules  $M_1, \dots, M_k$ , and let  $N_i$  be a submodule of  $M_i$ ,  $1 \leq i \leq k$ . Prove that

$$N_1 + \dots + N_k = N_1 \oplus \dots \oplus N_k.$$

Is every submodule of a direct sum itself a direct sum?

3. An  $R$ -module having an  $R$ -basis is  $R$ -torsion-free, provided that  $R$  has no divisors of zero.

4. Prove Theorems (11.8) through (11.12).

5. For the ring  $R = KG$ , consider the left  $R$ -module  $M = KG$ . Set

$$N = \left\{ \sum_{x \in G} \alpha_x x : \alpha_x \in K, \sum_{x \in G} \alpha_x = 0 \right\}.$$

Show that  $N$  is an  $R$ -submodule of  $M$ , and discuss the structure of the quotient module  $M/N$ .

6. Let  $M, M_1$  be  $R$ -modules, and let  $f \in \text{Hom}_R(M, M_1)$ . Suppose that  $N$  is the kernel of  $f$ , and let  $L$  be a submodule of  $N$ . Show that  $f$  induces an  $R$ -homomorphism of  $M/L$  into  $M_1$ .

7. Let  $K$  be a field, and let  $M$  be a finite-dimensional vector space over  $K$ . Show that  $M$  is a  $K$ -module whose submodules satisfy both chain conditions. If  $n = (M : K)$ , prove that  $M \cong K + \dots + K$  ( $n$  summands).

8. Let  $N$  be a submodule of the  $R$ -module  $M$ , and let  $N'$  be a submodule of the  $R$ -module  $M'$ . If  $M \cong M'$  and  $N \cong N'$ , does it follow that  $M/N \cong M'/N'$ ?

9. Let  $M, N$  be  $R$ -modules for which there exist maps  $f \in \text{Hom}_R(M, N)$  and  $g \in \text{Hom}_R(N, M)$  satisfying the conditions

(i)  $f(M) = N$ ,

(ii)  $f \cdot g = \text{identity on } N$ .

Prove that  $g$  is one-to-one and that

$$M \cong N + (M/g(N)).$$

10. Any abelian additive group is automatically a  $Z$ -module, where  $Z$  is the ring of rational integers. Give examples of  $Z$ -modules which fail to satisfy one or the other or both of the chain conditions. [Hint: To get a module which satisfies the D.C.C. but not the A.C.C., let  $M$  be the additive group of all rational numbers whose denominators are powers of a fixed prime  $p$ , modulo the subgroup consisting of the integers. Prove that every proper submodule of this module is finite.]

11. What are the maximal submodules of the  $K$ -module  $M$  given in Exercise 11.7? What are the minimal submodules? What does this imply about the possible uniqueness of maximal or minimal submodules? [See Definition 13.1.]

12. Let  $R$  be a commutative integral domain in which every ideal is principal. Show that the (left) ideals of  $R$  satisfy the A.C.C.
13. Let  $N$  be a submodule of the  $R$ -module  $M$ . If  $M$  is finitely generated, so is  $M/N$ .
14. Let  $N$  be a submodule of the  $R$ -module  $M$ , and suppose both  $N$  and  $M/N$  are noetherian modules. Prove that  $M$  is noetherian.
15. Let  $N$  be a submodule of the  $R$ -module  $M$ . If  $N$  and  $M/N$  are both finitely generated, does it follow that  $M$  is also finitely generated?
16. Let  $N$  be a submodule of the  $R$ -module  $M$ . Suppose the submodules of  $N$  and those of  $M/N$  satisfy the D.C.C. Prove that the submodules of  $M$  satisfy the D.C.C.
17. Let  $M = M_1 + \cdots + M_k$ , where the  $\{M_i\}$  are submodules of the  $R$ -module  $M$ . If the submodules of each  $M_i$  satisfy the D.C.C., so do those of  $M$ . The same result holds for the A.C.C. (Use Exercise 11.16.)
18. Suppose  $M$  is a finitely generated  $R$ -module, and that the left ideals of  $R$  satisfy the D.C.C. Prove that the submodules of  $M$  also satisfy the D.C.C. [Write  $M = Rm_1 + \cdots + Rm_k$ ,  $m_i \in M$ . By Exercise 11.17, it suffices to show that the submodules of each  $Rm_i$  satisfy the D.C.C. Then prove that every submodule of  $Rm_i$  is of the form  $Am_i$ , where  $A$  is a left ideal in  $R$ .]

## § 12. Tensor Products

We come now to a less elementary but extremely powerful and useful construction. In its most general form, it constructs from a given right  $R$ -module  $M$  and left  $R$ -module  $N$ , an abelian group  $M \otimes_R N$ , called the *tensor product* of  $M$  and  $N$ . In case  $R$  is a field  $K$ , it turns out that  $M \otimes_K N$  is a vector space over  $K$ , whose dimension over  $K$  is the product  $(M : K) \cdot (N : K)$ . In this case,  $M \otimes_K N$  can be thought of as the set of finite sums of formal “products”  $\sum m_i n_i$ ,  $m_i \in M$ ,  $n_i \in N$ , where the product  $mn$  satisfies the laws

$$\begin{aligned} m(n_1 + n_2) &= mn_1 + mn_2, & (m_1 + m_2)n &= m_1n + m_2n, \\ \alpha(mn) &= (\alpha m)n = m(\alpha n), & \alpha \in K, \end{aligned}$$

for all  $m \in M$ ,  $n \in N$ . But of course this vague notion of product cannot serve as a precise definition, and this intuitive description fails to account for the unpleasant fact that when the coefficient ring  $R$  is not a field, we may have  $mn = 0$  with both  $m$  and  $n$  different from zero. The key to the general concept comes from the study of bilinear mappings on a pair of vector spaces  $M$  and  $N$  over a field  $K$ . By definition, a *bilinear mapping*  $f$  assigns to each pair  $(m, n)$  belonging to the Cartesian product set  $M \times N$  an element of a third vector space  $V$ , and satisfies

$$\begin{aligned} f(\alpha_1 m_1 + \alpha_2 m_2, n) &= \alpha_1 f(m_1, n) + \alpha_2 f(m_2, n), \\ f(m, \alpha_1 n_1 + \alpha_2 n_2) &= \alpha_1 f(m, n_1) + \alpha_2 f(m, n_2) \end{aligned}$$

for all  $\alpha_i \in K$ ,  $m_i \in M$ , and  $n_i \in N$ . The tensor product space  $M \otimes_K N$  will be defined in such a way that there exists a fixed bilinear map  $\varphi: M \times N \rightarrow M \otimes_K N$  with the following properties:

(a) Every element of  $M \otimes_K N$  is a  $K$ -linear combination of elements of the form  $\varphi(m, n)$ ,  $m \in M$ ,  $n \in N$ , and

(b) For each vector space  $V$ , every bilinear map  $f: M \times N \rightarrow V$  is obtained by first mapping  $(m, n)$  into  $M \otimes_K N$  by  $\varphi$  and then mapping  $\varphi(m, n)$  into  $V$  by a *linear* mapping  $f^*: M \otimes_K N \rightarrow V$ . More compactly, we have

$$f(m, n) = f^*(\varphi(m, n))$$

where  $f^*$  is a *linear* transformation. Our point of view is that the theory of tensor products reduces the study of bilinear mappings to the more familiar theory of linear transformations.

Now we are ready to study tensor products in general. We shall have to consider mappings that are somewhat weaker than bilinear mappings, and, following Chevalley [3], we call them *balanced mappings* in the sense of the following definition:

(12.1) DEFINITION. Let  $M$  be a right module and  $N$  a left module over an arbitrary ring  $R$  with an identity element. Let  $P$  be an abelian group, written additively. A *balanced map*  $f$  of the Cartesian product set  $M \times N$  into  $P$  assigns to each pair  $(m, n) \in M \times N$  an element  $f(m, n) \in P$ , so that

$$\begin{aligned} f(m_1 + m_2, n) &= f(m_1, n) + f(m_2, n), \\ f(m, n_1 + n_2) &= f(m, n_1) + f(m, n_2), \\ f(m, rn) &= f(mr, n) \end{aligned}$$

for all  $r \in R$  and  $m_i \in M$ ,  $n_i \in N$ .

(12.2) DEFINITION. Let  $f: M \times N \rightarrow P$  and  $\varphi: M \times N \rightarrow T$  be balanced maps of  $M \times N$  into the additive abelian groups  $P$  and  $T$  respectively. We say that  $f$  can be *factored through*  $T$  if there exists a homomorphism  $f^*: T \rightarrow P$  such that

$$f = f^* \varphi,$$

or more explicitly

$$f(m, n) = f^*(\varphi(m, n))$$

for all  $(m, n) \in M \times N$ . In other words,  $f$  can be factored through  $T$  if there exists a homomorphism  $f^*: T \rightarrow P$  such that the diagram

$$\begin{array}{ccc} & T & \\ \varphi \swarrow & & \searrow f^* \\ M \times N & \xrightarrow{f} & P \end{array}$$

is commutative.

(12.3) THEOREM. Let  $M$  and  $N$  be right and left  $R$ -modules, respectively. There exists an abelian group  $T$  and a balanced map  $t: M \times N \rightarrow T$  such that

(i) The elements  $t(m, n)$  generate the additive group  $T$ , and in fact every element of  $T$  is a sum  $\sum t(m_i, n_i)$  where  $m_i \in M$ ,  $n_i \in N$ .

(ii) Every balanced map of  $M \times N$  into an arbitrary abelian group  $P$  can be factored through  $T$ .

PROOF. We start with the Cartesian product  $M \times N$  consisting of all ordered pairs  $(m, n)$ ,  $m \in M$ ,  $n \in N$ . Now form the free  $Z$ -module  $F$  which has as  $Z$ -basis the elements of  $M \times N$ , so that  $F$  is the additive abelian group which consists of all finite formal sums

$$\sum z_{ij}(m_i, n_j), \quad z_{ij} \in Z, m_i \in M, n_j \in N.$$

Let  $H$  be the subgroup of  $F$  generated by the formal sums

$$(12.4) \quad \left\{ \begin{array}{l} (m_1 + m_2, n) - (m_1, n) - (m_2, n), \\ (m, n_1 + n_2) - (m, n_1) - (m, n_2), \\ (m, rn) - (mr, n) \end{array} \right.$$

for all  $m \in M$ ,  $n \in N$ ,  $r \in R$ . Let  $T$  be the factor group  $F/H$ , and define a mapping

$$t: M \times N \rightarrow T$$

by means of

$$t(m, n) = (m, n) + H.$$

Since the sums listed in (12.4) all lie in  $H$ , we have at once

$$(12.5) \quad t(m_1 + m_2, n) - t(m_1, n) - t(m_2, n) = 0 \quad (\text{in } T),$$

and so on, which shows that  $t$  is a balanced map. From the fact that every element of  $F$  is a  $Z$ -linear combination of ordered pairs,

it follows that every element of  $T$  is a  $Z$ -linear combination of elements of the form  $t(m, n)$ ,  $m \in M$ ,  $n \in N$ . To show that every element of  $T$  is expressible in the form

$$\sum t(m_i, n_i), \quad m_i \in M, n_i \in N,$$

we need remark only that (12.5) implies

$$t(zm, n) = t(m, zn) = zt(m, n)$$

for all  $m \in M$ ,  $n \in N$ ,  $z \in Z$ .

Now let  $\varphi$  be any balanced map of  $M \times N \rightarrow P$ . Because the elements  $(m, n)$  form a  $Z$ -basis of  $F$ , the mapping  $\varphi$  defines a homomorphism  $\varphi'$  of  $F$  into  $P$  by means of

$$\varphi'(\sum z_{ij}(m_i, n_j)) = \sum z_{ij}\varphi(m_i, n_j).$$

The fact that  $\varphi$  is balanced implies that  $\varphi'(H) = 0$ . Therefore  $\varphi'$  induces a homomorphism  $\varphi^*$  of  $F/H = T$  into  $P$  such that

$$\varphi^*((m, n) + H) = \varphi(m, n), \quad (m, n) \in M \times N.$$

Since  $t(m, n) = (m, n) + H$ , we have

$$\varphi^*(t(m, n)) = \varphi(m, n),$$

and we have proved that  $\varphi$  can be factored through  $T$ . This completes the proof of the theorem.

(12.6) DEFINITION. The group  $T$  constructed in Theorem 12.3 is called the *tensor product* of  $M$  and  $N$ , and will be denoted by  $M \otimes_R N$ .

The next result shows that the tensor product is uniquely determined up to isomorphism by the properties (i) and (ii) of (12.3).

(12.7) COROLLARY. Let  $(M \otimes'_R N, t')$  be another pair consisting of an abelian group  $M \otimes'_R N$  and a balanced map  $t': M \times N \rightarrow M \otimes'_R N$  such that conditions (i) and (ii) of Theorem 12.3 hold. Then there exists a group isomorphism  $\lambda$  of  $M \otimes_R N$  onto  $M \otimes'_R N$  such that for all  $(m, n) \in M \times N$ , we have

$$\lambda(t(m, n)) = t'(m, n).$$

PROOF. Applying Theorem 12.3, there exist homomorphisms  $\lambda: M \otimes_R N \rightarrow M \otimes'_R N$  and  $\mu: M \otimes'_R N \rightarrow M \otimes_R N$  such that

$$\lambda(t(m, n)) = t'(m, n)$$

and

$$\mu(t'(m, n)) = t(m, n).$$

Because the elements  $\{t(m, n)\}$  and  $\{t'(m, n)\}$  generate the groups  $M \otimes_R N$  and  $M \otimes'_R N$ , respectively, it follows that  $\mu\lambda$  and  $\lambda\mu$  are the identity mappings on  $M \otimes_R N$  and  $M \otimes'_R N$ , respectively. Therefore both  $\lambda$  and  $\mu$  are isomorphisms onto, and the corollary is proved.

To recapitulate, we have now defined the tensor product  $M \otimes_R N$  and have constructed a balanced map

$$M \times N \rightarrow M \otimes_R N.$$

Henceforth we shall write  $m \otimes n$  for the image of  $(m, n)$  under this map. From the proof of Theorem 12.3, we see that the “products”  $m \otimes n$  satisfy

$$(12.8) \quad \begin{cases} (m_1 + m_2) \otimes n = m_1 \otimes n + m_2 \otimes n, \\ m \otimes (n_1 + n_2) = m \otimes n_1 + m \otimes n_2, \\ mr \otimes n = m \otimes rn, \quad m_i \in M, n_i \in N, r \in R. \end{cases}$$

These give, in a sense, the basic relations which hold in  $M \otimes_R N$ .

Now let  $f: M \times N \rightarrow P$  be a balanced map; then we know that there exists a homomorphism  $f^*: M \otimes_R N \rightarrow P$  such that

$$f^*(m \otimes n) = f(m, n).$$

Since every element of  $M \otimes_R N$  is expressible as  $\sum m_i \otimes n_i$ , this shows that in fact  $f^*$  is uniquely determined by  $f$ . In other words

(12.9) **COROLLARY.** *Every balanced map of  $M \times N$  into an arbitrary abelian group  $P$  can be factored in one and only one way through  $M \otimes_R N$ .*

(12.10) **THEOREM.** *Let  $f: M \rightarrow M'$  and  $g: N \rightarrow N'$  be  $R$ -homomorphisms, where  $M$  and  $M'$  are right  $R$ -modules and  $N$  and  $N'$  left  $R$ -modules. Then there exists a unique homomorphism  $f \otimes g$  of  $M \otimes_R N \rightarrow M' \otimes_R N'$  such that*

$$(f \otimes g)(m \otimes n) = f(m) \otimes g(n).$$

**PROOF.** The map  $(m, n) \rightarrow f(m) \otimes g(n)$  is balanced, and the existence of  $f \otimes g$  is immediate from Theorem 12.3. The uniqueness follows from (12.9).

If  $f$  and  $g$  are as in (12.10) and if  $f': M' \rightarrow M''$  and  $g': N' \rightarrow N''$  are  $R$ -homomorphisms, we have the important formula

$$(12.11) \quad (f' \otimes g')(f \otimes g) = f'f \otimes g'g.$$

The proof of (12.11) is immediate and will be omitted.

It is necessary to interject a word of caution before proceeding to the next result. Let  $M$  be a right  $R$ -module,  $N$  a left  $R$ -module, and  $M_1$  a submodule of  $M$ . Then  $M_1$  is itself a right  $R$ -module, and so we may form  $M_1 \otimes_R N$ . We thus have two balanced maps

$$\begin{aligned} t: M \times N &\rightarrow M \otimes_R N, \\ t_1: M_1 \times N &\rightarrow M_1 \otimes_R N. \end{aligned}$$

For  $m_1 \in M_1$  and  $n \in N$ , the symbol  $m_1 \otimes n$  is ambiguous since it could signify either  $t(m_1, n)$  or  $t_1(m_1, n)$ . One might hope to avoid the necessity of distinguishing between these two meanings by embedding  $M_1 \otimes_R N$  in  $M \otimes_R N$  in some natural way. Let us show by means of an example that this *cannot* be accomplished in general. Let us set

$$M = Q \text{ (rational field)}, \quad M_1 = Z, \quad N = Z/2Z,$$

all viewed as  $Z$ -modules. Then we claim that

$$M \otimes_Z N = 0, \quad M_1 \otimes_Z N \cong N.$$

The former holds since for  $x \in M$ ,  $n \in N$ ,

$$x \otimes n = \frac{1}{2}x \otimes 2n = \frac{1}{2}x \otimes 0 = 0.$$

The latter isomorphism is given by [see Theorem 12.14]

$$z \otimes n \rightarrow zn, \quad z \in M_1, n \in N.$$

In view of the above remarks, the fact that the following very useful result holds is remarkable:

(12.12) THEOREM. *Let  $M$  be a right  $R$ -module such that  $M = M_1 \oplus M_2$  where  $M_1$  and  $M_2$  are submodules, and let  $N$  be a left  $R$ -module. Then*

$$M \otimes_R N \cong M_1 \otimes_R N + M_2 \otimes_R N.$$

PROOF. By the remarks at the end of §11B, the existence of the direct sum decomposition  $M = M_1 \oplus M_2$  implies the existence of  $\pi_1, \pi_2 \in \text{Hom}_R(M, M)$  such that

$$(12.13) \quad 1 = \pi_1 + \pi_2, \quad \pi_1^2 = \pi_1, \quad \pi_2^2 = \pi_2, \quad \pi_1\pi_2 = \pi_2\pi_1 = 0, \\ \pi_1 M = M_1, \quad \pi_2 M = M_2.$$

Set  $\theta_i = \pi_i \otimes 1$ ,  $i = 1, 2$ ; by Theorem 12.10, each  $\theta_i$  is an endomorphism of  $M \otimes_R N$ , and, from (12.13) and (12.11), we have

$$1 = \theta_1 + \theta_2, \quad \theta_1^2 = \theta_1, \quad \theta_2^2 = \theta_2, \quad \theta_1\theta_2 = \theta_2\theta_1 = 0.$$

Setting

$$T_i = \theta_i(M \otimes_R N), \quad i = 1, 2,$$

we conclude that

$$M \otimes_R N = T_1 \oplus T_2.$$

In order to complete the proof, it is sufficient to show, for example, that  $T_1 \cong M_1 \otimes_R N$ . We shall prove this by showing that  $T_1$  has the characteristic properties of a tensor product as given in Theorem 12.3. We must find a balanced map  $\varphi: M_1 \times N \rightarrow T_1$  for which the images  $\{\varphi(m_1, n) : m_1 \in M_1, n \in N\}$  generate  $T_1$ , and such that every balanced map  $g: M_1 \times N \rightarrow P$  can be factored through  $T_1$  by means of  $\varphi$ .

Let us write

$$t: M \times N \rightarrow M \otimes_R N$$

for the mapping determined in Theorem 12.3.

Since  $M_1 \times N \subset M \times N$ , we may set  $\varphi = t|_{M_1 \times N}$ , so that

$$\varphi(m_1, n) = t(m_1, n), \quad m_1 \in M_1, n \in N.$$

It is clear from the equation  $M_1 = \pi_1 M$  and the definition of  $T_1$  that the image of  $M_1 \times N$  under  $\varphi$  does indeed generate  $T_1$ . Now let  $g: M_1 \times N \rightarrow P$  be a balanced map, where  $P$  is any additive abelian group. The bottom line of the following diagram gives a balanced map of  $M \times N$  into  $P$ , and so there exists a homomorphism  $g^*: M \otimes_R N \rightarrow P$  making the diagram commutative.

$$\begin{array}{ccccc} & & M \otimes_R N & & \\ & \nearrow t & & \searrow g^* & \\ M \times N & \xrightarrow{(\pi_1 \times 1)} & M_1 \times N & \xrightarrow{g} & P \end{array}$$

Let us set  $g_1 = g^*|_{T_1}$ , so that  $g_1$  is a homomorphism of  $T_1$  into  $P$ . To complete the proof, we need only verify that

$$g_1 \varphi = g \text{ on } M_1 \times N.$$

But for  $m_1 \in M_1, n \in N$ , we have

$$\begin{aligned} g_1 \varphi(m_1, n) &= g_1 t(m_1, n) = g^* t(m_1, n) \\ &= g(\pi_1 \times 1)(m_1, n) = g(\pi_1 m_1, n) = g(m_1, n). \end{aligned}$$

This establishes the result.

Of course, the argument of the preceding theorem can be extended to any finite number of direct summands of either  $M$  or  $N$ . The result is still valid for infinite direct sums (Bourbaki [1]), but this stronger theorem will not be needed anywhere in this book. It should also be pointed out that the theorem permits us to regard  $M_1 \otimes_R N$  as embedded in  $M \otimes_R N$  whenever  $M_1$  is an  $R$ -direct summand of  $M$ .

Now we investigate the circumstances under which  $M \otimes_R N$  is a module over some ring. We say that an abelian group  $M$  is an  $(S, R)$ -bimodule over the rings  $R$  and  $S$  if  $M$  is a left  $S$ -module and a right  $R$ -module, and if we have

$$(sm)r = s(mr)$$

for all  $s \in S$ ,  $r \in R$ ,  $m \in M$ . For example, any left module  $M$  over a commutative ring  $R$  is an  $(R, R)$ -bimodule if we define  $mr = rm$ ,  $r \in R$ ,  $m \in M$ .

Now we shall prove that if  $M$  is an  $(S, R)$ -bimodule and  $N$  a left  $R$ -module, then  $M \otimes_R N$  is a left  $S$ -module. Let  $s$  be a fixed element of  $S$ . Then the mapping  $(m, n) \rightarrow sm \otimes n$  of  $M \times N$  into  $M \otimes_R N$  is a balanced map, and, by Theorem 12.3, there exists an endomorphism  $\phi_s$  of  $M \otimes_R N$  such that  $\phi_s(m \otimes n) = sm \otimes n$ . We can now define, for each  $s \in S$ ,

$$s(\sum m_i \otimes n_i) = \phi_s(\sum m_i \otimes n_i) = \sum sm_i \otimes n_i,$$

and conclude that  $M \otimes_R N$  is a left  $S$ -module with respect to this operation.

(The above procedure for making  $M \otimes_R N$  into a left  $S$ -module may seem at first to be a roundabout approach. It would seem simpler to define

$$s(\sum m_i \otimes n_i) = \sum sm_i \otimes n_i,$$

but then we would have the difficulty of showing that the above definition is meaningful, since an element of  $M \otimes_R N$  is expressible in more than one way as a sum  $\sum m_i \otimes n_i$ . The use of a balanced map of  $M \times N$  into  $M \otimes_R N$  avoids the above difficulty.)

We remark that if  $M = M_1 \oplus M_2$ , all these being  $(S, R)$ -bimodules, and if  $N$  is a left  $R$ -module, then the isomorphism

$$M \otimes_R N \cong M_1 \otimes_R N + M_2 \otimes_R N$$

obtained in Theorem 12.12 is an isomorphism of left  $S$ -modules.

Now let  $N$  be a left  $R$ -module; since  $R$  is an  $(R, R)$ -bimodule,

the tensor product  $R \otimes_R N$  is a left  $R$ -module. The following result is basic:

(12.14) THEOREM.  $R \otimes_R N \cong N$  as left  $R$ -modules.

PROOF. The map  $(r, n) \rightarrow rn$  is a balanced map of  $R \times N$  into  $N$ , and so by (12.3) there exists a homomorphism  $\varphi: R \otimes_R N \rightarrow N$  such that

$$\varphi(r \otimes n) = rn .$$

On the other hand, we may define a homomorphism  $\psi: N \rightarrow R \otimes_R N$  by

$$\psi(n) = 1 \otimes n , \quad n \in N .$$

Clearly  $\varphi\psi = \text{identity map on } N$ ; furthermore,

$$\psi\varphi(r \otimes n) = \psi(rn) = 1 \otimes rn = r \otimes n ,$$

so  $\psi\varphi$  acts as the identity map on  $R \otimes_R N$ . This implies that  $\varphi$  is an isomorphism of  $R \otimes_R N$  onto  $N$ , and it is easily seen to be an  $R$ -isomorphism of left  $R$ -modules. The theorem is thus proved.

An equally basic result is

(12.15) THEOREM. (Associativity of the Tensor Product). Let  $L$  be a right  $R$ -module,  $M$  an  $(R, S)$ -bimodule, and  $N$  a left  $S$ -module where  $R$  and  $S$  are rings. Then  $L \otimes_R M$  is a right  $S$ -module,  $M \otimes_S N$  a left  $R$ -module, and we have

$$(L \otimes_R M) \otimes_S N \cong L \otimes_R (M \otimes_S N) .$$

PROOF. We use Theorem 12.3 to deduce that the mappings

$$\lambda: (l \otimes m) \otimes n \rightarrow l \otimes (m \otimes n) ,$$

$$\mu: l \otimes (m \otimes n) \rightarrow (l \otimes m) \otimes n ,$$

define homomorphisms for which  $\lambda\mu = 1$ ,  $\mu\lambda = 1$ . The details of the proof are left as an exercise to the reader.

For the remainder of this section, we shall discuss some important special cases of tensor products.

### § 12A. Tensor products of vector spaces

Let  $M$  and  $N$  be finite-dimensional left vector spaces over a field  $K$ . As we remarked earlier,  $M$  is a  $(K, K)$ -bimodule, and  $M \otimes_K N$  becomes a  $K$ -space if we define

$$\xi(\sum u_i \otimes v_i) = \sum \xi u_i \otimes v_i , \quad \xi \in K , u_i \in M , v_i \in N .$$

Now  $M$  is isomorphic to an external direct sum of  $r$  copies of  $K$  where  $r = (M : K)$ , and so by repeated use of Theorems (12.12) and (12.14), we have

$$M \otimes_K N \cong N + \cdots + N \quad (r \text{ copies})$$

as left  $K$ -modules. This proves that

$$(12.16) \quad (M \otimes_K N : K) = (M : K)(N : K).$$

Suppose now that

$$(12.17) \quad M = Km_1 \oplus \cdots \oplus Km_r, \quad N = Kn_1 \oplus \cdots \oplus Kn_s,$$

where  $s = (N : K)$ . Using the distributivity formulas (12.8), we see that every element of  $M \otimes_K N$  is expressible as

$$\sum_{\substack{1 \leq i \leq r \\ 1 \leq j \leq s}} \alpha_{ij} (m_i \otimes n_j), \quad \alpha_{ij} \in K.$$

Since the dimension of  $M \otimes_K N$  is  $rs$ , this proves that the elements  $\{m_i \otimes n_j : 1 \leq i \leq r, 1 \leq j \leq s\}$  form a  $K$ -basis of  $M \otimes_K N$ .

One interesting consequence of the above is that if  $m \in M$ ,  $m \neq 0$ , and  $n \in N$ ,  $n \neq 0$ , then also  $m \otimes n \neq 0$  in  $M \otimes_K N$ . For we may choose  $K$ -bases of  $M$  and  $N$  so that  $m$  is one of the basis elements for  $M$ , and  $n$  for  $N$ , and then we know that  $m \otimes n$  is one of the elements in a basis for  $M \otimes_K N$ . Therefore  $m \otimes n \neq 0$  in  $M \otimes_K N$ .

Let  $T: M_1 \rightarrow M'_1$  and  $U: M_2 \rightarrow M'_2$  be linear transformations, where  $M_i$ ,  $M'_i$ ,  $i = 1, 2$ , are vector spaces over  $K$ . Then the homomorphism  $T \otimes U$  defined in Theorem 12.10 is a  $K$ -homomorphism of  $M_1 \otimes_K M_2$  into  $M'_1 \otimes_K M'_2$ . In particular, let  $T \in \text{Hom}_K(M, M')$ ,  $U \in \text{Hom}_K(N, N)$ . Then  $T \otimes U \in \text{Hom}_K(M \otimes_K N, M' \otimes_K N)$ , and we shall compute its matrix with respect to the basis  $\{m_i \otimes n_j\}$  of  $M \otimes_K N$ , where  $M$  and  $N$  are given by (12.17). Let

$$Tm_i = \sum_{j=1}^r \alpha_{ji} m_j$$

and

$$Un_i = \sum_{j=1}^s \beta_{ji} n_j;$$

then  $T = (\alpha_{ij})$  and  $U = (\beta_{ij})$  are the matrices of  $T$  and  $U$  with respect to the bases  $\{m_i\}$  and  $\{n_i\}$ . For any  $i$  and  $j$ , we have

$$\begin{aligned}
 (T \otimes U)(m_i \otimes n_j) &= Tm_i \otimes Un_j \\
 &= \sum_{l=1}^r \alpha_{li} m_l \otimes \sum_{k=1}^s \beta_{kj} n_k \\
 &= \sum_{l=1}^r \sum_{k=1}^s \alpha_{li} \beta_{kj} (m_l \otimes n_k).
 \end{aligned}$$

It is clear that if we arrange the basis  $\{m_i \otimes n_j\}$  into  $s$  blocks of  $r$  vectors each,

$$m_1 \otimes n_j, \dots, m_r \otimes n_j, \quad 1 \leq j \leq s,$$

then the matrix of  $T \otimes U$  falls into  $s^2$  blocks of  $r \times r$  submatrices

$$\left( \begin{array}{c|c|c}
 m_1 \otimes n_j & \cdots & m_r \otimes n_j \\
 \hline
 m_1 \otimes n_k & & \\
 \vdots & & \\
 m_r \otimes n_k & & \beta_{kj} \mathbf{T} \\
 \hline
 & &
 \end{array} \right),$$

in which the  $r \times r$  block appearing in the  $k$ th row of blocks and  $j$ th column of blocks is  $\beta_{kj}$  times the matrix  $\mathbf{T}$  of  $T$ . In other words, we get the matrix of  $T \otimes U$  by taking the matrix  $(\beta_{kj})$  of  $U$  and replacing each entry  $\beta_{kj}$  by the  $r \times r$  matrix  $\beta_{kj}(\alpha_{pq})$ , where  $(\alpha_{pq})$  is the matrix of  $T$ . This matrix of  $T \otimes U$  is often referred to as the *Kronecker* or *direct product*  $\mathbf{T} \times \mathbf{U}$  of the matrices  $\mathbf{T}$  and  $\mathbf{U}$ .

These ideas lead to an important construction involving representations of finite groups. Let  $T: G \rightarrow GL(M)$  and  $U: G \rightarrow GL(N)$  be representations of a finite group  $G$ . Then the *tensor product representation*

$$T \otimes U: G \rightarrow GL(M \otimes N)$$

is the mapping which assigns to each  $g \in G$  the linear transformation  $(T \otimes U)(g)$  of  $M \otimes N$ , where  $(T \otimes U)(g)$  is given by

$$(T \otimes U)(g) = T(g) \otimes U(g).$$

The fact that  $T \otimes U$  is a representation follows from (12.11). Its importance stems from the fact that it mixes together the representations  $T$  and  $U$  in such a way that we may expect to find in a reduction of  $T \otimes U$  new representations besides  $T$  and  $U$ . (See Theorem 32.9, for example.)

The matrix representation afforded by  $T \otimes U$  is given by

$$\mathbf{T} \dot{\times} \mathbf{U}: g \rightarrow \mathbf{T}(g) \dot{\times} \mathbf{U}(g)$$

where  $\mathbf{T}$  and  $\mathbf{U}$  are matrix representations afforded by  $T$  and  $U$ , respectively.

Now let  $M$  and  $N$  be left  $KG$ -modules. Then  $M \otimes_K N$  becomes a left  $KG$ -module if we define

$$g(m \otimes n) = gm \otimes gn, \quad g \in G, m \in M, n \in N,$$

and extend the domain of left operators of  $M \otimes_K N$  to  $KG$  in the usual way. This module affords the representation  $T \otimes U$  defined above [It is important to realize that this idea does not mean that we can turn into a left  $A$ -module the tensor product of two left modules  $M$  and  $N$  over an algebra  $A$  by defining

$$a(m \otimes n) = am \otimes an, \quad a \in A, m \in M, n \in N.$$

In fact,  $M \otimes_K N$  is *not* a left  $A$ -module under this operation.]

We conclude this subsection with the result that

$$(12.18) \quad \text{Hom}_K(M \otimes_K N, M \otimes_K N) \cong \text{Hom}_K(M, M) \otimes_K \text{Hom}_K(N, N).$$

To prove this, let  $M$  and  $N$  be given by (12.17). For each  $i$  and  $j$ , let  $E_{ij}$  be the linear transformation of  $M$  such that

$$E_{ij}m_j = m_i, \quad E_{ij}m_k = 0 \quad \text{if } j \neq k,$$

and let  $F_{ij}$  be defined similarly on  $N$ . Then since  $\{m_i \otimes n_j\}$  is a basis of  $M \otimes_K N$ , it follows immediately that the linear transformations  $\{E_{ij} \otimes F_{kl}\}$  are linearly independent. Since there are  $r^2s^2$  distinct transformations among the  $\{E_{ij} \otimes F_{kl}\}$ , it follows that these linear transformations span  $\text{Hom}_K(M \otimes_K N, M \otimes_K N)$  over  $K$ . Therefore every linear transformation in  $\text{Hom}_K(M \otimes_K N, M \otimes_K N)$  can be expressed in the form

$$\sum T_i \otimes U_i, \quad T_i \in \text{Hom}_K(M, M), U_i \in \text{Hom}_K(N, N).$$

A count of the dimensions on both sides finishes the proof of (12.18). Using the isomorphism

$$K_r \cong \text{Hom}_K(M, M),$$

obtained in §8, where  $K_r$  is the ring of  $r \times r$  matrices over  $K$ , we deduce as a corollary to (12.18) the fact that

$$(12.19) \quad K_r \otimes_K K_s \cong K_{rs}.$$

### § 12B. Extension of the field of scalars of a vector space

Let  $V$  be a vector space over a field  $K$  with basis  $\{v_1, \dots, v_r\}$ , and let  $L$  be an arbitrary extension field over  $K$ . Since  $V$  consists

of all  $K$ -linear combinations of the  $\{v_i\}$ , it would seem natural to consider the set of all  $L$ -linear combinations of the  $\{v_i\}$  as a new vector space over  $L$  which contains the old space  $V$  and, in fact, has the same basis  $\{v_1, \dots, v_r\}$ . We shall use the theory of tensor products to give a rigorous justification of this procedure.

Since  $K$  is a subfield of  $L$ , it is clear that  $L$  is an  $(L, K)$ -bimodule, and so  $L \otimes_K V$  is a vector space over  $L$ . Since  $V$  is isomorphic to an external direct sum of  $r$  copies of  $K$ , it follows from Theorems (12.12) and (12.14) that  $L \otimes_K V$  is isomorphic (as left  $L$ -module) to an external direct sum of  $r$  copies of  $L$ . Therefore

$$(12.20) \quad (L \otimes_K V : L) = (V : K),$$

from which it follows immediately that the elements

$$(12.21) \quad 1 \otimes v_1, \dots, 1 \otimes v_r$$

form an  $L$ -basis for  $L \otimes_K V$ . Let us set

$$L \otimes_K V = V^L$$

for brevity, so that  $V^L$  is the  $L$ -space with basis given by (12.21); we have

$$\alpha(\sum \alpha_i \otimes v_i) = \sum \alpha \alpha_i \otimes v_i = \sum \alpha \alpha_i (1 \otimes v_i)$$

for all  $\alpha, \alpha_i \in L$ .

We remark finally that  $v \rightarrow 1 \otimes v$ ,  $v \in V$ , gives a  $K$ -isomorphism of  $V$  into  $V^L$ , and we shall often identify  $V$  with its image  $1 \otimes V$  in  $V^L$ . In this sense,  $V$  is a subspace of  $V^L$ , and any  $K$ -basis of  $V$  is also an  $L$ -basis for  $V^L$ .

Suppose now that  $A$  is a  $K$ -algebra; then it is easily verified that  $A^L$  is an  $L$ -algebra, with multiplication given by

$$(\sum \lambda_i a_i)(\sum \mu_j b_j) = \sum \lambda_i \mu_j a_i b_j$$

for  $\lambda_i, \mu_j \in L$ ,  $a_i, b_j \in A$ . (We have dropped the symbol  $\otimes$  since we are regarding  $A$  as embedded in  $A^L$ .) If furthermore  $M$  is an  $A$ -module, then  $M$  is also a  $K$ -space, and we may form  $M^L$ . It is then straightforward to show that  $M^L$  is an  $A^L$ -module, with module composition given by

$$(\sum \lambda_i a_i)(\sum \mu_j m_j) = \sum \lambda_i \mu_j (a_i m_j),$$

for all  $\lambda_i, \mu_j \in L$ ,  $a_i \in A$ ,  $m_j \in M$ .

### §12C. Tensor products of algebras over a field.

Let  $A$  and  $A'$  be algebras over  $K$  with identity elements  $1$  and  $1'$ , respectively. Then  $A \otimes_K A'$  is, by the discussion in §12A, a vector space over  $K$ . We shall prove that the multiplication

$$(12.22) \quad (\sum a_i \otimes a'_i)(\sum b_j \otimes b'_j) = \sum_{i,j} a_i b_j \otimes a'_i b'_j , \\ a_i, b_j \in A, a'_i, b'_j \in A' ,$$

is well defined and turns  $A \otimes_K A'$  into an algebra over  $K$ . It is sufficient to prove, for example, that if

$$\sum_{i=1}^n a_i \otimes a'_i = \sum_{i=1}^m \bar{a}_i \otimes \bar{a}'_i ,$$

then

$$\left( \sum_{i=1}^n a_i \otimes a'_i \right) (\sum b_j \otimes b'_j) = \left( \sum_{i=1}^m \bar{a}_i \otimes \bar{a}'_i \right) (\sum b_j \otimes b'_j) ,$$

and for this it is enough to prove that if  $\sum a_i \otimes a'_i = 0$ , then

$$(\sum a_i \otimes a'_i)(\sum b_j \otimes b'_j) = 0 .$$

Let  $\{e_1, \dots, e_r\}$  be a basis of  $A$ , and let  $\{e'_1, \dots, e'_s\}$  be a basis for  $A'$ . Then

$$a_i = \sum \alpha_{ik} e_k , \quad a'_i = \sum \alpha'_{il} e'_l , \quad \alpha_{ik}, \alpha'_{il} \in K ,$$

and

$$\sum a_i \otimes a'_i = \sum_{i,k,l} \alpha_{ik} \alpha'_{il} e_k \otimes e'_l = 0 .$$

Since the  $\{e_k \otimes e'_l\}$  form a basis for  $A \otimes_K A'$ , we have

$$(12.23) \quad \sum_i \alpha_{ik} \alpha'_{il} = 0$$

for all pairs  $(k, l)$ . Then

$$\begin{aligned} \sum_{i,j} a_i b_j \otimes a'_i b'_j &= \sum_{i,j,k,l} \alpha_{ik} \alpha'_{il} e_k b_j \otimes e'_l b'_j \\ &= \sum_{k,l,j} \left( \sum_i \alpha_{ik} \alpha'_{il} \right) e_k b_j \otimes e'_l b'_j = 0 \end{aligned}$$

by (12.23), and our assertion is proved. It is possible to give a more conceptual proof of this result, but no harm is done occasionally by performing the computation in what is, after all, a rather simple problem.

Once we have proved that the multiplication (12.22) is well defined, it is clear that  $A \otimes_K A'$  is an algebra over  $K$ . The subsets  $A \otimes 1'$  and  $1 \otimes A'$  are subalgebras of  $A \otimes_K A'$  which are isomorphic

to  $A$  and  $A'$ , respectively. The elements in  $A \otimes 1'$  and  $1 \otimes A'$  commute with each other, and their products generate  $A \otimes_K A'$  over  $K$ .

### § 12D. Induced representations and induced modules

Let  $H$  be a subgroup of a finite group  $G$ , and let  $K$  be an arbitrary field. All modules will be assumed to be finite-dimensional  $K$ -spaces. Since  $KH$  is a subalgebra of  $KG$ , every  $KG$ -module  $L$  is also a  $KH$ -module which we shall denote by  $L_H$ . Thus  $L_H$  has the same underlying vector space as  $L$ , but the domain of left operators is  $KH$  instead of  $KG$ . A matrix representation  $\mathbf{T}_H$  of  $H$  afforded by  $L_H$  is obtained from a matrix representation  $\mathbf{T}$  of  $G$  afforded by  $L$  by setting

$$\mathbf{T}_H = \mathbf{T}|_H.$$

Our objective here is to describe a construction, due originally to Frobenius [1], which associates with each  $KH$ -module  $M$  an *induced KG-module*  $M^G$ . This construction will prove to be of fundamental importance in Chapters VI and VII and is one of the basic tools in the entire theory of group representations. We shall begin with

(12.24) **DEFINITION.** Let  $H$  be a subgroup of  $G$ , and let  $M$  be a left  $KH$ -module. Then  $KG$  is a  $(KG, KH)$ -bimodule, and we may form the left  $KG$ -module

$$M^G = KG \otimes_{KH} M$$

which is said to be *induced from  $M$* . The representation of  $G$  afforded by  $M^G$  is called an *induced representation*.

In order to calculate with  $M^G$ , let us start with a left coset decomposition

$$(12.25) \quad G = g_1H \cup g_2H \cup \cdots \cup g_tH, \quad t = [G : H],$$

where  $g_1 = 1$ . Every element of  $G$  is expressible as a product  $g_i h$ ,  $1 \leq i \leq t$ ,  $h \in H$ , with uniquely determined  $g_i$  and  $h$ , and so every element of  $KG$  is uniquely expressible as

$$\sum_{i=1}^t g_i b_i, \quad b_i \in KH.$$

Thus we have

$$KG = g_1KH \oplus \cdots \oplus g_tKH,$$

so that  $KG$  is a free right  $KH$ -module with basis  $\{g_1, \dots, g_t\}$ .

Using Theorem 12.12, we obtain

$$M^g = g_1 KH \otimes_{KH} M \oplus \cdots \oplus g_t KH \otimes_{KH} M,$$

which we may rewrite as

$$(12.26) \quad M^g = g_1 \otimes M \oplus \cdots \oplus g_t \otimes M$$

by virtue of the formula

$$g_i b \otimes m = g_i \otimes bm, \quad b \in KH, m \in M.$$

In (12.26), we have a decomposition of  $M^g$  into  $K$ -subspaces which are, in general, neither left  $KG$ - nor  $KH$ -submodules of  $M^g$ . We note that, since  $g_i KH \cong KH$  as right  $KH$ -modules, with the isomorphism being given by  $g_i b \rightarrow b$ ,  $b \in KH$ , it follows that

$$g_i KH \otimes_{KH} M \cong KH \otimes_{KH} M \cong M$$

by Theorem 12.14. Thus

$$g_i b \otimes m \rightarrow bm, \quad b \in KH, m \in M,$$

gives an isomorphism

$$g_i KH \otimes_{KH} M \cong M$$

which is easily seen to be a  $K$ -isomorphism. Therefore

$$(12.27) \quad (M^g : K) = [G : H](M : K),$$

and we conclude further that every element of  $M^g$  is expressible as  $\sum g_i \otimes u_i$  with uniquely determined  $u_1, \dots, u_t$  in  $M$ . It follows from this that if  $\{m_1, \dots, m_r\}$  is a  $K$ -basis for  $M$ , then the elements

$$(12.28) \quad \{g_i \otimes m_j : 1 \leq i \leq t, 1 \leq j \leq r\}$$

form a  $K$ -basis for  $M^g$ .

We are now going to determine a matrix representation afforded by  $M^g$  once we know a matrix representation afforded by  $M$ . Suppose that, relative to its  $K$ -basis  $\{m_1, \dots, m_r\}$ ,  $M$  affords the matrix representation  $T$ , so that

$$hm_i = \sum \alpha_{ji}(h)m_j, \quad T(h) = (\alpha_{ij}(h)), \quad h \in H.$$

Relative to the  $K$ -basis (12.28) of  $M^g$ , let us compute the matrix representation  $U$  afforded by  $M^g$ ; to do this, we must express  $g(g_i \otimes m_j)$  as a  $K$ -linear combination of the basis elements. We may write

$$gg_i = g_k h,$$

for some  $h \in H$  and for some  $k$ ,  $1 \leq k \leq t$ ; then

$$\begin{aligned} g(g_i \otimes m_j) &= gg_i \otimes m_j = g_k \otimes hm_j \\ &= \sum_{s=1}^r \alpha_{sj}(h)g_k \otimes m_s . \end{aligned}$$

Now we have  $h = g_k^{-1}gg_i$ . If we agree to extend the domain of definition of  $\alpha_{sj}$  from  $H$  to  $G$  by setting

$$\alpha_{sj}(x) = 0 , \quad x \in G, x \notin H ,$$

then we may rewrite our formula as

$$g(g_i \otimes m_j) = \sum_{s=1}^r \sum_{k=1}^t \alpha_{sj}(g_k^{-1}gg_i) \cdot g_k \otimes m_s .$$

If we arrange the basis elements (12.28) in the order

$$g_1 \otimes m_1, \dots, g_1 \otimes m_r, g_2 \otimes m_1, \dots, g_2 \otimes m_r, \dots, g_t \otimes m_1, \dots, g_t \otimes m_r ,$$

then the preceding equation implies that for each  $g \in G$ ,

$$U(g) = \left( \begin{array}{c|c|c} (i, 1) \cdots (i, r) & & \\ \hline * & * & * \\ \hline * & T(g_j^{-1}gg_i) & * \\ \hline * & * & * \end{array} \right) \begin{matrix} (j, 1) \\ \vdots \\ (j, r) \end{matrix}$$

where  $T$  is extended to all of  $G$  by setting  $T(x) = 0$  for  $x \in G, x \notin H$ . Thus  $U(g)$  is partitioned into a  $t \times t$  array of  $r \times r$  blocks, and the block in the  $j$ th block row and  $i$ th block column is  $T(g_j^{-1}gg_i)$ . Specifically, we have

$$(12.29) \quad U(g) = \begin{bmatrix} T(g_1^{-1}gg_1) & \cdots & T(g_1^{-1}gg_t) \\ \ddots & \cdots & \ddots \\ T(g_t^{-1}gg_1) & \cdots & T(g_t^{-1}gg_t) \end{bmatrix}.$$

### Exercises

1. Let  $T \in \text{Hom}_K(M, M)$  and  $U \in \text{Hom}_K(N, N)$ . Prove that

$$\text{tr}(T \otimes U) = (\text{tr } T)(\text{tr } U) .$$

(See Exercise 8.1).

2. Let  $M$  and  $N$  be vector spaces over a field  $K$ . Prove that if  $m_1, \dots, m_r$  are linearly independent in  $M$ , then for  $n_i \in N$ ,  $\sum m_i \otimes n_i = 0$  implies  $n_1 = \dots = n_r = 0$ .

3. Let  $M$  and  $N$  be vector spaces over  $K$ , and let  $M \circ N$  be a vector space over  $K$  such that there exists a bilinear map  $(m, n) \rightarrow m \circ n$  of  $M \times N$  into  $M \circ N$  with the additional property that, whenever  $m_1, \dots, m_r$  are linearly independent in  $M$ , for  $n_i \in N$ ,  $\sum m_i \circ n_i = 0$  implies all  $n_i = 0$ . Prove that  $M \circ N \cong M \otimes_K N$ .

4. Let  $M$  and  $N$  be finite-dimensional vector spaces over  $K$ , and let  $M^*$  be the dual space of  $M$ , that is, the set of all linear functions on  $M$  to  $K$ . For each  $\psi \in M^*$ ,  $n \in N$ , show that the mapping  $\psi \circ n$  defined by

$$(\psi \circ n)(u) = \psi(u)n, \quad u \in M,$$

is an element of  $\text{Hom}_K(M, N)$ . Prove that  $(\psi, n) \rightarrow \psi \circ n$  is a bilinear mapping of  $M \times N$  into  $\text{Hom}_K(M, N)$  and that  $\text{Hom}_K(M, N)$  is generated as a  $K$ -module by the elements  $\psi \circ n$ . Finally prove that  $\text{Hom}_K(M, N) \cong M^* \otimes_K N$ .

5. Let  $A$  and  $B$  be subalgebras of a finite-dimensional algebra  $C$ , both containing the identity element of  $C$ . Suppose that  $ab = ba$  for all  $a \in A$ ,  $b \in B$ , and that  $(C : K) = (A : K)(B : K)$ . Prove that  $C \cong A \otimes_K B$  as  $K$ -algebras, assuming that  $C = A \cdot B$ .

6. Let  $D$  be a finite-dimensional algebra over  $K$ , and let  $D_m$  be the algebra of  $m \times m$  matrices over  $D$ . Prove that  $D_m \cong D \otimes_K K_m$  as  $K$ -algebras.

7. Prove that the isomorphisms given in (12.18) and (12.19) are isomorphisms of the algebras involved.

8. Let  $G_1, G_2$  be finite groups and  $G = G_1 \times G_2$  their direct product. Prove that  $K(G_1 \times G_2) \cong KG_1 \otimes_K KG_2$  as  $K$ -algebras.

9. Let  $H$  be a subgroup of a finite group  $G$ , and let  $T$  be the 1-representation of  $H$  which maps every  $h \in H$  onto the identity element 1 in  $K$ . Prove that the induced matrix representation  $T^G$  is a representation of  $G$  by permutation matrices. If  $H$  is the trivial subgroup consisting of the identity alone and  $T$  the 1-representation of  $H$ , prove that  $T^G$  is equivalent to the left regular representation of  $G$  (see § 10).

10. Let  $H$  be a subgroup of a finite group  $G$ , and let  $T$  be a one-to-one representation of  $H$ . Prove that  $T^G$  is a one-to-one representation of  $G$ .

### § 13. Composition Series

In the next three sections, we investigate more thoroughly the classification of modules begun for  $KG$ -modules in § 10. We shall call a submodule of an  $R$ -module  $M$  *trivial* if it coincides with either  $M$  or  $(0)$ ; otherwise it is *non-trivial*. A submodule  $N$  of  $M$  is properly contained in  $M$  if  $N \neq M$ ; in this case  $N$  is called a *proper submodule* of  $M$ .

(13.1) **DEFINITION.** A left  $R$ -module  $M \neq (0)$  is called *irreducible* if  $M$  contains no non-trivial submodules, whereas a module which con-

tains a non-trivial submodule is called *reducible*. A *maximal submodule*  $N$  of  $M$  is a maximal element in the set of proper submodules of  $M$ , ordered by inclusion. Thus a submodule  $N$  of  $M$  is maximal if and only if (i)  $N \neq M$  and (ii) for each submodule  $N'$  such that  $N \subset N' \subset M$ , either  $N' = N$  or  $N' = M$ . On the other hand,  $N$  is a *minimal submodule* of  $M$  if  $N$  is a non-zero submodule such that for each submodule  $N'$  of  $M$ , the inclusion  $N \supset N' \supset (0)$  implies that either  $N' = N$  or  $N' = (0)$ . In other words, a minimal submodule of  $M$  is the same thing as an irreducible submodule of  $M$ .

For any submodule  $N$  of  $M$ , (11.10) implies that  $M/N$  is irreducible if and only if  $N$  is a maximal submodule of  $M$ .

(13.2) **DEFINITION.** A descending chain

$$(13.3) \quad M = M_1 \supset M_2 \supset \cdots \supset M_k \supset M_{k+1} = (0)$$

of submodules is called a *composition series* of  $M$  if all the factor modules  $M_i/M_{i+1}$  are irreducible. These factor modules  $M_i/M_{i+1}$  are called the *factors* of the composition series. Two composition series are said to be *equivalent* if they have the same number of factors and if the factors can be paired off in such a way that corresponding factors are  $R$ -isomorphic. The number of factors  $k$  is called *length* of the composition series.

Our first task is to give a criterion for the existence of composition series.

(13.4) **THEOREM.** *An  $R$ -module  $M$  has a composition series if and only if  $M$  satisfies both the A.C.C. and the D.C.C. for submodules.*

**PROOF.** First, suppose both the A.C.C. and D.C.C. are satisfied. Applying (11.14) to the set of submodules different from  $M$ , we see that there exists a maximal submodule  $M_1 \subset M$ . Either  $M_1 = (0)$ , or  $M_1$  contains a maximal submodule  $M_2$ . Continuing in this way, we obtain either a composition series or an infinite strictly decreasing chain of submodules. The latter possibility is ruled out, and we conclude that a composition series exists.

Conversely, suppose  $M$  has a composition series of length  $k$

$$M = M_1 \supset M_2 \supset \cdots \supset M_{k+1} = (0).$$

We shall prove by induction on  $k$  that for any properly descending chain of submodules of  $M$ :

$$N_1 \supset N_2 \supset \cdots \supset N_t,$$

we have  $t \leq k + 1$ . From this statement follows that  $M$  satisfies

both chain conditions. The result is clear if  $k = 1$ . We assume  $k > 1$  and consider three cases.

**CASE 1.**  $N_1 = M$ ,  $N_2 \subset M_2$ . Since  $M_2$  has a composition series of length  $k - 1$ , we have by our induction hypothesis  $t - 1 \leq (k - 1) + 1$ , or  $t \leq k + 1$  as required.

**CASE 2.**  $N_1 = M$ ,  $N_2 \not\subset M_2$ . Again we apply the induction hypothesis to conclude that the submodules of  $M_2$  satisfy both chain conditions. Therefore any submodule of  $M_2$  has a composition series, by the first part of the proof. In particular,  $M_2 \cap N_2$  has a composition series

$$(M_2 \cap N_2) \supset L_2 \supset \cdots \supset L_{s+1} = (0),$$

and

$$M_2 \supset (M_2 \cap N_2) \supset L_2 \supset \cdots \supset L_{s+1} = (0)$$

is a strictly decreasing chain of  $s + 2$  submodules of  $M_2$ . Then  $s + 2 \leq k$ . Moreover, by (11.9), we have

$$(M_2 + N_2)/M_2 \cong N_2/(M_2 \cap N_2).$$

Then  $M_2 + N_2 = M$  since  $M_2$  is maximal in  $M$  and  $N_2$  is not contained in  $M_2$ . The module on the left side is irreducible, and hence  $N_2/(M_2 \cap N_2)$  is also irreducible. Therefore

$$N_2 \supset (M_2 \cap N_2) \supset L_2 \supset \cdots \supset L_{s+1} = (0)$$

is a composition series of  $N_2$  of length  $s + 1 \leq k - 1$ . By the induction hypothesis, any strictly descending chain of submodules of  $N_2$  contains at most  $s + 2$  terms. In particular,

$$t - 1 \leq s + 2 \leq k,$$

and  $t \leq k + 1$  as required.

**CASE 3.**  $N_1 \neq M$ . Then  $M \supset N_1 \supset N_2 \supset \cdots \supset N_t$  is a chain falling under one of the previous cases, and we have  $t + 1 \leq k + 1$ . This completes the proof of the theorem.

(13.5) COROLLARY. *If  $M$  is an  $R$ -module which has a composition series, then any two composition series of  $M$  have the same length.*

(13.6) COROLLARY. *Let  $M$  be an  $R$ -module having a composition series of length  $k$ . Then any strictly descending chain  $M \supset N_2 \supset \cdots \supset N_t$  of submodules of  $M$  can be made into a composition series by inserting new submodules at strategic places in the chain.*

Our next result is a still sharper uniqueness result for modules with composition series.

(13.7) THEOREM. (*Jordan-Hölder*). *If an  $R$ -module  $M$  possesses a composition series, any two composition series of  $M$  are equivalent.*

PROOF. Let  $M$  have two composition series:

$$(13.8) \quad \begin{aligned} M &= M_1 \supset M_2 \supset \cdots \supset M_{k+1} = (0), \\ M &= N_1 \supset N_2 \supset \cdots \supset N_{k+1} = (0). \end{aligned}$$

They necessarily have the same length by (13.5). Using induction on  $k$ , we may assume that any two composition series of length less than  $k$  of the same  $R$ -module are equivalent.

If  $M_2 = N_2$ , the result is immediately by the induction hypothesis. Thus we may suppose that  $M_2 \neq N_2$ . Then  $M_2 + N_2 = M$  because  $M_2$  is maximal in  $M$ . By (11.9), we have

$$(13.9) \quad M_1/M_2 \cong N_2/(M_2 \cap N_2), \quad N_1/N_2 \cong M_2/(M_2 \cap N_2),$$

and  $M_2 \cap N_2$  is a maximal submodule of both  $N_2$  and  $M_2$ . Let

$$(M_2 \cap N_2) \supset L_2 \supset \cdots \supset L_{t+1} = (0)$$

be a composition series for  $M_2 \cap N_2$ . Then

$$M = M_1 \supset M_2 \supset (M_2 \cap N_2) \supset L_2 \supset \cdots \supset L_{t+1} = (0)$$

and

$$M = N_1 \supset N_2 \supset (M_2 \cap N_2) \supset L_2 \supset \cdots \supset L_{t+1} = (0)$$

both are composition series of  $M$ . Because of (13.9), we see that these two series are equivalent. By the induction hypothesis, the first is equivalent to the first series of (13.8), whereas the second is equivalent to the second series of (13.8). Therefore the two composition series of (13.8) are equivalent to each other, and the Jordan-Hölder theorem is proved.

We conclude this section with some remarks on matrix representations. Let  $M$  be a left  $KG$ -module where  $KG$  is the group algebra of a finite group  $G$  over a field  $K$ . We assume that  $M$  is a finite-dimensional vector space over  $K$ , and hence  $M$  satisfies both chain conditions for  $KG$ -submodules. These submodules, incidentally, are identical with the  $G$ -subspaces introduced in § 10. By Theorem 13.4,  $M$  has a composition series

$$(13.10) \quad M = M_k \supset M_{k-1} \supset \cdots \supset M_1 \supset M_0 = (0)$$

of  $KG$ -submodules. By the argument used to obtain the formula (10.3), we see that, by choosing a basis for  $M$  so that the first block of basis vectors form a basis for  $M_1$ , the second a basis for  $M_2$  modulo  $M_1$ , etc.,  $M$  affords a matrix representation  $\mathbf{T}$  of  $G$  such that

$$(13.11) \quad \mathbf{T}(g) = \begin{pmatrix} \mathbf{T}_1(g) & & * \\ & \mathbf{T}_2(g) & . \\ 0 & & \ddots & \mathbf{T}_k(g) \end{pmatrix}$$

where each  $\mathbf{T}_i$  is an irreducible matrix representation of  $G$  afforded by the composition factor  $M_i/M_{i-1}$ . The matrices  $\mathbf{T}(g)$  have zeros below the blocks on the main diagonal but may have non-zero entries above the diagonal blocks. Finally, we can assert that if  $\mathbf{U}(g)$  is any matrix representation afforded by  $M$ , there exists a fixed  $S \in GL(d, K)$ ,  $d = (M : K)$ , such that

$$SU(g)S^{-1} = \mathbf{T}(g), \quad g \in G.$$

where  $\mathbf{T}(g)$  is given by (13.11). The point of the Jordan-Hölder theorem is that the irreducible matrix representations of  $G$  associated with some other composition series of  $M$  are equivalent to the  $\{\mathbf{T}_i\}$  taken in some order.

### Exercises

1. Give an example of a reducible module which contains no minimal submodules.
2. If  $M$  is an irreducible  $R$ -module, then for each non-zero  $m \in M$  we have  $M = Rm$ .
3. If  $M$  is an  $R$ -module which may be reducible, and if  $m$  is a non-zero element of  $M$ , is the submodule  $Rm$  necessarily irreducible?
4. If  $M$  is a finite-dimensional vector space over the field  $K$ , find a composition series for the  $K$ -module  $M$ . What are the composition factors?
5. Let  $N$  be a submodule of the  $R$ -module  $M$ . Show how to obtain a composition series for  $M$  from composition series for  $N$  and  $M/N$ .
6. If the  $R$ -module has a composition series, so does each submodule of  $M$ . The composition series of any proper submodule of  $M$  is shorter than that of  $M$ .
7. Let  $M$  be an irreducible  $R$ -module. Prove that  $\text{Hom}_R(M, M)$  is a skewfield. (This result will be referred to as *Schur's lemma*.)
8. Every irreducible left  $R$ -module  $M$  is isomorphic to a factor module  $R/I$ , where  $I$  is a maximal left ideal of  $R$ . [Hint: By Exercise 13.2,  $M = Rm$

for some  $m \neq 0$  in  $M$ . Then  $r \rightarrow rm$  is an  $R$ -homomorphism of the left regular module  ${}_R R$  onto  $M$  whose kernel is a left ideal in  $R$ .]

9. Let  $M, N$  be non-zero left  $R$ -modules, both of which have composition series. Let  $f: M \rightarrow N$  be a non-zero  $R$ -homomorphism of  $M$  into  $N$ . Prove that  $M, N$  have at least one composition factor in common.

### § 14. Indecomposable Modules

(14.1) **DEFINITION.** An  $R$ -module  $M$  is said to be *indecomposable* if  $M \neq (0)$  and if it is impossible to express  $M$  as a direct sum of two non-trivial submodules.

The importance of indecomposable modules lies in the fact that any module satisfying both chain conditions is a direct sum of indecomposable modules, and these modules are uniquely determined up to isomorphism. The purpose of this section is to prove these results.

(14.2) **THEOREM.** *If the submodules of  $M$  satisfy the D.C.C., then  $M$  can be expressed as a direct sum of a finite number of indecomposable modules.*

**PROOF.** Let  $S$  be the set of non-zero submodules of  $M$  which cannot be expressed as direct sums of finite sets of indecomposable submodules of  $M$ . Suppose that  $S$  is non-empty. Then by Theorem 11.15,  $S$  contains a minimal element  $M'$ . Clearly  $M' \neq 0$ , and  $M'$  cannot be indecomposable. Therefore  $M' = M_1 \oplus M_2$ , where  $M_1$  and  $M_2$  are proper submodules of  $M'$ . Neither  $M_1$  nor  $M_2$  can lie in  $S$ , and so each is a direct sum of indecomposable submodules of  $M$ . Therefore  $M'$  is also such a sum, and we have reached a contradiction. Therefore  $S$  is empty, and all submodules of  $M$ , including  $M$  itself, can be expressed as finite direct sums of indecomposable modules.

Before proceeding, it is necessary to recall from § 11B that the existence of a direct sum decomposition

$$M = M_1 \oplus \cdots \oplus M_k$$

is equivalent to the existence of a set of projections  $\pi_1, \dots, \pi_k$  in  $\text{Hom}_R(M, M)$  such that

$$1 = \pi_1 + \cdots + \pi_k,$$

$$\pi_i^2 = \pi_i, \quad 1 \leq i \leq k, \quad \pi_i \pi_j = \pi_j \pi_i = 0, \quad i \neq j,$$

and

$$\pi_i(M) = M_i,$$

$$1 \leq i \leq k.$$

Now we shall establish some lemmas preliminary to the proof of the uniqueness theorem for direct decompositions into indecomposable modules.

(14.3) LEMMA. *Let  $M$  be an indecomposable  $R$ -module, and let  $N$  be a non-zero  $R$ -module. Suppose there exist maps  $\theta \in \text{Hom}_R(N, M)$  and  $\pi \in \text{Hom}_R(M, N)$  such that  $\theta$  is an isomorphism,  $\pi$  maps  $M$  onto  $N$ , and  $\pi\theta$  is an  $R$ -automorphism of  $N$ . Then  $\theta$  is an isomorphism of  $N$  onto  $M$ , and  $\pi$  is an isomorphism of  $M$  onto  $N$ .*

PROOF. Let  $M_1$  be the kernel of  $\pi$ ; then  $M_1$  is a submodule of  $M$ . We now prove that  $M = \theta N \oplus M_1$ . If  $m \in M$ , then  $\pi m \in N$ , and so there exists an element  $n \in N$  such that  $\pi m = (\pi\theta)n$ . Therefore  $m - \theta n \in M_1$ , and so  $m = \theta n + \text{element of } M_1$ . Furthermore, let  $m \in \theta N \cap M_1$ ; then on the one hand  $\pi m = 0$ , and on the other  $m = \theta n$  for some  $n \in N$ . Thus  $0 = \pi m = \pi\theta n$ , and so  $n = 0$ . This shows that  $M = \theta N \oplus M_1$ .

However, the indecomposability of  $M$  implies that either  $\theta N = 0$  or  $M_1 = 0$ . Now  $N = \pi\theta N \neq 0$ , so  $\theta N \neq 0$ . Thus  $M_1 = 0$  and  $M = \theta N$ , which proves the lemma.

(14.4) LEMMA. *Let  $M$  be a non-zero indecomposable  $R$ -module whose submodules satisfy both chain conditions. Let  $\tau_1, \dots, \tau_r \in \text{Hom}_R(M, M)$  be such that  $\tau_1 + \dots + \tau_r$  is an automorphism\* of  $M$ . Then at least one  $\tau_i$  is an automorphism of  $M$ .*

PROOF. It suffices to prove the lemma when  $r = 2$ , since if the result is established for that case, then from

$$\tau_1 + (\tau_2 + \dots + \tau_r) = \text{automorphism of } M$$

we could deduce that either  $\tau_1$  is an automorphism of  $M$  (in which case we are through) or  $(\tau_2 + \dots + \tau_r)$  is an automorphism of  $M$  (in which case we repeat the argument).

Now let  $\tau_1 + \tau_2 = \phi$  be an automorphism of  $M$ ; letting  $\varphi_i = \tau_i \phi^{-1}$ , we have

$$\varphi_1 + \varphi_2 = 1, \quad \varphi_i \in \text{Hom}_R(M, M),$$

and it suffices to show that either  $\varphi_1$  or  $\varphi_2$  is an automorphism of  $M$ . Since  $\varphi_2 = 1 - \varphi_1$ , we see that  $\varphi_1$  and  $\varphi_2$  commute, and so for each positive integer  $k$  we have

$$1 = (\varphi_1 + \varphi_2)^k = \sum_{n=0}^k \binom{k}{n} \varphi_1^n \varphi_2^{k-n}.$$

---

\* "Automorphism" of course means " $R$ -automorphism."

If both  $\varphi_1$  and  $\varphi_2$  were nilpotent (that is, if there existed positive integers  $n_1, n_2$  such that  $\varphi_1^{n_1} = 0, \varphi_2^{n_2} = 0$ ), then choosing  $k = n_1 + n_2$  we would have  $1 = (\varphi_1 + \varphi_2)^k = 0$ , which is impossible. Therefore not both  $\varphi_1$  and  $\varphi_2$  are nilpotent. Suppose  $\varphi_1$  is not nilpotent; we shall prove that  $\varphi_1$  is an automorphism of  $M$ .

Set

$$N_j = \{m \in M : \varphi_1^j m = 0\}$$

Then  $N_j$  is a submodule of  $M$ , and we have two chains of submodules

$$N_1 \subset N_2 \subset \cdots, \quad M \supset \varphi_1 M \supset \varphi_1^2 M \supset \cdots.$$

Since the submodules of  $M$  are assumed to satisfy both chain conditions, both chains terminate, and so there exists a positive integer  $t$  such that

$$N_t = N_{t+1} = \cdots, \quad \varphi_1^t M = \varphi_1^{t+1} M = \cdots.$$

Set  $\mu = \varphi_1^t \in \text{Hom}_R(M, M)$ ; then  $\mu \neq 0$  since  $\varphi_1$  is not nilpotent.

We shall now apply Lemma 14.3 with  $N = \mu M$ , where  $\theta: N \rightarrow M$  is the injection map and where  $\pi = \mu$ . In order for the lemma to be applicable, we must verify that  $\pi\theta$  is an automorphism of  $N$ , that is, that  $\mu$  is an automorphism of  $\mu M$ . We have

$$\mu(\mu M) = \varphi_1^{2t} M = \varphi_1^t M = \mu M,$$

so  $\mu$  maps  $\mu M$  onto itself. Further, if  $m \in M$  is such that  $\mu(\mu m) = 0$ , then  $m \in N_t$ ; but  $N_{2t} = N_t$ , so  $\mu m = 0$ . Therefore,  $\mu$  is an automorphism of  $\mu M$ . We may therefore use Lemma 14.3 to deduce that  $M$  coincides with  $\mu M$  and that  $\mu$  is an automorphism of  $M$ . Since  $\varphi_1^t$  is an automorphism of  $M$ , obviously so is  $\varphi_1$ .

We may now prove the following basic result:

(14.5) THEOREM (Krull-Schmidt). *Let  $M$  be an  $R$ -module whose submodules satisfy both chain conditions, and let*

$$M = M_1 \oplus \cdots \oplus M_h = N_1 \oplus \cdots \oplus N_k$$

*be two decompositions of  $M$  into direct sums of non-zero indecomposable submodules. Then  $h = k$ , and there exists a permutation  $\{j_1, \dots, j_h\}$  of  $\{1, \dots, h\}$  such that*

$$M_1 \cong N_{j_1}, \dots, M_h \cong N_{j_h}.$$

PROOF. We use induction on  $h$ ; the result is trivial for  $h = 1$ . Suppose it proved for modules possessing a direct sum decomposition into fewer than  $h$  indecomposable submodules. We proceed to prove

the result for the module  $M$  given above.

Let  $\mu_i: M \rightarrow M_i$ ,  $\nu_j: M \rightarrow N_j$  be the projections associated with the above decompositions. Then we have

$$1 = \mu_1 + \cdots + \mu_k = \nu_1 + \cdots + \nu_k ,$$

$$\mu_i \mu_j = \nu_i \nu_j = 0 \quad (i \neq j) .$$

Therefore

$$\mu_1 = \mu_1 \nu_1 + \mu_1 \nu_2 + \cdots + \mu_1 \nu_k .$$

If we restrict the operators  $\mu_1 \nu_j$  to  $M_1$ , the above equation becomes

$$1 = \mu_1 \nu_1 + \cdots + \mu_1 \nu_k \text{ on } M_1 ,$$

and here each  $\mu_1 \nu_j \in \text{Hom}_R(M_1, M_1)$ . Since  $M_1$  is indecomposable, we deduce from Lemma 14.4 that some  $\mu_1 \nu_j$  is an automorphism of  $M_1$ . Suppose  $\mu_1 \nu_1$  is an automorphism of  $M_1$ ; then we have

$$M_1 \xrightarrow{\nu_1} N_1 \xrightarrow{\mu_1} M_1$$

so that  $\nu_1$  is an isomorphism and  $\mu_1$  is “onto.” We may therefore use Lemma 14.3 to deduce that both  $\nu_1$  and  $\mu_1$  are isomorphisms “onto.”

We now show that the sum  $N_1 + M_2 + \cdots + M_k$  is direct; for let  $n_1 + m_2 + \cdots + m_k = 0$ , and apply  $\mu_1$  to both sides. This gives  $\mu_1 n_1 = 0$ , whence (since  $\mu_1$  is an isomorphism) also  $n_1 = 0$ . Therefore  $m_2 + \cdots + m_k = 0$ , and so  $m_2 = \cdots = m_k = 0$ . Set

$$M' = N_1 \oplus M_2 \oplus \cdots \oplus M_k \subset M ,$$

and define  $\rho \in \text{Hom}_R(M, M)$  by

$$\rho = \nu_1 \mu_1 + \nu_2 \mu_2 + \cdots + \nu_k \mu_k .$$

It is then easy to see that  $\rho$  is an isomorphism of  $M$  onto  $M'$  which maps  $M_1$  onto  $N_1$ . We claim that in fact  $M' = M$ ; for the chain

$$M \supset \rho M \supset \rho^2 M \supset \cdots$$

terminates, so

$$\rho^a M = \rho^{a+1} M = \cdots$$

for some positive integer  $a$ . Therefore to each  $m \in M$  corresponds an element  $m^* \in M$  such that  $\rho^a m = \rho^{a+1} m^*$ . In that case,  $\rho^a(m - \rho m^*) = 0$ , so  $m = \rho m^*$ . This shows that  $M = \rho M = M'$ .

We have therefore obtained an automorphism  $\rho$  of  $M$  which maps  $M_1$  isomorphically onto  $N_1$ . Consequently

$$M/M_1 \cong \rho M/\rho M_1 = M/N_1 ;$$

that is,

$$M_1 \oplus \cdots \oplus M_k \cong N_1 \oplus \cdots \oplus N_k.$$

Let  $M_i \rightarrow M'_i$  in the above isomorphism. Then  $M_i \cong M'_i$ , and

$$M'_1 \oplus \cdots \oplus M'_k = N_1 \oplus \cdots \oplus N_k.$$

By the induction hypothesis, the  $\{M'_i\}$  are isomorphic to the  $\{N_j : j = 2, \dots, k\}$  in some order. This proves the theorem.

(14.6) COROLLARY. *Let  $M$  be an  $R$ -module whose submodules satisfy both chain conditions, and let  $M = M_1 \oplus \cdots \oplus M_k$  be a decomposition of  $M$  into a direct sum of non-zero indecomposable submodules. Then any submodule  $N$  of  $M$  which is a direct summand of  $M$  is isomorphic to a direct sum of a subset of the modules  $M_1, \dots, M_k$ .*

PROOF. Since  $N$  is a direct summand of  $M$ , there exists a submodule  $N'$  such that

$$M = N \oplus N'.$$

By Theorem 14.2, both  $N$  and  $N'$  can be expressed as direct sums of non-zero indecomposable submodules of  $M$ , say

$$N = N_1 \oplus \cdots \oplus N_t, \quad N' = N_{t+1} \oplus \cdots \oplus N_u.$$

Then  $M = N_1 \oplus \cdots \oplus N_u$  gives a direct sum decomposition of  $M$  into non-zero indecomposable submodules. By the Krull-Schmidt theorem, the  $\{N_i\}$  are the same as the  $\{M_j\}$  up to isomorphism and order of occurrence.

We may ask whether in a direct sum decomposition of  $M$  into non-zero indecomposable submodules, the individual summands are in fact unique. The Krull-Schmidt theorem asserts that the summands are unique up to operator isomorphism and order of occurrence, provided that the submodules of  $M$  satisfy both chain conditions. We may see from an example that the summands need not be unique; for let  $R$  be a field and  $M$  a finite-dimensional vector space over  $R$ . Then if  $\{m_1, \dots, m_k\}$  is any  $R$ -basis of  $M$ , we have  $M = Rm_1 \oplus \cdots \oplus Rm_k$ . Other choices of bases give decompositions with other summands.

### Exercises

1. Is the converse of Theorem 14.2 true?
2. Verify the statement which precedes Lemma 14.3.

3. Let  $M$  be an  $R$ -module, and let  $\varphi \in \text{Hom}_R(M, M)$ . Suppose there exists a positive integer  $k$  such that  $\varphi^k$  is an automorphism of  $M$ . Prove that  $\varphi$  is also an automorphism of  $M$ .

4. Let  $R$  be the group ring  $KG$  where  $[G : 1] > 1$  and  $K$  is the rational field. Set

$$e_1 = [G : 1]^{-1} \sum_{x \in G} x,$$

and  $e_2 = 1 - e_1$ , where  $1$  is the identity element of  $G$ . Prove that  $e_1^2 = e_1$ ,  $e_2^2 = e_2$ ,  $e_1 e_2 = e_2 e_1 = 0$  and that

$$R = Re_1 \oplus Re_2$$

gives a decomposition of  $R$  as a sum of two-sided ideals.

5. Let  $R$  be a ring with unity element  $1$ , and let  $e_1, \dots, e_n$  be elements of the center of  $R$  such that

$$1 = e_1 + \cdots + e_n, \quad e_i^2 = e_i, \quad e_i e_j = 0 \quad (i \neq j).$$

Show that

$$R = Re_1 \oplus \cdots \oplus Re_n$$

and that each  $Re_i$  is a two-sided ideal in  $R$ .

## § 15. Completely Reducible Modules

Powerful as the results of the last section may seem, they are difficult to apply in particular cases. The simplest situation, and the prototype of good behavior in a module, occurs when a module is a direct sum of irreducible modules, and it is to this phenomenon that this section is devoted. The fact that this theory is of limited applicability is shown by the example of the  $Z$ -module  $Z/(p^2)$ , where  $p$  is a prime, which is an indecomposable module satisfying both chain conditions but is neither irreducible nor a sum of irreducible submodules.

(15.1) **DEFINITION.** A left  $R$ -module  $M$  is said to be *completely reducible* if every submodule is a direct summand; in other words, for every submodule  $N$  there exists a submodule  $N'$  such that  $M = N \oplus N'$ . [The reader should compare this definition with Definition 10.2.]

Exactly as in the proof of Lemma 10.6, we have

(15.2) *A submodule of a completely reducible module is completely reducible.*

The connection between irreducible modules and completely reducible modules is brought out by the following theorem:

(15.3) THEOREM. *The following three statements about an  $R$ -module  $M$  are equivalent:*

- (i)  $M$  is completely reducible.
- (ii)  $M$  is a direct sum of irreducible submodules.
- (iii)  $M$  is a sum (not necessarily direct) of irreducible submodules.

PROOF. We may assume  $M \neq (0)$ , the result being trivial otherwise. We make the following preliminary remarks: Let  $S$  be any subset of  $M$ , and let  $\mathcal{N}$  be the set of all submodules  $N$  of  $M$  such that  $N \cap S = \phi$ . Clearly the union of any ascending sequence of modules in the collection  $\mathcal{N}$  is again in  $\mathcal{N}$ ; thus, if  $\mathcal{N}$  is non-empty, it follows from the maximum principle (see § 15A) that  $\mathcal{N}$  contains a maximal element. The same type of argument shows that, if  $T$  is a subset of  $M$  containing 0 and if there exist submodules  $N$  of  $M$  such that  $N \cap T = (0)$ , there is a maximal such submodule.

We are now ready to prove that (i) implies (ii); we begin by showing that each non-zero submodule  $N$  of  $M$  contains an irreducible submodule. Let  $n \in N$ ,  $n \neq 0$ , and consider the collection of all submodules  $N'$  of  $N$  such that  $n \notin N'$ . The collection contains the zero submodule and hence is non-empty, and so, by the above remarks, there is a maximal member  $N_0$  of this collection. Since  $N$  is a submodule of  $M$ , we know that  $N$  is completely reducible by (15.2), and so we may write  $N = N_0 \oplus N_1$  for some submodule  $N_1$  of  $N$ . We may show at once that  $N_1$  is irreducible. For otherwise  $N_1$  would contain a proper non-zero submodule  $N_2$ , and then  $N_1 = N_2 \oplus N_3$  for some non-zero submodule  $N_3$  in  $N_1$ . But this gives

$$N = N_0 \oplus N_2 \oplus N_3,$$

and surely either

$$(15.4) \quad n \notin N_0 + N_2 \quad \text{or} \quad n \notin N_0 + N_3$$

since

$$(N_0 + N_2) \cap (N_0 + N_3) = N_0.$$

However (15.4) contradicts the maximality of  $N_0$ , and this shows that  $N_1$  is irreducible.

We have now shown that  $M$  contains irreducible submodules. Let  $\{M_\alpha : \alpha \in A\}$  be the collection of all irreducible submodules of  $M$ , and let  $\mathcal{T}$  be the collection of all those subsets  $T$  of  $A$  for which the sum

$$\sum_{\alpha \in T} M_\alpha$$

is a direct sum of the  $\{M_\alpha\}$  involved. The union of an ascending chain of elements of  $\mathcal{T}$  is again in  $\mathcal{T}$ , and so, by the maximum principle,  $\mathcal{T}$  contains a maximal element  $T_0$ . We shall prove that

$$M = \sum_{\alpha \in T_0} \bigoplus M_\alpha.$$

Suppose  $M' = \sum_{\alpha \in T_0} M_\alpha$  is properly contained in  $M$ . By complete reducibility, we may write  $M = M' \oplus M''$  for some module  $M'' \neq (0)$ . Then  $M''$  contains an irreducible submodule  $M_\beta$  for some  $\beta$ , and then

$$\sum_{\alpha \in T_0} M_\alpha + M_\beta$$

is a direct sum, contradicting the maximality of  $T_0$ . Hence  $M' = M$ , and the first implication is proved.

The fact that (ii) implies (iii) is immediate, and it remains to prove that (iii) implies (i). Let  $N$  be a submodule of  $M$ , and let  $N'$  be a submodule maximal with respect to the property that  $N' \cap N = (0)$ . [At this point we cannot be sure whether  $N' \neq (0)$ .] We wish to prove that  $N \oplus N' = M$ , for by construction the sum  $N + N'$  is direct. Suppose the result is false. Then there exists  $m$  in  $M$  such that  $m \notin N + N'$ . By (iii),  $m = m_1 + \cdots + m_s$ , where the  $\{m_i\}$  belong to irreducible submodules  $\{M_i\}$ . Since  $m \notin N + N'$ , some  $m_i \notin N + N'$ , and there exists an irreducible submodule  $M_i$  such that  $M_i \subset N + N'$ . Because  $M_i$  is irreducible, we have  $M_i \cap (N + N') = (0)$ , and hence  $N' + M_i$  is a submodule properly containing  $N'$  whose intersection with  $N$  is zero. This contradicts the maximality of  $N'$ , and we must have  $N + N' = M$ . This completes the proof of the theorem.

An immediate consequence of Definition 15.1 is the fact that a completely reducible  $R$ -module satisfies the A.C.C. if and only if it satisfies the D.C.C. Hence we have

(15.5) COROLLARY. *Let the  $R$ -module  $M$  satisfy either chain condition. Then  $M$  is completely reducible if and only if  $M$  is a direct sum of a finite set of irreducible submodules.*

Because of its great importance for us, we state again, in the language of modules, the fundamental result of Maschke proved in § 10.

(15.6) THEOREM. *Let  $G$  be a finite group and  $K$  a field whose characteristic does not divide  $[G : 1]$ . Then every left  $KG$ -module is completely reducible.*

### § 15A. The Maximum Principle

A *partially ordered* set  $P$  is a set  $P$  together with a relation  $\geq$  which is *transitive* ( $a \geq b, b \geq c$  imply  $a \geq c$ ), *reflexive* ( $a \geq a$ ), and such that  $a \geq b, b \geq a$  together imply  $a = b$ . A subset  $S$  of a partially ordered set is said to be *totally ordered* if any two elements of  $S$  are comparable (that is,  $a, b \in S$  implies either  $a \geq b$  or  $b \geq a$ ). An element  $b \in P$  is called an *upper bound* of a subset  $S$  if  $b \geq s$  for all  $s \in S$ . An element  $t$  in a subset  $S$  is called a *maximal element* of  $S$  if  $t' \geq t, t' \in S$ , implies  $t' = t$ . The most familiar example of a partially ordered set in algebra is, of course, a family of subsets of some set, partially ordered by the relation of inclusion. We shall state as an axiom the following result, which is a form of Zorn's lemma, and is equivalent to the Axiom of Choice:

(15.7) MAXIMUM PRINCIPLE. *Let  $P$  be a partially ordered set, every totally ordered subset of which has an upper bound (in  $P$ ). Then  $P$  contains a maximal element.*

### Exercises

1. Let  $M = M_1 \oplus M_2 = N_1 \oplus M_2$  where  $M_i, N_i$  are submodules of the  $R$ -module  $M$ . Then does  $M_1 = N_1$ ?
2. Submodules and factor modules of completely reducible modules are completely reducible.
3. Let  $K$  have characteristic  $p \neq 0$ , and let  $p \mid [G : 1]$  where  $G$  is an arbitrary finite group. Let  $n = \sum_{x \in G} x \in KG$ . Then  $(KG)n$  is a submodule of the left regular  $KG$ -module  $KG$  but is not a direct summand of  $KG$ .
4. Let  $R$  be a ring and  $V$  a left  $R$ -module which is a direct sum

$$V = \sum_{j=1}^t \sum_{i=1}^{n_j} M_{ij},$$

where the  $\{M_{ij}\}$  are irreducible  $R$ -modules such that  $M_{ij} \cong M_{rs}$  if and only if  $j = s$ . Let

$$N_j = \sum_{i=1}^{n_j} M_{ij},$$

and prove that

$$\text{Hom}_R(V, V) \cong \sum_{j=1}^t \text{Hom}_R(N_j, N_j) \quad (\text{external direct sum of rings}).$$

[Hint: Let  $f \in \text{Hom}_R(V, V)$ . Then for  $x \in M_{rs}$ , write

$$f(x) = \sum_{i,j} x_{ij}, \quad x_{ij} \in M_{ij}.$$

The map  $x \rightarrow x_{tj}$  is an  $R$ -homomorphism of  $M_{rs}$  into  $M_{tj}$  and hence is the zero map for  $j \neq s$ . This implies that  $f(N_j) \subset N_j$ . If we extend  $f|N_j$  to a map  $f_j$  defined on  $V$  by letting  $f_j$  vanish outside  $N_j$ , we have

$$f = \sum_{j=1}^t f_j .]$$

## CHAPTER III

# Algebraic Number Theory

### Introduction

The purpose of this chapter is to furnish a self-contained introduction to those topics in algebraic number theory which are needed in this book. In Chapter V, familiarity with §17 is essential, and some results from §§18 and 19 are needed in one or two places. This entire chapter is needed for Chapter XI, and all but §22 for Chapter XII.

It goes without saying that, because of our limited objectives, no attempt has been made to treat the ideas of this chapter in their utmost generality. More detailed accounts of the subject may be found in the following books: Artin [4], Hasse [1], Hecke [1], Landau [1], Mann [2], Pollard [1], van der Waerden [2], Weyl [3], and Zariski and Samuel [1]. The material in §22 is taken largely from papers of Kaplansky [1] and Chevalley [1].

### §16. Modules over Principal Ideal Domains

Throughout this section  $R$  denotes an *integral domain*, that is, a commutative ring without zero divisors, containing 1. We assume further that  $R$  is a *principal ideal domain*; that is,  $R$  is an integral domain in which every ideal is a principal ideal. Then of course every ideal of  $R$  is finitely generated, so that the ideals of  $R$  satisfy the A.C.C. [by Theorem 11.14]. It is well known that a principal ideal domain is also a *unique factorization domain*, that is, an integral domain in which each non-unit  $\alpha \neq 0$  can be factored as a product of primes, and that these primes are uniquely determined up to unit factors.

The purpose of this section is to classify all finitely generated  $R$ -modules. Because  $R$  is commutative, the notions of left and right  $R$ -modules are the same. Most of the results we obtain are special cases of theorems, to be proved in §22, which will concern modules over Dedekind rings. The proofs are so much simpler in this special

case, however, that it seems worthwhile to include them.

We begin with a free left  $R$ -module  $M$  with a finite basis  $\{m_1, \dots, m_k\}$ . Then every element of  $M$  can be expressed uniquely in the form  $\sum \alpha_i m_i$ ,  $\alpha_i \in R$ . This is equivalent to the two statements: (i)  $M = \sum \oplus Rm_i$ , and (ii)  $\sum \alpha_i m_i = 0$ ,  $\alpha_i \in R$ , implies each  $\alpha_i = 0$ . These statements are, in turn, equivalent to the assertion that  $M \cong R + \cdots + R$  (external direct sum of  $k$  summands) where each summand is viewed as a left  $R$ -module. The module  $M$  is  $R$ -torsion-free; that is,  $\alpha m = 0$ ,  $\alpha \in R$ ,  $m \in M$ , implies that either  $\alpha = 0$  or  $m = 0$ .

Our first result is the following important theorem:

(16.1) THEOREM. *Let  $M$  be a free left  $R$ -module with a finite basis  $\{m_1, \dots, m_s\}$ , and let  $N$  be a submodule  $\neq 0$ . Then  $N$  is free and has a finite basis of  $r$  elements for some  $r \leq s$ .*

PROOF. We prove the theorem by induction on  $s$ , it being vacuously true if  $s = 0$ . Assume the theorem holds for modules with bases of  $s - 1$  or fewer elements, and consider  $M = \sum_1^s Rm_i$ ,  $s \geq 1$ . Let  $N \neq 0$  be a submodule; every  $n \in N$  can be expressed uniquely in the form

$$n = \alpha_1 m_1 + \cdots + \alpha_s m_s, \quad \alpha_i \in R.$$

The set of all coefficients  $\alpha_1$  which occur as  $n$  ranges over all elements of  $N$  is an ideal  $I$  in  $R$ . Because  $R$  is a principal ideal domain, there exists an element  $\sigma \in I$  such that  $I = R\sigma$ . Then  $\sigma$  occurs as the coefficient of  $m_1$  in some element

$$n_1 = \sigma m_1 + \alpha_2 m_2 + \cdots + \alpha_s m_s \in N.$$

If we set  $M' = Rm_2 \oplus \cdots \oplus Rm_s$ , then  $M' \cap N$  is a submodule of  $M'$  and has a basis of  $s - 1$  or fewer elements  $\{n_2, \dots, n_t\}$ ,  $t \leq s$ , by the induction hypothesis. From what we have proved, it is clear that  $N = Rn_1 + M' \cap N$  and that  $\{n_1, n_2, \dots, n_t\}$  is a basis of  $N$  (unless  $\sigma = 0$ , in which case  $n_1$  should be omitted). This completes the proof of the theorem.

(16.2) THEOREM. *Any two bases for a free  $R$ -module with a finite basis contain the same number of elements.*

PROOF. Let  $M = R + \cdots + R$  ( $n$  summands), and let  $P$  be any maximal ideal in  $R$ . Set  $\bar{R} = R/P$ ,  $\bar{M} = M/PM$ . Then  $\bar{R}$  is a field, and  $\bar{M} \cong \bar{R} + \cdots + \bar{R}$  ( $n$  summands). Therefore the dimension

$(\bar{M}: \bar{R}) = n$ , and, since the dimension of a vector space over a field is uniquely determined, the theorem is proved.

The reader will notice some similarity between the proof of Theorem 16.1, and the theorem in § 11 which asserts that a finitely generated module over a noetherian ring is noetherian.

(16.3) DEFINITION. The number of elements in a basis of a free  $R$ -module  $M$  with a finite basis is called the *rank* of  $M$  and is denoted by  $(M: R)$ .

A closer analysis of submodules of a free module, and the subsequent determination of finitely generated  $R$ -modules which are not necessarily free, depends on the theory of invariant factors of rectangular matrices with coefficients in  $R$ . Matrix theory comes into the picture in the following manner.

Let  $\{m_1, \dots, m_s\}$  be a basis of  $M$ . For  $X = (\xi_{ij}) \in R_s$  (ring of  $s \times s$  matrices with entries in  $R$ ), define the elements  $\{m'_1, \dots, m'_s\}$  by

$$\{m'_1, \dots, m'_s\} = \{m_1, \dots, m_s\}X,$$

which means simply that

$$m'_i = \sum_{j=1}^s \xi_{ji} m_j.$$

It is then immediate that  $\{m'_1, \dots, m'_s\}$  forms a basis of  $M$  if and only if  $X$  is an *unimodular matrix* over  $R$ , in the sense that there exists a matrix  $Y \in R_s$  such that  $XY = YX = I^{(s)}$  ( $s$ -rowed identity matrix). From the theory of determinants, we know that  $X$  is unimodular if and only if  $|X|$  is a unit in  $R$ .

Now let  $N$  be a submodule of  $M$ , and let  $\{n_1, \dots, n_t\}$ ,  $t \leq s$ , be a basis of  $N$ . Then we have

$$(16.4) \quad \{n_1, \dots, n_t\} = \{m_1, \dots, m_s\}A,$$

where  $A$  is an  $s \times t$  matrix  $(\alpha_{ij})$  whose entries are determined from

$$n_i = \sum_{j=1}^s \alpha_{ji} m_j, \quad i = 1, 2, \dots, t.$$

Suppose we change bases in  $M$  and  $N$ , obtaining

$$\{n'_1, \dots, n'_t\} = \{n_1, \dots, n_t\}X$$

and

$$\{m'_1, \dots, m'_s\} = \{m_1, \dots, m_s\}Y$$

where  $X$  and  $Y$  are unimodular matrices in  $R_t$  and  $R_s$ , respectively. We then obtain

$$\{n'_1, \dots, n'_t\} = \{m'_1, \dots, m'_s\} A'$$

where

$$A' = Y^{-1}AX.$$

Our objective is to show that  $X$  and  $Y$  can be chosen so that  $A' = \text{diag}\{\alpha'_1, \alpha'_2, \dots, \alpha'_r, 0, 0, \dots, 0\}$ , where  $\text{diag}\{x_1, x_2, \dots\}$  denotes a rectangular matrix of appropriate size whose diagonal elements are  $x_1, x_2, \dots$  and which has zeros in all positions off the main diagonal.

(16.5) DEFINITION. Two rectangular  $s \times t$  matrices  $A$  and  $B$  with coefficients in  $R$  are called *equivalent* (notation:  $A \sim B$ ) if there exist unimodular matrices  $X_1$  and  $X_2$  in  $R_s$  and  $R_t$ , respectively, such that  $B = X_1AX_2$ .

(16.6) THEOREM (*Invariant Factor Theorem for Matrices*). Let  $A$  be a rectangular matrix with coefficients in  $R$ . Then

$$A \sim \text{diag}\{\delta_1, \delta_2, \dots, \delta_r, 0, \dots, 0\}, \quad \delta_i \in R, \delta_i \neq 0,$$

where  $\delta_i | \delta_{i+1}$ ,  $1 \leq i \leq r - 1$ . The elements  $\{\delta_i\}$  are called the invariant factors of  $A$  and are determined up to unit factors.

PROOF. We give the familiar proof of this theorem, which consists of applying elementary row and column operations to the matrix  $A$ . Although long, this proof does provide an effective scheme for carrying out the reduction in special cases. We begin by constructing some particular unimodular matrices which effect the row and column operations that we wish to perform.

Let  $X_{ij}$  be the matrix obtained from the identity matrix  $I$  by interchanging the  $i$ th and  $j$ th rows. Then  $X_{ij}$  is unimodular, and, for a rectangular matrix  $B$ ,  $X_{ij}B$  is obtained from  $B$  by interchanging the  $i$ th and  $j$ th rows, whereas  $BX_{kl}$  is obtained from  $B$  by interchanging the  $k$ th and  $l$ th columns. (Of course  $X_{ij}$  and  $X_{kl}$  must be of the correct sizes for the products to make sense.)

Next let  $Y_{ij}(\alpha) = I + \alpha E_{ij}$ ,  $\alpha \in R$ , where  $i \neq j$  and  $E_{ij}$  is the matrix with a 1 in the  $(i, j)$  position and zeros elsewhere. Then  $Y_{ij}(\alpha)$  is unimodular, and  $Y_{ij}(\alpha)B$  is obtained from  $B$  by adding  $\alpha$  times the  $j$ th row of  $B$  to the  $i$ -th row. Similarly,  $BY_{kl}(\alpha)$  is obtained from  $B$  by adding  $\alpha$  times the  $k$ th column of  $B$  to the  $l$ th column.

We are now ready to prove the theorem. Let  $A$  denote an  $s \times t$  matrix,  $s \geq 1, t \geq 1$ , and we shall assume the theorem proved

for all  $(s - 1) \times (t - 1)$  matrices and also that  $A \neq 0$ . In the proof we distinguish two cases.

CASE (1). For some  $i$  and  $j$ ,  $\alpha_{ij} | \alpha_{kl}$  for all  $k, l$ . Then, by multiplying  $A$  on the right and left by matrices of the form  $X_{rs}$ , we obtain a matrix  $B = (\beta_{ij})$  equivalent to  $A$  such that  $\beta_{11} | \beta_{ij}$  for all  $i, j$ . Let  $\beta_{ij} = \beta_{11}\gamma_{ij}$ . Then, by successively multiplying  $B$  on the left by  $Y_{11}(-\gamma_{11})$ ,  $i = 2, \dots, s$ , and multiplying on the right by  $Y_{1j}(-\gamma_{1j})$ ,  $j = 2, \dots, t$ , we obtain a new matrix  $C \sim A$  of the form

$$C = \begin{bmatrix} \beta_{11} & 0 \\ 0 & C_1 \end{bmatrix}$$

where  $C_1$  is an  $(s - 1) \times (t - 1)$  matrix with the property that  $\beta_{11}$  divides all the coefficients of  $C_1$ . By the induction hypothesis there exist unimodular matrices  $X_1$ ,  $Y_1$  of appropriate size such that  $Y_1 C_1 X_1$  has the required form. Let  $X$  and  $Y$  be  $s \times s$  and  $t \times t$  matrices defined by

$$X = \begin{bmatrix} 1 & 0 \\ 0 & X_1 \end{bmatrix}, \quad Y = \begin{bmatrix} 1 & 0 \\ 0 & Y_1 \end{bmatrix}.$$

Then  $X$  and  $Y$  are unimodular, and

$$C \sim Y C X = \begin{bmatrix} \beta_{11} & 0 \\ 0 & Y_1 C_1 X_1 \end{bmatrix}.$$

Moreover,  $\beta_{11}$  divides the first diagonal entry of  $Y_1 C_1 X_1$  since  $\beta_{11}$  divides all the coefficients of  $C_1$ . Then  $Y C X$  has the required form, and the existence part of the theorem is proved in this case.

CASE (2). No  $\alpha_{ij}$  divides all the other coefficients of  $A$ . Let  $\alpha$  be a coefficient of  $A$  with the least number  $d$  of prime factors among all the coefficients of  $A$ . Since  $\alpha$  cannot be a unit, we have  $d > 0$ , and we shall prove that  $A \sim B$  where  $B$  has a coefficient with fewer prime factors than  $\alpha$ . We may arrange matters so that  $\alpha = \alpha_{11}$  appears in the (1,1) position. If  $\alpha \nmid \alpha_{1j}$  for some  $j$ , by rearranging rows we may assume that  $\alpha \nmid \alpha_{21}$ . Similarly, if  $\alpha \nmid \alpha_{ij}$  for some  $j$ , we may assume that  $\alpha \nmid \alpha_{12}$ . If  $\alpha = \alpha_{11}$  divides all the entries in the first row and column, then by the argument in Case (1), we obtain  $A \sim B$  where

$$B = \begin{bmatrix} \alpha_{11} & 0 \\ 0 & B_1 \end{bmatrix}$$

and where  $\alpha_{11} \nmid \beta^*$  for some coefficient  $\beta^*$  of  $B_1$ . Then, by adding

the column of  $B_1$  in which  $\beta^*$  appears to the first column and by interchanging rows, we obtain a matrix equivalent to  $A$  in which  $\alpha_{11}$  appears in the (1,1) position and does not divide the entry in the (2,1) position. Thus we may assume from the beginning in Case (2) that either  $\alpha_{11} \nmid \alpha_{21}$  or  $\alpha_{11} \nmid \alpha_{12}$ , and suppose the former holds. Then  $R\alpha_{11} + R\alpha_{21} = R\beta$  where  $\beta$  is the G.C.D. of  $\alpha_{11}$  and  $\alpha_{21}$ , and  $\beta$  has fewer prime factors than  $\alpha_{11}$ . We may thus write  $\beta = r_1\alpha_{11} + r_2\alpha_{21}$ , and  $Rr_1 + Rr_2 = R$  since  $\beta \mid \alpha_{11}$  and  $\beta \mid \alpha_{21}$ . Consequently, there exist  $\epsilon_1$  and  $\epsilon_2$  in  $R$  such that  $r_1\epsilon_1 - r_2\epsilon_2 = 1$ . But then the matrix

$$X = \begin{bmatrix} r_1 & r_2 & 0 \\ \epsilon_2 & \epsilon_1 & 0 \\ 0 & 0 & I \end{bmatrix}$$

is unimodular. Moreover,  $XA \sim A$ , and  $XA$  has  $\beta$  in the (1,1) position. (A similar calculation can be made when  $\alpha_{11} \nmid \alpha_{12}$ .)

To complete the reduction, we see that, after applying the argument of Case (2) a sufficient number of times, we obtain a matrix  $B \sim A$  such that the hypotheses of Case (1) hold for  $B$ . Then  $B$ , and hence also  $A$ , is equivalent to a diagonal matrix of the required form.

In order to give the uniqueness proof, let  $d_i(A)$  denote the G.C.D. of all  $i$ -rowed minors of the matrix  $A$ , where an  $i$ -rowed minor is the determinant of an  $i \times i$  submatrix obtained by striking out rows and columns of  $A$ . We shall call  $d_i(A)$  the  $i$ th *determinantal divisor* of the matrix  $A$ . From the theory of determinants, it follows that  $A \sim B$  implies  $d_i(A) = \eta_i d_i(B)$ ,  $\eta_i$  a unit in  $R$ , because the  $i$ -rowed minors of  $A$  are  $R$ -linear combinations of the  $i$ -rowed minors of  $B$ , and conversely. For a diagonal matrix

$$D = \text{diag} \{ \delta_1, \delta_2, \dots, \delta_r, 0, \dots, 0 \}, \quad \delta_i \mid \delta_{i+1}, 1 \leq i \leq r-1,$$

we have, for  $1 \leq i \leq r$ ,

$$\delta_1 = \epsilon_1 d_1(D), \quad \delta_2 = \epsilon_2 d_2(D)d_1(D)^{-1}, \dots, \delta_i = \epsilon_i d_i(D)d_{i-1}(D)^{-1}$$

where the  $\{\epsilon_i\}$  are units in  $R$ . The uniqueness of the invariant factors is an immediate consequence of these remarks.

In Theorem 16.8, we shall give a second proof, which is independent of the theory of determinants, for the uniqueness of the invariant factors.

First we require some preliminary remarks concerning modules with torsion. Let  $m$  be an element of an  $R$ -module  $M$ , and define

$$\text{order ideal of } m = \{\alpha \in R: \alpha m = 0\}.$$

The order ideal of  $m$ , also called the *annihilator* of  $m$ , is a principal ideal  $R\alpha$  in  $R$ , and the generator  $\alpha$  of this ideal is called the *order* of  $m$ . The order of  $m$  is determined up to a unit factor. If  $\alpha \neq 0$ , we shall call  $m$  a *torsion element* of  $M$ , whereas, if  $\alpha = 0$ , we shall call  $m$  *torsion-free*. A module  $M$  is a *torsion module* if all its elements are torsion elements, whereas  $M$  is called *torsion-free* if all its non-zero elements are torsion-free. Finally, we recall that an  $R$ -module with one generator is called a *cyclic*  $R$ -module.

In the proof of the next theorem, it will be useful to have the following result, the proof of which will be left to the reader.

(16.7) *Let  $M$  be an arbitrary  $R$ -module. The set  $T$  of all torsion elements of  $M$  forms a torsion submodule of  $M$  such that  $M/T$  is torsion-free.*

Now we can state a much sharper result than Theorem 16.1 concerning submodules of free  $R$ -modules.

(16.8) **THEOREM (Invariant Factor Theorem for Modules).** *Let  $M$  be a free left  $R$ -module with a finite basis, and let  $N$  be a non-zero submodule of  $M$ . Then there exists a basis  $\{m_1, \dots, m_s\}$  for  $M$ , and non-zero elements  $\delta_1, \dots, \delta_r, r \leq t$ , in  $R$  such that  $\delta_i | \delta_{i+1}$ ,  $1 \leq i \leq r - 1$ , and such that  $\{\delta_1 m_1, \dots, \delta_r m_r\}$  forms a basis for  $N$ . The elements  $\{\delta_i : 1 \leq i \leq r\}$  are called the invariant factors of the pair  $(M, N)$  and are determined by  $M$  and  $N$  up to unit factors.*

**PROOF.** The existence of the basis  $\{m_1, \dots, m_s\}$  and the elements  $\delta_1, \dots, \delta_r$  follows from Theorem 16.6 and the remarks preceding it. We shall give, however, a new proof of the uniqueness of the invariant factors which will turn out to be useful in our discussion of modules over Dedekind domains in §22. Let  $\{m_i\}$  and  $\{m'_i\}$ ,  $1 \leq i \leq s$ , be bases of  $M$ , and  $\{\delta_i\}$  and  $\{\delta'_i\}$ ,  $1 \leq i \leq r$ , elements of  $R$  such that  $\delta_i | \delta_{i+1}$ ,  $\delta'_i | \delta'_{i+1}$ ,  $1 \leq i \leq r - 1$ , and for which  $\{\delta_i m_i\}$  and  $\{\delta'_i m'_i\}$ ,  $1 \leq i \leq r$ , both form bases for  $N$ . (The number of elements in a basis for  $M$  or  $N$  is uniquely determined.)

The key to the proof of the uniqueness theorem is the study of the torsion submodule [see (16.7)] of  $M/N$ . This module is isomorphic to

$$R/R\delta_1 + \cdots + R/R\delta_r$$

and also to

$$R/R\delta'_1 + \cdots + R/R\delta'_r.$$

The modules  $R/R\delta_i$  and  $R/R\delta'_i$  are cyclic modules whose generators have orders  $\delta_i$  and  $\delta'_i$ , respectively. Changing notation slightly, we must prove that if

$$L = Ru_1 \oplus \cdots \oplus Ru_r \cong Ru'_1 \oplus \cdots \oplus Ru'_r = L'$$

where the  $Ru_i$  and  $Ru'_i$  are cyclic modules whose generators have non-zero orders  $\delta_i$  and  $\delta'_i$ , respectively, such that  $\delta_i \mid \delta_{i+1}$ ,  $\delta'_i \mid \delta'_{i+1}$ ,  $1 \leq i \leq r-1$ , then each  $\delta'_i$  is a unit times  $\delta_i$ . We require first the following lemma, which is similar to Lemma 4.4:

(16.9) **LEMMA.** *Let  $Ru$  be a cyclic  $R$ -module whose generator has the non-zero order  $\delta$ . Let  $\delta = \pi_1 \cdots \pi_q$  where the  $\{\pi_i\}$  are the distinct prime power factors of  $\delta$ . Then  $Ru = Ru_1 \oplus \cdots \oplus Ru_q$ , where, for  $1 \leq i \leq q$ , each  $Ru_i$  is an indecomposable cyclic submodule of  $Ru$  of order  $\pi_i$ .*

**PROOF.** Define  $\zeta_i = \delta \pi_i^{-1}$ ,  $1 \leq i \leq q$ ; then the elements  $\{\zeta_i\}$  have no common factor, and there exist elements  $\{\xi_i\} \in R$ ,  $1 \leq i \leq q$ , such that  $\sum \xi_i \zeta_i = 1$ . Let  $u_i = \zeta_i u$ ; then  $u_i$  has order  $\pi_i$ . Furthermore,  $Ru = \sum Ru_i$ , since for  $x \in Ru$  we have  $x = \sum \xi_i \zeta_i x$  with  $\xi_i \zeta_i x \in Ru_i$ . To show that the sum is direct, let  $\xi_i u_1 = \sum_{i>1} \xi_i u_i$ , for example, where the  $\{\xi_i\} \in R$ . There exist elements  $\varepsilon_1, \varepsilon_2$  in  $R$  such that

$$\pi_1 \varepsilon_1 + \pi_2 \varepsilon_2 + \cdots + \pi_q \varepsilon_q = 1,$$

and, applying this to the equation for  $\xi_1 u_1$ , we obtain

$$\xi_1 u_1 = (1 - \pi_1 \varepsilon_1) \xi_1 u_1 = \pi_2 \varepsilon_2 + \cdots + \pi_q \varepsilon_q \left( \sum_{i>1} \xi_i u_i \right) = 0.$$

Finally, we show that each  $Ru_i$  is indecomposable. We have  $Ru_i \cong R/R\pi_i$ , and it is easily seen that, because  $\pi_i$  is a power of a prime,  $Ru_i$  has a unique minimal submodule and hence is indecomposable. This completes the proof of (16.9).

Now we return to the proof of Theorem 16.8. By (16.9) we can express  $L$  and  $L'$  as direct sums of indecomposable cyclic modules whose annihilator ideals are generated by the different prime power factors of the  $\{\delta_i\}$  and  $\{\delta'_i\}$ , respectively, all counted according to their multiplicities. It is also clear that both  $L$  and  $L'$  possess composition series as  $R$ -modules. By the Krull-Schmidt theorem, the indecomposable direct summands of  $L$  and  $L'$  are the same, and consequently the set of prime power factors of the  $\{\delta_i\}$  coincides with the set of prime power factors of the  $\{\delta'_i\}$ . However, if

$\{\pi_1, \pi_2, \dots, \pi_k\}$  are all the prime power factors of the  $\{\delta_i\}$  then  $\delta_r$  is the L.C.M. of the  $\{\pi_i\}$ ,  $\delta_{r-1}$  is the L.C.M. of those which remain when the factors of  $\delta_r$  are deleted, etc. Thus the  $\{\delta_i\}$  are also uniquely determined, and the uniqueness part of Theorem 16.8 is proved.

Now we apply Theorem 16.8 to obtain the following structure theorem for finitely generated  $R$ -modules:

(16.10) THEOREM. *Any finitely generated  $R$ -module  $M$  can be expressed as a direct sum of cyclic modules*

$$M = Rm_1 \oplus \cdots \oplus Rm_r \oplus Rm_{r+1} \oplus \cdots \oplus Rm_s,$$

in which

$$Rm_{r+1} \oplus \cdots \oplus Rm_s$$

is a free  $R$ -module with basis  $\{m_{r+1}, \dots, m_s\}$ , while if  $\alpha_i \neq 0$  is the order of  $m_i$  ( $1 \leq i \leq r$ ), then  $\alpha_i | \alpha_{i+1}$ ,  $1 \leq i \leq r-1$ .

PROOF. Let  $M = \sum_i^s Rx_i$ , and construct a free  $R$ -module  $F$  with basis  $\{f_1, \dots, f_s\}$ . The map

$$\theta: \sum \alpha_i f_i \rightarrow \sum \alpha_i x_i$$

is an  $R$ -homomorphism of  $F$  onto  $M$ . Letting  $F_0 = \text{kernel of } \theta$ , we have  $F/F_0 \cong M$ .

Now apply Theorem 16.8 to the pair  $(F, F_0)$  to get

$$F = Ru_1 \oplus \cdots \oplus Ru_s,$$

$$F_0 = R\alpha_1 u_1 \oplus \cdots \oplus R\alpha_r u_r,$$

where  $1 \leq r \leq s$  and where  $\alpha_i | \alpha_{i+1}$ ,  $1 \leq i \leq r$ , with  $\alpha_r \neq 0$ . Then

$$M \cong F/F_0 \cong \frac{Ru_1}{R\alpha_1 u_1} \dot{+} \cdots \dot{+} \frac{Ru_r}{R\alpha_r u_r} \dot{+} Ru_{r+1} \dot{+} \cdots \dot{+} Ru_s.$$

The sum  $Ru_{r+1} \dot{+} \cdots \dot{+} Ru_s$  is a free  $R$ -module, and each  $Ru_i/R\alpha_i u_i$  is a cyclic module whose generator is the coset containing  $u_i$  and whose order is  $\alpha_i$ . This completes the proof.

We remark that Theorems 16.8 and 16.10 include as a special case the Invariant Factor Theorem 4.5 for finite abelian groups.

(16.11) COROLLARY. *Any finitely generated torsion-free  $R$ -module is a free  $R$ -module with a finite basis.*

We conclude this section with two appendices, §§ 16A and 16B, in which we collect some facts concerning pure submodules of a module and elementary divisors of a matrix, which are needed in Chapters XI and XII, respectively.

### § 16A. Pure submodules

For the moment let  $R$  be an arbitrary commutative ring.

(16.12) **DEFINITION.** A submodule  $N$  of an  $R$ -module  $M$  is called a *pure submodule* if, for every  $\alpha \in R$ ,

$$\alpha N = N \cap \alpha M.$$

Since the inclusion  $\alpha N \subset N \cap \alpha M$  always holds, we see that  $N$  is pure if and only if for all  $m \in M$  and  $\alpha \in R$ ,  $\alpha m \in N$  implies that  $\alpha m = \alpha n$  for some  $n \in N$ .

We state some immediate consequences of the definition.

(16.13) *Any direct summand of a module is a pure submodule.*

(16.14) *A submodule  $N$  of a torsion-free module  $M$  is pure if and only if for all  $m \in M$  and for all non-zero  $\alpha \in R$ ,  $\alpha m \in N$  implies  $m \in N$ .*

(16.15) *If  $M/N$  is torsion-free, then  $N$  is pure. If  $M$  is torsion-free and  $N$  is a pure submodule of  $M$ , then  $M/N$  is torsion-free.*

(16.16) **THEOREM.** *Let  $M$  be a free module with a finite basis over a principal ideal domain  $R$ . A submodule  $N$  of  $M$  is pure if and only if  $N$  is a direct summand of  $M$ .*

**PROOF.** If  $N$  is a direct summand of  $M$ , obviously  $N$  is pure. On the other hand, if  $N$  is pure, by (16.15)  $M/N$  is torsion-free. Using the notation of Theorem 16.10, we see that  $M/N$  is torsion-free if and only if each  $\alpha_i$ ,  $1 \leq i \leq r$ , is a unit in  $R$ . But this latter condition implies that  $N$  is a direct summand of  $M$ , and so the proof is complete.

(16.17) **COROLLARY.** *Let  $R$  be a principal ideal domain and  $M$  a free  $R$ -module with a finite basis. A submodule  $N$  of  $M$  is pure if and only if every basis of  $N$  can be extended to a basis of  $M$ .*

Finally, we give some applications to modules embedded in vector spaces over fields. Let  $R$  be a principal ideal domain with quotient field  $K$ , and let  $V_0$  be a finite-dimensional vector space over  $K$ , say,  $V_0 = Kv_1 \oplus \cdots \oplus Kv_m$ . If we set

$$V = Rv_1 \oplus \cdots \oplus Rv_m,$$

then  $V$  is a free  $R$ -module. We can now state (proofs left to the reader)

(16.18) *If  $W_0$  is a  $K$ -subspace of  $V_0$  and if  $W = W_0 \cap V$ , then  $W$  is*

a pure submodule of  $V$ .

(16.19) Let  $S$  be an arbitrary subset of  $V$  and  $KS$  the  $K$ -subspace of  $V_0$  generated by the elements of  $S$ . Then  $KS \cap V$  is the unique minimal pure submodule of  $V$  containing  $S$ .

### § 16B. Elementary divisors of a matrix

We shall restrict ourselves to rectangular matrices with coefficients in the ring of rational integers  $\mathbb{Z}$ .

(16.20) **DEFINITION.** Let  $A$  be a rectangular matrix with coefficients in  $\mathbb{Z}$ , and let  $\delta_1, \dots, \delta_r$  be the invariant factors of  $A$ . The prime power factors of the  $\{\delta_i\}$ , counted according to their multiplicities, are called the *elementary divisors* of  $A$ .

We emphasize that the proof of Theorem 16.6 gives an effective method for calculating the invariant factors and hence also the elementary divisors of a rectangular matrix.

For example, let

$$A = \text{diag} \{12, 36, 72, 0, 0\}.$$

Then the elementary divisors of  $A$  are

$$\{2^2, 3, 2^2, 3^2, 2^3, 3^2\}.$$

As we observed in Theorem 16.8, the invariant factors can be recovered in an unambiguous way from a knowledge of the elementary divisors. For example, the greatest invariant factor is the L.C.M. of all the elementary divisors, the next one is the L.C.M. of those that remain when the factors of the greatest invariant factor have been deleted, etc. For two rectangular matrices  $A$  and  $B$  of the same size, we may conclude from Theorem 16.6 that

(16.21) The elementary divisors of  $A$  and  $B$  are the same if and only if  $A \sim B$ .

The next result is often useful.

(16.22) Let  $A = \text{diag} \{\alpha_1, \dots, \alpha_r, 0, \dots, 0\}$ , where each  $\alpha_i \in \mathbb{Z}$ ,  $\alpha_i \neq 0$ . Then the prime power factors of the  $\{\alpha_i\}$  are the elementary divisors of  $A$ .

**PROOF.** Let  $\beta_1, \beta_2$  be non-zero integers such that  $\{\beta_1, \beta_2\}$  and  $\{\alpha_1, \alpha_2\}$  have the same set of prime power factors. Then  $\text{diag} \{\alpha_1, \alpha_2\} \sim \text{diag} \{\beta_1, \beta_2\}$ , since the two matrices have the same determinantal divisors. Using this fact repeatedly, we obtain

$$A \sim \text{diag} \{ \delta_1, \dots, \delta_r, 0, \dots, 0 \}$$

where  $\delta_1, \dots, \delta_r$  are non-zero integers such that the  $\{\alpha_i\}$  and  $\{\delta_i\}$  have the same set of prime power factors, and such that  $\delta_i \mid \delta_{i+1}$ ,  $1 \leq i \leq r-1$ . By Theorem 16.6, the  $\{\delta_i\}$  are the invariant factors of  $A$ . Consequently, the prime power factors of the  $\{\delta_i\}$  are the elementary divisors of  $A$ , and the result is proved.

### Exercises

$R$  always denotes a principal ideal domain.

- Let  $a, b \in R$  be such that  $Ra + Rb = R$ . Prove that

$$R/Rab \cong R/Ra \times R/Rb.$$

Is the result still true if we drop the hypothesis that  $Ra + Rb = R$ ?

- Prove (16.13) through (16.19).
- Let  $L \supset M \supset N$  be  $R$ -modules such that  $N$  is a pure submodule of  $M$  and  $M$  a pure submodule of  $L$ . Show that  $N$  is a pure submodule of  $L$ .
- Prove that the intersection of pure submodules of a torsion-free  $R$ -module is a pure submodule. Show, however, that the sum of pure submodules need not be pure.
- Let  $p$  be prime. For  $\alpha \in Z$ ,  $\alpha \neq 0$ , define  $v(\alpha)$  to be the integer such that  $p^{v(\alpha)} \mid \alpha$ . Let

$$\begin{pmatrix} u_1 \\ \vdots \\ u_n \end{pmatrix} = C \begin{pmatrix} f_1 \\ \vdots \\ f_n \end{pmatrix}$$

where the  $u$ 's,  $f$ 's, and entries of  $C$  are in  $Z$ , and set

$$a = v(G.C.D.(u_1, \dots, u_n)), b = v(G.C.D.(f_1, \dots, f_n)),$$

$p^a =$  highest power of  $p$  which is an elementary divisor of  $C$ . If  $a \geq b$ , prove that  $c \geq a - b$ .

## § 17. Algebraic Integers

We assume that the reader is familiar with the rudiments of Galois theory, as well as with the material in the preceding section of this chapter and in the early sections of Chapter II. Let  $Q$  denote the rational field throughout this chapter, and let  $Z$  be the ring of rational integers. Let  $x$  be an indeterminate over  $Q$ . A polynomial in  $R[x]$  is *monic* if its leading coefficient is 1. For an element  $\alpha$  of a finite extension of  $Q$ , let  $\text{Irr}(\alpha, Q)$  denote the unique monic irreducible polynomial in  $Q[x]$  of which  $\alpha$  is a zero.

(17.1) **DEFINITION.** An *algebraic integer* is an element  $\alpha$  of some finite extension of  $Q$  for which  $\text{Irr}(\alpha, Q) \in Z[x]$ . Obviously, all elements of  $Z$  are algebraic integers.

(17.2) **THEOREM.** Any zero of a monic polynomial in  $Z[x]$  is an algebraic integer.

**PROOF.** Let  $\alpha$  be a zero of the monic polynomial  $h(x) \in Z[x]$ , where  $h(x)$  may be reducible. If  $f(x) = \text{Irr}(\alpha, Q)$ , we have

$$(17.3) \quad h(x) = f(x)g(x), \quad g(x) \in Q[x].$$

The polynomial  $f(x)$  has rational coefficients; let us write  $f(x) = cF(x)/a$ , where  $a$  and  $c$  are positive integers, and where  $F(x) \in Z[x]$  is a primitive polynomial (that is, the G.C.D. of the coefficients of  $F(x)$  is 1). Similarly, write  $g(x) = dG(x)/b$ , where  $G(x) \in Z[x]$  is primitive and  $b$  and  $d$  are positive integers. From (17.3) we obtain

$$(17.4) \quad cdF(x)G(x) = abh(x).$$

If we can show that the product  $F(x)G(x)$  of the two primitive polynomials  $F(x), G(x)$  is again primitive, then (17.4) will imply that  $ab = cd$ , whence  $F(x)G(x) = h(x)$ . Therefore  $F(x)$  must be monic, so  $c = a$ , and  $f(x) \in Z[x]$ . This implies the desired conclusion.

Suppose  $F(x)G(x)$  were not primitive; there would then exist a rational prime  $p$  such that

$$(17.5) \quad F(x)G(x) \equiv 0 \pmod{p}$$

coefficientwise. Let  $\bar{Z}$  be the finite field  $Z/pZ$ , and let  $\bar{F}(x) \in \bar{Z}[x]$  be gotten from  $F(x)$  by replacing each coefficient of  $F(x)$  by its residue class mod  $p$ . Since  $F(x)$  and  $G(x)$  are both primitive, we have  $\bar{F}(x) \neq 0, \bar{G}(x) \neq 0$ . However,  $\bar{F}\bar{G} = \bar{F}\bar{G}$ , so (17.5) implies  $\bar{F}(x)\bar{G}(x) = 0$ . This is a contradiction: we have two non-zero polynomials in  $\bar{Z}[x]$  whose product is zero.

We now obtain a second characterization of algebraic integers, which is more useful for our purposes.

(17.6) **THEOREM.** An element  $\alpha$  of an extension field of  $Q$  is an algebraic integer if and only if  $Z[\alpha]$  is a finitely generated  $Z$ -module.

**PROOF.** If  $\alpha$  is an algebraic integer, then clearly

$$Z[\alpha] = Z \oplus Z\alpha \oplus Z\alpha^2 \oplus \cdots \oplus Z\alpha^{m-1},$$

where  $m$  is the degree of  $\text{Irr}(\alpha, Q)$ .

Suppose, conversely, that  $Z[\alpha]$  is a finitely generated  $Z$ -module, say

$$Z[\alpha] = Zf_1(\alpha) + \cdots + Zf_n(\alpha),$$

with each  $f_i(x) \in Z[x]$ . Choose  $N$  greater than the degrees of all the  $\{f_i(x)\}$ . Since  $\alpha^N \in Z[\alpha]$ , we may write

$$\alpha^N = a_1 f_1(\alpha) + \cdots + a_n f_n(\alpha), \quad a_i \in Z.$$

But this shows that  $\alpha$  is a zero of a monic polynomial in  $Z[x]$ , and so  $\alpha$  is an algebraic integer. This completes the proof.

(17.7) COROLLARY. *Let  $\alpha, \beta$  be elements of a finite extension of  $Q$ . If  $\alpha$  and  $\beta$  are algebraic integers, so are  $\alpha \pm \beta$  and  $\alpha\beta$ .*

PROOF. From the hypothesis we see that  $Z[\alpha]$  and  $Z[\beta]$  are finitely generated  $Z$ -modules, say  $Z[\alpha] = \sum_i Z\alpha_i$ ,  $Z[\beta] = \sum_j Z\beta_j$ . Then  $Z[\alpha, \beta] = Z[\alpha][\beta] = \sum_i Z[\beta]\alpha_i = \sum_{i,j} Z\beta_j\alpha_i$ , so  $Z[\alpha, \beta]$  is finitely generated. Then every  $Z$ -submodule of  $Z[\alpha, \beta]$  is also finitely generated. Since  $Z[\alpha + \beta]$ ,  $Z[\alpha - \beta]$ , and  $Z[\alpha\beta]$  are all submodules of  $Z[\alpha, \beta]$ , the result now follows from Theorem 17.6.

(17.8) DEFINITION. An *algebraic number field* is a finite extension field of  $Q$ .

Let  $R = \text{alg. int. } \{K\}$  denote the set of all algebraic integers contained in an algebraic number field  $K$ . By (17.7),  $R$  is a subring of  $K$ , and so  $R$  is obviously an integral domain. We claim that  $K$  is the quotient field of  $R$ . For let  $\gamma \in K$  be a zero of the primitive irreducible polynomial  $g(x) \in Z[x]$ , and let

$$g(x) = a_0x^n + a_1x^{n-1} + \cdots + a_n, \quad a_i \in Z, a_0 \neq 0.$$

Then  $a_0\gamma$  is a zero of

$$y^n + a_1 y^{n-1} + a_0 a_2 y^{n-2} + \cdots + a_0^{n-1} a_n,$$

a monic polynomial in  $Z[y]$ . Hence  $a_0\gamma \in R$ , and, since  $a_0 \in Z \subset R$ , this shows that  $\gamma$  is a quotient of elements of  $R$ . (In fact, it establishes the stronger result that every element of  $K$  is the quotient of an algebraic integer and a rational integer.)

(17.9) THEOREM. *Let  $R = \text{alg. int. } \{K\}$ , where  $K$  is an algebraic number field. Then  $R$  is a finitely generated  $Z$ -module, and  $(R:Z) = (K:Q)$ .*

PROOF. Since  $K$  is a finite separable extension of  $Q$ , there exists an element  $\gamma \in K$  such that  $K = Q(\gamma)$ . By the above discussion, we

may then choose  $\alpha \in Z, \alpha \neq 0$  such that  $a\gamma \in R$ . Set  $\alpha = a\gamma$ ; we then have  $K = Q(\alpha)$  and  $Z[\alpha] \subset R$ .

Now let  $\beta \in R$ ; we may write

$$\beta = \sum_{i=0}^{n-1} b_i \alpha^i, \quad b_i \in Q,$$

where  $n = (K:Q)$ . Let  $\alpha = \alpha_1, \alpha_2, \dots, \alpha_n$  be the distinct conjugates of  $\alpha$  in some normal extension  $L$  of  $Q$  which contains  $K$ . Then the conjugates of  $\beta$  in  $L$  are  $\beta = \beta_1, \beta_2, \dots, \beta_n$  (not necessarily distinct) where

$$(17.10) \quad \beta_j = \sum_{i=0}^{n-1} b_i \alpha_j^i, \quad 1 \leq j \leq n.$$

Let  $A$  denote the  $n \times n$  matrix whose  $(i, j)$  entry is  $\alpha_j^{i-1}$ ; since  $\{\alpha_1, \dots, \alpha_n\}$  are distinct, the van der Monde determinant  $|A|$  is not 0. Further,  $|A|^2$  is unchanged by all automorphisms in the Galois group of  $L$  over  $Q$  and so must lie in  $Q$ . On the other hand,  $|A|^2$  is a polynomial with rational integral coefficients in the algebraic integers  $\{\alpha_j^i\}$ . Therefore,  $|A|^2$  is also an algebraic integer. However, the only rational numbers which are algebraic integers are the rational integers, and therefore  $|A|^2 \in Z$ . Thus, setting  $c = |A|^2$ , we see that  $c$  is a non-zero element of  $Z$ .

We now use Cramer's rule to solve equations (17.10) for the coefficients  $\{b_i\}$ , obtaining

$$b_i = |A|^{-1} \sum_{j=1}^n r_{ij} \beta_j, \quad 0 \leq i \leq n-1,$$

where the  $\{r_{ij}\}$  are polynomials with rational integral coefficients in the  $\{\alpha_j^i\}$ . Therefore each  $r_{ij}$  is an algebraic integer (lying in  $L$ , but not necessarily in  $K$ ); since each  $\beta_j$  is an algebraic integer, we deduce that, for each  $i$ ,  $cb_i$  is an algebraic integer. However,  $cb_i \in Q$ , and consequently  $cb_i \in Z$  (see Exercise 1). Thus, every  $\beta \in R$  is expressible in the form

$$\beta = c^{-1} \sum_{i=0}^{n-1} a_i \alpha^i, \quad a_i \in Z,$$

which shows that  $R \subset c^{-1}Z[\alpha]$ . Since  $c^{-1}Z[\alpha]$  is a finitely generated  $Z$ -module, each of its submodules is also finitely generated. Therefore  $R$  is a finitely generated torsion-free  $Z$ -module and so must have a  $Z$ -basis. Finally, it is easily seen that any  $Z$ -basis of  $R$  is also a  $Q$ -basis for  $K$ .

The preceding proof also establishes

- (17.11) Let  $R = \text{alg. int. } \{K\}$ , where  $(K: Q) = n$ , and let  $\alpha \in R$  be such that  $K = Q(\alpha)$ . Let  $\alpha_1, \dots, \alpha_n$  be the conjugates of  $\alpha$  over  $Q$ , and set

$$c = \prod_{1 \leq i < j \leq n} (\alpha_i - \alpha_j)^2.$$

Then

$$c \cdot R \subset Z[\alpha].$$

We now make the following definition:

- (17.12) **DEFINITION.** A ring is *noetherian* if its left ideals satisfy the A.C.C.

We have shown in §11C that if a ring  $R$  is noetherian, the submodules of an  $R$ -module  $M$  satisfy the A.C.C. if and only if  $M$  is finitely generated, and that any submodule of a finitely generated  $R$ -module is also finitely generated.

Now let  $R$  be the ring of all algebraic integers in the algebraic number field  $K$ . We shall show that  $R$  is a noetherian ring. Let  $L$  be an ideal in  $R$ . Since  $Z \subset R$ , clearly  $L$  is a  $Z$ -submodule of  $R$ , and so  $L$  is finitely generated as  $Z$ -module. Therefore  $L$  is also finitely generated as  $R$ -module. We have thus established that any submodule of  $_R R$  is finitely generated, which implies by (11.14) that the submodules of  $_R R$  satisfy the A.C.C. Hence  $R$  is noetherian.

- (17.13) **DEFINITION.** Let  $R$  be an integral domain with quotient field  $K$ . We say that  $R$  is *integrally closed in  $K$*  if, whenever  $r \in K$  is such that the ring  $R[r]$  is a finitely generated  $R$ -module, then  $r \in R$ .

We show that if  $R = \text{alg. int. } \{K\}$ , where  $K$  is a finite extension field of  $Q$ , then indeed  $R$  is integrally closed in  $K$ . Let  $r \in K$  be such that  $R[r]$  is finitely generated as  $R$ -module. Since  $R$  is a finitely generated  $Z$ -module, it follows that  $R[r]$  is also a finitely generated  $Z$ -module. But then any  $Z$ -submodule of  $R[r]$  is finitely generated, so in particular  $Z[r]$  is a finitely generated  $Z$ -module. By Theorem 17.6 it follows that  $r \in R$ .

### Exercises

1. Prove that a rational number is an algebraic integer if and only if it is a rational integer.
2. The *content* of a polynomial  $f(x) \in Z[x]$  is defined to be the G.C.D. of

its coefficients. Prove that for  $f(x), g(x) \in Z[x]$ ,  $\{\text{content of } f(x)\} \cdot \{\text{content of } g(x)\} = \text{content of } f(x)g(x)$ .

3. Let  $\alpha$  be an algebraic integer,  $\alpha \neq 0$ , and let  $f(x) = \text{Irr}(\alpha, Q) \in Z[x]$ . Show that  $1/\alpha$  is an algebraic integer if and only if  $f(0) = \pm 1$ .

4. Let  $\alpha_1, \dots, \alpha_m$  be algebraic integers, and let  $\theta$  be a zero of the polynomial  $x^m + a_1x^{m-1} + \dots + a_m$ . Prove that  $\theta$  is also an algebraic integer. (Show successively that  $Z[\alpha_1, \dots, \alpha_m]$ ,  $Z[\alpha_1, \dots, \alpha_m, \theta]$ ,  $Z[\theta]$  are all finitely generated  $Z$ -modules.)

5. Let  $f(x) \in Z[x]$  be monic, and let  $\alpha$  be an element algebraic over  $Q$  such that  $f(\alpha)$  is an algebraic integer. Prove that  $\alpha$  is also an algebraic integer.

6. Is a subring of a noetherian ring necessarily noetherian?

7. Let  $K_1 \subset K_2$  be algebraic number fields, and set  $R_i = \text{alg. int. } \{K_i\}$ ,  $i = 1, 2$ . Considering  $R_1$  and  $R_2$  as  $Z$ -modules, show that  $R_1$  is a pure submodule of  $R_2$  and hence that any  $Z$ -basis of  $R_1$  can be completed to a  $Z$ -basis of  $R_2$ .

## § 18. Ideals

To begin with we fix an algebraic number field  $K$ , and let  $R$  be the ring of all algebraic integers in  $K$ .

(18.1) **DEFINITION.** An *ideal in  $K$*  (or *fractional ideal*) is a non-zero finitely generated  $R$ -submodule of  $K$ . An *integral ideal* is an ideal which is contained in  $R$ .

(18.2) **DEFINITION.** A *prime ideal  $P$*  is a (non-zero) integral ideal properly contained in  $R$  such that

$$\alpha, \beta \in R, \alpha, \beta \notin P \quad \text{imply} \quad \alpha\beta \notin P.$$

A *maximal ideal* in  $R$  is a proper ideal in  $R$  not properly contained in any proper ideal in  $R$ . It is immediate that every maximal ideal is prime. We show that, because of the special properties of  $R$ , the converse is also true.

(18.3) **THEOREM.** *Every prime ideal in  $R$  is maximal.*

**PROOF.** Let  $P$  be a prime ideal in  $R$ , and consider  $P \cap Z$ . Since  $P \neq (0)$ , there exists an element  $\alpha \in P, \alpha \neq 0$ . Let

$$\text{Irr}(\alpha, Q) = x^m + a_1x^{m-1} + \dots + a_m, \quad a_i \in Z.$$

Then  $a_m \neq 0$ , and

$$a_m = -(\alpha^m + a_1\alpha^{m-1} + \dots + a_{m-1}\alpha) \in P \cap Z.$$

Hence  $P \cap Z \neq (0)$ . Clearly,  $P \cap Z$  is a prime ideal of  $Z$ , for  $P \cap Z \neq Z$  because  $1 \notin P$ . Therefore  $P \cap Z = pZ$  for some rational prime  $p$ . We may remark that  $P$  cannot contain two distinct rational primes  $p, q$ , for, if so, we could choose  $a, b \in Z$  such that  $1 = ap + bq \in P$ , which is impossible.

Now let  $A$  be an integral ideal such that

$$P \subset A \subset R$$

where each inclusion is proper. Then  $A \cap Z$  is an ideal in  $Z$  which contains  $P \cap Z$ ; furthermore,  $1 \notin A$  implies  $1 \notin A \cap Z$ . Therefore we have (since  $pZ$  is a maximal ideal in  $Z$ )  $A \cap Z = pZ$ . Choose  $\beta \in A, \beta \notin P$ , and let

$$\text{Irr}(\beta, Q) = x^n + b_1x^{n-1} + \cdots + b_n, \quad b_i \in Z.$$

As above,  $b_n \in A \cap Z = P \cap Z$ , so

$$\beta(\beta^{n-1} + b_1\beta^{n-2} + \cdots + b_{n-1}) \in P.$$

Since  $\beta \notin P$  and  $P$  is prime, this implies

$$\beta^{n-1} + b_1\beta^{n-2} + \cdots + b_{n-1} \in P.$$

As above, we then have  $b_{n-1} \in A \cap Z = P \cap Z$ , and so on, until we find that  $\beta \in P$ . This yields a contradiction, and so no such  $A$  can exist. This completes the proof.

Combining this theorem with the results of the preceding section, we have now shown:

- (i)  $R$  is a noetherian ring; that is, the ideals of  $R$  satisfy the A.C.C.
- (ii) Every prime ideal in  $R$  is maximal.<sup>t</sup>
- (iii)  $R$  is integrally closed in its quotient field  $K$ ; that is, if  $r \in K$  is such that  $R[r]$  is a finitely generated  $R$ -module, then  $r \in R$ .

(18.4) DEFINITION. A *Dedekind domain* is an integral domain  $R$  satisfying conditions (i) through (iii).

For the remainder of this section, let  $R$  denote a Dedekind domain with quotient field  $K$ . Since  $R$  is noetherian, the ideals in  $R$  satisfy the A.C.C. and are finitely generated  $R$ -modules, a fact which we shall use repeatedly. By a *proper* ideal we shall mean here a (non-zero) ideal properly contained in  $R$ . In this section we shall show that “classical ideal theory” is valid for  $R$ ; that is, every proper

---

<sup>t</sup> In accordance with Definition 18.2, the term “prime ideal” will always mean “non-zero prime ideal” throughout this chapter.

ideal is uniquely expressible as a product of prime ideals.

(18.5) DEFINITION. The *sum*  $A + B$  of two fractional ideals  $A, B$  is given by

$$A + B = \{\alpha + \beta : \alpha \in A, \beta \in B\}.$$

The *product*  $AB$  is given by

$$AB = \{\sum \alpha_i \beta_i : \alpha_i \in A, \beta_i \in B\}$$

and consists of all finite sums of products of elements of  $A$  by those in  $B$ . The sum and product of fractional ideals are again fractional ideals. Addition (and multiplication) of ideals is commutative and associative.

(18.6) LEMMA. *Every integral ideal contains a product of prime ideals.*

PROOF. Consider the set  $S$  of integral ideals for which this statement is false. If  $S$  were non-empty, then, since  $R$  is noetherian,  $S$  would contain a maximal element  $A$ . Obviously  $A$  is a proper ideal which is not prime, and every integral ideal properly containing  $A$  must contain a product of prime ideals. Since  $A$  is not prime, there exist  $\alpha, \beta \in R$  such that  $\alpha, \beta \notin A$  but  $\alpha\beta \in A$ . The ideals  $A + \alpha R, A + \beta R$  both properly contain  $A$  and hence contain products of prime ideals. However,

$$(A + \alpha R)(A + \beta R) \subset A \cdot A + \alpha A + \beta A + \alpha\beta R \subset A,$$

so  $A$  also contains a product of prime ideals. This is a contradiction, and therefore  $S$  is empty. This proves (18.6).

(18.7) DEFINITION. For an integral ideal  $A$ , define

$$A^{-1} = \{\alpha \in K : \alpha A \subset R\}.$$

If  $x \in A, x \neq 0$ , then  $\alpha x \in R$  implies  $\alpha \in Rx^{-1}$ . Therefore  $A^{-1}$  is an  $R$ -submodule of the finitely generated  $R$ -module  $Rx^{-1}$ , and  $A^{-1}$  is also a finitely generated  $R$ -module. Thus  $A^{-1}$  is a fractional ideal, and clearly  $A^{-1} \supset R$ . Furthermore,  $R^{-1} = R$ , since, if  $\alpha \in K$  is such that  $\alpha R \subset R$ , then  $\alpha \cdot 1 \in R$ . We note also that  $A \supset B$  implies  $A^{-1} \subset B^{-1}$ .

(18.8) LEMMA. *If  $A$  is a proper ideal, then  $A^{-1}$  properly contains  $R$ .*

PROOF. By hypothesis,  $A$  is an ideal properly contained in  $R$ , and obviously  $A^{-1} \supset R$ . We must show that this latter inclusion is proper. Choose  $\alpha \in A, \alpha \neq 0$ ; by Lemma 18.6 we can find prime

ideals  $P_1, \dots, P_n$  such that

$$P_1 \cdots P_n \subset \alpha R \subset A.$$

Choose such a set of prime ideals with minimal possible  $n$ . Since  $A \neq R$ , the fact that the ideals of  $R$  satisfy the A.C.C. implies that  $A$  is contained in some maximal ideal  $P$ . Thus

$$P_1 \cdots P_n \subset P.$$

If no  $P_i = P$ , each  $P_i$  contains an element  $\alpha_i \notin P$ , and  $\alpha_1 \cdots \alpha_n \in P$ , which is impossible. Therefore  $P$  coincides with some  $P_i$ , say  $P = P_1$ . We now have

$$PP_2 \cdots P_n \subset \alpha R \subset A \subset P.$$

By the minimality of  $n$ , we know that  $P_2 \cdots P_n \subsetneq \alpha R$ . Choose  $\beta \in P_2 \cdots P_n$  such that  $\beta \notin \alpha R$ , and set  $\lambda = \alpha^{-1}\beta$ . Then  $\lambda \notin R$ , and we have

$$\lambda A = \alpha^{-1}\beta A \subset \alpha^{-1}\beta P \subset \alpha^{-1}PP_2 \cdots P_n \subset R,$$

so  $\lambda \in A^{-1}$ .

(18.9) **LEMMA.** *If  $A$  is an integral ideal, then  $A^{-1}A = R$ .*

**PROOF.** Set  $B = A^{-1}A$ ; certainly  $B$  is an integral ideal. Therefore  $AA^{-1}B^{-1} = BB^{-1} \subset R$ , so  $A^{-1}B^{-1} \subset A^{-1}$ . Hence for any  $\beta \in B^{-1}$  we have  $A^{-1}\beta \subset A^{-1}$ , and so  $A^{-1}\beta^m \subset A^{-1}$  for all  $m$ . But then  $A^{-1}[\beta]$  is an  $R$ -submodule of  $A^{-1}$  and is therefore finitely generated. However  $R[\beta]$ , being a submodule of  $A^{-1}[\beta]$ , is also finitely generated. Because  $R$  is integrally closed, it follows that  $\beta \in R$ . This shows that  $B^{-1} \subset R$ , and consequently  $B^{-1} = R$ . Using Lemma 18.8, we have  $B = R$  as required.

(18.10) **THEOREM.<sup>†</sup>** *Every proper ideal  $A$  is a product of prime ideals. If  $A = X_1 \cdots X_k = Y_1 \cdots Y_m$  are two expressions for  $A$  as a product of prime ideals, then  $k = m$ , and the  $\{X_i\}$  are a rearrangement of the  $\{Y_j\}$ .*

**PROOF.** By Lemma 18.6,  $A$  contains a product of prime ideals,

$$P_1 \cdots P_n \subset A.$$

Choose a maximal ideal  $P$  such that  $A \subset P$ . As in the proof of Lemma 18.8,  $P$  coincides with some  $P_i$ , say  $P = P_1$ . Then

$$P^{-1} \cdot PP_2 \cdots P_n = P_2 \cdots P_n \subset P^{-1}A \subset R.$$

---

<sup>†</sup>The reader should convince himself that any integral domain for which this theorem holds must be a Dedekind domain.

Suppose we have shown that an integral ideal which contains a product of fewer than  $n$  prime ideals is expressible as a product of prime ideals (a fact which is trivially true for  $n = 2$  because prime ideals are maximal). We then deduce that

$$P^{-1}A = Q_1 \cdots Q_r, \quad Q_j \text{ prime,}$$

whence

$$A = PP^{-1}A = PQ_1 \cdots Q_r.$$

The principle of mathematical induction completes the first part of the proof.

To prove uniqueness of the factorization, we establish a slightly more general result.

(18.11) LEMMA. *Let  $P_1 \cdots P_n \subset Q_1 \cdots Q_m$  where the  $\{P_i\}$  and  $\{Q_j\}$  are prime ideals. Then  $m \leq n$ , and the  $\{Q_j\}$  are a rearrangement of a subset of the  $\{P_i\}$ .*

PROOF. We have  $P_1 \cdots P_n \subset Q_1 \cdots Q_m \subset Q_1$  whence, as in Lemma 18.8,  $Q_1$  must equal some  $P_i$ , say  $Q_1 = P_1$ . Then

$$P_1^{-1} \cdot P_1 \cdots P_n \subset Q_1^{-1}Q_1 \cdots Q_m,$$

so  $P_2 \cdots P_n \subset Q_2 \cdots Q_m$ , and so on.

(18.12) COROLLARY. *If  $A$  and  $B$  are integral ideals, then  $A \subset B$  if and only if there exists an integral ideal  $C$  such that  $A = BC$ .*

Now let  $A$  be an ideal in  $K$ . Since  $A$  is a finitely generated  $R$ -module, we may write  $A = R\alpha_1 + \cdots + R\alpha_n$ ,  $\alpha_i \in A$ . Choose  $\beta \in R$  such that  $\beta\alpha_1, \dots, \beta\alpha_n$  all lie in  $R$ ; this is possible since  $K$  is the quotient field of  $R$ . We then have  $\beta A \subset R$ , and we may express  $\beta A$  as a product of prime ideals<sup>†</sup>

$$\beta A = P_1 \cdots P_n.$$

If  $\beta R = Q_1 \cdots Q_m$  with the  $\{Q_i\}$  prime ideals, we have

$$A = \beta^{-1}P_1 \cdots P_n = P_1 \cdots P_n Q_1^{-1} \cdots Q_m^{-1}.$$

Hence every fractional ideal can be expressed as a product of prime ideals and inverses of prime ideals. Furthermore, if we define  $A^{-1}$  [as in Definition 18.7] for any ideal, whether integral or not, we find at once that  $A^{-1} = P_1^{-1} \cdots P_n^{-1} Q_1 \cdots Q_m$ . Finally, the expression of  $A$  in the form  $A = P_1 \cdots P_n Q_1^{-1} \cdots Q_m^{-1}$ , where the  $\{P_i\}$  and the

<sup>†</sup> If it happens that  $\beta A = R$ , set  $n = 0$ , and interpret a vacuous product of prime ideals as being equal to  $R$ .

$\{Q_j\}$  are disjoint sets of prime ideals, is unique up to the order of occurrence of the factors. We have proved

(18.13) THEOREM. *Under the product operation the ideals in  $K$  form an abelian multiplicative group with identity element  $R$ , and in which the inverse of  $A$  is given by  $A^{-1} = \{\alpha \in K : \alpha A \subset R\}$ .*

The next result shows the striking similarity between prime factorization of ideals and prime factorization of rational integers.

(18.14) THEOREM. *Let  $A, B$  be integral ideals, and let*

$$A = P_1^{a_1} \cdots P_n^{a_n}, \quad B = P_1^{b_1} \cdots P_n^{b_n}, \quad a_i, b_i \in \mathbb{Z}, a_i, b_i \geq 0.$$

where the  $\{P_i\}$  are distinct prime ideals, and  $P_i^0$  is taken to be  $R$ . Then

$$A + B = \prod_{i=1}^n P_i^{\min(a_i, b_i)}, \quad A \cap B = \prod_{i=1}^n P_i^{\max(a_i, b_i)}.$$

PROOF. The ideal  $A + B$  is the smallest ideal containing both  $A$  and  $B$ , and hence by (18.12) it is the smallest ideal which is an integral ideal divisor of both  $A$  and  $B$ . This fact, combined with Theorem 18.10, proves the first assertion. A similar argument proves the formula for  $A \cap B$ .

As a corollary we have  $AB = (A + B)(A \cap B)$ .

(18.15) DEFINITION. Two integral ideals  $A$  and  $B$  are *relatively prime* if  $A + B = R$ . The integral ideals  $\{A_1, \dots, A_n\}$  are *pairwise relatively prime* if  $A_i + A_j = R, i \neq j$ .

Another immediate consequence of (18.14) is

(18.16) *Two integral ideals  $A$  and  $B$  are relatively prime if and only if they have no common prime factor. Further, if  $A + B = R$ , then  $AB = A \cap B$ .*

From (18.16) we obtain at once

(18.17) *The integral ideals  $A_1, \dots, A_n$  are pairwise relatively prime if and only if*

$$A_i + \prod_{j \neq i} A_j = R, \quad 1 \leq i \leq n.$$

(18.18) THEOREM (Chinese Remainder Theorem). *Let  $\{A_1, \dots, A_n\}$  be a set of pairwise relatively prime integral ideals, and let  $\{\alpha_1, \dots, \alpha_n\}$  be an arbitrary set of elements in  $R$ . Then there exists an element  $\alpha \in R$  such that*

$$\alpha \equiv \alpha_i \pmod{A_i}, \quad 1 \leq i \leq n.$$

The element  $\alpha$  is uniquely determined mod  $A_1 \cdots A_n$ .

PROOF. By (18.17) there exist elements  $\{\beta_i\} \in A_i$ ,  $\{\beta'_i\} \in \prod_{j \neq i} A_j$ , such that  $\beta_i + \beta'_i = 1$ ,  $1 \leq i \leq n$ . Set

$$\alpha = \beta'_1 \alpha_1 + \cdots + \beta'_n \alpha_n;$$

then  $\alpha \equiv \beta'_i \alpha_i \pmod{A_i}$ . Since  $\beta_i + \beta'_i = 1$ , we have  $\beta'_i \equiv 1 \pmod{A_i}$ . Combining these results, we have  $\alpha \equiv \alpha_i \pmod{A_i}$  as required. Now suppose  $\alpha'$  is another solution of the congruences; then

$$\alpha - \alpha' \in A_1 \cap \cdots \cap A_n = A_1 \cdots A_n,$$

by (18.17) and (18.16).

(18.19) COROLLARY. Let  $\{A_1, \dots, A_n\}$  satisfy the hypotheses of (18.18). Then there exists a ring isomorphism

$$R/(A_1 \cdots A_n) \cong R/A_1 + \cdots + R/A_n.$$

PROOF. Define a ring homomorphism by

$$\varphi: \alpha \rightarrow (\varphi_1(\alpha), \dots, \varphi_n(\alpha)), \quad \alpha \in R,$$

where  $\varphi_i$  is the natural homomorphism of  $R \rightarrow R/A_i$ ,  $1 \leq i \leq n$ . The kernel of this map is  $A_1 \cap \cdots \cap A_n$ , which is equal to  $A_1 \cdots A_n$  by (18.16). The mapping is onto by (18.18). This completes the proof of the corollary.

We conclude this section with several interesting results which will be needed later.

(18.20) THEOREM. Let  $A, B$  be integral ideals. Then there exists an integral ideal  $C$  which is relatively prime to  $B$  such that  $AC$  is a principal ideal.

PROOF. (See Hecke [1], p. 97.) Let us set

$$A = P_1^{a_1} \cdots P_n^{a_n}, \quad B = P_1^{b_1} \cdots P_n^{b_n}, \quad a_i \geq 0, b_i \geq 0,$$

where  $P_1, \dots, P_n$  are distinct primes. Choose  $\alpha_i \in P_i^{a_i}$  such that  $\alpha_i \notin P_i^{a_i+1}$ . By Theorem 18.18 we can find  $\alpha \in R$  such that

$$\alpha \equiv \alpha_i \pmod{P_i^{a_i+1}}, \quad 1 \leq i \leq n.$$

Then  $\alpha \in P_i^{a_i}$ ,  $\alpha \notin P_i^{a_i+1}$ ,  $1 \leq i \leq n$ . Therefore  $\alpha$  lies in the intersection of the ideals  $P_1^{a_1}, \dots, P_n^{a_n}$ , and thus  $\alpha \in A$ . Further, we

---

<sup>†</sup> We use the congruence notation  $a \equiv b \pmod{A}$  for the statement that  $a - b \in A$ .

have, from Theorem 18.14,

$$(18.21) \quad \alpha R + AB = A .$$

Since  $\alpha R \subset A$ , there exists by (18.12) an integral ideal  $C$  such that  $\alpha R = AC$ . Substituting in (18.21), we have

$$AC + AB = A ,$$

and multiplying by  $A^{-1}$  yields  $C + B = R$ . This completes the proof of the theorem.

(18.22) COROLLARY. *Let  $A$  be an integral ideal. Then there exist elements  $\rho, \sigma \in R$  such that  $A = \rho R + \sigma R$ .*

PROOF. Let  $\rho$  be any non-zero element of  $A$ , and choose an integral ideal  $B$  relatively prime to  $\rho R$  such that  $AB$  is principal, say  $AB = \sigma R$ . Then

$$\rho R + \sigma R = \rho R + AB \subset A .$$

On the other hand, we may write  $1 = \beta + \rho\alpha$ ,  $\beta \in B$ ,  $\alpha \in R$  since  $B + \rho R = R$ . Therefore, for each  $a \in A$ , we have

$$a = a\rho\alpha + a\beta \in \rho R + AB ,$$

and thus  $A \subset \rho R + \sigma R$ . This completes the proof.

(18.23) COROLLARY. *Let  $\{P_1, \dots, P_n\}$  be any set of distinct prime ideals and  $\{a_1, \dots, a_n\}$  a set of non-negative integers. Then there exists  $\alpha \in R$  and an integral ideal  $B$  prime to every  $P_i$  such that  $\alpha R = P_1^{a_1} \cdots P_n^{a_n} B$ .*

(18.24) COROLLARY. *Let  $A, B$  be integral ideals. Then the additive groups  $R/A$  and  $B/AB$  are isomorphic.*

PROOF. By Theorem 18.20 we may find an integral ideal  $C$  prime to  $A$  such that  $BC$  is a principal ideal, say  $BC = \rho R$ . Then

$$\varphi: \alpha \rightarrow \rho\alpha + AB , \quad \alpha \in R ,$$

is a group homomorphism of  $R$  onto  $B/AB$ , since

$$\rho R + AB = CB + AB = (C + A)B = RB = B .$$

It remains to determine the kernel of  $\varphi$ . Let  $\rho\alpha \in AB$ . Then  $\rho\alpha C \subset ABC = \rho A$ , and we have  $\alpha C \subset A$ . Because  $A + C = R$ , however, it follows that  $\alpha_0 + \gamma = 1$  for some  $\alpha_0 \in A$ ,  $\gamma \in C$ . Then

$$\alpha = \alpha\alpha_0 + \alpha\gamma \in A .$$

Conversely,  $\alpha \in A$  implies  $\varphi(\alpha) = \rho\alpha + AB = AB$ . Thus the kernel

of  $\varphi$  is  $A$ , and Corollary 18.24 is proved.

### Exercises

$R$  denotes a Dedekind domain throughout, with quotient field  $K$ .

- Prove that a fractional ideal can be expressed as a product of prime ideals and their inverses in only one way. In other words, if

$$P_1 \cdots P_m Q_1^{-1} \cdots Q_n^{-1} = A_1 \cdots A_r B_1^{-1} \cdots B_s^{-1},$$

all denoting prime ideals, and if no  $Q_i$  is a  $P_j$  and if no  $B_l$  is an  $A_j$ , then the  $\{P_i\}$  are a rearrangement of the  $\{A_j\}$ , the  $\{Q_i\}$  of the  $\{B_j\}$ .

- If  $A, B, C$  are integral ideals such that  $A$  is relatively prime to both  $B$  and  $C$ , then  $A$  is relatively prime to  $BC$ . (Prove directly from the definition without using factorization into prime ideals.)

- If  $\{A_1, \dots, A_n\}$  is a set of pairwise relatively prime ideals and if we set  $B_i = \prod_{j \neq i} A_j$ , then  $B_1 + \cdots + B_n = R$ .

- If  $A, B$  are relatively prime integral ideals, show that  $A^2$  and  $B^2$  are also relatively prime, without using factorization into prime ideals.

- Let  $A$  be an ideal in  $K$ . Prove that  $\{\alpha \in K : \alpha A \subset A\} = R$ .

- Show that the statement in Corollary 18.23 is valid even when some of the integers  $\{a_1, \dots, a_n\}$  are negative, provided that we change the assertion from " $\alpha \in R$ " to " $\alpha \in K$ ".

- Using the result of Problem 6, show that Corollary 18.24 of Theorem 18.20 holds even when the ideal  $B$  is fractional.

- Prove that if  $A$  is an integral ideal in  $R$ , then  $R/A$  satisfies the D.C.C. for ideals.

## § 19. Valuations; $P$ -adic Numbers

We assume, throughout this section, that  $R$  is the ring of all algebraic integers in an algebraic number field  $K$ . Let  $P$  be a prime ideal in  $R$ . If  $\alpha \in K, \alpha \neq 0$ , we may factor the principal ideal  $\alpha R$  into a product of positive and negative powers of prime ideals. Let  $\nu_P(\alpha)$  denote the exponent to which  $P$  occurs in this factorization; if  $P$  does not occur, set  $\nu_P(\alpha) = 0$ . When there is no danger of confusion, we shall write  $\nu(\alpha)$  instead of  $\nu_P(\alpha)$ . Let us set  $\nu(0) = +\infty$ . For  $\alpha \in R, \alpha \neq 0$ , we may characterize  $\nu(\alpha)$  by

$$\alpha \in P^{\nu(\alpha)}, \quad \alpha \notin P^{\nu(\alpha)+1}.$$

We have at once

$$(19.1) \quad \nu(\alpha\beta) = \nu(\alpha) + \nu(\beta), \quad \nu(\alpha/\beta) = \nu(\alpha) - \nu(\beta),$$

where  $\beta \neq 0$  in the latter equation.

If  $A$  is a non-zero ideal in  $K$ , we similarly define  $\nu_P(A)$  as the exponent to which  $P$  occurs in the factorization of  $A$  into powers of prime ideals, and denote it by  $\nu(A)$  for brevity. Set  $\nu(0) = +\infty$ . We may observe that  $\nu(\alpha) = \nu(\alpha R)$  for  $\alpha \in K$  and that, if  $A, B$  are ideals such that  $A \subset B$ , then  $A = BC$  for some integral ideal  $C$ , and so  $\nu(A) \geq \nu(B)$ . Hence, if  $A$  is any ideal, then  $\alpha \in A$  implies  $\alpha R \subset A$  so that  $\nu(\alpha) \geq \nu(A)$ . On the other hand, we may find an integral ideal  $C$  prime to  $P$  such that  $AC = \beta R$  is principal; then  $\beta \in A$ , and  $\nu(\beta) = \nu(A)$ . We have thus shown

$$(19.2) \quad \nu(A) = \min_{\alpha \in A} \nu(\alpha).$$

We next prove that

$$(19.3) \quad \nu(\alpha + \beta) \geq \min(\nu(\alpha), \nu(\beta)),$$

with equality when  $\nu(\alpha) \neq \nu(\beta)$ . Let  $r = \min(\nu(\alpha), \nu(\beta))$ . Then  $P^r$  occurs as a factor of both  $\alpha R$  and  $\beta R$  and hence of  $\alpha R + \beta R$ . Since  $(\alpha + \beta) \in \alpha R + \beta R$ , this shows that  $\nu(\alpha + \beta) \geq \nu(\alpha R + \beta R) \geq r$ . Furthermore, suppose  $\nu(\alpha) \neq \nu(\beta)$  and, say,  $r = \nu(\alpha) < \nu(\beta)$ . Then

$$r = \nu(\alpha) = \nu((\alpha + \beta) - \beta) \geq \min(\nu(\alpha + \beta), \nu(\beta)),$$

whence  $\nu(\alpha + \beta) = r$ .

(19.4) **DEFINITION.** A valuation of a field  $K$  is a mapping which assigns to each  $\alpha \in K$  a non-negative real number  $|\alpha|$  such that

- (i)  $|\alpha| = 0$  if and only if  $\alpha = 0$ .
- (ii)  $|\alpha\beta| = |\alpha||\beta|$ .
- (iii)  $|\alpha + \beta| \leq |\alpha| + |\beta|$ .

If the valuation satisfies the stronger condition

$$(iv) \quad |\alpha + \beta| \leq \max(|\alpha|, |\beta|),$$

call it *non-Archimedean*. The set of real numbers

$$\{|\alpha| : \alpha \in K, \alpha \neq 0\}$$

is called the *value group* associated with the valuation. If the value group is an infinite cyclic group, we say that the valuation is *discrete*.

We may define the  *$P$ -adic valuation* of the algebraic number field  $K$  by means of

$$|\alpha| = \{N(P)\}^{-\nu_P(\alpha)}, \quad \alpha \in K, \alpha \neq 0,$$

and  $|0| = 0$ . Here,  $N(P) = [R: P]$  is the *norm* of the prime ideal  $P$  (see §20) and is a rational integer greater than 1. This  $P$ -adic valuation is then easily seen to be a discrete non-Archimedean valua-

tion of  $K$ . (If instead of  $N(P)$  we had chosen a real number  $t > 1$  and had set  $|\alpha|' = t^{-v_P(\alpha)}$ , the valuation  $|\cdot|'$  would have been equivalent to the valuation  $|\cdot|$  in the sense that  $|\alpha|' \leq 1$  if and only if  $|\alpha| \leq 1$ .)

With the  $P$ -adic valuation is associated a *valuation ring*  $R^*$  defined by

$$R^* = \{\alpha \in K : |\alpha| \leq 1\}.$$

The elements of  $R^*$  are called the  *$P$ -adic integers in  $K$*  or the  *$P$ -integral elements of  $K$* . In  $R^*$  we single out the ideal

$$P^* = \{\alpha \in K : |\alpha| < 1\},$$

which is obviously a prime ideal in  $R^*$ . We have  $R \subset R^*$ , and  $P \subset P^*$ .

(19.5) THEOREM. *The ideals  $R^*, P^*, P^{*2}, P^{*3}, \dots$  are the only non-zero ideals in  $R^*$ . Consequently,  $P^*$  is a maximal ideal in  $R^*$ . Further, the fields  $R^*/P^*$  and  $R/P$  are isomorphic.*

PROOF. Let  $A^*$  be a non-zero ideal in  $R^*$ , and let  $\alpha \in A^*, \alpha \neq 0$ . If  $|\beta| \leq |\alpha|$ , then  $\beta/\alpha \in R^*$ , and so  $\beta = \alpha(\beta/\alpha) \in A^*$ . Thus, every ideal in  $R^*$  is a principal ideal, generated by an element of maximal absolute value. Choose  $\pi \in P$  such that  $\pi \notin P^2$ ; every ideal in  $R^*$  is of the form  $\pi^r R^* = (\pi R^*)^r$  for some non-negative integer  $r$ . Thus  $P^* = \pi R^*$ , and  $P^*$  is a maximal ideal in  $R^*$ .

We now show that  $R^*/P^* \cong R/P$ . Let  $\theta: R \rightarrow R^*/P^*$  be gotten by first mapping  $R$  into  $R^*$  (by the inclusion map) and then mapping  $R^*$  onto  $R^*/P^*$  (canonically). If  $\alpha \in R$  is such that  $\theta(\alpha) = 0$ , then  $\alpha = \pi\beta, \beta \in R^*$ . Therefore,  $|\alpha| = |\pi||\beta| \leq |\pi|$ , and so  $\alpha \in P$ . This shows that the kernel of  $\theta$  is  $P$ .

Finally, we must show that  $\theta(R) = R^*/P^*$ . If  $\beta \in R^*$ , we wish to prove the existence of an element  $\alpha \in R$  such that  $\alpha - \beta \in P^*$ . If  $\beta \in P^*$ , take  $\alpha = 0$ . Suppose hereafter that  $\beta \notin P^*$ . Then  $|\beta| = 1$  so that we may write  $\beta = \gamma/\delta, \gamma, \delta \in R, |\gamma| = |\delta|$ . Therefore  $|\delta\gamma^{-1}| = 1$ , and by (18.14)

$$\delta\gamma^{-1}R + P \supset R.$$

Hence there exist  $\lambda \in R$  and  $p \in P$  such that

$$\lambda\delta\gamma^{-1} + p = 1, \quad \text{or} \quad \lambda\delta + p\gamma = \gamma.$$

Therefore

$$|\lambda - \beta| = |\lambda - \gamma\delta^{-1}| = |\lambda\delta - \gamma||\delta| = |p\gamma||\delta| < 1,$$

and so we have an element  $\lambda \in R$  such that  $\lambda - \beta \in P^*$ . This com-

plete the proof.

To every  $R$ -ideal  $A$  in  $K$  there corresponds an  $R^*$ -ideal  $A^*$  in  $K$ , defined by

$$A^* = AR^* = \{ \sum \alpha_i \beta_i : \alpha_i \in A, \beta_i \in R^* \} .$$

If  $A \subset R$ , then  $A^* \subset R^*$ . Further, it is easily verified that, if we let  $\nu_P(A)$  denote the exponent to which  $P$  occurs in the factorization of  $A$  into powers of prime ideals, then

$$A^* = \{P^*\}^{\nu_P(A)} = \pi^{\nu_P(A)} R^*$$

where  $P^* = P \cdot R^*$  and  $\pi$  denotes some element of  $P$  for which  $\nu_P(\pi) = 1$ . We often use the following consequence of the above formula.

*If  $A$  and  $B$  are  $R$ -ideals in  $K$ , then  $\nu_P(A) = \nu_P(B)$  if and only if  $A^* = B^*$ .*

We finally observe (proof omitted) that, if  $A$  is any non-zero  $R$ -ideal in  $K$ , then

$$\{\alpha \in K : \alpha A^* \subset R^*\} = A^{-1}R^* .$$

As an immediate application of the above concepts, we prove a basic result on contents of polynomials.

(19.6) **DEFINITION.** Let  $f(x) = a_0x^n + a_1x^{n-1} + \cdots + a_n \in K[x]$ , and let  $R = \text{alg. int. } \{K\}$ . We set

$$\text{content of } f(x) = a_0R + a_1R + \cdots + a_nR ,$$

the ideal generated by the coefficients of  $f(x)$ .

We are now ready to prove

(19.7) **THEOREM.** *Let  $f(x)$  and  $g(x) \in K[x]$ . Then*

(19.8) (content of  $f(x)$ ) (content of  $g(x)$ ) = content of  $f(x)g(x)$ .

**PROOF.** Let  $P$  be any prime ideal of  $R$ , and let  $R^*$  be the ring of  $P$ -integral elements of  $K$ . It suffices to prove the above for the ring  $R^*$  instead of  $R$ , since this will imply that  $P$  occurs to the same exponent on both sides of equation (19.8). Keeping the earlier notation, we choose  $\pi \in P$  so that  $\pi \notin P^2$ , and let  $P^* = \pi R^*$  be the unique maximal ideal in  $R^*$ . We may write

$$f(x) = \pi^a f_0(x) , \quad g(x) = \pi^b g_0(x) ,$$

with  $f_0(x), g_0(x) \in R^*[x]$  such that (relative to  $R^*$ )

$$\text{content of } f_0(x) = \text{content of } g_0(x) = R^* .$$

If bars denote passage to the residue class field  $R^*/P^*$ , then  $\overline{f_0(x)}$  and  $\overline{g_0(x)}$  are non-zero polynomials over  $R^*/P^*$ . Hence  $\overline{f_0(x)g_0(x)} \neq 0$ , so that the content of  $f_0(x)g_0(x)$  is  $R^*$ . Therefore (relative to  $R^*$ ),

$$\text{content of } f(x)g(x) = \pi^{a+b}R^*,$$

which establishes the theorem.

Now let  $S$  be a finite set of distinct prime ideals  $\{P_1, \dots, P_r\}$  of  $R$ , and define

$$R_S = \{\alpha \in K : \nu_{P_1}(\alpha) \geq 0, \dots, \nu_{P_r}(\alpha) \geq 0\}.$$

Then  $R_S$  is a subring of  $K$ , the ring of *S-integral elements* of  $K$ , and clearly  $R_S \supset R$ . It is easily verified that  $R_S$  is a principal ideal ring; in fact, if  $\{a_1, \dots, a_r\}$  is any set of integers, then

$$\{\beta \in K : \nu_{P_1}(\beta) \geq a_1, \dots, \nu_{P_r}(\beta) \geq a_r\}$$

defines an  $R_S$ -ideal in  $K$ , and every  $R_S$ -ideal in  $K$  is of this form. If we choose, for each  $i$ ,  $1 \leq i \leq r$ , an element  $\pi_i \in P_i$  such that  $\pi_i \notin P_j^2$ ,  $\pi_i \notin P_j$  ( $j \neq i$ ), the above ideal is given by

$$\pi_1^{a_1} \cdots \pi_r^{a_r} R_S.$$

The ideal lies in  $R_S$  if and only if each  $a_i \geq 0$ . If  $A$  is any  $R$ -ideal in  $K$ , there corresponds to it an  $R_S$ -ideal in  $K$  given by

$$A_S = AR_S = \pi_1^{\nu_{P_1}(A)} \cdots \pi_r^{\nu_{P_r}(A)} R_S.$$

In particular, if  $A, B$  are  $R$ -ideals in  $K$  and if we let  $S$  be the set of all primes occurring with non-zero exponent in either  $A$  or  $B$ , we have

$$A = B \text{ if and only if } AR_S = BR_S.$$

The proofs of all the above statements are straightforward and will be left to the exercises.

We shall now discuss briefly the process of completing a field with respect to a valuation. The most familiar example of this is the manner in which the real field is obtained from the rational field by use of Cauchy sequences.

Let  $K$  be a field with a valuation  $| |$ , which may be either Archimedean or non-Archimedean. A *Cauchy sequence* is a sequence  $\{a_n\}$  of elements of  $K$  such that

$$\lim_{m, n \rightarrow \infty} |a_m - a_n| = 0;$$

that is, for each  $\epsilon > 0$  there exists an integer  $N$  such that

$$|a_m - a_n| < \epsilon \quad \text{for } m, n > N.$$

On the other hand, we say that the sequence  $\{a_n\}$  converges to  $a$  if  $\lim_{n \rightarrow \infty} |a_n - a| = 0$ ; that is, for each  $\epsilon > 0$ , there exists an integer  $N$  such that

$$|a_n - a| < \epsilon \quad \text{for } n > N.$$

The following are then easy consequences of the definitions:

- (i) Every convergent sequence is a Cauchy sequence.
- (ii) If a subsequence of a Cauchy sequence converges, so does the sequence, and to the same limit.
- (iii) If  $\{a_n\}$  and  $\{b_n\}$  are Cauchy sequences, so are  $\{a_n + b_n\}$ ,  $\{a_n - b_n\}$ ,  $\{a_n b_n\}$ ,  $\{aa_n\}$  (where  $a \in K$ ).
- (iv) If  $\{a_n\}$  is a Cauchy sequence which does not converge to 0, then  $a_n^{-1}$  exists from some  $n_0$  on. If we form  $\{a_n^{-1}\}$ , starting with  $a_{n_0}^{-1}$  as first term, then  $\{a_n^{-1}\}$  is also a Cauchy sequence.

The converse of (i) need not be true, as is evident from the case where  $K$  is the rational field and  $| \cdot |$  the ordinary absolute value.

(19.9) DEFINITION. A field  $K$  is *complete with respect to a valuation* if every Cauchy sequence (relative to the valuation) converges to an element of  $K$ .

We now show how to embed  $K$  in a field  $\tilde{K}$  which is complete with respect to an extension of the valuation from  $K$  to  $\tilde{K}$ . If  $\{a_n\}$  is any Cauchy sequence from  $K$ , let  $\{a_n\}^*$  denote the collection of all Cauchy sequences  $\{b_n\}$  from  $K$  such that

$$\lim_{n \rightarrow \infty} |a_n - b_n| = 0 ;$$

that is,

$$\begin{aligned} \{a_n\}^* &= \text{set of all Cauchy sequences } \{b_n\} \\ &\text{such that } \{a_n - b_n\} \text{ converges to 0.} \end{aligned}$$

We see at once that, if  $\{a_n\}$  and  $\{c_n\}$  are Cauchy sequences, then  $\{a_n\}^*$  and  $\{c_n\}^*$  either coincide or are disjoint, depending on whether  $\{a_n - c_n\}$  converges to 0 or not. For each  $a \in K$ , the sequence  $\{a_n\}$  defined by  $a_1 = a_2 = \dots = a$  is a Cauchy sequence; let us denote this  $\{a_n\}^*$  by  $a^*$ , for brevity. Then  $a^* = b^*$  if and only if  $a = b$ . Let  $\tilde{K}$  denote the collection of the distinct sets  $\{a_n\}^*$  obtained by letting  $\{a_n\}$  range over a complete set of non-equivalent Cauchy sequences. Define

$$\{a_n\}^* + \{b_n\}^* = \{a_n + b_n\}^*$$

$$\{a_n\}^* \{b_n\}^* = \{a_n b_n\}^*$$

$$\{a_n\}^* / \{b_n\}^* = \{a_n / b_n\}^* \quad \text{if } \{b_n\}^* \neq 0^*$$

where, in  $\{a_n/b_n\}$ , we start at an index  $n_0$  such that  $b_n \neq 0$  for  $n \geq n_0$ . It is easily checked that these definitions do not depend on the representative Cauchy sequences which are used. We find readily that  $\tilde{K}$  is a field with zero element  $0^*$  and unity element  $1^*$ . Further,  $a \rightarrow a^*$  is an isomorphism of  $K$  into  $\tilde{K}$ , and we may regard  $K$  as embedded in  $\tilde{K}$ .

Next we show how to extend the valuation from  $K$  to  $\tilde{K}$ . Let  $\alpha \in \tilde{K}$ ; then  $\alpha = \{a_n\}^*$  for some Cauchy sequence  $\{a_n\}$  from  $K$ . Define

$$|\alpha| = \lim_{n \rightarrow \infty} |a_n|.$$

Then we find at once that  $|\cdot|$  is a valuation on  $\tilde{K}$  which extends that of  $K$ . The valuation on  $\tilde{K}$  is Archimedean if and only if that of  $K$  is.

To show that  $\tilde{K}$  is complete with respect to the valuation thus defined, let  $\{\alpha_m\}$  be a Cauchy sequence of elements of  $\tilde{K}$ . For each  $m$ , we may find a Cauchy sequence  $\{a_n^{(m)} : n = 1, 2, \dots\}$  of elements of  $K$  such that

$$\alpha_m = \{a_n^{(m)}\}^*, \quad m = 1, 2, \dots.$$

One proves easily that  $\{a_n^{(n)} : n = 1, 2, \dots\}$  is a Cauchy sequence from  $K$ , and hence it determines an element  $\beta = \{a_n^{(n)}\}^* \in \tilde{K}$ . Then we have

$$\lim_{m \rightarrow \infty} |\alpha_m - \beta| = \lim_{m \rightarrow \infty} \lim_{n \rightarrow \infty} |a_n^{(m)} - a_n^{(n)}| = 0$$

so that  $\{\alpha_m\}$  converges to  $\beta$  in  $\tilde{K}$ . Thus  $\tilde{K}$  is a complete field. This shows, incidentally, that the process of completion terminates here; that is,  $(\tilde{K}) \cong \tilde{K}$ .

In the case of the rational field  $Q$ , if  $|\cdot|$  denotes the ordinary absolute value, then  $\tilde{Q}$  is the real field. On the other hand, if  $|\cdot|$  is the  $p$ -adic valuation of  $Q$  where  $p$  is a rational prime, then  $\tilde{Q}$  is the field of  $p$ -adic numbers over  $Q$ .

Now let  $K$  be an algebraic number field,  $R$  its ring of algebraic integers,  $P$  a prime ideal in  $R$ , and  $|\cdot|$  the  $P$ -adic valuation of  $K$ . It is easily shown that  $K$  is not complete with respect to this valuation. Let us form the  $P$ -adic completion  $\tilde{K}$ , and set

$$\tilde{R} = \{\alpha \in \tilde{K} : |\alpha| \leq 1\}, \quad \tilde{P} = \{\alpha \in \tilde{K} : |\alpha| < 1\}.$$

Then  $\tilde{P}$  is the unique maximal (prime) ideal in  $\tilde{R}$ , and  $\tilde{R}$  is a principal ideal ring with ideals  $\pi^m \tilde{R} (m = 0, 1, 2, \dots)$  where  $\pi \in P, \pi \notin P^2$ . Further, we have  $R^* = \tilde{R} \cap K$ , and

$$\tilde{R}/\tilde{P} \cong R/P.$$

(We omit the proofs of the above easily verified results.)  
Let  $\{a_n\}$  be a sequence of elements of  $R$  such that

$$(19.10) \quad a_{n+1} \equiv a_n \pmod{P^n}, \quad n \geq 1.$$

Then  $a_m \equiv a_n \pmod{P^n}$  for  $m > n$  so that  $|a_m - a_n| \rightarrow 0$  as  $n \rightarrow \infty$ ; thus  $\{a_n\}$  is a Cauchy sequence from  $R$ , and so defines an element  $\alpha = \{a_n\}^* \in \tilde{R}$ . Conversely, every element of  $\tilde{R}$  can be obtained in this way.

Now let  $L$  be a full set of residue class representatives of  $R/P$  which contains 0. Then (see §20)  $L$  is a finite set of elements of  $R$ , no two of which are congruent modulo  $P$ , and, for each sequence  $\{a_n\}$  satisfying (19.10), we may choose a sequence  $x_0, x_1, x_2, \dots$  of elements of  $L$  such that

$$a_n \equiv x_0 + x_1\pi + x_2\pi^2 + \cdots + x_{n-1}\pi^{n-1} \pmod{P^n}.$$

If  $s_n$  denotes the  $n$ th partial sum of the formal infinite series

$$x_0 + x_1\pi + x_2\pi^2 + \cdots,$$

then  $\lim(a_n - s_n) = 0$  so that  $\alpha = \{s_n\}^*$ . We frequently write

$$\alpha = x_0 + x_1\pi + x_2\pi^2 + \cdots$$

in this case. The elements of  $\tilde{K}$  are then of the form

$$\beta = \pi^t(x_0 + x_1\pi + x_2\pi^2 + \cdots), \quad x_i \in L, t \in Z, x_0 \neq 0,$$

with  $|\beta| = \{N(P)\}^{-t}$ . Each  $\beta \in \tilde{K}$  is uniquely expressible in this form.

### Exercises

- Find all possible valuations of the rational field.
- If  $A$  is a (non-zero)  $R$ -ideal in  $K$  and  $P$  is a prime ideal, prove that  $\{\alpha \in K : \alpha A^* \subset R^*\} = A^{-1}R^*$ .
- Prove the statements made about  $R_S$  where  $S$  is a finite set of distinct prime ideals in  $R$ .
- Let  $\tilde{Q}$  denote the  $p$ -adic completion of the rational field  $Q$  where  $p$  is a rational prime, and let  $L = \{0, 1, \dots, p-1\}$ . Every element of  $\tilde{Q}$  is then uniquely expressible in the form  $p'(x_0 + x_1p + \cdots)$ ,  $x_i \in L$ . Explain and illustrate the processes of addition, subtraction, multiplication, and division of such expressions.
- Let  $p$  be an odd prime, and define  $\tilde{Q}$  as above. If  $a \in Z$  is a quadratic residue  $\pmod{p}$  [that is, if there exists  $x_0 \in Z$  such that  $x_0^2 \equiv a \pmod{p}$ ],

and if  $p \nmid a$ , prove that there exists  $x \in \widetilde{Q}$  such that  $x^2 = a$ .

6. If  $\widetilde{Q}$  is the 2-adic completion of  $Q$ , show that  $x^2 = 17$  has a solution for  $x \in \widetilde{Q}$ .

7. Let  $R = \text{alg. int. } \{K\}$ ,  $P$  = prime ideal in  $R$ , and define  $v_P$  on  $K$  as at the beginning of this section. Prove that if  $\alpha, \beta \in K$  are such that  $v_P(\alpha) \geq v_P(\beta)$ , there exist elements  $\gamma, \delta \in R$  with  $v_P(\delta) = 0$  such that

$$\alpha/\beta = \gamma/\delta.$$

In other words, every  $P$ -integral element of  $K$  is expressible as a quotient of elements of  $R$  with the denominator a unit in  $R^*$ .

8. Keep the notation of the preceding problem. Let  $\alpha_1, \dots, \alpha_m \in K$  be such that  $\alpha_1 + \dots + \alpha_m = 0$ . Show that there exist at least two indices  $i$  and  $j$  for which

$$v_P(\alpha_i) = v_P(\alpha_j) = \min_{1 \leq t \leq m} v_P(\alpha_t).$$

9. Prove the "strong approximation theorem": Let  $P_1, \dots, P_n$  be distinct prime ideals in  $R$ , and let  $\alpha_1, \dots, \alpha_n$  be arbitrary elements of  $K$ . Let  $d_1, \dots, d_n$  be any preassigned set of positive integers. Then there exists an element  $\alpha \in K$  such that

$$\begin{aligned} v_{P_i}(\alpha - \alpha_i) &\geq d_i, & 1 \leq i \leq n, \\ v_P(\alpha) &\geq 0 & \text{for all } P \neq P_1, \dots, P_n. \end{aligned}$$

## § 20. Norms of Ideals; Ideal Classes

We assume throughout this section that  $R$  is the ring of all algebraic integers in an algebraic number field  $K$ . For  $P$  a prime ideal in  $R$ , we let  $N(P)$  (*norm* of  $P$ ) denote the number of residue classes into which  $R$  splits modulo  $P$ . Thus  $N(P)$  is the index  $[R:P]$  of the subgroup  $P$  in the additive group  $R$ . We have seen that  $P \cap Z = pZ$  where  $Z$  is the ring of rational integers and  $p$  is a rational prime. The prime  $p$  is in fact the unique rational prime contained in  $P$ . We then have

$$pR \subset P \subset R$$

so that  $N(P) = [R:P] \leq [R:pR] = p^n$ , where  $n = (R:Z)$  is the number of elements in a  $Z$ -basis for  $R$ . Since  $P$  is also a maximal ideal in  $R$ , the residue class ring  $R/P$  is a finite field with  $N(P)$  elements. Further,  $p(R/P) = 0$  shows that  $R/P$  is a field of characteristic  $p$ .

(20.1) DEFINITION. Let  $A$  be an ideal in  $R$ . The number of ele-

ments in  $R/A$  is the *norm* of  $A$  and is denoted by  $N(A)$ .

(20.2) THEOREM. If  $A, B$  are integral ideals, then  $N(AB) = N(A)N(B)$ . Consequently,

$$N(P_1^{a_1} \cdots P_n^{a_n}) = \{N(P_i)\}^{a_1} \cdots \{N(P_n)\}^{a_n}$$

where the  $\{P_i\}$  are prime ideals, the  $\{a_i\}$  non-negative integers.

PROOF. We give two separate proofs of this basic result.

(i) We have  $R \supset B \supset AB$ , all regarded as additive groups. Therefore [using Corollary 18.24],

$$N(AB) = [R: AB] = [R: B][B: AB] = [R: B][R: A] = N(B)N(A).$$

(ii) The second proof furnishes an insight into the structure of  $R/P^m$  where  $P$  is prime. From Corollary 18.19, we see that  $N(AB) = N(A)N(B)$  whenever  $A + B = R$ . To prove our theorem, we need only show that, for  $P$  a prime ideal and  $m$  a positive integer, we have  $N(P^m) = \{N(P)\}^m$ . We use induction on  $m$ . The result is clear for  $m = 1$ ; assume it holds for  $m \leq r - 1$ . We shall prove then that it holds for  $m = r$ .

Let  $\alpha_1, \dots, \alpha_s \in R$  be a complete residue system mod  $P$ ; then  $s = N(P)$ , and  $\alpha_i \not\equiv \alpha_j \pmod{P}$  for  $i \neq j$ . Let  $\beta_1, \dots, \beta_t$  be a complete residue system mod  $P^{r-1}$ ; by the induction hypothesis,  $t = \{N(P)\}^{r-1}$ . Choose  $\rho \in P^{r-1}$  such that  $\rho \notin P^r$ . Then the set of numbers

$$S = \{\alpha_i\rho + \beta_j : 1 \leq i \leq s, 1 \leq j \leq t\}$$

will be shown to form a complete residue system mod  $P^r$ , which will imply the desired result.

First, we note that

$$\alpha_i\rho + \beta_j \equiv \alpha_k\rho + \beta_l \pmod{P^r}$$

implies  $\beta_j \equiv \beta_l \pmod{P^{r-1}}$ , and so  $j = l$ . Therefore  $\rho(\alpha_i - \alpha_k) \in P^r$ , whence  $(\alpha_i - \alpha_k) \in P$ , and so  $i = k$ . This shows that no two distinct members of  $S$  can be congruent mod  $P^r$ .

On the other hand, let  $\xi$  be any element of  $R$ . We must show that  $\xi \equiv \alpha_i\rho + \beta_j \pmod{P^r}$  for some choice of  $i$  and  $j$ . Choose  $j$  such that  $\xi \equiv \beta_j \pmod{P^{r-1}}$ , and set  $\lambda = \xi - \beta_j \in P^{r-1}$ . From (18.14) we have

$$P^r + \rho R = P^{r-1},$$

and therefore we can find  $\tau \in P^r$  and  $\mu \in R$  such that  $\tau + \rho\mu = \lambda$ . Choose  $i$  so that  $\mu \equiv \alpha_i \pmod{P}$ . Then  $\lambda \equiv \rho\alpha_i \pmod{P^r}$ , and so  $\xi \equiv \rho\alpha_i + \beta_j \pmod{P^r}$ . This completes the proof.

We shall next obtain an expression for the norm of an ideal in terms of its conjugates and shall make the simplifying assumption that  $K$  is normal over  $Q$ . If  $G$  is the Galois group of  $K$  over  $Q$ , then  $G$  contains  $n$  elements  $\{\sigma_1, \dots, \sigma_n\}$  where  $n = (K:Q)$ . Setting  $R = \text{alg. int. } \{K\}$ , we see that each  $\sigma \in G$  maps  $R$  onto itself and carries each ideal  $A$  in  $R$  onto a *conjugate* ideal  $A^\sigma$ . Since  $\sigma$  induces an isomorphism

$$R/A \cong R^\sigma/A^\sigma,$$

we deduce that

$$(20.3) \quad N(A) = N(A^\sigma), \quad \sigma \in G.$$

Now we may prove

(20.4) THEOREM. *For  $A$  an ideal in  $R$  we have*

$$\prod_{\sigma \in G} A^\sigma = N(A)R.$$

PROOF. By (18.22) we may choose  $\alpha$  and  $\beta$  in  $R$  so that  $A = R\alpha + R\beta$ , and therefore

$$A^\sigma = R\alpha^\sigma + R\beta^\sigma, \quad \sigma \in G.$$

Set  $f(x) = \alpha + \beta x \in R[x]$ ; by (19.6) the content of  $f(x)$  is the ideal  $R\alpha + R\beta$  generated by the coefficients of  $f(x)$ . Thus we have, for  $\sigma \in G$ ,

$$\text{content of } f^\sigma(x) = A^\sigma.$$

On the other hand, the product

$$\prod_{\sigma \in G} f^\sigma(x) = F(x)$$

lies in  $Z[x]$ ; thus its content is of the form  $aR$ , where  $a$  is the positive rational integer which is the G.C.D. of the coefficients of  $F(x)$ . By Theorem 19.7 we conclude that

$$\prod_{\sigma \in G} A^\sigma = aR.$$

Taking norms and using (20.3), we obtain

$$N(A)^n = \text{number of elements in } R/aR = a^n.$$

This shows that  $a = N(A)$  and completes the proof.

(20.5) DEFINITION. Two fractional ideals  $A, B$  are *equivalent* if there exists  $r \in K, r \neq 0$  such that  $A = rB$ .

We see at once that this equivalence is reflexive, symmetric, and transitive, and so we may partition the set of fractional ideals into *ideal classes* with respect to this equivalence relation. The ideal class of  $A$  then contains all fractional ideals of the form  $rA$ ,  $r \in K$ ,  $r \neq 0$ . We note that, if  $A_i$  is equivalent to  $B_i$  ( $i = 1, 2$ ), then  $A_1 A_2$  is equivalent to  $B_1 B_2$ . We may therefore define multiplication of ideal classes by choosing as a representative of the product of two classes, the product of the representatives. With respect to this multiplication, the class containing  $R$  is the identity element, and the class of  $A^{-1}$  is the inverse of the class of  $A$ . Thus, the ideal classes form an abelian multiplicative group. The number of ideal classes is called the *class number* of the field  $K$  (or of the ring  $R$ ). We shall now show that this class number is finite. This result does not hold for an arbitrary Dedekind domain, although it is valid for the special case of the integers in an algebraic number field. We shall actually prove a more general theorem that will be needed later, which includes this result as a special case.

Let  $L$  be a skewfield of finite dimension over the rational field  $Q$ , say  $(L: Q) = n$ . Let  $L_0$  be a subring of  $L$  such that

- (i)  $L_0$  has a finite  $Z$ -basis,
- (ii)  $L_0$  contains a  $Q$ -basis for  $L$ .

In that case, it is clear that  $(L_0: Z) = (L: Q)$ . An  $L_0$ -ideal shall mean a non-zero left  $L_0$ -submodule of  $L$  which has a finite  $Z$ -basis. If  $X$  is an  $L_0$ -ideal, then  $QX \supset QL_0 X = LX = L$ , and so  $X$  also contains a  $Q$ -basis of  $L$ , and  $(X: Z) = n$ . For any pair of  $L_0$ -ideals  $X, Y$ , there exists a positive integer  $m \in Z$  such that  $mX \subset Y$ .

Now let us say that two  $L_0$ -ideals  $X, Y$  are in the same *class* if  $X = Y\alpha$  for some non-zero  $\alpha \in L$ .

(20.6) THEOREM. *The number of classes of  $L_0$ -ideals is finite. (In the special case where  $L$  is an algebraic number field and  $L_0$  the ring of all algebraic integers in  $L$ , this shows that the class number of  $L$  is finite.)*

PROOF. Since  $L_0$  has a  $Z$ -basis of  $n$  elements, we may choose  $u_1, \dots, u_n \in L_0$  such that

$$(20.7) \quad L_0 = Zu_1 \oplus \cdots \oplus Zu_n .$$

For any  $u \in L_0$ , we have

$$(20.8) \quad u_i u = \sum_{j=1}^n \rho_{ij}(u) u_j , \quad \rho_{ij}(u) \in Z .$$

Let  $R(u) = (\rho_{ij}(u))$ ; we find at once that  $R(uv) = R(u)R(v)$ ,  $u, v \in L_0$ . Now define the *norm of  $u$*  as<sup>†</sup>

$$N(u) = \det R(u).$$

[When  $L$  is an algebraic number field, this norm coincides with the usual norm  $N_{L/\mathbb{Q}}$ ; see § 20B at the end of this section.] Then  $N(uv) = N(u)N(v)$ , and

$$N(\alpha_1 u_1 + \cdots + \alpha_n u_n) = \det (\alpha_1 R(u_1) + \cdots + \alpha_n R(u_n)), \quad \alpha_i \in \mathbb{Z}.$$

On the other hand, let  $X$  be an  $L_0$ -ideal contained in  $L_0$ , and define

$$N(X) = [L_0 : X],$$

the number of residue classes of  $L_0$  modulo the additive subgroup  $X$ . Since there exists a positive integer  $q$  such that  $qL_0 \subset X$ , we have

$$[L_0 : X] \leq [L_0 : qL_0] = q^n,$$

the latter equality holding because  $(L_0 : \mathbb{Z}) = n$ . Thus  $N(X)$  is always finite.

To complete the proof of Theorem 20.6, we shall need several lemmas.

(20.9) LEMMA. *For  $u \in L_0$  we have  $N(L_0 u) = |N(u)|$ .*

PROOF. From (20.7) and (20.8), we have

$$L_0 = Z u_1 \oplus \cdots \oplus Z u_n, \quad L_0 u = Z v_1 \oplus \cdots \oplus Z v_n$$

where

$$\begin{bmatrix} v_1 \\ \vdots \\ v_n \end{bmatrix} = R(u) \begin{bmatrix} u_1 \\ \vdots \\ u_n \end{bmatrix}.$$

If  $P$  and  $F$  are unimodular matrices over  $\mathbb{Z}$ , then, setting

$$\begin{bmatrix} \bar{u}_1 \\ \vdots \\ \bar{u}_n \end{bmatrix} = P^{-1} \begin{bmatrix} u_1 \\ \vdots \\ u_n \end{bmatrix}, \quad \begin{bmatrix} \bar{v}_1 \\ \vdots \\ \bar{v}_n \end{bmatrix} = F \begin{bmatrix} v_1 \\ \vdots \\ v_n \end{bmatrix},$$

we have

---

<sup>†</sup> In this section we write  $\det A$  instead of  $|A|$  for the determinant of a matrix and  $|x|$  for the absolute value of the rational number  $x$ .

$$L_0 = Z\bar{u}_1 + \cdots + Z\bar{u}_n, \quad L_0 u = Z\bar{v}_1 + \cdots + Z\bar{v}_n,$$

and

$$\begin{bmatrix} \bar{v}_1 \\ \vdots \\ \bar{v}_n \end{bmatrix} = \mathbf{F}\mathbf{R}(u)\mathbf{P} \begin{bmatrix} \bar{u}_1 \\ \vdots \\ \bar{u}_n \end{bmatrix}.$$

By Theorem 16.6, we may choose  $\mathbf{F}$  and  $\mathbf{P}$  so that  $\mathbf{F}\mathbf{R}(u)\mathbf{P} = \text{diag}\{m_1, \dots, m_n\}$ ,  $m_i \in \mathbb{Z}$ . Then  $|\prod_i m_i| = |\det \mathbf{R}(u)| = |N(u)|$  and  $\bar{v}_i = m_i \bar{u}_i$ . Therefore

$$L_0 = Z\bar{u}_1 \oplus \cdots \oplus Z\bar{u}_n, \quad L_0 u = Zm_1\bar{u}_1 \oplus \cdots \oplus Zm_n\bar{u}_n,$$

and so  $L_0/L_0 u \cong Z/Zm_1 + \cdots + Z/Zm_n$  (as  $\mathbb{Z}$ -modules). Since  $[Z: Zm_i] = |m_i|$ , this shows that

$$N(L_0 u) = (L_0 : L_0 u) = \prod_i |m_i| = |N(u)|.$$

(20.10) **LEMMA.** *There exists a real positive constant  $c$  (depending on  $L$  and  $L_0$ ) such that for each  $L_0$ -ideal  $X$  in  $L_0$ , there exists a non-zero  $x \in X$  for which*

$$(20.11) \quad |N(x)| \leq c \cdot N(X).$$

**PROOF.** Let  $\xi_1, \dots, \xi_n$  denote real variables. Then

$$\det(\xi_1 \mathbf{R}(u_1) + \cdots + \xi_n \mathbf{R}(u_n)) = F(\xi_1, \dots, \xi_n)$$

is a homogeneous polynomial of degree  $n$  in the variables  $\xi_1, \dots, \xi_n$ . Hence there exists a positive real constant  $c$  that depends on the matrices  $\{\mathbf{R}(u_i)\}$  such that

$$|F(\xi_1, \dots, \xi_n)| \leq c \cdot a^n \quad \text{for } |\xi_1| \leq a, \dots, |\xi_n| \leq a.$$

We shall show that this  $c$  is the desired constant.

Let  $X$  be an  $L_0$ -ideal contained in  $L_0$ . The set of elements

$$\{b_1 u_1 + \cdots + b_n u_n, b_i \in \mathbb{Z}, 0 \leq b_i \leq \{N(X)\}^{1/n}\}$$

is a set of more than  $N(X)$  distinct elements of  $L_0$ ; hence two of them must be congruent mod  $X$ . Their difference is a non-zero element  $x \in X$  such that

$$x = a_1 u_1 + \cdots + a_n u_n, \quad a_i \in \mathbb{Z}, |a_i| \leq \{N(X)\}^{1/n}.$$

Then

$$\begin{aligned}|N(x)| &= |\det(a_1R(u_1) + \cdots + a_nR(u_n))| \\&= |F(a_1, \dots, a_n)| \leq c \cdot N(X),\end{aligned}$$

and Lemma 20.10 is proved.

(20.12) LEMMA. *Corresponding to each  $L_0$ -ideal  $X$ , there exists an  $L_0$ -ideal  $X'$  in the same class as  $X$  such that  $X' \supset L_0$  and  $[X':L_0] \leq c$ .*

PROOF. For  $m \in \mathbb{Z}$ ,  $m \neq 0$ , we observe that  $X$  and  $mX$  are in the same class. Because  $X$  has finite  $\mathbb{Z}$ -rank, we may choose  $m$  so that  $mX \subset L_0$ . For the remainder of the proof we may therefore assume that  $X$  is an  $L_0$ -ideal in  $L_0$ . Using Lemma 20.10, we may find a non-zero  $x \in X$  such that  $|N(x)| \leq cN(X)$ . Setting  $X' = Xx^{-1}$ , we see that  $X'$  is an  $L_0$ -ideal in the same class as  $X$ . Further  $x \in X$  implies  $L_0x \subset X$ , or  $L_0 \subset Xx^{-1}$ . Finally, by (20.9) we have

$$\begin{aligned}[X':L_0] &= [Xx^{-1}:L_0] = [X:L_0x] \\&= [L_0:L_0x]/[L_0:X] = |N(x)|/N(X) \leq c.\end{aligned}$$

[The second equality holds because if  $y_1, y_2 \in X$ , then  $y_1x^{-1} \equiv y_2x^{-1} \pmod{L_0}$  if and only if  $y_1 \equiv y_2 \pmod{L_0x}$ .]

We are now ready to complete the proof of Theorem 20.6. We have shown the existence of a positive constant  $c$  (which depends on  $L$  and  $L_0$ ) such that every ideal class contains an ideal  $X'$  for which  $X' \supset L_0$  and  $[X':L_0] \leq c$ . If we show that there are only a finite number of  $L_0$ -ideals  $X'$  which contain  $L_0$  and for which  $[X':L_0] \leq c$ , the theorem will be proved. We see that  $[X':L_0]$  can assume only a finite number of values, namely, those positive integers which are less than or equal to  $c$ . Let  $m$  be such a positive integer, and suppose  $[X':L_0] = m$ . Then

$$mL_0 \subset mX' \subset L_0,$$

so  $mX'$  is a subgroup of  $L_0$  which contains  $mL_0$ . The subgroups of  $L_0$  which contain  $mL_0$  are in one-to-one correspondence with the subgroups of  $L_0/mL_0$ . However,  $[L_0:mL_0] = m^n$ , and therefore there are only a finite number of possible groups  $mX'$ . Each  $mX'$  determines  $X'$  uniquely since all modules are  $\mathbb{Z}$ -torsion-free. Thus there are only finitely many possibilities for  $X'$ . This completes the proof of (20.6).

For our later discussion, we shall require some additional results from algebraic number theory, which we collect in three addenda to this section.

**§ 20A. A further result on ideal classes**

Let  $R$  be the ring of all algebraic integers in an algebraic number field  $K$ , and let  $R'$  be the ring of all algebraic integers in a finite extension  $K'$  of  $K$ . Every  $R$ -ideal  $A$  in  $K$  determines an  $R'$ -ideal  $A'$  in  $K'$  defined by

$$A' = \{ \sum \xi_i a_i : \xi_i \in R', a_i \in A \}.$$

Thus  $A'$  consists of all  $R'$ -linear combinations of the elements of  $A$ ; we shall therefore write  $A' = R'A$ . It is easily verified that  $A'$  is indeed an  $R'$ -ideal in  $K'$ .

If  $A$  is a principal ideal, so is  $A'$ . For if  $A = aR$ ,  $a \in K$ , then  $A' = AR' = aR'$ . However, it may happen that  $A'$  is principal even though  $A$  is not. Furthermore, if  $A, B$  are  $R$ -ideals in  $K$ , then

$$(A + B)' = A' + B' , \quad (AB)' = A'B' .$$

(20.13) **LEMMA.** *For each  $R$ -ideal  $A$  in  $K$  we have  $R'A \cap K = A$ . Consequently, distinct ideals in  $K$  induce distinct ideals in  $K'$ .*

**PROOF.** Suppose that there are  $N$  isomorphisms of  $K'$  into extensions of  $K$  which leave each element of  $K$  fixed, and let the images of an element  $\xi \in K'$  under these isomorphisms be denoted by  $\xi^{(1)}, \dots, \xi^{(N)}$  (where  $\xi^{(1)} = \xi$ ). Of course  $N$  is finite. Now let  $b \in R'A \cap K$ ; we may write

$$b = \xi_1 a_1 + \cdots + \xi_n a_n , \quad \xi_i \in R' , a_i \in A ,$$

and so

$$b = b^{(j)} = \xi_1^{(j)} a_1 + \cdots + \xi_n^{(j)} a_n , \quad 1 \leq j \leq N .$$

Therefore

$$b^N = \prod_{j=1}^N (\xi_1^{(j)} a_1 + \cdots + \xi_n^{(j)} a_n) .$$

After the multiplications on the right-hand side have been performed, the coefficient of any term  $a_{i_1} \cdots a_{i_N}$  is unchanged by all the  $K$ -isomorphisms of  $K'$  and hence lies in  $K$ . On the other hand, each such coefficient is a polynomial with rational integral coefficients in the  $\{\xi_i^{(j)}\}$ , hence is an algebraic integer. Therefore, each such coefficient lies in  $R$ , which shows that  $b^N \in A^N$ . Therefore  $A^N \supset b^N R$ , whence  $A \supset bR$ , and so  $b \in A$ . This completes the proof.

We are now ready to prove the main result of § 20A.

(20.14) **THEOREM.** *Let  $h$  be the class number of  $R$ . Then there*

exists an extension field  $K'$  of  $K$  such that  $(K':K) \leq h$  and such that all  $R'$ -ideals of  $K'$  which are induced by  $R$ -ideals of  $K$  are principal; that is, for every  $R$ -ideal  $A$  in  $K$ , there exists an element  $\alpha \in K'$  such that  $R'A = R'\alpha$ .

**PROOF.** The classes of ideals in  $K$  form an abelian multiplicative group of order  $h$ . We may write this group as a direct product of cyclic subgroups  $S_1, \dots, S_r$ , say, where  $S_i$  is of order  $n_i$ . For each  $i$ ,  $1 \leq i \leq r$ , we may choose an  $R$ -ideal  $A_i$  in  $K$  whose ideal class generates  $S_i$ . Then  $h = n_1 \cdots n_r$ , and every non-zero  $R$ -ideal  $A$  in  $K$  is expressible as

$$(20.15) \quad A = b \cdot A_1^{m_1} \cdots A_r^{m_r}, \quad 0 \leq m_i \leq n_i - 1, b \in K.$$

Now we have  $A_i^{n_i} = a_i R$ ,  $a_i \in K$ ,  $i = 1, \dots, r$ . For each  $i$ , adjoin to  $K$  one value of  $\sqrt[n_i]{a_i}$ , say  $\alpha_i$ , and let  $K' = K(\alpha_1, \dots, \alpha_r)$ . Clearly  $(K':K) \leq n_1 \cdots n_r = h$ . Furthermore, we have  $A_i^{n_i} = \alpha_i^{n_i} R$ , so

$$(A_i R')^{n_i} = (\alpha_i R')^{n_i},$$

whence  $A_i R' = \alpha_i R'$ ,  $1 \leq i \leq r$ . Using (20.15) we then obtain

$$AR' = b\alpha_1^{m_1} \cdots \alpha_r^{m_r} R',$$

which proves the result.

### § 20B. On the norm of an algebraic number

In the proof of Theorem 20.6, we defined the norm of an algebraic number as follows: Let  $K$  be an algebraic number field with  $(K:Q) = n$ , and let

$$K = Qu_1 \oplus \cdots \oplus Qu_n$$

where  $\{u_1, \dots, u_n\}$  forms a  $Z$ -basis for the ring  $R = \text{alg. int. } \{K\}$ . Let  $u \in K$ ; for each  $i$ ,  $1 \leq i \leq n$ , there exist  $\rho_{ij}(u) \in Q$  such that

$$u_i u = \sum_{j=1}^r \rho_{ij}(u) u_j.$$

Letting  $R(u)$  be the matrix  $\{\rho_{ij}(u)\}$ , we defined the *norm* of  $u$  by

$$N(u) = \det R(u)$$

and proved that  $N(uv) = N(u)N(v)$ . Since  $N(1) = 1$ , it follows that  $u \neq 0$  implies  $N(u) \neq 0$ . Further, if  $u \in R$ , each  $\rho_{ij}(u) \in Z$ , and hence  $N(u) \in Z$ . Thus the norm of a non-zero algebraic integer is a non-zero rational integer. We may further remark that  $N(u)$  is independent of the choice of  $Z$ -basis of  $R$ . Indeed, had we used in place of

$\{u_1, \dots, u_n\}$  any  $Q$ -basis of  $K$ , the matrix  $R(u)$  would have been replaced by  $T^{-1}R(u)T$  for some  $T$ , and we have  $\det T^{-1}R(u)T = \det R(u)$ .

It is the purpose of §20B to show that  $N(u)$  may be expressed as a product of conjugates of  $u$ . Choose  $\alpha \in K$  such that  $K = Q(\alpha)$ , where  $\text{Irr}(\alpha, Q)$  has degree  $n$ . Then any  $u \in K$  is uniquely expressible as

$$u = \sum_{j=0}^{n-1} b_j \alpha^j, \quad b_j \in Q.$$

Let  $L$  be the splitting field of  $\text{Irr}(\alpha, Q)$  over  $Q$ , and let  $\alpha_1 (= \alpha), \alpha_2, \dots, \alpha_n$  be the zeros of  $\text{Irr}(\alpha, Q)$  in  $L$ . The map  $\alpha \rightarrow \alpha_i$  induces a  $Q$ -isomorphism of  $K$  onto  $Q(\alpha_i)$ . These  $n$  maps  $\alpha \rightarrow \alpha_i$  ( $1 \leq i \leq n$ ) give all possible isomorphisms of  $K$  onto subfields of  $L$ . Set

$$u_i = \sum_{j=0}^{n-1} b_j (\alpha_i)^j, \quad 1 \leq i \leq n,$$

and call  $u_1, \dots, u_n$  the *conjugates* of  $u$  (in  $L$ ). Obviously,  $\text{Irr}(u, Q) = \text{Irr}(u_i, Q)$  for each  $i$ .

We now prove that

$$N(u) = u_1 \cdots u_n.$$

Let  $X$  denote an indeterminate over  $Q$ , and set

$$\text{Irr}(u, Q) = f(X) = X^m + c_1 X^{m-1} + \cdots + c_m.$$

Since  $Q(u)$  is a subfield of  $Q(\alpha)$ , we may write  $n = mr$  for some  $r \in \mathbb{Z}$ . We then have

$$\prod_{i=1}^n (X - u_i) = \{f(X)\}^r,$$

since the left-hand side is unchanged by all isomorphisms  $\alpha \rightarrow \alpha_i$  and hence lies in  $Q[X]$ . Therefore

$$(-1)^n u_1 \cdots u_n = c_m^r,$$

and so we need show only that  $N(u) = (-1)^n c_m^r$ .

Now we have

$$(K: Q(u)) = r, \quad (Q(u): Q) = m.$$

Let  $\{\xi_1, \dots, \xi_r\}$  be a  $Q(u)$ -basis for  $K$ . Then

$$\{\xi_i u^j : 1 \leq i \leq r, 0 \leq j \leq m-1\}$$

is a  $Q$ -basis for  $K$ . Let us compute  $N(u)$  by using this basis. We note that

$$\begin{aligned} (\xi_i u^j)u &= \xi_i u^{j+1}, & 1 \leq i \leq r, 0 \leq j \leq m-2, \\ (\xi_i u^{m-1})u &= \xi_i (-c_1 u^{m-1} - \cdots - c_m), & 1 \leq i \leq r. \end{aligned}$$

Therefore

$$\begin{aligned} N(u) &= \begin{vmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \cdot & \cdot & \cdot & \cdots & \cdot \\ -c_m & -c_{m-1} & -c_{m-2} & \cdots & -c_1 \end{vmatrix}^r \\ &= \{(-1)^m c_m\}^r = (-1)^n c_m^r, \end{aligned}$$

which establishes the formula  $N(u) = u_1 \cdots u_n$ .

### § 20C. Extensions of ideals

Let  $K \subset K'$  be any pair of algebraic number fields which are normal over  $Q$ , and set  $R = \text{alg. int. } \{K\}$ ,  $R' = \text{alg. int. } \{K'\}$ . If  $A$  is any non-zero ideal in  $R$ , we have seen in Theorem 20.4 that

$$N(A)R = \prod_{\sigma \in G} A^\sigma$$

where  $G$  is the Galois group of  $K$  over  $Q$ . We now consider the ideal  $AR'$  of  $R'$ ; its conjugates over  $Q$  are precisely

$$\{A^\sigma R' : \sigma \in G\},$$

each occurring with multiplicity  $m = (K':K)$ . Therefore

$$N(AR') \cdot R' = \left\{ \prod_{\sigma \in G} A^\sigma R' \right\}^m = N(A)^m \cdot R',$$

which implies that

$$(20.16) \quad N(AR') = \{N(A)\}^m.$$

(As we shall see in Exercise 22.7, this result holds even without the hypothesis that  $K$  and  $K'$  are normal over  $Q$ .)

Now let  $P$  be any prime ideal of  $R$ , and let

$$(20.17) \quad PR' = \prod_{i=1}^t P_i'^{e_i}$$

be the factorization of  $PR'$  into powers of distinct prime ideals  $\{P_i'\}$  of  $R'$ . For each  $i$ , we have  $P \subset P_i'$ , and so we may embed the residue class field  $R/P$  in the residue class field  $R'/P_i'$ . Define

$$f_i = (R'/P_i' : R/P).$$

Since  $R/P$  has  $N(P)$  elements, it follows at once that  $R'/P'_i$  has  $N(P)^{f_i}$  elements; that is,

$$N(P'_i) = \{N(P)\}^{f_i}, \quad 1 \leq i \leq t.$$

Taking norms in (20.17) and using (20.16), we obtain

$$\begin{aligned} N(P)^m &= N(PR') = \prod_i N(P'_i)^{e_i} \\ &= N(P)^{\sum e_i f_i}. \end{aligned}$$

This yields the important equality

$$(20.18) \quad \sum_{i=1}^t e_i f_i = (K': K).$$

A simple consequence of this fact, which we shall need in the following section, is

(20.19) *Let  $\alpha \in R$  be such that  $\nu_P(\alpha) = 1$ , and suppose that*

$$\alpha = \beta^s \gamma, \quad \beta, \gamma \in R',$$

*where  $\gamma$  is a unit in  $R'$ . Then  $(K': K) \geq s$ .*

PROOF. From  $\nu_P(\alpha) = 1$  we conclude [using the notation of (20.17)] that

$$\nu_{P'_1}(\alpha) = e_1.$$

But

$$\nu_{P'_1}(\alpha) = s \cdot \nu_{P'_1}(\beta),$$

and thus

$$s \leq e_1 \leq (K': K).$$

This completes the proof.

### Exercises

1. Which ideals have norm 1?
2. Prove that an ideal whose norm is prime is a prime ideal. Is the converse true?
3. Let  $K = Q(i)$ ,  $R = \mathbb{Z} \oplus \mathbb{Z}i$ . Show that  $R$  is the ring of all algebraic integers in  $K$ . Prove that  $R$  is a Euclidean ring and hence has class number 1. Find  $N(a + bi)$  for  $a, b \in \mathbb{Z}$ . Show that  $(1 + i)R$ ,  $(2 + i)R$ , and  $3R$  are prime ideals but  $(3 + i)R$  and  $(5 + i)R$  are not. What are the characteristics of the fields  $R/(1 + i)R$ ,  $R/(2 + i)R$ ,  $R/3R$ ?
4. Let  $R$  be the ring of algebraic integers in an algebraic number field  $K$ , and let  $\theta: K \rightarrow K_1$  be a  $Q$ -isomorphism of  $K$  onto  $K_1$ . Let  $\theta(R) = R_1$ . Show

that  $R_1$  is the ring of all algebraic integers in  $K_1$ . Prove that  $\theta$  carries prime ideals into prime ideals and preserves sums, products, and norms of ideals.

5. Let  $K$  be a normal extension of  $Q$ ,  $(K:Q) = h$ . For each  $\alpha \in K$ , let  $\bar{\alpha}$  denote the complex conjugate of  $\alpha$ , and set  $R = \text{alg. int. } \{K\}$ . For  $\alpha \in K$ , let  $\alpha_1 (= \alpha), \alpha_2, \dots, \alpha_h$  be its conjugates over  $Q$ . Prove that if  $\alpha \in R$ ,  $\alpha \neq 0$ , then

$$\sum_{i=1}^h \alpha_i \bar{\alpha}_i \geq h.$$

[Hint: If  $\alpha \neq 0$ ,  $\alpha \in R$ , then  $|N(\alpha)| = |\alpha_1 \cdots \alpha_h| \geq 1$ . In addition,  $|\bar{\alpha}_1 \cdots \bar{\alpha}_h| \geq 1$ , so that

$$1 \leq \prod_{i=1}^h (\alpha_i \bar{\alpha}_i),$$

But  $\alpha_1 \bar{\alpha}_1, \dots, \alpha_h \bar{\alpha}_h$  are a set of positive real numbers, and so their geometric mean is less than or equal to their arithmetic mean:

$$\left\{ \prod_{i=1}^h \alpha_i \bar{\alpha}_i \right\}^{1/h} \leq \left( \sum_{i=1}^h \alpha_i \bar{\alpha}_i \right) / h.$$

Combining this with the previous inequality, the desired result follows at once. (A special case of this theorem is due to Burnside [1]: this simple proof was furnished us by P. T. Bateman.)

## § 21. Cyclotomic Fields

Let  $K$  be a field of characteristic  $p$  where  $p \geq 0$ , and let  $X$  denote an indeterminate over  $K$ . The splitting field of the polynomial  $X^n - 1$  over  $K$  is then uniquely determined (up to  $K$ -isomorphism). We call this splitting field the *cyclotomic field of order n over K* and denote it by  $K(\sqrt[n]{1})$ . Since  $K(\sqrt[n]{1})$  is obtained from  $K$  by adjoining all roots of  $X^n - 1$ , it is clearly a normal finite algebraic extension of  $K$ . Our ultimate objective is to determine explicitly the algebraic integers in  $K(\sqrt[n]{1})$ .

Suppose for the moment that  $p \neq 0$ , and write  $n = p^a m$  where  $p \nmid m$ . Then we have

$$X^n - 1 = (X^m - 1)^{p^a},$$

which shows that

$$K(\sqrt[n]{1}) = K(\sqrt[m]{1}).$$

Hence, in our discussion of cyclotomic fields of order  $n$ , we may

restrict our attention to the case where  $p \nmid n$ .

Now let  $L = K(\sqrt[n]{1})$  where  $p \nmid n$  (if  $p \neq 0$ ). Then  $X^n - 1$  has no multiple zeros in any extension field of  $K$ , and so  $L$  contains precisely  $n$  distinct  $n$ th roots of 1, say,  $\omega_1, \dots, \omega_n$ . We then have

$$X^n - 1 = \prod_{i=1}^n (X - \omega_i).$$

Call  $\omega \in L$  a *primitive nth root of 1* if  $\omega^n = 1$  but  $\omega^k \neq 1$  for  $0 < k < n$ . The geometrical representation of roots of unity shows the existence of primitive  $n$ th roots of 1 when  $K$  is the field of rational numbers. The proof of their existence in the general case, however, is more complicated and depends on some number-theoretic results which we shall derive.

We begin by defining the Möbius  $\mu$ -function on the positive rational integers. Let  $p_1, \dots, p_r$  denote primes, and set

$$\mu(1) = 1, \mu(p_1 \cdots p_r) = \begin{cases} (-1)^r & \text{if the } \{p_i\} \text{ are distinct primes,} \\ 0, & \text{otherwise.} \end{cases}$$

It is easily verified (Exercise 1) that  $\mu(ab) = \mu(a)\mu(b)$  if  $(a, b) = 1$ , and

$$(21.1) \quad \sum_{d|n} \mu(d) = \begin{cases} 1, & n = 1 \\ 0, & n > 1. \end{cases}$$

Starting with a function  $f$ , we define its “Möbius transform”  $g$  by

$$(21.2) \quad g(n) = \sum_{d|n} \mu\left(\frac{n}{d}\right) f(d) = \sum_{d|n} \mu(d) f\left(\frac{n}{d}\right).$$

Then we have

$$\sum_{n|t} g(n) = \sum_{n|t} \sum_{d|n} \mu\left(\frac{n}{d}\right) f(d) = \sum_{d|t} \left\{ \sum_{n|d} \mu\left(\frac{n}{d}\right) \right\} f(d),$$

where, in the sum in braces,  $n$  ranges over all divisors of  $d$  which are multiples of  $t$ . In that case,  $n/d$  ranges over all divisors of  $t/d$  so that, by (21.1), the sum in braces vanishes except when  $d = t$ , in which case it is 1. Therefore we have shown that

$$(21.3) \quad f(t) = \sum_{n|t} g(n).$$

Formulas (21.2) and (21.3) are the Möbius inversion formulas. The latter formula expresses  $f$  in terms of its Möbius transform. Conversely, from (21.3), it is easy to deduce that  $g$  is given by (21.2).

In particular, let  $\varphi$  be the Euler function. Then, by definition,  $\varphi(n)$  is the number of positive integers less than or equal to  $n$  which are relatively prime to  $n$ . Using the fact that  $\varphi(ab) = \varphi(a)\varphi(b)$  when  $(a, b) = 1$ , which is a consequence of (18.18), one obtains the well-known formula

$$\begin{aligned}\varphi(n) &= n \prod_{p|n} \left(1 - \frac{1}{p}\right) = n \sum_{d|n} \frac{\mu(d)}{d} \\ &= \sum_{d|n} \mu(d) \cdot \frac{n}{d}\end{aligned}$$

where the first product is taken over the distinct primes dividing  $n$ . Thus,  $\varphi$  is the Möbius transform of the identity function. Formula (21.3) then yields

$$(21.4) \quad t = \sum_{n|t} \varphi(n).$$

(21.5) **THEOREM.** *Let  $L = K(\sqrt[d]{1})$  where  $\text{char}(K) \nmid n$ . Then  $L$  contains precisely  $\varphi(n)$  primitive  $n$ th roots of 1.*

**PROOF.** The result is trivial for  $n = 1$ . Let  $n > 1$ , and suppose the result holds for  $K(\sqrt[d]{1})$  where  $d$  is any proper divisor of  $n$ . Each  $n$ th root of 1 in  $L$  is a primitive  $d$ th root of 1 for some divisor  $d$  of  $n$ . Of the  $n$   $n$ th roots, only those are primitive  $n$ th roots which are not primitive  $d$ th roots for some proper divisor  $d$  of  $n$ . Hence, using the induction hypothesis,  $L$  contains

$$n - \sum_{\substack{d|n \\ d \neq n}} \varphi(d)$$

primitive  $n$ th roots of 1. By (21.4), this number is exactly  $\varphi(n)$ , and Theorem 21.5 is proved.

Let us define the *cyclotomic polynomial of order  $d$*  as

$$\Phi_d(X) = \prod_{\omega} (X - \omega)$$

where  $\omega$  ranges over all primitive  $d$ th roots of 1 in  $K(\sqrt[d]{1})$ . By the above reasoning, we see that  $\Phi_d(X)$  is of degree  $\varphi(d)$  and that

$$X^n - 1 = \prod_{d|n} \Phi_d(X).$$

From the Möbius inversion formula (written multiplicatively), we then have

$$(21.6) \quad \Phi_n(X) = \prod_{d|n} (X^d - 1)^{\mu(n/d)}.$$

Hence each  $\Phi_n(X)$  can be calculated by working in the ring  $K[X]$ . The polynomials  $\Phi_n(X)$  need not be irreducible in  $K[X]$ . For example, let  $K$  be the finite field with seven elements. Then, by formula (21.6), we obtain

$$\begin{aligned}\Phi_3(X) &= (X - 1)^{\mu(3)}(X^3 - 1)^{\mu(1)} \\ &= X^2 + X + 1 = (X - 2)(X + 3).\end{aligned}$$

If  $\omega$  denotes a specific primitive  $n$ th root of 1 over  $K$ , then  $\omega, \omega^2, \dots, \omega^n$  are all the  $n$ th roots in  $K(\sqrt[n]{1})$ , and so we have

$$X^n - 1 = \prod_{k=1}^n (X - \omega^k).$$

Furthermore,  $\omega^k$  is a primitive  $n$ th root of 1 if and only if  $(k, n) = 1$ . Hence, as  $k$  ranges over all positive integers less than or equal to  $n$  and relatively prime to  $n$ ,  $\omega^k$  ranges over all primitive  $n$ th roots of 1. Thus

$$\Phi_n(X) = \prod_{\substack{1 \leq k \leq n \\ (k, n) = 1}} (X - \omega^k).$$

This shows that

$$K(\sqrt[n]{1}) = K(\omega), \quad (K(\sqrt[n]{1}): K) \leq \varphi(n).$$

We are now going to restrict ourselves to algebraic number fields and shall begin with a calculation involving the cyclotomic polynomial

$$\Phi_{p^n}(X), \quad p \text{ prime, } n > 0.$$

Set  $M = \varphi(p^n)$ , and let  $\zeta_1, \dots, \zeta_M$  be the primitive  $p^n$ th roots of 1 over  $Q$ . By the above we have

$$(21.7) \quad \Phi_{p^n}(X) = \prod_{i=1}^M (X - \zeta_i).$$

But by (21.6)

$$(21.8) \quad \Phi_{p^n}(X) = (X^{p^n} - 1)/(X^{p^n-1} - 1)$$

$$(21.9) \quad = \sum_{r=0}^{p-1} X^{r \cdot p^{n-1}},$$

so that (setting  $X = 1$ )

$$(21.10) \quad p = \prod_{i=1}^M (1 - \zeta_i).$$

To simplify the notation, set  $\zeta_1 = \zeta$ , a fixed primitive  $p^n$ th root of 1 over  $Q$ , and let  $i$  be any index between 1 and  $M$ . On the one hand,  $\zeta_i$  is a power of  $\zeta$  so that

$$(1 - \zeta_i)/(1 - \zeta) \in Z[\zeta],$$

whereas, on the other hand,  $\zeta$  is a power of  $\zeta_i$  so that

$$(1 - \zeta)/(1 - \zeta_i) \in Z[\zeta_i] = Z[\zeta].$$

Thus

$$1 - \zeta_i = \epsilon_i(1 - \zeta), \quad 1 \leq i \leq M,$$

where each  $\epsilon_i$  is a unit in  $Z[\zeta]$ . Substitution in (21.10) then yields

$$(21.11) \quad p = (1 - \zeta)^M \cdot (\text{unit in } Z[\zeta]).$$

We shall use this result presently.

Next we deduce from (21.8) that, for  $1 \leq i \leq M$ ,<sup>t</sup>

$$\prod_{j \neq i} (\zeta_i - \zeta_j) = \phi'_{p^n}(\zeta_i) = p^n \zeta_i^{-1} / (\zeta_i^{p^n-1} - 1).$$

Consequently,

$$\begin{aligned} \pm \prod_{1 \leq i < j \leq M} (\zeta_i - \zeta_j)^2 &= \prod_{i=1}^M \phi'_{p^n}(\zeta_i) \\ &= p^{nM} \prod_{i=1}^M \zeta_i^{-1} / (\zeta_i^{p^n-1} - 1). \end{aligned}$$

Now (Exercise 21.5)

$$\prod_{i=1}^M \zeta_i = \pm 1.$$

Furthermore, as  $\zeta_i$  ranges over the  $p^{n-1}(p-1)$  primitive  $p^n$ th roots of 1, the expression

$$\zeta_i^{p^n-1}$$

ranges over the primitive  $p$ th roots of 1, say  $\lambda_1, \dots, \lambda_{p-1}$ , each  $\lambda_k$  occurring  $p^{n-1}$  times. Therefore,

$$\prod_{i=1}^M (\zeta_i^{p^n-1} - 1) = \left\{ \prod_{k=1}^{p-1} (\lambda_k - 1) \right\}^{p^{n-1}}.$$

We have, however, from (21.10) (with  $n = 1$ )

$$p = \pm \prod_{k=1}^{p-1} (\lambda_k - 1),$$

---

<sup>t</sup> We use  $\phi'$  to denote the derivative of  $\phi$ .

which proves that

$$(21.12) \quad \prod_{1 \leq i < j \leq M} (\zeta_i - \zeta_j)^2 = \pm p^{nM-p^{n-1}}.$$

We shall use this result in establishing the main theorem of this section.

(21.13) **THEOREM.** *For each  $N$ , the cyclotomic polynomial  $\Phi_N(X)$  is irreducible over  $Q$ . If  $\theta$  is a primitive  $N$ th root of 1 over  $Q$ , then  $(Q(\theta): Q) = \varphi(N)$ , and  $Z[\theta] = \text{alg. int. } \{Q(\theta)\}$ .*

**PROOF.** Use induction on the number of distinct prime divisors of  $N$ , remarking first that the result is trivial when  $N = 1$ . Suppose next that  $N = p^n$ ,  $p$  prime,  $n > 0$ , and let  $\zeta$  be a primitive  $p^n$ th root of 1 over  $Q$ . Then  $Q(\zeta)$  is normal over  $Q$ , and

$$(Q(\zeta): Q) \leqq M = \varphi(p^n).$$

But (21.11) states that

$$p = (1 - \zeta)^M \cdot \text{unit in } Z[\zeta],$$

so that by (20.19) we have

$$M \leqq (Q(\zeta): Q).$$

Together these show that  $(Q(\zeta): Q) = M$  and thus that  $\Phi_{p^n}(X)$  is irreducible over  $Q$ . [The irreducibility of  $\Phi_p(X)$  is an easy consequence of the Eisenstein criterion; the difficulty comes in the case  $n > 1$ .]

Now let  $R = \text{alg. int. } \{Q(\zeta)\}$ . By (17.11) we conclude that

$$\left\{ \prod_{1 \leq i < j \leq M} (\zeta_i - \zeta_j)^2 \right\} \cdot R \subset Z[\zeta],$$

and so, if we set  $b = nM - p^{n-1}$  and use (21.12), we obtain

$$(21.14) \quad p^b R \subset Z[\zeta].$$

We are trying to show that indeed  $R = Z[\zeta]$ . From (21.11), we may write

$$pR = \{(1 - \zeta)R\}^M$$

so that by taking norms we have

$$p^M = \{\text{norm } (1 - \zeta)R\}^M,$$

which shows that

$$\text{norm } (1 - \zeta)R = p.$$

Therefore  $(1 - \zeta)R$  is a prime ideal in  $R$ ; let  $\nu$  be the “additive valuation” associated with this prime ideal. Then the above implies at once that

$$\nu(1 - \zeta) = 1, \quad \nu(p) = M, \quad \nu(a) \equiv 0 \pmod{M} \quad \text{for all } a \in Z.$$

By (21.14) each  $\alpha \in R$  may be expressed as

$$\alpha = p^{-b} \sum_{j=0}^{M-1} y_j \zeta^j, \quad y_j \in Z,$$

and thus also as

$$\alpha = p^{-b} \sum_{j=0}^{M-1} x_j (1 - \zeta)^j, \quad x_j \in Z.$$

Therefore

$$-p^b \alpha + \sum_{j=0}^{M-1} x_j (1 - \zeta)^j = 0.$$

However, we observe that

$$\nu(x_j (1 - \zeta)^j) = j + \nu(x_j) \equiv j \pmod{M},$$

and so the values

$$\{\nu(x_j (1 - \zeta)^j) : 0 \leq j \leq M-1\}$$

are all distinct. It follows at once from Exercise 19.8 that there exists an index  $j_0$  such that

$$\nu(p^b \alpha) = \nu(x_{j_0} (1 - \zeta)^{j_0}) = \min_{0 \leq j \leq M-1} \nu(x_j (1 - \zeta)^j).$$

Therefore we have

$$Mb \leq \nu(p^b \alpha) \leq j + \nu(x_j), \quad 0 \leq j \leq M-1.$$

Since each  $\nu(x_j) \equiv 0 \pmod{M}$ , this implies at once that  $\nu(x_j) \geq Mb$  for each  $j$ , and hence each  $x_j$  is a multiple of  $p^b$ . Therefore  $\alpha \in Z[\zeta]$ , and so  $R = Z[\zeta]$ .

The theorem has thus been established for the case where  $N$  is a prime power. Now let us write

$$N = p^n t, \quad t > 1, p \nmid t,$$

and assume the result known for  $t$ . In other words, we assume that if  $\omega$  is a primitive  $t$ th root of 1 over  $Q$ , then

$$(Q(\omega): Q) = \varphi(t) = h \quad (\text{say}),$$

and

$$\text{alg. int. } \{Q(\omega)\} = Z[\omega] = R \quad (\text{say}) .$$

We shall show first that  $pR$  is not divisible by the square of any prime ideal in  $R$ . For any  $\alpha \in R$  we may write

$$\alpha = n_0 + n_1\omega + \cdots + n_{k-1}\omega^{k-1}, \quad n_i \in Z.$$

Therefore

$$\alpha^{p^k} \equiv n_0^{p^k} + n_1^{p^k}\omega^{p^k} + \cdots + n_{k-1}^{p^k}\omega^{(k-1)p^k} \pmod{pR} .$$

But by the Euler-Fermat theorem,

$$n^{p^k} \equiv n \pmod{p}, \quad n \in Z,$$

and  $p^k \equiv 1 \pmod{t}$ . Since  $\omega^t = 1$ , this latter congruence implies  $\omega^{p^k} = \omega$ , and thus

$$(21.15) \quad \alpha^{p^k} \equiv \alpha \pmod{pR} .$$

Now suppose there exists a prime ideal  $P$  in  $R$  such that  $P^2 \mid pR$ , and choose  $\alpha \in R$  so that  $\nu_P(\alpha) = 1$ . Then (21.15) implies

$$\nu_P(\alpha^{p^k} - \alpha) \geq 2 ,$$

and, since

$$\nu_P(\alpha^{p^k}) = p^k \geq 2 ,$$

we would have  $\nu_P(\alpha) \geq 2$ . This is impossible, and shows that  $pR$  is not divisible by the square of any prime ideal of  $R$ .

Let  $P$  be any prime ideal of  $R$  which divides  $pR$ ; we have just shown that  $\nu_P(p) = 1$ . Let  $\zeta$  denote a primitive  $p$ th root of 1 over  $Q$ , and set  $M = \varphi(p)$ . Then, on the one hand,

$$(Q(\omega)(\zeta): Q(\omega)) \leq M ,$$

although, on the other hand, using (21.11) and (20.19),

$$(Q(\omega)(\zeta): Q(\omega)) \geq M .$$

This shows that

$$(Q(\omega)(\zeta): Q(\omega)) = M ,$$

and thus

$$(Q(\omega)(\zeta): Q) = M \cdot h = \varphi(p^n)\varphi(t) = \varphi(N).$$

However,  $\theta = \omega\zeta$  is clearly a primitive  $N$ th root of 1, and  $Q(\omega)(\zeta) = Q(\theta)$ , so we have shown that  $(Q(\theta): Q) = \varphi(N)$ . This proves that  $\Phi_N(X)$  is irreducible over  $Q$ . The above also shows that  $\Phi_{p^n}(X)$  is irreducible over  $Q(\omega)$ .

Finally, let  $R' = \text{alg. int. } \{Q(\theta)\}$ . Each  $\alpha \in R'$  is expressible as

$$\alpha = \sum_{i=0}^{M-1} x_i \zeta^i, \quad x_i \in Q(\omega).$$

The argument which proved (17.11) then shows that

$$p^b R' \subset Z[\omega][\zeta] = Z[\theta]$$

where again  $b = nM - p^{n-1}$ . However, if  $q$  is any prime divisor of  $t$ , an analogous argument shows

$$q^c R' \subset Z[\theta]$$

for some positive integer  $c$ . Since  $p^b$  and  $q^c$  are relatively prime, we conclude that  $R' \subset Z[\theta]$ . Hence  $R' = Z[\theta]$ , and the theorem is proved.

### Exercises

- If  $\mu$  is the Möbius  $\mu$ -function, prove that  $\mu(ab) = \mu(a)\mu(b)$  if  $(a, b) = 1$ , and verify Formula (21.1).
- Show that formula (21.3) implies (21.2).
- If  $\theta_i$  is a primitive  $N_i$ th root of 1,  $1 \leq i \leq k$ , where  $\{N_1, \dots, N_k\}$  are pairwise relatively prime, show that  $\theta_1 \cdots \theta_k$  is a primitive  $(N_1 \cdots N_k)$ -th root of 1.
- Give an example of a field  $K$  of characteristic 0 such that  $\Phi_3(X)$  is reducible over  $K[X]$ .
- Compute the product of the primitive  $N$ th roots of 1.
- Let  $R = \text{alg. int. } \{K\}$ , and let  $\{\alpha_1, \dots, \alpha_n\}$  be a  $Z$ -basis of  $R$ . Let  $\{\alpha_i^{(j)} : j = 1, \dots, n\}$  denote the conjugates of  $\alpha_i$  in some normal extension of  $Q$  which contains  $K$ . Let  $D = \{\det(\alpha_i^{(j)})\}^2$ ; then  $D$  is the discriminant of the field  $K$ . Prove that the value of  $D$  is independent of the choice of  $Z$ -basis of  $R$ .
- Let  $N = p_1^{a_1} \cdots p_k^{a_k}$  be the factorization of  $N$  into powers of distinct primes, and let  $\theta_i$  be a primitive  $p_i^{a_i}$ th root of 1. As each exponent  $n_i$  ranges over the set of  $\varphi(p_i^{a_i})$  positive integers which are less than  $p_i^{a_i}$  and relatively prime to  $p_i$ , show that  $\theta_1^{n_1} \cdots \theta_k^{n_k}$  ranges over all  $\varphi(N)$  distinct primitive  $N$ th roots of 1.

8. Let  $\zeta_1, \dots, \zeta_t$  be roots of unity over  $Q$ . Prove that

$$|\zeta_1 + \cdots + \zeta_t| \leq t,$$

with equality if and only if  $\zeta_1 = \cdots = \zeta_t$ . Deduce from this that if

$$\omega = \zeta_1 + \cdots + \zeta_t$$

and if  $|\omega| < t$ , then also  $|\omega^*| < t$ , where  $\omega^*$  is any algebraic conjugate of  $\omega$  relative to  $Q$ .

9. Let  $K$  be a field of characteristic 0, and let  $\omega$  be a primitive  $n$ th root of 1 over  $K$ . Set  $G = \text{Galois group of } K(\omega) \text{ over } K$ . Prove that  $G$  is isomorphic to a subgroup of  $G(n)$ , where  $G(n)$  is the multiplicative group of the residue classes in  $Z/nZ$  which are relatively prime to  $n$ .

## § 22. Modules over Dedekind Domains

In this section,  $R$  denotes always a Dedekind domain. From § 18 we recall that  $R$  is an integral domain such that

- (i)  $R$  is noetherian (that is, the ideals of  $R$  satisfy the A.C.C.).
- (ii) Every prime ideal  $P \neq 0$  in  $R$  is maximal.

(iii)  $R$  is integrally closed in its quotient field  $K$  (that is, if  $r \in K$  and if  $R[r]$  is a finitely generated  $R$ -module, then  $r \in R$ ).

By an  $R$ -module we shall understand always a left  $R$ -module on which the identity element 1 of  $R$  acts as identity operator. We recall that an  $R$ -module  $M$  is *torsion-free* if  $\alpha m = 0$ ,  $\alpha \in R$ ,  $m \in M$  implies either  $\alpha = 0$  or  $m = 0$ .

We prove first that any torsion-free  $R$ -module  $M$  can be embedded in a vector space  $KM$  over the quotient field  $K$  of  $R$ . The space  $KM$  can be defined by exactly the same construction used to construct the quotient field of an integral domain, as follows: We consider the set  $S$  of all pairs  $(m, \alpha)$ ,  $m \in M$ ,  $\alpha \in R$ ,  $\alpha \neq 0$ , and define the equivalence relation on  $S$  suggested by thinking of  $(m, \alpha)$  as  $\alpha^{-1}m$ , namely,

$$(m_1, \alpha_1) \sim (m_2, \alpha_2) \quad \text{if and only if } \alpha_2 m_1 = \alpha_1 m_2.$$

That this relation is reflexive and symmetric is immediate; transitivity follows from the assumption that  $M$  is torsion-free. We may thus partition  $S$  into disjoint equivalence classes, and denote by  $[m, \alpha]$  the class in which  $(m, \alpha)$  lies. Define addition of classes by

$$[m_1, \alpha_1] + [m_2, \alpha_2] = [\alpha_2 m_1 + \alpha_1 m_2, \alpha_1 \alpha_2],$$

and verify at once that the sum of classes does not depend on the choice of representatives from those classes. The collection of

classes forms an additive abelian group with respect to this operation, with zero element  $[0, 1]$ . Now define the action of  $K$  on this group by means of

$$\frac{\beta}{r} \cdot [m, \alpha] = [\beta m, r\alpha], \quad r \neq 0.$$

This definition is meaningful since, if  $\beta'/r' = \beta/r$  and  $(m', \alpha') \sim (m, \alpha)$ , then  $(\beta'm', r'\alpha') \sim (\beta m, r\alpha)$ . The collection of equivalence classes thus becomes a vector space over  $K$ , denoted by  $KM$ . If  $M$  is a finitely generated  $R$ -module, it is easily seen that  $KM$  is a finite-dimensional vector space over  $K$ . Further, if  $M$  has an  $R$ -basis  $\{m_1, \dots, m_t\}$ , the elements  $[m_1, 1], \dots, [m_t, 1]$  form a  $K$ -basis for  $KM$ .

The mapping  $m \rightarrow [m, 1]$  is obviously an  $R$ -isomorphism of  $M$  into  $KM$ . We shall usually regard  $M$  as embedded in  $KM$  by means of this mapping and shall denote  $[m, 1]$  briefly by  $m$ . Since

$$[m, \alpha] = \alpha^{-1}[m, 1] = \alpha^{-1}m,$$

the elements of  $KM$  can be thought of as  $K$ -multiples of the elements of  $M$ , and we have, for  $m_1, m_2 \in M$ ,

$$\frac{\alpha}{\beta} m_1 + \frac{\gamma}{\delta} m_2 = (\beta\delta)^{-1}(\delta\alpha m_1 + \beta\gamma m_2).$$

If  $M = \sum Rm_i$ ,  $m_i \in M$ , we have  $KM = \sum Km_i$ ; furthermore,  $M = \sum \oplus Rm_i$  implies  $KM = \sum \oplus Km_i$ .

A more sophisticated approach to these matters can be given using the concept of tensor product introduced in § 12. There it was shown how to make  $K \otimes_R M$  into a vector space over  $K$ , and it is easily checked that  $\sum \xi_i \otimes m_i \rightarrow \sum \xi_i[m_i, 1]$ ,  $\xi_i \in K$ ,  $m_i \in M$ , is a  $K$ -isomorphism of  $K \otimes_R M$  onto  $KM$ . The remarks about bases in  $KM$ , etc., can also be proved using the theorems of § 12.

By the  $R$ -rank of the torsion-free  $R$ -module  $M$  we shall mean the dimension  $(KM: K)$ ; we have already shown that a finitely generated  $R$ -module has finite rank. The converse is false, however, as is evident from the example  $M = K$ . It may be shown that the rank of  $M$  is equal to the maximal number of  $R$ -free elements in  $M$ . We shall often denote the rank of  $M$  by  $(M: R)$ .

Now let  $M, N$  be two torsion-free  $R$ -modules, and let  $\theta: M \rightarrow N$  be an  $R$ -isomorphism of  $M$  onto  $N$ . It is straightforward to verify (and immediate from the theory of tensor products) that  $\theta$  can be extended to a  $K$ -isomorphism  $\theta'$  of  $KM$  onto  $KN$ , given by

$$\theta'[m, \alpha] = [\theta m, \alpha], \quad m \in M, \alpha \in R, \alpha \neq 0.$$

This implies in particular that, for  $m \in M$  and  $\xi \in K$ ,

$$\theta'(\xi m) = \xi \theta'(m) = \xi \theta(m).$$

Hence, if  $m \in M$  and  $\xi \in K$  are such that also  $\xi m \in M$ , we have

$$(22.1) \quad \theta(\xi m) = \xi \theta(m).$$

As an application of the above remarks, we prove

(22.2) **LEMMA.** *The fractional ideals  $M, N$  are  $R$ -isomorphic if and only if they are in the same ideal class.*

**PROOF.** If  $M, N$  are in the same class, there exists  $\alpha \in K$  such that  $M = \alpha N$ , and obviously  $M \cong N$  as  $R$ -modules. Conversely, let  $\theta: M \cong N$  be an  $R$ -isomorphism, and extend it to a  $K$ -isomorphism  $\theta': KM \cong KN$ . Then we have

$$\theta'(\xi m) = \xi \theta'(m), \quad m \in KM, \xi \in K.$$

In particular, take  $m = 1$ , and restrict  $\xi$  to lie in  $M$ . Then we have

$$\theta(\xi) = \theta'(\xi) = \xi \theta'(1), \quad \xi \in M.$$

Therefore  $\theta$  is given by multiplication by  $\theta'(1)$ , which shows that  $N = M\theta'(1)$ , as we wished to prove.

In this section, we shall classify all finitely generated  $R$ -modules and shall develop a theory of invariant factors analogous to that obtained for modules over principal ideal rings. The  $R$ -ideals in  $K$  (fractional ideals) will play an important role. One thing to remember is that the fractional ideals are the non-zero *finitely generated*  $R$ -submodules of  $K$ .

(22.3) **LEMMA.** *Every finitely generated torsion-free  $R$ -module  $M$  of rank 1 is  $R$ -isomorphic to an  $R$ -ideal in  $K$ .*

**PROOF.** From the hypothesis, we see that  $KM$  is a one-dimensional vector space  $Km$  where we may take  $m \in M$ ,  $m \neq 0$ . Let

$$I = \{\alpha \in K: \alpha m \in M\}.$$

Then  $I$  is an  $R$ -submodule of  $K$ , and the map  $\alpha \rightarrow \alpha m$  gives an  $R$ -isomorphism of  $I$  onto  $M$ . Since  $M$  is finitely generated, so is  $I$ , and thus  $I$  is an  $R$ -ideal in  $K$ . This completes the proof.

(22.4) **LEMMA.** *Let  $M$  be a finitely generated torsion-free  $R$ -module, and embed  $M$  in  $KM$ . If  $\alpha \in K$  is such that  $\alpha M \subset M$ , then  $\alpha \in R$ .*

PROOF. Choose  $m \in M$ ,  $m \neq 0$ , and set

$$I = \{\beta \in K : \beta m \in M\}.$$

As above,  $I$  is a fractional ideal in  $K$ , and clearly  $I \supset R$ . Now suppose  $\alpha \in K$  is such that  $\alpha M \subset M$ ; then  $\alpha \in I$ , so  $R[\alpha] \subset I$ . Since  $I$  is finitely generated and  $R$  is noetherian, also  $R[\alpha]$  is finitely generated. But  $R$  is integrally closed, so we conclude that  $\alpha \in R$ .

In § 16 A we had introduced the concept of a pure submodule of a module. The concept is of importance in our discussion of modules over Dedekind domains. Let  $N$  be a submodule of the  $R$ -module  $M$ . We called  $N$  a *pure* submodule of  $M$  if, for each  $\alpha \in R$ ,  $\alpha N = N \cap \alpha M$ . If  $M$  is  $R$ -torsion-free, then  $N$  is pure if and only if, for each non-zero  $\alpha \in R$  and each  $m \in M$ ,  $\alpha m \in N$  implies  $m \in N$ . We showed that any direct summand is pure, that a submodule  $N$  of a torsion-free module  $M$  is pure if and only if  $M/N$  is torsion-free, and that every subset of  $M$  generates a uniquely determined pure submodule of  $M$ . The result (16.18) remains valid and asserts that if  $\{v_1, \dots, v_n\}$  is a  $K$ -basis of a vector space  $V_0$ , and if we set  $V = Rv_1 \oplus \dots \oplus Rv_n$ , then for any  $K$ -subspace  $W_0$  of  $V_0$  the module  $W_0 \cap V$  is a pure submodule of  $V$ .

If  $I_1, \dots, I_n$  are  $R$ -ideals in  $K$ , the external direct sum  $I_1 + \dots + I_n$  is a finitely generated torsion-free  $R$ -module of rank  $n$ . We now prove the converse.

(22.5) THEOREM. *Every finitely generated torsion-free  $R$ -module  $M$  of rank  $n$  is isomorphic to an external direct sum of  $n$  fractional ideals.*

PROOF. We use induction on  $n$ . In Lemma 22.3, we have established the result for  $n = 1$ . Let  $n \geq 2$ , and suppose the result is proved for modules of rank  $n - 1$ . Let us embed  $M$  in the vector space  $KM$  over  $K$ . Choose  $m \in M$ ,  $m \neq 0$ , and let  $N = Km \cap M$  be the pure submodule of  $M$  generated by  $m$ . Then  $M/N$  is  $R$ -torsion-free, finitely generated, and of rank  $n - 1$ . It follows from the induction hypothesis that there exist fractional ideals  $I_1, \dots, I_{n-1}$  in  $K$  such that

$$(22.6) \quad M/N \cong I_1 + \dots + I_{n-1}.$$

At this point it will suffice to prove that  $N$  is an  $R$ -direct summand of  $M$ . For if we show that  $M = N \oplus T$  for some  $R$ -submodule  $T$ , then, on the one hand, we will have

$$T \cong M/N \cong I_1 + \cdots + I_{n-1},$$

and, on the other hand,  $N$  will be a torsion-free  $R$ -module of rank 1, and so  $N \cong$  fractional ideal by (22.3). This will yield the desired result.

The essential step in the next part of the argument amounts to showing (in the terminology of Chapter VIII) that the fractional ideals are projective  $R$ -modules.

Because of (22.6), there exists an  $R$ -homomorphism  $\varphi$  of  $M$  onto  $I_1 + \cdots + I_{n-1}$  with kernel  $N$ . For each  $j$ , let  $M_j = \varphi^{-1}(I_j)$ , and set  $\varphi_j = \varphi|_{M_j}$ . Then  $\varphi_j$  is a homomorphism of  $M_j$  onto  $I_j$  with kernel  $N$ . We shall deduce from this that  $N$  is a direct summand of each  $M_j$ . Since  $I_j^{-1}I_j = R$ , there exist elements  $\alpha_1, \dots, \alpha_t \in I_j^{-1}$  and  $\beta_1, \dots, \beta_t \in I_j$  such that

$$\alpha_1\beta_1 + \cdots + \alpha_t\beta_t = 1.$$

Choose elements  $x_1, \dots, x_t \in M_j$  such that  $\varphi_j(x_i) = \beta_i$ ,  $1 \leq i \leq t$ , and let  $\gamma$  be a fixed non-zero element of  $I_j$ . Then each  $\gamma\alpha_i \in R$ , and

$$z = (\gamma\alpha_1)x_1 + \cdots + (\gamma\alpha_t)x_t$$

is some fixed element of  $M_j$ . We then have

$$\varphi(z) = \sum(\gamma\alpha_i)\varphi(x_i) = \gamma \sum \alpha_i\beta_i = \gamma.$$

Now let

$$T_j = Kz \cap M_j$$

be the pure submodule of  $M_j$  generated by  $z$ . We shall prove that

$$(22.7) \quad M_j = T_j \oplus N$$

and begin by showing that  $T_j \cap N = 0$ . For if  $\xi z \in N$  where  $\xi \in K$ , then by (22.1) we have

$$0 = \varphi(\xi z) = \xi\varphi(z) = \xi\gamma.$$

But this implies  $\xi = 0$  since  $\gamma$  is a non-zero element of  $I_j$ . Suppose now that  $x$  is any element of  $M_j$ , and set  $\varphi_j(x) = \xi \in I_j$ . Then each  $\xi\alpha_i \in R$ , and so

$$w = (\xi\alpha_1)x_1 + \cdots + (\xi\alpha_t)x_t \in M_j.$$

But  $w = \xi\gamma^{-1}z \in Kz$ , so  $w \in Kz \cap M_j$ , that is,  $w \in T_j$ . Also

$$\varphi(w) = \xi\gamma^{-1}\varphi(z) = \xi$$

shows that  $x - w \in N$ , and we have  $x = w + (x - w)$ . This proves that (22.7) holds.

In each  $M_j$  we have thus found a pure submodule  $T_j$  such that  $M_j = T_j \oplus N$ , and  $\varphi(T_j) = \varphi(M_j) = I_j$ . We shall now show that

$$(22.8) \quad M = (T_1 + \cdots + T_{n-1}) \oplus N.$$

Clearly,  $M = T_1 + \cdots + T_{n-1} + N$  since  $\varphi(T_1 + \cdots + T_{n-1}) = I_1 + \cdots + I_{n-1}$ . If  $t_1 + \cdots + t_{n-1} \in N$  where each  $t_i \in T_i$ , then

$$\varphi(t_1) + \cdots + \varphi(t_{n-1}) = 0.$$

However, each  $\varphi(t_i) \in I_i$  and hence is 0. Thus each  $t_i = 0$ , which completes the proof that (22.8) holds. As we have observed, this also finishes the proof of the theorem.

Suppose now that

$$(22.9) \quad M \cong I_1 + \cdots + I_n$$

where the  $\{I_j\}$  are non-zero fractional ideals in  $K$ . We may find non-zero elements  $\alpha_1, \dots, \alpha_n \in K$  such that each  $\alpha_j I_j \supset R$ . Further,  $I_j \cong \alpha_j I_j$  implies that

$$M \cong \alpha_1 I_1 + \cdots + \alpha_n I_n.$$

This shows that, by multiplying the  $\{I_j\}$  in (22.9) by non-zero elements of  $K$ , we may assume hereafter that each  $I_j \supset R$ . Now choose  $m_j \in M$  so that  $m_j$  maps onto  $1 \in I_j$  in the isomorphism  $\psi$  [in (22.9)]. Then we have, applying (22.1) to the inverse of  $\psi$ ,

$$(22.10) \quad M = I_1 m_1 \oplus \cdots \oplus I_n m_n.$$

Thus,  $\{m_1, \dots, m_n\}$  forms a “basis” for  $M$  in the sense that every element  $m \in M$  is expressible in the form

$$m = \lambda_1 m_1 + \cdots + \lambda_n m_n, \quad \lambda_j \in I_j,$$

and  $\sum \lambda_j m_j = \sum \lambda'_j m_j$ ,  $\lambda_j, \lambda'_j \in I_j$ , implies  $\lambda_j = \lambda'_j$ ,  $1 \leq j \leq n$ .

(22.11) **THEOREM.** *Let  $M = I_1 + \cdots + I_m$ ,  $N = J_1 + \cdots + J_n$  be external direct sums of  $R$ -ideals in  $K$ . Then  $M \cong N$  if and only if  $m = n$  and the products  $I_1 \cdots I_m$  and  $J_1 \cdots J_n$  are in the same ideal class.*

**PROOF.** Assume first that  $M \cong N$ ; then  $m = (M: R) = (N: R) = n$ . Further, we may assume that each  $I_k$  and each  $J_k$  contains  $R$ , since we may achieve this state of affairs by replacing them by ideals in their classes, and this replacement does not affect the ideal class of the products  $I_1 I_2 \cdots I_m$ ,  $J_1 J_2 \cdots J_n$ .

Let  $\theta: M \cong N$ , and let  $\theta$  map  $1 \in I_k$  onto  $(\alpha_{k1}, \dots, \alpha_{km})$  where  $\alpha_{kl} \in J_l$ . Then, by (22.1),  $M$  maps onto

$$\left( \sum_k \alpha_{k1} I_k, \dots, \sum_k \alpha_{km} I_k \right)$$

so that

$$J_l = \alpha_{1l} I_1 + \dots + \alpha_{ml} I_m, \quad l = 1, \dots, m.$$

Therefore the product  $J_1 \cdots J_m$  contains all the ideals

$$\alpha_{1i_1} \cdots \alpha_{mi_m} I_1 \cdots I_m$$

where  $(i_1, \dots, i_m)$  is any permutation of  $(1, \dots, m)$ . If  $\delta = \det(\alpha_{ij})$ , then  $\delta$  is a sum of such products  $\prod \alpha_{ij}$  and their negatives, and so

$$J_1 \cdots J_m \supset \delta I_1 \cdots I_m.$$

On the other hand, we may find elements  $\beta_{lk} \in I_k$  such that  $\theta(\beta_{l1}, \dots, \beta_{lm}) = 1 \in J_l$ . Then  $(\beta_{ij})(\alpha_{ij})$  is the identity matrix, and so  $\det(\beta_{ij}) = \delta^{-1}$ . The above reasoning similarly shows that

$$I_1 \cdots I_m \supset \delta^{-1} J_1 \cdots J_m.$$

Therefore  $\delta I_1 \cdots I_m = J_1 \cdots J_m$ , which completes the first half of the proof.

To prove the converse, it suffices to show that, if  $I_1$  and  $I_2$  are fractional ideals, then

$$I_1 + I_2 \cong R + I_1 I_2.$$

Since we may replace  $I_1$  and  $I_2$  by ideals in their classes, we may show (Exercise 22.4) that we may assume  $I_1 + I_2 = R$  (sum of ideals in  $K$ ). Choose  $\alpha_1 \in I_1$ ,  $\alpha_2 \in I_2$  such that  $\alpha_1 - \alpha_2 = 1$ . Let

$$\varphi(\beta_1, \beta_2) = (\beta_1 + \beta_2, \alpha_1 \beta_2 + \alpha_2 \beta_1), \quad \beta_1 \in I_1, \beta_2 \in I_2.$$

Then  $\varphi: I_1 + I_2 \rightarrow R + I_1 I_2$  is an  $R$ -homomorphism. We now prove that  $\varphi$  is an isomorphism “onto.” Let  $\alpha \in R$ ,  $r \in I_1 I_2$ ; set  $\beta_1 = \alpha_1 \alpha - r$ ,  $\beta_2 = \alpha - \alpha_1 = r - \alpha_2 \alpha$ . We find readily that  $(\beta_1, \beta_2)$  is the unique element of  $I_1 + I_2$  such that  $\varphi(\beta_1, \beta_2) = (\alpha, r)$ . This completes the proof of the theorem.

**COROLLARY.** *If  $I_1, \dots, I_n$  are fractional ideals, then  $I_1 + \cdots + I_n \cong R + \cdots + R + (I_1 \cdots I_n)$  where there are  $(n-1)$   $R$ 's on the right-hand side.*

We are now ready to prove the invariant factor theorem for finitely generated torsion-free  $R$ -modules. We shall follow the treatment given by Chevalley [1].

(22.12) **THEOREM (Invariant Factor Theorem).** *Let  $M, N$  be finitely generated torsion-free  $R$ -modules of the same rank  $k$ , such that*

$N \subset KM$ . Then there exist elements  $m_1, \dots, m_k \in M$  and fractional ideals  $I_1, \dots, I_k, E_1, \dots, E_k$  such that  $E_j \supset E_{j+1}$  ( $j = 1, \dots, k - 1$ ) and such that

$$(22.13) \quad M = I_1 m_1 \oplus \cdots \oplus I_k m_k, \quad N = E_1 I_1 m_1 \oplus \cdots \oplus E_k I_k m_k.$$

The ideals  $E_1, \dots, E_k$  are uniquely determined by the pair  $M, N$  and are called the invariant factors of  $N$  in  $M$ .

PROOF. Step 1. Assume that  $k \geq 1$  and that the result has been proved for modules of rank  $k - 1$ . By virtue of the hypothesis, we may regard both  $M$  and  $N$  as embedded in a common  $k$ -dimensional vector space  $KM (= KN)$ . Thus, for any  $m \in M$ , there exists a non-zero  $\alpha \in R$  such that  $\alpha m \in N$ . Since  $M$  is finitely generated, this implies the existence of  $r \in R$ ,  $r \neq 0$ , such that

$$rM \subset N.$$

Step 2. Let

$$E' = \{\alpha \in K : \alpha N \subset M\}.$$

Obviously  $E'$  is a non-zero  $R$ -submodule of  $K$ . Further,  $\alpha \in E'$  implies  $\alpha N \subset M \subset r^{-1}N$ , and so  $r\alpha N \subset N$ . From Lemma 22.4, we deduce that  $r\alpha \in R$ , or  $\alpha \in r^{-1}R$ . Therefore  $E'$  is a submodule of  $r^{-1}R$  and so is a fractional ideal in  $K$ . From its definition,  $E'$  is the largest ideal such that  $E'N \subset M$ . Setting  $E = (E')^{-1}$ , we deduce that  $E$  is the unique minimal fractional ideal such that

$$N \subset EM.$$

For any proper integral ideal  $P$ , we therefore have  $N \notin PEM$ .

Let  $P_1, \dots, P_s$  be the distinct prime ideals which either contain the principal ideal  $rR$  or occur with negative exponent in the factorization of  $E$  into powers of prime ideals. For each  $i$ ,  $1 \leq i \leq s$ , choose  $n_i \in N$  such that  $n_i \notin P_i EM$ . Then choose  $\mu_i \in R$  such that

$$\mu_i \equiv 0 \pmod{\prod_{j \neq i} P_j}, \quad \mu_i \not\equiv 0 \pmod{P_i},$$

and set

$$n = \sum_{i=1}^s \mu_i n_i \in N.$$

We claim  $n \notin P_i EM$  for any  $i$ ; suppose, for example,  $n \in P_1 EM$ . Then  $\mu_i n_i \in P_1 N \subset P_1 EM$  for  $i \neq 1$ , and hence  $\mu_1 n_1 \in P_1 EM$ . Since

$P_i$  is a maximal ideal, we can choose  $\mu \in R$ ,  $p \in P_i$  such that  $p + \mu\mu_i = 1$ . Then

$$n_i = pn_i + \mu\mu_i n_i \in P_i EM,$$

which is impossible. We have thus obtained an element  $n \in N$  such that  $n \notin P_i EM$  for  $i = 1, \dots, s$ .

*Step 3.* The module  $Kn \cap N$  is a pure submodule of  $N$  of rank 1; similarly,  $Kn \cap M$  is a pure submodule of  $M$  of rank 1. An argument similar to the proof of Lemma 22.3 shows that there exist fractional ideals  $A, B$  such that

$$Kn \cap N = An, \quad Kn \cap M = Bn.$$

Then  $E'An \subset E'N \subset M$  implies  $E'A \subset B$ , so that  $B = C'E'A$  where  $C'$  is the inverse of an integral ideal  $C$ . Next, we have  $\gamma Bn \subset \gamma M \subset N$ , and so  $\gamma B \subset A$ , or  $\gamma \in AB^{-1} = CE$ . Therefore  $CE$  contains the principal ideal  $\gamma R$ , so that every prime ideal factor of  $C$  either contains  $\gamma R$  or occurs in the “denominator” of  $E$ . Hence the prime ideal divisors of  $C$  are among  $P_1, \dots, P_s$ . On the other hand, if  $P_i \supset C$ , then

$$n \in An = CEBn \subset CEM \subset P_i EM,$$

which is impossible. Therefore  $C = R$ , and  $B = E'A$ .

*Step 4.* Set  $N_i = An$ ,  $M_i = E'An$ ; we have shown that  $N_i, M_i$  are pure submodules of rank 1 of  $N, M$ , respectively. The proof of Theorem 22.5 then implies that  $M_i$  is an  $R$ -direct summand of  $M$ ; that is, there exists a complementary submodule  $M'_i$  of  $M$  such that

$$M = M_i \oplus M'_i.$$

We claim then that

$$N = N_i \oplus N'_i, \quad N'_i = KM'_i \cap N.$$

Obviously  $KN'_i = KM'_i$  so that

$$N_i \cap N'_i \subset KN_i \cap KN'_i = KM_i \cap KM'_i = (0).$$

Further, if  $x \in N$ , we may write

$$x = \alpha n + y, \quad \alpha \in K, y \in KM'_i,$$

Then  $E'x = E'\alpha n + E'y$ ; however,  $E'x \subset M$ ,  $E'\alpha n \subset KM_i$ ,  $E'y \subset KM'_i$  imply that  $E'\alpha n \subset M_i$ . Therefore  $\alpha n \in EM_i = N_i$ , and hence  $y \in KM'_i \cap N = N'_i$ . We have thus shown that

$$M = Bn \oplus M'_1, \quad N = EBn \oplus N'_1, \quad KM'_1 = KN'_1.$$

*Step 5.* We now apply the induction hypothesis to  $M'_1, N'_1$  to deduce the existence of elements  $m_1, \dots, m_{k-1} \in M'_1$  and ideals  $A_1, \dots, A_{k-1}, E_1, \dots, E_{k-1}$  in  $K$  such that  $E_j \supset E_{j+1}$  ( $j = 1, \dots, k-2$ ) and such that

$$\begin{aligned} M'_1 &= A_1 m_1 \oplus \cdots \oplus A_{k-1} m_{k-1}, \\ N'_1 &= E_1 A_1 m_1 \oplus \cdots \oplus E_{k-1} A_{k-1} m_{k-1}. \end{aligned}$$

To complete the proof of the first part of the theorem, it is sufficient to prove that  $E \supset E_1$ . It is immediate that  $E_1$  is characterized as the unique minimal  $R$ -ideal in  $K$  such that  $E_1 M'_1 \supset N'_1$ . But we have  $E M'_1 \supset N'_1$  so that  $E \supset E_1$ , as we wish to prove.

*Step 6.* We have to prove finally that the ideals  $E_1, \dots, E_k$  in (22.13) are uniquely determined. By replacing  $M$  by  $E_1 M$  if necessary, we may assume all the ideals  $\{E_i\}$  are integral ideals in  $R$ . Then, by Corollary 18.24 and Exercise 18.7, we have

$$M/N \cong I_1/E_1 I_1 + \cdots + I_k/E_k I_k \cong R/E_1 + \cdots + R/E_k.$$

The modules  $\{R/E_i\}$  are cyclic  $R$ -modules with annihilating ideals  $\{E_i\}$ ,  $1 \leq i \leq k$ . Moreover, each module  $R/E_i$  satisfies both chain conditions for submodules because there are at most a finite number of ideals between  $E_i$  and  $R$ . Therefore  $M/N$  has a composition series. The rest of the proof of the uniqueness of the  $\{E_i\}$  is entirely analogous to the proof of Theorem 16.8 and will be left as an exercise for the reader.

**REMARKS.** (1) If, in the above theorem, we assume also that  $N \subset M$ , obviously each  $E_i$  is an integral ideal. (2) Since the elements  $m_1, \dots, m_k$  all lie in  $M$ , it follows that each  $I_j$  contains 1, and hence each  $I_j \supset R$ .

A slight modification of the proof of the previous theorem establishes the following more general result.

(22.14) **COROLLARY.** *Let  $M$  and  $N$  be finitely generated torsion-free  $R$ -modules such that  $N \subset KM$ , and let  $M$  have rank  $k$ . Then there exist elements  $m_1, \dots, m_k$  in  $M$  and fractional ideals  $I_1, \dots, I_k, E_1, \dots, E_l$  [where  $l = (N:R)$ ] such that  $E_i \supset E_{i+1}$  for  $1 \leq i \leq l-1$ , and*

$$M = I_1 m_1 \oplus \cdots \oplus I_k m_k, \quad N = E_1 I_1 m_1 \oplus \cdots \oplus E_l I_l m_l.$$

*If  $N \subset M$ , each  $E_i$  is an integral ideal.*

(22.15) COROLLARY. Let  $M$  be a finitely generated torsion-free  $R$ -module over a Dedekind domain  $R$ . Then a submodule  $N$  of  $M$  is pure if and only if  $N$  is a direct summand of  $M$ .

PROOF. This result follows immediately from (22.14) and from the fact that  $N$  is pure if and only if  $M/N$  is torsion-free.

(22.16) COROLLARY. Every finitely generated  $R$ -module is isomorphic to an external direct sum of fractional ideals in  $K$  and  $R$ -modules of the form  $R/I$  where  $I$  is an integral ideal.

The proof is similar to the proof Theorem 16.10 in that  $M$  is first represented as a homomorphic image of a free  $R$ -module on a finite basis. Then Corollary 22.14 is applied, and the conclusion of (22.16) follows from the observation that

$$I_j m_j / E_j I_j m_j \cong I_j / E_j I_j \cong R / E_j$$

by Exercise 18.7.

### Exercises

$R$  denotes always a Dedekind ring with quotient field  $K$ .

- Let  $M$  be the left  $R$ -module  ${}_R R$ . Show that  $KM \cong K$ .
- Let  $V_0$  be a vector space over  $K$ , and let  $V$  be an  $R$ -submodule of  $V_0$ . Let  $M$  be a torsion-free  $R$ -module for which there exists an  $R$ -isomorphism  $\theta: V \cong M$ . If  $KV$  denotes the  $K$ -subspace of  $V_0$  generated by the elements of  $V$ , prove that  $\theta$  may be extended to a  $K$ -isomorphism  $\theta: KV \cong KM$ .
- Show that the  $R$ -rank  $(M: R)$  of the torsion-free  $R$ -module  $M$  equals the maximal number of  $R$ -free elements of  $M$ .
- If  $I$  and  $J$  are fractional ideals in  $K$ , show that there exist non-zero elements  $\alpha, \beta \in K$  such that  $\alpha I$  and  $\beta J$  are relatively prime integral ideals. [Hint: Choose non-zero  $\beta, \gamma \in K$  such that  $\beta J$  and  $\gamma I^{-1}$  are integral ideals. Choose  $F$  integral such that  $F \cdot \gamma I^{-1}$  is principal and  $F + \beta J = R$ . Then  $F = \alpha I$  for some  $\alpha \in K$ .] [Remark: In the above hint,  $F$  could have been chosen so as to be relatively prime to any preassigned integral ideal  $C$  as well as to  $\beta J$ .]
- Let  $I_1$  and  $I_2$  be fractional ideals,  $E_1$  and  $E_2$  integral ideals such that  $E_2 \subset E_1$ . Prove that there exists an isomorphism of  $I_1 + I_2$  onto  $R + I_1 I_2$  which carries  $E_1 I_1 + E_2 I_2$  onto  $E_1 + E_2 I_1 I_2$ . [Hint: After replacing  $I_1$  and  $I_2$  by equivalent ideals, we may assume (by the preceding exercise) that  $I_1$  and  $I_2$  are integral ideals such that  $I_1 + E_2 I_2 = R$ . Now choose  $\alpha_1 \in I_1$ ,  $\alpha_2 \in E_2 I_2$  such that  $\alpha_1 - \alpha_2 = 1$ , and proceed as in the latter half of the proof of Theorem 22.11].
- Let  $M$  be a finitely generated torsion-free  $R$ -module of rank  $k$ ,  $N$  a submodule of  $M$  of rank  $l$ , and  $E_1, \dots, E_l$  the invariant factors of  $N$  in  $M$ . Show that there exists a fractional ideal  $I$  and an isomorphism

$$\theta: M \cong R \dot{+} \cdots \dot{+} R \dot{+} I \quad (k \text{ summands})$$

such that

$$\theta(N) = \begin{cases} E_1 \dot{+} \cdots \dot{+} E_l, & l < k \\ E_1 \dot{+} \cdots \dot{+} E_{k-1} \dot{+} E_k I, & l = k \end{cases}$$

7. Using the notation of §20A, show that  $R'$  is a torsion-free finitely generated  $R$ -module of rank  $n = (K': K)$ . Hence we may write

$$R' = B_1 x_1 \oplus \cdots \oplus B_n x_n$$

with  $x_1, \dots, x_n \in K'$ , and the  $\{B_i\}$   $R$ -ideals in  $K$ . If  $A$  is any non-zero ideal in  $R$ , prove that

$$\frac{R'}{AR'} \cong \frac{B_1}{AB_1} \dot{+} \cdots \dot{+} \frac{B_n}{AB_n}$$

as  $R$ -modules. Using 18.24, prove from this that

$$N(AR') = \{N(A)\}^n.$$

[Compare with (20.16).]



## Semi-simple Rings and Group Algebras

We have seen in Chapter II that the study of group representations is equivalent of the study of modules over group algebras. Some of the main results in this theory depend not so much on special properties of group algebras as on properties which group algebras have because they belong to the larger class of rings with minimum condition. This chapter contains the Wedderburn structure theorems for semi-simple rings with minimum condition, together with applications to algebras, and in particular to group algebras, which are more or less direct consequences of these theorems. The specific applications to group representations, including the fundamental results of Burnside, Frobenius, and Schur, are collected in §27. These results are used in §28 to determine the irreducible representations of the symmetric group.

### § 23. Preliminary Remarks

Let us begin by recalling several definitions, first stated in Chapter II, which are used repeatedly in the present chapter. A ring  $R$  (with unity element 1) is called a *ring with minimum condition* if the left ideals of  $R$  satisfy the descending chain condition or, equivalently [see (11.15)], if in every non-empty set of left ideals of  $R$  there exists a left ideal which does not properly contain any other ideal in the set.

(The minimum condition as we have defined it should properly be called the *left minimum condition*; there is, of course, a *right minimum condition* too, and we could get a similar theory if we started from this finiteness assumption instead.)

An *algebra*  $A$  over the field  $K$  is a ring  $A$  (with 1) which is also a vector space over the field  $K$ , where the scalar multiplication in the vector space  $A$  and the ring multiplication in  $A$  are linked by

$$(23.1) \quad \alpha(ab) = (\alpha a)b = a(\alpha b)$$

for  $\alpha \in K$ ,  $a, b \in A$ . The algebra  $A$  is called *finite dimensional* over

$K$  if the vector space dimension  $(A : K)$  is finite. For example, if  $G$  is a finite group, the group ring  $KG$  is a finite-dimensional algebra over  $K$ .

Now we show that every algebra  $A$  finite dimensional over  $K$  is a ring with minimum condition. From (23.1) we have for all  $\alpha \in K$  and  $b \in A$ ,

$$ab = \alpha(1b) = (\alpha 1)b,$$

and

$$(23.2) \quad (\alpha 1)b = \alpha(1b) = \alpha(b1) = b(\alpha 1).$$

These imply that the set of elements

$$K_0 = \{\alpha 1 : \alpha \in K\}$$

is contained in the center of  $A$ , and is a field isomorphic to  $K$ . We shall always identify  $K$  and  $K_0$ , and regard  $K$  as embedded in  $A$ . Then (23.2) shows that every left, right, or two-sided ideal in the ring  $A$  is also a  $K$ -subspace of the *vector space*  $A$ . Since the subspaces of a finite-dimensional vector space satisfy the descending chain condition, it follows that  $A$  is a ring with minimum condition.

More generally, let  $M$  be a left  $A$ -module. The above remarks readily imply that  $M$  is a left vector space over  $K$  if we define

$$\alpha m = (\alpha 1)m, \quad \alpha \in K, m \in M.$$

Submodules of the  $A$ -module  $M$  are then necessarily subspaces of the vector space  $M$  over  $K$ . Thus if  $(M : K)$  is finite, the submodules of  $M$  satisfy both chain conditions.

We remark that not every ring with minimum condition can be regarded as an algebra over a field. For example, let  $m \in \mathbb{Z}$ ,  $m > 1$ , and suppose  $m$  is not a prime power. Then the ring  $\mathbb{Z}/(m)$  is finite and contains  $m$  elements. It is impossible for  $\mathbb{Z}/(m)$  to be an algebra over a field  $K$ , however, since  $K$  would have to be finite, and a finite-dimensional vector space over  $K$  would contain a prime power number of elements.

Finally, we must establish some notations for operations on subsets of a ring. The reader will sometimes have to distinguish these notations from corresponding notations for groups by the context. Let  $S, T$  be additive subgroups of a ring  $R$ . Then  $S + T$  denotes the additive subgroup of  $R$  given by

$$\{s + t : s \in S, t \in T\}.$$

On the other hand, if  $S$  and  $T$  are arbitrary subsets of  $R$ , define  $ST$  to be the additive subgroup of  $R$  generated by the set

$$(st : s \in S, t \in T).$$

Thus  $ST$  consists of all finite sums

$$\sum (\pm s_i t_i), \quad s_i \in S, t_i \in T.$$

It is easily verified that

$$(ST)U = S(TU), \quad S(T + U) = ST + SU.$$

Furthermore, if  $S$  and  $T$  are left ideals of  $R$ , so are  $S + T$  and  $ST$ ; similar results hold for right and two-sided ideals.

If  $\{S_i\}$  is a (possibly infinite) family of additive subgroups of  $R$ , the sum

$$\sum_i S_i$$

is defined as the subgroup consisting of all finite sums of form

$$\sum_{j=1}^t s_{ij}, \quad s_{ij} \in S_{ij}.$$

We may also remark that if  $S$  is a left ideal of  $R$  and if  $T$  is any subset of  $R$ , then  $ST$  is also a left ideal of  $R$ . Analogously, any left multiple of a right ideal is again a right ideal. The left ideal generated by an element  $a \in R$  is just  $Ra$ , the right ideal  $aR$ , the two-sided ideal  $RaR$ .

If  $S$  is a subset of  $R$ , we put

$$S^2 = SS, \quad S^3 = SSS, \dots.$$

Thus  $S^n$  consists of all finite sums of products of  $n$  elements of  $S$ :

$$(23.3) \quad S^n = \left\{ \sum_i (s_{i1}s_{i2} \cdots s_{in}), s_{ij} \in S \right\}.$$

If  $S$  is a left ideal of  $R$ , so are  $S^2, S^3, \dots$ .

## § 24. The Radical of a Ring with Minimum Condition

We start with a basic definition, whose importance will become clear as we proceed.

(24.1) **DEFINITION.** An element  $x \in R$  is *nilpotent* if there exists a positive integer  $m$  such that  $x^m = 0$ . An element  $x \in R$  is

*idempotent* if  $x^2 = x \neq 0$ . A left, right, or two-sided ideal  $I$  of  $R$  is *nilpotent* if there exists a positive integer  $m$  such that  $I^m = 0$ .

As an illustration, consider the case  $R = \mathbb{Z}/(p^n)$  where  $p$  is prime and  $n > 1$ . The nilpotent elements of  $R$  are just the residue classes of the form  $rp + (p^n)$ ,  $r \in \mathbb{Z}$ , so there are  $p^{n-1}$  nilpotent elements of  $R$ . On the other hand, the unity element of  $R$  is its only idempotent. The ideals of  $R$  are principal, generated by residue classes  $p^k + (p^n)$  for some  $k$ . Each proper ideal of  $R$  is nilpotent.

Returning to the general case, let  $I$  be a left ideal of  $R$ . Using (23.3), we see readily that  $I^m = 0$  if and only if for every choice of  $m$  elements  $a_1, \dots, a_m \in I$ , distinct or not, we have  $a_1 a_2 \cdots a_m = 0$ . Obviously, any left ideal containing an idempotent cannot be nilpotent. Conversely,

(24.2) THEOREM. *In a ring  $R$  with minimum condition, every non-nilpotent left ideal  $I$  contains an idempotent element.*

PROOF. We shall use repeatedly the fact that every non-empty collection of left ideals of  $R$  contains a minimal member. The collection of non-nilpotent left ideals of  $R$  contained in  $I$  is non-empty, since  $I$  is such an ideal. Let  $I_1$  be a minimal member of this collection; then any left ideal of  $R$  properly contained in  $I_1$  must be nilpotent. Now  $I_1^2$  is a non-nilpotent left ideal contained in  $I_1$ , and so  $I_1^2 = I_1$ .

Next consider the collection of all left ideals  $L$  such that

- (i)  $I_1 L \neq 0$ ,
- (ii)  $L \subset I_1$ .

The collection is not empty since it contains  $I_1$ , and hence it has a minimal member  $L_1$ . By (i), there exists an  $x \in L_1$  such that  $I_1 x \neq 0$ . Then  $I_1 x \subset L_1$ , and  $I_1 x$  is in the collection, so  $I_1 x = L_1$ . Hence there exists an  $a \in I_1$  such that  $x = ax$ , and so

$$x = ax = a^2 x = \cdots .$$

Therefore  $I_1$  contains the non-nilpotent element  $a$ , and  $(a^2 - a)x = 0$ . Now set

$$N = \{u \in I_1 : ux = 0\} \subset I_1 .$$

Since  $I_1 x = L_1 \neq 0$ , it follows that  $N$  is a left ideal properly contained in  $I_1$ , and hence  $N$  is nilpotent. Setting  $n_1 = a^2 - a \in N$ , we see that if  $n_1 = 0$  then  $a$  is an idempotent element of  $I_1$ , hence of  $I$ , and the theorem holds. If  $n_1 \neq 0$ , proceed as follows: Set

$$a_1 = a + n_1 - 2an_1 \in I_1.$$

Then  $a_1$ ,  $a$ , and  $n_1$  commute with each other, and hence if  $a_1$  is nilpotent, so is  $a = a_1 - n_1 + 2an_1$ . Thus  $a_1$  is a non-nilpotent element of  $I_1$ , and we find readily that

$$a_1^2 - a_1 = 4n_1^3 - 3n_1^2.$$

The element  $n_2 = a_1^2 - a_1$  is nilpotent, contains  $n_1^2$  as a factor, and commutes with  $a_1$ . By induction, we can successively construct non-nilpotent elements  $a_1, a_2, \dots$  in  $I_1$  such that  $a_i^2 - a_i$  contains  $n_1^{2^i}$  as a factor. Since  $n_1$  is nilpotent, this factor is zero for sufficiently large  $i$ , and some  $a_i$  is idempotent. This proves the theorem.

Now let  $N_1$  and  $N_2$  be nilpotent left ideals of  $R$ ; the sum  $N_1 + N_2$  is also a left ideal. Let  $N_1^q = N_2^r = 0$ . Then every element in  $(N_1 + N_2)^{q+r}$  is a sum of products  $x_1 \cdots x_{q+r}$  in which either at least  $q$  factors belong to  $N_1$  or at least  $r$  factors belong to  $N_2$ . In the former case, the above product may be written as

$$(x_1 \cdots x_{i_1})(x_{i_1+1} \cdots x_{i_2}) \cdots (x_{i_{s-1}+1} \cdots x_{i_s}) \cdots,$$

where  $x_{i_1}, x_{i_2}, \dots, x_{i_s} \in N_1$  and  $s \geq q$ . Each group in parentheses belongs to  $N_1$  since  $N_1$  is a left ideal. However, the product of any  $s$  elements of  $N_1$  is 0, and so the above product is 0. A similar argument holds when at least  $r$  factors belong to  $N_2$ . We have thus shown

(24.3) *The sum of any finite number of nilpotent left ideals is nilpotent.*

We shall use this in proving

(24.4) **THEOREM.** *The sum of all the nilpotent left ideals in a ring  $R$  with minimum condition is a two-sided nilpotent ideal  $N$ . The ideal  $N$  contains every nilpotent right ideal of  $R$ , and the factor ring  $R/N$  has no nilpotent ideals except 0.*

**PROOF.** Clearly the sum  $N$  of all nilpotent left ideals of  $R$  is a left ideal. If  $N$  were not nilpotent, then, by Theorem 24.2,  $N$  would contain an idempotent  $e$ . But  $e$  belongs to the sum of a finite number of nilpotent left ideals and so must be nilpotent by (24.3). This is impossible, and therefore  $N$  must be nilpotent.

Now consider the two-sided ideal  $NR$ ; for each  $i$ ,

$$(NR)^i = N(RN)(RN) \cdots (RN)R \subset N^i R.$$

Therefore  $NR$  is a nilpotent left ideal, and so  $NR \subset N$ . This shows that  $N$  is a two-sided ideal.

If  $J$  is any nilpotent right ideal of  $R$ , the above reasoning also shows that  $RJ$  is a nilpotent two-sided ideal, and so  $J \subset RJ \subset N$ .

Finally, every left ideal in  $R/N$  is of the form  $I/N$  for some left ideal  $I$  of  $R$  containing  $N$ . Then  $I/N$  is nilpotent in  $R/N$  if and only if some power of  $I$  is contained in  $N$ , and this can occur if and only if  $I$  is nilpotent and so is contained in  $N$ . Therefore  $R/N$  contains no nilpotent left ideals except 0, and by our previous discussion this implies that  $R/N$  contains no nilpotent right or two-sided ideals either, except 0.

(24.5) DEFINITION. Let  $R$  be a ring with minimum condition. The two-sided ideal which is the sum of all nilpotent left ideals of  $R$  is called the *radical* of  $R$  and is denoted by  $\text{rad } R$ . We say that  $R$  is *semi-simple* if  $\text{rad } R = 0$ .

If  $R$  is a ring with minimum condition, so is  $R/\text{rad } R$ , and the previous theorem then implies

$$(24.6) \quad R/\text{rad } R \quad \text{is semi-simple.}$$

It is perhaps desirable to remark that we may also speak about "semi-simplicity" for rings without minimum condition (see Jacobson [3]). Definition 24.5 is not the correct notion for such rings, and indeed a different definition of the radical is used, which reduces to the above for the special case of rings with minimum condition.

### *Exercises*

Throughout these exercises, all rings which occur are assumed to satisfy the minimum condition.

1. The radical of a commutative ring is the collection of all nilpotent elements.
2. For  $m > 1$ ,  $m \in \mathbb{Z}$ , what is  $\text{rad}(\mathbb{Z}/m\mathbb{Z})$ ?
3. A *nil* ideal is an ideal every element of which is nilpotent. Prove that every nil left ideal is nilpotent.
4. Show that every maximal left ideal  $I$  of a ring  $R$  contains  $\text{rad } R$ .  
[Hint: If not, then  $I + \text{rad } R = R$ . Hence we may write  $1 = a + x$ ,  $a \in I$ ,  $x \in \text{rad } R$ . Since  $x$  is nilpotent, the sum  $1 + x + x^2 + \dots$  is a finite sum, and the formula

$$(1 - x)(1 + x + x^2 + \dots) = 1$$

then shows that  $1 - x$  is a unit in  $R$ . This is impossible since  $1 - x = a \in I$ .]

5. Let  $e \in R$  be idempotent,  $N = \text{rad } R$ , and let  $R_1 = eRe$ . Show that  $R_1$  is a subring of  $R$  with unity element  $e$ , and that  $R_1$  is also a ring with mini-

mum condition. Using this fact, prove that

$$\text{rad } R_1 = eNe.$$

6. Let  $R \neq (0)$  be a ring with unity element whose only left ideals are  $(0)$  and  $R$ . Prove that  $R$  must be a skewfield. (In this problem  $R$  need not satisfy the minimum condition.)

7. Let  $K$  be a field,  $f(x) \in K[x]$  a non-constant polynomial, and  $R = K[x]/(f(x))$ . If

$$f(x) = \prod_{i=1}^m (f_i(x))^{e_i}$$

is the factorization of  $f(x)$  into powers of distinct irreducible polynomials, prove that

$$R \cong \sum_{i=1}^m K[x]/(f_i(x)^{e_i}) \quad (\text{direct sum}).$$

Show that

$$\text{rad } R \cong \sum_{i=1}^m (f_i(x))/(f_i(x)^{e_i}),$$

and hence that  $\text{rad } R = 0$  if and only if each  $e_i = 1$ . Show also that in general

$$R/\text{rad } R \cong \sum_{i=1}^m K[x]/(f_i(x))$$

and that the right-hand side is a direct sum of fields. Can you generalize all this for a ring  $R = D/I$  where  $D$  is a commutative principal ideal domain and  $I$  is a non-zero ideal?

## § 25. Semi-simple Rings and Completely Reducible Modules

Throughout this section, let  $R$  be a ring with minimum condition, containing a unity element 1. We have called  $R$  *semi-simple* if  $\text{rad } R = 0$ . We shall now give a second characterisation of semi-simple rings, due originally to Wedderburn, in terms of the structure of the left regular module  ${}_RR$ .

By a *minimal left ideal* of  $R$  we shall mean a non-zero left ideal  $L$  which contains no left ideals of  $R$  except 0 and  $L$ . Thus, the minimal left ideals of  $R$  are precisely the irreducible submodules of the left regular  $R$ -module  ${}_RR$ . If  $L$  is a non-nilpotent minimal left ideal, then by Theorem 24.2 there exists an idempotent  $e \in L$ . We then observe that  $Re$  is a non-zero left ideal contained in  $L$ , and so (because  $L$  is minimal)  $L = Re$ . We shall say that  $L$  is *generated* by the idempotent  $e$ . (It is easily seen from examples that, in general,  $e$  is not uniquely determined by  $L$ .) Further,

$$L = Re = \{x \in R : xe = x\}.$$

Set

$$L' = R(1 - e) = \{x \in R : xe = 0\}.$$

Then  $L'$  is also a left ideal of  $R$ , and  $L \cap L' = (0)$ . Since every  $x \in R$  is expressible as

$$x = xe + x(1 - e),$$

we deduce that

$$R = L \oplus L' = Re \oplus R(1 - e).$$

Now let  $I$  be a left ideal of  $R$  which contains  $L$ ; the above decomposition implies at once that

$$I = L \oplus (I \cap L').$$

We have therefore proved

(25.1) *Every non-nilpotent minimal left ideal of  $R$  is generated by an idempotent element, and is a direct summand of every left ideal containing it.*

Recalling an earlier definition (15.1), we called a left  $R$ -module  $M$  *completely reducible* if every submodule of  $M$  is a direct summand of  $M$ . For a completely reducible module, either chain condition implies the other; further, a completely reducible module satisfying both chain conditions is expressible as a direct sum of a finite number of irreducible submodules. Conversely, we showed that a module which is so expressible is completely reducible.

(25.2) **THEOREM.** *Let  $R$  be a ring with minimum condition. Then  $R$  is semi-simple if and only if  ${}_R R$  is a completely reducible left  $R$ -module.*

**PROOF.** Assume first that  $R$  is semi-simple, and let  $L_1$  be a minimal left ideal of  $R$ . Since  $\text{rad } R = 0$ , the ideal  $L_1$  is non-nilpotent and hence is generated by an idempotent  $e_1$ . From (25.1) we have

$$R = L_1 \oplus L'_1$$

where  $L'_1$  is some left ideal of  $R$ . If  $L'_1 \neq (0)$ , then  $L'_1$  contains a minimal left ideal  $L_2$ , and hence

$$L'_1 = L_2 \oplus L'_2$$

for some left ideal  $L'_2$  of  $R$ . Repeating this process, we obtain a strictly descending chain of left ideals

$$L'_1 \supset L'_2 \supset \cdots .$$

By the minimum condition, this chain must terminate in (0), and so we have a decomposition

$$(25.3) \quad R = L_1 \oplus L_2 \oplus \cdots \oplus L_n$$

into minimal left ideals. Thus  ${}_R R$  is completely reducible.

Suppose conversely that  ${}_R R$  is completely reducible, and let  $N = \text{rad } R$ . Since  $N$  is a left ideal of  $R$ , it is also a submodule of  ${}_R R$ , and therefore

$$R = N \oplus N'$$

for some left ideal  $N'$  of  $R$ . Then

$$1 = x + x' , \quad x \in N, x' \in N' ,$$

and so

$$x - x^2 = xx' \in N \cap N' ,$$

which shows that  $x - x^2 = 0$ . But then  $x = x^2 = x^3 = \cdots = 0$ , since  $x \in N$ , so that  $x' = 1$  and  $N' = R$ . Therefore  $N = 0$ , and  $R$  is semi-simple. This completes the proof.

Now let  $R$  be semi-simple, and consider the formula (25.3). Then we may write

$$(25.4) \quad 1 = e_1 + \cdots + e_n , \quad e_i \in L_i ,$$

for some set of elements  $\{e_i\}$  of  $R$ . (These  $\{e_i\}$  are not necessarily those occurring in the preceding proof.) From (25.4) we have

$$e_j = e_j e_1 + \cdots + e_j e_n , \quad e_j e_i \in L_i .$$

Since  $L_1 \oplus \cdots \oplus L_n$  is a direct sum, this yields

$$e_j e_1 = 0, e_j e_2 = 0, \dots, e_j e_j = e_j, e_j e_{j+1} = 0, \dots, e_j e_n = 0 .$$

Therefore

$$(25.5) \quad e_j e_i = 0 \quad \text{for } i \neq j, e_i^2 = e_i .$$

Let us show that  $L_i = Re_i$ , which will imply that  $e_i \neq 0$ . From (25.4), we have

$$R = Re_1 + \cdots + Re_n ,$$

and  $Re_i \subset L_i$ . Comparison with (25.3) then yields  $Re_i = L_i$ .

(25.6) **DEFINITION.** A set of idempotents  $\{e_i\}$  satisfying (25.5) is called an *orthogonal* set of idempotents.

We have therefore shown that if  $R$  is a semi-simple ring given by (25.3), where the  $\{L_i\}$  are minimal left ideals, and if we define the  $\{e_i\}$  by (25.4), then the  $\{e_i\}$  are an orthogonal set of idempotents. Further, (25.3) becomes

$$(25.7) \quad R = Re_1 \oplus \cdots \oplus Re_n, \quad L_i = Re_i.$$

An easy consequence of the above is

(25.8) *A ring  $R$  with minimum condition is semi-simple if and only if every left  $R$ -module is completely reducible.*

**PROOF.** It suffices to show that from (25.7) we may conclude that every left  $R$ -module  $M$  is completely reducible. We may write

$$(25.9) \quad M = \sum_{m \in M} \sum_{i=1}^n Re_i m.$$

Obviously each  $Re_i m$  is a submodule of  $M$ , but the sum need not be direct. The mapping  $Re_i \rightarrow Re_i m$  given by

$$xe_i \rightarrow xe_i m, \quad x \in R,$$

is clearly an  $R$ -homomorphism of  $Re_i$  onto  $Re_i m$ . Since  $Re_i (= L_i)$  is an irreducible  $R$ -module, the kernel of the homomorphism is either  $(0)$  or  $Re_i$ . Hence either  $Re_i m$  is also irreducible, or else  $Re_i m = 0$ . By (25.9) we then find that  $M$  is a sum (not necessarily direct) of irreducible submodules, which implies by (15.3) that  $M$  is completely reducible.

As a corollary to the above result, we have

(25.10) **THEOREM.** *If  $R$  is semi-simple, every irreducible  $R$ -module is isomorphic to some minimal left ideal of  $R$ .*

**PROOF.** In the proof of (25.8), let  $M$  be an irreducible  $R$ -module. Then some summand in (25.9) must be different from  $0$ , and that summand is isomorphic to  $Re_i$  for some  $i$ . But the summand is a submodule of the irreducible module  $M$ , and thus coincides with  $M$ .

The above theorem includes the result that starting with a decomposition of the semi-simple ring  $R$  into minimal left ideals:

$$R = L_1 \oplus \cdots \oplus L_n,$$

every minimal left ideal of  $R$  is isomorphic (as  $R$ -module) to some one of  $L_1, \dots, L_n$ . Furthermore, suppose we have another decomposition

$$R = L'_1 \oplus \cdots \oplus L'_m$$

into minimal left ideals. By the Jordan-Hölder theorem for  $R$ -modules, we have  $m = n$  and (renumbering the  $\{L'_i\}$  if need be)

$$L_i \cong L'_i, \quad 1 \leq i \leq n,$$

as left  $R$ -modules.

Now let  $L$  be any non-zero left ideal in the semi-simple ring  $R$ . Then there exists a left ideal  $L'$  of  $R$  such that

$$R = L \oplus L'$$

since  ${}_R R$  is completely reducible. Writing

$$1 = e + e', \quad e \in L, e' \in L',$$

we find as in the discussion preceding (25.1) that  $L = Re$ . Thus every non-zero left ideal of  $R$  is generated by an idempotent.

(25.11) THEOREM. *In the semi-simple ring  $R$ , let  $L = Re$  be a left ideal with generating idempotent  $e$ . Then  $L$  is a minimal left ideal if and only if  $eRe$  is a skewfield.*

PROOF. To begin with,  $eRe$  is a non-zero subring of  $R$  with unity  $e$ . By Exercise 24.6, it follows that  $eRe$  is a skewfield if and only if its only left ideals are 0 and  $eRe$ .

Suppose first that  $Re$  is a minimal left ideal of  $R$ , and let  $L_1$  be any non-zero left ideal of  $eRe$ . Then

$$RL_1 \subset R \cdot eRe \subset Re = L,$$

and so  $RL_1$  is left ideal of  $R$  contained in  $L$ , which implies that  $RL_1 = L$ . But since  $e$  is a two-sided unity for  $eRe$ , we have

$$eRe = eL = eRL_1 = eRe \cdot L_1 \subset L_1.$$

Therefore  $L_1 = eRe$ , proving that the only left ideals of  $eRe$  are itself and  $(0)$ , and hence that  $eRe$  is a skewfield.

Conversely, suppose  $L$  is not minimal. Then since every  $R$ -module is completely reducible, we may write

$$L = L_2 \oplus L_3,$$

a direct sum of non-zero left ideals of  $R$ . This gives a decomposition

$$e = e_2 + e_3, \quad e_2 \in L_2, e_3 \in L_3.$$

We note that

$$e_2e = e_2, \quad e_3e = e_3$$

since both  $e_2$  and  $e_3$  lie in  $L$ . On the other hand,

$$e = e^2 = ee_2 + ee_3$$

which shows that

$$ee_2 = e_2, \quad ee_3 = e_3.$$

Therefore  $e_2 = ee_2e$ ,  $e_3 = ee_3e$ , and  $eRe$  contains a pair of non-zero orthogonal elements  $e_2$  and  $e_3$ , and hence cannot be a skewfield.

We wish to investigate the isomorphisms among minimal left ideals of the semi-simple ring  $R$ . Let  $L, L'$  be minimal left ideals, and let

$$L = Re, \quad L' = Re'$$

where  $e$  and  $e'$  are idempotents.

(25.12) *The minimal left ideals  $L$  and  $L'$  are isomorphic if and only if  $L' = La'$  for some  $a' \in L'$ .*

PROOF. If  $L' = La'$ , then  $x \rightarrow xa'$  is an  $R$ -isomorphism of  $L$  onto  $L'$ . Conversely, let  $\varphi: L \cong L'$  be an  $R$ -isomorphism. Then

$$\varphi(xe) = x\varphi(e)$$

for every  $x \in R$  and hence also for  $x \in L$ . But  $xe = x$  when  $x \in L$ , so we have

$$\varphi(x) = x\varphi(e), \quad x \in L.$$

Setting  $a' = \varphi(e) \in L'$ , we have  $L' = La'$ .

Keeping the above notation, we note that for each  $a' \in L'$ ,  $La'$  is a left ideal of  $R$  and  $La' \subset L'$ , so that either  $La' = (0)$  or  $La' = L'$ . This yields

(25.13)  *$L \cong L'$  if and only if  $LL' = L'$ .*

We shall make use of this result to obtain information about the decomposition of a semi-simple ring  $R$  into two-sided ideals. We begin with

(25.14) **DEFINITION.** A ring  $S$  with unity element is *simple* if the left ideals of  $S$  satisfy the minimum condition and if the only two-sided ideals of  $S$  are the trivial ones  $(0)$  and  $S$ .

Let us show at once that a simple ring  $S$  is semi-simple. We note that  $N = \text{rad } S$  is a two-sided nilpotent ideal of  $S$  and that consequently  $N = (0)$  or  $S$ . The unity element  $1$  cannot belong to the nilpotent ideal  $N$ , hence  $N = (0)$  and  $S$  is semi-simple.

(25.15) **THEOREM.** *Let  $R$  be a semi-simple ring, and let  $L$  be a minimal left ideal of  $R$ . The sum  $B_L$  of all the minimal left ideals of*

*R* which are isomorphic to *L* is a simple ring and a two-sided ideal of *R*. Furthermore, *R* is the direct sum of all the ideals  $B_L$  obtained by letting *L* range over a full set of non-isomorphic minimal left ideals of *R*.

PROOF. Let *L*,  $L'$  be minimal left ideals of *R*. By (25.13), we see that  $L \cong L'$  if and only if  $B_L \cdot L' \neq (0)$ . But also  $L \cong L'$  if and only if  $L' \subset B_L$ . Since *R* is expressible as a finite direct sum of minimal left ideals, this shows that  $B_L$  is a two-sided ideal in *R* (and hence also a subring of *R*). Further,

$$B_L \cdot B_{L'} \neq (0) \quad \text{if and only if } L \cong L' .$$

Now let

$$(25.16) \quad R = L_1 \oplus \cdots \oplus L_n$$

where the  $\{L_i\}$  are minimal left ideals of *R* so numbered that  $L_1, \dots, L_m$  are pairwise non-isomorphic, and that each  $L_i$  is isomorphic to one of them. For convenience, define

$$B_i = B_{L_i}, \quad 1 \leq i \leq m .$$

Then since  $B_i$  contains all those  $L_j$  which are isomorphic to  $L_i$ , equation (25.16) implies that  $R \subset B_1 + \cdots + B_m$ , and so

$$(25.17) \quad R = B_1 + \cdots + B_m$$

where now  $B_i B_j \neq (0)$  if and only if  $i = j$ ,  $1 \leq i, j \leq m$ . In order to prove that the sum in (25.17) is direct, let us show (for example) that

$$B_1 \cap (B_2 + \cdots + B_m) = (0) .$$

Let *C* denote the above intersection. Since

$$B_1 B_j = 0, \quad B_j B_1 = 0, \quad 2 \leq j \leq m ,$$

it follows at once that

$$B_1 C = 0, \quad (B_2 + \cdots + B_m) C = 0 .$$

By (25.17), we may conclude that  $RC = 0$ , and therefore  $C = 0$ . We have thus established

$$(25.18) \quad R = B_1 \oplus \cdots \oplus B_m$$

where the  $\{B_i\}$  are subrings of *R* which annihilate each other. This also shows that  $B_1$  is not only the sum of *all* minimal left ideals isomorphic to  $L_1$ , but can also be defined as the direct sum

of those left ideals among  $L_1, \dots, L_n$  which are isomorphic to  $L_1$ .

Every two-sided ideal of any  $B_i$  is also a two-sided ideal of  $R$ . Let  $D$  be a non-zero two-sided ideal of the ring  $B_1$ , say; then  $D$  is also a left ideal in  $R$ , and so contains a minimal left ideal  $L$  of  $R$ . From

$$L \subset D \subset B_1,$$

we conclude that  $L \cong L_1$ . On the other hand

$$Lx \subset D, \quad x \in R,$$

since  $D$  is a right ideal. But by (25.12), as  $x$  ranges over all elements of  $R$ , the left ideals  $Lx$  give all minimal left ideals isomorphic to  $L$ . Therefore  $D = B_1$ , which proves that  $B_1$  contains no non-trivial two-sided ideals.

To complete the proof of the theorem, we must show that each  $B_i$  has a unity element and satisfies the minimum condition. Using (25.18), we may write

$$(25.19) \quad 1 = b_1 + \cdots + b_m, \quad b_i \in B_i,$$

and it is easily found that  $b_i$  is a unity element for  $B_i$ . Finally, left ideals of  $B_i$  are also left ideals of  $R$ , and hence satisfy the minimum condition.

(25.20) **DEFINITION.** The two-sided ideals  $B_1, \dots, B_m$  defined above are called the *simple components* of the semi-simple ring  $R$ . The number of simple components is the same as the number of non-isomorphic minimal left ideals of  $R$ . If  $L_1, \dots, L_m$  are a full set of such ideals, then  $B_i$  is just the sum of all minimal left ideals of  $R$  which are isomorphic to  $L_i$ .

We may also show, keeping the above notation

(25.21) *Any two-sided ideal  $B$  of  $R$  is a sum of a certain number of the simple components of  $R$ .*

**PROOF.** Excluding the trivial case  $B = 0$ , we see that  $B$  must contain a minimal left ideal  $L$  of  $R$ . Then also  $Lx \subset B$  for each  $x \in R$ , so that by (25.12)  $B_L \subset B$ . Let  $B'$  be the sum of all the simple components contained in  $B$ . Since  $R$  is semi-simple, every  $R$ -module is completely reducible, so that

$$B = B' \oplus B''$$

for some left ideal  $B''$  of  $R$ . If  $B'' \neq 0$ , then  $B''$  contains a minimal left ideal  $L''$ , and the above argument shows that

$$B_{L''} \subset B' ,$$

contradicting the fact that  $B' \cap B'' = 0$ . Therefore  $B'' = 0$ , and  $B$  is a (direct) sum of simple components of  $R$ .

(25.22) COROLLARY. *If the semi-simple ring  $R$  is expressed as a direct sum of two-sided ideals which are simple rings, these ideals are precisely the simple components of  $R$ .*

For the following discussion, let  $R$  be a ring with minimum condition which need not be semi-simple. Set

$$N = \text{rad } R , \quad \bar{R} = R/N .$$

Then  $\bar{R}$  is a semi-simple ring, and we may establish a one-to-one correspondence between left  $\bar{R}$ -modules  $\bar{M}$ , and left  $R$ -modules  $M$  which are annihilated by  $N$ . Indeed,  $\bar{M}$  and  $M$  have the same elements, and the actions of  $R$  and  $\bar{R}$  are related by

$$(25.23) \quad \bar{x}m = xm , \quad x \in R, m \in M ,$$

where  $\bar{x}$  is the image of  $x \in R$  under the natural map  $R \rightarrow \bar{R}$ . We use this to show

(25.24) THEOREM. *If  $M$  is an irreducible (left)  $R$ -module, then  $NM = 0$ , and the corresponding  $\bar{R}$ -module  $\bar{M}$  is an irreducible  $\bar{R}$ -module. Conversely, every irreducible  $\bar{R}$ -module  $\bar{M}$  yields an irreducible  $R$ -module  $M$ .*

PROOF. Let  $M$  be an irreducible  $R$ -module. Then  $NM$  is a submodule of  $M$ , so that either  $NM = 0$  or  $NM = M$ . The latter case cannot arise, because  $NM = M$  implies

$$M = NM = N^2M = \cdots = 0$$

since  $N$  is nilpotent. Therefore  $NM = 0$ , and so  $M$  can be viewed as  $\bar{R}$ -module  $\bar{M}$  by virtue of (25.23). Reducibility of  $\bar{M}$  would imply that of  $M$ .

The converse part of the above theorem is clear.

This result shows that, in order to obtain a full set of non-isomorphic irreducible  $R$ -modules, it is enough to find a full set of non-isomorphic minimal left ideals  $\{\bar{L}\}$  of the semi-simple ring  $\bar{R}$ , and then to make each of these into an  $R$ -module by defining  $x \cdot \bar{a} = \bar{x}\bar{a}$  for  $x \in R$  and each  $\bar{a} \in \bar{L}$ .

### Exercises

In the following exercises,  $R$  is a ring satisfying the minimum condition

and containing a unity element.

1. An idempotent  $e \in R$  is called *primitive* if it cannot be expressed as a sum of two orthogonal idempotents. If  $e$  is an idempotent in the semi-simple ring  $R$ , show that  $e$  is primitive if and only if  $Re$  is a minimal left ideal of  $R$ .

2. The *center* of a ring is the set of elements which commute with all elements of the ring. A *central idempotent* of a ring  $R$  is an idempotent in the center of  $R$ . Show that there is a one-to-one correspondence between decompositions of a ring  $R$  into a direct sum of two-sided ideals:

$$R = C_1 \oplus \cdots \oplus C_s$$

and decompositions of 1 into a sum of orthogonal central idempotents:

$$1 = c_1 + \cdots + c_s,$$

given by  $C_i = Re_i$ ,  $1 \leq i \leq s$ .

3. Let  $e$  be a central idempotent of the semi-simple ring  $R$ , and let  $B = Re$  be the two-sided ideal generated by  $e$ . Show that  $B$  is a simple component of  $R$  if and only if it is impossible to write  $e$  as a sum of two orthogonal central idempotents. Using the notation of (25.19), show that every central idempotent of  $R$  is a sum of certain of the  $\{b_i\}$ .

4. Let  $N = \text{rad } R$ , and let  $M$  be a left  $R$ -module. Prove that  $M$  is completely reducible if and only if  $NM = 0$ .

5. Let  $L$  be a left ideal of the semi-simple ring  $R$ . If  $\varphi : L \rightarrow R$  is an  $R$ -homomorphism of  $L$  into the left  $R$ -module  ${}_RR$ , show that there exists an element  $u \in R$  such that  $\varphi(x) = xu$  for all  $x \in L$ .

6. Show that a commutative simple ring must be a field (use Exercise 24.6). Therefore, a commutative semi-simple ring must be a direct sum of fields which annihilate one another.

7. Let  $B_1, \dots, B_m$  be simple rings, and define  $A = B_1 + \cdots + B_m$  (external direct sum) where addition and multiplication of  $m$ -tuples is performed by components. Prove that  $A$  is a semi-simple ring.

8. Let  $x \in R$  have the property that  $xM = 0$  for every irreducible left  $R$ -module  $M$ . Prove that  $x \in \text{rad } R$ . [Hint: Since  $R/\text{rad } R$  can be expressed as a direct sum of irreducible left  $R$ -modules, it follows that  $x(R/\text{rad } R) = 0$  and therefore that  $x \in \text{rad } R$ .] This exercise combined with (25.24) yields the important characterization of  $\text{rad } R$  as the set of all elements  $x \in R$  such that  $xM = 0$  for every irreducible  $R$ -module  $M$ .

9. Prove that  $\text{rad } R$  is the intersection of all maximal left ideals of  $R$ . [Hint: By Exercise 24.4, every maximal left ideal of  $R$  contains  $\text{rad } R$ . On the other hand, let  $x$  belong to the intersection of all maximal left ideals of  $R$ , and let  $M$  be an irreducible left  $R$ -module. Let  $m \in M$ ,  $m \neq 0$ ; then  $M = Rm$ , and  $a \mapsto am$ ,  $a \in R$ , is an  $R$ -homomorphism of  ${}_RR$  onto  $M$  whose kernel is a maximal left ideal. Therefore  $xm = 0$ , and it follows that  $xM = 0$ . Now use Exercise 25.8.]

10. Let  $Re$  be a minimal left ideal of the semi-simple ring  $R$ , where  $e$  is idempotent, and let  $M$  be any irreducible  $R$ -module. Prove that  $M \cong Re$  if

and only if  $eM \neq 0$ .

### § 26. The Structure of Simple Rings

A ring with unity element satisfying the minimum condition was called *semi-simple* if it contained no non-zero nilpotent left ideals, and *simple* if it contained no non-trivial two-sided ideals. In the preceding section, we showed that every semi-simple ring is expressible as a direct sum of a finite number of simple subrings which are at the same time two-sided ideals. We are now faced with the problem of determining all simple rings, and shall begin by investigating a special type of simple ring which will turn out to be the prototype for all simple rings.

Let  $D$  be a skewfield (that is, division ring), and let  $M$  be a right  $D$ -module with a finite basis  $\{m_1, \dots, m_n\}$ . We shall refer to  $M$  as an *n-dimensional right vector space* over  $D$ . Most of the results on vector spaces over fields carry over unchanged to the more general situation of vector spaces over skewfields (see van der Waerden, *Modern Algebra I*, section 33), and we shall use them freely when necessary.

Set

$$R = \text{Hom}_D(M, M) ;$$

then  $R$  is the set of all homomorphisms  $f: M \rightarrow M$  for which

$$f(m\alpha) = f(m)\alpha, \quad m \in M, \alpha \in D.$$

As in the case of vector spaces over fields,  $R$  can be made into a ring by defining for  $f, g \in R$ :

$$(f + g): m \rightarrow f(m) + g(m), \quad (fg): m \rightarrow f(g(m)), \quad m \in M.$$

For each  $f \in R$ , we may write

$$(26.1) \quad f(m_i) = \sum_{i=1}^n m_i \alpha_{ij}, \quad \alpha_{ij} \in D.$$

Let  $\mathbf{F} = (\alpha_{ij})$  be the matrix whose  $(i, j)$ -entry is  $\alpha_{ij}$ . If  $D_n$  denotes the ring of all  $n \times n$  matrices with entries in  $D$ , the map  $f \rightarrow \mathbf{F}$  gives a one-to-one mapping of  $R$  into  $D_n$ . Indeed  $R$  is mapped onto  $D_n$ , since, starting with an arbitrary  $(\alpha_{ij}) \in D_n$ , equation (26.1) serves to define an element  $f \in R$  for which  $\mathbf{F} = (\alpha_{ij})$ . If  $g \in R$  maps onto  $G = (\beta_{ij}) \in D_n$ , then

$$(f+g)(m_j) = \sum m_i(\alpha_{ij} + \beta_{ij}),$$

$$(fg)(m_j) = f\{\sum m_k\beta_{kj}\} = \sum f(m_k)\beta_{kj} = \sum m_i\alpha_{ik}\beta_{kj}.$$

These show that  $f+g \rightarrow F+G$ ,  $fg \rightarrow FG$ , so that the map  $f \rightarrow F$  gives a ring isomorphism

$$R = \text{Hom}_D(M, M) \cong D_n.$$

We may note further that this isomorphism permits us to turn  $M$  into a left  $D_n$ -module by defining

$$F(m) = f(m), \quad m \in M,$$

where  $F \hookrightarrow f$ .

We shall now show that  $D_n$  is a simple ring. To begin with, we make  $D_n$  into a left  $D$ -module by setting

$$\beta(\alpha_{ij}) = (\beta\alpha_{ij}), \quad \beta \in D.$$

Since the identity matrix of  $D_n$  is its unity element, it follows that every left ideal of  $D_n$  is also a  $D$ -subspace of  $D_n$ . If  $e_{ij}$  denotes the matrix with 1 at position  $(i, j)$  and zeros elsewhere, the elements

$$\{e_{ij} : 1 \leq i, j \leq n\}$$

form a left  $D$ -basis for  $D_n$ , and so the left dimension  $(D_n : D) = n^2$ . Consequently the left ideals of  $D_n$  satisfy the minimum condition. We note also that the basis elements  $\{e_{ij}\}$  of  $D_n$  multiply according to the rules

$$e_{ij}e_{jk} = e_{ik}, \quad e_{ij}e_{lk} = 0, \quad l \neq j.$$

We observe next that  $D_n e_{ii}$  is a left ideal of  $D_n$ , consisting of all matrices with arbitrary  $i$ th column and zeros elsewhere. Therefore

$$(26.2) \quad D_n = D_n e_{11} \oplus \cdots \oplus D_n e_{nn}$$

gives a decomposition of  $D_n$  into left ideals  $\{D_n e_{ii}\}$ . For each  $i$ , we may see that  $D_n e_{ii}$  is a minimal left ideal in  $D_n$ . Indeed, if  $L$  is a non-zero left ideal of  $D_n$  contained in  $D_n e_{ii}$ , choose  $l \in L$ ,  $l \neq 0$ . Then  $l$  has a nonzero entry in its  $i$ th column. From  $D_n l \subset L$  it follows easily that  $L$  contains all matrices with arbitrary  $i$ th column and zeros elsewhere so  $L = D_n e_{ii}$ . Finally, to show that  $D_n$  is simple we need only prove that for each  $i$  and  $j$ ,

$$(26.3) \quad D_n e_{ii} \cong D_n e_{jj}$$

as left  $D_n$ -modules. By (25.13), this will be the case if

$$e_{jj}D_ne_{ii} \neq (0) ,$$

and this is valid because

$$e_{ji} = e_{jj}e_{ji}e_{ii} \in e_{jj}D_ne_{ii} .$$

This completes the proof that  $D_n$  is a simple ring.

Now we come to the basic structure theorem for simple rings.

(26.4) THEOREM (*Wedderburn*). *Let  $A$  be a simple ring with minimum condition. Then  $A \cong \text{Hom}_D(M, M)$  for some finite-dimensional right vector space  $M$  over a skewfield  $D$ . The dimension  $(M:D)$  and the skewfield  $D$  are uniquely determined by  $A$ .*

*Proof.* Let  $M = Ae$  be a fixed minimal left ideal in  $A$ , and let  $A_L$  be the ring of endomorphisms of  $M$  consisting of all left multiplications  $a_L: m \rightarrow am$ ,  $m \in M$ . The map  $a \rightarrow a_L$  is a homomorphism of  $A$  onto  $A_L$ , whose kernel is a two-sided ideal in  $A$ . Since  $A$  is simple and  $A_L \neq 0$ , the kernel is  $(0)$ , and  $A \cong A_L$ .

The next step is to observe that  $M$  is an irreducible left  $A$ -module; hence by Schur's lemma (Exercise 13.7; see also (27.3))  $D = \text{Hom}_A(M, M)$  is a skewfield. Let us write the elements  $\delta \in D$  as right operators on  $M$ ; then  $M$  is a right vector space over  $D$ , and for every  $a_L \in A_L$ , we have

$$a_L(m\delta) = (a_Lm)\delta , \quad m \in M, \delta \in D .$$

Therefore  $A_L \subset \text{Hom}_D(M, M)$ , and we shall prove that  $A_L = \text{Hom}_D(M, M)$ .

From the many ways of proving this result, we choose a method due essentially to Brauer (see Weyl [2], p. 91). His procedure contains the leading ideas of another theorem as well, which we shall consider in Chapter VIII.

The general situation is this. We have a ring  $A$ , a left  $A$ -module  $M$ , and the ring  $A_L$  of endomorphisms of  $M$ . Let  $D = \text{Hom}_A(M, M)$ , regarded as a ring of right operators on  $M$ . We have, in general, the inclusion  $A_L \subset \text{Hom}_D(M, M)$ . Whenever  $A_L = \text{Hom}_D(M, M)$ , we say that the pair  $(A, M)$  has the *double centralizer property*.

The main assertion of Wedderburn's theorem is that  $(A, M)$  has the double centralizer property, where  $M$  is a minimal left ideal in the simple ring  $A$ . By Theorem 25.15, the direct sum  $V = M + \cdots + M$  of a certain number of copies of  $M$  is  $A$ -isomorphic to the left regular module  ${}_AA$ . We have for this latter module the

following result:

(26.5) LEMMA. *Let  $A$  be a ring with 1. Then the pair  $(A, {}_A A)$  has the double centralizer property.*

PROOF. Let  $\delta \in D = \text{Hom}_A({}_A A, {}_A A)$ , and let  $d = 1\delta$ , that is, the image of 1 under the map  $\delta$ . Then for all  $a \in A$ , since  $\delta \in D$  we have

$$a\delta = (a1)\delta = a(1\delta) = ad,$$

and thus  $\delta$  is the right multiplication  $d_R$ . The associative law shows that every right multiplication is in  $D$ , and we have proved that  $D = A_R$ . Similarly,  $\text{Hom}_D({}_A A, {}_A A) = A_L$ , and the lemma is proved.

The fact that the pair  $(A, M)$  has the double centralizer property is now an immediate consequence of the next lemma.

(26.6) LEMMA. *Let  $V = M + \cdots + M$  be the external direct sum of  $k$  copies of a left  $A$ -module  $M$ , for some positive integer  $k$ . If  $(A, V)$  has the double centralizer property, then  $(A, M)$  also has the double centralizer property.*

PROOF. The elements of  $V$  are  $k$ -tuples  $v = (m_1, \dots, m_k)$ ,  $m_i \in M$ . Let  $D = \text{Hom}_A(M, M)$ , and let  $f \in \text{Hom}_D(M, M)$ . Define an endomorphism  $f^*$  of  $V$  by setting

$$f^*v = (fm_1, \dots, fm_k), \quad v = (m_1, \dots, m_k) \in V.$$

Now let  $\theta \in D^* = \text{Hom}_A(V, V)$ , and write  $v = (m_1, \dots, m_k) = v_1 + \cdots + v_k$  where  $v_i = (0, \dots, 0, m_i, 0, \dots, 0)$ . Write  $v_i\theta = (v_{i1}, \dots, v_{ik})$ ,  $v_{ij} \in M$ , and note that the map  $m_i \rightarrow v_{ij}$  is a well-defined additive map of  $M$  into  $M$  which we shall denote by  $\theta_{ij}$ ,  $1 \leq i, j \leq k$ . Then we have for  $1 \leq i \leq k$ ,

$$v_i\theta = (0, \dots, 0, m_i, 0, \dots, 0)\theta = (m_i\theta_{i1}, \dots, m_i\theta_{ik}).$$

For  $a \in A$ , we have  $(av_i)\theta = a(v_i\theta)$  since  $\theta \in D^* = \text{Hom}_A(V, V)$ . This implies that, for all  $m \in M$  and each  $j$ ,  $1 \leq j \leq k$ ,  $(am)\theta_{ij} = a(m\theta_{ij})$ , and hence each  $\theta_{ij} \in \text{Hom}_A(M, M) = D$ . Since  $f \in \text{Hom}_D(M, M)$ , we have for each  $i$ ,  $1 \leq i \leq k$ ,

$$\begin{aligned} (f^*v_i)\theta &= (0, \dots, 0, fm_i, 0, \dots, 0)\theta = ((fm_i)\theta_{i1}, \dots, (fm_i)\theta_{ik}) \\ &= (f(m_i\theta_{i1}), \dots, f(m_i\theta_{ik})) = f^*(v_i\theta). \end{aligned}$$

Since  $v = \sum v_i$ , it follows that  $f^* \in \text{Hom}_D(V, V)$ . By hypothesis  $(A, V)$  has the double centralizer property, and so there exists an  $a \in A$  such that

$$f^*(m_1, \dots, m_k) = (am_1, \dots, am_k), \quad m_i \in M.$$

But  $f^*(m_1, \dots, m_k)$  is also equal to  $(fm_1, \dots, fm_k)$ , and therefore we obtain  $fm = am$  for all  $m \in M$ . Thus  $\text{Hom}_D(M, M) \subset A_L$ , and since the reverse inclusion holds in general, the proof of the lemma is completed.

Now we can finish the proof of the first part of Wedderburn's theorem. We know that for a certain positive integer  $k$ , the direct sum  $V$  of  $k$  copies of  $M$  is isomorphic to the left regular module  $A$ . By Lemma 26.5,  $(A, V)$  has the double centralizer property, and so, by Lemma 26.6,  $(A, M)$  has the double centralizer property. Therefore  $A \cong \text{Hom}_D(M, M)$ , where  $D$  is a skewfield.

Let us show next that  $M$  is a finite-dimensional right vector space over  $D$ . If not, then there exist elements  $\{m_1, m_2, \dots\}$  in  $M$  such that for each positive integer  $t$ ,  $\{m_1, \dots, m_t\}$  are linearly independent over  $D$ . For each  $t$ , define

$$I_t = \{a \in A : am_1 = \dots = am_t = 0\}.$$

Then  $I_t$  is a left ideal in  $A$ , and we have

$$I_1 \supset I_2 \supset I_3 \supset \dots.$$

We show that the inclusions are proper. To settle this point, we use some basic facts concerning infinite-dimensional vector spaces, namely that the linearly independent set  $\{m_1, m_2, \dots\}$  can be supplemented to give a basis of  $M$  over  $D$  (see Jacobson [2], p. 239), and that a linear transformation can be defined arbitrarily on a basis. It follows that we can define linear transformations on  $M$  which map  $\{m_1, m_2, \dots\}$  onto arbitrary vectors in  $M$ . Since the left multiplications by elements of  $A$  yield all linear transformations of  $M$  over  $D$ , for each  $t$  there exists  $a_t \in A$  such that  $a_t \in I_t$ ,  $a_t \notin I_{t+1}$ . Thus the inclusions are proper, and we have shown that if  $M$  is infinite dimensional, the assumption that  $A$  satisfies the minimum condition is contradicted. Therefore the dimension  $(M:D)$  is finite.

Finally we come to the uniqueness assertion. We prove first the following lemma, which is a generalization of the proof of (26.5):

(26.7) LEMMA. *Let  $M = Ae$ ,  $e^2 = e$ , be a left ideal in a ring  $A$  with minimum condition, and let  $D = \text{Hom}_A(M, M)$ , viewed as a ring of right operators on  $M$ . Then there exists an isomorphism  $f: D \cong eAe$  such that  $m\delta = mf(\delta)$  for all  $m \in M$ ,  $\delta \in D$ .*

PROOF. Let  $\delta \in D$ , and define  $f(\delta) = e\delta \in Ae$ . Then  $ef(\delta) = e(e\delta) = e\delta = f(\delta)$  so that  $f(\delta) \in eAe$ . The map  $f: D \rightarrow eAe$  has the further properties that

$$f(\delta + \delta') = f(\delta) + f(\delta'), \quad f(\delta\delta') = f(\delta) \cdot f(\delta').$$

If  $f(\delta) = 0$  then  $e\delta = 0$ , and for all  $a \in Ae$ ,  $a\delta = (ae)\delta = a(e\delta) = 0$  so that  $\delta = 0$  in  $D$ . Therefore  $f$  is a ring isomorphism of  $D$  into  $eAe$ . Finally let  $x \in eAe$ , and define  $\delta \in \text{Hom}_A(M, M)$  by setting  $m\delta = mx$ ,  $m \in M$ . Then  $f(\delta) = e\delta = ex = x$ , and the mapping is onto. This completes the proof of the lemma.

We summarize what has been proved so far in this section as follows:

(26.8) *Let  $A$  be a simple ring with minimum condition, and let  $Ae$  be a minimal left ideal in  $A$  generated by a primitive idempotent  $e$ . Then  $D = \text{Hom}_A(Ae, Ae)$  is a skewfield isomorphic to  $eAe$ , and the action of  $D$  upon  $Ae$  is the same as right multiplication by  $eAe$ . The right vector space  $Ae$  over  $eAe$  is finite dimensional, and if  $n = (Ae : eAe)$ , then*

$$A \cong \text{Hom}_{eAe}(Ae, Ae) \cong D_n.$$

*The dimension  $n$  can be characterized as the number of minimal left ideals appearing in a direct decomposition of  $A$ .*

The uniqueness part of Wedderburn's theorem follows easily from (26.8). If also  $A \cong A_m$  where  $A$  is a skewfield, then  $m$  is the number of minimal left ideals in a direct sum decomposition of  $A_m$ , whence  $m = n$ . Further, if  $\delta \in A_m$  is the matrix with 1 at the  $(1, 1)$  position and zeros elsewhere, then  $\delta$  is idempotent, and  $A_m\delta$  is a minimal left ideal of  $A_m$ . However, we have shown that  $\delta A_m\delta \cong A$ , and therefore  $A \cong D$ , since  $eAe \cong fAf$  for all primitive idempotents  $e$  and  $f$  in  $A$ .

### Exercises

1. Let  $M$  be a non-zero left  $A$ -module where  $A$  is a semi-simple ring. Prove that  $(A, M)$  has the double centralizer property. [Hint: See Lemma 59.4.]
2. A left  $A$ -module  $M$  is called *faithful* if  $aM = 0$ ,  $a \in A$ , implies  $a = 0$ . Prove that every simple ring has a faithful irreducible module. Further, if a ring  $A$  with unity, satisfying the minimum condition, has a faithful irreducible module, then  $A$  is simple.
3. Let  $M$  be a faithful left  $A$ -module, and let  $D = \text{Hom}_A(M, M)$  regarded as a ring of right operators on  $M$ . Prove that the map  $a \rightarrow a_L$  maps  $A$  isomorphically onto  $A_L \subset \text{Hom}_D(M, M)$ .
4. Keeping the notation of Exercise 26.3, set  $B = \text{Hom}_D(M, M)$  regarded as a ring of left operators on  $M$ . Prove that  $\text{Hom}_B(M, M) = D$ .
5. Let  $A$  be a semi-simple ring, and let  $M$  be an irreducible left  $A$ -module. The map  $\theta: a \rightarrow a_L$  maps  $A$  homomorphically into  $\text{Hom}(M, M)$ , and

the kernel of the map is the sum of those simple components  $B_{M'}$  of  $A$  which come from ideals  $M'$  not isomorphic to  $M$ . Further, let  $M = Ae$  where  $e$  is idempotent, and set  $D = \text{Hom}_A(M, M)$ . Then show that

$$\begin{aligned}\theta(A) &\cong \text{simple component } B_M \text{ of } A \\ &\cong \text{Hom}_D(M, M).\end{aligned}$$

6. Let  $A$  be a ring with 1 and satisfying the mininum condition, and let  $N = \text{rad } A$ . Let  $M$  be an irreducible  $A$ -module and let  $\theta: a \rightarrow a_L$  where

$$a_L: m \rightarrow am, \quad m \in M.$$

Then we may take for  $M$  a minimal left ideal in  $A/N$ , and the image  $\theta(A)$  is isomorphic to that simple component of  $A/N$  which contains  $M$ .

7. Let  $T \in K_n$ , where  $K$  is a field. The map  $K[x] \rightarrow K[T]$  maps the ring  $K[x]$  onto  $K[T]$ , and its kernel is an ideal in  $K[x]$ . This ideal is principal, generated by a monic polynomial  $f(x)$ , called the *minimum polynomial* of  $T$ . Therefore

$$K[T] \cong K[x]/(f(x)).$$

Let

$$f(x) = \prod_{i=1}^m (f_i(x))^{e_i}$$

be the factorization of  $f(x)$  into powers of distinct irreducible polynomials. Using Exercise 24.7, show that (i)  $K[T]$  is semi-simple if and only if each  $e_i = 1$  and (ii)  $K[T]$  is simple if and only if  $f(x)$  is irreducible.

## § 27. Theorems of Burnside, Frobenius, and Schur

In this section, we shall apply the theory of semi-simple rings to obtain some results concerning group representations. For the first few paragraphs, however, we find it more convenient to adopt a slightly more general viewpoint.

Throughout this section, let  $K$  be a field and  $A$  an algebra over  $K$  with unity element  $1_A$ , but we do not assume  $(A:K)$  finite. Let  $M$  be a left  $A$ -module, which we make into a vector space over  $K$  by defining

$$(27.1) \quad \alpha \cdot m = (\alpha 1_A)m, \quad \alpha \in K, m \in M,$$

and assume that  $(M:K)$  is finite. For each  $a \in A$ , we let

$$a_L: m \rightarrow am, \quad m \in M.$$

Then

$$a_L \in \text{Hom}_K(M, M),$$

and the map  $a \rightarrow a_L$  maps the algebra  $A$  homomorphically onto

$$A_L = \{a_L : a \in A\}.$$

Note that  $A_L$  is a subalgebra of  $\text{Hom}_K(M, M)$  since  $A_L$  contains in its center all the scalar multiplications of  $M$  by elements of  $K$ . We observe at once that  $M$  can also be viewed as a left  $A_L$ -module, and that the subspaces of  $M$  which are  $A$ -submodules are precisely the same as the subspaces which are  $A_L$ -submodules. The advantages of working with  $A_L$  instead of  $A$  are twofold:

(i)  $A_L$  is a finite-dimensional algebra over  $K$ , and indeed

$$(A_L : K) \leq (M : K)^2.$$

(ii)  $M$  is a *faithful*  $A_L$ -module; that is, a non-zero element in  $A_L$  cannot annihilate every element of  $M$ . (This is true because the elements of  $A_L$  are linear transformations on  $M$  and only the zero linear transformation annihilates all of  $M$ .)

Let us remark that  $A \cong A_L$  if and only if  $M$  is a faithful  $A$ -module.

Now consider

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

Each  $f \in D$  is a homomorphism  $f: M \rightarrow M$  such that

$$f(am) = af(m), \quad a \in A, m \in M.$$

In particular, letting  $a = \alpha 1_A$ ,  $\alpha \in K$ , and using (27.1), we get

$$f(\alpha m) = \alpha f(m), \quad m \in M.$$

This shows that  $f \in \text{Hom}_K(M, M)$ , and so

$$D = \text{Hom}_A(M, M) \subset \text{Hom}_K(M, M).$$

Furthermore,  $D$  contains all scalar multiplications of  $M$  by elements of  $K$ ; hence  $D$  is also a subalgebra of  $\text{Hom}_K(M, M)$ , and

$$(D : K) \leq (M : K)^2.$$

We note finally that

$$\text{Hom}_A(M, M) = \text{Hom}_{A_L}(M, M).$$

(27.2) DEFINITION. Let  $D$  be a skewfield and  $K$  a field. We call  $D$  a *division algebra* over  $K$  if  $K$  is a subfield of the center of  $D$ , that is,

$$\alpha d = d\alpha \quad \text{for all } \alpha \in K, d \in D.$$

Consequently, an algebra over  $K$  is a division algebra if and

only if each non-zero element of the algebra has a two-sided inverse with respect to multiplication. Note that we do not require  $(D:K)$  to be finite.

Suppose now that  $M$  is an irreducible  $A$ -module and hence also an irreducible  $A_L$ -module. Since  $M$  is a faithful  $A_L$ -module, it follows from Exercise 26.2 that  $A_L$  must be a simple ring and  $M$  is isomorphic (as an  $A_L$ -module) to a minimal left ideal  $A_L e$  of  $A_L$ , where  $e$  is an idempotent in  $A_L$ . In the proof of Theorem 26.4 we showed that

$$D = \text{Hom}_{A_L}(M, M) \cong eA_L e$$

and that  $eA_L e$  is a skewfield. (See also Schur's lemma, Exercise 13.7.) Hence  $D$  is a finite-dimensional division algebra over  $K$ , and we have proved in Theorem 26.4 that

$$A_L = \text{Hom}_D(M, M).$$

The following results are basic for the theory of group representations:

(27.3) SCHUR'S LEMMA. *Let  $A$  be a finite-dimensional algebra over an algebraically closed field  $K$ , and let  $M$  and  $N$  be irreducible left  $A$ -modules. Then  $\text{Hom}_A(M, N) = (0)$  if  $M$  and  $N$  are not isomorphic, whereas  $\text{Hom}_A(M, M) = K \cdot 1_M$  (where  $1_M$  is the identity map on  $M$ ). In terms of matrix representations, let  $T$  and  $U$  be irreducible matrix representations of  $A$ , and let  $S$  be a matrix such that*

$$T(a)S = SU(a), \quad a \in A.$$

*Then  $S = 0$  if  $T$  and  $U$  are inequivalent, and  $S = \xi \cdot I$  for some  $\xi \in K$  if  $T = U$ .*

PROOF. First let  $f \in \text{Hom}_A(M, N)$  where  $M$  and  $N$  are inequivalent. If  $f \neq 0$ , then because  $M$  and  $N$  are irreducible, it follows that  $f$  is an  $A$ -isomorphism of  $M$  onto  $N$ , contrary to our assumption.

Now let  $D = \text{Hom}_A(M, M)$ , and let  $d \in D$ . The elements  $1, d, d^2, \dots$  cannot all be linearly independent over  $K$ ; hence there exists a non-zero monic polynomial  $f(x) \in K[x]$  such that  $f(d) = 0$ . Since  $K$  is algebraically closed, there exist elements  $\alpha_1, \dots, \alpha_m \in K$  such that

$$f(x) = (x - \alpha_1) \cdots (x - \alpha_m).$$

But then

$$0 = f(d) = (d - \alpha_1) \cdots (d - \alpha_m)$$

since  $d$  commutes with all the elements of  $K$ . Because  $D$  is a skew-

field, the last equation implies that some  $d - \alpha_i = 0$ , so  $d \in K$ .

The results for matrix representations are immediate corollaries of the results on modules we have just proved. This completes the proof of Schur's lemma.

(27.4) **BURNSIDE'S THEOREM** (*Burnside [4]*). *Let  $A$  be an algebra over an algebraically closed field  $K$ , and let  $M$  be an irreducible left  $A$ -module. Then*

$$A_L = \text{Hom}_K(M, M).$$

**PROOF.** By Schur's lemma, we have,

$$D = \text{Hom}_A(M, M) = K \cdot 1_M.$$

By Theorem 26.4, it follows that

$$A_L = \text{Hom}_D(M, M) = \text{Hom}_K(M, M),$$

and the theorem is proved.

(27.5) **REMARK.** Keeping the above notation, let us fix a  $K$ -basis  $B$  of  $M$ . Relative to this basis,  $M$  affords a matrix representation  $\mathbf{T}$  of  $A$ , and in fact  $\mathbf{T}(a)$  is just the matrix of the linear transformation  $a_L$  relative to the basis  $B$ . Thus  $a_L \rightarrow \mathbf{T}(a)$  gives an isomorphism of  $A_L$  into an algebra of matrices. Theorem 27.4 states that if we set  $n = (M : K)$ , then there corresponds to each matrix  $X \in K^n$  an element  $a \in A$  such that

$$\mathbf{T}(a) = X.$$

Let us set

$$\mathbf{T}(a) = (f_{ij}(a))_{1 \leq i, j \leq n}, \quad a \in A.$$

Then each  $f_{ij}$  is a  $K$ -homomorphism of  $A$  into  $K$ . We shall call  $\{f_{ij} : 1 \leq i, j \leq n\}$  the *coordinate functions* of the matrix representation  $\mathbf{T}$ .

(27.6) **DEFINITION.** A set of functions  $\{g_1, \dots, g_m\}$  from  $A$  to  $K$  is called *linearly dependent* over  $K$  if there exist scalars  $\alpha_1, \dots, \alpha_m \in K$ , not all zero, such that

$$(27.7) \quad \alpha_1 g_1(a) + \dots + \alpha_m g_m(a) = 0 \quad \text{for all } a \in A.$$

On the other hand, if (27.7) implies that each  $\alpha_i = 0$ , we call  $\{g_1, \dots, g_m\}$  *linearly independent over  $K$* .

We are now ready to prove what may be regarded as a generalization of Burnside's theorem 27.4.

(27.8) THEOREM (*Frobenius and Schur* [2]). *Let  $K$  be algebraically closed,  $A$  an algebra over  $K$ , and  $M_1, \dots, M_k$  a set of pairwise non-isomorphic irreducible left  $A$ -modules, with  $(M_r : K) = n_r$ ,  $1 \leq r \leq k$ . For each  $r$ , let  $M_r$  afford a matrix representation  $T_r$  of  $A$  with coordinate functions  $\{f_{ij}^{(r)} : 1 \leq i, j \leq n_r\}$ . Then the set*

$$(27.9) \quad \{f_{ij}^{(r)} : 1 \leq i, j \leq n_r, 1 \leq r \leq k\}$$

*of all coordinate functions is linearly independent over  $K$ .*

PROOF. Setting

$$M = M_1 + \cdots + M_k,$$

we obtain a completely reducible left  $A$ -module  $M$ . The map  $a \rightarrow a_L$  maps  $A$  homomorphically onto a subalgebra  $A_L$  of  $\text{Hom}_K(M, M)$  and makes  $M$  into a left  $A_L$ -module. Since  $AM_r \subset M_r$ , we have  $A_L M_r \subset M_r$ , from which we deduce at once that each  $M_r$  is an irreducible left  $A_L$ -module. Furthermore,  $M_1, \dots, M_k$  are a set of pairwise non-isomorphic  $A_L$ -modules.

Next we observe that from  $A_L M_r \subset M_r$ , we obtain an embedding

$$A_L \rightarrow \text{Hom}_K(M_1, M_1) + \cdots + \text{Hom}_K(M_k, M_k).$$

We shall now show that indeed

$$(27.10) \quad A_L \cong \text{Hom}_K(M_1, M_1) + \cdots + \text{Hom}_K(M_k, M_k);$$

that is, given any elements  $\lambda_1, \dots, \lambda_k$  with  $\lambda_r \in \text{Hom}_K(M_r, M_r)$ ,  $1 \leq r \leq k$ , there exists an  $a_L \in A_L$  such that

$$a_L | M_r = \lambda_r, \quad 1 \leq r \leq k.$$

In order to establish (27.10), we note first that  $M$  is a completely reducible  $A_L$ -module; hence, by Exercise 25.4,  $\text{rad } A_L$  annihilates  $M$ . But  $M$  is a faithful  $A_L$ -module, and so  $\text{rad } A_L = 0$  and  $A_L$  is a semi-simple ring. However, over a semi-simple ring a module which is a direct sum of non-isomorphic irreducible modules is faithful if and only if the summands constitute a *full* set of non-isomorphic modules. Thus there are precisely  $k$  non-isomorphic minimal left ideals in  $A_L$ , and these are  $A_L$ -isomorphic to  $M_1, \dots, M_k$ , respectively. Furthermore, there are  $k$  simple components of  $A_L$ , and for each  $r$ , the simple component corresponding to  $M_r$  is isomorphic to  $\text{Hom}_K(M_r, M_r)$  [by (27.4)]. Therefore

$$A_L \cong \sum_{r=1}^k \text{Hom}_K(M_r, M_r),$$

which proves (27.10).

To complete the proof of our theorem, let us suppose we have a relation

$$(27.11) \quad \sum_{r=1}^k \sum_{i,j=1}^{n_r} \alpha_{ij}^{(r)} f_{ij}^{(r)}(a) = 0 \quad \text{for all } a \in A.$$

Let us fix  $i$ ,  $j$ , and  $r$ , and choose matrices  $X_1, \dots, X_k$  such that  $X_s = 0$  for  $s \neq r$  and  $X_r$  consists entirely of zeros except for 1 at position  $(i,j)$ . Then (27.5) and (27.10) imply the existence of an element  $a \in A$  such that

$$(27.12) \quad T_1(a) = X_1, \dots, T_k(a) = X_k.$$

Substituting this  $a$  into (27.11), we conclude from (27.12) that

$$\alpha_{ij}^{(r)} = 0.$$

But this shows that each coefficient  $\alpha_{ij}^{(r)}$  in (27.11) is zero, and so the functions given in (27.9) are linearly independent over  $K$ .

(27.13) COROLLARY. *Let  $G$  be a group (not necessarily finite), and let  $K$  be an algebraically closed field. Suppose  $T_1, \dots, T_k$  are inequivalent irreducible matrix representations of  $G$  in  $K$ , and let*

$$T_r(g) = (f_{ij}^{(r)}(g))_{1 \leq i, j \leq n_r}, \quad g \in G.$$

*Then the coordinate functions*

$$\{f_{ij}^{(r)} : 1 \leq i, j \leq n_r, 1 \leq r \leq k\}$$

*are linearly independent over  $K$ ; that is,*

$$(27.14) \quad \sum_{i,j,r} \alpha_{ij}^{(r)} f_{ij}^{(r)}(g) = 0 \quad \text{for all } g \in G$$

*implies that each  $\alpha_{ij}^{(r)} = 0$ .*

PROOF. Let us set  $A = KG$ , the group algebra of  $G$  over  $K$ . Each representation  $T_r$  can be extended by linearity to a representation of  $A$ . The hypothesis implies that the representation spaces which afford  $T_1, \dots, T_k$  are irreducible pairwise non-isomorphic  $A$ -modules. The coordinate functions defined above as maps from  $G$  into  $K$  can also be extended by linearity to maps of  $A$  into  $K$ . But then (27.14) implies (27.11), and so by the theorem just proved each  $\alpha_{ij}^{(r)} = 0$ .

(27.15) REMARK. The proof of the preceding corollary holds not only when  $G$  is a group but also when  $G$  is a multiplicative semi-

group, that is, a system closed under multiplication for which the associative law holds and which contains an identity element. Thus the above corollary is still valid when  $G$  is a (possibly infinite) semi-group.

We turn our attention to obtaining some important consequences of the preceding results.

Let us start with a semi-simple algebra which is a finite-dimensional vector space over a field  $K$ . Then all left, right, and two-sided ideals of  $A$  are  $K$ -subspaces of  $A$ . In particular, let  $M_1, \dots, M_n$  be a full set of non-isomorphic minimal left ideals of  $A$ ; each  $M_i$  is then a finite-dimensional vector space over  $K$ . Set

$$D^{(i)} = \text{Hom}_A(M_i, M_i),$$

a finite-dimensional division algebra over  $K$ . If  $A_i$  denotes the simple component of  $A$  which contains  $M_i$ , then  $M_i$  is a faithful irreducible  $A_i$ -module, and

$$A_i \cong \text{Hom}_{D^{(i)}}(M_i, M_i).$$

Let us define  $u_i = (M_i : D^{(i)})$ ; the above shows that

$$A_i \cong D_{u_i}^{(i)},$$

a full matrix ring over the division algebra  $D^{(i)}$ . Furthermore, it follows from the proof of Wedderburn's theorem, and also from the discussion at the beginning of § 26, that  $A_i$  is a direct sum of  $u_i$  copies of  $M_i$ . Thus we have

$$(27.16) \quad A = A_1 \oplus \cdots \oplus A_n, \quad A_i \cong D_{u_i}^{(i)},$$

and  $M_i$  may be taken to be a minimal left ideal in the simple ring  $A_i$ .

We shall equate the  $K$ -dimensions of both sides of (27.16) and begin by calculating  $(D_u : K)$ . We have already remarked (see Exercise 12.6) that

$$D_u \cong D \otimes_K K_u, \quad (D_u : K) = (D : K)u^2.$$

Therefore

$$(27.17) \quad (A : K) = \sum_{i=1}^n u_i^2 (D^{(i)} : K).$$

Suppose for the remainder of this section that  $K$  is algebraically closed. From (27.3) it follows that each  $D^{(i)}$  above coincides with  $K$ , so that for this case we have

$$(27.18) \quad A = A_1 \oplus \cdots \oplus A_n, \quad A_i \cong K_{u_i}, \quad u_i = (M_i : K),$$

and

$$(27.19) \quad (A : K) = \sum_{i=1}^n u_i^2.$$

Furthermore,  $M_i$  occurs with multiplicity  $u_i = (M_i : K)$  in the decomposition of  $A$  into a direct sum of minimal left ideals.

Now let  $G$  be a finite group of order  $[G : 1]$ , and suppose  $K$  is algebraically closed and

$$\text{char } K \nmid [G : 1].$$

By Maschke's theorem (15.6) and (25.8), we conclude that the group algebra  $KG$  is semi-simple. If  $M_1, \dots, M_n$  are a full set of non-isomorphic irreducible  $KG$ -modules, we have

$$(27.20) \quad KG = A_1 \oplus \cdots \oplus A_n, \quad \{A_i\} = \text{simple components of } KG, \text{ and}$$

$$A_i \cong K_{u_i}, \quad u_i = (M_i : K).$$

Further,  $KG$  contains  $u_i$  copies of  $M_i$  in its decomposition into minimal left ideals. From (27.19), we then deduce

$$(27.21) \quad [G : 1] = \sum_{i=1}^n u_i^2$$

since  $KG$  has  $K$ -dimension  $[G : 1]$ .

On the other hand, we may view (27.20) as giving a method for obtaining a full set of non-isomorphic irreducible  $KG$ -modules, or equivalently, a full set of inequivalent irreducible matrix representations of  $G$  in  $K$ . Namely, we have only to find a full set of non-isomorphic minimal left ideals in the group algebra  $KG$ ; these are the desired  $KG$ -modules, and the matrix representations they afford are the desired  $K$ -representations of  $G$ .

One test for determining whether a set of inequivalent irreducible representations of  $G$  in  $K$  is a complete set is given by (27.21), namely, such a set is complete if and only if the sum of the squares of the dimensions equals the order of  $G$ .

We cannot give any straightforward general method for obtaining the minimal left ideals of the group algebra  $KG$ . We can, however, give an intrinsic determination of the number  $n$  of inequivalent irreducible  $K$ -representations of  $G$ . This formula is given by the following striking result:

(27.22) THEOREM. *Let  $G$  be a finite group, and  $K$  an algebraically closed field such that  $\text{char } K \nmid [G : 1]$ . Then the number of*

*non-isomorphic irreducible  $KG$ -modules is the same as the number of conjugate classes of  $G$ .*

To prove this, we observe first that the rings  $A_i$  in (27.20) annihilate each other, so that we have

$$\text{center of } KG = (\text{center of } A_1) \oplus \cdots \oplus (\text{center of } A_n).$$

Now  $A_i \cong K_{u_i}$ , and it is easily verified that the only matrices which commute with all matrices in the full matrix ring  $K_{u_i}$  are the scalar matrices (that is, scalar multiples of the identity matrix). Therefore the center of  $K_{u_i}$  is one dimensional over  $K$ , and so

$$(\text{center of } A_i : K) = 1.$$

Consequently, we have

$$n = ((\text{center of } KG) : K)$$

Now let  $\mathfrak{C}_1, \dots, \mathfrak{C}_s$  denote the conjugate classes of  $G$ . For each  $i$ , define the element  $C_i$  in the group algebra  $KG$  by

$$(27.23) \quad C_i = \sum_{x \in \mathfrak{C}_i} x.$$

We shall show that  $s = n$  by proving

(27.24) **THEOREM.** *The elements  $C_1, \dots, C_s$  of  $KG$  form a  $K$ -basis for the center of  $KG$ . (This holds for an arbitrary field  $K$ , assuming only that  $G$  is a finite group.)*

**PROOF.** First of all, the elements  $\{C_i\}$  belong to the center of  $KG$  since for all  $h \in G$  (see Exercise 10.2),

$$hC_i h^{-1} = \sum_{x \in \mathfrak{C}_i} hxh^{-1} = C_i.$$

Moreover, the elements  $\{C_1, \dots, C_s\}$  are linearly independent over  $K$  since they are sums of non-overlapping sets of group elements. Finally, let  $y = \sum \alpha_g g$  belong to the center of  $KG$ . Then for each  $h \in G$  we have

$$\sum \alpha_g g = y = hyh^{-1} = \sum \alpha_{g'} \cdot hgh^{-1},$$

and comparing coefficients we obtain

$$\alpha_{h^{-1}gh} = \alpha_g \quad \text{for all } g \in G.$$

Thus  $\alpha_g = \alpha_{g'}$  whenever  $g, g'$  are in the same conjugate class of  $G$ , and so  $y$  is a  $K$ -linear combination of the  $\{C_i\}$ . This completes the proof of Theorems (27.24) and (27.22).

(27.25) **REMARK.** This argument shows that given a field  $K$ , not assumed to be algebraically closed, and such that  $\text{char } K \nmid [G : 1]$ , the number of non-isomorphic irreducible left  $KG$ -modules is always less than or equal to the number of conjugate classes in  $G$ .

We conclude this section with a basic theorem on non-semisimple group algebras. We require first some preliminary results. Let  $A$  be a finite-dimensional algebra over a field  $K$ , but  $A$  is not assumed to have a unity element. A *left ideal* in  $A$  is defined to be a  $K$ -subspace of  $A$  which is a left ideal in the ring  $A$ . Right ideals and two-sided ideals are defined similarly. Because  $A$  is a finite-dimensional  $K$ -space,  $A$  satisfies both the D.C.C. and A.C.C. for left and right ideals. The reader may check that the proofs of Theorems (24.2) and (24.4) hold for such an algebra  $A$ . Define  $\text{rad } A$  by (24.5). Then we shall prove

(27.26) **LEMMA.** *Let  $A \neq 0$  be a finite-dimensional algebra such that  $\text{rad } A = (0)$ . Then  $A$  has a unity element 1.*

**PROOF.** The proof of (25.1) holds as before if  $A(1 - e)$  is taken to mean the set of elements  $x \in A$  such that  $xe = 0$ . Then from (25.2) we obtain

$$A = Ae_1 \oplus \cdots \oplus Ae_n$$

where the  $\{e_i\}$  are orthogonal idempotents. Let  $e = e_1 + \cdots + e_n$ . Then  $xe = x$  for all  $x \in A$ , and we have

$$A = eA \oplus A_0$$

where  $A_0 = \{x \in A : ex = 0\}$ . Since  $A = Ae$ , we have  $AA_0 = 0$ , and it follows that  $A_0$  is a two-sided ideal in  $A$  such that  $A_0^2 = 0$ . Since  $\text{rad } A = (0)$ , we have  $A_0 = 0$ , and we have proved that  $e$  is a unity element in  $A$ .

(27.27) **THEOREM (Wedderburn).** *If a finite-dimensional algebra  $A$  over an algebraically closed field  $K$  has a basis consisting of nilpotent elements, then  $A$  is a nilpotent algebra; i.e.,  $A^m = 0$  for some positive integer  $m$ .*

**PROOF.** We note first that if  $A$  has a basis of nilpotent elements, so does any homomorphic image of  $A$ . We shall use induction on  $(A : K)$ , and may assume that  $(A : K) > 1$  and that the result is valid for any algebra with a nilpotent basis of fewer than  $(A : K)$  elements. If  $\text{rad } A \neq (0)$ , then  $(A/\text{rad } A : K) < (A : K)$ , and by the

induction hypothesis,  $A/\text{rad } A$  is nilpotent. This can happen only if  $\text{rad } A = A$ , and thus  $A$  is nilpotent in this case. The proof will be completed if we can show that the possibility  $\text{rad } A = (0)$  cannot occur. Indeed, suppose  $A$  has a basis of nilpotent elements, and let  $\text{rad } A = (0)$ . By (27.26),  $A$  has a unity element and is a semi-simple algebra. Since  $K$  is algebraically closed, we deduce from (27.18) that  $A$  has a homomorphic image which is isomorphic to a full matrix algebra  $K_n$  for some  $n > 0$ , and hence  $K_n$  has a basis of nilpotent elements. This implies that every matrix of  $K_n$  has trace zero, which is a contradiction, since  $e_{11}$  (for example) has a non-zero trace. The proof of Theorem 27.27 is completed.

(27.28) THEOREM. *Let  $G$  be a  $p$ -group for some prime  $p$ , and let  $K$  be an algebraically closed field of characteristic  $p$ . Then the elements  $\{g - 1 : g \in G, g \neq 1\}$  form a basis of  $\text{rad } KG$ . Moreover,  $KG$  has only one irreducible  $KG$ -module, namely the trivial one  $K$  with  $g\alpha = \alpha$ ,  $\alpha \in K$ ,  $g \in G$ .*

PROOF. Let  $N$  be the  $K$ -subspace of  $G$  generated by the elements  $\{g - 1 : g \in G, g \neq 1\}$ . For each  $g \in G$ , we have  $g^{p^k} = 1$  for some positive integer  $k$ , and it follows that  $(g - 1)^{p^k} = 0$  in  $KG$ . Thus  $N$  is a subspace of  $KG$  with a basis of nilpotent elements. For any  $x \in G$ ,  $g \in G$ , we have  $x(g - 1) = (xg - 1) - (x - 1) \in N$ , and  $(g - 1)x = (gx - 1) - (x - 1) \in N$ . Therefore  $N$  is a two-sided ideal in  $KG$ , and, by Theorem 27.27,  $N$  is nilpotent. Since the elements  $\{g - 1 : g \in G, g \neq 1\}$  form a basis for  $N$ , we have

$$KG = K \cdot 1 \oplus N,$$

and it follows that  $N = \text{rad } KG$ . The second statement follows at once from Theorem 25.24, and the fact  $KG/(\text{rad } KG) \cong K$ .

### Exercises

1. (Converse of Schur's lemma.) Let  $M$  be a completely reducible  $A$ -module where  $A$  is an algebra over  $K$ . Show that  $\text{Hom}_A(M, M) = K$  implies that  $M$  is irreducible. Show further that this result need not be true when  $M$  is not completely reducible, for example, when  $M$  is a two-dimensional space which is a module over the algebra

$$A = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} : a, b, c \in K \right\}.$$

2. Let  $G_i$  ( $i = 1, 2$ ) be finite groups,  $G = G_1 \times G_2$  their direct product. Let  $M_i$  be an irreducible  $KG_i$ -module ( $i = 1, 2$ ) where  $K$  is an algebraically closed field such that  $\text{char } K \nmid [G : 1]$ . Make  $M_1 \otimes_K M_2$  into a  $KG$ -module by setting

$$(g_1, g_2)(m_1 \otimes m_2) = g_1 m_1 \otimes g_2 m_2$$

for  $g_i \in G_i$ ,  $m_i \in M_i$ ,  $i = 1, 2$ . Show that  $M_1 \otimes_K M_2$  is an irreducible  $KG$ -module and that all irreducible  $KG$ -modules have this form [Hint: For arbitrary  $T_i \in \text{Hom}_K(M_i, M_i)$ , show that there exists  $x_i \in KG$  such that  $(x_i)_L = T_i$ ,  $i = 1, 2$ . Deduce from this that  $(KG)_L$  contains all  $K$ -homomorphisms of  $M_1 \otimes_K M_2$  of the form  $T_1 \otimes T_2$ , and so  $(KG)_L = \text{Hom}_K(M_1 \otimes_K M_2, M_1 \otimes_K M_2)$ , thereby establishing the irreducibility of  $M_1 \otimes_K M_2$ . By (27.21), it is then sufficient to show that  $M_1 \otimes_K M_2$  is not isomorphic to  $M'_1 \otimes_K M'_2$  unless  $M_1 \cong M'_1$  and  $M_2 \cong M'_2$ . For this, use the fact that if  $M_1 \not\cong M'_1$ , then there is an idempotent  $e \in KG_1$  such that  $eM_1 = M_1$  and  $eM'_1 = 0$ , and then

$$e(M_1 \otimes M_2) = M_1 \otimes M_2 \quad \text{while} \quad e(M'_1 \otimes M'_2) = 0.]$$

## § 28. Irreducible Representations of the Symmetric Group

As a first illustration of how the theorems of § 27 may be applied to calculate the irreducible representations of particular groups we consider the symmetric group  $G = S_n$  on  $n$  symbols. Let  $A = QG$  be the group algebra of  $G$  over the field  $Q$  of rational numbers. We shall construct all the minimal left ideals in  $A$ . We shall use the following facts, which have all been established earlier in this chapter:

(28.1) Every left  $A$ -module is a direct sum of irreducible left  $A$ -modules.

(28.2) Every irreducible left  $A$ -module is isomorphic to a minimal left ideal  $Ae$  in  $A$  where  $e$  is an idempotent.

(28.3) The number of non-isomorphic minimal left ideals in  $QG$  is less than or equal to the number of conjugate classes in  $G$ .

(28.4) A left ideal  $Ae$  generated by an idempotent  $e$  is minimal if and only if  $eAe$  is a skewfield.

The next result was proved in Chapter I (3.8).

(28.5) The number of conjugate classes in  $S_n$  is equal to the number of partitions of  $n$ , where a partition of  $n$  is an ordered set of positive integers  $\{n_1, \dots, n_k\}$  such that

$$(28.6) \quad n = n_1 + \dots + n_k, \quad n_1 \geq n_2 \geq \dots \geq n_k,$$

$k$  arbitrary.

We shall determine a minimal left ideal in  $A$  corresponding to each partition in such a way that ideals which correspond to different

partitions are not isomorphic (as  $A$ -modules). By (28.2) and (28.3), we may then conclude that these ideals form a full set of non-isomorphic irreducible  $A$ -modules.

We order the partitions lexicographically, that is, if we have two partitions  $n = n_1 + \cdots + n_k = n'_1 + \cdots + n'_k$ ,  $n_1 \geq \cdots \geq n_k > 0$ ,  $n'_1 \geq \cdots \geq n'_k > 0$ , we write

$$\{n_1, \dots, n_k\} > \{n'_1, \dots, n'_k\}$$

if at the first position where these arrays differ, we have  $n_i > n'_i$ .

In multiplying elements of  $S_n$ , let us agree to work from right to left, so that

$$(123)(12) = (13), \quad (12)(123) = (23).$$

Thus if  $\alpha$  is a digit, then

$$(gh)\alpha = g(h(\alpha)), \quad g, h \in S_n.$$

Let  $\epsilon_g = +1$  if  $g$  is an even permutation, and  $\epsilon_g = -1$  if  $g$  is an odd permutation. Then  $\epsilon_{gh} = \epsilon_g \epsilon_h$ ,  $g, h \in S_n$ .

Let us now start with a partition of  $n$  given by (28.6). With it we associate a *table* consisting of  $n_1$  spaces in the first row,  $n_2$  spaces in the second row, and so on. A *diagram* is the array obtained by filling in the spaces of a table with the digits  $1, \dots, n$  in any order. For example,

$$9 = 3 + 3 + 2 + 1$$


table

1	2	3
4	5	6
7	8	
9		

diagrams

1	3	5
4	8	9
2	6	
7		

Starting with a diagram  $D$ , let  $R(D)$  denote the set of *row permutations*, that is, the set of permutations  $p \in S_n$  which permute the elements in each row of  $D$ , but do not move any digit from one row to another. For example,

$$\text{diagram } \begin{array}{|c|c|} \hline 1 & 3 \\ \hline 2 & 5 \\ \hline 4 & \\ \hline \end{array}, \quad R(D) = \{(1), (13), (25), (13)(25)\}.$$

Then  $R(D)$  is a subgroup of  $S_n$ . Likewise define a *column permutation*  $q$  to be any element of  $S_n$  which permutes the elements of each column of  $D$  without moving any digit from one column to another. Let  $C(D)$  be the group of all column permutations; in the above example,  $C(D) = \{(1), (124), (142), (35), (35)(124), (35)(142), (12), (24),$

$(14), (12)(35), (24)(35), (14)(35)\}$ . Obviously  $C(D) \cap R(D) = (1)$ ; for if  $q \in S_n$  is such that it does not move any symbol either out of its row or out of its column, it must leave each symbol unchanged, and so  $q = (1)$ , the identity transformation.

Now define

$$e(D) = \sum_{\substack{p \in R(D) \\ q \in C(D)}} \epsilon_q pq \in A .$$

We may remark that as  $p$  ranges over all elements of  $R(D)$  and  $q$  over  $C(D)$ , the products  $pq$  thus obtained are all distinct, since  $p_1 q_1 = p_2 q_2$  implies  $p_2^{-1} p_1 = q_2 q_1^{-1} \in C(D) \cap R(D)$ , and therefore  $p_2^{-1} p_1 = q_2 q_1^{-1} = (1)$ . This shows that  $e(D)$  is a sum of certain group elements or their negatives, and so  $e(D) \neq 0$  in  $A$ . For  $p_1 \in R(D)$  and  $q_1 \in C(D)$ , we have at once

$$(28.7) \quad p_1 \cdot e(D) = \sum \epsilon_q p_1 pq = e(D) ,$$

$$(28.8) \quad e(D) \cdot q_1 = \sum \epsilon_q pqq_1 = \epsilon_{q_1} e(D) .$$

With the partition (28.6), we shall associate the left ideal  $A \cdot e(D)$ , where  $D$  is any diagram obtained from the table corresponding to the partition. [Caution:  $e(D)$  is not idempotent but will turn out to be a scalar multiple of an idempotent element of  $A$ .] We shall show that all these left ideals are minimal, that ideals coming from different diagrams *but the same table* are isomorphic, and that ideals coming from different tables are non-isomorphic. These ideals, one for each table, will then be the desired full set of non-isomorphic irreducible  $A$ -modules.

For any diagram  $D$  and any  $g \in S_n$ , define  $gD$  to be the diagram obtained from  $D$  by applying  $g$  to the digits in  $D$ . Example:

$$D = \begin{array}{|c|c|} \hline 1 & 3 \\ \hline 2 & 5 \\ \hline 4 & \\ \hline \end{array} , \quad g = (132)(45) , \quad gD = \begin{array}{|c|c|} \hline 3 & 2 \\ \hline 1 & 4 \\ \hline 5 & \\ \hline \end{array} .$$

Thus if  $\alpha$  is in position  $(i, j)$  of  $D$ , then  $g\alpha$  is in position  $(i, j)$  of  $gD$ .

(28.9) LEMMA. *Let  $D' = gD$ , and let  $h \in S_n$ . If we regard  $hD$  as obtained from  $D$  by moving entries from one position to another, this same set of moves will change  $D'$  into  $ghg^{-1}D'$ . In other words, if the  $(i, j)$  entry of  $D$  is the  $(i', j')$  entry of  $hD$ , then the  $(i, j)$  entry of  $D'$  is the  $(i', j')$  entry of  $ghg^{-1}D'$ .*

Example.  $g = (135)$ ,  $h = (132)(45)$ ,  $ghg^{-1} = (14)(235)$ .

$$D = \begin{array}{|c|c|} \hline 1 & 3 \\ \hline 2 & 5 \\ \hline 4 & \\ \hline \end{array}, \quad D' = gD = \begin{array}{|c|c|} \hline 3 & 5 \\ \hline 2 & 1 \\ \hline 4 & \\ \hline \end{array},$$

$$hD = \begin{array}{|c|c|} \hline 3 & 2 \\ \hline 1 & 4 \\ \hline 5 & \\ \hline \end{array}, \quad ghg^{-1}D' = \begin{array}{|c|c|} \hline 5 & 2 \\ \hline 3 & 4 \\ \hline 1 & \\ \hline \end{array},$$

In passing from  $D$  to  $hD$ , the  $(1, 1)$  entry of  $D$  moves to the  $(2, 1)$  position of  $hD$ ; in going from  $D'$  to  $ghg^{-1}D'$ , the same move occurs, and so on.

**PROOF.** If symbol  $\alpha$  at position  $(i, j)$  in  $D$  occurs at position  $(i', j')$  in  $hD$ , the symbol  $\beta$  which is in position  $(i', j')$  of  $D$  must satisfy  $h(\beta) = \alpha$ . The element at position  $(i, j)$  in  $D'$  is of course  $g(\alpha)$ ; that in position  $(i', j')$  of  $D'$  is  $g(\beta)$ . The element in  $(i', j')$  position in  $ghg^{-1}D'$  is therefore

$$ghg^{-1} \cdot g(\beta) = g(\alpha),$$

so that, in going from  $D'$  to  $ghg^{-1}D'$ , the symbol  $g(\alpha)$  in position  $(i, j)$  has moved to position  $(i', j')$ .

(28.10) **COROLLARY.** For  $g \in S_n$ , we have  $R(gD) = gR(D)g^{-1}$ ,  $C(gD) = gC(D)g^{-1}$ ,  $e(gD) = ge(D)g^{-1}$ .

**PROOF.** If  $p \in R(D)$ , then  $p$  leaves each entry of  $D$  in its row. By the lemma, it then follows that  $gpg^{-1}$  leaves each entry of  $gD$  in its row. This argument shows that  $p \in R(D)$  if and only if  $gpg^{-1} \in R(gD)$ . The same holds for column permutations, and the corollary follows at once.

We use the above corollary to show that if  $D$  and  $D'$  are diagrams with the same table, then  $A \cdot e(D) \cong A \cdot e(D')$ . For, there exists an element  $g \in S_n$  such that  $D' = gD$ , whence

$$A \cdot e(D') = Age(D)g^{-1} = A \cdot e(D)g^{-1}$$

since  $A \cdot g = A$ . But then

$$\theta : A \cdot e(D) \rightarrow A \cdot e(D')$$

defined by  $\theta(x) = xg^{-1}$  is easily seen to be an  $A$ -isomorphism of the left  $A$ -module  $A \cdot e(D)$  onto  $A \cdot e(D')$ .

(28.11) **LEMMA.** An element  $g \in S_n$  is expressible in the form  $g = pq$ ,  $p \in R(D)$ ,  $q \in C(D)$ , if and only if no two collinear symbols of  $D$  are co-columnar in  $gD$ .

**PROOF.** Assume  $g = pq$ , and let  $\alpha, \beta$  be collinear symbols of  $D$ .

Then  $\alpha, \beta$  are also collinear in  $pD$ . However,  $gD = (pqp^{-1})pD$ , and  $pqp^{-1}$  is a column permutation for  $pD$ , so that  $\alpha$  and  $\beta$  must lie in different columns of  $(pqp^{-1})pD$ .

Conversely, suppose no two collinear symbols of  $D$  are co-columnar in  $gD$ . Then any two symbols which are co-columnar in  $gD$  cannot be collinear in  $D$ . In particular, all the symbols in the first column of  $gD$  lie in different rows of  $D$ , and so there exists a row permutation  $p_1 \in R(D)$  which carries all these symbols into the first column of  $p_1 D$ . Repeat this procedure successively with the remaining columns of  $gD$ , thereby eventually obtaining a row permutation  $p \in R(D)$  such that for each  $i$ , the  $i$ th columns of  $gD$  and  $pD$  consist of the same symbols (differently arranged, however). But then

$$gD = q' \cdot pD \quad \text{for some } q' \in C(pD),$$

and so  $q' = pqp^{-1}$  for some  $q \in C(D)$ . Hence  $gD = (pqp^{-1})pD = pqD$ , whence  $g = pq$  with  $p \in R(D)$  and  $q \in C(D)$ . This completes the proof.

(28.12) LEMMA. *Let  $D$  be any diagram associated with the partition  $\{n_1, \dots, n_k\}$ , and  $D'$  with  $\{n'_1, \dots, n'_k\}$ , and suppose  $\{n_1, \dots, n_k\} > \{n'_1, \dots, n'_k\}$ . Then  $e(D') \cdot e(D) = 0$ .*

PROOF. We show first that there exist two symbols collinear in  $D$  and co-columnar in  $D'$ . Otherwise, the  $n_1$  entries in the first row of  $D$  must occur in different columns of  $D'$ ; since  $D'$  has  $n'_1$  columns, this shows that  $n_1 \leq n'_1$ , and so  $n_1 = n'_1$ . Now apply a column permutation on  $D'$  to obtain a new diagram  $D''$ , also associated with the partition  $\{n'_1, \dots, n'_k\}$  but which has the same first row as  $D$ . We then repeat the argument with the elements of  $D$  and  $D''$  not in the first row, getting  $n_2 = n'_2, \dots$ , which is impossible.

We have thus shown the existence of symbols  $\alpha, \beta$  collinear in  $D$  and co-columnar in  $D'$ . Set  $t = (\alpha\beta) \in S_n$ . Then  $t \in R(D)$ ,  $t \in C(D')$ , and

$$e(D') \cdot e(D) = e(D')t \cdot te(D) = -e(D') \cdot e(D)$$

by formulas (28.7) and (28.8). Therefore  $e(D')e(D) = 0$ , and (28.12) is proved.

We note that, for  $p \in R(D)$ ,  $q \in C(D)$ ,  $r \in Q$ , we have

$$p \cdot re(D) \cdot q = \varepsilon_q \cdot re(D).$$

We now prove, conversely, that the above property characterizes the scalar multiples of  $e(D)$ .

(28.13) LEMMA. Let  $x \in A$  be such that  $pxq = \epsilon_q x$  for all  $p \in R(D)$ ,  $q \in C(D)$ . Then there exists  $\tau \in Q$  such that  $x = \tau e(D)$ .

PROOF. Let  $x = \sum \alpha_g g$ , the sum extending over all  $g \in S_n$ , where each  $\alpha_g \in Q$ . Then

$$x = \epsilon_q p^{-1} x q^{-1} = \epsilon_q \sum_g \alpha_g (p^{-1} g q^{-1}) = \epsilon_q \sum_h \alpha_{phq} h$$

for each  $p \in R(D)$ ,  $q \in C(D)$ . Thus

$$(28.14) \quad \alpha_g = \epsilon_q \alpha_{pgq}, \quad p \in R(D), q \in C(D).$$

Setting  $g = (1)$ , we obtain

$$\alpha_{pq} = \epsilon_q \alpha_{(1)}, \quad p \in R(D), q \in C(D).$$

To complete the proof of the lemma, we need only show that  $\alpha_g = 0$  whenever  $g$  is not of the form  $pq$  for  $p \in R(D)$ ,  $q \in C(D)$ . Suppose that  $g$  is not of this form; by Lemma 28.11, there must then exist symbols  $\alpha, \beta$  collinear in  $D$  and co-columnar in  $gD$ . Let  $t = (\alpha\beta) \in S_n$ ; then  $t \in R(D)$ ,  $t \in C(gD)$ , and so  $t = gqg^{-1}$  for some  $q \in C(D)$ . Then  $q$  is also a transposition, and we have from (28.14)

$$\alpha_g = \epsilon_{q^{-1}} \alpha_{tqq^{-1}} = -\alpha_g$$

since  $tgg^{-1} = g$ . Therefore  $\alpha_g = 0$ , which proves the lemma.

Now we have for  $p \in R(D)$  and  $q \in C(D)$ ,

$$p \cdot e(D)^2 \cdot q = pe(D) \cdot e(D)q = \epsilon_q e(D)^2$$

[using (28.7) and (28.8)]. By the preceding lemma, we then have

$$e(D)^2 = \tau e(D)$$

where  $\tau$  is the coefficient of 1 in  $e(D)^2$ , and hence is an integer. We shall show that  $\tau \neq 0$ . Let  $T \in \text{Hom}_Q(A, A)$  be defined by  $T(x) = x \cdot e(D)$ ,  $x \in A$ , and let us consider the matrix description of  $T$  obtained by using the  $Q$ -basis of  $A$  consisting of the elements  $g_1 = (1)$ ,  $g_2, \dots, g_{n!}$  of  $S_n$ . Then if

$$e(D) = \alpha_1 g_1 + \dots, \quad \alpha_i \in Q,$$

we have

$$g_1 \cdot e(D) = \alpha_1 g_1 + \dots$$

$$g_2 \cdot e(D) = * + \alpha_1 g_2 + \dots$$

so that the trace of the matrix describing  $T$  is  $\alpha_1 n!$ . Furthermore  $\alpha_1 = 1$ , since  $(1)$  occurs with coefficient 1 in  $e(D)$ .

On the other hand, let us calculate the trace using a different  $Q$ -basis of  $A$ . We must get the same result, since the trace is

independent of the basis used. Let  $\{v_1, \dots, v_{n!}\}$  be a  $Q$ -basis of  $A$  such that  $\{v_1, \dots, v_f\}$  is a  $Q$ -basis of  $A \cdot e(D)$ . Here,  $f = (A \cdot e(D) : Q) \geq 1$  since  $e(D)$  is a non-zero element of  $A \cdot e(D)$ . Further,  $x \cdot e(D) = rx$  for  $x \in A \cdot e(D)$ , and so

$$\begin{aligned} v_1 \cdot e(D) &= rv_1 \\ v_2 \cdot e(D) &= \quad \quad \quad rv_2 \\ &\quad \dots \\ v_f \cdot e(D) &= \quad \quad \quad rv_f \\ v_{f+1} \cdot e(D) &= * + \dots + * + 0 \\ &\quad \dots \\ v_{n!} \cdot e(D) &= * + \dots + * + 0, \end{aligned}$$

since  $y \cdot e(D) \in A \cdot e(D)$  for  $y = v_{f+1}, \dots, v_{n!}$ . The trace is thus  $rf$ , so we have

$$rf = n!,$$

whence  $r \neq 0$ . (We note also that  $f | n!$ , a result which is a special case of a theorem to be obtained later.)

We may now show that each ideal  $A \cdot e(D)$  is minimal. Let  $u = r^{-1}e(D)$ , so that  $u^2 = u \neq 0$ . Then  $u$  is idempotent, and

$$Au = A \cdot e(D), \quad uAu = e(D)Ae(D).$$

In order to show that  $Au$  is a minimal left ideal of  $A$ , it suffices [by (28.4)] to prove that  $uAu$  is a skewfield. Let  $x \in uAu$ ; then  $x = e(D)ye(D)$  for some  $y \in A$ , and so

$$pxq = pe(D) \cdot y \cdot e(D)q = e(D)ye(D)\epsilon_q = \epsilon_q x$$

for all  $p \in R(D)$ ,  $q \in C(D)$ . By Lemma 28.13,  $x$  must therefore be a scalar multiple of  $e(D)$ . Thus

$$uAu = Qu \cong Q,$$

which shows in fact that  $uAu$  is a field.

Finally, let  $D, D'$  be diagrams with different tables, and let  $Au, Au'$  be the minimal left ideals associated with them. We shall show that  $Au$  and  $Au'$  are not isomorphic. If they were, then by (25.12) there would exist an element  $a \in A$  such that

$$Au = Au' \cdot a,$$

Hence  $u = bu'a$  for some  $b \in A$ , so that

$$u = u^2 = bu'au.$$

We shall show that  $u'au = 0$ , which will give the desired contradic-

tion. It suffices in fact to prove that  $u'gu = 0$  for all  $g \in S_n$ . However,  $u'gu = u' \cdot gug^{-1} \cdot g$ , and  $u' \cdot gug^{-1} = 0$  by Lemma 28.12 since  $u'$  and  $gug^{-1}$  come from  $D'$  and  $gD$ , respectively.

To summarize, we have established the following:

(28.15) THEOREM. *With each partition  $\{n_1, \dots, n_k\}$  of  $n$  we have associated a table. Each table gives rise to a collection of diagrams. From each diagram  $D$ , we obtain the group  $R(D)$  of row permutations and the group  $C(D)$  of column permutations. We set*

$$e(D) = \sum_{\substack{p \in R(D) \\ q \in C(D)}} \epsilon_q pq;$$

*then  $A \cdot e(D)$  is a minimal left ideal in the group algebra  $A = QS_n$ , and thus  $A \cdot e(D)$  is an irreducible  $A$ -module. Further, ideals coming from different diagrams with the same table are isomorphic, but ideals from diagrams with different tables are not. Hence the ideals  $\{A \cdot e(D)\}$ , where  $D$  ranges over a full set of diagrams with distinct tables, gives a full set of non-isomorphic irreducible  $A$ -modules.*

Our presentation furnishes some justification for our emphasis on modules and for working with the group algebra rather than the group itself. On the other hand, we may point out that we have used very strongly the nature of the group  $S_n$ . No general algorithm is known for specifically determining a full set of irreducible modules for an arbitrary finite group. Although we have in theory determined all irreducible  $Q$ -representations of  $S_n$ , in practice it may be somewhat cumbersome to obtain the matrix representations afforded by the modules we have given. One might also ask for a formula, in terms of  $n_1, \dots, n_k$ , for the degree of the representation afforded by the module  $Ae(D)$ . For further information on these questions, see Boerner [1], Murnaghan [1], or Rutherford [1]. For a comprehensive treatment of both ordinary and modular representations of  $S_n$ , see Robinson [1].

An interesting unsolved problem in this connection is whether the sort of algorithm used in the case of  $S_n$ , which gives a direct construction of the minimal left ideals in the group algebra from the conjugate classes in the group, is available for other classes of groups (see Exercise 28.3).

### Exercises

1. Construct a full set of inequivalent irreducible matrix representations for the symmetric group  $S_3$ .

2. Find the degrees of the different irreducible  $Q$ -representations of the symmetric group  $S_4$ .

3. Let  $G$  be a finite group which satisfies the following conditions:

(a) There exist subgroups  $P_1, P_2$  of  $G$  such that  $P_1 \cap P_2 = \{1\}$ ;

(b) There exists a homomorphism  $f$  of  $G$  into the multiplicative group of  $Q$  such that  $x \notin P_1 P_2$  implies  $f(u) \neq 1$  for some  $u \in P_1 \cap xP_2x^{-1}$ .

Prove that if

$$e = \sum_{\substack{p \in P_1 \\ q \in P_2}} f(q)pq$$

in  $QG$ , then  $QGe$  is a minimal left ideal in  $QG$ . [Hint: Imitate the proof of Theorem 28.15, especially Lemma 28.13.]

### § 29. Extension of the Ground Field\*

Let  $A$  be an algebra over the field  $K$ , and let  $L$  be any extension field of  $K$ . If  $\mathbf{T}$  is a  $K$ -representation of  $A$ , obviously  $\mathbf{T}$  is also an  $L$ -representation of  $A$ . Indeed we may introduce the algebra

$$A^L = A \otimes_K L$$

which is an algebra over  $L$ , and we may embed  $A$  in  $A^L$  by means of the isomorphism defined by  $a \rightarrow a \otimes 1$ ,  $a \in A$ . Then  $A^L$  consists precisely of the  $L$ -linear combinations  $\sum l_i a_i$  of the elements of  $A$ , and we may extend  $\mathbf{T}$  to an  $L$ -representation of  $A^L$  by setting

$$\mathbf{T}(\sum l_i a_i) = \sum l_i \mathbf{T}(a_i), \quad l_i \in L.$$

Some natural questions are:

- (i) If  $\mathbf{T}$  is irreducible over  $K$ , is  $\mathbf{T}$  irreducible over  $L$ ?
- (ii) If two  $K$ -representations are  $L$ -equivalent, are they necessarily  $K$ -equivalent?
- (iii) If  $A$  is semi-simple, is  $A^L$  also semi-simple?

In this section, we answer (i) and (ii) and make some remarks about (iii).

(29.1) DEFINITION. Let  $\mathbf{T}$  and  $\mathbf{U}$  be  $K$ -representations of  $A$ . A matrix  $X$  intertwines  $\mathbf{T}$  and  $\mathbf{U}$  if

$$(29.2) \quad \mathbf{T}(a)X = X\mathbf{U}(a) \quad \text{for all } a \in A.$$

Before switching over to modules, we shall use matrix terminology to prove a basic lemma.

(29.3) LEMMA. Let  $\mathbf{T}$  and  $\mathbf{U}$  be  $K$ -representations of  $A$ , and let  $S$

---

\* Some preliminary results are given in § 12B.

be the set of all matrices  $X$  with entries in  $K$  which intertwine  $T$  and  $U$ . Let  $S^L$  be the set of all matrices  $X$  with entries in  $L$  which intertwine  $T$  and  $U$ . Then  $S^L$  consists precisely of the  $L$ -linear combinations

$$\sum \alpha_i X_i, \quad \alpha_i \in L, X_i \in S.$$

PROOF. Each such linear combination obviously lies in  $S^L$ . Conversely let  $X \in S^L$ , and write

$$X = \alpha_1 X_1 + \cdots + \alpha_n X_n, \quad \alpha_i \in L,$$

where  $\{\alpha_1, \dots, \alpha_n\}$  are linearly independent over  $K$  and where each  $X_i$  has entries in  $K$ . Substitution into (29.2) yields

$$\sum \alpha_i (T(a)X_i - X_i U(a)) = 0, \quad a \in A.$$

From the linear independence of the  $\{\alpha_i\}$  we deduce that for each  $i$ ,

$$T(a)X_i - X_i U(a) = 0, \quad a \in A,$$

and so each  $X_i$  is in  $S$ . This completes the proof.

In module terminology, let  $V$  be a left  $A$ -module (every  $A$ -module is assumed to be finite dimensional over  $K$ ). We form the extended module

$$V^L = V \otimes_K L$$

and embed  $V$  in  $V^L$ . Then  $V^L$  consists of all  $L$ -linear combinations of the elements of  $V$ , and

$$(29.4) \quad (V^L : L) = (V : K).$$

Furthermore,  $V^L$  becomes a left  $A^L$ -module in a natural way if we define

$$(\sum \beta_i a_i)(\sum r_j v_j) = \sum \beta_i r_j (a_i v_j)$$

where the  $\{\beta_i\}$  and  $\{r_j\} \in L$ ,  $\{a_i\} \in A$ ,  $\{v_j\} \in V$ .

Suppose now that relative to the  $K$ -basis  $\{v_1, \dots, v_n\}$ ,  $V$  affords the matrix representation  $T$  of  $A$ . The elements  $\{v_i\}$  are also an  $L$ -basis of  $V^L$ , and relative to this basis, let  $V^L$  afford the matrix representation  $T^L$  of  $A^L$ . We have at once

$$T^L | A = T,$$

and

$$T^L (\sum \alpha_i a_i) = \sum \alpha_i T(a_i), \quad \alpha_i \in L, a_i \in A.$$

Note however that some  $L$ -bases of  $V^L$  need not be  $K$ -bases of  $V$ , so that in the set of mutually equivalent matrix representations of  $A^L$  over  $L$ , some of the matrix representations need not arise as extensions of  $K$ -representations of  $A$ .

If  $W$  and  $V$  are a pair of left  $A$ -modules, the set of  $K$ -matrices which intertwine the  $K$ -representations they afford is isomorphic (as  $K$ -space) to  $\text{Hom}_A(V, W)$ . The preceding lemma may therefore be restated as

(29.5) *Let  $V, W$  be left  $A$ -modules. Then*

$$\text{Hom}_A(V, W) \otimes_K L \cong \text{Hom}_{A^L}(V^L, W^L).$$

(We shall usually identify these isomorphic  $K$ -spaces.)

(29.6) **COROLLARY.** *If  $V$  and  $W$  have a common composition factor as  $A$ -modules, the  $A^L$ -modules  $V^L$  and  $W^L$  also have a common composition factor. Conversely, if  $V^L$  and  $W^L$  are completely reducible  $A^L$ -modules having a common composition factor, then  $V$  and  $W$  have a common composition factor.*

**PROOF.** Let  $V = V_1 \supset V_2 \supset \cdots \supset V_r \supset (0)$  be a composition series for the  $A$ -module  $V$ . Then

$$V^L = V_1^L \supset V_2^L \supset \cdots \supset V_r^L \supset (0)$$

can be refined to a composition series for the  $A^L$ -module  $V^L$ . Hence if  $X_1, \dots, X_r$  are the composition factors of  $V$ , then those of  $V^L$  are the composition factors of  $X_1^L, \dots, X_r^L$ . From this it follows at once that if  $V$  and  $W$  are  $A$ -modules having a common composition factor, then also  $V^L$  and  $W^L$  have a common composition factor.

Conversely let  $V^L$  and  $W^L$  be completely reducible  $A^L$ -modules having a common composition factor. Then  $\text{Hom}_{A^L}(V^L, W^L) \neq 0$ , and thus also  $\text{Hom}_A(V, W) \neq 0$ , which implies that  $V$  and  $W$  have a common composition factor. This completes the proof.

We may now answer question (ii) in the affirmative, by means of

(29.7) **THEOREM** (Noether [1], Deuring [1]). *Let  $T$  and  $U$  be  $K$ -representations of  $A$  of the same degree  $d$ . If  $T$  and  $U$  are  $L$ -equivalent, where  $L$  is any extension field of  $K$ , then they are  $K$ -equivalent.*

**PROOF.** Using the notation of (29.3), let  $\{X_1, \dots, X_n\}$  be a  $K$ -

basis of  $S$ ; it is also an  $L$ -basis of  $S^L$ , by virtue of (29.3). The  $L$ -equivalence of  $\mathbf{T}$  and  $\mathbf{U}$  implies that there exist elements  $\alpha_1, \dots, \alpha_n \in L$  such that

$$(29.8) \quad |\alpha_1 X_1 + \cdots + \alpha_n X_n| \neq 0.$$

Now let  $t_1, \dots, t_n$  be independent indeterminates over the field  $K$ , and define

$$F(t_1, \dots, t_n) = |t_1 X_1 + \cdots + t_n X_n| \in K[t_1, \dots, t_n].$$

By virtue of (29.8), we know that  $F(t_1, \dots, t_n)$  is not the zero polynomial; it is clearly homogeneous of degree  $d$ . One may easily establish by induction on  $n$  that if  $K$  has more than  $d$  elements, then there exist elements  $a_1, \dots, a_n \in K$  such that  $F(a_1, \dots, a_n) \neq 0$ . But then  $a_1 X_1 + \cdots + a_n X_n$  is a non-singular element of  $S$ , and so  $\mathbf{T}$  and  $\mathbf{U}$  are  $K$ -equivalent.

On the other hand, suppose that  $K$  does not have more than  $d$  elements. We then choose some finite extension  $E$  over  $K$  with more than  $d$  elements. The above discussion shows that we can find elements  $b_1, \dots, b_n \in E$  such that  $F(b_1, \dots, b_n) \neq 0$ , and consequently  $\mathbf{T}$  and  $\mathbf{U}$  are  $E$ -equivalent. Switching to module terminology, we are now faced with the following situation:

We are given a pair of  $A$ -modules  $V$  and  $W$ , and we have a finite extension  $E$  of  $K$  such that

$$V \otimes_K E \cong W \otimes_K E$$

as  $A \otimes_K E$ -modules. Thus there exists an isomorphism

$$(29.9) \quad \theta : V \otimes_K E \cong W \otimes_K E$$

such that  $\theta(ay) = a\theta(y)$  for  $a \in A$ ,  $y \in V \otimes_K E$ , where we have identified  $A$  and  $A \otimes 1$ . But let

$$E = Ke_1 \oplus \cdots \oplus Ke_r, \quad r = (E : K).$$

Then

$$V \otimes_K E = V \otimes e_1 \oplus \cdots \oplus V \otimes e_r,$$

so that as a left  $A$ -module,  $V \otimes_K E$  is isomorphic to an external direct sum of  $r$  copies of  $V$ . From (29.9) we then deduce that

$$(29.10) \quad V + \cdots + V \cong W + \cdots + W$$

as  $A$ -modules, where  $r$  summands occur on each side. Now express  $V$  and  $W$  as direct sums of indecomposable  $A$ -modules. The Krull-

Schmidt theorem applied to (29.10) then shows that  $V$  and  $W$  have the same indecomposable summands, counted according to multiplicity. Therefore  $V \cong W$  as left  $A$ -modules, and the theorem is proved.

In module terminology, the above may be stated as

(29.11) THEOREM. *Let  $V, W$  be left  $A$ -modules where  $A$  is a  $K$ -algebra, and let  $L$  be an extension field of  $K$ . If  $V^L \cong W^L$  as  $A^L$ -modules, then  $V \cong W$  as  $A$ -modules.*

Turning next to question (i), we begin with

(29.12) DEFINITION. Let  $A$  be a  $K$ -algebra, and  $V$  an irreducible  $A$ -module. Call  $V$  *absolutely irreducible* if  $V^L$  is an irreducible  $A^L$ -module for every extension field  $L$  of  $K$ . This terminology will also be used for matrix representations. An extension field  $L$  of  $K$  is called a *splitting field* for the  $K$ -algebra  $A$  if every irreducible  $A^L$ -module is absolutely irreducible.

We have already seen in Chapter II, §10 that an irreducible module need not be absolutely irreducible, so that the answer to (i) is negative. It is of importance, therefore, to obtain a necessary and sufficient condition for absolute irreducibility.

(29.13) THEOREM. *An irreducible  $A$ -module  $V$  is absolutely irreducible if and only if*

$$\text{Hom}_A(V, V) \cong K,$$

*that is, if and only if the only  $A$ -endomorphisms of  $V$  are left multiplications by elements of  $K$ .*

PROOF. The map  $a \rightarrow a_L$  maps  $A$  onto a subalgebra  $B$  of  $\text{Hom}_K(V, V)$ . In §27 we have shown that

$$D = \text{Hom}_A(V, V) = \text{Hom}_B(V, V)$$

is a finite-dimensional division algebra over  $K$ , that

$$(29.14) \quad B \cong D_n, \quad n = (V : D),$$

and that  $V$  may be chosen as a minimal left ideal in the simple algebra  $B$ . Clearly  $V$  is absolutely irreducible as an  $A$ -module if and only if  $V$  is absolutely irreducible as a  $B$ -module.

Suppose first that  $\text{Hom}_A(V, V) = K$ . Then  $D = K$  and  $V$  is a minimal left ideal in  $K_n$ , so that  $(V : K) = n$ . If  $L$  is any extension of  $K$ , we know that  $V^L$  is a left ideal in  $K_n^L$ . However,

$$K_n^L = K_n \otimes_K L \cong L_n,$$

and  $(V^L : L) = (V : K) = n$ , which shows that  $V^L$  is a minimal left ideal in  $K_n^L$ . Thus  $V^L$  is an irreducible  $K_n^L$ -module, which proves that  $V$  is absolutely irreducible.

Conversely, let  $V$  be absolutely irreducible, and let  $L$  be the algebraic closure of  $K$ . Then  $V^L$  is a faithful irreducible  $B^L$ -module, as follows easily from the fact that  $V$  is a faithful  $B$ -module. We conclude from Exercise 26.2 that  $B^L$  is a simple ring and that  $V^L$  is a minimal left ideal in  $B^L$ . But then (27.18) implies that

$$B^L \cong L_m, \quad (V^L : L) = m$$

for some  $m$ , and consequently

$$(B : K) = m^2, \quad (V : K) = m.$$

Comparison with (29.14) yields

$$m^2 = (B : K) = n^2(D : K).$$

But also  $(V : K) = (V : D)(D : K)$ , that is,  $m = n(D : K)$ . Thus  $(D : K)^2 = (D : K)$ , and hence  $D = K$ , which completes the proof of the theorem.

As an immediate consequence of the above proof, we have

(29.15) COROLLARY. *Let  $V$  be an irreducible  $A$ -module, where  $A$  is a  $K$ -algebra, and let  $L$  be the algebraic closure of  $K$ . If  $V^L$  is irreducible, then  $V$  is absolutely irreducible. In particular, for algebras over algebraically closed fields, every irreducible module is absolutely irreducible.*

We have now settled questions (i) and (ii). We shall postpone until Chapter X the full answer to (iii) and shall merely remark that it is possible for  $A^L$  to have a non-zero radical even when  $A$  is a simple algebra. (See Exercise 29.1.)

To conclude this section, we shall obtain a further result for group algebras. Let  $G$  be a finite group; we call a field  $K$  a *splitting field for  $G$*  if every irreducible  $KG$ -module is absolutely irreducible. Surely any algebraically closed field is a splitting field for  $G$ , by virtue of (29.15). We now prove

(29.16) THEOREM. *Given a finite group  $G$ , there exists an algebraic number field  $K$  which is a splitting field for  $G$ .*

PROOF. Let  $L$  denote the algebraic closure of the rational field  $Q$ . Then  $LG$  is an algebra over  $L$  and is semi-simple by Maschke's theorem (15.6); so, by (27.18), we may write  $LG$  as a direct sum of matrix algebras over  $L$ , say

$$LG = L_{n_1} + \cdots + L_{n_r}.$$

Let

$$\{e_{ij}^{(k)} : 1 \leq i, j \leq n_k, 1 \leq k \leq r\}$$

be a full set of matrix units in  $LG$ . These form an  $L$ -basis for  $LG$  and multiply according to the rule

$$(29.17) \quad e_{ij}^{(k)} e_{i'j'}^{(k')} = \delta_{ji'} \delta_{kk'} e_{ij'}^{(k')}.$$

For each  $g \in G$  we may write

$$(29.18) \quad g = \sum_{i,j,k} \alpha_{ij}^{(k)}(g) e_{ij}^{(k)}, \quad \alpha_{ij}^{(k)}(g) \in L.$$

On the other hand, each matrix unit is in  $LG$ , so that also

$$(29.19) \quad e_{ij}^{(k)} = \sum_{g \in G} \beta_{ijk}^{(g)} g, \quad \beta_{ijk}^{(g)} \in L.$$

The coefficients

$$\{\alpha_{ij}^{(k)}(g), \beta_{ijk}^{(g)} : \text{all } i, j, k, g\}$$

generate a finite extension  $K$  of  $Q$ . From (29.19) we see that each matrix unit lies in  $KG$ , and so, setting

$$\tilde{A} = \text{direct sum } \sum_{i,j,k} K e_{ij}^{(k)},$$

we see that  $\tilde{A}$  is a subalgebra of  $KG$ . But  $\tilde{A}$  contains each element of  $G$  because of (29.18), and hence  $\tilde{A} = KG$ . Since  $\tilde{A}$  contains a full set of matrix units which form a  $K$ -basis for  $\tilde{A}$ , we have

$$KG = \tilde{A} \cong K_{n_1} + \cdots + K_{n_r}.$$

By Theorem 29.13, every irreducible  $\tilde{A}$ -module is absolutely irreducible, which proves that  $K$  is a splitting field for  $G$ .

We may observe that the above proof also yields a more general result, namely

(29.20) *Let  $A$  be a semi-simple algebra of finite dimension over a field  $E$ , let  $F$  be the algebraic closure of  $E$ , and suppose that  $A^F$  is semi-simple. Then there exists a field  $K$  such that  $F \supset K \supset E$ ,  $(K : E)$  is finite, and every irreducible  $A^K$ -module is absolutely irreducible.*

The proof is left to the exercises.

We conclude with the basic result

(29.21) **THEOREM.** *Any extension of a splitting field is a splitting field. More precisely, let  $K$  be a splitting field for the  $K$ -algebra  $A$ , and let  $L$  be any extension field of  $K$ . Then  $L$  is also a splitting*

field for the algebra  $A$ . Furthermore, if  $V_1, \dots, V_r$  are a full set of non-isomorphic irreducible  $A$ -modules, then  $V_1^L, \dots, V_r^L$  are a full set of non-isomorphic irreducible  $A^L$ -modules.

**PROOF.** Since  $K$  is a splitting field for  $A$ , we may write

$$A/\text{rad } A \cong K_{n_1} \dot{+} \cdots \dot{+} K_{n_r},$$

and choose  $V_i$  to be a minimal left ideal in  $K_{n_i}$ ,  $1 \leq i \leq r$ . Then

$$(A/\text{rad } A)^L \cong (\sum K_{n_i})^L = \sum K_{n_i}^L \cong \sum L_{n_i},$$

so that every irreducible  $(A/\text{rad } A)^L$ -module is of the form  $V_i^L$  for some  $i$ .

On the other hand, let  $W$  be any irreducible  $A^L$ -module. Then  $\text{rad}(A^L) \cdot W = 0$ , and since

$$(\text{rad } A)^L \subset \text{rad}(A^L),$$

this shows that  $W$  is an irreducible  $A^L/(\text{rad } A)^L$ -module. However

$$A^L/(\text{rad } A)^L = (A/\text{rad } A)^L,$$

and so  $W = V_i^L$  for some  $i$ . But  $V_i$  is absolutely irreducible, whence so is  $W$ . Thus each irreducible  $A^L$ -module is absolutely irreducible, whence  $L$  is a splitting field for  $A$ . We have also established that  $V_1^L, \dots, V_r^L$  are a full set of irreducible  $A^L$ -modules, no two of which may be isomorphic [by (29.11)]. This proves the theorem.

(29.22) **COROLLARY.** *Keeping the above notation, we have*

$$\text{rad}(A^L) = (\text{rad } A)^L.$$

**PROOF.** Since  $\text{rad}(A^L)$  annihilates every irreducible  $A^L$ -module, it must annihilate  $A^L/(\text{rad } A)^L$ . This implies that

$$\text{rad}(A^L) \subset (\text{rad } A)^L,$$

whence the result follows.

(29.23) **COROLLARY.** *Let  $A$  be an algebra over a field  $K$ , and let  $E \supset K$  be a splitting field for  $A$ . Then any extension field  $L$  containing  $E$  is also a splitting field for  $A$ .*

**PROOF.** By hypothesis  $E$  is a splitting field for  $A^E$ , whence, by (29.21),  $L$  is also a splitting field for  $A^E$ ; that is, every irreducible  $(A^E)^L$ -module is absolutely irreducible. Since  $(A^E)^L \cong A^L$ , this shows that  $L$  is a splitting field for  $A$ .

*Exercises*

1. Let  $F$  be the prime field with  $p$  elements,  $K = F(t)$  a simple transcendental extension of  $F$ , and let  $L = K(\theta)$  where  $\text{Irr}(\theta, K) = X^p - t$ . Show that  $L \otimes_K L$  is a commutative algebra over  $K$  which has non-zero nilpotent elements, and hence is not semi-simple.

2. Let  $S$  be an irreducible set of linear transformations on a vector space  $V$  over a field  $K$ . Show that  $S$  is absolutely irreducible if and only if the only elements of  $\text{Hom}_K(V, V)$  which commute with all elements of  $S$  are the scalar multiplications  $v \rightarrow \alpha v$ ,  $\alpha \in K$ .

3. Show that irreducible modules given in §28 are absolutely irreducible.

4. Give the details of the proof of (29.20).

5. Let  $T: A \rightarrow K_A$  be a  $K$ -representation of a  $K$ -algebra  $A$ . Show that  $T$  is absolutely irreducible if and only if  $(T(A):K) = d^2$  where

$$T(A) = \{T(a) : a \in A\}.$$

6. Let  $G$  be a finite abelian group of exponent  $n$ . Prove that  $Q(\sqrt[n]{1})$  is a splitting field for  $G$ .

7. Let  $A$  be a  $K$ -algebra, and let  $V_1, \dots, V_r$  be a full set of non-isomorphic irreducible  $A$ -modules. Set  $D_i = \text{Hom}_A(V_i, V_i)$ . Show that

$$(A/\text{rad } A : K) = \sum_{i=1}^r (D_i : K)(V_i : K)^2.$$

In particular, if  $A$  is semi-simple, show that  $K$  is a splitting field for  $A$  if and only if

$$(A : K) = \sum_{i=1}^r (V_i : K)^2.$$

8. Let  $G$  be a finite group, let  $K \subset L$  be fields for which  $\text{char } K \nmid [G : 1]$ , and let  $W$  be an irreducible  $LG$ -module. Show that  $W$  is isomorphic to a direct summand of  $V^L$  for some irreducible  $KG$ -module  $V$ . [Hint: Since  $LG$  is semi-simple,  $W$  is a direct summand of  $LG$ . But  $LG = (KG)^L$ , and since  $KG$  is a direct sum  $\sum V_i$  of irreducible  $KG$ -modules  $\{V_i\}$ , we have

$$LG = \sum_i V_i^L.$$

Each  $V_i^L$  can in turn be written as a direct sum of irreducible  $LG$ -modules, and  $W$  must be isomorphic to one of these summands for some  $i$ .]

9. Show that Wedderburn's theorem 27.27 remains valid even without the hypothesis that  $K$  be algebraically closed.

## CHAPTER V

## Group Characters

## § 30. Introduction

The theory of group characters furnishes one of the most powerful methods for studying groups and their representations. We shall now develop some of the basic properties of characters, and shall apply them to the proof of several important results. A thorough knowledge of §§ 27 and 29 will be assumed throughout.

As usual, we let  $K_n$  denote the full matrix algebra of all  $n \times n$  matrices over a field  $K$ , and let  $I^{(n)}$  (or briefly  $I$ ) denote the identity matrix in  $K_n$ . Let  $X$  be an indeterminate over  $K$ .

(30.1) DEFINITION. The *characteristic polynomial* of a matrix  $A \in K_n$  is the determinant  $|XI - A|$  viewed as a polynomial in  $X$ . The *characteristic roots* of  $A$  are the zeros of this characteristic polynomial, counted according to their multiplicities. The *trace* of  $A$  is the sum of the elements on the main diagonal of  $A$ . We have (see Exercises 8.1, 8.2)

$$|XI - A| = X^n - (\text{tr } A)X^{n-1} + \cdots + (-1)^n |A|,$$

which shows that the trace of  $A$  is the sum of the characteristic roots of  $A$ .

Now let  $A \in K_n$ , and let  $L$  be an extension field of  $K$  over which the characteristic polynomial of  $A$  splits into linear factors. We may view  $A$  as an element of  $L_n$  and let  $A$  act on an  $n$ -dimensional vector space  $V$  over  $L$ . Then an element  $\alpha \in L$  is a characteristic root of  $A$  if and only if  $\alpha I - A$  is singular, that is, if and only if there exists a non-zero vector  $v \in V$  for which  $Av = \alpha v$ .

If  $A \in K_n$  has the form

$$A = \begin{pmatrix} B_1 & C \\ 0 & B_2 \end{pmatrix}. \quad B_i \in K_{n_i}, i = 1, 2,$$

where  $0$  is a zero matrix of appropriate size, then we have

$$|XI - A| = |XI - B_1| |XI - B_2|.$$

Thus the characteristic polynomial of  $A$  is the product of that of  $B_1$  with that of  $B_2$ . Further, the characteristic roots of  $A$  are those of  $B_1$  together with those of  $B_2$ .

By Exercise 8.2 we may speak of characteristic polynomials of linear transformations as well as of matrices. The characteristic polynomial of a transformation  $A \in \text{Hom}_K(V, V)$ , where  $V$  is a finite-dimensional vector space over  $K$ , is defined as  $|XI - A|$  where  $A$  is the matrix of  $A$  relative to any  $K$ -basis of  $V$ . Let  $W$  be a subspace of  $V$  for which  $AW \subset W$ , and set  $A_1 = A|W$  (the restriction of  $A$  to  $W$ ), so that  $A_1 \in \text{Hom}_K(W, W)$ . Note that  $A$  induces a linear transformation  $A_2$  on the factor space  $V/W$ . The remarks of the preceding paragraph show that

$$\text{char. pol. of } A = (\text{char. pol. of } A_1) (\text{char. pol. of } A_2).$$

Using this, we may prove the well-known result:

(30.2) THEOREM. *Let  $A, B \in K_n$  be such that  $AB = BA$ , and let  $\alpha_1, \dots, \alpha_n$  be the characteristic roots of  $A$  and  $\beta_1, \dots, \beta_n$  those of  $B$ . Then renumbering the  $\{\beta_i\}$  if need be, the characteristic roots of  $AB$  are  $\alpha_1\beta_1, \dots, \alpha_n\beta_n$ . If  $F(X) \in K[X]$ , the characteristic roots of  $F(A)$  are  $F(\alpha_1), \dots, F(\alpha_n)$ . Further if  $A$  is non-singular, then  $A^{-1}$  has characteristic roots  $\alpha_1^{-1}, \dots, \alpha_n^{-1}$ .*

PROOF. Replacing  $K$  by  $K(\alpha_1, \dots, \alpha_n, \beta_1, \dots, \beta_n)$ , we may assume for the remainder of the proof that the characteristic polynomials of  $A$  and  $B$  split into linear factors in  $K[X]$ . Working with linear transformations instead of matrices, we let  $A$  and  $B$  be a pair of commuting elements of  $\text{Hom}_K(V, V)$  where  $V$  is an  $n$ -dimensional  $K$ -space. We use induction on  $n$ , remarking that the result is trivially true for  $n = 1$ . Assume it true for matrices in  $K_m$ ,  $m < n$ , where now  $n > 1$ .

Now define

$$W = \{v \in V : Av = \alpha_1 v\}.$$

Since  $\alpha_1$  is a characteristic root of  $A$ , we conclude that  $W \neq (0)$ . Setting  $A_1 = A|W$ , we have

$$A_1 w = \alpha_1 w, \quad w \in W.$$

Hence if  $(W:K) = r$ , then  $A_1$  has  $\alpha_1$  as characteristic root with multiplicity  $r$ . Therefore  $\alpha_1$  is a characteristic root of  $A$  with multiplicity at least  $r$ , say  $\alpha_1 = \dots = \alpha_r$ . For each  $w \in W$ , we have

$$ABw = BAw = \alpha_1 Bw,$$

so  $BW \subset W$ . Letting  $B_1 = B|W$ , we see that  $A_1 B_1 \in \text{Hom}_K(W, W)$ ,

and the characteristic roots of  $A_1B_1$  are just  $\alpha_i$  times those of  $B_1$ . But the characteristic roots of  $B_1$  are among those of  $B$ , say  $\beta_1, \dots, \beta_r$ . Thus the characteristic roots of  $A_1B_1$  are  $\alpha_1\beta_1, \dots, \alpha_r\beta_r$ . If  $W = V$ , then the theorem is proved; therefore we may assume  $W \neq V$ .

We next observe that  $A$  induces a linear transformation  $A_2$  on  $V/W$ , and likewise  $B$  induces  $B_2$ . Since  $AB = BA$ , we have also  $A_2B_2 = B_2A_2$ . By numbering the  $\{\alpha_i\}$  so that  $\alpha_{r+1}, \dots, \alpha_n$  are the characteristic roots of  $A_2$ , the induction hypothesis shows that we may number the characteristic roots  $\beta_{r+1}, \dots, \beta_n$  of  $B_2$  so that  $\alpha_{r+1}\beta_{r+1}, \dots, \alpha_n\beta_n$  are the characteristic roots of  $A_2B_2$ . Since the characteristic roots of  $AB$  are those of  $A_1B_1$  together with those of  $A_2B_2$ , this completes the proof of the first part of the theorem.

Applying the foregoing argument to  $B = F(A)$ , we see that

$$B \cdot w = F(\alpha_1) \cdot w, \quad w \in W,$$

and so  $B|W$  has  $F(\alpha_1)$  as a characteristic root of multiplicity  $r$ . (Likewise when  $B = A^{-1}$ , the matrix of  $B|W$  has  $\alpha^{-1}$  as characteristic root of multiplicity  $r$ .) Using the induction hypothesis to determine the characteristic roots of  $B|(V/W)$ , the result follows as above. This completes the proof of (30.2).

Now let  $KG$  be the group algebra of a finite group  $G$  over a field  $K$ . By a  $KG$ -module we shall mean here a left  $KG$ -module which has a finite  $K$ -basis. If  $\{m_1, \dots, m_n\}$  is a  $K$ -basis of a  $KG$ -module  $M$ , then setting

$$xm_i = \sum_{j=1}^n t_{ji}(x)m_j, \quad t_{ji}(x) \in K, x \in KG,$$

we have seen that  $M$  affords the matrix representation  $x \rightarrow T(x)$  of  $KG$  where  $T(x) \in K_n$  has  $t_{ij}(x)$  as its  $(i, j)$ -entry. Set

$$\mu(x) = \text{tr}(T(x)) = \sum_{i=1}^n t_{ii}(x), \quad x \in KG.$$

By Exercise 8.1, for each  $x \in KG$  the value  $\mu(x)$  depends only upon the module  $M$  and not upon the  $K$ -basis used in obtaining a matrix representation.

(30.3) DEFINITION. Let the  $KG$ -module  $M$  afford a matrix representation  $T$ , and set  $\mu(x) = \text{tr}(T(x))$ ,  $x \in KG$ . The map  $\mu: KG \rightarrow K$  given by  $x \rightarrow \mu(x)$  is called the *character* of  $M$  (or of  $T$ ), and we say that  $M$  (or  $T$ ) *affords* the character  $\mu$ . Obviously

$$\mu(1) = (M: K) ,$$

where 1 is the unity element of  $KG$ . Furthermore we have

$$(30.4) \quad \mu(x+y) = \mu(x) + \mu(y) , \quad \mu(\alpha x) = \alpha \mu(x) , \quad x, y \in KG, \alpha \in K .$$

*Caution:*  $\mu(xy) \neq \mu(x)\mu(y)$  in general, since the trace function is not multiplicative.

By a *group character* we mean the restriction of  $\mu$  to  $G$ . A character  $\mu$  is completely determined by its restriction to  $G$ , as is evident from (30.4). We shall use repeatedly

(30.5) *Each group character  $\mu$  is a class function on  $G$ ; that is, for  $g \in G$  the value  $\mu(g)$  depends only upon the conjugate class to which  $g$  belongs.*

PROOF. If  $g, h \in G$ , we have

$$\begin{aligned} \mu(g) &= \text{tr } \mathbf{T}(g) = \text{tr } \mathbf{T}(h)\mathbf{T}(g)\mathbf{T}(h)^{-1} \\ &= \text{tr } \mathbf{T}(hgh^{-1}) = \mu(hgh^{-1}) . \end{aligned}$$

Isomorphic modules clearly afford the same character. In matrix terminology this means that equivalent representations afford the same character. We shall see later that the converse of this is valid if  $\text{char } K = 0$  but need not hold otherwise.

As an illustration, let us calculate the character  $\mu$  afforded by the left regular  $KG$ -module  $KG$ , using the  $K$ -basis consisting of the elements  $g_1 (= 1), g_2, \dots, g_N$  of  $G$ . For each  $g \in G$ , set

$$g \cdot g_i = \sum_{j=1}^N t_{ji}(g)g_j , \quad t_{ji}(g) \in K .$$

Then by definition

$$\mu(g) = \sum_{i=1}^N t_{ii}(g) , \quad g \in G ,$$

so that in order to calculate  $\mu(g)$ , it suffices to know for each  $j$  the coefficient of  $g_j$  in the expression for  $gg_i$ . We evidently have  $\mu(1) = N$ . On the other hand if  $g \neq 1$ , then  $gg_i$  is a group element distinct from  $g_i$ , and so  $t_{ii}(g) = 0$ . We have therefore shown that

$$\mu(g) = \begin{cases} [G: 1] , & g = 1 , \\ 0 , & g \neq 1 . \end{cases}$$

Now let

$$(30.6) \quad M = M_k \supset M_{k-1} \supset \cdots \supset M_1 \supset M_0 = (0)$$

be a chain of  $KG$ -modules, and let  $\mu_i$  be the character afforded by the factor module  $M_i/M_{i-1}$ ,  $1 \leq i \leq k$ . Then we claim that  $M$  affords the character  $\mu_1 + \cdots + \mu_k$ . For, as in (13.11), we may adapt a  $K$ -basis of  $M$  to the above chain of submodules. The matrix representation afforded by  $M$  takes the form

$$x \rightarrow T(x) = \begin{pmatrix} T_1(x) & & & \\ & * & & \\ T_2(x) & & & \\ & . & . & \\ & & . & \\ & 0 & & \\ & & & T_k(x) \end{pmatrix}, \quad x \in KG,$$

where  $T_i$  is the representation afforded by  $M_i/M_{i-1}$ ,  $1 \leq i \leq k$ . Therefore

$$\text{tr } T(x) = \mu_1(x) + \cdots + \mu_k(x), \quad x \in KG,$$

which proves the result.

Of particular importance is the special case where (30.6) is a composition series for  $M$ . From it we deduce

(30.7) **THEOREM.** *The character of a  $KG$ -module  $M$  is the sum of the characters of the composition factors of  $M$ . The same reasoning shows that the character of a direct sum  $M_1 + \cdots + M_k$  of  $KG$ -modules is the sum of the characters of the summands.*

Let  $M, N$  be  $KG$ -modules with characters  $\mu, \nu$  respectively. Since the character of  $M + N$  is  $\mu + \nu$ , we see that the sum of two characters is again a character. We shall show that also the product of two group characters is a group character, by means of the following construction (see § 12): For each  $x \in G$ , let  $T(x): m \rightarrow xm$ ,  $m \in M$ , and let  $U(x): n \rightarrow xn$ ,  $n \in N$ . Then  $T(x)$  and  $U(x)$  are linear transformations, and we may form the linear transformation  $T(x) \otimes U(x)$  of  $M \otimes_K N$  into itself. Then  $x \rightarrow T(x) \otimes U(x)$  is a representation of  $G$ . If we define

$$(30.8) \quad x(\sum m_i \otimes n_i) = (T(x) \otimes U(x))(\sum m_i \otimes n_i) \\ = \sum xm_i \otimes xn_i, \quad x \in G,$$

and extend this definition by linearity to  $KG$ , then  $M \otimes_K N$  becomes a left  $KG$ -module. By Exercise 12.1, we know that

$$\text{tr } (T(x) \otimes U(x)) = (\text{tr } T(x))(\text{tr } U(x)) \\ = \mu(x)\nu(x), \quad x \in G.$$

We have therefore established

(30.9) THEOREM. Let  $M, N$  be  $KG$ -modules with characters  $\mu, \nu$  respectively. Equation (30.8) makes  $M \otimes_K N$  into a  $KG$ -module whose character  $\tau$  is given by

$$\tau(x) = \mu(x)\nu(x), \quad x \in G.$$

Note that  $\tau(x) = \mu(x)\nu(x)$  does not hold for all elements  $x \in KG$ .

We shall use repeatedly

(30.10) Let  $\mathbf{T}$  be a matrix representation of  $KG$  with character  $\tau$ . Then for each  $g \in G$ ,  $\tau(g)$  is a sum of roots of unity over  $K$ .

PROOF. Let  $g \in G$  have order  $n$ ; then

$$\{\mathbf{T}(g)\}^n = \mathbf{I}.$$

From (30.2) it follows that every characteristic root of  $\mathbf{T}(g)$  is an  $n$ th root of 1 over  $K$ . Since  $\tau(g)$  is the sum of the characteristic roots of  $\mathbf{T}(g)$ , the result is established.

(30.11) COROLLARY. Keeping the above notation, suppose further that  $K$  is an algebraic number field, and let  $t = \text{degree of } \mathbf{T}$ . Then for each  $g \in G$  the value  $\tau(g)$  is an algebraic integer<sup>†</sup>, and we have

$$|\tau(g)| \leq t$$

with equality if and only if  $\mathbf{T}(g) = \alpha \mathbf{I}$  for some  $\alpha \in K$ .

PROOF. Let  $\zeta_1, \dots, \zeta_t$  be the characteristic roots of  $\mathbf{T}(g)$ . Each  $\zeta_i$  is an  $n$ th root of 1 over  $Q$ , where  $n$  is the order of  $g$ , and so taking absolute values we have, since  $|\zeta_i| = 1$ ,

$$|\tau(g)| = |\zeta_1 + \dots + \zeta_t| \leq |\zeta_1| + \dots + |\zeta_t| = t.$$

Furthermore, for complex numbers  $\xi, \eta$ , we have  $|\xi + \eta| = |\xi| + |\eta|$  if and only if  $\xi = a\eta$  for some real  $a > 0$ . Hence  $|\tau(g)| = t$  implies that

$$\zeta_1 = \dots = \zeta_t.$$

For brevity, set  $\alpha = \zeta_1$ . Then  $\mathbf{T}(g)$  satisfies the two equations

$$\mathbf{X}^n = \mathbf{I}, \quad (\mathbf{X} - \alpha \mathbf{I})^t = \mathbf{0},$$

and thus  $\mathbf{T}(g)$  is a zero of the G.C.D. of the polynomials

$$\mathbf{X}^n - 1, \quad (\mathbf{X} - \alpha)^t.$$

---

<sup>†</sup> See §17.

This G.C.D. is precisely  $X - \alpha$ , since  $X^n - 1$  has no repeated factors, and therefore  $T(g) = \alpha I$ . This proves the corollary.

For the remainder of this section, let  $Z_1, \dots, Z_s$  denote a full set of non-isomorphic irreducible  $KG$ -modules. (If  $\text{char } K \nmid [G:1]$  and if  $K$  is a splitting field for  $KG$ , we know by (27.22) that  $s$  is the number of conjugate classes in  $G$ , whereas if  $\text{char } K \mid [G:1]$  then  $s$  is less than or equal to the number of classes. For the time being we shall not assume  $\text{char } K \nmid [G:1]$ , but shall consider the general case). If  $M$  is any  $KG$ -module, we write

$$M \approx a_1 Z_1 + \cdots + a_s Z_s,$$

where the  $\{a_i\}$  are non-negative integers, to indicate that of the composition factors of  $M$  exactly  $a_1$  of them are isomorphic to  $Z_1$ ,  $a_2$  of them to  $Z_2$ , and so on.

Let

$$\begin{aligned} \zeta^{(i)} &= \text{character afforded by } Z_i, \\ z_i &= \zeta^{(i)}(1) = (Z_i:K), \quad 1 \leq i \leq s. \end{aligned}$$

By (30.7), the character  $\mu$  afforded by  $M$  is given by

$$\mu = a_1 \zeta^{(1)} + \cdots + a_s \zeta^{(s)}.$$

As a consequence of the Burnside-Frobenius-Schur theorem of §27, we obtain the fundamental result:

(30.12) **THEOREM.** *The functions  $\zeta^{(1)}, \dots, \zeta^{(s)}$  are linearly independent over  $K$  under either of the following hypotheses:*

- (i)  $K$  is a splitting field for  $G$ ,
- (ii)  $\text{char } K = 0$ .

**PROOF.** If (i) holds, then for every irreducible  $KG$ -module  $M$  we have

$$(30.13) \quad \text{Hom}_{KG}(M, M) \cong K.$$

Using this fact, we find that the proof of (27.8) goes through even when  $K$  is not algebraically closed, since only (30.13) is needed in the proof. But  $\zeta^{(1)}, \dots, \zeta^{(s)}$  are disjoint sums of coordinate functions and hence are linearly independent over  $K$  by (27.8).

Suppose on the other hand that  $\text{char } K = 0$ , and choose an extension field  $L$  of  $K$  which is a splitting field for  $G$ . [The existence of such an  $L$  follows from (29.20)]. Let  $W_1, \dots, W_r$  be a full set of non-isomorphic irreducible  $LG$ -modules, and let  $\omega^{(j)}$  be the character afforded by  $W_j$ ,  $1 \leq j \leq r$ . We may set

$$Z_i^L \approx \sum a_{ij} W_j, \quad a_{ij} \in Z,$$

and therefore (since  $Z_i$  and  $Z_i^L$  afford the same group character)

$$\zeta^{(i)} = \sum a_{ij} \omega^{(j)}, \quad 1 \leq i \leq s,$$

where now  $\zeta^{(i)}$  is a character on  $LG$ . However, for  $i \neq i'$ , the modules  $Z_i^L$  and  $Z_{i'}^L$  cannot have a composition factor in common, since if they did, then by (29.6) also  $Z_i$  and  $Z_{i'}$  would have a common composition factor, which is impossible. Thus no  $\omega^{(j)}$  can occur with positive coefficient in both  $\zeta^{(i)}$  and  $\zeta^{(i')}$  when  $i \neq i'$ . By part (i) of this proof, the characters  $\{\omega^{(j)}\}$  are linearly independent over  $L$ . Hence the  $\{\zeta^{(i)}\}$  are also linearly independent over  $L$ , and so also over  $K$ . This completes the proof.

(30.14) COROLLARY. *Let  $M, N$  be  $KG$ -modules with characters  $\mu, \nu$ , respectively, and let  $\text{char } K = 0$ . Then  $M \cong N$  if and only if  $\mu = \nu$ .*

PROOF. We need only prove that  $\mu = \nu$  implies  $M \cong N$ . Let

$$M \approx a_1 Z_1 + \cdots + a_s Z_s, \quad N \approx b_1 Z_1 + \cdots + b_s Z_s.$$

From  $\mu = \nu$  we conclude that

$$\sum_{i=1}^s (a_i - b_i) \zeta^{(i)} = 0,$$

and so by the preceding theorem each  $a_i - b_i = 0$ . Therefore  $M$  and  $N$  have the same composition factors. However, every  $KG$ -module is completely reducible since  $\text{char } K = 0$ , and therefore  $M \cong N$ .

We give an example to show that the hypothesis “ $\text{char } K = 0$ ” cannot be omitted. Let  $\text{char } K = p \neq 0$ , let  $G$  be any finite group, and define representations  $T, U$  by means of

$$T(g) = I^{(p)}, \quad U(g) = I^{(2p)}, \quad g \in G.$$

Then the characters afforded by  $T$  and  $U$  vanish on  $KG$ , but nevertheless  $T$  and  $U$  are not equivalent.

In the general case, we may however establish

(30.15) THEOREM. *Let  $M, N$  be absolutely irreducible  $KG$ -modules with characters  $\mu, \nu$ , respectively. Then  $M \cong N$  if and only if  $\mu = \nu$ .*

PROOF. It suffices to show that if  $M \not\cong N$ , then  $\mu \neq \nu$ . Let us set

$$A = KG/\text{rad } KG.$$

Then  $A$  is a semi-simple algebra over  $K$ . Then [using (25.24)]  $M$  and  $N$  are irreducible  $A$ -modules, and may be taken as minimal left ideals in certain simple components of  $A$ , say  $M$  is a left ideal in the component  $A_1$ ,  $N$  in  $A_2$ . Since  $M \not\cong N$ , we conclude that  $A_1$  and  $A_2$  are distinct. The absolute irreducibility of  $M$  and  $N$  implies that

$$A_1 \cong K_m, \quad A_2 \cong K_n$$

where

$$m = (M: K), \quad n = (N: K).$$

If  $M$  affords the matrix representation  $\mathbf{M}$  and  $N$  affords  $N$ , the proof of Theorem 27.8 guarantees the existence of an element  $\bar{x} \in A$  such that

$$\mathbf{M}(\bar{x}) = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ \cdot & \cdot & \cdots & \cdot \\ 0 & 0 & \cdots & 0 \end{pmatrix}, \quad N(\bar{x}) = \mathbf{0}.$$

If  $x \in KG$  is chosen to lie in the residue class  $\bar{x}$  of  $A$ , we have

$$\mu(x) = 1, \quad \nu(x) = 0.$$

This shows that  $\mu \neq \nu$ , and completes the proof.

To obtain further information in the case where  $\text{char } K \neq 0$ , we consider the characteristic roots instead of the traces of the representing matrices. We prove

(30.16) **THEOREM (Brauer-Nesbitt [1]).** *Let  $M, N$  be  $KG$ -modules affording matrix representations  $\mathbf{M}, \mathbf{N}$ , respectively. Suppose there exists\* an extension field  $L$  of  $K$  such that  $L$  is a splitting field for  $G$ , and with the property that if  $V$  is a completely reducible  $KG$ -module, then  $V^L$  is a completely reducible  $LG$ -module. (We may take  $L = K$  if  $K$  is already a splitting field.) Then  $M$  and  $N$  have the same composition factors if and only if for each  $g \in G$ , the matrices  $\mathbf{M}(g), \mathbf{N}(g)$  have the same characteristic roots (counted according to their multiplicities).*

**PROOF.** The result follows from Theorem 30.14 when  $\text{char } K = 0$ , and so suppose hereafter that  $\text{char } K = p \neq 0$ . In one direction the

---

\* In Chapter X (§ 69) we shall show that such a field  $L$  exists if  $K$  is any finite field, or more generally, any perfect field.

proof is trivial, so now let us assume that, for each  $g \in G$ , the matrices  $M(g), N(g)$  have the same characteristic roots. Replacing  $M$  by the direct sum of its composition factors does not change the set of characteristic roots of  $M(g)$ , so that for the remainder of the proof we may assume that  $M$  and  $N$  are direct sums of irreducible  $KG$ -modules. After pairing off as many summands as possible which occur in both  $M$  and  $N$ , we are left with a pair of completely reducible  $KG$ -modules  $M', N'$  having no common composition factor, and such that for each  $g \in G$ , the matrices  $M'(g), N'(g)$  have the same characteristic roots. We shall show that  $M' = N' = (0)$ , which will prove the theorem.

If  $M'$  and  $N'$  are not  $(0)$ , set  $T = (M')^L, U = (N')^L$ . Then by (29.6),  $T$  and  $U$  have no common composition factor, and we know that for each  $g \in G$ , the matrices  $T(g), U(g)$  have the same characteristic roots. Let  $W_1, \dots, W_r$  be a full set of non-isomorphic irreducible  $LG$ -modules; by (30.12), their characters  $\omega^{(1)}, \dots, \omega^{(r)}$  are linearly independent over  $L$ . But if

$$T \approx \sum a_i W_i, \quad U \approx \sum b_i W_i,$$

then we have

$$\sum a_i \omega^{(i)} = \sum b_i \omega^{(i)},$$

whence for each  $i$ ,  $a_i - b_i = 0$  in  $L$ ; that is,

$$a_i \equiv b_i \pmod{p}.$$

However  $T$  and  $U$  have no common composition factor, and so for each  $i$  either  $a_i = 0$  or  $b_i = 0$ . Therefore  $p|a_i$  and  $p|b_i$  for each  $i$ . Setting  $a'_i = pa_i, b'_i = pb_i$  for each  $i$ , define

$$T' \approx \sum a'_i W_i, \quad U' \approx \sum b'_i W_i.$$

Then  $T'$  and  $U'$  have no common composition factor. Furthermore the characteristic roots of  $T(g)$  are those of  $T'(g)$ , each counted  $p$  times, and analogously for  $U(g)$ , which shows that for each  $g \in G$ , the matrices  $T'(g), U'(g)$  have the same characteristic roots. But then as above  $p|a'_i$  and  $p|b'_i$  for each  $i$ . This process can be continued indefinitely, and thus each  $a_i$  and each  $b_i$  is divisible by arbitrarily high powers of  $p$ . Hence  $a_i = b_i = 0$  for all  $i$ , and so  $M' = N' = (0)$ . This completes the proof of the theorem.

### Exercises

1. Show by example that if  $A, B \in K_n$  fail to satisfy  $AB = BA$ , the

characteristic roots of  $AB$  need not be the products of those of  $A$  and  $B$ .

2. For the symmetric group on three symbols, compute the characters of its irreducible representations in the rational field. (See Exercise 28.1.)

3. Let the  $KG$ -module  $M$  afford the character  $\mu$ , where  $K$  is the complex field. Show that for each  $g \in G$ ,  $\mu(g^{-1}) = \overline{\mu(g)}$ , where the bar denotes the complex conjugate.

4. Let  $M, N$  be  $KG$ -modules with characters  $\mu, \nu$ , respectively, and assume that the composition factors of  $M$  and  $N$  are absolutely irreducible. Assume further that neither  $M$  nor  $N$  has a repeated composition factor. Prove that  $\mu = \nu$  if and only if  $M, N$  have the same composition factors.

5. Let  $M$  be an irreducible  $KG$ -module, and let  $\{m_1, \dots, m_n\}$  be a  $K$ -basis of  $M$ . Show that the  $KG$ -module  $M \otimes_K M$  contains the  $KG$ -submodules

$$N = \sum_{1 \leq i \leq j \leq n} K(m_i \otimes m_j + m_j \otimes m_i)$$

and

$$N' = \sum_{1 \leq i < j \leq n} K(m_i \otimes m_j - m_j \otimes m_i).$$

Hence if  $n > 1$  show that  $M \otimes_K M$  is reducible as  $KG$ -module.

6. Keeping the notation of Corollary 30.11, show that  $\tau(g) = \tau(1)$  if and only if  $T(g) = I$ .

7. Let  $T$  be a square matrix with complex entries such that  $T^n = I$  for some positive integer  $n$ . For  $m$  a positive integer, prove that  $T^m = I$  if and only if every characteristic root of  $T$  is an  $m$ th root of unity. [Hint: If every characteristic root of  $T$  is an  $m$ th root of 1, every characteristic root of  $T^m$  is 1. Since also  $T^m$  has finite order, it follows that  $T^m = I$ .]

## § 31. Orthogonality Relations

Let us assume throughout this section that  $K$  is a splitting field for the finite group  $G$ . (Later in this section we shall choose  $K$  to be the complex field, but we do not make that assumption at the outset.) Let  $Z_1, \dots, Z_s$  be a full set of non-isomorphic irreducible  $KG$ -modules. For each  $i$  between 1 and  $s$ , let  $Z_i$  afford the matrix representation  $Z_i$ , where

$$Z_i(g) = (a_{jk}^{(i)}(g)), \quad g \in G,$$

and let  $\zeta^{(i)}$  be the character of  $Z_i$ , so that

$$\zeta^{(i)}(g) = \sum_j a_{jj}^{(i)}(g), \quad g \in G.$$

Set

$$z_i = (Z_i: K) = \zeta^{(i)}(1).$$

We shall now obtain orthogonality relations which interconnect the irreducible characters  $\{\zeta^{(i)}\}$ . Rather than attempt to motivate each step, we shall just manipulate freely so as to derive the desired relations. Let  $C$  be an arbitrary  $z_m \times z_n$  matrix over  $K$ , and set

$$(31.1) \quad B = \sum_{g \in G} Z_m(g) C Z_n(g^{-1}) .$$

Using the fact that  $Z_m$  and  $Z_n$  are homomorphisms, we find at once that

$$Z_m(h)B = BZ_n(h) , \quad h \in G ,$$

so that  $B$  intertwines the representations  $Z_m$  and  $Z_n$ . By Schur's lemma 27.3, we have  $B = 0$  when  $m \neq n$ , whereas if  $m = n$  it follows from the fact that  $K$  is a splitting field that  $B$  is a scalar matrix  $b_m I$ , where  $b_m$  is a constant depending upon  $m$  and upon the choice of  $C$ . Set  $C = (c_{il})$ , and compare the  $(j, k)$ -entry on both sides of (31.1), thereby obtaining

$$\sum_{g,t,l} a_{jt}^{(m)}(g) c_{tl} a_{ik}^{(n)}(g^{-1}) = b_m \delta_{jk} \delta_{mn} .$$

In particular, fix  $u$  and  $i$ , and set  $c_{iu} = \delta_{iu} \delta_{ii}$ ; then we find

$$(31.2) \quad \sum_g a_{ju}^{(m)}(g) a_{ik}^{(n)}(g^{-1}) = b_m \delta_{jk} \delta_{mn} ,$$

and in particular

$$(31.3) \quad \sum_g a_{ju}^{(m)}(g) a_{ik}^{(m)}(g^{-1}) = b_m \delta_{jk}$$

where  $b_m$  depends upon  $m, u$ , and  $i$ , say  $b_m = b_m(u, i)$ . In (31.3), set  $g = h^{-1}$  so as to get

$$(31.4) \quad \sum_h a_{ik}^{(m)}(h) a_{ju}^{(m)}(h^{-1}) = b_m(u, i) \delta_{jk} .$$

But, by (31.3), the left-hand side of the above equation is equal to  $b_m(k, j) \delta_{iu}$ . Therefore  $b_m(u, i) \delta_{jk} = b_m(k, j) \delta_{iu}$  for all  $m, u, i, j, k$ ; thus  $b_m(i, i)$  is independent of  $i$ , and depends only upon  $m$ . Writing  $b_m$  instead of  $b_m(i, i)$ , we have

$$(31.5) \quad \sum_g a_{ju}^{(m)}(g) a_{ik}^{(m)}(g^{-1}) = b_m \delta_{jk} \delta_{ui} \delta_{mn} ,$$

and in this equation  $b_m$  depends only on  $m$  but not on  $j, u, i$ , or  $k$ . Now fix  $h \in G$ , multiply the above by  $a_{ij}^{(m)}(h)$ , and sum on  $j$ . Making use of the formula

$$a_{iu}^{(m)}(hg) = \sum_j a_{ij}^{(m)}(h) a_{ju}^{(m)}(g) ,$$

which is a consequence of

$$\mathbf{Z}_m(hg) = \mathbf{Z}_m(h)\mathbf{Z}_m(g),$$

we then obtain

$$\sum_g a_{lu}^{(m)}(hg)a_{ik}^{(n)}(g^{-1}) = a_{lk}^{(m)}(h)b_m\delta_{lu}\delta_{mn}.$$

Now set  $l = u$ ,  $k = i$ , and sum on  $u$  from 1 to  $z_m$ , on  $i$  from 1 to  $z_n$ ; the above yields

$$(31.6) \quad \sum_g \zeta^{(m)}(hg)\zeta^{(n)}(g^{-1}) = \zeta^{(m)}(h)b_m\delta_{mn}.$$

In particular, when  $h = 1$ , this becomes

$$(31.7) \quad \sum_g \zeta^{(m)}(g)\zeta^{(n)}(g^{-1}) = z_m b_m \delta_{mn}.$$

In order to evaluate  $b_m$ , we set  $u = i$ , and  $j = k$  in (31.3), and then sum on  $i$  from 1 to  $z_m$ , thereby obtaining

$$\sum_{g,i} a_{jl}^{(m)}(g)a_{ij}^{(m)}(g^{-1}) = z_m b_m.$$

The left-hand side is just the  $(j, j)$ -entry of

$$\sum_g \mathbf{Z}_m(g)\mathbf{Z}_m(g^{-1}).$$

Since  $\mathbf{Z}_m(g)\mathbf{Z}_m(g^{-1}) = I$ , we conclude that

$$b_m z_m = [G: 1] \quad \text{for each } m.$$

Thus (31.7) may be rewritten in the form

$$(31.8) \quad \sum_g \zeta^{(m)}(g)\zeta^{(n)}(g^{-1}) = [G: 1]\delta_{mn},$$

which is our first orthogonality relation for the group characters.

Before proceeding with our discussion, we make the simplifying assumption that  $\text{char } K \nmid [G: 1]$ . Since  $K$  is a splitting field for  $G$  and since  $KG$  is semi-simple, the proof of Theorem 27.22 shows that the number of non-isomorphic irreducible  $KG$ -modules coincides with the number of conjugate classes in  $G$ . Let us denote these classes by

$$\mathfrak{C}_1 (= 1), \mathfrak{C}_2, \dots, \mathfrak{C}_s.$$

By (30.5), the value  $\zeta^{(m)}(g)$  depends only upon the class to which  $g$  belongs, so we may define

$$(31.9) \quad \zeta_i^{(m)} = \zeta^{(m)}(g) \quad \text{for any } g \in \mathfrak{C}_i.$$

Let us also introduce the symbol  $\mathbb{C}_{i^*}$  which is to denote the class consisting of the inverses of the elements in  $\mathbb{C}_i$ . Specifically, we have

(31.10) **DEFINITION.** Let  $G$  be a group with conjugate classes  $\mathbb{C}_1, \dots, \mathbb{C}_s$ . For each  $i$ , define an integer  $i^*$  by the rule

$$g \in \mathbb{C}_i \quad \text{if and only if} \quad g^{-1} \in \mathbb{C}_{i^*}.$$

In that case we have for each  $m$ ,

$$\zeta^{(m)}(g^{-1}) = \zeta_{i^*}^{(m)} \quad \text{for all } g \in \mathbb{C}_i.$$

For the remainder of this chapter, let

$$h_i = \text{number of elements in } \mathbb{C}_i, \quad 1 \leq i \leq s.$$

By grouping the terms in (31.8) according to the class in which  $g$  lies, we obtain

$$(31.11) \quad \sum_{i=1}^s h_i \zeta_i^{(m)} \zeta_{i^*}^{(n)} = [G: 1] \delta_{mn}.$$

Let  $Z$  be the  $s \times s$  matrix whose  $(i, j)$ -entry is  $\zeta_j^{(i)}$ , and let  $W \in K_s$  have  $(i, j)$ -entry  $h_i \zeta_{i^*}^{(j)}$ . Then equation (31.11) is equivalent to the statement that

$$ZW = [G: 1]I.$$

Since we are assuming that  $[G: 1] \neq 0$  in  $K$ , we may conclude that  $Z$  and  $W$  are non-singular and that

$$W = [G: 1]Z^{-1}.$$

Therefore we have  $WZ = [G: 1]I$ , which yields

$$(31.12) \quad \sum_{n=1}^s h_i \zeta_{i^*}^{(n)} \zeta_j^{(n)} = [G: 1] \delta_{ij}.$$

Now  $h_i | [G: 1]$  so that  $h_i \neq 0$  in  $K$ , and we may therefore divide by  $h_i$  in the above equation. Letting  $g_i$  denote an element of class  $\mathbb{C}_i$ ,  $1 \leq i \leq s$ , we have consequently

$$(31.13) \quad \sum_{n=1}^s \zeta^{(n)}(g_i) \zeta^{(n)}(g_j^{-1}) = \frac{[G: 1]}{h_i} \delta_{ij}.$$

This is our second important orthogonality relation.

Setting  $g_i = g_j = 1$ , so that also  $h_i = 1$ , the above yields the familiar relation [see (27.21)]

$$(31.14) \quad \sum_{n=1}^s z_n^2 = [G: 1].$$

The orthogonality relations (31.5) and (31.13) are by no means independent of one another, and indeed Nagao [1] has shown that by assuming only (31.13) with  $g_i = 1$ , it is possible to derive formulas (31.5) and (31.13).

As a simple consequence of the orthogonality relations, we give a criterion for the irreducibility of a  $KG$ -module in terms of its character.

(31.15) *Let  $M$  be a  $KG$ -module with character  $\mu$ , where  $K$  is a splitting field for  $G$  such that  $\text{char } K = 0$ . Then  $M$  is irreducible if and only if*

$$\sum_{g \in G} \mu(g)\mu(g^{-1}) = [G: 1].$$

PROOF. In terms of the earlier notation, we may write

$$M \approx a_1 Z_1 + \cdots + a_s Z_s, \quad \mu = a_1 \zeta^{(1)} + \cdots + a_s \zeta^{(s)}.$$

Then

$$\begin{aligned} \sum_g \mu(g)\mu(g^{-1}) &= \sum_g \sum_{i,j} a_i a_j \zeta^{(i)}(g) \zeta^{(j)}(g^{-1}) \\ &= \sum_{i,j} a_i a_j [G: 1] \delta_{ij} \\ &= [G: 1] \sum_{i=1}^s a_i^2, \end{aligned}$$

which at once implies the desired result.

Finally we turn to the case where  $K$  is the complex field. For  $\alpha \in K$ , let  $\bar{\alpha}$  be its complex conjugate. If  $\alpha$  is a root of unity, then

$$|\alpha|^2 = \alpha \bar{\alpha} = 1,$$

so that

$$\bar{\alpha} = \alpha^{-1}.$$

But if  $T$  is a matrix representation of  $G$  in  $K$ , each characteristic root of  $T(g)$ ,  $g \in G$ , is a root of unity. Since the characteristic roots of  $T(g^{-1})$  are the inverses of those of  $T(g)$ , we conclude that

$$\text{tr } T(g^{-1}) = \overline{\text{tr } T(g)}.$$

Hence if  $\tau$  is the character of  $T$ , we have

$$\tau(g^{-1}) = \overline{\tau(g)}, \quad g \in G.$$

In terms of complex conjugates, our main orthogonality relations now become

$$(31.16) \quad \sum_{g \in G} \zeta^{(m)}(hg) \overline{\zeta^{(n)}(g)} = \frac{\zeta^{(m)}(h)[G:1]}{z_m} \delta_{mn},$$

$$(31.17) \quad \sum_{g \in G} \zeta^{(m)}(g) \overline{\zeta^{(n)}(g)} = [G:1] \delta_{mn},$$

$$(31.18) \quad \sum_{i=1}^s h_i \zeta_i^{(m)} \overline{\zeta_i^{(n)}} = [G:1] \delta_{mn},$$

$$(31.19) \quad \sum_{n=1}^s \zeta_i^{(n)} \overline{\zeta_j^{(n)}} = \sum_{n=1}^s \zeta_i^{(n)} \zeta_{j*}^{(n)} = \frac{[G:1]}{h_i} \delta_{ij}.$$

It is convenient to introduce the following terminology

(31.20) **DEFINITION.** The representation  $g \rightarrow (1)$ ,  $g \in G$ , is called the *1-representation* of  $G$ . Its character  $\zeta^{(1)}$  is the *1-character* (or *principal character*) of  $G$ .

(31.21) **THEOREM.** For  $1 \leq i \leq s$ , define  $\overline{\zeta^{(i)}}: KG \rightarrow K$  by means of

$$\overline{\zeta^{(i)}}: g \rightarrow \overline{\zeta^{(i)}(g)}, \quad g \in G,$$

where  $K$  is the complex field. Then  $\overline{\zeta^{(i)}}$  is one of the irreducible characters  $\{\zeta^{(j)}\}$ .

**PROOF.** Let  $\zeta^{(i)}$  be the character of the matrix representation  $Z_i$ . The mapping

$$U: g \rightarrow {}^t Z_i(g^{-1}), \quad g \in G,$$

where  ${}^t Z$  is the transpose of  $Z$ , is again an irreducible matrix representation of  $G$ . The character  $\eta$  afforded by  $U$  is given by

$$\begin{aligned} \eta(g) &= \text{tr } {}^t Z_i(g^{-1}) \\ &= \text{tr } Z_i(g^{-1}) = \overline{\zeta^{(i)}(g)}. \end{aligned}$$

This completes the proof.

### Exercises

- Let  $\mu$  and  $\nu$  be complex-valued functions on  $G$ . Define their inner product by

$$(\mu, \nu) = [G:1]^{-1} \sum_{g \in G} \mu(g) \nu(g^{-1}).$$

Prove that

$$(\zeta^{(1)}, \zeta^{(j)}) = (\zeta^{(j)}, \zeta^{(i)}) = \delta_{ij}.$$

Moreover prove that  $\zeta^{(1)}, \dots, \zeta^{(s)}$  form a basis for the complex vector space of class functions on  $G$ , and that if  $\varphi$  is any class function on  $G$ , we have

$$\varphi = \sum_{i=1}^s (\varphi, \zeta^{(i)}) \zeta^{(i)}.$$

Now let  $\{a_{tu}^{(i)}\}$  denote the coordinate functions of the irreducible representations  $Z_1, \dots, Z_s$ , given by the formulas

$$Z_i(g) = (a_{tu}^{(i)}(g)), \quad 1 \leq i \leq s, 1 \leq t, u \leq z_i.$$

Prove that

$$(a_{tu}^{(i)}, a_{vw}^{(j)}) = \frac{\delta_{ij}\delta_{tw}\delta_{uv}}{z_i}.$$

Finally prove that any complex-valued function  $\psi$  on  $G$  can be expressed as a linear combination of the coordinate functions

$$\psi(g) = \sum \xi_{jk}^i a_{jk}^{(i)}(g), \quad g \in G,$$

where the coefficients are given by

$$\xi_{jk}^i = z_i(\psi, a_{kj}^{(i)}).$$

2. Let  $[G:1] = 2N - 1$ , and let  $\zeta$  be any  $\zeta^{(i)}$  distinct from the 1-character  $\zeta^{(1)}$ . Prove that  $\zeta \neq \bar{\zeta}$  and hence that  $\zeta$  is not the character of any real irreducible representation of  $G$ . Therefore the only real absolutely irreducible representation of  $G$  is the 1-representation. [Hint: Suppose  $\zeta = \bar{\zeta}$  and  $\zeta \neq \zeta^{(1)}$ . Then by (31.8) we have  $\sum_g \zeta(g) = 0$ , so

$$\sum_{g \neq 1} \zeta(g) = -\zeta(1).$$

We shall show later that  $\zeta(1) | [G:1]$  [see (33.7)], so that  $\zeta(1)$  is an odd rational integer. On the other hand, the elements of  $G$  distinct from 1 may be arranged in  $N - 1$  disjoint pairs

$$\{g_2, g_2^{-1}\}, \{g_3, g_3^{-1}\}, \dots, \{g_N, g_N^{-1}\}$$

since only the identity element of a group of odd order can coincide with its inverse. Thus

$$\begin{aligned} \sum_{g \neq 1} \zeta(g) &= \sum_{i=2}^N \{\zeta(g_i) + \zeta(g_i^{-1})\} = \sum_i \{\zeta(g_i) + \overline{\zeta(g_i)}\} \\ &= 2 \sum_{i=2}^N \zeta(g_i), \end{aligned}$$

using  $\zeta = \bar{\zeta}$ . Therefore

$$\sum_{i=2}^N \zeta(g_i) = -\frac{1}{2}\zeta(1),$$

which is impossible since the left-hand side is an algebraic integer.]

3. Let  $\zeta$  be any  $\zeta^{(t)}$  such that  $z = \zeta(1) > 1$ . Then  $\zeta(g) = 0$  for at least one element  $g \in G$ . (Burnside [1]). [Hint: Assume  $\zeta(g) \neq 0$  for all  $g \in G$ . We shall obtain a contradiction by using the orthogonality relation (31.18):

$$z^2 + \sum_{i=2}^s h_i |\zeta(g_i)|^2 = [G:1]$$

where  $g_i \in \mathfrak{C}_i$ . For fixed  $x \in G$  of order  $m$  (say), the elements  $\{x^r : 1 \leq r \leq m, (r, m) = 1\}$  fall into  $u$  classes (say), each class containing the same number  $t$  of these elements, with  $tu = \varphi(m)$ . Let  $y_1, \dots, y_u$  be representatives chosen from these classes. Then

$$t \cdot \sum |\zeta(y_i)|^2 = \sum_{\substack{1 \leq r \leq m \\ (r, m) = 1}} |\zeta(x^r)|^2.$$

Now  $\zeta(x)\overline{\zeta(x)}$  is a sum of  $m$ th roots of 1, and lies in  $Q(\sqrt[m]{1})$ . Considered as an element of this field, it has  $\varphi(m)$  algebraic conjugates, given by the terms on the right-hand side of the above equation. Therefore this right-hand side is the sum of all the algebraic conjugates of  $|\zeta(x)|^2$ ; since  $\zeta(x) \neq 0$  by hypothesis, the right-hand side is a rational integer greater than or equal to  $\varphi(m)$  by Exercise 20.5. Each  $x \in G, x \neq 1$ , determines a collection  $W(x)$  of classes of  $G$ , and two such collections  $W(x), W(x')$  either coincide or are disjoint. Let  $x \neq 1$  range over a system of elements of  $G$  such that  $\cup_x W(x)$  contains each class not equal to  $\{1\}$  exactly once. Then

$$\begin{aligned} \sum_{j \neq 1} h_j |\zeta(g_j)|^2 &= \sum_x \sum_{W(x)} h_i |\zeta(y_i)|^2 \\ &\geq \sum_x \sum_{W(x)} h_i \cdot 1 = \sum_{j \neq 1} h_j = [G:1] - 1. \end{aligned}$$

Thus

$$[G:1] = z^2 + \sum_{i=2}^s h_i |\zeta(g_i)|^2 \geq z^2 + [G:1] - 1,$$

which gives a contradiction.]

## § 32. Simple Applications of the Orthogonality Relations

In this section we shall consider a few straightforward consequences of the orthogonality relations and shall reserve some deeper results for subsequent sections. Throughout the section we consider only representations and characters defined over the field of complex numbers  $K$ .

### § 32A. Character tables

We shall now show how to find the irreducible characters of a

group in some easy cases. We may arrange the values  $\{\zeta_i^{(j)}\}$  so as to form the *character table* of  $G$ , in which the rows are indexed by the distinct irreducible characters starting with the 1-character, and the columns by the conjugate classes of  $G$ , starting with the class consisting of the identity element.

	$\mathfrak{C}_1$	$\dots$	$\mathfrak{C}_s$
$\zeta^{(1)}$	$\zeta_1^{(1)}$	$\dots$	$\zeta_s^{(1)}$
$\vdots$	$\vdots$		$\vdots$
$\zeta^{(s)}$	$\zeta_1^{(s)}$	$\dots$	$\zeta_s^{(s)}$

The different rows of the table are orthogonal to each other in the sense of (31.18), whereas by (31.19) the columns are orthogonal to each other in the usual sense of vectors in a complex unitary space. Other relations among the entries in the table will be established in § 32C and in § 33.

*Example 1. Character Table of  $S_3$ .* We know that  $S_3$  has two one-dimensional representations, which we may identify with their characters  $\zeta^{(1)}$  and  $\zeta^{(2)}$ , namely the 1-representation, and the homomorphism of  $S_3$  onto the group  $\{1, -1\}$  whose kernel is the alternating group  $A_3$ .

There are three classes in  $S_3$ , which are given by

$$\mathfrak{C}_1 = \{(1)\}, \quad \mathfrak{C}_2 = \{(12), (23), (13)\}, \quad \mathfrak{C}_3 = \{(123), (132)\}.$$

Therefore  $S_3$  has three irreducible characters altogether, and the sum of the squares of their degrees must be  $[S_3 : 1] = 6$ . The third character  $\zeta^{(3)}$  has degree 2. For our character table, we have

	$\mathfrak{C}_1$	$\mathfrak{C}_2$	$\mathfrak{C}_3$
$\zeta^{(1)}$	1	1	1
$\zeta^{(2)}$	1	-1	1
$\zeta^{(3)}$	2	$\alpha$	$\beta$

where  $\alpha$  and  $\beta$  remain to be determined. Using the orthogonality relations for columns, we have

$$1 \cdot 1 + 1 \cdot 1 + 2 \cdot \beta = 0, \quad 1 \cdot 1 + 1 \cdot (-1) + 2 \cdot \alpha = 0,$$

and we obtain  $\beta = -1$ ,  $\alpha = 0$ . The complete table is therefore

	$\mathfrak{C}_1$	$\mathfrak{C}_2$	$\mathfrak{C}_3$
$\zeta^{(1)}$	1	1	1
$\zeta^{(2)}$	1	-1	1
$\zeta^{(3)}$	2	0	-1

*Example 2. Character Table of  $A_4$ .* An easy calculation shows that  $A_4$  has the following classes

$$\mathfrak{C}_1 = \{1\}$$

$$\mathfrak{C}_2 = \{(12)(34), (13)(24), (14)(23)\}$$

$$\mathfrak{C}_3 = \{(123), (214), (341), (432)\}$$

$$\mathfrak{C}_4 = \{(132), (241), (314), (423)\}.$$

Next we note that

$$H = \{(1), (12)(34), (13)(24), (14)(23)\} \triangle A_4,$$

and that  $A_4/H$  is cyclic of order 3. Letting  $\omega$  be a primitive cube root of 1, we see that  $A_4/H$  has besides the 1-representation the representations

$$\begin{aligned} H \rightarrow 1, \quad (123)H \rightarrow \omega, \quad (132)H \rightarrow \omega^2, \\ H \rightarrow 1, \quad (123)H \rightarrow \omega^2, \quad (132)H \rightarrow \omega. \end{aligned}$$

Composing these representations with the natural homomorphism of  $A_4 \rightarrow A_4/H$ , we obtain three distinct one-dimensional representations of  $A_4$ , which we shall identify with their characters. Since there are four classes, there is one additional character of degree 3, as we find by setting the sum of squares of the degrees equal to  $[A_4 : 1] = 12$ . For the character table, we obtain

	$\mathfrak{C}_1$	$\mathfrak{C}_2$	$\mathfrak{C}_3$	$\mathfrak{C}_4$
$\zeta^{(1)}$	1	1	1	1
$\zeta^{(2)}$	1	1	$\omega$	$\omega^2$
$\zeta^{(3)}$	1	1	$\omega^2$	$\omega$
$\zeta^{(4)}$	3	$\alpha$	$\beta$	$\gamma$

Again using the orthogonality relations on the columns, we find easily that  $\alpha = -1$ ,  $\beta = \gamma = 0$ .

*Example 3. Character Table of  $S_4$ .* The conjugate classes of  $S_4$

are  $\mathfrak{C}_1 = \{(1)\}$ ,  $\mathfrak{C}_2 = \{2\text{-cycles}\}$ ,  $\mathfrak{C}_3 = \{3\text{-cycles}\}$ ,  $\mathfrak{C}_4 = \{4\text{-cycles}\}$ ,  $\mathfrak{C}_5 = \{(12)(34), (13)(24), (14)(23)\}$ . Since  $[S_4, S_4] = A_4$ , there are two one-dimensional representations  $\zeta^{(1)}$  and  $\zeta^{(2)}$ , where  $\zeta^{(2)}$  maps the elements of  $A_4$  onto +1 and the elements of  $(12)A_4$  onto -1. As in the case of  $A_4$ ,

$$H = \{(1), (12)(34), (14)(23), (13)(24)\}$$

turns out to be a normal subgroup of  $S_4$ , and, since  $S_4/H$  is non-abelian, we have  $S_4/H \cong S_3$  since  $S_3$  is the only non-abelian group of order 6. The character  $\zeta^{(3)}$  in Example 1 yields, upon composition with the natural homomorphism of  $S_4 \rightarrow S_4/H$ , a third irreducible character of degree 2. By equating the sum of squares of the degrees to 24, we see that the two remaining characters  $\zeta^{(4)}$  and  $\zeta^{(5)}$  both have degree 3. Finally, from (31.19), we have

$$\zeta_i^{(1)} \overline{\zeta_1^{(1)}} + \zeta_i^{(2)} \overline{\zeta_1^{(2)}} + \zeta_i^{(3)} \overline{\zeta_1^{(3)}} + \zeta_i^{(4)} \overline{\zeta_1^{(4)}} + \zeta_i^{(5)} \overline{\zeta_1^{(5)}} = 0, \quad i = 2, 3, 4, 5,$$

and this yields

$$\zeta_i^{(4)} + \zeta_i^{(5)} = 0, \quad i = 2, 3, 4,$$

and

$$\zeta_5^{(4)} + \zeta_5^{(5)} = -2.$$

Filling in the table on the basis of the information so far, we have

	$\mathfrak{C}_1$	$\mathfrak{C}_2$	$\mathfrak{C}_3$	$\mathfrak{C}_4$	$\mathfrak{C}_5$
$\zeta^{(1)}$	1	1	1	1	1
$\zeta^{(2)}$	1	-1	1	-1	1
$\zeta^{(3)}$	2	0	-1	0	2
$\zeta^{(4)}$	3	$\alpha$	$\beta$	$\gamma$	$\delta$
$\zeta^{(5)}$	3	$-\alpha$	$-\beta$	$-\gamma$	$-2 - \delta$

We count the number of elements in the different conjugate classes and apply (31.18). We have

$$h_1 = 1, \quad h_2 = 6, \quad h_3 = 8, \quad h_4 = 6, \quad h_5 = 3,$$

and

$$\begin{cases} 1 \cdot 1 \cdot 3 + 6 \cdot 1 \cdot \alpha + 8 \cdot 1 \cdot \beta + 6 \cdot 1 \cdot \gamma + 3 \cdot 1 \cdot \delta = 0 \\ 1 \cdot 1 \cdot 3 + 6 \cdot (-1) \cdot \alpha + 8 \cdot 1 \cdot \beta + 6 \cdot (-1) \cdot \gamma + 3 \cdot 1 \cdot \delta = 0 \\ 1 \cdot 2 \cdot 3 + 6 \cdot (0) \cdot \alpha + 8 \cdot (-1) \cdot \beta + 6 \cdot 0 \cdot \gamma + 3 \cdot 2 \cdot \delta = 0. \end{cases}$$

Adding the first two equations yields

$$6 + 16\beta + 6\delta = 0 ,$$

whereas the last may be written as

$$6 - 8\beta + 6\delta = 0 .$$

These imply  $\beta = 0$ ,  $\delta = -1$ . Using the orthogonality relations for columns 2 and 4, we have

$$\alpha\gamma = -1 ,$$

whereas, from our first set of equations, we have

$$\alpha + \gamma = 0 .$$

From these, we obtain  $\alpha = 1$ ,  $\gamma = -1$ , and the table is completed.

For references to other calculations for particular groups, see §20 of van der Waerden's book [1]. Some other remarks which are useful for purposes of calculation appear at the end of §33.

### § 32B. Permutation groups

Let  $G$  be a subgroup of  $S_n$  acting on the set  $X = \{x_1, \dots, x_n\}$ . For each  $g \in G$ , the map

$$x_i \rightarrow gx_i , \quad 1 \leq i \leq n ,$$

is representable by an  $n \times n$  matrix  $\mathbf{T}(g)$  with entries 0's and 1's. The trace  $\tau(g)$  of this matrix is just the number of symbols in the set  $X$  left fixed by  $g$ .

Suppose now that  $X$  has  $r$  orbits  $X_1, \dots, X_r$  relative to  $G$ ; then  $G$  acts transitively on each  $X_i$ , and we may write

$$\mathbf{T} = \begin{pmatrix} \mathbf{T}_1 & & & \\ & \mathbf{T}_2 & & \\ & & \ddots & \\ 0 & & & \mathbf{T}_r \end{pmatrix}$$

where  $\mathbf{T}_i(g)$  is the matrix describing the action of  $g$  on the orbit  $X_i$ . Thus

$$\tau = \tau_1 + \dots + \tau_r$$

where  $\tau_i$  is the character of  $\mathbf{T}_i$ . Let us write  $X_i = \{x_1, \dots, x_s\}$ , say,

and set

$$(32.1) \quad H_i = \{g \in G : gx_i = x_i\}, \quad 1 \leq i \leq s.$$

Since  $G$  acts transitively on  $X_1$ , the subgroups  $H_1, \dots, H_s$  are mutually conjugate in  $G$ , and so

$$[H_i : 1] = [H_1 : 1], \quad 1 \leq i \leq s.$$

Now, under the action of  $G$ , each  $x_i$  is left fixed by exactly  $[H_i : 1]$  elements of  $G$ . Thus

$$\sum_{g \in G} \tau_i(g) = \sum_{i=1}^s [H_i : 1] = s[H_1 : 1].$$

But on the other hand, the number of distinct images of  $x_1$  under  $G$  is  $[G : H_1]$ , which implies that  $s = [G : H_1]$ . Therefore

$$\sum_{g \in G} \tau_i(g) = [G : 1],$$

and consequently

$$(32.2) \quad \sum_{g \in G} \tau(g) = r[G : 1].$$

(32.3) **THEOREM.** *Let  $G$  be a permutation group on a set  $X$ , and let  $X$  split into  $r$  orbits under the action of  $G$ . Then the representation of  $G$  by permutation matrices has  $r$  composition factors isomorphic to the 1-representation.*

**PROOF.** Use (32.2) and Exercise 31.1.

The above could have been used to help calculate the character table of  $S_3$  (see § 32A, Example 1). For  $S_3$  is a transitive permutation group on  $X = \{1, 2, 3\}$ , and thus has a three-dimensional permutation representation  $T$  with character  $\tau$ , say. By (32.3),  $T$  has just one composition factor isomorphic to the 1-representation  $\zeta^{(1)}$ , and so

$$\tau = \zeta^{(1)} + \eta$$

for some character  $\eta$  of degree 2. Now

$$\tau(1) = 3, \quad \tau(123) = 0, \quad \tau(12) = 1,$$

whence

$$\eta(1) = 2, \quad \eta(123) = -1, \quad \eta(12) = 0.$$

It is easily seen that  $\eta$  is not a linear combination of  $\zeta^{(1)}$  and  $\zeta^{(2)}$  with non-negative integral coefficients, and thus  $\eta$  is the desired irreducible character  $\zeta^{(3)}$ .

Now let  $G$  be a transitive permutation group on  $X = \{x_1, \dots, x_n\}$ , and define  $H_i$  by (32.1) for  $1 \leq i \leq n$ . These subgroups  $H_1, \dots, H_n$  are mutually conjugate in  $G$ . Suppose that  $X$  splits into  $r$  orbits relative to  $H_1$ . [It is easily shown (see Exercise 2.3) that  $r$  is the number of  $(H_1, H_1)$ -double cosets in  $G$ , though we do not need this fact here.] By the preceding theorem we have

$$\sum_{g \in H_i} \tau(g) = r[H_i : 1], \quad 1 \leq i \leq n,$$

since  $X$  splits into  $r$  orbits relative to  $H_i$  for each  $i$ . Therefore

$$\sum_{i=1}^n \sum_{g \in H_i} \tau(g) = rn[H_1 : 1].$$

But on the other hand the number  $n$  is given by  $[G : H_1]$ , and so

$$\sum_{i=1}^n \sum_{g \in G} \tau(g) = r[G : 1].$$

On the left-hand side,  $\tau(g)$  is counted once for each index  $i$  such that  $gx_i = x_i$ ; that is,  $\tau(g)$  is counted once for each symbol left fixed by  $g$ . Since  $g$  leaves  $\tau(g)$  symbols fixed, the left-hand side is just

$$\sum_{g \in G} \tau(g) \cdot \tau(g).$$

Using the fact that  $\tau(g)$  is real (indeed, lies in  $Z$ ), we have thus shown that

$$(32.4) \quad \sum_{g \in G} \tau(g) \overline{\tau(g)} = r[G : 1].$$

We may use this formula to study doubly transitive permutation groups. We call a permutation group  $G$  on a set  $X = \{x_1, \dots, x_n\}$  *doubly transitive* if for any two ordered pairs  $\{x, y\}, \{u, v\}$  (with  $x \neq y$  and  $u \neq v$ ) taken from  $X$ , there exists an element  $g \in G$  such that  $gx = u$  and  $gy = v$ .

(32.5) THEOREM. *Let  $G$  be a doubly transitive permutation group, with permutation representation  $T$ . Then  $T$  is equivalent to  $\mathbf{1} + U$  where  $\mathbf{1}$  is the 1-representation and  $U$  is irreducible.*

PROOF. Since  $G$  is doubly transitive on  $X = \{x_1, \dots, x_n\}$ , it is clear that  $H_1 = \{h \in G : hx_1 = x_1\}$  is transitive on the set  $\{x_2, \dots, x_n\}$ . Thus  $X$  has two orbits relative to  $H_1$ , and by (32.4) we have

$$\sum_{g \in G} \tau(g) \overline{\tau(g)} = 2[G : 1].$$

Therefore, by Exercise 31.1,  $\tau$  is a sum of two absolutely irreducible

characters, one of which is the 1-character by (32.3).

As an illustration, we observe that  $S_4$  is a doubly transitive group on  $X = \{1, 2, 3, 4\}$ , with a four-dimensional permutation representation whose character  $\tau$  satisfies

$$\begin{aligned}\tau(1) &= 4, & \tau(12) &= 2, & \tau(123) &= 1, \\ \tau(1234) &= 0, & \tau((12)(34)) &= 0.\end{aligned}$$

Then  $\tau = \zeta^{(1)} + \eta$ , where  $\eta$  is an irreducible character of degree 3, and we have

$$\begin{aligned}\eta(1) &= 3, & \eta(12) &= 1, & \eta(123) &= 0, \\ \eta(1234) &= -1, & \eta((12)(34)) &= -1.\end{aligned}$$

(This  $\eta$  is  $\zeta^{(4)}$  of Example 3, § 32A).

The reader may wish to apply this technique to obtain the character  $\zeta^{(4)}$  of  $A_4$  in § 32A, Example 2.

### § 32C. Products of irreducible representations

Let  $Z_1, \dots, Z_s$  be a full set of non-isomorphic irreducible  $KG$ -modules, where  $G$  is a finite group and  $K$  is the complex field. Suppose that  $\zeta^{(i)}$  is the character afforded by  $Z_i$ , and let  $\zeta_k^{(i)}$  denote the value of  $\zeta^{(i)}$  at any element of the conjugate class  $\mathfrak{C}_k$  of  $G$ . We have shown in Theorem 30.9 that the  $KG$ -module  $Z_i \otimes_K Z_j$  affords the character  $\zeta^{(i)} \zeta^{(j)}$ , and therefore we may write

$$(32.6) \quad \zeta^{(i)} \zeta^{(j)} = \sum_{k=1}^s g_{ijk} \zeta_k^{(k)},$$

where the  $\{g_{ijk}\}$  are a set of uniquely determined non-negative integers which are in fact the structure constants of the algebra  $K\zeta^{(1)} \oplus \dots \oplus K\zeta^{(s)}$ . The coefficient  $g_{ijk}$  is just the multiplicity with which  $Z_k$  occurs as a composition factor of the  $KG$ -module  $Z_i \otimes_K Z_j$ .

We derive now a few relations among the constants  $g_{ijk}$ . From (32.6) we have immediately

$$(32.7) \quad g_{ijk} = g_{jik} \quad \text{for all } i, j, k.$$

Next let  $\overline{\zeta^{(j)}}$  be the character  $\zeta^{(j')}$  [see Theorem 31.21]. Then we have  $\zeta^{(j)} = \overline{\zeta^{(j')}}$ , so that by (31.17),

$$\begin{aligned}\sum_{x \in G} \zeta^{(i)}(x) \zeta^{(j)}(x) &= \sum_{x \in G} \zeta^{(i)}(x) \overline{\zeta^{(j')}}(x) \\ &= [G:1] \delta_{ij'}.\end{aligned}$$

But by (32.6) and (31.17),

$$\sum_{x \in G} \zeta^{(i)}(x) \zeta^{(j)}(x) = \sum_k \sum_{x \in G} g_{ijk} \zeta^{(k)}(x) = [G:1]g_{ij1}.$$

This establishes the formula

$$g_{ij1} = \begin{cases} 1, & \text{if } \zeta^{(i)} = \overline{\zeta^{(j)}} \\ 0, & \text{otherwise.} \end{cases}$$

Next (32.6) yields by Exercise 31.1,

$$g_{ijk} = [G:1]^{-1} \sum_{x \in G} \zeta^{(i)}(x) \zeta^{(j)}(x) \zeta^{(k)}(x)$$

where  $\zeta^{(k)}$  is the character  $\overline{\zeta^{(k)}}$ . Taking complex conjugates and using the fact that  $g_{ijk}$  is real, we obtain

$$(32.8) \quad g_{ijk} = [G:1]^{-1} \sum \zeta^{(i')}(x) \zeta^{(k)}(x) \zeta^{(j')}(x) = g_{i'kj}.$$

Using (32.7) and (32.8) repeatedly, we get

$$g_{ijk} = g_{i'kj} = g_{jik} = g_{j'ki} = g_{kj'i} = g_{k'iij'} = g_{ik'j'} = g_{i'j'k'}.$$

We conclude this section with a solution due to Burnside of an interesting question about multiplication of characters. Namely, given a group character  $\zeta$ , we can express each of the powers of  $\zeta$  as an integral linear combination of the irreducible characters  $\zeta^{(1)}, \dots, \zeta^{(s)}$ . We may ask for conditions on  $\zeta$  which guarantee that every  $\zeta^{(i)}$  will appear with non-zero coefficient in some power of  $\zeta$ . One condition is simply that  $\zeta$  be the character of a *faithful* representation of  $G$ . The question of when  $G$  has a faithful irreducible representation is discussed in a paper by Köchendorffer [1] where some sufficient conditions are given.

(32.9) **THEOREM.** (Burnside [4]). *Let  $T: G \rightarrow GL(M)$  be a faithful representation of a finite group  $G$  (that is,  $T(g) = 1$  implies  $g = 1$ ). Let  $M^n$  denote the  $KG$ -module  $M \otimes \cdots \otimes M$  ( $n$  factors). Then every irreducible  $KG$ -module is a composition factor of at least one of the modules  $M^n$ ,  $n = 1, 2, \dots$ .*

**PROOF.** Let  $\tau$  be the character afforded by  $T$ . We may write

$$(32.10) \quad \tau^n = \sum_{i=1}^s a_{ni} \zeta^{(i)}, \quad n \geq 1,$$

where the  $\{a_{ni}\}$  are non-negative integers. To prove the theorem, we must show that for each  $i$ , there exists an  $n$  for which  $a_{ni} \neq 0$ . From Exercise 31.1, we have

$$a_{ni} = [G:1]^{-1} \sum_{t=1}^s h_t \overline{\zeta_t^{(i)}}(\tau_t)^n.$$

Let  $X$  denote a complex variable. Then we obtain

$$\sum_{n=1}^{\infty} a_{ni} X^n = [G:1]^{-1} \sum_{t=1}^s h_t \overline{\zeta_t^{(i)}} \sum_{n=1}^{\infty} (X\tau_t)^n$$

where all series involved converge for sufficiently small  $|X|$ . Therefore

$$(32.11) \quad \sum_{n=1}^{\infty} a_{ni} X^n = [G:1]^{-1} \sum_{t=1}^s \frac{h_t \overline{\zeta_t^{(i)}} \cdot X\tau_t}{1 - X\tau_t}.$$

Now  $\tau_1 = m$  (say) where  $m = (M:K)$ . On the other hand,  $\tau_t \neq m$  for  $t \neq 1$ , since  $\tau_t = m$  implies (Exercise 30.6) that  $T(t) = 1$  and thus (by hypothesis) that  $t = 1$ . The right-hand side of (32.11) therefore contains exactly one term with denominator  $1 - mX$ , and so the right-hand side is a non-zero rational function of  $X$  for each  $i$ . But then for fixed  $i$ , it is impossible to have  $a_{ni} = 0$  for all  $n$ . This completes the proof.

Fong and Gaschütz [1] have recently established the analogous theorem for the case where the underlying field is a finite field containing the  $[G:1]$ -th roots of 1. A very simple proof of (32.9) has been obtained by Brauer [28]; also see Steinberg [1].

### § 33. Central Idempotents

Throughout this section, we take  $K$  to be a splitting field of characteristic zero for  $G$ . For example,  $K$  may be the field of complex numbers. By (29.16), it is also possible to choose for  $K$  an algebraic number field. As in §17, we let alg. int.  $\{K\}$  denote the set of elements  $\alpha$  of  $K$  which are algebraic over the field of rational numbers  $Q$  and for which  $\text{Irr}(\alpha, Q) \in Z[x]$ . Then alg. int.  $\{K\}$  is a subring of  $K$  whose intersection with  $Q$  is the set of rational integers  $Z$ . Moreover, alg. int.  $\{K\}$  contains all elements of  $K$  which are zeros of monic polynomials in  $Z[x]$ .

Keeping the notation of the preceding section, let  $Z_1, \dots, Z_s$  be a full set of non-isomorphic irreducible  $KG$ -modules. Let  $\zeta^{(i)}$  be the character afforded by  $Z_i$ , and  $Z_i$  a matrix representation afforded by  $Z_i$ . Then

$$z_i = \zeta^{(i)}(1) = (Z_i; K)$$

is the degree of  $Z_i$ ,  $1 \leq i \leq s$ . Because each  $\zeta^{(i)}(g)$ ,  $g \in G$ , is a sum of  $[G:1]$ -th roots of 1, it follows that for all  $g \in G$ ,  $\zeta^{(i)}(g) \in \text{alg. int. } \{K\}$ .

The group algebra  $KG$  can be expressed as a direct sum of  $s$  simple components  $A_1, \dots, A_s$ , and for each  $i$ ,  $Z_i$  may be taken to be a minimal left ideal in  $A_i$ . Because  $K$  is a splitting field, each  $A_i \cong K_{z_i}$  [see (27.20)]. If we write

$$1 = c_1 + \cdots + c_s, \quad c_i \in A_i,$$

then the  $\{c_i\}$  are a set of mutually orthogonal central idempotents (see Exercise 25.2), and each central idempotent of  $KG$  is a sum of a subset of the  $\{c_i\}$ . We have  $A_i = KGc_i$ ,  $1 \leq i \leq s$ .

We shall devote this section to the problem of determining the central idempotents  $\{c_i\}$  once the characters  $\{\zeta^{(j)}\}$  are known. As by-products of our investigation, we shall show that each  $z_i$  divides  $[G:1]$ , a result which is itself of considerable importance (see Exercise 31.2, for example). Finally we shall show how, in theory at least, the values of the characters on the conjugate classes of  $G$  may be obtained from the multiplication formulas for these classes.

For  $1 \leq i \leq s$ , let  $g_i$  denote an element of the class  $\mathfrak{C}_i$ , and suppose there are  $h_i$  elements in  $\mathfrak{C}_i$ . We had defined in (27.23)

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

and had shown in Theorem 27.24 that  $\{C_1, \dots, C_s\}$  is a  $K$ -basis for the center of  $KG$ . Obviously  $C_i C_j$  also lies in the center of  $KG$ , and so it may be expressed as a  $K$ -linear combination of the  $\{C_k\}$ , say

$$(33.1) \quad C_i C_j = \sum_{k=1}^s c_{ijk} C_k, \quad c_{ijk} \in K.$$

Both  $C_i$  and  $C_j$  are sums of elements of  $G$ , so that the product  $C_i C_j$  is also a sum of elements of  $G$ , each element occurring a non-negative integral number of times. Therefore each  $c_{ijk}$  is a non-negative integer.

We may interpret the  $\{c_{ijk}\}$  as “structure constants” connecting the conjugate classes of  $G$ . If we let  $\mathfrak{C}_i \mathfrak{C}_j$  denote the collection of products

$$\{xy: x \in \mathfrak{C}_i, y \in \mathfrak{C}_j\},$$

counted according to multiplicities, then each element of  $\mathfrak{C}_k$  occurs  $c_{ijk}$  times in  $\mathfrak{C}_i \mathfrak{C}_j$ . In other words, if we fix an element  $z \in \mathfrak{C}_k$ , then  $c_{ijk}$  is the number of solutions  $(x, y)$  of

$$xy = z, \quad x \in \mathfrak{C}_i, y \in \mathfrak{C}_j.$$

As before we define for  $1 \leq i, j \leq s$ ,

$$\zeta_i^{(j)} = \zeta^{(j)}(g_i), \quad g_i \in \mathfrak{G}_i.$$

We have at once

$$(33.2) \quad \zeta^{(j)}(C_i) = \sum_{x \in \mathfrak{G}_i} \zeta^{(j)}(x) = h_i \zeta_i^{(j)}.$$

On the other hand,  $C_i \in$  center of  $KG$ , and so if  $Z_j$  affords the matrix representation  $Z_j$ , then  $Z_j(C_i)$  commutes with  $\{Z_j(x) : x \in KG\}$ . Using Theorem 29.13, we deduce that  $Z_j(C_i)$  is a scalar matrix, say

$$(33.3) \quad Z_j(C_i) = \omega_i^{(j)} I^{(s_j)}, \quad \omega_i^{(j)} \in K, 1 \leq i, j \leq s.$$

Taking traces gives

$$(33.4) \quad h_i \zeta_i^{(j)} = z_j \omega_i^{(j)},$$

so that

$$(33.5) \quad \omega_i^{(j)} = \frac{h_i \zeta_i^{(j)}}{z_j}, \quad 1 \leq i, j \leq s.$$

Now apply  $Z_r$  to both sides of (33.1), getting

$$Z_r(C_i) Z_r(C_j) = \sum_{k=1}^s c_{ijk} Z_r(C_k).$$

If we use (33.3), this yields

$$(33.6) \quad \omega_i^{(r)} \omega_j^{(r)} = \sum_k c_{ijk} \omega_k^{(r)}.$$

Let us rewrite (33.6) as

$$\sum_k (c_{ijk} - \delta_{ik} \omega_j^{(r)}) \omega_k^{(r)} = 0,$$

a system of  $s$  homogeneous equations in the variables  $\omega_1^{(r)}, \dots, \omega_s^{(r)}$ . Letting  $\mathfrak{G}_1 = \{1\}$  as usual, we have

$$Z_r(C_1) = I, \quad \omega_1^{(r)} = 1,$$

so that the above system has a non-trivial solution. Therefore

$$|c_{ijk} - \delta_{ik} \omega_j^{(r)}|_{\substack{1 \leq i \leq s \\ 1 \leq k \leq s}} = 0,$$

showing that for each  $r$  ( $1 \leq r \leq s$ ),  $\omega_j^{(r)}$  is a characteristic root of the matrix

$$V_j = [c_{ijk}]_{\substack{1 \leq i \leq s \\ 1 \leq k \leq s}}.$$

Since each  $c_{ijk} \in Z$ , this implies by Theorem 17.2 that  $\omega_j^{(r)}$  is an algebraic integer for all  $j$  and all  $r$ . Since  $\overline{\zeta_j^{(r)}} \in \text{alg. int. } \{K\}$ , we have

$$\sum_{j=1}^s \omega_j^{(r)} \overline{\zeta_j^{(r)}} \in \text{alg. int. } \{K\}, \quad 1 \leq r \leq s.$$

We may rewrite the above sum [by (33.5)] as

$$\sum_j \frac{h_j \zeta_j^{(r)} \overline{\zeta_j^{(r)}}}{z_r},$$

which is just  $[G:1]/z_r$  as a consequence of (31.18). Thus  $[G:1]/z_r \in \text{alg. int. } \{K\} \cap Q = Z$ , and we have established

(33.7) THEOREM. *The degrees of the irreducible representations of a finite group  $G$  in a splitting field of characteristic zero are divisors of  $[G:1]$ .*

REMARK. In §53, we shall prove a sharper result due to Ito [2], namely that the degrees  $z_i$  divide the index in  $G$  of every abelian normal subgroup of  $G$ . See Exercise 33.1 for a special case of Ito's theorem.

Now we come to the connection between the central idempotents in  $KG$  and the irreducible characters of  $G$ .

(33.8) THEOREM. *Let  $K$  be a splitting field of characteristic zero for  $G$ , and let  $Z_j$  be a minimal left ideal in the simple component  $A_j$  of  $KG$ . Then  $A_j = (KG)c_j$  for a uniquely determined central idempotent  $c_j$  in  $KG$ , and we have*

$$(33.9) \quad c_j = \frac{z_j}{[G:1]} \sum_{i=1}^s \overline{\zeta_i^{(j)}} C_i$$

where  $\zeta_i^{(j)}$  is the character afforded by  $Z_j$ ,  $z_j = (Z_j:K)$ , and  $C_i$  is the sum of the elements in the  $i$ th conjugate class of  $G$ .

PROOF. Let  $KG = A_1 \oplus \cdots \oplus A_s$  be the decomposition of  $KG$  into simple components, and

$$1 = c_1 + \cdots + c_s$$

the corresponding decomposition of 1 as a sum of central idempotents. Then  $c_j$  annihilates  $A_k$  for  $k \neq j$ , and is the identity element for  $A_j$ , which proves that

$$(33.10) \quad Z_k(c_i) = \delta_{ik} I^{(z_k)}.$$

On the other hand,  $c_1, \dots, c_s$  are linearly independent elements in the center of  $KG$ , hence form a  $K$ -basis of this center, and so each  $C_i$  is a  $K$ -linear combination of the  $\{c_j\}$ . Since

$$Z_k(C_i) = \frac{h_i \zeta_i^{(k)}}{z_k} I^{(z_k)}$$

by (33.3) and (33.5), it follows immediately from this and (33.10) that

$$(33.11) \quad C_i = \sum_{k=1}^s \frac{h_i \zeta_i^{(k)}}{z_k} c_k, \quad 1 \leq i \leq s.$$

Therefore

$$\begin{aligned} \frac{z_j}{[G:1]} \sum_i \overline{\zeta_i^{(j)}} C_i &= \frac{z_j}{[G:1]} \sum_{i,k} \frac{h_i \overline{\zeta_i^{(j)}} \zeta_i^{(k)}}{z_k} c_k \\ &= z_j \sum_k \frac{\delta_{jk} c_k}{z_k} = c_j, \end{aligned}$$

using (31.18). This proves the theorem.

To conclude this section, we shall show briefly how we may determine the character table of a group from a knowledge of the constants  $\{c_{ijk}\}$  defined in (33.1). Suppose the classes  $\{\mathfrak{C}_i\}$  are given, and suppose the  $h_i$  are known. Setting

$$\omega_i^{(j)} = \frac{h_i \zeta_i^{(j)}}{z_j}, \quad 1 \leq i, j \leq s,$$

$$V_j = [c_{ijk}]_{1 \leq i, k \leq s},$$

we have shown that  $\{\omega_j^{(1)}, \dots, \omega_j^{(s)}\}$  are characteristic roots of  $V_j$ , and that a characteristic vector belonging to the root  $\omega_j^{(r)}$  is the column vector

$$\begin{bmatrix} \omega_1^{(r)} \\ \vdots \\ \omega_s^{(r)} \end{bmatrix}.$$

Thus, if some  $V_j$  has  $s$  distinct characteristic roots, we may obtain (up to a constant factor) each of the above column vectors. But  $\omega_1^{(r)} = h_1 \zeta_1^{(r)} / z_r = 1$  for each  $r$ , where  $\mathfrak{C}_1 = \{1\}$ , and thus the above vectors are completely determined. From (31.18), we have

$$z_j^2 \sum_{i=1}^s \frac{\omega_i^{(j)} \overline{\omega_i^{(j)}}}{h_i} = [G:1],$$

which enables us to determine the degrees  $z_1, \dots, z_s$ . We may then

find the values  $\{\zeta_i^{(j)}\}$  explicitly.

The assumption that some  $V_j$  has distinct characteristic roots may be avoided by introducing a set of  $s$  indeterminates  $\lambda_1, \dots, \lambda_s$  and considering the characteristic roots of the matrix

$$\lambda_1 V_1 + \dots + \lambda_s V_s.$$

For details, we refer the reader to Burnside [4], sections 223–224, pp. 295–297, where the process is illustrated for the dihedral group of order 10, and to Burnside [4], Example 3, p. 318, where this method is used to determine the character table of  $A_5$ .

### Exercise

1. (Schur.) Prove that the degrees of the irreducible  $KG$ -modules, where  $K$  is a splitting field of characteristic zero, are factors of the index  $[G : C(G)]$  where  $C(G)$  is the center of the group  $G$ .

[Hint: We may assume that  $K$  is an algebraic number field. Let  $T: G \rightarrow GL(M)$  be an irreducible  $K$ -representation of  $G$ . In Chapter XI (see (75.4)) it is proved that for a suitable algebraic extension  $L$  of  $K$ , there exists a basis for  $M^L$  over  $L$  such that the matrices of  $T^L(g)$ , computed with respect to this basis, have all their entries in  $R = \text{alg. int. } \{L\}$ . For simplicity, set  $T = T^L$ , and let  $\mathbf{T}(g) = (a_{ij}(g))$ ,  $g \in G$ ,  $a_{ij}(g) \in R$ , be a matrix representation afforded by  $T$ . Because  $T$  is absolutely irreducible,  $x \in C(G)$  implies

$$\mathbf{T}(x) = \begin{bmatrix} a_{11}(x) & 0 \\ 0 & A \end{bmatrix}$$

where  $A$  is a  $(d-1) \times (d-1)$  matrix and where  $d = \deg T$ . Show that for all  $g \in G$ ,

$$\mathbf{T}(gx) = \begin{bmatrix} a_{11}(g)a_{11}(x) & * \\ * & * \end{bmatrix}$$

and that

$$\mathbf{T}(x^{-1}g^{-1}) = \begin{bmatrix} a_{11}(x^{-1})a_{11}(g^{-1}) & * \\ * & * \end{bmatrix}.$$

Therefore

$$a_{11}(g_1)a_{11}(g_1^{-1}) = a_{11}(g_2)a_{11}(g_2^{-1})$$

whenever  $g_1g_2^{-1} \in C(G)$ . By the orthogonality relations for the  $\{a_{ij}(g)\}$  (Exercise 31.1), we have

$$\sum_g a_{11}(g)a_{11}(g^{-1}) = \frac{[G : 1]}{d}, \quad d = \deg T.$$

Then show that

$$[C(G): 1] \sum' a_{11}(g) a_{11}(g^{-1}) = \frac{[G: 1]}{d}$$

where  $g$  ranges over a full set of coset representatives of  $G$  modulo  $C(G)$ , and hence

$$\sum' a_{11}(g) a_{11}(g^{-1}) = \frac{[G: C(G)]}{d} \in R \cap Q = Z.$$

Therefore  $d \mid [G: C(G)]$ .

### § 34. Burnside's Criterion for Solvable Groups

We can now give our first deep application of the theory of group characters to group theory. In the proof, we shall assume that  $K$  is an algebraic number field which is a splitting field for  $G$ , and shall use the notation and results of the preceding section.

(34.1) THEOREM (Burnside [4]). *If  $[G: 1] = p^a q^b$  where  $p$  and  $q$  are distinct primes, then  $G$  is solvable.*

PROOF. From § 5 we know that  $G$  is solvable if either  $a = 0$  or  $b = 0$ , and also that each abelian group is solvable. We shall use induction on the order of  $G$ , and need only prove that a non-abelian group  $G$  of order  $p^a q^b$ ,  $a > 0, b > 0$ , contains a proper normal subgroup  $N \neq \{1\}$ . Then both  $N$  and  $G/N$  have orders of the form  $p^a q^b$ . Thus  $N$  and  $G/N$  are solvable by the induction hypothesis, whence also  $G$  is solvable.

*Step 1.* Let  $H$  be a  $p$ -Sylow subgroup of  $G$  (see § 6). Since  $H$  has a non-trivial center [Theorem 3.5], we may choose an element  $h \neq 1$  in the center of  $H$ . Then

$$H \subset C(h) = \text{centralizer of } h \text{ in } G,$$

and so  $p \nmid [G: C(h)]$ . Therefore  $[G: C(h)]$  is a power of  $q$ . If  $[G: C(h)] = 1$ , then  $h \in C(G) = \text{center of } G$ , so  $G$  has a non-trivial normal subgroup  $C(G)$  in this case.

*Step 2.* We are left with the more difficult case where

$$[G: C(h)] = q^d, \quad d > 0.$$

Keeping our earlier notation, we have from (31.19) with  $i = j = 1$  [or from (27.21)]

$$\sum_{j=1}^s z_j^2 = [G:1] \equiv 0 \pmod{q}.$$

But  $z_1 = 1$ , where  $Z_1$  is the 1-representation, and thus  $q \nmid z_j$  for at least one index  $j > 1$ . For the remainder of the proof, we fix the subscript  $i$  by letting  $\mathbb{C}_i$  denote the conjugate class to which  $h$  belongs. Then  $\mathbb{C}_i$  contains  $h_i$  elements, where

$$h_i = [G: C(h)] = q^d.$$

Since  $z_j \mid [G:1]$  for each  $j$ , and since  $[G:1] = p^a q^b$ ,  $q \nmid z_j$  implies that  $(h_i, z_j) = 1$ .

*Step 3.* We now show that  $\zeta_i^{(j)} \neq 0$  for at least one  $j \neq 1$  such that  $q \nmid z_j$ . Suppose otherwise that  $\zeta_i^{(j)} = 0$  whenever  $j \neq 1$  and  $q \nmid z_j$ . Let  $R = \text{alg. int. } \{K\}$ . We have from (31.19),

$$0 = \sum_{n=1}^s \zeta_1^{(n)} \zeta_i^{(n)} = 1 + \sum_{j=2}^s z_j \zeta_i^{(j)}.$$

But each term  $z_j \zeta_i^{(j)}$  ( $j \geq 2$ ) lies in  $qR$  since either  $q \mid z_j$  or else  $\zeta_i^{(j)} = 0$ . This gives

$$0 \equiv 1 \pmod{qR},$$

which is impossible.

*Step 4.* We have shown that there is at least one index  $j > 1$  such that  $q \nmid z_j$  and such that  $\zeta_i^{(j)} \neq 0$ . We have shown earlier in this section that

$$\omega_i^{(j)} = \frac{h_i \zeta_i^{(j)}}{z_j} \in R.$$

Since  $(z_j, h_i) = 1$ , this implies that  $\zeta_i^{(j)}/z_j \in R$ , and thus the norm

$$N(\zeta_i^{(j)}/z_j)$$

is a non-zero rational integer. By (30.11), we know that

$$|\zeta_i^{(j)}/z_j| \leq 1,$$

with equality if and only if  $Z_j(h) = \text{scalar matrix}$ . If  $|\zeta_i^{(j)}/z_j| < 1$ , the same inequality would hold for each algebraic conjugate of  $\zeta_i^{(j)}/z_j$  (see Exercise 21.8), and we would have (by § 20B)

$$|N(\zeta_i^{(j)}/z_j)| < 1,$$

which is impossible.

We have therefore proved that  $Z_j(h) = \text{scalar matrix}$ , and so the group

$$G_1 = \{g \in G : Z_j(g) = \text{scalar matrix}\}$$

is a normal subgroup of  $G$  containing 1 and  $h$ . We shall conclude from this that  $G$  is not simple. For if  $G$  is simple then  $G_1 = G$ , and so we may set

$$Z_j(g) = u(g)I, \quad g \in G, u(g) \in K.$$

Then  $u: G \rightarrow K$  is a one-dimensional representation distinct from  $Z_1$  (since  $j \neq 1$ ), and thus  $u$  induces a representation

$$u: G/G' \rightarrow K$$

where  $G'$  is the commutator subgroup of  $G$ . Thus  $G/G'$  has two distinct one-dimensional representations, so that  $G' \neq G$ . However,  $G' \triangle G$ , and since we are assuming that  $G$  is simple, we deduce that  $G' = \{1\}$ . Therefore  $G$  is abelian, contrary to our original hypothesis. This completes the proof of the theorem.

### Exercise

1. If the number of elements in some conjugate class of  $G$  is a power of a prime, then  $G$  is not simple.

## § 35. The Frobenius-Wielandt Theorem on the Existence of Normal Subgroups in a Group

The construction of normal subgroups of a finite group  $G$  is one of the central problems in group theory. A famous theorem due to Frobenius enables us, under certain conditions, to show the existence of a normal subgroup with preassigned factor group. In this section we shall give Wielandt's generalization of Frobenius' theorem, the proof of which will use the theory of group characters.

Let us begin with some notation. Let  $G$  be a finite group whose irreducible characters in the complex field  $K$  are  $\zeta^{(1)}, \dots, \zeta^{(s)}$ , where  $\zeta^{(1)}$  is the 1-character. By a *class function* on  $G$  is meant a map  $\psi: G \rightarrow K$  such that  $\psi(g)$  depends only upon the conjugate class of  $g$ . Since there are  $s$  classes, the set of all class functions on  $G$  forms an  $s$ -dimensional vector space over  $K$ . By (30.5) and (30.12),  $\zeta^{(1)}, \dots, \zeta^{(s)}$  are class functions which are linearly independent over  $K$ , and thus constitute a  $K$ -basis for this vector space.

For any subset  $S$  of  $G$ , let  $G - S$  denote the set of elements in  $G$  which are not in  $S$ . Further define

$$t^s = s^{-1}ts, \quad s, t \in G,$$

and

$$(G - S)^x = \{y^x : y \in G - S\}.$$

We may now state Frobenius' theorem.

(35.1) THEOREM ((Frobenius [3])). *Let  $H$  be a subgroup of  $G$  such that*

$$(35.2) \quad H \cap H^t = 1 \quad \text{for all } t \in G - H.$$

*Set*

$$(35.3) \quad G^* = G - \bigcup_{s \in G} (H - 1)^s.$$

*Then  $G^* \triangle G$ , and we have*

$$(35.4) \quad H \cap G^* = 1, \quad HG^* = G, \quad G/G^* \cong H.$$

[The first two relations in (35.4) obviously imply the third. The formulas (35.4) assert that  $G$  is the semi-direct product of  $G^*$  and  $H$ .]

We shall prove here the following generalization.

(35.5) THEOREM (Wielandt [1]). *Let  $H^* \triangle H \subset G$  be groups such that*

$$(35.6) \quad H \cap H^t \subset H^* \quad \text{for all } t \in G - H.$$

*Then there is a unique solution  $G^*$  of the equations*

$$(35.7) \quad G^* \triangle G, \quad H \cap G^* = H^*, \quad HG^* = G.$$

*Indeed  $G^*$  coincides with the subset of  $G$  given by*

$$(35.8) \quad S = G - \bigcup_{g \in G} (H - H^*)^g.$$

(The existence of  $G^*$  was shown by Grün [1] under the assumption that  $H/H^*$  is solvable. Additional results are contained in a paper of D.G. Higman [1].)

We begin the proof with a pair of lemmas. Throughout this section, "character" will mean "character of a representation by matrices over  $K$ ".

(35.9) LEMMA. *Let  $H^* \triangle H \subset G$  be groups such that (35.7) holds for some  $G^*$ . Then we have*

(i)  $G/G^* \cong H/H^*$ .

(ii) *Every character of  $H$  which is constant on  $H^*$  can be extended to a character of  $G$  constant on  $G^*$ .*

(iii) *If  $F$  is a group such that  $H \subset F \subset G$ , then there exists a subgroup  $F^* \triangle F$  such that*

$$H \cap F^* = H^*, \quad HF^* = F.$$

**PROOF.** The homomorphism theorems easily imply (i). Now let  $T$  be a representation of  $H$  (by matrices over  $K$ ) with character  $\tau$ , and let  $\tau(h) = \tau(1)$  for  $h \in H^*$ . Then  $T(h) = T(1)$  for all  $h \in H^*$ , by Exercise 30.6. Extend  $T$  to a representation of  $G$  by setting

$$T(g) = T(h), \quad g \in G, h \in H,$$

where  $gG^*$  and  $hH^*$  correspond to each other in the isomorphism (i). Then the character of  $T$  on  $G$  is the desired extension of  $\tau$ . Finally we set  $F^* = G^* \cap F$  and easily verify (iii).

A partial converse of the first lemma, essentially due to Frobenius, is the following:

(35.10) **LEMMA.** *Let  $H^* \triangleleft H \subset G$  be groups, and  $S$  any subset of  $G$  containing 1. Suppose that every irreducible character  $\phi$  of  $H$  which is constant on  $H^*$  can be extended to a character of  $G$  constant on  $S$ . Then there exists a subgroup  $G^* \triangleleft G$  such that*

$$G^* \supset S, \quad H \cap G^* = H^*.$$

[However,  $HG^* = G$  need not hold, as may be seen from the example where  $G$  is cyclic of order  $p^2$  ( $p$  a prime),  $H$  is its subgroup of order  $p$ , and  $H^* = S = \{1\}$ .]

**PROOF.** The irreducible characters  $\phi$  of  $H$  which are constant on  $H^*$  are in one-to-one correspondence with the irreducible characters  $\tilde{\psi}$  of  $H/H^*$ , according to the rule

$$\phi(h) = \tilde{\psi}(hH^*), \quad h \in H.$$

The character  $\tilde{\chi}$  of the regular representation of  $H/H^*$  can be expressed as a sum of irreducible characters  $\tilde{\psi}_i$ , say

$$\tilde{\chi} = a_1 \tilde{\psi}_1 + \cdots + a_r \tilde{\psi}_r, \quad a_i \in Z.$$

Then

$$\chi = a_1 \phi_1 + \cdots + a_r \phi_r$$

is a character of a representation of  $H$  which is constant on  $H^*$  by Exercise 30.6. By the hypothesis, each  $\phi_i$  can be extended to a character  $\psi'_i$  of  $G$  which is constant on  $S \cup H^*$ . Let  $T$  be the representation of  $G$  whose character is  $a_1 \psi'_1 + \cdots + a_r \psi'_r$ . Then  $T$  is constant on  $S \cup H^*$  by Exercise 30.6, and for  $h \in H$ ,  $T(h) = I$ .

implies  $h \in H^*$ , since  $\tilde{\chi}$  is the character of a faithful representation of  $H/H^*$ . Now define

$$G^* = \{g \in G : T(g) = I\}.$$

Then  $G^* \triangle G$ ,  $H \cap G^* = H^*$ , and  $S \subset G^*$ . This proves the lemma.

Now let us start the proof of Wielandt's theorem. We are given groups  $H^* \triangle H \subset G$  for which (35.6) holds. The theorem is trivially true for the case  $H^* = H$  since then  $G^*$  must be  $G$ . For the remainder of the proof, we may assume that  $H^*$  is a proper subgroup of  $H$ . We show first the uniqueness of the solution  $G^*$ , if there is a solution. For suppose  $G^*$  satisfies (35.7); then on the one hand  $H \cap G^* = H^*$  implies that  $(H - H^*) \cap G^*$  is empty, whence also

$$(H - H^*)^g \cap G^*$$

is empty for each  $g \in G$ , and so  $G^* \subset S$ . On the other hand, we note that from (35.6) we may deduce that

$$(H - H^*)^y, \quad (H - H^*)^y$$

either are disjoint or coincide, according to whether or not  $y \in Hx$ . Hence the number of elements in  $S$  is

$$[G:1] - [G:H][H:1] - [H^*:1];$$

that is,  $S$  contains  $[G:H][H^*:1]$  elements. But  $G/G^* \cong H/H^*$  shows that

$$[G:H][H^*:1] = [G^*:1],$$

so  $S$  contains  $[G^*:1]$  elements, and thus  $G^* = S$ .

Second, we turn to the more difficult "existence" part of the theorem, and shall show that every irreducible character  $\psi$  of  $H$  constant on  $H^*$  may be extended to a character of  $G$  constant on  $S$ . The result is clear when  $\psi$  is the 1-character  $\psi^{(1)}$ , so we exclude this case hereafter. Let  $\chi$  be a (complex-valued) class function on  $G$  which extends  $\psi$  and which is constant on  $S$ . Then necessarily

$$\chi(g) = \begin{cases} \psi(1), & g \in S, \\ \psi(g^{x^{-1}}), & g \in (H - H^*)^x. \end{cases}$$

Conversely the above serves to define a class function on  $G$  which is constant on  $S$  and extends  $\psi$ . We wish to show that  $\chi$  is indeed a character of  $G$ , and to do this we shall make use of the orthogonality relations. Set

$$\omega = \chi - t, \quad t = \chi(1) = \psi(1),$$

so that  $\omega$  is also a class function, and is given by

$$\omega(g) = \begin{cases} 0, & g \in S \\ \psi(g^{x^{-1}}) - t, & g \in (H - H^*)^x. \end{cases}$$

Now we may write  $\omega$  as a  $K$ -linear combination of the irreducible characters  $\zeta^{(1)}, \dots, \zeta^{(s)}$  of  $G$ , say

$$\omega = a_1 \zeta^{(1)} + \dots + a_s \zeta^{(s)}, \quad a_i \in K.$$

The orthogonality relations yield

$$a_i = [G:1]^{-1} \sum_{g \in G} \omega(g) \overline{\zeta^{(i)}(g)}.$$

Since  $\omega$  vanishes on  $S$  and is a class function, we have

$$\begin{aligned} a_i &= [G:1]^{-1} \sum_{g \in G-S} \omega(g) \overline{\zeta^{(i)}(g)} = [G:1]^{-1} \sum_{\substack{z \in G \\ z \text{ mod } H}} \sum_{g \in (H-H^*)^z} \omega(g) \overline{\zeta^{(i)}(g)} \\ &= [G:1]^{-1} [G:H] \sum_{g \in H-H^*} \omega(g) \overline{\zeta^{(i)}(g)}, \end{aligned}$$

so that

$$a_i = [H:1]^{-1} \sum_{g \in H} \omega(g) \overline{\zeta^{(i)}(g)}, \quad 1 \leq i \leq s.$$

In particular,

$$a_1 = [H:1]^{-1} \sum_{g \in H} (\psi(g) - t) = -t$$

since  $\psi$  is not the 1-character of  $H$ .

From the orthogonality relations on  $H$  and the fact that  $\omega|H$  and  $\zeta^{(i)}|H$  are  $Z$ -linear combinations of characters of  $H$ , it follows that all the coefficients  $a_i \in Z$ . Further, from  $\omega = \sum a_i \zeta^{(i)}$  we have

$$\begin{aligned} \sum_{i=1}^s a_i^2 &= [G:1]^{-1} \sum_{g \in G} |\omega(g)|^2 = [H:1]^{-1} \sum_{h \in H} |\omega(h)|^2 \\ &= t^2 + 1, \end{aligned}$$

the second equality holding because  $\omega$  vanishes outside  $H$ , and the last equality following from the fact that

$$\omega|H = \psi - t \cdot \phi^{(1)}.$$

But we know that  $a_1 = -t$  and that  $\sum a_i^2 = t^2 + 1$ , and so, for  $i > 1$ , all but one  $a_i = 0$ , and that exceptional  $a_i$  is  $\pm 1$ . Hence

$$\omega = \pm \zeta - t \zeta^{(1)}$$

where  $\zeta$  is an irreducible character of  $G$ ,  $\zeta \neq \zeta^{(1)}$ , and so  $\chi = \pm\zeta$ . Since  $\chi(1) = t > 0$ , we conclude that  $\chi = \zeta$ , and we have shown that  $\chi$  is a character of  $G$ .<sup>†</sup>

The above discussion has shown that every irreducible character of  $H$  which is constant on  $H^*$  may be extended to a character of  $G$  constant on  $S$ . By Lemma 35.10, it follows that there exists a subgroup  $G^* \triangleleft G$  such that

$$G^* \supset S, \quad H \cap G^* = H^*.$$

To complete the proof, we need show only that  $HG^* = G$ . But

$$\begin{aligned} [HG^*: 1] &= \frac{[H: 1][G^*: 1]}{[H^*: 1]} \geq \frac{[H: 1][S: 1]}{[H^*: 1]} \\ &= \frac{[H: 1][G: H][H^*: 1]}{[H^*: 1]} = [G: 1], \end{aligned}$$

where  $[S: 1] =$  number of elements in  $S$ . Thus  $HG^* = G$ , and Wielandt's theorem is proved.

We leave as an exercise to the reader the deduction of the following formulation of the Wielandt-Frobenius theorem in terms of permutation groups:

(35.11) COROLLARY. *Let  $G$  be a transitive permutation group on the symbols  $x_1, \dots, x_n$ , and let*

$$H = \{g \in G : gx_1 = x_1\}.$$

*Let*

$$V = \{g \in H : gx_i = x_i \text{ for at least one } i > 1\},$$

*and suppose that  $V$  generates the subgroup  $H^*$  of  $H$ . Then  $G$  contains exactly one transitive normal subgroup  $G^*$  such that  $G^* \cap H = H^*$ .*

Let us observe now that if  $H \neq N_G(H)$ , the normalizer of  $H$  in  $G$ , we may choose  $t \in N_G(H)$  such that  $t \in G - H$ . For this  $t$ , we have

$$H \cap H^t = H,$$

and so (35.6) can only hold when  $H^* = H$ . Thus the only time the Frobenius-Wielandt theorem can be used is when  $H$  coincides with

---

<sup>†</sup> Another way of proving that  $\chi$  is a character on  $G$  is by means of induced characters; see the proof due to Witt (for the case  $H^* = 1$ ) given in Speiser [2].

its own normalizer. We shall generalize Theorem 35.5 still further so as to be able to obtain non-trivial results even when  $H \neq N_G(H)$ .

(35.12) **THEOREM (Wielandt [1]).** *Let  $H^* \triangle H \subset G$  be groups, and set  $F = N_G(H)$ . Assume that*

$$([F:H], [H:H^*]) = 1$$

*and that*

$$H \cap H^t \subset H^* \quad \text{for all } t \in G - F.$$

*Then there is at most one solution  $G^*$  of*

$$(35.13) \quad G^* \triangle G, \quad H \cap G^* = H^*, \quad HG^* = G.$$

*Such a solution exists if and only if there is a solution  $F^*$  of*

$$(35.14) \quad H^* \subset F^* \triangle F, \quad [F:F^*] = [H:H^*].$$

*This latter set of equations has at most one solution. From a solution  $F^*$  of (35.14) one obtains a solution  $G^*$  of (35.13) by setting*

$$(35.15) \quad G^* = G - \bigcup_{x \in G} (F - F^*)^x.$$

**PROOF.** If  $F^*$  satisfies (35.14), then  $[F:HF^*]$  divides both  $[F:F^*]$  and  $[F:H]$ ; hence  $[F:HF^*] = 1$ . But then

$$[H:H \cap F^*] = [HF^*:F^*] = [F:F^*] = [H:H^*],$$

and since  $H^* \subset H \cap F^*$ , we conclude that

$$H \cap F^* = H^*,$$

and therefore  $H^* \triangle F$ . In that case we may form the factor group  $F/H^*$ , and notice that  $F^*/H^*$  is a normal subgroup of  $F/H^*$ , whose index  $[F:F^*] (= [H:H^*])$  and order  $[F^*:H^*] (= [F:H])$  are relatively prime. It then follows (see Exercise 2.5) that the subgroup  $F^*/H^*$  is uniquely determined in  $F/H^*$ , and so there is at most one  $F^*$  satisfying (35.14).

Suppose now that  $F^*$  is a solution of (35.14), and let us show that

$$F \cap F^t \subset F^* \quad \text{for all } t \in G - F.$$

For let  $t \in G - F$ ,  $x \in F \cap F^t$ , and set

$$i = [F:H], \quad j = [H:H^*] = [F:F^*].$$

Since  $x \in F$  we have  $x^i \in H$ ; likewise  $x^i \in H^t$ , and so  $x^i \in H \cap H^t \subset H^* \subset F^*$ . On the other hand  $x^j \in F^*$ . Thus also  $x \in F^*$ , since

$[F:H]$  and  $[H:H^*]$  are relatively prime.

We may therefore apply Theorem 35.5 to deduce the existence of a subgroup  $G^*$  of  $G$  satisfying

$$G^* \triangle G, \quad F \cap G^* = F^*, \quad FG^* = G,$$

and  $G^*$  is given by (35.15). We find readily that  $G^*$  satisfies (35.13).

Finally we must show that there is at most one solution  $G^*$  of (35.13). For let  $G^*$  be any such solution and set  $F^* = F \cap G^*$ . We have

$$H^* \subset H \subset F, \quad H^* \subset G^*,$$

so

$$H^* \subset F \cap G^* = F^*.$$

Certainly  $H^* \triangle F^*$ . Finally,

$$G = HG^* \subset FG^* \subset G,$$

so that  $FG^* = G$ , and we have  $[F:F^*] = [G:G^*] = [H:H^*]$ . Thus  $F^*$  is the unique solution of (35.14), and so  $G^*$  must be given by (35.15). This completes the proof.

As an application of this result, let us consider the problem of determining the number of solutions of

$$x^n = 1, \quad x \in G,$$

where  $n$  is some fixed divisor of  $[G:1]$ . We shall show later (§ 41), by using induced characters, that the number of solutions is a multiple of  $n$  (see also M. Hall [2], pp. 136, 137). It has been conjectured that if there are exactly  $n$  solutions, then the set  $S$  of these solutions is a subgroup of  $G$ . (In this case  $S$  would automatically be a normal subgroup of  $G$ .) As a step toward answering this question, we prove a result due to Wielandt [1] which improves an earlier theorem of Feit [1].

(35.16) THEOREM. *Let  $H^* \triangle H \subset G$  be groups such that*

$$H \cap H^g \subset H^* \quad \text{for all } g \in G - N_G(H).$$

*Set*

$$[H:H^*] = j, \quad [G:1] = mj$$

*and assume that  $(m, j) = 1$ . If the equation*

$$x^m = 1, \quad x \in G,$$

*has precisely  $m$  solutions, these solutions form a characteristic*

subgroup  $G^*$  of  $G$ , and we have

$$H \cap G^* = H^*, \quad HG^* = G.$$

PROOF. Set  $F = N_G(H)$ ,  $i = [F:H]$ ,  $s = [H^*:1]$ , and let  $M = \{x \in G : x^m = 1\}$ ,  $M_0 = \{x \in F : x^m = 1\}$ . We note that  $H^* \triangle H$  and  $s \mid m$ , so that  $H^*$  is a normal subgroup of  $H$  whose index  $j$  is relatively prime to its order  $s$ . By Exercise 2.5, it follows that  $H^*$  is the only subgroup of  $H$  of order  $s$ , and consequently  $H^* \triangle F$ . Therefore we may form  $F/H^*$ , and we observe that

$$H/H^* \triangle F/H^*.$$

Now  $H/H^*$  has order  $j$ , and index  $i$  (in  $F/H^*$ ) which is relatively prime to  $j$ . By Schur's theorem 7.5, we may conclude that  $F/H^*$  contains a subgroup  $F^*/H^*$  of order  $i$ , where  $F^*$  is some subgroup of  $F$ . We have

$$H^* \subset F^* \subset F, \quad [F^*:H^*] = i = [F:H], \quad [F:F^*] = [H:H^*] = j.$$

In order to apply Theorem 35.12, we must verify that  $F^* \triangle F$ , and this we do by proving that  $F^* = M_0$ . Since  $F^*$  has order  $i \cdot s$  which divides  $m$ , it is clear that  $F^* \subset M_0$ . We are now going to show that  $M_0$  contains  $i \cdot s$  elements, and we already know (since  $F^* \subset M_0$ ) that  $M_0$  contains at least  $i \cdot s$  elements. Note that  $F$  contains  $ijs$  elements, so that the number of elements in  $F - M_0$  is at most  $ijs - is$ .

Suppose next that  $y \in G - M$ ; the order of  $y$  cannot divide  $m$ , and so there exists a prime  $p$  such that  $p \mid j$  and  $p \mid \text{order of } y$ . Hence some power of  $y$ , call it  $u$ , has order  $p$ , and  $u = u^\nu$ . Now  $u$  lies in some  $p$ -Sylow subgroup  $P_0$  of  $G$ ; since  $p \nmid [G:H]$ , we see that any  $p$ -Sylow subgroup  $P$  of  $H$  is also a  $p$ -Sylow group of  $G$ , and so we may write  $P_0 = P^t$  for some  $t \in G$ . Then  $u^\nu \in P^{t\nu t^{-1}}$ , and hence

$$u \in P^t \cap P^{t\nu} = (P \cap P^{t\nu t^{-1}})^t.$$

If  $tyt^{-1} \in G - F$ , then

$$P \cap P^{t\nu t^{-1}} \subset H \cap H^{t\nu t^{-1}} \subset H^*,$$

which is impossible because the order of  $H^*$  is relatively prime to  $p$ , whereas  $u$  has order  $p$ . This shows that  $tyt^{-1} \in F$ ; that is,  $y$  lies in some conjugate of  $F$ . Consequently

$$G - M = \bigcup_{t \in G} (F - M_0)^t.$$

The number of distinct conjugates of  $F$  is at most  $[G:F]$ , and the

number of elements in  $F - M_0$  is at most  $ijs - is$ , so the number of elements in  $G - M$  is at most

$$[G:F](ijs - is) = [G:1] - m.$$

Since  $G - M$  contains exactly  $[G:1] - m$  elements by hypothesis, this shows that  $F - M_0$  contains exactly  $ijs - is$  elements, and so  $M_0$  contains  $i \cdot s$  elements. Therefore  $F^* = M_0$  as stated above, which implies that  $F^* \triangleleft F$ .

Now we use Theorem 35.12 to deduce the existence of a normal subgroup  $G^*$  in  $G$  such that

$$H \cap G^* = H^*, \quad HG^* = G.$$

Then we find at once that

$$[G^*:1] = [G:1]/[H:H^*] = m,$$

so every element of  $G^*$  satisfies  $x^m = 1$ . The hypothesis implies that  $G^*$  coincides with  $\{x \in G : x^m = 1\}$ , and the theorem is proved.

Additional results dealing with this problem may be found in Feit [1].

### Exercise

1. (Frobenius.) Let  $H$  be a subgroup of  $G$  whose index  $m = [G:H]$  is relatively prime to its order  $[H:1]$ . Suppose that  $H = N_G(H)$ , and that for each  $g \in G$  either  $H^g = H$  or  $H^g \cap H = 1$ . Prove that there are exactly  $m - 1$  elements of  $G$  not lying in any subgroup  $H^g$ ,  $g \in G$ , and that these together with 1 form a normal subgroup  $S$  of  $G$ . Show furthermore that  $S = \{x \in G : x^m = 1\}$ .

## § 36. Theorems of Jordan, Burnside, and Schur on Linear Groups

Throughout this section, let  $K$  be the complex field,  $GL(n, K)$  the group of all non-singular  $n \times n$  matrices over  $K$ . A subgroup  $G$  of  $GL(n, K)$  is *periodic* if each  $g \in G$  is of finite order, that is,  $g^m = 1$  for some positive integer  $m$ . We call  $G$  *periodic of bounded period* if there is an upper bound on the orders of the elements of  $G$ , or equivalently, if there exists a positive integer  $m$  such that  $g^m = 1$  for all  $g \in G$ .

Burnside conjectured that a finitely generated abstract group of bounded period must necessarily be finite. This has been established for small values of  $m$  (see Hall [2]), but recently a negative answer example to this conjecture been announced (Novikov [1]). Never-

theless, we may prove

(36.1) THEOREM (Burnside [4]). *Every periodic subgroup of  $GL(n, K)$  of bounded period is finite.*

PROOF. Let  $G$  be a subgroup of  $GL(n, K)$  such that  $g^m = 1$  for all  $g \in G$ , where  $m$  is some fixed positive integer. Consider first the case where  $G$  is an irreducible group of linear transformations acting on an  $n$ -dimensional vector space  $M$  over  $K$ . Letting  $\chi(g)$  denote the trace of the linear transformation  $g$ , we see that for each  $g \in G$ , the number  $\chi(g)$  is a sum of  $n$   $m$ th roots of unity. Therefore the set  $\{\chi(g): g \in G\}$  has only a finite number of distinct elements.

Relative to some fixed  $K$ -basis of  $M$ , let the matrix of  $g \in G$  be

$$(f_{ij}(g))_{1 \leq i, j \leq n}, \quad f_{ij}(g) \in K.$$

By Corollary 27.13, there exist  $n^2$  elements  $g_1, \dots, g_{n^2} \in G$  such that the  $n^2$   $n^2$ -tuples

$$\{f_{ij}(g_k): 1 \leq i, j \leq n\}, \quad 1 \leq k \leq n^2,$$

are linearly independent over  $K$ . For  $g \in G$ , we have

$$\chi(g_k g) = \sum_{i=1}^n f_{ii}(g_k g) = \sum_{i,j=1}^n f_{ij}(g_k) f_{ji}(g).$$

Regarding this as a set of  $n^2$  linear equations in the  $n^2$  unknowns  $\{f_{ij}(g)\}$ , we see that the rows of the matrix of coefficients are linearly independent over  $K$ , and hence there is a unique solution for the  $\{f_{ij}(g)\}$ , this solution of course depending on the values  $\{\chi(g_k g)\}$ . But  $\chi$  takes on only a finite number of possible values, and hence so does each  $f_{ij}(g)$ . Therefore the group  $G$  is finite in this case.

We now use induction on  $n$ , and note that we have established the result when  $G$  is irreducible. Now let  $G$  be a reducible set of linear transformations. Relative to some  $K$ -basis of  $M$ , the matrices corresponding to the elements of  $G$  take the form

$$\begin{bmatrix} \mathbf{T}(g) & \mathbf{U}(g) \\ \mathbf{0} & \mathbf{V}(g) \end{bmatrix}.$$

The  $m$ th power of such a matrix has  $\mathbf{T}^m(g)$  and  $\mathbf{U}^m(g)$  as diagonal blocks, and thus the groups

$$\{\mathbf{T}(g): g \in G\}, \quad \{\mathbf{V}(g): g \in G\}$$

are periodic groups of linear transformations of bounded period. By the induction hypothesis, both of these groups are finite.

Set

$$H_1 = \{g \in G: T(g) = I\}, \quad H_2 = \{g \in G: V(g) = I\}.$$

Then  $H_1$  and  $H_2$  are normal in  $G$  and are of finite index. Hence also  $[G: H_1 \cap H_2]$  is finite. To complete the proof, we show that  $H_1 \cap H_2 = 1$ . For if  $g \in H_1 \cap H_2$ , the matrix of  $g$  is just

$$\begin{bmatrix} I & U(g) \\ 0 & I \end{bmatrix},$$

and its  $m$ th power is

$$\begin{bmatrix} I & mU(g) \\ 0 & I \end{bmatrix}.$$

Hence  $U(g) = 0$ , and so  $g = 1$ . This completes the proof of Burnside's theorem.

We may remark that the result is false for  $K$  an infinite field of characteristic  $p \neq 0$ . For example, the matrices

$$\left\{ \begin{pmatrix} 1 & \alpha \\ 0 & 1 \end{pmatrix}, \alpha \in K \right\},$$

form an infinite group whose elements other than the identity have order  $p$ .

(36.2) THEOREM (Schur [7]). *Any finitely generated periodic subgroup of  $GL(n, K)$  is finite.*

PROOF. Let  $A_1, \dots, A_r$  generate a periodic subgroup  $G$ , and let  $E$  be the field obtained by adjoining to the rational field  $Q$  the entries of all of these  $r$  matrices. Then the entries of each  $g \in G$  lie in the field  $E$ , and so each characteristic root of any such matrix is a root of unity which satisfies an  $n$ th degree equation with coefficients in  $E$ . We shall show that there are finitely many such roots of unity, whence there will exist a positive integer  $m$  such that each root of unity will be an  $m$ th root of unity. The matrix  $g^m$  will have all its characteristic roots equal to 1. Since also  $g^m$  has finite order, it follows from Exercise 30.7 that  $g^m = I$ . Thus  $G$  is of bounded period, and hence finite by Burnside's theorem.

We complete the proof as follows: We may write

$$E = Q(a_1, \dots, a_k, a_{k+1}, \dots, a_t)$$

where the subscripts are so arranged that  $\{a_1, \dots, a_k\}$  form a transcendence basis for  $E$  over  $Q$ . Let us set

$$T = Q(a_1, \dots, a_k).$$

Then  $a_{k+1}, \dots, a_t$  are algebraic over  $T$ , and hence  $(E: T) = d$  is finite. Now let

$$F = \{\alpha \in E : \alpha \text{ is algebraic over } Q\},$$

so that  $F$  is a subfield of  $E$ . We shall prove that  $(F: Q) \leq d$ . For let  $\alpha_1, \dots, \alpha_{d+1} \in F$ ; these elements are linearly dependent over  $T$ , and thus we may find polynomials  $\{P_i(X_1, \dots, X_k) : 1 \leq i \leq d+1\}$  not all zero, with coefficients in  $Q$ , such that

$$\sum_{i=1}^{d+1} P_i(\alpha_1, \dots, \alpha_k) \alpha_i = 0.$$

Set

$$R(X_1, \dots, X_k) = \sum_{i=1}^{d+1} P_i(X_1, \dots, X_k) \alpha_i,$$

so that  $R$  is a polynomial in  $X_1, \dots, X_k$  with algebraic coefficients. Let  $R^\sigma$  range over all possible conjugates of these polynomials and form  $\prod_\sigma R^\sigma \in Q[X_1, \dots, X_k]$ . This product vanishes at  $(\alpha_1, \dots, \alpha_k)$ , hence must be the zero polynomial because  $\{\alpha_1, \dots, \alpha_k\}$  are a transcendence basis for  $E$  over  $Q$ . But then  $R$  is the zero polynomial, so that if we choose  $x_1, \dots, x_k \in Q$  so that some  $P_i(x_1, \dots, x_k) \neq 0$ , we see that

$$0 = \sum_i P_i(x_1, \dots, x_k) \alpha_i$$

is a relation of linear dependence (over  $Q$ ) among  $\alpha_1, \dots, \alpha_{d+1}$ .

Now let  $\rho$  be a primitive  $m$ th root of unity which satisfies a polynomial equation over  $E$  of degree  $n$ , and set

$$f(X) = \text{Irr}(\rho, E) = X^s + b_1 X^{s-1} + \dots + b_s,$$

so that  $s \leq n$ . Since  $f(X) | (X^m - 1)$ , we conclude that each  $b_i \in Q(\sqrt[m]{1})$  and thus that  $f(X) \in F[X]$ . Let  $f^\sigma$  range over the conjugates of  $f$ ; there are at most  $d$  such conjugates. Then

$$r(X) = \prod_\sigma f^\sigma \in Q[X],$$

and  $r(\rho) = 0$ , whence  $\Phi_m(X) | r(X)$ , where  $\Phi_m(X)$  is the cyclotomic polynomial of order  $m$ . Therefore

$$nd \geq sd \geq \text{degree of } r(X) \geq \varphi(m).$$

However  $\varphi(m) \rightarrow \infty$  as  $m \rightarrow \infty$ , which proves that  $m$  is bounded once  $n$  and  $d$  are known. This shows that there are only a finite

number of roots of unity which satisfy  $n$ th degree equations over  $E$ . This completes the proof of Theorem 36.2.

(36.3) COROLLARY. *Every periodic subgroup of  $GL(n, K)$  is a completely reducible set of linear transformations.*

PROOF. Let  $G$  be a periodic subgroup of  $GL(n, K)$ , and let  $\{g_1, \dots, g_r\}$  be a maximal set of linearly independent elements of  $G$ . Every element of  $G$  is a  $K$ -linear combination of these  $\{g_i\}$ . Let  $H$  be the subgroup of  $G$  generated by  $\{g_1, \dots, g_r\}$ . Then  $H$  is finite by Theorem 36.2, and therefore by Maschke's theorem  $H$  is completely reducible as a set of linear transformations. But if  $M$  is the vector space on which  $G$  and  $H$  act,  $G$ -reducibility and  $H$ -reducibility are the same, since every element of  $G$  is a  $K$ -linear combination of elements of  $H$ . This proves that  $G$  is also completely reducible, and the corollary is established.

In order to derive further results on periodic subgroups of  $GL(n, K)$ , it will be necessary for us to consider unitary matrices. We shall accordingly devote the next few pages to a brief discussion of unitary matrices, in keeping with our aim of making this book as self-contained as is practicable.

For each complex number  $\alpha$ , let  $\bar{\alpha}$  denote its complex conjugate. If  $M$  is an  $n$ -dimensional vector space over the complex field  $K$ , we call a map  $f: M \times M \rightarrow K$  a *positive definite hermitian form* if  $f$  is additive in each component separately, and

$$f(\alpha m, m') = \alpha f(m, m') , \quad f(m, m') = \overline{f(m', m)} , \\ f(m, m) > 0 \text{ for } m \neq 0 ,$$

where  $m, m' \in M, \alpha \in K$  (see Exercises 10.6–10.7). The *unitary group* on  $M$  consists of all  $U \in \text{Hom}_K(M, M)$  for which

$$f(Um, Um') = f(m, m') , \quad m, m' \in M .$$

Choose  $m_1 \in M$  so that  $f(m_1, m_1) = 1$ . Now let  $m'_2 \in M, m'_2 \notin Km_1$ , and find  $\alpha \in K$  such that

$$f(m_1, \alpha m_1 + m'_2) = 0 .$$

Then set  $m_2 = \beta(\alpha m_1 + m'_2)$ , with  $\beta \in K$  chosen so that  $f(m_2, m_2) = 1$ . Continuing in this way, we obtain a basis  $\{m_1, \dots, m_n\}$  of  $M$  such that

$$f(m_i, m_j) = \delta_{ij} , \quad 1 \leq i, j \leq n .$$

We call such a basis a *unitary basis* of  $M$ . We see at once that a

transformation  $U \in \text{Hom}_K(M, M)$  is unitary if and only if  $U$  carries unitary bases onto unitary bases.

Relative to a unitary basis of  $M$ , every  $U \in \text{Hom}_K(M, M)$  is represented by a matrix  $U$ , and we find easily that  $U$  is unitary if and only if

$$(36.4) \quad U \cdot {}^t \bar{U} = I$$

where  ${}^t \bar{U}$  is the transpose of the complex conjugate of  $U$ . From the above, it follows that an  $n \times n$  matrix  $(u_{ij})$  is unitary if and only if

$$(36.5) \quad \sum_{j=1}^n u_{ij} \bar{u}_{kj} = \delta_{ik}, \quad 1 \leq i, k \leq n.$$

The following theorem is an immediate consequence of the definitions, and we omit its proof:

- (36.6) THEOREM. (i) Inverses of unitary matrices are unitary.
- (ii) If  $U$  and  $V$  are unitary, so are  $V^{-1}UV$  and  $UV$ .
- (iii) Every permutation matrix is unitary.
- (iv) A triangular matrix which is unitary must be diagonal.

A slightly more difficult result is

- (36.7) THEOREM. Given a complex matrix  $A$ , there exists a unitary  $U$  such that  $U^{-1}AU$  is triangular.

PROOF. Use induction on the size of  $A$ . Suppose  $A$  is the matrix of a transformation  $A \in \text{Hom}_K(M, M)$  relative to some unitary basis of the vector space  $M$ . Replacement of  $A$  by  $U^{-1}AU$ ,  $U$  unitary, amounts to change of unitary basis in  $M$ . Choose  $m \in M$ ,  $m \neq 0$ , to be a characteristic vector of  $A$ , so that  $Am = \alpha m$  for some  $\alpha \in K$ . The previous discussion shows that we can find a unitary basis  $\{m_1, \dots, m_n\}$  of  $M$  with  $m_1 = \beta m$  for some  $\beta \in K$ . Relative to this basis the matrix of  $A$  is just

$$\begin{pmatrix} \alpha & * \\ 0 & B \end{pmatrix}.$$

Use the induction hypothesis to triangularize  $B$  by a unitary transformation, and the result is proved.

- (36.8) COROLLARY. If  $V$  is unitary, there exists a unitary  $U$  such that  $U^{-1}VU$  is diagonal.

PROOF. Use (36.7) and (ii) and (iv) of (36.6).

As an immediate consequence of the above, we have

(36.9) COROLLARY. *The characteristic values of a unitary matrix have absolute value 1.*

We shall also need to know

(36.10) THEOREM. *A pair of commuting unitary matrices can be simultaneously diagonalized by a unitary transformation.*

PROOF. Let  $U, V$  be commuting unitary matrices. We wish to show the existence of a unitary  $W$  such that both  $W^{-1}UW$  and  $W^{-1}VW$  are diagonal, and we may begin by taking  $U$  in diagonal form, say

$$U = \text{diag } \{\alpha_1 I, \dots, \alpha_r I\},$$

where  $\alpha_1, \dots, \alpha_r$  are distinct. Since  $VU = UV$ , we have

$$V = \text{diag } \{V_1, \dots, V_r\}.$$

Choose  $W_i$  unitary such that  $W_i^{-1}V_iW_i$  is diagonal, and set

$$W = \text{diag } \{W_1, \dots, W_r\}.$$

Then both  $W^{-1}UW$  and  $W^{-1}VW$  are diagonal matrices, and the proof is completed.

We have seen that any finite subgroup of  $GL(n, K)$  can be identified with a group of unitary transformations on an  $n$  dimensional vector space (see Exercise 10.6). Indeed if  $G$  is a finite group of linear transformations acting on the  $n$ -dimensional space  $M$ , let  $h$  be any positive definite hermitian form on  $M$ , and set

$$f(m, m') = \sum_{z \in G} h(xm, xm'), \quad m, m' \in M.$$

This yields a new positive definite hermitian form  $f$  on  $M$ , and each  $g \in G$  is a unitary transformation on  $M$  relative to  $f$ . From this we showed (Exercise 10.7) that  $G$  must be completely reducible.

Suppose now that  $G$  is an irreducible group of unitary transformations of  $M$  relative to some positive definite hermitian form  $f$ . We claim that  $f$  is unique up to a non-zero constant factor. For let  $f'$  be another such form for which

$$f'(gm, gm') = f'(m, m'), \quad m, m' \in M.$$

Let  $\{m_1, \dots, m_n\}$  be a unitary basis of  $M$  such that

$$f(m_i, m_j) = \delta_{ij}.$$

Then each  $m \in M$  is expressible as

$$m = \sum_j f(m, m_j) m_j .$$

Observe next that the map

$$m \longrightarrow \sum_j f'(m, m_j) m_j$$

is a  $K$ -homomorphism of  $M$ , and thus has a non-zero characteristic vector  $m_0$  relative to a characteristic root  $\lambda$ , say. This gives

$$\sum_j f'(m_0, m_j) m_j = \lambda m_0 = \lambda \sum_j f(m_0, m_j) m_j ,$$

which implies that

$$f'(m_0, m_j) = \lambda f(m_0, m_j) \quad \text{for all } j ,$$

and thus that

$$f'(m_0, x) = \lambda f(m_0, x) \quad \text{for all } x \in M .$$

Let

$$N = \{m \in M : f'(m, x) = \lambda f(m, x) \text{ for all } x \in M\} .$$

Then  $N \neq (0)$ , and surely  $N$  is a  $G$ -subspace of  $M$ . The irreducibility of  $M$  implies that  $N = M$ , and therefore

$$f'(m, x) = \lambda f(m, x) , \quad m, x \in M .$$

In other words,  $f'$  is a constant multiple of  $f$ , and clearly the multiplier  $\lambda$  is different from zero.

Having completed our preliminary remarks on unitary transformations, we are ready to resume our study of periodic subgroups of  $GL(n, K)$ . We have seen above that every finite group of linear transformations on a vector space  $M$  consists of unitary transformations relative to some positive definite hermitian form on  $M$ . More generally we have

(36.11) **THEOREM** (Schur [7]). *Every periodic subgroup of  $GL(M)$  consists of unitary transformations relative to some positive definite hermitian form on  $M$ . In other words, every periodic subgroup of  $GL(n, K)$  is similar to a group of unitary transformations.*

**PROOF.** Because of (36.3), it suffices to prove the result for  $G$  an irreducible periodic subgroup of  $GL(M)$ . The argument in (36.3) shows the existence of a finite irreducible subgroup  $H$  contained in  $G$ . But then  $H$  consists of unitary transformations for some form  $f$  on  $M$ . We shall show that for each  $g \in G$ ,

$$(36.12) \quad f(gm, gm') = f(m, m'), \quad m, m' \in M,$$

so that every transformation in  $G$  is unitary. Choose  $g \in G$ , and let  $H'$  be the subgroup of  $G$  generated by  $g$  and  $H$ . Then  $H'$  consists of unitary transformations for some form  $f'$  on  $M$ . But then every transformation in  $H$  is unitary for  $f'$ , and by the irreducibility of  $H$ , we conclude that  $f'$  is a constant multiple of  $f$ . Therefore (36.12) holds since  $g \in H'$ , and the theorem is established.

We shall now turn our attention to the question of the existence of abelian normal subgroups of a group  $G \subset GL(n, K)$ . In this direction we have

(36.13) **THEOREM** (Jordan [1]). *There exists a positive integer-valued function  $f$  defined on the positive integers such that every finite subgroup  $G$  of  $GL(n, K)$  contains an abelian normal subgroup of index  $\leq f(n)$ .*

Jordan's proof was simplified by Blichfeldt (see Miller, Blichfeldt, and Dickson [1]), Bieberbach [1], and Frobenius [5], the last of whom also sharpened the bound  $f(n)$ . We shall give here the following generalization:

(36.14) **THEOREM** (Schur [7]). *Let  $G$  be a periodic subgroup of  $GL(n, K)$ . Then  $G$  contains an abelian normal subgroup of index at most equal to*

$$(\sqrt{8n} + 1)^{2n^2} - (\sqrt{8n} - 1)^{2n^2}.$$

By Theorem 36.11 we may assume that  $G$  is a periodic group of unitary transformations. In order to prove Theorem 36.14 it will be necessary to develop some properties of unitary matrices which are more special and perhaps less well known than those considered earlier. The following chain of reasoning is due primarily to Frobenius [5], and was applied by Schur [7] to prove the above theorem.

For a square matrix  $A$  over the complex field, we define a "norm"  $\|A\|$  as follows:

$$\|A\| = \text{tr}(A \cdot {}^t \bar{A}) = \sum_{i,j} |a_{ij}|^2,$$

where  $A = (a_{ij})$ . We have at once

$$\|UA\| = \|AU\| = \|A\| \quad \text{for } U \text{ unitary}.$$

(36.15) **LEMMA.** *Let  $A, B$  be unitary  $n \times n$  matrices, and set  $C = ABA^{-1}B^{-1}$ . If  $AC = CA$  and  $\|I - B\| < 1$ , then  $AB = BA$ .*

**PROOF.** From  $AC = CA$ , we deduce at once that  $A$  commutes with  $BAB^{-1}$ . Since replacing each matrix  $X$  by its unitary transform  $U^{-1}XU$  ( $U$  unitary) does not affect either the hypotheses or the conclusion of the lemma, we may assume by (36.10) that both  $A$  and  $BAB^{-1}$  are diagonal, say

$$A = \text{diag } \{a_1 I, \dots, a_r I\}, \quad \{a_i\} \text{ distinct.}$$

But  $A$  and  $BAB^{-1}$  have the same characteristic roots, and so there exists a permutation matrix  $P$  (which is automatically unitary) such that

$$BAB^{-1} = P^{-1}AP.$$

Setting  $R = PB$ , we have  $AR = RA$ , and thus  $R$  has the form

$$R = \text{diag } \{R_1, \dots, R_r\}.$$

Assume now that  $B$  does not commute with  $A$ ; then neither does  $P$ , and so if we partition  $P$  into blocks

$$P = \begin{bmatrix} P_{11} & \cdots & P_{1r} \\ \cdot & \cdots & \cdot \\ P_{r1} & \cdots & P_{rr} \end{bmatrix},$$

then some block above the diagonal must be different from  $0$ , and therefore also some block below the diagonal is not zero. Hence there exist at least two non-zero entries of  $P$  not in any diagonal block, say  $p_{ij} = 1, p_{kl} = 1$ . Now we have

$$\|I - B\| = \|P(I - B)\| = \|P - R\|,$$

and, setting  $R = (r_{ij})$ ,

$$\begin{aligned} \|P - R\| &\geq |p_{ij} - r_{ij}|^2 + |p_{kl} - r_{kl}|^2 \\ &\quad + \sum_{r_{im} \in R_i} |p_{im} - r_{im}|^2 + \sum_{r_{kt} \in R_k} |p_{kt} - r_{kt}|^2. \end{aligned}$$

Let  $\mathbf{R}_\alpha, \mathbf{R}_\beta$  be the diagonal blocks containing the  $i$ th and  $k$ th rows, respectively. Then  $r_{ij} = r_{kl} = 0, p_{im} = 0$  for  $r_{im} \in \mathbf{R}_\alpha, p_{kt} = 0$  for  $r_{kt} \in \mathbf{R}_\beta$ , so we have

$$\|P - R\| \geq 1 + 1 + \sum |r_{im}|^2 + \sum |r_{kt}|^2,$$

and each of the latter sums equals 1 by (36.5). We have thus shown that if  $B$  does not commute with  $A$ , then  $\|I - B\| \geq 4$ , and this implies the truth of the lemma.

(36.16) **LEMMA.** *Let  $A$  and  $B$  be unitary, and let  $C = ABA^{-1}B^{-1}$ . Then*

$$\|I - C\| \leq 2 \|I - A\| \|I - B\|.$$

PROOF. Without loss of generality, we may assume that  $A$  is a diagonal matrix; set  $A = (a_{ij})$ ,  $B = (b_{ij})$ . Then

$$\begin{aligned}\|I - C\| &= \|I - ABA^{-1}B^{-1}\| = \|BA - AB\| \\ &= \|(B - I)A + A(I - B)\| \\ &= \sum_{i,j} |(b_{ij} - \delta_{ij})a_{ij} + a_{ii}(\delta_{ij} - b_{ij})|^2 \\ &= \sum_{i,j} |a_{ii} - a_{jj}|^2 |\delta_{ij} - b_{ij}|^2.\end{aligned}$$

But

$$\begin{aligned}|a_{ii} - a_{jj}|^2 &= |(1 - a_{ii}) - (1 - a_{jj})|^2 \leq \{|1 - a_{ii}| + |1 - a_{jj}|\}^2 \\ &\leq 2\{|1 - a_{ii}|^2 + |1 - a_{jj}|^2\} \leq 2\|I - A\|\end{aligned}$$

for each  $i$  and  $j$ . Thus

$$\|I - C\| \leq 2\|I - A\| \sum_{i,j} |\delta_{ij} - b_{ij}|^2 = 2\|I - A\| \|I - B\|.$$

(36.17) LEMMA. Let  $A$  and  $B$  be unitary matrices belonging to some periodic group, and assume

$$\|I - A\| < 1/2 \quad \text{and} \quad \|I - B\| < 4.$$

Then  $AB = BA$ .

PROOF. The group  $G$  generated by  $A$  and  $B$  is a finitely generated periodic group of linear transformations and hence is finite by Theorem 36.2. Consequently the numbers

$$\|I - G\|, \quad G \in G, G \neq I,$$

are bounded away from zero. Now set

$$B_0 = B, B_1 = AB_0A^{-1}B_0^{-1}, \dots, B_i = AB_{i-1}A^{-1}B_{i-1}^{-1}, \dots.$$

Then setting  $a = \|I - A\|$ , we have by (36.16),

$$\|I - B_i\| \leq 2\|I - A\| \|I - B_{i-1}\| = 2a \|I - B_{i-1}\|,$$

and so by induction on  $i$  we conclude that

$$\|I - B_i\| \leq (2a)^i \|I - B\| \quad \text{for } i \geq 0.$$

Letting  $i \rightarrow \infty$ , we see that  $\|I - B_i\| \rightarrow 0$ , and thus  $B_i = I$  for large enough  $i$ . Hence for some  $n$ ,  $A$  and  $B_n$  commute. But surely  $\|I - B_{n-1}\| < 4$ , so by (36.15) also  $A$  and  $B_{n-1}$  commute. Repeated use of (36.15) shows eventually that also  $A$  and  $B$  commute.

We may now prove Schur's theorem 36.14. Let  $G$  be a periodic subgroup of  $GL(n, K)$ ; we have seen that  $G$  may be assumed to consist of unitary matrices. Let  $H$  be the subgroup of  $G$  generated by

$$\{A \in G : \|I - A\| < 1/2\}.$$

Lemma 36.17 shows that  $H$  is an abelian subgroup of  $G$ , and clearly  $H \triangle G$ . We must obtain an upper bound for the index  $[G : H]$ .

Let  $\{\mathbf{R}_i\}$  be a possibly infinite collection of coset representatives of the cosets of  $H$  in  $G$ . Since two matrices  $\mathbf{R}$  and  $\mathbf{S}$  in  $G$  belong to the same coset modulo  $H$  if  $\|\mathbf{R} - \mathbf{S}\| < 1/2$ , we have

$$\|\mathbf{R}_i - \mathbf{R}_j\| \geq 1/2 \quad \text{for } i \neq j.$$

We shall view each  $n \times n$  complex matrix  $A$  as a point in a  $2n^2$ -dimensional real space. Then  $\|A\|^{1/2}$  gives the usual Cartesian distance  $d(A)$  from the origin  $\mathbf{0}$  to the point  $A$ . Each  $\mathbf{R}_i$  is unitary, so

$$d(\mathbf{R}_i) = \|\mathbf{R}_i\|^{1/2} = \sqrt{n},$$

that is, each  $\mathbf{R}_i$  lies on the surface of a sphere of radius  $\sqrt{n}$  with center at  $\mathbf{0}$ . Further we know that

$$d(\mathbf{R}_i - \mathbf{R}_j) \geq 1/\sqrt{2}, \quad i \neq j,$$

so the little spheres of radius  $1/\sqrt{8}$  drawn about each  $\mathbf{R}_i$  are non-overlapping (though possibly tangent). Each such sphere lies in the shell defined by

$$\sqrt{n} - 1/\sqrt{8} \leq d(X) \leq \sqrt{n} + 1/\sqrt{8}.$$

Letting  $c \cdot r^{2n^2}$  be the volume of a sphere of radius  $r$  in this  $2n^2$ -dimensional real space, we therefore have

$$[G : H] \cdot c(1/\sqrt{8})^{2n^2} \leq c\{\sqrt{n} + 1/\sqrt{8}\}^{2n^2} - c\{\sqrt{n} - 1/\sqrt{8}\}^{2n^2}.$$

This yields

$$[G : H] \leq (\sqrt{8n} + 1)^{2n^2} - (\sqrt{8n} - 1)^{2n^2},$$

and proves the theorem.

A slightly different approach to Jordan's theorem 36.13 may be found in Speiser [2], in which the upper bound  $f(n)$  is given by

$$f(n) = n! \cdot 12^{\pi(n+1)+1},$$

where  $\pi(n+1)$  is the number of primes  $\leq n+1$ .

Another interesting result on the existence of abelian subgroups of matrix groups was proved by Blichfeldt [1] and improved by Brauer [11], Ito [5], Tuan [1] and Feit and Thompson [2]. Blichfeldt's original result asserts that, if  $G$  is a finite subgroup of  $GL(n, K)$ , then the set of elements in  $G$  whose orders are divisible by no prime  $p \leq (n-1)(2n+1)$  forms an abelian normal subgroup of  $G$ .

### *Exercise*

1. (Burnside). For  $K$  the complex field, prove that a subgroup of  $GL(n, K)$  which has only a finite number of conjugate classes is a finite group. [Hint: imitate the proof of Theorem 36.1.]

## § 37. Units in a Group Ring

We shall apply the theory of characters to study the units (elements which possess multiplicative inverses) in the group ring  $ZG$  of a finite abelian group  $G$  with coefficients in the ring of rational integers  $Z$ . This theory is the work of G. Higman [1], and we prove only one of his results. The result is sufficient, however, to yield the interesting theorem that if  $G$  and  $G'$  are finite abelian groups such that  $ZG \cong ZG'$ , then  $G \cong G'$ . The question of whether  $ZG \cong ZG'$  implies  $G \cong G'$  for arbitrary finite groups is, as far as we know, unsolved (see however Losey [1], Berman [2]-[4].)

[If on the other hand we take for our coefficient ring the complex field  $K$ , then for all finite abelian groups  $G$  and  $G'$  such that  $[G:1] = [G':1]$ , we have  $KG \cong KG'$ . (This follows readily from §27.) The question has been raised whether for finite groups  $G$  and  $G'$ ,  $\Omega G \cong \Omega G'$  for all algebraically closed fields  $\Omega$  of arbitrary characteristic implies  $G \cong G'$ . This problem is also unsolved (see however Perlis and Walker [1] and Deskins [1]).]

In this section,  $G$  denotes always a finite abelian group,  $Z$  the ring of rational integers, and  $Q$  the rational field. If  $m$  is the exponent of  $G$  and  $\zeta$  is a primitive  $m$ th root of 1, then  $K = Q(\zeta)$  is a splitting field for  $G$  [see Theorem 9.10], and there are  $[G:1]$  irreducible one-dimensional  $K$ -representations of  $G$ , which we may identify with their characters

$$\zeta^{(1)}, \zeta^{(2)}, \dots, \zeta^{(n)}, \quad n = [G:1].$$

By Theorem 33.8, the central idempotents in  $KG$  are given by

$$\eta_i = \frac{1}{[G:1]} \sum_{g \in G} \overline{\zeta^{(i)}(g)} g , \quad 1 \leq i \leq n .$$

An arbitrary element  $a \in KG$  can be expressed in the form

$$(37.1) \quad a = \sum_{g \in G} \alpha_g g = \sum_{i=1}^n \beta_i \eta_i ,$$

where

$$(37.2) \quad \beta_i = \sum_{g \in G} \alpha_g \overline{\zeta^{(i)}(g)}$$

and

$$(37.3) \quad \alpha_g = \frac{1}{[G:1]} \sum_{i=1}^n \beta_i \overline{\zeta^{(i)}(g)} .$$

(37.4) **THEOREM.** *Let  $R = \text{alg. int. } \{K\}$ . Any unit of finite order in  $RG$  has the form  $\epsilon g$  for some  $g \in G$  and some unit  $\epsilon$  in  $R$ .*

**PROOF.** Let  $a \in RG$  satisfy  $a^k = 1$  for some  $k$ . Then (37.1) implies that

$$\beta_i^k = 1 , \quad 1 \leq i \leq n .$$

Hence each  $\beta_i$  and all its conjugates have absolute value 1; by Theorem 9.10, the same is true for  $\zeta^{(i)}(g)$ , for all  $i$  and  $g$ . Since  $a$  is a unit, some  $\alpha_g$  in (37.1) is different from zero, and we have by (37.3)

$$(37.5) \quad |\alpha_g| = \frac{1}{[G:1]} \left| \sum_{i=1}^n \beta_i \zeta^{(i)}(g) \right| \leq \frac{1}{[G:1]} \sum_{i=1}^n |\beta_i \zeta^{(i)}(g)| = 1 ,$$

and the same is true for any algebraic conjugate of  $\alpha_g$ . The product of these conjugates is the norm of  $\alpha_g$ , and is a rational integer since  $\alpha_g \in R$ . Therefore we must have equality in (37.5). By Exercise 21.8, we may conclude that

$$\beta_1 \zeta^{(1)}(g) = \cdots = \beta_n \zeta^{(n)}(g) = \alpha_g$$

and hence

$$\beta_i = \alpha_g \overline{\zeta^{(i)}(g)} , \quad 1 \leq i \leq n .$$

Substituting in (37.3), we have the result that

$$\alpha_h = 0 , \quad h \neq g ,$$

and  $\alpha_g$  is a unit in  $R$ . This completes the proof.

Since  $Z \subset R$ , we have as an immediate consequence

(37.6) COROLLARY. *The units of finite order in  $ZG$  have the form  $\pm g$  for some  $g \in G$ .*

(37.7) THEOREM. *Let  $G$  and  $G'$  be finite abelian groups such that the group rings  $ZG$  and  $ZG'$  are isomorphic. Then  $G \cong G'$ .*

PROOF. Let  $U$  and  $U'$  denote the groups of units in  $ZG$  and  $ZG'$ , respectively. Then  $U$  and  $U'$  are (possibly infinite) abelian groups, and  $ZG \cong ZG'$  implies that  $U \cong U'$ . In any abelian group  $U$  the elements of finite order form a subgroup  $U_0$ , and  $U \cong U'$  implies  $U_0 \cong U'_0$ . Corollary 37.6 implies  $U_0 \cong G \times Z_2$ , where  $Z_2$  is the group  $\{\pm 1\}$ , and likewise  $U'_0 \cong G' \times Z_2$ . Then

$$G \times Z_2 \cong G' \times Z_2,$$

which implies  $G \cong G'$  by the elementary divisor theorem [Theorem 4.2], and the proof is completed.

Other results on group rings over the integers may be found in Berman [2], [4], [6], Takahashi [3], Cohn and Livingstone [1].

Additional references for this chapter are Dade [2], Gallagher [1], and Sah [1].

## Induced Characters

### § 38. Introduction

Throughout this section, let  $K$  be the complex field and  $G$  any finite group. We have seen in § 12D that for  $H$  a subgroup of  $G$ , to each  $KH$ -module  $M$  there corresponds an *induced*  $KG$ -module  $M^G$  given by

$$(38.1) \quad M^G = KG \otimes_{KH} M.$$

(We consider always left modules having finite  $K$ -bases.) If  $\mu$  is the character afforded by  $M$  and  $\mu^G$  that of  $M^G$ , we call  $\mu^G$  an *induced character* and say that  $\mu^G$  is *induced* from  $\mu$ .

In this chapter we shall be concerned mainly with characters, reserving until Chapter VII our discussion of induced modules. Let  $S$  be some collection of subgroups of  $G$ , such as the set of all cyclic subgroups of  $G$ . We may then form the set of characters of  $G$  which are induced from characters of  $KH$ -modules as  $H$  ranges over all subgroups in the collection  $S$ . Our object, roughly speaking, is to compare this set of induced characters of  $G$  with the set of all characters of  $G$ . Many significant results can be obtained from these considerations.

We shall assume familiarity with the results of § 12 on tensor products. We shall also make use of some elementary facts on algebraic integers and cyclotomic fields. As in Chapter III, we use  $\text{alg. int.}\{E\}$  to denote the ring of all algebraic integers in an extension field  $E$  of the rational field  $Q$ . For  $\epsilon$  a root of unity, we showed in § 21 that  $\text{alg. int.}\{Q(\epsilon)\} = Z[\epsilon]$ , but we do not need this relatively deep result here and shall use instead the trivial observation that every element of  $Z[\epsilon]$  is an algebraic integer. From Chapter IV, we shall use the results of § 27. In the application to splitting fields in § 41, familiarity with parts of § 29 will be essential.

Let us recall briefly some of the properties of the induction process; the details have been worked out in § 12D, and we shall not repeat them here. Let  $H$  be a subgroup of  $G$ , and let

$$G = g_1 H \cup \cdots \cup g_n H, \quad n = [G : H],$$

be the decomposition of  $G$  into left cosets with respect to  $H$ . If the  $KH$ -module  $M$  affords a matrix representation  $\dot{M}$ , we extend the domain of definition of  $\dot{M}$  to  $G$  by letting  $\dot{M}$  vanish outside  $H$ . Specifically we set

$$\dot{M}(y) = \begin{cases} M(y), & y \in H \\ 0, & y \notin H. \end{cases}$$

Then relative to a suitable basis,  $M^g$  affords a matrix representation  $\dot{M}^g$  given by

$$(38.2) \quad M^g(x) = (\dot{M}(g_j^{-1}xg_i))_{1 \leq i, j \leq n}, \quad x \in G.$$

The induced character  $\mu^g$  obtained from this satisfies

$$\mu^g(x) = \sum_{i=1}^n \dot{\mu}(g_i^{-1}xg_i), \quad x \in G,$$

where  $\dot{\mu}$  coincides with  $\mu$  on  $H$  and vanishes outside  $H$ . Since

$$\dot{\mu}(h^{-1}yh) = \dot{\mu}(y), \quad h \in H, y \in G,$$

we deduce that

$$(38.3) \quad \mu^g(x) = \frac{1}{[H:1]} \sum_{t \in g} \dot{\mu}(t^{-1}xt), \quad x \in G.$$

It will be convenient to use the above formula under slightly more general circumstances. We had called (§ 30) a map  $\theta: G \rightarrow K$  a *class function* if

$$\theta(t^{-1}gt) = \theta(g), \quad g, t \in G.$$

Since class functions can be added and multiplied, it is clear that the set  $\text{cf}(G)$  of all class functions on  $G$  forms an algebra over  $K$  of dimension equal to  $s$ , the number of conjugate classes in  $G$ . We have seen that

$$\text{cf}(G) = K\zeta^{(1)} \oplus \cdots \oplus K\zeta^{(s)}$$

where  $\zeta^{(1)}, \dots, \zeta^{(s)}$  are the characters of the non-isomorphic irreducible  $KG$ -modules. Formula 38.3 then provides a method for obtaining from each  $\mu \in \text{cf}(H)$  an induced class function  $\mu^g \in \text{cf}(G)$ .

In the following, we shall prove a number of basic results on induced characters and induced modules. Since the character of a module determines the module up to isomorphism (because  $K$  has

characteristic 0), it is clear that each result on characters will imply the corresponding result for modules, and vice versa. Nevertheless, we feel it will be instructive to give two separate proofs of some results, one by using (38.3), the other by use of Definition 38.1.

(38.4) THEOREM (*Transitivity of Induction*). *Let  $E \subset H \subset G$  be groups, and  $M$  a  $KE$ -module affording the character  $\mu$ . Then*

- (i)  $(\mu^H)^G = \mu^G$ .
- (ii)  $(M^H)^G \cong M^G$ .

PROOF. (i). Let  $\dot{\mu}$  coincide with  $\mu$  on  $E$  and vanish on all other elements of  $G$ . If we set  $\lambda = \mu^H$ , we have

$$\lambda(h) = [E : 1]^{-1} \sum_{t \in H} \dot{\mu}(t^{-1}ht), \quad h \in H.$$

Let  $\dot{\lambda}$  coincide with  $\lambda$  on  $H$  and vanish outside  $H$ . Then we claim that

$$\dot{\lambda}(g) = [E : 1]^{-1} \sum_{t \in H} \dot{\mu}(t^{-1}gt), \quad g \in G.$$

This is clear for  $g \in H$ , and also holds when  $g \notin H$  because then both sides vanish.

By (38.3) we have, for  $g \in G$ ,

$$\lambda^G(g) = [H : 1]^{-1} \sum_{x \in G} \dot{\lambda}(x^{-1}gx),$$

and therefore

$$\lambda^G(g) = [H : 1]^{-1} [E : 1]^{-1} \sum_{z \in G} \sum_{t \in H} \dot{\mu}(t^{-1}x^{-1}gxt).$$

For fixed  $t \in H$ , let  $y = xt$ ; as  $x$  ranges over all elements of  $G$ , so does  $y$ . Therefore for  $g \in G$  we have

$$\begin{aligned} \lambda^G(g) &= [H : 1]^{-1} [E : 1]^{-1} \sum_{y \in G} \sum_{t \in H} \dot{\mu}(y^{-1}gy) \\ &= [E : 1]^{-1} \sum_{y \in G} \dot{\mu}(y^{-1}gy) = \mu^G(g). \end{aligned}$$

This proves the theorem.

(ii). We must show that

$$KG \otimes_{KH} (KH \otimes_{KB} M) \cong KG \otimes_{KB} M.$$

But this follows at once from the associativity of the tensor product together with Theorem 12.14.

We turn next to a consideration of product modules. Let  $M$

and  $N$  be  $KG$ -modules with characters  $\mu, \nu$ , respectively. We may form the *product module*  $M \otimes_K N$  which is a vector space over  $K$  of dimension  $(M : K)(N : K)$ , and upon which the elements of  $G$  act according to the rule

$$g(\sum m_i \otimes n_i) = \sum gm_i \otimes gn_i, \quad g \in G.$$

As we have seen (§ 30), the character  $\tau$  of  $M \otimes_K N$  is just  $\mu\nu$ ; that is,

$$\tau(g) = \mu(g)\nu(g), \quad g \in G.$$

A basic result due to Frobenius relates the processes of induction and product formation, as follows.

(38.5) THEOREM. *Let  $H$  be a subgroup of  $G$ ,  $M$  a  $KH$ -module with character  $\mu$ , and  $N$  a  $KG$ -module with character  $\nu$ . Then*

- (i)  $\mu^G \cdot \nu = \{\mu \cdot (\nu | H)\}^G$ , where  $\nu | H$  denotes the restriction of  $\nu$  to  $H$ .
- (ii)  $M^G \otimes_K N \cong (M \otimes_K N)^G$  as  $KG$ -modules, where on the right  $N$  is to be viewed as the  $KH$ -module obtained by restriction of the operator domain.

*Remark.* As mentioned before, (i) and (ii) are equivalent statements, but we shall give proofs of each. Furthermore, we note that since (i) holds for characters, it also holds for  $\mu \in \text{cf}(H)$ ,  $\nu \in \text{cf}(G)$ .

PROOF. (i). Set  $\nu_1 = \nu | H$ , and define  $\dot{\mu}$  and  $\dot{\nu}_1$  by making them vanish outside  $H$ . Then we have

$$(\mu\nu_1)^* = \dot{\mu}\nu$$

since both sides vanish outside  $H$  and coincide on  $H$ . Therefore for each  $g \in G$ ,

$$(\mu\nu_1)^G(g) = [H : 1]^{-1} \sum_{x \in G} \dot{\mu}(x^{-1}gx)\nu(x^{-1}gx).$$

But  $\nu$  is a class function on  $G$ , and so the above becomes

$$(\mu\nu_1)^G(g) = \nu(g) \cdot [H : 1]^{-1} \sum_{x \in G} \dot{\mu}(x^{-1}gx) = \nu(g)\mu^G(g)$$

which proves (i).

(ii). The proof of the second conclusion of the theorem is somewhat more difficult. We wish to show that

$$(KG \otimes_{KH} M) \otimes_K N \cong KG \otimes_{KH} (M \otimes_K N).$$

[This does *not* follow from the associativity of the tensor product!]

To apply Theorem 12.15, we would have to view  $M \otimes_K N$  as a left  $KH$ -module by letting  $KH$  act only on the elements of  $M$ , whereas in the above formula  $M \otimes_K N$  is made into a left  $KH$ -module by defining

$$h(m \otimes n) = hm \otimes hn, \quad h \in H, m \in M, n \in N,$$

and extending the definition by linearity.] Both  $(KG \otimes M) \otimes N$  and  $KG \otimes (M \otimes N)$  have  $K$ -dimension  $[G : H](M : K)(N : K)$ , so that any  $K$ -homomorphism of one onto the other must be a  $K$ -isomorphism.

Let us regard all  $K$ -modules as two-sided, and let us omit the subscripts  $KH$  and  $K$  under the  $\otimes$ , since it will be clear from the context which is meant. For each  $g \in G$ , the map

$$M \times N \rightarrow (KG \otimes M) \otimes N$$

defined by

$$(m, n) \rightarrow (g \otimes m) \otimes gn$$

is a balanced map of  $K$ -modules, and thus there exists a  $K$ -homomorphism

$$\phi_g: M \otimes N \rightarrow (KG \otimes M) \otimes N$$

for which

$$\phi_g(m \otimes n) = (g \otimes m) \otimes gn.$$

Next we define a map

$$KG \times (M \otimes N) \rightarrow (KG \otimes M) \otimes N$$

by means of

$$\left( \sum_{z \in G} \alpha_z z, u \right) \rightarrow \sum_{z \in G} \alpha_z \phi_z(u),$$

where the  $\alpha$ 's are in  $K$ , and  $u \in M \otimes N$ . To verify that this is a balanced map of  $KH$ -modules, it suffices to check that for each  $x \in G$ ,  $h \in H$ , and  $m \otimes n \in M \otimes N$ , the pairs

$$(xh, m \otimes n) \quad \text{and} \quad (x, h(m \otimes n))$$

have the same image. The image of the former pair is

$$\phi_{xh}(m \otimes n) = (xh \otimes m) \otimes xhn,$$

whereas the image of the latter pair is

$$\phi_x(h(m \otimes n)) = \phi_x(hm \otimes hn) = (x \otimes hm) \otimes x(hn).$$

These images coincide because

$$xh \otimes m = x \otimes hm \quad \text{in } KG \otimes_{K\mathbb{H}} M.$$

We may now conclude that there exists a  $K$ -homomorphism

$$\theta: KG \otimes_{K\mathbb{H}} (M \otimes N) \rightarrow (KG \otimes_{K\mathbb{H}} M) \otimes N$$

given by

$$g \otimes (m \otimes n) \mapsto (g \otimes m) \otimes gn.$$

Since the elements  $\{(g \otimes m) \otimes gn : g \in G, m \in M, n \in N\}$  contain a  $K$ -basis for  $(KG \otimes M) \otimes N$ , the map is onto and thus is a  $K$ -isomorphism.

Finally, we shall show that  $\theta$  is a  $KG$ -isomorphism, and for this it is enough to verify that for  $x \in G$  we have

$$\theta(xg \otimes (m \otimes n)) = x\{(g \otimes m) \otimes gn\}.$$

The left-hand side is  $(xg \otimes m) \otimes (xg)n$ ; the right is (by the way in which a product module is defined)

$$\{x(g \otimes m)\} \otimes x(gn) = (xg \otimes m) \otimes (xg)n.$$

This completes the proof.

As in Exercise 31.1, we define an *inner product*  $(\theta, \eta)$  of two functions  $\theta, \eta \in \text{cf}(G)$  by means of

$$(\theta, \eta) = \frac{1}{[G : 1]} \sum_{x \in G} \theta(x) \overline{\eta(x)},$$

in which, as usual, the bar denotes complex conjugate. Then

$$(\zeta^{(i)}, \zeta^{(j)}) = \delta_{ij}, \quad 1 \leq i, j \leq s,$$

by (31.17), and

$$(38.6) \quad (\sum a_i \zeta^{(i)}, \sum b_j \zeta^{(j)}) = \sum a_i \bar{b}_i.$$

In particular, we have

(38.7) *Let  $\zeta^{(i)}$  be the character of the irreducible  $KG$ -module  $Z_i$ , and let  $\mu$  be the character of an arbitrary  $KG$ -module  $M$ . Then the inner product  $(\mu, \zeta^{(i)})$  is equal to the number of composition factors of  $M$  which are isomorphic to  $Z_i$ .*

We shall often say that  $(\mu, \zeta^{(i)})$  is the “multiplicity with which  $M$  contains  $Z_i$ ” (or the “multiplicity with which  $\mu$  contains  $\zeta^{(i)}$ ”).

Possibly the most often used result on induced characters is the following:

(38.8) THEOREM (*Frobenius Reciprocity Theorem*). *Let  $H$  be a subgroup of  $G$ , and let  $\zeta \in \text{cf}(G)$ ,  $\psi \in \text{cf}(H)$ . Then*

$$(38.9) \quad (\psi, \zeta|H) = (\psi^g, \zeta).$$

*In particular, if  $\zeta$  and  $\psi$  are characters of irreducible  $KG$ - and  $KH$ -modules, respectively, the multiplicity of  $\psi$  in  $\zeta|H$  is the same as the multiplicity of  $\zeta$  in  $\psi^g$ . In other words, if  $\{\zeta^{(i)}\}$  are characters of irreducible  $KG$ -modules and  $\{\psi^{(j)}\}$  those of irreducible  $KH$ -modules, then*

$$\zeta^{(i)}|H = \sum_j a_{ij} \psi^{(j)}, \quad a_{ij} \in Z,$$

*is equivalent to*

$$\psi^{(j)g} = \sum_i a_{ij} \zeta^{(i)}.$$

PROOF. We need only prove (38.9), since it implies the rest of the theorem. Define  $\dot{\phi}$  to coincide with  $\phi$  on  $H$  and vanish outside  $H$ . Then

$$\begin{aligned} (\psi^g, \zeta) &= [G : 1]^{-1} \sum_{g \in G} \psi^g(g) \overline{\zeta(g)} \\ &= [G : 1]^{-1} [H : 1]^{-1} \sum_{x, g \in G} \dot{\phi}(x^{-1}gx) \overline{\zeta(x^{-1}gx)}. \end{aligned}$$

For fixed  $x \in G$ , as  $g$  ranges over all elements of  $G$ , so does  $x^{-1}gx$ . Thus

$$\begin{aligned} (\psi^g, \zeta) &= [G : 1]^{-1} [H : 1]^{-1} \sum_{x \in G} \sum_{y \in G} \dot{\phi}(y) \overline{\zeta(y)} \\ &= [H : 1]^{-1} \sum_{y \in G} \dot{\phi}(y) \overline{\zeta(y)} \\ &= [H : 1]^{-1} \sum_{y \in H} \phi(y) \cdot \overline{(\zeta|H)(y)} \end{aligned}$$

since  $\dot{\phi}$  vanishes outside  $H$ . This proves the theorem.

An algebra-theoretic interpretation of the preceding theorem may be found in Nakayama [1]. The result also follows from Exercise 44.1.

In order to familiarize the reader with the manner in which these theorems are used, as well as to derive results which will be needed later, we shall give a few immediate applications of Theorems (38.4) and (38.8).

A *character* of  $G$  shall mean here the character afforded by some  $KG$ -module. If the character  $\mu$  is afforded by the module  $M$ , the dimension  $(M : K)$  is called the *degree* of  $\mu$ . Characters of degree 1 are usually referred to as *linear characters* or *one-dimensional characters*. The character of the 1-representation of  $G$  we denote by  $1_G$  in this discussion.

We have seen that the set of characters of  $G$  is closed under addition and multiplication. It is often convenient to consider also the difference of two characters, which we call a *generalized character*. Thus the set of generalized characters of  $G$  is precisely

$$\text{char}(G) = Z\zeta^{(1)} \oplus \cdots \oplus Z\zeta^{(s)},$$

where  $Z$  is the ring of rational integers. Obviously  $\text{char}(G)$  is a subring of  $\text{cf}(G)$ .

In order to simplify the following discussion, let  $T(G)$  denote the set of all linear combinations (with coefficients from  $Z$ ) of characters of  $G$  induced from 1-characters of cyclic subgroups of  $G$ . We now show

(38.10) Let  $H$  be a cyclic group, and define the class function  $f_H: H \rightarrow Z$  by means of

$$(38.11) \quad f_H(x) = \begin{cases} [H : 1], & \text{if } x \text{ generates } H \\ 0, & \text{otherwise.} \end{cases}$$

Then we have  $f_H \in T(H)$ .

PROOF. When  $H = \{1\}$ , we see that  $f_H$  is just the 1-character and hence lies in  $T(H)$ . We now use induction on the order of  $H$ , supposing the result established for proper subgroups of  $H$ . We show first that

$$(38.12) \quad \sum_{E \subset H} (f_E)^H = [H : 1]1_H$$

where  $E$  ranges over all subgroups of  $H$ . For each  $x \in H$  we have

$$\sum_E (f_E)^H(x) = \sum_E [E : 1]^{-1}[H : 1]\dot{f}_E(x).$$

However  $\dot{f}_E(x) = 0$  except when  $E$  is the subgroup generated by  $x$ , and for that one subgroup we have  $\dot{f}_E(x) = [E : 1]$ . Therefore

$$\sum_E (f_E)^H(x) = [H : 1] \quad \text{for all } x \in H,$$

which proves (38.12).

To complete the proof of (38.10), we may now write

$$f_H = [H : 1]1_H - \sum'_E (f_E)^H,$$

where  $E$  now ranges over all proper subgroups of  $H$ . For each such  $E$ , we know by the induction hypothesis that  $f_E \in T(E)$ , and therefore [by Theorem 38.4]  $(f_E)^H \in T(H)$ . The above equation then implies that also  $f_H \in T(H)$ , and so we are finished.

We shall make use of this theorem in the next section, but we leave it now to take up a more difficult result of the same general nature, due to Blichfeldt [2]. The proof given is due to Brauer [19].

(38.13) THEOREM. *Let  $p$  be a prime, and let  $H = [a] \times B$  be the direct product of a cyclic group  $[a]$ , whose order is relatively prime to  $p$ , and a  $p$ -group  $B$ . Let  $\theta$  be the character of an irreducible  $KH$ -module. Then there exists a subgroup  $B_0 \subset B$  and a linear character  $\phi_0$  of  $[a] \times B_0$  such that  $\theta = \phi_0^H$ .*

PROOF. From Exercise 27.2, we know that the irreducible  $KH$ -module whose character is  $\theta$  must be of the form  $M \otimes N$ , where  $M$  is an irreducible  $K[a]$ -module,  $N$  an irreducible  $KB$ -module, and the action of  $H$  given by

$$(a^r b)(m \otimes n) = a^r m \otimes bn.$$

Thus there exist irreducible characters  $\theta_1$  of  $[a]$ ,  $\theta_2$  of  $B$ , such that

$$\theta(a^r b) = \theta_1(a^r)\theta_2(b), \quad r \in Z, b \in B.$$

But  $[a]$  is an abelian group, so each irreducible  $K[a]$ -module is one-dimensional, and thus  $\theta_1$  is a linear character. If  $\deg \theta$  denotes the degree of the character  $\theta$ , it follows that  $\deg \theta = \deg \theta_2$ . Moreover, we know that  $\deg \theta_2 | [B : 1]$  by Theorem 33.7, and so  $\deg \theta = p^n$  for some non-negative integer  $n$ .

We now proceed to prove the theorem by using induction on  $n$ . When  $n = 0$ , we see that  $\theta$  is already a linear character, and so we may take  $B_0 = B$  and  $\phi_0 = \theta$ . Suppose the result has been established for irreducible characters of degree  $p^\nu$ , where  $\nu \leq n - 1$ , and let  $\deg \theta = p^n$ . Let  $\lambda$  be any linear character on  $H$ . Then of course  $\lambda$  is an irreducible character of  $H$ , and the multiplicity  $m$  with which  $\lambda$  occurs when we express the character  $\theta\bar{\theta}$  of  $H$  as a sum of irreducible characters, is given by the inner product  $(\theta\bar{\theta}, \lambda)$ . Using the definition of inner products, we find readily that

$$(\theta\bar{\theta}, \lambda) = (\theta, \theta\lambda),$$

and so  $m$  is also the multiplicity with which  $\theta$  occurs when we express the character  $\theta\lambda$  as a sum of irreducible characters. However,  $\theta$  is irreducible and  $\deg \theta = \deg \theta\lambda$ , so that  $m = 1$  if  $\theta = \theta\lambda$ , and  $m = 0$  if  $\theta \neq \theta\lambda$ .

Let  $A$  be the set of all linear characters  $\lambda$  on  $H$  such that  $\theta\lambda = \theta$ . Then  $A$  is a multiplicative group, and we have

$$\theta\bar{\theta} = \sum_{\lambda \in A} \lambda + \sum_i \psi_i$$

where the  $\{\psi_i\}$  are non-linear irreducible characters on  $H$ . By the discussion at the beginning of this proof, we deduce that  $p \mid \deg \psi_i$  for each  $i$ ; also  $p \mid \deg \theta\bar{\theta} = (\deg \theta)(\deg \bar{\theta})$ , and consequently the above equality implies that  $p \mid [A : 1]$ . Hence  $A$  contains an element  $\lambda_1$  of order  $p$ . Then  $\lambda_1 \neq 1_H$ , and  $\lambda_1^p = 1_H$ . It follows readily that

$$H_1 = \{h \in H : \lambda_1(h) = 1\}$$

is a normal subgroup of  $H$  for which  $[H : H_1] = p$ . Since  $p \nmid$  order of  $[a]$  and  $\{\lambda_1(a)\}^p = 1$ , we deduce that  $\lambda_1(a) = 1$ , and thus  $a \in H_1$ . Therefore (see Exercise 4.2)

$$H_1 = [a] \times B_1$$

for some subgroup  $B_1 \subset B$ .

Now we note that  $\lambda_1 \mid H_1 = 1$ . On the other hand,

$$(\theta\bar{\theta}) \mid H_1 = \sum_{\lambda \in A} (\lambda \mid H_1) + \sum_i (\psi_i \mid H_1),$$

and in the first sum  $1 \mid H_1$  also occurs. Thus the 1-representation of  $H_1$  occurs in  $(\theta\bar{\theta}) \mid H_1$  with multiplicity at least 2, and so

$$(\theta \mid H_1, \theta \mid H_1) \geq 2,$$

which implies that  $\theta \mid H_1$  is the character of a reducible representation.

Let  $\phi$  be an irreducible character of  $H_1$  which occurs with multiplicity at least 1 in  $\theta \mid H_1$ . Then  $\deg \phi < \deg \theta$  since  $\theta \mid H_1$  is reducible. By the Frobenius reciprocity theorem 38.8, we have

$$(\theta \mid H_1, \phi) = (\theta, \phi^H)$$

so that  $\theta$  occurs in  $\phi^H$  with non-zero multiplicity. Therefore

$$\deg \theta \leq \deg \phi^n = [H : H_1] \deg \phi = p \deg \phi.$$

Since we already know that  $\deg \phi < \deg \theta$ , and that both degrees are powers of  $p$ , we may conclude that  $\deg \phi^H = \deg \theta$ , and thus that  $\phi^H = \theta$ .

Now we observe that  $\phi$  is an irreducible character on  $H_1$  of degree  $p^\nu$ , where  $\nu < n$ . By the induction hypothesis, we deduce the existence of a subgroup  $B_0 \subset B_1$  and a linear character  $\phi_0$  on  $[a] \times B_0$  such that  $\phi$  is the character induced from  $\phi_0$ . The transitivity of induction [Theorem 38.4] then implies that  $\theta = \phi_0^H$  and completes the proof.

As we shall see in §52, the above theorem is a special case of a much more general result which states that every irreducible character of a nilpotent group  $G$  is induced from a linear character of some subgroup of  $G$ . Since the group  $[a] \times B$  considered in Theorem 38.13 is nilpotent, and since each subgroup thereof is of the form  $[a^l] \times B_0$  for some  $l$  and some subgroup  $B_0$  of  $B$ , it is an easy task to deduce the conclusion of Theorem 38.13 from the more general Theorem 52.1.

As a final application, we shall give a method due to Brauer and Suzuki (Suzuki [1]) for constructing *irreducible* characters of  $G$  once one knows some irreducible characters of a subgroup of  $G$ , provided that certain hypotheses are fulfilled. The importance of this method of “exceptional characters,” as they are called, stems from the fact that they are indeed irreducible and hence yield information about the character table of  $G$ .

Let  $S$  be a subset of the finite group  $G$  containing 1. For  $s \in S$  and  $x \in G$ , we set  $s^x = x^{-1}sx$ , and then define

$$S^x = \{s^x : s \in S\}.$$

If we write

$$H = \{x \in G : S^x = S\},$$

then  $H$  is a subgroup of  $G$ . We assume now that  $S \subset H$ , a hypothesis which is satisfied when  $S$  is a subgroup of  $G$  but which might fail to hold otherwise. Assume further that

$$(38.14) \quad S \cap S^x = \{1\} \quad \text{for } x \in G - H,$$

where  $G - H$  denotes the set of elements in  $G$  which are not in  $H$ .

(38.15) LEMMA. *If  $\alpha \in \text{char}(H)$  vanishes outside  $S$ , then  $\alpha^g$  and*

$\alpha$  coincide on  $S - \{1\}$ . If furthermore  $\alpha(1) = 0$ , and if  $\beta \in \text{char}(H)$  also vanishes outside  $S$ , we have

$$(\alpha, \beta) = (\alpha^G, \beta^G).$$

PROOF. Let  $\dot{\alpha}$  coincide with  $\alpha$  on  $H$  and vanish outside  $H$ . Then for  $x \in G$  we have

$$\alpha^G(x) = [H : 1]^{-1} \sum_{t \in G} \dot{\alpha}(t^{-1}xt).$$

Now let  $x \in S - \{1\}$ . If  $t \in G - H$ , then  $S \cap S^t = \{1\}$ , and so  $t^{-1}xt \notin S$ ; that is,  $\dot{\alpha}(t^{-1}xt) = 0$ . On the other hand, for  $t \in H$  we have

$$\dot{\alpha}(t^{-1}xt) = \alpha(t^{-1}xt) = \alpha(x).$$

This shows that

$$\alpha^G(x) = \alpha(x), \quad x \in S - \{1\}.$$

For the second part of the lemma, assume that  $\alpha(1) = 0$ . The number of distinct conjugates  $S^x$  of  $S$  is exactly  $[G : H]$ , and each pair has only the identity element in common, by (38.14). Now we have

$$(\alpha^G, \beta^G) = [G : 1]^{-1} \sum_{x \neq 1} \alpha^G(x) \overline{\beta^G(x)},$$

and furthermore  $\alpha^G(x) = 0$  unless  $x$  is conjugate to some element of  $S$ . Since  $\alpha^G$  and  $\beta^G$  are class functions, it follows that

$$\begin{aligned} (\alpha^G, \beta^G) &= [G : 1]^{-1} [G : H] \sum_{x \in S} \alpha(x) \overline{\beta(x)} \\ &= [H : 1]^{-1} \sum_{x \in H} \alpha(x) \overline{\beta(x)} = (\alpha, \beta), \end{aligned}$$

using here the fact that  $\alpha$  vanishes on  $H - S$ . This completes the proof.

(38.16) THEOREM (Brauer, Suzuki [1]). Keeping the above notation, we let  $\lambda_1, \dots, \lambda_n$  be a set of distinct irreducible characters of  $H$  vanishing outside  $S$ , such that  $\lambda_1(1) = \dots = \lambda_n(1)$  and  $n \geq 2$ . Then there exists an  $\varepsilon = \pm 1$ , and distinct irreducible characters  $\zeta_1, \dots, \zeta_n$  of  $G$ , such that

$$\lambda_i^G - \lambda_j^G = \varepsilon(\zeta_i - \zeta_j), \quad 1 \leq i, j \leq n.$$

PROOF. Set  $\alpha = \lambda_1 - \lambda_2 \in \text{char}(H)$ , so that  $\alpha$  satisfies the hypotheses of the preceding lemma, and  $\alpha(1) = 0$ . Therefore

$$(\alpha, \alpha) = (\alpha^G, \alpha^G).$$

But by (38.6),  $\alpha = \lambda_1 - \lambda_2$  implies that  $(\alpha, \alpha) = 2$ , and therefore

$$\alpha^G = \pm \zeta_1 \pm \zeta_2$$

for some irreducible characters  $\zeta_1, \zeta_2$  of  $G$ . (Here  $\zeta_1$  is just some irreducible character, not necessarily the 1-character.) Because  $\alpha^G(1) = 0$ , it follows that the signs do not agree, and so

$$\alpha^G = \zeta_1 - \zeta_2, \text{ say.}$$

The relations

$$(\lambda_1 - \lambda_3, \lambda_1 - \lambda_2) = 1, \quad (\lambda_1 - \lambda_3, \lambda_1 - \lambda_3) = 2$$

now imply that either

$$(\lambda_1 - \lambda_3)^G = \zeta_1 - \zeta_3$$

or

$$(\lambda_1 - \lambda_3)^G = \zeta_3 - \zeta_2$$

for some irreducible character  $\zeta_3$ . If the former alternative holds, we conclude readily that

$$(\lambda_1 - \lambda_j)^G = \zeta_1 - \zeta_j, \quad j = 2, \dots, n,$$

for suitable irreducible characters  $\{\zeta_j\}$ , and in this case we may choose  $\varepsilon = +1$ . If the latter alternative holds, the result is valid with  $\varepsilon = -1$ . This proves the theorem.

This theorem has been generalized by Feit [5] as follows:

Keeping the notation preceding Lemma 38.15, let  $\{\lambda_{is} : s = 1, \dots, n_i; i = 1, \dots, k\}$  be a collection of distinct irreducible characters of  $H$  vanishing outside  $S$ , so indexed that all characters with the same first index have the same degree, and such that

$$\lambda_{is}(1) = u_i \lambda_{11}(1),$$

where  $u_1, \dots, u_k$  are integers such that

$$1 = u_1 < u_2 < \dots < u_k.$$

Suppose  $n_1 \geq 2$  and that

$$\sum_{i=1}^{m-1} n_i u_i^2 > 2u_m, \quad 1 \leq m \leq k.$$

Then there exists a sign  $\varepsilon = \pm 1$  and distinct irreducible characters  $\{\zeta_{ij}\}$  of  $G$  such that for each set of rational integers  $\{a_{ij}\}$  satisfying  $\sum_{i,j} a_{ij} \lambda_{ij}(1) = 0$ , we have

$$\sum_{i,j} a_{ij} \lambda_{ij}^G = \epsilon \sum_{i,j} a_{ij} \zeta_{ij} .$$

The characters  $\{\zeta_{ij}\}$  are called the *exceptional characters* associated with the set  $\{\lambda_{ij}\}$ .

For further results on exceptional characters, see Feit and Thompson [1].

### Exercises

- Let  $H$  be a subgroup of  $G$ . For each irreducible character  $\psi$  of  $H$ , express  $\psi^G$  in terms of irreducible characters of  $G$ , in each of the following cases:
  - $H = S_2, G = S_3$
  - $H = S_3, G = S_4$
  - $H = \{(1), (12)(34), (13)(24), (14)(23)\}, G = A_4$
  - $G = \text{dihedral group of order } 2p, p \text{ prime}, H = \text{cyclic subgroup of order } p$ .
- For  $\lambda, \mu, \nu \in \text{cf}(G)$ , prove that  $(\lambda, \mu\nu) = (\lambda\bar{\mu}, \nu)$ .
- Let  $g = [G : 1]$ ,  $\omega = \text{primitive } g\text{th root of 1 over } Q$ , and let  $\sigma$  be any automorphism of  $Q(\omega)$  over  $Q$ . If  $\zeta$  is any irreducible character of  $G$ , define  $\zeta^\sigma$  on  $G$  by

$$\zeta^\sigma(x) = \{\zeta(x)\}^\sigma, \quad x \in G.$$

Show that the map  $\zeta \rightarrow \zeta^\sigma$  permutes the irreducible characters of  $G$ . Which characters are fixed under all such permutations?

- Let  $\zeta^{(1)}, \dots, \zeta^{(s)}$  be a full set of irreducible complex characters of  $G$ , and let  $\lambda \in \text{cf}(G)$ . Prove that  $\lambda \in \text{char}(G)$  if and only if  $(\lambda, \zeta^{(i)}) \in Z$  for all  $i$ . Further, show that  $\lambda$  is a character of  $G$  if and only if  $(\lambda, \zeta^{(i)})$  is a non-negative rational integer for each  $i$ .

- Let  $H$  be a subgroup of  $G$ , and set  $H_1 = g^{-1}Hg$ . For  $\theta \in \text{cf}(H)$ , define  $\theta_1 \in \text{cf}(H_1)$  by means of

$$\theta_1(x) = \theta(gxg^{-1}), \quad x \in H_1.$$

Prove that  $\theta^G = \theta_1^G$ . If  $\theta \in \text{char}(H)$ , prove that  $\theta_1 \in \text{char}(H_1)$ .

- Let  $H \triangle G$ , and let  $\{g_1, \dots, g_n\}$  be a set of left coset representatives of  $G$  modulo  $H$ . For  $\theta \in \text{char}(H)$ , define  $\theta_i \in \text{char}(H)$  by

$$\theta_i(x) = \theta(g_i x g_i^{-1}), \quad x \in H.$$

We may refer to  $\theta_i$  as a  $G$ -conjugate of  $\theta$ . Show that

$$\theta^G | H = \theta_1 + \dots + \theta_n.$$

If  $r$  is the number of distinct characters among  $\theta_1, \dots, \theta_n$ , show that  $r | n$  and that each character among the  $\{\theta_i\}$  occurs  $n/r$  times in the set  $\{\theta_1, \dots, \theta_n\}$ . Thus

$$\theta^G | H = (n/r)(\theta_1 + \cdots + \theta_r)$$

after renumbering the  $\{\theta_i\}$  if need be. (See §49.)

7. Let  $H \triangle G$  and let  $\theta$  be an irreducible character on  $G$ . Then there exists an irreducible character  $\psi$  on  $H$  such that  $\theta = \psi^G$  if and only if  $\theta$  vanishes outside  $H$ , and  $\theta | H$  is a sum of distinct irreducible characters of  $H$ . [Hint: (i) Let  $\theta = 0$  outside  $H$ , and let  $\theta | H = \psi_1 + \cdots + \psi_r$ , where the  $\{\psi_i\}$  are distinct irreducible characters numbered so that  $\deg \psi_1 \leq \deg \psi_i$ ,  $i \geq 1$ . Then  $\deg \theta \geq r \deg \psi_1$ . But  $\psi_1^G$  contains  $\theta$ , so  $[G : H] \deg \psi_1 \geq \deg \theta$ . Finally, we find by computing  $(\theta, \theta)$  that  $[G : H] = r$ . This shows that  $\psi_1^G = \theta$ , and shows incidentally that all the  $\{\psi_i\}$  have the same degree. (ii) Let  $\theta = \psi^G$  where  $\psi$  is irreducible on  $H$ . Clearly  $\theta = 0$  outside  $H$ . By the Frobenius reciprocity theorem,  $\theta | H$  contains  $\psi$  with multiplicity 1. Now use Exercise 38.6.]

8. Let  $H$  be an abelian subgroup of  $G$ , and let  $\zeta$  be an irreducible character of  $G$ . Then  $\deg \zeta \leq [G : H]$ . [Hint: Let  $\psi$  be any irreducible character of  $H$  contained in  $\zeta | H$ ; then  $\deg \psi = 1$ . But  $\zeta$  is contained in  $\psi^G$ , so  $\deg \zeta \leq \deg \psi^G = [G : H] \deg \psi$ .]

9. A representation  $T: G \rightarrow GL(M)$  is *faithful* if  $T$  is an isomorphism. The character  $\tau$  of this representation is also called *faithful*. Show that, if  $\tau$  is a faithful linear character of  $G$ , then  $G$  is cyclic.

### § 39. Rational Characters

Let  $Q$  be the rational field,  $G$  a finite group. A *rational character* of  $G$  is the character afforded by some  $QG$ -module. If  $\phi$  is a rational character then  $\phi(g) \in Z$  for each  $g \in G$ , since  $\phi(g)$  is an algebraic integer lying in  $Q$ . We shall again let  $T(G)$  denote the set of all linear combinations  $\sum a_i \psi_i^G$ ,  $a_i \in Z$ , where the  $\psi_i$  are 1-characters of cyclic subgroups of  $G$ . In his work on generalized  $L$ -series, Artin [1], [3] proved the following remarkable result:

(39.1) THEOREM. *Let  $\phi$  be any rational character of a finite group  $G$ . Then  $[G : 1]\phi \in T(G)$ ; in other words, there exist rational integers  $\{a_i\}$  and cyclic subgroups  $\{H_i\}$  of  $G$  such that*

$$\phi = \sum_i \frac{a_i}{[G : 1]} \psi_i^G$$

where  $\psi_i$  is the 1-character of  $H_i$ .

We shall devote this section to the proof of Artin's theorem. In later sections we shall deal with more complicated types of induction theorems. These theorems, and the methods used in deriving them, yield significant results in the theory of group representations.

For  $H$  a cyclic subgroup of  $G$ , define  $f_H: H \rightarrow Z$  by

$$(39.2) \quad f_H(x) = \begin{cases} [H : 1] & \text{if } x \text{ generates } H \\ 0 & \text{if } x \in H \text{ and } x \text{ does not generate } H. \end{cases}$$

We have shown in (38.10) that  $f_H \in T(H)$ , so that by the transitivity of the induction map we may conclude that each induced character  $f_H^G (= (f_H)^G)$  lies in  $T(G)$ . To prove the theorem it therefore suffices to show for each rational character  $\phi$  of  $G$ , that  $[G : 1]\phi$  is expressible as a  $Z$ -linear combination  $\sum a_i f_{H_i}^G$ , where the  $\{H_i\}$  are cyclic subgroups of  $G$ .

For convenience we write  $x =_c y$  to indicate that  $x$  and  $y$  are conjugate elements of  $G$ ; the notation  $x \neq_c y$  indicates that  $x$  and  $y$  are not conjugate in  $G$ .

Let us now prove

(39.3) LEMMA. *If  $H$  is a cyclic subgroup of  $G$ , then*

$$f_H^G(x) = \begin{cases} [N(H) : 1] & \text{if } x =_c \text{some generator of } H \\ 0 & \text{if } x \neq_c \text{any generator of } H \end{cases}$$

where  $N(H)$  is the normalizer of  $H$  in  $G$ .

PROOF. Let us write  $f$  instead of  $f_H$  for convenience, and let  $\dot{f}$  coincide with  $f$  on  $H$  and vanish outside  $H$ . We have

$$f^G(x) = [H : 1]^{-1} \sum_{t \in G} \dot{f}(t^{-1}xt), \quad x \in G.$$

Since  $f$  vanishes on all elements of  $H$  which do not generate  $H$ , it follows at once that

$$f^G(x) = 0 \quad \text{if } x \neq_c \text{some generator of } H.$$

On the other hand let  $x =_c y$ , where  $y$  is some generator of  $H$ . Then  $f^G(x) = f^G(y)$  since  $f^G$  is a class function. To calculate  $f^G(y)$ , we observe that  $[y]$  and  $[t^{-1}yt]$  are cyclic groups of the same order, and hence  $t^{-1}yt$  generates  $H$  if and only if  $t^{-1}yt \in H$ . Further,  $t^{-1}yt \in H$  if and only if  $t \in N(H)$ , since  $y$  generates  $H$ . Thus

$$\begin{aligned} f^G(y) &= \frac{1}{[H : 1]} \sum_{t \in N(H)} \dot{f}(t^{-1}yt) \\ &= \frac{1}{[H : 1]} \cdot [N(H) : 1][H : 1], \end{aligned}$$

which proves the lemma.

We also need

(39.4) LEMMA. *If  $\phi$  is a rational character of  $G$  and if  $x, y \in G$  are such that  $[x] = [y]$ , then  $\phi(x) = \phi(y)$ .*

PROOF. Let  $H = [x] = [y]$ , and set  $\theta = \phi|_H$ . Then  $\theta$  is a rational character of  $H$ , and suppose it is afforded by the matrix representation  $U: H \rightarrow Q_n$ . Then

$$\phi(x) = \theta(x) = \text{trace of } U(x), \quad \phi(y) = \theta(y) = \text{trace of } U(y).$$

But if  $y = x^a$  then  $U(y) = U(x)^a$ , and the characteristic roots of  $U(y)$  are the  $a$ th powers of those of  $U(x)$ . The characteristic roots of  $U(x)$ , say  $\epsilon_1, \dots, \epsilon_n$ , are  $h$ th roots of 1, where  $h = [H:1]$ . Thus

$$\theta(x) = \epsilon_1 + \dots + \epsilon_n, \quad \theta(y) = \epsilon_1^a + \dots + \epsilon_n^a.$$

On the other hand we have  $\text{G.C.D.}(a, h) = 1$ , since  $y$  generates  $H$ , and thus the map  $\zeta \rightarrow \zeta^a$  gives an automorphism of  $Q(\zeta)$ , where  $\zeta$  is a primitive  $h$ th root of 1. This map carries  $\theta(x)$  into  $\theta(y)$ . But  $\theta(x) \in Q$  since  $\theta$  is a rational character, and hence  $\theta(x) = \theta(y)$ . This proves the lemma.

Let us proceed with the proof of the induction theorem. Let  $H_1, \dots, H_m$  be a full set of non-conjugate cyclic subgroups of  $G$ , and set  $H_i = [x_i]$ ,  $1 \leq i \leq m$ . Let  $\phi$  be any rational character of  $G$ , and define  $\tau \in \text{cf}(G)$  by means of

$$\tau = \sum_{i=1}^m \frac{[G:1]\phi(x_i)}{[N(H_i):1]} f_{H_i}^G.$$

Since each  $f_{H_i}^G \in T(G)$  and each coefficient lies in  $Z$ , it is clear that also  $\tau \in T(G)$ . Artin's theorem will be proved as soon as we verify that  $\tau(x) = [G:1]\phi(x)$  for each  $x \in G$ , for  $[G:1]\phi$  will then lie in  $T(G)$ .

Let  $x$  be any element of  $G$ . The cyclic group  $[x]$  is conjugate to exactly one  $H_j$ , and so there is a unique index  $j$  (between 1 and  $m$ ) for which  $x$  is conjugate to some generator of  $H_j$ . Therefore

$$f_{H_i}^G(x) = 0 \quad \text{if } i \neq j, \quad f_{H_j}^G(x) = [N(H_j):1],$$

and so

$$\tau(x) = \frac{[G:1]\phi(x_j)[N(H_j):1]}{[N(H_j):1]} = [G:1]\phi(x_j).$$

But  $x$  is conjugate to a generator of  $H_j$ , say,  $x =_c y$ , where  $[y] = H_j$ . By the preceding lemma we have  $\phi(y) = \phi(x_j)$ , and thus  $\phi(x) = \phi(y) = \phi(x_j)$ . Therefore

$$\tau(x) = [G : 1]\phi(x),$$

and the theorem is established.

A striking consequence of this theorem is as follows:

(39.5) COROLLARY. *The number of non-isomorphic irreducible  $QG$ -modules coincides with the number of non-conjugate cyclic subgroups of  $G$ .*

PROOF. Let  $\chi_1, \dots, \chi_t$  be a full set of irreducible rational characters of  $G$ , and let  $H_1, \dots, H_m$  be a full set of non-conjugate cyclic subgroups of  $G$ . We must show that  $m = t$ .

On the one hand, each  $f_{H_i}^G$  lies in  $T(G)$ , and hence is a  $Z$ -linear combination of the  $\{\chi_j\}$ . Furthermore, the formula

$$f_{H_i}^G(x_j) = \delta_{ij}[N(H_i) : 1]$$

shows that the  $\{f_{H_i}^G : 1 \leq i \leq m\}$  are linearly independent over  $Q$ . This implies that  $m \leq t$ .

On the other hand, we know from §30 that the  $\{\chi_j\}$  are linearly independent over  $Q$ . Furthermore, by the proof of (39.1), each  $\chi_j$ , being a rational character, is a  $Q$ -linear combination of the  $\{f_{H_i}^g\}$ . Therefore  $t \leq m$ . Together these inequalities show that  $t = m$ , which proves the result.

Further results on rational characters may be found in Takahashi [2].

### Exercises

- Verify the conclusion of Artin's theorem for the case  $G = S_3$ .
- Let  $G$  be a cyclic group of order  $n$ , generated by an element  $x$ . For each  $d$  dividing  $n$ , let  $\theta_d$  denote a primitive  $d$ th root of 1 over  $Q$ , and make  $Q(\theta_d)$  into a  $QG$ -module by defining

$$x \cdot \alpha = \theta_d \alpha, \quad \alpha \in Q(\theta_d).$$

Prove that the modules  $\{Q(\theta_d) : d \mid n\}$  give a full set of non-isomorphic irreducible  $QG$ -modules.

- Let  $\phi: G \rightarrow Z$  be a class function with the property that if  $x, y \in G$

are such that  $[x] = [y]$ , then  $\phi(x) = \phi(y)$ . Prove that  $[G : 1]\phi \in T(G)$ .

### § 40. Brauer's Theorem on Induced Characters

In the preceding section, we showed that every rational character of a finite group  $G$  is a  $Q$ -linear combination of characters induced from 1-characters of cyclic subgroups of  $G$ . For many purposes, however, it is important to know that every complex character of  $G$  is a  $Z$ -linear combination  $\sum a_i\psi_i^g$ ,  $a_i \in Z$ , where the  $\{\psi_i\}$  are complex characters of certain types of subgroups of  $G$ . The first significant result in this direction is

(40.1) BRAUER'S THEOREM ON INDUCED CHARACTERS (*Brauer* [19]). *Every complex character of  $G$  is a  $Z$ -linear combination of characters induced from linear characters of elementary subgroups of  $G$ , where by an elementary subgroup of  $G$  we mean one which is a direct product of a cyclic group and a  $p$ -group for some prime  $p$ .*

Using this theorem, Brauer was able to prove an important conjecture in the theory of  $L$ -series, and to give new and simpler proofs of some of his earlier basic results on group representations. We shall have more to say on this latter subject later in the book.

The present section will be devoted to the greatly simplified proof of the above theorem given by Brauer and Tate [1] in 1955. In a later section (§ 42) we shall take up a generalization of the theorem to the case where the underlying field is an arbitrary subfield of the complex field. In order to set forth the underlying ideas as clearly as possible, however, it seems desirable to first consider the special case above, and to deal with the generalization in a separate discussion.

Briefly recalling some earlier notation, we let  $K$  be the complex field. Let  $G$  be a finite group; by a *character* of  $G$  we mean the character of some  $KG$ -module. If  $\zeta^{(1)}, \dots, \zeta^{(s)}$  are the characters of a full set of non-isomorphic irreducible  $KG$ -modules, we had introduced the *ring of generalized characters*

$$\text{char}(G) = Z\zeta^{(1)} \oplus \cdots \oplus Z\zeta^{(s)},$$

a subring of the ring  $\text{cf}(G)$  of all complex-valued class functions on  $G$ .

We begin the proof of Theorem 40.1 with some basic definitions.

(40.2) DEFINITION. Let  $p$  be a prime. An element  $g \in G$  is  $p$ -

*regular* if  $p \nmid$  the order of  $g$ . An element whose order is a power of  $p$  is called *p-singular*.

(40.3) LEMMA. *Every element  $g \in G$  is expressible as  $g = g_1g_2$  where  $g_1$  and  $g_2$  commute,  $g_1$  is p-regular, and  $g_2$  is p-singular. The elements  $g_1, g_2$  are uniquely determined by  $g$ , and are called the p-regular and p-singular components of  $g$ , respectively.*

PROOF. Let  $g$  have order  $p^nq$ , where  $p \nmid q$ . Choose  $a, b \in Z$  such that  $ap^n + bq = 1$ , and set

$$g_1 = g^{ap^n}, \quad g_2 = g^{bq}.$$

Then  $g = g_1g_2$ , and  $g_1$  commutes with  $g_2$ . Further,  $g_1$  has order  $q$ , and  $g_2$  has order  $p^n$ . This shows the existence of at least one decomposition of  $g$ .

Suppose that  $g = g_3g_4$  where  $g_3$  and  $g_4$  commute, with  $g_3$  p-regular,  $g_4$  p-singular. Since the orders of  $g_3$  and  $g_4$  are relatively prime, the order of their product must be the L.C.M. of their orders. Hence  $g_3$  has order  $q$ ,  $g_4$  has order  $p^n$ . But then

$$\begin{aligned} g_3 &= g_3^{ap^n+bq} = g_3^{ap^n} = (gg_4^{-1})^{ap^n} \\ &= g^{ap^n}g_4^{-ap^n} = g^{ap^n} \end{aligned}$$

since  $g_4^{-1}$  commutes with  $g$ . Similarly  $g_4 = g^{bq}$ . This completes the proof.

(40.4) DEFINITION. Let  $p$  be a prime. A *p-elementary subgroup* of  $G$  is a direct product  $[a] \times B$  of a cyclic group  $[a]$  generated by a *p-regular* element  $a \in G$ , and a *p-group*  $B \subset G$ . Every cyclic group  $[g]$  is a *p-elementary subgroup* since we may write  $[g] = [g_1] \times [g_2]$  where  $g_1, g_2$  are the *p-regular* and *p-singular* components of  $g$ , respectively.

(We remark that a *p-elementary subgroup* may also be defined as a direct product  $[a] \times B$  of *p-group*  $B$  and an arbitrary cyclic group  $[a]$ . For we may write  $a = a_1a_2$  where  $a_1$  and  $a_2$  are the *p-regular* and *p-singular* components of  $a$ , respectively. Then we have

$$[a] \times B = [a_1] \times ([a_2] \times B),$$

and the right-hand side is a direct product of a *p-group*  $[a_2] \times B$  and a cyclic group  $[a_1]$  generated by a *p-regular* element.)

Let  $\{H_i : 1 \leq i \leq l\}$  be the family of all *p-elementary subgroups* of  $G$  for all primes  $p$  dividing  $[G : 1]$ . Since every cyclic subgroup

of  $G$  is a  $p$ -elementary subgroup of  $G$  for each  $p$ , every element of  $G$  obviously lies in some  $H_i$ . Let  $\{\psi_{ij} : 1 \leq j \leq s_i\}$  be a full set of irreducible characters of  $H_i$  in  $K$ . Then by definition

$$\text{char}(H_i) = Z\psi_{i1} \oplus \cdots \oplus Z\psi_{is_i}, \quad 1 \leq i \leq l.$$

Each  $\psi_{ij}$  induces a character  $\psi_{ij}^g$  on  $G$ . Define

$$(40.5) \quad v(G) = \sum_{i,j} Z\psi_{ij}^g = \sum_i \{\text{char}(H_i)\}^g.$$

We see readily that

$$v(G) \subset \text{char}(G).$$

Let us show that in fact  $v(G)$  is an ideal in the ring  $\text{char}(G)$ . Clearly  $v(G)$  is an additive subgroup of  $\text{char}(G)$ , and so it suffices to show for  $\theta \in \text{char}(G)$  that  $\theta \cdot \psi_{ij}^g \in v(G)$  for all  $i, j$ . By Theorem 38.5 we have

$$\theta \cdot \psi_{ij}^g = \{(\theta | H_i)\psi_{ij}\}^g \in \{\text{char}(H_i)\}^g \subset v(G),$$

which establishes the result.

Now choose  $\epsilon \in K$  to be a primitive  $[G : 1]$ -th root of 1, and set  $R = \text{alg. int. } \{Q(\epsilon)\}$ . Define the ring of generalized characters with coefficients in  $R$  as

$$\text{char}_R(G) = R\zeta^{(1)} \oplus \cdots \oplus R\zeta^{(s)},$$

and also let

$$v_R(G) = \sum R\psi_{ij}^g = \sum \{\text{char}_R(H_i)\}^g.$$

Clearly

$$\text{char}(G) \subset \text{char}_R(G), \quad v(G) \subset v_R(G).$$

The major step in the proof of Brauer's theorem will be to establish that the 1-character  $\zeta^{(1)}$  lies in  $v_R(G)$ . Supposing this known, let us show that as a consequence we must have  $\text{char}(G) = v(G)$ , so that every character of  $G$  will be a  $Z$ -linear combination of characters induced from irreducible (but not necessarily linear) characters of elementary subgroups of  $G$ . Since we are assuming that  $\zeta^{(1)} \in v_R(G)$ , we have

$$\zeta^{(1)} = \sum_{i=1}^q \xi_i \tau_i, \quad \xi_i \in R, \tau_i \in v(G).$$

(At this point we could make use of the fact that  $R$  has a finite  $Z$ -basis containing 1, for indeed we have shown in § 21 that  $R = Z[\epsilon]$ .

We shall not proceed in this manner, however, because the same argument will be needed later in § 42 in a more general situation. For this reason, we give a slightly more complicated proof which will carry over unchanged to that general situation.)

Set  $\xi_0 = 1$ , and consider the  $Z$ -module

$$R_0 = Z\xi_0 + Z\xi_1 + \cdots + Z\xi_q \subset R.$$

Then  $R_0$  is a finitely generated torsion-free  $Z$ -submodule of  $R$  and hence has a finite  $Z$ -basis. Moreover, the submodule  $Z\xi_0$  is a pure  $Z$ -submodule of  $R$  since

$$R \cap Q(Z\xi_0) = R \cap Q = Z\xi_0,$$

and it follows at once from (16.17) that any  $Z$ -basis of  $Z\xi_0$  can be completed to a  $Z$ -basis of  $R_0$ . Thus, in particular, there exists a  $Z$ -basis  $\{\alpha_1, \dots, \alpha_u\}$  of  $R_0$  in which  $\alpha_1 = \xi_0 = 1$ . We may thus rewrite the expression for  $\zeta^{(1)}$  as

$$\zeta^{(1)} = \sum_{j=1}^u \alpha_j \mu_j, \quad \mu_j \in v(G),$$

where now  $\alpha_1 = 1$  and where  $\{\alpha_1, \dots, \alpha_u\}$  are elements of  $R$  which are linearly independent over  $Q$ .

On the other hand  $v(G) \subset \text{char}(G)$ , and so we may write

$$\mu_j = \sum_{k=1}^s a_{jk} \zeta^{(k)}, \quad a_{jk} \in Z, \quad 1 \leq j \leq u.$$

This yields

$$\zeta^{(1)} = \sum_{j,k} \alpha_j a_{jk} \zeta^{(k)},$$

and hence, because of the linear independence of the  $\{\zeta^{(j)}\}$  over  $K$ , we have

$$\sum_j \alpha_j a_{jk} = \delta_{1k}, \quad 1 \leq k \leq s.$$

The linear independence of the  $\{\alpha_j\}$  over  $Q$  now implies that

$$\begin{aligned} \alpha_{11} &= 1, & \alpha_{21} &= 0, \dots, \alpha_{u1} &= 0, \\ a_{jk} &= 0 & \text{for } 1 \leq j \leq u, \quad 2 \leq k \leq s. \end{aligned}$$

Consequently,

$$\mu_1 = \sum_{k=1}^s a_{1k} \zeta^{(k)} = \zeta^{(1)},$$

which shows that

$$\zeta^{(1)} = \mu_1 \in v(G).$$

But  $\zeta^{(1)}$  is the unity element of the ring  $\text{char}(G)$ , and, since  $v(G)$  is an ideal in that ring, we may conclude that  $v(G) = \text{char}(G)$ . We have therefore shown that if  $\zeta^{(1)} \in v_R(G)$ , then  $v(G) = \text{char}(G)$ .

We come now to the heart of the proof, namely the construction of a large enough class of induced characters to enable us to conclude that  $\zeta^{(1)} \in v_R(G)$ .

(40.6) LEMMA. *Let  $H = A \times B$  be a subgroup of  $G$ , where  $A$  is abelian and where  $[A : 1], [B : 1]$  are relatively prime. Suppose that  $H \subset H_i$  for some elementary subgroup  $H_i$ . Then for each  $a \in A$  there exists an element  $\phi = \phi_a \in v_R(G)$  such that*

- (i)  $\phi(g) \in Z$  for all  $g \in G$ ,
- (ii)  $\phi(g) = 0$  if  $g$  is not conjugate in  $G$  to an element of  $aB$ ,
- (iii)  $\phi(a) = [C(a) : B]$ , where  $C(a)$  is the centralizer of  $a$  in  $G$ .

[Of course  $B \subset C(a)$ .]

PROOF. We shall set  $\phi = \psi^a$  for a suitable  $\psi \in \text{char}_R(H)$ . Since

$$\phi = (\psi^{H_i})^a$$

by the transitivity of the induction map, and since  $\psi^{H_i} \in \text{char}_R(H_i)$ , it follows that  $\phi \in v_R(G)$ . We proceed to construct the desired  $\psi$ .

Since  $A$  is abelian, it will have  $[A : 1]$  distinct one-dimensional characters of the form  $\lambda_i: A \rightarrow K$ , and these give all irreducible representations of  $A$  in  $K$  (see §9, Example 4). Each element  $x \in A$  is mapped onto an  $[A : 1]$ -th root of 1 by the character  $\lambda_i$ . Now extend  $\lambda_i$  to a map  $\omega_i: H \rightarrow K$  by setting

$$\omega_i(xy) = \lambda_i(x), \quad x \in A, y \in B.$$

Then  $\omega_i$  is a one-dimensional representation of  $H$  in  $K$ , and so certainly  $\omega_i \in \text{char}(H)$ .

Let us fix an element  $a \in A$ . Then  $\omega_i(a) \in R$ , and so

$$\psi = \sum_i \overline{\omega_i(a)} \omega_i \in \text{char}_R(H),$$

where  $\overline{\omega_i(a)}$  denotes the complex conjugate of  $\omega_i(a)$ . For  $x \in A$ ,  $y \in B$  we have [by (31.19)]

$$\begin{aligned} \psi(xy) &= \sum_i \overline{\omega_i(a)} \omega_i(xy) \\ &= \sum_i \overline{\lambda_i(a)} \lambda_i(x) = \begin{cases} [A : 1] & \text{if } x = a \\ 0 & \text{if } x \neq a. \end{cases} \end{aligned}$$

Let  $\dot{\psi}$  coincide with  $\psi$  on  $H$  and vanish outside of  $H$ . Then by definition

$$\psi^g(g) = [H : 1]^{-1} \sum_{t \in \sigma} \dot{\phi}(t^{-1}gt), \quad g \in G.$$

Now  $\dot{\phi}(t^{-1}gt) = 0$  unless  $t^{-1}gt \in H$ . Further, if  $t^{-1}gt = xy \in H$ , where  $x \in A$ ,  $y \in B$ , then still  $\dot{\phi}(t^{-1}gt) = 0$  unless  $x = a$ ; in case  $x = a$ , then  $\dot{\phi}(t^{-1}gt) = [A : 1]$ . Therefore  $\psi^g(g) \neq 0$  implies

$$\psi^g(g) = [H : 1]^{-1} \sum_{t \in \sigma} [A : 1] = [H : 1]^{-1} [A : 1] [T : 1],$$

where  $[T : 1]$  denotes the number of elements in the set

$$T = \{t \in G : t^{-1}gt = ay \text{ for some } y \in B\}.$$

Clearly,  $t \in T$  implies  $tb \in T$  for each  $b \in B$ , and so  $T$  consists of left cosets modulo  $B$ , and therefore  $[T : 1]$  is a multiple of  $[B : 1]$ . Since  $[H : 1] = [A : 1][B : 1]$ , we may conclude that  $\psi^g(g) \in Z$  for each  $g \in G$ .

Let us set  $\phi = \psi^g$ ; we have shown that both (i) and (ii) hold. Furthermore we have  $\phi(a) = [B : 1]^{-1}[T : 1]$ , and  $t \in T$  if and only if  $t^{-1}at = ab$  for some  $b \in B$ . But then

$$1 = t^{-1}a^{[A:1]}t = a^{[A:1]}b^{[A:1]} = b^{[A:1]}.$$

Since  $[A : 1]$  and  $[B : 1]$  are relatively prime, this shows that  $b = 1$ , and so  $t \in C(a)$ . Thus  $T = C(a)$ , and

$$\phi(a) = [B : 1]^{-1}[C(a) : 1] = [C(a) : B].$$

This completes the proof.

(40.7) LEMMA. *Let  $p$  be a prime. Then there exists  $\theta \in v_R(G)$  such that  $\theta(g) \in Z$  for all  $g \in G$ , and  $\theta(g) \equiv 1 \pmod{p}$  for all  $g \in G$ .*

PROOF. A conjugate class  $\mathfrak{C}$  in  $G$  is  $p$ -regular if all its elements are  $p$ -regular. Let  $\{a_1, \dots, a_n\}$  be a full set of representatives of the  $p$ -regular classes  $\mathfrak{C}_1, \dots, \mathfrak{C}_n$  of  $G$ . For each  $a_i$  we shall find an element  $\eta_i \in v_R(G)$  such that

- (i)  $\eta_i(g) \in Z$  for all  $g \in G$ ,
- (ii)  $\eta_i(g) = 0$  if the  $p$ -regular component of  $g \notin \mathfrak{C}_i$ ,
- (iii)  $\eta_i(g) \equiv 1 \pmod{p}$  if the  $p$ -regular component of  $g \in \mathfrak{C}_i$ .

We shall then set

$$\theta = \eta_1 + \cdots + \eta_n,$$

in which case  $\theta(g) \in Z$  for all  $g \in G$ . Further, for an element  $g \in G$ , its  $p$ -regular component must lie in exactly one class  $\mathfrak{C}_i$  ( $1 \leq i \leq n$ ), so that

$$\theta(g) = \eta_1(g) + \cdots + \eta_n(g) = \eta_i(g) \equiv 1 \pmod{p}.$$

We proceed with the construction of  $\eta_a$  and drop the subscripts for convenience. Let  $a$  be an element of the  $p$ -regular class  $\mathfrak{C}$ , and let  $A = [a]$  be the cyclic group generated by  $a$ . If  $B$  is any  $p$ -Sylow subgroup of  $C(a)$ , then  $H = A \times B$  is a  $p$ -elementary subgroup and thus certainly satisfies the hypotheses of Lemma 40.6. Construct  $\phi_a$  as in that lemma; then  $\phi_a(g) \in Z$  for all  $g \in G$ ,  $\phi_a(g) = 0$  if no conjugate of  $g$  lies in  $aB$ , and

$$\phi_a(a) = [C(a) : B] \not\equiv 0 \pmod{p}.$$

Choose  $m_a \in Z$  such that  $m_a \phi_a(a) \equiv 1 \pmod{p}$ , and set  $\eta_a = m_a \phi_a \in v_R(G)$ ; then  $\eta_a$  satisfies condition (i) above.

In order to verify that (ii) holds, let  $g = g_1 g_2$  where  $g_1, g_2$  are the  $p$ -regular and  $p$ -singular components of  $g$ , respectively. If  $g_1 \notin \mathfrak{C}$ , we now show that no conjugate of  $g$  lies in  $aB$ . For suppose that  $t^{-1}gt = ab$ ,  $b \in B$ ; then

$$g = (tat^{-1})(tbt^{-1})$$

gives a decomposition of  $g$  into a  $p$ -regular element  $tat^{-1}$  and a  $p$ -singular element  $tbt^{-1}$ , where  $tat^{-1}$  commutes with  $tbt^{-1}$ . By Lemma 40.3 we deduce that  $tat^{-1} = g_1$ , whence  $g_1 \in \mathfrak{C}$ , which is impossible. Thus no conjugate of  $g$  lies in  $aB$ , and so  $\eta_a(g) = 0$ .

On the other hand, suppose that  $g = g_1 g_2$  as above, but where now  $g_1 \in \mathfrak{C}$ . We have

$$\eta_a(g_1) = \eta_a(a) \equiv 1 \pmod{p},$$

so in order to prove (iii) we need only show that

$$\eta_a(g) \equiv \eta_a(g_1) \pmod{p}.$$

Since  $\eta_a \in v_R(G) \subset \text{char}_R(G)$ , we know that for each subgroup  $H_i$  we have  $\eta_a|H_i \in \text{char}_R(H_i)$ . Hence, if we set  $\tilde{\eta} = \eta_a|_{[g]}$ , we have  $\tilde{\eta} \in \text{char}_R([g])$ . Let  $\{\mu_i\}$  be a full set of irreducible characters of  $[g]$ . Then we may write

$$\tilde{\eta} = \sum_i \alpha_i \mu_i, \quad \alpha_i \in R,$$

and  $\eta_a(g) = \tilde{\eta}(g)$ ,  $\eta_a(g_1) = \tilde{\eta}(g_1)$ . Let  $p^d$  be the order of  $g_2$ , where  $g = g_1 g_2$ . Then we have, taking congruences modulo  $pR$ ,

$$\begin{aligned} \tilde{\eta}(g) &\equiv \{\tilde{\eta}(g)\}^{p^d} \equiv \sum_i \alpha_i^{p^d} \mu_i(g^{p^d}) \\ &\equiv \sum_i \alpha_i^{p^d} \mu_i(g_1^{p^d}) \equiv \{\tilde{\eta}(g_1)\}^{p^d} \equiv \tilde{\eta}(g_1) \end{aligned}$$

which completes the proof.

We may now finish the proof that  $v(G) = \text{char}(G)$ ; we need only show that the unity element  $\zeta^{(1)}$  of  $\text{char}_R(G)$  lies in the ideal  $v_R(G)$ . We shall accomplish this by proving that if for each  $p \mid [G : 1]$  we set

$$[G : 1] = p^e t_p, \quad p \nmid t_p,$$

then  $t_p \zeta^{(1)} \in v_R(G)$ . For once this is established, then using the fact that  $\{t_p : p \mid [G : 1]\}$  form a set of relatively prime integers, we can conclude that also  $\zeta^{(1)} \in v_R(G)$ .

Let  $p \mid [G : 1]$ , and set  $[G : 1] = p^e t_p$ ,  $p \nmid t_p$ . Choose  $\theta \in v_R(G)$  as in the preceding lemma, so that  $\theta(g) \in Z$  and  $\theta(g) \equiv 1 \pmod{p}$  for all  $g \in G$ . In that case

$$\{\theta(g)\}^{p^e} \equiv 1 \pmod{p^e}, \quad g \in G.$$

Setting

$$\psi = t_p(\theta^{p^e} - \zeta^{(1)}) \in \text{char}_R(G),$$

we have

$$\psi(g) = t_p(\{\theta(g)\}^{p^e} - \zeta^{(1)}(g)) \equiv 0 \pmod{[G : 1]}$$

since  $\zeta^{(1)}(g) = 1$ .

We shall now prove that  $\psi \in v_R(G)$ . From each of the conjugate classes  $\mathfrak{C}_1, \dots, \mathfrak{C}_s$  choose one element, say  $a_i$  from  $\mathfrak{C}_i$ . Then  $[a_i] \times [1]$  is a group of the type described in Lemma 40.6 and is in fact an elementary subgroup of  $G$ , so that we may choose  $\phi_i \in v_R(G)$  such that  $\phi_i(g) \in Z$  for all  $g \in G$ ,  $\phi_i(g) = 0$  if  $g \notin \mathfrak{C}_i$ , and  $\phi_i(a_i) = [C(a_i) : 1]$ . Let us define  $\lambda$  by

$$\psi(g) = [G : 1]\lambda(g), \quad g \in G.$$

Then we have  $\lambda(a_i) \in Z$  for all  $a_i$ ,  $1 \leq i \leq s$ , and

$$\psi(g) = \sum_{i=1}^s \lambda(a_i) \frac{[G : 1]}{[C(a_i) : 1]} \phi_i(g), \quad g \in G,$$

since  $\phi_i(g) = 0$  except when  $g \in \mathfrak{C}_i$ , and when  $g \in \mathfrak{C}_i$  we know that  $\phi_i(g) = [C(a_i) : 1]$ . Further, the coefficient of each  $\phi_i(g)$  above lies in  $Z$ , and therefore  $\psi$  is a  $Z$ -linear combination of  $\phi_1, \dots, \phi_s$ . This shows that  $\psi \in v_R(G)$ .

Now we have

$$t_p(\theta^{p^e} - \zeta^{(1)}) \in v_R(G).$$

On the other hand, also  $t_p \theta^{p^e} \in v_R(G)$  because  $\theta \in v_R(G)$ , and so we

conclude that  $t_p \zeta^{(1)} \in v_R(G)$ . This completes the proof that  $\text{char}(G) = v(G)$ .

We now know that every character of  $G$  is a  $Z$ -linear combination of characters induced from characters of elementary subgroups of  $G$ . In order to complete the proof of Brauer's theorem, it suffices, in view of the transitivity of the induction map, to establish that every irreducible character of a  $p$ -elementary subgroup  $H$  of  $G$  is induced from a linear character of some  $p$ -elementary subgroup of  $H$ . But we have already shown this in Theorem 38.13, and so the proof of Theorem 40.1 is complete.

The first important consequence of Brauer's theorem is a criterion for a class function to be a generalized character.

(40.8) THEOREM. *Let  $\theta \in \text{cf}(G)$ . Then  $\theta$  is a generalized character of  $G$  if and only if  $\theta|H$  is a generalized character of  $H$  for each elementary subgroup  $H$  of  $G$ .*

PROOF. As before, let  $H_1, \dots, H_l$  denote the set of elementary subgroups of  $G$ , and  $\{\psi_{ij}\}$  their characters. Define

$$u(G) = \{\theta \in \text{cf}(G) : \theta|H_i \in \text{char}(H_i), 1 \leq i \leq l\}.$$

Then we are trying to prove that  $\text{char}(G) = u(G)$ . It is clear that  $u(G)$  is a ring with unity element  $\zeta^{(1)}$ , and we have the inclusions

$$v(G) \subset \text{char}(G) \subset u(G).$$

Since we already know that  $\zeta^{(1)} \in v(G)$ , the theorem will be proved once we show that  $v(G)$  is an ideal in  $u(G)$ . For this it suffices to show that if  $\theta \in u(G)$ , then  $\theta \cdot \psi_{ij}^g \in v(G)$  for all  $i$  and  $j$ , since the  $\{\psi_{ij}^g\}$  generate the additive group  $v(G)$ . But we have

$$\theta \cdot \psi_{ij}^g = \{(\theta|H_i)\psi_{ij}\}^g \in \{\text{char}(H_i)\}^g \subset v(G),$$

where  $\psi_{ij}$  is an irreducible character of the elementary subgroup  $H_i$  of  $G$ . Thus the theorem is established.

(40.9) COROLLARY. *Let  $A$  be the ring of algebraic integers in an algebraic number field, and let  $\theta \in \text{cf}(G)$ . Then  $\theta \in \text{char}_A(G)$  if and only if  $\theta|H \in \text{char}_A(H)$  for every elementary subgroup  $H$  of  $G$ . (The symbol  $\text{char}_A(G)$  denotes the set of  $A$ -linear combinations of the complex characters of  $G$ .) Also see Green [1a], Fischer [1], and Banaschewski [1].*

### Exercises

1. Let  $\theta \in \text{cf}(G)$ . Prove that  $\theta$  is an irreducible character on  $G$  if and only if the following three conditions are satisfied:

- (i)  $\theta | H_t \in \text{char}(H_t)$  for each elementary subgroup  $H_t \subset G$ .
- (ii)  $(\theta, \theta) = 1$ .
- (iii)  $\theta(1) > 0$ .

2. Let  $\theta \in \text{cf}(G)$ . Prove that  $\theta \in \text{char}(G)$  if and only if the inner product  $(\theta, \psi_{ij}^G) \in Z$  for all  $i$  and  $j$ , where the  $\psi_{ij}$  are defined as in the discussion preceding (40.5).

3. Let  $\theta \in \text{cf}(G)$ . Prove that  $\theta \in \text{char}_R(G)$  if and only if

$$(\theta | H_t, \lambda_t) \in R$$

for each elementary subgroup  $H_t \subset G$  and each linear character  $\lambda_t$  on  $H_t$ .

## § 41. Applications

### § 41A. Splitting fields

Let  $S$  be a subfield of the complex field  $K$ , and let  $G$  be a finite group. We now restate some of the definitions and results of § 29, taking advantage of the simplifications which arise from the fact that here we are working in the complex field. An irreducible  $SG$ -module  $V$  is called *absolutely irreducible* if the extended module  $K \otimes_S V$  is irreducible as  $KG$ -module. We have shown [Theorem 29.13] that, if  $V$  is taken to be a minimal left ideal in some simple component of  $SG$ , then  $V$  is absolutely irreducible if and only if that simple component is of the form  $S_m$ , a full matrix algebra over  $S$ .

The field  $S$  is called a *splitting field* for  $G$  if every irreducible  $SG$ -module is absolutely irreducible. From § 29 it follows at once that  $S$  is a splitting field for  $G$  if and only if

$$SG \cong S_{m_1} + \cdots + S_{m_k},$$

a direct sum of full matrix algebras over  $S$ .

We recall that the *exponent* of  $G$  is the smallest positive integer  $n$  such that  $x^n = 1$  for all  $x \in G$ . In this subsection we shall prove

(41.1) **THEOREM.** *Let  $n$  be the exponent of  $G$ , and let  $Q$  denote the rational field. Then  $Q(\sqrt[n]{1})$  is a splitting field for  $G$ .*

This result was first conjectured by Maschke about 1900. Although special cases of it were established subsequently, it was not until 1945 that Brauer [15] (see also [20]) succeeded in proving the general theorem. We shall present here a proof which makes use of the properties of the Schur index.<sup>†</sup> A detailed dis-

---

<sup>†</sup> A second proof, independent of the Schur index, will be given at the end of this subsection.

cussion of the Schur index will be given in Chapter X, and it will suffice here to give its definition and one of its main properties.

We start with a fixed subfield  $F$  of the complex field  $K$ . If  $\mu$  is the character afforded by an irreducible  $KG$ -module  $M$ , we let  $F(\mu)$  denote the field obtained by adjoining to  $F$  all the values  $\{\mu(g) : g \in G\}$ . Now consider those fields  $S$  such that

$$(41.2) \quad F \subset S \subset K$$

for which there exists an  $SG$ -module  $V$  such that

$$(41.3) \quad M \cong K \otimes_S V.$$

(Of course  $V$  will have to be irreducible.) For such a field  $S$  and module  $V$ , it is clear that an  $S$ -basis of  $V$  is also a  $K$ -basis of  $M$  and that, relative to such a  $K$ -basis, the module  $M$  affords a representation of  $G$  by matrices with entries in the field  $S$ . We describe this situation by saying that  $M$  affords a matrix representation *realizable* in  $S$ . Conversely, this occurs only when (41.3) holds for some  $SG$ -module  $V$ .

From (41.3) we deduce the obvious fact that

$$\mu(g) \in S, \quad g \in G,$$

since each  $\mu(g)$  is the trace of a matrix with entries in  $S$ . Thus we must have

$$F(\mu) \subset S \subset K$$

whenever  $M$  affords a representation which is realizable in  $S$ .

(41.4) **DEFINITION.** The *Schur index*  $m_F(\mu)$  of the module  $M$  (or of the character  $\mu$ ) is defined as

$$m_F(\mu) = \min(S : F(\mu)),$$

the minimum being taken over all fields  $S$  such that  $F \subset S \subset K$  and such that  $M$  affords a representation realizable in  $S$ . We note that obviously

$$m_F(\mu) = m_{F(\mu)}(\mu)$$

so that the Schur index is unchanged when  $F$  is replaced by  $F(\mu)$ . Further,  $m_F(\mu) = 1$  if and only if  $M$  affords a representation realizable in  $F(\mu)$ .

Now let  $M$  be an irreducible  $KG$ -module, which we may assume is a minimal left ideal in the group algebra  $KG$ , and let  $S$  be any subfield of  $K$ . From Exercise 29.8 we know that there exists a

minimal left ideal  $V$  in  $SG$  such that  $M$  is a direct summand of  $V^K = K \otimes_S V$ . Then (41.3) holds if and only if  $V^K$  is irreducible; that is, it holds if and only if  $V$  is an absolutely irreducible  $SG$ -module. It follows from these remarks, together with (27.25), that every irreducible  $K$ -representation of  $G$  is realizable in  $S$  if and only if  $S$  is a splitting field for  $G$ .

The following basic result on the Schur index, which could in fact have been used as an alternative definition thereof, will be proved in § 70:

(41.5) *Let  $M$  be an irreducible  $KG$ -module with character  $\mu$ , and let  $F$  be a subfield of  $K$ . Then for each  $FG$ -module  $W$ , the multiplicity with which  $M$  occurs as a composition factor of  $W^K$  is a multiple of  $m_F(\mu)$ .*

We may now prove Brauer's theorem on splitting fields 41.1. Let  $M$  be an irreducible  $KG$ -module with character  $\mu$ , and set  $F = Q(\sqrt[n]{1})$  where  $n$  is the exponent of  $G$ . Then  $\mu(g) \in F$  for each  $g \in G$ , and so surely  $F(\mu) = F$ . To prove the theorem, we need merely show that  $m_F(\mu) = 1$  for each  $\mu$ . But by Brauer's theorem on induced characters, we may write

$$(41.6) \quad \mu = \sum a_i \omega_i^g, \quad a_j \in Z,$$

where the  $\{\omega_i\}$  are one-dimensional characters of elementary subgroups of  $G$ . Now every one-dimensional representation of a subgroup of  $G$  is realizable in  $F$ , and from (12.29) we see that any induced representation is realizable in the same field as the original representation of the subgroup. Thus each  $\omega_i^g$  is the character of some  $FG$ -module, and so the multiplicity of  $\mu$  in each  $\omega_i^g$  is a multiple of  $m_F(\mu)$ . However, the multiplicity of  $\mu$  in  $\sum a_i \omega_i^g$  is one, by (41.6), and therefore  $m_F(\mu) = 1$ . This completes the proof of Theorem 41.1.

It is of interest to give a second proof of Theorem 41.1, due to Feit [3], which does not use the Schur index. Again let  $K =$  complex field,  $F = Q(\sqrt[n]{1})$ , and let  $M$  be an irreducible  $KG$ -module with character  $\mu$ . Write  $\mu$  in the form (41.6), and observe that each  $\omega_i^g$  is the character of an  $FG$ -module. Hence there exist a pair of  $FG$ -modules  $T_1$  and  $T_2$ , with characters  $\tau_1$  and  $\tau_2$ , such that  $\tau_2 = \tau_1 + \mu$ , or equivalently,

$$T_2^K \cong T_1^K + M.$$

Changing notation, let  $T_1$  be an  $FG$ -module of minimal dimension such that the above holds for some  $FG$ -module  $T_2$ . We need only

show that  $T_1 = 0$ . If not, there exists an irreducible  $FG$ -module  $U$  (with character  $\eta$ ) which is a composition factor of  $T_1$ , and therefore the inner product  $(\tau_1, \eta)$  is positive (see (38.6)). Then also  $(\tau_2, \eta) > 0$ , which implies that  $U$  is also a composition factor of  $T_2$ , since the relation  $(\eta', \eta) = 0$  for distinct irreducible characters  $\eta', \eta$ , is valid even if the representations involved are not absolutely irreducible. We may therefore find  $FG$ -modules  $T_3$  and  $T_4$  such that

$$T_1 = U + T_3, \quad T_2 = U + T_4,$$

and we have

$$U^\kappa + T_4^\kappa \cong U^\kappa + T_3^\kappa + M,$$

which implies that  $T_4^\kappa \cong T_3^\kappa + M$ . This contradicts the minimality of the dimension of  $T_1$ , and thus we must have  $T_1 = 0$ . The proof is complete.

### § 41B. A theorem of Frobenius

Let  $G$  be a finite group of order  $g$  with irreducible characters  $\zeta^{(1)}, \dots, \zeta^{(s)}$  in the complex field. Let  $\epsilon$  be a primitive  $g$ th root of 1 over  $Q$ , and let  $R = \text{alg. int. } \{Q(\epsilon)\}$ . Define  $\text{char}_R(G)$ , the ring of generalized characters on  $G$  with coefficients in  $R$ , by

$$\text{char}_R(G) = \sum_{i=1}^s R\zeta^{(i)}.$$

Let us fix a positive integer  $n$  for the remainder of the section. If  $\mathfrak{C}$  denotes a conjugate class of  $G$  containing  $c$  elements, we define a mapping  $\theta_{\mathfrak{C}, \epsilon}: G \rightarrow Z$  by means of

$$(41.7) \quad \theta_{\mathfrak{C}, \epsilon}(x) = \begin{cases} g/(g, cn), & x^n \in \mathfrak{C}, \\ 0, & x^n \notin \mathfrak{C}. \end{cases}$$

The aim of this section is to present a proof by Brauer [24] of the following theorem of Frobenius [4].

(41.8) THEOREM.  $\theta_{\mathfrak{C}, \epsilon} \in \text{char}_R(G)$ .

Before proceeding with the proof, we give several corollaries to emphasize the importance of the result.

(41.9) COROLLARY. For  $\psi \in \text{char}(G)$  we have

$$(41.10) \quad (g, cn)^{-1} \sum_{x^n \in \mathfrak{C}} \psi(x) \in R.$$

[Throughout this section,  $(a, b)$  denotes the greatest common divisor

of the integers  $a$  and  $b$ , whereas  $(\theta, \eta)$  denotes the inner product of the characters  $\theta, \eta$ .]

PROOF. For each such  $\psi$ , Theorem 41.8 implies that  $(\psi, \theta_{\mathfrak{C}, a}) \in R$ . However,

$$\begin{aligned} (\psi, \theta_{\mathfrak{C}, a}) &= g^{-1} \sum \psi(x) \overline{\theta_{\mathfrak{C}, a}(x)} \\ &= (g, cn)^{-1} \sum_{x^n \in \mathfrak{C}} \psi(x). \end{aligned}$$

(41.11) COROLLARY. *The number of elements  $x \in G$  for which  $x^n \in \mathfrak{C}$  is a multiple of  $(g, cn)$ . In particular, the number of solutions of  $x^n = 1, x \in G$ , is a multiple of  $(g, n)$ .*

PROOF. Take  $\psi$  to be the principal character in the preceding corollary.

*Remark.* It should be pointed out that Corollary 41.11 can be proved without the use of group characters (see M. Hall [2], Th. 9.1.1). We also remark that Corollary 41.9 implies Theorem 41.8. Solomon [3] gives a simple proof of (41.9) for the special case where  $\mathfrak{C}=\{1\}$ .

Let us begin the proof of Theorem 41.8 by making three observations about the function  $\theta_{\mathfrak{C}, a}$ .

(i). Let  $G = G_1 \times G_2$  be a direct product, and set  $g_i = [G_i : 1]$ . Each class  $\mathfrak{C}$  of  $G$  is a product  $\mathfrak{C}_1 \mathfrak{C}_2$  of a class  $\mathfrak{C}_1$  of  $G_1$  and a class  $\mathfrak{C}_2$  of  $G_2$ . If  $\mathfrak{C}_i$  contains  $c_i$  elements ( $i = 1, 2$ ), then  $\mathfrak{C}$  contains  $c_1 c_2$  elements. Suppose now that  $(g_1, g_2) = 1$ ; then we have

$$(g, c_1 c_2 n) = (g_1, c_1 n)(g_2, c_2 n),$$

and therefore

$$\theta_{\mathfrak{C}, a}(x_1 x_2) = \theta_{\mathfrak{C}_1, a_1}(x_1) \cdot \theta_{\mathfrak{C}_2, a_2}(x_2), \quad x_i \in G_i.$$

If we know further that

$$\theta_{\mathfrak{C}_i, a_i} \in \text{char}_R(G_i), \quad i = 1, 2,$$

then the remarks in Exercise 27.2 show that  $\theta_{\mathfrak{C}, a} \in \text{char}_R(G)$ .

(ii). Let  $\mathfrak{C}$  be a conjugate class in  $G$  containing  $c$  elements, and let  $H$  be a subgroup of  $G$  of order  $h$ . Clearly,  $\mathfrak{C} \cap H$  is made up of conjugate classes of  $H$ , say,

$$\mathfrak{C} \cap H = \mathfrak{C}'_1 \cup \dots \cup \mathfrak{C}'_k.$$

If  $\mathfrak{C}'_i$  contains  $c'_i$  elements, it is easily verified that

$$\frac{g}{(g, nc)} = u_i \cdot \frac{h}{(h, nc'_i)}$$

for some  $u_i \in Z$ . Therefore for  $y \in H$  we have

$$\theta_{\mathfrak{C}, \sigma}(y) = \sum_{i=1}^k u_i \theta_{\mathfrak{C}_i, H}(y).$$

This shows that

$$\theta_{\mathfrak{C}, \sigma} | H = \sum_{i=1}^k u_i \theta_{\mathfrak{C}_i, H}.$$

If it is known that  $\theta_{\mathfrak{C}', H} \in \text{char}_R(H)$  for each class  $\mathfrak{C}'$  of  $H$ , the above shows that  $\theta_{\mathfrak{C}, \sigma} | H \in \text{char}_R(H)$  for each class  $\mathfrak{C}$  of  $G$ .

(iii). Let  $\mathfrak{C}_1 = \{1\}$ ,  $\mathfrak{C}_2, \dots, \mathfrak{C}_s$  be the classes of  $G$ , and let  $\mathfrak{C}_i$  contain  $c_i$  elements. For each  $i$ ,  $1 \leq i \leq s$ , there exists an  $r_i \in \mathbb{Z}$  such that

$$(g, c_i n) = r_i(g, n),$$

and in particular  $r_1 = 1$ . Therefore

$$(41.12) \quad \theta_{\mathfrak{C}_1, \sigma} + \sum_{i=2}^s r_i \theta_{\mathfrak{C}_i, \sigma} = \frac{g}{(g, n)} \zeta^{(1)},$$

where  $\zeta^{(1)}$  is the character of the 1-representation of  $G$ . The right-hand side of (41.12) certainly lies in  $\text{char}_R(G)$ . Hence, if it can be shown that  $\theta_{\mathfrak{C}, \sigma} \in \text{char}_R(G)$  for each class  $\mathfrak{C} \neq \{1\}$ , it will follow from (41.12) that also  $\theta_{\mathfrak{C}_1, \sigma} \in \text{char}_R(G)$ .

Suppose now that Theorem 41.8 has been established for every elementary subgroup  $H$  of  $G$ . From (ii) it would then follow that

$$\theta_{\mathfrak{C}, \sigma} | H \in \text{char}_R(H)$$

for each class  $\mathfrak{C}$  of  $G$ . Since this holds for every elementary subgroup of  $G$ , Corollary 40.9 implies that  $\theta_{\mathfrak{C}, \sigma} \in \text{char}_R(G)$ . For the remainder of the proof we may therefore restrict our attention to elementary subgroups.

Next we note that every elementary subgroup is a direct product of  $p$ -groups for various primes  $p$ . By virtue of (i), it therefore suffices to prove Theorem 41.8 for  $p$ -groups. Finally, (iii) shows that we may restrict ourselves to classes different from  $\{1\}$ . We must prove that, if  $G$  is any  $p$ -group and  $\mathfrak{C}$  a class of  $G$  different from  $\{1\}$ , then  $\theta_{\mathfrak{C}, \sigma} \in \text{char}_R(G)$ . By Exercise 40.3, this is equivalent to showing that for each linear character  $\lambda$  on each subgroup  $H$  of  $G$ , we have

$$(41.13) \quad (\theta_{\mathfrak{C}, \sigma} | H, \lambda) \in R.$$

Let  $H$  be a subgroup of  $G$ , and set

$$(41.14) \quad g = [G : 1] = p^a, \quad h = [H : 1] = p^b, \quad n = p^a n_0, \quad p \nmid n_0.$$

Let  $\lambda$  be any linear character on  $H$ , and denote  $\theta_{\mathfrak{C}, \mathfrak{G}}$  briefly by  $\theta$ . Then by definition

$$(41.15) \quad (\theta | H, \lambda) = h^{-1} \sum_{y \in H} \theta(y) \lambda(y^{-1})$$

where  $\theta$  is given by (41.7). Therefore

$$(\theta | H, \lambda) = h^{-1} \cdot \frac{g}{(g, nc)} \sum_{\substack{y \in H \\ y^n \in \mathfrak{C}}} \lambda(y^{-1}).$$

Write  $\mathfrak{C} \cap H$  as a union of conjugate classes of  $H$ , say,

$$\mathfrak{C} \cap H = \mathfrak{C}'_1 \cup \dots \cup \mathfrak{C}'_k.$$

Then

$$(\theta | H, \lambda) = \frac{h^{-1}g}{(g, nc)} \sum_{i=1}^k \sum_{\substack{y \in H \\ y^n \in \mathfrak{C}'_i}} \lambda(y^{-1}).$$

It therefore suffices to show for each class  $\mathfrak{C}'$  in  $H$  different from  $\{1\}$  that

$$(41.16) \quad \frac{g}{h(g, nc)} \sum_{\substack{y \in H \\ y^n \in \mathfrak{C}'}} \lambda(y^{-1})$$

lies in  $R$ .

Now let  $y \in H$  be such that  $y^n \in \mathfrak{C}'$ , and let  $p^e = \text{order of } y$ . Since  $\mathfrak{C}' \neq \{1\}$  we have  $e > d$ , where  $d$  is given by (41.14). Let  $z$  be an element of the cyclic group  $[y]$  for which  $z^n = y^n$ . Setting  $z = y^r$ , we obtain  $y^{nr} = y^n$ , whence

$$nr \equiv n \pmod{p^e}$$

or

$$r \equiv 1 \pmod{p^{e-d}}.$$

Thus  $p \nmid r$ , and so  $[z] = [y]$ . Hence the elements  $y \in H$  such that  $y^n \in \mathfrak{C}'$  may be partitioned into disjoint sets  $A(y)$ , with two such elements  $y, z$  placed in the same set if and only if  $[y] = [z]$  and  $y^n = z^n$ . Further, the set  $A(y)$  containing  $y$  consists precisely of the distinct elements

$$y^{1+t \cdot p^{e-d}}, \quad 0 \leq t \leq p^d - 1.$$

Let the elements of  $\mathfrak{C}'$  be given by

$$u_1^{-1}vu_1, \dots, u_m^{-1}vu_m,$$

where  $v, u_1, \dots, u_m \in H$  and  $u_1 = 1$ . For fixed  $y \in H$  such that  $y^n = v$ , the sets

$$(41.17) \quad A(u_1^{-1}yu_1), \dots, A(u_m^{-1}yu_m)$$

are disjoint. Further, if  $y$  and  $\bar{y}$  are elements in  $H$  for which  $y^n = \bar{y}^n = v$ , the sets

$$A(u_1^{-1}\bar{y}u_1), \dots, A(u_m^{-1}\bar{y}u_m)$$

either coincide with those in (41.17) or are disjoint from them. Hence the expression in (41.16) is a sum of expressions of the form

$$(41.18) \quad \frac{g}{h(g, nc)} \sum_{i=1}^m \sum_{t=0}^{p^d-1} \lambda(u_i^{-1}y^{-(1+t \cdot p^e-d)}u_i).$$

But  $\lambda$  is a linear character, and, if we set

$$\omega = \lambda(y^{p^e-d}),$$

the expression in (41.18) becomes

$$(41.19) \quad \frac{g m \lambda(y^{-1})}{h(g, nc)} \sum_{t=0}^{p^d-1} \bar{\omega}^t.$$

Since  $y$  has order  $p^e$ , we see that  $\omega$  is a  $p^d$ th root of 1, and consequently

$$\sum_{t=0}^{p^d-1} \bar{\omega}^t = \begin{cases} p^d, & \bar{\omega} = 1 \\ 0, & \bar{\omega} \neq 1. \end{cases}$$

Therefore, the expression in (41.19) is either 0 or equals

$$(41.20) \quad \frac{g m \lambda(y^{-1}) p^d}{h(g, nc)}.$$

Let  $r$  be the order of the centralizer of  $v$  in  $G$  and  $\delta$  the order of the centralizer of  $v$  in  $H$ . Then  $\delta \mid r$ , and furthermore  $c = g/r$ ,  $m = h/\delta$ . Substituting into (41.20), we obtain

$$\frac{c r m \lambda(y^{-1}) p^d}{m \delta(c r, nc)} = r \delta^{-1} \cdot \lambda(y^{-1}) \cdot \frac{p^d}{(r, n)}.$$

However,  $r$  is a power of  $p$ , and so  $(r, n) = (r, p^d) \mid p^d$ . Therefore the above expression lies in  $R$ , whence so does the expression in (41.16), and the proof of Theorem 41.8 is completed.

(41.21) COROLLARY.  $\theta_{\{1\}, G} \in \text{char}(G)$ .

PROOF. For brevity, denote  $\theta_{\{1\}, G}$  by  $\theta$ . By Theorem 41.8, we may write

$$\theta = \sum_{i=1}^s a_i \zeta^{(i)}, \quad a_i \in R.$$

From the orthogonality relations we have

$$a_i = (\theta, \zeta^{(i)}) = g^{-1} \sum_{x \in G} \theta(x) \zeta^{(i)}(x^{-1}).$$

If  $\tau$  is any element of the Galois group of  $Q(\epsilon)$  over  $Q$ , then  $\tau$  is given by  $\epsilon \rightarrow \epsilon^t$  for some integer  $t$  relatively prime to  $g$ . Consequently,

$$\tau: \zeta^{(i)}(x^{-1}) \rightarrow \zeta^{(i)}(x^{-t}),$$

and so  $\tau$  maps  $a_i$  onto

$$g^{-1} \sum_{x \in G} \theta(x) \zeta^{(i)}(x^{-t}).$$

However,  $x^n \in \{1\}$  if and only if  $(x^t)^n \in \{1\}$ , and so  $\theta(x) = \theta(x^t)$ . Therefore

$$\tau(a_i) = g^{-1} \sum_{x \in G} \theta(x^t) \zeta^{(i)}(x^{-t}).$$

But as  $x$  ranges over all elements of  $G$ , so does  $x^t$ , and thus  $\tau(a_i) = a_i$ . We have thus shown that  $a_i$  is invariant under all elements of the Galois group of  $Q(\epsilon)$  over  $Q$ , and so  $a_i \in Q \cap R = Z$ . Therefore  $\theta \in \text{char}(G)$ .

We shall now state (without proof) an interesting generalization of Theorem 41.8 due to P. Hall [1]. Before proceeding to the statement of Hall's theorem let us first give a modified version of Corollary 41.9. Let  $a$  be some fixed element of  $\mathbb{C}$ , and let  $d$  be the order of the centralizer of  $a$  in  $G$ . Then  $g = cd$ , and  $(g, cn)^{-1} = c^{-1}(d, n)^{-1}$ . On the other hand,

$$\sum_{z^n \in \mathbb{C}} \psi(x) = c \sum_{z^n=a} \psi(x).$$

Therefore, Corollary 41.9 implies<sup>†</sup>

(41.22) COROLLARY. *For fixed  $a \in G$  and any  $\psi \in \text{char}(G)$ , we have*

$$(n, d)^{-1} \sum_{z^n=a} \psi(x) \in R,$$

where  $d$  is the order of the centralizer of  $a$ .

Hall's generalization is as follows: Let  $a_1, \dots, a_r$  be fixed elements of  $G$ , and let  $f(x; a_1, \dots, a_r)$  denote a word in the single variable  $x$  and in the elements  $a_1, \dots, a_r$ . Let  $S(f)$  be the sum of

<sup>†</sup> Note that Corollary 41.22 is equivalent to Theorem 41.8.

the exponents to which  $x$  occurs in  $f$ . We may now state

(41.23) THEOREM (P. Hall [1]). *Let  $a_1, \dots, a_r \in G$  be fixed, and let  $d$  be the order of the centralizer of  $\{a_1, \dots, a_r\}$  in  $G$ ; that is,  $d = \text{order of } \{x \in G : xa_1 = a_1x, \dots, xa_r = a_rx\}$ . Let  $f_i(x; a_1, \dots, a_r)$ ,  $1 \leq i \leq k$ , be words in  $x, a_1, \dots, a_r$ , and suppose*

$$n \mid S(f_i), \quad 1 \leq i \leq k.$$

*Define*

$$A = \{x \in G : f_i(x; a_1, \dots, a_r) = 1, 1 \leq i \leq k\}.$$

*Then for each  $\phi \in \text{char}(G)$  we have*

$$(n, d)^{-1} \sum_{x \in A} \phi(x) \in R.$$

We shall not give the proof of this theorem here since it involves detailed considerations of  $p$ -groups and is essentially group-theoretic in nature. Also see Sehgal [1].

### Exercises

1. Let  $H$  be a subgroup of  $G$ , and let  $\mathfrak{C}' \subset \mathfrak{C}$  where  $\mathfrak{C}'$  is a conjugate class of  $H$  containing  $c'$  elements, and  $\mathfrak{C}$  is a conjugate class of  $G$  containing  $c$  elements. If  $g = [G : 1]$  and  $h = [H : 1]$ , show that there exists an integer  $u \in \mathbb{Z}$  such that

$$\frac{g}{(g, nc)} = u \cdot \frac{h}{(h, nc')}$$

where  $n$  is some fixed positive integer.

2. Let  $S$  be the union of a collection of conjugate classes in  $G$ , and set  $g = [G : 1]$ . Let  $n$  be a fixed positive integer, and define

$$\theta(x) = \begin{cases} g/(g, n), & x^n \in S \\ 0, & x^n \notin S \end{cases}$$

Using Theorem 41.8, prove that  $\theta \in \text{char}_R(G)$ .

## § 42. The Generalized Induction Theorem

We shall present here a generalization of Brauer's theorem 40.1 on induced characters to the case where the underlying field  $K$  is an arbitrary subfield of the complex field. By making use of Roquette's simplification [1] of the proof of Brauer's theorem, Witt [2] and Berman [8] independently obtained the generalized result.

A much simpler proof of the Witt-Berman theorem was given by Solomon [1], [2] along the lines of the Brauer-Tate proof of Theorem 40.1 presented in § 40. The special case of the Witt-Berman theorem in which  $K = Q$  was independently proved by Swan [1], [2], [4]. (In connection with induction theorems see also Asana [1].)

In order to state the Witt-Berman theorem, we shall introduce some notation and definitions to be used throughout this section. We let  $\Omega$  denote the complex field. For  $m$  a positive integer, let  $\epsilon_m$  denote a primitive  $m$ th root of unity over  $K$ , where  $K$  is a subfield of  $\Omega$ . Then  $K(\epsilon_m)$  is a finite normal extension of  $K$ , and each automorphism of  $K(\epsilon_m)$  which leaves each element of  $K$  fixed is given by a map

$$(42.1) \quad \epsilon_m \rightarrow \epsilon_m^r,$$

where  $r$  is some integer relatively prime to  $m$ . We shall write  $I_m = I_m(K)$  for the multiplicative group consisting of those integers  $r$ , taken modulo  $m$ , for which (42.1) defines an automorphism of  $K(\epsilon_m)$  over  $K$ . Thus  $I_m$  is just the Galois group of  $K(\epsilon_m)$  over  $K$  and is of course abelian. For example,  $I_m(\Omega) = \{1\}$ , whereas  $I_m(Q)$  consists of all the residue classes (mod  $m$ ) which are relatively prime to  $m$ .

Let  $G$  be some finite group, fixed throughout the discussion, and suppose  $G$  has exponent  $n$ . For convenience we write  $\epsilon$  for  $\epsilon_n$  and  $I$  for  $I_n$ . Finally, we set  $R = \text{alg. int. } \{K(\epsilon)\}$ .

(42.2) **DEFINITION.** Let  $p$  be a prime, and let  $H$  be a subgroup of  $G$ . We call  $H$  a  *$K$ -elementary subgroup of  $G$  at  $p$*  if

(i)  $H$  is a semi-direct product  $[a]B$  of a  $p$ -group  $B$  and a cyclic group  $[a]$  whose order  $m$  is not a multiple of  $p$ , and

(ii) For each  $b \in B$  there exists an  $r \in I_m(K)$  such that  $bab^{-1} = a^r$ . (Thus the  $\Omega$ -elementary subgroups of  $G$  are precisely the elementary subgroups of § 40. The  $Q$ -elementary subgroups are usually called *hyper-elementary* subgroups.)

By a  *$K$ -character* of  $G$  we mean the character afforded by a  $KG$ -module. The principal result of this section is

(42.3) **THEOREM** (Witt [2], Berman [8]). *Every  $K$ -character of  $G$  is a  $Z$ -linear combination  $\sum a_i \psi_i^g$ ,  $a_i \in Z$ , where the  $\{\psi_i\}$  are  $K$ -characters of  $K$ -elementary subgroups of  $G$ .*

We begin the proof with several straightforward lemmas.

(42.4) **LEMMA.** *Let  $\phi$  be a  $K$ -character of  $G$ , and let  $a \in G$  have order  $m$ . Then*

$$\phi(a) = \phi(a^r), \quad r \in I_m,$$

and this equality holds also for all  $r \in I$ .

**PROOF.** [Compare Lemma 39.4.] The character value  $\phi(a)$  is the sum of the characteristic roots of a matrix whose  $m$ th power is the identity, and so we may write

$$\phi(a) = \varepsilon_m^{u_1} + \cdots + \varepsilon_m^{u_t}, \quad \phi(a^r) = \varepsilon_m^{ru_1} + \cdots + \varepsilon_m^{ru_t}.$$

If  $r \in I_m$ , then  $\varepsilon_m \rightarrow \varepsilon_m^r$  is an automorphism of  $K(\varepsilon_m)$  over  $K$  which carries  $\phi(a)$  into  $\phi(a^r)$ . But  $\phi(a) \in K$  since  $\phi$  is a  $K$ -character, and therefore  $\phi(a) = \phi(a^r)$ .

Finally if  $r \in I$  then  $\varepsilon \rightarrow \varepsilon^r$  gives an automorphism of  $K(\varepsilon)$  over  $K$  which upon restriction to  $K(\varepsilon_m)$  yields an automorphism  $\tau$  of  $K(\varepsilon_m)$  over  $K$ . Since  $\varepsilon_m$  is a power of  $\varepsilon$ , we have  $\tau(\varepsilon_m) = \varepsilon_m^r$ , and so  $r \pmod{m}$  lies in  $I_m$ . This completes the proof.

We next determine all irreducible  $KA$ -modules, where  $A = [a]$  is a cyclic group of order  $m$ . We have

$$KA = K[a] \cong K[u]/(u^m - 1),$$

where  $K[u]$  is the polynomial domain over  $K$  in an indeterminate  $u$ , and  $(u^m - 1)$  is the principal ideal generated by  $u^m - 1$ . If

$$u^m - 1 = f_1(u) \cdots f_s(u)$$

is the factorization of  $u^m - 1$  into (necessarily distinct) irreducible non-constant monic polynomials in  $K[u]$ , by the Chinese remainder theorem (applied to the principal ideal ring  $K[u]$ ) we have

$$K[u]/(u^m - 1) \cong \sum_{i=1}^s K[u]/(f_i(u)),$$

a direct sum of fields. This shows that there exactly  $s$  non-isomorphic irreducible  $KA$ -modules, say  $M_1, \dots, M_s$ , with

$$M_j = K[u]/(f_j(u)), \quad 1 \leq j \leq s,$$

the action of  $a$  on  $M_j$  being given by a left multiplication by  $u$ . Let  $d_j = \deg(f_j(u))$ ; the residue classes containing  $1, u, \dots, u^{d_j-1}$  form a  $K$ -basis of  $M_j$ , and relative to this basis the generator  $a$  of  $A$  maps onto the matrix

$$\begin{pmatrix} 0 & 0 & \cdots & 0 & -\alpha_0 \\ 1 & 0 & \cdots & 0 & -\alpha_1 \\ 0 & 1 & \cdots & 0 & -\alpha_2 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & -\alpha_{d_j-1} \end{pmatrix}$$

where

$$f_j(u) = \sum_{i=0}^{d_j} \alpha_i u^i, \quad \alpha_i \in K, \quad \alpha_{d_j} = 1.$$

Thus if  $\mu_j$  is the character afforded by  $M_j$  we have

$$\mu_j(a) = \text{sum of the zeros of } f_j(u),$$

and in general  $\mu_j(a^l)$  is the sum of the  $l$ th powers of the zeros of  $f_j(u)$ .

It will be convenient to introduce the full set  $\omega_0, \dots, \omega_{m-1}$  of irreducible complex characters of  $A$ . These are given by

$$\omega_i(a^l) = \epsilon_m^{il}, \quad 0 \leq l \leq m-1, \quad 0 \leq i \leq m-1.$$

Any automorphism of  $K(\epsilon_m)$  over  $K$  permutes the  $\{\omega_i\}$  among themselves, carrying each  $\omega_i$  onto a  $K$ -conjugate character  $\omega'_i$ . Let  $\epsilon_m^{e(j)}$  denote a fixed zero of  $f_j(u)$ ; then the zeros of  $f_j(u)$  are just the distinct conjugates of  $\epsilon_m^{e(j)}$  over  $K$ . This shows that  $\mu_j$  is the sum of the distinct conjugates of the character  $\omega_{e(j)}$ .

We make use of the above discussion in proving

(42.5) LEMMA. *Let  $H = [a]B$  be a semi-direct product of a cyclic group  $[a]$  of order  $m$  and some group  $B$ . Suppose that for each  $b \in B$  we have*

$$bab^{-1} = a^r$$

*for some  $r \in I_m$ . Then there exists a function  $\eta$  on  $H$  which is a linear combination of  $K$ -characters of  $H$  with coefficients in alg. int.  $\{Q(\epsilon_m)\}$ , and which satisfies*

$$(42.6) \quad \eta(a^i) = \begin{cases} m, & i \in I_m \\ 0, & i \notin I_m. \end{cases}$$

PROOF. Define a function  $\xi$  on  $[a]$  by replacing  $\eta$  by  $\xi$  in (42.6). Since  $\xi$  is a class function on  $[a]$ , we may write

$$(42.7) \quad \xi = \sum_{i=0}^{m-1} c_i \omega_i, \quad c_i \in \Omega.$$

The orthogonality relations connecting the  $\{\omega_i\}$  imply that

$$c_i = m^{-1} \sum_{j=0}^{m-1} \overline{\xi(a^j)} \overline{\omega_i(a^j)} = \sum_{j \in I_m} \overline{\omega_i(a^j)},$$

where bars denote complex conjugates. This shows that each

$c_i \in \text{alg. int. } \{Q(\epsilon_m)\}$ ; in fact, since  $c_i$  is a sum of  $K$ -conjugate elements, we also have  $c_i \in K$  for each  $i$ .

Now apply to both sides of (42.7) an automorphism of  $K(\epsilon_m)$  over  $K$ . Each such automorphism leaves  $\xi$  and each  $c_i$  unchanged but maps the  $\{\omega_i\}$  onto their conjugates over  $K$ . Thus  $K$ -conjugate characters occur with the same coefficients in (42.7), which proves that

$$\xi = \sum_{j=1}^r c_{\epsilon(j)} \mu_j.$$

To complete the proof of the lemma we need only show that each  $\mu_j$  is the restriction to  $[a]$  of some  $K$ -character of  $H$ , or in other words, that each  $K[a]$ -module  $M_j$  can be made into a  $KH$ -module in such a way as to preserve the action of the elements of  $[a]$ . For each  $b \in B$ , the map  $a \rightarrow bab^{-1}$  gives an automorphism  $\phi_b$  of  $[a]$ , and clearly  $\phi_{bb'} = \phi_b \phi_{b'}$ . We now turn  $K[a]$  into a left  $KH$ -module by defining

$$(xb) \cdot y = x\phi_b(y), \quad x, y \in [a], b \in B,$$

and extending the action of  $H$  to all  $K[a]$  by linearity. Let us check that  $K[a]$  does indeed become a left  $KH$ -module; for this it suffices to verify that

$$(x'b') \{(xb)y\} = \{(x'b')(xb)\}y, \quad x, x', y \in [a], b, b' \in B,$$

and this follows readily from the fact that

$$b'x = \{\psi_{b'}x\}b'.$$

Note that the action of  $H$  extends that of  $[a]$  on  $K[a]$ .

Finally we shall prove that, with the above action of  $H$  on  $K[a]$ , each  $M_j$  becomes a  $KH$ -module. As left  $K[a]$ -modules we have

$$K[a] \cong M_1 \oplus \cdots \oplus M_s,$$

and this is also a ring isomorphism. The map  $y \rightarrow b \cdot y$ ,  $y \in K[a]$ , is a ring automorphism of  $K[a]$  and hence permutes the simple components  $\{M_i\}$  among themselves. Suppose this map carries  $M_i$  onto  $M_j$ . Then  $M_j = bM_i$ , and the mapping  $m \rightarrow bm$ ,  $m \in M_i$ , is a  $K$ -isomorphism  $\theta : M_i \cong M_j$ . For each  $x \in [a]$ , we have

$$x \cdot \theta(m) = xbm = b \cdot b^{-1} xbm = \theta(\phi_{b^{-1}}(x)m), \quad m \in M_i.$$

If  $\{m_\nu\}$  is a  $K$ -basis of  $M_i$  and if we write

$$\phi_{b^{-1}}(x)m_\nu = \sum_\lambda \alpha_{\lambda\nu} m_\lambda, \quad \alpha_{\lambda\nu} \in K,$$

then applying  $\theta$  to both sides and using the previous relation, we obtain

$$x \cdot \theta(m_\nu) = \sum \alpha_{\lambda\nu} \theta(m_\lambda).$$

In other words, if relative to the basis  $\{m_\nu\}$  the module  $M_i$  affords the matrix representation  $T_i$  of  $[a]$ , then, relative to the basis  $\{\theta(m_\nu)\}$  the module  $M_j$  affords a matrix representation  $T_j$  given by

$$T_j(x) = T_i(\phi_{b^{-1}}(x)), \quad x \in [a].$$

Taking traces we obtain

$$\mu_j(x) = \mu_i(\phi_{b^{-1}}(x)), \quad x \in [a].$$

But  $\phi_{b^{-1}}(x) = x^r$  for some  $r \in I_m$ , and so by Lemma 42.4 we have

$$\mu_i(\phi_{b^{-1}}(x)) = \mu_i(x), \quad x \in [a].$$

Therefore  $\mu_i = \mu_j$  whence  $i = j$ . This shows that each  $M_i$  is a  $KH$ -module and completes the proof of the lemma.

Again let  $G$  be a finite group of exponent  $n$ , and keep the notation introduced earlier in this section, so that  $\epsilon$  is a primitive  $n$ th root of 1 over  $K$ , and  $I \cong$  Galois group of  $K(\epsilon)$  over  $K$ . Two elements  $a, b \in G$  are called  $K$ -conjugate (notation:  $a \sim_K b$ ) if

$$x^{-1}bx = a^r$$

for some  $x \in G$  and some  $r \in I$ . It is easily seen that  $K$ -conjugacy is an equivalence relation, and so  $G$  may be partitioned into  $K$ -conjugate classes. Note that elements in the same  $K$ -conjugate class have the same order.

Detouring slightly from the proof of the Witt-Berman induction theorem, we now establish the following remarkable result:

(42.8) THEOREM (Berman [8], Witt [2]). *The number  $w = w(KG)$  of non-isomorphic irreducible  $KG$ -modules is the same as the number of  $K$ -conjugate classes in  $G$ .*

*Remark.* For the special case in which  $K = Q(\epsilon)$ , we see that  $a \sim_K b$  if and only if  $a$  and  $b$  are conjugate in the usual sense. On the other hand, when  $K = Q$  we observe that  $a \sim_K b$  if and only if the cyclic groups  $[a]$  and  $[b]$  are conjugate in  $G$ . Thus the above theorem includes as special cases both Theorems (27.22) and (39.5).

PROOF. By (42.4), any  $K$ -character  $\chi$  is constant on each  $K$ -

conjugate class of  $G$ . If  $a_1, \dots, a_t$  denote a full set of representatives of these  $K$ -conjugate classes, then  $\chi$  is uniquely determined by the  $t$ -tuple

$$(\chi(a_1), \dots, \chi(a_t)).$$

The distinct irreducible  $K$ -characters of  $G$  are linearly independent over  $K$  by Theorem 30.12, and so the number of them cannot exceed  $t$ . This proves that  $w \leq t$ .

To prove the reverse inequality, we first construct for each  $i$ ,  $1 \leq i \leq t$ , a function  $\xi_i$  defined on  $[a_i]$ , satisfying

$$\xi_i(a_i^l) = \begin{cases} m_i, & l \in I_{m_i} \\ 0, & l \notin I_{m_i} \end{cases}$$

where  $m_i$  is the order of  $a_i$ . We have shown that each  $\xi_i$  is an  $R$ -linear combination of  $K$ -characters of  $[a_i]$ , and thus each induced character  $\xi_i^G$  is an  $R$ -linear combination of  $K$ -characters of  $G$ . If we can show that the characters  $\xi_1^G, \dots, \xi_t^G$  are linearly independent over  $K$ , we may then conclude that  $t \leq w$ , and the theorem will have been established.

Now we have

$$\xi_i^G(a_i) = m_i^{-1} \sum_{x \in G} \xi_i(x^{-1}a_i x),$$

where as usual  $\xi_i$  coincides with  $\xi_i$  on  $[a_i]$  and vanishes outside  $[a_i]$ . Each term in the above sum is a non-negative rational integer, and the term coming from  $x = 1$  is positive so that  $\xi_i^G(a_i) \neq 0$ . On the other hand,  $\xi_i^G(a_j) \neq 0$  implies that

$$a_j = x a_i^r x^{-1}$$

for some  $x \in G$  and some  $r \in I_{m_i}$ . The automorphism  $\varepsilon_{m_i} \rightarrow \varepsilon_{m_i}^r$  of  $K(\varepsilon_{m_i})$  over  $K$  can be extended to an automorphism  $\varepsilon \rightarrow \varepsilon^q$  of  $K(\varepsilon)$  over  $K$ . Since  $\varepsilon_{m_i}$  is a power of  $\varepsilon$ , this gives

$$\varepsilon_{m_i}^r = \varepsilon_{m_i}^q,$$

whence also

$$a_i^r = a_i^q.$$

Therefore

$$a_j = x a_i^q x^{-1}, \quad q \in I,$$

so that  $a_j \sim_K a_i$ . This shows that  $\xi_i^G$  vanishes on the elements of  $G$  which are not  $K$ -conjugates of  $a_i$ , and so the theorem is proved.

We are now ready to complete the proof of the Witt-Berman induction theorem. Let  $\text{char}_R(KG)$  be the ring of  $R$ -linear combinations of the  $K$ -characters of  $G$ , and set

$$v_R(KG) = \sum_H \{\text{char}_R(KH)\}^g,$$

where  $H$  ranges over all  $K$ -elementary subgroups of  $G$  at the various primes dividing  $[G : 1]$ . Define  $v_Z$  and  $\text{char}_Z$  analogously, replacing  $R$  by  $Z$ . As in § 40, we find that  $v_Z(KG)$  is an ideal in the ring  $\text{char}_Z(KG)$ , and we are trying to prove that  $v_Z(KG) = \text{char}_Z(KG)$ . The argument preceding Lemma 40.6 shows that it suffices to prove the 1-character  $\zeta^{(1)}$  of  $G$  lies in  $v_R(KG)$ , for then also  $\zeta^{(1)} \in v_Z(KG)$ .

(42.9) LEMMA. *Let  $p$  be a rational prime, and let  $a \in G$  be  $p$ -regular. There exists a function  $\phi = \phi_a \in v_R(KG)$  such that*

- (i)  $\phi(g) = 0$  if  $g$  is  $p$ -regular and is not  $K$ -conjugate to  $a$ ,
- (ii)  $\phi(a) \equiv 1 \pmod{p}$ .

PROOF. Define the  $K$ -normalizer of  $a$  in  $G$  as

$$N = \{x \in G : xax^{-1} = a^r \text{ for some } r \in I_m\}$$

where  $m$  is the order of  $a$ . Then  $N$  is a subgroup of  $G$ , and  $[a] \triangle N$ . If  $B$  is a  $p$ -Sylow subgroup of  $N$ , then  $H = [a]B$  is a  $K$ -elementary subgroup of  $G$  at  $p$ , and furthermore  $[H : 1] = m[B : 1]$ . Construct the function  $\eta$  on  $[a]B$  as in Lemma 42.5; then  $\eta \in \text{char}_R(KH)$ , and so by definition  $\eta^g \in v_R(KG)$ .

Letting  $\dot{\eta}$  coincide with  $\eta$  on  $[a]B$  and vanish outside  $[a]B$ , we have

$$\eta^g(g) = m^{-1}[B : 1]^{-1} \sum_{x \in g} \dot{\eta}(x^{-1}gx).$$

We wish to compute  $\eta^g(g)$  for  $p$ -regular  $g$ , and so we first need to decide which  $p$ -regular elements lie in  $[a]B$ . If  $g \in [a]B$  is  $p$ -regular, its image  $\bar{g}$  in  $[a]B/[a]$  is also  $p$ -regular. But this factor group has order  $[B : 1]$ , hence it is a  $p$ -group, and so we conclude that  $\bar{g} = 1$ , that is,  $g \in [a]$ . We have thus shown that the only  $p$ -regular elements of  $[a]B$  are those which lie in  $[a]$ .

Consequently we have  $\dot{\eta}(x^{-1}gx) = 0$  for  $p$ -regular  $g$  except when  $x^{-1}gx \in [a]$ ; if we write  $x^{-1}gx = a^r$ , then by (42.6) we have  $\dot{\eta}(x^{-1}gx) = 0$  unless  $r \in I_m$ . We have already seen that  $x^{-1}gx = a^r$  for some  $r \in I_m$  if and only if  $g$  and  $a$  are  $K$ -conjugate. Thus  $\eta^g$  vanishes on the  $p$ -regular elements of  $G$  which are not  $K$ -conjugates of  $a$ .

Finally we compute  $\eta^g(a)$ . As above, we see that  $\dot{\eta}(x^{-1}ax) = 0$

except when  $x^{-1}ax = a^r$ ,  $r \in I_m$ , that is, except when  $x \in N$ . Therefore

$$\eta^g(a) = m^{-1}[B : 1] \cdot \sum_{z \in N} m = [N : B],$$

and thus  $p \nmid \eta^g(a)$ . Choose an integer  $z \in Z$  such that  $z[N : B] \equiv 1 \pmod{p}$ , and set  $\phi = z\eta^g$ , thereby obtaining the desired function  $\phi$ .

We have denoted by  $R$  the ring of all algebraic integers in  $K(\epsilon)$ , where  $\epsilon$  is a primitive  $n$ th root of 1, and  $n$  is the exponent of  $G$ . Let  $p$  be some fixed prime divisor of  $n$ , and let  $P$  be any prime ideal of  $R$  which contains  $p$ . In the latter part of the proof of Lemma 40.7, we showed that if  $\chi$  is any  $K$ -character of  $G$ , or in fact if  $\chi \in \text{char}_R(KG)$ , then

$$\chi(g) \equiv \chi(g_1) \pmod{P},$$

where  $g_1$  is the  $p$ -regular component of  $g$ . We use this to prove

(42.10) LEMMA. *Let  $p$  be a prime divisor of  $n$ . Then there exists a function  $\zeta \in v_R(KG)$  such that*

$$\zeta(g) \equiv 1 \pmod{P}$$

for all  $g \in G$ .

PROOF. From each  $K$ -conjugate class of  $p$ -regular elements of  $G$  pick one representative, and let  $\{a_1, \dots, a_l\}$  be the set of elements thus obtained. Then  $a_i$  and  $a_j$  are not  $K$ -conjugate for  $i \neq j$ , and, further, the  $p$ -regular component of any element of  $G$  is  $K$ -conjugate to some  $a_i$ . For each  $i$ ,  $1 \leq i \leq l$ , we may find [by Lemma 42.9] a function  $\phi_i \in v_R(KG)$  such that

$$\begin{aligned} \phi_i(a_i) &\equiv 1 \pmod{P} \\ \phi_i(a_j) &= 0, \quad j \neq i. \end{aligned}$$

Set  $\zeta = \phi_1 + \dots + \phi_l$ , so that

$$\zeta(a_i) \equiv 1 \pmod{P}$$

for all  $i$ . But for any  $g \in G$ , let  $g_1$  be its  $p$ -regular component, and suppose that  $g_1 \sim_K a_i$ . Then

$$\zeta(g) \equiv \zeta(g_1) = \zeta(a_i) \equiv 1 \pmod{P},$$

and the lemma is proved.

By the remarks preceding Lemma 42.9, we see that in order to prove the Witt-Berman theorem we must show that  $\zeta^{(1)} \in v_R(KG)$ .

As in § 40, this will be established if we show that for each  $p$  dividing  $[G : 1]$  we have  $t_p \zeta^{(1)} \in v_R(KG)$ , where  $[G : 1] = p^e t_p$ ,  $p \nmid t_p$ . Letting  $\zeta$  be the function defined in the preceding lemma, we find easily by induction on  $r$  that

$$\{\zeta(g)\}^{p^r} \equiv 1 \pmod{P^r}, \quad g \in G, r = 1, 2, \dots$$

The construction of the function  $\zeta$  is independent of the particular prime ideal divisor  $P$  of  $p$  which we have chosen, and so the above holds for each such  $P$ . Hence for sufficiently large  $r$ , we have

$$\{\zeta(g)\}^{p^r} \equiv 1 \pmod{p^e R}, \quad g \in G.$$

Set  $\psi = t_p(1 - \zeta^{p^r}) \in \text{char}_R(KG)$ . Since we already know that  $t_p \zeta^{p^r} \in v_R(KG)$  [because  $\zeta \in v_R(KG)$ ], we may conclude that also  $t_p \zeta^{(1)} \in v_R(KG)$  once we can show that  $\psi \in v_R(KG)$ . The remainder of the proof is devoted to establishing this fact.

Let  $a_1, \dots, a_t$  be representatives of the  $K$ -conjugate classes of  $G$ . For each  $j$ ,  $1 \leq j \leq t$ , we construct the function  $\xi_j$  defined on  $[a_j]$  as in the proof of Theorem 42.8. Then we know that each  $\xi_j^g \in v_R(KG)$ , and we have shown that  $\xi_j^g$  vanishes on all elements of  $G$  which are not  $K$ -conjugate to  $a_j$ . An easy computation, carried out in the proof of Lemma 42.9 in a slightly more general situation, shows that

$$(42.11) \quad \xi_j^g(a_j) = [N_j : 1],$$

where  $N_j$  is the  $K$ -normalizer of  $a_j$  in  $G$ .

We now claim that

$$(42.12) \quad \psi = \sum_{j=1}^t \frac{\psi(a_j)}{[N_j : 1]} \xi_j^g.$$

Since  $\psi$  and each  $\xi_j^g$  are constant on  $K$ -conjugate classes, it is enough to verify that this holds for each  $a_i$ ; this, in turn, is obvious from formula (42.11). But we also know that

$$\psi(a_j) = t_p(1 - \{\zeta(a_j)\}^{p^r}) \equiv 0 \pmod{[G : 1]R},$$

and so each of the coefficients in the sum on the right-hand side of (42.12) lies in  $R$ . This shows that  $\psi \in v_R(KG)$  and completes the proof of the Witt-Berman theorem.

### Exercises

1. Prove that a class function  $\theta$  on  $G$  lies in the ring  $\text{char}(KG)$  of

generalized  $K$ -characters of  $G$  if and only if  $\theta|H$  is a generalized  $K$ -character of  $H$  for each  $K$ -elementary subgroup  $H$  of  $G$ .

2. (Solomon [1], [2].) A complex character  $\chi$  of  $G$  is said to *lie in  $K$*  if  $\chi(g) \in K$  for all  $g \in G$ . A *generalized character lying in  $K$*  is a sum  $\sum a_i \chi_i$ ,  $a_i \in Z$ ,  $\{\chi_i\}$  characters lying in  $K$ . Let  $\text{char}'(KG)$  be the ring of all generalized characters of  $G$  which lie in  $K$ . Prove that

$$\text{char}'(KG) = \sum_H \{\text{char}'(KH)\}^G,$$

the sum extending over all  $K$ -elementary subgroups  $H$  of  $G$ .

Show also that for  $\theta \in \text{cf}(G)$ , we have  $\theta \in \text{char}'(KG)$  if and only if  $\theta|H \in \text{char}'(KH)$  for every  $K$ -elementary subgroup  $H$  of  $G$ .

This page intentionally left blank

## Induced Representations

The analysis of the  $KG$ -modules of a finite group  $G$  in terms of the  $KH$ -modules, where  $H$  is a subgroup of  $G$ , was begun in Chapter VI. This chapter is concerned with the descriptions of the modules themselves rather than of the characters. Most of the results have not yet found suitable generalizations to rings with minimum condition or finite-dimensional algebras, nor do they work smoothly when the modules involved are not completely reducible.

However, as Frobenius demonstrated, the theory of induced modules provides us with an effective tool for the construction of the irreducible modules for particular groups, and several examples are treated in this chapter to indicate how this is done. The construction of the modules for particular groups will probably remain more of an art than a science, but there are in this chapter a number of helpful ideas. Some of the results on induced modules in the early part of the chapter are due to Mackey [1], although our presentation is based directly on the theory of tensor products of modules (§ 12D) rather than on Frobenius' or Mackey's construction of the induced representations. In the latter part of the chapter the problem is turned around, and we ask whether a given irreducible  $KG$ -module  $M$  can be constructed from  $KH$ -modules or  $K(G/H)$ -modules where  $H$  is a normal subgroup of  $G$  which may depend upon  $M$ . Our approach to this problem is based on a paper by Clifford [1]. The results are applied to show, for example, that all the irreducible representations of a nilpotent group are monomial representations. This result suggests that one should try to determine the kinds of groups whose representations have some special properties. This question seems to be a fruitful one for further investigation. The chapter closes with an introduction to Schur's theory of projective representations based on a paper by Asano and Shoda [1].

### § 43. Induced Representations and Modules

Let  $H$  be a subgroup of a finite group  $G$ , and let  $K$  be an arbitrary field. For a left  $KH$ -module  $L$ , we shall denote by  $L^g$  the left  $KG$ -module

$$L^g = KG \otimes_{KH} L.$$

On the other hand, if  $M$  is a left  $KG$ -module, we denote by  $M_H$  the left  $KH$ -module obtained by restriction of the set of operators on  $M$  from  $KG$  to  $KH$ . (The elementary properties of *induced modules*  $L^g$  have already been worked out in § 12D.) Similar terminology will be used for representations. For example, if  $S$  is the matrix representation of  $H$  afforded by the left  $KH$ -module  $L$ , the matrix representation afforded by  $L^g$  is called the *induced matrix representation* and will be denoted by  $S^g$ . If  $T$  is a matrix representation of  $G$ , then  $T_H$  denotes the restriction of  $T$  to  $H$ . We assume familiarity with all of § 12D and shall use results from that section without always pinpointing the reference.

Some special kinds of induced representations are of interest by themselves. The simplest is the representation induced from the 1-representation  $T: H \rightarrow \{1\}$  of a subgroup  $H$ . The degree of the induced representation  $T^g$  is the index  $[G : H]$  of  $H$  in  $G$ , and the matrices  $T^g(g)$ ,  $g \in G$ , all are permutation matrices (see Exercise 12.9).  $T^g$  is a *permutation representation* in the sense of § 9, Example 1. Not every permutation representation, however, is an induced representation (see Exercise 43.1).

Another representation which has proved to be useful is the *monomial representation*, which is the name given to a matrix representation  $T$  of  $G$  such that for each  $g \in G$ ,  $T(g)$  has exactly one non-zero entry in each row and column. For example, let  $U$  be a one-dimensional representation of a subgroup  $H$  of  $G$ , and let  $T = U^g$ . Then it is easily seen from the calculation of  $U^g$  given in § 12D that  $T$  is a monomial representation. To express ourselves clearly on this point, we shall call an *induced monomial representation* any induced representation  $U^g$ , where  $U$  is a one-dimensional representation of a subgroup. In Exercise 43.1, we shall give a sufficient condition for an arbitrary monomial representation to be an induced monomial representation. In § 50, the concept of monomial representation is generalized to the important notion of an imprimitive module, and from this theory it follows in particular that every irreducible monomial representation is an induced monomial representation.

sentation.

We consider now the operations of forming tensor products and contragredient modules, and prove that these operations commute with the operation of forming induced modules. We begin with tensor products.

(43.1) DEFINITION. Let  $G_1$  and  $G_2$  be finite groups, and let  $P = G_1 \times G_2$  be their direct product. Let  $L_i$  be a left  $KG_i$ -module,  $i = 1, 2$ . Then the *outer tensor product*  $L_1 \# L_2$  of  $L_1$  and  $L_2$  is the left  $KP$ -module whose underlying vector space is  $L_1 \otimes_K L_2$ , with the module operation given by

$$(g_1, g_2)(l_1 \otimes l_2) = g_1 l_1 \otimes g_2 l_2, \quad (g_1, g_2) \in P, \quad l_i \in L_i, \quad i = 1, 2,$$

and extended to  $KP$  and  $L_1 \otimes_K L_2$  by linearity.

In terms of representations, let  $T_1$  and  $T_2$  be the representations of  $G_1$  and  $G_2$  afforded by the modules  $L_1$  and  $L_2$ , respectively. Then the module  $L_1 \# L_2$  affords the representation  $T_1 \# T_2$  of  $P$ , where

$$(T_1 \# T_2)(g_1, g_2) = T_1(g_1) \otimes T_2(g_2), \quad (g_1, g_2) \in P.$$

From §12A we recall that if both  $L_1$  and  $L_2$  are  $KG$ -modules, we define a left  $KG$ -module  $L_1 \otimes_K L_2$  where the action of  $G$  is given by

$$g(l_1 \otimes l_2) = gl_1 \otimes gl_2, \quad g \in G, \quad l_i \in L_i, \quad i = 1, 2.$$

If  $L_1$  and  $L_2$  afford the representations  $T_1$  and  $T_2$ , then  $L_1 \otimes L_2$  affords the (inner) *tensor product* representation

$$T_1 \otimes T_2 : (T_1 \otimes T_2)(g) = T_1(g) \otimes T_2(g).$$

We may relate the concepts of outer and inner tensor products in the following manner. Let  $G_0$  be the *diagonal subgroup* of  $G \times G$ ; that is,

$$G_0 = \{(g, g) : g \in G\}.$$

Then  $G_0$  is isomorphic to  $G$ , and if we identify  $G_0$  with  $G$ , we have

$$(L_1 \# L_2)_{G_0} \cong L_1 \otimes_K L_2,$$

as left  $KG$ -modules, or in terms of representations, letting “ $\cong$ ” denote equivalence,

$$(T_1 \# T_2)_{G_0} \cong T_1 \otimes T_2.$$

A further comparison between outer and inner tensor products comes if we identify  $KP = K(G_1 \times G_2)$  with  $KG_1 \otimes_K KG_2$  (see Exercise 12.8). Then the reader may verify that on  $L_1 \# L_2$ , we have

$$(a_1 \otimes a_2)(l_1 \otimes l_2) = a_1 l_1 \otimes a_2 l_2, \quad a_i \in KG_i, \quad l_i \in L_i, \quad i = 1, 2$$

whereas it is *not true* for  $L_1 \otimes L_2$  that

$$a(l_1 \otimes l_2) = al_1 \otimes al_2$$

for all  $a \in KG$ , although it is true for  $a \in G$ .

(43.2) THEOREM. Let  $H_i$  be a subgroup of  $G_i$ ,  $i = 1, 2$ , and let  $L_i$  be a left  $KH_i$ -module,  $i = 1, 2$ . Then

$$(43.3) \quad (L_1 \# L_2)^{G_1 \times G_2} \cong L_1^{G_1} \# L_2^{G_2}.$$

PROOF. We first exploit the basic property of tensor products [Theorem 12.3] to construct a  $K(G_1 \times G_2)$ -homomorphism of  $(L_1 \# L_2)^{G_1 \times G_2}$  into  $L_1^{G_1} \# L_2^{G_2}$ . In this discussion we shall identify  $K(G_1 \times G_2)$  with  $KG_1 \otimes KG_2$  and shall ask the reader to tell from the context over what ring the various tensor products are taken. The whole argument is clear from the diagram:

$$\begin{array}{ccc} (KG_1 \otimes KG_2) \otimes_{KH_1 \otimes KH_2} (L_1 \# L_2) & = & (L_1 \# L_2)^{G_1 \times G_2} \\ \nearrow t & & \searrow \eta' \\ (KG_1 \otimes KG_2) \times (L_1 \# L_2) & \xrightarrow{\eta} & (KG_1 \otimes_{KH_1} L_1) \# (KG_2 \otimes_{KH_2} L_2) = L_1^{G_1} \# L_2^{G_2} \end{array}$$

where  $t$  is the canonical bilinear map of the cartesian product  $(KG_1 \otimes KG_2) \times (L_1 \# L_2) \rightarrow (L_1 \# L_2)^{G_1 \times G_2}$ , and  $\eta$  is the balanced map with respect to  $KH_1 \otimes KH_2$  given by

$$\eta(a_1 \otimes a_2, l_1 \otimes l_2) = (a_1 \otimes l_1) \otimes (a_2 \otimes l_2), \quad a_i \in KG_i, \quad l_i \in L_i, \quad i = 1, 2.$$

By Theorem 12.3, there exists a  $K$ -homomorphism  $\eta'$  of  $(L_1 \# L_2)^{G_1 \times G_2}$  into  $L_1^{G_1} \# L_2^{G_2}$  such that  $\eta't = \eta$ , that is

$$\begin{aligned} \eta'((a_1 \otimes a_2) \otimes (l_1 \otimes l_2)) &= (a_1 \otimes l_1) \otimes (a_2 \otimes l_2), \\ a_i \in KG_i, \quad l_i \in L_i, \quad i &= 1, 2. \end{aligned}$$

The mapping  $\eta'$  is clearly a  $KG_1 \otimes KG_2$ -homomorphism of  $(L_1 \# L_2)^{G_1 \times G_2}$  onto  $L_1^{G_1} \# L_2^{G_2}$ . Since the dimensions over  $K$  of  $(L_1 \# L_2)^{G_1 \times G_2}$  and  $L_1^{G_1} \# L_2^{G_2}$  are equal by (12.27), it follows that  $\eta'$  is an isomorphism, and Theorem 43.2 is proved.

Now we come to contragredient modules and representations. The contragredient representation has already appeared in Chapter V [see (31.21)] as the representation whose character is the complex conjugate of a given character. For our purposes in this chapter, we shall take a somewhat more general point of view.

First, we recall that the *dual space*  $L^*$  of a finite-dimensional vector space  $L$  over  $K$  is the space  $\text{Hom}_K(L, K)$  of all linear func-

tions  $\psi: L \rightarrow K$ . If  $\{l_1, \dots, l_s\}$  is a  $K$ -basis of  $L$ , then  $L^*$  has a dual basis consisting of the functions  $\{\psi_1, \dots, \psi_s\}$  such that

$$(43.4) \quad \psi_i(l_j) = \delta_{ij}, \quad 1 \leq i, j \leq s.$$

If  $T \in \text{Hom}_K(L, L)$ , the *transpose*  $T^*$  of  $T$  is the element of  $\text{Hom}_K(L^*, L^*)$  such that

$$(T^*\psi)(l) = \psi(Tl), \quad \psi \in L^*, l \in L.$$

Let  $T = (\alpha_{ij})$  be the matrix of  $T$  with respect to the basis  $\{l_1, \dots, l_s\}$ , so that

$$Tl_i = \sum_{j=1}^s \alpha_{ji} l_j, \quad 1 \leq i \leq s.$$

Then the matrix  $T^*$  of  $T^*$  with respect to the basis  $\{\psi_1, \dots, \psi_s\}$  satisfying (43.4) is the *transpose matrix*  $'T$  of  $T$ , and the  $(i, j)$  entry of  $'T$  is  $\alpha_{ji}$ .

(43.5) DEFINITION. Let  $A$  be an algebra over  $K$  and  $L$  a left  $A$ -module. Let  $L^*$  be the dual space of  $L$ . Then  $L^*$  becomes a right  $A$ -module if we define

$$(\psi a)(l) = \psi(al), \quad \psi \in L^*, a \in A, l \in L.$$

The right  $A$ -module  $L^*$  is called the *dual* of  $L$ . Similarly, we may associate with any right  $A$ -module its dual, which is a left  $A$ -module.

(43.6)  $L^*$  is an irreducible right  $A$ -module if and only if  $L$  is an irreducible left  $A$ -module.

PROOF. Let  $U$  be an  $A$ -submodule of  $L$ , and let

$$U^\perp = \{\psi \in L^* : \psi(U) = 0\}.$$

Then  $U^\perp$  is an  $A$ -submodule of  $L^*$ , whose dimension over  $K$  is  $(L:K) - (U:K)$ , as is easily seen by taking suitable dual bases (43.4) in  $L$  and  $L^*$ . Similarly, an  $A$ -submodule  $U^*$  of  $L^*$  gives rise to an  $A$ -submodule  $U$  of  $L$  where

$$U = \{l \in L : \psi(l) = 0 \text{ for all } \psi \in U^*\},$$

and we have  $(U:K) = (L:K) - (U^*:K)$ . The statement (43.6) is an immediate consequence of these remarks.

In general, the construction of dual modules has the unpleasant feature of forming right modules from left modules. If  $A = KG$  is the group algebra of a finite group, however, we can make the dual  $L^*$  of a left  $KG$ -module  $L$  into a left  $KG$ -module in the following way.

(43.7) **DEFINITION.** Let  $L$  be a left  $KG$ -module. The *contragredient module*  $L^*$  of  $L$  is the left  $KG$ -module in which the underlying vector space is the dual space  $L^*$  of  $L$  and with the module operation given by

$$(43.8) \quad (g\psi)(l) = (\psi g^{-1})(l) = \psi(g^{-1}l),$$

for  $g \in G$ ,  $\psi \in L^*$ ,  $l \in L$ . The operation is then extended to all  $KG$  by linearity.

It is easily verified that if  $L$  affords a matrix representation  $T$ , then relative to the dual basis,  $L^*$  affords a matrix representation  $W$  (called the *contragredient representation* of  $T$ ), given by

$$W(g) = {}^t T(g^{-1}), \quad g \in G,$$

where  ${}^t T$  denotes the transpose of the matrix  $T$ . [See (31.21).]

Now we prove

(43.9) **THEOREM.** Let  $H$  be a subgroup of  $G$  and  $L$  a left  $KH$ -module. Then

$$(L^G)^* \cong (L^*)^G$$

as left  $KG$ -modules.

**PROOF.** Once again it is clear that both modules have the same dimension over  $K$ , so that it is sufficient to set up a  $KG$ -homomorphism of one onto the other. We first define a balanced map, with respect to  $KH$ , of  $KG \times L^*$  into the dual space of  $L^G$  as follows: Let  $\{g_1, \dots, g_t\}$  be a set of left coset representatives of  $H$  in  $G$ ; then, from §12D, every element of  $KG$  can be expressed uniquely in the form  $\sum g_i b_i$ ,  $b_i \in KH$ , whereas every element of  $L^G$  can be expressed uniquely in the form  $\sum g_i \otimes l_i$ ,  $l_i \in L$ . Now let  $(\sum g_i b_i, \psi)$  be a pair belonging to  $KG \times L^*$ . To this pair we assign the element  $\varphi \in (L^G)^*$  whose action on an element  $x = \sum g_i \otimes l_i \in L^G$  is given by

$$\varphi(x) = \sum_{i=1}^t (b_i \psi)(l_i)$$

where  $b_i \psi$  is defined by (43.8). Evidently the pairs

$$(\sum g_i b_i, \psi) \quad \text{and} \quad (\sum g_i b_i, b\psi),$$

for a fixed  $b \in KH$ , are mapped onto the same linear function on  $L^G$ . Therefore the map is balanced, and there exists a  $K$ -homomorphism  $\eta$  of  $(L^*)^G$  into  $(L^G)^*$  such that

$$(43.10) \quad [(\eta(\sum g_i \otimes \psi_i))(\sum g_i \otimes l_i)] = \sum_{i=1}^t \psi_i(l_i)$$

for  $\psi_i \in L^*$  and  $l_i \in L$ . Let  $g \in G$ ; then we have for each  $i$ ,

$$gg_i = g_i h_{ji}$$

for some  $j$  depending on  $i$ , and some  $h_{ji} \in H$ . Then

$$\begin{aligned} [\eta(g(g_i \otimes \psi))] (\sum g_i \otimes l_i) &= \eta(g_i \otimes h_{ji}\psi) (\sum g_i \otimes l_i) \\ &= h_{ji}\psi(l_j) = \psi(h_{ji}^{-1}l_j), \end{aligned}$$

whereas, since  $g^{-1}g_i = g_i h_{ji}^{-1}$ , we have

$$[g(\eta(g_i \otimes \psi))] (\sum g_i \otimes l_i) = [\eta(g_i \otimes \psi)] (\sum g^{-1}g_i \otimes l_i) = \psi(h_{ji}^{-1}l_j).$$

Therefore  $\eta$  is a  $KG$ -homomorphism. From (43.10) it is clear that  $\eta((L^*)^G)$  has the same dimension as  $(L^G)^*$ . Therefore  $\eta$  is a  $KG$ -isomorphism of  $(L^*)^G$  onto  $(L^G)^*$ , and Theorem 43.9 is proved.

Theorem 43.9 is also easily proved if one works exclusively with matrix representations.

The next concept to be introduced is that of intertwining number, which is used to count the number of times one module appears as a component of another.

(43.11) DEFINITION. Let  $L$  and  $M$  be left  $KG$ -modules. Then  $\text{Hom}_{KG}(L, M)$  is a vector space over  $K$ , and its dimension is called the *intertwining number*  $i(L, M)$  of  $L$  and  $M$ .

The basic properties of the intertwining number are that it is additive:

$$i(L_1 \oplus L_2, M) = i(L_1, M) + i(L_2, M);$$

and, if  $KG$  is semi-simple,  $i(L, M)$  is symmetric:

$$i(L, M) = i(M, L).$$

The proofs of these facts require some preliminary discussion and are given later in this section [Corollary 43.16 and Exercise 43.6].

If  $T$  and  $U$  are matrix representations afforded by  $L$  and  $M$ , respectively, then  $i(L, M)$  is equal to the dimension over  $K$  of the set of intertwining matrices  $S$  such that

$$(43.12) \quad ST(g) = U(g)S$$

for all  $g \in G$ . (See § 29.)

(43.13) DEFINITION. Let  $L$  be a left  $KG$ -module. An *invariant* (or  $G$ -*invariant*) of  $L$  is an element  $l \in L$  such that  $gl = l$  for all  $g \in G$ . The set of all invariants of  $L$  forms a  $KG$ -submodule of  $L$ .

(43.14) THEOREM. Let  $L$  and  $M$  be left  $KG$ -modules. The intertwining number  $i(L, M)$  is equal to the dimension of the space of invariants of the  $KG$ -module  $L^* \otimes_K M$ .

PROOF. We begin with the observation (see Exercise 12.4) that, if we define for  $\phi \in L^*$ ,  $m \in M$ , the linear transformation  $\phi \circ m \in \text{Hom}_K(L, M)$  by

$$(\phi \circ m)(l) = \phi(l)m, \quad l \in L, m \in M, \phi \in L^*,$$

the mapping

$$(43.15) \quad \sum \psi_i \otimes m_i \rightarrow \sum \psi_i \circ m_i$$

is a  $K$ -isomorphism of  $L^* \otimes M$  onto  $\text{Hom}_K(L, M)$ . The linear transformation  $\sum \psi_i \circ m_i$  belongs to  $\text{Hom}_{KG}(L, M)$  if and only if for all  $l \in L$  and  $g \in G$ , we have

$$(\sum \psi_i \circ m_i)(gl) = g[(\sum \psi_i \circ m_i)(l)];$$

in other words

$$\sum \psi_i(gl)m_i = \sum \psi_i(l)gm_i.$$

This implies that for all  $g \in G$ ,

$$\sum g^{-1}\psi_i(l)g^{-1}m_i = \sum \psi_i(l)m_i.$$

Because of the isomorphism (43.15), it follows that

$$\sum g^{-1}\psi_i \otimes g^{-1}m_i = \sum \psi_i \otimes m_i$$

for all  $g \in G$ , and hence  $\sum \psi_i \otimes m_i$  is an invariant of  $L^* \otimes_K M$ . Conversely, any invariant of  $L^* \otimes_K M$  corresponds to an element of  $\text{Hom}_{KG}(L, M)$  under the isomorphism (43.15). This completes the proof of (43.14).

(43.16) COROLLARY. If  $L = L_1 \oplus L_2$ , then  $i(L, M) = i(L_1, M) + i(L_2, M)$  for any left  $KG$ -module  $M$ .

PROOF. It is only necessary to remark that  $L^* \cong L_1^* \oplus L_2^*$  as left  $KG$ -modules, and that the dimension of the space of  $G$ -invariants of a direct sum is the sum of the dimensions of the spaces of invariants in the components.

(43.17) DEFINITION. Let  $L$  be a completely reducible  $KG$ -module, and let  $M$  be an irreducible  $KG$ -module. We say that an integer  $m$  is the *number of times that  $M$  is contained in  $L$*  if a decomposition of  $L$  into irreducible components contains exactly  $m$  submodules isomorphic to  $M$ .

For example, if  $T$  and  $U$  are matrix representations of  $G$ , Theorem 43.14 asserts that the intertwining number  $i(T, U)$  is equal to the number of times the 1-representation is contained in  $T^* \otimes U$ .

(43.18) THEOREM. *Let  $L$  be a completely reducible  $KG$ -module, where  $K$  is an algebraically closed field, and let  $M$  be an irreducible  $KG$ -module. Then the number of times  $M$  is contained in  $L$  is equal to the intertwining number  $i(L, M)$ . A completely reducible module  $L$  is irreducible if and only if  $i(L, L) = 1$ .*

PROOF. Let  $L = L_1 \oplus \cdots \oplus L_r$ , where the  $\{L_i\}$  are irreducible. By (43.16) we have

$$i(L, M) = i(L_1, M) + \cdots + i(L_r, M).$$

Since  $K$  is algebraically closed, the results of §27 imply that

$$i(L_j, M) = \begin{cases} 0 & \text{if } L_j \not\cong M \\ 1 & \text{if } L_j \cong M \end{cases}.$$

Both assertions of the theorem follow from these remarks. (See Exercise 27.1.)

REMARK. In Theorem 43.18, it is only necessary to assume that  $K$  is a splitting field for  $G$ .

### Exercises

- Let  $M$  be a vector space over  $K$  with basis  $B = \{m_1, \dots, m_n\}$ , and let  $T$  be a permutation representation of a finite group  $G$  by linear transformations on  $M$  such that for each  $g \in G$ ,  $T(g)$  is a permutation of the basis  $B$ . The representation  $T$  is called a *transitive permutation representation* if for every  $i$  and  $j$ ,  $1 \leq i, j \leq n$ , there exists a  $g \in G$  such that  $T(g)m_i = m_j$ . Prove that  $T = U^G$  where  $U$  is the 1-representation of the subgroup  $H$  of  $G$  defined by

$$(43.19) \quad H = \{g \in G : T(g)m_1 = m_1\}.$$

Is every permutation representation an induced representation? More generally, a representation  $T$  is called a *monomial representation* if  $T(g)m_i = \alpha_{ji}(g)m_j$  for each  $g \in G$  and  $1 \leq i \leq n$ , where  $j$  is an index depending on  $i$  and  $g$ , and  $\alpha_{ji}(g) \in K$ . Then each  $T(g)$  defines a permutation of the basis  $B$ , and, if the permutations given by the  $T(g)$ ,  $g \in G$ , are transitive on  $B$ , then  $T \cong U^G$  where  $U$  is a certain one-dimensional representation of a subgroup  $H$  of  $G$  defined as in (43.19).

- By Exercise 10.6, every complex representation of a finite group  $G$  is equivalent to a unitary representation. Prove that every matrix representation of  $G$  by real orthogonal matrices is equivalent to its contragredient represen-

tation.

3. (Mackey [1]). Let  $H$  be a subgroup of  $G$ , and let  $L$  be a left  $KH$ -module. Let  $\hat{L}$  be the set of all functions  $f: G \rightarrow L$  such that  $f(hg) = hf(g)$ ,  $h \in H$ ,  $g \in G$ . The set  $\hat{L}$  becomes a vector space over  $K$  if we define

$$(f_1 + f_2)(g) = f_1(g) + f_2(g), \quad f_i \in \hat{L}, g \in G,$$

$$(\alpha f)(g) = \alpha f(g), \quad \alpha \in K,$$

and a left  $KG$ -module if we define

$$(gf)(x) = f(xg), \quad g, x \in G, f \in \hat{L}.$$

Prove that  $\hat{L} \cong L^G$  as left  $KG$ -modules.

4. (Higman [4]). Let  $H$  be a subgroup of  $G$ , and suppose that to every left  $KH$ -module  $L$  there corresponds a left  $KG$ -module  $I(L)$  such that the following conditions hold:

(i) there exists a  $KH$ -isomorphism  $\epsilon$  of  $L$  into  $I(L)_H$  such that  $I(L)$  is generated as a  $KG$ -module by  $\epsilon(L)$ ;

(ii) for any left  $KG$ -module  $M$  and any  $KH$ -homomorphism  $\lambda: L \rightarrow M_H$ , there exists a  $KG$ -homomorphism  $\lambda': I(L) \rightarrow M$  such that

$$\lambda' \epsilon = \lambda.$$

Prove that  $I(L)$  is uniquely determined up to  $KG$ -isomorphism by the properties (i) and (ii). Prove that if we set  $I(L) = L^g$ , then (i) and (ii) are satisfied.

5. If  $H \subset G$  and  $L$  is a left  $KH$ -module, prove that the dimension of the space of  $H$ -invariants of  $L$  is equal to the dimension of the space of  $G$ -invariants of  $L^g$ .

6. Let  $KG$  be a semi-simple algebra. Prove that, for any two  $KG$ -modules  $L$  and  $M$ ,  $i(L, M) = i(M, L)$ .

[Hint: Prove that  $(L^* \otimes_K M)^* \cong M^* \otimes_K L$ , and apply Theorem 43.14. Finally prove that if  $KG$  is semi-simple, the dimension of the space of  $G$ -invariants of  $N$  is equal to the dimension of the space of  $G$ -invariants of  $N^*$ , for all  $KG$ -modules  $N$ ]

7. Let  $T_1$  be an induced monomial representation of a group  $G_1$  and  $T_2$  an induced monomial representation of a group  $G_2$ . Prove that  $T_1 \# T_2$  is an induced monomial representation of the direct product  $G_1 \times G_2$ .

8. Let  $T$  be a permutation matrix representation of a finite group  $G$  by permutations acting on a set  $X$  of  $n$  elements. Prove that the number of times the 1-representation appears in  $T$  is equal to the number of orbits in  $X$  relative to  $G$ . [Hint: Apply Theorem 43.18 to show that the number of times the 1-representation appears is equal to the dimension of the space of invariants of  $1 \otimes T \cong T$  and that the space of invariants of  $T$  is spanned by the sums of basis vectors belonging to the different orbits.] [(See (32.3).)]

9. Let  $L$  and  $M$  be  $KG$ -modules where  $\text{char } K \nmid [G : 1]$ , and suppose that  $L$  is irreducible. Show that if  $M \otimes_K L^*$  contains the 1-representation of  $G$ , then  $M$  contains  $L$  as a direct summand. Is the converse true?

### § 44. The Tensor Product Theorem and the Intertwining Number Theorem

The object of this section is to study the direct sum decomposition of the tensor product of two induced modules  $L^g \otimes M^g$ , where  $L$  and  $M$  are modules for subgroups of  $G$ , and to find a formula for the intertwining number of the induced modules  $L^g$  and  $M^g$ . These results in their full generality are due to Mackey [1] although various special cases and consequences of them were known earlier.

Our discussion begins with an identity concerning induced representations, which has been called the subgroup theorem by Mackey [1]; our presentation is close to that of Green [1]. Let  $R$  and  $S$  be subgroups of a finite group  $G$ , and let  $L$  be a left  $KR$ -module, where  $K$  is an arbitrary field. Our objective is, roughly speaking, to show that the structure of the module  $(L^g)_S$  is determined by the  $(S, R)$  double cosets in  $G$  (see § 2).

We require first a useful characterization of induced modules. In this result,  $H$  denotes a subgroup of a finite group  $G$ .

(44.1) **LEMMA.** *Let  $M$  be a left  $KG$ -module such that for some  $KH$ -submodule  $L$  of  $M_H$ ,  $M$  is the direct sum*

$$M = \sum_{i=1}^m \bigoplus g_i L ,$$

*where the  $\{g_i\}$  form a set of representatives of the left cosets of  $H$  in  $G$ . Then  $M \cong L^g$  as  $KG$ -modules.*

**PROOF.** Using (12.26) we verify at once that

$$\sum g_i \otimes l_i \rightarrow \sum g_i l_i$$

is a  $KG$ -isomorphism of  $L^g$  onto  $M$ , and (44.1) is proved.

Now let  $G$  be the disjoint union of the left  $R$ -cosets  $x_1R, \dots, x_qR$ . Then by (12.26), we can express  $L^g$  as a direct sum of  $K$ -subspaces

$$L^g = \sum_{i=1}^q x_i \otimes L .$$

Focusing our attention on a fixed  $(S, R)$ -double coset  $SaR$ , we consider all cosets  $x_iR$  such that  $x_iR \subset SaR$ . We may assume they are the cosets  $x_1R, \dots, x_hR$ . Then

$$W = \sum_{i=1}^h x_i \otimes L$$

is an  $S$ -component of  $L^g$  which depends only on the double coset  $SaR$  and not upon the coset representatives  $\{x_i\}$  of  $R$  in  $G$ ; in fact, if  $x_iR = x'_iR$ , then  $W = \sum_{i=1}^h x_i \otimes L = \sum_{i=1}^h x_i R \otimes L = \sum_{i=1}^h x'_i R \otimes L = \sum_{i=1}^h x'_i \otimes L$ .

Next we observe that, for each coset  $x_iR \subset SaR$ , there exists an element  $t_i \in S$  such that

$$x_iR = t_i aR.$$

Moreover, two cosets  $t_i aR$  and  $t_j aR$  are identical if and only if  $a^{-1}t_j^{-1}t_i a \in R$ , or alternately,

$$t_j^{-1}t_i \in aRa^{-1} \cap S.$$

Therefore the  $\{t_i\}$  belong to distinct left cosets of the subgroup

$$\tilde{R} = aRa^{-1} \cap S$$

in  $S$ . For every  $s \in S$  we have  $sa = t_i ar$  for some  $r \in R$ ; hence  $s \in t_i \tilde{R}$ , and the  $\{t_i\}$  form a full set of left coset representatives of  $\tilde{R}$  in  $S$ .

Returning to the  $S$ -module  $W$ , we have

$$W = \sum_{i=1}^h x_i R \otimes L = \sum_{i=1}^h t_i a R \otimes L = \sum_{i=1}^h t_i (a \otimes L)$$

where  $a \otimes L$  is a left  $aRa^{-1}$ -module. Since  $\tilde{R} \subset aRa^{-1}$ ,  $a \otimes L$  is an  $\tilde{R}$ -submodule of  $W$ , and by Lemma 44.1 we have

$$W \cong (a \otimes L)_{\tilde{R}}^S.$$

Summarizing our discussion, we have proved:

(44.2) SUBGROUP THEOREM. *Let  $R$  and  $S$  be subgroups of  $G$ , and let  $L$  be a left  $KR$ -module, where  $K$  is an arbitrary field. For each  $(S, R)$ -double coset  $D = SaR$ ,  $a \otimes L$  is a left  $K\tilde{R}$ -module for the subgroup*

$$\tilde{R} = aRa^{-1} \cap S$$

*of  $S$ , and*

$$L(D) = (a \otimes L)_{\tilde{R}}^S.$$

*is a left  $KS$ -module which depends only on the double coset  $D$ . Moreover,*

$$(L^g)_S = \sum_D L(D) \quad (\text{direct sum})$$

as left  $KS$ -modules, where the sum is taken over all  $(S, R)$ -double cosets  $D$  in  $G$ .

The next two results are essentially corollaries of the subgroup theorem. Both give information about the reduction of the tensor product  $L_1^g \otimes L_2^g$  of two induced modules.

(44.3) **TENSOR PRODUCT THEOREM.** *Let  $H_1$  and  $H_2$  be subgroups of  $G$ , and let  $L_i$  be a left  $KH_i$ -module for  $i = 1, 2$ . Fix elements  $x \in G$  and  $y \in G$ , and set*

$$H^{(x,y)} = xH_1x^{-1} \cap yH_2y^{-1}.$$

Let

$$L_1^{(x)} = x \otimes L_1 \subset L_1^g, \quad L_2^{(y)} = y \otimes L_2 \subset L_2^g.$$

Then both  $L_1^{(x)}$  and  $L_2^{(y)}$  are  $KH^{(x,y)}$ -modules. Moreover, the induced module

$$(L_1^{(x)} \otimes L_2^{(y)})^g$$

depends only on the  $(H_1, H_2)$ -double coset  $D$  of  $G$  to which  $x^{-1}y$  belongs, and we have

$$L_1^g \otimes L_2^g = \sum_D (L_1^{(x)} \otimes L_2^{(y)})^g \quad (\text{direct sum})$$

where the sum is taken over all  $(H_1, H_2)$ -double cosets  $D$  of  $G$ .

**PROOF.** We begin by providing a dictionary to translate objects in the present theorem to their counterparts in the subgroup theorem.

Tensor product theorem	Subgroup theorem
$G \times G$	$G$
$H_1 \times H_2$	$R$
$G_0$ (diagonal subgroup of $G \times G$ )	$S$
$L_1 \# L_2$	$L$

To the element  $a$  in the subgroup theorem corresponds  $(x, y) \in G \times G$ , and to  $\tilde{R}$  corresponds the subgroup of  $G \times G$

$$H^*(x, y) = (x, y)(H_1 \times H_2)(x, y)^{-1} \cap G_0$$

which may be identified with

$$H^{(x,y)} = xH_1x^{-1} \cap yH_2y^{-1} \subset G.$$

Now we have the task of identifying the  $KH^*(x, y)$ -module

$$(x, y) \otimes (L_1 \# L_2) \subset (L_1 \# L_2)^{g \times g}$$

with the  $KH^{(x,y)}$ -module

$$(x \otimes L_1) \otimes (y \otimes L_2) = L_1^{(x)} \otimes L_2^{(y)}.$$

Clearly, there is a vector space isomorphism  $\varphi$  which takes  $(x, y) \otimes (l_1 \otimes l_2) \in (x, y) \otimes (L_1 \# L_2)$  onto  $(x \otimes l_1) \otimes (y \otimes l_2)$  in  $L_1^{(x)} \otimes L_2^{(y)}$ . Then for  $(x^*, y^*) \in H^*(x, y)$ , we have

$$x^* = x h_1 x^{-1} = y^* = y h_2 y^{-1}$$

for some  $h_1 \in H_1$ ,  $h_2 \in H_2$ , and

$$\begin{aligned} \varphi((x^*, y^*)[(x, y) \otimes (l_1 \otimes l_2)]) &= \varphi((x, y) \otimes (h_1 l_1 \otimes h_2 l_2)) \\ &= (x \otimes h_1 l_1) \otimes (y \otimes h_2 l_2) = x^*((x \otimes l_1) \otimes (y \otimes l_2)), \end{aligned}$$

where  $x^*$  is the element in  $H^{(x,y)}$  corresponding to  $(x^*, y^*)$  in  $H^*(x, y)$ . We have shown that to  $(a \otimes L)_R$  in the subgroup theorem corresponds the  $H^{(x,y)}$ -module  $L_1^{(x)} \otimes L_2^{(y)}$ . Finally, it is clear that  $(x, y)$  and  $(x_1, y_1)$  belong to the same  $(G_0, H_1 \times H_2)$ -double coset in  $G_1 \times G_2$  if and only if  $x^{-1}y$  and  $x_1^{-1}y_1$  belong to the same  $(H_1, H_2)$ -double coset  $D$  in  $G$ . With these preparations, the subgroup theorem now implies that  $(L_1^{(x)} \otimes L_2^{(y)})^G$  depends only on the  $(H_1, H_2)$ -double coset  $D$  to which  $x^{-1}y$  belongs and that

$$((L_1 \# L_2)^{G \times G})_{G_0} \cong \sum_D (L_1^{(x)} \otimes L_2^{(y)})^G$$

as left  $KG$ -modules, where we have of course identified  $G_0$  with  $G$ . Moreover, by (43.3), we have

$$((L_1 \# L_2)^{G \times G})_{G_0} \cong (L_1^G \# L_2^G)_{G_0} \cong L_1^G \otimes L_2^G$$

as left  $KG$ -modules, and the tensor product theorem is proved.

As a corollary, it is worthwhile stating the tensor product theorem as it applies to representations.

**(44.4) COROLLARY.** *Let  $H_1$  and  $H_2$  be subgroups of  $G$ , and let  $T_1$  and  $T_2$  be representations of  $H_1$  and  $H_2$ , respectively. Consider a fixed pair of elements  $x \in G$  and  $y \in G$ . Then*

$$T_1^{(x)}: h \rightarrow T_1(x^{-1}hx),$$

and

$$T_2^{(y)}: h \rightarrow T_2(y^{-1}hy)$$

both are representations of the subgroup  $H^{(x,y)} = xH_1x^{-1} \cap yH_2y^{-1}$  of  $G$ . Moreover, the induced representation  $(T_1^{(x)} \otimes T_2^{(y)})^G$  depends only on the  $(H_1, H_2)$ -double coset  $D$  in  $G$  to which  $x^{-1}y$  belongs, and we have

$$T_1^G \otimes T_2^G \cong \sum_D (T_1^{(x)} \otimes T_2^{(y)})^G \quad (\text{direct sum})$$

where the sum is taken over all  $(H_1, H_2)$ -double cosets  $D$  in  $G$ .

(44.5) INTERTWINING NUMBER THEOREM. Let  $G, H_1, H_2, L_1, L_2$  satisfy the hypotheses of the tensor product theorem. For  $(x, y) \in G \times G$ , the intertwining number  $i(L_1^{(x)}, L_2^{(y)})$  of  $KH^{(x,y)}$ -modules defined in the preceding theorem depends only on the  $(H_1, H_2)$ -double coset  $D$  in  $G$  to which  $x^{-1}y$  belongs, and will be denoted by  $i(L_1, L_2, D)$ . Then we have

$$i(L_1^G, L_2^G) = \sum_D i(L_1, L_2, D)$$

where the sum is taken over all  $(H_1, H_2)$ -double cosets  $D$  in  $G$ .

PROOF. By Theorems (43.14) and (43.9),  $i(L_1^G, L_2^G)$  is equal to the dimension of the space of invariants of the  $KG$ -module  $(L_1^*)^G \otimes L_2^G$ . This dimension is, by Theorem 44.2, the sum of the dimensions of the spaces of invariants of the modules  $((L_1^*)^{(x)} \otimes L_2^{(y)})^G$  associated with the  $(H_1, H_2)$ -double cosets in  $G$ . It is immediate that

$$(L_1^*)^{(x)} \cong (L_1^{(x)})^*$$

as  $KH^{(x,y)}$ -modules. Moreover, the dimension of the space of  $G$ -invariants of  $((L_1^*)^{(x)} \otimes L_2^{(y)})^G$  is equal to the dimension of the space of  $H^{(x,y)}$ -invariants of  $(L_1^*)^{(x)} \otimes L_2^{(y)} \cong (L_1^{(x)})^* \otimes L_2^{(y)}$ , by Exercise 43.5. By Theorem 43.14, this dimension is precisely  $i(L_1^{(x)}, L_2^{(y)})$ . Since  $(L_2^{(x)})^* \otimes L_1^{(y)}$  depends only on the  $(H_1, H_2)$ -double coset  $D$  to which  $x^{-1}y$  belongs,  $i(L_1^{(x)}, L_2^{(y)})$  also depends only upon this coset. Putting our remarks together, we have proved Theorem 44.5.

### Exercises

1. (Mackey.) Let  $H$  be a subgroup of  $G$ ; let  $L$  be a left  $KH$ -module and  $M$  a left  $KG$ -module, where  $K$  is an algebraically closed field such that  $\text{char } K \nmid [G : 1]$ . Prove from (44.5) that

$$i(L, M_H) = i(L^G, M).$$

From this result and (43.18), prove the Frobenius reciprocity theorem 38.8.

2. Prove that the restriction of an (induced) monomial representation to a subgroup is a direct sum of induced monomial representations, and prove a similar result for transitive permutation representations. [Hint: Use the subgroup theorem.]

### § 45. Irreducibility and Equivalence of Induced Modules

In this section we apply the intertwining number theorem to investigate when the irreducibility of  $L$  implies the irreducibility of  $L^G$ , and also when two induced modules  $L_1^G$  and  $L_2^G$  are isomorphic. These problems were studied by Shoda [1] and Mann [1].

We shall assume that the base field  $K$  is algebraically closed and that  $\text{char } K \nmid [G : 1]$ . Because of these assumptions, all modules involved are completely reducible, and the basic result concerning intertwining numbers [Theorem 43.18] is available.

(45.1) **DEFINITION.** Two completely reducible left  $KG$ -modules (or representations)  $L_1$  and  $L_2$  are said to be *disjoint* if they have no composition factors in common.

From (43.16) and (43.18), we see that  $L_1$  and  $L_2$  are disjoint if and only if  $i(L_1, L_2) = 0$ . (See also Exercise 13.9.) We also recall that  $L$  is irreducible if and only if  $i(L, L) = 1$ . From §44, we recall that for a  $KH$ -module  $L$ ,  $L^{(x)}$  denotes the  $K(xHx^{-1})$ -module  $x \otimes L \subset L^G$ ; and that if  $H^{(x)}$  is the subgroup  $H \cap xHx^{-1}$  of  $H$ , then  $L_{H^{(x)}}$  is the restriction of  $L$  to  $KH^{(x)}$ .

(45.2) **THEOREM.** Let  $L$  be an irreducible left  $KH$ -module where  $H$  is a subgroup of  $G$ . Then  $L^G$  is irreducible if and only if for all  $x \notin H$ , the  $KH^{(x)}$ -modules  $L_{H^{(x)}}$  and  $(x \otimes L)_{H^{(x)}}$  are disjoint, where  $H^{(x)} = xHx^{-1} \cap H$ .

**PROOF.** By Theorem 44.5 we have

$$(45.3) \quad i(L^G, L^G) = \sum_D i(L, L, D) = \sum_D i(L^{(x)}, L^{(y)})$$

where the sum is taken over all  $(H, H)$ -double cosets  $D$  in  $H$ . Taking  $y = 1$  in the tensor product theorem, the subgroup  $H^{(x,y)}$  in that theorem becomes  $H^{(x)} = xHx^{-1} \cap H$ , whereas  $L^{(y)}$  becomes  $L_{H^{(x)}}$ . For the double coset  $D = H$ , we have  $i(L, L, H) = i(L, L) = 1$  because  $L$  is irreducible. By (45.3),  $i(L^G, L^G) = 1$  if and only if  $i(x \otimes L, L) = 0$  for every  $x \notin H$ , and this proves Theorem 45.2.

Because of the practical importance of Theorem 45.2 for purposes of computation, we shall restate the theorem and work out several corollaries in terms of representations.

(45.2)' **THEOREM.** Let  $T$  be an irreducible representation of a subgroup  $H$  of  $G$ . Then  $T^G$  is irreducible if and only if for all  $x \notin H$ , the representations  $T^{(x)}: h \rightarrow T(x^{-1}hx)$  and  $T_{H^{(x)}}$  are disjoint representations of the subgroup  $H^{(x)} = xHx^{-1} \cap H$  of  $G$ .

Applying this to the case of a one-dimensional representation of  $H$ , we obtain the following criterion for irreducibility of monomial representations:

(45.4) COROLLARY (Shoda [1]). *Let  $T$  be a one-dimensional representation of  $H$ . Then the induced monomial representation  $T^g$  of  $G$  is irreducible if and only if, for each  $x \notin H$ , there exists  $y \in xHx^{-1} \cap H$  such that  $T(y) \neq T(x^{-1}yx)$ .*

The test becomes even simpler if  $H$  happens to be a normal subgroup. In fact, we have

(45.5) COROLLARY. *Let  $H \triangle G$ , and let  $T$  be an irreducible representation of  $H$ . Then the induced representation  $T^g$  is irreducible if and only if, for all  $x \notin H$ , the representations  $T$  and  $T^{(x)}: h \rightarrow T(x^{-1}hx)$  of  $H$  are disjoint.*

Of equal importance with Theorem 45.2 is the following test for isomorphism of induced modules, whose proof is almost identical with the proof of Theorem 45.2 and is left to the reader:

(45.6) THEOREM. *Let  $H_1$  and  $H_2$  be subgroups of  $G$ , and let  $L_i$  be an irreducible  $KH_i$ -module,  $i = 1, 2$ , such that each induced module  $L_i^g$  is irreducible. Then  $L_1^g$  and  $L_2^g$  are not  $KG$ -isomorphic if and only if, for all  $x \in G$ , the  $KH^{(x)}$ -modules  $x \otimes L_1$  and  $L_2$  are disjoint, where  $H^{(x)} = xH_1x^{-1} \cap H_2$ .*

## § 46. Examples: The Tetrahedral and Octahedral Groups

As a first illustration of the practical uses of induced representations, we shall construct the irreducible representations in the field of complex numbers of the group of rotations of the tetrahedron and the cube. In contrast with the following section, the elaborate machinery of the last two sections is not needed.

The groups we have chosen are finite subgroups of the rotation group  $O_3^+$  in three-dimensional Euclidean space, where  $O_3^+$  may be defined algebraically as the group of orthogonal transformations of determinant +1. These groups are perhaps the main subject in Weyl's fascinating book on symmetry (Weyl [4]), and the complete list of finite subgroups of  $O_3^+$  is as follows:

$C_m$ , the cyclic group of order  $m$ ,  $m = 1, 2, \dots$ ,

$D_m$ , the dihedral group of order  $2m$ ,  $m = 1, 2, \dots$ ,

$T$ , the tetrahedral group of order 12,

- $O$ , the octahedral group of order 24,  
 $I$ , the icosahedral group of order 60.

The irreducible representations of  $C_n$  have already been determined in Example 4 of § 9; those of  $D_n$  are given in the next section as an application of some more general results. We shall give here a sketch of the representations of  $T$  and  $O$ , whereas the characters of the icosahedral group, which is isomorphic to the alternating group  $A_5$  of order 60, are worked out in Speiser [2], for example.

*Example 1. The Tetrahedral Group.* We leave it to the reader to verify  $T \cong A_4$ , the alternating group of order 12. The characters of  $T$  were already determined in Chapter V, and we shall add only a few remarks on the actual construction of the representations. We recall that the conjugate classes of  $A_4$  are:

$$\begin{aligned} \mathfrak{C}_1 & \{1\} \\ \mathfrak{C}_2 & \{(12)(34), (13)(24), (14)(23)\} \\ \mathfrak{C}_3 & \{(123), (214), (341), (432)\} \\ \mathfrak{C}_4 & \{(132), (241), (314), (423)\}. \end{aligned}$$

The character table of  $A_4$  is given by

	$\mathfrak{C}_1$	$\mathfrak{C}_2$	$\mathfrak{C}_3$	$\mathfrak{C}_4$
$\zeta^{(1)}$	1	1	1	1
$\zeta^{(2)}$	1	1	$\omega$	$\omega^2$
$\zeta^{(3)}$	1	1	$\omega^2$	$\omega$
$\zeta^{(4)}$	3	-1	0	0

where  $\zeta^{(1)}, \zeta^{(2)}, \zeta^{(3)}$  are characters of the three one-dimensional representations of  $T$ . We indicate two ways to construct the representation  $U_4$  whose character is  $\zeta^{(4)}$ , although we shall not actually write down the matrices.

Because of the geometrical interpretation of  $T$ , there is a one-to-one representation  $U_4: T \rightarrow O_3^+$  of degree 3. If we extend the base field to the field of complex numbers, then  $U_4$  cannot split up as the direct sum of the one-dimensional representations previously obtained, since the group  $T$  is not abelian. Therefore  $U_4$  must have an irreducible component of degree 2 or 3, and this component must be  $U_4$  itself, otherwise we violate the formula for the sum of squares of the degrees of the irreducible representations. We conclude that

$U_4$  is absolutely irreducible, and it must be the representation whose character is  $\zeta^{(4)}$ .

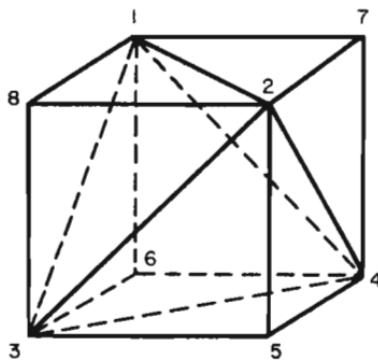
The representation  $U_4$  can also be given as an induced representation. Let  $H$  be the subgroup of  $T$  consisting of the identity element and the elements of order 2. Let  $S$  be the representation of  $H$  such that

$$S((12)(34)) = -1, \quad S((13)(24)) = -1.$$

Then the induced monomial representation  $S^T$  has degree 3. Since none of the irreducible one-dimensional representations  $(\zeta^{(i)})_H$ ,  $i = 1, 2, 3$ , contains  $S$ , the Frobenius reciprocity theorem implies that  $S^T$  cannot contain  $\zeta^{(1)}$ ,  $\zeta^{(2)}$ , or  $\zeta^{(3)}$  as a component, and therefore is irreducible.

*Example 2. The Group of Rotations of the Cube.* The octahedral group  $O$  of order 24 is isomorphic to the group of rotations of the cube, as is easily seen from the fact that the centroids of the six faces of a cube form the vertices of an octahedron. We shall use this geometrical description of the group  $O$  as a basis for our calculation of the representations. It can be shown that the octahedral group is isomorphic to the symmetric group  $S_4$ , so the results in this section give another approach to the calculation of the character table of  $S_4$  given in §32.

(46.2)



In Figure (46.2), it is clear that the vertices  $\{1, 2, 3, 4\}$  form the vertices of a regular tetrahedron; it follows that the subgroup of  $O$  consisting of those rotations which permute the vertices  $\{1, 2, 3, 4\}$  is a subgroup  $T$  of  $O$  isomorphic to the tetrahedral group of the previous example. Since  $T$  has order 12,  $[O : T] = 2$ , and  $T \triangle O$ . Our next step is to list the classes of  $O$ . We shall describe the

classes geometrically and merely give a representative of each class.

$$\mathfrak{C}_1 = \{1\},$$

$\mathfrak{C}_2 = \{(12)(34)(56)(78)\}$ , the elements of order 2 each of which is obtained by rotating a face through an angle of  $\pi$ ;

$$\mathfrak{C}_3 = \{(123)(756)\}, \text{ all elements of order 3};$$

$$\mathfrak{C}_4 = \{(2817)(5364)\}, \text{ all elements of order 4};$$

$\mathfrak{C}_5 = \{(28)(46)(37)(51)\}$ , the rotations through an angle  $\pi$  about an axis which bisects each of two opposite edges. (An easy geometrical argument shows that the classes  $\mathfrak{C}_2$  and  $\mathfrak{C}_5$  are distinct.)

Note that  $\mathfrak{C}_1, \mathfrak{C}_2, \mathfrak{C}_3$  all have representatives in the subgroup  $T$ , whereas  $\mathfrak{C}_4$  and  $\mathfrak{C}_5$  do not.

There are five irreducible representations altogether, and the sum of the squares of their degrees must equal 24.

Since  $O/T$  has order 2, there are two one-dimensional representations, which we may identify with their characters  $\zeta^{(1)}$  and  $\zeta^{(2)}$ , where  $\zeta^{(1)}$  is the 1-representation. The part of the character table involving  $\zeta^{(1)}$  and  $\zeta^{(2)}$  is given by

	$\mathfrak{C}_1$	$\mathfrak{C}_2$	$\mathfrak{C}_3$	$\mathfrak{C}_4$	$\mathfrak{C}_5$
$\zeta^{(1)}$	1	1	1	1	1
$\zeta^{(2)}$	1	1	1	-1	-1

where the -1's occur since the representatives of  $\mathfrak{C}_4$  and  $\mathfrak{C}_5$  do not belong to  $T$ .

As in Example 1,  $O$  has a one-to-one representation  $U$  of degree 3 by orthogonal transformations in Euclidean 3-space. Since the restriction of  $U$  to the subgroup  $T$  is irreducible by Example 1,  $U$  is irreducible. Using the character table for  $T$ , we find for the character  $\zeta^{(3)}$  of  $U$

	$\mathfrak{C}_1$	$\mathfrak{C}_2$	$\mathfrak{C}_3$	$\mathfrak{C}_4$	$\mathfrak{C}_5$
$\zeta^{(3)}$	3	-1	0	1	-1

where the last two entries are obtained by observing that the representatives of those classes are represented (in suitable coordinate systems) by the matrices

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & -1 \\ 0 & 1 & 0 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{pmatrix},$$

respectively.

At this point we see by counting sums of squares that we must have a three-dimensional representation and a two-dimensional one left; in particular  $\zeta^{(1)}$  and  $\zeta^{(2)}$  are the only two one-dimensional representations. Let  $F$  be the one-dimensional representation of the subgroup  $T$  whose character is given by

$$\{1, 1, \omega, \omega^2\}$$

in Table (46.1). The induced representation

$$S = F^o$$

has degree 2, and, from the Frobenius reciprocity theorem we see that neither  $\zeta^{(1)}$  nor  $\zeta^{(2)}$  is a component of  $S$ . Therefore  $S$  is irreducible. The induced character  $\zeta^{(4)}$  of  $S$  is given by

$$\zeta^{(4)}(g) = \chi(g) + \chi(\sigma g \sigma^{-1})$$

where  $\chi$  is the character of  $F$ , extended to  $O$  by setting it equal to zero outside  $T$  and where  $\sigma$  is some element not in  $T$ . An easy calculation, using Table (46.1) and the fact that  $T \triangle O$ , yields, for the values of  $\zeta^{(4)}$

	$\mathbb{C}_1$	$\mathbb{C}_2$	$\mathbb{C}_3$	$\mathbb{C}_4$	$\mathbb{C}_5$
$\zeta^{(4)}$	2	2	-1	0	0

Using the orthogonality relations on the columns of the character table, it is easily seen that the character of the remaining representation is given by

	$\mathbb{C}_1$	$\mathbb{C}_2$	$\mathbb{C}_3$	$\mathbb{C}_4$	$\mathbb{C}_5$
$\zeta^{(5)}$	3	-1	0	-1	1

Since  $\zeta^{(5)} = \zeta^{(2)} \zeta^{(3)}$ , it follows that the irreducible representation whose character is  $\zeta^{(5)}$  is given by  $\zeta^{(2)} \otimes U$ . This completes our discussion of the examples. The reader will note that the theory of induced representations played a role only in combination with various other special devices, one of the most important being the observation in Example 2 that the tensor product of two of the irreducible representations sometimes gives us a third one.

## § 47. Applications: Representations of Metacyclic Groups

In this section we shall investigate the irreducible  $KG$ -modules for a metacyclic group  $G$ , that is, a group  $G$  which contains a cyclic

normal subgroup  $A$  such that  $G/A$  is also cyclic. The dihedral groups and the generalized quaternion groups defined in § 7 are examples of metacyclic groups. It is known that any group of square-free order, or more generally, any group all of whose Sylow groups are cyclic, is a metacyclic group (see M. Hall [2], § 9.4.)

The main tools will be the results of § 45. Throughout this section,  $K$  always denotes an algebraically closed field whose characteristic is either zero or prime to the order of  $G$ .

Now let us consider a group  $G$  containing a cyclic normal subgroup  $A = [a]$  of order  $m$  and with a cyclic factor group  $G/A = [bA]$  of order  $s$ . Then we must have for some integer  $r$ ,

$$(47.1) \quad b^{-1}ab = a^r$$

where  $\sigma: a^i \rightarrow b^{-1}a^i b$  is an automorphism of  $A$ . The powers of  $\sigma$  are determined by

$$(47.2) \quad \sigma^k(a) = a^{r^k} = b^{-k}ab^k.$$

If  $\sigma$  has order  $u$ , then

$$\begin{cases} r^k - 1 \not\equiv 0 \pmod{m}, \\ r^u - 1 \equiv 0 \pmod{m}. \end{cases} \quad 1 \leq k \leq u-1,$$

Finally we must have for some non-negative integers  $s$  and  $t$ ,

$$(47.3) \quad b^s = a^t.$$

The integers  $m, s, r, u, t$  must satisfy the following additional conditions, as we check easily from the definition:

$$(47.4) \quad (m, r) = 1,$$

$$(47.5) \quad m \mid t(r-1),$$

$$(47.6) \quad u \mid s, \quad \text{and in particular, } r^s - 1 \equiv 0 \pmod{m}.$$

Finally, we observe that the elements of  $G$  can be expressed uniquely in the form

$$(47.7) \quad g = a^i b^j, \quad 0 \leq i \leq m-1, 0 \leq j \leq s-1.$$

The subgroup  $[a]$  has exactly  $m$  non-isomorphic one-dimensional modules  $L_i = Kl_i$ ,  $1 \leq i \leq m$ , where the action of  $a$  on  $L_i$  is given by

$$al_i = \zeta^i l_i, \quad 1 \leq i \leq m;$$

here  $\zeta$  is a primitive  $m$ th root of 1.

In order to calculate the modules  $L_i^g$ , we note first that the left cosets  $1A, bA, \dots, b^{s-1}A$  are distinct. Then  $L_i^g$  has a basis over  $K$  consisting of the elements

$$1 \otimes l_i, b \otimes l_i, \dots, b^{s-1} \otimes l_i,$$

and the actions of  $a$  and  $b$  on these basis elements are given as follows:

$$\begin{aligned} b(b^k \otimes l_i) &= b^{k+1} \otimes l_i, & 0 \leq k \leq s-1 \\ b(b^{s-1} \otimes l_i) &= 1 \otimes a^t l_i = \zeta^{it}(1 \otimes l_i), \end{aligned}$$

whereas by (47.2), we have

$$a(b^k \otimes l_i) = b^k \otimes a^{rk} l_i = \zeta^{ir^k} (b^k \otimes l_i).$$

Let  $T_i$  be the matrix representation of  $A$  given by  $T_i(a) = \zeta^i$ . Then the induced matrix representation  $T_i^G$  of  $G$  computed with respect to the basis  $\{b^k \otimes l_i\}$  of  $L_i^G$  maps  $a$  and  $b$  onto the following matrices:

$$a \rightarrow T_i^G(a) = \begin{pmatrix} \zeta^i & & & & & 0 \\ & \zeta^{ir} & & & & \\ & & \zeta^{ir^2} & & & \\ & & & \ddots & & \\ & 0 & & & \ddots & \zeta^{ir^{s-1}} \end{pmatrix},$$

$$b \rightarrow T_i^G(b) = \begin{pmatrix} 0 & \cdot & \cdot & \cdot & 0 & \zeta^{it} \\ 1 & & & & 0 & \\ & 1 & & & & \cdot \\ & & \ddots & & & \cdot \\ & 0 & & & 1 & 0 \end{pmatrix}.$$

Our first result concerns the irreducibility of  $T_i^G$ .

(47.8)  $T_i^G$  is irreducible if and only if

$$r^j i \not\equiv i \pmod{m}, \quad 1 \leq j \leq s-1.$$

PROOF. By Corollary 45.5 and Exercise 9.1,  $T_i^G$  is irreducible if and only if for all  $g = a^i b^j$  not in  $[a]$ , we have

$$T_i(a) \neq T_i(g^{-1}ag).$$

The preceding equation becomes

$$\zeta^i \neq T_i(b^{-j}ab^j) = T_i(a^{r^j}) = \zeta^{ir^j}, \quad 1 \leq j \leq s-1,$$

which is identical with the condition stated in (47.8).

Next we apply Theorem 45.6 to obtain a test for the inequivalence of  $T_i^G$  and  $T_{i'}^G$  for  $i \neq i'$ ,  $1 \leq i, i' \leq m$ .

(47.9) Let  $T_i^G$  and  $T_{i'}^G$  be irreducible. Then  $T_i^G$  and  $T_{i'}^G$  are inequivalent if and only if we have

$$r^j i \not\equiv i' \pmod{m}, \quad 0 \leq j \leq s-1.$$

PROOF. By Theorem 45.6,  $T_i^g$  and  $T_{i'}^g$  are inequivalent if and only if for all  $g \in G$ ,

$$T_i(a) \neq T_{i'}(g^{-1}ag),$$

and this is immediately seen to be equivalent to the condition stated in (47.9).

We are also interested in one-dimensional representations of  $G$ . By the results of § 9, these will be irreducible representations of  $G/[G, G]$  where  $[G, G]$  is the commutator group of  $G$ . Our next result determines  $[G, G]$ .

(47.10) *The commutator group  $[G, G]$  of  $G$  is the subgroup  $[a^{r-1}]$  of order  $m/(r-1, m)$  where  $(r-1, m)$  is the G.C.D. of  $r-1$  and  $m$ .*

PROOF. Because every subgroup of a cyclic group is the set of all  $h$ th powers of the elements of the group for some  $h$ , it follows that every subgroup of  $[a]$  is a characteristic subgroup; that is, it is sent into itself by all automorphisms of  $[a]$ . Therefore all subgroups of  $[a]$  are normal in  $G$  since  $[a] \triangle G$ . Let  $\nu$  be the natural homomorphism of  $G \rightarrow G/[a^{r-1}]$ . Applying  $\nu$  to (47.1) we have

$$\nu(b)^{-1}\nu(a)\nu(b) = \nu(a^r) = \nu(a),$$

and it follows that  $G/[a^{r-1}]$  is abelian. Therefore  $[G, G] \subset [a^{r-1}]$ . On the other hand, from (47.1) we have

$$[b^{-1}, a] = b^{-1}aba^{-1} = a^{r-1},$$

and hence  $[a^{r-1}] = [G, G]$ . Finally, it follows at once from the fact that  $a$  has order  $m$  that the order of  $[a^{r-1}]$  is  $m/(r-1, m)$ . This completes the proof of (47.10).

Now we are ready to state our main result.

(47.11) **THEOREM.** *Every irreducible matrix representation of  $G$  is either one dimensional or equivalent to one of the monomial representations  $T_i^g$ ,  $1 \leq i \leq m$ , if and only if, for each  $i$  and  $j$ ,  $1 \leq i \leq m$ ,  $1 \leq j \leq s-1$ ,*

$$(47.12) \quad r^j i \equiv i \pmod{m} \text{ implies } ri \equiv i \pmod{m}.$$

PROOF. Assume first that (47.12) holds, let  $X = \{1, \dots, m\}$ , and let  $\varphi : X \rightarrow X$  be defined by

$$x \rightarrow rx \pmod{m},$$

$$x \in X.$$

Condition (47.12) asserts that for each  $j$ ,  $1 \leq j \leq s-1$ , the maps  $\varphi$  and  $\varphi^j$  leave the same symbols fixed. If  $R$  is the cyclic group generated by  $\varphi$ , then by (47.6)  $R$  is a finite group whose order divides  $s$ . From (47.12) we conclude that the order of  $\varphi$  is either 1 or  $s$ .

If  $\varphi$  has order 1, then  $r \equiv 1 \pmod{m}$ , and by (47.1)  $G$  is abelian. Then all the irreducible representations are one dimensional, and the theorem is proved.

Now let  $\varphi$  have order  $s$ . We partition the set  $X$  into orbits relative to the transformation group  $R$ . The condition (47.12) implies that every orbit contains either 1 or  $s$  elements. The results (47.8) and (47.9) find a neat interpretation in terms of these orbits: (47.8) states that  $T_i^G$  is irreducible if and only if the orbit containing  $i$  contains  $s$  distinct elements, whereas (47.9) asserts that if  $i$  and  $i'$  belong to orbits containing  $s$  elements each, then  $T_i^G$  and  $T_{i'}^G$  are inequivalent if and only if these orbits are disjoint.

Therefore the number of inequivalent irreducible representations among the  $T_i^G$  is equal to the number of orbits containing  $s$  elements. This number will be  $(m-d)/s$  where  $d$  is the number of orbits containing exactly one element. It is easily seen that  $d = (r-1, m)$ . Therefore the number of distinct irreducible representations among the  $T_i^G$ ,  $1 \leq i \leq m$ , is exactly  $(m-d)/s$ , and the sum of the squares of the degrees of these representations is

$$\frac{(m-d)s^2}{s}.$$

On the other hand, the number of distinct one-dimensional representations is, by Example 4 of §9, the order of  $G/[G, G]$  which is by (47.10), equal to  $sd$ . The sum of squares of the degrees of these representations is  $sd$ . Therefore the sum of the squares of the degrees of the inequivalent irreducible representations we have found so far is equal to

$$(47.13) \quad \frac{(m-d)s^2}{s} + sd = ms = [G : 1],$$

and it follows that these are all the irreducible representations of  $G$ .

Suppose conversely that all the irreducible representations of  $G$  either have degree one or are equivalent to one of the represen-

tations  $T_i^g$ ,  $1 \leq i \leq m$ . Then by (47.10) there are  $sd$  distinct one-dimensional representations. As before, there are exactly  $d = (r - 1, m)$  orbits in  $X$  consisting of single elements. In order for formula (47.13) to hold, the remaining elements must split up into  $(m - d)/s$  distinct orbits, each containing  $s$  distinct elements, and this implies the relation (47.12). This completes the proof of the theorem.

(47.14) COROLLARY. *Let  $G$  be a metacyclic group with generators  $a$  and  $b$  satisfying the relations*

$$b^{-1}ab = a^r, \quad b^s = a^t, \quad a^m = 1, \quad m = \text{order of } a,$$

*where  $(m, r) = 1$ ,  $m \mid t(r - 1)$ , and  $s$  is a prime. Then all the irreducible matrix representations of  $G$  are either one dimensional or monomial representations  $T^g$ , where  $T$  is a one-dimensional representation of the subgroup  $[a]$  of  $G$ .*

PROOF. Since the order of the automorphism  $a \rightarrow b^{-1}ab$  of  $[a]$  is a factor of  $s$ , either this automorphism is the identity and  $G$  is abelian, or the order of the cyclic transformation group  $R$  is equal to  $s$ . Since the number of elements in the orbit containing  $x$  is equal to  $[R : F_x]$  where  $F_x = \{\psi \in R : \psi(x) = x\}$ , it follows that (47.12) holds, and the corollary is proved.

(47.15) COROLLARY. *Let  $G$  be a metacyclic group satisfying the hypotheses of Corollary 47.14. The number of distinct irreducible representations of  $G$  is equal to*

$$sd + \frac{(m - d)}{s}$$

*where  $d = (r - 1, m)$ .*

This result is immediate from the proof of Theorem 47.11.

The question arises of what can be said about the irreducible  $KG$ -modules for a group  $G$  satisfying the hypotheses of this section, if the condition of Theorem 47.11 is not satisfied. We shall indicate a proof of the fact that *in all cases the irreducible modules of  $G$  are either one dimensional or components of modules  $L^g$ , where  $L$  is a one-dimensional module for the subgroup  $A$ .* We consider the subgroup  $G_1$  of  $G$  consisting of the identity element, and let  $L_1$  be the unique one-dimensional  $G_1$ -module. Then on the one hand,  $L_1^g$  is isomorphic to the left regular module  $\kappa_G KG$ , so that all the irreducible  $G$ -

modules are components of  $L_i^G$ . On the other hand, by Theorem 38.4, we have

$$L_i^G \cong (L_i^A)^G.$$

Then  $L_i^A = \sum \bigoplus M_i$  where the  $M_i$  constitute all irreducible (and hence one-dimensional)  $A$ -modules. Then, by (12.12), we have

$$L_i^G = \sum \bigoplus M_i^G,$$

and our result follows from the theory of completely reducible modules (§ 15).

We shall see later (§ 52) that all the irreducible representations of  $G$  are monomial representations, but it is not as easy to give them explicitly. Their determination has been given by P. Tucker [1].

We conclude this section with some examples to illustrate these theorems.

*Example 1. The Dihedral Group  $D_m$ .* In this case, the defining relations are (see § 7)

$$a^m = 1, \quad b^{-1}ab = a^{-1}, \quad b^2 = 1.$$

Since  $s = 2$ , Corollary 47.14 applies. We have

$$d = (r - 1, m) = \begin{cases} 1 & \text{if } m \text{ is odd} \\ 2 & \text{if } m \text{ is even} \end{cases}.$$

Thus the number of one-dimensional representations is 2 if  $m$  is odd and 4 if  $m$  is even, whereas the number of distinct induced representations  $T_i^G$  is  $(m - 1)/2$  if  $m$  is odd and  $(m - 2)/2$  if  $m$  is even. The matrices  $T_i^G$  are given by

$$a \rightarrow \begin{pmatrix} \zeta^i & 0 \\ 0 & \zeta^{-i} \end{pmatrix}, \quad 1 \leq i \leq m,$$

and

$$b \rightarrow \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

*Example 2. The Generalized Quaternion Group  $Q_m$ .*

In this case, we have (see § 7) for the generators  $a, b$ ,

$$a^{2m} = 1, \quad bab^{-1} = a^{-1}, \quad b^2 = a^{-m}.$$

Again  $s = 2$ , and Corollary 47.14 applies. This time

$$d = (r - 1, 2m) = 2,$$

so there are four one-dimensional representations and  $m - 1$  distinct induced representations  $T_i^g$ . The matrices  $T_i^g$  are given by

$$\begin{aligned} a &\rightarrow \begin{pmatrix} \zeta^i & 0 \\ 0 & \zeta^{-i} \end{pmatrix}, \\ b &\rightarrow \begin{pmatrix} 0 & \zeta^{-im} \\ 1 & 0 \end{pmatrix} \end{aligned}$$

where  $\zeta$  is a primitive  $2m$ th root of 1.

*Example 3.* Finally, we give an example of a metacyclic group which does not satisfy the hypothesis (47.12) of Theorem 47.11. The reader can verify that the group with two generators  $a, b$  satisfying

$$a^{52} = 1, \quad b^{-1}ab = a^3, \quad b^6 = 1$$

is such an example.

### Exercises

1. Let  $F_p$  be the finite field of  $p$  elements where  $p$  is a prime. Let  $G$  be the group of all  $2 \times 2$  triangular matrices

$$\begin{pmatrix} a & b \\ 0 & a^{-1} \end{pmatrix}, \quad a \in F_p, a \neq 0, b \in F_p.$$

Determine all the irreducible representations of  $G$  in the field of complex numbers. (It goes without saying that the results of this section have something to do with the problem.)

2. Apply the tensor product theorem to obtain the irreducible components of the tensor product of two irreducible representations of the dihedral group.

## § 48. A Second Application: Multiplicity-free Representations

In this section, we apply the intertwining number theorem to prove a theorem due to Mackey [3] which gives a sufficient condition for the tensor product of two irreducible  $KG$ -modules to be multiplicity-free in the sense of the following definition. As in §47, we assume that  $K$  is algebraically closed, and  $\text{char } K \nmid [G : 1]$ .

(48.1) **DEFINITION.** A left  $KG$ -module  $M$  is said to be *multiplicity-free* if every irreducible component of  $M$  appears exactly once in a direct decomposition of  $M$  into irreducible submodules.

(48.2) THEOREM (*Mackey*). *Let  $G$  be a group containing an abelian normal subgroup  $A$  of index two. Then the tensor product of any two irreducible  $G$  modules is multiplicity-free.*

PROOF. From what has been said at the end of the previous section, every irreducible  $KG$ -module is either one dimensional or a component of a module  $L^g$  where  $L$  is a one-dimensional  $A$ -module. Because the modules  $L^g$  are two dimensional, the irreducible  $KG$ -modules are therefore either one dimensional or of the form  $L^g$ , for a one-dimensional  $KA$ -module  $L$ . For the rest of the proof we use the language of representations.

We have three cases to consider: the tensor product of two one-dimensional representations, the tensor product of a one-dimensional representation with an irreducible two-dimensional one, and the tensor product of two irreducible two-dimensional representations.

In the first case, the tensor product is again one dimensional and hence irreducible.

For the second case, we shall prove that the tensor product of an irreducible two-dimensional representation  $U$  by a one-dimensional representation  $S$  of a group  $G$  is always irreducible and hence multiplicity-free. To show this let  $M$  be the space of  $U$  and  $L = Kl$  the space of  $S$ . Then every element of  $M \otimes L$  can be expressed uniquely in the form  $m \otimes l$  with  $m \in M$ . If  $U \otimes S$  is reducible, for some non-zero  $m \otimes l \in M \otimes L$  we have

$$(U \otimes S)(g)(m \otimes l) = \xi(g)(m \otimes l) = U(g)m \otimes S(g)l = U(g)S(g)(m \otimes l)$$

where  $\xi(g), S(g) \in K$ . Comparing these expressions, we obtain  $U(g)m = S(g)^{-1}\xi(g)m, g \in G$ , contrary to the assumption that  $U$  is irreducible.

As preparation for the final case, we recall that an irreducible two-dimensional representation  $U$  of  $G$  has the form  $T^g$  where  $T$  is a one-dimensional representation of  $A$ . Let  $g_0 \in G, g_0 \notin A$ . Then every element of  $G$  not in  $A$  belongs to the coset  $g_0A$ . Since  $A$  is abelian, for every  $g \notin A$  and all  $a \in A$ , we have

$$(48.3) \quad g^{-1}ag = g_0^{-1}ag_0.$$

By Corollary 45.5  $T^g$  is irreducible if and only if  $T \neq T^{(g)}$  for all  $g \in G, g \notin A$ , where  $T^{(g)}(a) = T(g^{-1}ag), a \in A$ . By (48.3) the irreducibility of  $T^g$  is equivalent to the single statement

$$(48.4) \quad T \neq T^{(g_0)}.$$

We now consider the tensor product  $T_1^g \otimes T_2^g$  of two irreducible induced representations where  $T_1$  and  $T_2$  are one-dimensional representations of  $A$ . By (48.4) we have

$$(48.5) \quad T_1 \neq T_1^{(g_0)}, \quad T_2 \neq T_2^{(g_0)}.$$

By the tensor product theorem, we obtain

$$T_1^g \otimes T_2^g = (T_1 \otimes T_2)^g \oplus (T_1 \otimes T_2^{(g_0)})^g,$$

whereas the intertwining number theorem asserts that

$$(48.6) \quad i((T_1 \otimes T_2)^g, (T_1 \otimes T_2^{(g_0)})^g) = i(T_1 \otimes T_2, T_1 \otimes T_2^{(g_0)}) + i(T_1 \otimes T_2, (T_1 \otimes T_2^{(g_0)})^{(g_0)}).$$

Since the representations  $T_1$  and  $T_2$  are one dimensional, the tensor products  $T_1 \otimes T_2$ , etc., can be regarded as ordinary products of the functions. By (48.5), we have

$$T_1 T_2 \neq T_1 T_2^{(g_0)}$$

and

$$T_1 T_2 \neq (T_1 T_2^{(g_0)})^{(g_0)}$$

since  $g_0^2 \in A$  implies  $(T_2^{(g_0)})^{(g_0)} = T_2$  and

$$(T_1 T_2^{(g_0)})^{(g_0)} = T_1^{(g_0)} T_2.$$

Therefore, both intertwining numbers on the right side of (48.6) are zero, and we conclude, by (48.6), that  $T_1^g \otimes T_2^g$  is multiplicity-free, provided that the summands  $(T_1 \otimes T_2)^g$  and  $(T_1 \otimes T_2^{(g_0)})^g$  are themselves multiplicity-free. We shall prove more generally that for any one-dimensional representation  $T$  of  $A$ ,  $T^g$  is always multiplicity-free. In fact, by the intertwining number theorem,

$$i(T^g, T^g) = i(T, T) + i(T, T^{(g_0)})$$

which is either 1 if  $T^g$  is irreducible, or 2 if  $T = T^{(g_0)}$ . But when  $T^g$  is reducible, the components are equivalent if and only if  $i(T^g, T^g) = 4$ . Therefore  $T^g$  is multiplicity-free in all cases, and Theorem 48.2 is proved.

We remark that the dihedral groups and the generalized quaternion groups all satisfy the hypotheses of Theorem 48.2.

#### § 49. The Restriction of Irreducible Modules to Normal Subgroups

In the next two sections, we reverse the procedure of starting

from known  $KH$ -modules  $L$ , where  $H$  is a subgroup of  $G$ , and studying the induced module  $L^G$ . Instead, we begin with a fixed irreducible  $KG$ -module  $M$  and ask two questions. First, what is the structure of  $M_H$  when  $H$  is a normal subgroup of  $G$ ? Second, when is  $M$  an induced module  $L^G$ , where  $L$  is some  $KH$ -module and  $L$  and  $H$  may depend upon  $M$ ?

The first question was answered for group characters by Frobenius ([1], p. 506). Our approach to both questions follows a paper by Clifford [1] in which other historical remarks concerning these problems may be found.

*Throughout this section,  $H$  denotes a normal subgroup of  $G$  and  $K$  an arbitrary field.*

(49.1) **DEFINITION.** Let  $L$  be a left  $KH$ -module. For a fixed  $g \in G$ , let  $L^{(g)}$  be the left  $KH$ -module whose underlying vector space is  $L$  and on which  $H$  acts according to the rule

$$h * l = g^{-1} h g l, \quad l \in L,$$

where  $h * l$  denotes the module operation in  $L^{(g)}$  and  $hl$  the operation in  $L$ . Such a  $KH$ -module  $L^{(g)}$  is called a *conjugate* of  $L$  and the representation  $T^{(g)}$  afforded by  $L^{(g)}$ , a *conjugate* of the representation  $T$  afforded by  $L$ . We have, for all  $h \in H$ ,

$$T^{(g)}(h) = T(g^{-1}hg).$$

(49.2) **THEOREM (Clifford).** *Let  $M$  be an irreducible  $KG$ -module where  $K$  is an arbitrary field, and let  $H \triangle G$ . Then  $M_H$  is a completely reducible  $KH$ -module, and the irreducible  $KH$ -submodules of  $M_H$  are all conjugates of each other.*

**PROOF.** Let  $L$  be an irreducible  $KH$ -submodule of  $M_H$ . For any  $g \in G$ ,  $gL$  is also a  $KH$ -submodule of  $M_H$ , since for all  $h \in H$  we have

$$h(gL) = g(g^{-1}hgl) \subset gL,$$

where  $g^{-1}hg \in H$  because  $H \triangle G$ . Moreover, the irreducibility of  $L$  implies that  $gL$  is also an irreducible  $KH$ -module.

Next we prove that  $gL \cong L^{(g)}$  as  $KH$ -modules. The mapping

$$\varphi: l \mapsto gl, \quad l \in L^{(g)},$$

is a  $K$ -isomorphism of  $L^{(g)}$  onto  $gL$ , and for all  $h \in H$ , we have

$$\varphi(h * l) = \varphi(g^{-1}hgl) = gg^{-1}hgl = hgl = h\varphi(l).$$

This proves our assertion.

Finally we see that

$$\sum_{g \in G} gL$$

is a  $KG$ -submodule of  $M$  different from zero. Therefore

$$M = \sum_{g \in G} gL$$

because  $M$  is an irreducible  $KG$ -module. The  $KH$ -submodules  $gL$  are all irreducible and conjugates of one another, and  $M_H$  is completely reducible by Theorem 15.3. This completes the proof of Clifford's theorem.

We remark that Clifford's theorem and the proof we have given are valid even if  $G$  and  $H$  are infinite groups.

Clifford's theorem tells us that if we know an irreducible  $KH$ -submodule  $L$  of an irreducible  $KG$ -module  $M$ , we know all the other irreducible  $KH$ -submodules of  $M$ , but it does not tell us how to find the irreducible module  $L$ . For example, we have determined in Chapter IV all the irreducible  $KS_n$ -modules where  $S_n$  is the symmetric group, and Clifford's theorem tells us something about the irreducible  $KA_n$ -modules obtained from the irreducible  $KS_n$ -modules, where  $A_n$  is the alternating group. It turns out that some irreducible  $KS_n$ -modules are also irreducible  $KA_n$ -modules whereas some are not, and the complete information on this point has been given by Frobenius [2]. Some interesting connections between this problem and other seemingly unrelated ideas have been found by Kostant [1].

For application in the next section, we shall work out a sharper form of Clifford's theorem as follows. From Clifford's theorem and by Theorem 15.3, we have

$$(49.3) \quad M_H = \sum_{i=1}^s g_i L \quad (\text{direct sum})$$

where the  $KH$ -modules  $g_i L$  are certain conjugates of  $L$ . Let us suppose that  $\{g_1 L, \dots, g_r L\}$  form a maximal set of non-isomorphic  $KH$ -modules among the  $\{g_i L\}$ ,  $1 \leq i \leq s$ . For each  $i$ ,  $1 \leq i \leq r$ , let  $M_i$  be the sum of all the conjugates  $g_j L$ ,  $1 \leq j \leq s$ , such that  $g_j L \cong g_i L$  as left  $KH$ -modules. Then

$$(49.4) \quad M_H = M_1 \oplus \cdots \oplus M_r.$$

Moreover, let  $L' = gL$  be an arbitrary conjugate of  $L$ . Then, by the Jordan-Hölder theorem,  $L' \cong g_i L$  for some  $g_i$ ,  $1 \leq i \leq r$ . We assert that  $L' \subset M_i$ . If not then for some  $l \in L'$  we have

$$l = l_1 + \cdots + l_r, \quad l_i \in M_i,$$

and some  $l_j$ ,  $j \neq i$ , is different from zero. Then the mapping  $l \rightarrow l_j$ ,  $l \in L'$ , is a  $KH$ -homomorphism of  $L'$  into  $M_j$  which is different from zero. Therefore, since  $L'$  is irreducible,  $M_j$  contains a composition factor isomorphic to  $g_i L$ , contrary to the way  $M_j$  was defined. We have thus proved that the  $KH$ -submodule  $M_i$  is the sum of all conjugates  $gL$ ,  $g \in G$ , such that  $gL \cong g_i L$ , and it follows that the modules  $M_i$  are independent of the particular decomposition (49.3) of  $M$  from which we start.

(49.5) **DEFINITION.** The uniquely determined  $KH$ -submodules  $M_i$  of  $M_H$  defined in (49.4) are called the *homogeneous components* of  $M_H$ . Each is a direct sum of  $KH$ -isomorphic conjugates of  $L$ .

(49.6) *For any  $g \in G$  and  $M_i$ ,  $1 \leq i \leq r$ , we have  $gM_i = M_j$  for some  $j$ . Moreover,  $G$  acts as a transitive permutation group on the set  $\{M_1, \dots, M_r\}$ .*

**PROOF.** For the first assertion, it is sufficient to prove that, if  $g_1 L \cong g_2 L$  as  $KH$ -modules, then  $gg_1 L \cong gg_2 L$ . Let  $\varphi: g_1 L \rightarrow g_2 L$  be a  $KH$ -isomorphism. Then  $g\varphi g^{-1}: gg_1 L \rightarrow gg_2 L$  is a vector space isomorphism of  $gg_1 L$  onto  $gg_2 L$ , and, for all  $h \in H$  and  $gg_1 l \in gg_1 L$ , we have

$$\begin{aligned} (g\varphi g^{-1})[h(gg_1 l)] &= g\varphi g^{-1}[(gg_1)(gg_1)^{-1}h(gg_1)l] \\ &= g\varphi[(g^{-1}hg)g_1 l] = g(g^{-1}hg)\varphi(g_1 l) = h(g\varphi g^{-1}(gg_1 l)) \end{aligned}$$

since  $g^{-1}hg \in H$  and  $\varphi$  is a  $KH$ -isomorphism. For the second statement, it is enough to observe that, if  $M_i$  is the homogeneous component containing  $L$ , then  $M_i = g_i M_i$  for some  $g_i \in G$  because of the way  $M_i$  was defined. This completes the proof.

Since  $gM_i = M_j$  implies that  $M_i$  and  $M_j$  have the same number of irreducible components, we can state as an immediate consequence of (49.6):

(49.7) **THEOREM.** *Let  $H$  be a normal subgroup of  $G$ , and let  $M$  be an irreducible  $KG$ -module, and  $L$  an irreducible  $KH$ -submodule of  $M_H$ . Then*

$$(49.8) \quad M_H \cong e(L^{(g_1)} + \cdots + L^{(g_r)})$$

where  $\{L^{(g_1)}, \dots, L^{(g_r)}\}$  are a full set of non-isomorphic conjugates of  $L$ , and  $e$  is a positive integer. [Here of course (49.8) means that  $M_H$  is isomorphic to a direct sum of  $e$  copies of  $L^{(g_1)} + \cdots + L^{(g_r)}$ .]

*Exercise*

1. Show that the number  $r$  of distinct homogeneous components is equal to the index  $[G : H^*]$  where  $H^*$  is the subgroup of  $G$  consisting of all  $g \in G$  such that  $gL \cong L$ . We call  $H^*$  the *inertia group* of  $L$ .

### § 50. Imprimitive Modules

Throughout this section,  $K$  denotes an arbitrary field. We shall take up the second question raised in § 49, namely, when a  $KG$ -module  $M$  can be identified with an induced module  $L^g$  for some  $KH$ -module  $L$  where  $H$  is a subgroup of  $G$ . The method depends on the following definition, which leads to a new characterization of induced modules:

(50.1) **DEFINITION.** A left  $KG$ -module  $M$  is called an *imprimitive module* if there exist  $K$ -subspaces  $M_1, \dots, M_r$  of  $M$  such that  $M$  is the direct sum of the  $\{M_i\}$ , and for any  $g \in G$ , left multiplication by  $g$  permutes the spaces  $\{M_i\}$  among themselves. In other words, for each  $i$ ,  $gM_i$  is identical with some space  $M_j$ . An imprimitive module  $M$  is said to be *transitive* if for any pair  $M_i$  and  $M_j$ , there is a  $g \in G$  such that  $gM_i = M_j$ . The subspaces  $\{M_i\}$  are called a *system of imprimitivity* for  $M$ .

We already know how to construct imprimitive modules. Indeed, let  $H$  be a subgroup of  $G$ , let  $L$  be a left  $KH$ -module, and let  $M = L^g$ . Then by (12.26) we have  $L^g = \sum_{i=1}^m g_i \otimes L$ , where the  $g_i$  are representatives of the distinct left cosets of  $H$  in  $G$ . Upon setting  $M_i = g_i \otimes L$ ,  $1 \leq i \leq m$ , it is clear that  $L^g$  is a transitive imprimitive module with system of imprimitivity  $M_1, \dots, M_m$ . Our next result asserts that, in a sense, this is the only example of a transitive imprimitive module.

(50.2) *Let  $M$  be a transitive imprimitive  $KG$ -module with system of imprimitivity  $\{M_1, \dots, M_r\}$ . Let  $H$  be the subgroup of  $G$  consisting of all  $h \in G$  such that  $hM_1 = M_1$ . Then  $M_1$  is a left  $KH$ -module, and  $M \cong M_1^g$ .*

**PROOF.** Because of the transitivity, each  $M_i$  can be expressed in the form  $g_i M_1$  for some  $g_i \in G$ . Moreover,  $g_i M_1 = g_j M_1$  if and only if the left cosets  $g_i H$  and  $g_j H$  are identical. Therefore  $M$  is a direct sum of subspaces  $g_i M_1$  where the  $\{g_i\}$  form a set of left coset representatives of  $H$  in  $G$ , and by Lemma 44.1, we have  $M \cong M_1^g$ .

as required.

For example, consider the situation described in Exercise 43.1. We are given a vector space  $M$  over  $K$  with basis  $\{m_1, \dots, m_n\}$  and a monomial representation  $T: G \rightarrow GL(M)$  such that for each  $g \in G$ ,  $T(g)m_i = \alpha_{ji}(g)m_j$ ,  $1 \leq i \leq n$ , where  $j$  is some integer depending on  $i$  and  $g$ . Then the one-dimensional spaces  $\{Km_1, \dots, Km_n\}$  form a system of imprimitivity. If we have a transitive system of imprimitivity, Theorem 50.2 asserts that  $T$  is an induced monomial representation.

In the more general case of an imprimitive but not necessarily transitive module, we have the following result:

(50.3) *Let  $M$  be an imprimitive left  $KG$ -module with system of imprimitivity  $\{M_1, \dots, M_r\}$ . Then  $M$  is a direct sum of induced modules  $\{M_{i_\alpha}^G\}$  where the  $\{M_{i_\alpha}\}$  are representatives of the orbits of the set  $\{M_1, \dots, M_r\}$  under the permutation group  $G$ .*

**PROOF.** We regard  $G$  as a group of permutations on the set  $X = \{M_1, \dots, M_r\}$  where the  $\{M_i\}$  form a system of imprimitivity for  $M$ . Then  $X$  can be decomposed into disjoint orbits relative to  $G$ . The sum  $\hat{M}$  of the  $M_i$  belonging to any one orbit is a transitive imprimitive  $KG$ -module, and by (50.2),  $\hat{M}$  is an induced module. Since  $M$  is the direct sum of the  $\hat{M}$  taken over the distinct orbits,  $M$  is a direct sum of induced modules, and (50.3) is proved.

As a corollary, we have at once

(50.4) **COROLLARY.** *An irreducible (or indecomposable) imprimitive  $KG$ -module is transitive. In particular, any irreducible monomial representation is an induced monomial representation.*

Now we return to the situation considered in Clifford's theorem. We let  $G$  be a group,  $H$  a normal subgroup, and  $M$  an irreducible  $KG$ -module. Then we have  $M = \sum_{g \in G} gL$  where  $L$  is an irreducible  $KH$ -submodule of  $M$ . Let  $M_i$  be the sum of all the irreducible  $KH$ -modules  $gL$  which are  $KH$ -isomorphic to a fixed module  $g_i L$ . The distinct  $KH$ -submodules  $M_i$  obtained in this way, by taking all possible choices of  $g_i \in G$ , are finite in number, and their direct sum is  $M$ . In § 49 we called them the *homogeneous components* of the completely reducible  $KH$ -module  $M_H$ . Our first main result of this section is the following restatement of (49.4) and (49.6):

(50.5) **THEOREM.** *Let  $M$  be an irreducible  $KG$ -module, and let  $\{M_1, \dots, M_r\}$  be the homogeneous components of  $M_H$ , where  $H$  is a normal subgroup of  $G$ . Then  $M$  is a transitive imprimitive  $KG$ -module*

with system of imprimitivity  $M_1, \dots, M_r$ .

(50.6) COROLLARY. Keeping the above notation, let  $H^*$  be the subgroup of  $G$  consisting of all elements  $h \in G$  such that  $hM_1 = M_1$  where  $M_1$  is one of the homogeneous components. Then  $M_1$  is an indecomposable  $KH^*$ -module, and  $M = M_1^g$ .

The proof is immediate by Theorems 50.5, 50.2 and 50.4.

(50.7) COROLLARY (Blichfeldt). Let  $G$  be a finite subgroup of  $GL(M)$  for some vector space  $M$  over an algebraically closed field  $K$  such that  $\text{char } K \nmid [G : 1]$ , and let  $M$  be an irreducible  $KG$ -module. Suppose that  $G$  contains an abelian normal subgroup  $A$  not contained in the center of  $G$ . Then there exists a proper subgroup  $H^*$  of  $G$ , and an irreducible  $KH^*$ -submodule  $L$  of  $M$ , such that  $M \cong L^g$ .

PROOF. By Clifford's theorem and the facts that  $A$  is abelian and  $K$  is algebraically closed,  $M_A$  is a direct sum of one-dimensional  $KA$ -submodules which are all conjugates of each other. If all the irreducible  $KA$ -submodules of  $M_A$  are isomorphic, then, for each  $a \in A$ ,  $a_L$  has exactly one characteristic value  $\xi_a$ , and we have  $a_L = \xi_a L$ . Then  $A$  is contained in the center of  $G$ , contrary to assumption. Therefore there is more than one homogeneous component of the module  $M_A$ , and the subgroup  $H^*$  of Corollary 50.6 is different from  $G$ . The homogeneous components of  $M_A$  are irreducible  $KH^*$ -modules, because Corollary 50.6 asserts that the homogeneous components are indecomposable, and the fact that  $\text{char } K \nmid [G : 1]$  implies that every indecomposable  $KH^*$ -module is irreducible. The statement that  $M \cong L^g$  for an irreducible  $KH^*$ -module  $L$  is the content of Corollary 50.6, and Blichfeldt's theorem is proved.

## § 51. Projective Representations

We continue the investigations of the last two sections. This time, however, we assume that  $K$  is algebraically closed and of characteristic which is zero or is prime to the order of  $G$ . We consider a normal subgroup  $H$  of  $G$  and an irreducible  $KG$ -module  $M$  such that  $M_H$  is a homogeneous  $KH$ -module. In other words, letting  $L$  be an irreducible  $KH$ -submodule of  $M_H$ , we have

$$M = \sum_{g \in G} gL \quad (\text{not necessarily a direct sum}),$$

where all the conjugates  $\{gL\}$  are  $KH$ -isomorphic to  $L$ . In the terminology of Corollary 50.6,  $M$  corresponds to  $M_1$ ,  $G$  to  $H^*$ , and  $H$  to  $H$ .

For example, let  $G$  be a direct product  $G = G_1 \times G_2$ , and let  $M$  be an irreducible  $KG$ -module. Let  $L$  be an irreducible  $KG_1$ -submodule of  $M$ . Then, from Clifford's theorem we obtain

$$M = \sum_{(g_1, g_2) \in G} (g_1, g_2)L.$$

We have  $(g_1, g_2)L = (1, g_2)(g_1, 1)L = (1, g_2)L$ , and it is easily checked that all the  $KG_1$ -submodules  $(1, g_2)L$  are  $KG_1$ -isomorphic. Thus in what might be viewed as the simplest case, the results of the previous section provide no definitive information at all concerning the structure of  $M$ . The main result of this section is a far-reaching generalization of the ideas necessary to treat this example.

Returning to the general situation, let  $R$  be the representation of  $H$  afforded by  $L$  and  $S$  the representation of  $G$  afforded by  $M$ . We shall prove that

$$S = W \otimes X$$

where  $W$  can be viewed as a representation of  $G/H$ , and  $X$  is a representation of  $G$  which is obtained rather simply from the representation  $R$  of  $H$ . For our result, we must adopt a more general concept of representation than that used until now.

We begin with the following definition:

(51.1) **DEFINITION.** Let  $G$  be a finite group. A *projective representation* of  $G$  is a map  $T: G \rightarrow GL(M)$ , where  $M$  is a vector space over  $K$ , such that

$$T(1) = 1_M$$

and

$$T(s)T(t) = T(st)\alpha(s, t)$$

for all  $s, t \in G$ , where  $\alpha(s, t)$  is a non-zero element of  $K$  depending on the pair  $(s, t)$ . The function  $(s, t) \mapsto \alpha(s, t)$  is called the *factor set* of the representation. The projective representation  $T$  is called *irreducible* if there are no non-trivial subspaces of  $M$  which are sent into themselves by all the transformations  $T(g)$ ,  $g \in G$ .

Some elementary properties of projective representations are given in the exercises at the end of this section; later (in §53) we prove one of the main theorems concerning them due to Schur

[1]. Our immediate purpose is to show that they occur in an unavoidable way in the study of ordinary representations.

We require, first, two preliminary results.

(51.2) LEMMA. *Let  $R$  be an irreducible representation of  $H$  afforded by a  $KH$ -module  $L$  and let  $M = U \otimes_K L$  where  $U$  is some finite-dimensional vector space over  $K$ . Let  $A$  be a linear transformation of  $M$  such that*

$$A(1 \otimes R(h)) = (1 \otimes R(h))A$$

*for all  $h \in H$ . Then  $A = B \otimes 1$  for some linear transformation  $B$  on  $U$ .*

PROOF. Let  $\{u_1, \dots, u_m\}$  be a basis for  $U$  over  $K$ . Then for all  $l \in L$ , we have

$$(51.3) \quad A(u_i \otimes l) = \sum_{j=1}^m u_j \otimes A_{ji}l, \quad 1 \leq i \leq m,$$

where the mappings  $A_{ji} \in \text{Hom}_K(L, L)$ . For all  $h \in H$  we have

$$\begin{aligned} A(1 \otimes R(h))(u_i \otimes l) &= A(u_i \otimes R(h)l) = \sum_{j=1}^m u_j \otimes A_{ji}R(h)l \\ &= (1 \otimes R(h))A(u_i \otimes l) = \sum_{j=1}^m u_j \otimes R(h)A_{ji}l. \end{aligned}$$

Because the  $\{u_i\}$  are linearly independent, we have

$$R(h)A_{ji} = A_{ji}R(h), \quad h \in H, 1 \leq i, j \leq m.$$

By Schur's lemma, since  $K$  is algebraically closed, we have  $A_{ji} = \alpha_{ji}1_L$  for some  $\alpha_{ji} \in K$ . Define a linear transformation  $B$  on  $U$  by

$$Bu_i = \sum_{j=1}^m \alpha_{ji}u_j, \quad 1 \leq i \leq m.$$

Then (51.3) implies that  $A = B \otimes 1$  as required.

(51.4) LEMMA. *Let  $M = U \otimes L$  as in Lemma 51.2, and let  $R$  and  $R'$  be equivalent irreducible representations of  $H$  on  $L$ . Let  $X$  be an invertible linear transformation on  $L$  such that*

$$(51.5) \quad X^{-1}R(h)X = R'(h), \quad h \in H,$$

*and let  $S$  be an invertible linear transformation on  $M$  such that*

$$(51.6) \quad S^{-1}(1 \otimes R(h))S = 1 \otimes R'(h), \quad h \in H.$$

*Then there exists an invertible linear transformation  $Y$  on  $U$  such*

that

$$S = Y \otimes X.$$

PROOF. Let  $X' = 1 \otimes X$ , then by (51.5) we have

$$(X')^{-1}(1 \otimes R(h))(X') = 1 \otimes R'(h), \quad h \in H,$$

and upon comparing this equation with (51.6), we obtain

$$S(X')^{-1}(1 \otimes R(h))X'S^{-1} = 1 \otimes R(h).$$

Lemma 51.2 thus implies that

$$S(X')^{-1} = Y \otimes 1$$

for some linear transformation  $Y$  on  $U$ . Hence

$$S = (Y \otimes 1)X' = Y \otimes X,$$

and Lemma 51.4 is proved.

Now we come the main theorem of this section.

(51.7) THEOREM. *Let  $H$  be a normal subgroup of  $G$ , and let  $S$  be an irreducible representation of  $G$ . Let  $R$  be an irreducible component of the restriction of  $S$  to  $H$ , and assume that  $R$  is equivalent to all its conjugates  $R^{(g)}$ ,  $g \in G$ . Then, for all  $g \in G$ ,*

$$(51.8) \quad S(g) = Y(g) \otimes X(g)$$

*where  $Y$  and  $X$  are irreducible projective representations of  $G$  such that the degree of  $X$  is equal to the degree of  $R$  and  $Y(h) = 1$  for  $h \in H$ , so that  $Y$  can be viewed as a projective representation of the factor group  $G/H$ . The representations  $Y$  and  $X$  can be taken to be ordinary representations of  $G$  if there exists an ordinary representation  $X$  of  $G$  such that  $X(h) = R(h)$  for all  $h \in H$ .*

PROOF. By Theorem 49.2,  $S$  is the direct sum of a certain number, say  $t$ , of conjugates of  $R$ , and these are all equivalent to  $R$ . Let  $U$  be a  $t$ -dimensional vector space over  $K$ , and form the vector space  $U \otimes_K L$ , where  $L$  is the representation space of  $R$ . Then  $1 \otimes R$  defines a representation of  $H$  on  $U \otimes_K L$  which is the direct sum of  $t$  copies of  $R$ . Let  $l_1, \dots, l_d$  be a basis for  $L$ . Then there exists a basis  $\{m_{ij}\}$ ,  $1 \leq i \leq t$ ,  $1 \leq j \leq d$ , for the representation space  $M$  of  $S$  such that for a fixed  $i$ ,  $1 \leq i \leq t$ ,  $\sum_j \xi_j l_j \rightarrow \sum_j \xi_j m_{ji}$ ,  $\xi_j \in K$ , defines a  $KH$ -isomorphism of  $L$  onto a submodule of  $M_H$ . Let  $\{u_1, \dots, u_t\}$  be a basis of  $U$ . Then we can make  $U \otimes_K L$  into a  $KG$ -module by requiring that the mapping  $\sum_i \xi_i (u_i \otimes l_i) \rightarrow \sum_i \xi_i m_{ii}$  be a  $KG$ -isomorphism of  $U \otimes_K L$  onto  $M$ . If we again denote by  $S$  the representation afforded by  $U \otimes_K L$ , then

$$(51.9) \quad S(h) = 1 \otimes R(h), \quad h \in H.$$

Now let  $g$  be a fixed element of  $G$ . Then the conjugates  $R^{(g)}$  and  $R$  are equivalent, and there exists an invertible linear transformation  $X(g)$  on  $L$  such that

$$(51.10) \quad R(g^{-1}hg) = R^{(g)}(h) = X(g)^{-1}R(h)X(g), \quad h \in H.$$

If  $g$  is in  $H$ , we may take  $X(g) = R(g)$ . In general, the mapping  $g \rightarrow X(g)$  is not a representation of  $G$  on  $L$ , but it is always a projective representation. In fact, let  $g_1, g_2 \in G$ ; we have

$$X(g_1g_2)^{-1}R(h)X(g_1g_2) = R^{(g_1g_2)}(h) = X(g_2)^{-1}X(g_1)^{-1}R(h)X(g_1)X(g_2).$$

From this equation we obtain for  $h \in H$ ,

$$X(g_1)X(g_2)X(g_1g_2)^{-1}R(h) = R(h)X(g_1)X(g_2)X(g_1g_2)^{-1}.$$

By Schur's lemma, since  $R$  is irreducible and  $K$  is algebraically closed, there exists an element  $\alpha(g_1, g_2) \neq 0$  in  $K$  such that

$$X(g_1)X(g_2)X(g_1g_2)^{-1} = \alpha(g_1, g_2)1_L,$$

and we have

$$X(g_1)X(g_2) = X(g_1g_2)\alpha(g_1, g_2).$$

Since  $1 \in H$ , we may take  $X(1) = 1$ , and we have proved that  $X$  is a projective representation of  $G$  on the space  $L$ .

Now we investigate the decomposition of the representation  $S$  on  $M$ . For all  $g \in G$  we have because of (51.9) the result that

$$(51.11) \quad S(g^{-1}hg) = S(g)^{-1}(1 \otimes R(h))S(g) = 1 \otimes R^{(g)}(h).$$

We can then apply Lemma 51.4 to conclude that there exists an invertible linear transformation  $Y(g)$  on  $U$  such that

$$(51.12) \quad S(g) = Y(g) \otimes X(g)$$

on  $M$ .

Because  $X$  is a projective representation of  $G$  with factor set  $\{\alpha(g_1, g_2)\}$  and  $S$  is an ordinary representation, (51.12) implies that  $Y$  is a projective representation of  $G$  with factor set  $\{\alpha(g_1, g_2)^{-1}\}$ . Moreover, for  $h \in H$  we have by (51.12) and (51.9),

$$S(h) = 1 \otimes R(h) = Y(h) \otimes X(h);$$

hence  $Y(h) = 1$  for all  $h \in H$ . The projective representations  $Y$  and  $X$  are irreducible, because a reduction of either one would imply a reduction of  $S$ , contrary to the hypothesis that  $S$  is irreducible.

Finally, let us suppose that there exists a representation  $X$  of  $G$  on  $L$  such that  $X(h) = R(h)$  for  $h \in H$ . Then (51.10) holds for this choice of  $X(g)$ , and we have (51.12) as before. This time, however, the fact that  $X(g)$  is an ordinary representation implies that  $Y(g)$  is also an ordinary representation. This completes the proof of Theorem 51.7.

(51.13) COROLLARY. *Let  $G = G_1 \times G_2$  be the direct product of  $G_1$  and  $G_2$ . Then every irreducible representation  $S$  of  $G$  can be expressed as an outer tensor product*

$$(51.14) \quad S = T_1 \# T_2,$$

where  $T_i$  is an irreducible representation of  $G_i$ ,  $i = 1, 2$ .

PROOF. (See Exercise 27.2.) We have already observed earlier in this section that if we let  $T_2$  be an irreducible  $KG_2$ -component of  $S$ , then  $T_2$  is equivalent to all its conjugates. Define

$$T_2(g) = T_2(g_2)$$

where  $g = (g_1, g_2) \in G$ . Then  $T_2$  is a representation of  $G$ , and, as in the proof of Theorem 51.7, we have, for all  $g = (g_1, g_2) \in G$ ,

$$S(g) = T_1(g) \otimes T_2(g) = T_1(g_1) \otimes T_2(g_2)$$

where  $T_1(g) = 1$  if  $g \in G_1$  so that we may identify  $T_1(g)$  with  $T_1(g_1)$ . Since  $T_2$  is an ordinary representation of  $G$ , both  $T_1$  and  $T_2$  are irreducible ordinary representations, and the corollary is proved.

We conclude this section with a sufficient condition for the extension described in the last statement of Theorem 51.7 to exist; this result is suggested by the preceding corollary where we investigated the representations of a direct product.

(51.15) THEOREM (Mackey). *Let  $H$  be an abelian normal subgroup of  $G$  such that  $G$  is a semi-direct product of  $H$  and  $G/H$ . Let  $R: H \rightarrow GL(V)$  be an irreducible representation of  $H$  such that  $R$  is equivalent to all its conjugates  $R^{(g)}$ ,  $g \in G$ . Then there exists a representation  $X: G \rightarrow GL(V)$  such that  $X(h) = R(h)$  for all  $h \in H$ .*

PROOF. The hypothesis implies that there exists a subgroup  $B$  of  $G$  whose elements form a complete set of coset representatives for the left cosets of  $H$  in  $G$ . We can express any  $g \in G$  uniquely in the form  $g = bh$ ,  $b \in B$ ,  $h \in H$ . We then define

$$X(g) = R(h).$$

Because  $H$  is abelian,  $R$  has degree 1, and the fact that  $R \cong R^{(g)}$  for all  $g \in G$  implies  $R(h) = R(ghg^{-1})$  for all  $g \in G$ . Then if  $g_i = b_i h_i$ ,  $i = 1, 2$ ,

$$\begin{aligned} X(g_1 g_2) &= X(b_1 h_1 b_2 h_2) = X(b_1 b_2 b_2^{-1} h_1 b_2 h_2) \\ &= R(b_2^{-1} h_1 b_2 h_2) = R(b_2^{-1} h_1 b_2) R(h_2) \\ &= R(h_1) R(h_2) = X(g_1) X(g_2), \end{aligned}$$

and  $X$  is indeed a representation of  $G$  with the required property.

For groups satisfying the hypotheses of Theorem 51.15, the results of the last three sections provide a complete reduction of the problem of constructing representations of  $G$  to the corresponding problem for subgroups and their homomorphic images. We shall leave it to the reader to check this assertion; probably the most important observation to be made is that the subgroup  $H^*$  which appears in Corollary 50.6, is itself a split extension of  $H$  so that Theorem 51.15 can be applied to  $H^*$ . On the other hand, the discussion in §47 shows that it is by no means necessary for  $G$  to be a split extension of  $H$  in order to compute the representations of  $G$  in terms of the representations of subgroups and homomorphic images.

In the general case, it should be mentioned that the theorems of the last three sections all hold, with suitable interpretations, for projective representations, so that, if we enlarge the scope of our whole discussion to include projective representations from the beginning, we obtain a reduction of the representations of any group extension to the representations of subgroups and their homomorphic images (see Mackey [4]).

### *Exercises*

1. The center  $Z^*$  of the group  $GL(M)$  is the set of scalar multiples of the identity transformation. The group  $GL(M)/Z^*$  is called the projective general linear group  $PGL(M)$  on  $M$ . Let  $\pi: GL(M) \rightarrow PGL(M)$  be the natural mapping. Prove that if  $T: G \rightarrow GL(M)$  is a projective representation of a group  $G$ , then  $\pi T$  is a homomorphism of  $G$  into  $PGL(M)$ . Conversely, prove that if  $\rho$  is a homomorphism of  $G$  into  $PGL(M)$  and if for each  $g \in G$  we select a unique element  $T(g)$  in the coset  $\pi^{-1}(g)$ , choosing  $T(1) = 1$ , then  $g \rightarrow T(g)$  is a projective representation of  $G$  on the space  $M$ .

2. Two projective representations  $T_i: G \rightarrow GL(M_i)$ ,  $i = 1, 2$ , are said to be *equivalent* if there exists a vector space isomorphism  $U: M_1 \rightarrow M_2$ , and a function  $g \rightarrow \beta(g)$  of  $G$  into the set of non-zero elements of  $K$ , such that

$$T_2(g)U = UT_1(g)\theta(g), \quad g \in G.$$

The factor sets of equivalent projective representations are said to be equivalent. Work out this condition explicitly. What is the condition that a projective representation be equivalent to an ordinary representation? What condition must a function  $(g_1, g_2) \rightarrow \alpha(g_1, g_2)$  of  $G \times G \rightarrow K$  satisfy in order that a mapping  $g \rightarrow T(g)$  of  $G \rightarrow GL(V)$  such that

$$T(g_1g_2) = T(g_1)T(g_2)\alpha(g_1, g_2)$$

define a projective representation of  $G$ ?

3. Prove that a projective representation of a finite group  $G$  in a field whose characteristic is zero or prime to the order of  $G$  is completely reducible.  
(Hint: Imitate the proof of Maschke's theorem.)

4. Let  $\widehat{Q}$  be the algebra of real quaternions with the basis  $1, i, j, k$  such that  $i^2 = j^2 = k^2 = -1$ ,  $ij = k = -ji$ ,  $jk = i = -kj$ ,  $ki = j = -ik$ . Let  $q \rightarrow q_L$  be the regular representation of  $\widehat{Q}$ . Let  $G$  be the "four group" consisting of elements  $1, a, b, c$  such that  $a^2 = b^2 = c^2 = 1$ . Prove that

$$1 \rightarrow 1_L, \quad a \rightarrow i_L, \quad b \rightarrow j_L, \quad c \rightarrow k_L,$$

defines an irreducible projective representation of  $G$  on  $\widehat{Q}$  of degree 4.

5. (Mackey.) Let  $G$  be the group of order 8 consisting of the quaternions  $\{\pm 1, \pm i, \pm j, \pm k\}$  as in Exercise 4. Show that  $H = \{\pm 1\}$  is the center of  $G$  and that  $-1 \in [G, G]$ . Let  $R$  be a one-dimensional representation of  $H$  such that  $R(-1) \neq 1$ . Show that there is no one-dimensional representation  $X$  of  $G$  such that  $X(h) = R(h)$ ,  $h \in H$ . [See Theorem 51.15.] Of course what happens in this case is that  $G$  is not a semi-direct product of  $H$  and  $G/H$ .

6. Prove that the tensor product of two projective representations is a projective representation.

## § 52. Applications

We shall prove first that all the irreducible representations of a nilpotent group are monomial representations. The converse of this result is false as the results of § 47 show. We do prove at least that, if all the irreducible representations of a group  $G$  are monomial, then  $G$  is solvable.

We begin with a few preliminary remarks. We have defined a monomial representation of  $G$  as an induced representation  $T^g$  where  $T$  is a one-dimensional representation of a subgroup  $H$  of  $G$ . Notice that one-dimensional representations of  $G$  are themselves monomial representations according to this definition. In this section,  $K$  denotes an algebraically closed field whose characteristic does not divide  $[G : 1]$ .

(52.1) THEOREM. *Let  $G$  be a finite nilpotent group. Then every irreducible  $K$ -representation of  $G$  is a monomial representation.*

PROOF. We use induction on the order of  $G$ , and observe that the result is clear if  $G$  is abelian. We may assume, therefore, that  $G$  is not abelian and that the theorem is true for any nilpotent group smaller than  $G$ . In the language of modules, we have to prove that any irreducible  $KG$ -module  $M$  can be expressed as an induced module  $P^G$ , where  $P$  is a one-dimensional  $KH$ -module for some subgroup  $H$  of  $G$ . The mapping  $g \rightarrow g_L$ , where  $g_L$  is the linear transformation  $m \rightarrow gm$  of  $M$ , is a homomorphism of  $G$  onto a nilpotent subgroup  $G_L$  of  $GL(M)$ , and  $M$  is an irreducible  $KG_L$ -module. If  $g \rightarrow g_L$  has a non-trivial kernel, then  $[G_L : 1] < [G : 1]$ , and by the induction hypothesis, there exists a subgroup  $H_L$  of  $G_L$  and a one-dimensional  $KH_L$ -submodule  $P$  of  $M$  such that  $M = P^{g_L}$ . Letting  $g_{1L}, \dots, g_{tL}$  be a set of left coset representatives of  $H_L$  in  $G_L$ , we have  $M = \sum^t g_{iL}P$  (vector space direct sum). Now let  $H$  be the subgroup of  $G$  consisting of all  $h \in G$  such that  $h_L \in H_L$ , and let  $g_1, \dots, g_t$  be elements of  $G$  which map onto  $g_{1L}, \dots, g_{tL}$ , respectively. Then  $\{g_1, \dots, g_t\}$  is a set of left coset representatives of  $H$  in  $G$ , and  $M$  is a vector space direct sum  $\sum^t g_i P$ , where  $P$  is a one-dimensional  $KH$ -module. We have  $M = P^G$  by (44.1).

We may therefore assume that  $g \rightarrow g_L$  is an isomorphism of  $G$  onto  $G_L$ , and we shall identify  $G$  with  $G_L$ . Since  $G$  is nilpotent and not abelian,  $G$  has a nontrivial center  $C \neq G$ . Moreover,  $G$  has a normal subgroup  $C_1$  properly containing  $C$  such that  $[C_1, G] \subset C$ . There exists a subgroup  $H$  of  $G$  such that  $C_1 \supset H \supset C$  and  $H/C$  is cyclic and not equal to (1). It follows that  $H$  is an abelian normal subgroup not contained in the center. By Blichfeldt's theorem [Corollary 50.7], there exists a proper subgroup  $H^*$  of  $G$  and an irreducible  $KH^*$ -submodule  $M_1$  of  $M$  such that  $M = M_1^G$ . Since  $H^*$  is a proper subgroup of  $G$  and is nilpotent, we can apply the induction hypothesis to obtain a subgroup  $B$  of  $H^*$ , and a one-dimensional  $KB$ -submodule  $V$  of  $M_1$  such that  $M_1 = V^{H^*}$ . By Theorem 38.4, we have  $M \cong V^G$ , and the theorem is proved.

Theorem 52.1 gives another proof of Theorem 38.13 on the irreducible representations of  $p$ -groups. By Theorem 6.12, any nilpotent group  $G$  is a direct product of  $p$ -groups, consequently the irreducible representations of  $G$  are tensor products of the irreducible representations of the  $p$ -Sylow subgroups of  $G$ , by Corollary 51.13.

By the same method of proof, we obtain

(52.2) THEOREM. *Let  $G$  be a finite group with an abelian normal subgroup  $H$  such that  $G/H$  is abelian. Then every irreducible  $K$ -representation of  $G$  is a monomial representation.*

PROOF. Let us call groups satisfying the hypothesis of the theorem *metabelian* groups. Since any subgroup or homomorphic image of a metabelian group is metabelian, the proof of Theorem 52.1 will apply if we can show that any metabelian group  $G$  which is not abelian has an abelian normal subgroup not contained in the center. Let  $H$  be an abelian normal subgroup such that  $G/H$  is abelian, and let  $C$  be the center of  $G$ . If  $H \subset C$ , there is nothing to prove, so we may assume  $H \subsetneq C$ . Since  $[G, G] \subset H$ , any subgroup containing  $C$  is normal in  $G$ . If  $G$  is not abelian, we can find a subgroup  $H^* \supset C$  such that  $H^*/C$  is cyclic and not equal to (1). Then  $H^*$  is an abelian normal subgroup not contained in the center, and the theorem is proved.

(52.3) COROLLARY. *Let  $G$  be a finite group all of whose Sylow subgroups are cyclic. Then every irreducible  $K$ -representation of  $G$  is a monomial representation.*

PROOF. By Theorem (9.4.3) of M. Hall [2],  $G$  is a metabelian group, and the preceding theorem can be applied.

(52.4) COROLLARY. *The result of Theorem 52.2 holds for any group  $G$  such that  $[G : 1]$  is a product of distinct primes.*

PROOF. For any prime  $p \mid [G : 1]$ , the  $p$ -Sylow subgroup of  $G$  has order  $p$  and hence is cyclic. Thus Corollary 52.3 can be applied.

We remark that groups whose Sylow subgroups are cyclic are, by Theorem (9.4.3) of M. Hall [2], metacyclic groups with two generators  $a, b$  satisfying the relations set down in § 47. In that section, however, we asked whether the irreducible representations belonged to a particular set of monomial representations, so that the results of that section do not necessarily include Corollary 52.3 as a special case. We should mention also that the results (52.1)-(52.3) have been extended considerably by Ito [4] and Huppert [1].

Let us call a group all of whose irreducible  $K$ -representations are monomial an *M-group*. The following result and its proof have been communicated to us by Feit and Thompson.

(52.5) THEOREM (Taketa [1]). *Every M-group is solvable.*

PROOF. Suppose the result is false, and let  $G$  be a non-solvable *M-group* of minimal order. Since the property of being an *M-group*

is inherited by homomorphic images, every proper homomorphic image of  $G$  is solvable. We prove first that  $G$  has a unique minimal normal subgroup not equal to  $(1)$ . Indeed, suppose  $A$  and  $B$  are distinct minimal normal subgroups of  $G$ . Then  $A \cap B = (1)$ , and  $G/A$  and  $G/B$  are both solvable. Since  $A \cap B = (1)$ , the obvious homomorphism of  $G \rightarrow G/A \times G/B$  is an isomorphism of  $G$  into a solvable group, which is impossible in view of our assumption that  $G$  is not solvable.

Now let  $H$  be the unique minimal normal subgroup of  $G$ , and let  $h \in H$ ,  $h \neq 1$ . Then there exists an irreducible representation  $T$  of  $G$  such that  $T(h) \neq 1$ . The kernel of  $T$  is either  $(1)$  or it contains  $H$ , and the latter possibility is ruled out since  $T(h) \neq 1$ . Therefore  $T$  is a faithful representation of  $G$ , and since  $G$  is an  $M$ -group,  $T$  is a monomial representation. Let  $\mathbf{T}$  be a faithful irreducible monomial matrix representation of minimal degree, and let  $\mathbf{T}_0$  be the permutation matrix representation derived from  $\mathbf{T}$  by setting all non-zero entries of the matrices  $\{\mathbf{T}(g), g \in G\}$  equal to 1. The kernel  $H^*$  of  $\mathbf{T}_0$  is isomorphic to a group of diagonal matrices and is abelian. Since  $\mathbf{T}_0$  is reducible (see Exercise 43.8),  $\mathbf{T}_0$  is not faithful; otherwise  $\mathbf{T}_0$  has an irreducible component  $\mathbf{U}$  of lower degree than  $\mathbf{T}$ , such that  $\mathbf{U}(h) \neq 1$  for some  $h \in H$ , and therefore  $\mathbf{U}$  is faithful, which contradicts the way  $\mathbf{T}$  was chosen. Therefore  $H^*$  is an abelian normal subgroup not equal to  $(1)$ , and we know that  $G/H^*$  is solvable. It follows that  $G$  is solvable, contrary to our original assumption. This completes the proof. (For further results, see Berman [11].)

### § 53. Schur's Theory of Projective Representations

The observation that the study of relations between representations of a group and representations of a factor group inevitably leads to projective representations is due to Schur. In a series of definitive papers (Schur [1], [4], [6]) he laid the foundations of a general theory of projective representations. Further results have been obtained from time to time (Frucht [1], Mackey [4]), and the subject remains an attractive one for study. Our purpose is to prove one of Schur's main results, which will serve as an introduction to the theory. Our presentation follows rather closely a somewhat simplified approach to Schur's results given by Asano and Shoda [1].

In this section  $G$  denotes a finite group of order  $n$  and  $K$  an

algebraically closed field of arbitrary characteristic. We recall that a projective representation of  $G$  is a map  $T: G \rightarrow GL(V)$ , where  $V$  is a vector space over  $K$ , such that

$$T(s)T(t) = T(st)\alpha(s, t), \quad s, t \in G,$$

where  $\alpha$  is a function on  $G \times G \rightarrow K^* = \{\xi \in K : \xi \neq 0\}$ . We call  $\alpha$  the *factor set* of the representation. The representation is called *irreducible* if  $V$  has no non-trivial  $G$ -subspaces.

From the associative law we obtain the fundamental property of the factor set

$$(53.1) \quad \alpha(s, tu)\alpha(t, u) = \alpha(s, t)\alpha(st, u),$$

for all  $s, t, u \in G$ .

(53.2) **DEFINITION.** Any function  $\alpha: G \times G \rightarrow K^*$  which satisfies (53.1) is called a *factor set* of  $G$  (or a  $K$ -factor set). Two factor sets  $\alpha$  and  $\alpha'$  are called *equivalent* if there exists a function  $\rho: G \rightarrow K^*$  such that

$$\alpha'(s, t) = \alpha(s, t)\rho(st)\rho(s)^{-1}\rho(t)^{-1}$$

for all  $s, t \in G$ . This is an equivalence relation, and the equivalence class containing the factor set  $\alpha$  will be denoted by  $\{\alpha\}$ . For any two factor sets  $\alpha, \alpha'$ , let  $\alpha\alpha'$  denote the function defined by

$$(\alpha\alpha')(s, t) = \alpha(s, t)\alpha'(s, t), \quad s, t \in G.$$

Then  $\alpha\alpha'$  is a factor set. If  $\alpha^{-1}$  denotes the function for which

$$\alpha^{-1}(s, t) = \alpha(s, t)^{-1}, \quad s, t \in G,$$

then  $\alpha^{-1}$  is also a factor set. The set of equivalence classes of factor sets forms an abelian group  $M$  if we define

$$\{\alpha\}\{\alpha'\} = \{\alpha\alpha'\}, \quad \alpha, \alpha' \in M.$$

The identity element in  $M$  is given by  $\{1\}$  where  $1$  is the factor set  $1(s, t) = 1$ ,  $s, t \in G$ ; and for any  $\{\alpha\} \in M$ , we have  $\{\alpha\}^{-1} = \{\alpha^{-1}\}$ . The group  $M$  of classes of factor sets is called the *multiplier*  $M$  of  $G$ .

In the course of Definition 53.2 a number of statements were made which require verification, and we shall leave these details as exercises for the reader. The definition of equivalence of factor sets is motivated by Exercise 51.2.

Our first task is to examine more closely the structure of the multiplier  $M$  under the hypothesis that  $K$  is algebraically closed.

(53.3) **THEOREM.** *The multiplier  $M$  of  $G$  has finite order not*

divisible by the characteristic of  $K$ . The order of every element in  $M$  is a factor of the order of  $G$ .

PROOF. First let  $\{\alpha\} \in M$  and  $n = [G : 1]$ . For any  $s \in G$ , define

$$\rho(s) = \prod_{r \in G} \alpha(s, r).$$

Then from (53.1), we have

$$\alpha(s, t)^n = \frac{\rho(s)\rho(t)}{\rho(st)},$$

and it follows that  $\{\alpha\}^n = 1$ . This proves the second statement of the theorem.

Now let  $e$  be the order of  $\{\alpha\}$  in  $M$ , and if  $\text{char } K = p > 0$ , write  $e = p^a q$  where  $a \geq 0$  and  $p \nmid q$ . Then there is a function  $\beta: G \rightarrow K^*$  such that for all  $s, t \in G$ , we have

$$(53.4) \quad \alpha(s, t)^e = \frac{\beta(s)\beta(t)}{\beta(st)}.$$

Since  $K$  is algebraically closed,  $K$  is a perfect field, and we may extract  $p$ th roots in  $K$ . We obtain from (53.4)

$$(\alpha(s, t)^q)^{p^a} = \left( \frac{\beta(s)^{1/p^a} \beta(t)^{1/p^a}}{\beta(st)^{1/p^a}} \right)^{p^a},$$

and, because  $p^a$ th roots are unique in  $K$ , we have

$$\alpha(s, t)^q = \frac{\beta(s)^{1/p^a} \beta(t)^{1/p^a}}{\beta(st)^{1/p^a}},$$

which contradicts our assumption that  $e$  is the order of  $\{\alpha\}$  unless  $p^a = 1$ . Therefore  $p \nmid e$ . Returning to (53.4), for each  $s \in G$  we can find  $\rho(s) \in K^*$  such that  $\rho(s)^e = \beta(s)^{-1}$ . Upon setting

$$\alpha'(s, t) = \frac{\rho(s)\rho(t)}{\rho(st)} \alpha(s, t),$$

we see that

$$(\alpha'(s, t))^e = \frac{\beta(s)^{-1} \beta(t)^{-1}}{\beta(st)^{-1}} \alpha(s, t)^e = 1.$$

We have proved that every class  $\{\alpha\} \in M$  of order  $e$  contains a representative  $\alpha'$  whose values  $\alpha'(s, t)$  are  $e$ th roots of 1 in  $K$ . Since  $e \mid n$ , it follows that there are at most a finite number of classes of factor sets, and the order of  $M$  is finite. Furthermore, since the order of every element of  $M$  is not divisible by the characteristic of

$K$ , it follows that  $\text{char } K \nmid [M : 1]$ , and Theorem 53.3 is proved.

Let  $\{\alpha\}$  be an element of  $M$  of order  $e$ . A representative  $\alpha' \in \{\alpha\}$  whose values are  $e$ th roots of 1 is called a *normalized factor set*, and will turn out to be useful in what follows.

We consider now a natural way in which projective representations might arise. Let  $G^*$  be an extension of  $G$  with kernel  $N$ , and suppose that  $N$  is contained in the center of  $G^*$  [see Definition 7.4]. Then  $G^*/N \cong G$ , and we may find a set of coset representatives  $\{u_s, s \in G\}$  in one-to-one correspondence with the elements of  $G$  such that for all  $s, t \in G$  we have

$$u_s u_t = u_{st} a(s, t)$$

where  $a(s, t) \in N$ . Now let  $T: G^* \rightarrow GL(V)$  be an (ordinary) representation of  $G^*$  such that for all  $s, t \in G$ ,

$$(53.5) \quad T(a(s, t)) = \alpha(s, t) 1_V$$

for some element  $\alpha(s, t) \in K^*$ . (This will be the case, for example, if  $T$  is an irreducible representation of  $G^*$ . For then, since  $N$  is contained in the center of  $G^*$ , Schur's lemma implies that the elements of  $N$  are mapped onto multiples of  $1_V$ .) Then because of (53.5) the mapping  $T: G \rightarrow GL(V)$ , given by

$$s \rightarrow T(u_s),$$

defines a projective representation of  $G$  with factor set  $\alpha(s, t)$ . We say that a projective representation of  $G$  which is constructed in this way from an ordinary representation of  $G^*$  can be *lifted* to  $G^*$ .

(53.6) **DEFINITION.** A *representation-group*  $G^*$  of  $G$  is a finite group  $G^*$  which is an extension of  $G$  with kernel contained in the center of  $G^*$  such that every projective representation of  $G$  is equivalent to one which can be lifted to  $G^*$ .

Now we come to the main theorem of this section.

(53.7) **THEOREM** (Schur [1]). *Let  $G$  be a finite group of order  $n$  and  $K$  an algebraically closed field of arbitrary characteristic. Then  $G$  has at least one representation-group  $G^*$  of order  $nm$  where  $m = [M : 1]$ , and the kernel of the extension is isomorphic to the multiplier  $M$  of  $G$ .*

**PROOF.** By Theorem 4.5  $M$  is a direct product of cyclic groups. Let  $\{\alpha^{(1)}\}, \dots, \{\alpha^{(d)}\}$  be generators of these groups, and let their orders be  $e_1, \dots, e_d$  where, by Theorem 53.3,  $\text{char } K \nmid e_i$  for  $1 \leq i \leq d$ .

We may assume that for each  $i$ ,  $1 \leq i \leq d$ ,  $\alpha^{(i)}(r, s)$  is an  $e_i$ th root of 1 for all  $r, s \in G$ . Because  $\text{char } K \nmid e_i$ , there exists for each  $i$  a primitive  $e_i$ th root of 1, say  $\zeta_i^{(i)}$ , whose order is exactly  $e_i$ . Then for each  $i$  we have

$$\alpha^{(i)}(r, s) = \zeta_i^{a_{r,s}^{(i)}}$$

where  $a_{r,s}^{(i)}$  is an integer between 0 and  $e_i - 1$ . By (53.1) we have for each  $i$ ,  $1 \leq i \leq d$ ,

$$(53.8) \quad a_{s,tu}^{(i)} + a_{t,u}^{(i)} \equiv a_{s,t}^{(i)} + a_{st,u}^{(i)} \pmod{e_i}.$$

An arbitrary factor set  $\alpha$  is equivalent to one of the form

$$(53.9) \quad \begin{aligned} \beta(r, s) &= (\alpha^{(1)}(r, s))^{x_1} \cdots (\alpha^{(d)}(r, s))^{x_d} \\ &= (\zeta_1^{x_1})^{a_{r,s}^{(1)}} \cdots (\zeta_d^{x_d})^{a_{r,s}^{(d)}}, \end{aligned} \quad r, s \in G,$$

where  $0 \leq x_i < e_i$ . Now let  $N$  be an abstract abelian group isomorphic to  $M$ , and let  $n_1, \dots, n_d$  be generators of  $N$  corresponding to  $\{\alpha^{(1)}\}, \dots, \{\alpha^{(d)}\}$ . For each pair  $r, s \in G$ , let  $a(r, s) \in N$  be defined by

$$(53.10) \quad a(r, s) = n_1^{a_{r,s}^{(1)}} \cdots n_d^{a_{r,s}^{(d)}},$$

because of (53.8) we have

$$(53.11) \quad a(s, tu)a(t, u) = a(s, t)a(st, u)$$

for all  $s, t, u \in G$ .

By a *linear character* of  $N$ , we mean a homomorphism of  $N$  into the multiplicative group  $K^*$  of  $K$ . Let  $\phi$  be any  $K$ -character; applying  $\phi$  to (53.10), we have

$$\phi(a(r, s)) = \phi(n_1)^{a_{r,s}^{(1)}} \cdots \phi(n_d)^{a_{r,s}^{(d)}},$$

and because of (53.11),  $(r, s) \rightarrow \phi(a(r, s))$  is a factor set. Moreover, the  $\phi(n_i)$  are  $e_i$ th roots of 1, and for each set of integers  $\{x_1, \dots, x_d\}$ ,  $0 \leq x_i < e_i$ , there exists a linear character  $\phi$  of  $N$  with

$$\phi(n_i) = \zeta_i^{x_i}, \quad 1 \leq i \leq d.$$

Then (53.9) implies that as  $\phi$  runs over all linear characters of  $N$ , the factor sets  $(r, s) \rightarrow \phi(a(r, s))$  run through a complete set of representatives of the classes of factor sets belonging to  $M$ .

Now define  $G^*$  as follows:  $G^*$  consists of all ordered pairs  $(s, n)$  with  $s \in G$  and  $n \in N$ , and we define multiplication by

$$(r, n)(s, n') = (rs, a(r, s)nn')$$

where  $r, s \in G$  and  $n, n' \in N$ . The associative law follows from (53.11), and the other group axioms are easily verified. The mapping

$$n \rightarrow (1, \alpha(1, 1)^{-1} n)$$

is an isomorphism of  $N$  into the center of  $G^*$ , and we shall identify  $N$  with its image in  $G^*$ . Let  $u_s = (s, 1)$  for each  $s \in G$ . Then the elements  $\{u_s\}$  are representatives of the distinct cosets of  $N$  in  $G$ , and we have

$$(53.12) \quad u_r u_s = u_{rs} a(r, s), \quad r, s \in G.$$

It follows that  $G^*/N \cong G$ .

Now let  $T: G \rightarrow GL(V)$  be a projective representation of  $G$  with factor set  $\alpha$ . By choosing an equivalent representation if necessary, we may assume that there exists a linear character  $\psi$  of  $N$  such that

$$(53.13) \quad \psi(a(r, s)) = \alpha(r, s). \quad r, s \in G.$$

Define a mapping  $T^*: G^* \rightarrow GL(V)$  by

$$(53.14) \quad T^*(u_s n) = T(s)\psi(n), \quad s \in G, n \in N.$$

Then, by (53.12), we have

$$T^*(gh) = T^*(g)T^*(h), \quad g, h \in G^*.$$

and

$$T^*(1) = 1.$$

Therefore,  $T^*$  is a representation of  $G^*$ , and (53.14) asserts that  $T$  can be lifted to  $G^*$ . Since  $G^*$  has order  $nm$ , the proof of Theorem 53.7 is complete.

We remark that it can be shown that no representation-group of order less than  $nm$  exists and that some information concerning the uniqueness of  $G^*$  is available. For these details, we refer to Schur's papers or to Asano and Shoda [1].

(53.15) COROLLARY. *A finite group  $G$  has at most a finite number of inequivalent irreducible projective representations in an algebraically closed field  $K$ .*

PROOF. First let  $G^*$  be a representation group, and let  $T: G \rightarrow GL(V)$  be an irreducible projective representation of  $G$ . By replacing  $T$  by an equivalent representation if necessary, we can find a representation  $T^*: G^* \rightarrow GL(V)$  such that

$$T^*(u_s) = T(s), \quad s \in G.$$

Then  $T^*$  is an irreducible representation of  $G^*$ . Moreover, let  $S: G \rightarrow GL(W)$  be a second projective representation of  $G$ ; it also can be lifted to  $G^*$ , so that for some representation  $S^*: G^* \rightarrow GL(W)$ , we have

$$S^*(u_s) = S(s), \quad s \in G.$$

Then, if  $S^*$  and  $T^*$  are equivalent representations of  $G^*$ ,  $S$  and  $T$  are equivalent projective representations of  $G$ . Therefore the number of inequivalent irreducible projective representations of  $G$  cannot exceed the number of inequivalent irreducible representations of  $G^*$ , and this number is known to be finite from the results in Chapter IV. This completes the proof of the corollary.

We conclude this section with some remarks on the degrees of the irreducible representations of a finite group  $G$  in the complex field  $K$ .

(53.16) THEOREM. *The degrees of the irreducible projective representations of  $G$  divide the order of  $G$ .*

PROOF. Let  $T$  be an irreducible projective representation of  $G$ . By Theorem 53.7 there exists a representation group  $G^*$  of order  $m[G:1]$ , where  $m$  is the order of a subgroup of the center of  $G^*$ , and  $T$  can be lifted to an ordinary irreducible representation  $T^*$  of  $G^*$  such that  $\deg T^* = \deg T$ . By Exercise 33.1,  $\deg T^* | [G^*:C(G^*)]$  where  $C(G^*)$  is the center of  $G^*$ , and hence  $\deg T | [G:1]$  as we wished to prove.

Now we can prove a much sharper result than the one given in Exercise 33.1, which was pointed out to us by Reynolds.

(53.17) THEOREM. *Let  $G$  be a finite group and  $H$  a normal subgroup of  $G$ . Then the dimension of any irreducible  $KG$ -module  $M$  divides  $[G:H]d_1$ , where  $d_1$  is the dimension of an irreducible  $KH$ -module.*

PROOF. As in § 49, we write

$$M_H = M_1 \oplus \cdots \oplus M_r$$

where the  $M_i$  are the homogeneous components of  $M_H$ . We may assume the result for groups of lower order than  $G$ . We have to consider two cases.

CASE 1.  $r > 1$ . Then the subgroup  $H^* = \{h \in G : hM_1 = M_1\}$  is properly contained in  $G$ , and we have, by Corollary 50.6,

$$M = M_1^G$$

where  $M_1$  is an irreducible  $KH^*$ -module. Applying the induction hypothesis, we have

$$(M : K) = [G : H^*](M_1 : K) \mid [G : H^*][H^* : H]d_1$$

where  $d_1$  is the dimension of an irreducible  $KH$ -module. Thus the result is true in this case.

CASE 2.  $r = 1$ . Then, by Theorem 51.7, we have

$$(M : K) = ef$$

where  $e$  is the degree of an irreducible projective representation of  $G/H$ , and  $f$  is the degree of some irreducible  $KH$ -module. By Theorem 53.16,  $e \mid [G : H]$ , and hence  $(M : K) \mid [G : H]f$ , and the theorem is completely proved.

(53.18) COROLLARY (Ito [2]). *Let  $H$  be any abelian normal subgroup of  $G$ . Then the degrees of the irreducible  $K$ -representations of  $G$  all divide  $[G : H]$ .*

Additional references for the chapter are Conlon [1], Tucker [2]-[4], and Reynolds [3].

This page intentionally left blank

## CHAPTER VIII

### Non-Semi-Simple Rings

In Chapters IV-VII, we were mostly concerned with representations of a finite group in a field whose characteristic does not divide the order of the group. Our approach was first to derive general theorems on semi-simple rings and algebras and then to apply these results to group algebras. Many of the results in Chapters V-VII, of course, required special techniques peculiar to group theory, and at the same time furnished information about the structure of the finite groups themselves. Our program in Chapters VIII, IX, and XII is to study in the same way representations of finite groups in fields whose characteristic divides the order of the group, and to give some idea of the applications of these methods to group theory. Because the group algebras involved will no longer be semi-simple, it is necessary to develop properties of non-semi-simple rings and algebras, and Chapters VIII and IX are devoted to these prerequisites. We should not hide the fact that these chapters contain far more material than that is actually needed for the theory of modular representations of groups. This part of ring theory, which centers around the notions of quasi-Frobenius rings and Frobenius algebras, is today an attractive subject for study in its own right, chiefly because of the pioneering work of T. Nakayama, and we have attempted to give the reader an up-to-date account of these theories.

One of the main tools is the theory of projective and injective modules, which play a basic role in Cartan and Eilenberg's book *Homological Algebra* [1].

The parts of Chapters VIII and IX which are essential for modular representations of groups are §§ 54-56 in Chapter VIII and §§ 60-65 of Chapter IX.

#### § 54. Principal Indecomposable Modules

Throughout §§ 54-56 we let  $A$  denote a ring with minimum

condition, with unity element 1. In particular, as we have remarked in Chapter IV, the results of this chapter are applicable to finite-dimensional algebras over fields. The material on semi-simple rings presented in Chapter IV will be used frequently here without citing the reference each time.

As in the semi-simple case, it will be useful to consider the left regular module  $\mathbb{A} A$ , the submodules of which are just the left ideals in the ring  $A$ . Our first task is to show that  $\mathbb{A} A$  has a composition series and thus satisfies both the maximum and minimum conditions. This fact is of course trivial if  $A$  is a finite-dimensional algebra over a field. The surprising result that it holds in general was proved first by Hopkins [1].

(54.1) **THEOREM.** *Let  $A$  be a ring with minimum condition containing a unity element. Then  $\mathbb{A} A$  has a composition series, and thus the left ideals of  $A$  satisfy both the D.C.C. and the A.C.C.*

**PROOF.** Setting  $N = \text{rad } A$ , we have

$$N^s \neq 0, \quad N^{s+1} = 0$$

for some integer  $s$ . Letting  $N^0 = A$ , we may write the series of submodules

$$(54.2) \quad A = N^0 \supset N^1 \supset N^2 \supset \cdots \supset N^s \supset 0$$

in which each module properly contains the next. For each  $k$ ,  $1 \leq k \leq s + 1$ , consider the factor module

$$M_k = N^{k-1}/N^k.$$

Since  $M_k$  is a submodule of  $A/N^k$ , and this in turn is a homomorphic image of  $\mathbb{A} A$ , it follows that  $M_k$  satisfies the minimum condition on submodules.

On the other hand, we have  $N M_k = 0$  for each  $k$ , so by Exercise 25.4,  $M_k$  is a completely reducible left  $A$ -module. From (15.5), we conclude that  $M_k$  satisfies the A.C.C. as well as the D.C.C. Thus each  $M_k$  has a composition series, and because of (54.2),  $\mathbb{A} A$  also has a composition series. This proves the result.

We may now apply the results of §14 to the module  $\mathbb{A} A$ . We know that  $\mathbb{A} A$  is expressible as a finite direct sum  $A_1 \oplus \cdots \oplus A_n$  of indecomposable submodules, and that these submodules  $\{A_i\}$  are uniquely determined up to isomorphism and order of occurrence. This justifies

(54.3) **DEFINITION.** Let  $\mathbb{A} A = A_1 \oplus \cdots \oplus A_n$  be a decomposition of

$\triangle A$  into non-zero indecomposable submodules  $\{A_i\}$ . These summands  $\{A_i\}$  are called the (left) *principal indecomposable modules* of  $A$ .

It may very well happen that several of the summands  $\{A_i\}$  are mutually isomorphic. In any case, however, there are only a finite number of non-isomorphic principal indecomposable modules of  $A$ .

Since the theory of non-semi-simple rings is a generalization of the semi-simple case, it is enlightening to check, from time to time, what our definitions become in the semi-simple case. If  $A$  is semi-simple, we know that a non-zero  $A$ -module is indecomposable if and only if it is irreducible. Thus the decomposition of  $\triangle A$  into non-zero indecomposable submodules is just the decomposition of  $\triangle A$  into irreducible submodules (i.e., minimal left ideals of  $A$ ), and so the principal indecomposable modules of  $A$  are precisely the minimal left ideals of  $A$ .

Returning to the general case, we begin by recalling some definitions from Chapter IV.

(54.4) DEFINITION. Two idempotents  $e, f$  in  $A$  are said to be *orthogonal* if  $ef = fe = 0$ . An idempotent  $e$  is called *primitive* if it is impossible to express  $e$  as the sum of two orthogonal idempotents.

In terms of this definition, we can now give a simple criterion for a left ideal to be a principal indecomposable module.

(54.5) THEOREM. A left ideal  $I$  of  $A$  is a principal indecomposable module of  $A$  if and only if  $I = Ae$  for some primitive idempotent  $e$  in  $A$ .

PROOF. Let  $e$  be an idempotent in  $A$ . We establish first that the left ideal  $Ae$  is indecomposable if and only if  $e$  is primitive. On the one hand, if  $e = e_1 + e_2$  is a sum of orthogonal idempotents, then

$$Ae = Ae_1 + Ae_2$$

is a decomposition of  $Ae$  into non-zero submodules (because  $1 \in A$ ), and the sum is direct since  $e_1$  is a right unity for  $Ae_1$  and a right annihilator of  $Ae_2$ . On the other hand, if  $Ae$  is decomposable, say

$$Ae = L_1 \oplus L_2$$

for non-zero submodules  $L_1, L_2$ , then we may write

$$e = e_1 + e_2, e_1 \in L_1, e_2 \in L_2,$$

and it is easily seen that  $e_1$  and  $e_2$  are orthogonal idempotents.

Now let  $I$  be a left ideal of  $A$ . If  $I = Ae$  for some primitive idempotent  $e \in A$ , then by the above  $I$  is indecomposable. But also

$$A = Ae \oplus A(1 - e),$$

so that  $I$  is a direct summand of  $A$  and is thus a principal indecomposable module.

Conversely, let  $L$  be a principal indecomposable module of  $A$ , and write

$$A = L \oplus L'$$

where  $L'$  is a left ideal of  $A$ . Then

$$1 = e + e' , \quad e \in L, e' \in L' ,$$

and, as we have seen several times before,  $e$  is an idempotent and  $L = Ae$ . Since  $L$  is indecomposable,  $e$  is primitive. This proves the theorem.

In Theorem 25.11, we proved that given any idempotent  $e$  in a semi-simple ring  $A$ , the left ideal  $Ae$  is minimal if and only if  $eAe$  is a skewfield. The next two theorems establish the connection in the general case between a left ideal  $Ae$  generated by an idempotent  $e$  and the structure of the ring  $eAe$ .

(54.6) THEOREM. *Let  $e \in A$  be idempotent, and let  $N = \text{rad } A$ . Then  $eAe$  is a ring with minimum condition having unity element  $e$ , and*

$$\text{rad}(eAe) = eNe .$$

PROOF. (See Exercise 24.5.) Clearly  $e$  is the unity element in the ring  $eAe$ . Now let  $L$  be a left ideal in  $eAe$ ; then  $AL$  is the smallest left ideal in  $A$  containing  $L$ . We shall show that

$$L = AL \cap eAe .$$

Setting  $L' = AL \cap eAe$ , clearly  $L \subset L'$ . On the other hand,  $L' \subset eAe$  implies that  $L' = eL'$ , and so

$$L' = eL' \subset eAL = eAe \cdot L \subset L$$

since  $L$  is a left ideal in  $eAe$ . This shows that  $L = L'$ .

Now let  $L_1 \supset L_2 \supset \dots$  be a descending chain of left ideals in  $eAe$ ; then  $AL_1 \supset AL_2 \supset \dots$  is a descending chain of left ideals in  $A$ , and we have  $AL_k = AL_{k+1} = \dots$  for some  $k$ . Taking intersections with  $eAe$ , we obtain  $L_k = L_{k+1} = \dots$ , and we have proved that  $eAe$

satisfies the minimum condition.

Now let  $N' = \text{rad } eAe$ ; clearly  $eNe \subset N'$ . On the other hand,  $AN'$  is a left ideal in  $A$ , and we have

$$(AN')^r = AN' \cdot AN' \cdots AN' = A \cdot (N'eAe) \cdots (eAe)N' \subset A(N')^r.$$

Since  $N'$  is nilpotent, so is  $AN'$ , and thus  $AN' \subset N$ . Hence  $N' \subset N$ , and so  $N' = eN'e \subset eNe$ , which proves the theorem.

(54.7) DEFINITION. Let  $A$  be a ring with minimum condition and unity element 1. We call  $A$  *completely primary* if the set of non-units in  $A$  forms a two-sided ideal of  $A$ .

The fact that when  $A$  is completely primary, the ideal of non-units coincides with the radical is proved, along with some other facts, in the following lemma.

(54.8) LEMMA. Let  $A$  be a ring with minimum condition having a unity element. The following statements are equivalent:

- (i)  $A$  is completely primary.
- (ii)  $A$  contains no idempotent distinct from 1.
- (iii) If  $N$  is the radical of  $A$ , then  $A/N$  is a skewfield.

PROOF. We give a cyclic proof. Assume (i), and suppose that  $e$  is an idempotent not equal to 1. Then  $e(1 - e) = 0$ , so that  $e$  and  $1 - e$  are both non-units. Because the sum of two non-units lies in the ideal of non-units, it follows that 1 is a non-unit, which is of course impossible. Therefore no idempotent  $e \neq 1$  can occur, and (ii) is proved.

Assume (ii), and let  $N = \text{rad } A$ . We shall prove that each element  $a \in A$  which is not contained in  $N$  is a unit in  $A$ , which will imply (iii). The ideal  $Aa$  cannot be nilpotent since  $a \notin N$ . By Theorem 24.2, it follows that  $Aa$  contains an idempotent  $e$ . But (ii) shows that  $e = 1$ , so  $Aa = A$ . Therefore  $xa = 1$  for some  $x$ . It remains to show that  $ax = 1$ . If, to the contrary,  $ax - 1 \neq 0$ , then  $(ax - 1)a = 0$ , and the left ideal  $L_a = \{u \in A : ua = 0\}$  is not equal to 0. Since  $L_a \subset L_{a^2} \subset \dots$ , Theorem 54.1 implies  $L_{a^i} = L_{a^{i+1}}$  for some  $i$ . Let  $u \in L_{a^i}$ . Then  $ua^i = 0$ , and since  $u = uxa$ , we have  $uxa^{i+1} = 0$ . Therefore  $uxa^i = 0$ , and hence  $u = uxa \in L_{a^{i-1}}$ . Therefore  $L_{a^i} = L_{a^{i-1}}$ . Continuing in this way, we see that  $L_a = 0$ , contrary to assumption. Therefore (ii) implies (iii).

Finally, assume (iii), and let  $S$  be the set of non-units of  $A$ . Since  $N$  is nilpotent, each element of  $N$  is a non-unit of  $A$ , and so  $N \subset S$ . To prove (i), we shall show  $N = S$ . It is sufficient to prove that every element  $z \notin N$  is a unit. By (iii) the coset  $z + N$  is a unit

in the quotient ring  $A/N$ . Therefore we can find  $n \in N$  and  $y \in A$  such that

$$zy + n = 1.$$

Since  $n$  is nilpotent,  $1 - n$  is a unit with  $(1 - n)^{-1} = 1 + n + n^2 + \dots$ , and  $z$  has a right inverse  $y(1 - n)^{-1}$ . Similarly  $z$  has a left inverse, and it follows that  $z$  is a unit.

(54.9) THEOREM. *An idempotent  $e$  in  $A$  is primitive if and only if  $eAe$  is a completely primary ring. Therefore the left ideal  $Ae$  is indecomposable if and only if  $eAe$  is completely primary.*

PROOF. First suppose that  $e$  is primitive. By Theorem 54.6,  $eAe$  is a ring with minimum condition, and by Lemma 54.8, it is sufficient to prove that if  $f$  is an idempotent in  $eAe$ , then  $f = e$ . Assume to the contrary that  $f \neq e$ ; then  $f \in eAe$  and  $f$  and  $e - f$  are orthogonal idempotents whose sum is  $e$ , contrary to the assumption that  $e$  is primitive. Therefore  $f = e$  and  $eAe$  is completely primary.

Conversely, let  $eAe$  be completely primary. Then  $e$  is primitive, for if not, we have  $e = e_1 + e_2$  where  $e_1$  and  $e_2$  are orthogonal idempotents. We show that  $e_1, e_2 \in eAe$ , contrary to (ii) of (54.8). We have  $e = e^2 = ee_1 + ee_2$ , and subtracting from the original equation, we obtain

$$e_1 + e_2 - ee_1 - ee_2 = 0.$$

Multiplying on the right by  $e_1$  or  $e_2$ , we conclude that  $e_1$  and  $e_2$  both belong to  $eA$ . Similarly they belong to  $Ae$ , and Theorem 54.9 is proved.

(54.10) COROLLARY. *A left ideal  $Ae$  generated by an idempotent  $e$  is indecomposable if and only if the right ideal  $eA$  is indecomposable.*

Again let us revert to the special case where  $A$  is semi-simple. An idempotent  $e \in A$  is primitive if and only if  $Ae$  is a minimal left ideal. On the other hand,  $eAe$  is completely primary if and only if  $eAe/eNe$  is a skewfield, where  $N = \text{rad } A$ . Since  $N = 0$ , we conclude from Theorem 54.9 that the left ideal  $Ae$  is minimal if and only if  $eAe$  is a skewfield, and so we again obtain Theorem 25.11.

The next theorem establishes a basic relation between the principal indecomposable modules of  $A$  and the irreducible  $A$ -modules.

(54.11) THEOREM. *Let  $N = \text{rad } A$ , and let  $Ae$  be a principal indecomposable module of  $A$ . Then  $Ae$  has a unique maximal submodule, and this submodule is  $Ne$ . Two principal indecomposable*

*modules  $Ae$  and  $Af$  are isomorphic if and only if the irreducible modules  $Ae/Ne$  and  $Af/Nf$  are isomorphic.*

**PROOF.** Let  $L$  be any left ideal properly contained in  $Ae$  and suppose that  $L$  is not nilpotent. By Theorem 24.2,  $L$  contains an idempotent  $e_1 \neq e$ . Then  $e = e_1 + (e - e_1)$ , and we have  $e_1(e - e_1) = 0$ . It follows that  $Ae = Ae e_1 \oplus Ae(e - e_1)$ , and this contradicts our assumption that  $Ae$  is indecomposable. Therefore every left ideal properly contained in  $Ae$  is nilpotent, and the sum  $N_1$  of all such left ideals is the unique maximal subideal of  $Ae$ . Since  $N_1$  is a sum of nilpotent left ideals, we have  $N_1 \subset N \cap Ae$ . On the other hand,  $N \cap Ae$  is a nilpotent left ideal properly contained in  $Ae$ ; hence  $N \cap Ae \subset N_1$ , and so we have  $N_1 = N \cap Ae = Ne$  as required.

The “only if” part of the second assertion is clear, namely that if  $Ae$  and  $Af$  are  $A$ -isomorphic, so are  $Ae/Ne$  and  $Af/Nf$ , since the isomorphism will take the unique maximal subideal of  $Ae$  onto the unique maximal subideal of  $Af$ .

Finally, suppose that  $\eta$  is an  $A$ -isomorphism of  $Ae/Ne$  onto  $Af/Nf$ , and set

$$\eta(e + Ne) = u + Nf$$

for some  $u \in Af$ ,  $u \notin Nf$ . Since  $e(e + Ne) = e + Ne$ , we have  $eu \notin Nf$ , and replacing  $u$  by  $eu$ , we obtain an element  $u \in eAf$ ,  $u \notin N$ . Then  $Aeu$  is a left ideal contained in  $Af$  and not in  $Nf$ , and, because  $Nf$  is the unique maximal subideal of  $Af$ , we have  $Aeu = Af$ . In a similar way, we find an element  $v \in fAe$ ,  $v \notin N$ , such that  $Afv = Ae$ . Then  $uv \in eAe$ , and  $uv \notin eNe$ ; otherwise we have the impossible situation  $Ae = Aeuv \subset N$ . By Theorem 54.9,  $uv$  is a unit in the completely primary ring  $eAe$ . Now we consider the mapping  $\phi: b \rightarrow bu$  of  $Ae$  onto  $Af$ . Clearly  $\phi$  is an  $A$ -homomorphism. If  $\phi(b) = bu = 0$  for some  $b \in Ae$ , then upon solving the equation  $uvw = e$  for  $w \in eAe$ , we obtain  $0 = buvw = be = b$ . Therefore  $\phi$  is an  $A$ -isomorphism of  $Ae$  onto  $Af$ , and Theorem 54.11 is proved.

*Remark.* Theorem 54.11 gives an alternative proof, independent of the Krull-Schmidt theorem, that the principal indecomposable modules appearing in two direct decompositions of  $A$  can be paired off into isomorphic pairs.

(54.12) **THEOREM.** *Let  $M$  be a left  $A$ -module which has a composition series, and let  $Ae$  be a principal indecomposable module of  $A$ . A necessary and sufficient condition that  $M$  have a composition factor  $A$ -isomorphic to  $Ae/Ne$  is that  $eM \neq 0$ .*

PROOF. Let

$$M = M_1 \supset M_2 \supset \cdots \supset M_t \supset M_{t+1} = 0$$

be a composition series of  $M$ , and suppose that  $eM \neq 0$ . If  $eM_i \subset M_{i+1}$  for all  $i$ , then  $eM = e^t M \subset M_{t+1} = 0$  contrary to assumption. Therefore some composition factor  $V = M_i/M_{i+1}$  has the property that  $eV \neq 0$ . Then  $Aev \neq 0$  for some  $v \neq 0$  in  $V$ , and since  $V$  is irreducible we have  $Aev = V$ . The mapping  $a \rightarrow av$  of  $Ae$  onto  $V$  is an  $A$ -homomorphism whose kernel is a maximal submodule of  $Ae$ . Since  $Ae$  has a unique maximal submodule, the kernel is  $Ne$  and  $Ae/Ne$  is isomorphic to  $V$ .

Conversely, suppose  $\psi$  is an  $A$ -isomorphism of  $Ae/Ne$  onto a composition factor  $V = M_i/M_{i+1}$  of  $M$ . Then  $\psi(e+Ne) \neq 0$ , and we have  $\psi(e+Ne) = v + M_{i+1}$  for some  $v \in M_i$ ,  $v \notin M_{i+1}$ . Since  $e(e+Ne) = e+Ne$ , we have  $ev \notin M_{i+1}$ , and we have  $eM \neq 0$  as required.

(54.13) COROLLARY. *Every irreducible left  $A$ -module  $V$  is isomorphic to  $Ae/Ne$  for some principal indecomposable module  $Ae$ .*

PROOF. Since the identity element in  $A$  is a sum of primitive idempotents, there exists a primitive idempotent  $e$  such that  $eV \neq 0$ . By the preceding theorem,  $V$  is isomorphic to  $Ae/Ne$ .

(54.14) COROLLARY. *There is a one-to-one correspondence between classes of isomorphic principal indecomposable modules and classes of isomorphic irreducible left  $A$ -modules.*

PROOF. The mapping  $\{Ae\} \rightarrow \{Ae/Ne\}$  gives the desired correspondence. We have in fact shown the following: Let

$$\mathbb{A} = A_1 \oplus \cdots \oplus A_n$$

be a decomposition of the left regular module  $\mathbb{A}$  into indecomposable submodules  $A_1, \dots, A_n$ , and suppose these submodules to be numbered so that  $A_1, \dots, A_m$  are a full set of non-isomorphic modules among the  $\{A_i\}$ . Write  $A_i = Ae_i$  where  $e_i$  is a primitive idempotent in  $A$ , and set

$$V_i = Ae_i/Ne_i, \quad N = \text{rad } A.$$

Then  $V_1, \dots, V_m$  are a full set of non-isomorphic irreducible  $A$ -modules. Furthermore  $Ae_i \cong Ae_j$  ( $1 \leq i, j \leq n$ ) if and only if  $V_i \cong V_j$ .

Corollary 54.14 is trivial when  $A$  is semi-simple. Corollary 54.13 is a generalization of Theorem 25.10, and Theorem 54.12 is a generalization of Exercise 25.10.

We conclude this section with some applications of the preceding results to modules over finite-dimensional algebras. In this discussion,  $A$  denotes always a finite-dimensional algebra over a field  $K$ . All modules are assumed to be finite-dimensional vector spaces over  $K$ .

If  $V$  and  $W$  are left  $A$ -modules, the *intertwining number*  $i(V, W)$  is a non-negative integer defined by

$$i(V, W) = (\text{Hom}_A(V, W): K).$$

[See Definition 43.11.] Our first result is

(54.15) THEOREM. *Let  $M$  be a left  $A$ -module, and let  $e$  be an idempotent in  $A$ . Then*

$$(eM: K) = i(Ae, M).$$

PROOF. Let  $\{m_1, \dots, m_r\}$  be a  $K$ -basis for  $eM$ . For each  $i$ ,  $1 \leq i \leq r$ , define  $\phi_i \in \text{Hom}_A(Ae, M)$  by

$$\phi_i(a) = am_i, \quad a \in Ae.$$

It is immediate that the  $\{\phi_i\}$  belong to  $\text{Hom}_A(Ae, M)$ . We show next that they are linearly independent over  $K$ . If  $\sum \xi_i \phi_i = 0$ ,  $\xi_i \in K$ , we have

$$\sum \xi_i \phi_i(e) = \sum \xi_i (em_i) = \sum \xi_i m_i = 0$$

since  $m_i \in eM$ . The fact that the  $\{m_i\}$  are linearly independent implies that  $\xi_1 = \dots = \xi_r = 0$ , as we wished to show. Finally, let  $\phi \in \text{Hom}_A(Ae, M)$ . Then  $\phi(e) = \phi(e^2) = e\phi(e) \in eM$ , and if we write  $\phi(e) = \sum \xi_i m_i$ ,  $\xi_i \in K$ , then for all  $a \in A$  we have

$$\phi(ae) = a\phi(e) = \sum \xi_i am_i = \sum \xi_i \phi_i(ae).$$

Therefore  $\phi = \sum \xi_i \phi_i$ , and Theorem 54.15 is proved.

Our next result shows that if  $e$  is a primitive idempotent, the intertwining number  $i(Ae, M)$  counts the number of composition factors of  $M$  which are  $A$ -isomorphic to  $Ae/Ne$  [cf. (43.18) for the completely reducible case].

(54.16) THEOREM. *Let  $K$  be a splitting field for a finite-dimensional algebra  $A$ , and let  $M$  be a left  $A$ -module. For any primitive idempotent  $e \in A$ , the number of composition factors of  $M$  which are  $A$ -isomorphic to  $Ae/Ne$ , where  $N = \text{rad } A$ , is exactly  $(eM: K)$ .*

PROOF. Let

$$M = M_1 \supset M_2 \supset \cdots \supset M_{i+1} = (0)$$

be a composition series for  $M$ . Suppose that  $k$  of the composition factors of  $M$  are isomorphic to  $Ae/Ne$ , and let these composition factors be  $\{M_{i,j}/M_{i,j+1}; i_1 < i_2 < \cdots < i_k\}$ . By (54.12),  $M_{i,j}/M_{i,j+1} \cong Ae/Ne$  if and only if  $eM_{i,j} \not\subset M_{i,j+1}$ . Therefore we can find  $\{m_{i,1}, \dots, m_{i,k}\}$  in  $M_{i,1}, \dots, M_{i,k}$ , respectively, such that

$$em_{i,j} \notin M_{i,j+1}, \quad 1 \leq j \leq k.$$

Replacing  $m_{i,j}$  by  $em_{i,j}$ , we may assume that the  $\{m_{i,j}\}$  belong to  $eM$ . Since  $M_{i,j}/M_{i,j+1}$  is irreducible for all  $j$ , we have

$$Am_{i,j} + M_{i,j+1} = M_{i,j}, \quad 1 \leq j \leq k,$$

and hence

$$(54.17) \quad eM_{i,j} = eAe m_{i,j} + M_{i,j+1}, \quad 1 \leq j \leq k.$$

For any  $M_i$  such that  $i \notin \{i_1, \dots, i_k\}$ , we have

$$eM_i \subset M_{i+1}.$$

Let  $a \rightarrow \bar{a}$  be the natural mapping of  $A$  onto the semi-simple algebra  $\bar{A} = A/N$  where  $N = \text{rad } A$ . From Lemma 26.7 we have  $\text{Hom}_A(\bar{A}\bar{e}, \bar{A}\bar{e}) \cong \bar{e}\bar{A}\bar{e}$ , and  $\bar{e}\bar{A}\bar{e} = K \cdot \bar{e}$  since  $K$  is a splitting field for  $A$  (see § 29). Then we have  $eAe = K \cdot e + eNe$ , and, since  $eNe M_i \subset M_{i+1}$  for all  $i$ , we have from (54.17) the result that

$$(54.18) \quad eM_{i,j} = Km_{i,j} + M_{i,j+1}, \quad 1 \leq j \leq k.$$

We prove finally that  $\{m_{i,1}, \dots, m_{i,k}\}$  form a  $K$ -basis for  $eM$ . Obviously they are linearly independent. Now let  $m \in eM$ . Then  $m = em$  implies that  $m \in M_{i,1}$ . By (54.18) there exists  $\xi_1 \in K$  such that

$$m - \xi_1 m_{i,1} \in eM_{i+1},$$

and in fact  $m - \xi_1 m_{i,1} \in M_{i,2}$ . An easy induction argument shows that there exist elements  $\xi_1, \dots, \xi_k \in K$  such that  $m = \sum \xi_j m_{i,j}$ , and the theorem is proved.

Now we indicate what can be done if  $K$  is not a splitting field for  $A$ . This result requires some theorems which will be proved in Chapter X.

(54.19) THEOREM. *Let  $K$  be a perfect field,  $A$  a finite-dimensional algebra over  $K$ , and  $M$  a left  $A$ -module. Let  $k$  be the number of composition factors of  $M$  which are  $A$ -isomorphic to  $Ae/Ne$ , where  $e$  is a primitive idempotent in  $A$ . Then*

$$(eM: K) = k \cdot c,$$

where  $c = (\text{Hom}_A(Ae/Ne, Ae/Ne}): K$ .

**PROOF.** Take a composition series  $\{M_i\}$  and define elements  $\{m_{ij}\}$  as in the proof of Theorem 54.16. Because  $\bar{A}\bar{e} = Ae/Ne$  is an irreducible  $A$ -module,  $D^* = \text{Hom}_A(\bar{A}\bar{e}, \bar{A}\bar{e})$  is a finite-dimensional division algebra over  $K$ . As in (54.16),  $D^* \cong \bar{e}\bar{A}\bar{e} \cong eAe/eNe$ , and by Theorem 54.6,  $eNe = \text{rad } eAe$ . Moreover, because  $K$  is a perfect field,  $D^*$  is a separable algebra over  $K$  (see Chapter X, especially the exercises in §§ 69 and 71). By the Wedderburn-Malcev theorem in § 72, we have

$$eAe = D \oplus eNe$$

where  $D$  is a division algebra in  $eAe$  such that  $D \cong D^*$ . As in the proof of Theorem 54.16, we obtain

$$eM = Dm_{i_1} \oplus \cdots \oplus Dm_{i_k}.$$

Counting dimensions over  $K$ , we have

$$(eM: K) = (D: K)k,$$

and the theorem is proved.

### Exercises

- Let  $A = KG$  where  $G$  is a  $p$ -group for a prime  $p$ , and  $K$  is a field of characteristic  $p$ . Prove that the left regular module  $\mathbb{A}$  is indecomposable and hence that  $\mathbb{A}$  is the unique principal indecomposable  $A$ -module. [Hint: Use Theorem 27.28, which holds even when  $K$  is not algebraically closed.]
- Prove that every direct summand of  $\mathbb{A}$  is a sum of principal indecomposable  $A$ -modules. More generally, show that every direct summand of the module  $\mathbb{A} + \cdots + \mathbb{A}$  ( $n$  terms) is a direct sum of principal indecomposable  $A$ -modules.

## § 55. The Classification of the Principal Indecomposable Modules into Blocks

In this section we take up the two-sided decomposition of a non-semi-simple ring  $A$ . For a general ring with minimum condition, this problem turns out to be a somewhat more delicate matter than the corresponding problem for semi-simple rings presented in Chapter IV. Two facts are needed as a starting point: first, that  $\mathbb{A}$  and each of its submodules possesses a composition series [Theorem 54.1]; and second, that a principal indecomposable module  $Af$  has

a composition factor isomorphic to  $Ae/Ne$  if and only if  $eAf \neq 0$  [Theorem 54.12].

A two-sided ideal  $B$  in  $A$  is said to be *indecomposable* if it is impossible to express  $B$  as a direct sum of two non-zero two-sided ideals of  $A$ . From the minimum condition, it follows that we may write

$$A = B_1 \oplus \cdots \oplus B_s$$

where the  $B_i$  are non-zero indecomposable two-sided ideals. We shall see that the ideals  $B_i$  are uniquely determined in the strong sense that if  $B$  is any two-sided ideal such that  $A = B \oplus B'$  for some other two-sided ideal  $B'$ , then  $B$  is a direct sum of some of the  $B_i$ ,  $1 \leq i \leq s$ . The essential problem is to characterize in some reasonable way the principal indecomposable modules which are contained in a given ideal  $B_i$ . The next definition turns out to settle the question.

(55.1) **DEFINITION.** Two principal indecomposable modules of  $A$  generated by primitive idempotents  $e$  and  $f$  are said to be *linked* if there exists a sequence  $e_1, \dots, e_m$  of primitive idempotents with  $e_1 = e$ ,  $e_m = f$ , such that for each  $i$ ,  $Ae_i$  and  $Ae_{i+1}$  have a composition factor in common. Two primitive idempotents  $e$  and  $f$  are said to be *linked* whenever the modules  $Ae$  and  $Af$  are linked. The relation of being linked is an equivalence relation, and we may split up the set of all principal indecomposable modules into a finite number of equivalence classes. The sum of all the principal indecomposable modules belonging to a given equivalence class is called a *block* of  $A$ .

(55.2) **THEOREM.** *The blocks of  $A$  are two-sided ideals, no two of which have a composition factor in common when regarded as left  $A$ -modules. The blocks are indecomposable two-sided ideals, and  $A$  is their direct sum. If  $A = B_1 \oplus B_2 \oplus \cdots \oplus B_s$  is any decomposition of  $A$  into indecomposable two-sided ideals, the direct summands  $B_i$  are precisely the blocks of  $A$ .*

**PROOF.** In this argument  $Ae$ ,  $Af$ ,  $Ae_i$ ,  $\dots$  denote principal indecomposable modules generated by primitive idempotents  $e$ ,  $f$ ,  $e_i$ ,  $\dots$ . If  $Ae$  and  $Af$  belong to different equivalence classes, then  $AeAf=0$ ; otherwise  $eAf \neq 0$ , and  $Ae$  and  $Af$  have a composition factor in common by Theorem 54.12. If  $Ae$  and  $Af$  belong to the same equivalence class then  $AeAf \subset Af$ . Since the blocks are sums of principal indecomposable modules, these remarks imply that the blocks are two-sided ideals  $B_1, \dots, B_s$  such that  $B_iB_j = 0$  if  $i \neq j$ .

It is clear that  $A$  is the sum of the blocks.

For a given primitive idempotent  $e$ , a block  $B_i$  has a composition factor isomorphic to  $Ae/Ne$  if and only if  $eB_i \neq 0$ . Now suppose  $eB_i \neq 0$  and  $eB_j \neq 0$  for two blocks  $B_i$  and  $B_j$ . Then for some principal indecomposable modules  $Ae_i$  and  $Ae_j$  belonging to the equivalence classes of  $B_i$  and  $B_j$ , respectively, we have  $eAe_i \neq 0$  and  $eAe_j \neq 0$ . These relations imply that  $Ae_i$  and  $Ae_j$  are linked and that  $B_i = B_j$ . Therefore two distinct blocks cannot have a common composition factor, and it follows that  $A$  is the direct sum of the blocks.

Finally, we shall prove that the blocks are indecomposable and unique in the following way: As we have pointed out, the minimum condition implies that

$$(55.3) \quad A = B'_1 \oplus \cdots \oplus B'_t,$$

where the  $B'_i$  are indecomposable two-sided ideals. We shall prove that the set of the  $\{B'_i\}$ ,  $1 \leq i \leq t$ , coincides with the set of blocks. Let  $e$  be a primitive idempotent in  $A$ . Then (55.3) implies that

$$Ae = B'_1 e \oplus \cdots \oplus B'_t e,$$

and because  $Ae$  is indecomposable, we have  $Ae = B'_k e$  for some  $k$ . Therefore each principal indecomposable module  $Ae$  belongs to exactly one summand  $B'_k$  of (55.3). Next we observe that  $AeA$  belongs to a unique summand of (55.3), namely, the one to which  $Ae$  belongs. From this, we see that  $eAf \neq 0$  implies that  $AeA \cap AfA \neq 0$ , and hence  $AeA$  and  $AfA$  belong to a unique summand  $B'_k$  which also contains  $eAf \subset AeA \cap AfA$ .

Now let  $Ae \subset B'_k$ , and let  $Af$  belong to the same equivalence class as  $Ae$ . Then there exist primitive idempotents  $e_1, \dots, e_h$  with  $e_1 = e$ ,  $e_h = f$ , such that  $Ae_i$  and  $Ae_{i+1}$  have a composition factor in common for  $i = 1, 2, \dots, h-1$ . For a fixed  $i$ , the composition factor common to  $Ae_i$  and  $Ae_{i+1}$  is isomorphic to  $Ae'/Ne'$  for some primitive idempotent  $e'$ . Then  $e'Ae_i \neq 0$  and  $e'Ae_{i+1} \neq 0$ . Therefore  $Ae_i A$  and  $Ae_{i+1} A$  both belong to the same summand of (55.3) as  $Ae' A$ . Applying this argument for  $i = 1, 2, \dots, h-1$ , we conclude that  $Ae$  and  $Af$  belong to the same summand  $B'_k$ . Therefore  $B'_k$  is a direct sum of blocks, and since  $B'_k$  is assumed to be indecomposable,  $B'_k$  actually coincides with one of the blocks. Since every block is contained in one of the summands  $B'_i$ , it follows that the  $B'_i$  constitute the full set of blocks, and Theorem 55.2 is proved.

(55.4) DEFINITION. Two irreducible left  $A$ -modules are said to belong to the same block if they both are composition factors of the

same block.

By Theorem 55.2, it follows that an irreducible module appears as a composition factor of exactly one block, so that we may speak unambiguously of the block to which a given irreducible  $A$ -module belongs. We note also that the irreducible modules  $Ae/Ne$  and  $Af/Nf$  belong to the same block if and only if  $Ae$  and  $Af$  are linked.

### Exercises

1. Prove directly that in a ring  $A$  with minimum condition, we have a decomposition

$$A = B_1 \oplus \cdots \oplus B_s$$

where the  $B_i$  are indecomposable two-sided ideals, and that if  $B$  is a two-sided ideal such that

$$A = B \oplus B'$$

for some other two-sided ideal  $B'$ , then  $B$  is a sum of a subfamily of the  $\{B_i\}$ ,  $1 \leq i \leq s$ .

2. An idempotent  $e$  in a ring with minimum condition is called *centrally primitive* if  $e$  belongs to the center of  $A$  and if  $e$  is not a sum of orthogonal idempotents belonging to the center. Prove that  $e$  is a centrally primitive idempotent if and only if  $Ae$  is a block of  $A$ .

3. Let  $A$  be a finite-dimensional algebra over an algebraically closed field  $K$ . Let  $V_1$  and  $V_2$  be irreducible left  $A$ -modules, and  $F_1$  and  $F_2$  the irreducible representations of  $A$  afforded by  $V_1$  and  $V_2$ , respectively. For any element  $c$  of the center of  $A$ , we have, by Schur's lemma,  $F_i(c) = \xi_i(c)1_{V_i}$ ,  $i = 1, 2$ , where  $\xi_i(c) \in K$  and  $1_{V_i}$  is the identity mapping on  $V_i$ . Prove that  $V_1$  and  $V_2$  belong to the same block if and only if  $\xi_1(c) = \xi_2(c)$  for all  $c$  belonging to the center of  $A$ . [Hint: Use the preceding exercise, and show that, if  $e$  is a centrally primitive idempotent, then  $Ce$  is a completely primary ring where  $C$  is the center of  $A$ ; then look at the action of the elements of  $Ce$  on the irreducible modules belonging to the block  $eA$ .]

## § 56. Projective Modules

Not every indecomposable left module for a ring with minimum condition is a principal indecomposable module. In this section we shall give a useful characterization of modules which are direct sums of principal indecomposable modules. We require first a few preliminary remarks.

Let  $\{M_i\}$  be a family, not necessarily finite, of submodules of a left  $A$ -module  $M$ . We recall from Chapter II, § 11, that  $M$  is said to be the *direct sum* of the submodules  $\{M_i\}$  if (a)  $\sum M_i = M$  and

(b) every element of  $M$  can be expressed uniquely as a finite sum of elements belonging to distinct submodules  $M_i$ . A module  $M$  is called a *free* left  $A$ -module if  $M$  is a direct sum of a family of submodules  $\{M_i\}$  each of which is  $A$ -isomorphic to  $_A A$ .

A subset  $X$  of a module  $M$  is called a *set of generators* of  $M$  if every element of  $M$  can be expressed in the form  $\sum a_i x_i$  with coefficients  $a_i$  in  $A$  and  $x_i$  in  $X$ . The module  $M$  is said to be *finitely generated* if  $M$  has a finite set of generators. A set of generators  $X$  of  $M$  is called a *basis* of  $M$  if the expressions  $\sum a_i x_i$  are unique, i.e.,  $\sum a_i x_i = \sum b_i x_i$  implies  $a_i = b_i$  for all  $i$ . It is easily checked that a left  $A$ -module is free if and only if it has a basis.

A *sequence* of  $A$ -modules

$$(56.1) \quad M_1 \xrightarrow{\theta_1} M_2 \xrightarrow{\theta_2} M_3 \longrightarrow \dots$$

consists of an ordered family of  $A$ -modules  $M_1, M_2, \dots$ , with  $A$ -homomorphisms  $\theta_i: M_1 \rightarrow M_2, \theta_2: M_2 \rightarrow M_3$ , etc. For  $i > 1$ , we say that the sequence is *exact* at  $M_i$  if the image  $\theta_{i-1}(M_{i-1})$  coincides with the kernel of  $\theta_i$ . Thus the sequence

$$0 \longrightarrow L \xrightarrow{\lambda} M$$

is exact at  $L$  if and only if  $\lambda$  is an isomorphism of  $L$  into  $M$ . Likewise the sequence

$$M \xrightarrow{\mu} N \longrightarrow 0$$

is exact at  $N$  if and only if  $\mu$  maps  $M$  onto  $N$ .

The sequence (56.1) is said to be *exact* if it is exact at each  $M_i, i = 2, 3, \dots$ . In particular, suppose we have an exact sequence

$$(56.2) \quad 0 \longrightarrow L \xrightarrow{\lambda} M \xrightarrow{\mu} N \longrightarrow 0,$$

and set  $L' = \lambda(L)$ . Then  $L' \cong L$ , and  $L'$  is the kernel of  $\mu$ , so that

$$M/L' \cong N.$$

In accordance with the terminology of § 7, whenever we have an exact sequence (56.2), we shall call  $M$  an *extension* of  $N$  by  $L$ . We shall say that  $M$  is a *split extension* and that the sequence (56.2) *splits*, provided that  $L'$  is a direct summand of  $M$ .

(56.3) *The exact sequence (56.2) splits if and only if there exists a homomorphism  $\nu: N \rightarrow M$  such that  $\mu\nu = 1$  on  $N$ .*

For the proof see the discussion following Definition 7.4.

(56.4) DEFINITION. A left  $A$ -module  $M$  is called a *projective*  $A$ -module if every exact sequence

$$0 \rightarrow P \rightarrow N \rightarrow M \rightarrow 0$$

splits.

Because of what has been said, an  $A$ -module  $M$  is projective if and only if

$$M \cong N/P$$

implies that  $P$  is a direct summand of  $N$ , for all  $A$ -modules  $N$  and  $P$ .

(56.5) THEOREM. Let  $M = M_1 \oplus M_2$ , where  $M_1$  and  $M_2$  are submodules of  $M$ . Then  $M$  is projective if and only if  $M_1$  and  $M_2$  are projective.

PROOF. Let  $M$  be projective, and let  $\eta$  be a homomorphism of a module  $N$  onto  $M_1$  with kernel  $P$ . Then, using the identity mapping of  $M_2$  onto itself, we obtain a homomorphism of  $N + M_2$  onto  $M_1 \oplus M_2 = M$ , still with kernel  $P$ . Since  $M$  is projective, there exists a submodule  $S$  of  $N + M_2$  such that  $N + M_2 = P \oplus S$ . Let  $P' = S \cap N$ . Then  $P \cap P' = 0$ , and, upon writing  $n$  in  $N$  in the form  $n = p + s$ ,  $p \in P$ ,  $s \in S$ , we have  $s \in P'$ , and so  $N = P \oplus P'$ . Therefore  $M_1$  is projective. Similarly  $M_2$  is projective.

Conversely, let  $M_1$  and  $M_2$  be projective, and let  $\eta$  be a homomorphism of a module  $N$  onto  $M = M_1 \oplus M_2$  with kernel  $P$ . Let  $\theta$  be the projection of  $M$  onto  $M_1$ , and let  $R = \eta^{-1}(M_2)$ . Then  $\theta\eta$  is a homomorphism of  $N$  onto  $M_1$  with kernel  $R$ . Since  $M_1$  is projective,  $N = R \oplus R'$  for some submodule  $R'$ . Then  $\eta$  restricted to  $R$  is a homomorphism of  $R$  onto  $M_2$  with kernel  $P$ , and, since  $M_2$  is projective,  $R = P \oplus R''$ . Then  $N = P \oplus R' \oplus R''$ , and we have proved that  $M$  is projective.

(56.6) THEOREM. Let  $M$  be a finitely generated left  $A$ -module, where  $A$  is a ring with minimum condition. Then the following conditions are equivalent:

- (i)  $M$  is projective.
- (ii)  $M$  is a direct summand of a free left  $A$ -module.
- (iii)  $M$  is a direct sum of principal indecomposable modules of  $A$ .

PROOF. Condition (i) implies (ii). Let  $\{x_i\}$  be a set of generators of  $M$ , and let  $F$  be a free left  $A$ -module with a basis  $\{y_i\}$  which is in one-to-one correspondence with the elements  $\{x_i\}$ . Then the

mapping  $\sum a_i y_i \rightarrow \sum a_i x_i$ ,  $a_i \in A$ , is a homomorphism  $\eta$  of  $F$  onto  $M$ . Let  $P$  be the kernel of  $\eta$ . Since  $M$  is projective,  $F = P \oplus P'$  for some module  $P'$ , and we have  $P' \cong M$ , proving that  $M$  is isomorphic to a direct summand of a free module.

Condition (ii) implies (iii). (See Exercise 54.2.) Because each generator of  $M$  is a linear combination of at most a finite number of basis elements of the free module, and because  $M$  is finitely generated, it follows that  $M$  is actually a direct summand of a free module  $F$  with a finite basis. The module  $F$  itself is a direct sum of a finite number of principal indecomposable modules of  $A$ . Because  $M$  is a direct summand of  $F$ , the Krull-Schmidt theorem may be applied, and we obtain the result that  $M$  is a direct sum of a finite number of principal indecomposable modules of  $A$ .

Obviously (iii) implies (ii). We prove finally that (ii) implies (i). By Theorem 56.5, it is sufficient to prove that a free module  $F$  is projective. Let  $\{x_i\}$  be a basis for  $F$ , and let  $\theta$  be a homomorphism of a module  $N$  onto  $F$  with kernel  $P$ . Choose elements  $\{y_i\}$  in  $N$  such that  $\theta y_i = x_i$ . Then  $\zeta: \sum a_i x_i \rightarrow \sum a_i y_i$  is a homomorphism of  $F$  into  $N$  such that  $\theta \zeta = 1$ . Let  $\zeta(F) = P'$ . Then  $P \cap P' = 0$ , since  $p \in P \cap P'$ ,  $p = \zeta f$ ,  $f \in F$ , imply  $f = \theta \zeta f = 0$ , and hence  $p = 0$ . For every  $n \in N$ , we have  $n - \zeta \theta n \in P$ . Therefore  $N = P \oplus P'$ , and we have proved that  $F$  is projective.

We remark that the equivalence of conditions (i), (ii), and (iii) of Theorem 56.6 holds even when the hypothesis that  $M$  is finitely generated is dropped altogether (Cartan and Eilenberg [1], p. 6; Nagao and Nakayama [1]).

### Exercises

1. Are submodules or quotient modules of projective modules necessarily projective?
2. Prove that a projective module over a completely primary ring is free.
3. The statements below show that in some respects the standard theorems on vector spaces over skewfields admit generalizations to projective modules over arbitrary rings with minimum condition. Throughout the discussion let  $A$  be a ring with minimum condition, and let  $M$  be a projective finitely generated left  $A$ -module. As in the vector space case, we define the *dual*  $M'$  of  $M$  to be  $\text{Hom}_A(M, AA)$ . Then  $M'$  becomes a right  $A$ -module if we define

$$(fa)(x) = f(x)a, \quad x \in M, f \in M', a \in A.$$

Then:

- (a)  $M'$  is a projective finitely generated right  $A$ -module.
- (b)  $M$  is naturally isomorphic with  $M''$ .
- (c) For  $f \in M'$ ,  $x \in M$ , let  $f \otimes x$  be the (right) operator on  $M$  defined by

$$u(f \otimes x) = f(u)x, \quad u \in M.$$

Prove that the "product"  $f \otimes x$  is biadditive and that

$$fa \otimes x = f \otimes ax, \quad a \in A.$$

(d) Show that  $f \otimes x \in \text{Hom}_A(M, M)$  for all  $f \in M, x \in M$ , and that every element of  $\text{Hom}_A(M, M)$  can be expressed in the form  $\sum f_i \otimes x_i, f_i \in M'$ ,  $x_i \in M$ .

(e) For an  $A$ -submodule  $N'$  of  $M'$ , show that  $N' \otimes M = \{\sum f_i \otimes u_i : f_i \in N', u_i \in M\}$  is a left ideal in  $\text{Hom}_A(M, M)$  and that the mapping  $N' \rightarrow N' \otimes M$  is a one-to-one correspondence between the set of all  $A$ -submodules of  $M'$  and the left ideals in  $\text{Hom}_A(M, M)$ .

(f) Prove that  $\text{Hom}_A(M, M)$  is a ring with minimum condition.

4. Let  $A$  be a ring with minimum condition, and let  $F$  be a free left  $A$ -module with a finite basis. Prove that  $\text{Hom}_A(F, F)$  satisfies the minimum condition for left ideals, either using Exercise 56.3 or by a more direct argument.

5. Let  $A$  be a ring with minimum condition, and let  $M$  be a finitely generated projective left  $A$ -module. Then  $M$  is a direct summand of a free module  $F$  with a finite basis. Prove that  $\text{Hom}_A(M, M)$  is isomorphic to  $eCe$  where  $C = \text{Hom}_A(F, F)$  and  $e$  is an idempotent in  $C$ .

6. (Cartan and Eilenberg [1]) Let  $R$  be a commutative integral domain with quotient field  $K$ . Prove that an ideal  $I$  in  $R$  is a projective  $R$ -module if and only if  $I$  is an invertible ideal in the sense that there exist  $\mu_1, \dots, \mu_n \in K$ ,  $\alpha_1, \dots, \alpha_n \in I$  such that  $\mu_i \alpha_i \in R$ ,  $1 \leq i \leq n$ , and  $\sum \mu_i \alpha_i = 1$ . (See §22.) In particular, show that every ideal in a Dedekind ring is projective and more generally, that every finitely generated torsion free module over a Dedekind ring is projective.

7. (Cartan-Eilenberg.) Let  $A$  be an arbitrary ring with 1. Prove that a left  $A$ -module  $M$  is projective if and only if every diagram

$$\begin{array}{ccc} M & & \\ \downarrow & & \\ P \rightarrow R \rightarrow 0 & & \end{array}$$

in which the row is exact can be completed to a commutative diagram

$$\begin{array}{ccc} M & & \\ \swarrow \downarrow & & \\ P \rightarrow R \rightarrow 0 & & \end{array}$$

[Hint: First prove the equivalence of (i) and (ii) of Theorem 56.6 in the general case.]

## § 57. Injective Modules

There is a fairly obvious dual concept to the notion of projective module defined in (56.4). Namely, we might consider those

modules  $M$  with the property that every exact sequence

$$0 \rightarrow M \rightarrow N \rightarrow P \rightarrow 0$$

is a split exact sequence. A module  $M$  has this property if and only if whenever  $M$  is a submodule of a module  $N$ , then  $M$  is a direct summand of  $N$ . In these terms, this concept was first defined and studied for abelian groups by Baer [1]. It turns out to be of great importance in the theory of rings with minimum condition, and this section is devoted to the development of this idea. After some preliminary remarks, a definition is given which is apparently different from the one above but is more convenient in some ways; later in the section its equivalence with the first definition will be established.

Unlike the theory of projective modules, it does not seem to be possible to study the above concept wholly in the framework of rings with minimum condition. In this section we shall consider a ring  $A$  with 1, and left  $A$ -modules which are not assumed to satisfy any finiteness conditions.

It will also be necessary to use a form of Zorn's lemma, which we shall formulate as an axiom (See § 15 A). We begin with some definitions. A *partially ordered set* is a set together with a relation  $\geq$  (read "contains") which is *transitive* ( $a \geq b, b \geq c$  imply  $a \geq c$ ) *reflexive* (i.e.,  $a \geq a$ ), and satisfies the condition that  $a \geq b, b \geq a$  imply  $a = b$ . A subset  $S$  of a partially ordered set is said to be *totally ordered* if any two elements of  $S$  are comparable, i.e.,  $a, b \in S$  imply either  $a \geq b$  or  $b \geq a$ . An element  $b$  is called an *upper bound* of a subset  $S$  if  $b \geq s$  for all  $s \in S$ . An element  $t$  in a subset  $S$  is called a *maximal element* of  $S$  if  $t' \geq t$  for  $t' \in S$  implies  $t' = t$ . The most familiar example of a partially ordered set is a family of subsets of some set, partially ordered by the relation of inclusion. We shall state as an axiom the following result, which is a form of Zorn's lemma and is equivalent to the axiom of choice.

(57.1) **MAXIMUM PRINCIPLE.** *Let  $P$  be a partially ordered set with the property that every totally ordered subset of  $P$  has an upper bound. Then  $P$  contains a maximal element.*

Now we come to the definition of injective modules.

(57.2) **DEFINITION.** A left  $A$ -module  $M$  is said to be *injective* if whenever we are given left  $A$ -modules  $P$  and  $R$  with  $P \subset R$ , and a homomorphism  $\eta$  of  $P$  into  $M$ , there always exists a homomorphism  $\eta'$  of  $R$  into  $M$  such that  $\eta'$  is an extension of  $\eta$ , i.e.,  $\eta'|P = \eta$ .

In terms of sequences, a left  $A$ -module  $M$  is injective if and only if every diagram

$$\begin{array}{ccc} 0 & \longrightarrow & P \xrightarrow{i} R \\ & \eta \downarrow & \\ & & M \end{array}$$

in which the row is an exact sequence, can be completed to a diagram

$$\begin{array}{ccc} 0 & \longrightarrow & P \xrightarrow{i} R \\ & \eta \downarrow & \swarrow \eta' \\ & & M \end{array}$$

which is commutative in the sense that  $\eta'i = \eta$ .

(57.3) THEOREM. Let  $M = M_1 \oplus M_2$  where  $M_1$  and  $M_2$  are submodules of  $M$ . Then  $M$  is an injective left  $A$ -module if and only if  $M_1$  and  $M_2$  are both injective left  $A$ -modules.

PROOF. Let  $M$  be injective, let  $P \subset R$ , and let  $\eta$  be a homomorphism of  $P$  into  $M_1$ . Because  $M$  is injective, there exists a homomorphism  $\eta'$  of  $R$  into  $M$  which extends  $\eta$ . Let  $\pi$  be the projection of  $M$  onto  $M_1$ . Then  $\eta'' = \pi\eta'$  is also an extension of  $\eta$  which maps  $R$  into  $M_1$ , and we have proved that  $M_1$  is injective. Similarly  $M_2$  is injective.

Conversely, let  $M_1$  and  $M_2$  be injective, let  $P \subset R$  be left  $A$ -modules, and let  $\eta$  be an  $A$ -homomorphism of  $P$  into  $M$ . Let  $\pi_1$  and  $\pi_2$  be the projections of  $M$  onto  $M_1$  and  $M_2$ , respectively. Because  $M_1$  and  $M_2$  are injective, the mappings  $\pi_1\eta$  and  $\pi_2\eta$  can be extended to homomorphisms  $\eta'_1$  and  $\eta'_2$  of  $R$  into  $M_1$  and  $M_2$ , respectively. Define  $\eta'r = \eta'_1r + \eta'_2r$ ,  $r \in R$ ; then it is immediate that  $\eta'$  is a homomorphism of  $R$  into  $M$ . Because

$$\eta'p = \eta'_1p + \eta'_2p = \pi_1\eta p + \pi_2\eta p = \eta p,$$

$\eta'$  extends  $\eta$ , and we have proved that  $M$  is injective.

We begin a series of lemmas which lead up to the important result that every left  $A$ -module can be imbedded in an injective one. Our approach to this problem is based on an ingenious paper of Eckmann and Schöpf [1].

(57.4) DEFINITION. Let  $Z$  be the ring of rational integers. A left  $Z$ -module  $G$  is *divisible* if  $mG = G$  for all integers  $m \neq 0$ .

(57.5) LEMMA. *A left  $Z$ -module  $G$  is divisible if and only if it is injective.*

PROOF. Let  $G$  be divisible. Let  $P \subset R$ , where  $P$  and  $R$  are  $Z$ -modules, and let  $\phi: P \rightarrow G$  be a homomorphism. We shall use the maximum principle to construct an extension of  $\phi$  to  $R$ . Consider the set of all pairs  $(P', \phi')$  where  $R \supset P' \supset P$  and  $\phi'$  is an extension of  $\phi$ . We define a partial ordering  $(P', \phi') \geq (P'', \phi'')$  if  $P' \supset P''$  and if  $\phi'$  is an extension of  $\phi''$ . By the maximum principle, there exists a maximal element  $(P_0, \phi_0)$ . We prove that  $P_0 = R$  by showing that if  $P_0$  is a proper submodule of  $R$ , we contradict the maximal property of  $P_0$ . Let  $P_0 \neq R$ , and let  $u \in R, u \notin P_0$ . If the sum  $Zu + P_0$  is direct, we can extend  $\phi_0$  to  $P'_0 = Zu \oplus P_0$  by defining  $\phi'_0$  arbitrarily on  $u$ . Suppose that  $Zu \cap P_0 \neq 0$ , and let  $m$  be the least positive integer such that  $mu \in P_0$ . Because  $mG = G$ , there exists an element  $g \in G$  such that  $mg = \phi_0(mu)$ . Then define  $\phi'_0(au + p_0) = ag + \phi_0(p_0), p_0 \in P_0, a \in Z$ . We first verify that  $\phi'_0$  is well defined. If  $au + p_0 = 0$ , then  $m|a$  and  $a = ma'$  for some integer  $a'$ . Then  $a'(mu) + p_0 = 0$  where both summands are in  $P_0$ , and  $\phi'_0(a'mu + p_0) = ag + \phi_0(p_0) = 0$ . Thus  $\phi'_0$  is well defined. The mapping  $\phi'_0$  is clearly an  $A$ -homomorphism extending  $\phi_0$ ; hence  $(P'_0, \phi'_0)$  strictly contains  $(P_0, \phi_0)$ . Since  $(P_0, \phi_0)$  was assumed to be maximal, we must have  $P_0 = R$ , proving that  $G$  is injective.

Conversely, suppose that  $G$  is injective, and let  $m \neq 0$  be an element of  $Z$ . For any  $g$  in  $G$ , the mapping  $\phi: km \rightarrow kg, k \in Z$ , is a homomorphism of  $Zm$  into  $G$ . Then  $\phi$  can be extended to a homomorphism  $\phi'$  of  $Z$  into  $G$ . Let  $h = \phi'(1)$ . Then  $\phi'(m1) = mh = g$ , and we have proved that  $mG = G$ . Therefore  $G$  is divisible, and Lemma 57.5 is proved.

(57.6) LEMMA. *Every  $Z$ -module  $G$  can be imbedded in a divisible one.*

PROOF. Obviously the additive group of rational numbers  $Q$  is divisible; the direct sum of any number of copies of  $Q$  is divisible, and any homomorphic image of such a module is divisible. Let  $\{x_i\}$  be a set of generators for  $G$ ; then the free module  $F$  with basis  $\{y_i\}$  in one-to-one correspondence with the basis  $\{x_i\}$  admits a homomorphism  $\phi$  of  $F$  onto  $G$  namely  $\sum a_i y_i \rightarrow \sum a_i x_i, a_i \in Z$ . Now  $F$  is a submodule of a  $Z$ -module  $H = \sum Qy_i$ , which is a direct sum of copies of  $Q$ . Let  $P$  be the kernel of  $\phi$  in  $F$ ; then  $P$  is also a submodule of  $H$ , and we have  $G \cong F/P \subset H/P$ . Since  $H/P$  is divisible, Lemma 57.6 is proved.

(57.7) LEMMA. Let  $G$  be an injective  $Z$ -module, and let  $A$  be an arbitrary ring with 1. Then  $\text{Hom}_Z(A, G)$  is an injective left  $A$ -module.

PROOF. We first make  $\text{Hom}(A, G)$  into a left  $A$ -module by defining

$$(a\phi)b = \phi(ba),$$

for  $a, b \in A$  and  $\phi \in \text{Hom}_Z(A, G)$ . From the definition, we have  $ab\phi = a(b\phi)$ , and the other module axioms are easily verified.

Now we have to prove that  $\text{Hom}_Z(A, G)$  is injective. Let  $P$  and  $R$  be left  $A$ -modules, with  $P \subset R$ , and let

$$\psi: P \rightarrow \text{Hom}_Z(A, G)$$

be an  $A$ -homomorphism. Our plan is to show that  $\psi$  gives rise to a  $Z$ -homomorphism  $\Psi$  of  $P \rightarrow G$ . Then since  $G$  is an injective  $Z$ -module,  $\Psi$  can be extended to a  $Z$ -homomorphism  $\Psi^*: R \rightarrow G$ . But then  $\Psi^*$  will give us an  $A$ -homomorphism

$$\psi^*: R \rightarrow \text{Hom}_Z(A, G)$$

which extends  $\psi$ . In more detail, define the  $Z$ -homomorphism  $\Psi: P \rightarrow G$  by

$$\Psi(p) = [\psi(p)](1), \quad p \in P,$$

where 1 is the identity element of  $A$ . It is clear that  $\Psi \in \text{Hom}_Z(P, G)$ , and since  $G$  is injective, there exists a  $Z$ -homomorphism  $\Psi^*: R \rightarrow G$  which is an extension of  $\Psi$ . Now define  $\psi^*: R \rightarrow \text{Hom}_Z(A, G)$  by setting

$$[\psi^*(r)](a) = \Psi^*(ar), \quad a \in A, r \in R.$$

Then  $\psi^*(r) \in \text{Hom}_Z(A, G)$ , and  $\psi^*$  is clearly a  $Z$ -homomorphism. Now let  $a, b \in A$  and  $r \in R$ ; then

$$[\psi^*(ar)](b) = \Psi^*(bar)$$

whereas

$$[a\psi^*(r)](b) = [\psi^*(r)](ba) = \Psi^*(bar),$$

so we have proved that  $\psi^*$  is an  $A$ -homomorphism. Finally we have to check that  $\psi^*$  is an extension of  $\psi$ . Let  $p \in P, a \in A$ ; then

$$\begin{aligned} [\psi^*(p)](a) &= \Psi^*(ap) = \Psi(ap) = [\psi(ap)](1) \\ &= [a\psi(p)](1) = [\psi(p)](a) \end{aligned}$$

since  $\Psi^*$  extends  $\Psi$ , and since  $\psi$  is an  $A$ -homomorphism. This

completes the proof.

(57.8) THEOREM. *Let  $A$  be a ring with 1, and  $M$  a left  $A$ -module. Then  $M$  can be imbedded in an injective left  $A$ -module.*

PROOF. First, we view  $M$  as a left  $Z$ -module. As such, it can be imbedded in an injective  $Z$ -module  $G$ , by Lemmas (57.6) and (57.5). Now the trick is to observe that, as left  $A$ -modules,

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

and that

$$\text{Hom}_A(A, M) \subset \text{Hom}_Z(A, M) \subset \text{Hom}_Z(A, G).$$

By Lemma 57.7,  $\text{Hom}_Z(A, G)$  is an injective left  $A$ -module, and the theorem is proved.

We are now in a position to prove the equivalence of the concept of injective module with the definition given at the beginning of the section.

(57.9) THEOREM. *A left  $A$ -module  $M$  is injective if and only if for each left  $A$ -module  $N$ ,  $M \subset N$  implies that  $M$  is a direct summand of  $N$ .*

PROOF. First, suppose  $M$  is injective, and let  $M \subset N$  for some  $A$ -module  $N$ . Let  $\eta: M \rightarrow M$  be the homomorphism given by  $\eta m = m$ ,  $m \in M$ . By Definition 57.2,  $\eta$  can be extended to an  $A$ -homomorphism  $\eta': N \rightarrow M$ . Then  $\eta' m = m$  for all  $m \in M$ , and  $\eta'$  is a projection of  $N$  upon  $M$ . Therefore  $M$  is a direct summand of  $N$ .

Conversely, suppose  $M$  is a direct summand of every module which contains it. By Theorem 57.8,  $M$  can be imbedded in an injective module. Therefore  $M$  is a direct summand of an injective module, and is injective by Theorem 57.3. This completes the proof of the theorem.

Our next objective is to show that every  $A$ -module  $M$  can be imbedded in a uniquely determined smallest injective module, and we shall determine some of the properties of this module which were first discovered by Eckmann and Schopf [1].

(57.10) DEFINITION. Let  $M$  be a left  $A$ -module. A module  $N$  containing  $M$  is called an *injective hull* of  $M$  if (a)  $N$  is injective; and (b) there is no injective left  $A$ -module  $R$  different from  $N$  such that  $M \subset R \subset N$ .

(57.11) DEFINITION. A left  $A$ -module  $N$  containing  $M$  as a submodule is called a *related extension* of  $M$  if every non-zero submodule

of  $N$  has a non-zero intersection with  $M$ . A related extension  $N$  of  $M$  is called a *maximal related extension* if it is impossible to find another related extension  $N'$  of  $M$  and an isomorphism  $\phi$  of  $N$  into  $N'$  with  $\phi m = m$ ,  $m \in M$ , such that  $\phi(N) \neq N'$ .

The next lemma states that every related extension of  $M$  can be imbedded isomorphically in an arbitrary injective module containing  $M$ .

(57.12) LEMMA. *Let  $T$  be a fixed injective module containing  $M$ , and let  $N$  be an arbitrary related extension of  $M$ . Then there exists a submodule  $N'$  of  $T$  containing  $N$  such that the identity mapping  $\epsilon$  of  $M$  onto itself can be extended to an isomorphism of  $N$  onto  $N'$ . Furthermore,  $N'$  is a related extension of  $M$ .*

PROOF. Since  $M \subset N$  and  $\epsilon: M \rightarrow M \subset T$  is a homomorphism, Definition 57.2 implies that  $\epsilon$  can be extended to an  $A$ -homomorphism  $\epsilon'$  of  $N$  into  $T$ . Let  $N' = \epsilon'(N)$ . The kernel of  $\epsilon'$ , if different from zero, must have a non-zero intersection with  $M$  because  $N$  is a related extension of  $M$ , and this contradicts the fact that  $\epsilon'$  extends  $\epsilon$ . Therefore  $\epsilon'$  is an isomorphism of  $N$  onto  $N'$ , and  $N'$  is a related extension of  $M$ . This completes the proof.

(57.13) THEOREM (Eckmann and Schöpf [1]). *Let  $M$  be a left  $A$ -module. Any injective module  $N$  containing  $M$  contains an injective hull of  $M$ . A left  $A$ -module  $N$  containing  $M$  is an injective hull of  $M$  if and only if  $N$  is a maximal related extension of  $M$ . Let  $\phi: M \cong M'$  be an  $A$ -isomorphism, and let  $H$  and  $H'$  be injective hulls of  $M$  and  $M'$  respectively. Then  $\phi$  can be extended to an  $A$ -isomorphism of  $H$  onto  $H'$ .*

PROOF. Let  $T$  be an arbitrary injective module containing  $M$ . By the maximum principle, there exists a related extension  $H$  of  $M$  such that  $M \subset H \subset T$  and such that  $H$  is not properly contained in any other related extension  $H'$  such that  $M \subset H \subset H' \subset T$ . We prove now that  $H$  is a maximal related extension of  $M$  in the sense of Definition 57.11. Suppose to the contrary that  $H''$  is a related extension of  $M$  properly containing  $H$ . Then  $H''$  is a related extension of  $H$ , and since  $T$  is an injective module containing  $H$ , we can apply Lemma 57.12 to obtain an isomorphism  $\phi$  of  $H''$  into  $T$  which agrees with the identity mapping on  $H$ , and hence on  $M$ . Then  $\phi(H'')$  is a related extension of  $M$  which properly contains  $H$  and is contained in  $T$ , contrary to the way  $H$  was selected. Thus  $H$  is a maximal related extension of  $M$ . We shall prove that  $H$  is an

injective hull of  $M$ . Our first task is to prove that  $H$  is injective, and, for this, it is sufficient by Theorem 57.3 to prove that  $H$  is a direct summand of  $T$ .

By the maximum principle, we can find a submodule  $R$  of  $T$  such that  $R \cap H = 0$ , and, if  $R'$  is any submodule of  $T$  properly containing  $R$ , then  $R' \cap H \neq 0$ . Then the mapping

$$\phi: H \rightarrow T/R$$

given by  $\phi(h) = h + R$ ,  $h \in H$ , is an  $A$ -isomorphism of  $H$  into  $T/R$ , and  $T/R$  is a related extension of  $\phi(H)$ . Since  $T/R$  is a related extension of  $\phi(H)$ , and  $\phi(H)$  is a maximal related extension of  $\phi(M)$ , it follows that  $\phi(H) = T/R$ . Now let  $\nu: T \rightarrow T/R$  be the natural homomorphism. Then  $\pi = \phi^{-1}\nu$  is an  $A$ -homomorphism of  $T$  into  $H$  such that for all  $h \in H$ ,

$$\pi(h) = \phi^{-1}\nu(h) = \phi^{-1}(h + R) = h.$$

Therefore  $\pi$  is a projection of  $T$  upon  $H$ , and  $H$  is a direct summand of  $T$ . By Theorem 57.3,  $H$  is an injective module. Now let  $U$  be an injective module such that  $M \subset U \subset H$ . If  $U \neq H$ , then by (57.9),  $U$  is a direct summand of  $H$ , contrary to the fact that  $H$  is a related extension of  $M$ . This completes the proof that  $H$  is an injective hull of  $M$  and that any maximal related extension of  $M$  is an injective hull of  $M$ .

Now suppose that  $T$  is an injective hull of  $M$ ; we have to prove that  $T$  is a maximal related extension of  $M$ . By the first part of the proof, there exists a maximal related extension  $R^*$  of  $M$  such that  $M \subset R^* \subset T$ . Again by the first part of the proof,  $R^*$  is injective. Hence  $T = R^*$  and  $T$  is a maximal related extension of  $M$ , as we wished to prove.

Finally, let  $\phi: M \cong M'$  be an  $A$ -isomorphism, and let  $H$  and  $H'$  be injective hulls of  $M$  and  $M'$ , respectively. We have to prove that  $\phi$  can be extended to an  $A$ -isomorphism of  $H$  onto  $H'$ . Since  $M \subset H$ , and  $\phi$  is an  $A$ -isomorphism of  $M$  into the injective module  $H'$ ,  $\phi$  can be extended to an  $A$ -homomorphism  $\phi^*$  of  $H$  into  $H'$ . Since  $H$  is a related extension of  $M$ , it follows that  $\phi^*$  is an  $A$ -isomorphism of  $H$  onto an injective module  $\phi^*(H)$  such that  $M' \subset \phi^*(H) \subset H'$ . Because  $H'$  is an injective hull of  $M'$ , we have  $\phi^*(H) = H'$ , and Theorem 57.13 is completely proved.

Because Theorem 57.13 asserts that an injective hull of  $M$  is uniquely determined up to  $A$ -isomorphism, we shall frequently speak

of the injective hull of  $M$  and denote it by  $H(M)$ .

We conclude this section with a useful criterion for modules to be injective.

(57.14) THEOREM. *A necessary and sufficient condition for a left  $A$ -module  $M$  to be injective is that every homomorphism  $\eta$  of a left ideal  $L$  of  $A$  into  $M$  can be extended to an element of  $\text{Hom}_{\mathbf{A}}(\mathbf{A}A, M)$ ; i.e., there exists an element  $z \in M$  such that  $\eta(a) = az$  for all  $a$  in  $L$ .*

PROOF. If  $M$  is injective, a homomorphism  $\eta$  of  $L$  into  $M$  can be extended to a homomorphism  $\eta'$  of  $\mathbf{A}A$  into  $M$ . Let  $z = \eta'(1)$ ; then for all  $a$  in  $L$  we have  $\eta(a) = \eta'(a) = \eta'(a1) = az$  as required. Conversely, let the condition be satisfied, and let  $P \subset R$  be  $A$ -modules, and  $\eta$  an  $A$ -homomorphism of  $P$  into  $M$ . Consider the set of all pairs  $(P', \eta')$  consisting of submodules  $P'$  of  $R$  containing  $P$  and homomorphisms  $\eta'$  of  $P'$  into  $M$ , partially ordered by the relation  $(P', \eta') \geq (P, \eta'')$  if  $P' \supset P''$  and if  $\eta'$  extends  $\eta''$ . By the maximum principle, there is a maximal pair  $(P_0, \eta_0)$ . We prove that  $P_0 = R$ . Suppose  $P_0 \neq R$ , and let  $r$  be an element of  $R$  which does not belong to  $P_0$ . The set of all  $a$  in  $A$  such that  $ar \in P_0$  is a left ideal  $L$  in  $A$ , and the mapping  $\phi: a \rightarrow \eta_0(ar)$  is a homomorphism of  $L$  into  $M$ . By the hypothesis of the theorem, there exists an element  $z$  in  $M$  such that  $\eta_0(ar) = az$  for all  $a$  in  $L$ . Then the mapping  $\zeta: ar + P_0 \rightarrow az + \eta_0(P_0)$  is an  $A$ -homomorphism of  $Ar + P_0$  into  $M$  which extends  $\eta_0$ , and we contradict the maximality of  $(P_0, \eta_0)$ . Therefore  $P_0 = R$ , and Theorem 57.14 is proved. (Cf. the proof of (57.5))

*Remark.* According to Definition 57.2,  $M$  is injective if every diagram

$$\begin{array}{ccc} 0 & \rightarrow & H \rightarrow K \\ & & \downarrow \\ & & M \end{array}$$

where the row is exact can be imbedded in a commutative diagram

$$\begin{array}{ccc} 0 & \rightarrow & H \rightarrow K \\ & & \downarrow \swarrow \\ & & M \end{array}$$

The essence of Theorem 57.14 is that  $M$  is injective if for each left ideal  $L$  of  $A$ , the diagram

$$\begin{array}{ccc} 0 & \rightarrow & L \rightarrow {}_A A \\ & & \downarrow \\ & & M \end{array}$$

can be completed in the required way.

### *Exercises*

1. Show that if  $A$  is the algebra of all matrices

$$\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}$$

where  $a, b, c$ , are taken arbitrarily from a field  $K$ , then  ${}_A A$  is a projective but not injective left  $A$ -module.

2. Let  $A = Z/[p^k]$ , where  $p$  is a prime number,  $Z$  is the ring of rational integers, and  $k$  is a positive integer. Prove that  ${}_A A$  is the injective hull of the irreducible  $A$ -module  $[p^{k-1}]/[p^k]$ .

3. Let  $A$  be an integral domain with 1. A left  $A$ -module  $M$  is *divisible* if for each  $a \in A, a \neq 0$ , we have  $aM = M$ . Prove that any injective module is divisible. If in particular  $A$  is a principal ideal domain ring, show conversely that every divisible module is injective.

## § 58. Quasi-Frobenius Rings

Some explanation is required before plunging into what may seem to be a very special subject. Let  $A$  be a ring with minimum condition. In § 56, we saw that the left regular module  ${}_A A$  is always projective. The quasi-Frobenius rings are those rings with minimum condition for which the left regular module is injective. The class of quasi-Frobenius rings includes all semi-simple rings with minimum condition, as well as all group algebras of finite groups, semi-simple or not. They receive their name because of a representation-theoretic characterization of quasi-Frobenius algebras to be studied in the next chapter. We shall confine ourselves in this chapter to results that can be proved in the general context of rings with minimum condition. Our definition of quasi-Frobenius rings is an intrinsic one in terms of annihilators of one-sided ideals. This idea was first discovered by M. Hall [1] for semi-simple algebras, and was made the keystone of Nakayama's far-reaching theory of Frobenius and quasi-Frobenius rings and algebras (Nakayama [2, I], [2, II]). Our study of quasi-Frobenius rings is motivated partly by our interest in group algebras, and partly by the fact that many results which can be proved rather easily for semi-simple rings can

still be proved in a suitably generalized form for quasi-Frobenius rings, but are false for general rings with minimum condition.

Before we give the definition of quasi-Frobenius rings, we derive a few preliminary results. We shall assume throughout the rest of the chapter that  $A$  is a ring with 1 which satisfies the left minimum condition. Sometimes we shall consider rings that satisfy also the right minimum condition, and under these circumstances we may apply the results of Chapter IV and in the first part of this chapter to right  $A$ -modules as well as to left  $A$ -modules.

We shall use repeatedly the facts established in Chapter II that the following statements concerning a left  $A$ -module  $M$  are equivalent: (a)  $M$  is finitely generated; (b)  $M$  satisfies the A.C.C. and the D.C.C. for submodules; and (c)  $M$  has a composition series. In case  $A$  also satisfies the right minimum condition, analogous statements can be made concerning right modules.

Let  $M$  be a left  $A$ -module, and let

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

be the additive group whose elements are the  $A$ -homomorphisms of  $M$  into  ${}_A A$ . The abelian group  $M'$  becomes a right  $A$ -module if we define

$$(\phi a)(x) = \phi(x)a, \quad x \in M, \phi \in M', a \in A,$$

and is the precise generalization to modules of the concept of dual vector space (see the exercises following §56). We shall call  $M'$  the *dual* of  $M$ . Similarly we can associate with every right  $A$ -module  $R$  its dual,

$$R' = \text{Hom}_A(R, A_A),$$

which becomes a left  $A$ -module if we define

$$(a\phi)(r) = a\phi(r), \quad a \in A, \phi \in R', r \in R.$$

Next we come to a concept whose importance in the theory of rings with minimum condition was recognized by Nakayama and Dieudonné.

(58.1) DEFINITION. Let  $M$  be a left  $A$ -module. The *socle* of  $M$  is the sum of all the irreducible submodules of  $M$ . Similarly we may define the socle of a right  $A$ -module. In particular, the *left socle* of the ring  $A$  is the socle of the left regular module  ${}_A A$ ; the *right socle* of  $A$  is the socle of the right regular module  $A_A$ .

In case  $M$  is a finitely generated left  $A$ -module, Theorem 15.3 implies that the socle of  $M$  is the unique maximal completely reducible submodule of  $M$ .

(58.2) DEFINITION. Let  $S$  be a subset of  $A$ . The *left annihilator*  $l(S)$  of  $S$  is defined as

$$l(S) = \{a \in A : aS = 0\},$$

whereas the *right annihilator*  $r(S)$  is given by

$$r(S) = \{a \in A : Sa = 0\}.$$

We proceed to derive some simple consequences of the definitions.

(58.3) LEMMA. *Let  $A$  be a ring which satisfies both the left and right minimum conditions, and let  $N = \text{rad } A$ . The left socle of  $A$  is the two-sided ideal  $r(N)$ , whereas the right socle is the two-sided ideal  $l(N)$ .*

The proof is immediate by Exercise 25.4.

(58.4) LEMMA. *Let  $e$  be an idempotent in a ring  $A$ , and let  $N$  be a two-sided ideal in  $A$ . Then the dual of the left  $A$ -module  $Ae/Ne$  is isomorphic to the right  $A$ -module  $er(N)$ .*

PROOF. Let  $V = Ae/Ne$ , and for each  $b \in er(N)$ , define a mapping  $\phi_b: V \rightarrow A$  by setting

$$\phi_b(x + Ne) = xb.$$

It is immediate that  $\phi_b$  is well defined and belongs to the dual  $V'$  of  $V$ . The mapping  $b \rightarrow \phi_b$  is an  $A$ -homomorphism of  $er(N)$  into  $V'$ . If  $\phi_b = \phi_{b'}$  for  $b, b' \in er(N)$ , then  $\phi_b(e + Ne) = \phi_{b'}(e + Ne)$ , and we have  $eb = eb'$ ; consequently  $b = b'$  because  $b$  and  $b'$  both belong to  $eA$ . This shows that  $b \rightarrow \phi_b$  is an  $A$ -isomorphism of  $er(N)$  into  $V'$ . For any  $\phi \in V'$ , let  $b = \phi(e + Ne)$ . Then  $eb = b$ , and, for all  $a \in Ae$ ,

$$\phi(a + Ne) = \phi(ae + Ne) = a\phi(e + Ne) = ab.$$

Moreover, for all  $n \in N$ ,  $nb = \phi(n(e + Ne)) = 0$ , so that  $b \in r(N) \cap eA = er(N)$  and  $\phi = \phi_b$ . Therefore  $b \rightarrow \phi_b$  is onto, and we have proved Lemma 58.4.

(58.5) DEFINITION. A ring  $A$  satisfying the left minimum condition is called a *quasi-Frobenius ring* if

$$l(r(L)) = L$$

and

$$r(l(J)) = J$$

for every left ideal  $L$  and right ideal  $J$  in  $A$ .

If  $A$  is quasi-Frobenius, the mapping  $L \rightarrow r(L)$  sets up a one-to-one inclusion reversing correspondence between the sets of left ideals and right ideals in  $A$ . Because  $A$  satisfies the maximum condition for left ideals by Theorem 54.1, it follows that  $A$  satisfies the right minimum condition as well as the left minimum condition.

Our main objective in this section is to prove the following theorem:

(58.6) THEOREM. *Let  $A$  be a ring with identity which satisfies both the left and right minimum conditions. Then the following statements concerning  $A$  are equivalent to one another:*

(i)  *$A$  is a quasi-Frobenius ring.*

(ii) *If  $P$  is an irreducible left  $A$ -module, the dual module  $P'$  is an irreducible right  $A$ -module, and if  $R$  is an irreducible right  $A$ -module, its dual  $R'$  is an irreducible left  $A$ -module.*

(iii)  *$A$  is an injective left  $A$ -module.*

PROOF. First we show that (i) implies (ii). By Corollary 54.13, any irreducible left  $A$ -module  $P$  is isomorphic to  $Ae/Ne$  for some primitive idempotent  $e$ , where  $N = \text{rad } A$ . By Lemma 58.4,  $P' \cong er(N)$ . Moreover,

$$er(N) = eA \cap r(Ne) = r(A(1 - e) + Ne),$$

and  $A(1 - e) + Ne$  is a maximal left ideal in  $A$  since

$$\frac{A}{A(1 - e) + Ne} = \frac{A(1 - e) \oplus Ae}{A(1 - e) + Ne} \cong Ae/Ne.$$

Because  $A$  is quasi-Frobenius, the right annihilator of a maximal left ideal is a minimal right ideal. Therefore  $er(N)$  is an irreducible right  $A$ -module. The same argument applies to irreducible right  $A$ -modules and their duals. This proves the implication (i)  $\rightarrow$  (ii).

Before proceeding with the proof of the theorem, it is necessary to establish a theorem about modules over rings which satisfy condition (ii) of Theorem 58.6.

(58.7) DEFINITION. A left  $A$ -module  $P$  and a right  $A$ -module  $R$  are said to be *paired to  $A$*  if there exists a function  $f: P \times R \rightarrow A$  such that

$$f(ax_1 + bx_2, y) = af(x_1, y) + bf(x_2, y)$$

$$f(x, y_1a + y_2b) = f(x, y_1)a + f(x, y_2)b$$

for all  $a, b \in A$ ,  $x$ 's in  $P$ , and  $y$ 's in  $R$ . The pairing  $(P, R, f)$  is said to be *non-degenerate* if  $f(x, R) = 0$  implies  $x = 0$  and  $f(P, y) = 0$  implies  $y = 0$ . For any subset  $U$  of  $P$ , let

$$(0: U) = \{y \in R: f(U, y) = 0\}$$

and for  $V \subset R$ , let

$$(0: V) = \{x \in P: f(x, V) = 0\}.$$

If  $(P, R, f)$  is a non-degenerate pairing, then for each  $y \in R$ , the mapping  $\lambda_y: P \rightarrow A$  defined by

$$\lambda_y(x) = f(x, y), \quad x \in P,$$

is an element of  $P'$ , and the mapping  $y \rightarrow \lambda_y$  is an isomorphism of  $R$  into  $P'$ . The next theorem gives among other things a sufficient condition for this mapping to carry  $R$  onto  $P'$ .

(58.8) THEOREM (Morita and Tachikawa [1]). *Let  $A$  satisfy both the left and right minimum conditions, and let  $(P, R, f)$  be a non-degenerate pairing of finitely generated modules  $P$  and  $R$ . Suppose condition (ii) of Theorem 58.6 is satisfied. Then the mapping  $y \rightarrow \lambda_y$  is an  $A$ -isomorphism of  $R$  onto  $P'$ . For all submodules  $U$  of  $P$  and  $V$  of  $R$ , we have*

$$(0: (0: U)) = U, \quad (0: (0: V)) = V.$$

PROOF. As we remarked at the beginning of this section, the fact that  $P$  is finitely generated implies that  $P$  has a composition series

$$(58.9) \quad P = P_0 \supset P_1 \supset P_2 \supset \cdots \supset P_{t-1} \supset P_t = 0.$$

Corresponding to the composition series (58.9) we have a normal series

$$(58.10) \quad R = (0: P_t) \supset (0: P_{t-1}) \supset \cdots \supset (0: P_0) = 0$$

of submodules of  $R$ . Let  $V_i = P_{i-1}/P_i$  be one of the composition factors of  $P$ , and for each coset  $\bar{y} = y + (0: P_{i-1})$  belonging to  $(0: P_i)/(0: P_{i-1})$ , define a mapping  $\mu_{\bar{y}}$  of  $V_i \rightarrow A$  by

$$\mu_{\bar{y}}(\bar{x}) = f(x, y)$$

for  $\bar{x} = x + P_i \in V_i$ . The mapping  $\mu_{\bar{y}}$  is well defined and belongs to  $V_i'$ . Moreover, if for some  $\bar{y}$ , we have  $\mu_{\bar{y}} = 0$ , then  $f(x, y) = 0$  for all  $x \in P_{i-1}$ ; consequently  $y \in (0: P_{i-1})$  and  $\bar{y} = 0$ . Therefore  $\bar{y} \rightarrow \mu_{\bar{y}}$  is an  $A$ -isomorphism of  $(0: P_i)/(0: P_{i-1})$  into  $V_i'$ . Because of hypothesis (ii) of Theorem 58.6,  $V_i'$  is irreducible, and we conclude that

$(0: P_i)/(0: P_{i-1})$  is either zero or irreducible. Therefore the normal series (58.10) for  $R$  is actually a composition series when repeated terms are deleted.

Let us denote the length of a composition series for a left  $A$ -module  $P$  by  $[P]_l$  and the composition series length of a right module  $R$  by  $[R]_r$ . Then we have proved that  $[P]_l \geq [R]_r$ . By the symmetry of  $P$  and  $R$ , we obtain  $[P]_l \leq [R]_r$ , and therefore,

$$[P]_l = [R]_r.$$

On the other hand, we have a natural pairing of  $P \times P' \rightarrow A$  given by

$$(x, \phi) = \phi(x), \quad \phi \in P', x \in P.$$

Although we cannot conclude that this is a non-degenerate pairing, we do know that  $\phi(P) = 0$  implies  $\phi = 0$ , and the argument given in the first part of the proof can be repeated to show that

$$[P']_r \leq [P]_l.$$

Finally, since  $R$  is isomorphic to a submodule of  $P'$ , we have

$$[R]_r \leq [P']_r.$$

Combining these inequalities, we have

$$[P]_l \leq [R]_r \leq [P']_r \leq [P]_l.$$

Therefore all the inequalities are in fact equalities, and in particular  $[R]_r = [P']_r$ . This implies that the mapping  $y \rightarrow \lambda_y$  is onto, and the first assertion of Theorem 58.8 is proved.

For the second assertion, we begin with the fact that (58.10) is a composition series of  $R$ . By the argument in the first part of the proof,

$$P = (0: (0: P_0)) \supset (0: (0: P_1)) \supset \cdots \supset (0: (0: P_{t-1})) \supset 0$$

is a composition series for  $P$ . Because  $(0: (0: P_i)) \supset P_i$  for each  $i$ , it follows that  $(0: (0: P_i)) = P_i$  for each  $i$ . Because any submodule  $U$  of  $P$  is a term in some composition series of  $P$ , we have

$$(0: (0: U)) = U$$

for all  $U \subset P$ . Similarly  $(0: (0: V)) = V$  for all  $V \subset R$ , and Theorem 58.8 is proved.

Now we are ready to return to the proof of Theorem 58.6.

We shall prove that (ii) implies (iii). By Theorem 57.14, it is sufficient to prove that if  $L$  is a left ideal in  $A$ , then any homomorphism  $\eta$  of  $L$  into  ${}_A A$  can be extended to an endomorphism of  ${}_A A$  and is therefore the restriction to  $L$  of a right multiplication by a fixed element of  $A$ . We introduce first the non-degenerate pairing  $({}_A A, A_A, f)$  where

$$f(x, y) = xy, \quad x, y \in A.$$

It is immediate that  $(L, A_A/(0:L), f_1)$  is also a non-degenerate pairing where  $f_1$  is given by

$$f_1(x, \bar{y}) = f(x, y) = xy$$

for  $x \in L, \bar{y} = y + (0:L), y \in A$ . Our given homomorphism  $\eta$  of  $L$  into  ${}_A A$  is a element of  $L'$ , and, applying Theorem 58.8 to the pairing  $(L, A_A/(0:L), f_1)$ , we see that  $L' \cong A_A/(0:L)$ . Therefore there exists an element  $y \in A$  such that

$$\eta(x) = f_1(x, \bar{y}) = xy$$

for all  $x \in L$ . This completes the proof that  ${}_A A$  is an injective module.

Finally we prove that (iii) implies (i). The argument we present is due to Ikeda and Nakayama [1]. The proof is by repeated application of Theorem 57.14. Because of our assumption (iii), whenever we are given a homomorphism  $\eta$  from a left ideal  $L \subset A$  into  ${}_A A$ , we know that  $\eta$  is the restriction to  $L$  of a right multiplication.

Consider first a principal right ideal  $aA$ , and let  $b \in r(l(aA))$ . Then  $l(a) \subset l(b)$ , and  $xa \rightarrow xb$  is a homomorphism of  $Aa$  onto  $Ab$ . By Theorem 57.14, there exists  $c \in A$  such that  $ac = b$ , and we have  $b \in aA$ . Therefore  $r(l(aA)) = aA$  for any principal right ideal  $aA$  since the inclusion  $aA \subset r(l(aA))$  is obvious. Next we show that for any two left ideals  $L_1$  and  $L_2$ , we have

$$(58.11) \quad r(L_1 \cap L_2) = r(L_1) + r(L_2).$$

The inclusion  $r(L_1) + r(L_2) \subset r(L_1 \cap L_2)$  is obvious, and to prove the reverse inclusion, we shall set up another application of Theorem 57.14. Let  $b \in r(L_1 \cap L_2)$ , and consider the mappings  $\theta_1$  and  $\theta_2$  of  $L_1 \rightarrow L_1$  and  $L_2 \rightarrow L_2(1+b)$ , respectively, defined by

$$\theta_1(x_1) = x_1, \quad x_1 \in L_1$$

and

$$\theta_2(x_2) = x_2(1+b), \quad x_2 \in L_2.$$

These mappings coincide on  $L_1 \cap L_2$  and hence define an  $A$ -homomorphism  $\theta$  of  $L_1 + L_2$  onto  $L_1 + L_2(1+b)$ , namely

$$\theta(x_1 + x_2) = \theta_1(x_1) + \theta_2(x_2), \quad x_i \in L_i, i = 1, 2.$$

Again by Theorem 57.14,  $\theta(x) = xa$  for all  $x \in L_1 + L_2$  and some fixed  $a \in A$ . Then  $1 - a \in r(L_1)$ , and  $1 + b - a \in r(L_2)$ . Therefore

$$b = (1 + b - a) - (1 - a) \in r(L_1) + r(L_2),$$

and we have proved (58.11).

Now let  $R$  be any right ideal in  $A$ . Because  $A$  satisfies the right minimum condition and hence the right maximum condition, there exist elements  $a_1, \dots, a_s \in R$  such that  $R = a_1A + \dots + a_sA$ . We note also the obvious relation

$$l(a_1A + \dots + a_sA) = l(a_1A) \cap \dots \cap l(a_sA).$$

Then, by what has been proved, we have

$$\begin{aligned} r(l(R)) &= r(l(a_1A + \dots + a_sA)) = r(l(a_1A) \cap \dots \cap l(a_sA)) \\ &= r(l(a_1A)) + \dots + r(l(a_sA)) = a_1A + \dots + a_sA = R. \end{aligned}$$

We begin the final step of the proof with the observation that since  ${}_A A$  is injective, Theorem 57.3 implies that any direct summand of  ${}_A A$  is injective. In particular, the left ideal  $Ae$  generated by a primitive idempotent  $e$  is injective. Let  $H$  be an irreducible submodule of  $Ae$ . By Theorem 57.13,  $Ae$  contains an injective hull  $H^*$  of  $H$ . Then, by Theorem 57.9,  $H^*$  is a direct summand of  $Ae$ . Since  $Ae$  is indecomposable, we see that  $Ae$  is the injective hull of any one of its irreducible submodules  $H$ . By Theorem 57.13 again,  $Ae$  is a related extension of  $H$ , and it follows that  $H$  is the unique minimal submodule of  $Ae$ . Now let  $Ae_1$  and  $Ae_2$  be principal indecomposable modules with unique minimal submodules  $H_1$  and  $H_2$ . Because of the uniqueness of the injective hull [Theorem 57.13],  $H_1 \cong H_2$  if and only if  $Ae_1 \cong Ae_2$ . Therefore there are as many non-isomorphic minimal left ideals in  $A$  as there are non-isomorphic principal indecomposable modules, and, by Corollary 54.14, we conclude that every irreducible left  $A$ -module is  $A$ -isomorphic to some minimal left ideal in  $A$ .

Now let  $L$  be an arbitrary left ideal in  $A$ ; then  $L \subset l(r(L))$ , and we have to prove equality. Let us assume tentatively that the inclusion is proper. Then there exists a left ideal  $L_0 \subset l(r(L))$  such that  $L_0/L$  is an irreducible left  $A$ -module. From what has been said, there exists a minimal left ideal  $H$  of  $A$  which is isomorphic to

$L_0/L$ ; consequently there exists an  $A$ -homomorphism  $\zeta \neq 0$  of  $L_0$  into  $A$  such that  $\zeta(L) = 0$ . Then by Theorem 57.14,  $\zeta(x) = xc$ ,  $x \in L_0$ , for a fixed  $c \in A$ , and we have  $Lc = 0$ . Then  $c \in r(L)$  and  $L_0 \subset l(r(L)) \subset l(c)$ . Therefore  $\zeta(L_0) = L_0c = 0$  contrary to assumption. We conclude that  $L = l(r(L))$ , and Theorem 58.6 is completely proved.

The next theorem states explicitly and somewhat more fully some properties of quasi-Frobenius rings which have already made an appearance in the proof of Theorem 58.6.

(58.12) THEOREM. *Let  $A$  be a quasi-Frobenius ring; let  $N = \text{rad } A$ . Then  $l(N) = r(N)$ , and consequently the left and right socles of  $A$  are identical. Every principal indecomposable module  $Ae$  has a unique minimal submodule  $l(N)e$ . If  $e$  and  $f$  are primitive idempotents, then  $l(N)e \cong l(N)f$  if and only if  $Ae \cong Af$ .*

PROOF. By Lemma 58.4 and (ii) of Theorem 58.6, we know that  $er(N)$  is an irreducible right  $A$ -module for every primitive idempotent  $e$ . Then  $er(N)N = 0$  by Exercise 25.4, and, because the identity element 1 is a sum of primitive idempotents, we have  $r(N)N = 0$ . Therefore  $r(N) \subset l(N)$ . The same argument with right and left modules interchanged shows that  $l(N) \subset r(N)$ , and we conclude that  $l(N) = r(N)$ . By Lemma 58.3, this implies that the left and right socles of  $A$  are equal.

Now let  $Ae$  be a principal indecomposable module. By (ii) of Theorem 58.6 and the counterpart of Lemma 58.4 for right modules,  $l(N)e$  is different from zero and is an irreducible submodule of  $Ae$ . Because  $Ae$  is indecomposable and injective, it follows by the argument on page 400 that  $l(N)e$  is the unique minimal submodule of  $Ae$ , and that  $Ae$  is the injective hull of  $l(N)e$ . The last statement of the theorem is a consequence of the uniqueness of the injective hull.

In the case of a group algebra of a finite group, or more generally, if  $A$  is a symmetric algebra (see §66), it can be proved that  $l(N)e \cong Ae/Ne$  for all primitive idempotents  $e$ . A proof of this fact is outlined in Exercise 83.1.

(58.13) COROLLARY. *Let  $A$  be a quasi-Frobenius ring. Then every irreducible left  $A$ -module is isomorphic to a left ideal in  $A$ .*

This result has already been proved in the derivation of Theorem 58.6 and follows from the last assertion of Theorem 58.12 because the number of distinct irreducible  $A$ -modules is equal to the number of distinct principal indecomposable modules.

(58.14) THEOREM. *Let  $M$  be a finitely generated module over a quasi-Frobenius ring  $A$ . Then  $M$  is projective if and only if  $M$  is injective.*

PROOF. By Theorem 58.6,  $\mathcal{A}A$  is an injective module, hence any finitely generated free left  $A$ -module is injective. If  $M$  is projective, then  $M$  is a direct summand of a free module and is injective by Theorem 57.3. Conversely, suppose  $M$  is an injective left  $A$ -module. Since  $M$  is a direct sum of a finite number of indecomposable modules, it is sufficient to prove that an injective indecomposable module  $M$  is projective. Let  $M_1$  be an irreducible submodule of  $M$ . Then  $M$  is the injective hull of  $M_1$ , whereas by Theorem 58.12 and its corollary,  $M_1$  is isomorphic to the unique minimal subideal of some principal indecomposable module  $Ae$ . Since  $Ae$  is the injective hull of its unique minimal subideal, the uniqueness of the injective hull implies that  $Ae \cong M$ , proving that  $M$  is projective. This completes the proof of Theorem 58.14.

### Exercises

1. In connection with Theorem 58.6, prove the implication  $(ii) \rightarrow (i)$  as a direct application of Theorem 58.8 using the pairing  $(\mathcal{A}A, \mathcal{A}A, f)$  where  $f(a, b) = ab, a, b \in A$ .
2. Prove that the following rings are quasi-Frobenius:
  - (a) A semi-simple ring with minimum condition.
  - (b) The ring  $A_n$  of all  $n \times n$  matrices with coefficients in a quasi-Frobenius ring  $A$ .
  - (c) A proper homomorphic image of a commutative principal ideal domain  $D$ . In particular, if  $M$  is a finite-dimensional vector space over a field  $K$ , and if  $T$  is a linear transformation on  $M$ , the algebra  $K[T]$  of all polynomials in  $T$  is a quasi-Frobenius ring.
  - (d) The group ring  $AG$  of a finite group  $G$  with coefficients in a quasi-Frobenius ring  $A$ . In particular, the group algebra  $KG$  of a finite group  $G$  over a field  $K$  is quasi-Frobenius. [Hint:  $AG$  consists of all formal linear combinations  $\sum a_{gg}g, a_g \in A, g \in G$ . Define a pairing  $f$  of  $AG \times AG \rightarrow A$  by setting  $f(\sum a_{gg}g, \sum b_{gg}g) = c$  where  $c$  is the coefficient of 1 in the product  $(\sum a_{gg}g)(\sum b_{gg}g)$ . Prove that  $f$  is a non-degenerate pairing of  $AG \times AG$  to  $A$  where  $AG$  is viewed as a left or right  $A$ -module. Apply the Morita-Tachikawa theorem 58.8 to conclude that, for any left ideal  $L$  or right ideal  $R$  in  $AG$ , we have  $(0: (0: L)) = L$  and  $(0: (0: R)) = R$ . Finally show that these relations imply that  $l(r(L)) = L$  and  $r(l(R)) = R$ .]
  3. Let  $T$  be a linear transformation of a vector space  $V$  over a field  $K$ , and let  $K[T]$  be the subalgebra of  $\text{Hom}_K(V, V)$  generated by 1 and  $T$ . Then  $K[T] \cong K[X]/(m(X))$  where  $m(X)$  is a non-zero polynomial of least degree such that  $m(T) = 0$ . It is an elementary result that there exists a vector  $v \in V$

whose order ideal is  $(m(X))$ , and therefore  $K[T]v \cong K[T]$  as left  $K[T]$ -modules. By the result of Exercise 58.2 (c) and Theorem 58.6,  $K[T]$  is an injective  $K[T]$ -module; hence  $K[T]v$  is a  $K[T]$ -direct summand of  $V$ . Apply this result to prove that the following statements are equivalent: (a)  $V$  is an indecomposable  $K[T]$ -module; (b)  $V$  is a cyclic  $K[T]$ -module; and the minimal polynomial  $m(X)$  of  $T$  is a prime power. From this result and the Krull-Schmidt theorem follows the elementary divisor theorem, namely, that  $V$  is a direct sum of cyclic indecomposable  $K[T]$ -submodules  $V_1, \dots, V_r$ , such that the minimal polynomials of the restrictions of  $T$  to the submodules  $V_1, \dots, V_r$  are uniquely determined prime powers, called the elementary divisors of  $T$ . Then, as for finite abelian groups (§ 4), it is easy to prove the invariant factor theorem, namely that  $V$  is a direct sum of cyclic  $K[T]$ -submodules  $W_1, \dots, W_s$ , such that the minimal polynomials  $d_i(X)$  of  $T$  restricted to the spaces  $W_i$  have the property that  $d_i(X) \mid d_{i+1}(X)$ ,  $i = 1, 2, \dots$ . (Curtis has given this approach to the elementary divisor theory of a single linear transformation in lectures at the University of Wisconsin; this idea has also been sketched by Brauer [21].)

4. Is every homomorphic image of a quasi-Frobenius ring quasi-Frobenius? (see Nakayama [2, I].)

5. Prove that, if  $A$  is a ring with 1, satisfying the left and right minimum conditions, then  $\mathbf{A}A$  is an injective left  $A$ -module if and only if  $A\mathbf{A}$  is an injective right  $A$ -module.

## § 59. Modules over Quasi-Frobenius Rings

This section contains two results on modules over quasi-Frobenius rings which generalize familiar theorems for semi-simple rings. The first is the result that any faithful module over a quasi-Frobenius ring has the double centralizer property. The argument we give is due to Nesbitt and Thrall [1], and has already been used in our proof of Wedderburn's theorem 26.4. This theorem has two noteworthy special cases. First, it implies that any module over a semi-simple ring has the double centralizer property (see Exercise 26.1). On the other hand, let  $V$  be a vector space over a field  $K$ , and  $T$  a linear transformation of  $V$ . By Exercise 58.2 (c), the ring  $K[T]$  of polynomials in  $T$  is a quasi-Frobenius ring, and the double centralizer theorem for the pair  $(V, K[T])$  states that the only linear transformations of  $V$  which commute with every linear transformation which commutes with  $T$  are polynomials in  $T$ . This result is a well-known theorem of Wedderburn ([1], p. 106). However, not every algebra of linear transformations  $A$  on a vector space  $V$  has the double centralizer property (see Exercise 59.1), and no characterization of algebras with this property is known at present (see Thrall

[2] and Morita [2]).

The second result has as its starting point the fact that if  $M$  is any finitely generated left module over a semi-simple ring  $A$ , then  $\text{Hom}_A(M, M)$  is a semi-simple ring (this result follows easily from Exercise 15.4 and the material in Chapter IV). We give in this section a sufficient condition for  $\text{Hom}_A(M, M)$  to be quasi-Frobenius when  $A$  is a quasi-Frobenius ring.

We begin the section with an important lemma.

(59.1) LEMMA. *Let  $e$  be a primitive idempotent in a quasi-Frobenius ring  $A$ , and let  $I$  be the unique minimal subideal of  $Ae$ . Let  $V$  be a left  $A$ -module such that  $IV \neq 0$ . Then  $V$  contains a direct summand isomorphic to  $Ae$ .*

PROOF. By Theorem 58.12,  $Ae$  does have a unique minimal submodule  $I = l(N)e$ . The hypothesis of the lemma implies that there exists an element  $v \in V$  such that  $Iv \neq 0$ , and we may assume  $v = ev$ . Then

$$\theta: ae \rightarrow aev = av$$

is an  $A$ -homomorphism of  $Ae$  onto  $Av$ . The kernel of  $\theta$  is either zero or contains  $I$ . Since  $Iv \neq 0$ , the kernel is zero, and  $Av \cong Ae$ . By Theorem 58.12,  $Ae$  is an injective module; hence  $Av$  is a direct summand of  $V$ , and the lemma is proved.

(59.2) DEFINITION. Let  $A$  be a ring with minimum condition, and let  $A_0$  be the direct sum of a full set of non-isomorphic left principal indecomposable modules of  $A$ . Then  $A_0$  is called the *reduced regular module* of  $A$ .

(59.3) THEOREM. *Let  $M$  be a faithful, finitely generated left module over a quasi-Frobenius ring  $A$ . Then  $M$  has a direct summand  $M_i$  which is isomorphic to the reduced regular module  $A_0$  of  $A$ .*

PROOF. Because  $M$  is finitely generated,  $M$  has a composition series so that the Krull-Schmidt theorem applies to direct decompositions of  $M$ . Now let  $Ae_1, \dots, Ae_r$  be a full set of non-isomorphic principal indecomposable modules of  $A$ . Suppose that for some  $i$ ,  $0 \leq i < r$ ,  $M$  contains a direct summand  $M_i$  isomorphic to  $Ae_1 + \dots + Ae_i$ .<sup>\*</sup> We show how to obtain a direct summand isomorphic to  $Ae_1 + \dots + Ae_{i+1}$ . Let  $M = M_i \oplus M'_i$  where  $M_i \cong Ae_1 + \dots + Ae_i$ . Let  $I$  be the

---

\* When  $i = 0$ , it is understood that  $Ae_1 + \dots + Ae_i = 0$ .

unique minimal subideal of  $Ae_{i+1}$ . Because  $M$  is a faithful  $A$ -module, either  $IM_i \neq 0$  or  $IM'_i \neq 0$ . If  $IM_i \neq 0$ , then by Lemma 59.1,  $M_i$  contains a direct summand isomorphic to  $Ae_{i+1}$ , and we contradict the Krull-Schmidt theorem since  $Ae_{i+1}$  is not isomorphic to  $Ae_j$  for  $1 \leq j \leq i$ . Therefore  $IM'_i \neq 0$ , and again by Lemma 59.1,  $M'_i$  contains a direct summand isomorphic to  $Ae_{i+1}$ . This summand together with  $M_i$  form a direct summand of  $M$  isomorphic to  $Ae_1 + \cdots + Ae_{i+1}$ . This completes the proof of the theorem.

(59.4) LEMMA. *Let  $A$  be any ring with unity element,  $N$  any left  $A$ -module, and consider the left  $A$ -module  $M$  given by*

$$(59.5) \quad M = {}_A A + N \quad (\text{external direct sum}).$$

*Then  $(A, M)$  has the double centralizer property.*

PROOF. Let  $D_1 = \text{Hom}_A({}_A A, {}_A A)$ . Each  $\lambda \in D_1$  may be extended to an element  $\lambda' \in D = \text{Hom}_A(M, M)$  by letting  $\lambda'|{}_A A = \lambda$ ,  $\lambda'|N = 0$ . This map  $\lambda \rightarrow \lambda'$  then embeds  $D_1$  in  $D$ ; call  $E$  the image of  $D_1$ . Then surely  $\text{Hom}_D(M, M) \subset \text{Hom}_E(M, M)$ .

Next let  $\pi$  be the projection of  $M$  on  ${}_A A$  defined by (59.5). Then  $\pi \in D$ , so that for  $f \in \text{Hom}_D(M, M)$  we have

$$f(m\pi) = (fm)\pi, \quad m \in M,$$

which shows that  $f({}_A A) \subset A$ . Surely  $f|{}_A A$  commutes with every element of  $D_1$ ; but by (26.5) the pair  $(A, {}_A A)$  has the double centralizer property, and so there exists an element  $a_0 \in A$  such that  $f|{}_A A = (a_0)_L$ .

For each  $n \in N$ , define

$$(a, n')\mu_n = (0, an), \quad (a, n') \in {}_A A + N.$$

We find readily that  $\mu_n \in D$ , and so the above  $f$  satisfies

$$f(m\mu_n) = (fm)\mu_n, \quad m \in M.$$

Choosing  $m = (1, 0) \in M$ , we have  $fm = (a_0, 0)$ , and so  $f(0, n) = (0, a_0n)$ . Therefore  $f$  on  $M$  is precisely  $(a_0)_L$ , which proves that  $\text{Hom}_D(M, M) \subset A_L$ . This proves the result.

Now we come to the double centralizer theorem.

(59.6) THEOREM. *Let  $M$  be a faithful, finitely generated left module over a quasi-Frobenius ring  $A$ . Then  $(A, M)$  has the double centralizer property.*

**PROOF.** By Lemmas (26.5) and (59.4), it is sufficient to prove that the direct sum of  $M$  with itself a certain number of times contains a direct summand isomorphic to  ${}_A A$ , and this is immediate by Theorem 59.3. This completes the proof of Theorem 59.6.

The next theorem was proved independently by Curtis [3] and Morita [1].

(59.7) **THEOREM.** *Let  $M$  be a faithful finitely generated projective left module for a quasi-Frobenius ring  $A$ . Then  $\text{Hom}_A(M, M)$  is quasi-Frobenius, and  $M$  is a projective finitely generated  $\text{Hom}_A(M, M)$ -module.*

**PROOF.** We shall write the elements of  $C = \text{Hom}_A(M, M)$  as right operators, so that we have

$$(ax)c = a(xc)$$

for  $a \in A$ ,  $x \in M$ , and  $c \in C$ . Because  $M$  is finitely generated and projective,  $M$  is a direct summand of a finitely generated free left  $A$ -module  $F$ . Then  $C = \text{Hom}_A(M, M)$  is isomorphic to  $eBe$  where  $B = \text{Hom}_A(F, F)$  and  $e$  is the projection of  $F$  upon  $M$ . Because  $F$  is finitely generated,  $B$  is isomorphic to a full matrix ring over  $A$ , and consequently  $B$  satisfies the minimum condition for left and right ideals. By Theorem 54.6,  $eBe$  and hence  $C$  also satisfy the left and right minimum conditions (see also Exercise 56.3).

The rest of the proof proceeds in two steps. First, we show that  $M$  is a projective right  $C$ -module and then that  ${}_c C$  is an injective left  $C$ -module. Because  $C$  satisfies both the left and right minimum conditions, the fact that  $C$  is quasi-Frobenius will then be a consequence of Theorem 58.6.

Before proceeding with this program, we record a useful identity. Let  $R$  and  $S$  be rings,  $P$  and  $N$  left  $R$ -modules, and let  $P$  be an  $(R, S)$ -bimodule. Then

$$r(xs) = (rx)s$$

for all  $r \in R$ ,  $x \in P$ , and  $s \in S$ . Briefly we may say we have the situation  $({}_R P_S, {}_RN)$ . Then  $\text{Hom}_R(P, N)$  becomes a left  $S$ -module if we define  $(sf)(x) = f(xs)$ ,  $s$  in  $S$ ,  $f \in \text{Hom}_R(P, N)$ ,  $x \in P$ . In particular, if  $P = N$  and  $S$  is the ring  $\text{Hom}_R(P, P)$  the composition we have just defined is identical with left multiplication in the ring  $S$ . Let  $e$  be an idempotent in  $S$ ; then  $Pe$  is an  $R$ -direct summand of  $R$ , and  $\text{Hom}_R(Pe, N)$  may be viewed as a subgroup of  $\text{Hom}_R(P, N)$ . If  $N$  happens to be a right  $T$ -module for a ring  $T$ , then  $\text{Hom}_R(P, N)$  is

a right  $T$ -module, and  $\text{Hom}_R(Pe, N)$  is a  $T$ -submodule of the right  $T$ -module  $\text{Hom}_R(P, N)$ . With either interpretation, as subgroup or submodule, we have

$$(59.8) \quad \text{Hom}_R(Pe, N) = e \text{Hom}_R(P, N).$$

Now we are ready to prove that  $M$  is a projective right  $C$ -module. We begin by expressing the identity element 1 in  $A$  as a sum of primitive idempotents,  $1 = \sum_{i=1}^r e_i$ . We can also express  $M$  as  $\sum_j \oplus M_j$ , where the  $M_j$  are indecomposable  $A$ -direct summands of  $M$ . By Theorem 56.6 and the Krull-Schmidt theorem, each module  $M_j$  is isomorphic to a principal indecomposable module  $Ae_{i(j)}$ , where  $e_{i(j)}$  is one of the idempotents selected in the expression  $1 = \sum_i e_i$ . Now we apply (59.8) (with  $P = {}_R R_R$ ,  $N = {}_R M_C$ ) and the easily verified facts that  $\text{Hom}_A(\sum_j \oplus M_j, M) \cong \sum_j \oplus \text{Hom}_A(M_j, M)$  and  $\text{Hom}_A(A, M) \cong M$  to obtain

$$\begin{aligned} C &= \text{Hom}_A(M, M) \cong \sum_j \oplus \text{Hom}_A(M_j, M) \\ &\cong \sum_j \oplus \text{Hom}_A(Ae_{i(j)}, M) \\ &= \sum_j \oplus e_{i(j)} \text{Hom}_A(A, M) \cong \sum_j \oplus e_{i(j)} M \end{aligned}$$

as right  $C$ -modules. Since  $C$  is a free right  $C$ -module, Theorem 56.6 implies that the  $C$ -modules  $e_{i(j)}M$  are all projective. Now we use the fact that  $M$  is faithful. By Theorem 59.3, every  $Ae_i$ ,  $1 \leq i \leq r$ , is isomorphic to one of the  $M_j$ . Therefore every idempotent  $e_i$ ,  $1 \leq i \leq r$ , can be taken as an idempotent  $e_{i(j)}$  for which  $Ae_{i(j)} \cong M_j$ . Therefore  $e_i M$  is a projective right  $C$ -module for all  $i$ ,  $1 \leq i \leq r$ , and since  $M = \sum_i \oplus e_i M$ , we conclude by Theorem 56.5 that  $M$  is a projective right  $C$ -module. We have shown also that  $e_i M$  is isomorphic to a right ideal in  $C$  for each  $i$ , and it follows that  $M$  is a finitely generated  $C$ -module.

As we have pointed out, in order to complete the proof of the theorem it is sufficient to prove that whenever we have the situation  $({}_R P_S, {}_R N)$  where  $P$  is a projective right  $S$ -module and  $N$  an injective left  $R$ -module, then  $\text{Hom}_R(P, N)$  is an injective left  $S$ -module. (In our case  $P = M$ ,  $R = A$ ,  $S = C = \text{Hom}_R(M, M)$ ,  $N = M$ .) The required result is Proposition VI. 1.4 in Cartan-Eilenberg [1]. We shall sketch the proof. According to Definition 57.2, we have to prove that if

$$(59.9) \quad 0 \longrightarrow A \xrightarrow{\phi} B$$

is an exact sequence of left  $S$ -modules, then there exists an exact sequence of groups

$$(59.10) \quad \text{Hom}_S(B, \text{Hom}_R(P, N)) \xrightarrow{\Phi} \text{Hom}_S(A, \text{Hom}_R(P, N)) \rightarrow 0$$

such that  $(\Phi f)(\phi a) = f(\phi a)$  for  $a \in A$  and  $f \in \text{Hom}_S(B, \text{Hom}_R(P, N))$ . Starting from (59.9), we verify that, because  $P$  is projective, we have the exact sequence

$$(59.11) \quad 0 \longrightarrow P \otimes_S A \xrightarrow{1 \otimes \phi} P \otimes_S B$$

where  $(1 \otimes \phi)(p \otimes a) = p \otimes \phi(a)$ ,  $p \in P$ ,  $a \in A$ . Since  $N$  is an injective left  $R$ -module, we obtain from (59.11) and Definition 57.2 an exact sequence

$$(59.12) \quad \text{Hom}_R(P \otimes_S B, N) \xrightarrow{\Psi} \text{Hom}_R(P \otimes_S A, N) \longrightarrow 0$$

where for all  $T \in \text{Hom}_R(P \otimes_S B, N)$ ,  $p \in P$ ,  $a \in A$ , we have  $(\Psi T)(p \otimes a) = T(p \otimes \phi a)$ . We observe next that there exists a group isomorphism  $\lambda$  of  $\text{Hom}_R(P \otimes_S A, N)$  onto  $\text{Hom}_S(A, \text{Hom}_R(P, N))$  such that, for all  $T \in \text{Hom}_R(P \otimes_S A, N)$ ,  $a \in A$ ,  $p \in P$ ,  $[(\lambda T)a](p) = T(p \otimes a)$ . Similarly there is an isomorphism  $\mu$  of  $\text{Hom}_R(P \otimes_S B, N)$  onto  $\text{Hom}_S(B, \text{Hom}_R(P, N))$ . Then it is immediate that the mapping  $\Phi = \lambda \Psi \mu^{-1}$  gives rise to an exact sequence 59.10 and has the required extension property. This completes the proof of Theorem 59.7.

### Exercises

1. Show that the algebra  $A$  of matrices

$$\left\{ \begin{pmatrix} a & c \\ 0 & b \end{pmatrix} : a, b, c \in K \right\}$$

considered in Exercise 57.1 does not have the double centralizer property. Show also that  $A$  is not a quasi-Frobenius ring.

2. Let  $T$  be a linear transformation on a finite-dimensional vector space over a field, let  $m(X)$  be the minimal polynomial of  $T$ , and let  $p_1(X)^{e_1}, \dots, p_r(X)^{e_r}$  be the elementary divisors of  $T$ , where the  $p_i(X)$  are irreducible polynomials in  $K[X]$ . Prove that  $V$  is a projective  $K[T]$ -module if and only if for every elementary divisor  $p_i(X)^{e_i}$ , the polynomial

$$\frac{m(X)}{p_i(X)^{e_i}}$$

is not divisible by  $p_i(X)$ .

3. Let  $T$  be a linear transformation with elementary divisors  $X, X^2$  on a three-dimensional vector space  $V$ . Show that  $V$  is not a projective  $K[T]$ -module and that  $\text{Hom}_{K[T]}(V, V)$  is not a quasi-Frobenius ring. [Thus the hypothesis of (59.7) that  $M$  be projective cannot be omitted. The hypothesis that  $M$  be faithful cannot be omitted from (59.7) either, according to an example of Rosenberg and Zelinsky [1].]

## Frobenius Algebras

This chapter begins with the definition and characterization of injective modules for finite-dimensional algebra. Because this discussion is quite elementary, we have made it independent of the material in § 57. Next comes the theory of Frobenius and quasi-Frobenius algebras, which we have arranged in such a way that most of it can be read without a knowledge of § 58. We then prove that group algebras of finite groups over arbitrary fields are Frobenius algebras, and show that general Frobenius algebras have some features, notably an “averaging process,” which makes them seem more closely related to group algebras than the definition would indicate. The next three sections are devoted to D. G. Higman’s theory of relatively projective and injective modules over group algebras, and its application by Higman and Green to the study of indecomposable modules over group algebras. The chapter ends with a generalization to symmetric algebras of Weyl’s theory of the centralizer of a module over the group algebra of a finite group and its application to the construction of the irreducible tensor representations of the full linear group.

### § 60. Injective Modules for a Finite-Dimensional Algebra

Throughout this chapter,  $A$  denotes a finite-dimensional algebra over an arbitrary field  $K$ . All vector spaces are assumed to be finite dimensional. For brevity, we shall call an  $A$ -direct summand of an  $A$ -module  $M$  a *component* of  $M$ . We begin by recalling definitions of projective and injective  $A$ -modules.

(60.1) **DEFINITION.** A left  $A$ -module  $M$  is *projective* if, whenever we have a homomorphism

$$\phi: U \rightarrow M$$

of an  $A$ -module  $U$  onto  $M$ , the kernel of  $\phi$  is a component of  $U$ . In other words,

$$U/V \cong M$$

implies that  $V$  is a component of  $U$ . A left  $A$ -module  $M$  is called *injective\** if, whenever we have an isomorphism

$$\eta: M \rightarrow U$$

of  $M$  into an  $A$ -module  $U$ , the image  $\eta M$  is a component of  $U$ .

We shall assume familiarity with the more elementary parts (§§ 54–56) of Chapter VIII. In particular, we defined the *principal indecomposable modules* of  $A$  to be the indecomposable components of the left regular module  $\mathbf{A}A$ . These all have the form  $Ae$ , where  $e$  is some primitive idempotent in  $A$ . We proved in § 56 that a left  $A$ -module  $M$  is projective if and only if  $M$  is isomorphic to a direct sum of principal indecomposable modules. Although no analogous result is known for injective modules over arbitrary rings with minimum condition, we can give a very simple characterization of injective modules over finite-dimensional algebras.

For a left  $A$ -module  $M$ , the vector space structure of  $M$  permits us to define a dual module  $M^*$  of  $M$  by

$$M^* = \text{Hom}_K(M, K).$$

The properties of  $M^*$  as a vector space over  $K$  are assumed to be familiar to the reader. For  $\phi \in M^*$ ,  $a \in A$ , we define

$$(\phi a)(x) = \phi(ax), \quad x \in M.$$

Then  $\phi a \in M^*$ , and it is easily checked that  $M^*$  is a right  $A$ -module, which we shall call the  *$K$ -dual* of  $M$  (see 43.5). The  $K$ -dual  $R^*$  of a right  $A$ -module  $R$  is defined similarly, and is a left  $A$ -module. Since  $M$  is finite dimensional, we have

$$(M^*: K) = (M: K),$$

and there is a natural isomorphism

$$M \cong M^{**}$$

as  $A$ -modules.

For a subspace  $P$  of  $M$ , we shall define

$$P^\perp = \{\phi \in M^*: \phi(P) = 0\}.$$

---

\* See (57.9)

If  $P$  is an  $A$ -submodule of the left  $A$ -module  $M$ , then  $P^\perp$  is an  $A$ -submodule of  $M^*$ , and we find easily that

$$(60.2) \quad M^*/P^\perp \cong P^*$$

as right  $A$ -modules.

We shall require a few elementary properties of the operation  $P \rightarrow P^\perp$  which we list for reference.

$$(60.3) \quad \begin{cases} P_1 \subset P_2 \text{ implies } P_2^\perp \subset P_1^\perp; \\ P^{\perp\perp} = P; \\ (P_1 + P_2)^\perp = P_1^\perp \cap P_2^\perp; \\ (P_1 \cap P_2)^\perp = P_1^\perp + P_2^\perp, \end{cases}$$

for all subspaces  $P, P_1, P_2$  of  $M$ . Note that the fourth relation follows from the second and third.

(60.4) LEMMA. *Let  $M$  be a left  $A$ -module such that  $M = M_1 \oplus M_2$  where  $M_1, M_2$  are submodules of  $M$ . Then*

$$M^* \cong M_1^* + M_2^*$$

as right  $A$ -modules.

PROOF. From the formulas (60.3) we obtain  $M^* = M_1^\perp \oplus M_2^\perp$ , and each  $M_i^\perp$  is an  $A$ -submodule of  $M^*$ ,  $i = 1, 2$ . By (60.2), we have  $M_1^\perp \cong M_2^*$  and  $M_2^\perp \cong M_1^*$ , and the lemma is proved.

(60.5) LEMMA. *Let  $e$  be an idempotent in the algebra  $A$ . Then the left  $A$ -module  $(eA)^*$  is injective.*

PROOF. Let  $M = (eA)^*$ . By Definition 60.1, we must prove that if  $M$  is a submodule of a left  $A$ -module  $P$ , then  $M$  is a component of  $P$ . By (60.2) we have

$$P^*/M^\perp \cong M^* = (eA)^{**} \cong eA,$$

as right  $A$ -modules. Because  $eA$  is a projective right  $A$ -module,  $M^\perp$  is a component of  $P^*$ , and there exists a submodule  $N \subset P^*$  such that

$$P^* = N \oplus M^\perp.$$

Taking annihilators, we obtain by (60.3)

$$0 = (P^*)^\perp = (N + M^\perp)^\perp = N^\perp \cap M^{\perp\perp} = N^\perp \cap M,$$

and

$$P = 0^\perp = (N \cap M^\perp)^\perp = N^\perp + M^{\perp\perp} = N^\perp + M.$$

Therefore  $P = M \oplus N^\perp$ , and since  $N^\perp$  is an  $A$ -submodule of  $P$ ,  $M$  is a component of  $P$ . This completes the proof.

(60.6) **THEOREM** (*Nagao and Nakayama [1]*). *A left  $A$ -module  $M$  is injective if and only if  $M$  is a direct sum of  $K$ -duals of principal indecomposable right  $A$ -modules.*

**PROOF.** By Lemma 60.5 and Theorem 57.3, the sufficiency of the condition is clear.<sup>†</sup>

Conversely let  $M$  be an injective left  $A$ -module, and let  $H = \text{Hom}_K(A, M)$ . For  $\phi \in H, a, b \in A$ , define

$$(a\phi)(b) = \phi(ba),$$

thereby making  $H$  a left  $A$ -module. For each  $m \in M$ , define  $\phi_m \in H$  by

$$\phi_m(a) = am, \quad a \in A.$$

Then it is immediate that  $m \rightarrow \phi_m$  is an  $A$ -isomorphism of  $M$  into  $H$ . Since  $M$  is injective, Definition 60.1 implies that  $M$  is  $A$ -isomorphic to a component of  $H$ .

Now we look at  $H$  from a different point of view. Let  $\{m_1, \dots, m_n\}$  be a  $K$ -basis for  $M$ , and for  $\phi \in H$ , put

$$(60.7) \quad \phi(a) = \sum_{i=1}^n \tau_i(a)m_i, \quad a \in A,$$

where the  $\{\tau_i(a)\}$  are uniquely determined elements of  $K$ . For each  $i$ ,  $1 \leq i \leq n$ , the mapping

$$\tau_i: a \rightarrow \tau_i(a), \quad a \in A,$$

is an element of  $\text{Hom}_K(A, K)$  and can therefore be identified with an element of  $A_A^*$ . Formula (60.7) therefore defines a  $K$ -isomorphism

$$\phi \rightarrow (\tau_1, \dots, \tau_n)$$

of  $H$  into the direct sum of  $n$  copies of  $A_A^*$ . For any element  $a' \in A$ , we have for all  $\tau \in A_A^*$  and  $a \in A$ ,

$$\tau(aa') = (a'\tau)(a).$$

This remark, together with (60.7), implies that for all  $a, a' \in A$  and  $\phi \in H$  we have

$$(a'\phi)(a) = \phi(aa') = \sum_{i=1}^n \tau_i(aa')m_i = \sum_{i=1}^n (a'\tau_i(a))m_i.$$

---

<sup>†</sup> To avoid using the results of §57, the assertion of (57.3) can easily be proved directly from Definition 60.1.

Therefore the mapping  $\phi \rightarrow (\tau_1, \dots, \tau_n)$  is an  $A$ -isomorphism of  $H$  into  $A_A^* + \cdots + A_A^*$ . Since (60.7) defines an element of  $H$  for any choice of  $\{\tau_i\}$  from  $A_A^*$ , we have

$$H \cong A_A^* + \cdots + A_A^*, \quad n \text{ summands}.$$

By Lemma 60.4,  $A_A^*$  is the direct sum of  $K$ -duals  $(eA)^*$  of principal indecomposable right  $A$ -modules  $eA$ , and the left  $A$ -modules  $(eA)^*$  are indecomposable. Since  $M$  is isomorphic to a component of  $H$ , we can apply the Krull-Schmidt theorem to conclude that  $M$  is isomorphic to a direct sum of  $K$ -duals of principal indecomposable right  $A$ -modules, and the proof of Theorem 60.6 is completed.

A somewhat neater approach to Lemma 60.5 and Theorem 60.6 perhaps is furnished by the observation that an exact sequence  $M \xrightarrow{f} N \xrightarrow{g} P$  gives rise to an exact sequence  $P^* \xrightarrow{g^*} N^* \xrightarrow{f^*} M^*$ , where  $g^*$  and  $f^*$  are transpose mappings of  $f$  and  $g$ . We leave as an exercise the possibility of using this remark to prove (60.5) and (60.6).

### Exercise

- Verify the isomorphism  $M^*/P^\perp \cong P^*$  as stated in formula (60.2).

## § 61. Frobenius and Quasi-Frobenius Algebras

Every finite-dimensional algebra  $A$  has two natural representations. The *first regular representation* of  $A$  is the representation afforded by the left regular module  ${}_A A$ . The *second regular representation* is the representation afforded by the  $K$ -dual  $(A_A)^*$  of the right regular module  $A_A$ . Frobenius was the first to study algebras for which these representations are equivalent.

(61.1) **DEFINITION.** A finite-dimensional algebra  $A$  over  $K$  is called a *Frobenius algebra* if the left  $A$ -modules  ${}_A A$  and  $(A_A)^*$  are isomorphic. An algebra  $A$  is called a *quasi-Frobenius algebra* if the modules  ${}_A A$  and  $(A_A)^*$  have the same distinct indecomposable components, although possibly with different multiplicities.

The reader interested primarily in modular representations of groups will need from this section only the equivalence of statements (i), (ii), and (iii) of Theorem 61.3, and (61.12)–(61.16), which can be read at this point without any preliminary discussion.

Quasi-Frobenius rings have already been defined in Chapter VIII [see Definition 58.5], and our first task is to show that this defini-

tion is consistent with (61.1).

(61.2) THEOREM. *The following statements concerning a finite dimensional algebra  $A$  are equivalent:*

- (i)  $A$  is a quasi-Frobenius algebra in the sense of Definition 61.1.
- (ii) For every left ideal  $L$  and right ideal  $R$  in  $A$ , we have

$$l(r(L)) = L, \quad r(l(R)) = R$$

[that is,  $A$  is quasi-Frobenius in the sense of Definition 58.5].

- (iii)  $\mathcal{A}A$  is injective.

PROOF. The equivalence of (ii) and (iii) has already been proved in Theorem 58.6. We shall prove here only that (i) and (iii) are equivalent.

Assuming (i), it follows that the indecomposable components of  $\mathcal{A}A$  are isomorphic to  $K$ -duals of principal indecomposable right  $A$ -modules. By Lemma 60.5 and Theorem 57.3, we conclude that  $\mathcal{A}A$  is injective.

Conversely, suppose  $\mathcal{A}A$  is injective. By the Krull-Schmidt theorem and Theorem 60.6, it follows that every indecomposable component of  $\mathcal{A}A$  is isomorphic to the  $K$ -dual of a principal indecomposable right  $A$  module. It remains to prove that for every principal indecomposable right  $A$ -module  $V$ , its  $K$ -dual  $V^*$  is isomorphic to a component of  $\mathcal{A}A$ . This will follow if we can prove that the number of non-isomorphic indecomposable components of  $\mathcal{A}A$  and  $(A_A)^*$  are the same, and for this it is sufficient to prove that  $\mathcal{A}A$  and  $A_A$  have the same number of non-isomorphic indecomposable components. The number of non-isomorphic indecomposable components of  $\mathcal{A}A$  is, by Corollary 54.14 and Theorem 25.24, equal to the number of irreducible left modules of the semi-simple algebra  $A/N$ , where  $N = \text{rad } A$ . Similarly, the number of non-isomorphic indecomposable components of  $A_A$  is equal to the number of irreducible right modules of  $A/N$ . From Theorem 25.15, the number of irreducible left modules of  $A/N$  is equal to the number of simple components of  $A/N$ ; and this, in turn, is equal to the number of irreducible right modules. This completes the proof of the theorem.

The next theorem establishes the equivalence of several important and useful characterizations of Frobenius algebras.

(61.3) THEOREM. *The following statements about a finite-dimensional algebra  $A$  are equivalent:*

- (i)  $A$  is a Frobenius algebra.

(ii) There exists a non-degenerate bilinear form  $f: A \times A \rightarrow K$  which is associative in the sense that

$$f(ab, c) = f(a, bc), \quad a, b, c \in A.$$

(iii) There exists a linear function  $\lambda \in A^*$  whose kernel  $\lambda^\perp$  contains no left or right ideals different from zero.

(iv) For all left ideals  $L$  and right ideals  $R$  in  $A$  we have

$$l(r(L)) = L, \quad \text{and} \quad (r(L): K) + (L: K) = (A: K);$$

$$r(l(R)) = R, \quad \text{and} \quad (l(R): K) + (R: K) = (A: K).$$

PROOF. Condition (i) implies (ii). We are given  ${}_A A \cong A_A^*$  as left  $A$ -modules. Let  $\theta: {}_A A \rightarrow A_A^*$  be the given  $A$ -isomorphism. Then  $\theta(ab) = a\theta(b)$  for all  $a, b \in A$ . This formula means that for all  $x \in A$ , we have

$$(61.4) \quad \theta(ab)x = (a\theta(b))x = \theta(b)xa,$$

We define a bilinear function  $f: A \times A \rightarrow K$  by setting

$$f(x, y) = \theta(y)x.$$

Then  $f$  is a non-degenerate because  $\theta$  is a  $K$ -isomorphism; in fact,  $f(A, y) = 0$  implies  $\theta(y) = 0$ , hence  $y = 0$ , and it is easily checked that we must also have  $f(x, A) = 0$  implying  $x = 0$  (see Exercise 61.1). The associative property of  $f$ ,

$$f(xy, z) = f(x, yz), \quad x, y, z \in A,$$

is clear from (61.4), and we have proved that (i) implies (ii). Conversely, suppose (ii) holds, and let  $f$  be the given associative non-degenerate bilinear form on  $A$ . Define  $\theta: {}_A A \rightarrow A_A^*$  by setting

$$\theta(y)x = f(x, y), \quad x, y \in A.$$

Then  $\theta$  is a  $K$ -isomorphism because  $f$  is non-degenerate, and is an  $A$ -isomorphism because  $f$  is associative. Thus (i) and (ii) are equivalent.

Now we prove that (ii) implies (iii). Given the bilinear function  $f(x, y)$ , we define a linear function  $\lambda$  by

$$\lambda(x) = f(x, 1), \quad x \in A.$$

Then  $\lambda(xA) = 0$  implies  $f(xA, 1) = f(x, A) = 0$ , and because  $f$  is non-degenerate,  $x = 0$ . Similarly,  $\lambda(Ax) = 0$  implies  $x = 0$ , and it follows that the kernel of  $\lambda$  contains no left or right ideals different from zero.

Conversely, given a linear function  $\lambda$  as in (iii), we define

$$f(x, y) = \lambda(xy)$$

and verify at once that  $f$  satisfies (ii). At this point, we have proved the equivalence of (i), (ii), and (iii).

Next we prove that (ii) implies (iv). Let  $L$  be a left ideal in  $A$ ; we then assert that

$$r(L) = \{x \in A : f(L, x) = 0\}.$$

If  $u \in r(L)$ , then  $f(L, u) = f(Lu, 1) = 0$ , whereas  $f(L, x) = 0$  implies  $f(AL, x) = f(A, Lx) = 0$ , and  $Lx = 0$ . Thus we have shown  $r(L) = L^\perp$ ; similarly we have  $l(R) = R^\perp$ . The assertions made in (ii) are now immediate from the standard properties of annihilators of subspaces in pairs of vector spaces which are dual with respect to a non-degenerate bilinear form. (See for example Jacobson [2].)

Finally we establish the most difficult implication: Condition (iv) implies (i). From the relations  $l(r(L)) = L$  and  $r(l(R)) = R$  for all left ideals  $L$  and right ideals  $R$ , we know that,  $A$  is a quasi-Frobenius algebra. By Theorem 61.2, the distinct indecomposable components of  ${}_A A$  and  ${}_{A^*} A^*$  are the same. Let  $\{Ae_1, \dots, Ae_r\}$  be a full set of non-isomorphic principal indecomposable left modules; by (54.10) and the proof of (61.2),  $\{e_1 A, \dots, e_r A\}$  is a full set of non-isomorphic principal indecomposable right  $A$ -modules. For each  $k$ ,  $1 \leq k \leq r$ ,  $(e_k A)^*$  is isomorphic to exactly one module  $Ae_{\pi(k)}$ ,  $1 \leq \pi(k) \leq r$ . The mapping  $k \rightarrow \pi(k)$  is a permutation of  $\{1, 2, \dots, r\}$ . For each  $k$ ,  $1 \leq k \leq r$ , let  $f(k)$  denote the number of summands isomorphic to  $Ae_k$  in a direct decomposition of  ${}_A A$  into indecomposable submodules. Our objective is to prove that  ${}_A A \cong {}_{A^*} A^*$ , and this will be accomplished if we can prove that

$$(61.5) \quad f(k) = f(\pi(k)), \quad 1 \leq k \leq r.$$

Now let  $N = \text{rad } A$ . By Theorem 58.12,  $l(N) = r(N)$ ; we shall denote the completely reducible left and right  $A$ -module  $l(N) (= r(N))$  by  $S$ . Throughout the proof, we shall set

$$\bar{a} = a + N$$

to denote the image of  $a \in A$  under the natural map of  $A$  onto the semi-simple algebra  $A/N = \bar{A}$ . By Theorem 54.11,  $\bar{A}\bar{e}_i$  is an irreducible  $\bar{A}$ -module, and the multiplicity  $f(k)$  of  $Ae_k$  in  ${}_A A$  is equal

to the multiplicity of  $\bar{A}\bar{e}_k$  in  $\bar{A}\bar{A}$ . By the results of §26, we see therefore that  $f(k)$  is equal to the right dimension of  $\bar{A}\bar{e}_k$  over the division algebra  $\bar{e}_k\bar{A}\bar{e}_k$ . An analogous argument shows that  $f(k)$  is also equal to the left dimension of  $\bar{e}_k\bar{A}$  over  $\bar{e}_k\bar{A}\bar{e}_k$ .

Now we turn to the properties of the permutation  $k \rightarrow \pi(k)$ . We prove first that, for each  $k$ ,  $1 \leq k \leq r$ , we have

$$(61.6) \quad \bar{A}\bar{e}_k \cong Se_{\pi(k)}$$

as left  $A$ -modules. We begin by noting that Theorem 58.12 (applied to right modules) asserts that  $e_kS$  is the unique minimal subideal of  $e_kA$ ; consequently,  $(e_kS)^\perp$  is the unique maximal subideal of  $(e_kA)^* \cong Ae_{\pi(k)}$ . By Theorem 54.12,

$$e_{\pi(k)}(e_kA)^* \subsetneq (e_kS)^\perp.$$

Therefore for some non-zero  $\phi$  in  $(e_kA)^*$ , we have

$$(e_{\pi(k)}\phi)(e_kS) = \phi(e_kSe_{\pi(k)}) \neq 0.$$

It follows that

$$(61.7) \quad e_kSe_{\pi(k)} \neq 0,$$

which implies by Theorem 54.12 that (61.6) is valid. The relation (61.7) also implies that

$$(61.8) \quad \bar{e}_{\pi(k)}\bar{A} \cong e_kS$$

as right  $A$ -modules.

Now let  $D$  be the division algebra  $\bar{e}_k\bar{A}\bar{e}_k$ , and let  $D' = \bar{e}_{\pi(k)}\bar{A}\bar{e}_{\pi(k)}$ . Then (61.6) and (61.8) imply that

$$e_kSe_{\pi(k)} \cong D \quad \text{and} \quad e_kSe_{\pi(k)} \cong D'$$

as  $K$ -spaces. Therefore

$$(61.9) \quad (\bar{e}_k\bar{A}\bar{e}_k: K) = (\bar{e}_{\pi(k)}\bar{A}\bar{e}_{\pi(k)}: K).$$

So far we have not used the information in (iv) concerning the dimensions of the annihilators. From these relations we have (see the first part of the proof of (58.6))

$$\begin{aligned} (61.10) \quad (e_kS: K) &= (A: K) - (l(e_kS): K) \\ &= (A: K) - (Ne_k + A(1 - e_k): K) \\ &= (\bar{A}\bar{e}_k: K). \end{aligned}$$

On the other hand, (61.8) implies

$$(61.11) \quad (e_k S: K) = (\bar{e}_{\pi(k)} \bar{A}: K).$$

From what has been proved, we have

$$(\bar{A} \bar{e}_k: K) = (\bar{A} \bar{e}_k: D)_r(D: K) = f(k)(\bar{e}_k \bar{A} \bar{e}_k: K),$$

whereas

$$(\bar{e}_{\pi(k)} \bar{A}: K) = (\bar{e}_{\pi(k)} \bar{A}: D')_l(D': K) = f(\pi(k))(\bar{e}_{\pi(k)} \bar{A} \bar{e}_{\pi(k)}: K).$$

Using (61.11), (61.10), and (61.9), we obtain

$$f(k) = f(\pi(k)),$$

and Theorem 61.3 is completely proved.

An example of a quasi-Frobenius algebra which is not a Frobenius algebra has been given by Nakayama [2, I].

We proceed now to derive some multiplicity relations for Frobenius algebras. We shall use the results in the last part of §54, and as in §54, we first treat the case in which the base field is a splitting field. We require a preliminary lemma.

(61.12) **LEMMA.** *Let  $\bar{A}$  be a semi-simple algebra over an arbitrary field  $K$ , and let  $\bar{e}$  be a primitive idempotent in  $\bar{A}$ . Then  $(\bar{A} \bar{e}: K) = (\bar{e} \bar{A}: K)$ .*

**PROOF.** Let  $\bar{A} \bar{e}$  belong to a simple component  $\bar{B}$  of  $\bar{A}$ . Then  $\bar{B}$  is a direct sum of certain number  $d$  of copies of  $\bar{A} \bar{e}$ . From the structure of  $\bar{B}$  (see §26), we know that  $\bar{B}$  is also the direct sum of  $d$  copies of  $\bar{e} \bar{A}$ . Therefore  $d(\bar{A} \bar{e}: K) = d(\bar{e} \bar{A}: K)$ , and the lemma is proved.

We shall say that an indecomposable  $A$ -module  $V$  appears  $u$  times as a component of a module  $M$  if in a decomposition of  $M$  as a direct sum of indecomposable modules, exactly  $u$  of the components are isomorphic to  $V$ .

(61.13) **THEOREM.** *Let  $A$  be a Frobenius algebra over a field  $K$ , and suppose  $K$  is a splitting field for  $A$ . Let  $e$  be a primitive idempotent in  $A$ , and  $N = \text{rad } A$ . Then the number of times that  $Ae/Ne$  appears as a composition factor of  ${}_A A$  is exactly  $u = (Ae: K)$ , whereas the number of times  $Ae$  appears as a component of  ${}_A A$  is  $d = (Ae/Ne: K)$ .*

**PROOF.** By Theorem 54.16, the number of composition factors of  ${}_A A$  which are isomorphic to  $Ae/Ne$  is equal to  $(eA: K)$ . Let  $f$  be an associative non-degenerate bilinear form on  $A$ . Suppose  $x \in Ae$  has the property that  $f(x, eA) = 0$ . Then we have  $f(xe, A) = f(x, A) = 0$ ,

and  $x = 0$ . Similarly,  $f(Ae, y) = 0$  implies  $y = 0$  for all  $y \in eA$ . We have proved that  $Ae$  and  $eA$  are dual vector spaces with respect to  $f$ , and it follows that  $(Ae: K) = (eA: K)$ . This completes the proof of the first statement.

For the second statement, let

$$(61.14) \quad A = Ae_1 \oplus \cdots \oplus Ae_n$$

be a decomposition of  $A$  into principal indecomposable modules. Letting  $\bar{x}$  denote the image of  $x \in A$  under the natural mapping of  $A \rightarrow \bar{A} = A/N$ , we have corresponding to (61.14) the decomposition

$$(61.15) \quad \bar{A} = \bar{A}\bar{e}_1 \oplus \cdots \oplus \bar{A}\bar{e}_n$$

where the  $\{\bar{A}\bar{e}_i\}$  are minimal left ideals in  $\bar{A}$ . By Theorem 54.11,  $\bar{A}\bar{e}_i \cong \bar{A}\bar{e}_j$  if and only if  $Ae_i \cong Ae_j$ . Since  $K$  is a splitting field for  $A$ , the number of times  $\bar{A}\bar{e}_i$  appears in  ${}_A\bar{A}$  is  $(\bar{e}_i \bar{A}: K)$ , by (54.16); by Lemma 61.12, we have

$$(\bar{e}_i \bar{A}: K) = (\bar{A}\bar{e}_i: K) = (Ae_i/Ne_i: K).$$

Combining our remarks, we have proved that  $Ae_i$  appears exactly  $(Ae_i/Ne_i: K)$  times as a component of  ${}_AA$ , and the theorem is proved.

Finally, we state the general multiplicity theorem for Frobenius algebras over perfect fields.

(61.16) THEOREM. *Let  $A$  be a Frobenius algebra over a perfect field  $K$ , and let  $e$  be a primitive idempotent in  $A$ . Let*

$$c = (\text{Hom}_A(Ae/Ne, Ae/Ne): K), d = (Ae/Ne: K), \text{ and } u = (Ae: K).$$

*Then  $Ae/Ne$  appears exactly  $u/c$  times as a composition factor of  ${}_AA$ , and  $Ae$  appears  $d/c$  times as a component of  ${}_AA$ .*

The proof is the same as that of Theorem 61.13, except that Theorem 54.19 has to be used in place of Theorem 54.16. The reader may complete the proof of Theorem 61.16 as an exercise.

Further results on Frobenius algebras, including a generalization of the orthogonality relations given in §31, may be found in Nesbitt and Thrall [1], Brauer [14], Osima [2], [4], and Nakayama [2, I].

### Exercises

1. Prove that, if  $f$  is a bilinear form on a vector space  $V$  such that  $f(V, y) = 0$  implies  $y = 0$ , then also  $f(x, V) = 0$  implies  $x = 0$ .
2. Let  $A$  be a finite-dimensional algebra, and let  $a_R: x \rightarrow xa$  denote right multiplication by the element  $a$ . Let  $a_R^*$  be the linear transformation of  $A^*$  given by

$$(a_R^*\phi)(x) = \phi(a_R x), \quad x \in A, \phi \in A^*.$$

Prove that  $a \rightarrow a_R^*$  is the second regular representation of  $A$ .

3. Prove that every semi-simple algebra over a field is a Frobenius algebra.

[Hint: Use (iv) of Theorem 61.3, and Lemma 61.12.]

4. (Jacobson.) Let  $A$  and  $B$  be Frobenius algebras over  $K$ , and let  $\phi$  and  $\psi$  be linear functions on  $A$  and  $B$  whose kernels contain no right or left ideals different from zero. Show that there exists a linear function  $\lambda$  on  $A \otimes_K B$  such that

$$\lambda(a \otimes b) = \phi(a)\psi(b), \quad a \in A, b \in B.$$

Prove that the kernel of  $\lambda$  contains no right or left ideals different from zero, and that  $A \otimes_K B$  is a Frobenius algebra.

## § 62. Projective and Injective Modules for a Frobenius Algebra

Maschke's idea of "averaging" over a finite group, used to prove Theorem 10.8, has supported a tower of successive generalizations in the last ten years. The first was contained in Gaschütz's paper [2], in which the relation between Maschke's idea and the concepts of projective and injective modules was first pointed out for group algebras. Then came Ikeda's work [2] in which the same thing was shown for Frobenius algebras. The connection with relatively projective and injective modules was exploited by Higman [2] and Kasch [1]. Still more general formulations of the idea were given by Higman [4], and finally the theory was absorbed in the relative homological algebra of Hochschild [3] and Higman [6]. Because many of these developments find a place in this chapter, it seems worthwhile to begin at the beginning and present in this section the original results of Gaschütz and Ikeda. These will serve to motivate many of the theorems which appear later in the chapter.

(62.1) THEOREM. *Let  $A = KG$  be the group algebra of a finite group  $G$  over a field  $K$ . Then  $A$  is a Frobenius algebra.*

PROOF. Define a linear function  $\lambda$  on  $A$  by setting

$$(62.2) \quad \lambda\left(\sum_{g \in G} \alpha_g g\right) = \alpha_1,$$

where 1 is the unity element of  $G$ . Now suppose that for some  $a \in A$ ,  $\lambda(Aa) = 0$ . Then in particular,  $\lambda(g^{-1}a) = 0$  for each  $g \in G$ . Since (62.2) implies that  $\lambda(g^{-1}a)$  is the coefficient of  $g$  in  $a$  we conclude that  $a = 0$ . Similarly,  $\lambda(aA) = 0$  implies  $a = 0$ , and by (iii) of Theorem 61.3, it follows that  $A$  is a Frobenius algebra.

(62.3) THEOREM. Let  $A = KG$  be the group algebra of a finite group  $G$  over an arbitrary field  $K$ , and let  $M$  be an arbitrary left  $A$ -module. Then the following statements concerning  $M$  are equivalent:

- (i)  $M$  is projective,
- (ii)  $M$  is injective,
- (iii) There exists a linear transformation  $X \in \text{Hom}_K(M, M)$  such that

$$\sum_{g \in G} g^{-1} X g m = m$$

for all  $m \in M$ , or, more briefly,

$$\sum_{g \in G} g^{-1} X g = 1.$$

PROOF. By Theorem 62.1,  $A$  is a Frobenius algebra, and hence is a quasi-Frobenius ring by (iv) of Theorem 61.3. Therefore (i) and (ii) are equivalent by Theorem 58.14. We shall prove only the equivalence of (ii) and (iii). [It is also easy to give a direct proof, independent of §58, of the equivalence of (i) and (iii).]

First, suppose  $M$  is an injective left  $A$ -module. We form the tensor product space  $A \otimes_K M$ , and observe that this space is a left  $A$ -module in which we have

$$a(b \otimes m) = ab \otimes m, \quad a, b \in A, m \in M.$$

Let  $\theta: M \rightarrow A \otimes_K M$  be the  $K$ -homomorphism defined by

$$\theta(m) = \sum_{g \in G} g^{-1} \otimes gm.$$

Since the elements  $\{g^{-1}: g \in G\}$  are a  $K$ -basis of  $A$ ,  $\theta(m) = 0$  implies  $g^{-1} \otimes gm = 0$  for all  $g$ , and in particular,  $1 \otimes 1m = 0$ . Thus  $\theta(m) = 0$  implies  $m = 0$ , and so  $\theta$  is a  $K$ -isomorphism. For each  $h \in G$  we have

$$\theta(hm) = \sum_{g \in G} g^{-1} \otimes ghm,$$

whereas

$$h\theta(m) = \sum_{g \in G} hg^{-1} \otimes gm.$$

Comparing these expressions, we see that  $\theta$  is a  $KG$ -isomorphism of  $M$  into  $A \otimes_K M$ . Because  $M$  is injective, Definition 60.1 implies that  $\theta(M)$  is a component of  $A \otimes_K M$ , and we have

$$(62.4) \quad A \otimes_K M = \theta(M) \oplus N$$

for some other  $A$ -submodule  $N$  of  $A \otimes_K M$ .

From § 12 we know that every element of  $A \otimes_K M$  can be expressed uniquely in the form  $\sum g \otimes m_g$ ,  $m_g \in M$ . The mapping

$$r: \sum g \otimes m_g \rightarrow 1 \otimes m_1$$

is a  $K$ -endomorphism of  $A \otimes_K M$ , and we now verify that

$$(62.5) \quad \sum_{g \in G} g^{-1} r g u = u$$

for all  $u \in A \otimes_K M$ . In fact, for all  $h \in G$ ,  $m \in M$ ,

$$\left( \sum_{g \in G} g^{-1} r g \right) (h \otimes m) = \sum_{g \in G} g^{-1} r (gh \otimes m) = h \otimes m ,$$

which proves (62.5). Now let  $\epsilon$  be the projection of  $A \otimes_K M$  onto  $\theta(M)$  determined by (62.4), and let  $X_1$  be the  $K$ -endomorphism of  $\theta(M)$  given by  $\epsilon \gamma \epsilon$ . Then from (62.5) we have, for all  $u \in \theta(M)$ ,

$$(62.6) \quad \begin{aligned} \sum_{g \in G} g^{-1} X_1 g u &= \sum_{g \in G} g^{-1} \epsilon \gamma g u \\ &= \epsilon \left( \sum_{g \in G} g^{-1} r g \right) \epsilon u = u , \end{aligned}$$

since  $\epsilon g = g \epsilon$ ,  $g \in G$ , and  $\epsilon u = u$  for all  $u \in \theta(M)$ . Finally, let

$$X = \theta^{-1} X_1 \theta ;$$

then  $X \in \text{Hom}_K(M, M)$ , and from (62.6) we have

$$\sum_{g \in G} g^{-1} X g = 1 .$$

This completes the proof that (ii) implies (iii).

Conversely, let  $X$  be a linear transformation of  $M$  such that (iii) holds. We have to prove that if  $M$  is a submodule of an  $A$ -module  $N$ , then  $M$  is a component of  $N$ . Because  $N$  is a vector space over  $K$ , we have

$$N = M \oplus M'$$

for some  $K$ -subspace  $M'$  of  $N$ . Let  $\pi \in \text{Hom}_K(N, N)$  be the corresponding projection of  $N$  upon  $M$ . Define  $\pi' \in \text{Hom}_K(N, N)$  by the formula

$$\pi' n = \sum_{g \in G} g^{-1} X \pi g n , \quad n \in N .$$

Then for all  $h \in G$ ,  $n \in N$ , we have

$$\pi'hn = \sum g^{-1}X\pi ghn = h\pi'n,$$

and it follows that  $\pi' \in \text{Hom}_A(N, N)$ . For  $m \in M$ , we have  $\pi m = m$ , and hence by (iii),

$$\pi'm = \sum g^{-1}X\pi gm = \sum g^{-1}Xgm = m.$$

For  $n \in N$  we have  $\pi'n \in M$ . Therefore  $\pi'$  is a projection of  $N$  upon  $M$  which belongs to  $\text{Hom}_A(N, N)$ , and we conclude that  $M$  is a component of  $N$ . This completes the proof of the theorem [see the proof of (10.8)].

We point out that Maschke's theorem (10.8) is included as a special case of Gaschütz's theorem.

**COROLLARY (Maschke).** *Let  $M$  be a left  $KG$ -module, where  $G$  is a finite group and  $K$  a field such that  $\text{char } K \nmid [G:1]$ . Then  $M$  is a completely reducible  $KG$ -module.*

**PROOF.** Let  $N$  be a  $KG$ -submodule of  $M$ . We shall prove that  $N$  is a component of  $M$ , and for this it is sufficient to show that  $N$  is an injective  $KG$ -module. Let  $1_N$  be the identity transformation on  $N$ . Since  $[G:1] \neq 0$  in  $K$ , we have

$$\sum_{g \in G} g^{-1}([G:1]^{-1}1_N)g = 1_N.$$

By Theorem 62.3,  $N$  is injective, and the corollary is proved.

We shall now give Ikeda's generalization of the preceding result to Frobenius algebras. Let  $A$  be a Frobenius algebra over  $K$ , and let  $f: A \times A \rightarrow K$  be a non-degenerate associative bilinear form on  $A$  (see (61.3)). For each fixed  $b \in A$ , the mapping  $x \mapsto f(x, b)$ ,  $x \in A$ , is an element  $\phi_b$  of the  $K$ -dual  $A^*$  of  $A$ . Because  $f$  is non-degenerate, the mapping  $b \mapsto \phi_b$  is a  $K$ -isomorphism of  $A$  into  $A^*$ , and, since  $(A:K) = (A^*:K)$  we see that  $b \mapsto \phi_b$  is a  $K$ -isomorphism of  $A$  onto  $A^*$ . Let  $\{a_1, \dots, a_n\}$  be a  $K$ -basis of  $A$ . Because  $A \cong A^*$ , there exist elements  $\{b_1, \dots, b_n\}$  in  $A$  such that

$$(62.7) \quad f(a_i, b_j) = \delta_{ij}, \quad 1 \leq i, j \leq n.$$

A pair of bases  $\{a_i\}$  and  $\{b_i\}$  of  $A$  satisfying (62.7) are called *dual bases* of  $A$  with respect to  $f$ . Note that dual bases of a Frobenius algebra must be named in the correct order, since  $f(a, b) \neq f(b, a)$  in general.

We have already proved [Theorem 61.3] that  $A$  is a Frobenius algebra if and only if  $A$  has a non-degenerate associative bilinear form and that every group algebra  $KG$  is a Frobenius algebra [Theorem 62.1]. Let  $A = KG$ , and let  $\lambda$  be the function on  $A \rightarrow K$  defined by (62.2). Then

$$f(a, b) = \lambda(ab)$$

defines a non-degenerate associative bilinear form on  $A$ . Moreover, if  $\{g_1, \dots, g_n\}$  is the basis of  $KG$  consisting of the elements of  $G$ , then  $\{g_1^{-1}, \dots, g_n^{-1}\}$  is the dual basis to  $\{g_i\}$  with respect to  $f$ . The key to the Gaschütz theorem, in this terminology, is that for any left  $KG$ -module  $M$  and any  $X \in \text{Hom}_K(M, M)$ ,  $\sum_{i=1}^n g_i X g_i^{-1}$  belongs to  $\text{Hom}_{KG}(M, M)$ . The next lemma shows that the same result holds for dual bases of an arbitrary Frobenius algebra.

(62.8) LEMMA. *Let  $A$  be a Frobenius algebra with associative bilinear form  $f$ , and let  $\{a_i\}$  and  $\{b_i\}$  be a pair of dual bases of  $A$  with respect to  $f$ . Let  $M$  be a left  $A$ -module, and let  $X \in \text{Hom}_K(M, M)$ . Then*

$$\sum_{i=1}^n b_i X a_i \in \text{Hom}_A(M, M).$$

PROOF. For each  $a \in A$ , let

$$(62.9) \quad a; a = \sum_{j=1}^n \lambda_{ij}(a) a_j, \quad \lambda_{ij}(a) \in K, 1 \leq i \leq n.$$

We shall prove that

$$(62.10) \quad ab_i = \sum_{j=1}^n b_j \lambda_{ji}(a), \quad 1 \leq i \leq n$$

where, to make the notation clear, we shall write the scalars to the right as well as to the left of the elements of  $A$ . In fact, we can certainly express  $ab_i$  as a linear combination  $\sum b_j \xi_{ji}$  of the basis elements  $b_i$ . Now, using the fact

$$f(a; a, b_j) = f(a_i, ab_j)$$

together with the assumed property

$$f(a_i, b_j) = \delta_{ij},$$

we obtain

$$\lambda_{ij}(a) = \xi_{ij}$$

as required. Letting  $X \in \text{Hom}_K(M, M)$  and using (62.9) and (62.10),

we obtain

$$a \left( \sum_{i=1}^n b_i X a_i \right) = \sum_{i=1}^n \sum_{j=1}^n b_j \lambda_{ji}(a) X a_i , \quad a \in A ,$$

and

$$\left( \sum_{i=1}^n b_i X a_i \right) a = \sum_{i=1}^n \sum_{j=1}^n b_i X \lambda_{ij}(a) a_j , \quad a \in A .$$

Since the two double summations are equal, Lemma 62.8 is proved.

We may now state Ikeda's generalization of Gaschütz's theorem. The proof will be given in outline only; most of the omitted computations are based on the formulas (62.9) and (62.10).

(62.11) THEOREM. *Let  $A$  be a Frobenius algebra over a field  $K$ , and let  $\{a_i\}$  and  $\{b_i\}$  be a pair of dual bases of  $A$ . Then the following statements concerning a left  $A$ -module  $M$  are equivalent:*

- (i)  $M$  is projective,
- (ii)  $M$  is injective,
- (iii) For some  $K$ -linear transformation  $X$  of  $M$ ,

$$(62.12) \quad \sum_{i=1}^n b_i X a_i = 1_M$$

where  $1_M$  denotes the identity transformation on  $M$ .

PROOF. The proof of Theorem 62.3 can be applied almost verbatim. As in Theorem 62.3, it is sufficient to prove, for example, that (ii) and (iii) are equivalent.

Assume (ii), and form the tensor product space  $A \otimes_K M$ , viewed as a left  $A$ -module. Every element of  $A \otimes_K M$  can be expressed uniquely in the form  $\sum b_i \otimes x_i$ ,  $x_i \in M$ . Because of the relations (62.9) and (62.10), it follows that the mapping

$$\eta: m \rightarrow \sum b_i \otimes a_i m , \quad m \in M ,$$

is an  $A$ -isomorphism of  $M$  into  $A \otimes_K M$ . Since  $M$  is injective,  $\eta(M)$  is a component of  $A \otimes_K M$ , and there exists an  $A$ -endomorphism  $\epsilon$  of  $A \otimes_K M$  which projects  $A \otimes_K M$  onto  $\eta(M)$ .

The unity element  $1 \in A$  can be expressed in the form  $1 = \sum \xi_i a_i$ ,  $\xi_i \in K$ . Define a  $K$ -endomorphism  $r$  of  $A \otimes_K M$  by setting

$$r(\sum b_i \otimes m_i) = \sum 1 \otimes \xi_i m_i , \quad m_i \in M .$$

We shall prove that

$$(62.13) \quad \sum b_i r a_i = 1 .$$

For any  $m \in M$  we have by the relations (62.9) and (62.10),

$$\begin{aligned}\sum_i b_i \gamma a_i (b_j \otimes m) &= \sum_i b_i \gamma (\sum_k b_k \lambda_{kj}(a_i) \otimes m) \\ &= \sum_i b_i (\sum_k 1 \otimes \xi_k \lambda_{kj}(a_i) m) \\ &= \sum_i b_i \otimes (\sum_k \xi_k \lambda_{kj}(a_i) m).\end{aligned}$$

Because  $f(a_i, b_j) = \delta_{ij}$ , we have, from (62.9),

$$\lambda_{kj}(a_i) = f(a_k a_i, b_j).$$

Therefore,

$$\begin{aligned}\sum_k \xi_k \lambda_{kj}(a_i) &= \sum_k \xi_k f(a_k a_i, b_j) \\ &= f((\sum_k \xi_k a_k) a_i, b_j) = f(a_i, b_j) = \delta_{ij},\end{aligned}$$

and we have

$$(\sum b_i \gamma a_i)(b_j \otimes m) = b_j \otimes m.$$

This proves the relation (62.13). Then, as in the proof of Gaschütz's theorem,

$$X = \eta^{-1} \varepsilon \gamma \varepsilon \eta$$

is a  $K$ -endomorphism of  $M$  which satisfies (62.12).

Conversely, let  $X \in \text{Hom}_K(M, M)$  satisfy (62.12). Suppose that  $M$  is a submodule of  $N$ , and let  $\pi \in \text{Hom}_K(N, N)$  be a projection of  $N$  upon  $M$ . Define  $\pi' \in \text{Hom}_K(N, N)$  by

$$\pi' = \sum b_i X \pi a_i.$$

By Lemma 62.8,  $\pi' \in \text{Hom}_A(M, M)$ , and it is easily checked that  $\pi'$  projects  $N$  upon  $M$ . It follows that  $M$  is a component of  $N$ , and we have proved that (iii) implies (ii). This completes the proof of the theorem.

### Exercises

1. Give an example of a Frobenius algebra which is not the group algebra of a finite group.
2. Let  $M$  be a projective  $KG$ -module, where  $KG$  is the group algebra of a finite group, and let  $U$  be an arbitrary  $KG$ -module. Prove that  $M \otimes_K U$  is a projective  $KG$ -module. [Here  $g(m \otimes u) = gm \otimes gu$ ,  $m \in M$ ,  $u \in U$ ,  $g \in G$ .]

### § 63. Relative Projective and Injective Modules

In this section we derive a generalization of Gaschütz's theorem

62.3 which characterized projective and injective modules over group algebras. These results will be applied in the next two sections to study indecomposable modules over group algebras.

Throughout this section  $K$  denotes an arbitrary field,  $G$  a finite group, and  $H$  a subgroup of  $G$ .

(63.1) **DEFINITION.** A left  $KG$ -module  $M$  is said to be  $(G, H)$ -projective (or *projective relative to  $H$* ) if every exact sequence of  $KG$ -modules

$$0 \rightarrow R \rightarrow S \rightarrow M \rightarrow 0$$

for which the associated sequence of  $KH$ -modules

$$0 \rightarrow R_H \rightarrow S_H \rightarrow M_H \rightarrow 0$$

splits, is also a split exact sequence of  $KG$ -modules. The  $KG$ -module  $M$  is called  $(G, H)$ -injective if every exact sequence of  $KG$ -modules

$$0 \rightarrow M \rightarrow R \rightarrow S \rightarrow 0,$$

for which

$$0 \rightarrow M_H \rightarrow R_H \rightarrow S_H \rightarrow 0$$

is a split exact sequence of  $KH$ -modules, is also a split exact sequence of  $KG$ -modules.

In less mysterious language, a  $KH$ -module  $M$  is  $(G, H)$ -projective if whenever  $M$  is a homomorphic image of a  $KG$ -module  $S$  such that the kernel of the homomorphism is a  $KH$ -component of  $S_H$ , then the kernel is a  $KG$ -component of  $S$ . Similarly,  $M$  is  $(G, H)$ -injective if whenever  $M$  is a submodule of a  $KG$ -module  $R$  such that  $M_H$  is a  $KH$ -component of  $R_H$ , then  $M$  is a  $KG$ -component of  $R$ .

If  $H = \{1\}$ , the  $(G, H)$ -projective and  $(G, H)$ -injective modules are simply the previously defined projective and injective  $KG$ -modules.

The next two theorems are straightforward generalizations of Gaschütz's theorem, except that some more sophisticated properties of induced modules (§ 12) are required.

(63.2) **THEOREM.** *The following statements concerning a left  $KG$ -modules  $M$  are equivalent:*

- (i)  $M$  is  $(G, H)$ -injective,
- (ii)  $M$  is isomorphic to a  $KG$ -component of  $(M_H)^G = KG \otimes_{K_H} M$ ,
- (iii) For any set of left coset representatives  $\{g_1, \dots, g_s\}$  of  $H$  in  $G$ , there exists an element  $r \in \text{Hom}_{K_H}(M, M)$  such that

$$\sum_{i=1}^s g_i r g_i^{-1} = 1.$$

PROOF. Statement (i) implies (ii). By (12.26), every element of  $(M_H)^G$  can be expressed uniquely in the form

$$(63.3) \quad \sum_{i=1}^s g_i \otimes m_i, \quad m_i \in M,$$

and we may assume that  $g_1 \in H$ . Define a mapping  $\phi: M \rightarrow (M_H)^G$  by

$$\phi(m) = \sum_{i=1}^s g_i \otimes g_i^{-1}m, \quad m \in M.$$

Then  $\phi$  is clearly a  $K$ -homomorphism of  $M$  into  $(M_H)^G$ . If  $\phi(m) = 0$  we have by the uniqueness of the expressions (63.3),

$$g_1 \otimes g_1^{-1}m = g_1 g_1^{-1} \otimes m = 1 \otimes m = 0$$

since  $g_1 \in H$ , and we obtain  $m = 0$ . Finally, we prove that  $\phi$  is a  $KG$ -isomorphism. Let  $g \in G$ ; then for each  $i$ ,  $1 \leq i \leq s$ , there is a unique  $j$ ,  $1 \leq j \leq s$ , such that for some  $h_{ij} \in H$ ,

$$g^{-1}g_i = g_j h_{ij}.$$

Therefore

$$g^{-1}g = h_{ij}^{-1}g_j^{-1},$$

and from these equations it is clear that

$$g^{-1}\phi(gm) = \phi(m), \quad m \in M,$$

which shows that  $\phi$  is a  $KG$ -isomorphism of  $M$  onto a submodule  $\phi(M)$  of  $(M_H)^G$ . The set  $M_1$  of all elements  $\sum g_i \otimes m_i \in (M_H)^G$  such that  $m_1 = 0$  forms a  $KH$ -submodule of  $(M_H)^G$ . Let us show that

$$(63.4) \quad (M_H)^G = \phi(M) \oplus M_1$$

as  $KH$ -modules. We have

$$\sum g_i \otimes m_i = \phi(g_1 m_1) + [(\sum g_i \otimes m_i) - \phi(g_1 m_1)],$$

and

$$\sum g_i \otimes m_i - \phi(g_1 m_1) \in M_1.$$

It is clear that  $\phi(M) \cap M_1 = 0$ . Thus (63.4) holds, and since we have assumed that  $M$  is  $(G, H)$ -injective, (63.4) implies that  $\phi(M)$  is a  $KG$ -component of  $(M_H)^G$ , and we have proved (ii).

Statement (ii) implies (iii). As in the proof of Gaschütz's theorem, we begin with the observation that the mapping

$$r^*: \sum g_i \otimes m_i \rightarrow g_1 \otimes m_1$$

is a  $KH$ -endomorphism of  $(M_H)^G$  such that

$$\sum_{i=1}^s g_i \gamma^* g_i^{-1} = 1.$$

The hypothesis (ii) implies that there is a  $KG$ -endomorphism  $\epsilon$  of  $(M_H)^G$  such that  $\epsilon^2 = \epsilon$  and  $\epsilon[(M_H)^G]$  is  $KG$ -isomorphic to  $M$ . Then  $\epsilon\gamma^*\epsilon$  is a  $KH$ -endomorphism of  $\epsilon[(M_H)^G]$  such that for all  $m \in \epsilon[(M_H)^G]$  we have

$$\sum_{i=1}^s g_i \epsilon \gamma^* \epsilon g_i^{-1} m = \epsilon \left( \sum_{i=1}^s g_i \gamma^* g_i^{-1} \right) \epsilon m = m.$$

Because  $\epsilon[(M_H)^G] \cong M$ , it follows that there exists a  $KH$ -endomorphism  $\tau$  of  $M$  such that  $\sum g_i \tau g_i^{-1} = 1$ , as required.

Statement (iii) implies (i). We must prove that whenever  $M$  is a submodule of a  $KG$ -module  $R$  such that  $M_H$  is a component of  $R_H$ , then  $M$  is a component of  $R$ . Let  $\epsilon$  be a  $KH$ -endomorphism of  $R$  such that  $\epsilon R = M$  and  $\epsilon^2 = \epsilon$ . Then it is easily verified that because of (iii),

$$\epsilon' = \sum_{i=1}^s g_i \tau \epsilon g_i^{-1}$$

is a  $KG$ -endomorphism of  $R$  such that  $\epsilon' m = m$  for all  $m \in M$  and  $\epsilon' R \subset M$ . Therefore  $R$  is the direct sum of its  $KG$ -submodules  $\epsilon' R = M$  and  $(1 - \epsilon')R$ . This completes the proof of Theorem 63.2.

The next result is in a way dual to the previous theorem, and we shall not give so detailed a proof.

(63.5) THEOREM. *The following statements concerning a left  $KG$ -module are equivalent:*

- (i)  $M$  is  $(G, H)$ -projective,
- (ii)  $M$  is isomorphic to a  $KG$ -component of  $(M_H)^G$ ,
- (iii) There exists a  $KH$ -endomorphism  $\tau$  of  $M$  such that  $\sum g_i \tau g_i^{-1} = 1$ , where the  $\{g_i\}$  are representatives of the distinct left cosets of  $H$  in  $G$ .

PROOF. Statement (i) implies (ii). First, we verify that

$$\phi: \sum g_i \otimes m_i \rightarrow \sum g_i m_i, \quad m_i \in M,$$

is a  $KG$ -homomorphism of  $(M_H)^G$  onto  $M$  whose kernel

$$M'' = \{\sum g_i \otimes u_i : \sum g_i u_i = 0\}$$

is a  $KH$ -direct summand of  $(M_H)^G$ . Because  $M$  is  $(G, H)$ -projective, it

follows that  $M''$  is a  $KG$ -direct summand of  $(M_H)^g$ , and the  $KG$ -submodule complementary to  $M''$  is isomorphic to  $M$ , proving that (i) implies (ii).

Statement (ii) implies (iii) as in the previous theorem.

Finally, let us assume (iii). We have to prove that if  $R$  is a  $KG$ -module and  $\eta$  a  $KG$ -homomorphism of  $R$  onto  $M$  whose kernel  $R''$  is a  $KH$ -direct summand of  $R_H$ , then  $R''$  is a  $KG$ -direct summand of  $R$ . Let  $\lambda$  be a  $KH$ -homomorphism of  $M$  into  $R$  such that  $\eta\lambda = 1$ , and set  $\mu = \Sigma g_i \lambda \gamma g_i^{-1}$ . Then  $\mu$  is a  $KG$ -homomorphism of  $M$  into  $R$  such that  $\eta\mu = 1$ . It follows that  $R''$  is a  $KG$ -direct summand of  $R$ . This completes the proof of Theorem 63.5.

The application of these results to the study of indecomposable  $KG$ -modules is based on the following two results:

(63.6) THEOREM. *Let  $H$  be a subgroup of  $G$ , and  $K$  an arbitrary field. Let  $L$  be any  $KH$ -module. Then  $L$  is isomorphic to a  $KH$ -component of  $(L^g)_H$ .*

PROOF. Let  $\{g_1 = 1, g_2, \dots, g_s\}$  be a set of representatives of the left cosets of  $H$  in  $G$ . Then the mapping

$$l \rightarrow g_1 \otimes l = 1 \otimes l$$

is a  $KH$ -isomorphism of  $L$  onto the  $KH$ -submodule  $1 \otimes L$  of  $(L^g)_H$ . Moreover, it is clear that  $L^* = \sum_{i=2}^s g_i \otimes L$  is a  $KH$ -submodule of  $(L^g)_H$  complementary to  $1 \otimes L$ , and Theorem 63.6 is proved.

(63.7) THEOREM. *Let  $K$  be a field of characteristic  $p > 0$ , and let  $P$  be a fixed  $p$ -Sylow subgroup of  $G$ . Then every left  $KG$ -module  $M$  is  $(G, P)$ -injective.*

PROOF. Let  $\{g_1, \dots, g_s\}$  be a set of representatives of the left cosets of  $P$  in  $G$ . The index  $s = [G: P]$  is prime to  $p$ ; hence  $s \cdot 1 \neq 0$  in  $K$ , and if we set  $\gamma = s^{-1}1_M$  where  $1_M$  is the identity mapping on  $M$ , then  $\sum g_i \gamma g_i^{-1} = 1_M$ . By Theorem 63.2,  $M$  is  $(G, P)$ -injective.

(63.8) COROLLARY. *Let  $K$  be a field of characteristic  $p > 0$ , and let  $P$  be a fixed  $p$ -Sylow subgroup of  $G$ . Then any  $KG$ -module  $M$  is isomorphic to a  $KG$ -component of an induced module  $L^g$  for a suitably chosen  $KP$ -module  $L$ .*

PROOF. By Theorem 63.7,  $M$  is  $(G, P)$ -injective. By Theorem 63.2,  $M$  is isomorphic to a component of  $(M_P)^g$ , and the corollary is established.

## § 64. Group Algebras of Finite Representation Type

In this section,  $G$  denotes a finite group and  $K$  any field whose characteristic  $p$  divides  $[G: 1]$ . Then  $KG$  is a non-semi-simple algebra. Although we have some information about the principal indecomposable modules of  $KG$ , we have little information about the number of other indecomposable  $KG$ -modules or their dimensions. We say that  $KG$  has *finite representation type* if there exist only a finite number of non-isomorphic indecomposable  $KG$ -modules, and has *bounded representation type* if the dimensions of the indecomposable  $KG$ -modules are bounded. The next result shows that for group algebras, the two notions are equivalent. Whether the same is true for finite dimensional algebras in general is an unsolved problem (see, however, Jans [1], and Curtis and Jans [1]).

(64.1) **THEOREM** (Higman [3]; Kasch, Kneser, Kupisch [1]). *Let  $G$  be a finite group and  $K$  a field of characteristic  $p > 0$ . If the  $p$ -Sylow subgroups of  $G$  are cyclic, there are at most  $[G: 1]$  non-isomorphic indecomposable  $KG$ -modules. If  $G$  has a non-cyclic  $p$ -Sylow subgroup, there are indecomposable  $KG$ -modules of arbitrarily large dimension.*

**PROOF.** By way of introduction, we note that, because the  $p$ -Sylow subgroups are all conjugate, one is cyclic if and only if all are cyclic.

Now let  $P$  be a fixed  $p$ -Sylow subgroup of  $G$ , and suppose  $P$  is cyclic with generator  $b$  of order  $p^s$ . We require first the following lemma:

(64.2) **LEMMA.** *Let  $P = [b]$  be a cyclic group of order  $p^s$ ,  $s \geq 1$ , and let  $K$  be any field of characteristic  $p$ . Then  $KP$  has exactly  $p^s$  indecomposable non-isomorphic modules, whose dimensions are  $1, 2, \dots, p^s$ .*

**PROOF.** First, let  $M$  be an indecomposable  $KP$ -module, and let  $B$  be the linear transformation on  $M$  corresponding to  $b$ . Then

$$B^{p^s} - 1 = (B - 1)^{p^s} = 0,$$

so that  $B$  has a minimum polynomial  $(X - 1)^k$  for some  $k \leq p^s$ . Since  $M$  is an indecomposable  $KP$ -module,  $M$  is by Exercise 58.3, a cyclic  $K[B]$ -module and  $[M: K] = k$ . Two indecomposable  $KP$ -modules are isomorphic if and only if they have the same dimension. Finally, for each  $k \leq p^s$ , there exists a cyclic indecomposable transformation  $B$  whose minimum polynomial is  $(X - 1)^k$ , and for this  $B$  we have  $B^{p^s} = 1$ . Therefore  $KP$  has an indecomposable module of dimension

$k$  for each  $k$ ,  $1 \leq k \leq p^s$ . This completes the proof of Lemma 64.2.

Now we can prove the first statement of the theorem. Let  $M$  be any indecomposable  $KG$ -module. By Theorems (63.7) and (63.2),  $M$  is a component of  $(M_P)^G$ . It follows from the Krull-Schmidt theorem that  $M$  is a  $KG$ -component of  $L^G$  for some indecomposable  $KP$ -component  $L$  of  $M_P$ , and in particular we have

$$(M: K) \geq (L: K).$$

Now let  $\{N_i\}$  be a full set of indecomposable  $KP$ -modules such that  $(N_i: K) = i$ ,  $1 \leq i \leq p^s = [P: 1]$ , constructed as in the preceding lemma. The preceding argument shows that every indecomposable  $KG$ -module  $M$  appears as a component of dimension greater than or equal to  $j = (N_j: K)$  of some induced module  $N_j^G$ ,  $1 \leq j \leq p^s$ . Since

$$(N_j^G: K) = [G: P](N_j: K) = j[G: P],$$

there are at most  $[G: P]$  non-isomorphic  $KG$ -components of  $N_j^G$  of dimension greater than or equal to  $j$ . Therefore the total number of non-isomorphic indecomposable  $KG$ -modules does not exceed

$$p^s[G: P] = [G: 1],$$

and the first part of the theorem is proved.

Conversely, suppose  $G$  has a non-cyclic  $p$ -Sylow subgroup  $P$ . Let  $L$  be an indecomposable  $KP$ -module. By Theorem 63.6,  $L$  is  $KP$ -isomorphic to a  $KP$ -component of  $L^G$ . Therefore, by the Krull-Schmidt theorem,  $L^G$  has a  $KG$ -component of dimension greater than or equal to  $(L: K)$ . It follows that, if we can find indecomposable  $KP$ -modules of arbitrarily high dimension,  $KG$  will also be of unbounded representation type, and the theorem will be proved.

Thus we may assume that  $G$  itself is a non-cyclic  $p$ -group. By (6.10),  $G$  has a factor group  $G/H \cong A \times A$ , where  $A$  is a cyclic group of order  $p$ . Since every indecomposable  $K(G/H)$ -module is also an indecomposable  $KG$ -module, we have reduced the problem to proving the following lemma.

(64.3) LEMMA. *Let  $G = [a] \times [b]$  where  $a$  and  $b$  both have order  $p$ , and let  $K$  be a field of characteristic  $p$ . Then  $KG$  has an indecomposable module of dimension  $2n + 1$  for every positive integer  $n$ .*

PROOF. (Heller and Reiner [1]) Let  $M$  be a vector space over  $K$  with basis  $\{x_0, x_1, \dots, x_n; y_1, \dots, y_n\}$ . Define

$$(64.4) \quad \begin{cases} ax_i = bx_i = x_i, & 0 \leq i \leq n; \\ (a-1)y_i = x_i, & 1 \leq i \leq n; \\ (b-1)y_i = x_{i-1}, & 1 \leq i \leq n. \end{cases}$$

We leave to the reader the easy computation that shows that  $M$  is a  $KG$ -module. Let

$$M = X \oplus Y,$$

where  $X$  is the  $K$ -subspace spanned by  $\{x_0, \dots, x_n\}$  and  $Y$  is spanned by  $\{y_1, \dots, y_n\}$ . Let  $\pi$  be the projection of  $M$  onto the subspace  $Y$ .

Equations (64.4) imply that left multiplications by  $a - 1$  and by  $b - 1$  both map  $Y$  isomorphically into  $X$ , and send  $X$  into  $(0)$ .

Now suppose that  $M$  is decomposable, and let

$$M = M_1 \oplus M_2$$

where  $M_1$  and  $M_2$  are non-zero  $KG$ -submodules. Let

$$(\pi(M_1): K) = r$$

for some  $r$ ,  $1 \leq r \leq n$ . Then  $(a - 1)M_1 \subset M_1$ , and  $(a - 1)M_1 = (a - 1)\pi(M_1)$  so that  $((a - 1)M_1: K) = r$ . Moreover,  $(b - 1)M_1$  contains at least one vector not in  $(a - 1)M_1$ . Therefore

$$(64.5) \quad (M_1: K) \geq 2r + 1, \quad 0 \leq r \leq n. *$$

A corresponding inequality holds for  $M_2$ . Now let

$$(\pi(M_1): K) = r, \quad (\pi(M_2): K) = s.$$

Then  $r + s \geq n$ , and

$$(M_1: K) \geq 2r + 1, \quad (M_2: K) \geq 2s + 1.$$

Therefore

$$(M: K) \geq 2(r + s) + 2 \geq 2n + 2$$

which is impossible since  $(M: K) = 2n + 1$ . Therefore  $M$  is an indecomposable  $KG$ -module. This completes the proof of Lemma 64.3 as well as the proof of Theorem 64.1.

We conclude this section with another theorem by Kasch, Kneser, and Kupisch [1].

(64.6) THEOREM. *Let  $G$  be a finite group with a cyclic  $p$ -Sylow subgroup  $P$ , and let  $K$  be a field of characteristic  $p$ . Then  $KG$  has exactly  $[G: 1]$  non-isomorphic indecomposable modules if and only if  $P \triangleleft G$ ,  $G/P$  is abelian, and  $K$  contains a primitive  $m$ th root of 1, where  $m$  is the exponent of  $G/P$ .*

PROOF. Let  $\{N_i\}$  be a full set of indecomposable  $KP$ -modules, where  $(N_i: K) = i$ ,  $1 \leq i \leq p^s = [P: 1]$ . From the proof of Theorem 64.1, there exist  $[G: 1]$  different indecomposable  $KP$ -modules if and only if for each  $i$ ,  $1 \leq i \leq p^s$ ,  $N_i^G$  is a direct sum of  $[G: P]$  non-isomorphic

---

\* The inequality is trivially true if  $r = 0$ , since  $M_1 \neq 0$ .

indecomposable  $KG$ -modules of dimension  $i$ . If this happens, then in particular there are  $[G: P]$  distinct one-dimensional representations of  $G$ . The intersection of the kernels of these representations contains  $P$ , since  $K$  has characteristic  $p$ , and has index greater than or equal to  $[G: P]$ . It follows that  $P \triangle G$ ,  $G/P$  is abelian, and  $K$  contains a primitive  $m$ th root of 1, where  $m$  is the exponent of  $G/P$ .

Suppose, conversely, that these conditions are satisfied; let  $P = [b]$ , and let  $N = KG(1 - b)$ . For all  $g \in G$ , we have

$$\begin{aligned} (1 - b)g &= g(1 - g^{-1}bg) = g(1 - b^j) && (\text{for some } j) \\ &= g(1 + b + \cdots + b^{j-1})(1 - b) \in KG(1 - b), \end{aligned}$$

and therefore

$$N = KG(1 - b) = (1 - b)KG.$$

Since  $(1 - b)^{p^e} = 0$ , it follows that  $N$  is a nilpotent two-sided ideal in  $KG$ . Let  $f$  be the natural mapping of  $G \rightarrow G/P$ ; then  $f$  defines a homomorphism  $\tilde{f}: KG \rightarrow K(G/P)$  whose kernel contains  $N$  and has dimension  $[G: 1] - [G: P] = [G: P]([P: 1] - 1)$ . It is clear that  $N$  contains at least  $[G: P]([P: 1] - 1)$  linearly independent elements, namely,  $\{x_j(b^i - 1)\}, 1 \leq j \leq [G: P], 1 \leq i < p^e$ , where the  $\{x_j\}$  are coset representatives of  $P$  in  $G$ . It follows that  $N$  is the kernel of  $\tilde{f}$ , and we have  $KG/N \cong K(G/P)$ . Since  $K(G/P)$  is semi-simple,  $N = \text{rad } KG$ , and all the irreducible  $KG$ -modules are irreducible  $K(G/P)$ -modules, and are one-dimensional since  $K$  is a splitting field for  $G/P$ . Set  $A = KG$ , and let  $Ae_1, \dots, Ae_t$  be a complete set of non-isomorphic principal indecomposable modules for  $KG$ . Then  $t = [G: P]$ , and by Theorem 61.13, each  $Ae_i$  appears exactly once as a component of the left regular module. Each module  $Ae_i$  has a composition series

$$Ae_i = M_{id_i} \supset M_{i, d_i-1} \supset \cdots \supset M_{i1} \supset 0, \quad d_i = (Ae_i: K),$$

where each composition factor  $M_{ij}/M_{i,j-1}$  is one-dimensional over  $K$ . Since  $KG$  is a quasi-Frobenius ring,  $M_{i1}$  is the unique minimal subideal of  $Ae_i$ . Therefore all the modules  $M_{ij}$  are indecomposable. We show finally that no two distinct modules  $M_{ij}$  are isomorphic. Since the second index  $j = (M_{ij}: K)$ ,  $M_{ij} \cong M_{kl}$  implies that  $j = l$ . We then have  $M_{ij} \cong M_{kj}$  implying  $M_{i1} \cong M_{k1}$ . Since  $KG$  is a quasi-Frobenius ring, we can apply Theorem 58.12 to deduce that  $M_{i1} = M_{k1}$  implies  $i = k$ . We have proved that there exist  $\sum_{i=1}^t (Ae_i: K) = [G: 1]$  distinct indecomposable modules, and the proof of Theorem 64.6 is completed.

*Exercise*

1. (See Wallace [2].) Let  $P$  be a normal  $p$ -Sylow subgroup of a finite group  $G$ , and let  $K$  be a field of characteristic  $p$ . Prove that

$$N = \sum_{\substack{y \in P \\ y \neq 1}} (y - 1)KG$$

coincides with  $\text{rad } KG$  and that  $(N: K) = [G: P](|P: 1| - 1)$ . [Hint: Prove that  $T = \sum_{y \in P, y \neq 1} K(y - 1)$  is a subalgebra of  $KG$  having a nilpotent basis, so that  $T$  is nilpotent by Theorem 27.27 and Exercise 29.9. Then prove  $N = T \cdot KG = KG \cdot T$  and hence that  $N$  is a nilpotent two-sided ideal in  $KG$ . Finally, prove as in Theorem 64.6 that  $KG/N \cong K(G/P)$ . The dimension of  $N$  is determined as in the argument of Theorem 64.6.]

### § 65. The Vertex and Source of an Indecomposable Module

We shall continue our study of indecomposable  $KG$ -modules, where  $K$  is a field of characteristic  $p$  dividing  $[G: 1]$ . The main results in this section, due to Green [1], show that to each indecomposable  $KG$ -module  $M$  corresponds a  $p$ -subgroup  $B$  of  $G$ , called the *vertex* of  $M$ , and an indecomposable  $KB$ -module  $L$ , called the *source* of  $M$ , such that  $M$  is a component of  $L^g$ .

We begin with a few more remarks about induced modules. Let  $H$  be a subgroup of  $G$ , and  $L$  a left  $KH$ -module. For any  $x \in G$ ,  $x \otimes L$  is a  $K$ -subspace of the induced module  $L^g = KG \otimes_{KH} L$ . The subspace  $x \otimes L$  is in fact a left  $K(xHx^{-1})$ -module since for all  $h \in H$ ,  $l \in L$ ,

$$(xhx^{-1})x \otimes l = xh \otimes l = x \otimes hl \in x \otimes L.$$

Thus, in particular,  $x \in N(H)$  implies that  $x \otimes L$  is a  $KH$ -module. When we write  $x \otimes L$ , it will be understood that we are referring to  $x \otimes L$  as a  $K(xHx^{-1})$ -submodule of  $L^g$ .

(65.1) LEMMA. *For all  $x \in G$ ,  $(x \otimes L)^g \cong L^g$  as left  $KG$ -modules.*

PROOF. (See Exercise 38.5.) Let  $\{x_1, \dots, x_n\}$  be a set of left coset representatives of  $H$  in  $G$ . Then  $\{x_1x^{-1}, \dots, x_nx^{-1}\}$  is a set of left coset representatives of  $xHx^{-1}$  in  $G$ , and the mapping

$$\theta: \sum x_i \otimes l_i \rightarrow \sum x_i x^{-1} \otimes (x \otimes l_i)$$

is a one-to-one mapping of  $L^g$  onto  $(x \otimes L)^g$ . It is easily checked that  $\theta$  is a  $KG$ -isomorphism. In fact,  $gx_i = x_j h_{ji}$ ,  $h_{ji} \in H$ , implies that  $gx_i x^{-1} = x_j x^{-1}(x_j h_{ji} x^{-1})$ , and from this we obtain easily

$$\theta(g(\sum x_i \otimes l_i)) = g\theta(\sum x_i \otimes l_i).$$

(65.2) LEMMA. A left  $KG$ -module  $M$  is  $(G, H)$ -projective if and only if there exists a left  $KH$ -module  $L$  such that  $M$  is a component of  $L^g$ .

PROOF. If  $M$  is  $(G, H)$ -projective, then by Theorem 63.5,  $M$  is a component of  $(M_H)^g$ . Conversely, suppose  $M$  is a component of  $L^g$  for some  $KH$ -module  $L$ . Then for a set of left coset representatives  $\{x_1, \dots, x_n\}$  of  $H$  in  $G$  with  $x_1 = 1$ , the mapping  $\gamma^*: \sum x_i \otimes l_i \rightarrow 1 \otimes l_1$  satisfies the condition

$$\sum_{i=1}^n x_i \gamma^* x_i^{-1} = 1.$$

Because  $M$  is a component of  $L^g$ , there exists a  $KG$ -projection  $\epsilon$  of  $L^g$  upon  $M$ . Then, as in the proof of Theorem 63.2,  $\epsilon \gamma^* \epsilon$  is a  $KH$ -endomorphism of  $M$  such that  $\sum x_i \epsilon \gamma^* \epsilon x_i^{-1} = 1$ , proving that  $M$  is  $(G, H)$ -projective [by Theorem (63.5)].

(65.3) DEFINITION. We shall use the notation

$$H_1 =_e H_2$$

to indicate that the subgroups  $H_1$  and  $H_2$  are conjugate in  $G$ , and

$$H_1 \subset_e H_2$$

to mean that  $xH_1x^{-1} \subset H_2$  for some  $x \in G$ .

(65.4) LEMMA. If  $M$  is a  $(G, H)$ -projective  $KG$ -module, it is  $(G, R)$ -projective for every subgroup  $R$  such that  $H \subset_e R$ .

PROOF. By hypothesis, there exists a  $KH$ -module  $L$  such that  $M$  is a component of  $L^g$ , and an element  $x$  such that  $xHx^{-1} \subset R$ . Then  $(x \otimes L)^R$  is a  $KR$ -module, and

$$((x \otimes L)^R)^g \cong (x \otimes L)^g \cong L^g$$

by Lemma 65.1. By Lemma 65.2,  $M$  is  $(G, R)$ -projective.

(65.5) LEMMA. Let  $L$  be a left  $KH$ -module and  $M$  a  $KG$ -component of  $L^g$ . If  $L$  is  $(H, H_0)$ -projective for a subgroup  $H_0$  of  $H$ , then  $M$  is  $(G, H_0)$ -projective.

PROOF. By Lemma 65.2, there exists a  $KH_0$ -module  $L_0$  such that  $L_0^H \cong L + L'$  for some  $KH$ -module  $L'$ . Then

$$(L_0^H)^g \cong L_0^g \cong L^g + L'^g.$$

Since  $M$  is a component of  $L^g$ , it is also a component of  $L_0^g$ , and the lemma is proved.

For convenience we shall restate the subgroup theorem [Theorem 44.2] in the following form:

(65.6) *Let  $B$  and  $H$  be subgroups of  $G$  and  $L$  a left KB-module. Let  $D_1 = Ha_1B, \dots, D_t = Ha_tB$  be the distinct  $(H, B)$ -double cosets of  $G$ . Then*

$$(65.7) \quad (L^g)_H = \sum_{i=1}^t \oplus Z(D_i),$$

where  $Z(D_i) = ((a_i \otimes L)_{H_i^*})^H$ , and  $H_i^* = a_i B a_i^{-1} \cap H, 1 \leq i \leq t$ .

(65.8) **LEMMA.** *Let  $M$  be a left KG-module, let  $B, H$  be subgroups of  $G$ , and let  $L$  be a left KB-module such that  $M$  is a component of  $L^g$ . Let*

$$M_H = V_1 \oplus \cdots \oplus V_s$$

where the  $\{V_i\}$  are indecomposable KH-modules. Then for each  $i$ ,  $1 \leq i \leq s$ , there exists an  $x_i \in G$  such that

- (i)  $V_i$  is  $(H, H_i^*)$ -projective where  $H_i^* = x_i B x_i^{-1} \cap H$ , and
- (ii)  $V_i$  is a component of  $L_i^H$  where  $L_i = (x_i \otimes L)_{H_i^*}$ .

**PROOF.** The proof is immediate by the subgroup theorem. Indeed, since  $M$  is a component of  $L^g$ ,  $M_H$  is a component of  $(L^g)_H$ , and by the subgroup theorem (65.6) and the Krull-Schmidt theorem, each  $V_i$  is a component of some  $Z(D_i)$  in (65.7). This proves (ii), and (i) now follows from Lemma 65.2.

(65.9) **REMARK.** *Let  $M$  be a left KG-module. Let  $V(M)$  be the set of all subgroups  $H$  of  $G$  such that  $M$  is  $(G, H)$ -projective. Then  $V(M)$  contains a minimal member  $B$  with respect to the quasi-ordering  $\subseteq_e$ . Thus, if  $C \in V(M)$  and  $C \subset_e B$ , then  $C =_e B$ . If  $H \in V(M)$  and  $R \supset_e H$ , then by Lemma 65.4,  $M$  is  $(G, R)$ -projective and  $R \in V(M)$ .*

(65.10) **LEMMA.** *Let  $M$  be an indecomposable KG-module. Let  $B$  be a minimal member of  $V(M)$  as in remark (65.9), let  $L$  be a left KB-module such that  $M$  is a component of  $L^g$ , and let  $H$  be any subgroup in  $V(M)$ . Let*

$$M_H = V_1 \oplus \cdots \oplus V_s$$

where the  $\{V_i\}$  are indecomposable KH-modules. Then for at least one  $V_i$ ,  $M$  is a component of  $V_i^H$ . For any such  $V_i$ , there exists an  $x_i \in G$  such that

$$x_i B x_i^{-1} \subset H,$$

and  $V_i$  is a component of  $(x_i \otimes L)^H$ .

**PROOF.** Since  $M$  is  $(G, H)$ -projective,  $M$  is a component of  $(M_H)^G$  and hence of some  $V_i^g$ . By Lemma 65.8,  $V_i$  is  $(H, H_i^*)$ -projective where  $H_i^* \subset_c B$ . Since  $B$  is minimal, we have  $H_i^* =_c B$ , and  $H_i^* = x_i B x_i^{-1} \subset H$  for some  $x_i \in G$ . By Lemma 65.8 again,  $V_i$  is a component of  $(x_i \otimes L)^H$ .

Now we come to our first main result.

(65.11) **THEOREM.** *Let  $M$  be an indecomposable  $KG$ -module. Then there exists a subgroup  $B \subset G$  such that*

- (i)  $M$  is  $(G, B)$ -projective, and
- (ii) if  $M$  is  $(G, H)$ -projective, then  $B \subset_c H$ .

The subgroup  $B$  is uniquely determined up to conjugacy.

**PROOF.** The existence and properties of  $B$  are immediate consequences of remark (65.9) and Lemma 65.10. The uniqueness of  $B$  follows from statement (ii) above.

(65.12) **DEFINITION.** Let  $M$  be an indecomposable  $KG$ -module. The subgroup  $B$  of  $G$  which satisfies conditions (i) and (ii) of that theorem is called a *vertex* of  $M$ . By Theorems (63.7) and (65.11), a vertex is always a  $p$ -subgroup of  $G$ .

(65.13) **DEFINITION.** Let  $M$  be an indecomposable  $KG$ -module, and let  $B$  be a vertex of  $M$ . An indecomposable  $KB$ -module  $L$  is called a *B-source* of  $M$  if  $M$  is a component of  $L^g$ .

We note that if  $M$  is indecomposable with vertex  $B$  and  $B$ -source  $L$ , then for any  $x \in G$ ,  $x B x^{-1}$  is a vertex of  $M$ , and  $x \otimes L$  is a  $x B x^{-1}$ -source of  $M$ , since  $(x \otimes L)^g \cong L^g$  by Lemma 65.1.

(65.14) **THEOREM.** *Let  $B$  be a vertex of the indecomposable left  $KG$ -module  $M$ , and let  $L$  and  $L'$  be two  $B$ -sources for  $M$ . Then there exists  $x \in N(B)$  such that  $L' \cong x \otimes L$  as left  $KB$ -modules.*

**PROOF.** Letting  $B = H$  in Lemma 65.10, we can find  $V_i$  such that  $M$  is a component of  $V_i^g$ , and for this  $i$ ,  $x_i B x_i^{-1} \subset B$ . Then  $x_i \in N(B)$ , and  $V_i$  is a component of the  $KB$ -module  $(x_i \otimes L)^B = x_i \otimes L$ , so that  $V_i = x_i \otimes L$  since  $L$  is indecomposable. Now replace  $L$  by  $L'$ , and obtain  $x_j \in N(B)$  such that  $x_i \otimes L \cong x_j \otimes L'$ . Then  $x_j^{-1} x_i \in N(B)$ , and we have

$$L' \cong 1 \otimes L' \cong x_j^{-1} x_i \otimes L$$

as we wished to prove.

(65.15) THEOREM. Let  $M$  be an indecomposable  $KG$ -module with vertex  $B$ , and  $H$  a subgroup of  $G$  such that  $M$  is  $(G, H)$ -projective. Let

$$M_H = V_1 \oplus \cdots \oplus V_s$$

where the  $\{V_i\}$  are indecomposable  $KH$ -modules, and for each  $i$ ,  $1 \leq i \leq s$ , let  $B_i$  be a vertex of  $V_i$ . Then

- (i)  $B_i \subset_c B$  for  $1 \leq i \leq s$ ;
- (ii) there exists a  $V_i$  such that  $M$  is a component of  $V_i^g$ , and for this  $i$ , we have
- (iii)  $B_i =_c B$ .

PROOF. We apply Lemma 65.10 to prove the first statement. Let  $L$  be a  $B$ -source of  $M$ . Then by Lemma 65.8, each  $V_i$  is  $(H, H_i^*)$ -projective, and we have

$$B_i \subset_c H_i^* \subset_c B$$

since  $H_i^* = x_i B x_i^{-1} \cap H$ .

Now we apply Lemma 65.10 to obtain statement (ii). Indeed, if  $M$  is a component of  $V_i^g$  and  $V_i$  is  $(H, B_i)$ -projective, then by Lemma 65.5,  $M$  is  $(G, B_i)$ -projective. Since  $B$  is a vertex of  $M$ , we have  $B \subset_c B_i$ , and by the first part of the proof we have  $B =_c B_i$ .

We can apply this rather intricate machinery to obtain a very sharp and interesting result concerning the principal indecomposable modules of  $KG$ .

(65.16) THEOREM. Let  $K$  be a field of characteristic  $p > 0$ , and let  $M$  be a principal indecomposable  $KG$ -module. Let  $P$  be an arbitrary  $p$ -Sylow subgroup of  $G$ . Then  $M_P$  is isomorphic to a direct sum of  $KP$ -modules all isomorphic to the left regular module  ${}_{KP}KP$ .

PROOF. Since  $M$  is a component of  $KG \cong KG \otimes_K K1$ , we see that  $M$  is a  $(G, \{1\})$ -projective module and has the vertex  $\{1\}$ . Let

$$M_P = V_1 \oplus \cdots \oplus V_s$$

where the  $V_i$  are indecomposable  $KP$ -modules, and let  $B_i$  be a vertex of  $V_i$  for  $1 \leq i \leq s$ . By Theorem 65.15,  $B_i \subset_c \{1\}$ ; hence  $B_i = \{1\}$  for  $1 \leq i \leq s$ . Therefore, each  $V_i$  is a component of the left regular module  $KP$ . Since  $P$  is a  $p$ -group, it follows from Exercise 54.1 that the left regular module of  $KP$  is indecomposable. Therefore, each  $V_i \cong KP$  as left  $KP$ -modules, and Theorem 65.16 is proved.

(65.17) COROLLARY (Dickson [1]). Let  $[G:1] = p^a q$  where  $p$  is a

prime and  $p \nmid q$ . Let  $K$  be a field of characteristic  $p$ , and let  $M$  be a principal indecomposable  $KG$ -module. Then

$$p^a \mid (M: K).$$

### § 66. Centralizers of Modules over Symmetric Algebras

In this section, we denote by  $A$  a symmetric algebra (to be defined below) over an arbitrary field,  $M$  a left  $A$ -module, and  $C = \text{Hom}_A(M, M)$  the centralizer of  $M$ . We shall show that if the ideal  $B = \{a \in A : aM = 0\}$  is a component of  $A$ , then there is a one-to-one correspondence between the  $C$ -components of  $M$  and the right ideal components of a certain two-sided ideal of  $A$ . These results hold in particular if  $A = KG$  is the group algebra of a finite group, and were established in this case by Weyl [1]. In § 67 we shall apply these results to construct the irreducible tensor representations of the full linear group, following the ideas of Weyl in his book [2]. Our presentation is based on two papers by Curtis ([1], [2]).

(66.1) DEFINITION. A finite-dimensional algebra  $A$  over a field  $K$  is called a *symmetric algebra* if  $A$  admits a non-degenerate bilinear form  $f: A \times A \rightarrow K$  which is associative:

$$f(ab, c) = f(a, bc), \quad a, b, c \in A,$$

and symmetric:

$$f(a, b) = f(b, a), \quad a, b, c \in A.$$

REMARK 1. It follows at once from the definition and the proof of Theorem 61.3 that  $A$  is symmetric if and only if there exists a linear function  $\nu: A \rightarrow K$  whose kernel contains no left or right ideals different from zero, and contains all additive commutators  $ab - ba$ ,  $a, b \in A$ .

REMARK 2. We have the following inclusions for classes of finite-dimensional algebras over  $K$ :

$$\{\text{group algebras}\} \subset \{\text{symmetric algebras}\}$$

$$\subset \{\text{Frobenius algebras}\} \subset \{\text{quasi-Frobenius algebras}\}.$$

The second inclusion is immediate by Theorem 61.3 and Definition 66.1, the third has already been proved, and we shall now prove the first. Let  $A = KG$  be the group algebra of a finite group  $G$  and

define the linear function  $\lambda$  on  $G$  by setting

$$\lambda\left(\sum_{g \in G} a_g g\right) = \alpha_1 .$$

We have already proved in Theorem 62.1 that the kernel of  $\lambda$  contains no non-zero left or right ideals. It remains to prove that

$$\lambda(ab - ba) = 0$$

for all  $a, b \in A$ . Let  $a = \sum a_g g$ ,  $b = \sum \beta_g g$ ; then the coefficient of 1 in  $ab$  is  $\sum_{gh=1} a_g \beta_h$ , whereas the coefficient of 1 in  $ba$  is  $\sum_{gh=1} \beta_h \alpha_g$ , and we have  $\lambda(ab - ba) = 0$  as required.

Now we assume that  $A$  is an arbitrary symmetric algebra with associative symmetric form  $f$ . Let  $\{a_i\}$  and  $\{b_j\}$  be dual bases of  $A$  with respect to  $f$ . Because of the symmetry of  $f$ , we have two sets of relations

$$(66.2) \quad ab_i = \sum_j b_j \lambda_{j,i}(a) \iff a_i a = \sum_j \lambda_{i,j}(a) a_j$$

and

$$(66.3) \quad b_i a = \sum_j \mu_{i,j}(a) b_j \iff a a_i = \sum_j a_j \mu_{j,i}(a) ,$$

instead of the formulas (62.9) and (62.10) which we used in §62.

Now let  $M$  be a left  $A$ -module, and let  $M^* = \text{Hom}_K(M, K)$  be the  $K$ -dual of  $M$  viewed as a right  $A$ -module according to the definition

$$(66.4) \quad (\psi a)(x) = \psi(ax) , \quad \psi \in M^*, x \in M, a \in A .$$

We define a mapping  $\tau: M \times M^* \rightarrow A$  by the rule

$$(66.5) \quad \tau(x, \psi) = \sum_i b_i \psi(a_i x) .$$

The mapping  $\tau$  is obviously biadditive, and it is immediate by (66.2), (66.3), and (66.4) that  $\tau$  is  $A$ -bilinear in the sense that

$$\tau(ax + by, \psi) = a\tau(x, \psi) + b\tau(y, \psi)$$

and

$$\tau(x, \phi a + \psi b) = \tau(x, \phi)a + \tau(x, \psi)b ,$$

for all  $x, y \in M$ ,  $a, b \in A$ ,  $\phi, \psi \in M^*$ . The function  $\tau$  is non-degenerate. Suppose, for example, that

$$\tau(x, \psi) = 0$$

for all  $x \in M$ ; since the  $\{b_i\}$  are linearly independent, we then have

$$\phi(a_i x) = 0, \quad 1 \leq i \leq (A:K), x \in M,$$

and since 1 is a linear combination of the  $\{a_i\}$ , we have  $\phi(M) = 0$  and  $\phi = 0$ . Similarly,  $\tau(x, \phi) = 0$  for all  $\phi$  implies  $x = 0$ .

Because of the  $A$ -bilinearity of the form  $\tau$ , the set of all finite sums

$$\sum \tau(x_i, \phi_i), \quad x_i \in M, \phi_i \in M^*,$$

is a two-sided ideal in  $A$  which we shall call the *nucleus* of  $M$  and denote by  $A_M$ .

(66.6) DEFINITION. A left  $A$ -module  $M$  is called *regular with respect to the pairing  $\tau$*  if the nucleus  $A_M$  contains an idempotent  $\epsilon$  such that  $a\epsilon = \epsilon a = a$  for all  $a \in A_M$ .

The next theorem shows that any module  $M$  is regular if either  $A$  acts faithfully on  $M$  or if  $A$  is semi-simple. The theory we shall present later in this section is based on a number of formal calculations which can be performed in case  $M$  is a regular module; it is not known what happens if  $M$  fails to be regular.

(66.7) THEOREM. A left  $A$ -module  $M$  over a symmetric algebra  $A$  is regular with respect to the pairing  $\tau$  given by (66.5) if either

- (i)  $A$  is semi-simple, or
- (ii)  $M$  is a faithful  $A$ -module.

In case (ii),  $A_M$  coincides with  $A$ .

PROOF. Since  $A_M$  is a two-sided ideal in  $A$ , we have  $A = A_M \oplus A'$  for some two-sided ideal  $A'$ , if  $A$  is semi-simple, and it follows that  $A_M = \epsilon A = A\epsilon$  for some central idempotent  $\epsilon$ , proving that  $M$  is regular with respect to  $\tau$  in this case.

The proof that  $M$  is regular with respect to  $\tau$  when  $M$  is faithful, lies somewhat deeper. First, let us make the stronger assumption that  $M$  contains a direct summand  $R$  which is isomorphic to  $A$ . Let  $x \in R$  correspond to 1 in  $A$  under the isomorphism; then the elements  $\{a_i x\}$ ,  $1 \leq i \leq (A:K)$ , are linearly independent over  $K$ . Therefore there exists for each  $i$  an element  $\phi_i \in M^*$  such that  $\phi_i(a_j x) = 1$ ,  $\phi_i(a_j x) = 0$ ,  $j \neq i$ . Then from (66.5) we have  $\tau(x, \phi_i) = b_i$ ,  $1 \leq i \leq (A:K)$ , and thus  $A_M = A$ , which of course implies that  $M$  is regular with respect to  $\tau$ .

Now let  $M$  be an arbitrary faithful module. Because  $A$  is a quasi-Frobenius algebra, Theorem 59.3 implies that the direct sum of  $M$  with itself a certain number of times contains a direct sum-

mand isomorphic to  $\mathbf{A}A$ . We have shown that, for this larger module  $U$ ,  $A_U = A$ , and since  $A_{U_1} = A_{U_2}$  for isomorphic  $A$ -modules  $U_1$  and  $U_2$ , the proof of Theorem 66.7 will be completed if we can prove the following lemma:

(66.8) LEMMA. *Let  $M$  be the direct sum of  $A$ -submodules  $M_1$  and  $M_2$ . Then  $A_M = A_{M_1} + A_{M_2}$ .*

PROOF. We have  $M^* = M_1^\perp \oplus M_2^\perp$  where  $M_2^\perp$  can be identified with  $M_1^*$ , and  $M_1^\perp$  with  $M_2^*$ . Let  $\tau_i$  be the form (66.5) associated with  $M_i$ ,  $i = 1, 2$ , where  $M_{3-i}^\perp$  is taken as  $M_i^*$ . Let  $x \in M$ ,  $\phi \in M^*$ ; then  $x = x_1 + x_2$ ,  $x_i \in M_i$ , and  $\phi = \phi_1 + \phi_2$ ,  $\phi_i \in M_{3-i}^\perp$ ,  $i = 1, 2$ . Then, from (66.5) we have

$$\begin{aligned}\tau(x, \phi) &= \sum b_i \phi(a_i x) = \sum b_i \phi_1(a_i x_1) + \sum b_i \phi_2(a_i x_2) \\ &= \tau_1(x_1, \phi_1) + \tau_2(x_2, \phi_2),\end{aligned}$$

and it follows that  $A_M = A_{M_1} + A_{M_2}$ . This completes the proof of Lemma 66.8 as well as the proof of Theorem 66.7.

Now we proceed to investigate the properties of an arbitrary regular module  $M$  with respect to a pairing  $\tau$  given by (66.5). The identity element  $\epsilon$  in  $A_M$  can be expressed in the form

$$\epsilon = \sum \tau(x_i^0, \phi_i^0), \quad x_i^0 \in M, \phi_i^0 \in M^*.$$

For all  $\phi \in M^*$  we have

$$\tau(\epsilon x - x, \phi) = \epsilon \tau(x, \phi) - \tau(x, \phi) = 0,$$

and because of the non-degeneracy of the form  $\tau$  we conclude that  $\epsilon x = x$  for all  $x \in M$ . Similarly  $\phi \epsilon = \phi$  for all  $\phi \in M^*$ .

Let  $C = \text{Hom}_{\mathbf{A}}(M, M)$ , and write the elements of  $C$  as right operators on  $M$ . Our object is to study the properties of  $M$  as a right  $C$ -module. Our first result is that the  $A$ -module  $M$  has the double centralizer property.

(66.9) THEOREM. *Let  $\gamma \in \text{Hom}_A(M, M)$ . Then there exists an element  $a \in A_M$  such that  $ax = \gamma x$  for all  $x \in M$ .*

PROOF. First, we construct for each pair  $(\phi, x) \in M^* \times M$  an endomorphism  $\phi \square x$  of  $M$  by the rule

$$(66.10) \quad m(\phi \square x) = \tau(m, \phi)x, \quad m \in M.$$

For all  $a \in A$  we have, because of the bilinearity of  $\tau$ ,

$$(am)[\phi \square x] = \tau(am, \phi)x = a(\tau(m, \phi)x) = a(m(\phi \square x)),$$

and we have proved that  $\phi \square x \in C$  for all  $\phi \in M^*$  and  $x \in M$ . We

are given that  $\gamma \in \text{Hom}_C(M, M)$ ; therefore in particular  $\gamma$  must commute with all the endomorphisms  $\phi \square x$ , and we have for all  $m \in M$ ,

$$(\gamma m)\phi \square x = \gamma(m(\phi \square x)).$$

From this equation, we have by (66.10) the result that

$$(66.11) \quad \tau(\gamma m, \phi)x = \gamma[\tau(m, \phi)x]$$

for all  $m, x$  in  $M$  and  $\phi \in M^*$ . Now let

$$a = \sum \tau(rx_i^0, \phi_i^0) \in A_M,$$

where  $\epsilon = \sum \tau(x_i^0, \phi_i^0)$  is the identity element of  $A_M$ . Applying (66.11), we obtain for all  $m \in M$

$$am = \sum \tau(rx_i^0, \phi_i^0)m = \gamma(\sum \tau(x_i^0, \phi_i^0)m) = \gamma(\epsilon m) = \gamma m$$

since  $\epsilon m = m$ , and Theorem 66.9 is proved.

We shall establish a connection between right ideals in  $A_M$  and  $C$ -submodules of  $M$  in the following way. For each right ideal  $I \subset A_M$ ,  $IM$  is a  $C$ -submodule of  $M$ , and for each  $C$ -submodule  $R$  of  $M$ ,

$$\tau(R, M^*) = \{\sum \tau(u_i, \phi_i) : u_i \in R, \phi_i \in M^*\}$$

is a right ideal of  $A$  contained in  $A_M$ , because of the bilinearity of  $\tau$ . In particular,  $\tau(M, M^*) = A_M$ .

The mappings  $I \rightarrow IM$  and  $R \rightarrow \tau(R, M^*)$  have the following properties:

$$(66.12) \quad I \supset \tau(IM, M^*), \quad R \supset \tau(R, M^*)M,$$

the first since  $\tau(IM, M^*) = I\tau(M, M^*) \subset I$  because  $I$  is a right ideal in  $A_M$ , the second because for all  $r \in R, \phi \in M^*, x \in M$ ,

$$\tau(r, \phi)x = r(\phi \square x)$$

and  $R$  is a  $C$ -submodule of  $M$ . We are interested in the cases when these inclusions can be replaced by equality.

(66.13) LEMMA. *Let  $R$  be a  $C$ -component of  $M$ . Then there exists an idempotent  $e \in A_M$  such that  $\tau(R, M^*) = eA$  and  $\tau(R, M^*)M = R$ .*

PROOF. Let  $\pi$  be a projection of  $M$  upon  $R$  which belongs to  $\text{Hom}_C(R, M)$ . By the proof of Theorem 66.9,  $\pi x = ex$ ,  $x \in M$ , where

$$e = \sum \tau(\pi x_i^0, \phi_i^0) \in \tau(R, M^*).$$

If  $a = \sum \tau(r_i, \phi_i)$  is an arbitrary element of  $\tau(R, M^*)$ , then

$$ea = \sum \tau(er_i, \psi_i) = a$$

since  $er_i = \pi r_i = r_i$  for  $r_i \in R$ . Therefore  $\tau(R, M^*) = eA$  and  $e^2 = e$ .

Now let  $x \in R$ ; then  $x = ex \in \tau(R, M^*)M$ . In view of (66.12), this implies  $R = \tau(R, M^*)M$ , and Lemma 66.13 is proved.

(66.14) **LEMMA.** *Let  $I = eA$  where  $e^2 = e \in A_{\mathbb{M}}$ . Then  $IM = eM$  is a C-component of  $M$ , and  $\tau(IM, M^*) = I$ .*

**PROOF.** We have  $IM = eAM = eM$  and  $M = eM \oplus (1 - e)M$ , where  $eM$  and  $(1 - e)M$  are C-submodules of  $M$ , thus proving the first statement. For the second, let  $a \in I$ ; then

$$a = ae = \sum \tau(ax_i^0, \psi_i^0) \in \tau(IM, M^*) .$$

This result combined with (66.12) proves the second statement, and Lemma 66.14 is established.

Now we come to the main theorem of this section.

(66.15) **THEOREM.** *Let  $A$  be a symmetric algebra, and let  $M$  be a regular module with respect to the pairing  $\tau$  defined by (66.5). The mappings*

$$I = eA \rightarrow IM = eM$$

and

$$R \rightarrow \tau(R, M^*) ,$$

*between the set of right ideal components  $I$  of  $A_{\mathbb{M}}$  and the C-components  $R$  of  $M$ , are one-to-one and are inverses of each other. Two right ideals  $I_1 = e_1A$  and  $I_2 = e_2A$ , generated by idempotents belonging to  $A_{\mathbb{M}}$ , are  $A$ -isomorphic if and only if the C-modules  $e_1M$  and  $e_2M$  are C-isomorphic.*

**PROOF.** The fact that the mappings are one-to-one and are inverses of each other has already been proved in Lemmas (66.13) and (66.14). It remains to discuss the last statement of the theorem.

Let  $\theta: e_1A \rightarrow e_2A$  be an  $A$ -isomorphism, and let  $\theta(e_1) = a$ ,  $\theta^{-1}(e_2) = b$ . Then

$$\theta(e_1c) = \theta(e_1)c = \theta(e_1)e_1c = ae_1c , \quad c \in A$$

and

$$\theta^{-1}(e_2d) = \theta^{-1}(e_2)d = be_2d , \quad d \in A .$$

Therefore  $e_2A = ae_1A$ ,  $e_1A = be_2A$ . Moreover,  $bac = c$  for all  $c \in e_1A$ , and  $abd = d$  for all  $d \in e_2A$ . Now we define mappings  $\tilde{\theta}$  and  $\tilde{\zeta}$  be-

tween  $e_1M$  and  $e_2M$  by the rules

$$\tilde{\theta}(e_1x) = ae_1x, \quad x \in M$$

and

$$\tilde{\zeta}(e_2y) = be_2y, \quad y \in M.$$

It is clear that  $\tilde{\theta}$  and  $\tilde{\zeta}$  are  $C$ -homomorphisms, and from what has been proved, it follows that these mappings are inverses of each other. Therefore  $e_1M$  and  $e_2M$  are  $C$ -isomorphic.

Conversely, suppose we have a  $C$ -isomorphism  $\eta: x \rightarrow \eta x$  of  $e_1M$  onto  $e_2M$ . Define

$$\bar{\eta}: \sum \tau(x_i, \phi_i) \rightarrow \sum \tau(\eta x_i, \phi_i)$$

for  $x_i \in e_1M, \phi_i \in M^*$ . Then  $\bar{\eta}$  maps  $\tau(e_1M, M^*) = e_1A$  onto  $\tau(e_2M, M^*) = e_2A$ . We prove next that  $\bar{\eta}$  is well defined. Suppose that  $\sum \tau(x_i, \phi_i) = 0, x_i \in e_1M, \phi_i \in M^*$ . Then

$$0 = \sum \tau(x_i, \phi_i)M = \sum x_i(\phi_i \square M),$$

and since  $\eta$  is a  $C$ -isomorphism,

$$(66.16) \quad 0 = \sum \eta x_i(\phi_i \square M) = \sum \tau(\eta x_i, \phi_i)M.$$

Since  $\epsilon = \sum \tau(\phi_i^0, x_i^0)$  is a right identity element in  $A_M$ , we have by (66.16),

$$\begin{aligned} \sum \tau(\eta x_i, \phi_i) &= \sum \tau(\eta x_i, \phi_i)\epsilon \\ &= \sum_j \tau\left(\sum_i \tau(\eta x_i, \phi_i)x_j^0, \phi_j^0\right) = 0, \end{aligned}$$

and we have proved that  $\bar{\eta}$  is well defined. A similar argument shows that

$$\bar{\theta}: \sum \tau(x_i, \phi_i) \rightarrow \sum \tau(\eta^{-1}x_i, \phi_i),$$

for  $x_i \in e_2M, \phi_i \in M^*$ , is a well-defined mapping of  $\tau(e_2M, M^*)$  onto  $\tau(e_1M, M^*)$  such that

$$\bar{\eta}\bar{\theta} = 1, \quad \bar{\theta}\bar{\eta} = 1.$$

Moreover, it is clear that the mappings  $\bar{\theta}$  and  $\bar{\eta}$  are right  $A$ -homomorphisms between the right ideals  $\tau(e_2M, M^*)$  and  $\tau(e_1M, M^*)$ . It follows that  $\tau(e_2M, M^*) \cong \tau(e_1M, M^*)$  as right  $A$ -modules. This completes the proof of Theorem 66.15.

Of particular importance is the following special case of the preceding theorem:

(66.17) THEOREM. Let  $A$  be a symmetric algebra and  $M$  a left  $A$ -module such that  $M$  is regular relative to the pairing  $\tau$ , and suppose that the nucleus  $A_{\infty}$  of  $\tau$  is a semi-simple ring. Let  $C = \text{Hom}_A(M, M)$ . Then

(i)  $I \rightarrow IM$  is a one-to-one mapping of the set of all right ideals of  $A_{\infty}$  onto the set of all  $C$ -submodules of  $M$ . Every  $C$ -submodule has the form  $eM$  where  $e$  is an idempotent in  $A_{\infty}$ . The  $C$ -module  $eM$  is irreducible if and only if  $e$  is a primitive idempotent in  $A_{\infty}$ .

(ii)  $M$  is a completely reducible  $C$ -module.

PROOF. Because  $A_{\infty}$  is semi-simple, it follows easily from the structure theory that  $A_{\infty}$  is a completely reducible right  $A_{\infty}$ -module, and every right ideal of  $A_{\infty}$  is a component of  $A_{\infty}$ . Now let  $e$  be a primitive idempotent in  $A_{\infty}$ ; we shall prove that  $eM$  is an irreducible  $C$ -submodule of  $M$ . In fact, let  $R$  be a non-zero  $C$ -submodule of  $eM$ . Then from Lemma 66.14, we obtain

$$eA = \tau(eM, M^*) \supset \tau(R, M^*) ,$$

and since  $eA = eA_{\infty}$  is a minimal ideal in  $A_{\infty}$  and  $\tau(R, M^*) \neq 0$ , we have

$$eA = \tau(R, M^*) .$$

Then by (66.12),

$$\tau(R, M^*)M = eM \subset R ,$$

and we have proved that  $eM$  is an irreducible  $C$ -module. Because  $A_{\infty}$  is a completely reducible right  $A_{\infty}$ -module, we have  $A_{\infty} = \sum eA_{\infty}$ , where the  $\{eA_{\infty}\}$  are minimal right ideals. It follows that

$$M = \sum eM ,$$

where the  $\{eM\}$  are irreducible  $C$ -modules, and by Theorem 15.3,  $M$  is a completely reducible  $C$ -module, and every  $C$ -submodule of  $M$  is a component of  $M$ . The preceding theorem can now be applied, and shows that the mapping  $I \rightarrow IM$  carries the set of right ideals of  $A_{\infty}$  onto the set of all  $C$ -submodules of  $M$ , and Theorem 66.17 is completely proved.

We remark that all the hypothesis of Theorem 66.17 are automatically satisfied if  $A = KG$  is a semi-simple group algebra.

In applications of this theory, it may be easy to find primitive idempotents in  $A$  but difficult to tell whether they belong to the ideal  $A_{\infty}$ . Because of this problem, the following result is often useful.

(66.18) COROLLARY. *Let  $A$  and  $M$  satisfy the hypotheses of Theorem 66.17. Let  $e$  be any primitive idempotent in  $A$ . Then either  $eM = 0$  or  $eM$  is an irreducible  $C$ -submodule of  $M$ .*

PROOF. Because  $M$  is regular with respect to  $\tau$ , there is an idempotent  $\epsilon \in A_M$  such that  $\epsilon a = a\epsilon = a$  for all  $a \in A_M$ , and  $\epsilon m = m$  for all  $m \in M$ . Now let  $B = \{b \in A : bM = 0\}$ . Then, since  $\epsilon = \sum \tau(x_i, \phi_i)$ ,  $b \in B \cap A_M$  implies  $b = b\epsilon = 0$ . For all  $a \in A$ ,  $a\epsilon - \epsilon a \in B \cap A_M$ , and it follows that  $\epsilon$  is a central idempotent in  $A$ . If  $e$  is any primitive idempotent in  $A$ , then

$$e = e\epsilon + e(1 - \epsilon)$$

where  $e\epsilon$  and  $e(1 - \epsilon)$  are orthogonal. Since  $e$  is a primitive idempotent, either  $e\epsilon = e$  and  $e \in A_M$  so that by Theorem 66.17,  $eM$  is an irreducible  $C$ -module, or  $e(1 - \epsilon) = e$  and  $eM = 0$ . This completes the proof of the Corollary.

### Exercises

1. Prove that any semi-simple algebra  $A$  over an algebraically closed field is a symmetric algebra. [Hint: Use the trace function in each of the simple components of  $A$ .]
2. Let  $M$  be a left  $A$ -module for a symmetric algebra  $A$ , and let  $B$  be the annihilating ideal of  $M$ . Prove that  $M$  is regular if and only if  $A = A_M \oplus B$ . Use this result to find an example of a module for a symmetric algebra  $A$  which is not regular. [Hint: Consider the algebra  $A$  with basis  $\{1, n\}$  where  $n^2 = 0$ .]
3. Let  $A = KG$  be the group algebra of a finite group. Then  $\{g_1, g_2, \dots\}$  and  $\{g_1^{-1}, g_2^{-1}, \dots\}$  are dual bases of  $KG$  with respect to the bilinear form  $f$  which assigns to the pair  $(x, y)$  the coefficient of 1 in the product  $xy$ . Let  $M$  be a left  $KG$ -module and  $M^*$  the  $K$ -dual of  $M$ . For  $\psi \in M^*$ ,  $x \in M$ , let  $\psi \otimes x$  be the linear transformation  $u \rightarrow \psi(u)x$ . Let  $\tau$  be the function defined by (66.5), and  $\psi \square x$  by (66.10). Prove that

$$\psi \square x = \sum_{g \in G} g^{-1}(\psi \otimes x)g.$$

Prove that every element of  $C = \text{Hom}_{K\alpha}(M, M)$  is a sum of transformations  $\psi \square x$  if and only if  $M$  is a projective  $KG$ -module. [Use the results of §62.]

4. (See Fitting [1].) Let  $A$  be a symmetric algebra over  $K$  and  $M$  a left  $A$ -module which is regular with respect to the pairing  $\tau$ . Show that for any primitive idempotent  $e$  in  $A$ , either  $eM = 0$  or  $eM$  is a  $C$ -component of  $M$ . For any  $C$ -component  $R$  of  $M$ , prove that

$$\tau(R, M^*) = \{a \in A : aM \subset R\}.$$

### § 67. Irreducible Tensor Representations of $GL(V)$

In this section we shall formulate and solve a problem in which representations of a certain infinite group are determined explicitly in terms of known representations of a finite group (in this case the symmetric group), the connecting link in this case being the results of § 66.

Let  $V$  be a vector space over a field  $K$  of characteristic zero, and let  $\{e_1, \dots, e_n\}$  be a basis of  $V$  over  $K$ . Let  $G = GL(V)$  be the group of all invertible linear transformations on  $V$ . For a fixed  $m$ , let  $V^{(m)}$  be the  $m$ -fold tensor product of  $V$  with itself over  $K$ ; then  $V^{(m)}$  consists of all tensors

$$u = \sum_i v_1^i \otimes \cdots \otimes v_m^i$$

where the  $v_j^i \in V$ . The space  $V^{(m)}$  has a basis consisting of the  $n^m$  tensors  $e_{i_1} \otimes \cdots \otimes e_{i_m}$ ,  $1 \leq i_j \leq n$ .

The group  $G$  acts on  $V^{(m)}$  in a natural way. If  $F \in G$ , we let  $F^{(m)}$  denote the linear transformation

$$(67.1) \quad u \rightarrow F^{(m)}u = (\underbrace{F \otimes \cdots \otimes F}_m)u = \sum_i Fv_1^i \otimes \cdots \otimes Fv_m^i.$$

Then the mapping  $F \rightarrow F^{(m)}$  defines a representation of  $G$  in the tensor space  $V^{(m)}$ . We shall determine the irreducible  $G$ -submodules of the tensor space  $V^{(m)}$ .

We attack the problem indirectly. We first consider the symmetric group  $S_m$  on  $m$  symbols, and let  $A = KS_m$  be the group algebra of  $S_m$ . For each  $s \in S_m$  we wish to define the action of  $s$  on the tensor space  $V^{(m)}$ . Consider a tensor

$$v_1 \otimes \cdots \otimes v_m \in V^{(m)}.$$

Then we define

$$(67.2) \quad s(v_1 \otimes \cdots \otimes v_m) = v_{s^{-1}(1)} \otimes \cdots \otimes v_{s^{-1}(m)};$$

in other words, the result of applying  $s$  to the tensor  $v_1 \otimes \cdots \otimes v_m$  is to move the  $i^{\text{th}}$  factor  $v_i$  into the  $s(i)^{\text{th}}$  place since the  $s(i)^{\text{th}}$  factor on the right side is  $v_{s^{-1}(s(i))}$ . It is important to note that the action of  $s$  on a particular tensor does not change the vectors of  $V$  which appear as "factors" in the tensor, but only the positions of the factors. Now let  $t \in S_m$  also. We have

$$(st)(v_1 \otimes \cdots \otimes v_m) = v_{(st)^{-1}(1)} \otimes \cdots \otimes v_{(st)^{-1}(m)},$$

whereas from the definition we have

$$\begin{aligned}s(t(v_1 \otimes \cdots \otimes v_m)) &= s(v_{t^{-1}(1)} \otimes \cdots \otimes v_{t^{-1}(m)}) \\ &= v_{t^{-1}(s^{-1}(1))} \otimes \cdots \otimes v_{t^{-1}(s^{-1}(m))}.\end{aligned}$$

It follows that (67.2) defines a representation of  $S_m$  on the tensor space  $V^{(m)}$ , and therefore  $V^{(m)}$  becomes a left  $KS_m$ -module. An element  $a \in KS_m$ ,  $a = \sum_{s \in S_m} \alpha_s s$ , viewed as a linear transformation on the tensor space  $V^{(m)}$ , is called a *symmetry operator* on  $V^{(m)}$ .

Our first observation is that the transformations  $F^{(m)}$  all commute with the symmetry operators. For this it is sufficient to show that for  $s \in S_m$ ,  $v_i \in V$ , we have

$$F^{(m)}(s(v_1 \otimes \cdots \otimes v_m)) = s(F^{(m)}(v_1 \otimes \cdots \otimes v_m)),$$

and this is obvious from (67.1) and (67.2).

Because  $K$  has characteristic zero,  $KS_m$  is a semi-simple symmetric algebra, and  $V^{(m)}$  is a regular module with respect to the function  $\tau$  defined in §66. Moreover, the nucleus of the module  $V^{(m)}$  is also semi-simple, so that Theorem 66.17 can be applied to determine the irreducible  $C$ -submodules of  $V^{(m)}$  where

$$C = \text{Hom}_{KS_m}(V^{(m)}, V^{(m)}).$$

These modules all have the form

$$eV^{(m)}$$

where  $e$  is a primitive idempotent in  $KS_m$ , and for any primitive idempotent  $e$  in  $KS_m$ , either  $eV^{(m)} = 0$  or  $eV^{(m)}$  is an irreducible  $C$ -submodule of  $V^{(m)}$ . The primitive idempotents in  $KS_m$  have all been determined in §28. We have already shown that the transformations  $F^{(m)}$ ,  $F \in GL(V)$ , belong to  $C$ . We shall prove the following basic lemma:

(67.3) LEMMA. *Let  $C = \text{Hom}_{KS_m}(V^{(m)}, V^{(m)})$ . Then  $C$  is the enveloping algebra of the set of transformations  $F^{(m)}$ ,  $F \in G$ . Therefore the  $C$ -submodules of  $V^{(m)}$  are identical with the  $G$ -submodules of  $V^{(m)}$ .*

PROOF. It is sufficient to prove that any linear function on  $C$  which vanishes on all the  $F^{(m)}$ ,  $F \in G$ , vanishes on all of  $C$ . Let  $\gamma \in C$ ; then  $\gamma$  is described by its coefficients  $\gamma(j_1, \dots, j_m, i_1, \dots, i_m)$  with respect to a basis, where

$$\gamma(e_{i_1} \otimes \cdots \otimes e_{i_m}) = \sum_{(j_1, \dots, j_m)} \gamma(j_1, \dots, j_m, i_1, \dots, i_m) e_{j_1} \otimes \cdots \otimes e_{j_m}.$$

The statement  $\gamma \in C$  is equivalent to the conditions

$$(67.4) \quad \gamma(j_1, \dots, j_m; i_{s-1(1)}, \dots, i_{s-1(m)}) = \gamma(j_{s(1)}, \dots, j_{s(m)}, i_1, \dots, i_m),$$

for  $1 \leq i_k, j_k \leq n, s \in S_m$ . A linear function on  $C$  assigns to each  $\gamma \in C$  an element of  $K$  given by

$$(67.5) \quad \sum_{(j_1, \dots, j_m; i_1, \dots, i_m)} \alpha(j_1, \dots, j_m; i_1, \dots, i_m) \gamma(j_1, \dots, j_m; i_1, \dots, i_m),$$

where the  $\alpha$ 's are fixed elements of  $K$  subject to the symmetry conditions (67.4). We are given that the linear function vanishes for all  $F^{(m)}$ . The coordinate functions of  $F^{(m)}$  are given by

$$F^{(m)}(e_{i_1} \otimes \dots \otimes e_{i_m}) = \sum \xi_{j_1, i_1} \dots \xi_{j_m, i_m} e_{j_1} \otimes \dots \otimes e_{j_m},$$

where

$$Fe_i = \sum \xi_{j_i} e_j$$

on  $V$ . Therefore we have

$$(67.6) \quad \sum \alpha(j_1, \dots, j_m; i_1, \dots, i_m) \xi_{j_1, i_1} \dots \xi_{j_m, i_m} = 0.$$

Let us rename the  $\{\xi_{ij}\}$  calling them  $\lambda_1, \dots, \lambda_{n^2}$ . Then (67.6) can be rewritten as a polynomial

$$(67.7) \quad P(\lambda_1, \dots, \lambda_{n^2}) = \sum \beta(k_1, \dots, k_{n^2}) \lambda_1^{k_1} \dots \lambda_{n^2}^{k_{n^2}} = 0$$

where  $k_1 + \dots + k_{n^2} = m$ , and, by (67.6),  $\beta(k_1, \dots, k_{n^2})$  is  $m!/(k_1! \dots k_{n^2}!)$  times any one of the coefficients  $\alpha(j_1, \dots, j_m, i_1, \dots, i_m)$  of  $\xi_{j_1, i_1} \dots \xi_{j_m, i_m}$  in which  $k_1$  of the  $\xi_{ji}$  are equal to  $\lambda_1$ ,  $k_2$  of them are equal to  $\lambda_2$ , etc. The relation (67.7) holds for all  $\lambda$ 's in  $K$  for which a second polynomial relation

$$Q(\lambda_1, \dots, \lambda_{n^2}) \neq 0,$$

namely, the relation which expresses the fact that the determinant of  $F$  is different from zero. It follows that in the polynomial ring  $K[X_1, \dots, X_{n^2}]$  we have

$$P(X_1, \dots, X_{n^2}) Q(X_1, \dots, X_{n^2}) = 0.$$

Since  $Q(X_1, \dots, X_{n^2}) \neq 0$ , we have

$$P(X_1, \dots, X_{n^2}) = 0.$$

Therefore all the coefficients  $\beta(k_1, \dots, k_{n^2}) = 0$ , and we have shown that all the original coefficients  $\alpha(j_1, \dots, j_m, i_1, \dots, i_m) = 0$ . This completes the proof of Lemma 67.3.

On the strength of Lemma 67.3 and Theorem 66.17, we can state the following result:

(67.8) THEOREM. Let  $G = GL(V)$  be the general linear group on a vector space  $V$  over a field of characteristic zero, and let  $V^{(m)}$  be the space of  $m$ -fold tensors over  $V$ . Then  $V^{(m)}$  is a completely reducible  $G$ -module, and the irreducible  $G$ -submodules are obtained as follows. Let  $e$  be a primitive idempotent in the group algebra  $KS_m$ ; then  $eV^{(m)}$  is either zero or an irreducible  $G$ -submodule of  $V^{(m)}$ . All irreducible  $G$ -submodules of  $V^{(m)}$  are obtained in this way. Moreover, two irreducible  $G$ -modules  $eV^{(m)}$  and  $e'V^{(m)}$  are  $G$ -isomorphic if and only if  $eKS_m$  and  $e'KS_m$  are isomorphic right  $KS_m$ -modules.

### Exercises

Let  $G$ ,  $V^{(m)}$ , etc., satisfy the hypotheses of Theorem 67.8.

1. Let

$$e = \frac{1}{m!} \left( \sum_{s \in S_m} s \right).$$

Then  $e$  is a primitive idempotent in  $KS_m$ , and, for all  $m$ ,  $eV^{(m)}$  is an irreducible  $G$ -module called the *space of symmetric tensors*. Prove that a tensor  $u \in V^{(m)}$  is a symmetric tensor if and only if  $su = u$  for all  $s \in S_m$ . Prove that the space of symmetric tensors is  $G$ -isomorphic to the space of homogeneous polynomials in  $n = (V: K)$  variables of degree  $m$ , viewed as a  $G$ -module in the obvious way.

2. Let  $\varepsilon_s$  be  $\pm 1$  according as  $s$  is even or odd, and let

$$f = \frac{1}{m!} \sum_{s \in S_m} \varepsilon_s s.$$

Then  $fV^{(m)}$  is an irreducible  $G$ -submodule of  $V^{(m)}$  for  $1 \leq m \leq (V: K)$ , called the *space of skew symmetric tensors*. Prove that for  $1 \leq m \leq (V: K)$ ,

$$(fV^{(m)}: K) = \binom{n}{m},$$

and that, for  $m > n$ ,  $fV^{(m)} = 0$ .

3. Prove that, if  $m \leq (V: K)$ ,  $V^{(m)}$  is a faithful  $KS_m$ -module.

## Splitting Fields and Separable Algebras

This chapter begins with two introductory sections, one on splitting fields for simple algebras, and one on the behavior of a semi-simple algebra upon extension of the base field. These results are applied in § 70 to study the concept of the Schur index in the theory of group representations and in particular to establish the result already used in § 41 to prove Brauer's theorem that the absolutely irreducible representations of a finite group  $G$  are all realizable in the field of  $n$ th roots of unity, where  $n$  is the exponent of  $G$ . The work of § 69 leads also to the concept of a separable algebra, and in § 71 we derive a useful characterization of separable algebras due to D. G. Higman which will be needed in Chapter XI. The chapter concludes with a proof (along the lines of the Gaschütz-Ikeda-Higman theory of Chapter IX) of the Wedderburn Principal Theorem for algebras  $A$  such that  $A/\text{rad } A$  is separable.

For §§ 68–70, we assume familiarity only with Chapter IV and especially § 29, where the concept of splitting field was introduced. In § 69 and 71, some knowledge of the first few sections of Chapter IX is needed.

### § 68. Splitting Fields for Simple Algebras and Division Algebras

The subject of this section is an extensive one, but we shall restrict ourselves to those results which are needed in this book. For more comprehensive discussions the reader may consult Jacobson [1], Artin, Nesbitt, Thrall [1], and Bourbaki [2].

Let  $A$  be a simple algebra over a field  $F$  such that  $(A : F)$  is finite, and let  $K$  be the center of  $A$ . By Wedderburn's theorem,  $A \cong D_r$ , where  $D$  is a division algebra over  $F$ . It follows easily that the center of  $A$  is isomorphic to the center of  $D$ , and is a finite extension field of  $F$ . Both  $D$  and  $A$  may be viewed as algebras over  $K$ , and the next result shows why it is convenient to study  $A$  as an algebra over its center.

(68.1) THEOREM. *Let  $A$  be a simple algebra with center  $K$ , and let*

*E* be an extension field of *K*. Then  $A^E$  (i.e.,  $A \otimes_K E$ ) is a simple algebra with center *E*.

PROOF. Let  $B \neq 0$  be a two-sided ideal in  $A^E$ . We need prove only that  $B$  contains an element  $a \otimes e \neq 0$  for some  $a \in A$  and  $e \in E$ . For then  $B$  contains  $a \otimes eE = a \otimes E$  and hence contains  $AaA \otimes E = A(a \otimes E)A$ . But  $AaA = A$  because  $A$  is simple; hence  $B$  contains  $A \otimes E$ , and thus  $A^E$  is simple. Now suppose that  $B$  does not contain any non-zero elements of the form  $a \otimes e$ . Among all elements

$$b = \sum_{i=1}^s a_i \otimes e_i \in B, \quad a_i \in A, e_i \in E,$$

with the  $\{e_i\}$  linearly independent over *K*, choose a non-zero element  $b$  for which  $s$  is as small as possible. Then  $s > 1$ , and  $a_1 \neq 0$ . Keeping  $e_1, \dots, e_s$  fixed, consider the set  $A_1$  of all elements  $a'_1 \in A$  such that

$$(68.2) \quad a'_1 \otimes e_1 + \sum_2^s a'_i \otimes e_i \in B,$$

for some elements  $\{a'_i\} \in A$ . Since  $B$  contains the sum of any two elements of the form (68.2) as well as

$$a(a'_1 \otimes e_1) + a\left(\sum_2^s a'_i \otimes e_i\right) = aa'_1 \otimes e_1 + \sum_2^s aa'_i \otimes e_i$$

and

$$(a'_1 \otimes e_1)a + \left(\sum_2^s a'_i \otimes e_i\right)a = a'_1 a \otimes e_1 + \sum_2^s a'_i a \otimes e_i$$

for all  $a \in A$ , it follows that  $A_1$  is an ideal in  $A$  different from zero. The fact that  $A$  is a simple algebra implies that  $A_1 = A$ ; hence

$$(68.3) \quad b^* = 1 \otimes e_1 + \sum_2^s a'_i \otimes e_i \in B$$

for some  $\{a'_i\}$  in  $A$ . Then, for all  $a \in A$ ,

$$b^*a - ab^* \in B,$$

and it follows that

$$\sum_{i=2}^s (a'_i a - aa'_i) \otimes e_i \in B.$$

Because of the way  $s$  was chosen, this element is zero, and since the  $\{e_i\}$  are linearly independent over  $K$ , we have

$$a'_i a = a a'_i, \quad i = 2, \dots, s, \quad a \in A.$$

Therefore the  $\{a'_i\}$  all belong to the center  $K$  of  $A$ , and since we are taking tensor products with respect to  $K$ , (68.3) becomes

$$1 \otimes (e_1 + \sum a'_i e_i) \in B.$$

This contradicts the way  $s$  was chosen, and the proof of the first statement is completed. A similar argument shows that the center of  $A^E$  is  $E$ , and the theorem is proved.

From Definition 29.12, we recall that if  $A$  is an algebra over  $K$ , an extension field  $E$  of  $K$  is a *splitting field* for  $A$  if every irreducible  $A^E$ -module is absolutely irreducible where  $A^E = A \otimes_K E$ . The next result gives a more useful characterization of splitting fields of simple algebras.

(68.4) THEOREM. *Let  $A$  be a simple algebra with center  $K$ . An extension field  $E$  of  $K$  is a splitting field for  $A$  if and only if  $A^E \cong E_t$  for some positive integer  $t$ .*

PROOF. By the preceding theorem, we know that  $A^E$  is a simple algebra over  $E$ , and hence by Wedderburn's theorem 26.4, we have  $A^E \cong D_t$  for some division algebra  $D$  over  $E$ . If  $V$  is an irreducible  $A^E$ -module, it follows from § 26 that

$$\text{Hom}_{A^E}(V, V) \cong D.$$

Thus  $E$  is a splitting field for  $A$  if and only if  $D \cong E$ , by (29.13).

(68.5) COROLLARY. *Let  $A$  be a simple algebra over its center  $K$  such that  $A \cong D_t$ , where  $D$  is a division algebra over  $K$ . Then an extension field  $L$  of  $K$  is a splitting field for  $A$  if and only if  $L$  is a splitting field for  $D$ .*

PROOF. First, let  $D \otimes_K L \cong L_r$ ; then

$$\begin{aligned} D_t \otimes_K L &\cong (K_t \otimes_K D) \otimes_K L \\ &\cong K_t \otimes_K (D \otimes_K L) \cong K_t \otimes_K L_r \\ &\cong L_{tr}, \end{aligned}$$

by the results in § 12 (see Exercises 12.6 and 12.7 in particular.) It follows from Theorem 68.4 that  $L$  is a splitting field for  $A$ . Conversely, suppose  $L$  is a splitting field for  $D_t$ . Then by Theorem 68.4,

$$D_t \otimes_K L \cong L_{tr}$$

for some  $u$ . On the other hand, Theorem 68.1 implies that  $D \otimes_K L$  is a simple algebra; hence there is a division algebra  $E$  over  $L$  such that

$$D \otimes_K L \cong E_v,$$

for some  $v$ . Then

$$D_t \otimes_K L \cong K_t \otimes_K (D \otimes_K L) \cong K_t \otimes_K E_v \cong E_{tv}.$$

By the uniqueness part of the Wedderburn theorem [Theorem 26.4], we have  $E \cong L$ ; hence  $D \otimes_K L \cong L_v$ , and  $L$  is a splitting field for  $D$ .

Because of Corollary 68.5, the study of splitting fields for a simple algebra  $A$  with center  $K$  is reduced to the construction of splitting fields of the division algebra part of  $A$ . With this in mind, we can settle the problem of existence of splitting fields of simple algebras by means of the following basic theorem.

(68.6) THEOREM. *Let  $D$  be a division algebra with center  $K$  such that  $(D : K)$  is finite, and let  $E$  be any maximal subfield of  $D$ . Then  $E$  is a splitting field for  $D$ . Moreover*

$$(D : K) = (E : K)^2.$$

PROOF. Clearly  $E \supset K$ ; otherwise  $EK$  is a subfield of  $D$  properly containing  $E$ . We may view  $D$  as a right  $E$ -module and as a left  $D$ -module. Thus  $D$  is a  $(D, E)$ -bimodule since

$$(\delta d)e = \delta(de), \quad \delta, d \in D, e \in E.$$

Let  $\delta_L$  denote the left multiplication by  $\delta \in D$ , and  $e_R$  the right multiplication by  $e \in E$ . Then we have

$$\delta_L e_R = e_R \delta_L, \quad e \in E, \delta \in D.$$

Let  $S = D_L \cdot E_R = \{\sum \delta_L^{(i)} e_R^{(i)} : \delta^{(i)} \in D, e^{(i)} \in E\}$ . Then  $S$  is a subring of  $\text{Hom}_E(D, D)$  where  $D$  is viewed as a right  $E$ -space. We remark also that the right dimension  $(D : E)$  is finite.

Now form  $\text{Hom}_S(D, D)$ . For any  $\phi \in \text{Hom}_S(D, D)$ , we have  $\delta_L \phi = \phi \delta_L$ ,  $\delta \in D$ . Therefore  $\phi = x_R$  for some  $x \in D$ , and the mapping

$$\phi \rightarrow x_R$$

is an isomorphism of  $\text{Hom}_S(D, D)$  onto a division subalgebra  $\Gamma_R$  of  $D_R$  such that  $\Gamma_R \supset E_R$ . Moreover  $E_R$  is contained in the center of  $\Gamma_R$  since  $S \supset E_R$ . If  $\gamma_R \in \Gamma_R$ , then  $E_R[\gamma_R]$  is a subfield of  $D_R$  containing  $E_R$ , and, since  $E_R$  is a maximal subfield of  $D_R$ , we have  $\Gamma_R = E_R$ . We have now shown that  $\text{Hom}_S(D, D) = E_R$ . We observe also that, because  $D$  is a division algebra, the only  $S$ -submodules of

$D$  are (0) and  $D$ , since  $S \supset D_L$ . By the results in §§ 26 and 27, we have

$$S = D_L E_R = \text{Hom}_{S_R}(D, D) \cong E_d$$

where  $d$  is the right dimension of  $D$  over  $E$ .

On the other hand,

$$\sum \delta^{(i)} \otimes e^{(i)} \rightarrow \sum \delta_L^{(i)} e_R^{(i)}$$

is a homomorphism of  $D \otimes_K E$  onto  $D_L E_R$ . Since  $D \otimes_K E$  is a simple algebra by Theorem 68.1, we have

$$D \otimes_K E \cong D_L E_R \cong E_d,$$

which proves that  $E$  is a splitting field for  $D$ . Comparing dimensions, we have

$$(D : K)(E : K) = d^2(E : K);$$

consequently,

$$(D : K) = d^2$$

where  $d = (D : E)$ . We have also  $d^2 = (D : E)(E : K)$ , and it follows that  $d = (E : K)$ . This completes the proof of the theorem.

We emphasize that the previous theorem asserts that  $\sqrt{(D : K)}$  is the dimension of any maximal subfield of  $D$ . The next theorem shows that the maximal subfields are the splitting fields of least dimension over  $K$ .

(68.7) THEOREM. *Let  $D$  be a division algebra with center  $K$ , and let  $E$  be any finite algebraic extension of  $K$  which is a splitting field for  $D$  (note that  $E$  is not assumed to be a subfield of  $D$ ). Then*

$$\sqrt{(D : K)} | (E : K).$$

PROOF. By Theorem 68.4 we have

$$(68.8) \quad D \otimes_K E \cong E_r$$

for some positive integer  $r$ . Any minimal left ideal of  $D \otimes_K E$  is a left  $D$ -module, and is consequently a direct sum of a certain number  $h$  of copies of  $D$ . Since  $D \otimes_K E$  is a direct sum of  $r$  minimal left ideals, we see that  $D \otimes_K E$  is a direct sum of  $rh$  copies of  $D$ . On the other hand,  $D \otimes_K E$  is a free left  $D$ -module with a basis of  $(E : K)$ -elements. Therefore  $(E : K) = rh$ .

Taking dimensions over  $K$  in (68.8), we have also  $(D : K) = r^2$ . Combining these results we have

$$\sqrt{(D : K)} | (E : K),$$

and the theorem is proved.

The number  $d = \sqrt{(D : K)}$  will be called the *index* of  $D$ .

We conclude this section with a proof due to Witt [1] of Wedderburn's theorem that every finite skewfield is a field.

(68.9) THEOREM. *Every finite skewfield  $D$  satisfies the commutative law for multiplication.*

PROOF. Let  $K$  be the center of  $D$ . The skewfield  $D$  is a finite dimensional vector space over the finite field  $K$ . Now  $K$  contains  $q$  elements, where  $q$  is a prime power, and therefore  $D$  contains  $q^n$  elements where  $n = (D : K)$ . We are trying to prove that  $n = 1$ . Suppose instead that  $n > 1$ ; we shall derive a contradiction.

Let  $K^*$  and  $D^*$  denote the multiplicative groups of  $K$  and  $D$ , respectively. Then  $K^*$  is the center of  $D^*$ , and we have  $[D^* : 1] = q^n - 1$  and  $[K^* : 1] = q - 1$ . The class equation for  $D^*$  [see (3.4)] has the form

$$q^n - 1 = q - 1 + \sum_{C(x) \neq D^*} [D^* : C(x)], \dagger$$

the sum being taken over some elements  $\{x\}$  in  $D^*$ . Let  $x \in D^*$  be such that  $C(x) \neq D^*$ ; then  $C(x)$  is the multiplicative group  $C^*$  of a subskewfield  $C$  of  $D$ , and clearly  $C \supset K$ . Therefore

$$[D^* : C(x)] = [D^* : C^*] = \frac{q^n - 1}{c - 1}$$

where  $q^n$  is the number of elements in  $D$  and  $c$  the number of elements in  $C$ . If  $d = (C : K)$ ,  $C$  contains  $q^d$  elements; furthermore  $(D : K) = (D : C)d$ , and  $d < n$  since  $C(x) \neq D^*$ . The class equation then becomes

$$(68.10) \quad q^n - 1 = q - 1 + \sum_d \frac{q^n - 1}{q^d - 1}$$

where the sum is taken over certain proper divisors  $d$  of  $n$ , and possibly there is more than one summand for a given  $d$ . We may write

$$q^n - 1 = \prod_{m|n} \Phi_m(q), \quad q^d - 1 = \prod_{m|d} \Phi_m(q)$$

where  $\Phi_m(X)$  is the cyclotomic polynomial of order  $m$ . From (68.10), it follows at once that  $\Phi_n(q) | (q - 1)$ . But

---

$\dagger$   $C(x)$  is the centralizer of  $x \in D^*$ .

$$(68.11) \quad \Phi_n(q) = \prod_i (q - \zeta_i)$$

where the  $\{\zeta_i\}$  are the  $\phi(n)$  primitive  $n$ th roots of 1. We now show that

$$|\Phi_n(q)| > q - 1.$$

The result is obvious for  $n = 2$  since  $\Phi_2(q) = q + 1$ . When  $n > 2$ , there are at least two factors in (68.11), and we have for each factor

$$|q - \zeta_i| > q - 1$$

(since no  $\zeta_i = 1$ ), whence

$$|\Phi_n(q)| > (q - 1)^{\phi(n)} \geq q - 1.$$

This contradicts our earlier result that  $|\Phi_n(q)| \leq q - 1$ , and the theorem is proved.

### § 69. Separable Extensions of the Base Field

In this section we prove that, if  $A$  is a semi-simple algebra over a field  $K$  and if  $E$  is a finite separable extension field of  $K$ , then  $A^E = A \otimes_K E$  is a semi-simple algebra. (See §29, especially Exercise 29.1). This section also contains an application to representation theory and will serve as motivation for the more elaborate theory of separable algebras to be presented in §71.

Our methods in this section are based on the theory of Frobenius algebras. Although we could make our presentation independent of Chapter IX, the reader will have a better appreciation of our procedure if he has some familiarity with the results of Gaschütz and Ikeda discussed in Chapter IX. Some results from the theory of finite separable field extensions such as are given in Zariski-Samuel [1] are also assumed.

Throughout this section,  $E$  denotes a finite extension field of  $K$ . Let  $\{e_1, \dots, e_r\}$  be a basis of  $E$  over  $K$ . For any  $x \in E$ , we have a system of equations

$$(69.1) \quad xe_i = \sum_{j=1}^r \alpha_{ij}(x)e_j, \quad \alpha_{ij}(x) \in K.$$

We set (see § 20B of Chapter III)

$$(69.2) \quad T_{E/K}(x) = \text{tr } (\alpha_{ij}(x)) = \sum_{i=1}^r \alpha_{ii}(x).$$

Then  $T_{E/K}(x)$  is a  $K$ -linear function on  $E$  to  $K$  and is independent

of the choice of the basis  $\{e_1, \dots, e_r\}$  of  $E$  over  $K$ . The only result from field theory which we assume is the following characterization of separable extensions.

(69.3) *A finite extension field  $E$  of  $K$  is separable if and only if there exists an element  $x \in E$  such that  $T_{E/K}(x) \neq 0$ .*

For a proof, we refer the reader to Zariski and Samuel [1], Corollary to Theorem 22, p. 95. In particular, (69.3) implies that  $E$  is always separable over  $K$  if  $\text{char } K = 0$ , since  $T_{E/K}(1) = (E : K) \neq 0$  in this case.

Our main result is the following theorem:

(69.4) **THEOREM.** *Let  $E$  be a finite separable extension field of  $K$ , and let  $A$  be a semi-simple algebra over  $K$ . Then  $A^E$  is a semi-simple algebra over  $E$ .*

**PROOF.** First, we define a bilinear form  $f$  on  $E$  by setting

$$(69.5) \quad f(x, y) = T_{E/K}(xy)$$

and will prove that  $f$  is non-degenerate. If  $f(x, E) = 0$  for  $x \neq 0$ , then since  $xE = E$ , we have  $T_{E/K}(xE) = T_{E/K}(E) = 0$ , contrary to (69.3). Since  $f$  is obviously symmetric, we see also that  $f(E, y) = 0$  implies  $y = 0$ , and therefore  $f$  is non-degenerate. It is also clear from the definition that for all  $x, y, z$  in  $E$ , we have

$$f(xy, z) = f(x, yz).$$

Thus  $f$  is a non-degenerate associative bilinear form on  $E$ , and therefore  $E$  is a Frobenius algebra over  $K$ . Now let  $\{e_1, \dots, e_r\}$  and  $\{e'_1, \dots, e'_r\}$  be dual bases of  $E$  over  $K$ , that is,  $f(e_i, e'_j) = \delta_{ij}$  for  $1 \leq i, j \leq r$ . We shall exploit the special nature of the form  $f$  to prove that

$$(69.6) \quad \sum_{i=1}^r e_i e'_i \neq 0.$$

Suppose that (69.6) is false; then  $\sum e_i e'_i = 0$ ; and for each  $j$ ,  $1 \leq j \leq r$ , we have, using (69.1),

$$\sum_{i=1}^r e_j e_i e'_i = \sum_{i=1}^r \sum_{k=1}^r \alpha_{ik}(e_j) e_k e'_i = 0.$$

Taking traces, we obtain

$$\sum_{i,k=1}^r \alpha_{ik}(e_j) T_{E/K}(e_k e'_i) = \sum_{i,k=1}^r \alpha_{ik}(e_j) \delta_{ki} = 0;$$

hence

$$\sum_{i=1}^r \alpha_{ii}(e_j) = T_{E/K}(e_j) = 0, \quad 1 \leq j \leq r.$$

It follows that  $T_{E/K}(x) = 0$  for all  $x \in E$ , contrary to (69.3). Therefore (69.6) is valid. If we set  $x = (\sum e_i e'_i)^{-1}$ , we have

$$(69.7) \quad \sum_{i=1}^r e_i x e'_i = 1.$$

With these preliminary steps out of the way, we are now ready to complete the proof of Theorem 69.4. It is sufficient to prove that, if  $M$  is any finite-dimensional left  $A^E$ -module, then  $M$  is completely reducible [see Theorem 25.8]. Let  $N$  be a non-zero  $A^E$ -submodule of  $M$ . Since  $A^E$  contains the semi-simple subalgebra  $A$ , it follows that  $N$  is an  $A$ -component of  $M$ . Therefore there exists a projection  $\pi \in \text{Hom}_A(M, M)$  such that  $\pi(M) \subset N$  and  $\pi|N = 1$ . As in the proofs of the theorems of Gaschütz and Ikeda (see Chapter IX), we define  $\pi' \in \text{Hom}_K(M, M)$  by setting

$$\pi'(m) = \sum_{i=1}^r e_i \pi x e'_i m, \quad m \in M,$$

where  $x \in E$  is defined by (69.7). By Lemma 62.8 we have  $\pi' \in \text{Hom}_E(M, M)$ . Since we have also  $ae = ea$  for all  $a \in A$ ,  $e \in E$ , it follows from the definition of  $\pi'$  that  $\pi' \in \text{Hom}_A(M, M)$  and hence that  $\pi' \in \text{Hom}_{A^E}(M, M)$ . We have obviously  $\pi'(M) \subset N$ , and for  $n \in N$  we have

$$\pi'(n) = \sum_{i=1}^r e_i \pi x e'_i n = \sum_{i=1}^r e_i x e'_i n = n$$

because of (69.7) and the fact that  $\pi|N = 1$ . We have proved that  $\pi'$  is an  $A^E$ -projection of  $M$  upon  $N$ , and hence that  $N$  is an  $A^E$ -component of  $M$ . Thus  $M$  is completely reducible, and the theorem is proved.

(69.8) COROLLARY. *Let  $A$  be an arbitrary finite-dimensional algebra over  $K$ , and let  $M$  be a completely reducible left  $A$ -module. Then, for any finite separable extension field  $E$  of  $K$ ,  $M^E$  is a completely reducible left  $A^E$ -module.*

PROOF. Let  $A_L$  denote the algebra of all linear transformations  $a_L : m \rightarrow am$  of  $M$  determined by the elements of  $A$ . Since  $M$  is completely reducible,  $A_L$  has a faithful completely reducible module, and it follows from the results of Chapter IV that  $A_L$  is semi-simple. Then, by Theorem 69.4,  $A_L^E$  is a semi-simple algebra, and

hence  $M^E$  is a completely reducible  $A_L^E$ -module. This means that  $M^E$  is a completely reducible  $A^E$ -module, and the corollary is proved.

As a special case of Corollary 69.8, we may state

(69.9) COROLLARY. *Let  $G$  be a finite group,  $K$  an arbitrary field, and  $M$  a completely reducible  $KG$ -module. Let  $E$  be a finite separable extension field of  $K$ . Then  $M^E$  is a completely reducible  $EG$ -module.*

Still another useful result is

(69.10) COROLLARY. *Let  $A$  be an arbitrary finite-dimensional algebra over  $K$ , and let  $E$  be a finite separable extension field of  $K$ . Then  $\text{rad } A^E = (\text{rad } A)^E$ .*

PROOF. The inclusion  $(\text{rad } A)^E \subset \text{rad } A^E$  is clear, since  $(\text{rad } A)^E$  is a nilpotent ideal. On the other hand,  $M = A/\text{rad } A$  is a completely reducible left  $A$ -module. By Corollary 69.8,  $M^E = A^E/(\text{rad } A)^E$  is a completely reducible left  $A^E$ -module. Therefore

$$(\text{rad } A^E)M^E = 0,$$

and it follows that  $\text{rad } A^E \subset (\text{rad } A)^E$ . This completes the proof.

We conclude this section with the following result on the existence of splitting fields, which is a generalization of Theorem 29.16:

(69.11) THEOREM. *Let  $G$  be a finite group and  $K$  a perfect field. Then there exists a splitting field  $E \supset K$  for  $G$  such that  $(E:K)$  is finite.*

PROOF. [Cf. (29.20).] Let  $A$  denote the semi-simple algebra  $KG/\text{rad } KG$ . The hypothesis implies that every finite extension field  $E$  of  $K$  is separable over  $K$ , and hence by Corollary 69.10 that

$$A^E \cong EG/(\text{rad } KG)^E \cong EG/\text{rad } EG.$$

Therefore the irreducible  $EG$ -modules are the same as the irreducible  $A^E$ -modules, and it follows that  $E$  is a splitting field for  $G$  if and only if  $E$  is a splitting field for  $A$ .

Now let  $K^*$  be the algebraic closure of  $K$ . We prove first that  $A^{K^*}$  is semi-simple. Suppose to the contrary that  $a^* \neq 0$  belongs to a nilpotent two sided ideal in  $A^{K^*}$ . If  $\{a_1, \dots, a_r\}$  is a basis of  $A$  over  $K$ , we have

$$a^* = \xi_1^* a_1 + \dots + \xi_r^* a_r, \quad \xi_i^* \in K^*.$$

Then  $a^* \in A^E$  where  $E = K(\xi_1^*, \dots, \xi_r^*)$  is a finite separable extension

field of  $K$ , and thus  $A^{\otimes}$  is not semi-simple. This contradicts Theorem 69.4, and we have proved that  $A^{K^*}$  is semi-simple. By (29.20) [which is essentially the argument of Theorem 29.16], we can find a finite extension field  $E$  of  $K$  with  $K \subset E \subset K^*$  such that  $E$  is a splitting field for  $A$ . From our discussion in the first part of the proof,  $E$  is also a splitting field for  $G$ , and the theorem is proved.

### Exercises

1. Let  $D$  be a finite-dimensional division algebra over a field  $K$ , and let  $C$  be the center of  $D$ . Then  $D \supset C \supset K$ . Prove that if  $C$  is separable over  $K$ , then  $D^{\otimes} = D \otimes_K E$  is semi-simple for all extension fields  $E$  of  $K$ . [Hint: Write

$$D \otimes_K E = D \otimes_C (C \otimes_K E).$$

We have

$$C \otimes_K E = K(\alpha) \otimes_K E \cong E(\alpha) \cong E[X]/(f(X))$$

for some element  $\alpha \in C$ , where  $f(X) = \text{Irr}(\alpha, K)$ . Let

$$f(X) = \prod_{i=1}^r f_i(X)$$

in  $E[X]$ , where the  $\{f_i(X)\}$  are distinct irreducible factors. It follows that

$$C \otimes_K E \cong F_1 + \cdots + F_r$$

where each  $F_i \cong E[X]/(f_i(X))$  is an extension field of  $C$ . Then

$$D \otimes_K E = D \otimes_C (C \otimes_K E) \cong \sum D \otimes_C F_i$$

is semi-simple by Theorem 68.1.]

2. Letting the notation be as in Exercise 69.1, prove that if  $C$  is an inseparable extension of  $K$ , there exists a field  $E \supset K$  such that  $C \otimes_K E$  is not semi-simple. [Hint: If  $C$  is inseparable, then  $\text{char } K = p > 0$ , and there exists an element  $\alpha \in C$  such that

$$\text{Irr}(\alpha, K) = (X^p)^n + \xi_1(X^p)^{n-1} + \cdots + \xi_n, \quad \xi_i \in K.$$

Let  $E$  be the field  $K(\xi_1^{1/p}, \dots, \xi_n^{1/p})$ . Then

$$\beta = \alpha^n + \xi_1^{1/p} \alpha^{n-1} + \cdots + \xi_n^{1/p}$$

belongs to the center of  $C \otimes_K E$  and has the property that  $\beta \neq 0$  and  $\beta^p = 0$ . Thus  $C \otimes_K E$  is not semi-simple.]

### §70. The Schur Index

We shall apply the results of the last two sections to study the behavior of an irreducible representation of a finite group under

extension of the base field.

Throughout this section,  $k$  denotes always a *perfect field*, that is, a field such that every extension field  $E$  for which  $(E:k)$  is finite, is separable over  $k$ . In particular,  $k$  is perfect if (a)  $k$  has characteristic zero or (b)  $k$  is a finite field.

Let  $G$  be a finite group. By a  *$k$ -representation* of  $G$ , we mean a representation of  $G$  afforded by a left  $kG$ -module. In other words, a  $k$ -representation  $T$  of  $G$  is a homomorphism  $T: G \rightarrow GL(M)$  where  $M$  is a vector space over  $k$ . We shall use the notation  $\text{env}(T)$  to denote the *enveloping algebra* of  $T$ , that is, the smallest subalgebra of  $\text{Hom}_k(M, M)$  containing the linear transformations  $\{T(g), g \in G\}$ . Then  $\text{env}(T)$  consists of all linear combinations  $\sum_g \alpha_g T(g)$ ,  $\alpha_g \in k$ . Similarly, for a matrix representation  $T$ ,  $\text{env}(T)$  denotes the algebra of matrices consisting of all sums  $\sum \alpha_g T(g)$ ,  $\alpha_g \in k$ .

As we have seen in Chapter IV,  $\text{env}(T)$  can be studied also in terms of  $kG$ -modules. Let  $M$  be a left  $kG$ -module, and for each  $a \in kG$ , let  $a_L$  denote the linear transformation

$$a_L: m \rightarrow am, \quad m \in M.$$

Then

$$A = (kG)_L = \{a_L : a \in kG\}$$

is an algebra over  $k$  such that  $M$  is a faithful left  $A$ -module. If  $T$  is the representation afforded by  $M$ , then  $\text{env}(T) = (kG)_L$ . The  $kG$ -submodules of  $M$  are identical with the  $(kG)_L$ -submodules of  $M$ . In particular, if  $M$  is a completely reducible  $kG$ -module, then  $M$  is a completely reducible  $(kG)_L$ -module, and in this case  $(kG)_L$  is a semisimple algebra.

Now let  $M$  be a left  $kG$ -module, and let  $E$  be an extension field of  $k$ . Then we set

$$M^E = M \otimes_k E, \quad A^E = A \otimes_k E.$$

We note that  $M^E$  is a left  $EG$ -module, and it is easily proved that

$$(70.1) \quad (EG)_L \cong A^E = (kG)_L^E,$$

Because of (70.1), we shall usually identify  $(EG)_L$  with  $(kG)_L^E$ , and regard  $(kG)_L$  as a  $k$ -subalgebra of  $(EG)_L$ .

(70.2) DEFINITION. Let  $U: G \rightarrow GL(n, K)$  be a matrix representation of  $G$ . We say that  $U$  is *realizable in a subfield  $k$  of  $K$*  if there exists a matrix representation  $T: G \rightarrow GL(n, k)$  such that  $U$  and  $T$  are  $K$ -equivalent representations. In module terminology, let

$U$  be afforded by a  $KG$ -module  $M$ . Then  $U$  is realizable in  $k$  if and only if there exists a  $kG$ -module  $N$  such that  $M \cong N^K$  as left  $KG$ -modules.

We can characterize splitting fields in terms of the concept of realizability as follows:

(70.3) THEOREM. *Let  $K^*$  denote an algebraically closed field. A subfield  $k$  of  $K^*$  is a splitting field for  $G$  if and only if every irreducible  $K^*$ -representation is realizable in  $k$ .*

PROOF. First let  $k$  be a splitting field for  $G$ , and let  $\{V_1, \dots, V_r\}$  be a full set of non-isomorphic irreducible  $kG$ -modules. By Theorem 29.21,  $\{V_1^{K^*}, \dots, V_r^{K^*}\}$  is a full set of non-isomorphic irreducible  $K^*G$ -modules, and we have proved that every irreducible  $K^*$ -representation is realizable in  $k$ .

Conversely, suppose  $\{V_1, \dots, V_r\}$  are irreducible  $kG$ -modules such that  $\{V_1^{K^*}, \dots, V_r^{K^*}\}$  are a full set of non-isomorphic irreducible  $K^*G$ -modules. Then no two of the  $\{V_i\}$  are  $kG$ -isomorphic, and by Corollary 29.15, the  $\{V_i\}$  are all absolutely irreducible. Let

$$S = kG/\text{rad } kG = B_1 \oplus \cdots \oplus B_s$$

be the two-sided decomposition of the semi-simple algebra  $S$ . By the argument in the proof of Theorem 69.11,  $S^{K^*}$  is semi-simple, and we have

$$S^{K^*} \cong K^*G/\text{rad } K^*G \cong B_1^{K^*} \oplus \cdots \oplus B_s^{K^*}$$

where the  $\{B_i^{K^*}\}$  are two-sided ideals in  $S^{K^*}$ . Since  $S^{K^*}$  has exactly  $r$  non-isomorphic irreducible modules, the results of §25 imply that  $s \leq r$ , and hence the number of irreducible  $S$ -modules is exactly  $r$ . Therefore  $\{V_1, \dots, V_r\}$  form a full set of non-isomorphic irreducible  $S$ -modules, and all are absolutely irreducible. This proves that  $k$  is a splitting field for  $G$ , and the proof of the theorem is completed.

Suppose now that  $E$  is an arbitrary extension field of  $k$ , and let  $U$  be an  $E$ -representation of  $G$ . Let  $\zeta$  be the character of  $U$ ; then by definition,

$$\zeta(g) = \text{tr } U(g), \quad g \in G.$$

We shall denote by  $k(\zeta)$  the extension field of  $k$  generated by the elements  $\{\zeta(g), g \in G\}$ . Then  $k(\zeta)$  is a finite algebraic extension field of  $k$ , since each  $\zeta(g)$  is a sum of roots of unity. Moreover,  $k(\zeta) = k$  if  $U$  is realizable in  $k$ . Now we come to the main idea of this section.

(70.4) DEFINITION. Let  $K^*$  be the algebraic closure of  $k$ , let  $U$  be an irreducible  $K^*$ -representation of  $G$ , and let  $\zeta$  be the character of  $U$ . The Schur index of  $U$  with respect to  $k$  is defined by

$$m_k(U) = \min(F : k(\zeta))$$

where the minimum is taken over all extension fields  $F$  of  $k(\zeta)$  such that  $U$  is realizable in  $F$ . We shall also write  $m_k(\zeta) = m_k(U)$ , so that we may speak of the Schur index of the  $K^*$ -character  $\zeta$ .

First, we note that, if  $U$  is realizable in  $F$ , then automatically  $F \supset k(\zeta)$ . The Schur index is thus either a non-negative integer or  $+\infty$ , which measures how close  $U$  comes to being realizable in  $k(\zeta)$ . Our first main result asserts that  $m_k(U)$  is always finite, and gives one of the two main characterizations of  $m_k(U)$  which we shall obtain.

Before proceeding with this theorem, we prove some lemmas. In the first lemma and subsequently in this section, we shall denote by  $mU$  the direct sum of  $m$  copies of a given representation  $U$  of  $G$ .

It is also appropriate at this time to explain that in this section the results of Chapter IV and the first part of this chapter will be applied to enveloping algebras of representations of  $G$  rather than to the group algebras themselves. The reason for this is that the theory of the Schur index involves only simple and semi-simple algebras, even though we consider representations in a field  $k$  such that the group algebra  $kG$  is not semi-simple.

(70.5) LEMMA. Let  $T$  be an irreducible  $K$ -representation of  $G$  for some field  $K$ , and let  $A = \text{env}(T)$ . We have

(i)  $A \cong D_n$ , for some  $n$  and some division algebra  $D$  whose center contains  $K$ .

(ii) If the center of  $D$  coincides with  $K$  and if  $D$  has index  $m = \sqrt{(D : K)}$ , then for any splitting field  $F$  for  $D$  we have

$$A \otimes_K F \cong F_{mn}.$$

(iii) Keeping the hypothesis of (ii), let  $U$  be an irreducible  $F$ -representation of  $G$  afforded by a minimal left ideal in  $A \otimes_K F$ . Then  $U$  is absolutely irreducible, and we have

$$T^F \sim mU,$$

(equivalence of  $F$ -representations), which shows that  $mU$  is realizable in  $K$ . Moreover, for  $m'$  a positive integer,  $m'U$  is realizable in  $K$  if and only if  $m | m'$ .

**PROOF.** The algebra  $A$  has a faithful irreducible representation; hence  $A$  is a simple algebra over  $K$ , and the first assertion follows from Theorem 26.4.

For the second assertion, let  $F$  be a splitting field for  $D$ ; this means that  $F \supset K$ , and  $F \otimes_K D$  is a full matrix algebra over  $F$ . By (68.5), we may therefore write

$$A \otimes_K F \cong F_t$$

for some positive integer  $t$ . But

$$(A \otimes_K F : F) = (A : K) = (D_n : K) = n^2(D : K) = n^2m^2,$$

whereas

$$(F_t : F) = t^2.$$

This shows that  $t = mn$ , and establishes the second assertion.

Finally, let  $U$  be the irreducible  $F$ -representation afforded by a minimal left ideal in  $A \otimes_K F$ . Since  $A \otimes_K F$  is a full matrix algebra over  $F$ , it follows that  $U$  is absolutely irreducible. Furthermore,  $U$  is the only irreducible  $F$ -representation of  $A \otimes_K F$ . Since  $T^F$  is an  $F$ -representation of  $A \otimes_F F$ , we have  $T^F \sim sU$  for some positive integer  $s$ . We wish to show that  $s = m$ . The representation  $T$  is afforded by a minimal left ideal  $I$  in  $A$ , and since  $A \cong D_n$ , we see that  $A$  is isomorphic to the direct sum of  $n$  copies of  $I$ . Hence  $A^F = A \otimes_K F$  is a direct sum of  $n$  copies of  $I \otimes_K F$ . On the other hand, the isomorphism  $A^F \cong F_{mn}$  shows that  $A^F$  is a direct sum of  $mn$  minimal left ideals. Therefore  $I \otimes_K F$  is a direct sum of  $m$  minimal left ideals of  $A^F$ ; that is,  $T^F \sim mU$ .

Clearly, if  $m \mid m'$ , then  $m'U$  is realizable in  $K$ . Suppose conversely that  $m'U$  is realizable in  $K$ . Then  $m'U \sim W^F$  for some  $K$ -representation  $W$  of  $G$ . Since  $T(a) = 0$  implies  $U(a) = 0$  and hence  $W(a) = 0$  for all  $a \in KG$ ,  $W$  is a representation of  $A = \text{env}(T)$ , hence  $W$  is  $K$ -equivalent to  $rT$  for some  $r$ . Then

$$m'U \sim rT^F \sim rmU,$$

and  $m' = rm$ . This completes the proof of the lemma.

In the rest of this section,  $(D)_n$  will denote a full matrix algebra over  $D$ , whereas  $D_i$  refers to the  $i$ th skewfield in a set of skewfields under consideration.

In the next two lemmas, let  $\{M_1, \dots, M_r\}$  denote a full set of non-isomorphic irreducible  $K^*G$ -modules where  $K^*$  is the algebraic closure of the field  $k$ . For each  $i$ ,  $1 \leq i \leq r$ , let  $M_i$  afford the representation  $U_i$  with character  $\zeta_i$ . Let  $z_i = (M_i : K^*)$ , and let  $K_i = k(\zeta_i)$

for  $1 \leq i \leq r$ . Since  $U_i$  is absolutely irreducible, we have  $\text{env}(U_i) = (K^*)_{z_i}$ . Let

$$(70.6) \quad A_i = \sum_{g \in G} K_i U_i(g),$$

Then  $A_i$  is a  $K_i$ -subalgebra of  $\text{env}(U_i)$ . We prove that if  $z_i \neq 0$  in  $K_i$ , then  $A_i$  is simple, and

$$(70.7) \quad \text{env}(U_i) = A_i \otimes_{K_i} K^*.$$

Since  $A_i K^* = \text{env}(U_i)$ ,  $A_i$  is semi-simple. By (70.8) below,  $A_i$  is central simple. By (68.1)  $A_i \otimes_{K_i} K^*$  is simple, and since  $\text{env}(U_i) = A_i K^*$  is a homomorphic image of  $A_i \otimes_{K_i} K^*$ , we have (70.7). Finally

$$A_i \cong (D_i)_{n_i}$$

where  $D_i$  is a division algebra over  $k$  whose center contains  $K_i$ .

(70.8) LEMMA. *If either  $\text{char } k = 0$  or  $\text{char } k \nmid z_i$ , the center of  $A_i$  is identical with  $K_i I^{(z_i)}$ .*

PROOF. Let  $\gamma$  belong to the center of  $A_i$ . Then by (70.7),  $\gamma$  belongs also to the center of  $\text{env}(U_i)$ . Therefore from (70.6), we have

$$(70.9) \quad \gamma = \sum_{g \in G} \xi_g U_i(g) = \xi I^{(z_i)}$$

for some  $\xi_g \in K_i$  and  $\xi \in K^*$ , since the center of  $\text{env}(U_i)$  is  $K^* I^{(z_i)}$ . Taking traces in (70.9), we obtain

$$\sum_{g \in G} \xi_g \zeta_i(g) = \xi \cdot z_i.$$

Therefore, since  $z_i \neq 0$  in  $K_i$  by hypothesis, we have  $\xi \in K_i$ , and (70.9) asserts  $\gamma \in K_i I^{(z_i)}$ . This completes the proof of the lemma.

(70.10) COROLLARY. *Let  $z_i \neq 0$  in  $k$ . Then*

$$z_i = m_i n_i$$

where  $m_i = \sqrt{(D_i : K_i)}$  and  $A_i = (D_i)_{n_i}$ .

PROOF. We have by (70.7),

$$A_i \otimes_{K_i} K^* = \text{env}(U_i) = (K^*)_{z_i}.$$

On the other hand,  $K^*$  is a splitting field for  $D_i$ , and  $(D_i : K_i) = m_i^2$ . Since  $K_i$  is the center of  $D_i$  by Lemma 70.8, we have

$$A_i \otimes_{K_i} K^* \cong (D_i)_{n_i} \otimes_{K_i} K^* \cong (K^*)_{m_i n_i},$$

by Lemma 70.5, and the corollary is proved.

(70.11) LEMMA. Let  $z_i \neq 0$  in  $k$ , and let  $E$  be a finite algebraic extension field of  $k$ . Then  $U_i$  is realizable in  $E$  if and only if  $E$  is a splitting field for  $D_i$ .

PROOF. We may assume that  $K^* \supset E \supset K_i$ . By Lemma 70.8 and Theorem 68.1, the algebra

$$B_i = A_i \otimes_{K_i} E$$

is a simple algebra with center  $E$ . Therefore there exists a division algebra  $L_i$  with center  $E$  such that for some  $s$ ,

$$B_i \cong (L_i)_s \cong L_i \otimes_E (E)_s.$$

Let  $e_i = \sqrt{(L_i : E)}$ . Since  $B_i \otimes_E K^* \cong A_i \otimes_{K_i} K^*$ , we see that  $U_i$  is afforded by a minimal left ideal in  $B_i \otimes_E K^*$ . Hence by (70.5),  $e_i U_i$  is realizable in  $E$ , and  $e_i$  is minimal with this property. Then  $U_i$  is realizable in  $E$  if and only if  $L_i = E$ , that is, if and only if  $A_i \otimes_{K_i} E \cong (E)_s$ . The result now follows from (68.5).

Now we come to our first main result.

(70.12) THEOREM. Let  $U_i$  be an irreducible  $K^*$ -representation of  $G$  with character  $\zeta_i$ , and assume that  $z_i \neq 0$  in  $K^*$ .

(i) There exists a finite algebraic extension field  $F_i$  of  $k$  in which  $U_i$  is realizable such that

$$(F_i : k(\zeta_i)) = m_k(U_i).$$

(ii) For any finite algebraic extension  $F$  of  $k$  in which  $U_i$  is realizable, we have

$$m_k(U_i) \mid (F : k(\zeta_i)).$$

(iii)  $m_k(U_i)$  is the minimal value of  $m$  such that  $mU_i$  is realizable in  $K_i = k(\zeta_i)$ .

(iv)  $m_k(U_i) \mid \deg U_i$ .

PROOF. The first two statements of the theorem are immediate consequences of Lemma 70.11 and the theory of splitting fields of division algebras [see in particular Theorems (68.6) and (68.7)].

For the third and fourth statements, we use Lemma 70.8 to deduce that the center of  $A_i = \sum_g K_i U_i(g)$  is identical with  $K_i$ . If  $m_i = \sqrt{(D_i : K_i)}$ , we know by Lemma 70.11 and Theorems (68.6) and (68.7) that

$$(70.13) \quad m_i = \sqrt{(D_i : K_i)} = m_k(U_i).$$

By Lemma 70.5, we have statement (iii), whereas Corollary 70.10

combined with (70.13) proves (iv). This completes the proof of the theorem.

The actual computation of the Schur index is usually a formidable task. We shall give an example to show how the preceding theorem can be used to find the Schur index in a simple case.

*Example.* Let  $G$  be the quaternion group of order 8, consisting of the quaternions  $\{\pm 1, \pm i, \pm j, \pm k\}$  satisfying the usual multiplication rules. By the results of §47, we can verify easily that  $G$  has four one-dimensional linear characters in the complex field, and a unique two-dimensional irreducible complex character  $\chi$  such that

$$\chi(1) = -\chi(-1) = 2, \quad \chi(i) = \chi(j) = \chi(k) = 0$$

where  $1, -1, i, j, k$  are representatives of the distinct conjugate classes of  $G$ . By (iv) of Theorem 70.12,  $m_\varphi(\chi)$  is 1 or 2, and we shall show that it is 2. Suppose instead that  $m_\varphi(\chi) = 1$ . Then the two-dimensional irreducible matrix representation  $\mathbf{U}$  with character  $\chi$  is realizable in  $Q$ . For a suitable basis, we may assume that

$$\mathbf{U}(1) = \mathbf{I}^{(2)}, \quad \mathbf{U}(-1) = -\mathbf{I}^{(2)}, \quad \mathbf{U}(i) = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

From  $ij = -ji$  we have

$$\mathbf{U}(j) = \begin{pmatrix} a & b \\ b & -a \end{pmatrix};$$

then  $j^2 = -1$  implies that  $a^2 + b^2 = -1$ , which is impossible for rational numbers  $a$  and  $b$ . Therefore  $\mathbf{U}$  is not realizable in  $Q$ , and  $m_\varphi(\chi) = 2$ , as we wished to prove.

Theorem 70.12 approaches the Schur index by “looking down” from an irreducible  $K^*$ -representation to view the fields in which it is realizable. The next result gives another characterization of the Schur index obtained by “looking up” to see the way an irreducible  $k$ -representation splits into absolutely irreducible components under extension of the base field.

We begin by noting that, by Theorems (29.16) and (69.11), we can find a finite algebraic extension field  $E$  of  $k$  which is a splitting field for  $G$ , and that, by (29.21), we may assume that  $E$  is a normal separable extension of  $k$ . Let  $G_{E/k}$  be the Galois group of  $E$  over  $k$ ; then an element  $\lambda \in E$  is in  $k$  if and only if  $\lambda^\sigma = \lambda$  for all  $\sigma \in G_{E/k}$ .

Now let  $\{\mathbf{U}_1, \dots, \mathbf{U}_r\}$  denote a full set of non-isomorphic irreducible  $E$ -representations of  $G$ . Then the  $\{\mathbf{U}_i\}$  are absolutely irreducible, and we define  $\zeta_i, K_i = k(\zeta_i), z_i, A_i, D_i$ , etc., as in the dis-

cussion preceding Lemma 70.8. The automorphisms  $\sigma \in G_{E/k}$  permute the  $\{U_i\}$  in the following way: For each  $g \in G$ , let  $U_i^g(g)$  denote the matrix obtained by letting  $\sigma$  act on all the coefficients of  $U_i(g)$ . Then it is clear that  $U_i^g$  is an absolutely irreducible matrix representation of  $G$ , and it is therefore equivalent to one of the representations  $U_j$ ,  $1 \leq j \leq r$ . If  $\zeta_i$  is the character of  $U_i$ , then  $\zeta_i^g$  is the character of  $U_i^g$ , and, since the  $\{U_i\}$  are absolutely irreducible, Theorem 30.15 implies that  $U_i$  and  $U_i^g$  are equivalent if and only if  $\zeta_i = \zeta_i^g$ . The representation  $U_i^g$ ,  $\sigma \in G_{E/k}$ , is called a *conjugate representation* of  $U_i$ .

Our main objective is to study the decomposition of a representation  $T^E$ , where  $T$  is an irreducible  $k$ -representation of  $G$ . Let  $M$  be an irreducible  $kG$ -module which affords the representation  $T$ , and let  $A = (kG)_L$ . Then  $A$  is a simple subalgebra of  $\text{Hom}_k(M, M)$ . Since  $E$  is separable over  $k$ , Corollary 69.9 implies that  $M^E$  is a completely reducible  $EG$ -module. Then as we have shown,  $A^E = (EG)_L$ , and  $A^E$  is a semi-simple subalgebra of  $\text{Hom}_E(M^E, M^E)$ . Finally we note that the matrix representation  $T^E$  is afforded by the module  $M^E$ .

Let  $\{\epsilon_1, \dots, \epsilon_t\}$  be the central primitive idempotents in  $A^E$ . Then

$$A^E = \epsilon_1 A^E \oplus \cdots \oplus \epsilon_t A^E$$

where each  $\epsilon_i A^E$  is a simple component of  $A^E$ . Corresponding to this decomposition of  $A^E$ , we have

$$M^E = \epsilon_1 M^E \oplus \cdots \oplus \epsilon_t M^E.$$

Each submodule  $\epsilon_i M^E$  contains only irreducible submodules belonging to the component  $\epsilon_i A^E$  of  $A^E$ . Therefore we may express each  $\epsilon_i M^E$ ,  $1 \leq i \leq t$ , as a direct sum

$$\epsilon_i M^E = M_{i1} \oplus \cdots \oplus M_{id(i)}$$

where the  $M_{ij}$ ,  $j = 1, 2, \dots, d(i)$ , are absolutely irreducible isomorphic  $EG$ -modules. We may assume the  $\{U_i\}$  so ordered that  $U_i$  is the representation of  $G$  afforded by any module  $M_{ij} \subset \epsilon_i M^E$ ,  $1 \leq j \leq d(i)$ . If  $T$  is a matrix representation afforded by  $M$ , we have

$$(70.14) \quad T^E \sim d(1)U_1 + \cdots + d(t)U_t.$$

Our second main result on the Schur index can be stated as follows.

(70.15) **THEOREM.** *Let  $T$  be an irreducible  $k$ -representation of  $G$ , and let  $E$  be a splitting field for  $G$  which is a finite normal extension*

of  $k$ . Then  $\mathbf{T}^E$  is completely reducible, and the components  $\{U_i\}$  of  $\mathbf{T}^E$  [see (70.14)] are conjugates of each other. The number of different conjugates in (70.14) is exactly  $(k(\zeta_1) : k)$  where  $\zeta_1$  is the character of  $U_1$ . Finally, if  $k$  has characteristic zero, we have  $d(1) = \dots = d(t) = m_k(U_1)$  in (70.14).

PROOF. Let  $\sigma \in G_{E/k}$ . Then by the results of §12,

$$S_\sigma: \sum e_j \otimes m_j \rightarrow \sum e_j^\sigma \otimes m_j, \quad e_j \in E, m_j \in M,$$

is a  $k$ -automorphism of  $M^E$ , and

$$\sum e_j \otimes a_j \rightarrow \sigma(\sum e_j \otimes a_j) \rightarrow \sum e_j^\sigma \otimes a_j, \quad e_j \in E, a_j \in A,$$

is an automorphism of the algebra  $A^E$ . Some basic properties of these mappings are as follows.

(70.16) If  $u \in A^E$ , and if  $\sigma(u) = u$  for all  $\sigma \in G_{E/k}$ , then  $u \in A$ .

(70.17)  $\sigma(u)S_\sigma x = S_\sigma(ux)$ ,  $u \in A^E, \sigma \in G_{E/k}, x \in M^E$ .

(70.18) If  $V$  is an irreducible  $EG$ -submodule of  $M^E$  which affords the representation  $U_i$ , then  $S_\sigma V$  affords the representation  $U_i^\sigma$ .

The proofs of (70.16) through (70.18) are left as exercises.

Now we are ready to prove the theorem. For any  $\sigma \in G_{E/k}$ ,  $\sigma(\epsilon_1)$  is again a central primitive idempotent of  $A^E$  and therefore coincides with some  $\epsilon_j$  for  $1 \leq j \leq t$ . If  $\epsilon_1, \epsilon_2, \dots, \epsilon_s$  are the different conjugates  $\sigma(\epsilon_1)$  of  $\epsilon_1$ , then

$$f = \epsilon_1 + \dots + \epsilon_s$$

has the property that  $\sigma(f) = f$  for all  $\sigma \in G_{E/k}$ . Therefore by (70.16),  $f$  is a central idempotent in  $A$ , and since  $A$  is simple, we have  $f = 1$ . Therefore  $s = t$ , and all the  $\{\epsilon_i\}$  in  $A^E$  are conjugates of  $\epsilon_1$ .

Next let  $M_{ii}$  be an irreducible  $EG$ -submodule of  $\epsilon_1 M^E$ . Then for any  $\sigma \in G_{E/k}$ , we have by (70.17)

$$S_\sigma M_{ii} = S_\sigma \epsilon_i M_{ii} = \sigma(\epsilon_i) S_\sigma M_{ii}.$$

If  $U_i$  is the representation afforded by  $M_i$ , it follows by (70.18) that  $S_\sigma M_{ii}$  affords the representation  $U_i^\sigma$ , and the above relation shows that  $S_\sigma M_{ii} \subset \sigma(\epsilon_i) M^E$ . In other words, if  $U_j$  is the representation of  $G$  associated with  $\sigma(\epsilon_i)$ , we have shown that  $U_j$  is equivalent to  $U_i^\sigma$ . Since all  $\{\epsilon_i\}$  are conjugates of  $\epsilon_1$ , these remarks show that if  $\epsilon_i = \sigma(\epsilon_1)$ , then  $U_i \sim U_i^\sigma$ , and all the  $\{U_i\}$  appearing in (70.14) are conjugate representations.

We have shown that  $\epsilon_i = \sigma(\epsilon_1)$  implies  $U_i \sim U_i^\sigma$ , and hence

$\zeta_i = \zeta_1^\sigma$ . Conversely, suppose  $\zeta_i = \zeta_1^\sigma$  for some  $i$ ,  $1 \leq i \leq t$ . Then by Theorem 30.15, we have  $U_i \sim U_1^\sigma$ , and we wish to prove that  $\epsilon_i = \epsilon_1^\sigma$ . If  $U_1$  is afforded by the module  $M_{11}$ , then  $U_1^\sigma$  is afforded by the module  $S_\sigma M_{11}$ , and since  $U_1^\sigma \sim U_i$ , we have  $\epsilon_i S_\sigma M_{11} \neq 0$ . Therefore, by (70.17)

$$\epsilon_i S_\sigma M_{11} = \epsilon_i S_\sigma \epsilon_1 M_{11} = \epsilon_i \sigma(\epsilon_1) S_\sigma M_{11} \neq 0,$$

and  $\epsilon_i \sigma(\epsilon_1) \neq 0$ . This shows that  $\epsilon_i = \sigma(\epsilon_1)$ , and we have proved

$$(70.19) \quad \text{For any } \sigma \in G_{E/k}, \epsilon_i = \sigma(\epsilon_1) \text{ if and only if } \zeta_i = \zeta_1^\sigma.$$

Now let  $H$  be the subgroup of  $G_{E/k}$  consisting of all  $\sigma \in G_{E/k}$  such that  $\sigma(\epsilon_1) = \epsilon_1$ . Then the number of distinct conjugates  $t$  in (70.14) is the index  $[G_{E/k} : H]$ . By (70.19),  $\sigma \in H$  if and only if  $\sigma$  leaves fixed every element of  $k(\zeta_1)$ . Therefore, by Galois theory, the number of conjugates of  $U_1$  in (70.14) is

$$[G_{E/k} : H] = (k(\zeta_1) : k),$$

and the first two assertions of the theorem are proved.

Finally, let  $k$  be a field of characteristic zero, and let  $K_i = k(\zeta_i)$ ,  $1 \leq i \leq t$ . Then for each  $i$ ,  $1 \leq i \leq t$ ,  $A^{K_i}$  is a semi-simple sub-algebra of  $A^E$ . Let  $\sigma_1 = 1, \sigma_2, \dots, \sigma_t$  be distinct left coset representatives of  $H$  in  $G_{E/k}$ ; then we may assume that  $\epsilon_i = \sigma_i(\epsilon_1)$ ,  $1 \leq i \leq t$ , and hence by (70.19), we have  $K_i = \sigma_i(K_1)$ ,  $1 \leq i \leq t$ . Since  $\sigma(\epsilon_1) = \epsilon_1$  for all  $\sigma \in H$ ,  $\epsilon_1 \in A^{K_1}$ , and hence  $\epsilon_i = \sigma_i(\epsilon_1) \in A^{K_i}$ ,  $1 \leq i \leq t$ , and the automorphism  $\sigma_i$  carries  $\epsilon_1 A^{K_1}$  onto  $\epsilon_i A^{K_i}$ . Let  $f_i$  be a primitive idempotent in  $\epsilon_1 A^{K_1}$ . Then  $f_i = \sigma_i(f_1)$  is a primitive idempotent in  $\epsilon_i A^{K_i}$ . Let  $f = \sum_{i=1}^t f_i$ . Then  $\sigma(f) = f$  for all  $\sigma \in G_{E/k}$  and  $f \in A$ . Moreover the fact that  $f_i \epsilon_i = f_i$ , where  $\epsilon_i$  is a central idempotent in  $A^E$ , implies that  $f$  is an idempotent in  $A$ . If  $f = f' + f''$ , where  $f'$  and  $f''$  are orthogonal idempotents in  $A$ , then  $f' = \sum \epsilon_i f'_i$ ,  $f'' = \sum \epsilon_i f''_i$ , and  $\epsilon_i f'_i = \sigma_i(\epsilon_1 f'_i)$ ,  $\epsilon_i f''_i = \sigma_i(\epsilon_1 f''_i)$ ,  $1 \leq i \leq t$ . The fact that  $f_1 = \epsilon_1 f = \epsilon_1 f' + \epsilon_1 f''$  implies that either  $\epsilon_1 f'$  or  $\epsilon_1 f''$  coincides with  $f_1$ , since  $f_1$  is a primitive idempotent in  $\epsilon_1 A^{K_1}$ . Suppose  $\epsilon_1 f' = f_1$ ; then  $\epsilon_i f' = \sigma_i f_1 = f_i$ , and  $f' = \sum \epsilon_i f'_i = \sum f_i = f$ . We have proved that  $f = \sum f_i$  is a primitive idempotent in  $A$ . Then  $Af$  is a minimal left ideal in  $A$  and affords the representation  $T$ . Moreover,

$$(70.20) \quad A^E f = (A^{K_1} f_1)^E \oplus \cdots \oplus (A^{K_t} f_t)^E.$$

The argument of Lemma 70.8 can be applied to show that  $K_i$  is the center of  $A^{K_i}$ ,  $1 \leq i \leq t$ , since  $k$  has characteristic zero. Then Lemma 70.5 implies that  $(A^{K_i} f_i)^E$  affords the representation  $m_k(U_i)U_i$

for  $1 \leq i \leq t$ . Since  $A^E f$  affords the representation  $\mathbf{T}^E$ , we obtain from (70.20) the result that

$$\mathbf{T}^E \sim m_k(\mathbf{U}_1)\mathbf{U}_1 + \cdots + m_k(\mathbf{U}_t)\mathbf{U}_t,$$

and, comparing this with (70.14), we have  $m_k(\mathbf{U}_i) = d(i)$ ,  $1 \leq i \leq t$ . Finally, we note that the Schur indices of conjugate representations are equal, by the third statement of Theorem 70.12. This completes the proof of Theorem 70.15.

We shall conclude this section with some important applications of Theorems (70.12) and (70.15). The first is the following corollary of Theorem 70.15, which has already been stated in § 41 [see (41.5)], and is one of the key results used in our proof that  $Q(\overline{\mathcal{V}^1})$  is a splitting field for  $G$  if  $m$  is the exponent of  $G$ .

(70.21) COROLLARY. *Let  $F$  be a subfield of the complex field  $K$ , and let  $M$  be an irreducible  $KG$ -module which affords the absolutely irreducible representation  $\mathbf{U}$ . Then for any  $FG$ -module  $W$ , the multiplicity with which  $M$  occurs as a composition factor of  $W^K$  is a multiple of  $m_F(\mathbf{U})$ .*

PROOF. Let  $W = W_1 \oplus \cdots \oplus W_s$  where the  $\{W_i\}$  are irreducible  $FG$ -modules. Then

$$W^K = W_1^K \oplus \cdots \oplus W_s^K.$$

Then  $\mathbf{U}$  is realizable in the splitting field  $E$  of Theorem 70.15, and by Theorem 70.15, the multiplicity with which  $M$  occurs in each  $W_i^K$  is a multiple of  $m_E(\mathbf{U})$ . This completes the proof of the corollary.

Because an important part of Theorem 70.15 is valid for fields of characteristic  $p > 0$ , we are now able to prove a splitting field theorem for characteristic  $p$ .

(70.22) LEMMA. *Let  $k$  be a finite field such that  $k = k(\zeta)$  for all characters  $\zeta$  of irreducible  $K^*$ -representations of  $G$  where  $K^*$  is the algebraic closure of  $k$ . Let  $\mathbf{T}$  be an irreducible  $k$ -representation of  $G$ . Then the center of the enveloping algebra  $A$  of  $\mathbf{T}$  consists exactly of the elements  $r \cdot \mathbf{I}$ ,  $r \in k$ .*

PROOF. By the first part of Theorem 70.15, we can find a suitable splitting field  $E$  of  $G$  such that

$$\mathbf{T}^E \sim m_1 \mathbf{U}_1 + \cdots + m_t \mathbf{U}_t$$

where  $\mathbf{U}_1, \dots, \mathbf{U}_t$  are irreducible  $E$ -representations of  $G$  and are precisely the distinct conjugates of  $\mathbf{U}_1$ . If  $c$  belongs to the center

of  $A$ , we have by Schur's Lemma

$$c = m_1\gamma_1 U_1(1) + \cdots + m_t\gamma_t U_t(1), \quad \gamma_i \in E,$$

where  $\gamma_1, \dots, \gamma_t$  are conjugates of  $\gamma_1$ . Since  $k$  contains the field  $k(\zeta_1)$ , Theorem 70.15 implies that  $t = 1$ ; hence  $\gamma_1$  coincides with all its conjugates and is an element of  $k$ . Then

$$c = \gamma_1(m_1 U_1(1) + \cdots + m_t U_t(1)) = \gamma_1 I, \quad \gamma_1 \in k,$$

and the lemma is proved.

(70.23) THEOREM. *Let  $k$  be a finite field containing  $k(\zeta)$  for all irreducible  $K^*$ -characters  $\zeta$  of  $G$ . Then every irreducible  $k$ -representation  $T$  of  $G$  is absolutely irreducible.*

PROOF. Let  $M$  be a left  $kG$ -module which affords  $T$ , and let  $A = (kG)_L$ . Since  $k$  is a finite field, it follows that

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

is a division algebra over  $k$  containing a finite number of elements. By Wedderburn's Theorem 68.9,  $D$  is commutative. By the results of § 26 we have

$$A = \text{Hom}_D(M, M),$$

and it follows that  $D$  is contained in the center of  $A$ . By Lemma 70.22, we have  $D = k \cdot I$ ; and hence by Theorem 29.13,  $T$  is absolutely irreducible. This proves the theorem.

(70.24) COROLLARY. *Let  $m$  be the exponent of  $G$ , and let  $k$  be the prime field of  $p$  elements for some prime  $p$ . Then  $k(\sqrt[m]{1})$  is a splitting field for  $G$ .*

PROOF. For any absolutely irreducible  $K^*$ -character  $\zeta$  of  $G$ , we have  $k(\zeta) \subset k(\sqrt[m]{1})$ . Therefore, by Theorem 70.23,  $k(\sqrt[m]{1})$  is a splitting field for  $G$ , and the corollary is proved.

Our final result in this section is an application by Solomon [1], [2] of the Witt-Berman induction theorem of § 42 to prove a result of Brauer which shows that the problem of computing Schur indices for a group  $G$  may be reduced to computing the Schur indices of certain solvable subgroups of  $G$ . We begin by recalling some definitions and notations.

Throughout the remainder of this section,  $K$  denotes a subfield of the complex field  $\Omega$ . As in § 42, let  $\epsilon$  denote a primitive  $m$ th root of 1 for some positive integer  $m$ , and let  $I_m(K)$  denote the Galois group of the finite normal extension  $K(\epsilon)$  over  $K$ . A subgroup  $H$

of  $G$  is said to be a *K-elementary subgroup* at the prime  $p$  if  $H$  is a semi-direct product

$$H = [a]P$$

where  $[a]$  is a cyclic normal subgroup of  $H$  of order  $m$ ,  $P$  a  $p$ -group for a prime  $p \nmid m$ , and for each  $x \in P$  we have

$$xax^{-1} = a^i$$

where  $\epsilon \rightarrow \epsilon^i$  is an element of the Galois group  $I_m(K)$ .

We recall that a *K-character* of  $G$  is a character afforded by a left  $KG$ -module. We say that a character  $\chi$  of  $G$  lies in  $K$  if  $\chi(g) \in K$  for all  $g \in G$ . Evidently every  $K$ -character of  $G$  lies in  $K$ , but the converse is not necessarily true, as our example of the quaternion group given earlier in this section shows.

For two  $\Omega$ -characters  $\chi$  and  $\psi$  of a group  $H$ , we let  $(\chi, \psi)$  denote the inner product of  $\chi$  and  $\psi$  as defined in Exercise 31.1 and in §38. If  $\chi$  is an irreducible character, then  $(\chi, \psi)$  is equal to the multiplicity of  $\chi$  in  $\psi$ , i.e., the number of times  $\chi$  appears when  $\psi$  is expressed as a sum of irreducible characters.

(70.25) LEMMA. *Let  $\chi$  be an irreducible  $\Omega$ -character of  $G$ . Let  $n$  be the exponent of  $G$ ,  $\epsilon$  a primitive  $n$ th root of 1, and  $F$  a field such that*

$$K(\chi) \subset F \subset K(\epsilon),$$

*where  $(K(\epsilon) : F)$  is a power of  $p$  for some prime  $p$ . Then there exists a subgroup  $H$  of  $G$  which is  $F$ -elementary at a prime  $q$  (possibly  $q \neq p$ ), and an irreducible  $\Omega$ -character  $\xi$  of  $H$  lying in  $F$  such that*

$$p \nmid (\chi | H, \xi).$$

PROOF. Let  $p^e \parallel [G : 1]$ , and write  $[G : 1] = t_p p^e$ . By the Witt-Berman induction theorem 42.3, we have

$$t_p = t_p \zeta^{(1)} = \sum a_i \psi_i^q, \quad a_i \in Z,$$

where  $\zeta^{(1)}$  is the 1-character of  $G$  and the  $\{\psi_i\}$  are  $F$ -characters of  $F$ -elementary subgroups  $\{H_i\}$  of  $G$  at various primes  $\{q_i\}$ . By Theorem 38.5, we have

$$(70.26) \quad t_p \chi = \sum a_i \psi_i^q \chi = \sum a_i (\psi_i(\chi | H_i))^q.$$

For a field  $E$  such that  $F \subset E \subset \Omega$ , we say that an isomorphism  $\sigma: E \rightarrow \Omega$  is an *F-isomorphism* of  $E$  into  $\Omega$  if  $\sigma = 1$  on  $F$ . If  $(E : F)$  is finite, then from Galois theory, we know that the number of  $F$ -isomorphisms of  $E \rightarrow \Omega$  is finite and is equal to  $(E : F)$  (see Zariski-

Samuel [1], p. 77). Now let  $\xi$  be an irreducible  $\Omega$ -character of one of the subgroups  $H_i$  appearing in (70.26). We define the  $F$ -trace of  $\xi$  by

$$\text{sp}_F(\xi) = \sum \xi^\sigma$$

where the  $\xi^\sigma$  are conjugate characters of  $\xi$  determined by the distinct  $F$ -isomorphisms  $\sigma$  of  $F(\xi) \rightarrow \Omega$ . The character  $\xi$  lies in  $F$  if and only if  $\text{sp}_F(\xi) = \xi$ . Let  $\mu$  be any character of  $H_i$  lying in  $F$ . Then  $\mu$  is a  $Z$ -linear combination of irreducible  $\Omega$ -characters of  $H_i$ , and, from  $\text{sp}_F(\mu) = \mu$ , we deduce that  $\mu$  is a sum of  $F$ -traces  $\text{sp}_F(\xi)$  of irreducible  $\Omega$ -characters  $\xi$  of  $H_i$ .

Returning to (70.26), we note that since  $\chi$  lies in  $F$  by hypothesis, each  $\psi_i(\chi | H_i)$  lies in  $F$ ; hence

$$(70.27) \quad t_p \chi = \sum b_i (\text{sp}_F(\xi_i))^\sigma, \quad b_i \in Z,$$

where the  $\{\xi_i\}$  are irreducible  $\Omega$ -characters of the  $F$ -elementary subgroups  $H_i$  appearing in (70.26). Since  $\chi$  lies in  $F$ , we have

$$(\chi | H_i, \xi_i^\sigma) = (\chi | H_i, \xi_i)$$

for each  $F$ -isomorphism  $\sigma: F(\xi_i) \rightarrow \Omega$ . Therefore

$$(\chi | H_i, \text{sp}_F(\xi_i)) = (F(\xi_i) : F)(\chi | H_i, \xi_i)$$

where  $(F(\xi_i) : F)$  is the number of distinct  $F$ -isomorphisms  $\sigma$  of  $F(\xi_i)$  into  $\Omega$ . By (70.27),  $\chi$  has multiplicity  $t_p$  in  $\sum b_i (\text{sp}_F(\xi_i))^\sigma$ . Applying the Frobenius reciprocity theorem 38.8 to (70.27), we have

$$\begin{aligned} t_p &= (\chi, \sum b_i (\text{sp}_F(\xi_i))^\sigma) = \sum b_i (\chi | H_i, \text{sp}_F(\xi_i)) \\ &= \sum b_i (F(\xi_i) : F)(\chi | H_i, \xi_i). \end{aligned}$$

Since  $p \nmid t_p$ , we deduce that for some  $i_0$ ,

$$p \nmid (F(\xi_{i_0}) : F)(\chi | H_{i_0}, \xi_{i_0}).$$

Since

$$F \subset F(\xi_i) \subset K(\epsilon), \quad (K(\epsilon) : F) = \text{power of } p,$$

we have  $F(\xi_{i_0}) = F$ . We have shown that  $\xi_{i_0}$  is an irreducible  $\Omega$ -character of an  $F$ -elementary subgroup  $H_{i_0}$  lying in  $F$  and that  $p \nmid (\chi | H_{i_0}, \xi_{i_0})$ . This completes the proof of the lemma.

In the next theorem,  $m_K(\chi)$  denotes the Schur index of an irreducible  $\Omega$ -character  $\chi$ . For an integer  $m > 0$  and a prime  $p$ , we shall call the  $p$ -part of  $m$  the prime power  $p^a$  such that  $p^a \parallel m$ .

(70.28) THEOREM (Brauer [23]). *Let  $G$  be a finite group,  $K$  an algebraic number field,  $\chi$  an irreducible  $\Omega$ -character of  $G$ , and suppose*

that  $K = K(\chi)$ . Let  $p$  be a prime such that  $p \mid m_K(\chi)$ . Then there exists an algebraic number field  $F$  containing  $K$ , a subgroup  $H$  of  $G$  which is  $F$ -elementary at  $p$ , and an irreducible  $\Omega$ -character  $\xi$  of  $H$  lying in  $F$  such that  $m_K(\xi)$  is the  $p$ -part of  $m_K(\chi)$ .

PROOF. We remark that the assumption  $K = K(\chi)$  is a natural one since  $m_K(\chi) = m_{K(\chi)}(\chi)$ .

We note also that, if  $H$  is an  $F$ -elementary subgroup of  $G$  at a prime  $q$ , and if  $\xi$  is an irreducible  $\Omega$ -character of  $H$ , then by Ito's theorem [Corollary 53.18], the degree of  $\xi$  is a power of  $q$ . By (70.10) and (iv) of Theorem 70.12, we see that  $m_K(\xi) \mid \deg \xi$ , so that  $m_K(\xi)$  is a power of  $q$ .

Let  $\epsilon$  be a primitive  $n$ th root of 1, where  $n$  is the exponent of  $G$ . Since the Galois group  $I_n(K)$  of  $K(\epsilon)$  over  $K$  is abelian, it has a unique  $p$ -Sylow subgroup, and hence there exists a uniquely determined field  $F$  such that

$$K = K(\chi) \subset F \subset K(\epsilon)$$

with  $(K(\epsilon) : F)$  equal to the  $p$ -part of  $(K(\epsilon) : K)$ . By Lemma 70.25, there exists an  $F$ -elementary subgroup  $H$  of  $G$  at a prime  $q$  (where possibly  $q \neq p$ ) and an irreducible  $\Omega$ -character  $\xi$  of  $H$  lying in  $F$  such that  $p \nmid (\chi | H, \xi)$ .

Now we set

$$\theta = m_K(\chi)\chi = m_K(\chi)sp_K(\chi).$$

From Theorems (70.12) and (70.15) (see also Exercise 70.2), it follows that  $\theta$  is an irreducible  $K$ -character of  $G$ . By Corollary 70.21,  $\theta | H$  contains  $\xi$  with multiplicity a multiple of  $m_K(\xi)$ . Therefore we have

$$(70.29) \quad m_K(\xi) \mid m_K(\chi)(\chi | H, \xi)$$

where  $m_K(\xi)$  is a power of  $q$  and  $p \nmid (\chi | H, \xi)$ .

Now we investigate the character  $\xi$  more closely. Since  $\xi$  lies in  $F$ , Theorem 70.12 implies that  $m_F(\xi)\xi$  is an  $F$ -character of  $H$ . It also follows from (70.12) that  $m_F(\xi) \mid m_K(\xi)$ , and hence  $m_K(\xi)\xi$  is an  $F$ -character of  $H$ . Hence  $m_K(\xi)\xi^G$  is an  $F$ -character of  $G$ . By Corollary 70.21 and the Frobenius reciprocity theorem, we have

$$(70.30) \quad (m_K(\xi)\xi^G, \chi) = m_K(\xi)(\xi^G, \chi) = m_K(\xi)(\xi, \chi | H) \equiv 0 \pmod{m_F(\chi)}.$$

By Theorem 70.12, the  $\Omega$ -representation which affords  $\chi$  is realizable in a field  $E \supset F$  such that  $(E : F) = m_F(\chi)$ . From (70.30) we then have

$$(E : F) \mid m_K(\xi)(\xi, \chi | H)$$

and hence

$$(E : K) \mid m_K(\xi)(\xi, \chi | H)(F : K).$$

But by Theorem 70.12,  $m_K(\chi) \mid (E : K)$ , and since  $(\xi, \chi | H)(F : K) \not\equiv 0 \pmod{p}$ , we conclude that the  $p$ -part of  $m_K(\chi)$  divides  $m_K(\xi)$ . Since  $m_K(\xi)$  is a power of  $q$  and  $p \nmid m_K(\chi)$ , this shows that  $q = p$ . Returning to (70.29), we now deduce that  $m_K(\xi) \mid m_K(\chi)$  since  $p \nmid (\chi | H, \xi)$ . We have established that  $m_K(\xi)$  is the  $p$ -part of  $m_K(\chi)$ , and the proof of Theorem 70.28 is completed.

As we have pointed out, Theorem 70.28 reduces the problem of finding the Schur indices for  $G$  to the corresponding problem for certain solvable subgroups of  $G$ , namely the  $F$ -elementary subgroups. From the proof of the theorem, it is clear that the field  $F$  can be constructed independently of the particular irreducible  $\Omega$ -character  $\chi$  we are studying at the time.

The complete theory of Schur indices for  $F$ -elementary groups does not seem to have been given. For a nilpotent group  $G$ , Roquette [2] has proved that the Schur index  $m_K(\chi)$  of an irreducible  $\Omega$ -character  $\chi$  of  $G$  is 1 if  $2 \nmid [G : 1]$ , and is either 1 or 2 if  $2 \mid [G : 1]$ . The example given earlier in this section shows that the case  $m_K(\chi) = 2$  can actually occur.

Further results on the Schur index may be found in Schur's paper [3]. A related investigation concerned with the characters of  $G$  lying in the real field has been carried out in an interesting series of papers by Frobenius and Schur [1], Frame [1], and Mackey [2], and Fong [3].

### Exercises

1. Prove that if  $U$  is an irreducible representation of  $G$  in the complex field, then  $m_k(U) \mid [G : 1]$  for any subfield  $k$  of the complex field. [Hint: Use (iv) of Theorem 70.12.]

2. (Schur.) Let  $E$  be a splitting field for  $G$  which is a finite normal extension of the rational field  $Q$ , and let  $\{\chi_1, \dots, \chi_r\}$  be the irreducible  $E$ -characters of  $G$ . Let  $K$  be a subfield of  $E$ . We have already shown in Theorem 70.15 that if  $\theta$  is an irreducible  $K$ -character, then  $\theta = m_K(\chi_i)(\chi_i + \chi_i^\sigma + \dots)$  where the  $\{\chi_i^\sigma\}$  are the distinct conjugates of  $\chi_i$ . Prove conversely that, if  $\{\chi_j, \chi_j^\sigma, \dots\}$  are the distinct conjugates of any irreducible  $E$ -character  $\chi_j$ , then  $\zeta = m_K(\chi_j)(\chi_j + \chi_j^\sigma + \dots)$  is an irreducible  $K$ -character of  $G$ . Thus the knowledge of the  $\{\chi_i\}$ , together with their Schur indices over  $K$ , is sufficient to construct all the irreducible  $K$ -characters of  $G$ .

### § 71. Separable Algebras

In § 69 we proved that if  $E$  is a finite separable extension field of  $K$  and if  $A$  is a semi-simple algebra over  $K$ , then  $A^E = A \otimes_K E$  is a semi-simple algebra. In this section, we shall characterize those algebras  $A$  over  $K$  such that  $A^E$  is semi-simple for every extension field  $E$  of  $K$ . The main result we shall obtain is due to D. G. Higman [5] and is used in the theory of integral representations presented in Chapter XI.

(71.1) **DEFINITION.** An algebra  $A$  over a field  $K$  is called a *separable algebra* (over  $K$ ) if  $A^E = A \otimes_K E$  is a semi-simple algebra over  $E$  for every extension field  $E$  of  $K$ . In particular  $A^K \cong A$  must be semi-simple if  $A$  is separable.

(71.2) **THEOREM.** An algebra  $A$  over  $K$  is separable if and only if there exists an extension field  $E$  of  $K$  such that  $A^E$  is isomorphic to a direct sum of full matrix algebras over  $E$ .

**PROOF.** First let  $A$  be separable over  $K$ , and let  $E$  be an algebraically closed field containing  $K$ . Then by Definition 71.1,  $A^E$  is semi-simple; hence

$$A^E \cong A^{(1)} + \cdots + A^{(s)}$$

where the  $\{A^{(i)}\}$  are finite-dimensional simple algebras over the algebraically closed field  $E$ . By the results of § 27, each  $A^{(i)} \cong E_{n_i}$  for some integer  $n_i > 0$ , and we have proved the “only if” part of the theorem.

Conversely, suppose that for some extension field  $E$  of  $K$ , we have

$$(71.3) \quad A^E \cong E_{n_1} + \cdots + E_{n_s}$$

for some positive integers  $n_1, \dots, n_s$ . Let  $F$  be an arbitrary extension field of  $K$ ; we have to prove that  $A^F$  is semi-simple. First, we show that there exists a common extension field  $FE$  of both  $F$  and  $E$ . In fact, let  $F \otimes_K E$  be the tensor product algebra of  $F$  and  $E$ . The fields  $F$  and  $E$  may be identified with subfields  $F \otimes 1$  and  $1 \otimes E$  of  $F \otimes_K E$ . By the maximum principle (§ 15), there exists a maximal ideal  $M$  of  $F \otimes_K E$ . Then  $(F \otimes_K E)/M$  is a field  $FE$ . Moreover the natural homomorphism of  $F \otimes_K E$  onto  $FE$  maps both  $F$  and  $E$  isomorphically onto subfields of  $FE$ . Thus, after the identifications have been made,  $FE$  can be viewed as a common extension field of  $F$  and  $E$ .

Now we are ready to prove that  $A^F$  is semi-simple. From (71.3), we obtain

$$A^{FE} \cong (A^E)^{FE} \cong E_{n_1}^{FE} + \cdots + E_{n_s}^{FE} \cong (FE)_{n_1} + \cdots + (FE)_{n_s}$$

consequently  $A^{FE}$  is a semi-simple algebra. On the other hand,

$$(71.4) \quad A^{FE} \cong (A^F)^{FE} \cong (A \otimes_K F) \otimes_F FE.$$

If  $A^F$  is not semi-simple, then  $A^F$  has a non-zero nilpotent ideal, and it follows from (71.4) that  $A^{FE}$  also has a non-zero nilpotent ideal, contrary to the fact that  $A^{FE}$  is semi-simple. Therefore  $A^F$  is semi-simple, and Theorem 71.2 is proved.

Theorem 71.2 has the disadvantage that in order to use it to decide whether an algebra  $A$  is separable, it is necessary to consider algebras  $A^E$  for extension fields  $E$  of  $K$ , just as in the original definition (71.1). The main purpose of this section is to give an *intrinsic* criterion for separability, so that separability can be decided in the original algebra  $A$  without passing to extensions  $A^E$ . For this we shall use the theory of Frobenius algebras from Chapter IX.

Let  $A$  be a Frobenius algebra over an arbitrary field  $K$ , and let  $f$  be an associative non-degenerate bilinear form on  $A$ . Let  $\{a_1, \dots, a_n\}$  and  $\{b_1, \dots, b_n\}$  be a pair of dual bases of  $A$  with respect to  $f$ , i.e.,  $f(a_i, b_j) = \delta_{ij}$ . Lemma 62.8 implies that for all  $a \in A$ , the element

$$c(a) = \sum_{i=1}^n b_i a a_i \in C(A),$$

where  $C(A)$  is the center of the algebra  $A$ .<sup>†</sup> Let us set

$$(71.5) \quad \Gamma(A) = \{ \sum b_i a a_i, a \in A \} = \{ c(a) : a \in A \}.$$

Then it is immediate that  $\Gamma(A)$  is an ideal in the center of  $A$ . It will be shown now that the ideal  $\Gamma(A)$  is independent of the choice of the form  $f$  and the dual bases  $\{a_i\}$  and  $\{b_i\}$ .

First, let  $\{a_i\}, \{b_i\}$  and  $\{a'_i\}, \{b'_i\}$  be two pairs of dual bases of  $A$  with respect to a fixed associative bilinear form  $f$ . Let

$$a'_i = \sum_j \xi_{ij} a_j, \quad b'_i = \sum_j \eta_{ij} b_j, \quad \xi_{ij}, \eta_{ij} \in K.$$

Then for fixed  $i$  and  $j$  we have

$$\begin{aligned} \delta_{ij} &= f(a'_i, b'_j) = f\left(\sum_k \xi_{ik} a_k, \sum_l \eta_{jl} b_l\right) \\ &= \sum_{k,l} \xi_{ik} \eta_{jl} f(a_k, b_l) = \sum_{k,l} \xi_{ik} \eta_{jl} \delta_{kl} \\ &= \sum_k \xi_{ik} \eta_{jk}. \end{aligned}$$

<sup>†</sup> The mapping  $c: A \rightarrow C$  will be referred to as the "Gaschütz-Ikeda operator" associated with  $f$ .

In terms of the matrices  $(\xi_{ij})$  and  $(\eta_{ij})$ , we have shown that

$${}^t(\xi_{ij})(\eta_{ij}) = I^{(n)}.$$

Now let  $a \in A$ . Then

$$\begin{aligned} \sum_i b'_i aa'_i &= \sum_i \left( \sum_j \eta_{ij} b_j \right) a \left( \sum_k \xi_{ik} a_k \right) \\ &= \sum_{j,k} \left( \sum_i \eta_{ij} \xi_{ik} \right) b_j a a_k \\ &= \sum_{j,k} \delta_{jk} b_j a a_k = \sum_j b_j a a_j. \end{aligned}$$

Now let  $f_1$  and  $f_2$  be non-degenerate associative bilinear forms on  $A \times A \rightarrow K$ . Then as we saw in the proof of Theorem 61.3, the mappings  $\theta_1$  and  $\theta_2$  defined by

$$\theta_i(y)x = f_i(x, y), \quad i = 1, 2,$$

are  $A$ -isomorphisms of  ${}_A A$  onto  $(A_A)^*$ . Therefore  $\theta_2^{-1}\theta_1$  is an  $A$ -automorphism of  ${}_A A$ , and we have

$$\theta_2^{-1}\theta_1 = c_R$$

for some invertible element  $c \in A$ . From this, we have  $\theta_1 = \theta_2 c_R$ , and for all  $x, y \in A$ , it follows that

$$f_1(x, y) = \theta_1(y)x = (\theta_2 c_R)(y)x = \theta_2(yc)x = f_2(x, yc).$$

Now let  $\{a_i\}$  and  $\{b_i\}$  be dual bases of  $A$  with respect to  $f_1$ . Then  $\{a_i\}$  and  $\{b_i c\}$  are dual bases with respect to  $f_2$ , and for all  $a \in A$ , we have

$$\sum b_i a a_i = \sum b_i c(c^{-1}a)a_i$$

Since  $c^{-1}A = A$ , our remarks show that  $\Gamma(A)$  is independent of the choice of the form  $f$  and the dual bases with respect to  $f$ .

(71.6) **THEOREM** (D. G. Higman [5]). *The following statements concerning a finite-dimensional algebra  $A$  over a field  $K$  are equivalent:*

(i)  *$A$  is a separable algebra.*

(ii)  *$A$  is a Frobenius algebra such that the ideal  $\Gamma(A)$  defined by (71.5) coincides with the center of  $A$ .*

(iii) *For some  $K$ -basis  $\{a_1, \dots, a_n\}$  of  $A$ , there exist elements  $a'_1, \dots, a'_n$  in  $A$  such that*

$$\sum_{i=1}^n a'_i a_i = 1,$$

and such that, for  $a \in A$ ,

$$a_i a = \sum_{j=1}^n \lambda_{ij}(a) a_j , \quad \lambda_{ij}(a) \in K$$

implies

$$aa'_i = \sum_{j=1}^n a'_j \lambda_{ji}(a) .$$

PROOF. Statement (i) implies (ii). Given that  $A$  is separable, we know by Theorem 71.2 that there exists an extension field  $E$  of  $K$  such that  $A \otimes_K E$  is a direct sum of full matrix algebras over  $E$ . We shall prove first of all that the statement (ii) holds for the algebra  $A \otimes_K E$  over  $E$ . Because  $A \otimes_K E$  is a direct sum of full matrix algebras over  $E$ ,  $A \otimes_K E$  has a basis over  $E$  consisting of matrix units  $\{e_{ij}^k\}$  where, for each  $k$ , the  $\{e_{ij}^k\}$  are the matrix units in the  $k$ th matrix algebra. The  $\{e_{ij}^k\}$  satisfy the multiplication rule

$$e_{ij}^k e_{pq}^r = \delta_{kr} \delta_{jp} e_{iq}^k .$$

Define a bilinear form  $f_B$  on  $A^E \times A^E \rightarrow E$  by its action on the basis elements as follows:

$$f_B(e_{ij}^k, e_{pq}^r) = \delta_{kr} \delta_{iq} \delta_{jp} .$$

It is clear that  $f_B$  is non-degenerate, and we shall prove the associative law  $f_B(xy, z) = f_B(x, yz)$ ,  $x, y, z \in A^E$ . We have

$$\begin{aligned} f_B(e_{ij}^k e_{qr}^p, e_{vw}^u) &= \delta_{kp} \delta_{jq} f_B(e_{ir}^k, e_{vw}^u) \\ &= \delta_{kp} \delta_{jq} \delta_{ku} \delta_{iw} \delta_{rv} \end{aligned}$$

whereas

$$\begin{aligned} f_B(e_{ij}^k, e_{qr}^p e_{vw}^u) &= \delta_{pu} \delta_{rv} f_B(e_{ij}^k, e_{qw}^p) \\ &= \delta_{pu} \delta_{rv} \delta_{kp} \delta_{iw} \delta_{jq} , \end{aligned}$$

and it is clear that the two expressions are equal for all choices of the indices.

From the properties of  $f_B$ , it follows by Theorem 61.3 that  $A \otimes_K E$  is a Frobenius algebra. For each basis element  $e_{ij}^k$ , define  $(e_{ij}^k)^* = e_{ji}^k$ ; then

$$f_B((e_{ij}^k)^*, e_{qr}^p) = 0$$

unless  $(e_{ij}^k)^*$  is the basis element  $(e_{qr}^p)^*$  paired with  $e_{qr}^p$ , and we have

$$f_B((e_{qr}^p)^*, e_{qr}^p) = 1 .$$

Therefore  $\{e_{ij}^k\}$  and  $\{(e_{ij}^k)^*\}$  form a pair of dual bases if we order the second basis in such a way that  $(e_{ij}^k)^*$  stands in the same position in the second basis as  $e_{ij}^k$  stands in the first. Now let  $b = \sum_t e_{11}^t \in A^E$ . Applying the averaging process to  $b$ , we obtain

$$\begin{aligned}\sum_{i,j,k} e_{ij}^k b e_{ji}^k &= \sum_{i,j,k,t} e_{ij}^k e_{11}^t e_{ji}^k \\ &= \sum_{i,j,k} e_{ij}^k e_{11}^k e_{ji}^k = \sum_{i,k} e_{ii}^k = 1.\end{aligned}$$

Therefore  $\Gamma(A^E)$  contains the identity element of  $A^E$ , and since  $\Gamma(A^E)$  is an ideal in the center of  $A^E$ , we have  $\Gamma(A^E) = C(A^E)$ .

Now we have to prove that (ii) holds also for the algebra  $A$  itself. Because  $A$  is semi-simple,  $A$  is a quasi-Frobenius algebra. In Exercise 61.3, we indicated that in fact  $A$  is a Frobenius algebra. We shall give a fuller account of the details here. By part (iv) of Theorem 61.3, it is sufficient to prove that for any left ideal  $L$  in  $A$ ,

$$(71.7) \quad (L : K) + (r(L) : K) = (A : K),$$

and a similar result for right ideals. Since  $A$  is semi-simple, we have  $L = Ae$  for some idempotent  $e$ , and  $r(L) = (1 - e)A$ . In order to prove (71.7), it is enough to show that  $(Ae : K) = (eA : K)$ . Let  $e = e_1 + \cdots + e_k$  where the  $e_i$  are primitive idempotents; then our problem reduces to proving that  $(e_i A : K) = (A e_i : K)$  for a primitive idempotent  $e_i$ . This has already been done in (61.12), and the proof of (71.7) is completed. The same argument proves the analogous statement for right ideals, and we have shown that  $A$  is a Frobenius algebra.

Let  $\phi$  be a non-degenerate associative bilinear form on  $A \times A \rightarrow K$ , and let  $\phi^E$  denote the extension of  $\phi$  to  $A^E$ . Let  $\{a_i\}, \{b_i\}$  be dual bases of  $A$  with respect to  $\phi$ ; then they are also dual bases of  $A^E$  with respect to  $\phi^E$ . By what has been proved, the equation

$$(71.8) \quad \sum_{i=1}^n b_i a_i = 1$$

has a solution for some  $a \in A^E$ , since  $\Gamma(A^E) = C(A^E)$ , and  $\Gamma(A^E)$  is independent of the choice of the bilinear form. The formula (71.8) is equivalent to the assertion that a certain system of linear equations with coefficients in  $K$  has a solution in  $E$ . It is well known that there must then also exist a solution in  $K$ . Therefore (71.8) has a solution  $a \in A$ , and it follows that  $\Gamma(A) = C(A)$ . This completes the

proof that (i) implies (ii).

The implication (ii)  $\rightarrow$  (iii) is obvious from the existence of an element  $a^* \in A$  such that  $\sum b_i a^* a_i = 1$ ; it is only necessary to take  $a'_i = b_i a^*$ ,  $1 \leq i \leq n$ .

Finally we have to prove that (iii) implies (i). Let  $E$  be an extension field of  $K$ ; we shall prove that every left  $A^E$ -module  $M$  is completely reducible. [For this argument, see also the proof of Theorem 69.4.] Let  $N$  be an  $A^E$ -submodule of  $M$ , and let  $\pi \in \text{Hom}_{A^E}(M, M)$  be a projection of  $M$  upon  $N$ . Let  $\pi'$  be the linear transformation of  $M$  defined by

$$\pi'(x) = \sum (a'_i \otimes 1)\pi(a_i \otimes 1)x, \quad x \in M.$$

Because of (iii), it follows as in the proof of Lemma 62.8 that  $\pi' \in \text{Hom}_{A^E}(M, M)$ . Moreover it is easily checked that  $\pi'$  is a projection on  $M$  upon  $N$ . Therefore  $N$  is an  $A^E$ -component of  $M$ , and  $M$  is completely reducible. This completes the proof of the theorem.

(71.9) COROLLARY. *A finite algebraic extension field  $E$  of  $K$  is a separable algebra over  $K$  if and only if  $E$  is a separable extension of  $K$  in the sense of Galois theory.*

PROOF. This result is immediate from Theorem 71.6 and the results of §69.

(71.10) THEOREM. *Let  $B$  be a semi-simple algebra and  $A$  a separable algebra over  $K$ . Then  $A \otimes_K B$  is semi-simple.*

Using Theorem 71.6, we can prove Theorem 71.10 by an argument wholly analogous to the proof of Theorem 69.4, and we shall leave this discussion as an exercise for the reader.

### Exercises

1. Prove that, if the group algebra  $KG$  of a finite group  $G$  over a field  $K$  is semi-simple, then  $KG$  is a separable algebra over  $K$ .
2. Let  $A$  be a semi-simple algebra over  $K$ , and let  $A = A_1 \oplus \cdots \oplus A_r$ , where the  $\{A_i\}$  are simple algebras over  $K$  with centers  $\{C_1, \dots, C_r\}$ , respectively. Prove that  $A$  is a separable algebra if and only if each field  $C_i$  is a separable extension field of  $K$ . [Hint: Use Exercises 69.1 and 69.2.]

## § 72. The Wedderburn-Malcev Theorem

We shall conclude this chapter with an application of the theory of separable algebras. Our presentation follows closely a paper of

Hochschild [1] in which the Levi-Malcev theorem for Lie algebras was also treated by the same method. The results in this section seem to be the origin of the cohomology theory of associative algebras (Hochschild [2], Cartan-Eilenberg [1].)

We begin with some elementary remarks concerning an algebra  $A$  over a field  $K$ , and left  $A$ -modules  $M$ . Throughout this section, as before,  $A$  and  $M$  are assumed to be finite dimensional over  $K$ . We shall omit some of the computations, which the reader may easily fill in for himself.

(72.1) **DEFINITION.** A left  $A$ -module  $U$  is called an *extension* of  $M$  if there exists an  $A$ -homomorphism  $\phi$  of  $U$  onto  $M$ . The kernel of  $\phi$  is called the *kernel of the extension*. The extension

$$\phi: U \rightarrow M$$

is called a *split extension* if the kernel of  $\phi$  is an  $A$ -direct summand of  $U$ .

(72.2) **LEMMA.** Let  $\phi: U \rightarrow M$  be an extension of  $M$  with kernel  $N$ . The extension is a split extension if and only if there exists an  $A$ -homomorphism  $\psi$  of  $M$  into  $U$  such that  $\phi\psi = 1$ .

**PROOF.** If  $U$  is a split extension of  $M$ , then  $U = N \oplus M'$  for some  $A$ -submodule  $M'$  of  $U$ . Then  $\phi$  maps  $M'$  isomorphically upon  $M$ ; for each  $m \in M$ , we may let  $\psi(m)$  be the uniquely determined element in  $M'$  such that  $\phi(\psi(m)) = m$ . Then  $\psi: M \rightarrow U$  is an  $A$ -homomorphism with the required property.

The proof of the converse is the same as the argument following Definition 7.4 in Chapter I, and we shall omit the details.

Now let  $\phi: U \rightarrow M$  be an arbitrary extension with kernel  $N$ , and let

$$T = \text{Hom}_K(M, N).$$

Then  $T$  becomes an  $(A, A)$ -bimodule if we define

$$(\tau a)m = \tau(am), \quad (a\tau)m = a(\tau m), \quad m \in M, \tau \in T, a \in A.$$

Let  $\psi$  be a  $K$ -homomorphism of  $M$  into  $U$  such that  $\phi\psi = 1$ ; the existence of  $\psi$  is clear since there exist  $K$ -subspaces of  $U$  complementary to  $N$ . Now we define  $f \in \text{Hom}_K(A, T)$  by

$$(72.3) \quad f(a)m = \psi(am) - a\psi(m), \quad a \in A, m \in M.$$

Roughly speaking,  $f$  measures the extent to which  $\psi$  misses being an  $A$ -homomorphism. We note first that  $f(a)m$  is indeed an element

of  $N$  because for all  $a \in A$  and  $m \in M$  we have

$$\begin{aligned}\phi(f(a)m) &= (\phi\psi)am - \phi(a\psi(m)) \\ &= am - a(\phi\psi(m)) = 0.\end{aligned}$$

It is easily checked that  $f$  is a  $K$ -homomorphism and that in addition, we have

$$(72.4) \quad f(ab) = af(b) + f(a)b, \quad a, b \in A.$$

These remarks lead to the following definition:

(72.5) **DEFINITION.** Let  $T$  be an arbitrary  $(A, A)$ -bimodule. A  $K$ -homomorphism  $f: A \rightarrow T$  is called a *generalized derivation* if

$$f(ab) = af(b) + f(a)b, \quad a, b \in A.$$

For any fixed  $t \in T$ , the function  $f: A \rightarrow T$  defined by

$$(72.6) \quad f(a) = at - ta, \quad a \in A,$$

is a generalized derivation called an *inner generalized derivation*.

We leave it to the reader to check that (72.6) does indeed define a generalized derivation. The connection between these ideas and extensions of modules is given by the following lemma:

(72.7) **LEMMA.** Let  $\phi: U \rightarrow M$  be an extension of a left  $A$ -module  $M$  with kernel  $N$ , and let  $\psi: M \rightarrow U$  be a  $K$ -homomorphism such that  $\phi\psi = 1$ . The extension  $\phi: U \rightarrow M$  is a split extension if and only if the generalized derivation

$$f: A \rightarrow T = \text{Hom}_K(M, N)$$

given by (72.3) is inner.

**PROOF.** First, suppose that  $f$  is inner. Then there exists an element  $\tau \in T$  such that

$$f(a) = a\tau - \tau a, \quad a \in A.$$

Define a new  $K$ -homomorphism  $\psi': M \rightarrow U$  by the rule

$$\psi'(m) = \psi(m) + \tau(m), \quad m \in M.$$

Then  $\phi\psi' = 1$  since  $\phi\psi = 1$  and  $\phi\tau = 0$ . Moreover for all  $a \in A$  we have

$$\begin{aligned}(72.8) \quad \psi'(am) &= \psi(am) + \tau(am) \\ &= a\psi(m) + f(a)m + (\tau a)m \\ &= a\psi(m) + (a\tau - \tau a)m + (\tau a)m \\ &= a\psi(m) + a\tau(m) = a\psi'(m).\end{aligned}$$

Therefore  $\phi' \in \text{Hom}_A(M, U)$ , and, by Lemma 72.2,  $\phi: U \rightarrow M$  is a split extension.

Conversely, suppose there exists an  $A$ -homomorphism  $\psi^*: M \rightarrow U$  such that  $\phi\psi^* = 1$ . Define  $\tau \in T$  by setting

$$\tau(m) = \psi^*(m) - \phi(m).$$

Then  $\phi\tau = 0$  so that  $\tau(m)$  is in  $N$  as we claim. Moreover, for all  $a \in A$  we have, by reversing the argument (72.8), the result that

$$f(a)m = \psi(am) - a\psi(m) = (a\tau - \tau a)m,$$

and this lemma is proved.\*

A second extension problem which arises naturally in the theory of algebras is described in the following definition:

(72.9) DEFINITION. Let  $B$  be a finite-dimensional algebra, let  $\phi: B \rightarrow A$  be a homomorphism of  $B$  onto an algebra  $A$ , and let  $N$  be the kernel of  $\phi$ . Then  $B$  is called an *extension* of  $A$  with kernel  $N$  [cf. Definition 7.4]. The extension  $\phi: B \rightarrow A$  is called a *split extension* if there exists an algebra homomorphism  $\psi$  of  $A \rightarrow B$  such that  $\phi\psi = 1$ .

As in the case of extensions of modules and groups [see (72.2) and the discussion following (7.4)], the following result is easily proved:

(72.10) LEMMA. *Let  $\phi: B \rightarrow A$  be an extension of  $A$  with kernel  $N$ . The extension is a split extension if and only if there exists a subalgebra  $A_1$  of  $B$  such that  $B$  is the semi-direct sum of  $A_1$  and  $N$  in the sense that*

$$B = A_1 \oplus N \quad (\text{vector space direct sum}).$$

*Remark.* We point out that, if  $B$  is the semi-direct sum of a subalgebra  $A_1$  and a two-sided ideal  $N$ , it does not necessarily follow that  $A_1N = 0$  or that  $A_1$  is an ideal in  $B$ .

As in the case of modules, we can in certain cases associate with an extension  $\phi: B \rightarrow A$  a function from  $A$  to an  $(A, A)$ -bimodule. Let  $\psi$  be a  $K$ -homomorphism of  $A \rightarrow B$  such that  $\phi\psi = 1$ . Then, again letting  $N$  be the kernel of  $\phi$ , the equation

$$(72.11) \quad f(a, b) = \psi(ab) - \psi(a)\psi(b), \quad a, b \in A,$$

defines a bilinear function  $f: A \times A \rightarrow N$  which measures the extent

---

\* The reader should compare this result and the concept of generalized derivations with their analogues in §73.

to which  $\phi$  fails to be an algebra homomorphism. Besides being bilinear,  $f$  satisfies another condition which is a consequence of the associative law. We have from (72.11)

$$\begin{aligned}\phi((ab)c) &= \phi(ab)\phi(c) + f(ab, c) \\ &= \phi(a)\phi(b)\phi(c) + f(a, b)\phi(c) + f(ab, c)\end{aligned}$$

whereas

$$\begin{aligned}\phi(a(bc)) &= \phi(a)\phi(bc) + f(a, bc) \\ &= \phi(a)\phi(b)\phi(c) + \phi(a)f(b, c) + f(a, bc).\end{aligned}$$

Subtracting, we have

$$f(ab, c) - f(a, bc) + f(a, b)\phi(c) - \phi(a)f(b, c) = 0.$$

We are ready to define the function  $f$  abstractly as soon as we can make  $N$  into an  $(A, A)$ -bimodule in which the operations are defined by

$$na = n\phi(a)$$

and

$$an = \phi(a)n, \quad n \in N, a \in A.$$

This does not make  $N$  into an  $(A, A)$ -bimodule except under special conditions. A sufficient condition for these definitions to make  $N$  into an  $(A, A)$ -bimodule is that  $N^2 = 0$ . For in that case

$$\begin{aligned}(na)b - n(ab) &= (n\phi(a))\phi(b) - n\phi(ab) \\ &= -nf(a, b) = 0\end{aligned}$$

if  $N^2 = 0$ , since  $f(a, b) \in N$ .

The next definition is motivated by what has been said, together with the easily worked out condition in terms of  $f$  for the extension to be split in the special case  $N^2 = 0$ .

(72.12) **DEFINITION.** Let  $A$  be an algebra over  $K$  and  $N$  an  $(A, A)$ -bimodule. A bilinear function  $f: A \times A \rightarrow N$  is called a *factor set* provided that

$$(72.13) \quad f(ab, c) - f(a, bc) + f(a, b)c - af(b, c) = 0$$

for all  $a, b, c$  in  $A$ . The factor set  $f$  is called a *split factor set* provided that there exists a linear transformation  $F: A \rightarrow N$  such that for all  $a$  and  $b$ ,

$$(72.14) \quad f(a, b) = aF(b) - F(ab) + F(a)b.$$

(72.15) **LEMMA.** *Let  $\phi: B \rightarrow A$  be an extension whose kernel  $N$  has the property that  $N^2 = 0$ , and let  $f$  be the factor set defined by (72.11) relative to a vector space homomorphism  $\psi: A \rightarrow B$  such that  $\phi\psi = 1$ . Then  $f$  is a split factor set if and only if the extension is a split extension.*

The proof is entirely analogous to the proof of Lemma 72.2 and will be omitted.

Now we come to an important property of separable algebras.

(72.16) **THEOREM.** *Let  $A$  be a separable algebra over a field  $K$ . Then every generalized derivation is inner and every factor set defined on  $A$  is a split factor set.*

**PROOF.** The proof is based entirely on statement (iii) of Theorem 71.6. We are given a basis  $\{a_1, \dots, a_n\}$  of  $A$  together with a set of elements  $\{a'_1, \dots, a'_n\}$  in  $A$  such that

$$(72.17) \quad a'_i a_i = 1$$

and for all  $a \in A$ ,

$$(72.18) \quad a_i a = \sum_{j=1}^n \lambda_{ij}(a) a_j, \quad \lambda_{ij}(a) \in K, \quad \text{implies} \quad a a'_i = \sum_{j=1}^n a'_j \lambda_{ji}(a).$$

First, let  $f: A \rightarrow T$  be a generalized derivation of  $A$ , and let  $t = \sum a'_i f(a_i)$ . Then, using (72.4), (72.17), and (72.18), we obtain the result that for all  $a \in A$ ,

$$\begin{aligned} at - ta &= \sum a a'_i f(a_i) - \sum a'_i f(a_i) a \\ &= \sum a a'_i f(a_i) - \sum a'_i f(a_i a) + (\sum a'_i a_i) f(a) \\ &= f(a). \end{aligned}$$

Thus  $f$  is an inner generalized derivation.

Now let  $h$  be a factor set, and let  $F$  be the linear mapping of  $A$  into the given  $(A, A)$ -bimodule defined by

$$F(a) = \sum h(a, a'_i) a_i.$$

Then, applying (72.13) to the first summand below and (72.17) and (72.18) later on, we have

$$\begin{aligned} aF(b) - F(ab) + F(a)b &= \sum ah(b, a'_i) a_i - \sum h(ab, a'_i) a_i + \sum h(a, a'_i) a_i b \\ &= \sum h(ab, a'_i) a_i - \sum h(a, ba'_i) a_i + \sum h(a, b)a'_i a_i \\ &\quad - \sum h(ab, a'_i) a_i + \sum h(a, a'_i) a_i b \\ &= h(a, b), \end{aligned}$$

and we have proved that  $h$  is a split factor set. This completes the proof of Theorem 72.16.

(72.19) **THEOREM (Wedderburn-Malcev).** *Let  $B$  be a finite-dimensional algebra over a field  $K$  with radical  $N$  such that the residue class algebra  $A = B/N$  is separable. Then there exists a semi-simple subalgebra  $S$  of  $B$  such that  $B$  is the semi-direct sum of  $S$  and  $N$ . If  $S_1$  and  $S_2$  are subalgebras such that  $B = S_i \oplus N$ ,  $i = 1, 2$ , then there exists an element  $n \in N$  such that  $S_1 = (1 - n)S_2(1 - n)^{-1}$ .*

**PROOF.** We first prove the existence of at least one subalgebra  $S$ . We use induction on the dimension of  $B$ , assuming the truth of the first part of the theorem for all algebras of dimension less than the dimension of  $B$ . We may assume that  $N^2 \neq 0$ ; otherwise the assertion of the theorem is immediate from Theorem 72.16 and Lemma 72.15. Since  $N^2 \neq 0$ ,  $(B/N^2 : K) < (B : K)$ . The radical of  $B/N^2$  is  $N/N^2$ , since  $N/N^2$  is a nilpotent ideal and  $(B/N^2)/(N/N^2) \cong B/N = A$ , which is separable by assumption. Therefore we can apply our induction hypothesis, and conclude that there exists a subalgebra  $S_1$  of  $B$  such that

$$(72.20) \quad B = S_1 + N, \quad S_1 \cap N = N^2.$$

Since  $N \neq N^2$ ,  $S_1 \neq B$ . Moreover  $S_1/N^2 \cong A$ , so that the induction hypothesis can be applied to  $S_1$ , yielding a subalgebra  $S$  of  $S_1$  such that

$$(72.21) \quad S_1 = S + N^2, \quad S \cap N^2 = 0.$$

Combining (72.20) and (72.21), we obtain

$$B = S + N, \quad S \cap N = 0,$$

and the first part of the theorem is proved.

Now we prove Malcev's uniqueness assertion (Malcev [1]). Given the subalgebras  $S_1$  and  $S_2$ , there exist algebra homomorphisms  $\psi_1$  and  $\psi_2$  of  $A$  into  $B$  such that  $\phi\psi_1 = 1$  and  $\phi\psi_2 = 1$ , where  $\phi$  is the natural mapping of  $B \rightarrow A$ , and  $S_i = \psi_i(A)$ ,  $i = 1, 2$ . Because the  $\{\psi_i\}$  are algebra homomorphisms,  $N$  becomes an  $(A, A)$ -bimodule if we define

$$na = n\psi_2(a)$$

and

$$an = \psi_1(a)n.$$

Then consider the function  $f: A \rightarrow B$  defined by

$$f(a) = \psi_1(a) - \psi_2(a).$$

Since  $\phi\psi_i = 1$ ,  $i = 1, 2$ ,  $f(a) \in N$  for all  $a \in A$ , and we have,

$$\begin{aligned} f(ab) &= \psi_1(ab) - \psi_2(ab) \\ &= \psi_1(a)[\psi_1(b) - \psi_2(b)] + [\psi_1(a) - \psi_2(a)]\psi_2(b) \\ &= af(b) + f(a)b, \end{aligned} \quad a, b \in A.$$

Therefore  $f$  is a generalized derivation, and by Theorem 72.16 there exists an element  $n \in N$  such that

$$f(a) = \psi_1(a) - \psi_2(a) = an - na = \psi_1(a)n - n\psi_2(a), \quad a \in A.$$

Rewriting this equation, we have

$$\psi_1(a)[1 - n] = [1 - n]\psi_2(a), \quad a \in A.$$

Since  $n$  is a nilpotent element,  $1 - n$  is invertible. Therefore we have

$$\psi_1(a) = (1 - n)\psi_2(a)(1 - n)^{-1}$$

for all  $a \in A$ . In other words

$$S_1 = (1 - n)S_2(1 - n)^{-1},$$

and Theorem 72.19 is proved.

### *Exercises*

1. Prove that if every generalized derivation of a finite-dimensional algebra  $A$  is inner, the algebra is separable. [Cf. Theorem 72.16.]
2. Let  $K$  be a perfect field; that is, every finite algebraic extension of  $K$  is separable in the sense of Galois theory. A linear transformation  $S$  on a vector space  $V$  over  $K$  is called completely reducible if  $V$  is a completely reducible  $K[S]$ -module. Prove that every linear transformation  $X$  of  $V$  over  $K$  can be expressed as a sum of a completely reducible linear transformation  $S$  and a nilpotent transformation  $N$ , such that both  $S$  and  $N$  belong to the algebra  $K[X]$  generated by  $X$ . Prove that, if  $X = S' + N'$  where  $S'$  and  $N'$  are completely reducible and nilpotent, respectively, and  $S'N' = N'S'$ , then  $S = S'$ ,  $N = N'$ . [Hint: Apply Theorem 72.19.]

## Integral Representations

Most of the theory of group representations so far developed in this book has dealt with the representations of some finite group  $G$  by matrices with entries in a field. In this chapter, on the other hand, we turn our attention to representations of  $G$  by matrices with entries in a ring  $R$ . The theory of such representations is greatly complicated by the fact that the group ring  $RG$  usually fails to satisfy the minimum condition, and as a consequence, several of the most useful theorems on representations in a field no longer hold. In particular, the Jordan-Hölder and Krull-Schmidt theorems both fail for  $RG$ -modules, and Maschke's theorem also breaks down. As a result, the entire theory of  $RG$ -modules has remained a vast area of unsolved problems and conjectures, and only recently have some general theorems and methods begun to emerge. It is our purpose here to give the main results so far obtained.

The first section will introduce for the special case of  $Z$ -representations of a finite group  $G$ , those ideas which play a basic role throughout the remainder of the chapter. The results of this section carry over unchanged to the case of  $R$ -representations of  $G$ , where  $R$  is a principal ideal domain, but only in one place [Theorem 73.6] have we stated the corresponding results explicitly.

In the second section, we shall work out explicitly a full set of inequivalent  $Z$ -representations of a cyclic group of prime order. Indeed, one of the outstanding problems in the theory of integral representations is to do the same for more complicated groups.

The framework for the rest of the chapter is established in § 75. In it we pass from the group ring  $RH$  of a finite group  $H$  to an operator domain which is an  $R$ -order in an algebra  $A$  over the quotient field  $K$  of  $R$ , and we show that when  $A$  is a separable algebra over  $K$ , there is an ideal in  $R$  which plays the same role as does the group order  $[H : 1]$  in the group ring case.

Maranda's theory of  $P$ -integral equivalence occupies our attention in § 76. His results are applied in the next section, where we obtain Swan's theorems on projective  $RG$ -modules,  $R$  a valuation ring. Swan's global theory of projective  $RG$ -modules ( $R = \text{alg. int. } \{K\}$ ,

$K = \text{algebraic number field}$ ) is taken up in § 78.

Finally, § 79 is devoted to proving the Jordan-Zassenhaus theorem. The chapter concludes with Maranda's theory of genus and related results. A brief appendix deals with the problem of the finiteness of the number of indecomposable  $Z$ -representations of a finite group.

This chapter has been written in a somewhat simpler style than the immediately preceding chapters, in order that it may be read independently of them. The results of Chapter II and III are used freely here, those of Chapter IV occasionally, and those of Chapter V–X almost not at all. However, in §§77–78 we shall need some of the elementary facts on projective modules obtained in § 56.

### § 73. Introduction

We shall be concerned here with representations of a finite group  $G$  by matrices with entries in  $Z$ , or equivalently, with  $ZG$ -modules having finite  $Z$ -bases. For the remainder of this section, a  $ZG$ -module will always mean a left  $ZG$ -module having a finite  $Z$ -basis. Later in this chapter, we shall treat a more general situation in which  $ZG$  is replaced by a more general type of operator domain. The basic definitions will be better understood, however, if we meet them first for this special case.

(73.1) DEFINITION. Two  $Z$ -representations  $T, U$  of  $G$  are  $Q$ -equivalent (notation:  $T \sim_Q U$ ) if  $T$  and  $U$  are intertwined by a non-singular matrix  $S$  with entries in  $Q$ ; that is,

$$(73.2) \quad T(g) = S^{-1}U(g)S, \quad g \in G.$$

We shall call a square matrix  $S$  unimodular over  $Z$  if  $S$  has entries in  $Z$  and  $\det(S)$  is a unit in  $Z$ . Thus  $S$  is unimodular over  $Z$  if and only if  $S^{-1}$  exists and both  $S, S^{-1}$  have entries in  $Z$ .

(73.3) DEFINITION. Two  $Z$ -representations  $T, U$  of  $G$  are  $Z$ -equivalent ( $T \sim_Z U$ ) if they are intertwined by a matrix unimodular over  $Z$ .

Obviously,  $Z$ -equivalence implies  $Q$ -equivalence. The converse is false, as we may see by the following example. Let  $G$  be cyclic, generated by an element  $g$  of order  $n$ . To specify a matrix representation  $T$  of  $G$ , it suffices to give a matrix  $T(g)$  for which  $(T(g))^n = I$ . Two  $Z$ -representations  $T, U$  of  $G$  are  $Z$ -equivalent if and only if

$$(73.4) \quad T(g) = S^{-1}U(g)S \quad g \in G,$$

for some  $S$  unimodular over  $Z$ , whereas  $T \sim_Q U$  if (73.4) holds for

some  $S$  non-singular over  $Q$ . For the special case where  $n = 2$ , set

$$\mathbf{T}(g) = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad \mathbf{U}(g) = \begin{pmatrix} 1 & 1 \\ 0 & -1 \end{pmatrix}.$$

Then we find readily that  $\mathbf{T} \sim_0 \mathbf{U}$ , but  $\mathbf{T}, \mathbf{U}$  are not  $Z$ -equivalent.

Switching to  $ZG$ -modules, let us pick a  $ZG$ -module  $M$ . Relative to a  $Z$ -basis,  $M$  affords a  $Z$ -representation of  $G$ . Any two  $Z$ -bases of  $M$  are connected by a matrix which is unimodular over  $Z$ ; this matrix intertwines the representations afforded by use of these bases. Hence, each  $ZG$ -module affords a set of mutually  $Z$ -equivalent  $Z$ -representations of  $G$ .

On the other hand, every  $Z$ -representation of  $G$  is also a  $Q$ -representation. Thus we may reasonably expect that with each  $ZG$ -module  $M$  there should be associated, in some natural manner, a  $QG$ -module  $M^*$  with the property that all the  $Z$ -representations afforded by  $M$  should be among the  $Q$ -representations afforded by  $M^*$ . We have already seen (§ 22) how to construct such an  $M^*$  in a canonical way. The module  $M^*$  can be defined by

$$M^* = Q \otimes_{\mathbb{Z}} M$$

with the action of  $G$  on  $M^*$  given by

$$g(\sum \alpha_i \otimes m_i) = \sum \alpha_i \otimes gm_i, \quad g \in G, \alpha_i \in Q, m_i \in M.$$

If  $\{m_1, \dots, m_r\}$  is a  $Z$ -basis of  $M$ , the elements

$$1 \otimes m_1, \dots, 1 \otimes m_r$$

form a  $Q$ -basis of  $M^*$ , relative to which  $M^*$  affords the same  $Z$ -representation of  $G$  as does  $M$  relative to  $\{m_1, \dots, m_r\}$ . Therefore the  $Q$ -representations afforded by  $M^*$  include all  $Z$ -representations afforded by  $M$ . Of course,  $M^*$  also affords  $Q$ -representations which are not  $Z$ -representations. We note finally that the  $Z$ -rank ( $M : Z$ ) of  $M$ , which is by definition  $(M^* : Q)$ , equals the maximal number of  $Z$ -free elements of  $M$ .

For convenience, we identify  $1 \otimes m_i$  with  $m_i$ , and regard  $M$  as embedded in  $M^*$ . We then write  $M = Zm_1 \oplus \dots \oplus Zm_r$ ,  $M^* = Qm_1 \oplus \dots \oplus Qm_r$ . If  $QM$  denotes the set of  $Q$ -linear combinations of the elements of  $M$ , then  $M^* = QM$ . Note also that  $M$  determines  $M^*$  uniquely (up to  $QG$ -isomorphism).

In the other direction, we have

(73.5) THEOREM. *Every  $QG$ -module  $M^*$  with finite  $Q$ -basis contains a  $ZG$ -submodule  $M$  such that  $M^* = QM$  and  $(M : Z) = (M^* : Q)$ . In*

other words, every  $Q$ -representation of  $G$  is  $Q$ -equivalent to a  $Z$ -representation of  $G$ .

**PROOF.** Let  $\{m_1^*, \dots, m_r^*\}$  be a  $Q$ -basis for  $M^*$ , and define

$$M = \sum_{g \in G} \sum_{j=1}^r Zgm_j^* .$$

Then  $M$  is a finitely generated torsion-free  $Z$ -module and hence has a finite  $Z$ -basis. Since each  $m_j^* \in M$ , we deduce at once that  $QM = M^*$  and  $(M^* : Q) = (M : Z)$ . Obviously  $GM \subset M$ .

*Caution:*  $M^*$  does not determine  $M$  uniquely, not even up to  $ZG$ -isomorphism, for such uniqueness would imply that two  $Z$ -representations of  $G$  which were  $Q$ -equivalent would necessarily be  $Z$ -equivalent, and we have already seen that this is false.

In our later work, it will be convenient to have a generalization of the preceding theorem.

(73.6) **THEOREM.** *Let  $R$  be a principal ideal domain with quotient field  $K$ . Then every  $K$ -representation of  $G$  is  $K$ -equivalent to an  $R$ -representation of  $G$ . In other words, every  $KG$ -module  $M^*$  with a finite  $K$ -basis contains an  $RG$ -submodule  $M$  such that  $M^* = KM$  and  $(M : R) = (M^* : K)$ .*

**PROOF.** Let  $\{m_1^*, \dots, m_r^*\}$  be a  $K$ -basis of  $M^*$ , and set

$$M = \sum_{g \in G} \sum_{j=1}^r Rgm_j^* .$$

The reasoning of the preceding proof carries over to this case, and the result follows.

Let the  $Z$ -module  $M$  having a finite  $Z$ -basis be embedded in the  $Q$ -space  $M^* = QM (= Q \otimes_Z M)$ . Any  $Z$ -submodule  $N$  of  $M$  will also have a finite  $Z$ -basis, and we have

$$(N : Z) = (QN : Q) .$$

Thus  $QN = M^*$  if and only if  $(N : Z) = (M : Z)$ .

We had defined (§ 16)  $N$  to be a *pure*  $Z$ -submodule of  $M$  if  $\alpha N = N \cap \alpha M$ ,  $\alpha \in Z$ , and showed in (16.17) that  $N$  is a pure  $Z$ -submodule of  $M$  if and only if every  $Z$ -basis of  $N$  can be completed to a  $Z$ -basis of  $M$ . (Alternately,  $N$  is pure if and only if  $N$  is a  $Z$ -direct summand of  $M$ .) We shall frequently use the following fact: If  $V$  is any  $Q$ -subspace of  $QM$ , then  $V \cap M$  is a pure  $Z$ -submodule of  $M$  such that  $Q(V \cap M) = V$ .

(73.7) **DEFINITION.** A  $ZG$ -module  $M$  is *decomposable* if it is ex-

pressible as a direct sum of two non-zero submodules; otherwise, it is *indecomposable*.

The previous definition of reducibility must be modified, however, since each non-zero  $ZG$ -module  $M$  contains non-trivial submodules  $2M$ ,  $3M$ , etc. A new definition is suggested by the following matrix considerations:

(73.8) DEFINITION. A  $Z$ -representation  $\mathbf{T}$  (of  $G$ ) is  *$Z$ -reducible* if

$$\mathbf{T} \sim_z \begin{pmatrix} * & * \\ 0 & * \end{pmatrix}.$$

Analogously, a  $ZG$ -module  $M$  is  *$Z$ -reducible* if it contains a non-zero  $ZG$ -submodule of smaller  $Z$ -rank. A non-zero  $ZG$ -module which is not reducible is called  *$Z$ -irreducible*.

Let  $M$  be a non-zero  $ZG$ -module, and set  $M^* = QM$ . If  $M$  contains a non-zero  $ZG$ -submodule  $N$  of lower  $Z$ -rank, then  $QN$  is a non-zero  $QG$ -submodule  $N$  of smaller  $Q$ -dimension. Hence if  $M$  is a reducible  $ZG$ -module, then  $QM$  is a reducible  $QG$ -module. Similarly, decomposability of  $M$  implies that of  $QM$ . (Both these remarks are trivial from the standpoint of matrix representations.)

The example given earlier in this section shows that a  $Z$ -representation may be  $Q$ -decomposable but  $Z$ -indecomposable. For reducibility, however, the key result is

(73.9) THEOREM. A  $ZG$ -module  $M$  is  *$Z$ -reducible if and only if  $QM$  is reducible (as  $QG$ -module).*

PROOF. Let  $V$  be a proper  $QG$ -submodule of  $QM$ ,  $V \neq (0)$ . Then  $V \cap M$  is a non-zero  $ZG$ -submodule of  $M$  of smaller  $Z$ -rank; hence  $M$  is  *$Z$ -reducible*. This proves the result.

In the above proof,  $V \cap M$  is a pure  $Z$ -submodule of  $M$ , and so any  $Z$ -basis of  $V \cap M$  may be completed to a  $Z$ -basis of  $M$ . Thus, any  $Z$ -representation of  $M$  is  $Z$ -equivalent to a reduced representation of the form

$$\begin{pmatrix} \mathbf{T}_1 & * \\ 0 & \mathbf{T}_2 \end{pmatrix}$$

where  $V \cap M$  affords  $\mathbf{T}_1$  and  $M/(V \cap M)$  affords  $\mathbf{T}_2$ .

More generally, let  $M$  be a  $ZG$ -module, and suppose that we are given any composition series for  $M^*$  ( $= QM$ ), say.

$$(73.10) \quad M^* = M_k^* \supset M_{k-1}^* \supset \cdots \supset M_1^* \supset M_0^* = (0).$$

We have seen in §13 that upon adapting a  $Q$ -basis of  $M^*$  to this

composition series,  $M^*$  affords a  $Q$ -representation

$$\begin{pmatrix} U_1 & & * \\ & U_2 & \\ 0 & \ddots & \ddots \\ & & U_k \end{pmatrix}$$

where for each  $i$ ,  $1 \leq i \leq k$ ,  $U_i$  is an irreducible matrix representation of  $G$  afforded by  $M_i^*/M_{i-1}^*$ . Now define

$$M_i = M_i^* \cap M, \quad 0 \leq i \leq k.$$

Then we have a chain

$$(73.11) \quad M = M_k \supset M_{k-1} \supset \cdots \supset M_1 \supset M_0 = (0)$$

about which we find [as in the proof of Theorem 73.9] that

- (i)  $M_{i-1}$  is a  $ZG$ -submodule of  $M_i$ ,
- (ii)  $M_{i-1}$  is a pure  $Z$ -submodule of  $M_i$ ,
- (iii)  $M_i/M_{i-1}$  is a  $Z$ -irreducible  $ZG$ -module, and in fact

$$Q \otimes_Z (M_i/M_{i-1}) \cong M_i^*/M_{i-1}^*, \quad 1 \leq i \leq k.$$

We refer to a chain satisfying (i)–(iii) as a *Z-composition series* for  $M$ , and we call the factor modules  $\{M_k/M_{k-1}, \dots, M_1/M_0\}$  a set of *Z-composition factors* of  $M$ . (We shall always list them in their order of occurrence in some *Z*-composition series). We shall see from the examples given at the end of this section that the *Z*-composition factors of  $M$  are *not* uniquely determined up to  $ZG$ -isomorphism and order of occurrence. On the other hand, the Jordan-Hölder theorem does hold for  $QG$ -modules; hence, if  $\{N_1, \dots, N_r\}$  and  $\{N'_1, \dots, N'_s\}$  are two sets of *Z*-composition factors of  $M$ , the two sets of  $QG$ -modules

$$\{QN_1, \dots, QN_r\} \quad \text{and} \quad \{QN'_1, \dots, QN'_s\}$$

are the same up to order of occurrence and  $QG$ -isomorphism, and in particular  $r = s$ .

The above remarks also establish

(73.12) COROLLARY. *Let  $T$  be a  $Q$ -representation of  $G$ , and let*

$$T \sim_Q \begin{pmatrix} U_1 & & * \\ & \ddots & \\ 0 & \ddots & U_r \end{pmatrix},$$

*where the  $\{U_i\}$  are not necessarily irreducible. Then also*

$$T \sim_Z \begin{pmatrix} V_1 & & * \\ & \ddots & \\ 0 & \ddots & V_r \end{pmatrix}$$

where for  $1 \leq i \leq r$ ,  $V_i$  is a  $Z$ -representation of  $G$  such that  $V_i \sim_Q U_i$ .

There is, nevertheless, one important case in which we can assert a type of uniqueness of the  $Z$ -composition factors of a  $ZG$ -module.

(73.13) THEOREM. *Let  $M$  be a  $ZG$ -module such that  $QM$  has no repeated composition factors. Suppose we have two  $Z$ -composition series for  $M$  with  $Z$ -composition factors  $\{N_1, \dots, N_r\}$  and  $\{N'_1, \dots, N'_r\}$ , respectively, and suppose that  $QN_i \cong QN'_i$ ,  $1 \leq i \leq r$ . Then  $N_i \cong N'_i$ ,  $1 \leq i \leq r$ .*

PROOF. This proof is best expressed in matrix form. Let us assume that  $M$  affords a pair of  $Z$ -equivalent  $Z$ -representations, say

$$A = \begin{pmatrix} T_1 & \cdots & T_{1r} \\ \vdots & \ddots & \vdots \\ 0 & \cdots & T_r \end{pmatrix}, \quad B = \begin{pmatrix} V_1 & \cdots & V_{1r} \\ \vdots & \ddots & \vdots \\ 0 & \cdots & V_r \end{pmatrix},$$

where the  $\{T_i\}$  and  $\{V_i\}$  are two sets of  $Z$ -composition factors of  $M$  such that  $T_i \sim_Z V_i$ ,  $1 \leq i \leq r$ .

Since  $A \sim_Z B$ , there exists a matrix  $W$  unimodular over  $Z$  such that  $WA = BW$ . Partition  $W$  into submatrices  $W_{ij}$  according to the partitioning of  $A$  and  $B$ . Then we have, for each  $g \in G$ ,

$$\begin{bmatrix} W_{11} & \cdots & W_{1r} \\ \vdots & \cdots & \vdots \\ W_{r1} & \cdots & W_{rr} \end{bmatrix} \begin{bmatrix} T_1 & & * \\ \vdots & \ddots & \vdots \\ 0 & \cdots & T_r \end{bmatrix} = \begin{bmatrix} V_1 & & * \\ \vdots & \ddots & \vdots \\ 0 & \cdots & V_r \end{bmatrix} \begin{bmatrix} W_{11} & \cdots & W_{1r} \\ \vdots & \cdots & \vdots \\ W_{r1} & \cdots & W_{rr} \end{bmatrix}.$$

We notice first that  $W_{r1}T_1(g) = V_r(g)W_{r1}$ ,  $g \in G$ . Since  $T_1$  and  $V_r$  are  $Q$ -irreducible and are not  $Q$ -equivalent (because  $QM$  has no repeated composition factors), it follows that  $W_{r1} = 0$ . Then, from

$$W_{r1}T_{12} + W_{r2}T_2 = V_rW_{r2},$$

we deduce in the same manner that  $W_{r2} = 0$ . Continuing in this way, we see that in fact

$$W = \begin{pmatrix} W_{11} & & * \\ \vdots & \ddots & \vdots \\ 0 & & W_{rr} \end{pmatrix}$$

and that

$$W_{ii}T_i = V_iW_{ii}, \quad 1 \leq i \leq r.$$

However, since  $W$  is unimodular over  $Z$ , so is each  $W_{ii}$ , and so  $T_i \sim_Z V_i$ . This completes the proof.

As we shall see from the examples at the end of this section,

the  $Z$ -composition factors of a  $ZG$ -module  $M$  need not be uniquely determined. The same is true for the indecomposable components of  $M$ , as will be apparent in the example to be considered in the next section.

Let us turn now to the concept of binding functions, which play a fundamental role in the theory of integral representations. We shall consider them first from a matrix viewpoint and then in terms of modules.

(73.14) **DEFINITION.** Let  $\mathbf{T}, \mathbf{U}$  be  $Z$ -representations of  $G$  of degrees  $t, u$ , respectively. A *binding function* for the pair  $\mathbf{T}, \mathbf{U}$  is a mapping  $\mathbf{L}$  which assigns to each  $g \in G$  a  $t \times u$  matrix  $\mathbf{L}(g)$  with entries in  $Z$ , such that

$$(73.15) \quad g \rightarrow \begin{pmatrix} \mathbf{T}(g) & \mathbf{L}(g) \\ \mathbf{0} & \mathbf{U}(g) \end{pmatrix}, \quad g \in G,$$

is a  $Z$ -representation of  $G$ . Let  $B(\mathbf{T}, \mathbf{U})$  denote the set of all binding functions for the pair  $\mathbf{T}, \mathbf{U}$ .<sup>†</sup>

From this we see that  $\mathbf{L} \in B(\mathbf{T}, \mathbf{U})$  if and only if

$$(73.16) \quad \begin{pmatrix} \mathbf{T}(g) & \mathbf{L}(g) \\ \mathbf{0} & \mathbf{U}(g) \end{pmatrix} \begin{pmatrix} \mathbf{T}(h) & \mathbf{L}(h) \\ \mathbf{0} & \mathbf{U}(h) \end{pmatrix} = \begin{pmatrix} \mathbf{T}(gh) & \mathbf{L}(gh) \\ \mathbf{0} & \mathbf{U}(gh) \end{pmatrix}, \quad g, h \in G.$$

This condition is equivalent to

$$(73.17) \quad \mathbf{L}(gh) = \mathbf{T}(g)\mathbf{L}(h) + \mathbf{L}(g)\mathbf{U}(h), \quad g, h \in G.$$

Let  $\mathbf{L}_1, \mathbf{L}_2 \in B(\mathbf{T}, \mathbf{U})$ , and define

$$(\mathbf{L}_1 \pm \mathbf{L}_2)g = \mathbf{L}_1(g) \pm \mathbf{L}_2(g), \quad g \in G.$$

Then, since equation (73.17) is linear in  $\mathbf{L}$ , we see that also  $\mathbf{L}_1 \pm \mathbf{L}_2 \in B(\mathbf{T}, \mathbf{U})$ . Thus  $B(\mathbf{T}, \mathbf{U})$  is an additive abelian group which we shall view as a  $Z$ -module. It is obviously torsion free.

We shall show at once that  $B(\mathbf{T}, \mathbf{U})$  is a finitely generated  $Z$ -module. Let  $G = \{g_1, \dots, g_n\}$ , and let  $\mathfrak{A}$  be the additive group of all  $t \times nu$  matrices with entries in  $Z$ . For  $\mathbf{L} \in B(\mathbf{T}, \mathbf{U})$ , define

$$A_{\mathbf{L}} = (\mathbf{L}(g_1), \mathbf{L}(g_2), \dots, \mathbf{L}(g_n)) \in \mathfrak{A}.$$

Then  $\mathbf{L} \rightarrow A_{\mathbf{L}}$  gives an isomorphism of  $B(\mathbf{T}, \mathbf{U})$  onto a subgroup  $\mathfrak{B}$  of  $\mathfrak{A}$ . Since  $\mathfrak{A}$  is a finitely generated  $Z$ -module, so is  $\mathfrak{B}$ , and so also

---

<sup>†</sup> Some authors refer to  $\{\mathbf{L}(g) : g \in G\}$  as a “binding system.” However, one is usually interested in the mapping  $\mathbf{L}$  rather than the collection of matrices  $\{\mathbf{L}(g) : g \in G\}$ . Thus, the terminology “binding functions” seems more appropriate.

is  $B(\mathbf{T}, \mathbf{U})$ .

An element  $\mathbf{L} \in B(\mathbf{T}, \mathbf{U})$  is called an *inner binding function* if there exists a  $t \times u$  matrix  $\mathbf{D}$  over  $Z$  such that

$$(73.18) \quad \mathbf{L}(g) = \mathbf{T}(g)\mathbf{D} - \mathbf{D}\mathbf{U}(g), \quad g \in G.$$

It is easily verified that for each  $\mathbf{D}^{t \times u}$  over  $Z$ , the above defines a binding function  $\mathbf{L}$ . The set of all inner binding functions  $B'(\mathbf{T}, \mathbf{U})$  is a subgroup of  $B(\mathbf{T}, \mathbf{U})$ .

The reader should compare the preceding discussion with its analogue in § 72.

(73.19) **DEFINITION.** Let  $\mathbf{L}_1, \mathbf{L}_2 \in B(\mathbf{T}, \mathbf{U})$ . We write  $\mathbf{L}_1 \approx_z \mathbf{L}_2$  and call  $\mathbf{L}_1, \mathbf{L}_2$  *Z-equivalent* if  $\mathbf{L}_1 - \mathbf{L}_2 \in B'(\mathbf{T}, \mathbf{U})$ . We write  $\mathbf{L}_1 \approx_q \mathbf{L}_2$  and call  $\mathbf{L}_1, \mathbf{L}_2$  *Q-equivalent* if there exists a matrix  $\mathbf{D}$  over  $Q$  such that

$$(73.20) \quad \mathbf{L}_1(g) - \mathbf{L}_2(g) = \mathbf{T}(g)\mathbf{D} - \mathbf{D}\mathbf{U}(g), \quad g \in G.$$

The importance of the subgroup  $B'(\mathbf{T}, \mathbf{U})$  stems from

(73.21) **LEMMA.** Let  $\mathbf{L}_1, \mathbf{L}_2 \in B(\mathbf{T}, \mathbf{U})$  be Z-equivalent. Then

$$\begin{pmatrix} \mathbf{T} & \mathbf{L}_1 \\ \mathbf{0} & \mathbf{U} \end{pmatrix} \sim_z \begin{pmatrix} \mathbf{T} & \mathbf{L}_2 \\ \mathbf{0} & \mathbf{U} \end{pmatrix}.$$

**PROOF.** By hypothesis, there exists a matrix  $\mathbf{D}$  over  $Z$  satisfying (73.20). Since

$$\begin{pmatrix} \mathbf{I} & \mathbf{D} \\ \mathbf{0} & \mathbf{I} \end{pmatrix}^{-1} = \begin{pmatrix} \mathbf{I} & -\mathbf{D} \\ \mathbf{0} & \mathbf{I} \end{pmatrix},$$

we have

$$\begin{pmatrix} \mathbf{I} & \mathbf{D} \\ \mathbf{0} & \mathbf{I} \end{pmatrix} \begin{pmatrix} \mathbf{T}(g) & \mathbf{L}_1(g) \\ \mathbf{0} & \mathbf{U}(g) \end{pmatrix} \begin{pmatrix} \mathbf{I} & \mathbf{D} \\ \mathbf{0} & \mathbf{I} \end{pmatrix}^{-1} = \begin{pmatrix} \mathbf{T}(g) & \mathbf{L}_2(g) \\ \mathbf{0} & \mathbf{U}(g) \end{pmatrix}$$

for all  $g \in G$ . This proves the lemma.

A slight modification of the proof of Maschke's theorem yields the following basic result:

(73.22) **THEOREM.** Let  $\mathbf{T}, \mathbf{U}$  be Z-representations of  $G$ , and set  $n = [G : 1]$ . Then

$$n \cdot B(\mathbf{T}, \mathbf{U}) \subset B'(\mathbf{T}, \mathbf{U}).$$

Consequently, for each  $\mathbf{L} \in B(\mathbf{T}, \mathbf{U})$ , we have  $\mathbf{L} \approx_q 0$ .

**PROOF.** Let  $\mathbf{L} \in B(\mathbf{T}, \mathbf{U})$ , and rewrite (73.17) as

$$\mathbf{L}(h) = \mathbf{T}(g^{-1})\mathbf{L}(gh) - \mathbf{T}(g^{-1})\mathbf{L}(g)\mathbf{U}(h).$$

Summing over all  $g \in G$ , this yields

$$\mathbf{n} \cdot \mathbf{L}(h) = \sum_g \mathbf{T}(g^{-1})\mathbf{L}(gh) - \sum_g \mathbf{T}(g^{-1})\mathbf{L}(g)\mathbf{U}(h).$$

Setting  $g' = gh$ , we see that as  $g$  ranges over  $G$  so does  $g'$ , whence

$$\begin{aligned} \sum_g \mathbf{T}(g^{-1})\mathbf{L}(gh) &= \sum_{g'} \mathbf{T}(hg'^{-1})\mathbf{L}(g') \\ &= \mathbf{T}(h) \sum_{g'} \mathbf{T}(g'^{-1})\mathbf{L}(g'). \end{aligned}$$

If we set  $\mathbf{D} = \sum_g \mathbf{T}(g^{-1})\mathbf{L}(g)$ , then  $\mathbf{n} \cdot \mathbf{L}(h) = \mathbf{T}(h)\mathbf{D} - \mathbf{D}\mathbf{U}(h)$ ,  $h \in G$ . This proves the theorem. (See also the proof of Theorem 72.16).

**REMARK.** The above theorem shows that each  $\mathbf{L}$  in  $B(\mathbf{T}, \mathbf{U})$  satisfies  $\mathbf{L} \approx_0 \mathbf{0}$ . This is the matrix analogue of Maschke's theorem 10.8 which states that every  $QG$ -module is completely reducible. An easy modification of the above proof shows also that every  $KG$ -module is completely reducible, for  $K$  a field such that  $\text{char } K \nmid [G : 1]$ , the crucial step being the fact that this hypothesis permits us to divide by  $n$  in both sides of the last formula in the proof of the above theorem.

If  $A_1, A_2$  are integral matrices, write  $A_1 \equiv A_2 \pmod{n}$  to indicate that the corresponding entries of  $A_1, A_2$  are congruent modulo  $n$ . As a consequence of Theorem 73.22, we have

(73.23) **COROLLARY.** *Let  $\mathbf{T}, \mathbf{U}$  be  $Z$ -representations of  $G$ , and let  $n = [G : 1]$ . If  $\mathbf{L}_1, \mathbf{L}_2 \in B(\mathbf{T}, \mathbf{U})$  are such that*

$$\mathbf{L}_1(g) \equiv \mathbf{L}_2(g) \pmod{n}, \quad g \in G,$$

*then  $\mathbf{L}_1 \approx_Z \mathbf{L}_2$ .*

**PROOF.** Set  $\mathbf{L} = \mathbf{L}_1 - \mathbf{L}_2 \in B(\mathbf{T}, \mathbf{U})$ . From the hypothesis,  $\mathbf{L}(g) \equiv \mathbf{0} \pmod{n}$  for each  $g \in G$ . We may therefore write

$$\mathbf{L}(g) = \mathbf{n} \cdot \mathbf{K}(g), \quad g \in G,$$

where for each  $g$ , the matrix  $\mathbf{K}(g)$  has entries in  $Z$ . Since  $\mathbf{L}$  satisfies condition (73.17), so does  $\mathbf{K}$ , whence  $\mathbf{K} \in B(\mathbf{T}, \mathbf{U})$ . Consequently,  $\mathbf{L} \in \mathbf{n} \cdot B(\mathbf{T}, \mathbf{U}) \subset B'(\mathbf{T}, \mathbf{U})$ . This proves the result.

In terms of  $ZG$ -modules, the reduced representation given in (73.15) is obtained from a reducible<sup>†</sup>  $ZG$ -module  $M$  as follows:  $M$  contains a  $ZG$ -submodule  $N$  which is a  $Z$ -direct summand of  $M$  such that  $0 < (N : Z) < (M : Z)$ . If we choose a  $Z$ -basis of  $M$  so that the

<sup>†</sup> Theorem 73.9 allows us to speak of reducibility rather than  $Z$ - or  $Q$ -reducibility.

first  $t$  elements form a  $\mathbb{Z}$ -basis of  $N$ , then  $M$  affords a representation (73.15) in which  $N$  affords  $T$ , and  $M/N$  affords  $U$ . It is then easy to see that, for each  $g \in G$ , the matrix  $L(g)$  defines a  $\mathbb{Z}$ -homomorphism of  $M/N$  into  $N$ . Let us show how these  $\mathbb{Z}$ -homomorphisms arise without use of  $\mathbb{Z}$ -bases.

As above, let  $M$  be a  $ZG$ -module containing the  $ZG$ -submodule  $N$  which is a  $\mathbb{Z}$ -direct summand of  $M$  and for which  $0 < (N: \mathbb{Z}) < (M: \mathbb{Z})$ . Then  $M = N \oplus X$  for some  $\mathbb{Z}$ -submodule  $X$  of  $M$ , and obviously  $X \cong M/N$  as  $\mathbb{Z}$ -modules. Every element of  $M$  is therefore uniquely representable as an ordered pair  $(n, y)$ ,  $n \in N$ ,  $y \in M/N$ , and these pairs are added componentwise.

Now we shall investigate the action of  $G$  on  $M$ . Since  $N$  is a  $ZG$ -submodule of  $M$ , we have

$$g(n, 0) = gn = (gn, 0), \quad n \in N, g \in G.$$

On the other hand,  $(0, y)$  is an element of  $M$  which maps onto  $y$  under the map  $M \rightarrow M/N$ , and thus we may write

$$(73.24) \quad y = (0, y) + N.$$

Therefore

$$gy = g(0, y) + N,$$

and so we have

$$g(0, y) = (F_g(y), gy), \quad g \in G, y \in M/N,$$

where  $F_g(y) \in N$ . Clearly  $F_g \in \text{Hom}_{\mathbb{Z}}(M/N, N)$ , and we may write

$$(73.25) \quad g(n, y) = (gn + F_g(y), gy), \quad g \in G, n \in N, y \in M/N.$$

The  $ZG$ -module  $M$  is thus completely determined by the modules  $N$  and  $M/N$ , and the map

$$(73.26) \quad F: G \rightarrow \text{Hom}_{\mathbb{Z}}(M/N, N),$$

according to (73.25). The module  $M$  will be denoted by  $(N, M/N; F)$ .

The map  $F$  is not arbitrary, however, since we must have

$$(hg)(n, y) = h(g(n, y)), \quad h, g \in G, n \in N, y \in M/N.$$

This condition is easily seen to be equivalent to

$$(73.27) \quad F_{gh}(y) = gF_h(y) + F_g(hy), \quad g, h \in G, y \in M/N.$$

Let  $B(N, M/N)$  denote the set of all maps  $F$  given in (73.26) which satisfy (73.27). For any such  $F$ , one readily finds that equation (73.25) does in fact define a  $ZG$ -module  $M$ .

We have therefore established that if  $M$  is a  $ZG$ -module containing a non-zero  $ZG$ -submodule  $N$  of lower  $Z$ -rank, such that  $N$  is a  $Z$ -direct summand of  $M$ , then there exists a map  $F \in B(N, M/N)$  for which  $M = (N, M/N; F)$ . Conversely, each  $F \in B(N, M/N)$  determines a  $ZG$ -module  $M$  with these properties. We may refer to  $F$  as a *binding function* for the pair  $N, M/N$ .

Let us now remark that the modules  $M, N$  do not determine the map  $F$  uniquely since in the determination of  $F$  we had to choose a  $Z$ -complement of  $N$  in  $M$  and a  $Z$ -isomorphism of  $M/N$  onto this complement. Suppose also that  $M = N \oplus X'$  for some  $Z$ -submodule  $X'$  of  $M$ , where again  $X' \cong M/N$ . Each element of  $M$  is again represented as an ordered pair  $(n, y)'$  (say),  $n \in N$ ,  $y \in M/N$ , where the action of  $G$  is now given by

$$g(n, y)' = (gn + F'_g(y), gy)'.$$

As before, each  $F'_g \in \text{Hom}_Z(M/N, N)$ . Since  $(0, y)$  and  $(0, y)'$  differ by an element of  $N$ , we may define a map  $D \in \text{Hom}_Z(M/N, N)$  by means of

$$D(y) = (0, y)' - (0, y), \quad y \in M/N.$$

We then have for  $g \in G$ ,

$$\begin{aligned} g \cdot D(y) &= (F'_g(y), gy)' - (F_g(y), gy), \\ &= D(gy) + (F'_g(y), gy) - (F_g(y), gy), \quad y \in M/N. \end{aligned}$$

This proves that for each  $g \in G$ ,

$$F'_g(y) = F_g(y) + Dgy - gDy, \quad y \in M/N.$$

We call a map  $f: G \rightarrow \text{Hom}_Z(M/N, N)$  an *inner binding function* if there exists a map  $D \in \text{Hom}_Z(M/N, N)$  such that  $f_g = Dg - gD$ ,  $g \in G$ . The set of inner binding functions forms an additive subgroup  $B'(N, M/N)$  of  $B(N, M/N)$ . Define

$$C(N, M/N) = B(N, M/N)/B'(N, M/N).$$

Then the pair  $M, N$  determines a unique element  $F + B'$  in  $B/B'$ . Conversely, Lemma 73.21 shows that  $(N, M/N; F) \cong (N, M/N; F')$  whenever  $F' - F \in B'$ .

We note finally that any  $F$  given by (73.26) can be extended in a unique way to a  $Z$ -homomorphism of the group ring  $ZG$  into  $\text{Hom}_Z(M/N, N)$ .

We conclude with a number of illustrative examples due to Diederichsen [1], Maranda [1], and Reiner [4].

*Example 1.* The symmetric group  $S_3$  has two generators  $a, b$  satisfying

$$a^2 = b^3 = (ab)^2 = 1 .$$

The  $Z$ -representations

$$a \rightarrow \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad b \rightarrow \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}$$

and

$$a \rightarrow \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad b \rightarrow \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}$$

are  $Q$ -equivalent but not  $Z$ -equivalent.

*Example 2.* Let  $G$  be the dihedral group of order 8 with generators  $a$  and  $b$  satisfying

$$a^4 = b^2 = (ab)^2 = 1 .$$

Set

$$\mathbf{A}_1 = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad \mathbf{B}_1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix};$$

$$\mathbf{A}_2 = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad \mathbf{B}_2 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix},$$

and define  $Z$ -representations  $\mathbf{T}_1, \mathbf{T}_2$  of  $G$  by means of

$$\mathbf{T}_i(a) = \mathbf{A}_i, \quad \mathbf{T}_i(b) = \mathbf{B}_i, \quad i = 1, 2 .$$

Then  $\mathbf{T}_1$  and  $\mathbf{T}_2$  are irreducible and are  $Q$ -equivalent but not  $Z$ -equivalent.

Now define  $\mathbf{L}_i \in B(\mathbf{T}_i, \mathbf{T}_i)$ ,  $i = 1, 2$ , as follows:

$$\mathbf{L}_1(a) = \mathbf{0}, \quad \mathbf{L}_1(b) = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}; \quad \mathbf{L}_2(a) = \mathbf{0}, \quad \mathbf{L}_2(b) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} .$$

Then

$$(73.28) \quad \begin{pmatrix} \mathbf{T}_1 & \mathbf{L}_1 \\ \mathbf{0} & \mathbf{T}_1 \end{pmatrix}, \quad \begin{pmatrix} \mathbf{T}_2 & \mathbf{L}_2 \\ \mathbf{0} & \mathbf{T}_2 \end{pmatrix}$$

are  $Z$ -equivalent representations of  $G$ , the first of which has  $Z$ -composition factors  $\mathbf{T}_1, \mathbf{T}_1$ , the second  $\mathbf{T}_2, \mathbf{T}_2$ . This shows that  $Z$ -composition factors are determined up to  $Q$ -equivalence only and not up to  $Z$ -equivalence.

Continuing our discussion, let  $\mathbf{U}$  be the  $Z$ -representation of  $G$  defined by

$$\mathbf{U}(a) = \left( \begin{array}{cc|c} \mathbf{A}_1 & & 1 \\ & 0 & 0 \\ \hline 0 & 0 & 1 \end{array} \right), \quad \mathbf{U}(b) = \left( \begin{array}{cc|c} \mathbf{B}_1 & & 1 \\ & -1 & \\ \hline 0 & 0 & 1 \end{array} \right)$$

so that  $\mathbf{U}$  has  $Z$ -composition factors  $\mathbf{T}_1$  and  $\mathbf{1}$ . Set

$$\mathbf{S} = \begin{pmatrix} 1 & 0 & 1 \\ -1 & -1 & -1 \\ 2 & 1 & 1 \end{pmatrix}.$$

Then  $\mathbf{S}^{-1}\mathbf{U}\mathbf{S} = \mathbf{V}$  where

$$\mathbf{V}(a) = \left( \begin{array}{c|cc} 1 & 1 & 0 \\ 0 & & \\ \hline 0 & & \mathbf{A}_2 \end{array} \right), \quad \mathbf{V}(b) = \left( \begin{array}{c|cc} 1 & 0 & 1 \\ 0 & & \\ \hline 0 & & \mathbf{B}_2 \end{array} \right).$$

Thus  $\mathbf{V}$  has  $Z$ -composition factors  $\mathbf{1}$ ,  $\mathbf{T}_2$ . This shows that changing the order of occurrence of the factors can change the  $Z$ -equivalence classes of those factors.

### Exercises

1. Explain where the proof of the Jordan-Hölder theorem breaks down when we try to prove uniqueness of the  $Z$ -composition factors of a  $ZG$ -module.
2. Let  $\{\mathbf{T}_i : 1 \leq i \leq r\}$  and  $\{\mathbf{U}_i : 1 \leq i \leq r\}$  be two sets of  $Z$ -representations of  $G$  such that  $\mathbf{T}_i \sim_q \mathbf{U}_i$  for  $1 \leq i \leq r$ . Suppose that for  $i \neq j$ ,  $\mathbf{T}_i$  and  $\mathbf{T}_j$  have no common  $Q$ -composition factor. If

$$\begin{pmatrix} \mathbf{T}_1 & * \\ & \ddots \\ 0 & \mathbf{T}_r \end{pmatrix}, \quad \begin{pmatrix} \mathbf{U}_1 & * \\ & \ddots \\ 0 & \mathbf{U}_r \end{pmatrix}$$

are a pair of  $Z$ -equivalent  $Z$ -representations of  $G$ , prove that in fact  $\mathbf{T}_i \sim_Z \mathbf{U}_i$ ,  $1 \leq i \leq r$ .

3. Determine all  $Z$ -representations of degree 2 of the cyclic group of order 2.

### § 74. The Cyclic Group of Prime Order

Throughout this section, let  $G$  denote a cyclic group generated by an element  $g$  of prime order  $p$ . We shall apply the results of Chapter III to the problem of determining (and classifying according to  $ZG$ -isomorphism) all  $ZG$ -modules having a finite  $Z$ -basis. This will furnish the reader with a concrete example which may help

him better to understand the subsequent discussion. It will also give him some appreciation of the difficulties that arise in classifying modules which are not vector spaces over fields.

Throughout this section, let  $\theta$  denote a primitive  $p$ th root of 1 over  $Q$ , and let  $K = Q(\theta)$ . Then  $\text{Irr}(\theta, Q)$  is the cyclotomic polynomial of order  $p$ , given by

$$\text{Irr}(\theta, Q) = \Phi_p(X) = \sum_{r=0}^{p-1} X^r.$$

Let  $R$  denote the ring of all algebraic integers in  $K$ ; in §21 we showed that  $R$  is a Dedekind domain with  $Z$ -basis  $\{1, \theta, \dots, \theta^{p-2}\}$ , so that  $(K:Q) = (R:Z) = p - 1$ .

Suppose now that  $A$  is any  $R$ -ideal in  $K$  (see §18). Then  $A$  has  $Z$ -rank  $p - 1$ , and  $RA \subset A$ . We may turn  $A$  into a  $ZG$ -module, again denoted by  $A$ , by defining

$$g \cdot a = \theta a, \quad a \in A,$$

since obviously  $g^p \cdot a = \theta^p \cdot a = a, a \in A$ . Because of this definition, two  $R$ -ideals  $A$  and  $B$  in  $K$  are isomorphic as  $ZG$ -modules if and only if  $A \cong B$  as  $R$ -modules. On the other hand, we showed [Lemma 22.2] that  $A \cong B$  as  $R$ -modules if and only if  $A$  and  $B$  are in the same ideal class. (See §20.)

A more complicated  $ZG$ -module may be constructed as follows. Let  $A$  be an  $R$ -ideal in  $K$ , and let  $a_0$  be some fixed element of  $A$ . We turn the external direct sum  $A + Zy$  of the  $Z$ -module  $A$  and the free  $Z$ -module  $Zy$  into a  $ZG$ -module by defining

$$(74.1) \quad g \cdot a = \theta a, \quad a \in A, \quad gy = a_0 + y.$$

In order to show that  $g^p u = u$  for all  $u \in A + Zy$ , it is clear that we need verify only that  $g^p y = y$ . We have

$$\begin{aligned} gy &= a_0 + y, \\ g^2y &= g(a_0 + y) = (\theta + 1)a_0 + y, \dots, \\ g^py &= \Phi_p(\theta) \cdot a_0 + y = y. \end{aligned}$$

Thus  $A + Zy$  is now a  $ZG$ -module of  $Z$ -rank  $p$ ; we denote this module by  $(A, a_0)$  for the remainder of this section.

(74.2) LEMMA. *Let  $c \in Z$  be such that  $p \nmid c$ . Then  $(A, a_0) \cong (A, ca_0)$ .*

PROOF. We have

$$\begin{aligned} (A, a_0) &= A + Zy_1, & ga = \theta a, \quad a \in A, & gy_1 = a_0 + y_1, \\ (A, ca_0) &= A + Zy_2, & ga = \theta a, \quad a \in A, & gy_2 = ca_0 + y_2. \end{aligned}$$

Define  $\zeta = (\theta^c - 1)/(\theta - 1) \in R$ . Since  $p \nmid c$ , we may choose  $d \in Z$

such that  $cd \equiv 1 \pmod{p}$ . Then  $\zeta^{-1} = (\theta^{ca} - 1)/(\theta^c - 1) \in R$ , so that  $\zeta$  is a unit in  $R$ .

Next we note that for  $c > 0$ ,

$$\zeta - c = \sum_{j=0}^{c-1} (\theta^j - 1) \equiv 0 \pmod{(\theta - 1)R}.$$

The same holds for  $c < 0$  because we may replace  $c$  by  $c + kp$ , and  $p \in (\theta - 1)R$  by (21.11). Consequently, there exists an element  $\omega \in A$  such that

$$(\zeta - c)a_0 = (\theta - 1)\omega.$$

Now let  $\psi: (A, a_0) \rightarrow (A, ca_0)$  be the  $Z$ -linear map defined by

$$\psi(a) = \zeta a, \quad a \in A, \quad \psi(y_1) = \omega + y_2$$

where  $y_1$  and  $y_2$  are given above. Obviously,  $\psi$  is a  $Z$ -isomorphism of  $(A, a_0)$  onto  $(A, ca_0)$ . The lemma will be proved if we can show that  $\psi$  is a  $ZG$ -isomorphism. Trivially,  $g\psi(a) = \psi(ga)$  for all  $a \in A$ . Furthermore,

$$g\psi(y_1) = g(\omega + y_2) = \theta\omega + ca_0 + y_2 = \zeta a_0 + \omega + y_2,$$

whereas

$$\psi(gy_1) = \psi(a_0 + y_1) = \zeta a_0 + \omega + y_2.$$

This proves the lemma.

We shall prove that every  $ZG$ -module is a direct sum of modules of the types  $A$ ,  $(A, a_0)$ , and  $Z$ -modules on which  $G$  acts trivially. Specifically, we shall establish

(74.3) THEOREM (Diederichsen [1], Reiner [2]). *Every  $ZG$ -module  $M$  is isomorphic to a direct sum*

$$(A_1, a_1) \dot{+} \cdots \dot{+} (A_r, a_r) \dot{+} A_{r+1} \dot{+} \cdots \dot{+} A_n \dot{+} Y$$

where the  $\{A_i\}$  are  $R$ -ideals in  $K$ , where the  $\{a_i\}$  are chosen so that  $a_i \in A_i$ ,  $a_i \notin (\theta - 1)A_i$ , and where  $Y$  is a  $Z$ -module having a finite  $Z$ -basis such that  $gy = y$  for all  $y \in Y$ . The isomorphism class of  $M$  is determined by the integers  $r, n$ , the  $Z$ -rank of  $Y$ , and the ideal class of  $A_1 \cdots A_n$  in  $K$ .

The proof will occupy the remainder of the section. We begin by observing that  $ZG$  is a commutative group ring and that

$$ZG = Z \oplus Zg \oplus \cdots \oplus Zg^{p-1}.$$

Define

$$s = 1 + g + \cdots + g^{p-1} \in ZG,$$

and let  $(s)$  denote the principal ideal generated by  $s$  in  $ZG$ . Then  $ZG/(s)$  is a commutative ring.

(74.4) LEMMA.  $ZG/(s) \cong R$ .

PROOF. The map

$$\sum_{r=0}^{p-1} a_r g^r \rightarrow \sum_{r=0}^{p-1} a_r \theta^r, \quad a_i \in Z,$$

defines a ring homomorphism of  $ZG$  onto  $R$ . The kernel of the homomorphism clearly contains  $(s)$ . On the other hand, if  $F(g) = \sum a_r g^r$  lies in the kernel, then  $F(\theta) = 0$ . Letting  $X$  denote an indeterminate over  $Q$ , we therefore have

$$F(X) = \emptyset_p(X) \cdot H(X)$$

for some  $H(X) \in Z[X]$ . This implies that  $F(g) = \emptyset_p(g) \cdot H(g) = s \cdot H(g)$ , which proves the lemma.

Now let  $M$  be any  $ZG$ -module, and define

$$M_s = \{m \in M : sm = 0\}.$$

Clearly,  $M_s$  is a  $ZG$ -submodule of  $M$ . We show further that  $M_s$  is a pure  $Z$ -submodule of  $M$ ; we must verify that if  $a \in Z$ ,  $a \neq 0$ , and if  $am \in M_s$  for some  $m \in M$ , then also  $m \in M_s$ . However,

$$0 = s \cdot am = a \cdot sm$$

implies  $sm = 0$  since  $M$  is  $Z$ -torsion-free, and so  $m \in M_s$ .

Since  $M_s$  is a pure  $Z$ -submodule of  $M$ , it is also a  $Z$ -direct summand of  $M$  [see Theorem 16.16]. Consequently,  $M$  contains a  $Z$ -submodule  $X$  such that

$$M = M_s \oplus X.$$

However,  $X$  need not be a  $ZG$ -submodule of  $M$ .

Because  $(s)$  annihilates  $M_s$ , we may turn  $M_s$  into a left  $ZG/(s)$ -module in a canonical way by defining

$$\{x + (s)\} \cdot m = xm, \quad x \in ZG, m \in M_s.$$

In view of the isomorphism  $ZG/(s) \cong R$ , we may then turn  $M_s$  into a left  $R$ -module by setting  $\theta \cdot m = gm$ ,  $m \in M_s$ . Certainly  $M_s$  is then a left  $R$ -module having a finite  $Z$ -basis. Let us show that  $M_s$  is a torsion-free  $R$ -module. Let  $\alpha \in R$ ,  $\alpha \neq 0$ ; then  $N(\alpha)$ , the norm of  $\alpha$ , is a non-zero element of  $Z$ , and there exists  $\beta \in R$  such that  $N(\alpha) = \alpha\beta$ . Therefore, if  $\alpha m = 0$  for some  $m \in M_s$ , also  $N(\alpha)m = 0$ , which shows that  $m = 0$ . Finally, we observe the inclusion

$M_s \supset (g - 1)M$ , since  $s(g - 1) = 0$  in  $ZG$ .

We have thus arrived at the following situation: Starting with a  $ZG$ -module  $M$ , we have obtained from it a submodule  $M_s$  which is a finitely generated torsion-free  $R$ -module containing an  $R$ -submodule  $(g - 1)M$ . Note that  $M_s$  and  $(g - 1)M$  have the same  $R$ -rank. We may thus apply Exercise 22.6 to deduce the existence of an integer  $n$ , of elements  $b_1, \dots, b_n \in M_s$  which are  $R$ -free, of an  $R$ -ideal  $A$  in  $K$ , and of ideals  $E_1, \dots, E_n$  in  $R$  satisfying  $E_i | E_{i+1}$  for  $1 \leq i \leq n - 1$ , such that

$$(74.5) \quad \begin{cases} M_s = Rb_1 \oplus \cdots \oplus Rb_{n-1} \oplus Ab_n, \\ (g - 1)M = E_1b_1 \oplus \cdots \oplus E_{n-1}b_{n-1} \oplus E_nAb_n. \end{cases}$$

Further, the integer  $n$ , the ideal class of  $A$ , and the ideals  $E_1, \dots, E_n$  are all uniquely determined by the pair  $M_s, (g - 1)M$ .

From the obvious inclusion

$$(g - 1)M \supset (g - 1)M_s = (\theta - 1)M_s$$

we obtain

$$\begin{aligned} E_1b_1 \oplus \cdots \oplus E_{n-1}b_{n-1} \oplus E_nAb_n \\ \supset (\theta - 1)Rb_1 \oplus \cdots \oplus (\theta - 1)Rb_{n-1} \oplus (\theta - 1)Ab_n, \end{aligned}$$

which implies

$$R \supset E_i \supset (\theta - 1)R, \quad 1 \leq i \leq n.$$

Since  $(\theta - 1)R$  is a maximal ideal in  $R$  (see § 21), we conclude that each  $E_i$  is either  $R$  or  $(\theta - 1)R$ . Consequently, there exists an integer  $r$  (uniquely determined by  $M$ ) such that

$$E_1 = \cdots = E_r = R, \quad E_{r+1} = \cdots = E_n = (\theta - 1)R.$$

Let us set

$$L = (g - 1)M / (\theta - 1)M_s.$$

Then from (74.5) and the equations for the  $\{E_i\}$  we deduce that

$$(74.6) \quad L \cong R/(\theta - 1)R + \cdots + R/(\theta - 1)R \quad (r \text{ summands})$$

where the last summand should be  $A/(\theta - 1)A$  in the special case where  $r = n$ .

Write  $\bar{Z} = Z/pZ$ . Since  $(\theta - 1)R$  is a prime ideal of  $R$  of norm  $p$  (see § 21), it follows that  $R/(\theta - 1)R \cong \bar{Z}$ . Also  $A/(\theta - 1)A \cong \bar{Z}$ , by (18.24). Thus  $L$  is isomorphic to a direct sum of  $r$  copies of  $\bar{Z}$ , and if we let  $b_i \in M_s$  map onto  $b_i^* \in L$ , we have

$$(74.7) \quad L = \bar{Z}b_1^* \oplus \cdots \oplus \bar{Z}b_r^*.$$

From the relation  $M = M_s \oplus X$ , we deduce

$$(g - 1)M = (g - 1)M_s + (g - 1)X = (\theta - 1)M_s + (g - 1)X.$$

Hence in every coset of  $(g - 1)M / (\theta - 1)M_s$  there lies an element of  $(g - 1)X$ . Therefore the map  $\varphi: X \rightarrow L$ , given by

$$\varphi: x \mapsto (g - 1)x + (\theta - 1)M_s, \quad x \in X,$$

is a  $Z$ -homomorphism of  $X$  onto  $L$ . Let  $\{x_1, \dots, x_k\}$  be a  $Z$ -basis of  $X$ , and set

$$\varphi(x_i) = \sum_{j=1}^r \bar{a}_{ij} b_j^*, \quad a_{ij} \in Z, \quad 1 \leq i \leq k.$$

The fact that  $\varphi$  maps  $X$  onto  $L$  means that the  $k \times r$  matrix  $\bar{A} = (\bar{a}_{ij})$  has rank  $r$  (over  $\bar{Z}$ ) and thus incidentally shows that  $k \geq r$ .

Suppose that  $\{x'_1, \dots, x'_k\}$  is another  $Z$ -basis of  $X$ , and let

$$x'_i = \sum_{j=1}^k u_{ij} x_j, \quad u_{ij} \in Z.$$

Then  $U = (u_{ij})$  is unimodular over  $Z$ , and we have

$$\varphi(x'_i) = \sum_{j,l} \bar{u}_{ij} \bar{a}_{jl} b_l^*, \quad 1 \leq i \leq k.$$

Thus, by using the basis  $\{x'_i\}$  instead of  $\{x_i\}$ , the matrix  $\bar{A}$  is replaced by  $\bar{U}\bar{A}$  (where  $\bar{U}$  is obtained from  $U$  by replacing each entry of  $U$  by its residue class mod  $p$ ). The method of proof of Theorem 16.6 shows that it is possible to choose  $U$  unimodular over  $Z$  so that  $\bar{U}\bar{A}$  takes the form

$$\bar{U}\bar{A} = \begin{pmatrix} \bar{c}_1 & 0 & \cdots & 0 \\ 0 & \bar{c}_2 & \cdots & 0 \\ \cdot & \cdot & \cdots & \cdot \\ 0 & 0 & \cdots & \bar{c}_r \\ 0 & 0 & \cdots & 0 \\ \cdot & \cdot & \cdots & \cdot \\ 0 & 0 & \cdots & 0 \end{pmatrix}, \quad c_i \in Z,$$

where  $\bar{c}_1, \dots, \bar{c}_r$  are non-zero elements of  $\bar{Z}$ . (We have used here the fact that  $\bar{A}$  has rank  $r$ .) For this choice of  $U$  we now have

$$\varphi(x'_i) = \bar{c}_i b_i^*, \quad 1 \leq i \leq r,$$

$$\varphi(x'_j) = 0, \quad r + 1 \leq j \leq k.$$

In other words,

$$\begin{aligned} (g-1)x'_i &\equiv c_i b_i \} & 1 \leq i \leq r \\ (g-1)x'_j &\equiv 0 \} \text{ mod } (\theta-1)M_s, & r+1 \leq j \leq k. \end{aligned}$$

Write

$$\begin{aligned} (g-1)x'_i &= c_i b_i + (\theta-1)u_i, & 1 \leq i \leq r, \\ (g-1)x'_j &= (\theta-1)u_j, & r+1 \leq j \leq k, \end{aligned}$$

with  $u_1, \dots, u_k \in M_s$ . Define  $y_1, \dots, y_k \in M$  by

$$y_i = x'_i - u_i, \quad 1 \leq i \leq k.$$

From  $M = M_s \oplus X$  we then obtain

$$M = M_s \oplus Z y_1 \oplus \cdots \oplus Z y_k,$$

and from the above,

$$(74.8) \quad gy_i = c_i b_i + y_i, \quad 1 \leq i \leq r, \quad gy_j = y_j, \quad r+1 \leq j \leq k.$$

Combining (74.8) with equation (74.5) for  $M_s$ , we may write

$$\begin{aligned} M &= (Rb_1 \oplus Zy_1) \oplus \cdots \oplus (Rb_r \oplus Zy_r) \\ &\quad \oplus Rb_{r+1} \oplus \cdots \oplus Rb_{n-1} \oplus Ab_n \oplus Zy_{r+1} \oplus \cdots \oplus Zy_k. \end{aligned}$$

Now the sum  $Rb_i \oplus Zy_i$  is itself a  $ZG$ -module, and in fact

$$Rb_i \oplus Zy_i \cong (R, c_i)$$

in terms of the notation introduced earlier in this section. Further, for  $1 \leq i \leq r$ , we know that  $p \nmid c_i$ , and so by Lemma 74.2

$$(R, c_i) \cong (R, 1).$$

(In the special case where  $r = n$ , we obtain

$$gy_n = c_n b_n + y_n,$$

where now  $c_n \in A$  but  $c_n \notin (\theta-1)A$ . If  $a_0$  is some fixed element of  $A$  such that  $a_0 \notin (\theta-1)A$ , the residue classes of  $a_0, 2a_0, \dots, pa_0 \text{ mod } (\theta-1)A$  give all the elements of  $A/(\theta-1)A$ , and hence there exists an integer  $h \in Z$  such that  $p \nmid h$ , and

$$c_n \equiv ha_0 \pmod{(\theta-1)A}.$$

Since  $c_n$  was determined only mod  $(\theta-1)A$ , we may in fact assume that  $c_n = ha_0$ . Lemma 74.2 then implies that

$$Ab_n \oplus Zy_n \cong (A, c_n) \cong (A, a_0).$$

We have therefore shown that for any  $ZG$ -module  $M$ , there exists an isomorphism

$$(74.9) \quad \begin{aligned} M &\cong (R, 1) + \cdots + (R, 1) & (r \text{ summands}) \\ &+ R + \cdots + R + A & (n - r \text{ summands}) \\ &+ Z + \cdots + Z & (k - r \text{ summands}). \end{aligned}$$

In the special case where  $r = n$ , this becomes

$$(74.10) \quad \begin{aligned} M &\cong (R, 1) + \cdots + (R, 1) + (A, a_0) & (n \text{ summands}) \\ &+ Z + \cdots + Z & (k - n \text{ summands}). \end{aligned}$$

Four canonical invariants which are determined uniquely by  $M$  are

- (i)  $k = Z\text{-rank of } M/M_s$ ,
- (ii)  $n = R\text{-rank of } M_s$ ,
- (iii)  $r = \bar{Z}\text{-rank of } (g - 1)M/(\theta - 1)M_s$ ,
- (iv) the ideal class of  $A$ , where  $M_s \cong R + \cdots + R + A$

$(n \text{ summands})$ .

Further, these canonical invariants completely characterize  $M$ . Thus, two  $ZG$ -modules are  $ZG$ -isomorphic if and only if they have the same set of invariants  $k, n, r$ , and ideal class of  $A$ . On the other hand, given three integers  $k, n, r$  such that

$$k \geq r \geq 0, \quad n \geq r \geq 0,$$

and given an ideal class with representative  $A$ , formula (74.9) [or (74.10)] defines a  $ZG$ -module having the given invariants.

The above discussion completes the proof of the first part of the theorem, and in fact shows that of the ideals  $A_1, \dots, A_n$ , we may choose all but one of them to be  $R$ . In order to prove the second statement of the theorem, suppose that

$$(74.11) \quad M = (A_1, a_1) + \cdots + (A_r, a_r) + A_{r+1} + \cdots + A_n + Y$$

where  $Y$  has a finite  $Z$ -basis of  $t$  elements, where the  $\{A_i\}$  are  $R$ -ideals in  $K$ , and where  $a_i \in A_i$ ,  $a_i \notin (\theta - 1)A_i$ . We shall show that  $r + t, n, r$ , and the ideal class of  $A_1 \cdots A_n$  are indeed the canonical invariants of  $M$ , which will complete the proof of the theorem. It is easily seen that

$$M_s \cong A_1 + \cdots + A_n,$$

so that  $n = R\text{-rank of } M_s$ , as it should. Also,

$$M_s \cong A_1 + \cdots + A_n \cong R + \cdots + R + (A_1 \cdots A_n) \quad (n \text{ summands})$$

which shows that the ideal class of  $A_1 \cdots A_n$  is the ideal class invariant of  $M$ . Furthermore,

$$M/M_s \cong \underbrace{Z + \cdots + Z}_{r \text{ summands}} + Y$$

so that the  $Z$ -rank of  $M/M_s$  is  $r + t$ .

We must finally prove that  $r$  is the  $\bar{Z}$ -rank of  $(g - 1)M/(\theta - 1)M_s$ . Now  $(g - 1)Y = 0$ , and  $(g - 1)A_j = (\theta - 1)A_j$ ,  $r + 1 \leq j \leq n$ , so that it suffices to establish the following lemma:

(74.12) LEMMA. *Let  $A$  be an  $R$ -ideal in  $K$ , and let  $a_0 \in A$ ,  $a_0 \notin (\theta - 1)A$ . Then*

$$(g - 1)(A, a_0)/(\theta - 1)A \cong \bar{Z}.$$

PROOF. By definition,

$$(A, a_0) = A + Zy, \quad gy = a_0 + y, \quad ga = \theta a, \quad a \in A.$$

Therefore

$$(g - 1)(A, a_0) = (g - 1)A + Z(g - 1)y = (\theta - 1)A + Za_0.$$

However,  $(\theta - 1)A + Za_0$  is an ideal in  $A$  which properly contains  $(\theta - 1)A$ . Since  $(\theta - 1)A$  is a maximal ideal in  $A$ , we have  $A = (\theta - 1)A + Za_0$ . Hence

$$(g - 1)(A, a_0)/(\theta - 1)A \cong A/(\theta - 1)A \cong \bar{Z}.$$

This proves the lemma and also the theorem.

We may remark that if  $M = A + B$  is a  $ZG$ -module in which  $A, B$  are  $R$ -ideals in  $K$ , then

$$M \supset A \supset (0)$$

is a  $Z$ -composition series for  $M$ , so that  $M$  has  $Z$ -composition factors  $A, B$ . On the other hand,  $M \cong R + AB$ , the latter having  $Z$ -composition factors  $R, AB$ . Thus the  $Z$ -composition factors of a  $ZG$ -module are not uniquely determined by the module. This also shows that the indecomposable components of a  $ZG$ -module are not uniquely determined.

Further results on  $Z$ -representations of cyclic groups may be found in §81A.

### Exercises

1. Prove that  $Q \otimes_Z (A, a_0) \cong QG$  as left  $QG$ -modules.
2. Prove that  $(R, 1) \cong ZG$  as left  $ZG$ -modules.
3. Let  $a, a' \in A$ , where  $A$  is an  $R$ -ideal in  $K$ . If  $a \equiv a' \pmod{(\theta - 1)A}$ , prove that  $(A, a) \cong (A, a')$ .
4. Up to  $ZG$ -isomorphism, there are exactly  $2h + 1$  indecomposable  $ZG$ -

modules, given by

$$Z, B_1, \dots, B_h, (B_t, b_t) \quad (1 \leq t \leq h),$$

where  $B_1, \dots, B_h$  are representatives of the  $h$  distinct ideal classes of  $K$ , and where  $b_t \in B_t$ ,  $b_t \notin (\theta - 1)B_t$ .

### § 75. Modules over Orders

The following definitions and notations in this section will underlie the subsequent work of this chapter. Let  $R$  be a Dedekind domain with quotient field  $K$  (see § 18). Among the cases of particular interest to us are the following:<sup>†</sup>

- (i)  $R = Z, K = Q$ .
- (ii)  $R =$  principal ideal domain,  $K =$  quotient field of  $R$ .
- (iii)  $K =$  field with a discrete valuation,  $R =$  ring of elements of  $K$  which are integral with respect to the valuation (i.e.,  $R =$  valuation ring).
- (iv)  $K =$  algebraic number field,  $R =$  ring of all algebraic integers in  $K$ .

We shall be interested in representations of a finite group  $H$  by matrices with entries in  $R$ . Two such representations are said to be  $R$ -equivalent if they can be intertwined by a matrix unimodular<sup>‡</sup> over  $R$ , and  $K$ -equivalent if they can be intertwined by a non-singular matrix with entries in  $K$ . Obviously,  $R$ -equivalence implies  $K$ -equivalence but not conversely. Among other matters, we shall consider in some detail the relation between these two types of equivalence.

Instead of working with  $R$ -representations of  $H$ , it is often more convenient to deal with left  $RH$ -modules having finite  $R$ -bases. Each such module affords a set of mutually  $R$ -equivalent  $R$ -representations of  $H$ . As a matter of fact, it will be useful to consider the more general case of  $RH$ -modules which, as  $R$ -modules, are finitely generated and torsion free, but which need not have  $R$ -bases. [In case (ii), each such module will necessarily have an  $R$ -basis.]

<sup>†</sup> Of course, (i) and (iii) are both special cases of (ii). Also, (i) is a special case of (iv).

<sup>‡</sup> A square matrix  $S$  is *unimodular over  $R$*  if  $S$  has entries in  $R$ , and  $\det S =$  unit in  $R$ .

Furthermore, in most of our discussion the group  $H$  will play a somewhat secondary role, with primary emphasis placed upon the group ring  $RH$ . This group ring  $RH$  is a subring of the group algebra  $KH$ ;  $RH$  contains the unity element of  $KH$  as well as a  $K$ -basis of  $KH$ , and further,  $RH$  is a finitely generated  $R$ -module. This suggests the following definition:

(75.1) DEFINITION. Let  $A$  be a finite-dimensional algebra over  $K$ , with a unity element  $e$ . An  *$R$ -order in  $A$*  is a subset  $G$  of  $A$  which satisfies

- (1)  $G$  is a subring of  $A$ ,
- (2)  $e \in G$ ,
- (3)  $G$  contains a  $K$ -basis of  $A$ ,
- (4)  $G$  is a finitely generated  $R$ -module.

Thus,  $RH$  is an  $R$ -order in  $KH$ . As another example, the ring of all algebraic integers in an algebraic number field  $L$  is a  $Z$ -order in  $L$ .

(For a detailed discussion of orders in algebras, we refer the reader to Deuring [2] and Jacobson [1].

Questions concerning modules over  $Z$ -orders can be reformulated in terms of matrices with integral entries. Of the vast theory of integral matrices we have been able to include only those topics which are closely related to group representations. An excellent survey of the theory has recently been given by Taussky [1], where an extensive bibliography may be found.)

(The reader who is interested mainly in integral representations of groups may restrict himself to the special case  $G = RH$  in the following. He may then omit the part of this section from Theorem 75.11 to formula (75.21), inclusive, in which we give Higman's theory of orders in separable algebras, the main purpose of which is to obtain an analogue of the group order  $[H:1]$  in the general case. The reader should then continue with the remaining material in this section, taking  $i(G) = [H:1]$  in the discussion and proof of Theorem 75.25 and its corollaries.)

We embed  $K$  in  $A$  by the mapping  $\alpha \rightarrow \alpha e$ ,  $\alpha \in K$ ; this also embeds  $R$  in  $G$ . Given an  $A$ -module  $M^*$ , we shall always make  $M^*$  into a  $K$ -module by setting  $\alpha m = (\alpha e)m$ ,  $\alpha \in K$ ,  $m \in M^*$ . Since  $em = m$ ,  $m \in M^*$ , this makes  $M^*$  into a vector space over  $K$ . Similarly, a  $G$ -module  $M$  becomes a torsion-free  $R$ -module under the above definition. Throughout the rest of this chapter, we shall reserve the term  *$G$ -module* for left  $G$ -modules which are finitely

generated and torsion free as  $R$ -modules. Analogously, all  $A$ -modules will be assumed to be finite dimensional over  $K$ .

We have shown (see §§22 and 73) that a  $G$ -module  $M$  can be embedded in the  $A$ -module  $M^*$  where  $M^* = K \otimes_R M$ . Then  $M^*$  is a finite-dimensional  $K$ -space; we have defined the  $R$ -rank of  $M$  [denoted by  $(M : R)$ ] to be  $(M^* : K)$ . Then  $(M : R)$  is just the maximal number of  $R$ -free elements of  $M$ . The action of  $A$  on  $M^*$  is given by

$$(\alpha x)(\beta \otimes m) = \alpha \beta \otimes xm, \quad \alpha, \beta \in K, x \in G, m \in M.$$

The embedding of  $M$  in  $M^*$  is given by  $m \rightarrow 1 \otimes m$ ; we shall write  $M^* = KM$  to indicate that  $M^*$  consists of all  $K$ -linear combinations of the elements of  $M$ .

Analogously to Theorem 73.5, we have

(75.2) THEOREM. *Let  $M^*$  be an  $A$ -module such that  $(M^* : K) = n$ . Then  $M^*$  contains a  $G$ -module  $M$  of  $R$ -rank  $n$  such  $M^* = KM$ .*

PROOF. Let  $M^* = Km_1^* \oplus \cdots \oplus Km_n^*$ , and define

$$M = \sum_{j=1}^n GM_j^* = \left\{ \sum_j x_j m_j^* : x_j \in G \right\}.$$

Then

$$GM \subset \sum G^2 m_j^* \subset \sum Gm_j^* = M$$

since  $G$  is a ring. Next,  $M$  is a finitely generated  $R$ -module because  $G$  is. Further,  $e \in G$  implies that each  $m_j^* \in M$ , so that  $M^* = KM$ , and (75.2) is proved.

(75.3) COROLLARY [Compare Theorem 73.6]. *If  $R$  is a principal ideal ring, every  $K$ -representation of  $G$  is  $K$ -equivalent to an  $R$ -representation of  $G$ .*

PROOF. Any  $K$ -representation  $T$  of  $G$  can be extended to a  $K$ -representation  $T^*$  of  $A$ , and  $T^*$  is afforded by some  $A$ -module  $M^*$ . Then  $T$  is merely the restriction of  $T^*$  to  $G$ . Choose  $M$  as in Theorem 75.2. Since  $M$  is a finitely generated torsion-free  $R$ -module and  $R$  is a principal ideal ring, it follows that  $M$  has an  $R$ -basis. Relative to this basis,  $M$  affords an  $R$ -representation which is clearly  $K$ -equivalent to  $T$ . This proves the corollary.

If  $R$  is not a principal ideal ring,  $M$  need not have an  $R$ -basis, and the result no longer holds. It is nevertheless possible to salvage something from the above. Suppose  $R$  is the ring of the algebraic integers in the algebraic number field  $K$ , and let  $h$  be its class

number. In Theorem 20.14 we showed the existence of an extension field  $K'$ , where  $(K':K) \leq h$ , having ring of integers  $R'$ , with the property that to each  $R$ -ideal  $A$  in  $K$  there corresponds an element  $\alpha \in K'$  such that  $R'A = R'\alpha$ . In other words, all  $R'$ -ideals of  $K'$  which are induced by  $R$ -ideals of  $K$  are principal. We use this to prove a result which has already been used in Chapter V (see Exercise 33.1).

(75.4) COROLLARY. *Every  $K$ -representation  $\mathbf{T}$  of  $G$  is  $K'$ -equivalent to an  $R'$ -representation of  $G$ .*

PROOF. Define  $M^*$  and  $M$  as in the proofs of (75.2) and (75.3). By § 22, there exist elements  $m_1, \dots, m_n \in M$  and  $R$ -ideals  $A_1, \dots, A_n$  in  $K$  such that

$$M = A_1m_1 \oplus \cdots \oplus A_nm_n.$$

Then we have

$$M^* = Km_1 \oplus \cdots \oplus Km_n.$$

Now let  $M' = K' \otimes_K M^*$ ,  $A' = K' \otimes_K A$ , and regard  $M^*$  as embedded in  $M'$ , and  $A$  in  $A'$ . Then

$$M' = K'm_1 \oplus \cdots \oplus K'm_n.$$

If  $\mathbf{T}'$  is any  $K'$ -representation afforded by  $M'$ , then  $\mathbf{T}'|G$  is  $K'$ -equivalent to  $\mathbf{T}$ .

However, from the choice of  $K'$  we deduce the existence of elements  $\alpha_1, \dots, \alpha_n \in K'$  such that  $R'A_i = R'\alpha_i$ . Therefore

$$R'M = R'\alpha_1m_1 \oplus \cdots \oplus R'\alpha_nm_n.$$

Now  $R'M$  is a  $G$ -module having an  $R'$ -basis  $\{\alpha_1m_1, \dots, \alpha_nm_n\}$  and so affords an  $R'$ -representation  $\mathbf{U}$  of  $G$ . These elements are also a  $K'$ -basis of  $M'$ , relative to which  $M'$  affords the  $K'$ -representation  $\mathbf{T}'$  (say) with  $\mathbf{T}'|G = \mathbf{U}$ . Thus  $\mathbf{T}' \sim_{K'} \mathbf{U}$ , and the corollary is proved.

Along these lines, there is an interesting result due to Schur. As above, we suppose that  $R = \text{alg. int. } \{K\}$ , where  $K$  is an algebraic number field, and let  $h = \text{class number of } R$ . Then we have

(75.5) THEOREM. *If  $n$  is relatively prime to  $h$ , every  $n$ th degree  $K$ -representation of  $G$  is  $K$ -equivalent to an  $R$ -representation of  $G$ .*

PROOF. Any  $n$ th degree  $K$ -representation of  $G$  is afforded by some  $A$ -module  $M^*$  with  $(M^*:K) = n$ , by restriction of the operator domain from  $A$  to  $G$ . The theorem will be proved if we can show that  $M^*$  contains a  $G$ -submodule having a finite  $R$ -basis. We

already know that  $M^*$  contains a  $G$ -submodule  $M$  which is torsion-free and has  $R$ -rank  $n$ . By § 22, we may find elements  $x_1, \dots, x_n \in M$  such that

$$M = B_1 x_1 \oplus \cdots \oplus B_n x_n$$

where the  $\{B_i\}$  are  $R$ -ideals in  $K$ .

Now let  $A$  be any  $R$ -ideal in  $K$ , and form  $AM$ ; it is given by

$$AM = AB_1 x_1 \oplus \cdots \oplus AB_n x_n.$$

Then  $AM$  is also a  $G$ -submodule of  $M^*$ , and we know from § 22 that  $AM$  will have an  $R$ -basis if and only if the ideal

$$AB_1 \cdot AB_2 \cdots AB_n$$

is principal. The above ideal is just  $A^n B_1 \cdots B_n$ . But, since  $n$  is relatively prime to  $h$ , as  $A$  ranges over the representatives of all of the ideal classes, so does  $A^n$ . Hence we may choose  $A$  so that  $A^n B_1 \cdots B_n$  is principal, and this completes the proof of Schur's theorem.

We turn now to questions of reducibility and decomposability. A  $G$ -module is *decomposable* if it is expressible as a direct sum of two non-zero submodules; otherwise, it is *indecomposable*. A  $G$ -module  $M$  is  $R$ -reducible if  $M$  contains a non-zero  $G$ -submodule of smaller  $R$ -rank. An *irreducible*  $G$ -module is a non-zero  $G$ -module which is not  $R$ -reducible.

As in § 73, we have

(75.6) THEOREM. *Let  $M$  be a  $G$ -module embedded in the  $A$ -module  $M^* = KM$ . Then  $M$  is  $R$ -reducible if and only if  $M^*$  is reducible as an  $A$ -module.*

PROOF.  $R$ -reducibility of  $M$  obviously implies reducibility of  $M^*$ . Conversely, let  $N^*$  be a non-zero proper  $A$ -submodule of  $M^*$ . Then  $N = N^* \cap M$  is a non-zero  $G$ -submodule of  $M$  of smaller  $R$ -rank, so the theorem is established.

Note that in fact  $N$  is a pure  $R$ -submodule of  $M$ . Hence if  $M$  is reducible, it contains a  $G$ -submodule  $N$  such that  $0 < (N: R) < (M: R)$ , and such that  $N$  is a pure  $R$ -submodule of  $M$ . We may refer to  $N$  as an  $R$ -pure  $G$ -submodule of  $M$ , for brevity.

The analogues of  $Z$ -composition series and factors present no difficulties, and we shall assume that we know what are meant by  $R$ -composition series and  $R$ -composition factors of a  $G$ -module  $M$ . As before, the  $R$ -composition factors are not uniquely determined

by  $M$ , although the analogue of Theorem 73.13 is still valid.

We turn next to the concept of binding functions and shall merely outline the results, the proofs of which are entirely analogous to those given in §73. A *binding function* for the pair  $M_1, M_2$  of  $G$ -modules is an  $R$ -homomorphism  $F: G \rightarrow \text{Hom}_R(M_2, M_1)$  satisfying

$$(75.7) \quad F_{gh}(m) = gF_h(m) + F_g(hm), \quad g, h \in G, m \in M_2.$$

The set of all binding functions for the pair  $M_1, M_2$  forms an additive group  $B(M_1, M_2)$  which may be made into an  $R$ -module in a natural way. Since  $M_1, M_2$  and  $G$  are all finitely generated as  $R$ -modules, so also is  $B(M_1, M_2)$ . Clearly,  $B(M_1, M_2)$  is  $R$ -torsion-free.

An *inner binding function* for  $M_1, M_2$  is one of the form

$$(75.8) \quad F_g(m) = gDm - Dgm, \quad m \in M_2, g \in G.$$

for some  $D \in \text{Hom}_R(M_2, M_1)$ . The set of all inner binding functions forms an  $R$ -submodule  $B'(M_1, M_2)$  of  $B(M_1, M_2)$ , and we define

$$C(M_1, M_2) = B(M_1, M_2)/B'(M_1, M_2).$$

Each  $F \in B$  maps onto a coset  $[F] = F + B' \in C$ .

Given any  $F \in B(M_1, M_2)$ , we can define a  $G$ -module  $M$  denoted by  $(M_1, M_2; F)$ , as follows:

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

where addition is performed componentwise and where

$$(75.9) \quad g(m_1, m_2) = (gm_1 + F_g(m_2), gm_2), \quad g \in G, m_1 \in M_1, m_2 \in M_2.$$

If  $F$  and  $F'$  are elements of  $B(M_1, M_2)$  which differ by an inner binding function (or in other words,  $[F] = [F']$ ), then we have  $(M_1, M_2; F) \cong (M_1, M_2; F')$ .

On the other hand, if  $M$  is any  $G$ -module having a  $G$ -submodule  $N$  which is an  $R$ -direct summand of  $M$ , then there exists a binding function  $F \in B(N, M/N)$  such that

$$M \cong (N, M/N; F).$$

The binding function  $F$  need not be uniquely determined by the pair  $M, N$ , but its image  $[F]$  in  $C(N, M/N)$  is uniquely determined.

In the special case where  $G = RH$  is the group ring of a finite group  $H$ , we have as in Theorem 73.22, the basic result

(75.10) THEOREM. *If  $M_1, M_2$  are any pair of  $RH$ -modules, then*

$$[H:1] \cdot B(M_1, M_2) \subset B'(M_1, M_2).$$

We omit the proof, which is an obvious generalization of that

of Theorem 73.22.

We cannot proceed much further with the general case where  $G$  is an  $R$ -order in an algebra  $A$ , without having a generalization of the preceding theorem. It will be necessary to impose a further restriction on  $A$  in order to achieve this. We devote much of the remainder of this section to this topic. Let  $T$  be a  $(G, G)$ -bimodule, and define (compare with § 72)

$$B(T) = \{F \in \text{Hom}_R(G, T) : F_{gh} = gF_h + F_g h, g, h \in G\}.$$

Then  $B(T)$  is an  $R$ -module whose elements are called *1-cocycles*. Let  $B'(T)$  consist of all maps  $F \in \text{Hom}_R(G, T)$  for each of which there exists an element  $t \in T$  such that

$$F_g = gt - tg, \quad g \in G.$$

Then  $B'(T)$  is an  $R$ -submodule of  $B(T)$  whose elements are called *1-coboundaries*. The *1-cohomology group*  $C(T)$  is then defined by

$$C(T) = B(T)/B'(T)$$

and is again an  $R$ -module. Since we assume that  $T$  is finitely generated as  $R$ -module, so also are  $B(T)$ ,  $B'(T)$ , and  $C(T)$ .

[When we considered binding functions of a pair  $M_1, M_2$  of  $G$ -modules, we had in fact introduced the above ideas in a special case. For let

$$T = \text{Hom}_R(M_2, M_1),$$

and turn  $T$  into a  $(G, G)$ -bimodule by defining, for  $g \in G$  and  $t \in T$ ,

$$(gt)m_2 = g(tm_2), \quad (tg)m_2 = t(gm_2), \quad m_2 \in M_2.$$

We then have  $B(M_1, M_2) = B(T)$ ,  $B'(M_1, M_2) = B'(T)$ , and  $C(M_1, M_2) = C(T)$ .]

Now define the annihilator ideal  $\text{ann } C(T)$  as

$$\text{ann } C(T) = \{\alpha \in R : \alpha \cdot C(T) = 0\}.$$

Then  $\text{ann } C(T)$  is an ideal in  $R$ . The extreme cases where  $\text{ann } C(T) = (0)$  or  $R$  are both possible.

We now define

$$i(G) = \bigcap_T \text{ann } C(T),$$

where  $T$  ranges over all  $(G, G)$ -bimodules. Then  $i(G)$  is also an ideal in  $R$ . In the special case where  $G = RH$ , we have by Theorem 75.10 the result that

$$i(G) \supset [H:1]R,$$

and so  $i(G) \neq (0)$ . In the general case, the ideal  $i(G)$  will play the role of the group order (more precisely, of the ideal  $[H:1]R$  generated by the group order). We shall prove the following basic result of D. G. Higman [5]:

(75.11) THEOREM.  $i(G) \neq 0$  if and only if  $A$  is a separable algebra over  $K$ .

PROOF. Step 1. We begin by introducing a specific 1-cocycle  $F$  of a specific  $(G, G)$ -bimodule  $P$ , with the property that

$$i(G) = \{\alpha \in R : \alpha F \in B'(P)\}.$$

Form the tensor product  $G \otimes_R G$ , which is easily seen to be finitely generated and torsion free as  $R$ -module, using the results of §§12 and 22. We may view  $G \otimes_R G$  as a  $(G, G)$ -bimodule in an obvious way.

Now let  $P$  be the  $R$ -submodule of  $G \otimes_R G$  generated by the elements

$$\{x \otimes y - xy \otimes e : x, y \in G\}$$

where  $e$  is the unity element of  $A$  (and of  $G$ ). Then  $P$  is also a finitely generated torsion-free  $R$ -module which is a  $(G, G)$ -bimodule. Define  $F \in \text{Hom}_R(G, P)$  by

$$F(g) = e \otimes g - g \otimes e, \quad g \in G.$$

It is easily verified that  $F \in B(P)$ .

Define

$$\lambda(F) = \{\alpha \in R : \alpha F \in B'(P)\},$$

so that an element  $\alpha$  in  $R$  lies in  $\lambda(F)$  if and only if there exists an element  $p \in P$  such that

$$\alpha F(g) = gp - pg, \quad g \in G,$$

or equivalently,

$$(75.12) \quad \alpha(e \otimes g - g \otimes e) = gp - pg, \quad g \in G.$$

Step 2. We shall now show that  $\lambda(F) = i(G)$ . Since  $i(G) \cdot B(P) \subset B'(P)$ , the inclusion  $i(G) \subset \lambda(F)$  is obvious.

Suppose now that  $\alpha \in \lambda(F)$ , and let  $T$  be any  $(G, G)$ -bimodule and  $f$  any element of  $B(T)$ . If we can prove that  $\alpha f \in B'(T)$ , this will show that  $\lambda(F) \subset i(G)$ , and Step 2 will be proved. Since  $\alpha \in \lambda(F)$ , equation (75.12) holds for some  $p \in P$ .

Since  $f$  is an element of  $B(T)$ , we know that  $f \in \text{Hom}_R(G, T)$  and that

$$(75.13) \quad f(gh) = gf(h) + f(g)h, \quad g, h \in G.$$

Now define  $\mu: G \times G \rightarrow T$  by means of

$$\mu(x, y) = xf(y), \quad x, y \in G.$$

Then  $\mu$  is a balanced map (of  $R$ -modules), and so by §12 there exists a unique  $R$ -homomorphism  $\eta: G \otimes_R G \rightarrow T$  such that

$$\eta(x \otimes y) = xf(y), \quad x, y \in G.$$

Set  $\theta = \eta|_P$ , so that  $\theta \in \text{Hom}_R(P, T)$ . We have then

$$(\theta F)(g) = \theta(F(g)) = \theta(e \otimes g - g \otimes e) = f(g) - gf(e), \quad g \in G.$$

But from (75.13) we conclude that  $f(e) = 0$ , and thus  $f = \theta F$ . Therefore for  $g \in G$ ,

$$(\alpha f)(g) = \theta(\alpha F)(g) = \theta(gp - pg) = \theta(gp) - \theta(pg).$$

However, one easily checks that  $\theta(gp) = g\theta(p)$ , and  $\theta(pg) = p\theta(g)$ , since  $p$  is an  $R$ -linear combination of elements of the form  $x \otimes y - xy \otimes e$ . Thus

$$(\alpha f)(g) = g\theta(p) - \theta(p)g, \quad g \in G,$$

which proves that  $\alpha f \in B'(T)$ . This completes the proof of Step 2.

*Step 3.* Passing from  $G$  to  $A$ , we let  $i(A)$  be the intersection of the annihilators of the 1-cohomology groups of all  $(A, A)$ -bimodules. Let  $P^*$  be the  $K$ -submodule of  $A \otimes_K A$  generated by the elements  $\{x \otimes y - xy \otimes e : x, y \in A\}$ , and make  $P^*$  into an  $(A, A)$ -bimodule. Define  $F^* \in B(P^*)$  by

$$F^*(x) = e \otimes x - x \otimes e, \quad x \in A,$$

Then the previous step, with  $R$  replaced by  $K$ ,  $G$  by  $A$ ,  $P$  by  $P^*$ , and  $F$  by  $F^*$ , shows that

$$i(A) = \{\alpha \in K : \alpha F^* \in B'(P^*)\}.$$

We shall now show that

$$(75.14) \quad i(A) = K \cdot i(G).$$

Since each side is an ideal of  $K$ , each side is either  $(0)$  or  $K$ . If  $i(G) \neq 0$ , let  $\alpha$  be a non-zero element in  $i(G)$ . Then  $\alpha F \in B'(P)$ , whence obviously  $\alpha F^* \in B'(P^*)$ , and so  $\alpha \in i(A)$ . Thus if  $i(G) \neq 0$  then also  $i(A) \neq 0$ . Conversely, suppose that  $\alpha \in i(A)$ ,  $\alpha \neq 0$ . Then

there exists an element  $p^* \in P^*$  such that

$$\alpha F^*(g) = gp^* - p^*g, \quad g \in G.$$

Choose  $\delta \in R$ ,  $\delta \neq 0$ , such that  $\delta p^* \in P$  and also  $\delta\alpha \in R$ . Then

$$\delta\alpha F^*(g) = g(\delta p^*) - (\delta p^*)g, \quad g \in G,$$

proving that  $\delta\alpha \in i(G)$ , and so  $i(G) \neq 0$ .

*Remark.* Let  $S$  be a finite set of distinct prime ideals of  $R$ , and let  $R_S$  be the set of all elements  $K$  which are integral at each prime ideal  $P \in S$  [see the discussion following Theorem 19.7]. Then the above reasoning also establishes that

$$(75.15) \quad i(R_S G) = R_S \cdot i(G).$$

*Step 4.* Suppose, for the moment, that  $G$  has an  $R$ -basis  $\{g_1, \dots, g_n\}$ . We show that  $\alpha \in i(G)$  if and only if there exist elements  $\{g_1^*, \dots, g_n^*\}$  of  $G$  such that  $\alpha = \sum_{i=1}^n g_i^* g_i$ , and such that for  $g \in G$ ,

$$g_i g = \sum \alpha_{ij} g_j, \quad \alpha_{ij} \in R, \quad \text{implies} \quad gg_i^* = \sum \alpha_{ij} g_j^*.$$

For we know that  $\alpha \in i(G)$  if and only if (75.12) holds for some  $p \in P$ . We rewrite (75.12) as

$$(75.16) \quad g(p + e \otimes \alpha e) = (p + e \otimes \alpha e)g, \quad g \in G.$$

Since  $\{g_1, \dots, g_n\}$  is an  $R$ -basis of  $G$ , we may write

$$(75.17) \quad p + e \otimes \alpha e = \sum_{i=1}^n g_i^* \otimes g_i.$$

Condition (75.16) then becomes

$$(75.18) \quad \sum gg_i^* \otimes g_i = \sum g_i^* \otimes g_i g, \quad g \in G.$$

Set  $g_i g = \sum \alpha_{ij} g_j$ ,  $\alpha_{ij} \in R$ . Then (75.18) yields

$$\sum gg_i^* \otimes g_i = \sum_j \left( \sum_i g_i^* \alpha_{ij} \right) \otimes g_j.$$

However,  $G \otimes G = G \otimes g_1 \oplus \dots \oplus G \otimes g_n$ , so we must have

$$gg_i^* = \sum_i \alpha_{ij} g_j^*.$$

Next, the map  $\tau: G \times G \rightarrow G$  given by  $\tau(x, y) = xy$  is balanced (relative to  $R$ ). Hence there exists a unique  $R$ -homomorphism  $\mu: G \otimes G \rightarrow G$  given by

$$\mu(\sum x_i \otimes y_i) = \sum x_i y_i.$$

Since every element of  $P$  is an  $R$ -linear combination of expressions of the form  $x \otimes y - xy \otimes e$ , certainly  $\mu(P) = 0$ . Conversely,  $\mu(\sum x_i \otimes y_i) = 0$  implies

$$\sum x_i \otimes y_i = \sum (x_i \otimes y_i - x_i y_i \otimes e) \in P.$$

Hence  $P$  is the kernel of  $\mu$ .

Now apply  $\mu$  to both sides of (75.17). Then

$$\alpha = \alpha e = \sum_{i=1}^n g_i^* g_i.$$

All steps are reversible, and the assertion made at the beginning of the step is proved.

*Step 5.* Since  $A$  has a  $K$ -basis  $\{a_1, \dots, a_n\}$  (say), we have (by Step 4)  $\alpha \in i(A)$  if and only if there exist elements  $\{a_1^*, \dots, a_n^*\}$  in  $A$  such that  $\alpha = \sum a_i^* a_i$ , and such that for  $a \in A$ ,

$$aa = \sum \alpha_{ij} a_j, \quad \alpha_{ij} \in K, \quad \text{implies} \quad aa^* = \sum \alpha_{ji} a_j^*.$$

By Theorem 71.6 we then conclude that  $i(A) \neq (0)$  if and only if  $A$  is separable over  $K$ . From (75.14), we now deduce that  $i(G) \neq (0)$  if and only if  $A$  is separable over  $K$ . This completes the proof of Higman's theorem.

Let us make a closer study of the ideal  $i(G)$ , assuming to start with that  $A$  is a Frobenius algebra over  $K$ , having an invariant non-degenerate bilinear form  $f$ . We seek to characterize  $i(G)$  in terms of  $f$ . We define the *inverse different*

$$I(G) = \{a \in A : f(G, a) \subset R\},$$

which is clearly an  $R$ -module. Let us write

$$G = Rg_1 + \cdots + Rg_n, \quad g_i \in G,$$

which is possible since  $G$  is a finitely generated  $R$ -module. Then the map  $I(G) \rightarrow R + \cdots + R$  ( $n$  summands) given by

$$a \in I(G) \rightarrow (f(g_1, a), \dots, f(g_n, a))$$

is an  $R$ -isomorphism (since  $f$  is non-degenerate), and hence  $I(G)$  is also a finitely generated  $R$ -module. The above argument also shows that for each  $b \in A$ , there exists a non-zero  $\alpha \in R$  such that  $ab \in I(G)$ . Hence we have

$$K \cdot I(G) = A.$$

Define  $I(KG)$  as above, replacing  $G$  by  $KG$  and  $R$  by  $K$ . Also, let  $S$  denote a finite set of prime ideals in  $R$ , and define  $I(R_S G)$  by

replacing  $G$  by  $R_sG$ ,  $R$  by  $R_s$  in the above. We have shown that  $I(KG) = K \cdot I(G)$ . We now prove that

$$I(R_sG) = R_s \cdot I(G).$$

The inclusion  $R_s \cdot I(G) \subset I(R_sG)$  is obvious. Conversely, let  $a \in I(R_sG)$ . Then  $f(R_sG, a) \subset R_s$  implies  $f(G, a) \subset R_s$ , whence  $f(g_i, a) \in R_s$  for  $1 \leq i \leq n$ . We may therefore choose a unit  $\alpha \in R_s$  such that  $f(g_i, \alpha a) \in R$ ,  $1 \leq i \leq n$ . But then  $\alpha a \in I(G)$ , whence  $a \in \alpha^{-1} I(G) \subset R_s I(G)$ .

Next define the *different*

$$D(G) = \{x \in A : I(G) \cdot x \subset G\}.$$

As above, one easily verifies that  $D(G)$  is a finitely generated  $R$ -module and that

$$D(KG) = K \cdot D(G) = A, \quad D(R_sG) = R_s D(G).$$

Let  $c: A \rightarrow C$  be the Gaschütz-Ikeda operator\* associated with the form  $f$ , where  $C$  is the center of  $A$ . In Theorem 71.6 we saw that  $A$  was separable over  $K$  if and only if  $c(A) = C$ . We now prove:

(75.19) THEOREM.  $i(G) = c(D(G)) \cap R$ .

PROOF. Step 1. We show that  $c(D(G)) \cap R \neq (0)$  if and only if  $A$  is separable. We have

$$K(c(D(G)) \cap R) = c(D(KG)) \cap K = c(A) \cap K.$$

If  $A$  is separable, then  $c(A) \cap K = C \cap K = K \neq (0)$ . Conversely, if  $c(A) \cap K \neq (0)$ , then  $e \in c(A)$ ; since  $c(A)$  is an ideal in  $C$ , this shows  $c(A) = C$ , and so  $A$  is separable.

Step 2. For the remainder of the proof we may assume  $A$  separable over  $K$ . Suppose, in this step, that  $G$  has an  $R$ -basis  $\{g_1, \dots, g_n\}$ . These elements also form a  $K$ -basis for  $A$ , so there exist elements  $\{\bar{g}_1, \dots, \bar{g}_n\}$  of  $A$  such that  $f(g_i, \bar{g}_j) = \delta_{ij}$ ,  $1 \leq i, j \leq n$ . Then obviously

$$I(G) = R\bar{g}_1 \oplus \cdots \oplus R\bar{g}_n,$$

$$D(G) = \{x \in A : \bar{g}_j x \in G \text{ for } 1 \leq j \leq n\},$$

$$c(D(G)) = \{\sum \bar{g}_j x g_i : x \in D(G)\}.$$

Hence if  $a \in c(D(G))$ , we may write  $a = \sum g_i^* g_i$ , where  $g_i^* = \bar{g}_i x$

---

\* See (71.5) and the formula preceding it.

for some  $x$ , and we note that

$$(75.20) \quad g_i g = \sum \alpha_{ij} g_j, \quad \alpha_{ij} \in K \quad \text{implies} \quad gg_i^* = \sum \alpha_{ji} g_j^*. \quad .$$

If also  $a \in R$ , Step 4 of the proof of Theorem 75.11 implies that  $a \in i(G)$ . Hence

$$c(D(G)) \cap R \subset i(G).$$

*Step 3.* Keeping the hypotheses of Step 2, suppose that  $\alpha \in i(G)$ , and write  $\alpha = \sum g_i^* g_i$  for some elements  $\{g_1^*, \dots, g_n^*\}$  of  $G$  satisfying (75.20). Define  $\tau \in \text{Hom}_K(A, A)$  by  $\tau(\bar{g}_i) = g_i^*$ . For  $x \in G$ , we have

$$g_j x = \sum \xi_{jk} g_k \quad \text{implies} \quad x \bar{g}_j = \sum \xi_{kj} \bar{g}_k, \quad \xi_{jk} \in K,$$

so that

$$\tau(x \bar{g}_j) = \sum \xi_{kj} g_k^* = x g_j^* = x \tau(\bar{g}_j).$$

Hence  $\tau(xa) = x\tau(a)$  for all  $x, a \in A$ , and in particular

$$\tau(x) = x\tau(e) = xb, \quad \text{where } b = \tau(e).$$

Therefore,  $g_j^* = \bar{g}_j b$ ,  $1 \leq j \leq n$ . Since each  $g_j^* \in G$ , we see that  $b \in D(G)$ . Then

$$\alpha = \sum g_j^* g_j = \sum \bar{g}_j b g_j \in c(D(G)).$$

Hence  $i(G) \subset c(D(G)) \cap R$ . Combining the results of Steps 2 and 3, we have thus established the validity of the theorem for the case where  $G$  has an  $R$ -basis.

*Step 4.* Assume still that  $A$  is separable over  $K$ , but drop the hypothesis that  $G$  has an  $R$ -basis. Since  $A$  is separable, both  $i(G)$  and  $c(D(G)) \cap R$  are non-zero ideals in  $R$ . Let  $S$  be the set of all prime ideals occurring to a positive power in either of these ideals. Since  $R_S$  is a principal ideal ring,  $R_S G$  has an  $R_S$ -basis. Hence, by the results of the previous steps,

$$i(R_S G) = c(D(R_S G)) \cap R_S.$$

Therefore

$$\begin{aligned} R_S \cdot i(G) &= i(R_S G) = c(D(R_S G)) \cap R_S \\ &= R_S \{c(D(G)) \cap R\}. \end{aligned}$$

By the discussion in §19, this implies

$$i(G) = c(D(G)) \cap R,$$

and the theorem is proved.

Let us apply this theorem to the case where  $G = RH$ ,  $A = KH$ ,

and  $\text{char } K \nmid [H : 1]$ . Then  $A$  is certainly separable over  $K$ , and  $A$  is a Frobenius algebra with bilinear form  $f: A \times A \rightarrow K$  defined by

$$f(g, h) = \begin{cases} 0, & gh \neq 1, \\ 1, & gh = 1. \end{cases}$$

Let  $H = \{h_1, \dots, h_n\}$  where  $n = [H : 1]$ . Then  $\{h_1, \dots, h_n\}$  is an  $R$ -basis for  $G$ , and we have

$$f(h_i, h_j^{-1}) = \delta_{ij}, \quad 1 \leq i, j \leq n.$$

Hence  $I(G) = Rh_1^{-1} \oplus \cdots \oplus Rh_n^{-1} = G$ , and thence also  $D(G) = G$ . Therefore

$$i(G) = c(G) \cap R.$$

However, the elements of  $c(G)$  are of the form

$$(75.21) \quad \sum_i h_i^{-1} x h_i$$

where  $x \in G$ . The constant term in (75.21) is just  $\sum h_i^{-1} \alpha h_i$ , where  $\alpha$  is the constant term in  $x$ . Therefore

$$i(G) = c(G) \cap R = [H : 1]R,$$

as we promised at the beginning of the discussion.

To conclude this section, we shall obtain the decomposition of the 1-cohomology group  $C(T)$  of a  $(G, G)$ -bimodule  $T$  into its  $P$ -primary components, where  $P$  ranges over the prime ideal divisors of  $i(G)$ . We assume for this discussion that  $i(G) \neq 0$ , which is equivalent to the hypothesis that  $KG$  is a separable algebra over  $K$ . Since  $i(G) \cdot C(T) = 0$ , we see that  $C(T)$  is a torsion module (as  $R$ -module). We also know that  $C(T)$  is a finitely generated  $R$ -module.

Define the  $P$ -primary part of  $C(T)$  as

$$C_P(T) = \{[F] \in C(T) : P^a[F] = 0\}$$

where  $P^a$  is the power of  $P$  occurring in  $i(G)$ . Then clearly

$$(75.22) \quad C(T) = \sum_{P \mid i(G)} \bigoplus C_P(T).$$

Let  $R_P$  be the ring of  $P$ -integral elements of  $K$ . We shall prove that

$$(75.23) \quad C_P(T) \cong C(R_P T)$$

for each  $P$  dividing  $i(G)$ . Each  $F \in B(T)$  is an  $R$ -homomorphism of  $G$  into  $T$ , and hence can be extended to an  $R_P$ -homomorphism of

$R_P G$  into  $R_P T$ . We say briefly that we have extended  $F$  to an element of  $B(R_P T)$ , and this gives an embedding of  $B(T)$  in  $B(R_P T)$ . This embedding takes  $B'(T)$  into  $B'(R_P T)$ , and so induces a map of  $C(T)$  into  $C(R_P T)$ . This map surely gives an  $R$ -homomorphism of  $C_P(T)$  into  $C(R_P T)$ , and we assert that this is the desired isomorphism (75.23).

To begin with, we shall show that the map is “onto.” Let  $f \in B(R_P T)$  be arbitrary. Choose  $\pi \in P$  such that  $\pi \notin P^2$ . Then  $i(R_P G) = P^\alpha$ , and so  $\pi^\alpha f \in B'(R_P T)$ . Consequently, there exists an element  $u \in R_P T$  such that

$$(75.24) \quad \pi^\alpha f(g) = gu - ug, \quad g \in G.$$

Choose  $\beta \in R$  such that  $\beta \equiv 1 \pmod{P^\alpha}$  and also  $\beta u \in T$ . Then  $[(\beta - 1)f] = 0$  by (75.24), so  $[\beta f] = [f]$ . Replacing  $f$  by  $\beta f$  does not change the class  $[f]$ , and so we may assume hereafter that the element  $u$  occurring in (75.24) lies in  $T$ .

Now choose  $\xi \in R$  such that  $\xi \equiv 1 \pmod{P^{2\alpha}}$  and such that  $\xi/\pi^\alpha$  is integral at all primes except  $P$ . Set

$$F(g) = \xi \pi^{-\alpha} (gu - ug), \quad g \in G.$$

At  $P$ , we have  $F(g) \equiv f(g) \pmod{R_P T}$ , whence  $F(g) \in R_P T$  for each  $g \in G$ . At all other primes  $P' \neq P$ , surely  $F(g) \in R_{P'} T$ . Thus  $F(g) \in T$  for all  $g \in G$ , which implies that  $F \in B(T)$ . Furthermore,

$$\pi^\alpha(f(g) - F(g)) = (1 - \xi)(gu - ug), \quad g \in G,$$

so that  $\pi^\alpha(f - F) \in \pi^{2\alpha} B(R_P T)$ . This shows that  $(f - F) \in \pi^\alpha B(R_P T) \subset B'(R_P T)$ , and so  $[F] = [f]$  in  $B(R_P T)$ , which proves that  $C_P(T)$  maps onto  $C(R_P T)$ .

To show that the above defined map of  $C_P(T)$  onto  $C(R_P T)$  is an isomorphism, let  $f \in B(T)$  be such that  $P^\alpha[f] = 0$ , and suppose  $[f] = 0$  in  $C(R_P T)$ . Then choose  $u \in R_P T$  so that

$$f(g) = gu - ug, \quad g \in G.$$

Let  $\beta \in R$  be chosen such that  $\beta \equiv 1 \pmod{P^\alpha}$ ,  $\beta u \in T$ . Then  $\beta f \in B'(T)$ ,  $\pi^\alpha f \in B'(T)$ , whence also  $f \in B'(T)$ . Thus  $[f] = 0$  in  $C(R_P T)$  if and only if  $[f] = 0$  in  $C_P(T)$ .

We have therefore proved

(75.25) THEOREM (de Leeuw [1], Reiner [3]; see also Nunke [1]).  
For each  $(G, G)$ -bimodule  $T$  we have

$$C(T) \cong \sum_{P \mid \mathbb{Z}(G)} \bigoplus C(R_P T).$$

*Remark.* In the above summation, it suffices to let  $P$  range over all divisors of the annihilator ideal  $\text{ann } C(T)$ .

An obvious deduction from the preceding proof is

(75.26) COROLLARY. *Let  $F$  and  $F' \in B(T)$  be such that*

$$F_g \equiv F'_g \pmod{i(G)T} \quad \text{for all } g \in G.$$

*Then  $[F] = [F']$  in  $C(T)$ .*

Suppose now that  $M$  and  $N$  are a pair of  $G$ -modules, and set  $T = \text{Hom}_R(M, N)$ . As before we may make  $T$  into a  $(G, G)$ -bimodule, and the elements of  $B(T)$  are then called *binding functions* for the pair  $N, M$ . For this special case, we write  $B(N, M)$  instead of  $B(T)$ , with corresponding notation for  $B'$  and  $C$ .

For  $P$  a prime ideal in  $R$ , it is easily verified that

$$R_P \cdot \text{Hom}_R(M, N) = \text{Hom}_{R_P}(R_P M, R_P N),$$

from which we conclude that

$$C(R_P T) = C(R_P N, R_P M).$$

Therefore we have [as a consequence of Theorem 75.25]

$$(75.27) \quad C(N, M) \cong \sum_{P \mid i(G)} \bigoplus C(R_P N, R_P M).$$

We shall use this result repeatedly. In particular, let  $F \in B(N, M)$ , and form the module  $(N, M; F)$ . Then we have  $(N, M; F) \cong N + M$  if for each  $P$  dividing  $i(G)$ ,  $[F] = 0$  in  $C(R_P N, R_P M)$ .

### Exercises

- Carry out the proof of the analogue of Theorem 73.13 for the case in which  $M^*$  has exactly two composition factors.
  - Show by example that if  $M_1, M_2$  are  $G$ -modules, and  $E, F \in B(M_1, M_2)$ , then  $(M_1, M_2; E) \cong (M_1, M_2; F)$  need not imply that  $E - F \in B'(M_1, M_2)$ .
  - Give the details of the proof of Theorem 75.10.
  - Let  $P$  be a prime ideal in  $R$ , and define  $R_P$  to be the ring of  $P$ -integral elements of  $K$ . If  $P$  occurs with exponent  $m$  in  $i(G)$ , and if  $M_1, M_2$  are  $G$ -modules, prove that
- $$P^m \cdot B(R_P M_1, R_P M_2) \subset B'(R_P M_1, R_P M_2).$$
- Let  $G = ZH$ ,  $A = QH$ , where  $H$  is a cyclic group of prime order  $p$ . Let  $M_2$  be an ideal in the ring of integers of  $Q(\sqrt[p]{1})$ , and turn  $M_2$  into a  $G$ -module as in §74. Let  $M_1 = Z$  be a  $G$ -module on which  $H$  acts trivially. Discuss  $B(M_1, M_2)$ ,  $B'(M_1, M_2)$ , and prove that  $C(M_1, M_2)$  is a group with  $p$  elements.

6. Give the details of the proof that  $i(R_S G) = R_S \cdot i(G)$ .  
 7. Verify that  $D(G)$  is a finitely generated  $R$ -module and that  $D(R_S G) = R_S D(G)$ .

### § 76. *P*-Integral Equivalence

We shall assume familiarity with the results of § 19. Throughout this section, let  $K$  be a field with a discrete valuation  $| \cdot |$ , with valuation ring

$$R = \{\alpha \in K : |\alpha| \leq 1\}.$$

The ring  $R$  contains a unique maximal ideal  $P$ , given by

$$P = \{\alpha \in K : |\alpha| < 1\}.$$

There exists an element  $\pi \in P$  such that  $P = \pi R$ ; then  $P^n = \pi^n R$ ,  $n = 1, 2, \dots$ . The non-zero ideals of  $R$  are just  $R, P, P^2, \dots$ , all of which are principal.

Let  $K^*$  be the completion of  $K$  with respect to the valuation  $| \cdot |$ , and regard  $K$  as embedded in  $K^*$ . Let  $R^*$  be the valuation ring for  $K^*$  with maximal ideal  $P^*$ . Then we know that  $P^* = \pi R^*$  and that  $R/P \cong R^*/P^*$ .

In the material which follows, the reader who is interested primarily in finite groups may take  $A = KH$  (where  $H$  is a finite group and  $\text{char } K \nmid [H:1]$ ) and may assume that  $G = RH$  is the group ring of  $H$  over  $R$ . The ideal  $i(G)$  referred to below is then the principal ideal  $[H:1]R$  generated by the group order. This remark also applies to the material in the later sections.

Now let  $A$  be a separable algebra over  $K$ , with unity element  $e$ , and let  $G$  be an  $R$ -order in  $A$ . We define  $A^* = K^* \otimes_K A$ , and regard  $A$  as embedded in  $A^*$ . Then we may write  $A^* = K^*A$ , and  $A^*$  is separable over  $K^*$ . Similarly,  $G^* = R^*G$  is an  $R^*$ -order in  $A^*$ .

We have seen in § 75 that there exists a non-zero ideal  $i(G)$  in  $R$  which annihilates the 1-cohomology groups of all  $(G, G)$ -bimodules. Let us set

$$(76.1) \quad i(G) = \pi^{k_0} R.$$

Then for each pair  $M_1, M_2$  of  $G$ -modules, we have

$$(76.2) \quad \pi^{k_0} B(M_1, M_2) \subset B'(M_1, M_2).$$

Note that  $k_0 = 0$  if and only if every exact sequence of  $G$ -modules

splits. We leave as an exercise the fact that  $i(G^*) = \pi^{k_0} R^*$ .

As usual, let  $R_m$  denote the ring of  $m \times m$  matrices over  $R$ , and let  $I$  be the identity matrix.

(76.3) **DEFINITION.** By a  $P^k$ -modular representation of  $G$  of degree  $m$ , we mean a map  $\mathbf{T}: G \rightarrow R_m$  satisfying

$$(76.4) \quad \mathbf{T}_{g+h} \equiv \mathbf{T}_g + \mathbf{T}_h, \quad \mathbf{T}_{gh} \equiv \mathbf{T}_g \mathbf{T}_h, \quad \mathbf{T}_{\alpha g} \equiv \alpha \mathbf{T}_g, \quad \mathbf{T}_e \equiv I \pmod{P^k},$$

$g, h \in G, \alpha \in R$ . Two  $P^k$ -modular representations are equivalent if there exists a matrix  $X$  unimodular over  $R$  such that

$$X^{-1} \mathbf{T}_g X \equiv \mathbf{U}_g \pmod{P^k}, \quad g \in G.$$

(76.5) **DEFINITION.** Let  $\mathbf{T}, \mathbf{U}$  be  $P^k$ -modular representations of  $G$  of degrees  $t, u$ , respectively, and let  $\mathbf{L}$  be a map which assigns to each  $g \in G$  a  $t \times u$  matrix  $\mathbf{L}_g$  over  $R$ . We call  $\mathbf{L}$  a  $P^k$ -modular binding function for the pair  $\mathbf{T}, \mathbf{U}$  if

$$g \rightarrow \begin{pmatrix} \mathbf{T}_g & \mathbf{L}_g \\ \mathbf{0} & \mathbf{U}_g \end{pmatrix}, \quad g \in G,$$

is a  $P^k$ -modular representation of  $G$ . The set of all such maps  $\mathbf{L}$  forms an  $R$ -module  $B(\mathbf{T}, \mathbf{U}; P^k)$ . Necessary and sufficient conditions that  $\mathbf{L} \in B(\mathbf{T}, \mathbf{U}; P^k)$  are

$$(76.6) \quad \mathbf{L}_{g+h} \equiv \mathbf{L}_g + \mathbf{L}_h, \quad \mathbf{L}_{\alpha g} \equiv \alpha \mathbf{L}_g, \quad \mathbf{L}_{gh} \equiv \mathbf{T}_g \mathbf{L}_h + \mathbf{L}_g \mathbf{U}_h \pmod{P^k},$$

$g, h \in G, \alpha \in R$ . Let  $B'(\mathbf{T}, \mathbf{U}; P^k)$  be the  $R$ -submodule of  $B(\mathbf{T}, \mathbf{U}; P^k)$  consisting of all maps  $\mathbf{L}$  of the form

$$\mathbf{L}_g \equiv \mathbf{T}_g \mathbf{D} - \mathbf{D} \mathbf{U}_g \pmod{P^k}, \quad g \in G,$$

for some  $t \times u$  matrix  $\mathbf{D}$  over  $R$ . Then

$$(76.7) \quad \pi^{k_0} B(\mathbf{T}, \mathbf{U}; P^k) \subset B'(\mathbf{T}, \mathbf{U}; P^k),$$

the proof of which we leave as an exercise.

The results we shall give in this section are due mainly to Maranda [1], [2].

(76.8) **THEOREM.** Let  $\mathbf{T}, \mathbf{U}$  be  $R$ -representations of  $G$ . If  $\mathbf{T}, \mathbf{U}$  are  $R$ -equivalent, they are also equivalent mod  $P^k$  for each  $k$ . Conversely, if for some  $k > k_0$  we have  $\mathbf{T}, \mathbf{U}$  equivalent mod  $P^k$ , then  $\mathbf{T}, \mathbf{U}$  are also  $R$ -equivalent.

**PROOF.** The first statement is obvious. As to the second, let  $k > k_0$ , and suppose that  $\mathbf{T}, \mathbf{U}$  are equivalent mod  $P^k$ . Then there exists  $S$  unimodular over  $R$  such that

$$\mathbf{T}_g \mathbf{S} - \mathbf{S} \mathbf{U}_g \equiv \mathbf{0} \pmod{P^k}, \quad g \in G.$$

Let us set

$$\mathbf{L}_g = \pi^{-k}(\mathbf{T}_g \mathbf{S} - \mathbf{S} \mathbf{U}_g), \quad g \in G.$$

It is easily verified that  $\mathbf{L} \in B(\mathbf{T}, \mathbf{U})$ , so that there exists a matrix  $\mathbf{D}$  with entries in  $R$  such that

$$\pi^{k_0} \mathbf{L}_g = \mathbf{T}_g \mathbf{D} - \mathbf{D} \mathbf{U}_g, \quad g \in G.$$

This implies

$$\mathbf{T}_g (\mathbf{S} - \pi^{k-k_0} \mathbf{D}) = (\mathbf{S} - \pi^{k-k_0} \mathbf{D}) \mathbf{U}_g, \quad g \in G.$$

Since  $k > k_0$ ,

$$\det(\mathbf{S} - \pi^{k-k_0} \mathbf{D}) \equiv \det \mathbf{S} \not\equiv 0 \pmod{P},$$

so that  $\mathbf{S} - \pi^{k-k_0} \mathbf{D}$  is unimodular over the valuation ring  $R$ . Therefore  $\mathbf{T} \sim_R \mathbf{U}$ , and we are finished.

The corresponding result holds for  $R^*$ -representations of  $G^*$  when we replace  $P$  by  $P^*$ .

(76.9) COROLLARY. *Let  $\mathbf{T}, \mathbf{U}$  be  $R$ -representations of  $G$  of degree  $m$ . Then  $\mathbf{T} \sim_R \mathbf{U}$  if and only if  $\mathbf{T} \sim_{R^*} \mathbf{U}$ .*

PROOF. Clearly,  $R$ -equivalence implies  $R^*$ -equivalence. Conversely,  $\mathbf{T} \sim_{R^*} \mathbf{U}$  implies that  $\mathbf{T}, \mathbf{U}$  are equivalent mod  $P^{*k}$ , where  $k = k_0 + 1$ . Hence there exists a matrix  $\mathbf{S}^*$  unimodular over  $R^*$  such that

$$\mathbf{T}_g \mathbf{S}^* \equiv \mathbf{S}^* \mathbf{U}_g \pmod{P^{*k}}, \quad g \in G.$$

Since

$$R/P^k \cong R^*/P^{*k},$$

we may choose  $\mathbf{S} \in R_m$  such that  $\mathbf{S} \equiv \mathbf{S}^* \pmod{P^{*k}}$ . Then  $\mathbf{S}$  is unimodular over  $R$ , and

$$\mathbf{T}_g \mathbf{S} \equiv \mathbf{S} \mathbf{U}_g \pmod{P^k}, \quad g \in G.$$

By the preceding theorem we therefore conclude that  $\mathbf{T} \sim_R \mathbf{U}$ , which completes the proof of the corollary.

(76.10) COROLLARY. *For  $\mathbf{T}$  a fixed  $R$ -representation of  $G$  of degree  $m$ , let  $S(\mathbf{T})$  denote the set of all  $R$ -representations  $\mathbf{U}$  of  $G$  such that  $\mathbf{U} \sim_R \mathbf{T}$ . If  $R/P$  is a finite field, then  $S(\mathbf{T})$  splits into a finite number of classes with respect to  $R$ -equivalence.*

PROOF. Let  $k = k_0 + 1$ ; then since  $R/P$  is a finite field, we deduce (see Chapter III) that  $\hat{R} = R/P^k$  is a finite ring. Let us write

$$G = Rg_1 + \cdots + Rg_n, \quad g_i \in G.$$

For  $X \in R_m$ , let  $\hat{X}$  be obtained by replacing each entry of  $X$  by its residue class in  $\hat{R}$ . Now define, for  $U \in \mathcal{S}(T)$ ,

$$\sigma(U) = (\hat{U}_{g_1}, \dots, \hat{U}_{g_n}) \in \hat{R}_m + \cdots + \hat{R}_m.$$

If  $U, U' \in \mathcal{S}(T)$  are such that  $\sigma(U) = \sigma(U')$ , Theorem 76.8 implies that  $U \sim_R U'$ . Consequently, the number of classes into which  $\mathcal{S}(T)$  splits under  $R$ -equivalence cannot exceed the number of elements in the finite ring  $\hat{R}_m + \cdots + \hat{R}_m$ .

For our next result, we shall have to work with the complete field  $K^*$  rather than  $K$ .

(76.11) THEOREM. *Let  $W$  be an  $R^*$ -representation of  $G^*$ , and let  $k$  be some fixed integer greater than  $2k_0$ . Suppose  $W$  is reducible mod  $P^{*k}$ , that is, suppose there exists a matrix  $X$  unimodular over  $R^*$  such that*

$$X^{-1}W_g X \equiv \begin{pmatrix} T_g & L_g \\ 0 & U_g \end{pmatrix} \pmod{P^{*k}}, \quad g \in G^*.$$

*Then  $W$  is also  $R^*$ -reducible, and in fact*

$$W \sim_{R^*} \begin{pmatrix} T' & L' \\ 0 & U' \end{pmatrix}$$

*where for all  $g \in G^*$ ,*

$$(76.12) \quad T'_g \equiv T_g, \quad U'_g \equiv U_g \pmod{P^{*k-k_0}}.$$

PROOF. Replacing  $W$  by  $X^{-1}WX$ , we may assume that

$$W_g = \begin{pmatrix} T_g & L_g \\ \pi^k M_g & U_g \end{pmatrix}, \quad g \in G^*,$$

where each matrix  $T_g, L_g, M_g, U_g$  has entries in  $R^*$ . Then both  $T$  and  $U$  are  $P^{*k}$ -modular representations of  $G^*$ . The relation  $W_{gh} = W_g W_h (g, h \in G^*)$  readily implies that  $M \in B(U, T; P^{*k})$ , and so there exists a matrix  $D_1$  over  $R^*$  for which

$$(76.13) \quad \pi^{k_0} M_g \equiv U_g D_1 - D_1 T_g \pmod{P^{*k}}, \quad g \in G^*.$$

Now set

$$X_1 = \begin{pmatrix} I & 0 \\ -\pi^{k-k_0} D_1 & I \end{pmatrix}, \quad W_1 = X_1^{-1} W X_1 = \begin{pmatrix} T^{(1)} & L^{(1)} \\ N^{(1)} & U^{(1)} \end{pmatrix}.$$

Routine calculation shows that  $L_g^{(1)} = L_g$ , and

$$T_g^{(1)} = T_g - \pi^{k-k_0} L_g D_1, \quad U_g^{(1)} = U_g + \pi^{k-k_0} D_1 L_g,$$

$$N_h^{(1)} = \pi^{k-k_0} \{ \pi^{k_0} M_g - (U_g D_1 - D_1 T_g) \} - \pi^{2(k-k_0)} D_1 L_g D_1,$$

for all  $g \in G^*$ . Using (76.13) and the fact that  $k > 2k_0$ , it follows at once that we may write  $N_g^{(1)} = \pi^{k+1} M_g^{(1)}$ ,  $g \in G^*$ , where  $M_g^{(1)}$  has entries in  $R^*$ . Thus we have

$$W_1 = \begin{pmatrix} T^{(1)} & L^{(1)} \\ \pi^{k+1} M^{(1)} & U^{(1)} \end{pmatrix}.$$

By the same argument, we can find a matrix

$$X_2 = \begin{pmatrix} I & 0 \\ -\pi^{k+1-k_0} D_2 & I \end{pmatrix}$$

such that

$$W_2 = X_2^{-1} W_1 X_2 = \begin{pmatrix} T^{(2)} & L^{(2)} \\ \pi^{k+2} M^{(2)} & U^{(2)} \end{pmatrix},$$

and so on. However, the product  $X_1 X_2 \cdots$ , converges to

$$X' = \begin{pmatrix} I & 0 \\ \pi^{k-k_0}(D_1 + \pi D_2 + \cdots) & I \end{pmatrix},$$

and so the products  $(X_1 X_2 \cdots X_n)^{-1} W (X_1 X_2 \cdots X_n) = W_n$  also converge. But

$$\lim W_n = \begin{pmatrix} * & * \\ 0 & * \end{pmatrix},$$

and so we have

$$(X')^{-1} W X' = \begin{pmatrix} T' & L' \\ 0 & U' \end{pmatrix}$$

with (76.12) holding. This proves the theorem.

Let us set

$$(76.14) \quad \bar{K} = R/P = R^*/P^*, \quad \bar{G} = G/\pi G = G^*/\pi G^*.$$

Then  $\bar{G}$  is a finite-dimensional algebra over  $\bar{K}$ . For  $\alpha \in R$  (or  $\alpha \in R^*$ ), let  $\bar{\alpha}$  denote its image in  $\bar{K}$ ; similarly, for  $g \in G$  (or  $g \in G^*$ ), let  $\bar{g}$  denote its image in  $\bar{G}$ . These two uses of the bar are consistent by virtue of the embedding of  $R$  in  $G$ . For  $X = (\alpha_{ij}) \in R_m$ , let  $\bar{X} = (\bar{\alpha}_{ij}) \in \bar{K}_m$  and similarly for  $X \in R_m^*$ . Now let  $W$  be any  $R$ -representation of  $G$  of degree  $m$ , and define  $\bar{W}: \bar{G} \rightarrow \bar{K}_m$  by

$$\bar{W}_{\bar{g}} = \bar{W}_g, \quad g \in G.$$

Then  $\bar{W}$  is a  $\bar{K}$ -representation of  $\bar{G}$ . Obviously,  $W \sim_R U$  implies  $\bar{W} \sim_{\bar{K}} \bar{U}$ , though not conversely.

We may now state a corollary to Theorem 76.11.

(76.15) COROLLARY. Assume that  $k_0 = 0$ ; let  $W$  be an  $R^*$ -representation of  $G^*$ , and let  $\bar{W}$  be the  $\bar{K}$ -representation of  $\bar{G}$  associated with  $W$ . Then  $W$  is irreducible if and only if  $\bar{W}$  is irreducible.

PROOF. Reducibility of  $W$  obviously implies reducibility of  $\bar{W}$ . Conversely, reducibility of  $\bar{W}$  implies the existence of a non-singular matrix  $S$  with entries in  $\bar{K}$  such that

$$S^{-1} \bar{W} S = \begin{pmatrix} * & * \\ 0 & * \end{pmatrix}.$$

Choose  $X$  with entries in  $R^*$  such that  $\bar{X} = S$ . Then

$$X^{-1} W X \equiv \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \pmod{P^*}.$$

Thus  $W$  is reducible mod  $P^*$ , and hence [by Theorem 76.11]  $W$  is  $R^*$ -reducible. This completes the proof.

(76.16) COROLLARY. Let  $k_0 = 0$ , and let  $T, U$  be irreducible  $m$ th degree  $R^*$ -representations of  $G^*$ . Suppose there exists a non-zero  $X \in R_m^*$  such that

$$T_g X = X U_g, \quad g \in G^*.$$

Then we may write  $X = \pi^a X_1$  for some non-negative integer  $a$  and some  $X_1$  unimodular over  $R$ .

PROOF. By Corollary 76.15, we see that  $\bar{T}, \bar{U}$  are irreducible. Let  $\pi^a$  be the highest power of  $\pi$  which divides all entries of  $X$ , and write  $X = \pi^a X_1$ . Then  $\bar{X}_1 \neq 0$ , and

$$\bar{T}_{\bar{g}} \bar{X}_1 = \bar{X}_1 \bar{U}_{\bar{g}}, \quad \bar{g} \in \bar{G}.$$

Thus  $\bar{X}_1$  is a non-zero matrix intertwining the irreducible  $\bar{K}$ -representations  $\bar{T}, \bar{U}$ ; we conclude from Schur's lemma that  $\bar{X}_1$  is non-singular. This implies that  $X_1$  is unimodular over  $R^*$ , and the corollary is established.

(76.17) THEOREM. Assume  $k_0 = 0$ , and let  $T, U$  be  $R$ -representations of  $G$ . Then

$$T \sim_R U \iff T \sim_K U \iff \bar{T} \sim_{\bar{K}} \bar{U}.$$

PROOF. From Theorem 76.8, it follows that  $T$  and  $U$  are  $R$ -equivalent if and only if the representations  $\bar{T}$  and  $\bar{U}$  are  $\bar{K}$ -equivalent. Since  $R$ -equivalence implies  $K$ -equivalence, the only part that still requires proof is the statement that  $K$ -equivalence

implies  $R$ -equivalence. Assume therefore that  $\mathbf{T} \sim_K \mathbf{U}$ . Extend  $\mathbf{T}, \mathbf{U}$  to  $R^*$ -representations  $\mathbf{T}^*, \mathbf{U}^*$  of  $G^*$ ; then  $\mathbf{T} \sim_K \mathbf{U}$  implies  $\mathbf{T}^* \sim_{R^*} \mathbf{U}^*$ . If  $\mathbf{T}^*$  and  $\mathbf{U}^*$  are irreducible, Corollary 76.16 implies that  $\mathbf{T}^* \sim_{R^*} \mathbf{U}^*$ . By Corollary 76.9, we then deduce  $\mathbf{T} \sim_R \mathbf{U}$ .

On the other hand, suppose  $\mathbf{T}^*$  is reducible. Then from the discussion of composition series given in the preceding sections, it follows that we may write

$$\mathbf{T}^* \sim_{R^*} \begin{pmatrix} \mathbf{T}_1 & & * \\ & \ddots & \\ 0 & & \mathbf{T}_m \end{pmatrix}, \quad \mathbf{U}^* \sim_{R^*} \begin{pmatrix} \mathbf{U}_1 & & * \\ & \ddots & \\ 0 & & \mathbf{U}_m \end{pmatrix}$$

where  $\mathbf{T}_i \sim_{K^*} \mathbf{U}_i$ ,  $1 \leq i \leq m$ , and  $\mathbf{T}_1, \dots, \mathbf{T}_m$  are irreducible. However,  $k_0 = 0$  implies that  $B(\mathbf{T}_i, \mathbf{T}_j) \subset B'(\mathbf{T}_i, \mathbf{T}_j)$ , and also for the  $\mathbf{U}$ 's, and therefore

$$(76.18) \quad \mathbf{T}^* \sim_{R^*} \begin{pmatrix} \mathbf{T}_1 & & 0 \\ & \ddots & \\ 0 & & \mathbf{T}_m \end{pmatrix}, \quad \mathbf{U}^* \sim_{R^*} \begin{pmatrix} \mathbf{U}_1 & & 0 \\ & \ddots & \\ 0 & & \mathbf{U}_m \end{pmatrix}.$$

Since  $\mathbf{T}_i$  and  $\mathbf{U}_i$  are irreducible, the first half of the proof shows that from  $\mathbf{T}_i \sim_{K^*} \mathbf{U}_i$ , we may conclude  $\mathbf{T}_i \sim_{R^*} \mathbf{U}_i$ ,  $1 \leq i \leq m$ . Using (76.18), we then deduce that  $\mathbf{T}^* \sim_{R^*} \mathbf{U}^*$ , and again the theorem follows from Corollary 76.9.

(76.19) COROLLARY. *Assume  $k_0 = 0$ , and let  $W$  be any  $R$ -representation of  $G$ . Then the  $R$ -composition factors of  $W$  are uniquely determined up to  $R$ -equivalence and order of occurrence.*

In connection with Theorem 76.17, we may make the following observation. When  $k_0 \neq 0$ ,  $K$ -equivalence of a pair of  $R$ -representations does not, in general, imply their  $\bar{K}$ -equivalence. However, we shall show (Theorem 82.1) that if  $\mathbf{T}$  and  $\mathbf{U}$  are  $K$ -equivalent  $R$ -representations of  $G$ , then their associated modular representations  $\bar{\mathbf{T}}$  and  $\bar{\mathbf{U}}$  of  $\bar{G}$  have the same composition factors. (In particular, if  $k_0 = 0$ , then  $\bar{G}$  is semi-simple, and so this gives a second proof that  $K$ -equivalence implies  $\bar{K}$ -equivalence.)

Next we give an example to show that the conclusion of Corollary 76.19 need not hold when  $k_0 \neq 0$ . We take  $K = Q$ ,  $R = \text{ring of } 2\text{-adic integers in } Q$ , and let  $G = RH$ , where

$$H = \{a, b : a^4 = b^2 = (ab)^2 = 1\}.$$

In § 73, Example 2, the matrix representations  $\mathbf{T}_1$  and  $\mathbf{T}_2$  of  $G$  are  $R$ -representations which are  $K$ -equivalent but not  $R$ -equivalent. (Further, the associated representations  $\bar{\mathbf{T}}_1$  and  $\bar{\mathbf{T}}_2$  are not  $\bar{K}$ -equiva-

lent, though they have the same composition factors.) The representations of  $G$  given in (73.28) are  $R$ -equivalent but have different  $R$ -composition factors.

Next we shall prove the analogue of the Deuring-Noether theorem 29.7 for the case of integral representations in valuation rings. In the following, we let  $K$  be an algebraic number field,  $R$  a valuation ring in  $K$  with maximal ideal  $P$ , and suppose that  $K'$  is a finite extension field of  $K$ . In  $K'$  we choose any valuation ring  $R'$  containing  $R$ . Let  $A$  be a finite-dimensional algebra which is separable over  $K$ , and take  $G$  to be an  $R$ -order in  $A$ . (This includes the case  $A = KH$ ,  $G = RH$ , where  $H$  is a finite group.) Define  $k_0$  by (76.1), as before.

We now set

$$A' = K' \otimes_K A, \quad G' = R' \otimes_R G,$$

so that  $G'$  is an  $R'$ -order in the  $K'$ -algebra  $A'$ . To each  $G$ -module  $M$  there corresponds a  $G'$ -module

$$M' = R' \otimes_R M.$$

(76.20) THEOREM (Zassenhaus and Reiner [1]). *Let  $M$  and  $N$  be  $G$ -modules. Then  $M' \cong N'$  as  $G'$ -modules if and only if  $M \cong N$ .*

PROOF. It suffices to show that  $M' \cong N'$  implies  $M \cong N$ , the reverse implication being obvious. Set  $k = k_0 + 1$ , and define

$$\hat{R} = R/P^k, \quad \hat{R}' = R'/P^k R'.$$

We may then view  $\hat{R}$  as a subring of  $\hat{R}'$ . Furthermore, it is easily verified that  $\hat{R}'$  is a free  $\hat{R}$ -module with a finite basis. If we set

$$\hat{G} = G/P^k G, \quad \hat{G}' = G'/P^k G',$$

we find readily that

$$\hat{G}' = \hat{R}' \otimes_{\hat{R}} \hat{G}.$$

Similarly, for the  $G$ -module  $M$ , we let

$$\hat{M} = M/P^k M, \quad \hat{M}' = M'/P^k M',$$

and we have

$$(76.21) \quad \hat{M} = \hat{R}' \otimes_{\hat{R}} \hat{M}.$$

Thus  $\hat{M}$  is a  $\hat{G}$ -module, and by extension of the ground ring from  $\hat{R}$  to  $\hat{R}'$ , we obtain the  $\hat{G}'$ -module  $\hat{M}'$ .

If now  $M' \cong N'$ , then also  $\hat{M}' \cong \hat{N}'$  as  $\hat{G}'$ -modules. If  $\hat{R}'$  has  $\hat{R}$ -rank  $q$ , it follows from (76.21) that as  $\hat{G}$ -module,  $\hat{M}'$  is isomorphic to a direct sum of  $q$  copies of  $\hat{M}$ , and in addition  $\hat{N}'$  is direct sum of  $q$  copies of  $\hat{N}$ . Thus

$$\hat{M} + \cdots + \hat{M} \cong \hat{N} + \cdots + \hat{N} \quad \text{as } \hat{G}\text{-modules}$$

where  $q$  summands occur on each side. Letting  $\hat{M} = \sum M_i$ ,  $\hat{N} = \sum N_j$  be decompositions into indecomposable  $\hat{G}$ -submodules, we have

$$(76.22) \quad q(\sum M_i) = q(\sum N_j).$$

However,  $\hat{G}$  is a ring with minimum condition, and so the Krull-Schmidt theorem holds for  $\hat{G}$ -modules. From (76.22), we conclude that the  $\{M_i\}$  are (up to isomorphism) merely a rearrangement of the  $\{N_j\}$ , and thus  $\hat{M} \cong \hat{N}$ . Then  $M \cong N$  by Theorem 76.8, and we have finished the proof.

Turning next to questions of indecomposability, we have a basic theorem of Maranda's [1].

(76.23) THEOREM. *Let  $W$  be an  $R^*$ -representation of  $G^*$ , and assume that for some  $k > 2k_0$ ,  $W$  is decomposable mod  $P^{*k}$ , that is, there exists an  $R^*$ -unimodular  $X$  such that*

$$(76.24) \quad X^{-1}WX \equiv \begin{pmatrix} T & 0 \\ 0 & U \end{pmatrix} \quad (\text{mod } P^{*k}).$$

*Then  $W$  is also  $R^*$ -decomposable, and, in fact,*

$$W \sim_{R^*} \begin{pmatrix} T' & 0 \\ 0 & U' \end{pmatrix}$$

*with*

$$T'_g \equiv T_g, \quad U'_g \equiv U_g \quad (\text{mod } P^{*k-k_0}), \quad g \in G^*.$$

PROOF. Since (76.24) holds, we may apply Theorem 76.11 to conclude that

$$W \sim_{R^*} \begin{pmatrix} T'' & L \\ 0 & U'' \end{pmatrix}$$

for some  $L$ , with  $T'' \equiv T$ ,  $U'' \equiv U$  (mod  $P^{*k-k_0}$ ). Upon further transformation by permutation matrices, this yields

$$W \sim_{R^*} \begin{pmatrix} U'' & 0 \\ L & T'' \end{pmatrix}.$$

A second use of Theorem 76.11 completes the proof.

(We now sketch another proof of this result, and in fact of a stronger version thereof, due independently to Swan [unpublished] and Heller [1]. See also D. G. Higman [8].

Let  $M$  be a  $G^*$ -module, and set  $k = k_0 + 1$ ,  $\hat{G} = G^*/\pi^k G^*$ ,  $\hat{M} = M/\pi^k M$ , and so on. Then  $\hat{M}$  is a  $\hat{G}$ -module having an  $\hat{R}$ -basis. We show now that  $M$  is decomposable if and only if  $\hat{M}$  is decomposable. It is enough to show that if  $\hat{M}$  is decomposable so is  $M$ , the reverse implication being trivial.

We observe first that the proof of Theorem 76.8 can be easily modified so as to yield the following more general statement:

(76.25) *Let  $M$  and  $N$  be  $G^*$ -modules, and let  $\varphi \in \text{Hom}_{\hat{G}}(\hat{M}, \hat{N})$ , where  $\hat{G}, \hat{M}, \hat{N}$  are defined as above. Then there exists a pair of  $R^*$ -homomorphisms  $f$  and  $h$  of  $M$  into  $N$  such that  $\hat{f} = \varphi$  (where  $\hat{f}: \hat{M} \rightarrow \hat{N}$  is induced by  $f$ ) and such that  $f + \pi h \in \text{Hom}_{G^*}(M, N)$ .*

Let us make use of this result. Suppose that  $\hat{M}$  is a decomposable  $\hat{G}$ -module. Then we can find an idempotent  $\varphi \in \text{Hom}_{\hat{G}}(\hat{M}, \hat{M})$  such that  $\varphi \neq 1$ . Choose  $f$  and  $h$  as above, and set  $B = \text{Hom}_{G^*}(M, M)$ ; then  $f + \pi h \in B$ , and  $\hat{f} = \varphi$ . Therefore the image of  $f + \pi h$  in  $B/\pi B$  is idempotent. By the method of “lifting idempotents” given in §77, it follows that there exists an idempotent  $f' \in B$  such that  $f' \equiv f + \pi h \pmod{\pi B}$ . From  $\hat{f} = \varphi$  we find readily that  $f' \neq 0, 1$  and hence that  $M$  is decomposable.)

We shall use Theorem 76.23 to deduce the following result (Borevich and Faddeev [1, 11], Swan [4], Reiner [7], and Azumaya [1]).

(76.26) **THEOREM.** *The Krull-Schmidt theorem holds for  $G^*$ -modules; that is, if  $\{M_i\}$  and  $\{N_j\}$  are sets of indecomposable  $G^*$ -modules for which*

$$(76.27) \quad M_1 + \cdots + M_r \cong N_1 + \cdots + N_s,$$

*then  $r = s$ , and the  $\{M_i\}$  are (up to isomorphism) a rearrangement of the  $\{N_j\}$ .*

**PROOF.** Choose  $k = 2k_0 + 1$ , and let  $\hat{M} = M/\pi^k M$ , etc. From (76.27) we obtain

$$\hat{M}_1 + \cdots + \hat{M}_r \cong \hat{N}_1 + \cdots + \hat{N}_s,$$

and each of the above summands is indecomposable by Theorem 76.23. But  $\hat{G}$  is a ring with minimum condition, so the Krull-Schmidt theorem holds for  $\hat{G}$ -modules. Therefore  $r = s$ , and, renumbering the  $\{\hat{N}_j\}$  if need be, we have  $\hat{M}_i \cong \hat{N}_i$ ,  $i = 1, \dots, r$ . The conclusion now follows from Theorem 76.8.

Before proceeding to an extension of the above theorem due to Heller, we establish a useful fact. We shall say that a  $G^*$ -module  $M$  comes from a  $G$ -module  $M_0$  (by extension of the ground ring from  $R$  to  $R^*$ ) if  $M_0$  is a  $G$ -submodule of  $M$  having an  $R$ -basis of the same cardinality as an  $R^*$ -basis of  $M$  and such that  $M = R^*M_0$ .

(76.28) LEMMA (Heller [1]). *Let  $X$  be a  $G^*$ -module such that  $K^*X$  comes from some  $KG$ -module by extension of the ground field from  $K$  to  $K^*$ . Then  $X$  comes from a  $G$ -module.*

PROOF. Let  $V$  be any  $KG$ -module such that  $K^*V = K^*X$ , and set  $M = V \cap X$ . We shall show that  $M$  is the desired  $G$ -module from which  $X$  comes. Let us write

$$X = R^*b_1 \oplus \cdots \oplus R^*b_n.$$

Then  $K^*X = \sum K^*b_i$ , so  $(V:K) = n$ , and we may suppose that  $V = \sum Kc_i$ , where

$$c_i = \sum_{j=1}^n \sigma_{ij}b_j, \quad 1 \leq i \leq n, \quad \sigma_{ij} \in K^*.$$

The matrix  $S = (\sigma_{ij})$  is then invertible over  $K^*$ . Now choose a matrix  $T$  with entries in  $K$ , so that relative to the valuation of  $K^*$ , each entry of  $T$  lies very close to the corresponding entry of  $S^{-1}$ . In that case, the entries of  $TS$  are close to those of the identity matrix, which shows that  $TS$  is unimodular over  $R^*$ .

Let us write  $T = (\tau_{ij})$ , and set

$$c'_i = \sum_{j=1}^n \tau_{ij}c_j = \sum_{j,k=1}^n \tau_{ij}\sigma_{jk}b_k, \quad 1 \leq i \leq n.$$

Since  $T$  is invertible over  $K$ , we have  $V = \sum Kc'_i$ . Also since  $TS$  is unimodular over  $R^*$ , we conclude that  $X = \sum R^*c'_i$ . But then

$$M = V \cap X = (\sum Kc'_i) \cap (\sum R^*c'_i) = \sum_{i=1}^n R^*c'_i.$$

Clearly  $M$  is a  $G$ -module, has  $R$ -rank  $n$ , and  $X = R^*M$ , as desired.

(76.29) THEOREM (Heller [1]). *If  $K$  is a splitting field for the separable algebra  $KG$ , then the Krull-Schmidt theorem holds for  $G$ -modules.*

PROOF. It suffices to show that if  $M$  is an indecomposable

$G$ -module, then  $R^*M$  is an indecomposable  $G^*$ -module, for the result will then follow from the application of Theorems 76.26 and 76.9.

Since  $K$  is a splitting field for the separable algebra  $KG$ , each irreducible  $K^*G$ -module comes from some irreducible  $KG$ -module. Furthermore,  $K^*G$  is also separable, so every  $K^*G$ -module is a direct sum of irreducible modules. Thus, every  $K^*G$ -module comes from some  $KG$ -module, and so we shall be able to apply the preceding lemma.

Now let  $M$  be an indecomposable  $G$ -module, and suppose that  $R^*M$  is decomposable. By the preceding lemma, we can find  $G$ -modules  $M'$  and  $M''$  such that

$$R^*M = R^*M' \oplus R^*M''.$$

This implies that  $R^*M \cong R^*(M' \oplus M'')$ , and so (by Theorem 76.9)  $M \cong M' \oplus M''$ . Hence, if  $M$  is indecomposable, so is  $R^*M$ . This completes the proof.

## § 77. Projective Modules: Local Theory

We shall continue to use the notation and hypotheses introduced at the beginning of the previous section. We have shown there that the behavior of a  $G$ -module  $M$  is in some sense determined by its behavior mod  $P^k$  for sufficiently large  $k$ . We wish to consider next the question of whether  $M$  is a projective  $G$ -module, and to show that the answer depends only upon what happens mod  $P$ . The results of § 56 will be used freely.

(77.1) **THEOREM** (*Reiner [1], Nakayama [5-7]*). *A  $G$ -module  $M$  is projective if and only if the associated  $\bar{G}$ -module  $\bar{M}$  is projective, where  $\bar{M} = M/PM$ ,  $\bar{G} = G/PG$ .*

**PROOF.** If  $M$  is projective, then  $M$  is a direct summand of a free  $G$ -module. This clearly implies that  $\bar{M}$  is a direct summand of a free  $\bar{G}$ -module, and so  $\bar{M}$  is also projective.

Suppose conversely that  $\bar{M}$  is projective, and let us show that for each  $G$ -module  $N$  we have  $B(N, M) \subset B'(N, M)$ . This will imply that every exact sequence of  $G$ -modules

$$0 \rightarrow N \rightarrow L \rightarrow M \rightarrow 0$$

splits and hence that  $M$  is projective. Let  $F \in B(N, M)$  be arbitrary, and set  $V = (N, M; F)$ , the module whose elements are ordered pairs  $(n, m)$ ,  $n \in N$ ,  $m \in M$ , where addition is componentwise and where

$$g(n, m) = (gn + F(g)m, gm), \quad g \in G.$$

Then the associated  $\bar{G}$ -module  $\bar{V} = V/PV$  has the form  $\bar{V} = (\bar{N}, \bar{M}; \bar{F})$  where  $F$  induces the map  $\bar{F}$ . Since  $\bar{M}$  is projective, there exists a homomorphism  $\bar{t}_0 \in \text{Hom}_{\bar{R}}(\bar{M}, \bar{N})$  such that

$$\bar{F}(\bar{g}) = \bar{g}\bar{t}_0 - \bar{t}_0\bar{g}, \quad g \in G.$$

Now it is easily verified that

$$\overline{\text{Hom}_R(M, N)} \cong \text{Hom}_{\bar{R}}(\bar{M}, \bar{N}),$$

and so we may choose  $t_0 \in \text{Hom}_R(M, N)$  whose image is  $\bar{t}_0$ . Then for each  $g \in G$  the map

$$F(g) - (gt_0 - t_0g)$$

carries  $M$  into  $\pi N$ , where  $\pi$  is such that  $P = \pi R$ . Hence we may define  $F_1$  by

$$F_1(g) = \pi^{-1}\{F(g) - (gt_0 - t_0g)\}, \quad g \in G.$$

Since  $F_1$  also satisfies condition (75.8), we find that  $F_1 \in B(N, M)$ , and so  $(N, M; F_1)$  is also a  $G$ -module. Repeating the procedure, we may write

$$F_2(g) = \pi^{-1}\{F_1(g) - (gt_1 - t_1g)\}, \quad g \in G,$$

for some  $t_1 \in \text{Hom}_R(M, N)$  and some  $F_2 \in B(N, M)$ . Continuing in this way, we obtain

$$\begin{aligned} F(g) &= g(t_0 + \pi t_1 + \cdots + \pi^n t_n) \\ &\quad - (t_0 + \pi t_1 + \cdots + \pi^n t_n)g + \pi^{n+1} F_{n+1}(g), \end{aligned} \quad g \in G,$$

where each  $t_i$  lies in  $\text{Hom}_R(M, N)$ , and  $F_{n+1} \in B(N, M)$ . Choose  $n$  so large that  $\pi^{n+1} B(N, M) \subset B'(N, M)$ . Then the above equation shows that  $F \in B'(N, M)$ . This completes the proof.

Along the same lines, we show next that a projective  $G$ -module is completely determined by its behavior mod  $P$ .

(77.2) THEOREM (Swan [1], [2], [4]). *Let  $M$  and  $N$  be projective  $G$ -modules, and let bars denote passage to residues mod  $P$ . Then  $M \cong N$  if and only if  $\bar{M} \cong \bar{N}$ .*

PROOF. Surely  $M \cong N$  implies  $\bar{M} \cong \bar{N}$ , so that we need only consider the reverse implication. Let  $\theta: N \rightarrow \bar{M}$  be defined by

$$N \rightarrow N/PN \cong \bar{M},$$

and regard  $\bar{M}$  as a  $G$ -module by means of

$$g \cdot \bar{m} = \overline{gm}, \quad g \in G.$$

(The condition that  $\bar{M}$  be  $R$ -torsion-free no longer holds, but it does not affect the proof.) We have a diagram

$$\begin{array}{ccccccc} & & & M & & & \\ & & & \downarrow f & & & \\ 0 & \longrightarrow & PN & \longrightarrow & N & \xrightarrow{\theta} & \bar{M} \longrightarrow 0 \\ & & & & \downarrow t & & \\ & & & & \bar{M} & & \end{array}$$

where  $t: M \rightarrow \bar{M}$  is the mapping  $M \rightarrow M/PM$ . Since  $M$  is projective, there exists an  $f \in \text{Hom}_G(M, N)$  making the diagram commutative, that is,  $\theta f = t$ . We shall show that  $f: M \cong N$ .

For each  $n \in N$  we may choose an  $m \in M$  such that

$$\theta(n) = m + PM = tm = \theta f(m).$$

Therefore  $n - f(m) \in PN$ , and so we have proved that  $N = PN + f(M)$ . Hence

$$(77.3) \quad \frac{N}{f(M)} = \frac{PN + f(M)}{f(M)} = P \cdot \frac{N}{f(M)}.$$

If  $N/f(M) \neq 0$ , it follows from the structure theory of modules over a principal ideal ring that  $N/f(M)$  is a finite direct sum of a free module with finite basis and modules of the form  $R/P^\nu$ , and clearly for any such sum, equation (77.3) cannot hold.<sup>†</sup> Thus  $f(M) = N$ , and so  $f$  is "onto."

Next let  $M' = \text{kernel of } f$ . Thus there exists an exact sequence

$$0 \longrightarrow M' \longrightarrow M \xrightarrow{f} N \longrightarrow 0.$$

But  $N$  is projective, and so

$$M \cong M' + N.$$

Therefore  $\bar{M} \cong \bar{M}' + \bar{N}$ , which shows that  $\bar{M}' = 0$  (since all the modules involved are vector spaces over  $\bar{K}$ , and  $\bar{M} \cong \bar{N}$ ). This proves that  $PM' = M'$ , and so by the above argument  $M' = 0$ . Therefore  $M \cong N$ , and the result is proved.

It will now be necessary to work with the complete field  $K^*$  rather

---

<sup>†</sup> We have in fact proved: If  $L$  is a finitely generated  $R$ -module such that  $PL = L$ , then  $L = 0$ .

than with  $K$ . We have denoted by  $R^*$  the ring of  $P$ -adic integers in  $K^*$ . Then  $R^*$  is a principal ideal domain, and torsion-free  $R^*$ -modules will have  $R^*$ -bases. We shall discuss the method of “lifting idempotents,” which will be needed again in Chapter XII.

Set  $G^* = R^*G$ , and topologize  $G^*$  by saying that two elements  $x, y \in G^*$  are “close” if  $x - y$  lies in a high power of the ideal  $P^*G^*$ . However, it is easily verified that

$$(P^*G^*)^t = P^{*t}G^*, \quad t = 1, 2, \dots.$$

Thus, for  $x \in G^*$ , a complete system of neighborhoods of  $x$  is given by

$$x + G^* \supset x + P^*G^* \supset x + P^{*2}G^* \supset \dots,$$

whose intersection consists of the single element  $x$ . Indeed, for  $y \in G^*$ , let  $t$  be maximal such that  $y \in x + P^{*t}G^*$ , and set  $\rho(x, y) = 2^{-t}$ . Then  $G^*$  is a metric space with distance function  $\rho$ .

Now let  $\{x_1, \dots, x_m\}$  be an  $R^*$ -basis of  $G^*$ . The preceding discussion implies at once that given a sequence of elements of  $G^*$ , say

$$\sum_{i=1}^m \alpha_i^{(1)} x_i, \quad \sum_{i=1}^m \alpha_i^{(2)} x_i, \dots, \{\alpha_i^{(n)}\} \in R^*,$$

we have

$$\lim_{n \rightarrow \infty} \sum_{i=1}^m \alpha_i^{(n)} x_i = \sum_{i=1}^m \left( \lim_{n \rightarrow \infty} \alpha_i^{(n)} \right) x_i,$$

the existence of either side implying the existence of the other.

The map  $G^* \rightarrow G^*/P^*G^* = \bar{G}$  is a ring homomorphism. For  $x \in G^*$ , let  $\bar{x}$  denote its image in  $\bar{G}$ . We show that if  $e \in G^*$  is idempotent, so is  $\bar{e}$ . Since  $e^2 = e$ , clearly  $\bar{e}^2 = \bar{e}$ , and so we need show only that  $\bar{e} \neq 0$ . But if  $\bar{e} = 0$  then  $e \in P^*G^*$ , and thus

$$e^2 \in (P^*)^2 G^*, \quad e^3 \in (P^*)^3 G^*, \dots.$$

This shows that  $\lim_{n \rightarrow \infty} e^n = 0$ , which is impossible since  $e = e^2 = e^3 = \dots$ . Conversely, we have

(77.4) LEMMA. *Let  $\epsilon \in \bar{G}$  be idempotent. Then there exists an idempotent  $e \in G^*$  such that  $\bar{e} = \epsilon$ .*

PROOF. Step 1. For each  $n$ , we have

$$1 = (x + (1 - x))^{2n} = \sum_{j=0}^{2n} \binom{2n}{j} x^{2n-j} (1 - x)^j.$$

Set

$$(77.5) \quad f_n(x) = \sum_{j=0}^n \binom{2n}{j} \cdot x^{2n-j}(1-x)^j.$$

Then  $f_n(x) \in \mathbb{Z}[x]$ , and

$$(77.6) \quad f_n(x) \equiv 0 \pmod{x^n}, \quad f_n(x) \equiv 1 \pmod{(x-1)^n}.$$

Since  $f_n^2(x)$  also satisfies the above congruences, we conclude that

$$(77.7) \quad f_n^2(x) \equiv f_n(x) \pmod{x^n(x-1)^n}.$$

Replacing  $n$  by  $n-1$  in (77.6) further implies

$$(77.8) \quad f_n(x) \equiv f_{n-1}(x) \pmod{x^{n-1}(x-1)^{n-1}}.$$

Finally, direct computation shows

$$(77.9) \quad f_1(x) \equiv x \pmod{(x^2 - x)}.$$

*Step 2.* Let  $\varepsilon \in \bar{G}$  be idempotent, and choose  $a \in G^*$  such that  $\bar{a} = \varepsilon$ . Then  $\overline{a^2 - a} = \varepsilon^2 - \varepsilon = 0$ , so  $a^2 - a \in P^*G^*$ . Therefore

$$f_n(a) \equiv f_{n-1}(a) \pmod{P^{*n-1}G^*}, \quad n \geq 2,$$

and so  $\lim_{n \rightarrow \infty} f_n(a) = e$  exists in  $R^*G$ . Equation (77.7) implies that  $e^2 = e$ . On the other hand, we have

$$f_n(x) \equiv x \pmod{(x^2 - x)}, \quad n \geq 1,$$

so  $e \equiv a \pmod{P^*G^*}$ ; that is,  $\bar{e} = \bar{a} = \varepsilon$ . This completes the proof.

(77.10) **LEMMA.** *Let  $\varepsilon_1, \varepsilon_2$  be orthogonal idempotents in  $\bar{G}$  (that is,  $\varepsilon_1\varepsilon_2 = \varepsilon_2\varepsilon_1 = 0$ ), and let  $e \in G^*$  be any idempotent such that  $\bar{e} = \varepsilon_1 + \varepsilon_2$ . Then there exist orthogonal idempotents  $e_1, e_2 \in G^*$  such that*

$$e = e_1 + e_2, \quad \bar{e}_1 = \varepsilon_1, \quad \bar{e}_2 = \varepsilon_2.$$

**PROOF.** Choose  $a \in G^*$  such that  $\bar{a} = \varepsilon_1$ , and set  $b = eae \in G^*$ .

Then

$$\bar{b} = \bar{e}\bar{a}\bar{e} = (\varepsilon_1 + \varepsilon_2)\varepsilon_1(\varepsilon_1 + \varepsilon_2) = \varepsilon_1, \quad be = eb = b.$$

Therefore  $b^2 - b \in P^*G^*$ , whence  $\{f_n(b)\}$  converges to an idempotent  $e_1 \in G^*$  such that

$$\bar{e}_1 = \bar{b}_1 = \varepsilon_1, \quad e_1e = ee_1 = e_1.$$

Setting  $e_2 = e - e_1$ , we see that  $e_2$  is idempotent, and

$$e_1e_2 = e_2e_1 = 0, \quad \bar{e}_2 = \bar{e} - \bar{e}_1 = \varepsilon_2.$$

This proves the result.

We have seen that there is a one-to-one correspondence between

decompositions of a group algebra into a direct sum of left ideals and decompositions of 1 into a sum of orthogonal idempotents. Let 1 denote the identity in  $G^*$ ,  $\bar{1}$  in  $\bar{G}$ .

(77.11) THEOREM. *Let  $\bar{1} = \varepsilon_1 + \cdots + \varepsilon_n$  be a decomposition into orthogonal idempotents in  $\bar{G}$ . Then there exist orthogonal idempotents  $e_1, \dots, e_n$  in  $G^*$  such that*

$$1 = e_1 + \cdots + e_n, \quad \bar{e}_1 = \varepsilon_1, \dots, \bar{e}_n = \varepsilon_n.$$

PROOF. The result is trivial for  $n = 1$ . Assume  $n > 1$  and that the result holds at  $n - 1$ . Set  $\delta = \varepsilon_{n-1} + \varepsilon_n$ . Then

$$\bar{1} = \varepsilon_1 + \cdots + \varepsilon_{n-2} + \delta$$

is an orthogonal decomposition, so by the induction hypothesis there exist orthogonal idempotents  $e_1, \dots, e_{n-2}, e \in R^*G$  such that

$$1 = e_1 + \cdots + e_{n-2} + e, \quad \bar{e}_1 = \varepsilon_1, \dots, \bar{e}_{n-2} = \varepsilon_{n-2}, \bar{e} = \delta.$$

Lemma 77.10 shows the existence of orthogonal idempotents  $e', e'' \in R^*G$  such that  $e = e' + e'', \bar{e}' = \varepsilon_{n-1}, \bar{e}'' = \varepsilon_n$ . Then  $1 = e_1 + \cdots + e_{n-2} + e' + e''$ , and it is easily verified that this is an orthogonal decomposition. The result has thus been proved.

We now combine Swan's theorem 77.2 with the preceding theorem on lifting idempotents to obtain a characterization of the projective  $G^*$ -modules.

Let

$$\bar{G} = \bar{G}\varepsilon_1 \oplus \cdots \oplus \bar{G}\varepsilon_m$$

be a decomposition of the left regular module  $\bar{\sigma}\bar{G}$  into indecomposable submodules, where

$$\bar{1} = \varepsilon_1 + \cdots + \varepsilon_m$$

is the corresponding decomposition of  $\bar{1}$  into orthogonal idempotents  $\{\varepsilon_i\}$ . These  $\{\bar{G}\varepsilon_i\}$  are then the principal indecomposable modules of  $\bar{G}$ , and we may suppose them indexed so that no two of

$$\bar{G}\varepsilon_1, \dots, \bar{G}\varepsilon_r$$

are isomorphic, and each  $\bar{G}\varepsilon_j$ ,  $r < j \leq m$ , is isomorphic to one of the above.

By Theorem 77.11, there exist orthogonal idempotents  $\{e_i\}$  such that  $\bar{e}_i = \varepsilon_i$ ,  $1 \leq i \leq m$ , and

$$G^* = G^*e_1 \oplus \cdots \oplus G^*e_m.$$

Each  $G^*e_i$  is projective, and we have  $\overline{G^*e_i} = \bar{G}\varepsilon_i$ ,  $1 \leq i \leq m$ . From

Theorem 77.2, we conclude that  $G^*e_i \cong G^*e_j$  if and only if  $\bar{G}e_i \cong \bar{G}e_j$ .

We now show

(77.12) THEOREM.<sup>†</sup> *Each projective  $G^*$ -module  $M$  is of the form*

$$M \cong a_1(G^*e_1) + \cdots + a_r(G^*e_r), \quad a_i \geq 0, a_i \in \mathbb{Z},$$

*where the right-hand side denotes an external direct sum  $a_i$  of whose summands are  $G^*e_1, \dots, a_r$  of whose summands are  $G^*e_r$ . The non-negative integers  $\{a_i\}$  are uniquely determined by  $M$ .*

PROOF. From Theorem 77.1, we know that  $\bar{M}$  is projective as  $\bar{G}$ -module. By Theorem 56.6, we may therefore write

$$\bar{M} \cong a_1(\bar{G}e_1) + \cdots + a_r(\bar{G}e_r), \quad a_i \geq 0, a_i \in \mathbb{Z}.$$

Set

$$N = a_1(G^*e_1) + \cdots + a_r(G^*e_r).$$

Then  $N$  is projective and  $\bar{M} \cong \bar{N}$ , whence by Theorem 77.2 also  $M \cong N$ . This proves the result.

(77.13) COROLLARY. *Let  $M$  be a projective  $G^*$ -module. Then  $M$  is free if and only if  $\bar{M}$  is free.*

We must now abandon our general approach and restrict ourselves to the case  $G = RH$ ,  $H =$  finite group,  $R =$  valuation ring in an algebraic number field  $K$ . For this special case, we now prove a remarkable result which asserts that a projective  $G$ -module is completely determined by its behavior over the field  $K$ . To save space, we shall not give Swan's original proof, but rather shall follow the method suggested by Rim (unpublished) and Giorgiutti [1] (see also Bass [1]) which makes use of a result that will be derived in Chapter XII.

(77.14) THEOREM (Swan [1], [2], [4]). *Let  $M$  and  $N$  be projective  $RH$ -modules, where  $H$  is a finite group. Then  $M \cong N$  if and only if  $KM \cong KN$ , where as usual we have embedded  $M$  in  $KM = K \otimes M$ , and  $N$  in  $KN$ .*

PROOF. We need prove only that  $KM \cong KN$  implies  $M \cong N$ , the reverse implication being trivial. Choose a field  $K'$  which is a finite extension of  $K$  and which is a splitting field for  $H$ , and let

---

<sup>†</sup> The result can also be deduced readily from the Krull-Schmidt theorem 76.26 for  $G^*$ -modules. The relation between decompositions of  $\bar{G}$  and  $G^*$  will be needed later on, however.

$R'$  be the valuation ring of  $K'$  arising from any extension of the given valuation from  $K$  to  $K'$ . Then  $KM \cong KN$  implies  $K'M' \cong K'N'$ , where

$$M' = R'M (= R' \otimes_R M), \quad N' = R'N.$$

Surely  $M'$  and  $N'$  are projective  $R'H$ -modules, and we shall show that if  $K'M' \cong K'N'$  then also  $M' \cong N'$ . From Theorem 76.20, it will follow that  $M \cong N$ , and the theorem will be proved.

Let  $P'$  be the unique maximal ideal of  $R'$ , and set  $\bar{K}' = R'/P'$ ,  $\bar{M}' = M'/P'M'$ ,  $\bar{N}' = N'/P'N'$ . In Chapter XII (Theorem 82.1) we shall show that the isomorphism  $K'M' \cong K'N'$  implies that  $\bar{M}'$  and  $\bar{N}'$  have the same composition factors. Let us write

$$\bar{K}'H = \sum_{i=1}^m \bar{K}'H \cdot \varepsilon_i,$$

a sum of indecomposable submodules, so numbered that those modules for  $1 \leq i \leq r$  give all non-isomorphic modules among the above. Then we have, since  $\bar{M}'$  and  $\bar{N}'$  are projective,

$$\bar{M}' = \sum_{i=1}^r a_i(\bar{K}'H \cdot \varepsilon_i), \quad \bar{N}' = \sum_{i=1}^r b_i(\bar{K}'H \cdot \varepsilon_i),$$

where the  $\{a_i\}$  and  $\{b_i\}$  are non-negative integers. With each principal indecomposable module  $\bar{K}'H \cdot \varepsilon_i$  is associated an irreducible module

$$F_i = \frac{\bar{K}'H \cdot \varepsilon_i}{(\text{rad } \bar{K}'H) \varepsilon_i}, \quad 1 \leq i \leq r,$$

and we have shown in Chapter VIII that  $F_1, \dots, F_r$  are a full set of irreducible  $\bar{K}'H$ -modules. Set

$$\bar{K}'H \cdot \varepsilon_i \approx \sum_{j=1}^r c_{ij} F_j, \quad 1 \leq i \leq r,$$

the above indicating that each  $F_j$  occurs  $c_{ij}$  times as a composition factor of  $\bar{K}'H \cdot \varepsilon_i$ . In Chapter XII, we shall prove that the *Cartan matrix*  $(c_{ij})$  is non-singular. Taking this for granted, we have

$$\bar{M}' \approx \sum_{i,j} a_i c_{ij} F_j, \quad \bar{N}' \approx \sum_{i,j} b_i c_{ij} F_j.$$

Since  $\bar{M}'$  and  $\bar{N}'$  have the same composition factors, this gives

$$\sum_i (a_i - b_i) c_{ij} = 0, \quad 1 \leq j \leq r.$$

Therefore  $a_i = b_i$  for  $1 \leq i \leq r$  since  $(c_{ij})$  is non-singular, and conse-

quently  $\bar{M}' \cong \bar{N}'$ . Theorem 77.2 now implies that  $M' \cong N'$ , and so the result is established.

*Remark.* Swan's original proof of this theorem provides a new proof of the non-singularity of the Cartan matrix  $(c_{ij})$ . His argument requires the Artin induction theorem and some knowledge of Grothendieck rings. See also Hattori [1].

### Exercise

- Suppose that the center of  $G^*$  maps onto the center of  $\bar{G}$ . Let  $\epsilon$  be a central idempotent in  $\bar{G}$ . Show that there exists a central idempotent  $e \in R^*G$  such that  $\bar{e} = \epsilon$ . Further, if  $f \in R^*G$  is any idempotent such that  $\bar{f} = \epsilon$ , prove that  $f = e$ . [Hint: In Step 2 of the proof of Lemma 77.4, show that if  $\epsilon$  is a central idempotent, the element  $a \in G^*$  such that  $\bar{a} = \epsilon$  may be chosen from the center of  $G^*$ . Use this fact to conclude that the idempotent  $e$  constructed in Lemma 77.4 is central. Then show that  $f(1 - e)$  and  $e(1 - f)$  are equal to their own squares, lie in  $P^*G^*$ , and hence are 0.]

## § 78. Projective Modules: Global Theory

The following notations will be used throughout this section:  $H$  = finite group,  $K$  = algebraic number field,  $R$  = alg. int.  $\{K\}$ ,  $P$  = prime ideal in  $R$ ,  $R_P$  =  $P$ -adic integers in  $K$ ,  $\bar{K} = R/P$ . An  $RH$ -module shall mean a left  $RH$ -module which, as  $R$ -module, is finitely generated and torsion-free. (An  $R_PH$ -module is defined analogously, replacing  $R$  by  $R_P$ .) With each  $RH$ -module  $M$  is associated the  $\bar{K}H$ -module  $\bar{M} = M/PM$ . If  $M$  is projective, then  $M$  is a direct summand of a free  $RH$ -module, and consequently  $\bar{M}$  is a direct summand of a free  $\bar{K}H$ -module, which shows that  $\bar{M}$  is also projective. The following result shows that projectivity can be characterized locally:

(78.1) **THEOREM** (Reiner [1], Nakayama [5]–[7]). *An  $RH$ -module  $M$  is projective if and only if, for each  $P$  dividing  $[H:1]$ , the associated module  $\bar{M} = M/PM$  is  $\bar{K}H$ -projective.*

**PROOF.** In view of the preceding remarks, it suffices to show that if for each  $P$  dividing  $[H:1]$  the module  $M/PM$  is projective, then so is  $M$ . Now we note that  $M$  is projective if and only if the 1-cohomology group  $C(N, M) = 0$  for each  $RH$ -module  $N$ , since this requirement is equivalent to the condition that every exact sequence

$$0 \rightarrow N \rightarrow L \rightarrow M \rightarrow 0$$

of  $RH$ -modules should split. Using Theorem 75.25, we have

$$C(N, M) \cong \sum_{P \in [H:1]} \bigoplus C(R_P N, R_P M).$$

Thus our result will be established once we show that if  $M/PM$  is projective, so is  $R_P M$ . But this is precisely what we showed in Theorem 77.1, since  $R_P/PR_P \cong \bar{K}$ , and so the theorem is proved.

We shall now prove the fundamental result that if  $M$  is a projective  $RH$ -module, then  $KM$  is  $KH$ -free. An easy consequence of this fact is the result that for each prime ideal  $P$  of  $R$ , the module  $M/PM$  is free as  $(R/P)H$ -module.

As preliminary to the proof, we recall some concepts from §43. Let  $L$  be an  $RH$ -module; an element  $l \in L$  was called *H-invariant* if  $hl = l$  for all  $h \in H$ . The set  $L'$  of  $H$ -invariant elements of  $L$  is an  $RH$ -submodule of  $L$ , and it is easily verified that  $L'$  is a pure  $R$ -submodule of  $L$ . Furthermore,

$$(L \oplus M)' = L' \oplus M',$$

if  $L$  and  $M$  are arbitrary  $RH$ -modules.

A straightforward calculation shows that

$$(RH)' = R \cdot \sum_{h \in H} h,$$

so that

$$(RH:R) = [H:1]((RH)':R).$$

Consequently

$$(L:R) = [H:1](L':R)$$

for each free  $RH$ -module  $L$ . A corresponding formula holds when  $R$  is replaced by  $R_P$ .

Now let  $L$  be an arbitrary  $RH$ -module, where  $H = H_1 \times H_2$ , and set

$$L_1 = \{l \in L : h_1 l = l \text{ for all } h_1 \in H_1\}.$$

Then  $L'$  is precisely the set of  $H_2$ -invariant elements of  $L_1$ . In the special case where  $L = RH$ , we see easily that

$$L_1 = RH_2 \cdot \sum_{h \in H_1} h.$$

Hence, more generally, whenever  $L$  is  $RH$ -free, the module  $L_1$  is  $RH_2$ -free.

Returning to the general situation, suppose next that  $L$  is a projective  $RH$ -module, where  $H = H_1 \times H_2$ . Then  $L$  is a direct summand of some free  $RH$ -module  $F$ ; let  $F = L \oplus M$  for some  $RH$ -module  $M$ . If  $F_1$  denotes the set of  $H_1$ -invariant elements of  $F$ , and

$M_1$  that of  $M$ , then  $F_1 = L_1 \oplus M_1$ . The argument in the preceding paragraph shows that  $F_1$  is  $RH_2$ -free, whence  $L_1$  is  $RH_2$ -projective. We shall need this fact presently.

One further preliminary is necessary.

(78.2) LEMMA. i) Let  $H_1$  be a  $p$ -group, let  $P$  be a prime ideal of  $R$  containing  $p$ , and set  $\bar{K} = R/P$ . If  $M_1$  is a projective  $RH_1$ -module, then  $\bar{M}_1$  is  $\bar{K}H_1$ -free.

ii) Let  $M$  be  $RH$ -projective, where  $H$  is an arbitrary group. Then  $[H:1]$  divides  $(M:R)$ .

PROOF. i) From Theorem 78.1 it follows that  $\bar{M}_1$  is  $\bar{K}H_1$ -projective. But  $H_1$  is a  $p$ -group, and  $\bar{K}$  has characteristic  $p$ , so by Exercise 54.1 it follows that  $\bar{K}H_1$  is indecomposable as left  $\bar{K}H_1$ -module. Thus every projective  $\bar{K}H_1$ -module is  $\bar{K}H_1$ -free, proving (i). We deduce further that  $[H_1:1]|(M_1:R)$ , since  $(M_1:R) = (\bar{M}_1:\bar{K})$ .

ii) Now let  $H$  be arbitrary, and let  $M$  be a projective  $RH$ -module. In order to prove that  $[H:1]|(M:R)$ , it suffices to show that for each  $p$ -Sylow subgroup  $H_1$  of  $H$ , we have  $[H_1:1]|(M:R)$ . Now  $M$  is  $RH$ -projective, and  $RH$  is free as  $RH_1$ -module, so that  $M$  is also  $RH_1$ -projective. Therefore  $[H_1:1]|(M:R)$  by the last remark in part (i) of the proof. The lemma is therefore established.

We may now prove the following major result.

(78.3) THEOREM. (Swan [1], [2], [4]). If  $M$  is  $RH$ -projective, then  $KM$  is  $KH$ -free.

PROOF. Step 1. Suppose the result established for cyclic groups, and let  $H$  be an arbitrary group,  $M$  a projective  $RH$ -module. If  $\mu$  is the character afforded by the  $KH$ -module  $KM$  then by (ii) of (78.2) we have

$$\mu(1) = (M:R) = r[H:1]$$

for some integer  $r$ . Next, let  $h \in H$ ,  $h \neq 1$ , and let  $H_1$  be the cyclic subgroup  $[h]$  of  $H$ . Since  $M$  is  $RH$ -projective, it is also  $RH_1$ -projective, and therefore  $KM$  is  $KH_1$ -free (because we are assuming the theorem known for cyclic groups). Thus  $\mu$  vanishes on all of  $H_1$  except the identity element, and so  $\mu(h) = 0$ .

We may therefore conclude that  $\mu = r\tau$ , where  $\tau$  is the character afforded by the left regular module  $KH$ . Consequently  $KM$  is isomorphic to the direct sum of  $r$  copies of the left regular module, and so  $KM$  is  $KH$ -free. Thus, if the theorem is valid for cyclic groups, it is valid in general.

Step 2. We show next that if  $M$  is  $RH$ -projective, and  $N$  is any  $RH$ -module, then the  $RH$ -module  $N \otimes_R M$  is also  $RH$ -projective.

Since projective modules can be characterized as direct summands of free modules, it is enough to prove that  $N \otimes_R RH$  is projective. Let  $\bar{K} = R/P$ , where  $P$  is a prime ideal of  $R$ . Then by (78.1) we need only show that  $\bar{N} \otimes_{\bar{K}} \bar{K}H$  is  $\bar{K}H$ -projective.

Now let  $\{x_1, \dots, x_k\}$  be a  $\bar{K}$ -basis for  $\bar{N}$ . For  $x \in \bar{N}$ ,  $h \in H$ , we may write

$$x \otimes h = h \cdot (h^{-1}x \otimes 1) = h \cdot \{(\alpha_1 x_1 + \dots + \alpha_k x_k) \otimes 1\}$$

for some  $\alpha$ 's in  $\bar{K}$ . Therefore

$$\bar{N} \otimes_{\bar{K}} \bar{K}H = \bar{K}H \cdot (x_1 \otimes 1) \oplus \dots \oplus \bar{K}H \cdot (x_k \otimes 1),$$

so in fact  $\bar{N} \otimes_{\bar{K}} \bar{K}H$  is a free  $\bar{K}H$ -module. This completes Step 2.

*Step 3.* Now let  $M$  be an  $RH$ -projective module, where  $H$  is a cyclic group. By (78.2), part (ii), there exists a free  $RH$ -module  $F$  of the same  $R$ -rank as  $M$ . To complete the proof of the theorem, we need only show that  $KM \cong KF$ . In order to prove this, let us take an arbitrary irreducible  $KH$ -module  $T$ , and suppose that  $T$  occurs with multiplicity  $m$  in a decomposition of  $KM$  into a direct sum of irreducible modules. For fixed  $T$ , we shall show that  $m$  depends only upon the  $R$ -rank of the projective module  $M$ . It will then follow at once that  $KM \cong KF$ , as desired.

We observe that  $\text{Hom}_{KH}(T, KM)$  is a direct sum of  $m$  copies of  $\text{Hom}_{KH}(T, T)$ . Therefore

$$m \cdot \dim_K \text{Hom}_{KH}(T, T) = \dim_K \text{Hom}_{KH}(T, KM),$$

and it suffices to show that for fixed  $T$ , the right-hand expression depends only on  $(M:R)$ .

Let  $T^*$  denote the contragredient of  $T$  (see (43.7)). By Theorem 43.14,

$$\dim_K \text{Hom}_{KH}(T, KM) = \dim_K (T^* \otimes_K KM'),$$

where the superscript ' indicates the set of  $H$ -invariant elements of the module considered. Choose an  $RH$ -module  $N$  such that  $T^* = KN$ . Then

$$T^* \otimes_K KM = KN \otimes_K KM \cong K(N \otimes_R M).$$

If we set  $L = N \otimes_R M$ , then by the preceding step  $L$  is  $RH$ -projective. Furthermore,

$$(L:R) = (N:R)(M:R) = (T:K)(M:R),$$

so we need only show that  $\dim_K (KL)'$  depends only upon  $(L:R)$ .

Next we claim that

$$((KL)':K) = (L':R).$$

For  $L'$  is a pure  $R$ -submodule of  $L$ , and so  $KL'$  can be considered as a subspace of  $(KL)'$ . On the other hand, let  $x \in (KL)'$ . Choose  $a \in R$ ,  $a \neq 0$ , such that  $ax \in L$ . Since  $x$  is  $H$ -invariant, so is  $ax$ , and therefore  $ax \in L'$ . This shows that  $x \in KL'$ , and thus  $(KL)' = KL'$ . But then

$$((KL)':K) = (KL':K) = (L':R),$$

as claimed.

We have thus shown that

$$\dim_K \text{Hom}_{KH}(T, KM) = ((KL)':K) = (L':R),$$

and we must prove that  $(L':R)$  depends only upon  $(L:R)$ . For this it suffices to establish the following proposition:

If  $L$  is a projective  $RH$ -module, where  $H$  is cyclic, then  $(L:R) = [H:1](L':R)$ .

*Step 4.* We shall prove the above proposition by induction on  $[H:1]$ . Suppose first that  $H$  is a cyclic  $p$ -group, and let  $P$  be a prime ideal of  $R$  containing  $p$ , and set  $\bar{K} = R/P$ . If  $L_P$  denotes the  $R_PH$ -module  $R_PL$ , then it is easily seen that  $(L_P)' = (L')_P$ . Since the passage from  $R$  to  $R_P$  does not affect ranks, it suffices to prove the above proposition for projective  $R_PH$ -modules. But  $\bar{L}$  is  $\bar{K}H$ -free by (78.2), part (i), so by (77.2) we may conclude that  $L_P$  is  $R_PH$ -free. For free modules, we already have established the proposition, by means of the discussion preceding (78.2). Thus the proposition is valid when  $H$  is a cyclic  $p$ -group.

Suppose now that  $H$  is a cyclic group which is not a  $p$ -group, and write  $H = H_1 \times H_2$ , where  $H_1$  and  $H_2$  are proper subgroups of  $H$ . As in the discussion preceding (78.2), let  $L_1$  be the set of  $H_1$ -invariant elements of the projective  $RH$ -module  $L$ . Then by the induction hypothesis

$$(L:R) = [H_1:1](L_1:R).$$

On the other hand,  $L_1$  is  $RH_2$ -projective, and  $L'$  is the set of  $H_2$ -invariant elements of  $L_1$ ; thus, again using the induction hypothesis,

$$(L_1:R) = [H_2:1](L':R).$$

Together these yield

$$(L:R) = [H:1](L':R),$$

thereby proving both the proposition and Theorem 78.3.

**COROLLARY.** Let  $M$  be a projective  $RH$ -module, where  $H$  is an arbitrary group, and let  $P$  be any prime ideal in  $R$ . Then  $R_P M$  is a free  $R_PH$ -module, and  $M/PM$  is a free  $(R/P)H$ -module.

**PROOF.** We know that  $R_P M$  is  $R_PH$ -projective, and that

$K \cdot R_P M (= KM)$  is  $KH$ -free. By (77.14) we conclude that  $R_P M$  is free. Then use (77.13) to conclude that  $M/PM$  is also free.

We recall some results on  $R$ -modules, all of which are assumed finitely generated. For an  $R$ -module  $M$ , we define

$$\text{ann } M = \{\alpha \in R : \alpha M = 0\}.$$

If  $M \supset N$  are  $R$ -modules, we then have

$$\text{ann}(M/N) = \{\alpha \in R : \alpha M \subset N\}.$$

(78.4) LEMMA. *Let  $M \supset N$  be  $R$ -modules and  $I$  any ideal of  $R$ . The following statements are equivalent:*

- (i) *The map  $N/IN \rightarrow M/IM$  induced by the embedding of  $N$  in  $M$  is an isomorphism of  $N/IN$  onto  $M/IM$ .*
- (ii)  $I(M/N) = M/N$ .
- (iii)  $I + \text{ann}(M/N) = R$ .

PROOF. From (i) we deduce that every residue class in  $M/IM$  contains an element of  $N$ ; that is,  $M = N + IM$ . This at once implies (ii). Next suppose (ii) holds, and exclude the trivial case  $I = 0$ . Then  $M/N$  is a torsion module, and so  $M/N$  is a finite-direct sum of modules of the form  $R/J_t$ ,  $J_t$  a non-zero ideal in  $R$ . From (ii) we deduce that  $I + J_t = R$  for each  $t$ , and, since  $\text{ann}(M/N) = \bigcap_t J_t$ , we conclude that (iii) is valid. Suppose finally that (iii) holds. Then we have  $M = IM + N$ , since

$$\frac{M}{N} = (I + \text{ann}(M/N)) \cdot \frac{M}{N} = I \cdot \frac{M}{N} = \frac{IM + N}{N}.$$

Further,  $IM \cap N = IN$ , since the quotient  $(IM \cap N)/IN$  is annihilated by both  $I$  and  $\text{ann}(M/N)$ , hence by  $R$ . Together these imply (i).

(78.5) THEOREM (Swan). *Let  $M$  be a projective  $RH$ -module, and let  $I$  be a given non-zero ideal in  $R$ . Then there exists a free  $RH$ -module  $F$  contained in  $M$ , of the same  $R$ -rank as  $M$ , such that*

$$I + \text{ann}(M/F) = R.$$

PROOF. We first dispose of the case in which  $I = R$  by showing that any projective  $RH$ -module  $M$  contains a free  $RH$ -module. Since  $KM$  is  $KH$ -free [Theorem 78.3], there exists a  $KH$ -isomorphism  $\theta: KH \rightarrow KM$ , where  $X$  is a free  $RH$ -module of the same  $R$ -rank as  $M$ . Then  $\theta(X)$  is a finitely generated free  $RH$ -module contained in  $KM$ , and there exists a non-zero  $\alpha \in R$  such that  $\alpha \cdot \theta(X) \subset M$ . Clearly,  $\alpha \cdot \theta(X)$  is a free  $RH$ -module.

We turn next to the case where  $I \neq R$ , and let  $P$  be a prime ideal dividing  $I$ . Since  $KM$  is  $KH$ -free, it follows at once that  $R_P M$  is  $R_P H$ -free by (77.13). This shows that  $M/PM$  is  $(R/P)H$ -free for each  $P$  dividing  $I$  (in fact, for each prime ideal  $P$  in  $R$ ).

Let us write

$$I = \prod_{i=1}^k P_i^{n_i}, \quad \{P_i\} \text{ distinct prime ideals.}$$

Then for each  $i$ ,  $1 \leq i \leq k$ , there exist elements  $m_{1i}, \dots, m_{qi} \in M$  such that

$$M/P_i M = \sum_{j=1}^q (R/P_i) H \cdot \bar{m}_{ji},$$

and clearly  $q[H:1] = R\text{-rank of } M = (KM:K)$ , so that  $q$  is independent of  $i$ . Choose elements  $\alpha_1, \dots, \alpha_k \in R$  such that

$$\alpha_i \equiv \delta_{ij} \pmod{P_j}, \quad 1 \leq i, j \leq k.$$

Set

$$x_j = \alpha_1 m_{j1} + \dots + \alpha_k m_{jk}, \quad 1 \leq j \leq q,$$

$$F = RH \cdot x_1 + \dots + RH \cdot x_q.$$

Then surely  $F$  is an  $RH$ -submodule of  $M$ , which must be  $RH$ -free since any non-trivial relation

$$\sum_{i,j} \alpha_{ij} h_j x_i = 0, \quad \{\alpha_{ij}\} \in R, \{h_j\} \in H,$$

would imply that  $(KF:K) < q[H:1]$ , contradicting the fact that  $F/PF$  has dimension  $q[H:1]$  for any  $P$  dividing  $I$ .

By construction, we have

$$F/PF \cong M/PM \quad \text{for } P \text{ dividing } I.$$

From Lemma 78.4, we conclude that

$$P + \text{ann}(M/F) = R$$

for each  $P$  dividing  $I$ , whence also

$$I + \text{ann}(M/F) = R.$$

This proves the theorem.

(78.6) COROLLARY. *Let  $M$  be a projective  $RH$ -module and  $I$  a given non-zero ideal in  $R$ . Then there exists a free  $RH$ -module  $F'$  containing  $M$  such that*

$$I + \text{ann}(F'/M) = R.$$

**PROOF.** When  $I = R$ , we first choose a free module  $F$  contained in  $M$  having the same  $R$ -rank as  $M$ , which is possible by the beginning remarks in the preceding proof. Since  $M$  is finitely generated, there exists an  $\alpha \in R$  such that  $\alpha M \subset F$ , and then  $M \subset \alpha^{-1}F$ , giving the desired result.

Suppose now that  $I \neq R$ , and choose a free  $F$  contained in  $M$  as in the preceding theorem, so that

$$I + \text{ann}(M/F) = R .$$

Then there exist  $\alpha \in I$  and  $\beta \in \text{ann}(M/F)$  such that  $\alpha + \beta = 1$ ,  $\beta \neq 0$ . Then  $\beta M \subset F$ , so  $M \subset \beta^{-1}F = F'$ , say. We have  $\beta \in \text{ann}(F'/M)$ , and thus

$$I + \text{ann}(F'/M) = R .$$

This completes the proof.

(78.7) **LEMMA.** *Let  $M$  be a left ideal in  $RH$  such that*

$$[H:1]R + \text{ann}(RH/M) = R .$$

*Then  $M$  is  $RH$ -projective.*

**PROOF.** The hypothesis implies, using Lemma 78.4, that  $M/PM \cong (R/P)H$  for each prime ideal  $P$  dividing  $[H:1]$ . Now use Theorem 78.1 to complete the proof.

(78.8) **LEMMA.** *Let  $M$  be a projective  $RH$ -module, and let  $I$  be a non-zero ideal in  $R$ . Then there exists a finite set of left ideals  $\{M_i\}$  of  $RH$ , which are projective  $RH$ -modules satisfying*

$$I + \text{ann}(RH/M_i) = R \quad \text{for each } i,$$

*such that*

$$M \cong \sum_i \bigoplus M_i .$$

**PROOF.** By (78.6) there exists a free  $RH$ -module  $F'$  containing  $M$  such that

$$[H:1]I + \text{ann}(F'/M) = R .$$

Let  $F'$  be a direct sum of  $k$  copies of  $RH$ , and let  $\theta: F' \rightarrow RH$  be the projection of  $F'$  onto the first summand. This map carries  $M$  onto a left ideal  $M_1$  of  $RH$ . If  $\alpha F' \subset M$ , then  $\alpha \cdot RH \subset M_1$ , so that

$$\text{ann}(F'/M) \subset \text{ann}(RH/M_1) .$$

Consequently

$$[H:1]I + \text{ann}(RH/M_1) = R ,$$

so that

$$[H:1]R + \text{ann}(RH/M_1) = R, \quad I + \text{ann}(RH/M_1) = R.$$

The first of these equations implies that  $M_1$  is projective, by virtue of Lemma 78.7.

But now we may write an exact sequence

$$0 \rightarrow N \rightarrow M \rightarrow M_1 \rightarrow 0$$

where  $N = \{x \in M : \theta x = 0\}$ . Since  $M_1$  is projective the sequence splits, and so  $M \cong M_1 + N$ , and also  $N$  is projective [by Theorem 56.5]. Now repeat the argument on  $N$ , and observe that this procedure terminates because the  $R$ -rank of  $N$  is less than that of  $M$ . This completes the proof.

We may now prove Swan's main result.

(78.9) THEOREM (Swan [1], [2], [4]). *Let  $M$  be a projective  $RH$ -module, and let  $I$  be a non-zero ideal in  $R$ . Then there exists a free  $RH$ -module  $F$  and a projective left ideal  $M_0$  of  $RH$  such that*

$$M \cong F + M_0, \quad I + \text{ann}(RH/M_0) = R.$$

PROOF. In view of the result in Lemma 78.8, it suffices to show that, if  $M_1$  and  $M_2$  are projective left ideals in  $RH$  such that

$$I + \text{ann}(RH/M_i) = R, \quad i = 1, 2,$$

then there exists a projective left ideal  $M_3$  in  $RH$  such that

$$I + \text{ann}(RH/M_3) = R, \quad M_1 + M_2 \cong RH + M_3.$$

Let us set  $J = \text{ann}(RH/M_1)$ . By Lemma 78.8, there exists a projective left ideal  $M'_2$  in  $RH$  such that

$$M_2 \cong M'_2, \quad IJ + \text{ann}(RH/M'_2) = R.$$

Clearly  $M_1 + M_2 \cong M_1 + M'_2$ , and we can choose

$$\alpha \in \text{ann}(RH/M_1), \quad \beta \in \text{ann}(RH/M'_2)$$

such that  $\alpha + \beta = 1$ .

Now let  $\{e_1, e_2\}$  be an  $RH$ -basis for the free module

$$F = RH \cdot e_1 + RH \cdot e_2.$$

Then  $N = M_1e_1 + M'_2e_2 \cong M_1 + M'_2$ , and  $\text{ann}(F/N) + I = R$ . Set

$$e'_1 = \alpha e_1 + \beta e_2, \quad e'_2 = e_1 - e_2.$$

Then  $\{e'_1, e'_2\}$  is also an  $RH$ -basis for  $F$ , since we can solve for  $e_1, e_2$

in terms of  $e'_1, e'_2$  by using the relation  $\alpha + \beta = 1$ . Since  $\alpha \in M_1$  (because  $\alpha \cdot RH \subset M_1$ ) and  $\beta \in M'_2$ , we have  $e'_1 \in N$ . Hence

$$N = RH \cdot e'_1 + M_3 \cdot e'_2$$

where

$$M_3 = \{x \in RH : xe'_2 \in N\}.$$

Clearly  $M_3$  is a projective left ideal in  $RH$  for which  $M_1 + M'_2 \cong N \cong RH + M_3$ . Further,  $\text{ann}(RH/M_3) = \text{ann}(F/N)$ , so  $I + \text{ann}(RH/M_3) = R$ . This completes the proof.

*Remarks.* (1) The reader should compare these results with those obtained in §22 on modules over Dedekind rings. Setting  $H = \{1\}$  in the above theorems yields many of the results of §22.

(2) Swan's theorem 78.9 shows that a projective  $RH$ -module is not too far removed from a free  $RH$ -module, and in fact is of the form  $F + M_0$ , where  $F$  is free and  $M_0$  is a projective left ideal in  $RH$ . Concerning such an ideal  $M_0$ , we know that for each prime ideal  $P$  in  $R$ , the module  $M_0/PM_0$  is free as  $(R/P)H$ -module. Furthermore, we know that  $KM_0 = KH$ . By the Jordan-Zassenhaus theorem (§79), there are only a finite number of non-isomorphic  $RH$ -modules  $M_0$  such that  $KM_0 = KH$ , and thus there exist a finite number of projective left ideals  $M_i$  of  $RH$  such that every projective  $RH$ -module is of the form  $F + M_i$  for some free module  $F$  and some  $i$ . (In the terminology of Rim [1], [2], the projective class group of  $RH$ -modules is finite.)

(3) Swan [5] has shown that for  $H$  the generalized quaternion group of order 32, there exists a projective left ideal  $M$  in  $ZH$  such that  $M$  is not free, and for which

$$M + ZH \cong ZH + ZH.$$

(4) The problem of classifying projective modules over a  $Z$ -order can often be reduced to a corresponding problem for commutative rings. In this connection, see Eichler [1], [2], Swan [5], Takahashi [1].

To conclude this section, we list the following interesting result:

(78.10) *The group ring  $RH$  contains no idempotents except 1.*

**PROOF.** This is an immediate corollary of Theorem 78.3. The following independent proof, due to Takahashi [3], is of interest:

Let  $Z_1, \dots, Z_s$  be a full set of inequivalent irreducible complex representations of  $H$ , and let  $\zeta^{(i)}$  denote the character of  $Z_i$ . Let

$a \in RH$  be idempotent, and set  $b = 1 - a$ . Then  $b$  is also idempotent, and  $a + b = 1$ . From the equations

$$Z_i(a) = Z_i(a^2) = \{Z_i(a)\}^2, \quad 1 \leq i \leq s,$$

we may conclude that all eigenvalues of each  $Z_i(a)$  are 0's and 1's, and thus each  $\zeta^{(i)}(a)$  is a non-negative rational integer. The same holds for each  $\zeta^{(i)}(b)$ .

We may write

$$a = \sum_{h \in H} \alpha_h h, \quad b = \sum_{h \in H} \beta_h h, \quad \alpha_h, \beta_h \in R.$$

Define

$$S = [H : 1]^{-1} \sum_{i=1}^s \zeta^{(i)}(a) \zeta^{(i)}(1) = [H : 1]^{-1} \sum_{i,h} \alpha_h \zeta^{(i)}(h) \zeta^{(i)}(1).$$

By (31.13) we have

$$[H : 1]^{-1} \sum_i \zeta^{(i)}(h) \zeta^{(i)}(1) = \begin{cases} 0, & h \neq 1 \\ 1, & h = 1. \end{cases}$$

Consequently we find that  $S = \alpha_1$ , and if we write  $z_i = \zeta^{(i)}(1)$ , the above becomes

$$(78.11) \quad \alpha_1 = [H : 1]^{-1} \sum_i \zeta^{(i)}(a) z_i.$$

But  $0 \leq \zeta^{(i)}(a) \leq z_i$  for each  $i$ , since  $\zeta^{(i)}(a)$  is a sum of at most  $z_i$  1's. Hence [by (31.14)] we have  $0 \leq \alpha_1 \leq 1$ . Similarly,  $0 \leq \beta_1 \leq 1$ . However, the above shows that both  $\alpha_1$  and  $\beta_1$  are rational numbers; since both lie in  $R$ , it follows that each is 0 or 1. On the other hand, from  $1 = a + b$ , we conclude that  $1 = \alpha_1 + \beta_1$ , and thus one of  $\alpha_1, \beta_1$  is 1, the other 0; suppose  $\alpha_1 = 1$ . Then from (78.11) we conclude that  $\zeta^{(i)}(a) = z_i$  for each  $i$ . By Exercise 30.6, it follows that  $Z_i(a)$  must be the identity map for each  $i$ . But this means that  $a \rightarrow 1$  in every irreducible representation of  $H$ , and so  $a \rightarrow 1$  in the left regular representation of  $KH$ . Since  $KH$  is faithful as left  $KH$ -module, we conclude that  $a = 1$ , and the proof is complete.

### § 79. The Jordan-Zassenhaus Theorem

Throughout this section, we shall let  $A$  be a semi-simple algebra over  $Q$  with  $(A : Q)$  finite. Let  $G$  be a fixed  $Z$ -order in  $A$  [see Definition 75.1]; the reader may keep in mind the example in which  $G = ZH$ , the group ring of a finite group  $H$ , which is a  $Z$ -order in

$A = QH$ . By a  $G$ -module we mean (as before) a left  $G$ -module having a finite  $\mathbb{Z}$ -basis; the number of elements in a  $\mathbb{Z}$ -basis of the module is called the  $\mathbb{Z}$ -rank of the module. In § 73 we had agreed to call two  $G$ -modules  $M$  and  $N$   $\mathbb{Z}$ -equivalent (notation:  $M \sim_z N$ ) if  $M \cong N$  as  $G$ -modules. On the other hand, we called them  $Q$ -equivalent ( $M \sim_q N$ ) if  $QM \cong QN$  as  $A$ -modules.

*Example.* Let  $K$  be an algebraic number field, and set  $A = K$ ,  $G = \text{alg. int. } \{K\}$ . Then  $G$  is a  $\mathbb{Z}$ -order in  $A$ . If  $M$  and  $N$  are non-zero  $G$ -ideals in  $K$  (that is, non-zero  $G$ -modules contained in  $K$ ), it follows at once from Chapter III that  $M \sim_z N$  if and only if  $M$  and  $N$  are in the same ideal class. On the other hand,  $M \sim_q N$  always holds since  $QM = QN = K$ .

Returning to the general situation, let  $L^*$  be a fixed  $A$ -module, and let  $\sigma(L^*)$  be the set of all  $G$ -modules  $L$  contained in  $L^*$  such that  $QL = L^*$ . From § 73 we know that any  $G$ -module  $M$  for which  $QM \cong L^*$  is in fact  $G$ -isomorphic to some  $L$  in  $\sigma(L^*)$ .

In this section we shall prove the following result:

(79.1) **THEOREM** (Jordan; Zassenhaus [3]). *The set  $\sigma(L^*)$  splits into a finite number of classes under  $\mathbb{Z}$ -equivalence.*

As is evident from the above example, the Jordan-Zassenhaus theorem is a sweeping generalization of the theorem on the finiteness of the number of ideal classes in an algebraic number field. In fact, the proof will make use of the generalization of this already obtained in Theorem 20.6.

*Step 1.* Let us begin with the special case in which  $L^*$  is an irreducible  $A$ -module. Since  $A$  is semi-simple, it is expressible as a direct sum of simple components. In that case,  $L^*$  may be taken to be a minimal left ideal in some one of these simple components, say in  $B$ . The simple component  $B$  may in turn be written as a full matrix algebra

$$(79.2) \quad B = D_f, \quad (D : Q) = n,$$

where  $D$  is a skewfield of dimension  $n$  over  $Q$ . Then

$$(79.3) \quad (B : Q) = f^2n, \quad (L^* : Q) = fn.$$

We may view  $D$  as embedded in  $A$ ; now define

$$(79.4) \quad D_0 = D \cap G.$$

Then  $D_0$  is a  $\mathbb{Z}$ -submodule of  $G$  and hence has finite  $\mathbb{Z}$ -rank. Further,

$$QD_0 = QD \cap QG = D \cap A = D,$$

so, in fact,  $D_0$  has  $Z$ -rank  $n$ .

Assume first that  $f = 1$ , so that  $D = L^* = B$ . For each  $X \in \sigma(L^*)$ , we have  $QX = L^* = D$ , and thus  $X$  is a  $Z$ -submodule of  $D$  of  $Z$ -rank  $n$ . Furthermore,

$$D_0 X \subset GX \subset X,$$

so that  $X$  is an  $D_0$ -ideal in  $D$  (see § 20). When are two modules  $X, X'$  in  $\sigma(L^*)$   $G$ -isomorphic? Any  $G$ -isomorphism of  $X$  onto  $X'$  can be extended to an  $A$ -isomorphism of  $QX$  onto  $QX'$ , and hence is given by a right multiplication by a non-zero element of  $D$ . Conversely,  $X' = Xb$ ,  $b \in D$ ,  $b \neq 0$ , implies that  $X' \sim_Z X$ . Therefore the number of classes into which  $\sigma(L^*)$  splits under  $Z$ -equivalence is the same as the number of classes of  $D_0$ -ideals in  $D$ . By virtue of Theorem 20.6, this number is finite. Hence our theorem is proved for the case  $f = 1$ .

*Step 2.* Assume now that  $f > 1$ , and keep the notation of equations (79.2)–(79.4). Let  $\{e_{ij} : 1 \leq i, j \leq f\}$  be a full set of matrix units in  $B$ . These units form a  $D$ -basis for  $B$ , commute with all the elements of  $D$ , and satisfy

$$(79.5) \quad e_{ij}e_{kl} = \delta_{jk}e_{il}, \quad \sum_{i=1}^f e_{ii} = \text{identity element of } B.$$

Since  $L^*$  is any minimal left ideal in  $B$ , we may in fact choose

$$(79.6) \quad L^* = e_{11}D \oplus e_{21}D \oplus \cdots \oplus e_{f1}D.$$

Let the element  $l \in L^*$  be expressed as  $\sum e_{ii}\alpha_i$ ,  $\{\alpha_i\} \in D$ , and define  $\theta_i : L^* \rightarrow D$  by  $\theta_i(l) = \alpha_i$ ,  $1 \leq i \leq f$ . We shall use the linear functions  $\{\theta_i\}$  in a moment.

Now suppose that  $X \in \sigma(L^*)$ . Then  $X$  is a  $G$ -module, and its  $Z$ -rank is given by

$$(79.7) \quad (X : Z) = (QX : Q) = (L^* : Q) = fn.$$

Define

$$(79.8) \quad X_i = X \cap (e_{11}D \oplus \cdots \oplus e_{ii}D).$$

Then

$$0 = X_0 \subset X_1 \subset \cdots \subset X_f = X,$$

and if we set  $\varphi_i = \theta_i|_{X_i}$ , the map  $\varphi_i : X_i \rightarrow D$  is a  $Z$ -homomorphism with kernel  $X_{i-1}$ . Therefore  $X_i/X_{i-1}$  is isomorphic (as additive group)

to some additive subgroup  $\phi_i(X)$  of  $D$ . An element  $\alpha \in D$  lies in  $\phi_i(X)$  if and only if there exists an element  $x \in X$  of the form

$$(79.9) \quad x = \alpha_1 e_{11} + \cdots + \alpha_{i-1} e_{i-1,1} + \alpha e_{ii}, \\ \alpha_1, \dots, \alpha_{i-1} \in D.$$

Since  $X_i$  is a finitely generated  $Z$ -module, so is  $\phi_i(X)$ . Also  $\phi_i(X)$  lies in a vector space over  $Q$ , and hence is  $Z$ -torsion-free. Together, these show that  $\phi_i(X)$  has a finite  $Z$ -basis. We claim that in fact each  $\phi_i(X)$  is an  $D_0$ -ideal in  $D$ , where  $D_0$  is given by (79.4). For let  $\alpha \in \phi_i(X)$ , and let (79.9) hold for some  $x \in X$ . If  $\gamma \in D_0$ , we have

$$\gamma x = (\gamma \alpha_1) e_{11} + \cdots + (\gamma \alpha_{i-1}) e_{i-1,1} + (\gamma \alpha) e_{ii},$$

and  $\gamma x \in X$  since  $\gamma \in G$ ; therefore  $\gamma \alpha \in \phi_i(X)$ . [We must still check that  $\phi_i(X) \neq 0$ . However,  $QX = L^*$  implies that for some  $a \in Z$ ,  $a \neq 0$ , we have  $ae_{ii} \in X$ , and so  $a \in \phi_i(X)$ .]

The above shows that with each  $X \in \sigma(L^*)$  is associated a set of  $D_0$ -ideals (in  $D$ ), namely  $\phi_1(X), \dots, \phi_f(X)$ . Obviously if  $X, X' \in \sigma(L^*)$  and  $X' \subset X$ , then  $\phi_i(X') \subset \phi_i(X)$ ,  $1 \leq i \leq f$ . On the other hand,  $aX \subset X' \subset X$  for some positive  $a \in Z$ , and so the index  $[X : X']$  is finite; this also shows that each  $[\phi_i(X) : \phi_i(X')]$  is finite. One easily verifies that

$$(79.10) \quad [X : X'] = \prod_{i=1}^f [\phi_i(X) : \phi_i(X')].$$

We know from Step 1 that there exist a finite number of  $D_0$ -ideals in  $D$ , say  $E_1, \dots, E_t$ , such that every  $D_0$ -ideal is a right multiple of some  $E_i$ . Set

$$Y_i = GE_i e_{ii}, \quad 1 \leq i \leq t.$$

It is easily seen that each  $Y_i \in \sigma(L^*)$ .

We are now ready to show the existence of a finite set of modules in  $\sigma(L^*)$  such that each module in  $\sigma(L^*)$  is  $G$ -isomorphic to some module in the finite set. Let  $X \in \sigma(L^*)$  be arbitrary, and define  $\phi_1(X), \dots, \phi_f(X)$  as above. Then for some non-zero  $\xi \in D$  and some  $E$  chosen from  $E_1, \dots, E_t$ , we have  $\phi_1(X) = E\xi$ . For the moment, set  $\tilde{X}_1 = X\xi^{-1}$ . Then  $\tilde{X}_1 \in \sigma(L^*)$ ,  $\tilde{X}_1 \cong X$  as  $G$ -modules, and

$$\phi_1(\tilde{X}_1) = \phi_1(X)\xi^{-1} = E.$$

Replacing  $X$  by  $\tilde{X}_1$  and calling the new module  $X$  once again, we may henceforth assume that  $\phi_1(X) = E$ . For fixed  $E$ , we shall show that there are only a finite number of possible  $X$ 's, and this will complete the proof of Step 2.

We note first that  $Ee_{11} = \psi_1(X)e_{11} \subset X$ , so  $Y = GEe_{11} \subset GX \subset X$ . By (79.10), we have

$$[X : Y] = \prod_{j=1}^f [\psi_j(X) : \psi_j(Y)].$$

Let us choose positive rational integers  $\{a_j\}, \{b_j\}$  (independently of  $X$ ) such that

$$a_j e_{j1} \in G, \quad b_j e_{1j} \in G, \quad 1 \leq j \leq f.$$

For each  $\alpha \in \psi_j(X)$ , there is an  $x \in X$  such that (79.9) holds (with  $i$  replaced by  $j$ ). Then  $X$  also contains  $b_j e_{1j} x = b_j \alpha e_{11}$ , so  $b_j \alpha \in \psi_1(X)$ . We have thus shown that

$$b_j \psi_j(X) \subset E, \quad 1 \leq j \leq f.$$

A similar argument shows that  $a_j E \subset \psi_j(X)$ ,  $1 \leq j \leq f$ , and so  $a_j E \subset \psi_j(X) \subset b_j^{-1} E$ . Further,  $Ee_{11} \subset Y$  implies  $a_j e_{j1} \cdot Ee_{11} \subset Y$ , and so  $a_j E \subset \psi_j(Y)$ . We therefore have

$$a_j E \subset \psi_j(Y) \subset \psi_j(X) \subset b_j^{-1} E, \quad 1 \leq j \leq f.$$

Therefore the index  $[\psi_j(X) : \psi_j(Y)]$  is bounded by  $|a_j b_j|^{Z \text{-rank of } E}$ , and so  $[X : Y]$  is also bounded (independently of  $X$ ), say  $[X : Y] \leq C$ . Hence for some  $a \in Z$ , where  $0 < a \leq C$ , we conclude that  $aX \subset Y$ , and so  $Y \subset X \subset a^{-1}Y$ . For fixed  $Y$ , the above shows that there are only finitely many possible  $X$ 's. But there are just  $t$  possible  $Y$ 's, and so Step 2 is completed.

*Step 3.* In the preceding two steps, we have established the theorem whenever  $L^*$  is irreducible. Suppose now that  $L^*$  is a reducible  $A$ -module with  $k$  composition factors,  $k > 1$ , and that the theorem has been proved for  $A$ -modules having  $k - 1$  composition factors. Let  $M^*$  be an irreducible  $A$ -submodule of  $L^*$ , and set  $N^* = L^*/M^*$ . Then  $N^*$  has  $k - 1$  composition factors, and so by the induction hypothesis we may choose a finite set of modules  $N_1, \dots, N_r$  which are a complete set of representatives of the classes into which  $\sigma(N^*)$  splits under  $G$ -isomorphism. In the same manner, choose representatives  $M_1, \dots, M_s$  of the classes in  $\sigma(M^*)$ . We have shown in §73 that each  $X \in \sigma(L^*)$  is  $G$ -isomorphic to a module

$$(79.11) \quad (N_i, M_j; F)$$

for some  $F \in B(N_i, M_j)$  and some  $i$  and  $j$ ,  $1 \leq i \leq r$ ,  $1 \leq j \leq s$ . On the other hand, the number of non-isomorphic modules given by (79.11) is at most equal to the number of elements in the 1-coho-

mology group  $C(N_i, M_j)$ . Since  $A$  is a separable algebra over  $Q$  (because  $Q$  has characteristic 0), the results of §75 show the existence of a positive integer  $a$  (depending only upon  $G$  and  $A$ ) such that

$$a \cdot C(N_i, M_j) = 0, \quad 1 \leq i \leq r, 1 \leq j \leq s.$$

Using the fact that  $C(N_i, M_j)$  is a finitely generated  $Z$ -module, we find the above implies that  $C(N_i, M_j)$  is finite. This completes the proof of Theorem 79.1.

Since there are only a finite number of non-isomorphic  $A$ -modules of some fixed  $Q$ -dimension, we have

(79.12) COROLLARY. *For each  $n \geq 1$ , the set of all  $G$ -modules of  $Z$ -rank  $n$  splits into a finite number of classes under  $Z$ -equivalence.*

In order to generalize this corollary, we take  $K$  to be an algebraic number field,  $R$  a  $Z$ -order in  $K$ ,  $\bar{A}$  a finite-dimensional algebra over  $K$  which is semi-simple, and  $\bar{G}$  an  $R$ -order in  $\bar{A}$ . By a  $\bar{G}$ -module, we shall mean a left  $\bar{G}$ -module  $M$  which, as  $R$ -module, is finitely generated and torsion-free, the action of  $R$  on  $M$  being given by the embedding of  $R$  in  $\bar{G}$ . Let us now show

(79.13) THEOREM (Zassenhaus). *For each  $n \geq 1$ , the set of all  $\bar{G}$ -modules of  $R$ -rank  $n$  splits into a finite number of classes under  $\bar{G}$ -isomorphism.*

PROOF. Obviously  $\bar{A}$  is also a semi-simple algebra over  $Q$ ; considered as an algebra over  $Q$ , we shall denote it by  $A$ . Similarly,  $\bar{G}$  is a  $Z$ -order in  $A$ , and we shall denote it by  $G$ . Each  $\bar{G}$ -module  $M$  is then a  $G$ -module, and

$$\text{Z-rank of } M = (\text{Z-rank of } R)(\text{R-rank of } M).$$

By the preceding corollary, for fixed  $n \geq 1$ , the set of  $\bar{G}$ -modules of  $R$ -rank  $n$  splits into a finite number of classes under  $G$ -isomorphism. However,  $G$ -isomorphism of  $\bar{G}$ -modules implies  $\bar{G}$ -isomorphism of the modules, which implies the result.

## § 80. Order Ideals

Let  $R$  be a Dedekind domain with quotient field  $K$ . The term " $R$ -module" shall mean, throughout this section, a finitely generated left  $R$ -module. We devote this section to a discussion of order ideals of  $R$ -modules, and assume that the reader is familiar with the results in §22.

We called an element  $m$  of an  $R$ -module  $M$  *torsion-free* if  $m \neq 0$  and if  $\alpha m = 0$ ,  $\alpha \in R$ , implies that  $\alpha = 0$ . A *torsion module* is one which contains no torsion-free elements. We saw that every  $R$ -module  $M$  is expressible as a direct sum of fractional ideals in  $K$  and torsion modules of the form  $R/I$  where  $I$  is a non-zero integral ideal [see Corollary 22.16].

If  $M$  is not a torsion module, that is, if  $M$  contains torsion-free elements, we define the *order ideal* of  $M$  as  $\text{ord}(M) = 0$ . On the other hand, if  $M$  is a torsion module we may write

$$(80.1) \quad M \cong \frac{R}{A_1} \dotplus \cdots \dotplus \frac{R}{A_k}$$

where the  $\{A_i\}$  are (non-zero) integral ideals in  $R$ . These ideals are not in general uniquely determined by  $M$ , and in fact we know that

$$\frac{R}{AB} \cong \frac{R}{A} + \frac{R}{B}$$

whenever  $A + B = R$ . We have shown in § 22 that these ideals  $\{A_i\}$  are uniquely determined if we impose the added condition that for each  $i$ ,  $A_i | A_{i+1}$ . From this remark, or alternately from Step 6 of the proof of Theorem 22.12, it follows that the product  $A_1 \cdots A_k$  is uniquely determined by  $M$ . We now define the *order ideal* of  $M$  to be

$$(80.2) \quad \text{ord } M = A_1 \cdots A_k.$$

Let  $B$  be an ideal in  $R$  which is relatively prime to each  $A_i$ . From  $B + A_i = R$  we deduce easily that

$$B \cdot (R/A_i) = R \cdot (R/A_i) = R/A_i$$

for each  $i$ , and thus  $BM = M$  where  $M$  is given by (80.1). This shows at once that a prime ideal  $P$  is a divisor of  $\text{ord } M$  if and only if  $PM \neq M$ . (The same result of course holds when  $\text{ord } M = 0$ .)

Let us obtain another characterization of the order ideal of a torsion module  $M$ , where  $M$  is given by (80.1). The  $R$ -submodules of  $R/A_i$  are of the form  $B/A_i$  where  $B$  is an ideal such that  $A_i \subset B \subset R$ . Since  $R$  is a Dedekind domain, there are only finitely many such  $B$ 's. Therefore  $R/A_i$  satisfies both chain conditions, and so (80.1) implies that the  $R$ -module  $M$  satisfies both chain conditions. Consequently,  $M$  possesses a composition series

$$M = M_1 \supset M_2 \supset \cdots \supset M_n \supset M_{n+1} = (0),$$

with composition factors  $\{M_i/M_{i+1} : 1 \leq i \leq n\}$  which are uniquely determined up to  $R$ -isomorphism and order of occurrence. Let  $B_i = \text{annihilator of } M_i/M_{i+1}$ ; that is,

$$B_i = \{\alpha \in R : \alpha M_i \subset M_{i+1}\}.$$

Then we claim that

$$(80.3) \quad B_1 B_2 \cdots B_n = \text{ord } M.$$

We may prove this by exhibiting one specific composition series for  $M$  such that (80.3) holds. Such a series is given by

$$\begin{aligned} M &\supset P_1/A_1 + R/A_2 + \cdots + R/A_k \supset P_1 P_2/A_1 + R/A_2 + \cdots + R/A_k \supset \\ &\cdots \supset P_1 P_2 \cdots P_l/A_1 + R/A_2 + \cdots + R/A_k \\ &= R/A_2 + \cdots + R/A_k \supset Q_1/A_2 + R/A_3 + \cdots + R/A_k \supset \cdots \supset (0), \end{aligned}$$

where  $A_1 = P_1 P_2 \cdots P_l$ ,  $\{P_i\}$  prime ideals,  $A_2 = Q_1 \cdots Q_s$ ,  $\{Q_i\}$  prime ideals, and so on. The annihilators of the composition factors are successively  $P_1, P_2, \dots, P_l, Q_1, \dots$ , and their product is  $A_1 A_2 \cdots A_k$ .

Now let  $M \supset N$  be  $R$ -modules, and define the *order ideal*  $\text{ord}(M:N)$  by

$$\text{ord}(M:N) = \text{ord}(M/N).$$

Then, from the characterization of order ideals in terms of composition series, we see that

$$(80.4) \quad \text{ord}(M:N) \text{ ord } N = \text{ord } M.$$

Another obvious result is the following: Let  $M$  be a torsion-free  $R$ -module and  $B$  a non-zero ideal in  $R$ . Then  $\text{ord}(M:BM) = B^t$ , where  $t$  is the  $R$ -rank of  $M$ . To prove this, note that we may write

$$M = A_1 + \cdots + A_t, \quad A_i = \text{ideal in } R, \quad A_i \neq (0).$$

Then  $BM = BA_1 + \cdots + BA_t$ , and

$$M/BM \cong A_1/BA_1 + \cdots + A_t/BA_t.$$

However, we may construct a composition series for  $M/BM$  by the method used above, which shows that  $\text{ord}(M/BM) = B^t$ .

Suppose now that  $M, N$  are torsion-free  $R$ -modules, and embed them in the  $K$ -spaces  $KM, KN$ , as in §75. Then any  $T \in \text{Hom}_R(M, N)$  can be extended to a map (also denoted by  $T$ ) in  $\text{Hom}_K(KM, KN)$ , given by

$$T(\alpha m) = \alpha T(m), \quad \alpha \in K, \quad m \in M.$$

The extended map is uniquely determined by the original  $T$  [see the discussion preceding Lemma 22.2]. Similarly, if  $R_S$  denotes the ring of all elements of  $K$  which are integral at all primes in the finite collection  $S$  of prime ideals, the above procedure extends  $T$  to a map  $T \in \text{Hom}_{R_S}(R_S M, R_S N)$ . We may therefore write

$$\begin{aligned} M &\subset R_S M \subset KM, \quad N \subset R_S N \subset KN, \\ \text{Hom}_R(M, N) &\subset R_S \cdot \text{Hom}_R(M, N) = \text{Hom}_{R_S}(R_S M, R_S N) \\ &\subset K \cdot \text{Hom}_R(M, N) = \text{Hom}_K(KM, KN). \end{aligned}$$

We now introduce an ideal which plays the role of the determinant of a linear transformation. For  $M, N$  a pair of torsion-free  $R$ -modules, and for  $T \in \text{Hom}_R(M, N)$ , define the *determinant ideal* of  $T$  by

$$\delta(T) = \text{ord}(N : TM).$$

Then certainly we have  $\delta(T)N \subset TM$ , from the definition of order ideal. Viewing  $T$  as element of  $\text{Hom}_K(KM, KN)$ , define its determinant ideal as

$$\delta_K(T) = (KN : T(KM)).$$

If  $M, N$  have the same rank, we can represent  $T$  by a  $K$ -matrix, and in that case

$$(80.5) \quad \delta_K(T) = K \cdot \det T.$$

Furthermore, in the general case we may view  $T$  as element of  $\text{Hom}_{R_S}(R_S M, R_S N)$ , with determinant ideal defined by

$$\delta_{R_S}(T) = \text{ord}(R_S N : T(R_S M)).$$

We easily see that

$$(80.6) \quad \delta_K(T) = K \cdot \delta(T), \quad \delta_{R_S}(T) = R_S \cdot \delta(T).$$

We omit the proofs.

Suppose now that  $M, N$  have the same  $R$ -rank. From (80.5) and (80.6), we see that  $T$  is a one-to-one mapping of  $M$  into  $N$  if and only if  $\delta(T) \neq (0)$ . Furthermore,  $TM = N$  if and only if  $\delta(T) = R$ . Thus, if  $M, N$  have the same  $R$ -rank, it follows that  $T$  is an isomorphism of  $M$  onto  $N$  if and only if  $\delta(T) = R$ .

Let  $B$  be an ideal in  $R$ , and let  $T, U \in \text{Hom}_R(M, N)$ . The notation  $T \equiv U(\text{mod } B)$  shall be used to denote the fact that

$$T(m) - U(m) \in BN, \quad m \in M.$$

We now establish

(80.7) LEMMA. Let  $M, N$  be torsion-free  $R$ -modules, let  $T, U \in \text{Hom}_R(M, N)$ , and suppose that there exists an ideal  $B$  in  $R$  for which  $T \equiv U(\text{mod } B)$ . Then  $\delta(T) + B = R$  implies  $\delta(U) + B = R$ .

PROOF. Since the result is obviously true when  $B = (0)$ , assume for the rest of the proof that  $B \neq (0)$ . Then from  $\delta(T) + B = R$  we conclude that

$$N = RN = \delta(T)N + BN \subset TM + BN,$$

so that in fact  $N = TM + BN$ . However,  $T \equiv U(\text{mod } B)$  then shows that  $N = UM + BN$ , whence  $N \equiv BN(\text{mod } UM)$ . Suppose there exists a prime ideal  $P$  dividing both  $\delta(U)$  and  $B$ . Since  $P \mid \delta(U)$ , that is,  $P \mid \text{ord}(N/UM)$ , the remark made at the beginning of this section shows that  $P(N/UM)$  is properly contained in  $N/UM$ , and so  $PN \not\equiv N(\text{mod } UM)$ . However,  $P \mid B$  implies that  $PN \supset BN$ , and so certainly  $BN \not\equiv N(\text{mod } UM)$ . This gives a contradiction, and so no such prime  $P$  exists; that is,  $B + \delta(U) = R$ . This completes the proof.

### § 81. Genus

Reverting to the notation of § 75, we suppose again that  $R$  is a Dedekind domain with quotient field  $K$ . Let  $A$  be a separable algebra over  $K$  with unity  $e$ , and let  $G$  be an  $R$ -order in  $A$ . We let  $i(G)$  be the non-zero ideal of  $R$  defined in § 75; then  $i(G)$  is the intersection of the annihilators of the 1-cohomology groups of all  $(G, G)$ -bimodules. (It may help to keep in mind the special case in which  $R$  is the ring of all algebraic integers in the algebraic number field  $K$ , where  $G = RH$  is the group ring of the finite group  $H$ , and where  $A = KH$ . In this case,  $i(G)$  is the principal ideal generated by the group order  $[H : 1]$ .)

Throughout this section, a  $G$ -module shall be a left  $G$ -module which is finitely generated and torsion-free as  $R$ -module (the action of  $R$  being induced by the embedding of  $R$  in  $G$ ). If  $M, N$  are  $G$ -modules, we write  $M \sim_R N$  to indicate that  $M \cong N$  as  $G$ -modules. As usual, embed  $M, N$  in the  $A$ -modules  $KM, KN$ , and write  $M \sim_K N$  if  $KM \cong KN$  as  $A$ -modules. Finally, if  $B$  is a non-zero ideal in  $R$ , we shall let  $R_B$  denote the ring of elements of  $K$  which are integral at all primes dividing  $B$ . (This represents a minor change from previous notation.) Then  $M \sim_B N$  shall mean that  $R_B M \cong R_B N$  as  $R_B G$ -modules. Obviously

$$M \sim_R N \Rightarrow M \sim_B N \Rightarrow M \sim_K N.$$

Let  $\sigma(M)$  denote the set of all  $G$ -modules  $N$  such that  $N \sim_K M$ . Let  $\nu_R$  be the number of classes of  $R$ -equivalent modules into which  $\sigma(M)$  splits; possibly  $\nu_R = \infty$ . In addition, for  $B$  a non-zero ideal in  $R$ , let  $\nu_B$  be the number of classes into which  $\sigma(M)$  splits under  $B$ -equivalence. The aim of this section is to investigate the connection between  $\nu_R$  and  $\{\nu_P : P = \text{prime ideal in } R\}$ .

We shall begin with some results due to Maranda [2]. A slightly different approach to these theorems may be found in Takahashi [1]. Let  $B$  be a non-zero ideal in  $R$ , and suppose  $B = B_1B_2$  where  $B_1, B_2$  are relatively prime ideals in  $R$ . We wish to show that the intersection of the partitions of  $\sigma(M)$  into  $B_1$ -equivalence classes and into  $B_2$ -equivalence classes yields the partition of  $\sigma(M)$  into  $B$ -classes. Specifically we shall prove that two modules are  $B$ -equivalent if and only if they are both  $B_1$ - and  $B_2$ -equivalent. Further, we shall show that each intersection of a  $B_1$ -class with a  $B_2$ -class is non-empty. These facts together will imply that

$$(81.1) \quad \nu_{B_1B_2} = \nu_{B_1}\nu_{B_2} \quad \text{if } B_1 + B_2 = R.$$

To establish the preceding statements, it suffices to prove

(81.2) **THEOREM (Maranda [2]).** *Let  $M, N \in \sigma(M)$ . Then*

- (i)  $M \sim_B N$  if and only if  $M \sim_{B_1} N$  and  $M \sim_{B_2} N$ ;
- (ii) there exists a module  $M' \in \sigma(M)$  such that

$$M' \sim_{B_1} M, \quad M' \sim_{B_2} N.$$

**PROOF.** *Step 1.* We shall begin by proving that  $M \sim_B N$  if and only if there exists a map  $T \in \text{Hom}_G(M, N)$  such that  $\delta(T) + B = R$ , where  $\delta(T)$  is the determinant ideal introduced in §80. If such a  $T$  exists, extend it to a map

$$T \in \text{Hom}_{R_B G}(R_B M, R_B N).$$

Then

$$\delta_B(T) = R_B \delta(T) = R_B$$

since  $\delta(T)$  is relatively prime to each prime ideal dividing  $B$ . But  $\delta_B(T) = R_B$  implies (since  $M, N$  have the same  $R$ -rank) that  $T$  is an  $R_B G$ -isomorphism of  $R_B M$  onto  $R_B N$ , and so  $M \sim_B N$ .

Conversely, suppose that  $M \sim_B N$ . There then exists an  $R_B G$ -isomorphism  $T : R_B M \cong R_B N$ . Replacing  $T$  by  $\alpha T$  if need be, where  $\alpha$  is a unit in  $R_B$ , we may in fact assume that  $TM \subset N$ . Then

surely  $T \in \text{Hom}_\sigma(M, N)$ , and we have

$$R_B \cdot \delta(T) = \delta(R_B T) = R_B$$

(since  $T$  is an isomorphism onto). This immediately implies that  $\delta(T) + B = R$ , and completes the proof of the assertion made at the beginning of this step.

*Step 2.* If  $M \sim_B N$ , there exists  $T \in \text{Hom}_\sigma(M, N)$  such that  $\delta(T) + B = R$ . Obviously this implies that  $\delta(T) + B_i = R$ ,  $i = 1, 2$ , and hence  $M \sim_{B_i} N$ ,  $i = 1, 2$ .

Suppose that conversely  $M \sim_{B_i} N$ ,  $i = 1, 2$ . Choose  $T_i \in \text{Hom}_\sigma(M, N)$  such that

$$\delta(T_i) + B_i = R, \quad i = 1, 2.$$

Since  $B_1 + B_2 = R$ , we may choose  $b_1 \in B_1$ ,  $b_2 \in B_2$  such that  $b_1 + b_2 = 1$ . Set  $T = b_1 T_2 + b_2 T_1 \in \text{Hom}_\sigma(M, N)$ . Then  $T \equiv b_2 T_1 \pmod{B_1}$  implies [by Lemma 80.7] that

$$\delta(T) + B_1 = R \text{ if and only if } \delta(b_2 T_1) + B_1 = R.$$

However,  $\delta(b_2 T_1) = b_2^n \delta(T_1)$ , where  $n = \text{rank of } M$ , and so  $\delta(b_2 T_1) + B_1 = R$ . Therefore,  $\delta(T) + B_1 = R$ ; similarly,  $\delta(T) + B_2 = R$ , and consequently  $\delta(T) + B = R$ . Thus  $M \sim_B N$ .

*Step 3.* Let  $M, N \in \sigma(M)$  be given. There then exists an  $A$ -isomorphism  $T : KM \cong KN$ . Replacing  $T$  by  $\alpha T$ ,  $\alpha \neq 0$ ,  $\alpha \in K$ , we may assume that  $TM \subset N$ . Then surely  $T \in \text{Hom}_\sigma(M, N)$ . Set  $B = \delta(T)$ , a non-zero ideal in  $R$ . Using the fact that  $R_B$  is a principal ideal ring, we may choose an  $R_B$ -basis  $x_1, \dots, x_n$  of  $R_B N$  and elements  $\alpha_1, \dots, \alpha_n \in R_B$  such that  $\alpha_1 x_1, \dots, \alpha_n x_n$  form an  $R_B$ -basis of  $T(R_B M)$ . Thus

$$\begin{aligned} R_B N &= R_B x_1 \oplus \cdots \oplus R_B x_n, \\ T(R_B M) &= R_B \alpha_1 x_1 \oplus \cdots \oplus R_B \alpha_n x_n, \end{aligned}$$

and so  $\delta_B(T) = (R_B N : T(R_B M)) = \alpha_1 \cdots \alpha_n R_B \neq (0)$ .

Let us write for  $1 \leq i \leq n$ ,

$$\alpha_i R_B = D_i E_i$$

where  $D_i$  contains only the prime ideals which occurs in  $B_i$ , and  $E_i$  only those in  $B_1$ . Set

$$D = \bigcap_{i=1}^n D_i.$$

Then  $D^{-1}T(R_B M)$  is an  $R_B G$ -module, and setting

$$M' = N \cap D^{-1}T(R_B M),$$

we easily see that  $M'$  is a  $G$ -module. Furthermore,

$$\begin{aligned} R_B M' &= R_B N \cap D^{-1}T(R_B M) \\ &= (R_B \cap D^{-1}\alpha_1)x_1 \oplus \cdots \oplus (R_B \cap D^{-1}\alpha_n)x_n. \end{aligned}$$

(This shows incidentally that  $KM' = KN$ , so  $M' \in \sigma(M)$ .) Now we have for  $1 \leq i \leq n$ ,

$$R_B \cap D^{-1}\alpha_i = E_i$$

so that

$$R_B M' = E_1x_1 \oplus \cdots \oplus E_nx_n.$$

Comparing this with our expression for  $T(R_B M)$ , we see that  $T(R_B M) \subset R_B M'$ , and

$$\delta_B(T) = \text{ord}(R_B M' : T(R_B M)) = \prod_{i=1}^n \alpha_i E_i^{-1} = \prod_{i=1}^n D_i.$$

Thus  $\delta_B(T)$  is coprime to  $B_1$ , whence  $\delta(T)$  is also coprime to  $B_1$ . Since  $T \in \text{Hom}_G(M, M')$ , we may conclude that  $M' \sim_{B_1} M$ .

On the other hand, the inclusion map of  $M'$  into  $N$  is a  $G$ -homomorphism with order ideal  $\text{ord}(N : M')$ . But

$$R_B \text{ord}(N : M') = \text{ord}(R_B N : R_B M') = E_1 \cdots E_n,$$

so  $\text{ord}(N : M')$  is coprime to  $B_2$ , and thus  $M' \sim_{B_2} N$ . This proves the theorem.

Repeated use of formula (81.1) gives

$$\nu_B = \prod_{P|B} \nu_P$$

where  $P$  ranges over the distinct prime ideal factors of the non-zero ideal  $B$  in  $R$ . If we assume that for each  $P$  in  $R$  the residue class field  $R/P$  is finite, then Corollary 76.10 shows that each  $\nu_P$  is finite.

(81.3) DEFINITION. Two  $G$ -modules  $M, N$  are in the same *genus* if for each prime ideal  $P$  in  $R$ , we have  $M \sim_P N$ . The notation  $M \vee N$  will be used to denote the fact that  $M, N$  are in the same genus.

Certainly  $M \vee N$  implies  $M \sim_K N$ . On the other hand, Theorem 76.17 shows that if  $M \sim_K N$ , then also  $M \sim_P N$  for each  $P$  not

dividing  $i(G)$ . Consequently,  $M \vee N$  if and only if  $M \sim_K N$  and  $M \sim_P N$  for each prime  $P$  dividing  $i(G)$ . The number of genera into which  $\sigma(M)$  splits is therefore given by

$$(81.4) \quad \nu_{i(G)} = \prod_{P|i(G)} \nu_P.$$

This number is certainly finite if each field  $R/P$  is finite.

Let us prove that for each  $G$ -module  $M$  and each non-zero ideal  $B$  in  $R$ , the modules  $M$  and  $BM$  are in the same genus. They are obviously  $K$ -equivalent. Now choose<sup>t</sup> an ideal  $C$  in  $R$  coprime to  $i(G)$  so that  $BC$  is principal, say  $BC = \alpha R$ . Define the map  $T \in \text{Hom}_G(M, BM)$  by  $T(m) = \alpha m$ ,  $m \in M$ . In that case

$$\delta(T) = \text{ord}(BM : TM) = \text{ord}(BM : BCM) = C^n,$$

by the remarks of § 80 (where  $n = R$ -rank of  $M$ ). Step 1 of Theorem 81.2 at once implies that  $M \sim_{i(G)} BM$ , since  $C$  is coprime to  $i(G)$ . Therefore  $M \vee BM$ .

Conversely, we shall show

(81.5) THEOREM (Maranda [2]). *Let  $M$  be an absolutely irreducible  $G$ -module (that is,  $KM$  is an absolutely irreducible  $A$ -module), and let  $N \in \sigma(M)$ . Then  $N \vee M$  if and only if  $M \cong BN$  for some non-zero ideal  $B$  in  $R$ .*

PROOF. The discussion preceding Theorem 81.5 has already established the “if” part of the theorem, so let us proceed to the converse. Let  $N \in \sigma(M)$ ,  $N \vee M$ ; there then exists  $T \in \text{Hom}_G(M, N)$  such that  $\delta(T) + i(G) = R$ . Let  $n$  be the  $R$ -rank of  $M$ , and let

$$\delta(T) = \prod_{i=1}^r P_i^{k_i}$$

be the factorization of  $\delta(T)$  into powers of distinct prime ideals. Let  $P$  denote any one of the  $P_i$ , and drop subscripts for the moment. Then

$$\delta_P(T) = R_P \delta(T) = P^k$$

on the one hand, whereas

$$\delta_P(T) = \text{ord}(R_P N : T(R_P M))$$

on the other. Choose  $R_P$ -bases of  $R_P N$  and  $R_P M$ ; then  $T$  is represented by an  $n \times n$  matrix  $X$  over  $R_P$ , where  $n$  is the  $R$ -rank of  $M$ ,

<sup>t</sup> This can be done by Theorem 18.20.

and further  $\delta_P(T) = R_P \det X$ . This matrix  $X$  is non-zero and intertwines the  $R_P$ -representations of  $R_P G$  afforded by  $R_P N$  and  $R_P M$ . Now let  $K^*$  be the  $P$ -adic completion of  $K$ , with  $R^*$  its ring of  $P$ -adic integers. Then  $X$  also intertwines the  $R^*$ -representations of  $R^* G$  afforded by  $R^* N$  and  $R^* M$ . These  $R^*$ -representations are irreducible since  $M$  was assumed to be an absolutely irreducible  $G$ -module. Corollary 76.16 is therefore applicable [since  $P$  is coprime to  $i(G)$ ], and so we may write  $X = \pi^u X_1$  for some integer  $u$  and some  $X_1$  unimodular over  $R^*$ . Then  $\det X = \pi^{u u} \cdot \text{unit in } R^*$ , so that  $\delta_P(T) = P^{u u}$ . Furthermore,  $T \equiv 0 \pmod{P^u}$ .

Thus, for each  $i$  ( $1 \leq i \leq r$ ), we have  $k_i = n u_i$  and  $T \equiv 0 \pmod{P_i^{u_i}}$ . Set

$$B = \prod_{i=1}^r P_i^{u_i}.$$

Then  $\delta(T) = B^*$ , and  $T \equiv 0 \pmod{B}$ . The latter implies that  $TM \subset BN$ , so that we have

$$\begin{aligned} B^* &= \delta(T) = \text{ord}(N : TM) = \text{ord}(N : BN) \text{ord}(BN : TM) \\ &= B^* \text{ord}(BN : TM). \end{aligned}$$

This shows that  $\text{ord}(BN : TM) = R$ , whence  $BN = TM$ . However,  $T$  is an isomorphism of  $M$  onto  $TM$ , and so we have proved that  $M \cong BN$ , which establishes the result.

We have now shown that for an absolutely irreducible  $G$ -module  $M$ , a genus in  $\sigma(M)$  consists of all the  $G$ -modules in  $\sigma(M)$  which are  $G$ -isomorphic to  $BN$ , where  $N$  is a specific module in the genus and where  $B$  ranges over all non-zero ideals in  $R$ . Let us at once settle the question of when two modules  $BN, CN$  of the same genus are  $G$ -isomorphic. Surely, if  $B = \alpha C$ ,  $\alpha \in K$ ,  $\alpha \neq 0$ , then  $CN \cong \alpha CN = BN$  as  $G$ -modules. Thus,  $BN \cong CN$  if  $B, C$  are in the same ideal class. Conversely, suppose that there exists a  $G$ -isomorphism  $T : BN \cong CN$ . Extend  $T$  to an  $A$ -isomorphism  $T : KN \cong KN$ . Since  $N \in \sigma(M)$ ,  $KN$  is an absolutely irreducible  $A$ -module, and so  $T$  must be given by a scalar multiplication. Thus there exists  $\alpha \in K$ ,  $\alpha \neq 0$  such that  $T(x) = \alpha x$ ,  $x \in BN$ . Therefore  $\alpha BN = CN$ , which easily implies that  $\alpha B = C$ . Consequently,  $BN \cong CN$  as  $G$ -modules if and only if  $B, C$  are in the same ideal class. If  $h$  denotes the number of ideal classes in  $R$ , each genus in  $\sigma(M)$  splits into  $h$  classes under  $R$ -equivalence. Hence the number  $\nu_{\sigma(M)}$  of genera in  $\sigma(M)$  and the number  $\nu_R$  of classes under  $R$ -equivalence are related by the formula (due to Maranda)

$$(81.6) \quad \nu_R = h\nu_{i(G)},$$

and the finiteness of either side implies the finiteness of the other. (This gives another proof of the Jordan-Zassenhaus theorem for the special case in which  $M$  is absolutely irreducible).

We shall now investigate the validity of formula (81.6) when the hypothesis that  $M$  be irreducible is dropped. To begin with, we again use  $C(N, M)$  to denote the  $R$ -module whose elements are classes of binding functions for the pair  $N, M$ . An immediate consequence of formula (75.27) is the following:

(81.7) LEMMA. *Let  $M, M', N, N'$  be  $G$ -modules such that  $M \vee M'$  and  $N \vee N'$ . Then*

$$C(N, M) \cong C(N', M').$$

For the remainder of this section, we take  $L^*$  to be a fixed  $A$ -module with a composition series  $L^* \supset N^* \supset (0)$  of length 2. Set  $M^* = L^*/N^*$ , and make two restrictive assumptions:

- (i)  $M^*$  and  $N^*$  are not  $A$ -isomorphic.
- (ii)  $M^*$  and  $N^*$  are absolutely irreducible.

We shall obtain explicit formulas for both  $\nu_R$  and  $\nu_{i(G)}$ .

To begin with, let  $L \in \sigma(L^*)$ , and set  $N = N^* \cap L$ . Then  $L \supset N \supset (0)$  is an  $R$ -composition series for  $L$  with  $R$ -composition factors  $M = L/N$ , and  $N$ . In §75, we showed the existence of an element  $F \in B(N, M)$  such that  $L \cong (N, M; F)$ , the latter being defined as in §75. We now show

(81.8) LEMMA. *If  $(N, M; F) \cong (N, M; F')$ , there exist units  $\alpha, \beta$  in  $R$ , and a homomorphism  $t \in \text{Hom}_R(M, N)$  such that*

$$\alpha F_g = F'_g \beta + gt - tg, \quad g \in G.$$

*Conversely, the existence of such  $\alpha, \beta, t$  implies the above isomorphism.*

PROOF. Let  $(n, 0) \in (N, M; F)$  map onto  $(u(n), v(n)) \in (N, M; F')$ . Since this is a  $G$ -isomorphism, we have

$$g(n, 0) \rightarrow g(u(n), v(n)) = (gu(n) + F'_g v(n), gv(n)),$$

which implies

$$u(gn) = gu(n) + F'_g v(n), \quad v(gn) = gv(n).$$

But then  $v \in \text{Hom}_G(N, M)$ , and hence  $v = 0$  because  $N^*, M^*$  are irreducible and not isomorphic. Thus  $u \in \text{Hom}_G(N, N)$ , and by assumption (ii), we see that  $u$  is just a scalar multiplication by some unit  $\alpha$  in  $R$ .

Next suppose  $(0, m) \rightarrow (t(m), w(m))$ . Then

$$(F_g m, gm) = g(0, m) \rightarrow g(t(m), w(m)) = (gt(m) + F'_g w(m), gw(m)) ,$$

whereas also

$$(F_g m, gm) \rightarrow (\alpha F_g m + t(gm), w(gm)) .$$

This shows firstly that  $w \in \text{Hom}_G(M, M)$ , and so  $w$  is given by a scalar multiplication by a unit  $\beta$  in  $R$ , and secondly that

$$\alpha F_g + tg = gt + F'_g w ,$$

that is,

$$\alpha F_g = F'_g \beta + gt - tg , \quad g \in G .$$

This proves the first part of the lemma. [Compare the proof of Theorem 73.13.] The converse is straightforward since the steps are reversible.

Let us now set  $U = \text{group of units in } R$ . For each integral (non-zero) ideal  $I$  in  $R$ , let  $\phi(I)$  denote the number of residue classes in  $R/I$  which are relatively prime to  $I$ . If  $I + J = R$ , then  $\phi(IJ) = \phi(I)\phi(J)$ . Let  $u(I)$  be the number of distinct residue classes in  $(U + I)/I$ ; of course,  $u(I) | \phi(I)$ . However,  $u(I)$  is not a multiplicative function of  $I$ , as can be seen from the case in which  $R = \mathbb{Z}$ ,  $K = \mathbb{Q}$ .

Keeping assumptions (i) and (ii) and the preceding notation, we now prove

(81.9) **THEOREM** (Reiner [3]). *Let  $\sigma(N^*)$  split into  $\nu$  genera with representative modules  $N_1, \dots, N_\nu$ . Let  $\sigma(M^*)$  split into  $\mu$  genera with representative modules  $M_1, \dots, M_\mu$ . For each ideal  $I$  dividing  $i(G)$ , let  $d_{ij}(I)$  be the number of elements in the cohomology group  $C(N_i, M_j)$  having annihilator ideal  $I$ . Then  $\sigma(L^*)$  splits into  $\nu_R$  classes (under  $R$ -equivalence) and  $\nu_{i(G)}$  genera, where*

$$\nu_R = h^2 \sum_{I \mid i(G)} \sum_{i,j} \frac{d_{ij}(I)}{u(I)} ,$$

$$\nu_{i(G)} = \sum_{I \mid i(G)} \sum_{i,j} \frac{d_{ij}(I)}{\phi(I)} ,$$

and where, in the summations,  $i$  ranges from 1 to  $\nu$ ,  $j$  from 1 to  $\mu$ , and  $h = \text{class number of } R$ .

**PROOF.** Step 1. We have already shown that every  $L \in \sigma(L^*)$  is of the form  $(N, M; F)$  for some  $N \in \sigma(N^*)$ ,  $M \in \sigma(M^*)$ , and

$F \in B(N, M)$ . We now show

(i)  $(N, M; F) \sim_R (N, M; \bar{F})$  if and only if there exists a unit  $\eta \in U$  such that  $[\bar{F}] = \eta[F]$ .

(ii)  $(N, M; F) \vee (N, M; \bar{F})$  if and only if there exists an element  $\alpha \in R$  such that  $\alpha R + i(G) = R$  and  $[\bar{F}] = \alpha[F]$ .

To prove (i), we observe that by (81.8) the given modules are isomorphic if there exist units  $\alpha, \beta \in U$ , and an element  $t \in \text{Hom}_R(M, N)$  such that

$$\alpha F_g = \bar{F}_g \beta + gt - tg, \quad g \in G.$$

Dividing by  $\beta$ , this shows that  $[\bar{F}] = \alpha\beta^{-1}[F]$ . Conversely, a relation  $[\bar{F}] = \eta[F]$ ,  $\eta \in U$ , implies that  $(N, M; F) \cong (N, M; \bar{F})$  by reversing these steps.

To establish (ii), suppose first that the given modules are in the same genus. The preceding argument, with  $R$  replaced by  $R_P$ , shows that for each  $P$  dividing  $i(G)$  there exists a unit  $\alpha_P$  in  $R_P$  such that

$$[\bar{F}] = \alpha_P[F] \quad \text{in } C(R_P N, R_P M).$$

Write

$$i(G) = \prod_{P|i(G)} P^{\gamma(P)},$$

and choose  $\alpha \in R$  such that

$$\alpha \equiv \alpha_P \pmod{P^{\gamma(P)}}, \quad P|i(G).$$

Then  $\alpha R + i(G) = R$ , and we have

$$(\alpha - \alpha_P)[F] \in B'(R_P N, R_P M), \quad P|i(G).$$

Thus

$$\alpha[F] = \alpha_P[F], \quad P|i(G),$$

and so

$$[\bar{F}] = \alpha[F] \quad \text{in } C(R_P N, R_P M)$$

for each  $P|i(G)$ . Theorem 75.25 then implies that  $[\bar{F}] = \alpha[F]$  in  $C(N, M)$ . The reverse implication is straightforward, and so (ii) is proved.

*Step 2.* We next investigate the connection between classes (and genera) in  $\sigma(N^*)$ ,  $\sigma(M^*)$ , and those of  $\sigma(L^*)$ . If  $v$  is the number of genera into which  $\sigma(N^*)$  splits, we have seen [equation (81.6)]

that  $\sigma(N^*)$  splits into  $h\nu$  classes under  $R$ -equivalence. Let

$$\{N_{ij} : 1 \leq i \leq \nu, 1 \leq j \leq h\}$$

be representatives of these  $h\nu$  classes, chosen so that modules with the same index  $i$  lie in the same genus. In the same manner, choose representatives

$$\{M_{ij} : 1 \leq i \leq \mu, 1 \leq j \leq h\}$$

of the  $h\mu$  classes into which  $\sigma(M^*)$  splits. Let us show that given  $L \in \sigma(L^*)$ , there exist uniquely determined indices  $i, j$  such that

$$(81.10) \quad L \vee (N_{ii}, M_{ji}; \bar{F})$$

for some  $\bar{F} \in B(N_{ii}, M_{ji})$ . For suppose that  $L = (N, M; F)$ ,  $F \in B(N, M)$ , and choose  $i, j$  such that

$$N \vee N_{ii}, \quad M \vee M_{ji}.$$

Then for each  $P$  dividing  $i(G)$ , there exists an element  $H^P \in B(R_P N_{ii}, R_P M_{ji})$  such that

$$(R_P N, R_P M; F) \sim_P (R_P N_{ii}, R_P M_{ji}; H^P)$$

By Theorem 75.25, there exists  $\bar{F} \in B(N_{ii}, M_{ji})$  such that  $[\bar{F}] = [H^P]$ ,  $P \mid i(G)$ . Therefore

$$(N, M; F) \sim_P (N_{ii}, M_{ji}; \bar{F}), \quad P \mid i(G),$$

whence  $(N, M; F) \vee (N_{ii}, M_{ji}; \bar{F})$ . Thus (81.10) holds for some choice of  $i, j$ . On the other hand, the method of proof of Theorem 73.13 shows that if

$$(N_{ii}, M_{ji}; \bar{F}) \vee (N_{i'i}, M_{j'j}; \bar{F}'),$$

then  $i = i'$  and  $j = j'$ . This establishes the uniqueness of  $i, j$  in (81.10). Of course,  $\bar{F}$  is not uniquely determined.

*Step 3.* Let us set

$$S(i, \xi; j, \eta) = \{(N_{i\xi}, M_{j\eta}; F) : F \in B(N_{i\xi}, M_{j\eta})\}.$$

Thus  $S(i, \xi; j, \eta)$  is the collection of modules gotten by fixing  $N_{i\xi}, M_{j\eta}$  and then letting  $F$  range over all binding functions for that pair. Suppose that  $S(i, \xi; j, \eta)$  splits into  $s(i, \xi; j, \eta)$  classes under  $R$ -equivalence and into  $r(i, \xi; j, \eta)$  genera. Of course

$$r(i, \xi; j, \eta) \leq s(i, \xi; j, \eta).$$

We have shown in Step 2 that every module in  $\sigma(L^*)$  is in the

same genus as some module in  $S(i, 1; j, 1)$  for some uniquely determined  $i, j$ . Therefore the number of genera into which  $\sigma(L^*)$  splits is

$$(81.11) \quad \nu_{i(G)} = \sum_{i,j} r(i, 1; j, 1).$$

On the other hand, every module  $L$  in  $\sigma(L^*)$  is  $G$ -isomorphic to some module in some  $S(i, \xi; j, \eta)$ , and by Lemma 81.8, the indices  $i, \xi; j, \eta$  are uniquely determined by  $L$ . Hence, the number of classes into which  $\sigma(L^*)$  splits is

$$(81.12) \quad \nu_R = \sum_{i,\xi,j,\eta} s(i, \xi; j, \eta).$$

However, Step 1 states that

$$(N_{i\xi}, M_{j\eta}; F) \sim_R (N_{i\xi}, M_{j\eta}; \bar{F})$$

if and only if  $[\bar{F}] = \beta[F]$  for some  $\beta \in U$ . Furthermore, (81.7) implies that  $C(N_{j\xi}, M_{j\eta})$  is, as  $R$ -module, independent of  $\xi$  and  $\eta$ . Therefore

$$s(i, \xi; j, \eta) = s(i, 1; j, 1) \quad \text{for all } \xi, \eta.$$

Hence we have

$$(81.13) \quad \nu_R = h^2 \sum_{i,j} s(i, 1; j, 1).$$

*Step 4.* For  $N \in \sigma(N^*)$  and  $M \in \sigma(M^*)$ , let us use the symbol  $(N, M; c)$  to denote the collection of mutually isomorphic modules  $\{(N, M; F) : F \in c\}$  in which  $c$  is a cohomology class in  $C(N, M)$ . In Step 3, we were led to consider the number of classes and genera into which

$$S = \{(N, M; F) : F \in B(N, M)\}$$

splits. We shall regard  $S$  as a union of subcollections  $(N, M; c)$  as  $c$  ranges over all elements of  $C(N, M)$ .

For  $I$  a divisor of  $i(G)$ , we let  $d(I)$  be the number of elements of  $C(N, M)$  with annihilator ideal  $I$ . Now Step 1 tells us that  $(N, M; c)$  and  $(N, M; c')$  cannot lie in the same genus unless  $c, c'$  have the same annihilator ideal. Consider the set of  $d(I)$  elements of  $C(N, M)$  with given order ideal  $I$ . For a fixed  $c$  in this set, all  $c'$  of the form  $\alpha c$ , where  $\alpha \in R$  is such that  $\alpha R + i(G) = R$ , will yield modules in the same genus as those obtained from  $c$ . But, as  $\alpha$  ranges over all elements of  $R$  which are coprime to  $i(G)$ ,  $\alpha c$  gives exactly  $\phi(I)$  distinct elements of  $C(N, M)$ , where  $\phi(I)$  is the number

of residue classes in  $R/I$  which are coprime to  $I$ . Consequently, the number of genera in  $S$  is

$$(81.14) \quad r = \sum_I \frac{d(I)}{\phi(I)},$$

the sum extending over all ideals  $I$  which divide  $i(G)$ .

A similar argument now shows that number of classes in  $S$  is

$$(81.15) \quad s = \sum_I \frac{d(I)}{u(I)}$$

where  $u(I)$  is the number of distinct residue classes in  $(U + I)/I$ .

*Step 5.* Returning to the main result, we see that the modules  $N_1, \dots, N_v, M_1, \dots, M_\mu$  mentioned in the hypothesis of the theorem are just what have been denoted by  $N_{11}, \dots, N_{v1}, M_{11}, \dots, M_{\mu 1}$ . We need only substitute into formulas (81.11) and (81.13) the expressions given in (81.14) and (81.15) for  $r(i, 1; j, 1)$  and  $s(i, 1; j, 1)$ , to obtain the result stated in the theorem. This proves the theorem.

(81.16) **COROLLARY.** *We have  $\nu_R \geq h^2 \nu_{i(G)}$ , with equality provided that  $\phi(i(G)) = u(i(G))$ . Furthermore, if any  $C(N_i, M_i)$  contains an element with annihilator ideal  $I$  for which  $u(I) < \phi(I)$ , then  $\nu_R > h^2 \nu_{i(G)}$ .*

The preceding corollary may be generalized to the case where  $L^*$  has  $k$  distinct absolutely irreducible composition factors,  $k \geq 2$ ; (see Reiner [3]).

It would be of interest to obtain relations between  $\nu_R$  and  $\nu_{i(G)}$  without such restrictive hypotheses on the module  $L^*$ . Even when  $L^*$  is irreducible but not absolutely irreducible, the problem is already a very deep one, as can be seen from Takahashi [1] and Eichler [1] and [2].

### §81A. *Indecomposable modules*

Throughout this appendix, let  $R$  be the ring of all algebraic integers in an algebraic number field  $K$ , and let  $G$  be a finite group. By  $n(RG)$  we denote the number of indecomposable  $RG$ -modules, where we choose one module from each isomorphism class. We shall give a brief survey of the present state of knowledge concerning the finiteness of  $n(RG)$ , with special emphasis on the case  $R = \mathbb{Z}$ .

In §74 we proved that  $n(ZG)$  is finite for  $G$  cyclic of prime order  $p$ . Heller and Reiner [2, I] have shown that  $n(ZG)$  is finite for  $G$  cyclic of order  $p^2$ , where  $p$  is any prime. (This result has

been obtained independently by Knee [1], and for the special case where  $p = 2$ , by Roiter [1] and Troy [1]). On the other hand, Heller and Reiner [2, II], and independently Dade [1], have proved that  $n(ZG)$  is infinite if  $G$  is cyclic of order  $p^n$ ,  $n \geq 3$ ,  $p$  prime, and also that  $n(ZG)$  is infinite if  $G$  is a non-cyclic  $p$ -group. (For this last result, see also Borevich and Faddeev [1, II]).

Turning now from  $p$ -groups to arbitrary finite groups, we sketch a proof of the following striking result:

(81.18) **THEOREM** (Jones [1]). *The number  $n(ZG)$  of indecomposable  $ZG$ -modules is finite if and only if for each prime  $p$  dividing the order of  $G$ , each  $p$ -Sylow subgroup of  $G$  is cyclic of order at most  $p^2$ .*

In one direction, the theorem is fairly simple. Suppose that  $G$  has a  $p$ -Sylow subgroup  $H$  which is either non-cyclic or else cyclic of order greater than  $p^2$ . We shall show that  $n(ZG)$  must be infinite. For suppose otherwise, and let  $\{Y_1, \dots, Y_t\}$  be a full set of indecomposable  $ZG$ -modules. From the results of Heller and Reiner [2, II] (or those of Dade [1]) one easily deduces the existence of an infinite set  $\{M_1, M_2, \dots\}$  of indecomposable  $ZH$ -modules, with the following properties: (i) The  $Z$ -rank  $(M_i : Z)$  steadily increases with increasing  $i$ , and (ii) Each  $M_i^*$  is also indecomposable, where  $M_i^* = Z_p^* \otimes_Z M_i$ , and where  $Z_p^*$  denotes the ring of  $p$ -adic integers in the  $p$ -adic completion of  $\mathbb{Q}$ .

For each  $i$ , the induced  $ZG$ -module  $M_i^G$  may be written as a direct sum of copies of  $Y_1, \dots, Y_t$ . Thence  $(M_i^*)^G$  is a direct sum of copies of  $Y_1^*, \dots, Y_t^*$ , where  $Y_i^* = Z_p^* \otimes_Z Y_i$ . Letting the subscript  $H$  denote restriction to  $H$ , we have for each  $i$ :

$$(81.19) \quad \{(M_i^*)^G\}_H \cong \text{direct sum of copies of } (Y_1^*)_H, \dots, (Y_t^*)_H.$$

As in the proof of Theorem 63.6, we find readily that  $M_i^*$  is a direct summand of the left-hand side. Furthermore,  $M_i^*$  is an indecomposable  $Z_p^* H$ -module. It follows from (81.19) and the Krull-Schmidt theorem for  $Z_p^* H$ -modules (see (76.26)) that  $M_i^*$  is isomorphic to a direct summand of  $(Y_j^*)_H$  for some  $j$ . This gives an upper bound, independent of  $i$ , for the  $Z$ -ranks  $(M_i : Z)$ , and so we have obtained a contradiction. Thus  $n(ZG)$  must be infinite in this case.

In order to prove the more difficult half of (81.18), we need several preliminary results. Hereafter, let  $R'$  denote the ring of all elements of  $K$  which are integral at all prime ideals of  $R$  which divide the order of  $G$ . Let  $R_P$  be the ring of  $P$ -integral elements of  $K$ , where  $P$  is a prime ideal of  $R$ , and let  $R_P^*$  denote the com-

pletion of  $R_P$ .

(81.20) LEMMA (Reiner [9]). *Let  $M$  be an  $RG$ -module, and define  $R'M$  as  $R' \otimes_R M$ . Then  $M$  is indecomposable if and only if the  $R'G$ -module  $R'M$  is indecomposable.*

PROOF. Decomposability of  $M$  clearly implies that of  $R'M$ . Conversely, let  $N'$  be an  $R'G$ -direct summand of  $R'M$ . As in the proof of (75.2), there exists an  $RG$ -submodule  $N$  of  $M$  such that  $R'N = N'$ . It follows that for each prime ideal  $P$  dividing the order of  $G$ , the module  $R_P N$  is a direct summand of  $R_P M$ . From (75.27) we conclude at once that  $N$  is a direct summand of  $M$ .

Using this result, together with the Jordan-Zassenhaus Theorem 79.1, we have

(81.21) COROLLARY.  *$n(RG)$  is finite if and only if  $n(R'G)$  is finite.*

The basic lemma for the proof of (81.18) is as follows:

(81.22) LEMMA (Jones [1]).  *$n(R'G)$  is finite if for each  $P$  which divides the order of  $G$ ,  $n(R_P^* G)$  is finite.*

PROOF. Suppose  $n(R_P^* G)$  finite for each  $P$  dividing the order of  $G$ . Let  $M$  be any  $R'G$ -module, and let  $R_P^* M$  be defined as  $R_P^* \otimes_{R'} M$ . For each of the above  $P$ 's,  $R_P^* M$  may be expressed as a direct sum of copies of the  $n(R_P^* G)$  indecomposable  $R_P^* G$ -modules, with multiplicities  $a_1^P, \dots, a_{n(R_P^* G)}^P$ , say. Arrange the non-negative integers

$$\{a_i^P : 1 \leq i \leq n(R_P^* G), P \mid [G : 1]\}$$

into a sequence in some fixed way, and denote this finite sequence by  $\varphi(M) = (a_1, \dots, a_t)$ , say. Partially order the set  $\mathcal{S}$  of all such  $t$ -tuples (which arise from  $R'G$ -modules) by writing  $(a_1, \dots, a_t) \leq (b_1, \dots, b_t)$  whenever  $a_i \leq b_i$  for  $1 \leq i \leq t$ .

Suppose now that  $M$  and  $N$  are  $R'G$ -modules for which  $\varphi(N) < \varphi(M)$ . We claim that  $N$  is isomorphic to a direct summand of  $M$ . For the hypothesis implies that

$$R_P^* M \cong R_P^* N \oplus X_P^*, \quad P \mid [G : 1],$$

for some  $R_P^* G$ -module  $X_P^*$ . As in the proof of (76.28), and using the technique due to Feit given at the end of §41A, one deduces the existence of an  $R_P G$ -module  $Y_P$  such that  $R_P^* Y_P = X_P^*$ . It follows from (81.2) that there exists an  $R'G$ -module  $X$  such that  $Y_P = R_P X$  for each  $P$  dividing the order of  $G$ . But then  $R_P^* M \cong R_P^* (N + X)$  for each such  $P$ . By (76.9) this implies  $R_P M \cong R_P (N + X)$  for each such  $P$ , whence  $M \cong N + X$ .

The above argument shows that an  $R'G$ -module  $M$  is indecomposable if and only if  $\varphi(M)$  is a minimal element of the partially ordered set  $\mathcal{S}$ . A straightforward proof, which we leave to the reader, shows that  $\mathcal{S}$  can have only a finite number of minimal elements. This completes the proof of the lemma.

Suppose now that for each prime  $p$  dividing  $[G : 1]$ , each  $p$ -Sylow subgroup of  $G$  is cyclic of order at most  $p^2$ . If  $H_p$  denotes any  $p$ -Sylow subgroup of  $G$ , then from Heller and Reiner [2, I] it follows that  $n(Z_p^*H_p)$  is finite. However, the finiteness of  $n(Z_p^*H_p)$  implies the finiteness of  $n(Z_p^*G)$ , since the proof of the relevant part of Theorem 64.1 applies equally well to  $Z_p^*G$ -modules. We have thus shown that  $n(Z_p^*G)$  is finite for each  $p$  dividing  $[G : 1]$ . By (81.22), this implies the finiteness of  $n(ZG)$ , and so (81.18) is established.

To conclude this chapter, we list some additional references. The indecomposable integral representations of a cyclic group of squarefree order are given in Knee [1] and Oppenheim [Ph. D. thesis, University of Illinois, 1962]. Those of the dihedral group of order  $2p$ ,  $p$  an odd prime, have been determined by Leahey [1] and Lee [1]. Nazarova [1] has fully described the infinite set of indecomposable  $ZG$ -modules for the case where  $G$  is a direct product of two cyclic groups of order 2.

Additional references for this chapter are Bass [2, 3], Berman [16, 17], Berman and Gudivok [1, 2, 3], Faddeev [11], Gruenberg [1], Gudivok [1, 2, 3, 4], Gudivok, Drobotenko, and Lichtman [1], Heller and Reiner [3, 4, 5], Jones [2, 3, 4], Kneser [1], Lee [2], Nazarova [2], Nazarova and Roiter [1], Pu [1], Rayna [1], Reiner [10, 11, 12, 13], Roiter [2, 3], Swan [5, 6].

This page intentionally left blank

## Modular Representations

Throughout this chapter, let  $G$  be a finite group of order of order  $g$ , and  $\bar{K}$  a field of characteristic  $p$ . We shall be concerned with  $\bar{K}$ -representations of  $G$ , and most of the interest will center in the case where  $p \nmid g$ . The main results are due to Brauer, who has obtained many striking and important theorems on this subject in a long series of papers during the last 35 years. It has not been possible to include all of Brauer's work, but we have attempted to give those major results which could be fitted into a unified treatment and which do not require many specialized preliminaries from algebraic number theory or group theory. In § 90, we have sketched briefly some of the results which we were unable to treat in detail and have given references there for further reading. As general references for this chapter, we may cite the semi-expository papers by Brauer and Nesbitt [3] and Brauer [27].

The theory of modular representations establishes deeper connections between the structure of the group and the properties of the representations than the theory presented in Chapters IV through VI, and for this reason it is to be hoped that modular representations will find many applications to group theory. We have not attempted to include in the book the applications which have been obtained so far. We do present in § 92, however, a brief guide to the literature on these questions, which should serve as a starting point for further study.

We shall assume that the reader is familiar with some of the earlier theorems in this book, and in particular, we shall need results from the following sections:

Chapter III, §§ 16–21; Chapter V, §§ 30–31, § 33; Chapter VI, § 38, § 40; Chapter VIII, §§ 54–55; Chapter IX, §§ 60–63; Chapter X, §§ 68–70; Chapter XI, beginning of § 73, part of § 77.

Some simple examples are worked out in § 91, and the reader is urged to refer ahead to this section to see examples of the main concepts as he proceeds through the chapter.

A great deal of notation will be fixed once and for all for the purposes of this chapter. We list some of it here, and the rest in

some of the subsequent sections.

$G$  = finite group of order  $g$

$K$  = algebraic number field,  $R$  = alg. int.  $\{K\}$

$P$  = prime ideal in  $R$ ,  $p$  = unique rational prime in  $P$

$\nu$  = "additive" valuation on  $K$  associated with the prime ideal

$P$ , multiplied by a factor to make  $\nu(p) = 1$  (see § 19)

$\pi$  = element of  $R$  with smallest positive  $\nu(\pi)$

$R_P$  = ring of  $P$ -integral elements of  $K = \{\alpha \in K : \nu(\alpha) \geq 0\}$

$\pi R_P$  = unique maximal ideal in  $R_P$

$\bar{K} = R/P \cong R_P/\pi R_P$  = residue class field = finite field of characteristic  $p$

$K^*$  =  $P$ -adic completion of  $K$ ,  $R^*$  =  $P$ -adic integers in  $K^*$ ,

$P^* = \pi R^*$ ,  $\bar{K} \cong R^*/P^*$

$\alpha \in R$  (or  $\alpha \in R_P$  or  $\alpha \in R^*$ )  $\rightarrow \bar{\alpha} \in \bar{K}$ .

For  $X = (\alpha_{ij})$ ,  $\{\alpha_{ij}\} \in R$ , let  $\bar{X} = (\bar{\alpha}_{ij})$  = matrix over  $\bar{K}$ . Let  $|X| = \det X$  = determinant of  $X$ .

$\bar{\bar{\alpha}}$  = complex conjugate of the complex number  $\alpha$

Let  $x \in G$  have order  $n$ ; call  $x$  *p-regular* if  $p \nmid n$ , *p-irregular* if  $p \mid n$ , *p-singular* if  $n$  = power of  $p$ . (Caution: this represents a change from the terminology used in the literature.)

## § 82. Introduction

Let us begin by showing how to associate with each representation  $T: G \rightarrow K_n$  a collection of  $\bar{K}$ -representations of  $G$ . Since  $R_P$  is a principal ideal domain with quotient field  $K$ , we may apply Theorem 73.6 to deduce that  $T$  is  $K$ -equivalent to an  $R_P$ -representation  $U$  which maps each  $x \in G$  onto an  $n \times n$  matrix  $U(x)$  with entries in  $R_P$ . Define  $\bar{U}: G \rightarrow \bar{K}_n$  by means of

$$\bar{U}(x) = \overline{U(x)}, \quad x \in G.$$

It is easily seen that  $\bar{U}$  is a  $\bar{K}$ -representation of  $G$ ; we say that  $\bar{U}$  is a *modular representation associated with T* (or with  $U$ ). In general the  $K$ -representation  $T$  does not determine  $U$  up to  $R_P$ -equivalence, and hence the  $\bar{K}$ -representations  $\bar{U}$  associated with  $T$  are not necessarily  $\bar{K}$ -equivalent. For example, let  $G = [x]$  be cyclic of order 2, and let

$$T_1(x) = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad T_2(x) = \begin{pmatrix} 1 & 1 \\ 0 & -1 \end{pmatrix},$$

thereby defining a pair of  $Q$ -representations  $\mathbf{T}_1$  and  $\mathbf{T}_2$  of  $G$ . We find readily that  $\mathbf{T}_1 \sim_Q \mathbf{T}_2$  but that  $\bar{\mathbf{T}}_1$  and  $\bar{\mathbf{T}}_2$  are *not*  $\bar{Q}$ -equivalent where  $\bar{Q} = Z/2Z$ . (Note however that  $\bar{\mathbf{T}}_1$  and  $\bar{\mathbf{T}}_2$  have the same composition factors!)

Let us restate the above in terms of modules. By Theorem 73.6, each  $KG$ -module  $M_0$  contains an  $R_P G$ -submodule  $M$  having an  $R_P$ -basis of  $(M_0 : K)$  elements, and such that  $M_0 = KM$ . We then form the left  $\bar{K}G$ -module  $\bar{M} = M/PM$ , and obviously  $(\bar{M} : \bar{K}) = (M_0 : K)$ . The module  $M$  is not uniquely determined by  $M_0$ , not even up to  $R_P G$  isomorphism, and so the module  $\bar{M}$  need not be determined up to  $\bar{K}G$ -isomorphism by  $M_0$ .

In view of this fact, the following basic result is even more remarkable:

(82.1) **THEOREM** (*Brauer and Nesbitt [1]*). *Two  $\bar{K}$ -representations of  $G$  associated with the same  $K$ -representation have the same composition factors.*

**FIRST PROOF.** Let  $\mathbf{T}$  and  $\mathbf{U}$  be a pair of  $R_P$ -representations of  $G$  which are  $K$ -equivalent. We must show that  $\bar{\mathbf{T}}$ ,  $\bar{\mathbf{U}}$  have the same composition factors. For each  $x \in G$ , the matrices  $\mathbf{T}(x)$  and  $\mathbf{U}(x)$  have the same characteristic polynomial since  $\mathbf{T} \sim_K \mathbf{U}$ . But the characteristic polynomial of  $\bar{\mathbf{T}}(x)$  is gotten from that of  $\mathbf{T}(x)$  by taking each coefficient mod  $PR_P$ , and so for each  $x \in G$ , the matrices  $\bar{\mathbf{T}}(x)$  and  $\bar{\mathbf{U}}(x)$  have the same characteristic roots. Since  $\bar{K}$  is a finite field, it follows from Chapter X [§69, especially (69.9) and (69.11)] that the hypotheses of Theorem 30.16 are valid, and consequently that  $\bar{\mathbf{T}}$  and  $\bar{\mathbf{U}}$  have the same composition factors.

**SECOND PROOF.** Let  $\mathbf{T}$  and  $\mathbf{U}$  be as above. Since  $\mathbf{T} \sim_K \mathbf{U}$ , there exists a non-singular  $K$ -matrix  $\mathbf{W}$  such that

$$\mathbf{T}(x)\mathbf{W} = \mathbf{W}\mathbf{U}(x), \quad x \in G.$$

Replacing  $\mathbf{W}$  by  $\pi^a \mathbf{W}$  for suitable  $a$ , we may assume that all entries of  $\mathbf{W}$  are in  $R_P$  with at least one entry a unit in  $R_P$ . If  $|\bar{\mathbf{W}}| \neq 0$ , then from  $\bar{\mathbf{T}}(x)\bar{\mathbf{W}} = \bar{\mathbf{W}}\bar{\mathbf{U}}(x)$ ,  $x \in G$ , we deduce that  $\bar{\mathbf{T}} \sim_{\bar{K}} \bar{\mathbf{U}}$ , and we have completed the proof. If  $|\bar{\mathbf{W}}| = 0$ , choose  $\mathbf{Y}$  and  $\mathbf{Z}$  unimodular over  $R_P$  such that

$$\mathbf{Y}\mathbf{W}\mathbf{Z} = \begin{pmatrix} A & 0 \\ 0 & \pi B \end{pmatrix}$$

where  $A$  is unimodular over  $R_P$  and  $B$  is non-singular with entries in  $R_P$ . Set

$$\mathbf{T}' = \mathbf{Y} \mathbf{T} \mathbf{Y}^{-1}, \quad \mathbf{U}' = \mathbf{Z}^{-1} \mathbf{U} \mathbf{Z}.$$

Then

$$\mathbf{T}' \sim_{\kappa} \mathbf{U}', \quad \mathbf{T}' \cdot \mathbf{Y} \mathbf{W} \mathbf{Z} = \mathbf{Y} \mathbf{W} \mathbf{Z} \cdot \mathbf{U}',$$

and it suffices to show that  $\bar{\mathbf{T}}'$ ,  $\bar{\mathbf{U}}'$  have the same composition factors.

Let us write

$$\mathbf{T}' = \begin{pmatrix} \mathbf{A}_1 & \mathbf{B}_1 \\ \mathbf{C}_1 & \mathbf{D}_1 \end{pmatrix}, \quad \mathbf{U}' = \begin{pmatrix} \mathbf{A}_2 & \mathbf{B}_2 \\ \mathbf{C}_2 & \mathbf{D}_2 \end{pmatrix}.$$

[Actually we mean  $A_1(x), \dots, x \in G$ .] Then we have

$$\begin{pmatrix} \mathbf{A}_1 & \mathbf{B}_1 \\ \mathbf{C}_1 & \mathbf{D}_1 \end{pmatrix} \begin{pmatrix} \mathbf{A} & \\ \pi \mathbf{B} & \end{pmatrix} = \begin{pmatrix} \mathbf{A} & \\ \pi \mathbf{B} & \end{pmatrix} \begin{pmatrix} \mathbf{A}_2 & \mathbf{B}_2 \\ \mathbf{C}_2 & \mathbf{D}_2 \end{pmatrix},$$

and so  $\mathbf{C}_1 \mathbf{A} = \pi \mathbf{B} \mathbf{C}_2$ ,  $\pi \mathbf{B}_1 \mathbf{B} = \mathbf{A} \mathbf{B}_2$ . Since  $\bar{\mathbf{A}}$  is non-singular, this gives  $\bar{\mathbf{C}}_1 = \mathbf{0}$ ,  $\bar{\mathbf{B}}_2 = \mathbf{0}$ , and consequently

$$\bar{\mathbf{T}}' = \begin{pmatrix} \bar{\mathbf{A}}_1 & \bar{\mathbf{B}}_1 \\ \bar{\mathbf{0}} & \bar{\mathbf{D}}_1 \end{pmatrix}, \quad \bar{\mathbf{U}}' = \begin{pmatrix} \bar{\mathbf{A}}_2 & \bar{\mathbf{0}} \\ \bar{\mathbf{C}}_2 & \bar{\mathbf{D}}_2 \end{pmatrix}.$$

The composition factors of  $\bar{\mathbf{T}}'$  are those of  $\bar{\mathbf{A}}_1$  together with those of  $\bar{\mathbf{D}}_1$ , whereas the composition factors of  $\bar{\mathbf{U}}'$  are those of  $\bar{\mathbf{A}}_2$  together with those of  $\bar{\mathbf{D}}_2$ . But we have  $\bar{\mathbf{A}}_1 \bar{\mathbf{A}} = \bar{\mathbf{A}} \bar{\mathbf{A}}_2$ ,  $\bar{\mathbf{D}}_1 \mathbf{B} = \mathbf{B} \bar{\mathbf{D}}_2$ , with  $\mathbf{B}$  non-singular. The first of these equations shows that  $\bar{\mathbf{A}}_1$  and  $\bar{\mathbf{A}}_2$  have the same composition factors (indeed, are  $\bar{K}$ -equivalent), whereas the second equation permits us to conclude by an induction argument that  $\bar{\mathbf{D}}_1$  and  $\bar{\mathbf{D}}_2$  have the same composition factors. This completes the proof.

(Other proofs are given by Brauer [27 I, p. 443] and Swan [4].)

(82.2) COROLLARY. If  $p \nmid g$  and if  $\mathbf{T}, \mathbf{U}$  are  $R_p$ -representations of  $G$  which are  $K$ -equivalent, then  $\bar{\mathbf{T}}$  and  $\bar{\mathbf{U}}$  are  $\bar{K}$ -equivalent.

PROOF. The preceding theorem shows that  $\bar{\mathbf{T}}$  and  $\bar{\mathbf{U}}$  have the same composition factors. The result now follows from the semi-simplicity of  $\bar{K}G$ .

[This corollary has also been established in (76.17).]

We shall refer to  $\bar{K}$ -representations as *modular representations*. As can be seen from Exercise 82.1, there exist modular representations which are not associated with any  $K$ -representation of  $G$ . We have already noticed, in the example preceding Theorem 30.15, that inequivalent modular representations may have the same character. On the other hand, we have used Theorem 30.16 which states that the composition factors of a modular representation are deter-

mined by the characteristic roots of the representing matrices. Our next aim is to improve this last result. For  $x \in G$ , let  $x = x_1x_2$  be its decomposition into a  $p$ -regular component  $x_1$  and a  $p$ -singular component  $x_2$  [see Lemma 40.3]. If  $\mathbf{T}$  is any  $\bar{K}$ -representation of  $G$ , then

$$\mathbf{T}(x) = \mathbf{T}(x_1)\mathbf{T}(x_2).$$

Since  $x_1$  and  $x_2$  commute, so do  $\mathbf{T}(x_1)$  and  $\mathbf{T}(x_2)$ , and from this it follows [by Theorem 30.2] that the characteristic roots of  $\mathbf{T}(x)$  are the products of the characteristic roots of  $\mathbf{T}(x_1)$  with those of  $\mathbf{T}(x_2)$  in some order. But  $x_2$  is  $p$ -singular, so each characteristic root of  $\mathbf{T}(x_2)$  equals 1. Thus the characteristic roots of  $\mathbf{T}(x)$  coincide with those of  $\mathbf{T}(x_1)$ , and we have proved

(82.3) THEOREM. *Let  $S$  and  $T$  be  $\bar{K}$ -representations of  $G$ . Then  $S$  and  $T$  have the same composition factors if and only if for each  $p$ -regular  $x \in G$ , the matrices  $S(x)$  and  $T(x)$  have the same characteristic roots.*

The above remarks also establish

(82.4) THEOREM. *Let  $\sigma$  and  $\tau$  be characters of  $\bar{K}$ -representations of  $G$ . Then  $\sigma = \tau$  if and only if  $\sigma(x) = \tau(x)$  for all  $p$ -regular  $x \in G$ .*

As a consequence of this we have

(82.5) COROLLARY. *Let  $S$  and  $T$  be absolutely irreducible  $\bar{K}$ -representations of  $G$ , with characters  $\sigma$  and  $\tau$ , respectively. Then  $S \sim_{\bar{K}} T$  if and only if  $\sigma(x) = \tau(x)$  for all  $p$ -regular  $x$  in  $G$ .*

PROOF. Use Theorems (30.15) and (82.4).

Another important result which follows from the above is:

(82.6) COROLLARY. *The number of non-isomorphic absolutely irreducible  $\bar{K}G$ -modules is less than or equal to the number of  $p$ -regular classes in  $G$ .*

PROOF. Let  $\bar{\varphi}^{(1)}, \dots, \bar{\varphi}^{(r)}$  be the characters of the absolutely irreducible  $\bar{K}G$ -modules. These characters are linearly independent over  $\bar{K}$  by Theorem 30.12. On the other hand, if  $x_1, \dots, x_t$  are representatives of the  $t$   $p$ -regular classes in  $G$ , then by Theorem 82.4 each  $\bar{\varphi}^{(i)}$  is determined by the  $t$ -tuple

$$(\bar{\varphi}^{(i)}(x_1), \dots, \bar{\varphi}^{(i)}(x_t)),$$

and thus these  $r t$ -tuples are also linearly independent over  $\bar{K}$ . This shows at once that  $r \leq t$  and proves the result.

*Remarks.* (i) When  $p \nmid g$ , this reduces to a special case of (27.25).

(ii) In § 83, we shall show that  $r = t$  whenever  $\bar{K}$  is a splitting field for  $G$ .

Now let  $M$  be an  $R_P G$ -module affording the character  $\mu$ . Clearly  $\mu(x) \in R_P$  for all  $x \in G$ , and so we may form its residue class  $\overline{\mu(x)}$  in  $\bar{K}$ . The map

$$\bar{\mu}: x \rightarrow \overline{\mu(x)}, \quad x \in G,$$

is well defined, and indeed  $\bar{\mu}$  is the character afforded by the  $\bar{K}G$ -module  $\bar{M} = M/PM$ . Thus with each character  $\mu$  of a  $K$ -representation of  $G$  is associated a *modular character*  $\bar{\mu}$ , and  $\bar{\mu}$  depends only on  $\mu$  because of Theorem 82.1.

We shall now reverse this process, in a sense, and show how to assign to each modular representation of  $G$  a new kind of character, which we shall call the *Brauer character\** and which maps each  $p$ -regular element of  $G$  onto a sum of *complex* roots of 1. Let  $m = \text{L.C.M.}$  of the orders of the  $p$ -regular elements of  $G$ , and set

$$\tilde{K} = K(\sqrt[m]{1}), \quad \tilde{R} = \text{alg. int. } \{\tilde{K}\}.$$

Let  $\tilde{P}$  be some fixed prime ideal of  $\tilde{R}$  such that  $\tilde{P} \supset P$ ; then  $\tilde{R}/\tilde{P}$  is a field which is a finite extension of  $\bar{K}$ . We again use  $\bar{\alpha}$  to denote the image in  $\tilde{R}/\tilde{P}$  of an element  $\alpha \in \tilde{R}$ . Let  $\delta \in \tilde{R}$  be a primitive  $m$ th root of 1 over  $K$ . If  $X$  denotes an indeterminate, we have

$$X^m - 1 = \prod_{a=1}^m (X - \delta^a).$$

Taking residues mod  $\tilde{P}$ , we obtain

$$X^m - \bar{1} = \prod_{a=1}^m (X - \bar{\delta}^a),$$

which shows that  $\bar{\delta}$  is a primitive  $m$ th root of 1 over  $\bar{K}$ . Thus we have  $\tilde{R}/\tilde{P} = \bar{K}(\bar{\delta}) = \bar{K}(\sqrt[m]{1})$ ; also  $(K(\delta): K) \cong (\bar{K}(\bar{\delta}): \bar{K})$ , but equality need not hold. In any case, the mapping  $\delta^a \rightarrow \bar{\delta}^a$ ,  $1 \leq a \leq m$ , is an isomorphism of the multiplicative group of  $m$ th roots of 1 over  $K$  onto the corresponding group over  $\bar{K}$ . This isomorphism may be realized in more than one way, however, since there are usually several choices for the ideal  $\tilde{P}$ .

Suppose now that  $T: G \rightarrow \bar{K}_n$  is a modular representation with

\*This “Brauer character” has sometimes been referred to in the literature as a “modular character.” We feel that our present terminology is less misleading.

character  $\tau$ , and let  $x \in G$  be  $p$ -regular. The characteristic roots of  $T(x)$  are powers of  $\bar{\delta}$ , and so we may write, say,

$$\tau(x) = \bar{\delta}^{a_1} + \cdots + \bar{\delta}^{a_n}.$$

Define

$$\chi(x) = \delta^{a_1} + \cdots + \delta^{a_n} \in \tilde{R}.$$

We call  $\chi$  the *Brauer character* of  $T$  and  $\tau$  the (modular) *character* of  $T$ . Clearly

$$\overline{\chi(x)} = \tau(x), \quad x \in G, x \text{ } p\text{-regular}.$$

Equivalent modular representations have the same Brauer character. On the other hand, if  $W$  is an  $R_p$ -representation of  $G$  with character  $\omega$ , and if  $\bar{W}$  is the modular representation of  $G$  associated with  $W$ , the Brauer character of  $\bar{W}$  coincides with  $\omega$  on the  $p$ -regular elements of  $G$ .

The importance of the Brauer character stems from

(82.7) THEOREM. *Let  $T$  and  $U$  be  $\bar{K}$ -representations of  $G$  with Brauer characters  $\tau$  and  $\eta$ , respectively. Then  $T$  and  $U$  have the same composition factors if and only if  $\tau = \eta$ .*

PROOF. The implication is trivial in one direction. For the other, suppose that  $\tau(x) = \eta(x)$  for  $p$ -regular  $x$  in  $G$ . If  $x \in G$  is  $p$ -regular, so also are  $x^2, x^3$ , etc., and thus

$$(82.8) \quad \tau(x^c) = \eta(x^c), \quad c = 0, 1, 2, \dots.$$

But for each such  $x$ , let us write, say,

$$\tau(x) = \delta^{a_1} + \cdots + \delta^{a_n}, \quad \eta(x) = \delta^{b_1} + \cdots + \delta^{b_n}.$$

By (82.8), we have

$$(\delta^{a_1})^c + \cdots + (\delta^{a_n})^c = (\delta^{b_1})^c + \cdots + (\delta^{b_n})^c, \quad c = 0, 1, 2, \dots.$$

This implies (see van der Waerden [2,I]) that the elementary symmetric functions of the sets  $\{\delta^{a_1}, \dots, \delta^{a_n}\}$  and  $\{\delta^{b_1}, \dots, \delta^{b_n}\}$  coincide, and hence the sets are identical. We have thus shown that for each  $p$ -regular  $x$  in  $G$ , the matrices  $T(x)$  and  $U(x)$  have the same characteristic roots. The result now follows from Theorem 82.3.

### Exercises

1. Let  $p$  be prime,  $p > 3$ . Let  $G$  be cyclic, generated by an element  $x$  of order  $p$ . Set  $\bar{Q} = Z/pZ$ , and let  $T$  be the  $\bar{Q}$ -representation of  $G$  defined by

$$T(x) = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

Show that  $T$  is not associated with any  $Q$ -representation of  $G$ .

2. Let  $x$  and  $y$  be  $p$ -regular elements of  $G$  belonging to the same conjugate class, and let  $\chi$  be a Brauer character of  $G$ . Prove that  $\chi(x) = \chi(y)$ .

### § 83. Cartan Invariants and Decomposition Numbers

Keeping the notation of the preceding section, we now make the simplifying hypothesis that  $K$  is a splitting field for  $G$  and for all subgroups and factor groups of  $G$ . This will surely be the case if  $\sqrt[n]{1} \in K$ , where  $n$  is the exponent of  $G$ , but we do not really need this deep result for our discussion, and can instead rely on Theorem 29.16 which guarantees the existence of such an algebraic number field  $K$ . (In § 83 A, we treat briefly the more general case where  $K$  need not be a splitting field for  $G$ , but most of the discussion in this chapter will be restricted to the splitting field case.)

For the remainder of this chapter, we fix the following notation:  
(83.1):

Rep. space	Matrix rep.	Degree	Brauer char.	Ordinary char.	Index set
$Z_i$	$Z_i$	$z_i$	—	$\zeta^{(i)}$	$1 \leq i \leq s$
$F_j$	$F_j$	$f_j$	$\varphi^{(j)}$	$\bar{\varphi}^{(j)}$	$1 \leq j \leq r$
$U_j$	$U_j$	$u_j$	$\eta^{(j)}$	$\bar{\eta}^{(j)}$	$1 \leq j \leq r$

Here  $Z_1, \dots, Z_s$  are a full set of inequivalent irreducible  $K$ -representations of  $G$ . By Theorem 73.6 we may choose these representations so that each  $Z_i$  is an  $R_P$ -representation of  $G$ , afforded by the  $R_P G$ -module  $Z_i$ . Since  $K$  is assumed to be a splitting field for  $G$ , each  $KG$ -module  $KZ_i$  is absolutely irreducible, and thus  $s$  is the number of conjugate classes of  $G$ .

In the above chart,  $F_1, \dots, F_r$  are a full set of non-isomorphic irreducible  $\bar{K}G$ -modules, and  $U_1, \dots, U_r$  are a full set of non-isomorphic principal indecomposable submodules of  $\bar{K}G$ . From § 54, we may write

$$(83.2) \quad \bar{K}G = \bar{K}G \cdot e_1 \oplus \cdots \oplus \bar{K}G \cdot e_m,$$

where the summands are the principal indecomposable submodules of  $\bar{K}G$ , the  $\{e_i\}$  being orthogonal idempotents such that  $\bar{I} = e_1 + \cdots + e_m$ .

We have seen in (54.11) and (54.13) that we may number the  $\{\epsilon_i\}$  so that

$$U_j = \bar{K}G \cdot \epsilon_j, \quad F_j = \frac{\bar{K}G \cdot \epsilon_j}{(\text{rad } \bar{K}G)\epsilon_j}, \quad 1 \leq j \leq r.$$

From our earlier results [Theorems (54.16) and (61.13)], we have at once.

(83.3) THEOREM. *Let  $\bar{K}$  be a splitting field for  $G$ . For each  $i$ ,  $1 \leq i \leq r$ , exactly  $u_i$  of the composition factors of the left regular module  $\bar{K}G$  are isomorphic to  $F_i$ , and exactly  $f_i$  of the summands in (83.2) are isomorphic to  $U_i$ . For any  $\bar{K}G$ -module  $M$ , the number of composition factors of  $M$  which are isomorphic to  $F_i$  is just  $(\epsilon_i M : \bar{K})$ .*

*Remark.* As we shall see in a moment [Corollary 83.7], the hypothesis that  $\bar{K}$  is a splitting field is automatically satisfied if  $K$  is a splitting field for  $G$ .

For  $1 \leq i \leq s$ , we let  $\bar{Z}_i = Z_i/PZ_i = \bar{K}G$ -module. We may write

$$(83.4) \quad \bar{Z}_i \approx \sum_{j=1}^r d_{ij} F_j, \quad 1 \leq i \leq s,$$

indicating thereby the composition factors of each  $\bar{Z}_i$ . We call the non-negative integers  $\{d_{ij}\}$  the *decomposition numbers* of  $KG$  with respect to  $P$ , and define the *decomposition matrix*  $D = (d_{ij})$ , an  $s \times r$  matrix.

For a matrix  $X$  over  $Z$ , we define the *p-rank* of  $X$  to be the rank of the matrix  $\bar{X}$  whose entries are in  $Z/pZ$ .

(83.5) THEOREM (Brauer [4]). *If both  $K$  and  $\bar{K}$  are splitting fields for  $G$ , then  $r$  (the number of non-isomorphic irreducible  $\bar{K}G$ -modules) coincides with the number of p-regular classes in  $G$ , and  $D$  has p-rank  $r$ .*

PROOF. Let  $n$  be the exponent of  $G$ . Replacing  $K$  by  $K(\sqrt[n]{-1})$  does not affect the matrix  $D$ , nor does it alter the hypotheses of the theorem. For the remainder of the proof, we may therefore assume that  $\sqrt[n]{-1} \in K$ .

Let  $\mathfrak{C}_1, \dots, \mathfrak{C}_t$  denote the  $p$ -regular classes of  $G$ . In (82.6) we showed that  $r \leq t$ , and we now prove  $t \leq r$ . In the proof of Lemma 40.7 we showed the existence of generalized characters  $\xi_1, \dots, \xi_t \in \text{char}_K(G)$  such that for each  $i$ ,  $1 \leq i \leq t$ , we have

$$(83.6) \quad \begin{cases} \xi_i(x) \in Z, x \in G \\ \xi_i(x) \equiv 1 \pmod{p}, x \in \mathbb{G}_i \\ \xi_i(x) = 0, x \in \mathbb{G}_j, j \neq i, 1 \leq j \leq t. \end{cases}$$

Now each  $\xi_i$  is an  $R$ -linear combination of  $\zeta^{(1)}, \dots, \zeta^{(s)}$ , and so each  $\bar{\xi}_i$  is a  $\bar{K}$ -linear combination of the  $\{\bar{\zeta}^{(i)}\}$  and hence also of the  $\{\bar{\varphi}^{(j)} : 1 \leq j \leq r\}$ . But by (83.6) we see that  $\{\bar{\xi}_1, \dots, \bar{\xi}_t\}$  are linearly independent over  $\bar{K}$ , and so necessarily  $t \leq r$ . This completes the proof that  $t = r$ .

Now suppose that  $\bar{D}$  has rank less than  $r$ . Then at most  $r - 1$  of the characters  $\{\bar{\zeta}^{(i)} : 1 \leq i \leq s\}$  are linearly independent over  $\bar{K}$ , and thus the same is true for  $\{\bar{\xi}_1, \dots, \bar{\xi}_t\}$ . This is impossible, and therefore  $D$  has  $p$ -rank  $r$ .

(83.7) COROLLARY. *If  $K$  is a splitting field for  $G$ , then so is  $\bar{K}$ .*

PROOF. From Chapter X, we know that there exists a finite extension field  $\bar{L}$  of  $\bar{K}$  which is a splitting field for  $G$ . We may find an algebraic number field  $L$  containing  $K$  whose residue class field (relative to some prime ideal containing  $P$ ) is precisely  $\bar{L}$ . Let  $\varphi^{(1)}, \dots, \varphi^{(r)}$  be the characters of the non-isomorphic irreducible  $\bar{L}G$ -modules. To prove that  $\bar{K}$  is a splitting field for  $G$  it suffices, in view of Theorem 70.23, to show that for each  $x \in G$  and each  $i$  ( $1 \leq i \leq r$ ), we have  $\bar{\varphi}^{(i)}(x) \in \bar{K}$ .

Now let the  $\{\zeta^{(j)}\}$  be defined as in (83.1). They are also a full set of irreducible  $LG$ -characters, and we may write (83.4) just as before, where now the underlying fields are  $L$  and  $\bar{L}$ . Since both of these fields are splitting fields for  $G$ , the preceding theorem shows that the decomposition matrix  $D$  has maximal  $p$ -rank, and thus we may solve the equations

$$\bar{\zeta}^{(i)} = \sum_{j=1}^r \bar{d}_{ij} \bar{\varphi}^{(j)}, \quad 1 \leq i \leq s,$$

for  $\{\bar{\varphi}^{(j)}\}$  in terms of the  $\{\bar{\zeta}^{(i)}\}$ , with coefficients from  $GF(p)$ . Since  $\bar{\zeta}^{(i)}(x) \in \bar{K}$  for all  $x \in G$ , this shows that also  $\bar{\varphi}^{(j)}(x) \in \bar{K}$  for all  $x \in G$ , and completes the proof.

(Let us discuss briefly the way in which  $D$  depends upon the prime  $p$ . On the one hand, if we replace the  $\{Z_i\}$  by other representations which are  $K$ -equivalent to them, we know from Theorem 82.1 that the composition factors of the  $\{\bar{Z}_i\}$  are unchanged, and thus also  $D$  is unchanged. On the other hand, we may ask what happens if instead of the prime ideal  $P$  we use another prime ideal

$P'$  of  $R$  such that  $P'$  contains  $p$ . If we make the simplifying assumption that  $K$  is a *normal* extension of  $Q$ , then from Theorem 20.4 it follows readily that there exists an automorphism  $\sigma$  of  $K$  which carries  $P$  onto  $P'$ . This automorphism induces an isomorphism of  $R/P$  onto  $R/P'$ . On the other hand, the modules  $\{Z_i^\sigma\}$  are a full set of irreducible  $R_P G$ -modules, and

$$Z_i^\sigma / P' Z_i^\sigma \cong Z_i / P Z_i,$$

so that relative to these modules  $\{Z_i^\sigma\}$ , we obtain the same set of decomposition numbers as before. Thus  $D$  is unchanged if we number the modules used for  $P'$  in the manner described above.)

Our next basic notion is that of the Cartan invariants of the algebra  $\bar{K}G$ ; these enumerate the composition factors of the principal indecomposable submodules of  $\bar{K}G$ . Set

$$(83.8) \quad U_i \approx \sum_{j=1}^r c_{ij} F_j, \quad 1 \leq i \leq r,$$

and call the non-negative integers  $\{c_{ij}\}$  the *Cartan invariants* of  $\bar{K}G$ . The *Cartan matrix* is  $C = (c_{ij})$ , an  $r \times r$  matrix over  $Z$ .

In order to obtain a relation between the Cartan matrix  $C$  and the decomposition matrix  $D$ , it will be necessary to work for a while with the  $P$ -adic completion  $K^*$  of  $K$ . Let  $R^*$  be the ring of  $P$ -adic integers in  $K^*$ , and  $P^*$  the unique maximal ideal in  $R^*$ . For  $1 \leq i \leq s$ , define  $Z_i^* = R^* Z_i$ , so that  $Z_1^*, \dots, Z_s^*$  are a full set of non-isomorphic irreducible  $R^* G$ -modules, and each  $K^* Z_i^*$  is an absolutely irreducible  $K^* G$ -module. We have further

$$Z_i^* / P^* Z_i^* \cong Z_i / P Z_i = \bar{Z}_i.$$

Thus, if we work with the ground field  $K^*$  rather than  $K$ , the matrices  $C$  and  $D$  are exactly as before.

The main result of this section is as follows:

(83.9) **THEOREM** (Brauer [5], Brauer and Nesbitt [3], Nakayama [1]). *The Cartan matrix  $C$  and the decomposition matrix  $D$  are related by the equation*

$$C = {}^t D \cdot D.$$

**PROOF.** We have shown<sup>†</sup> that there exist orthogonal idempotents  $e_1, \dots, e_m \in R^* G$  such that

$$1 = e_1 + \cdots + e_m, \quad \bar{e}_1 = e_1, \dots, \bar{e}_m = e_m,$$

---

<sup>†</sup> See Theorem 77.11. This part of §77 can be read independently of the rest of §77. As a matter of fact, since we are assuming here that  $K$  is a splitting field for  $G$ , it follows from (76.28) that the idempotents  $e_1, \dots, e_m$  may be chosen from  $R_P G$ , and so we could avoid passing to the  $P$ -adic completion.

where the bars indicate the passage from  $R^*G$  to  $\bar{K}G$ . Then we have

$$K^*G = K^*G \cdot e_1 \oplus \cdots \oplus K^*G \cdot e_m.$$

By Theorem 54.15, the multiplicity  $a_{ij}$  of  $K^*Z_i^*$  as composition factor of  $K^*G \cdot e_j$  is equal to the dimension  $(e_j K^*Z_i^* : K^*)$ . Therefore  $a_{ij}$  also equals the number of elements in an  $R^*$ -basis for  $e_j Z_i^*$ . But  $e_j Z_i^* = \epsilon_j \bar{Z}_i$ , and thus

$$a_{ij} = (\epsilon_j \bar{Z}_i : \bar{K}).$$

By Theorem 83.3, the above dimension  $(\epsilon_j \bar{Z}_i : \bar{K})$  is the same as the multiplicity  $d_{ij}$  of  $F_j$  as composition factor of  $\bar{Z}_i$ . This shows that  $a_{ij} = d_{ij}$ , and consequently

$$K^*G \cdot e_j \approx \sum_{i=1}^s d_{ij} (K^*Z_i^*), \quad 1 \leq j \leq m.$$

Passing to the associated  $\bar{K}G$ -modules, we have [by Theorem 82.1]

$$U_j \approx \sum_{i=1}^s d_{ij} \bar{Z}_i = \sum_{i=1}^s \sum_{k=1}^r d_{ij} d_{ik} F_k, \quad 1 \leq j \leq m.$$

Therefore

$$c_{jk} = \sum_{i=1}^s d_{ij} d_{ik},$$

which proves the theorem.

(83.10) COROLLARY.  $C$  is a symmetric matrix.

*Example.* Let  $G$  be a  $p$ -group, and let  $Z_1, \dots, Z_s$  be the irreducible  $K$ -representations of  $G$ . By Exercise 54.1, there is only one irreducible  $\bar{K}$ -representation  $F_1$ , and only one principal indecomposable representation  $U_1$ . Then

$$d_{ii} = z_i, \quad 1 \leq i \leq s,$$

and we have

$${}^t DD = \sum_{i=1}^s z_i^2 = [G : 1] = c_{11},$$

which is exactly the statement of Theorem 83.9 in this special case.

### § 83A. Appendix A

Let us see what happens when we drop the assumption that  $K$  and  $\bar{K}$  are splitting fields for  $G$ . We define the  $\{F_j\}$  and  $\{U_j\}$  just

as before, keeping the notation (83.2), and again define the  $\{c_{ij}\}$  by (83.8). The decomposition numbers  $\{d_{ij}\}$  will be defined in a different manner, however. Let  $K^*$  be the  $P$ -adic completion of  $K$ , and let  $Z_1^*, \dots, Z_t^*$  be a full set of non-isomorphic irreducible  $R^*G$ -modules. (We no longer have a relation  $Z_i^* = R^*Z_i$  since in going from  $K$  to  $K^*$  an irreducible  $KG$ -module may become reducible.) Now define the decomposition numbers  $\{d_{ij}\}$  by

$$\overline{Z_i^*} = Z_i^*/P^*Z_i^* \approx \sum_{j=1}^r d_{ij}F_j, \quad 1 \leq i \leq t.$$

Then the decomposition matrix  $D = (d_{ij})$  is a  $t \times r$  matrix.

Paralleling the proof of Theorem 83.9, define the orthogonal idempotents  $\{e_j\}$  just as before. The multiplicity  $a_{ij}$  of  $K^*Z_i^*$  as composition factor of  $K^*G \cdot e_j$  is now given by [see Theorems (54.15) and (54.19)]

$$a_{ij} = (e_j K^* Z_i^* : K^*) / r_i,$$

where

$$r_i = (\mathcal{A}^{(i)} : K^*), \quad \mathcal{A}^{(i)} = \text{Hom}_{K^*G}(K^*Z_i^*, K^*Z_i^*).$$

(Thus,  $\mathcal{A}^{(i)}$  is the division algebra over  $K^*$  associated with the irreducible module  $K^*Z_i^*$ .)

As before, we have

$$(e_j K^* Z_i^* : K^*) = (\varepsilon_j \bar{Z}_i^* : \bar{K}).$$

By the results of §54 and 61, the multiplicity  $d_{ij}$  of  $F_j$  as composition factor of  $\bar{Z}_i^*$  is

$$d_{ij} = (\varepsilon_j \bar{Z}_i^* : \bar{K}) / s_j$$

where

$$s_j = (\Omega^{(j)} : \bar{K}), \quad \Omega^{(j)} = \text{Hom}_{\bar{K}G}(F_j, F_j), 1 \leq j \leq r.$$

Thus

$$a_{ij} = \frac{s_j d_{ij}}{r_i}, \quad 1 \leq i \leq t, 1 \leq j \leq r,$$

and we have

$$K^*G \cdot e_j \approx \sum_{i=1}^t \frac{s_j d_{ij}}{r_i} K^* Z_i^*, \quad 1 \leq j \leq r.$$

Passing to the associated  $\bar{K}G$ -modules, we obtain

$$U_j \approx \sum_{i=1}^t \frac{s_j d_{ij}}{r_i} \sum_{k=1}^r d_{ik} F_k.$$

This yields

$$c_{jk} = \sum_{i=1}^t \frac{s_j d_{ij} d_{ik}}{r_i}, \quad 1 \leq j, k \leq r.$$

### § 83B. Appendix B

Since Theorem 83.5 is of such basic importance, it is of interest to give an alternate proof due to Brauer [27, I] which does not depend on induced characters. Let  $E$  be the algebraic closure of  $\bar{K}$ , so that by Theorem 29.21, the modules  $F_1^E, \dots, F_r^E$  are a full set of non-isomorphic irreducible  $EG$ -modules. (We are assuming here that  $\bar{K}$  is a splitting field for  $G$ .)

Define  $S$  to be the  $E$ -subspace of  $EG$  generated by  $\{xy - yx : x, y \in EG\}$ . It is easily verified that  $S$  consists precisely of those sums  $\sum_{x \in G} \alpha_x x$ ,  $\alpha_x \in E$ , such that, for each conjugate class  $\mathfrak{C}$  of  $G$ ,  $\sum_{x \in \mathfrak{C}} \alpha_x = 0$ . The subspace  $S$  will not (in general) be an ideal in  $EG$ . For  $x, y \in EG$ , we have

$$(x + y)^p = x^p + x^{p-1}y + x^{p-2}yx + \cdots + xyx^{p-2} + yx^{p-1} + \cdots + y^p.$$

However

$$x^{p-1}y \equiv x^{p-2}yx \equiv \cdots \equiv yx^{p-1} \pmod{S},$$

and so

$$\sum_{a=1}^p x^{p-a}yx^{a-1} \equiv 0 \pmod{S}.$$

Continuing in this way, we obtain

$$(83.11) \quad (x + y)^p \equiv x^p + y^p \pmod{S}, \quad x, y \in EG.$$

In particular, for  $x, y \in EG$ ,

$$(83.12) \quad (xy - yx)^p \equiv x\{y(xy)^{p-1}\} - \{y(xy)^{p-1}\}x \equiv 0 \pmod{S},$$

so that  $S$  is closed under the operation of raising to the  $p$ th power.

Next we define

$$T = \{x \in EG : x^{p^m} \in S \text{ for some } m > 0\}.$$

By (83.11) and (83.12), we see that  $T$  is an  $E$ -subspace of  $EG$  which contains  $S$ .

Now let  $x_1, \dots, x_t \in G$  be representatives chosen from the  $t$   $p$ -regular classes of  $G$ . We shall show that  $(EG/T : E) = t$  by proving that the images of  $x_1, \dots, x_t$  in  $EG/T$  form an  $E$ -basis for  $EG/T$ . To begin with, any  $x \in G$  is expressible as  $x = x'x'', x'$   $p$ -regular,  $x''$   $p$ -singular,  $x'x'' = x''x'$ . Setting the order of  $x''$  equal to  $q$ , a

power of  $p$ , we have

$$(x - x')^q \equiv x'^q - x'^q \equiv 0 \pmod{S},$$

and so  $x \equiv x' \pmod{T}$ . Furthermore, conjugate elements of  $G$  are congruent mod  $T$ . Thus every element of  $EG$  is congruent mod  $T$  to a sum  $\sum_{i=1}^t \alpha_i x_i$ ,  $\alpha_i \in E$ , which shows that  $(EG/T : E) \leq t$ . To prove equality, we must show that  $\sum \alpha_i x_i \in T$  implies that each  $\alpha_i = 0$ . Now if  $\sum \alpha_i x_i \in T$ , then  $\{\sum \alpha_i x_i\}^{p^m} \in S$  for all sufficiently large  $m$ . Since each  $x_i$  is  $p$ -regular, we may in fact choose  $m$  so that also

$$x_i^{p^m} = x_i, \quad 1 \leq i \leq t.$$

Then

$$\sum_i \alpha_i^{p^m} x_i \in S,$$

and since the  $\{x_i\}$  lie in different conjugate classes of  $G$ , it follows from the description of  $S$  given above that each  $\alpha_i^{p^m}$  equals 0. Thus each  $\alpha_i = 0$ , and so we have established that  $t = (EG/T : E)$ .

Let  $N = \text{rad}(EG)$ , and consider  $EG/N$ . The number of simple components of  $EG/N$  coincides with the number of non-isomorphic irreducible  $EG$ -modules. Thus we need show only that  $EG/N$  has precisely  $(EG/T : E)$  simple components. We write

$$EG/N = A_1 \oplus \cdots \oplus A_r,$$

where the  $\{A_i\}$  are the simple components of  $EG/N$ , and where each  $A_i$  is a full matrix algebra  $E_{f_i}$  over  $E$ . Define  $\tilde{S}$  and  $\tilde{T}$  for the algebra  $EG/N$  in the same way as  $S$  and  $T$  are defined for  $EG$ , and likewise define  $S_i$  and  $T_i$  for  $A_i$ . It is easily seen that

$$\tilde{S} = S_1 \oplus \cdots \oplus S_r, \quad \tilde{T} = T_1 \oplus \cdots \oplus T_r.$$

On the other hand, the nilpotency of  $N$  implies that  $N \subset T$ , from which one verifies that  $T/N = \tilde{T}$ . Thus

$$EG/T \cong (EG/N)/(T/N) \cong A_1/T_1 \oplus \cdots \oplus A_r/T_r,$$

and so

$$(EG/T : E) = \sum_{i=1}^r (A_i/T_i : E).$$

To complete the proof, we need only check that each  $(A_i/T_i : E)$  equals 1.

Now we have  $A_i \cong E_f$  (a full matrix algebra) and it is not hard to check that  $S_i$  consists precisely of those matrices in  $E_f$  with zero

trace. Thus  $(S_i; E) = f^2 - 1$ . From

$$A_i \supset T_i \supset S_i,$$

we have thus either  $T_i = S_i$  or  $T_i = A_i$ . But  $e_{ii} \in A_i$  and  $e_{ii} \notin T_i$ , so  $T_i = S_i$ . Hence  $(A_i/T_i; E) = 1$ , and the proof is complete.

### Exercises

1. If  $U_i \neq F_i$ , prove that  $c_{ii} > 1$ . [Hint: Let  $U_i = \bar{K}Ge_i$ . Then  $U_i$  has a unique maximal submodule  $M_i$  such that  $U_i/M_i \cong F_i$ . Since  $\bar{K}G$  is a quasi-Frobenius ring, it follows from the results of Chapters VIII and IX that  $U_i$  has a unique minimal submodule  $S_i$ . Using the fact that  $\bar{K}G$  is a symmetric algebra (see § 66), show that  $e_i S_i \neq 0$ , and hence  $S_i \cong F_i$ . Therefore  $c_{ii} \geq 2$ .]

2. Show that  $\varphi^{(1)}, \dots, \varphi^{(r)}$  are linearly independent over  $K$ . Prove the same for  $\eta^{(1)}, \dots, \eta^{(r)}$ .

### § 84. Orthogonality Relations

We shall keep the notation of the preceding two sections and assume hereafter that  $K$  and  $\bar{K}$  are splitting fields for  $G$  and for all subgroups and factor groups of  $G$ . By Theorem 83.5, we may number the conjugate classes  $\mathfrak{C}_1, \dots, \mathfrak{C}_s$  of  $G$  so that  $\mathfrak{C}_1, \dots, \mathfrak{C}_r$  are the  $p$ -regular classes of  $G$  and so that  $\mathfrak{C}_1 = \{1\}$ . Then  $s$  is the number of  $\zeta$ 's,  $r$  the number of  $\varphi$ 's, in the chart (83.1). From (83.4) and (83.8) we have

$$(84.1) \quad \zeta^{(i)} = \sum_{j=1}^r d_{ij} \varphi^{(j)}, \quad 1 \leq i \leq s,$$

$$(84.2) \quad \eta^{(i)} = \sum_{j=1}^r c_{ij} \varphi^{(j)}, \quad 1 \leq i \leq r,$$

but we must remember that the Brauer characters  $\{\varphi^{(j)}\}$  and  $\{\eta^{(j)}\}$  are defined on the  $p$ -regular elements of  $G$  only. By using Theorem 83.9, we may rewrite (84.2) as

$$(84.3) \quad \eta^{(i)} = \sum_{k=1}^s d_{ki} \zeta^{(k)}, \quad 1 \leq i \leq r.$$

Evaluating all characters involved in (84.1) through (84.3) at the unity element of  $G$ , we obtain

$$(84.4) \quad z_i = \sum_{j=1}^r d_{ij} f_j, \quad u_i = \sum_{j=1}^r c_{ij} f_j = \sum_{k=1}^s d_{ki} z_k.$$

From (83.3), we also have

$$(84.5) \quad \sum_{i=1}^r f_i u_i = g .$$

We now introduce additional notation for the remainder of the chapter.

$$[G:1] = g = p^e g_0, \quad p \nmid g_0 .$$

$$(84.6) \quad \left\{ \begin{array}{l} g_i = \text{number of elements in the class } \mathfrak{C}_i . \\ x_i = \text{element of } \mathfrak{C}_i . \\ \mathfrak{C}_{i^*} = \text{class of inverses of } \mathfrak{C}_i \text{ [see (31.10)]} . \\ \varphi_j^{(t)} = \varphi^{(i)}(x_j), \eta_j^{(t)} = \eta^{(i)}(x_j), \zeta_j^{(t)} = \zeta^{(i)}(x_j), \\ \emptyset = (\varphi_j^{(t)})^{r \times r}, H = (\eta_j^{(t)})^{r \times r}, Z = (\zeta_j^{(i)})^{s \times r} . \end{array} \right.$$

Equations (84.1) through (84.3) become

$$(84.7) \quad Z = D\emptyset, \quad H = C\emptyset = {}^t D \cdot Z .$$

Let us show at once that  $\emptyset$  is non-singular, and in fact that the matrix  $\bar{\emptyset}$  (over  $\bar{K}$ ) is also non-singular. On the one hand, we know [Theorem 30.12] that  $\{\bar{\varphi}^{(1)}, \dots, \bar{\varphi}^{(r)}\}$  are linearly independent over  $\bar{K}$ , since  $\bar{K}$  is a splitting field for  $G$ . On the other hand, each  $\bar{\varphi}^{(i)}$  is completely determined by the  $r$ -tuple  $(\bar{\varphi}_1^{(t)}, \dots, \bar{\varphi}_r^{(t)})$ , by Corollary 82.5. Together these imply that  $\bar{\emptyset}$  is non-singular, and hence  $\emptyset$  is unimodular over  $R_P$ . We shall use these facts repeatedly.

The relation  $\bar{Z} = \bar{D}\bar{\emptyset}$  shows [by use of Theorem 83.5] that  $\bar{Z}$ ,  $\bar{D}$  and  $\bar{\emptyset}$  all have rank  $r$  over  $\bar{K}$ .

The orthogonality relations (31.13) may be written in our present notation as follows:

$$\sum_{k=1}^s \zeta_i^{(k)} \zeta_j^{(k)} = \frac{g}{g_i} \delta_{ij^*} .$$

In particular, if we let  $i$  and  $j$  range between 1 and  $r$ , this yields

$${}^t Z \cdot Z = \left( \frac{g}{g_i} \delta_{ij^*} \right)^{r \times r} .$$

Let us denote by el. div.  $X$  the set of elementary divisors of the matrix  $X$  with rational integral entries and by  $p$ -el. div., the powers of  $p$  occurring in the elementary divisors. Then

$$(84.8) \quad \text{el. div.}({}^t ZZ) = \left\{ \frac{g}{g_1}, \dots, \frac{g}{g_r} \right\} .$$

But, on the other hand,

$$(84.9) \quad {}^t ZZ = {}^t \emptyset D D \emptyset = {}^t \emptyset C \emptyset .$$

Since  $\emptyset$  is unimodular over  $R_P$ , this yields

$$p\text{-el. div.}({}^t ZZ) = p\text{-el. div. }C .$$

so by (84.8) we have

$$(84.10) \quad p\text{-el. div. }C = \text{powers of } p \text{ in } \left\{ \frac{g}{g_1}, \dots, \frac{g}{g_r} \right\} .$$

We shall show later [Theorem 84.17] that in fact  $|C|$  is a power of  $p$ , so all elementary divisors of  $C$  are powers of  $p$ .

Let us set

$$Y = \left( \frac{g}{g_i} \delta_{ij^*} \right), \quad Y^{-1} = \left( \frac{g_i}{g} \delta_{ij^*} \right) .$$

We find readily that

$$\emptyset Y^{-1} {}^t H = I, \quad \emptyset Y^{-1} {}^t \emptyset = C^{-1}, \quad HY^{-1} {}^t H = C ,$$

which yields

$$(84.11) \quad \sum_{j=1}^r g_j \varphi_j^{(i)} \eta_j^{(k)} = g \delta_{ik} ,$$

$$(84.12) \quad \sum_{j=1}^r g_j \varphi_j^{(i)} \varphi_j^{(k)} = g \gamma_{ik} , \quad \text{where } C^{-1} = (\gamma_{ik}) ,$$

$$(84.13) \quad \sum_{j=1}^r g_j \eta_j^{(i)} \eta_j^{(k)} = g c_{ik} .$$

*Remarks.* (1) In the special case where  $p \nmid g$ , we have  $U_i = F_i$ ,  $1 \leq i \leq r$ , and also  $C = I$ , and  $r = s$ . From  ${}^t DD = C$  it follows that  $D$  is just a permutation matrix. Therefore, after renumbering the  $\{F_i\}$ , we may take  $\bar{Z}_i = F_i$ ,  $1 \leq i \leq r$ . Thus the irreducible  $R_P$ -representations of  $G$  give rise to irreducible  $\bar{K}$ -representations of  $G$ . Consequently every  $\bar{K}$ -representation of  $G$  is associated with some  $K$ -representation of  $G$  in this case.

(2) The orthogonality relations (84.11) through (84.13) all have been generalized to the case of a Frobenius algebra (see Brauer [14], Osima [2], Nesbitt and Thrall [1].)

Returning now to the general case, we remark that  $|\emptyset|^2 \in Q$  as a consequence of (84.9). Since all entries of  $\emptyset$  are algebraic integers, we conclude that  $|\emptyset|^2 \in Z$ . Furthermore we know that  $\emptyset$  is unimo-

dular over  $R_P$ , and thus  $p \nmid |\emptyset|^2$ . Let  $pR = P_1^{m_1} \cdots P_u^{m_u}$  be the factorization of  $pR$  into powers of distinct prime ideals in  $R$ , with  $P_1 = P$ , say. Then  $\emptyset$  is unimodular over  $R_{P_i}$  for each  $i, 1 \leq i \leq u$ . We shall use this fact to prove a generalization of a theorem of Dickson's. For  $\alpha \in R$ , let  $\nu_i(\alpha)$  denote the exponent of the power of  $P_i$  occurring in the factorization of  $\alpha R$ . We now prove

(84.14) THEOREM. *For each  $i, 1 \leq i \leq u$ , we have*

$$\nu_i(\eta_k^{(j)}) \geq \nu_i\left(\frac{g}{g_k}\right), \quad 1 \leq j, k \leq r,$$

PROOF. We observe, first, that  $H = {}^t\emptyset^{-1} {}^tY$ . Equating  $k$ th columns on both sides, we obtain

$$\begin{pmatrix} \eta_k^{(1)} \\ \vdots \\ \eta_k^{(r)} \end{pmatrix} = {}^t\emptyset^{-1} \cdot \frac{g}{g_k} \begin{pmatrix} 0 \\ \vdots \\ 1 \\ \vdots \\ 0 \end{pmatrix}$$

where the 1 occurs at position  $k^*$ . Since  $\emptyset$  is unimodular over each  $R_{P_i}, 1 \leq i \leq u$ , this implies that

$$\nu_i(g/g_k) = \min_{1 \leq j \leq r} \nu_i(\eta_k^{(j)}),$$

and the theorem is proved.

Taking  $k = 1$  in the above, we obtain  $\nu_i(g) = \min_{1 \leq j \leq r} \nu_i(u_j)$ . But  $g$  and the  $\{u_j\}$  are rational integers, so we have [see also Corollary 65.17]

(84.15) COROLLARY (Dickson).  $\nu(g) = \min_{1 \leq j \leq r} \nu(u_j)$ .

We shall now use the theory of induced characters developed in § 40 to prove that  $|C|$  is a power of  $p$ .

(84.16) LEMMA. *Let  $\varphi$  be the Brauer character of some modular representation of  $G$ , and define*

$$\theta(x) = \begin{cases} p^e \varphi(x), & x \text{ } p\text{-regular, } e = \nu(g) \\ 0, & \text{otherwise.} \end{cases}$$

*Then  $\theta$  is a generalized character of  $G$ .*

PROOF. Clearly  $\theta$  is a class function on  $G$ . To show that  $\theta \in \text{char}(G)$ , it suffices [in view of Theorem 40.8] to show that for every elementary subgroup  $E$  of  $G$ ,  $\theta|E \in \text{char}(E)$ . The subgroup

$E$  may be  $p$ -elementary or  $q$ -elementary for some prime  $q \neq p$ . In either case we may write  $E = A \times B$  where  $B$  is a  $p$ -group and  $p \nmid [A:1]$ . By remark (1) following (84.13), we see that  $\varphi|_A$  is an ordinary  $K$ -character of  $A$ . Let  $\rho$  be the character of the left regular representation of  $KB$ , so that  $\rho(1) = [B:1] = p^n$ , whereas  $\rho(b) = 0$  for  $b \in B, b \neq 1$ . Define  $\psi$  on  $E$  by

$$\psi(ab) = \varphi(a)\rho(b), \quad a \in A, b \in B.$$

We have seen [§38 and (43.1)] that  $\psi \in \text{char}(E)$ . For  $p$ -regular  $x \in E$ , we have  $x = a \in A$ , and so

$$\psi(x) = \varphi(a)\rho(1) = p^n\varphi(a) = p^{n-e}\theta(x),$$

which gives

$$\theta(x) = p^{e-n}\psi(x).$$

But this also holds for  $p$ -irregular  $x \in E$ , since then  $x = ab, a \in A, b \in B, b \neq 1$ , and then both  $\theta(x)$  and  $\psi(x)$  vanish. This proves that  $\theta|_E = p^{e-n}\psi \in \text{char}(E)$ , and the lemma is established.

(84.17) THEOREM. (Brauer [8], [24]).  $|\mathbf{C}| = \text{power of } p$ .

PROOF. For each  $\varphi^{(i)}, 1 \leq i \leq r$ , define  $\theta_i$  as in the preceding lemma. Since each  $\theta_i \in \text{char}(G)$ , we have

$$\theta_i = \sum_{j=1}^s a_{ij} \zeta^{(j)}, \quad a_{ij} \in Z, 1 \leq i \leq r.$$

Evaluating both sides on all  $p$ -regular classes of  $G$  and expressing the result in matrix form, we obtain  $p^e \emptyset = AZ$ , where  $A = (a_{ij})$ . But also  $p^e \emptyset = p^e C^{-1} {}^t DZ$ , and since  $Z$  has  $p$ -rank  $r$ , we obtain

$$A = p^e C^{-1} {}^t D.$$

From this it follows that

$$A \cdot {}^t A = p^{2e} C^{-1} {}^t D D C^{-1} = p^{2e} C^{-1},$$

and thus

$$|\mathbf{C}| |A \cdot {}^t A| = |p^{2e} I| = \text{power of } p.$$

But  $|A \cdot {}^t A| \in Z$ , and thus also  $|\mathbf{C}|$  is a power of  $p$ . This completes the proof.

(84.18) COROLLARY. *The first  $r$  determinantal divisors of  $D$  are all equal to 1, where the  $k$ th determinantal divisor  $d_k$  is the G.C.D. of the  $k \times k$  minors of  $D$  (see §16).*

PROOF. Since  $d_i | d_{i+1}, i = 1, \dots, r-1$ , we need show only that  $d_r = 1$ . Now  $p \nmid d_r$  because  $D$  has  $p$ -rank  $r$ . On the other hand,

let  $q$  by any prime not equal to  $p$ , and suppose  $q \mid d_r$ . Then  $\mathbf{D}$  has  $q$ -rank less than  $r$ , and hence also  $\mathbf{C} = {}^t\mathbf{D}\mathbf{D}$  has  $q$ -rank less than  $r$ . This is impossible since  $|\mathbf{C}|$  is relatively prime to  $q$ , and so the result is proved.

### Exercises

1. Let  $\bar{\mathbf{X}}$  be obtained from the complex matrix  $\mathbf{X}$  by replacing each entry of  $\mathbf{X}$  by its complex conjugate. Prove that

$${}^t\bar{\mathbf{Z}}\mathbf{C}\bar{\mathbf{Z}} = {}^t\bar{\mathbf{Z}}\mathbf{Z} = \left( \frac{g}{g_i} \delta_{ij} \right).$$

2. (Nakayama [1], Brauer and Nesbitt [3].) Let  $\hat{G}$  be a subgroup of  $G$ , and let  $\hat{\varphi}, \hat{\eta}$ , etc., have the same significance for  $\hat{G}$  as  $\varphi, \eta$ , etc., have for  $G$ . Let  $\hat{\eta}^G$  denote an induced character, as in Chapter VI. Show that there exist non-negative integers  $\{\alpha_{ij}\}$  and  $\{\beta_{ij}\}$  such that on all  $p$ -regular elements of  $G$ , we have

$$\begin{aligned} \hat{\eta}^{(i)G} &= \sum_j \alpha_{ij} \hat{\eta}^{(j)}, & \varphi^{(j)}|_{\hat{G}} &= \sum_i \alpha_{ij} \hat{\varphi}^{(i)}, \\ \hat{\varphi}^{(i)G} &= \sum_j \beta_{ij} \varphi^{(j)}, & \eta^{(j)}|_{\hat{G}} &= \sum_i \beta_{ij} \hat{\eta}^{(i)}. \end{aligned}$$

It can also be shown that if  $\hat{U}$  is a  $\bar{K}$ -representation of  $\hat{G}$  which affords the Brauer character  $\hat{\eta}$ , then  $\hat{\eta}^G$  is the Brauer character afforded by  $\hat{U}^G$  (see Brauer and Nesbitt [3], § 25).

3. (Brauer and Nesbitt [3].) Keep the notation of the preceding problem and let  $\varphi^{(1)}, \hat{\varphi}^{(1)}$  be 1-characters. In the above formulas,  $\alpha_{11} = 1, \alpha_{i1} = 0$  for  $i \neq 1$ . Hence  $\eta^{(1)}$  occurs in the character  $\hat{\eta}^{(1)G}$ , and this latter character has degree  $\hat{u}_1[G: \hat{G}]$ . Therefore  $u_1 \leq \hat{u}_1[G: \hat{G}]$ . Deduce from this that  $u_1 \leq [G: \hat{G}]$  whenever  $p \nmid [\hat{G}: 1]$ .

4. (Brauer [24].) Using the notation of Theorem 83.9 for the moment, let  $\tau_j$  be the character of the  $K^*G$ -module  $K^*G \cdot e_j$ . Since  $K^*Z_i^*$  occurs as composition factor of  $K^*G \cdot e_j$  with multiplicity  $d_{ij}$ , we have  $\tau_j = \sum_i d_{ij} \zeta^{(i)}$ . Use this to show that  $\tau_j$  vanishes on all  $p$ -irregular elements of  $G$ . [Hint: From the orthogonality relations, we get

$$g^{-1} \sum_{y \in G} |\tau_j(y)|^2 = \sum_i d_{ij}^2 = c_{jj}.$$

On the other hand,

$$g^{-1} \sum_{\substack{x \in G \\ x \text{ } p\text{-regular}}} |\tau_j(x)|^2 = g^{-1} \sum_{\substack{x \in G \\ x \text{ } p\text{-regular}}} |\eta^{(j)}(x)|^2 = c_{jj},$$

by (84.13). This implies that  $\tau_j(y) = 0$  for  $y$   $p$ -irregular.]

5. (Brauer [24].) Let  $\theta$  be a complex-valued class function on  $G$  which vanishes on the  $p$ -irregular elements of  $G$ . Show that there exist complex numbers  $\alpha_1, \dots, \alpha_n$  such that

$$(84.19) \quad \theta = \alpha_1\tau_1 + \cdots + \alpha_r\tau_r,$$

where the  $\{\tau_i\}$  are defined above. Furthermore,  $\theta \in \text{char}(G)$  implies that each  $\alpha_i \in \mathbb{Z}$ . [Hint: For  $p$ -regular  $x$  in  $G$  we have  $\tau_i(x) = \eta^{(i)}(x)$ . If  $x_1, \dots, x_r$  are chosen from the  $r$   $p$ -regular classes of  $G$ , we may solve the equations

$$\theta(x_i) = \alpha_1\eta_i^{(1)} + \cdots + \alpha_r\eta_i^{(r)}, \quad 1 \leq i \leq r,$$

for the complex numbers  $\alpha_1, \dots, \alpha_r$ . For these  $\{\alpha_i\}$ , it is clear that (84.19) holds. By (84.11), we get  $\alpha_j = g^{-1} \sum_{i=1}^r g_i \theta(x_i) \varphi^{(j)}(x_i^{-1})$ . But  $\varphi^{(j)}$  is a  $\mathbb{Z}$ -linear combination of the  $\{\zeta^{(k)}\}$  by (84.18), so that  $\alpha_j$  is a sum (with coefficients from  $\mathbb{Z}$ ) of combinations of the form

$$g^{-1} \sum_{i=1}^r g_i \theta(x_i) \zeta^{(k)}(x_i^{-1}) = g^{-1} \sum_{y \in G} \theta(y) \zeta^{(k)}(y^{-1}),$$

and each such expression lies in  $\mathbb{Z}$  because  $\theta \in \text{char}(G)$ .]

## § 85. Blocks

Let us continue to use the notation of the preceding sections. The algebra  $\bar{K}G$  satisfies both chain conditions, and so by Theorem 55.2 it can be expressed as

$$(85.1) \quad \bar{K}G = B_1 \oplus \cdots \oplus B_t$$

where the  $\{B_i\}$  are indecomposable two-sided ideals of  $\bar{K}G$ . These ideals  $\{B_i\}$  are uniquely determined, and we refer to them as the *blocks* of  $\bar{K}G$ . Correspondingly we have

$$(85.2) \quad \bar{I} = \delta_1 + \cdots + \delta_t, \quad \delta_i \in \mathcal{I}_i, \quad B_i = \bar{K}G \cdot \delta_i,$$

where the  $\{\delta_i\}$  are a set of orthogonal central idempotents of  $\bar{K}G$ , called the *block idempotents* of  $\bar{K}G$ . From Theorem 55.2 (or Exercise 55.1), we know that every two-sided ideal of  $\bar{K}G$  which is a direct summand of  $\bar{K}G$  is a sum of blocks, and that every central idempotent of  $\bar{K}G$  is a sum of block idempotents.

In the special case where  $p \nmid g$ , the blocks of  $\bar{K}G$  are just the simple components of  $\bar{K}G$ , and there is a one-to-one correspondence between irreducible  $\bar{K}G$ -modules and the simple components of  $\bar{K}G$ . We shall obtain, for the general case, a classification of the  $\{Z_i\}$ ,  $\{F_i\}$ , and  $\{U_i\}$  according to the blocks of  $\bar{K}G$ . This theory, due mainly to Brauer, will occupy our attention for the remainder of the chapter.

As a general reference for the results of this chapter, we may list Brauer [27] and Osima [6]. In a recent paper Rosenberg [1] has given an independent treatment of part of the theory of blocks.

His approach, which avoids the hypothesis that  $K$  and  $\bar{K}$  are splitting fields for  $G$ , contains different proofs of many of the results of the next few sections. We may also remark that Osima has introduced the more general concept of blocks of  $\bar{K}G$  relative to a subgroup  $H$  of  $G$ . For a discussion of this generalization, see Osima [1], [8], and Iizuka [2], [3].

As we saw in §83, we may write

$$\bar{K}G = \bar{K}G \cdot \varepsilon_1 \oplus \cdots \oplus \bar{K}G \cdot \varepsilon_m,$$

a direct sum of principal indecomposable modules of  $\bar{K}G$ , numbered so that  $U_1 = \bar{K}G \cdot \varepsilon_1, \dots, U_r = \bar{K}G \cdot \varepsilon_r$  are a full set of non-isomorphic modules among these summands. We showed in §55 that each  $U_i$  is contained in some block  $B_j$ ; we shall say that  $U_i$  belongs to the block  $B_j$  in this case. From §55, we have furthermore

$$(85.3) \quad B_j = \sum_{\substack{1 \leq i \leq m \\ \bar{K}G \cdot \varepsilon_i \subset B_j}} \bar{K}G \cdot \varepsilon_i, \quad \delta_j = \sum_{\substack{1 \leq i \leq m \\ \bar{K}G \cdot \varepsilon_i \subset B_j}} \varepsilon_i.$$

Since  $B_i B_j = 0$  for  $i \neq j$ , we note that  $\bar{K}G \cdot \varepsilon_i \subset B_j$  if and only if  $\delta_j \cdot \bar{K}G \cdot \varepsilon_i \neq 0$ .

On the other hand, we have set

$$F_i = \bar{K}G \cdot \varepsilon_i / (\text{rad } \bar{K}G) \cdot \varepsilon_i, \quad 1 \leq i \leq r.$$

Then  $F_1, \dots, F_r$  are a full set of non-isomorphic irreducible  $\bar{K}G$ -modules. From §55, we know that different blocks have no common composition factor. Furthermore, for  $1 \leq i \leq r$ , we know that  $F_i$  is a composition factor of  $U_i$ , and so it is also a composition factor of the block  $B_j$  containing  $U_i$ . We shall assign  $F_i$  to the block  $B_j$  whenever  $F_i$  is a composition factor of  $B_j$ , or equivalently, whenever  $U_i \subset B_j$ . We say that  $F_i$  belongs to the block  $B_j$  in this case, and we use the notation  $F_i \in B_j$ . Since left multiplication by  $\delta_j$  is the identity operator on  $B_j$ , and is the zero operator on  $B_k$  for  $k \neq j$ , we have at once

(85.4) LEMMA.  $F_i \in B_j$  if and only if  $F_i(\delta_j) = I$ .

In order to assign the irreducible  $KG$ -modules  $\{KZ_i\}$  to blocks, we again make use of the  $P$ -adic completion  $K^*$  of  $K$ , and set  $Z_i^* = R^* Z_i, 1 \leq i \leq s$ , so that the modules  $\{K^* Z_i\}$  are a full set of non-isomorphic irreducible  $K^* G$ -modules, and we have  $\bar{Z}_i^* = \bar{Z}_i$ .

(85.5) THEOREM. For each  $Z_i, 1 \leq i \leq s$ , there exists a block  $B_j$  of  $\bar{K}G$  such that all composition factors of  $\bar{Z}_i$  belong to  $B_j$ . (We shall say that  $Z_i$  belongs to  $B_j$  in this case and denote this by  $Z_i \in B_j$ .)

PROOF. As we see from the remarks preceding the statement

of the theorem, we may work over  $K^*$  without affecting our results. By using the technique of raising idempotents discussed in § 77 (see in particular Exercise 77.1), we may find a set of orthogonal central idempotents<sup>†</sup>  $e_1, \dots, e_t \in R^*G$  such that

$$1 = e_1 + \dots + e_t, \quad \bar{e}_1 = \delta_1, \dots, \bar{e}_t = \delta_t.$$

(It will turn out later that each  $e_i \in R_P G$ , as a matter of fact.) Then

$$(85.6) \quad K^*G = \sum_{j=1}^t K^*G \cdot e_j$$

gives a decomposition into two-sided ideals, and so each irreducible  $K^*G$ -module  $K^*Z_i^*$  lies in some summand. If  $K^*Z_i^* \subset K^*G \cdot e_j$ , then

$$Z_i^*(e_j) = I.$$

But then  $\bar{Z}_i^*(\delta_j) = \bar{I}$ , and therefore also  $F_k(\delta_j) = \bar{I}$  for each composition factor  $F_k$  of  $\bar{Z}_i^*$ . Then  $F_k \in B_j$  by (85.4), and the theorem is proved.

Of great importance will be a second characterization of blocks by means of certain maps defined on  $\bar{\Lambda}$ , the center of  $\bar{K}G$ . A *linear character* on  $\bar{\Lambda}$  is a non-zero map  $\psi: \bar{\Lambda} \rightarrow \bar{E}$  (= extension field of  $K$ ) such that

$$\begin{aligned} \psi(\alpha x) &= \alpha \psi(x), & \psi(x+x') &= \psi(x) + \psi(x'), & \psi(xx') &= \psi(x)\psi(x'), \\ && \alpha \in \bar{K}, x, x' \in \bar{\Lambda}. \end{aligned}$$

(It will turn out in a moment that  $\bar{E} = \bar{K}$  in our present discussion.) The class sums  $C_1, \dots, C_s$  form a  $\bar{K}$ -basis for  $\bar{\Lambda}$ , and, to define a linear character  $\psi$  on  $\bar{\Lambda}$ , we need only specify  $\psi(C_1), \dots, \psi(C_s)$ . Since each  $C_k$ , as element of the group ring  $KG$ , commutes with each  $x \in G$ , it follows that for each  $i$  the matrix  $Z_i(C_k)$  commutes with  $\{Z_i(x): x \in G\}$ . But  $K$  is a splitting field for  $G$ , and so we deduce (from Schur's lemma) that for some  $\omega^{(i)}(C_k) \in K$ ,

$$(85.7) \quad Z_i(C_k) = \omega^{(i)}(C_k) I^{(z_i)}, \quad 1 \leq k \leq s.$$

Furthermore, each  $\omega^{(i)}(C_k) \in R_P$  since  $Z_i$  is an  $R_P$ -representation of  $G$ . Extending  $\omega^{(i)}$  to a map on the center of  $KG$  by linearity, we have at once

$$\omega^{(i)}(C_k C_l) = \omega^{(i)}(C_k) \omega^{(i)}(C_l).$$

We now define  $\bar{\omega}^{(i)}: \bar{\Lambda} \rightarrow \bar{K}$  by setting

$$\overline{\omega^{(i)}(C_k)} = \bar{\omega}^{(i)}(C_k), \quad 1 \leq k \leq s,$$

and extending by linearity. Then  $\bar{\omega}^{(i)}$  is a non-zero linear character

<sup>†</sup> These  $\{e_i\}$  are not those used in Theorem 83.9.

on  $\bar{\Lambda}$ ; in fact, if  $Z_i \in B_j$ , then  $\bar{Z}_i(\delta_j) = \bar{I}$ , so that  $\bar{\omega}^{(i)}(\delta_j) = \bar{I}$ . On the other hand, for  $B_i \neq B_j$  we have  $\bar{Z}_i(\delta_j) = 0$ , and so  $\bar{\omega}^{(i)}(\delta_j) = 0$ . We have thus shown

$$(85.8) \quad Z_i \in B_j \quad \text{if and only if } \bar{\omega}^{(i)}(\delta_j) = \bar{I}.$$

Next we observe that the  $\{\delta_i\}$  are orthogonal central idempotents of  $\bar{K}G$ , no one of which is expressible as a sum of two orthogonal central idempotents. Hence

$$\bar{\Lambda} = \bar{\Lambda}\delta_1 \oplus \cdots \oplus \bar{\Lambda}\delta_t$$

gives a decomposition of the commutative algebra  $\bar{\Lambda}$  into indecomposable ideals. Set  $\bar{N} = \text{rad } \bar{\Lambda}$ ; by Theorem 54.11 we know that  $\bar{N}\delta_j$  is a maximal submodule of  $\bar{\Lambda}\delta_j$ , and therefore is also a maximal ideal in the ring  $\bar{\Lambda}\delta_j$ . Hence  $\bar{\Lambda}\delta_j/\bar{N}\delta_j = \bar{K}_j$  is a field which contains  $\bar{K}$ . Let us show that each  $\bar{K}_j$  coincides with  $\bar{K}$ . For let  $Z_i \in B_j$ , and define  $\bar{\omega}^{(i)}$  as above. The kernel of  $\bar{\omega}^{(i)}$  is a maximal ideal in  $\bar{\Lambda}$  which contains  $\{\delta_\nu : \nu \neq j\}$  and hence is given by

$$(85.9) \quad (\sum_{\nu \neq j} \oplus \bar{\Lambda}\delta_\nu) \oplus \bar{N}\delta_j.$$

Then

$$\bar{K} \cong \frac{\bar{\Lambda}}{\ker \bar{\omega}^{(j)}} \cong \frac{\bar{\Lambda}\delta_j}{\bar{N}\delta_j} \cong \bar{K}_j.$$

We may now define  $\psi_j : \bar{\Lambda}\delta_j \rightarrow \bar{\Lambda}\delta_j/\bar{N}\delta_j \cong \bar{K}$ , and extend  $\psi_j$  to a mapping of all  $\bar{\Lambda}$  into  $\bar{K}$  by letting  $\psi_j$  vanish on  $\{\bar{\Lambda}\delta_\nu : \nu \neq j\}$ . The map  $\psi_j : \bar{\Lambda} \rightarrow \bar{K}$  thus obtained is clearly a linear character on  $\bar{\Lambda}$ , and so we have found a set of  $t$  distinct linear characters  $\psi_1, \dots, \psi_t$ , one for each block of  $\bar{K}G$ . Furthermore we have

$$(85.10) \quad \psi_i(\delta_j) = \begin{cases} \bar{I}, & i = j \\ 0, & i \neq j. \end{cases}$$

Finally, these  $\{\psi_i\}$  give all linear characters on  $\bar{\Lambda}$ , since the kernel of any linear character must be a maximal ideal in  $\bar{\Lambda}$ , and hence is of the form (85.9) for some  $j$ . Moreover, two linear characters with the same kernel are identical.

Collecting our results, we have now established the following:

(85.11) THEOREM. *Let  $B_1, \dots, B_t$  be the blocks of  $\bar{K}G$ , with block idempotents  $\delta_1, \dots, \delta_t$ . Let  $\bar{\Lambda}$  = center of  $\bar{K}G$ , and  $\bar{N}$  = rad  $\bar{\Lambda}$ . Then, for each  $j$ , we have  $\bar{\Lambda}\delta_j/\bar{N}\delta_j \cong \bar{K}$ , and we may define linear characters  $\psi_1, \dots, \psi_t$  on  $\bar{\Lambda}$  such that  $\psi_j$  maps  $\bar{\Lambda}\delta_j$  onto  $\bar{\Lambda}\delta_j/\bar{N}\delta_j$ , and  $\psi_k(\bar{\Lambda}\delta_j) = 0$ ,  $k \neq j$ . These  $\{\psi_i\}$  give all of the linear characters of  $\bar{\Lambda}$ . Each  $K$ -representation  $Z_i$  also determines a linear character  $\omega^{(i)}$  on the center*

of  $\bar{K}G$  and a linear character  $\bar{\omega}^{(i)}$  on  $\bar{A}$ . We have  $Z_i \in B_j$  if and only if  $\bar{\omega}^{(i)} = \psi_j$ .

(In connection with the following corollary, see Exercise 55.3.)

(85.12) COROLLARY. *The modules  $Z_i$  and  $Z_j$  belong to the same block if and only if  $\bar{\omega}^{(i)} = \bar{\omega}^{(j)}$ .*

For later use, we record here an obvious equality, gotten by taking traces in (85.7), namely

$$(85.13) \quad \omega^{(i)}(C_j) = \frac{g_j \zeta_j^{(i)}}{z_i}, \quad 1 \leq i, j \leq s,$$

where  $g_j$  is the number of elements in the class  $C_j$  [see also (33.5)]. From (85.12) and (85.13) we obtain a means of classifying the  $\{Z_i\}$  into blocks from a knowledge of the character table of  $G$ . (See §91.)

We are now going to obtain decompositions of the matrices  $C$  and  $D$  relative to the blocks of  $\bar{K}G$ . Suppose that for each  $j$ ,  $1 \leq j \leq t$ , precisely  $x_j$  of  $Z_1, \dots, Z_s$  belong to  $B_j$ . Then [in the notation of (85.6)] the two-sided ideal  $K^*G \cdot e_j$  of  $K^*G$  must decompose into a direct sum of  $x_j$  simple components of  $K^*G$ , say

$$(85.14) \quad K^*G \cdot e_j = \sum_{k=1}^{x_j} K^*G \cdot e_{jk}, \quad 1 \leq j \leq t,$$

and

$$K^*G = \sum_{j=1}^t \sum_{k=1}^{x_j} K^*G \cdot e_{jk}$$

is the decomposition of  $K^*G$  into its simple components. Also we have

$$e_j = \sum_{k=1}^{x_j} e_{jk},$$

and we may remark that no subsum of the right-hand side above can lie in  $R^*G$ , since if this occurred then upon taking residues mod  $P^*$  we would obtain a decomposition of  $\delta_j$  into a sum of orthogonal central idempotents, and this cannot happen.

Suppose next that precisely  $y_j$  of  $F_1, \dots, F_r$  belong to  $B_j$ . Re-number the  $Z$ 's,  $F$ 's, and  $U$ 's if need be, so that the first bunch belong to  $B_1$ , the next to  $B_2$ , and so on. Then  $c_{ij} = 0$  if  $U_i$  and  $F_j$  belong to different blocks, and likewise  $d_{ij} = 0$  if  $Z_i$  and  $F_j$  belong to different blocks. Consequently, we may write

$$(85.15) \quad C = \begin{bmatrix} C_1^{y_1 \times y_1} & 0 \\ \cdot & \cdot \\ 0 & C_t^{y_t \times y_t} \end{bmatrix}, \quad D = \begin{bmatrix} D_1^{x_1 \times y_1} & 0 \\ \cdot & \cdot \\ 0 & D_t^{x_t \times y_t} \end{bmatrix},$$

$$(85.16) \quad C_j = {}^t D_j D_j, \quad 1 \leq j \leq t.$$

The non-singularity of  $C$  implies that each  $C_j$  is non-singular, so from (85.16) we have

$$(85.17) \quad x_j \geq y_j, \quad 1 \leq j \leq t,$$

and each  $D_j$  is of maximal  $p$ -rank  $y_j$ . (In connection with this see Exercise 86.2.)

We note that each  $C_j$  is indecomposable in the following sense. If for some permutation of the rows we have

$$C_j = \begin{pmatrix} C' & 0 \\ 0 & C'' \end{pmatrix},$$

then some pair of  $U$ 's belonging to  $B_j$  could not be linked (§ 55); this is impossible. Since  $C_j$  is indecomposable, so is  $D_j$ .

From equations (85.15) and (86.16), we obtain

$$(85.18) \quad Z_i \in B_k \text{ implies } \zeta^{(i)} = \sum_{F_j \in B_k} d_{ij} \varphi^{(j)},$$

$$(85.19) \quad \begin{aligned} U_i \in B_k \text{ implies } \eta^{(i)} &= \sum_{F_j \in B_k} c_{ij} \varphi^{(j)} \\ &= \sum_{Z_l \in B_k} d_{il} \zeta^{(l)}. \end{aligned}$$

Suppose next that  $x \in G$  is  $p$ -irregular. From (31.13) we have

$$(\zeta^{(1)}(x), \dots, \zeta^{(s)}(x)) (\zeta_j^{(i)})^{s \times r} = 0.$$

If we use (84.7) and the fact that  $\emptyset$  is non-singular, this gives

$$(\zeta^{(1)}(x), \dots, \zeta^{(s)}(x)) \begin{pmatrix} D_1 & & 0 \\ & \ddots & \cdot \\ 0 & & D_t \end{pmatrix} = 0;$$

that is,

$$(85.20) \quad \sum_{Z_l \in B_k} \zeta^{(i)}(x) d_{ln} = 0 \text{ for } 1 \leq k \leq t, 1 \leq n \leq r.$$

Multiply both sides by  $\varphi^{(n)}(y)$ , where  $F_n \in B_k$ , and where  $y$  is  $p$ -regular. Summing on  $n$  and using (85.18), we deduce that

$$(85.21) \quad \sum_{Z_l \in B_k} \zeta^{(i)}(x) \zeta^{(i)}(y) = 0$$

where  $x, y \in G$ ,  $x$   $p$ -irregular,  $y$   $p$ -regular.

To conclude this section, we sketch the proof of Osima's result that condition (85.21) characterizes the blocks of  $\bar{K}G$ .

(85.22) THEOREM (Osima [4]). Let  $B$  be a subset of  $\{\zeta^{(1)}, \dots, \zeta^{(s)}\}$  such that (85.21) holds for  $x$   $p$ -irregular,  $y$   $p$ -regular. Then  $B$  is a union of all those  $\zeta$ 's belonging to some collection of blocks.

PROOF. Let  $T_j = B \cap \{\zeta^{(i)} : \zeta^{(i)} \in B_j\}$ . The argument which established (85.21) can be modified to give

$$(85.23) \quad \sum_{\zeta^{(i)} \in T_j} \zeta^{(i)}(x) \zeta^{(i)}(y) = 0 \quad x \text{ } p\text{-irregular}, y \text{ } p\text{-regular}.$$

For each  $p$ -regular  $y \in G$ , define  $\theta_y = \sum_{T_j} \zeta^{(i)}(y) \cdot \zeta^{(i)}$ . Assuming without loss of generality that  $\sqrt[p]{1} \in K$ , we find that  $\theta_y \in \text{char}_R(G)$  and  $\theta_y$  vanishes on the  $p$ -irregular elements of  $G$ . By Exercises 84.4 and 84.5, we may therefore write  $\theta_y = \sum_n \alpha_n(y) \tau_n$  with coefficients  $\{\alpha_n(y)\}$  in  $R$ . Therefore

$$g^{-1} \sum_{T_j} \zeta^{(i)}(y) z_i = g^{-1} \theta_y(1) = g^{-1} \sum_n \alpha_n(y) u_n \in R_P.$$

Let  $e'_i$  be the central idempotent of  $K^*G$  which corresponds to  $\zeta^{(i)}$ ; we may compute  $e'_i$  by Theorem 33.8. Now set

$$\begin{aligned} E_j &= \sum_{\zeta^{(i)} \in T_j} e'_i = g^{-1} \sum_{\zeta^{(i)} \in T_j} \left\{ \sum_{n=1}^s z_i \zeta_{n*}^{(i)} C_n \right\} \\ &= g^{-1} \sum_{n=1}^s \left( \sum_{T_j} z_i \zeta_{n*}^{(i)} \right) C_n = g^{-1} \sum_{n=1}^s \left( \sum_{T_j} z_i \zeta_{n*}^{(i)} \right) C_n, \end{aligned}$$

the last step by (85.23). Thus  $E_j \in R_P G$ , and  $\delta_j = \bar{E}_j + (\delta_j - \bar{E}_j)$  gives a decomposition of  $\delta_j$  into orthogonal central idempotents unless one of them is zero. Hence  $\bar{E}_j$  is either 0 or  $\delta_j$ , and so  $T_j$  either is empty or coincides with  $\{\zeta^{(i)} : \zeta^{(i)} \in B_j\}$ . This completes the proof.

### Exercise

- Let  $B_1$  be the block of  $\bar{K}G$  containing the 1-character  $\varphi^{(1)}$ . Show that  $G$  contains a normal subgroup of index  $p^e$  if and only if  $\varphi^{(1)}$  is the only  $\varphi$  contained in  $B_1$ . [Hint: Let  $H \triangle G$ ,  $[G:H] = p^e$ . Since  $p^e | u_1$ , we have  $\eta^{(1)} = \hat{\varphi}^{(1)}\sigma$  where  $\hat{\varphi}^{(1)}$  is the 1-character of  $H$ . Therefore  $\eta^{(1)}(x) = p^e$  for  $p$ -regular  $x$  in  $G$ , which shows that  $\eta^{(1)} = p^e \varphi^{(1)}$ ,  $C_1 = (p^e)$ , and  $\varphi^{(1)}$  is the only  $\varphi$  in  $B_1$ .

Conversely, let  $\varphi^{(1)}$  be the only  $\varphi$  in  $B_1$ , and define

$$H = \{x \in G : Z_t(x) = I^{(\epsilon_t)} \text{ for each } Z_t \in B_1\}.$$

Then  $H \triangle G$ , and each  $Z_t$  induces an irreducible representation of  $G/H$ . Therefore (letting  $h = [H:1]$ ),

$$g/h \geq \sum_{Z_t \in B_1} z_t^2 = u_1 f_1 \geq p^e.$$

On the other hand, for each  $Z_i \in B_1$  we have  $\zeta^{(i)} = d_{i1}\varphi^{(1)}$ , and so  $\zeta^{(i)}$  is constant on the  $p$ -regular elements of  $G$ . As in the beginning of the proof of (35.9), it follows that  $Z_i(x) = I^{(z_i)}$  for  $x$   $p$ -regular in  $G$ . Thus  $H$  contains all  $p$ -regular elements of  $G$ , and so  $H$  contains all  $q$ -Sylow subgroups of  $G$  for each prime  $q \neq p$ . Therefore  $h$  is a multiple of  $g/p^e$ , and so  $h \geq g/p^e$ . Thus  $h = g/p^e$ .]

### § 86. The Defect of a Block

We keep the notation of the preceding sections, and recall that for  $a \in Z$  we have defined  $\nu(a)$  by  $p^{\nu(a)} \mid\mid a$ . The formula

$$\nu(G.C.D.\{a_1, \dots, a_n\}) = \min_{1 \leq i \leq n} \nu(a_i)$$

will be used frequently.

In § 85 we showed how the  $R_P G$ -modules  $Z_1, \dots, Z_s$  could be assigned to the blocks  $B_1, \dots, B_t$  of  $\bar{K}G$ . By Theorem 33.7, we know that each  $z_i$  divides  $g$ , and hence that  $\nu(z_i) \leq e$ ,  $1 \leq i \leq s$ , where  $e = \nu(g)$ .

(86.1) **DEFINITION.** Let  $B_j$  be a block of  $\bar{K}G$ . The *defect*  $d_j$  of  $B_j$  is given by

$$(86.2) \quad d_j = e - \min_{Z_i \in B_j} \nu(z_i).$$

In other words,  $p^{e-d_j} \mid z_i$  for all  $Z_i \in B_j$ , and  $p^{e-d_j+1} \nmid z_i$  for some  $Z_i \in B_j$ . Clearly each  $d_j \geq 0$ .

Let us show that the theory of blocks of defect 0 is relatively uncomplicated.

(86.3) **THEOREM (Brauer and Nesbitt [3]).** If  $\nu(z_i) = e$ , then  $Z_i$  belongs to a block of defect 0. Each block of defect 0 contains exactly one  $U_i$ , one  $F_i$ , and one  $Z_i$ , and in fact  $\bar{Z}_i = F_i = U_i$ . For such a  $Z_i$ , we have  $\zeta^{(i)}(x) = 0$  for  $p$ -irregular  $x$  in  $G$ .

**PROOF.** Let  $\nu(z_i) = e$ , and let  $Z_i \in B_j$ . From (85.14) we have

$$e_j = \sum_{k=1}^{z_j} e_{jk},$$

and assume (to fix the notation) that  $Z_i$  is afforded by a minimal left ideal in  $K^*G \cdot e_{j1}$ . From (33.8), we have

$$e_{j1} = g^{-1} \sum_{x \in G} z_i \zeta^{(i)}(x^{-1})x.$$

Since  $\nu(z_i) = \nu(g)$ , we conclude that  $e_{j1} \in R^*G$ . But then, if  $x_j > 1$ ,

$$\delta_j = \bar{e}_j = \bar{e}_{j1} + \left( \sum_{2 \leq k \leq z_j} e_{jk} \right)$$

gives a decomposition of  $\delta_j$ , which is impossible. Hence  $x_j = 1$ , so by (85.17) also  $y_j = 1$ . Thus  $C_j$  and  $D_j$  are  $1 \times 1$  matrices, which already shows that  $B_j$  has defect 0, and that exactly one  $Z_i$ ,  $F_i$ , and  $U_i$  belong to  $B_j$ .

We show further that  $C_j = D_j = (1)$  if  $B_j$  is a block of defect 0. To prove this, it suffices to show that  $\bar{Z}_i$  is irreducible, where  $Z_i \in B_j$ , for then  $\bar{Z}_i = F_i = U_i$ . Suppose  $\bar{Z}_i$  were reducible; upon replacing  $Z_i$  by  $X^{-1}Z_iX$ , with  $X$  unimodular over  $R^*$ , we may take

$$Z_i(x) = (\alpha_{mn}^{(i)}(x))_{1 \leq m, n \leq z_i}, \quad x \in G,$$

with the lower left-hand entry  $\alpha_{z_i 1}^{(i)}(x) \in P$  for all  $x \in G$ . From Exercise 31.1, we have

$$\sum_{x \in G} \alpha_{z_i 1}^{(i)}(x) \alpha_{1 z_i}^{(i)}(x^{-1}) = g/z_i.$$

The left-hand side lies in  $P$ , whence so does  $g/z_i$ . This cannot hold, because  $\nu(g) = \nu(z_i)$ . Thus  $\bar{Z}_i$  must be irreducible.

To complete the proof of the theorem, we use formula (85.20) for the block  $B_j$ . There is just one term in the summation, and for that term  $d_{im} = 1$ , and so we deduce that  $\zeta^{(i)}(x) = 0$  for  $p$ -irregular  $x \in G$ . This finishes the proof.

Let us obtain another characterization of the defect  $d_j$  of the block  $B_j$ . From §85, we know that  $D_j$  has maximal  $p$ -rank  $y_j$ . Furthermore, if  $\{Z_{jk}: 1 \leq k \leq x_j\}$  are the  $Z$ 's belonging to  $B_j$ , and if  $\{F_{jk}: 1 \leq k \leq y_j\}$  are the  $F$ 's belonging to  $B_j$ , then from (85.18) we have

$$(86.4) \quad \begin{pmatrix} \zeta^{(j1)}(x) \\ \vdots \\ \zeta^{(jx_j)}(x) \end{pmatrix} = D_j \begin{pmatrix} \varphi^{(j1)}(x) \\ \vdots \\ \varphi^{(jy_j)}(x) \end{pmatrix}, \quad x \text{ } p\text{-regular}.$$

Taking  $x = 1$ , we obtain

$$\begin{pmatrix} z_{j1} \\ \vdots \\ z_{jx_j} \end{pmatrix} = D_j \begin{pmatrix} f_{j1} \\ \vdots \\ f_{jy_j} \end{pmatrix},$$

and from this (since  $D_j$  has maximal  $p$ -rank), we conclude that

$$\nu(\text{G.C.D.}(z_{j1}, \dots, z_{jx_j})) = \nu(\text{G.C.D.}(f_{j1}, \dots, f_{jy_j})).$$

This establishes the important formula:

$$(86.5) \quad d_j = e - \min_{F_i \in B_j} \nu(f_i), \quad 1 \leq j \leq t,$$

which gives the defect of a block  $B_j$  in terms of the set of  $\varphi$ 's belonging to  $B_j$ .

Turning next to formula (85.19), let us evaluate both sides at the identity element of  $G$ . We obtain at once

$$(86.6) \quad \begin{pmatrix} u_{j1} \\ \vdots \\ u_{jy_j} \end{pmatrix} = C_j \begin{pmatrix} f_{j1} \\ \vdots \\ f_{jy_j} \end{pmatrix}, \quad 1 \leq j \leq t.$$

Set

$$a_j = \nu(G.C.D. (u_i))_{\substack{U_i \subset B_j}}.$$

By (84.15), we have  $a_j \geq e$ , and so

$$a_j \geq e \geq e - d_j = \nu(G.C.D. (f_i))_{\substack{F_i \in B_j}}.$$

Using Exercise 16.5, we may conclude that some elementary divisor of  $C_j$  is  $\geq p^{a_j - (e - d_j)}$ , and this is  $\geq p^{d_j}$ . This proves

(86.7) THEOREM. *If the block  $B_j$  has defect  $d_j$ , then at least one elementary divisor of  $C_j$  is  $\geq p^{d_j}$ . (We shall improve on this result in § 89.)*

We shall now define the defect of a conjugate class of  $G$ , and shall introduce some notation which will be used for the remainder of the chapter.

(86.8) DEFINITION. For  $1 \leq i \leq s$ , let  $\mathfrak{C}_i$  be a conjugate class of  $G$ . Let  $x_i$  denote an element of  $\mathfrak{C}_i$ , and set  $N(x_i)$  = normalizer of  $x_i$  in  $G$ . Let  $n_i = [N(x_i): 1]$ ,  $h_i = \nu(n_i)$ , and call  $h_i$  the defect of the class  $\mathfrak{C}_i$ . The number of elements in  $\mathfrak{C}_i$  is  $g_i = g/n_i$  [see (84.6)].

(86.9) THEOREM. *The number of blocks of defect  $d$  does not exceed the number of  $p$ -regular classes of  $G$  of defect  $\geq d$ .*

PROOF. By Theorem 86.7, to each block  $B_j$  of defect  $d$  corresponds an elementary divisor of  $C_j$  which is  $\geq p^d$ . On the other hand, by (84.10),

$$\text{el. div. } C = \text{powers of } p \text{ in } \{n_1, \dots, n_r\}.$$

Thus to each  $B_j$  of defect  $d$  corresponds (at least) one  $n_i$  which is a multiple of  $p^d$ . This completes the proof.

(86.10) **THEOREM (Brauer and Nesbitt [3]).** *The number of blocks of defect  $e$  equals the number of  $p$ -regular classes of defect  $e$ .*

**PROOF.** Since no class can have defect  $> e$ , it follows from Theorem 86.9 that the number of blocks of defect  $e$  is  $\leq$  the number of  $p$ -regular classes of defect  $e$ .

On the other hand, we have from (84.10)

$$\text{el. div. } (gC^{-1}) = \text{powers of } p \text{ in } \{g_1, \dots, g_r\},$$

so that the rank of  $\overline{gC^{-1}}$  equals the number of  $p$ -regular classes of defect  $e$ . To complete the proof of the theorem, we need show only that the rank of  $\overline{gC^{-1}}$  is  $\leq$  the number of blocks of defect  $e$ . By (84.12) we have  $\overline{gC^{-1}} = (\bar{\alpha}_{ij})$  where

$$(86.11) \quad \bar{\alpha}_{ij} = \sum_{l=1}^r \bar{g}_l \bar{\varphi}_l^{(i)} \bar{\varphi}_l^{(j)}.$$

Let  $F_i \in B_n$ ; then  $F_i$  is a composition factor of  $\bar{Z}_k$  for some  $Z_k \in B_n$ . However,

$$\bar{Z}_k(C_l) = \psi_n(C_l) I^{(z_k)} \quad \text{for each } l,$$

where  $\psi_n$  is the linear character associated with the block  $B_n$ . Therefore

$$F_i(C_l) = \psi_n(C_l) I^{(f_i)}, \quad 1 \leq l \leq r,$$

and taking traces we obtain

$$(86.12) \quad \bar{g}_l \bar{\varphi}_l^{(i)} = \psi_n(C_l) \bar{f}_i, \quad 1 \leq l \leq r, F_i \in B_n.$$

We may thus rewrite (86.11) as

$$\begin{aligned} \bar{\alpha}_{ij} &= \bar{f}_i \sum_{l=1}^r \psi_n(C_l) \bar{\varphi}_l^{(j)}, & F_i \in B_n, \\ &= \bar{f}_i S_j(n), \end{aligned}$$

say. If both  $F_i$  and  $F_j$  belong to  $B_n$ , then using the symmetry of  $g^{-1}C$  we get

$$\bar{\alpha}_{ij} = \bar{f}_i \bar{f}_j s_n, \quad F_i, F_j \in B_n,$$

where  $s_n \in \bar{K}$  and  $s_n$  depends only upon  $n$ . Therefore  $\overline{gC_n^{-1}}$  equals  $0$  unless  $B_n$  has defect  $e$ , and has rank  $\leq 1$  when  $B_n$  has defect  $e$ . Consequently the rank of  $\overline{gC^{-1}}$  is at most equal to the number of blocks of defect  $e$ , and this completes the proof. [Another proof of Theorem 86.10 will be given in §89.]

The remainder of this section deals with relations between defects of blocks of  $\bar{K}G$  and defects of  $p$ -regular classes of  $G$ . The results given here are due to Brauer [27] and Osima [6], and the methods used are those of Osima.

We have seen that to each block idempotent  $\delta_j$  of  $\bar{K}G$  there corresponds a central idempotent  $e_j \in R^*G$  such that  $\bar{e}_j = \delta_j$ . Furthermore, from (85.14), we know that  $e_j$  is a sum of those central idempotents of  $K^*G$  which correspond to  $\zeta$ 's belonging to the block  $B_j$ . Since each such central idempotent is given explicitly in terms of its character by Theorem 33.8, we have

$$e_j = g^{-1} \sum_{z_i \in B_j} \sum_{n=1}^s z_i \zeta_n^{(i)} (x_n^{-1}) C_n,$$

where  $x_n$  denotes an element in the class  $\mathfrak{C}_n$ . We rewrite the above as

$$(86.13) \quad e_j = \sum_{n=1}^s b_{jn} C_n, \quad b_{jn} = g^{-1} \sum_{z_i \in B_j} z_i \zeta_n^{(i)}.$$

To begin with, we shall show that  $b_{jn}$  vanishes if the class  $\mathfrak{C}_n$  is not  $p$ -regular.

(86.14) **LEMMA.** *For  $p$ -irregular classes  $\mathfrak{C}_n$ , we have  $b_{jn} = 0$  for all  $j$ .*

**PROOF.** Let  $x$  be a  $p$ -irregular element of  $G$ , and take  $y = 1$  in (85.21). The result follows at once.

Next we use (85.18) and (85.19) to write (for  $1 \leq n \leq r$ )

$$(86.15) \quad b_{jn} = g^{-1} \sum_{z_i \in B_j} z_i \left\{ \sum_{F_m \in B_j} d_{im} \varphi_{n^*}^{(m)} \right\} = g^{-1} \sum_{F_m \in B_j} u_m \varphi_{n^*}^{(m)}.$$

Since  $\nu(u_m) \geq e$  for all  $m$ , this shows that each  $b_{jn} \in R_P$ , and also that each  $e_j \in R_P G$ .\*

Let us now make use of the mappings  $\{\omega^{(k)}\}$  defined on the center of  $KG$  as in § 85. We have [from (85.13)]

$$\begin{aligned} \omega^{(k)}(e_j) &= \sum_{n=1}^s b_{jn} \omega^{(k)}(C_n) \\ &= g^{-1} \sum_{z_i \in B_j} \sum_{n=1}^s z_i \zeta_n^{(i)} \cdot \frac{g_n \zeta_n^{(k)}}{z_k}. \end{aligned}$$

Applying the orthogonality relation (31.18), this yields

$$(86.16) \quad \omega^{(k)}(e_j) = \begin{cases} 1, & Z_k \in B_j \\ 0, & Z_k \notin B_j \end{cases}$$

---

\* We could have predicted that  $e_j \in R_P G$  without this calculation because of (76.28) (see footnote to the proof of (83.9).)

Using this together with Lemma 86.14, we have

$$(86.17) \quad \sum_{n=1}^r \bar{b}_{jn} \overline{\omega^{(k)}(C_n)} = \begin{cases} \bar{1}, & Z_k \in B_j \\ 0, & Z_k \notin B_j. \end{cases}$$

In terms of the linear character  $\psi_i$  associated with the block  $B_i$ , this becomes

$$(86.18) \quad \sum_{n=1}^r \bar{b}_{jn} \psi_i(C_n) = \begin{cases} 0, & i \neq j \\ \bar{1}, & i = j. \end{cases}$$

As an immediate consequence of this we have the following improvement of (85.12).

(86.19) THEOREM.  $Z_k \in B_j$  if and only if

$$\sum_{n=1}^r \bar{b}_{jn} \overline{\omega^{(k)}(C_n)} = \bar{1}.$$

Two modules  $Z_i$  and  $Z_k$  belong to the same block if and only if  $\bar{\omega}^{(i)}(C_n) = \bar{\omega}^{(k)}(C_n)$ ,  $1 \leq n \leq r$ .

(86.20) COROLLARY. Each block  $B_j$  contains a  $U_i$  for which  $\nu(u_i) = e$ .

PROOF. We already know that  $\nu(u_i) \geq e$  for all  $i$ , by (84.15). If  $\nu(u_i) > e$  for all  $U_i \in B_j$ , then from (86.15) we see that  $\bar{b}_{jn} = 0$  for all  $n$ ,  $1 \leq n \leq r$ , which contradicts (86.18).

(86.21) LEMMA. For  $1 \leq k \leq r$ , we have  $\bar{b}_{jk} = 0$  whenever  $h_k > d_j$ , where  $h_k$  is the defect of the class  $\mathfrak{C}_k$  (see (86.8)) and  $d_j$  is the defect of the block  $B_j$ .

PROOF. Fix  $j$  and  $k$ , and suppose that  $h_k > d_j$ . From (85.13), we have

$$\zeta_k^{(i)} = n_k \cdot \frac{z_i}{g} \cdot \omega^{(i)}(C_k);$$

for each  $Z_i \in B_j$  this yields

$$\nu(n_k) + \nu(z_i/g) = h_k + \nu(z_i) - e \geq h_k + (e - d_j) - e > 0,$$

which shows that  $\zeta_k^{(i)} \equiv 0 \pmod{P}$ . But then each entry on the left-hand side of equation (86.4) lies in  $P$ , and, since  $D_j$  has maximal  $p$ -rank, also each entry of the column vector on the right-hand side of (86.4) lies in  $P$ . Thus  $\varphi_k^{(i)} \in P$  for all  $F_i \in B_j$ , and it follows from the second expression for  $b_{jn}$  in (86.15) that also  $b_{jk} \in P$ . This completes the proof since  $h_k = h_k$ .

(86.22) LEMMA. If the block  $B_j$  has defect  $d_j$ , then  $\psi_j(C_k) = 0$  whenever  $h_k < d_j$ .

PROOF. We may choose  $Z_i \in B_j$  with  $\nu(z_i) = e - d_j$ . Then

$$\omega^{(i)}(C_k) = \frac{q}{z_i} \cdot \frac{1}{n_k} \zeta_k^{(i)},$$

so  $\psi_j(C_k) = \bar{\omega}^{(i)}(C_k) = 0$  whenever  $h_k < d_j$ .

By making use of the preceding two lemmas, we obtain an improved version of Theorem 86.19.

(86.23) THEOREM. Let  $\psi_i$  be the linear character associated with the block  $B_i$ . Suppose that  $d_i = d_j$ . Then

$$(86.24) \quad \sum_{\substack{1 \leq n \leq r \\ h_n = d_j}} \bar{b}_{jn} \psi_i(C_n) = \begin{cases} 1, & i = j, \\ 0, & i \neq j. \end{cases}$$

PROOF. Since  $d_i = d_j$ , we find that  $\bar{b}_{jn} \psi_i(C_n) = 0$  whenever  $h_n \neq d_j$ , by (86.21) and (86.22). Therefore

$$\sum_{\substack{1 \leq n \leq r \\ h_n = d_j}} \bar{b}_{jn} \psi_i(C_n) = \sum_{n=1}^r \bar{b}_{jn} \psi_i(C_n),$$

and the result follows from Theorem 86.19

(86.25) COROLLARY. Suppose that  $Z_i$  and  $Z_k$  both belong to blocks of defect  $d$ . Then  $Z_i$  and  $Z_k$  belong to the same block if and only if  $\bar{\omega}^{(i)}(C_n) = \bar{\omega}^{(k)}(C_n)$  for all  $p$ -regular classes  $C_n$  of defect  $d$ .

(86.26) COROLLARY. Let  $B_j$  be a block of defect  $d$ . Then there exists a  $p$ -regular class  $C_n$  of defect  $d$  such that  $\bar{b}_{jn} \psi_j(C_n) \neq 0$ .

(86.27) COROLLARY. The module  $Z_i$  belongs to a block of defect  $d$  if and only if  $\omega^{(i)}(C_k) \equiv 0 \pmod{P}$  whenever  $h_k < d$ ,  $1 \leq k \leq r$ , whereas  $\omega^{(i)}(C_l) \not\equiv 0 \pmod{P}$  for some  $p$ -regular class  $C_l$  of defect  $d$ .

(86.28) COROLLARY. If  $\omega^{(i)}(C_k) \not\equiv 0 \pmod{P}$  for some  $p$ -regular class  $C_k$ , then  $Z_i$  belongs to a block of defect  $\leqq h_k$ .

### Exercises

1. Let  $p^m$  be the greatest elementary divisor of  $C_j$ , and let  $F_t \in B_j$ . Prove that  $\nu(\varphi_k^{(t)}) \geq \nu(n_k) - m$ ,  $1 \leq k \leq r$ , where  $\nu$  is extended from  $Q$  to  $K$  so that  $\nu(p) = 1$ . Deduce further that for each  $Z_t \in B_j$ , we have  $\nu(\zeta_k^{(t)}) \geq \nu(n_k) - m$ ,  $1 \leq k \leq r$ .

2. In the notation of (85.17), show that  $x_j = y_j$  if and only if  $B_j$  is a block of defect 0. [Hint: If  $x_j = y_j$ , then  $D_j$  is a square matrix of determinant  $\pm 1$ , and so  $|C_j| = 1$ . By (86.7), this shows that  $B_j$  has defect 0.]

3. (Brauer and Nesbitt [3].) Using (84.12) with  $i = k = 1$  and  $\varphi^{(1)} =$

1-character of  $G$ , show that the number  $N$  of  $p$ -regular elements of  $G$  satisfies  $N = g\gamma_{11}$ . The matrix  $C$  is positive definite, which implies that  $\gamma_{11} \geq 1/c_{11}$ , with equality if and only if  $c_{12} = \dots = c_{1r} = 0$ . Hence  $c_{11} \geq g/N$ , with equality if and only if  $\varphi^{(1)}$  is the only  $\varphi$  in its block  $B_1$ . By Exercise 85.1, the latter occurs if and only if  $G$  contains a normal subgroup of index  $p^e$ , and in this case  $c_{11} = p^e$ .

### § 87. Defect Groups

In the preceding section, we established a connection between defects of blocks of  $\bar{K}G$  and defects of  $p$ -regular classes of  $G$ . This connection will be made even stronger here, and we shall show how to assign to each block  $B$  of defect  $d$  a subgroup of  $G$  of order  $p^d$ , called the *defect group* of the block  $B$ . This defect group of  $B$  will be uniquely determined by  $B$  up to conjugacy. Most of the results are due to Brauer [13], [16], [27], but for several proofs we shall use the simplifications given by Osima [6].

(87.1) DEFINITION. Let  $N(x_i)$  be the normalizer (in  $G$ ) of an element  $x_i \in \mathbb{C}_i$ . If  $H_i$  is any  $p$ -Sylow subgroup of  $N(x_i)$ , we call  $H_i$  a *defect group* of the class  $\mathbb{C}_i$ . [By Theorem 6.7, we see that  $H_i$  is uniquely defined up to conjugacy in  $N(x_i)$ .] We then have  $[H_i : 1] = p^{h_i}$ , where  $h_i$  is the *defect* of  $\mathbb{C}_i$  [see Definition 86.8.]

Briefly recalling some earlier definitions, we had denoted by  $C_i$  the sum of the elements in the class  $\mathbb{C}_i$ , by  $g_i$  the number of elements in  $\mathbb{C}_i$  and  $n_i = g/g_i = [N(x_i) : 1]$ ,  $x_i \in \mathbb{C}_i$ . Also we used  $\mathbb{C}_{i^*}$  for the class of inverses of the elements in  $\mathbb{C}_i$ . Now write

$$(87.2) \quad C_i C_j = \sum_{k=1}^s a_{ijk} C_k, \quad 1 \leq i, j \leq s,$$

where the  $\{a_{ijk}\}$  are non-negative integers. One easily verifies that

$$(87.3) \quad a_{ijk} = a_{jik}, \quad \sum_{i=1}^s a_{ijk} = g_j,$$

and we leave the proof of these as exercises.

(87.4) LEMMA. For  $1 \leq i, j, k \leq s$ , we have

$$a_{ijk} = \frac{n_k}{n_j} a_{i^*kj}.$$

PROOF. From (87.2) we see that  $g_k a_{ijk}$  is the number of solutions of

$$(87.5) \quad x_i x_j \in \mathbb{C}_k, \quad x_i \in \mathbb{C}_i, \quad x_j \in \mathbb{C}_j,$$

whereas  $g_j a_{ijk}$  is the number of solutions of

$$(87.6) \quad y_i y_k \in \mathbb{C}_j, \quad y_i \in \mathbb{C}_i, \quad y_k \in \mathbb{C}_k.$$

But if  $(x_i, x_j)$  is any solution of (87.5), then  $(x_i^{-1}, x_i x_j)$  is a solution of (87.6). Therefore

$$g_k a_{ijk} \leq g_j a_{ijk}.$$

Since the argument may be reversed, equality must hold above. Substituting  $g/n_k$  for  $g_k$ ,  $g/n_j$  for  $g_j$ , we obtain the desired result.

As an obvious consequence of Lemma 87.4, we have

(87.7) COROLLARY. If  $h_j < h_k$ , then  $p \mid a_{ijk}$ . Therefore

$$C_i C_j \equiv \sum_{\substack{1 \leq k \leq s \\ H_k \subset H_j}} a_{ijk} C_k \pmod{PG}.$$

(87.8) DEFINITION. If  $H$  and  $H'$  are subgroups of  $G$ , the notation  $H =_c H'$  shall mean that  $H$  and  $H'$  are conjugate in  $G$ , whereas  $H \subset_c H'$  shall indicate that  $H$  is contained in some conjugate of  $H'$ .

We may now improve Corollary 87.7 as follows:

(87.9) LEMMA. For  $1 \leq i, j \leq s$ , we have

$$C_i C_j \equiv \sum_{\substack{1 \leq k \leq s \\ H_k \subset H_j \\ H_k \subset H_i}} a_{ijk} C_k \pmod{PG}.$$

PROOF. Fix  $i$  and  $j$ , and fix  $x_k$  in  $\mathbb{C}_k$ . Let  $H_k$  be a  $p$ -Sylow subgroup of  $N(x_k)$ , and suppose that  $H_k$  is not contained in any conjugate of  $H_j$ . Then we shall prove that  $p \mid a_{ijk}$ , which will imply the desired result.

We observe that  $a_{ijk}$  is the number of solutions  $(x, y)$  of

$$(87.10) \quad xy = x_k, \quad x \in \mathbb{C}_i, \quad y \in \mathbb{C}_j.$$

With each solution  $(x, y)$  we associate the set

$$S(x, y) = \{(h^{-1}xh, h^{-1}yh) : h \in H_k\}.$$

Two sets  $S(x, y)$  and  $S(x', y')$  either coincide or are disjoint, as is easily verified.

We shall now determine the number of distinct ordered pairs in  $S(x, y)$ . We have

$$x = h^{-1}xh, \quad y = h^{-1}yh, \quad h \in H_k,$$

if and only if

$$h \in H_k \cap N(x) \cap N(y).$$

The number of distinct pairs in  $S(x, y)$  is therefore

$$[H_k : H_k \cap N(x) \cap N(y)].$$

Since  $H_k$  is a  $p$ -group, each such index is a power of  $p$  (possibly  $p^0$ ) and therefore  $a_{ijk}$  will be a multiple of  $p$  unless for some  $x \in \mathfrak{C}_i$  and some  $y \in \mathfrak{C}_j$  we have  $H_k \subset N(x) \cap N(y)$ . But then  $H_k \subset_c H_j$ , where  $H_j$  is a  $p$ -Sylow subgroup of  $N(y)$ . Thus we have shown that if  $H_k$  is not contained in any conjugate of  $H_j$ , we have  $p \mid a_{ijk}$ , and the lemma is proved.

One of the main results of this section is the connection between blocks of  $\bar{K}G$  and blocks of  $\bar{K} \cdot N(H)$  for some subgroup  $H$  of  $G$ . The basic tool in this discussion will be a certain homomorphism of the center of  $\bar{K}G$  into the center of  $\bar{K} \cdot N(H)$ , and we now proceed to define this homomorphism.

Let  $H$  be some  $p$ -subgroup of  $G$  to be specified later, and let  $N(H)$  be its normalizer,  $C_G(H)$  its centralizer in  $G$ . Clearly  $H \cdot C_G(H) \subset N(H)$ . We define

$$(87.11) \quad C'_i = \sum_{x \in \mathfrak{C}_i \cap C_G(H)} x, \quad 1 \leq i \leq s,$$

or  $C'_i = 0$  if  $\mathfrak{C}_i \cap C_G(H)$  is empty. Let us show that if  $C'_i \neq 0$ , then  $C'_i$  is a sum of elements which make up certain conjugate classes in  $N(H)$ . For if  $x \in \mathfrak{C}_i \cap C_G(H)$ , the transform of  $x$  by any element of  $N(H)$  also lies in  $\mathfrak{C}_i \cap C_G(H)$  (see Exercise 87.1), and this proves the assertion. Thus each  $C'_i$  lies in the center of  $\bar{K} \cdot N(H)$ .

We shall use repeatedly

(87.12) **LEMMA.**  $C'_i \neq 0$  if and only if  $H \subset_c H_i$ . In particular, if  $H = H_n$  (the defect group of  $\mathfrak{C}_n$ ), then  $C'_n \neq 0$ , and in fact  $\mathfrak{C}_n \cap C_G(H)$  consists of a single class in  $N(H)$ .

**PROOF.** We note that  $C'_i \neq 0$  if and only if there exists an  $x$  in  $\mathfrak{C}_i \cap C_G(H)$ . But such an  $x$  exists if and only if  $H \subset N(x)$  for some  $x \in \mathfrak{C}_i$ , that is, if and only if  $H \subset_c H_i$ .

Now let  $H = H_n = p$ -Sylow subgroup of  $N(x)$ , where  $x \in \mathfrak{C}_n$  is fixed. The above shows at once that  $C'_n \neq 0$ . We must now prove that if  $t \in G$  is such that  $t^{-1}xt \in C_G(H)$ , then

$$(87.13) \quad t^{-1}xt = z^{-1}xz \quad \text{for some } z \in N(H).$$

Now  $t^{-1}xt \in C_G(H)$  implies  $H \subset N(t^{-1}xt)$ . Since  $N(x)$  and  $N(t^{-1}xt)$  have the same order and  $H$  is a  $p$ -Sylow subgroup of  $N(x)$ , we conclude

that  $H$  is also a  $p$ -Sylow subgroup of  $N(t^{-1}xt)$ . Each  $p$ -Sylow subgroup of  $N(t^{-1}xt)$  is of the form  $t^{-1}H_0t$ , where  $H_0$  is a  $p$ -Sylow subgroup of  $N(x)$ . Thus

$$H = t^{-1}H_0t$$

for some  $p$ -Sylow subgroup  $H_0$  of  $N(x)$ . But all  $p$ -Sylow subgroups of  $N(x)$  are conjugate in  $N(x)$ , and so  $H_0 = y^{-1}Hy$  for some  $y \in N(x)$ . This yields

$$H = t^{-1}y^{-1}Hyt,$$

whence  $yt \in N(H)$ . Set  $yt = z \in N(H)$ . Then

$$x = y^{-1}xy = tz^{-1}xzt^{-1},$$

which implies (87.13), and the lemma is established.

(87.14) **LEMMA.** *For  $1 \leq i, j \leq s$ ,*

$$C'_i \cdot C'_j \equiv \sum_{1 \leq k \leq s} a_{ijk} C'_k \pmod{PG}.$$

**PROOF.** Set  $C_i = C'_i + C''_i$ , where

$$C''_i = \sum_{\substack{x \in \mathfrak{G}_i \\ x \notin C_G(H)}} x.$$

Then

$$(C'_i + C''_i)(C'_j + C''_j) = \sum_{k=1}^s a_{ijk}(C'_k + C''_k).$$

Since no element of  $C'_i C'_j$  or  $C'_i C''_j$  can lie in  $C_G(H)$ , the lemma will be proved once we show that the number  $N''$  of times an element  $z \in C_G(H)$  occurs in  $C'_i C''_j$  is a multiple of  $p$ . Now  $N''$  is the number of solutions of

$$xy = z, \quad x \in \mathfrak{G}_i, y \in \mathfrak{G}_j, x \notin C_G(H), y \notin C_G(H).$$

The argument used in the proof of Lemma 87.9 can be readily applied to this case to show that  $p \mid N''$ , and the result follows.

Let us set

$$\bar{\Lambda} = \text{center of } \bar{K}G, \quad \bar{\Lambda}_H = \text{center of } \bar{K} \cdot N(H),$$

$$\bar{\Lambda}' = \sum_{i=1}^s \bar{K}C'_i \subset \bar{\Lambda}_H.$$

By Lemma 87.14, we see that  $\bar{\Lambda}'$  is a subring of  $\bar{\Lambda}_H$ . We may define a  $\bar{K}$ -homomorphism of  $\bar{\Lambda}$  onto  $\bar{\Lambda}'$  by means of  $C_i \mapsto C'_i$ ,  $1 \leq i \leq s$ . Lemma 87.14 shows that this map is in fact an *algebra* homomor-

phism; that is, it preserves addition, multiplication, and the action of  $\bar{K}$ . The kernel of the mapping is

$$(87.15) \quad \bar{T} = \sum_{\delta_i' = 0} \bar{K} C_i$$

and is an ideal in  $\bar{A}$ . Then  $\bar{A}/\bar{T} \cong \bar{A}'$  as  $\bar{K}$ -algebras.

We had denoted by  $\delta_1, \dots, \delta_t$  the block idempotents of  $\bar{K}G$ , and we had defined linear characters  $\phi_1, \dots, \phi_t$  such that for each  $i$ ,  $1 \leq i \leq t$ ,  $\phi_i: \bar{A} \rightarrow \bar{K}$  is a  $\bar{K}$ -homomorphism for which  $\phi_i(\delta_j) = \bar{1}$  or  $\bar{0}$  according to whether  $j = i$  or  $j \neq i$ . Now let  $\{\tilde{B}_i\}$  denote the blocks of  $\bar{K} \cdot N(H)$ , with block idempotents  $\{\tilde{\delta}_i\}$  and linear characters  $\{\tilde{\psi}_i\}$ , where each  $\tilde{\psi}_i$  maps  $\bar{A}_H$  into  $\bar{K}$ .

Suppose that under the mapping  $\bar{A} \rightarrow \bar{A}' \subset \bar{A}_H$ , the idempotent  $\delta_i$  maps onto  $\delta_i'$ . Since  $\bar{1} = \sum \delta_i$ , we have also  $\bar{1} = \sum \delta_i'$ , and the  $\{\delta_i'\}$  are orthogonal central idempotents in  $\bar{A}_H$ , except that some of the  $\{\delta_i'\}$  may be zero. Each non-zero idempotent  $\delta_i'$  is then uniquely expressible as a sum of block idempotents  $\{\tilde{\delta}_j\}$ . We shall call these  $\{\tilde{\delta}_j\}$  the *subordinates* of  $\delta_i$  (relative to the subgroup  $H$  of  $G$ ) and shall say that  $\delta_i$  *dominates* each such  $\tilde{\delta}_j$  (notation:  $\tilde{\delta}_j < \delta_i$  or  $\delta_i > \tilde{\delta}_j$ ). Note that  $\delta_i' = 0$  if and only if  $\delta_i \in \bar{T}$ . Obviously we have  $\tilde{\delta}_j < \delta_i$  if and only if  $\tilde{\psi}_j(\delta_i') = \bar{1}$ .

(87.16) **LEMMA.**  $\tilde{\delta}_j < \delta_i$  if and only if  $\tilde{\psi}_j(C_k) = \phi_i(C_k)$  for  $1 \leq k \leq s$ .

**PROOF.** If  $\tilde{\psi}_j(C_k) = \phi_i(C_k)$  for all  $k$ , then  $\tilde{\psi}_j(\delta_i') = \phi_i(\delta_i) = \bar{1}$ , and so  $\tilde{\delta}_j < \delta_i$ . Suppose conversely that  $\tilde{\delta}_j < \delta_i$ , so that  $\tilde{\psi}_j(\delta_i') = \bar{1}$ , and consider the map  $\theta: \bar{A} \rightarrow \bar{K}$  defined by

$$\bar{A} \rightarrow \bar{A}/\bar{T} \cong \bar{A}' \xrightarrow{\tilde{\psi}_j} \bar{K}.$$

Then  $\theta$  is surely a linear character on  $\bar{A}$ , and thus  $\theta$  must coincide with a linear character  $\phi_l$  for some  $l$ . In that case

$$\phi_l(\delta_i) = \tilde{\psi}_j(\delta_i') = \bar{1},$$

proving that  $l = i$  and establishing the fact that  $\phi_i(C_k) = \tilde{\psi}_j(C'_k)$  for all  $k$ . Thus the proof is completed.

(87.17) **COROLLARY.**  $\delta_i' = 0$  if and only if  $\phi_i(C_n) \neq 0$  for some  $n$  such that  $C'_n = 0$ .

**PROOF.** If  $\delta_i' \neq 0$ , then  $\delta_i > \tilde{\delta}_j$  for some  $j$ , and hence  $\phi_i(C_n) = \tilde{\psi}_j(C'_n) = 0$  whenever  $C'_n = 0$ . On the other hand, suppose  $\delta_i' = 0$ ; then (using (86.13))

$$0 = \delta_i' = \sum_{n=1}^s \tilde{b}_{in} C'_n,$$

and thus  $\bar{b}_{in} = 0$  whenever  $C'_n \neq 0$ . This implies that

$$\delta_i = \sum_{n=1}^s \bar{b}_{in} C_n = \sum_{\substack{1 \leq n \leq s \\ C'_n = 0}} \bar{b}_{in} C_n,$$

and consequently

$$I = \psi_i(\delta_i) = \sum_{\substack{1 \leq n \leq s \\ C'_n = 0}} \bar{b}_{in} \psi_i(C_n).$$

Therefore  $\psi_i(C_r) \neq 0$  for at least one  $n$  for which  $C'_n = 0$ , and the corollary is proved.

In (87.1) we have defined defect groups of  $p$ -regular classes of  $G$ . We are now ready to associate defect groups with the blocks of  $\bar{K}G$ .

(87.18) **DEFINITION.** To each block  $B_j$  of defect  $d_j$  there corresponds [because of (86.26)] a  $p$ -regular class  $\mathfrak{C}_n$  of defect  $d_j$  such that  
(87.19) 
$$\bar{b}_{jn} \psi_j(C_n) \neq 0,$$

where  $b_{jn}$  is defined by (86.13), and where  $\psi_j$  is the linear character associated with the block  $B_j$ . Any defect group  $H_n$  of the class  $\mathfrak{C}_n$  is called a *defect group* of the block  $B_j$ .

Although the defect group of a class is determined up to conjugacy, it is by no means clear that the defect group of a block is unique up to conjugacy, since (87.19) may hold for more than one  $p$ -regular class  $\mathfrak{C}_n$ . The next result will imply (among other things) that the defect groups of a block are uniquely determined up to conjugacy.

(87.20) **THEOREM.** Let  $H_k$  be a defect group for the block  $B_j$ . Then  $\bar{b}_{jn} \neq 0$  implies that  $H_n \subset_c H_k$ .

**PROOF.** In (87.11) through (87.16), take  $H = H_n$ , and suppose that  $H_n \subset_c H_k$  is false. By Lemma 87.12, we conclude that  $C'_k = 0$ . But by (87.17) we then deduce that  $\delta'_j = 0$  because  $\psi_j(C_k) \neq 0$ . As in the proof of (87.17), from the fact that  $\delta'_j = 0$ , we may conclude that  $\bar{b}_{jn} = 0$  whenever  $C'_n \neq 0$ . But by (87.12) we have  $C'_n \neq 0$ , and hence  $\bar{b}_{jn} = 0$ . This completes the proof.

(87.21) **COROLLARY.** The defect group of a block is uniquely determined up to conjugacy.

(87.22) **COROLLARY.** Let  $H_k$  be a defect group of the block  $B_j$ . Then

$$\delta_j = \sum_{\substack{1 \leq n \leq r \\ H_n \subset_c H_k}} \bar{b}_{jn} C_n ,$$

and

$$\sum_{\substack{1 \leq n \leq r \\ H_n = H_k}} \bar{b}_{jn} \psi_j(C_n) = \bar{1} .$$

PROOF. From (86.13) and (86.14), we have

$$\delta_j = \bar{e}_j = \sum_{n=1}^r \bar{b}_{jn} C_n .$$

The first result now follows from Theorem 87.20. Since  $\bar{1} = \psi_j(\delta_j)$ , the second equality is a consequence of the first as soon as (86.22) is taken into account.

(87.23) COROLLARY. Let  $H_k$  be a defect group of the block  $B_j$  of defect  $d_j$ , and let  $B_i$  be any block of defect  $d_i$ . If

$$\sum_{\substack{1 \leq n \leq r \\ H_n = H_k}} \bar{b}_{jn} \psi_i(C_n) = \bar{1} ,$$

then  $i = j$ .

PROOF. If  $H_n$  has smaller order than  $H_k$ , then  $\psi_i(C_n) = 0$  by (86.22). We may thus rewrite the given equation as

$$\sum_{\substack{1 \leq n \leq r \\ H_n \subset_c H_k}} b_{jn} \psi_i(C_n) = \bar{1}$$

By Corollary 87.22 the left-hand side is just  $\psi_i(\delta_j)$ , and since  $\psi_i(\delta_j) = \bar{1}$ , we must have  $i = j$ . This completes the proof.

An obvious consequence is as follows:

(87.24) COROLLARY. Let  $Z_i$  and  $Z_k$  belong to blocks with the same defect group  $H$ . Then they belong to the same block if and only if  $\bar{\omega}^{(i)}(C_n) = \bar{\omega}^{(k)}(C_n)$  for all  $p$ -regular classes  $C_n$  whose defect group  $H_n$  is conjugate to  $H$ .

A bit less immediate is yet another implication of the preceding results.

(87.25) COROLLARY.  $\psi_j(C_n) \neq 0$  implies that  $H_k \subset_c H_n$  where  $H_k$  is a defect group of  $B_j$ .

PROOF. Take  $H = H_k$  in (87.11) through (87.16), and suppose  $H_k \subset_c H_n$  is false. Then by (87.12) we have  $C'_n = 0$ . By hypothesis,  $\psi_j(C_n) \neq 0$ , so we deduce that  $\delta'_j = 0$  [from Corollary 87.17]. But

$\delta'_j$  cannot be 0 since  $\bar{b}_{jk}C'_k$  is a non-zero summand of  $\delta'_j$ . This completes the proof.

We state now another preliminary result which is a special case of Theorem 88.3 of the next section. The proof is given in the first two paragraphs of the proof of that theorem and may be read at this point.

(87.26) LEMMA. *Let  $H \triangleleft G$ ,  $[H:1] = p^d$ ,  $d > 0$ . Then every block of  $\bar{K}G$  has defect  $\geq d$ .*

One last preliminary result is necessary before we can prove the main theorem.

(87.27) LEMMA. *Let  $B_j$  be a block of  $\bar{K}G$  with defect group  $H_k$  and block idempotent  $\delta_j$ . Suppose that  $\delta_j > \tilde{\delta}_i$  where  $\tilde{\delta}_i$  is the block idempotent of a block  $\tilde{B}_i$  of  $\bar{K} \cdot N(H_k)$ . Then  $H_k$  is also a defect group for  $\tilde{B}_i$ .*

PROOF. In (87.11) through (87.16), take  $H = H_k$ . Then we know from Lemma 87.12 that  $C'_k \neq 0$ . Since also  $\bar{b}_{jk} \neq 0$ , we conclude that  $\delta'_j \neq 0$ , and therefore there is at least one subordinate  $\tilde{\delta}_i$  of  $\delta_j$ . From (87.16) we obtain  $\tilde{\psi}_i(C'_k) = \psi_j(C_k) \neq 0$ , the latter because  $H_k$  is a defect group for  $B_j$ .

By Lemma 87.12 we know that  $C'_k$  is the sum of all elements in some  $p$ -regular conjugate class  $\mathfrak{C}'$  of  $N(H)$ . Let  $x \in \mathfrak{C}'$ , and let  $N'(x)$  be its normalizer in  $N(H)$ . Since  $H$  is the defect group of  $B_j$ , we may assume that  $H$  is a  $p$ -Sylow subgroup of  $N(x)$ . Then we have

$$H \subset N'(x) \subset N(x),$$

and thus  $H$  is also a  $p$ -Sylow subgroup of  $N'(x)$ . This shows that  $H$  is (up to conjugacy) a defect group of the class  $\mathfrak{C}'$ .

Now let  $H'_i$  be any defect group of the block  $\tilde{B}_i$ . Since  $\tilde{\psi}_i(C'_k) \neq 0$ , we conclude from (87.25) that  $H'_i \subset_c H$ . On the other hand,  $H \triangleleft N(H)$ , and  $H$  is a  $p$ -group, and so by (87.26) we have  $[H:1] \mid [H'_i:1]$ . This shows that  $H'_i =_c H$  and completes the proof.

(87.28) COROLLARY.  *$H_k$  is a maximal normal  $p$ -subgroup of  $N(H_k)$ .*

PROOF. The preceding lemma shows that  $H_k$  is a defect group of a block of  $\bar{K} \cdot N(H_k)$ . By Lemma 87.26 we therefore know that the order of  $H_k$  is a multiple of the order of any normal  $p$ -subgroup of  $N(H_k)$ , and this gives the result.

We may now prove the main result of this section.

(87.29) THEOREM (Brauer [13], [16], [27]; Osima [6]). *There is a one-to-one correspondence between the blocks of  $\bar{K}G$  with defect*

group  $H$  and the blocks of  $\bar{K} \cdot N(H)$  with defect group  $H$ .

PROOF. Let  $B_1, \dots, B_n$  be the blocks of  $\bar{K}G$  with defect group  $H$ . We showed in (87.27) that for each  $\delta_j, 1 \leq j \leq n$ , there is at least one block  $\tilde{B}_i$  of  $\bar{K} \cdot N(H)$  such that  $\delta_j > \tilde{\delta}_i$  and such that  $H$  is also the defect group of  $\tilde{B}_i$ . On the other hand, let  $\tilde{B}$  be any block of  $\bar{K} \cdot N(H)$  with defect group  $H$ , and let  $\tilde{\delta}$  be its block idempotent,  $\tilde{\psi}$  its linear character. Since  $\tilde{\delta} = \delta'_1 + \dots + \delta'_t$ , it follows that  $\tilde{\delta}$  is a summand of some  $\delta'_i, 1 \leq i \leq t$ , and so  $\tilde{\delta} < \delta_i$  for some  $i, 1 \leq i \leq t$ . Let us show that  $B_i$  has defect group  $H$ , so that  $B_i$  is one of the blocks  $B_1, \dots, B_n$ . Suppose that  $B_i$  has defect group  $D$ , a  $p$ -Sylow subgroup in  $N(x_i)$ . Since  $H$  is a defect group, we may write  $H = p$ -Sylow subgroup in  $N(x_k)$ , and we have shown in (87.12) that  $C'_k$  is just a class sum in  $N(H)$ . We now have (since  $H$  is a defect group for  $\tilde{B}$ )

$$\psi_i(C_k) = \tilde{\psi}(C'_k) \neq 0,$$

so that by (87.25) we have  $D \subset_c H$ . On the other hand, we have

$$\tilde{\psi}(C'_l) = \psi_i(C_l) \neq 0$$

since  $D$  is a defect group for  $B_i$ , and therefore [again using (87.25)] the defect group  $H$  of  $\tilde{B}$  is contained in a conjugate of the normalizer of  $x_l$  in  $N(H)$  for the above  $x_l$ . The normalizer of  $x_l$  in  $N(H)$  is just  $N(x_l) \cap N(H)$ , and since  $D$  is a  $p$ -Sylow subgroup of  $N(x_l)$ , we deduce from  $H \subset_c N(x_l) \cap N(H)$  that  $[H:1] \mid [D:1]$ . Hence  $H =_c D$ , and so  $B_i$  has defect group  $H$ .

In order to complete the proof, we need show only that for each  $\delta_i, 1 \leq i \leq n$ , there is only one block idempotent of  $\bar{K} \cdot N(H)$  subordinate to  $\delta_i$ . Suppose (to fix the notation) that both  $\tilde{\delta}_1 < \delta_1$  and  $\tilde{\delta}_m < \delta_1$ . By Lemma 87.16 we have  $\tilde{\psi}_1(C'_l) = \tilde{\psi}_m(C'_l)$  for  $1 \leq l \leq s$ . Now let  $\mathfrak{C}'$  be any  $p$ -regular class in  $N(H)$  with defect group  $H$ . By (87.12), we know that  $\mathfrak{C}' = \mathfrak{C}_k \cap N(H)$  for some  $p$ -regular class  $\mathfrak{C}_k$  of defect group  $H$ , and that  $C'_k$  is just a class sum in  $N(H)$ . Therefore we have shown that  $\tilde{\psi}_1(C'_k) = \tilde{\psi}_m(C'_k)$ , where  $C'_k$  is the class sum in  $N(H)$  of any  $p$ -regular class of  $N(H)$  with defect group  $H$ . It follows from (87.23) that  $m = 1$ , and the theorem is proved.

This result enables us to work with the group  $N(H)$  rather than  $G$  when we are trying to determine the blocks of  $\bar{K}G$  with defect group  $H$ . The advantage of this is that  $H \triangleleft N(H)$ , and as we shall see in §88, the determination of the blocks of a group is considerably simplified by the existence of a normal  $p$ -subgroup.

*Exercises*

1. If  $x \in C_G(H)$  and  $y \in N(H)$ , prove that  $y^{-1}xy \in C_G(H)$ . From this, deduce that  $H \cdot C_G(H) \Delta N(H)$ .

2. (Osima [6]). Prove that, for fixed  $n$ , the sum

$$\sum_{t_1 \leq t \leq n} \bar{K}C_t$$

is an ideal in the center of  $\bar{K}G$ . Furthermore, for fixed  $j$  the sum

$$\sum_{\substack{1 \leq t \leq s \\ H_t \subset H_j \\ c}} \bar{K}C_t$$

is an ideal in the center of  $\bar{K}G$ .

3. If  $G$  is a  $p$ -group, show that  $\bar{K}G$  contains only one block.

### § 88. Block Theory for Groups with Normal $p$ -Subgroups

We have seen in § 87 how the problem of determining the blocks of a group can be reduced to a corresponding problem for another group which has a normal  $p$ -subgroup. We shall consider here what additional information is obtainable from the existence of such normal  $p$ -subgroups. The results in this section are due to Brauer [27].

Throughout this section, we let  $H \triangle G$ ,  $[H:1] = p^b$ ,  $b \geq 0$ , and we keep the notations of § 85. Write  $G^* = G/H$ , and let  $x^* \in G^*$  denote the image of  $x \in G$ . The mapping  $G \rightarrow G^*$  induces an algebra homomorphism of  $\bar{K}G$  onto  $\bar{K}G^*$ , and this homomorphism maps the center  $\bar{A}$  of  $\bar{K}G$  into the center  $A^*$  of  $\bar{K}G^*$ . We shall show how this permits us to assign to each block  $B$  of  $\bar{K}G$  a collection of blocks  $\{B_i^*\}$  of  $\bar{K}G^*$ .

Let  $z \in \bar{K}G$  map onto  $\hat{z} \in \bar{K}G^*$  under the homomorphism induced by  $G \rightarrow G^*$ . If  $\bar{I} = \delta_1 + \cdots + \delta_t$  is the decomposition of  $\bar{I}$  into block idempotents of  $\bar{K}G$ , then clearly

$$\bar{I} = \hat{\delta}_1 + \cdots + \hat{\delta}_t,$$

and these  $\{\hat{\delta}_i\}$  are orthogonal central idempotents in  $\bar{K}G^*$  (except that some of them may be zero). Let us show at once that each  $\hat{\delta}_i \neq 0$ . For fixed  $i$ , let  $F$  be an irreducible  $\bar{K}G$ -module belonging to the block  $B_i$  of  $\bar{K}G$ . By (85.4), we have  $F(\delta_i) \neq 0$ . By Clifford's theorem 49.2 and Theorem 27.28, it follows that  $F(h) = I$  for  $h \in H$ , and so  $F$  induces an irreducible  $\bar{K}$ -representation  $F^*$  of  $G^*$  by means of

$$(88.1) \quad F^*(x^*) = F(x), \quad x \in G.$$

Then  $F^*(\hat{\delta}_i) = F(\delta_i) \neq 0$ , which proves that  $\hat{\delta}_i \neq 0$ .

It follows from the above that each  $\hat{\delta}_i$  is a sum of block idempotents  $\{\delta_j^*\}$  of  $\bar{K}G^*$ , called the *subordinates* of  $\delta_i$ . We shall say that  $\delta_i$  *dominates* each of its subordinates  $\delta_j^*$  and shall write  $\delta_i > \delta_j^*$ ,  $\delta_j^* < \delta_i$ . (We use a corresponding notation for the blocks themselves.) The preceding discussion shows that  $\delta_i > \delta_j^*$  if and only if (88.1) holds for each  $F \in B_i$  and each  $F^* \in B_j^*$ .

On the other hand, we may characterize the above connection between blocks of  $G$  and  $G^*$  by means of the respective linear characters  $\{\psi\}$  and  $\{\psi^*\}$ . It is clear that  $\delta_i > \delta_j^*$  if and only if  $\psi_j^*(\hat{\delta}_i) = \bar{1}$ . We use this to prove

(88.2) LEMMA. *Let  $B$  be a block of  $\bar{K}G$  with linear character  $\psi$ , let  $B^*$  be a block of  $\bar{K}G^*$  with linear character  $\psi^*$ , and let  $\tau: \bar{A} \rightarrow \bar{A}^*$  be the homomorphism induced by  $G \rightarrow G^*$ . Then  $B > B^*$  if and only if  $\psi = \psi^*\tau$ .*

PROOF. Let  $B^*$  be a block of  $\bar{K}G^*$ , and suppose that  $B^* < B_i$ , so that  $\psi^*(\hat{\delta}_i) \neq 0$ . Now  $\psi^*\tau$  is a non-zero algebra homomorphism of  $\bar{A}$  into  $\bar{K}$ , and by the results of § 85, we must have  $\psi^*\tau = \psi_j$  for some  $j$ . Then

$$\psi_j(\delta_i) = \psi^*\tau(\delta_i) = \psi^*(\hat{\delta}_i) \neq 0,$$

which implies that  $i = j$ . This proves that if  $B^* < B_i$ , then  $\psi^*\tau = \psi_i$ .

Conversely,  $\psi^*\tau = \psi_i$  implies  $\bar{1} = \psi_i(\delta_i) = \psi^*(\hat{\delta}_i)$ , and so  $B_i > B^*$ . This completes the proof.

The first main result of this section gives a sharpened form of Lemma 87.26.

(88.3) THEOREM. *The defect group of any block of  $\bar{K}G$  contains a conjugate of  $H$ , and so the defect of any block must be  $\geq b$ . If  $B$  and  $B^*$  are blocks of  $\bar{K}G$  and  $\bar{K}G^*$ , respectively, with defects  $d$  and  $d^*$  and defect groups  $D$  and  $D^*$ , and if  $B > B^*$ , then  $D^* \subset_c DH/H$  and  $d^* \leq d - b$ . Furthermore, there exists at least one  $B^*$  subordinate to  $B$  for which  $d^* = d - b$ .*

PROOF. Let  $\psi$  be the linear character defining the block  $B$ . Then we may take  $D$  to be a  $p$ -Sylow subgroup of  $N(x_i)$ , where  $x_i \in \mathbb{C}_i$  and  $\psi(C_i) \neq 0$ , and we have  $[D:1] = p^a$ . Let  $B > B^*$ , and let  $\psi^*$  be the linear character associated with  $B^*$ , so that  $\psi^*(\hat{C}_i) = \psi(C_i) \neq 0$ .

Since  $C_i$  is a sum of  $g/n_i$  conjugates of  $x_i$ , it is clear that  $\hat{C}_i$  is a sum of conjugates of  $x_i^*$ . Because  $\hat{C}_i \in \bar{A}^*$ , each conjugate of  $x_i^*$

(in  $G^*$ ) occurs with the same multiplicity in  $\hat{C}_i$ . Now  $x_i^*$  has  $p^{-b}g/n_i^*$  distinct conjugates, where  $n_i^* = \text{order of } N(x_i^*)$ , and their sum  $C_i^*$  is the class sum for  $x_i^*$ . Therefore

$$\hat{C}_i = \frac{g/n_i}{g/n_i^* p^b} C_i^* = \frac{n_i^* p^b}{n_i} C_i^*,$$

which shows incidentally that  $n_i^* p^b / n_i \in \mathbb{Z}$ . We now have

$$0 \neq \psi^*(\hat{C}_i) = \frac{n_i^* p^b}{n_i} \psi^*(C_i^*)$$

where the coefficient is taken modulo  $p$ . This proves that  $n_i^* p^b / n_i$  is not divisible by  $p$  and also that  $\psi^*(C_i^*) \neq 0$ .<sup>†</sup>

We observe next that  $N(x_i)H/H$  is a subgroup of  $N(x_i^*)$ , and so its order divides  $n_i^*$ . If we set  $m_i = \text{order of } N(x_i) \cap H$ , then

$$[N(x_i)H : H] = [N(x_i) : N(x_i) \cap H] = n_i/m_i,$$

and furthermore  $m_i \mid p^b$  since  $N(x_i) \cap H$  is a subgroup of  $H$ . But

$$\frac{n_i^* p^b}{n_i} = \frac{p^b}{m_i} \cdot \frac{n_i^*}{n_i/m_i},$$

and the left-hand side is not a multiple of  $p$ , so that we must have  $m_i = p^b$ . This implies that  $H \subset N(x_i)$ . Since  $H$  is a  $p$ -group contained in  $N(x_i)$ , it follows from (6.6) that  $H \subset_c D$ , which proves the first statement in the theorem.

Continuing with the proof, we find from (87.25) that since  $\psi^*(C_i^*) \neq 0$ , we have  $D^* \subset_c H_i^*$  where  $H_i^*$  is a  $p$ -Sylow subgroup of  $N(x_i^*)$ . The preceding argument shows that any  $p$ -Sylow subgroup of  $N(x_i)/H$  is also a  $p$ -Sylow subgroup of  $N(x_i^*)$ . Furthermore we have

$$\frac{[N(x_i) : H]}{[DH : H]} = \frac{[N(x_i) : 1]}{[DH : 1]} = \frac{[N(x_i) : D]}{[DH : D]},$$

since  $p \nmid [N(x_i) : D]$ , this proves that  $DH/H$  is a  $p$ -Sylow subgroup of  $N(x_i)/H$ . Therefore  $D^* \subset_c DH/H$ , and from this, we find readily that  $d^* \leq d - b$ .

Finally, choose  $F \in B$  so that  $\nu(f) = e - d$ . Then  $F^* \in B^*$  for some subordinate  $B^*$  of  $B$ , and so  $d^* \geq \nu(p^{-b}g) - \nu(f) = d - b$ . But we already know that  $d^* \leq d - b$ , and therefore  $d^* = d - b$ . This completes the proof.

<sup>†</sup> Since  $n_i^* p^b / n_i$  is not a multiple of  $p$ , we have  $d = \nu(n_i) \geq b$ . and thus Lemma 87.26 is established.

We are now ready to improve the result of Corollary 87.22 by taking advantage of the hypotheses of this section.

(88.4) THEOREM. *Let  $B_j$  be a block of  $\bar{K}G$  with defect group  $H$ . Then its block idempotent  $\delta_j$  is given by*

$$\delta_j = \sum_{\substack{1 \leq n \leq r \\ H_n = H}} \bar{b}_{jn} C_n .$$

PROOF. In (87.11) through (87.16), choose  $H$  to be the  $H$  of this section. Then  $N(H) = G$ , and so for each  $i$ ,  $1 \leq i \leq s$ , either  $C'_i = C_i$  or  $C'_i = 0$ . By Lemma 87.12 we have  $C'_i = C_i$  if and only if  $H \subset_c H_i$ .

We show next that  $\delta'_j = \delta_j$  for  $1 \leq j \leq t$ . By (87.22), we may write

$$\delta_j = \sum_{\substack{H_n \subset H \\ c}} \bar{b}_{jn} C_n , \quad \delta'_j = \sum_{\substack{H_n \subset H \\ c}} \bar{b}_{jn} C'_n$$

where  $1 \leq n \leq r$  in each summation. Since  $C'_n = 0$  unless  $H \subset_c H_n$ , we may rewrite the latter formula as

$$\delta'_j = \sum_{\substack{1 \leq n \leq r \\ H_n = H \\ c}} \bar{b}_{jn} C_n ,$$

and so

$$\psi_j(\delta'_j) = \sum_{\substack{1 \leq n \leq r \\ H_n = H \\ c}} \bar{b}_{jn} \psi_j(C_n) = \bar{I}$$

by (87.22). But by Theorem 87.29 we know that  $\delta'_j$  is a block idempotent of  $\bar{K} \cdot N(H)$ , that is, of  $\bar{K}G$ . Then  $\psi_j(\delta'_j) = \bar{I}$  shows that  $\delta_j = \delta'_j$ . Finally, since  $H \triangle G$ ,  $H_n =_c H$  implies  $H_n = H$ , and the theorem is proved.

Next we shall show how the problem of finding the blocks of  $\bar{K}G$  with defect group  $H$  can be reduced to a problem involving the blocks of defect 0 of  $W^* = W/H$  where  $W = H \cdot C_G(H)$ . Since  $H \triangle G$ , it is easily seen that also  $W \triangle G$ . We shall now establish a one-to-one correspondence between blocks of  $\bar{K}G$  with defect group  $H$  and collections of  $G^*$ -conjugate irreducible  $K$ -characters  $\{\theta_i\}$  of  $W^*$ , each  $\theta_i$  belonging to a block of  $\bar{K}W^*$  of defect 0, and the number  $n$  of distinct conjugates in each collection satisfying  $\nu(n) = \nu([G:W])$ .

To begin with, we recall some results from §49. Let  $\theta$  be any  $K$ -character of  $W$ . For fixed  $y \in G$  define

$$\theta'(x) = \theta(yxy^{-1}) , \quad x \in W .$$

Then  $\theta'$  is a  $G$ -conjugate of  $\theta$ , has the same degree as  $\theta$ , and is

again a  $K$ -character of  $W$ . The inertia group  $I_G(\theta)$  consists of all  $y \in G$  for which  $\theta'$  coincides with  $\theta$ . Then  $W \subset I_G(\theta) \subset G$ , and the number of distinct  $G$ -conjugates of  $\theta$  is  $[G : I_G(\theta)]$ . If  $\theta$  belongs to a block of defect 0, so does each of its  $G$ -conjugates.

We note further that if the representation of  $W$  whose character is  $\theta$  maps each  $h \in H$  onto  $I$ , this representation induces a representation of  $W^* = W/H$ , and so  $\theta$  may be viewed as a character of  $W^*$ . It is easily found that the inertia group  $I_{G^*}(\theta)$  gotten from considering  $\theta$  as a character of  $W^*$  is given by  $I_{G^*}(\theta) = I_G(\theta)/H$ . This shows that

$$[G^* : I_{G^*}(\theta)] = [G : I_G(\theta)],$$

and so in computing the distinct conjugates of  $\theta$ , we may work equally well in  $G$  or in  $G^*$ . Finally we observe that this entire procedure could be reversed if we started with a character  $\theta$  of  $W^*$ .

Suppose now that  $B$  is a block of  $\bar{K}G$  with defect group  $H$ . By Theorem 88.3 we have  $B > B^*$  for some block  $B^*$  of  $\bar{K}G^*$ , and  $B^*$  has defect 0. Let  $Z$  be the unique irreducible  $K$ -representation of  $G^*$  belonging to  $B^*$ ; let  $\zeta$  be its character and  $z = \zeta(1)$  its degree. Then

$$(88.5) \quad \nu(z) = \nu([G^*: 1]) = e - b.$$

The representation  $Z$  induces a representation of  $G$ , also denoted by  $Z$ , by setting

$$Z(x) = Z(x^*) , \quad x \in G.$$

By Exercise 88.2, we know that  $Z \in B$ . Let  $\omega$  be defined as in (85.13), so that

$$\omega(C_j) = \frac{g\zeta(x_j)}{zn_j} , \quad 1 \leq j \leq s.$$

Since  $H$  is the defect group of  $B$ , there exists a  $p$ -regular class  $C_j$  for which  $\omega(C_j) \neq 0$ , such that  $H$  is a  $p$ -Sylow subgroup of  $N(x_j)$ . This latter condition implies that  $x_j \in C_G(H) \subset W$ .

By Theorem 49.7 we may write

$$(88.6) \quad \zeta|W = q(\theta_1 + \cdots + \theta_n)$$

where the  $\{\theta_i\}$  are mutually  $G$ -conjugate distinct irreducible  $K$ -characters of  $W$  and  $n = [G : I_G(\theta_1)]$ . Since  $Z(h) = I$  for each  $h \in H$ , we see that the representations of  $W$  whose characters are the  $\{\theta_i\}$  also map each  $h \in H$  onto the identity matrix and thus induce representations of  $W^*$ . Therefore each  $\theta_i$  may also be viewed as an irreducible character of  $W^*$ . We shall show now that  $p \nmid q$ ,

$p \nmid [I_G(\theta_1): W]$ , and that  $\theta_1$  (and hence  $\theta_i$ ) belongs to a block of  $W^*$  of defect 0. We have  $\overline{\omega(C_j)} \neq 0$  and hence

$$\nu(g) + \nu(\zeta(x_j)) = \nu(z) + \nu(n_j).$$

Using (88.5) and the fact that  $\nu(n_j) = b$ , we obtain  $\nu(\zeta(x_j)) = 0$ . But since  $\zeta(x_j) = q \sum \theta_i(x_j)$ , we conclude that  $p \nmid q$ . Next we observe that  $\theta_1$  is a character on  $W^*$ , and so, setting  $m = \theta_1(1)$ , we have  $\nu(m) \leq \nu(w) - b$ , where  $w = [W:1]$ . But also

$$z = \zeta(1) = qn\theta_1(1) = qnm,$$

which yields

$$\nu(m) = \nu(z) - \nu(n) = e - b - \nu(n).$$

These relations imply that  $e \leq \nu(w) + \nu(n)$ , and therefore  $e = \nu(w) + \nu(n)$ . This shows first that  $\nu(n) = \nu([G: W])$ , and second that  $\nu(m) = \nu(w) - b$ . From the latter equation, we may deduce at once that  $\theta_1$  belongs to a block of  $W^*$  of defect 0.

Conversely, let  $\theta$  be a  $K$ -character of  $W^*$  belonging to a block of defect 0, and let  $n = [G^*: I_{G^*}(\theta)]$  be the number of distinct  $G^*$ -conjugates of  $\theta$ . We assume that  $\nu(n) = \nu([G^*: W^*]) = \nu([G: W])$ . Setting  $m = \theta(1)$ , we have  $\nu(m) = \nu(w) - b$ . We now view  $\theta$  as a  $K$ -character of  $W$  afforded by a representation which maps each  $h \in H$  onto the identity matrix. If  $\theta_1 (= \theta), \theta_2, \dots, \theta_n$  are the distinct  $G^*$ -conjugates of  $\theta$ , they are also the distinct  $G$ -conjugates of  $\theta$ .

Form the induced character  $\theta^G$  [see (38.3)] defined by

$$\theta^G(x) = w^{-1} \sum_{y \in G} \theta(yxy^{-1}), \quad x \in G,$$

where  $\theta$  coincides with  $\theta$  on  $W$  and vanishes outside  $W$ . For  $x \in W$ , the above may be rewritten as

$$\theta^G(x) = [I_G(\theta): W]\{\theta_1(x) + \dots + \theta_n(x)\}, \quad x \in W.$$

If  $\zeta$  is any irreducible  $K$ -character of  $G$  which occurs in  $\theta^G$ , then in the decomposition (88.6) the same  $\{\theta_i\}$  occur as those given above. Since the representations which afford the characters  $\{\theta_i\}$  map each  $h \in H$  onto the identity matrix, the same is true for the representations affording  $\theta^G$  and  $\zeta$ , and so  $\zeta$  may be viewed as a character on  $G^*$ . If  $z = \zeta(1)$ , this proves that  $\nu(z) \leq e - b$ . An easy calculation shows then that  $\nu(z) = e - b$  and  $\nu(q) \neq 0$ . Thus  $\zeta$  (as character of  $G^*$ ) belongs to a block  $B^*$  of defect 0.

Now let  $B$  be the block of  $\bar{K}G$  which dominates  $B^*$ , so that  $\zeta$  (as character of  $G$ ) belongs to  $B$ . In order to prove that  $B$  has de-

fect group  $H$ , it suffices to show that the defect of  $B$  is  $\leq b$ , since we already know that the defect group of  $B$  must contain  $H$ . By (86.28), we need exhibit only a  $p$ -regular class  $\mathfrak{C}_i$  of defect  $b$  such that  $\bar{\omega}(C_i) \neq 0$ , where  $\omega$  is the linear character associated with  $\zeta$ .

The characters  $\theta_1, \dots, \theta_n$  of  $W^*$  belong to blocks of defect 0, hence to distinct blocks. It follows from Exercise 89.2 that there exist  $p$ -regular elements  $\hat{a}_1, \dots, \hat{a}_n \in W^*$  such that the determinant

$$|\theta_i(\hat{a}_j)|_{1 \leq i, j \leq n}$$

is a unit in  $R_P$ . Let us fix  $i$ ,  $1 \leq i \leq n$ , and choose  $\alpha \in Z$  such that  $\hat{a}_i^\alpha = 1$ ,  $p \nmid \alpha$ . If we choose  $b_i \in W$  so that its image in  $W^*$  is  $\hat{a}_i$ , we have  $b_i^\alpha \in H$ . Let  $\beta \in Z$  satisfy  $\alpha\beta \equiv 1 \pmod{p^b}$ , and set  $a_i = b_i \cdot b_i^{-\alpha\beta}$ . Then it is not difficult to see that  $a_i^\alpha = 1$ , that  $\hat{a}_i$  is the image of  $a_i$ , and finally that  $N_G(a_i)/H = N_G(\hat{a}_i)$ . Therefore the class of each  $a_i$  has defect  $\geq b$ .

If  $\mathfrak{C}_j$  is the class of  $G$  containing  $a_j$ , we have (since  $zq^{-1} = nm$ )

$$(88.7) \quad \begin{aligned} \omega(C_j) &= \frac{g\zeta(a_j)}{zn_j} = \frac{gq}{zn_j} \{ \theta_1(a_j) + \dots + \theta_n(a_j) \} \\ &= \frac{g}{nmn_j} \{ \theta_1(a_j) + \dots + \theta_n(a_j) \}, \quad 1 \leq j \leq n. \end{aligned}$$

Next we observe that  $\nu(nmn_j/g) = \nu(m) + \nu(n) - \nu(g/n_j) \geq (e-b) - (e-b) = 0$ , so each  $nmn_j/g$  lies in  $R_P$ . Now

$$\sum_{i=1}^n \theta_i(a_j) = (nmn_j/g)\omega(C_j), \quad 1 \leq j \leq n,$$

and the determinant  $|\theta_i(a_j)|$  equals the determinant  $|\theta_i(\hat{a}_j)|$ , and thus is a unit in  $R_P$ . This implies that for at least one  $j$ ,  $1 \leq j \leq n$ , the expression  $(nmn_j/g)\omega(C_j)$  is a unit in  $R_P$ . For this particular  $j$ , we have  $\nu(n_j) = b$  and  $\bar{\omega}(C_j) \neq 0$ . Thus there exists an  $a_j \in G$  whose class  $\mathfrak{C}_j$  has defect  $b$  and such that  $\bar{\omega}(C_j) \neq 0$ . This completes the proof that  $B$  has defect  $b$  and defect group  $H$ .

We have now obtained a correspondence  $B \leftrightarrow \{\theta_i\}$  between blocks  $B$  of  $\bar{K}G$  with defect group  $H$  and collections of  $G^*$ -conjugate characters  $\{\theta_i\}$  of  $W^*$  belonging to blocks of defect 0, such that  $\nu(n) = \nu([G:W])$ , where  $n =$  number of distinct conjugates of  $\theta_1$ . Next we prove that another block  $B'$  of  $\bar{K}G$  with defect group  $H$  cannot give rise to the same collection  $\{\theta_i\}$  as does  $B$ . If it did, then by (88.7) (with  $x_j$  replacing  $a_j$ , where  $x_j \in W$ ) we would have  $\bar{\omega}(C_j) = \bar{\omega}'(C_j)$  for all classes  $\mathfrak{C}_j$  such that  $x_j \in W$ . (Here  $\omega'$  has the same significance for  $B'$  as  $\omega$  does for  $B$ .) Let  $\mathfrak{C}_k$  be a  $p$ -regular class such that

$H_k = {}_c H$ . Since  $H \triangle G$ , we must have  $H_k = H$ , and therefore  $x_k \in C_G(H) \subset W$ . Consequently,  $\bar{\omega}(C_k) = \bar{\omega}'(C_k)$  for each  $p$ -regular class  $C_k$  such that  $H_k = {}_c H$ , which implies [by (87.24)] that  $B = B'$ .

Finally, let  $\theta'$  be a character of  $W^*$  belonging to a block of defect 0, having  $n'$   $G$ -conjugates, where  $\nu(n') = \nu([G:W])$ ; let  $B'$  be the block of  $\bar{K}G$  which  $\theta'$  determines. We must show that if  $\theta' \neq \theta_i$ ,  $1 \leq i \leq n$ , then  $B' \neq B$ . Let  $\theta'_1, \dots, \theta'_{n'}$  denote the conjugates of  $\theta'$ ; the analogue of (88.7) holds for  $\omega'$ . From § 89, we may find  $n + n'$   $p$ -regular elements  $\{\hat{a}_k\}$  in  $W^*$  such that the  $(n + n') \times (n + n')$  determinant

$$|\theta_i(\hat{a}_k) \theta'_{i'}(\hat{a}_k)|_{\substack{1 \leq i \leq n, 1 \leq i' \leq n' \\ 1 \leq k \leq n+n'}}$$

is a unit in  $R_P$ . Using (88.7) for  $\omega$  and  $\omega'$ , we conclude that  $\bar{\omega} \neq \bar{\omega}'$ , and so  $B \neq B'$ . We have thus proved that  $B \leftrightarrow \{\theta_i\}$  is a one-to-one correspondence, thereby completing the proof of the statement made after Theorem 88.4.

By combining the results just obtained with the methods of § 87, it is not difficult to establish the following result;

(88.8) THEOREM. *Let  $D$  be a  $p$ -subgroup of  $G$ , say  $[D:1] = p^d$ , and let  $\{\theta_j\}$  be a full system of characters of  $D \cdot C_G(D)/D$  belonging to blocks of defect 0, and such that  $p \nmid [I_j : DC_G(D)]$  for each  $j$ , where  $I_j/D$  is the inertia group of  $\theta_j$  in  $N(D)/D$ . From this system  $\{\theta_j\}$ , choose a subsystem  $\{\theta_i\}$  no two characters of which are conjugate relative to  $N(D)/D$ . To each  $\theta_i$  in the subsystem, there corresponds a block  $B_i$  of  $\bar{K}G$  with defect group  $D$ , and these give all blocks of  $\bar{K}G$  with defect group  $D$ . Different  $\theta$ 's in the subsystem give different blocks.*

PROOF. We refer the reader to Brauer [27, I, pp. 437–439] for details.

### Exercises

1. If  $C_G(H)$  is a  $p$ -group, then  $\bar{K}G$  has only one block. [Hint: Using the notation of the proof of Theorem 88.4, show that each  $C'_i$  lies in  $\bar{K} \cdot C_G(H)$ , and so each  $\delta'_m$  is an idempotent in the center of  $\bar{K} \cdot C_G(H)$ . Since  $C_G(H)$  is a  $p$ -group, there is only one central idempotent in  $\bar{K} \cdot C_G(H)$ .]

2. Let  $W$  be an irreducible  $K$ -representation of  $G^*$  belonging to the block  $B^*$  of  $\bar{K}G$ , and let  $Z$  be the  $K$ -representation of  $G$  defined by  $Z(x) = W(x^*)$ ,  $x \in G$ . Show that  $Z$  belongs to a block  $B$  of  $\bar{K}G$  such that  $B > B^*$ .

### § 89. Block Distribution of Classes

We shall give here Brauer's method of assigning  $p$ -regular classes of  $G$  to the blocks of  $\bar{K}G$ . This method yields new proofs of some of the earlier results, and in some cases gives significant improvements of those results. We continue to use the notation of §§ 84–86.

We had defined

$$(89.1) \quad \emptyset = (\varphi_j^{(i)})^{r \times r}$$

and had proved in § 84 that  $\emptyset$  is unimodular over  $R_P$ . The Brauer characters  $\varphi^{(1)}, \dots, \varphi^{(r)}$  were assigned to the blocks  $B_1, \dots, B_t$  of  $\bar{K}G$  so that the first  $y_1$  of them belong to  $B_1$ , the next  $y_2$  to  $B_2$ , and so on, with

$$y_1 + \cdots + y_t = r.$$

The Laplace expansion of  $\det \emptyset$  gives

$$\det \emptyset = \sum \pm A_1 \cdots A_t$$

where  $A_j$  denotes the general  $y_j \times y_j$  minor of  $\emptyset$  formed by using entries in those rows where  $\varphi^{(i)} \in B_j$ . Since  $\det \emptyset \notin P$ , at least one term  $A_1 \cdots A_t$  is a unit in  $R_P$ . Renumbering the classes if need be, we may hereafter assume that  $A_1, \dots, A_t$  are principal minors of  $\emptyset$ . Thus

$$\emptyset = \begin{bmatrix} \emptyset_{11} & \cdots & \emptyset_{1t} \\ \cdot & \cdots & \cdot \\ \emptyset_{t1} & \cdots & \emptyset_{tt} \end{bmatrix}$$

where each  $\emptyset_{jj}$  is a  $y_j \times y_j$  matrix unimodular over  $R_P$ . We shall say that the  $y_j$   $p$ -regular classes of  $G$  whose subscripts appear in  $\emptyset_{jj}$  belong to the block  $B_j$ . This distribution of classes is usually *not* unique, and in what follows we deal with some fixed distribution. We write  $\mathfrak{C}_i \in B_j$  to indicate that  $\mathfrak{C}_i$  belongs to  $B_j$ .

As usual, let  $h_i = \text{defect of } \mathfrak{C}_i$ . From (84.10) and (84.17) we have

$$(89.2) \quad \text{el. div. } C = \{p^{h_1}, \dots, p^{h_r}\}$$

and thus

$$\det C = \prod_{i=1}^r p^{h_i}.$$

Now we show that the contribution to  $\det C$  from  $C_j$  comes from the classes belonging to  $B_j$ .

(89.3) THEOREM. *For each block  $B_j$ , we have*

$$\text{el. div. } C_j = \{p^{h_i} : \mathfrak{C}_i \in B_j\}.$$

PROOF. We shall begin by proving that

$$(89.4) \quad \det C_j \geq \prod_{\mathfrak{C}_i \in B_j} p^{h_i}, \quad 1 \leq j \leq t.$$

From this, it will follow by use of (89.2) that equality must hold. For the moment, set

$$L_j = \left( \frac{\eta_k^{(i)}}{n_k} \right)_{\eta^{(i)} \in R_j, \mathfrak{C}_k \in B_j}.$$

Theorem 84.14 shows that each entry of  $L_j$  lies in  $R_P$ , and thus also  $\det L_j \in R_P$ . On the other hand,

$$(89.5) \quad L_j = C_j \Phi_{jj} \text{diag} \{n_k^{-1} : \mathfrak{C}_k \in B_j\},$$

so that

$$\det L_j = (\det C_j)(\det \Phi_{jj}) \prod_{\mathfrak{C}_k \in B_j} n_k^{-1}.$$

This at once implies (89.4) since  $\det \Phi_{jj}$  is a unit in  $R_P$ . As we have remarked above, equality must hold in (89.4), and consequently  $L_j$  is unimodular over  $R_P$ . But then, from (89.5) and (16.22), it follows that the elementary divisors of  $C_j$  are just the powers of  $p$  in  $\{n_k : \mathfrak{C}_k \in B_j\}$ . This proves the result.

Using this, we may give a new proof of (86.27). Suppose that  $Z_i \in B_j$  where  $B_j$  has defect  $d_j$ . By Lemma 86.22, we already know that  $\bar{\omega}^{(i)}(C_k) = 0$  whenever  $h_k < d_j$ , and we need prove only that  $\bar{\omega}^{(i)}(C_l) \neq 0$  for some  $p$ -regular class  $\mathfrak{C}_l$  of defect  $d_j$ . We have

$$z_i \omega^{(i)}(C_k) = \zeta_k^{(i)} g_k,$$

which gives

$$\text{diag} \{z_1, \dots, z_s\} \cdot (\omega^{(i)}(C_k))^{s \times r} = D \Phi \cdot \text{diag} \{g_1, \dots, g_r\}.$$

Restricting ourselves to  $Z$ 's and  $\mathfrak{C}$ 's belonging to  $B_j$ , this yields

$$(89.6) \quad \text{diag} \{z_i : Z_i \in B_j\} \cdot Q_j = D_j \Phi_{jj} \cdot \text{diag} \{g_i : \mathfrak{C}_i \in B_j\}$$

where

$$Q_j = (\omega^{(i)}(C_k))_{Z_i \in B_j, \mathfrak{C}_k \in B_j}.$$

Since  $\nu(z_i) \geq e - d_j$  for all  $Z_i \in B_j$ , each entry on the left-hand side of (89.6) is a multiple of  $p^{e-d_j}$ . Both  $D_j$  and  $\Phi_{jj}$  are unimodular over  $R_P$ , and hence for each  $i$  such that  $\mathfrak{C}_i \in B_j$  we have  $p^{e-d_j} | g_i$ . In other words, we have shown that

$$(89.7) \quad \nu(n_i) \leq d_j \quad \text{if } \mathfrak{C}_i \in B_j, d_j = \text{defect of } B_j.$$

By Theorem 89.3, this shows that the maximal elementary divisor of  $C_j$  is at most  $p^{d_j}$ . Using Theorem 86.7 we conclude that the maximal elementary divisor of  $C_j$  is precisely  $p^{d_j}$ . The above discussion then shows that  $\bar{Q}_j \neq 0$ , and so we must have  $\bar{\omega}^{(i)}(C_k) \neq 0$  for some  $Z_i \in B_j$  and some  $\mathfrak{C}_k \in B_j$ . Of necessity,  $\mathfrak{C}_k$  has defect  $d$ . Finally, for any  $Z_i \in B_j$ , we have  $\bar{\omega}^{(i)}(C_k) = \bar{\omega}^{(i)}(C_k) \neq 0$ , which completes this new proof of (86.27).

The preceding discussion also gives

(89.8) THEOREM. *The greatest elementary divisor of  $C_j$  is  $p^{d_j}$ , and all other elementary divisors are  $< p^{d_j}$ .*

PROOF. We have already shown that  $p^{d_j}$  is the greatest elementary divisor of  $C_j$ . If another elementary divisor were  $p^{d_j}$ , then after division by  $p^{e-d_j}$ , the right-hand side of (89.6) would have  $P$ -rank  $\geq 2$ , and thus also  $\bar{Q}_j$  would have rank  $\geq 2$ . But all the rows of  $\bar{Q}_j$  are the same, since  $\bar{\omega}^{(i)} = \bar{\omega}^{(i)}$  if  $Z_i$  and  $Z_i$  belong to  $B_j$ . Thus  $\bar{Q}_j$  has rank 1, and the theorem is proved.

(89.9) COROLLARY. *Each block  $B_j$  contains a  $U_i$  with  $\nu(u_i) = e$ .*

PROOF. Use the preceding theorem together with the argument which proved (86.7).

*Remark.* We gave another proof of (89.9) in §86 [Corollary 86.20].

(89.10) COROLLARY. *If  $d_j = 0$ , then  $C_j = (1)$ .*

PROOF. Theorem 89.8 shows that if  $d_j = 0$  then  $C_j$  has a single elementary divisor, equal to 1.

*Remark.* This gives a new proof of Theorem 86.3.

### Exercises

1. Show that there exist  $r$  characters  $\zeta^{(i_1)}, \dots, \zeta^{(i_r)}$  such that

$$\begin{vmatrix} \zeta_1^{(i_1)} & \cdots & \zeta_r^{(i_1)} \\ \cdot & \cdots & \cdot \\ \zeta_1^{(i_r)} & \cdots & \zeta_r^{(i_r)} \end{vmatrix} \not\equiv 0 \pmod{P}.$$

2. Let  $\zeta^{(1)}, \dots, \zeta^{(n)}$  be a set of distinct characters belonging to blocks of defect 0. Show that there exist  $n$   $p$ -regular elements  $a_1, \dots, a_n \in G$ , lying in classes of defect 0, such that

$$\det(\zeta^{(i)}(a_j)) \not\equiv 0 \pmod{P}.$$

### § 90. Miscellaneous Topics

We shall treat briefly here a variety of topics in the theory of blocks which could not be conveniently fitted into the preceding discussion, or which could not be covered in detail because of space limitations. The notations of the earlier sections will be used throughout, unless otherwise stated.

#### § 90A. Generalized decomposition numbers

Let  $x$  be a  $p$ -singular element of  $G$  of order  $p^a$ , and form its normalizer  $N(x)$ . Let  $\zeta^{(i)}, \varphi^{(i)}$ , and so on, have the same significance for  $N(x)$  as  $\zeta^{(i)}, \varphi^{(i)}$ , and so on, have for  $G$ . We shall prove that there exist algebraic integers  $\{d_{ij}^{(x)}\}$  lying in the field  $Q(\epsilon)$ , where  $\epsilon$  is a primitive  $p^a$ th root of 1, such that for  $1 \leq i \leq s$ ,

$$(90.1) \quad \zeta^{(i)}(xy) = \sum_j d_{ij}^{(x)} \varphi^{(j)}(y), \quad y \in N(x), y \text{ } p\text{-regular.}$$

These  $\{d_{ij}^{(x)}\}$  will be called *generalized decomposition numbers* relative to  $x$ .

For each  $i$ , we may write  $\zeta^{(i)}|N(x)$  as a sum of characters  $\xi^{(k)}$  of  $N(x)$ . Let  $\hat{Z}_k$  be a matrix representation of  $N(x)$  with character  $\xi^{(k)}$ . Since  $x$  lies in the center of  $N(x)$ , we see that

$$\hat{Z}^{(k)}(x) = \epsilon_k I, \quad \epsilon_k = \text{power of } \epsilon.$$

From this, we obtain at once

$$\hat{\zeta}^{(k)}(xy) = \epsilon_k \hat{\zeta}^{(k)}(y), \quad y \in N(x).$$

But each  $\xi^{(k)}$ , when restricted to the  $p$ -regular elements of  $N(x)$ , is a  $Z$ -linear combination of the  $\{\varphi^{(j)}\}$ . Hence for  $p$ -regular  $y \in N(x)$ , each  $\zeta^{(i)}(xy)$  is a linear combination of the  $\{\varphi^{(j)}(y)\}$  with coefficients which are algebraic integers in  $Q(\epsilon)$ , and which depend only on  $x$  and not on  $y$ . This proves (90.1).

When  $x = 1$ , the generalized decomposition numbers become the ordinary decomposition numbers which were defined previously. Note also that (90.1) determines the  $\{d_{ij}^{(x)}\}$  uniquely since the characters  $\{\varphi^{(j)}\}$  are linearly independent over the complex field.

Let us denote by  $\bar{\alpha}$  the complex conjugate of the complex number  $\alpha$ , and by  $\bar{X}$  the matrix gotten from the complex matrix  $X$  by replacing each of its entries by its complex conjugate.

We now introduce the Cartan matrix  $\mathbf{C}^{(x)}$  of  $N(x)$  and the generalized decomposition matrix  $\mathbf{D}^{(x)} = (d_{ij}^{(x)})$ . If  $\hat{r}$  is the number of  $p$ -regular classes in  $N(x)$ , then  $\mathbf{C}^{(x)}$  is an  $\hat{r} \times \hat{r}$  matrix, whereas  $\mathbf{D}^{(x)}$  is of size  $s \times \hat{r}$  where  $s$  is the number of conjugate classes of  $G$ . It is easily verified (Brauer [9], [27, II]) that replacing  $x$  by a conjugate element  $x'$  does not affect the matrix  $\mathbf{D}^{(x)}$ , except possibly for a rearrangement of the columns.

(90.2) THEOREM (Brauer [9], [27, II]). *We have*

$${}^t \bar{\bar{\mathbf{D}}}^{(x)} \cdot \mathbf{D}^{(x)} = \mathbf{C}^{(x)} .$$

PROOF. Let  $y_1, \dots, y_{\hat{r}}$  be representatives of the  $p$ -regular classes of  $N(x)$ , and define

$$\mathbf{Z}^{(x)} = (\zeta^{(i)}(xy_j))_{\substack{1 \leq i \leq s \\ 1 \leq j \leq \hat{r}}}, \quad \emptyset^{(x)} = (\hat{\phi}^{(i)}(y_j))_{\substack{1 \leq i \leq \hat{r} \\ 1 \leq j \leq \hat{r}}} .$$

From (90.1), we have  $\mathbf{Z}^{(x)} = \mathbf{D}^{(x)} \emptyset^{(x)}$ . Since the normalizer  $N_G(xy_i)$  coincides with  $N_{N(x)}(y_i)$ , the orthogonality relations give

$${}^t \bar{\bar{\mathbf{Z}}}^{(x)} \mathbf{Z}^{(x)} = (\hat{n}_i \delta_{ij}) .$$

But the matrix  $(\hat{n}_i \delta_{ij})$  is just that obtained for the group  $N(x)$  if we form

$${}^t \bar{\bar{\emptyset}}^{(x)} \mathbf{C}^{(x)} \emptyset^{(x)}$$

(see Exercise 84.1). This gives

$${}^t \bar{\bar{\mathbf{Z}}}^{(x)} \mathbf{Z}^{(x)} = \bar{\bar{\emptyset}}^{(x)} \mathbf{C}^{(x)} \emptyset^{(x)} ,$$

which readily implies the result since  $\emptyset^{(x)}$  is non-singular.

(90.3) COROLLARY. *If  $x$  and  $x'$  are non-conjugate  $p$ -singular elements of  $G$ , then*

$$\sum_{m=1}^s \bar{\bar{d}}_{mi}^{(x)} d_{mj}^{(x')} = 0 \quad \text{for all } i, j .$$

PROOF. Let  $\{y'_j\}$  give the representatives of the  $p$ -regular classes of  $N(x')$ . For all  $i$  and  $j$ , we find at once that  $xy_i \neq_c x'y'_j$ , and so  ${}^t \bar{\bar{\mathbf{Z}}}^{(x)} \mathbf{Z}^{(x')} = 0$ . As above, this implies that

$${}^t \bar{\bar{\mathbf{D}}}^{(x)} \mathbf{D}^{(x')} = 0 ,$$

which yields the desired result.

For the remainder of §90A, we choose fixed representatives  $x_1, \dots, x_u$  of the  $u$   $p$ -singular classes in  $G$ , with  $x_1 = 1$ . Let  $r_i$  be the

number of  $p$ -regular classes in  $N(x_i)$ . Since each  $z \in G$  satisfies  $z =_c x_i y_j$  with uniquely determined  $i, 1 \leq i \leq u$ , and a  $p$ -regular  $y_j \in N(x_i)$  whose class is also uniquely determined, we have

$$s = r_1 + \cdots + r_u.$$

Note that  $r_i$  is the number  $r$  of  $p$ -regular classes in  $G$  and that  $D^{(x_i)}$  is the previously defined decomposition matrix  $D$  for the group  $G$ .

We now form the  $s \times s$  matrix

$$\mathbf{M} = (D^{(x_1)}, D^{(x_2)}, \dots, D^{(x_u)})$$

It is easily seen that

$$(Z^{(x_1)}, \dots, Z^{(x_u)}) = M \begin{bmatrix} \Phi^{(x_1)} & & 0 \\ & \ddots & \\ 0 & & \Phi^{(x_u)} \end{bmatrix}.$$

Since every  $z \in C$  is conjugate to some  $x_i y_j$ , as remarked above, the left-hand matrix in the above equation is (except for possible rearrangements of rows and columns) the same as the matrix  $(\zeta_j^{(i)})$  in which  $1 \leq i \leq s, 1 \leq j \leq s$ , and thus is non-singular. This proves that  $M$  is non-singular. Let us show that in fact  $(\det M)^2 = \pm$  power of  $p$ . We have

$$\begin{aligned} {}^t \bar{\bar{M}} M &= \text{diag}\{{}^t \bar{\bar{D}}^{(x_1)} D^{(x_1)}, \dots, {}^t \bar{\bar{D}}^{(x_u)} D^{(x_u)}\} \\ &= \text{diag}\{C^{(x_1)}, \dots, C^{(x_u)}\}. \end{aligned}$$

Since each  $\det C^{(x_i)}$  is a power of  $p$ , also  $(\det \bar{\bar{M}})(\det M) = \text{power of } p$ . It is easily shown that  $\bar{\bar{M}}$  and  $M$  are the same except for a permutation of columns, and thus  $\det \bar{\bar{M}} = \pm \det M$ . This proves the above assertion.

To conclude, we state without proof the following main result of Brauer [27, II, Theorem 6A], which generalizes formula (85.18). (A simplification of Brauer's proof was given by Iizuka [5].)

Let  $x$  be a  $p$ -singular element of  $G$ , and  $\phi^{(i)}$  a Brauer character of  $N(x)$  belonging to the block  $\tilde{B}$  of  $\bar{K} \cdot N(x)$ . There exists a block  $B$  of  $\bar{K}G$  which dominates  $\tilde{B}$  (see § 87), and, for each irreducible  $K$ -character  $\zeta^{(i)}$  of  $G$ , we have  $d_{ij}^{(x)} = 0$  whenever  $\zeta^{(i)} \notin B$ .

For further results on generalized decomposition numbers and for their applications to the theory of group representations, the reader may be referred to Brauer [9], [10], [11, I] and [27, II]; see also Osima [3], Iizuka [5].

1. Prove that  $Z^{(x)} \cdot (\hat{n}_t \delta_{tj})^{-1} \bar{\bar{\phi}}^{(x)} C^{(x)} = D^{(x)}$ , and therefore that

$$d_{ij}^{(x)} = \sum_{\alpha, \beta} \zeta^{(i)}(xy_\alpha) \hat{n}_\alpha \bar{\bar{\varphi}}_\alpha^{(\beta)} c_{\beta j}^{(x)}$$

where  $\{y_\alpha\}$  ranges over a set of representatives of the  $p$ -regular classes of  $N(x)$ ,  $\{\bar{\bar{\varphi}}^{(\beta)}\}$  over the irreducible Brauer characters of  $N(x)$ .

### § 90B. Conjugate characters

The irreducible complex characters  $\{\zeta^{(i)}\}$  of a group  $G$  are permuted among themselves by any automorphism of an algebraic number field containing their values. This permits us to partition the set of characters into subsets of algebraically conjugate characters in various ways. In particular, let us write  $[G:1] = g = p^e g_0$ ,  $p \nmid g_0$ , and let  $A$  be the Galois group of  $Q(\sqrt[p^e]{1})$  over  $Q(\sqrt[p^e]{1})$ . For  $\sigma \in A$ , the irreducible complex characters  $\zeta$  and  $\zeta^\sigma$  are said to be  $p$ -conjugate characters. Since the Brauer characters of  $G$  have their values in  $Q(\sqrt[p^e]{1})$ , these Brauer characters are unchanged under each  $\sigma \in A$ . Therefore  $\zeta$  and  $\zeta^\sigma$  contain the same Brauer characters, which shows that  $p$ -conjugate characters necessarily belong to the same block of  $\bar{K}G$ .

Among the characters  $\{\zeta^{(i)}\}$  belonging to a fixed block  $B$  of  $\bar{K}G$ , let  $\zeta^{(1)}, \dots, \zeta^{(n)}$  be a full set of non- $p$ -conjugate characters. Let  $m$  of the  $\varphi$ 's belong to  $B$ . If  $B$  is a block of defect 0, then of course  $m = n = 1$ . We now obtain the following improvement of Exercise 86.2.

(90.4) **THEOREM (Brauer [9]).** *If  $B$  has positive defect, then  $m < n$ .*

**PROOF.** From (85.20) we have for  $p$ -irregular  $x$  in  $G$ ,

$$(90.5) \quad \sum_{z_t \in B} d_{iz} \zeta^{(i)}(x) = 0, \quad 1 \leq j \leq m.$$

Since  $d_{iz} = d_{kj}$  whenever  $\zeta^{(i)}$  and  $\zeta^{(k)}$  are  $p$ -conjugate, if we introduce the notation

$$\lambda_i = \text{sum of the } p\text{-conjugates of } \zeta^{(i)},$$

we may rewrite (90.5) as

$$(90.6) \quad \sum_{i=1}^n d_{iz} \lambda_i(x) = 0, \quad 1 \leq j \leq m, x \in G, x \text{ } p\text{-irregular}.$$

Now let  $H$  be a  $p$ -Sylow subgroup of  $G$ , and suppose that  $\zeta^{(i)}|H$  contains the 1-character of  $H$  with multiplicity  $q_i$ . This holds also

for each of the  $t_i$   $p$ -conjugates of  $\zeta^{(i)}$ , and so  $\lambda_i|H$  contains the 1-character of  $H$  with multiplicity  $q_i t_i$ . Now introduce integer variables  $\{a_j\}$ , and set

$$d_i = \sum_{j=1}^m d_{ij} a_j, \quad 1 \leq i \leq n.$$

Define  $\chi \in \text{char}(H)$  by

$$\chi(h) = \sum_{i=1}^n d_i \lambda_i(h), \quad h \in H.$$

Then  $\chi$  contains the 1-character of  $H$  with multiplicity  $\sum_{i=1}^n d_i q_i t_i$ . From (90.6), we see that  $\chi(h) = 0$  for  $h \in H, h \neq 1$ , and thus (by orthogonality relations) the multiplicity of 1 in  $\chi$  is just  $p^{-e}\chi(1)$ , that is,  $p^{-e} \sum d_i t_i z_i$ . We have then

$$(90.7) \quad \sum_{i=1}^n d_i t_i (p^e q_i - z_i) = 0$$

for any choice of integers  $\{a_j\}$ . If only one  $d_i \neq 0$ , this would imply that  $p^e | z_i$ , and so  $B$  would be a block of defect 0, contrary to hypothesis. Thus there is no choice of integers  $\{a_j\}$  for which exactly one  $d_i \neq 0$ .

Put

$$(90.8) \quad \mathbf{D}^0 = (d_{ij})_{\substack{1 \leq i \leq n \\ 1 \leq j \leq m}}, \quad \mathbf{D}' = (d_{ij})_{\substack{1 \leq i \leq l \\ 1 \leq j \leq m}}$$

where  $l$  is the number of  $\zeta$ 's belonging to  $B$ . Since  $d_{ij} = d_{kj}$  if  $\zeta^{(i)}$  and  $\zeta^{(k)}$  are  $p$ -conjugate, the rows of  $\mathbf{D}'$  are the same as those of  $\mathbf{D}^0$ , except each row may occur more than once. Thus  $\mathbf{D}^0$  and  $\mathbf{D}'$  have the same rank, which is  $m$ . This shows that  $n \geq m$ . If  $n = m$ , we could choose integers  $\{a_1, \dots, a_m\}$  such that exactly one  $d_i \neq 0$ , and this is impossible. We have thus proved that  $n > m$ , and we are finished.

(90.9) COROLLARY. *Let  $\varphi^{(j)}$  be a Brauer character belonging to a block of positive defect. Then there are at least two non- $p$ -conjugate  $\zeta$ 's belonging to  $B$  which contain  $\varphi^{(j)}$ .*

PROOF. In the notation of the preceding proof, if the assertion is false we would have, say,  $d_{1j} > 0, d_{2j} = 0, \dots, d_{nj} = 0$ . Then we could make exactly one  $d_i \neq 0$ , and this is impossible.

We list without proof some further results on  $p$ -conjugate characters.

(90.10) THEOREM (Brauer [10]). *Let  $\zeta$  be an irreducible  $K$ -character of degree  $z$ , and suppose it has  $v$   $p$ -conjugates. Then  $v(v) + v(z) \leq e$ .*

*Equality holds if and only if  $\nu(z) = e$ , that is,  $\zeta$  belongs to a block of defect 0.*

(90.11) THEOREM (Brauer [10]). *Let  $\zeta^{(i)}$  be an irreducible  $K$ -character of  $G$  having  $v$   $p$ -conjugates. If  $\nu(z_i) = e - 1$ , then  $\zeta^{(i)}$  belongs to a block  $B$  of defect 1. Let  $B$  contain  $m$  Brauer characters  $\{\varphi^{(j)}\}$ . Then  $v = m + 1$ . Furthermore, in the matrix  $D^0$  defined in (90.8), each column contains exactly two 1's, the other entries in the column being 0's. Therefore each block of defect 1 contains two  $\zeta$ 's which are not  $p$ -conjugate and for which the associated  $\bar{\zeta}$ 's are irreducible  $\bar{K}$ -characters of  $G$ .*

[The proofs of the preceding theorems are rather deep. It would be desirable to have simple proofs of these results. In (90.19), we give an easy proof of the fact that, if  $\nu(z_i) = e - 1$ , then  $z_i$  belongs to a block of defect 1.]

### § 90C. The number of characters belonging to a block

For this discussion, we follow a paper of Brauer and Feit [1]. Let  $B_l$  be a block of  $\bar{K}G$  of defect  $d$ , and let  $\zeta^{(1)}, \dots, \zeta^{(m)}$  be the irreducible  $K$ -characters of  $G$  belonging to  $B_l$ . Our object is to obtain upper bounds on  $m$  which depend on  $d$ . For example, Theorem 86.3 tells us that  $m = 1$  when  $d = 0$ . Brauer has conjectured that  $m \leq p^d$  for each  $d$ . Brauer and Feit [1] state (without proof) that the inequality  $m \leq p^d$  is valid for  $d = 0, 1$ , and 2; they indicate that the proof depends on some earlier results of Brauer [10].

To begin with, we shall establish

(90.12) THEOREM (Brauer and Feit [1]). *We have*

$$m \leq \frac{1}{4} p^{2d} + 1 .$$

PROOF. Define

$$(90.13) \quad a_{ij} = g^{-1} p^d \sum_{\substack{x \in G \\ z \text{ p-regular}}} \zeta^{(i)}(x) \zeta^{(j)}(x^{-1}) , \quad 1 \leq i, j \leq m .$$

Suppose  $\varphi^{(1)}, \dots, \varphi^{(n)}$  are the Brauer characters belonging to  $B_l$ , so that surely  $n \leq m$ . Let  $V = (a_{ij})$ , an  $m \times m$  matrix. Using (85.18) and (84.12), we obtain

$$(90.14) \quad V = p^d D_l C_l^{-1} D_l .$$

Since  $|C_l|$  is a power of  $p$  and its largest elementary divisor is  $p^d$  (§§ 84 and 89), we conclude from (90.14) that all entries of  $V$  are

rational integers. Furthermore, at least one entry of  $V$  is not a multiple of  $p$ , because  $D_l$  has maximal  $p$ -rank.

In terms of the maps  $\omega^{(i)}$  associated with the characters  $\zeta^{(i)}$ , we rewrite (90.13) as

$$a_{ij} = g^{-1} p^d z_i \sum_{k=1}^r \omega^{(i)}(C_k) \zeta_{k*}^j, \quad 1 \leq i, j \leq m.$$

But by (85.12) we have  $\bar{\omega}^{(i)} = \bar{\omega}^{(q)}$  for  $1 \leq i, q \leq m$  and hence

$$(90.15) \quad \frac{ga_{ij}}{p^d z_i} \equiv \frac{ga_{qj}}{p^d z_q} \pmod{p}. \quad 1 \leq i, j, q \leq m.$$

For  $\alpha, \beta \in Q$ , write  $\alpha \equiv \beta \pmod{p^a}$  to indicate that  $\nu(\alpha - \beta) \geq a$ . Choose  $\zeta^{(q)} \in B_l$  so that  $\nu(z_q) = e - d$ ; then  $g/p^d z_q$  is a  $p$ -adic unit in  $Q$ . Then the above implies

$$a_{qj} \equiv (z_q/z_i) a_{ij} \pmod{p}, \quad 1 \leq i, j \leq m.$$

Set

$$\lambda_i = \nu(z_i) - (e - d) = \nu(z_i) - \nu(z_q), \quad 1 \leq i \leq m,$$

and refer to  $\lambda_i$  as the *height* of  $\zeta^{(i)}$ . Thus  $\lambda_i \geq 0$  for  $1 \leq i \leq m$ , and  $\lambda_i - \lambda_j = \nu(z_i/z_j)$ ,  $1 \leq i, j \leq m$ . From (90.15) we obtain (using the fact that  $a_{jq} = a_{qj}$ )

$$(90.16) \quad a_{ij} \equiv \frac{z_i z_j}{z_q} a_{qq} \pmod{p^{1+\lambda_i}}, \quad 1 \leq i, j \leq m.$$

This shows first that  $p \nmid a_{qq}$  (since some entry of  $V$  is not a multiple of  $p$ ), and second that  $\nu(a_{iq}) = \lambda_i$  for  $1 \leq i \leq m$ , so surely each  $a_{iq} \neq 0$ .

We find readily that  $V^2 = p^d V$ , which gives

$$(90.17) \quad a_{1j}^2 + \cdots + a_{mj}^2 = p^d a_{jj}, \quad 1 \leq j \leq m.$$

Since each  $a_{iq} \neq 0$ , we have

$$p^d a_{qq} = a_{1q}^2 + \cdots + a_{mq}^2 \geq m - 1 + a_{qq}^2,$$

and thus  $m - 1 \leq p^d a_{qq} - a_{qq}^2$ . The maximum value of  $p^d x - x^2$  occurs at  $x = p^d/2$ , and hence  $m - 1 \leq p^{2d}/4$ , which proves the result.

(90.18) **THEOREM** (Brauer [10], Brauer and Feit [1]). *If  $d \geq 2$ , then  $\lambda_i \leq d - 2$  for  $1 \leq i \leq m$ . For  $d = 0, 1, 2$ , each  $\lambda_i = 0$ .*

**PROOF.** From (90.17), each  $a_{jj} > 0$ , since the non-zero term  $a_{qq}^2$  occurs on the left. Also  $a_{jj} \leq p^d$  from its definition. If ever  $a_{jj} = p^d$  for some  $j \neq q$ , the left-hand side of (90.17) contains  $a_{qj}^2 + a_{jj}^2$ ,

which exceeds  $p^d a_{jj}$ . Hence we have

$$0 < a_{jj} < p^d, \quad j \neq q, \quad 0 < a_{qq} \leq p^d.$$

Also  $p \nmid a_{qq}$ , so the only case in which  $a_{qq} = p^d$  is that where  $d = 0$ . If now  $\lambda_i > 0$  for some  $i, 1 \leq i \leq m$ , we deduce from (90.16) that  $p^{1+\lambda_i} \mid a_{ii}$ . Since surely  $d > 0$  if any  $\lambda_i > 0$ , we have  $a_{ii} < p^d$  and hence  $1 + \lambda_i < d$ . This completes the proof.

(90.19) COROLLARY. [See Theorem 90.11.] *If  $\nu(z_i) = e - 1$ , then  $Z_i$  belongs to a block of defect 1.*

PROOF. If  $Z_i$  belongs to a block of defect  $d$  with  $d \geq 2$ , then

$$\lambda_i = \nu(z_i) - (e - d) = d - 1,$$

which contradicts the theorem.

We state (without proof) some further results of Brauer and Feit:

- (90.20) (i) *If any  $\lambda_i > 0, 1 \leq i \leq m$ , then  $m < p^{2d-2}/2$ .*
- (ii) *For  $d > 2$ , we have  $m < p^{2d-2}$ .*
- (iii) *If  $B_i$  has a cyclic defect group, then  $m \leq p^d$ .*

Also of interest is a theorem due to Brauer [11, Theorem 8]:

(90.21) THEOREM. *Let  $\nu(g) = 1$ , and let  $H$  be a  $p$ -Sylow subgroup of  $G$ , and  $N(H)$  its normalizer. The total number of  $\zeta$ 's in blocks of  $\bar{K}G$  of defect 1 equals the number of conjugate classes in  $N(H)$ .*

To conclude, we mention a conjecture due to Brauer [26]: The block  $B_i$  contains a character  $\zeta^{(i)}$  of positive height if and only if the defect group of  $B_i$  is not abelian. In this connection, see Fong [1], [2].

#### § 90D. Numerical bounds

In § 90C, we considered briefly the number of  $\zeta$ 's in a block  $B_i$  of  $\bar{K}G$  of defect  $d$ . One may also try to obtain bounds for the entries  $\{d_{ij}\}$  and  $\{c_{ij}\}$  of the decomposition matrix  $D_i$  and Cartan matrix  $C_i$  associated with the block  $B_i$ . For  $d = 0$ , we know that  $C_i = D_i = (1)$ . For  $d = 1$ , it follows from (90.11) that each entry in  $D_i$  is either 0 or 1, and it can be shown that each  $c_{ij}$  in  $C_i$  satisfies  $c_{ij} \leq p$ . Brauer has conjectured that in fact  $c_{ij} \leq p^d$  in the general case, but this is as yet unproved. For further discussion of these

problems, we refer the reader to Brauer [26].

It is also of interest to give bounds for the  $f_i$ 's and  $u_i$ 's. Results of this nature may be found in Brauer and Nesbitt [3]. The conjecture that  $\nu(f_i) \leq e$  for all  $i$  is still open.

Brauer and Nesbitt ([3]) proved that if  $N = \text{rad } \bar{K}G$ , then  $(N: K) \leq [G: 1](1 - 1/u_1)$ , where  $u_1 = \deg U_1$ , and  $U_1$  is the principal indecomposable module corresponding to the 1-representation of  $G$ . [see Wallace [2].]

### § 91. Examples

In this section we work out some simple examples to illustrate some of the results of this chapter.

#### § 91A. The dihedral group $D_6$ of order 12

The results we require concerning dihedral groups are given in § 47. The group  $D_6$  has a cyclic normal subgroup  $\langle a \rangle$  of order 6, and is generated by  $a$  and an element  $b$  such that

$$a^6 = 1, \quad b^{-1}ab = a^{-1}, \quad b^2 = 1.$$

First, we determine the character table of  $D_6$ . The conjugate classes are

$$\begin{aligned} \mathfrak{C}_1 &= \{1\}, & \mathfrak{C}_2 &= \{a, a^5\}, & \mathfrak{C}_3 &= \{a^2, a^4\}, \\ \mathfrak{C}_4 &= \{a^3\}, & \mathfrak{C}_5 &= \{b, a^2b, a^4b\}, & \mathfrak{C}_6 &= \{ab, a^3b, a^5b\}. \end{aligned}$$

Using the results of § 47 (see Example 47.1), we find easily that the character table of  $D_6$  is given by:

	$\mathfrak{C}_1$	$\mathfrak{C}_2$	$\mathfrak{C}_3$	$\mathfrak{C}_4$	$\mathfrak{C}_5$	$\mathfrak{C}_6$
(91.1)	$\zeta^{(1)}$	1	1	1	1	1
	$\zeta^{(2)}$	1	1	1	-1	-1
	$\zeta^{(3)}$	1	-1	1	-1	-1
	$\zeta^{(4)}$	1	-1	1	-1	1
	$\zeta^{(5)}$	2	1	-1	-2	0
	$\zeta^{(6)}$	2	-1	-1	2	0

In order to distribute the characters into blocks, we use (85.12) and make a table in which the  $(i, j)$  entry is  $g_j z_i^{-1} \zeta_j^{(i)}$ .

(91.2)	1	2	2	1	3	3
	1	2	2	1	-3	-3
	1	-2	2	-1	3	-3
	1	-2	2	-1	-3	3
	1	1	-1	-1	0	0
	1	-1	-1	1	0	0

Now we consider the modular representations of  $D_6$  in a field of characteristic which divides  $[D_6 : 1]$ .

CASE i.  $p = 2$ . In this case, there are exactly two blocks:

$B_1 = \{\zeta^{(1)}, \zeta^{(2)}, \zeta^{(3)}, \zeta^{(4)}\}$  of defect 2;

$B_2 = \{\zeta^{(5)}, \zeta^{(6)}\}$  of defect 1.

There are two  $p$ -regular classes  $\mathfrak{C}_1$  and  $\mathfrak{C}_3$ , and hence there are two irreducible  $\bar{K}$ -representations  $F_1$  and  $F_2$ . For  $F_1$  we may take the 1-representation and note that all the other one-dimensional representations  $\bar{Z}_2, \bar{Z}_3, \bar{Z}_4$  are  $\bar{K}$ -equivalent to  $F_1$ . We show next that  $\bar{Z}_5$  is irreducible and may be taken to be  $F_2$ . If  $\bar{Z}_5$  were reducible, then for a suitable basis the matrices would all have the form

$$\begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix}$$

and hence would have trace zero in  $\bar{K}$ , contrary to what we see from the character table (91.1). With the representations  $F_1$  and  $F_2$  in hand, we find easily for the matrix of decomposition numbers

$D$	$F_1$		$F_2$	
	$Z_1$	$Z_2$	$Z_3$	$Z_4$
	1	0		
	1	0		
	1	0		
	1	0		
$Z_5$	0	1		
$Z_6$	0	1		

For the Cartan matrix, we have

$$C = {}^t D D = \begin{pmatrix} 4 & 0 \\ 0 & 2 \end{pmatrix}.$$

The principal indecomposable modules  $U_1$  and  $U_2$  have degrees 4 and 2, respectively, and  $U_1$  occurs once as a component of the left regular module while  $U_2$  appears twice.

The 2-regular class  $\mathfrak{C}_1$  is of defect 2, and the defect group in this case is the 2-Sylow group of  $D_6$ . The class  $\mathfrak{C}_3$  is of defect 1, and it follows that the defect group  $H_2$  of  $B_2$  is the cyclic group  $[a^3]$  of order 2, whereas  $N(H_2)$  is all of  $D_6$ . In both cases, the defect group is normal in  $G$ , and the reader may verify the results of §88 as they apply to this example.

CASE ii.  $p = 3$ . In this case, there are two blocks:

$$B_1 = \{\zeta^{(1)}, \zeta^{(2)}, \zeta^{(6)}\} \text{ of defect 1;}$$

$$B_2 = \{\zeta^{(3)}, \zeta^{(4)}, \zeta^{(5)}\} \text{ of defect 1.}$$

There are four  $p$ -regular classes, and it is clear that the irreducible modular representations are  $\bar{Z}_1, \bar{Z}_2, \bar{Z}_3, \bar{Z}_4$ . The matrices  $D$  and  $C$  are given by

$$D = \begin{array}{c|cc|cc} & \bar{Z}_1 & \bar{Z}_2 & \bar{Z}_3 & \bar{Z}_4 \\ \hline Z_1 & 1 & 0 & & \\ Z_2 & 0 & 1 & & 0 \\ Z_6 & 1 & 1 & & \\ \hline Z_3 & & & 1 & 0 \\ Z_4 & & 0 & 0 & 1 \\ Z_5 & & & 1 & 1 \end{array}$$
  

$$C = \begin{array}{c|cc|cc} & 2 & 1 & & 0 \\ & 1 & 2 & & \\ \hline 0 & & & 2 & 1 \\ & & & 1 & 2 \end{array}$$

### § 91B. The symmetric group $S_4$

We have also pointed out in Chapter VII, § 46, that  $S_4$  is isomorphic to the octahedral group (See § 32, Example 3). The classes of  $S_4$  are

$$\mathfrak{C}_1 = \{1\}, \quad \mathfrak{C}_2 = \text{2-cycles}, \quad \mathfrak{C}_3 = \text{3-cycles},$$

$$\mathfrak{C}_4 = \text{4-cycles}, \quad \mathfrak{C}_5 = \{(12)(34), (13)(24), (14)(23)\}$$

The character table (from § 32) is

	$\mathfrak{C}_1$	$\mathfrak{C}_2$	$\mathfrak{C}_3$	$\mathfrak{C}_4$	$\mathfrak{C}_5$	
$\zeta^{(1)}$	1	1	1	1	1	
$\zeta^{(2)}$	1	-1	1	-1	1	
$\zeta^{(3)}$	2	0	-1	0	2	,
$\zeta^{(4)}$	3	1	0	-1	-1	
$\zeta^{(5)}$	3	-1	0	1	-1	

whereas the matrix  $g_j z_i^{-1} \zeta_j^{(i)}$  required to check (85.12) is

$$\begin{pmatrix} 1 & 6 & 8 & 6 & 3 \\ 1 & -6 & 8 & -6 & 3 \\ 1 & 0 & -4 & 0 & 3 \\ 1 & 2 & 0 & -2 & -1 \\ 1 & -2 & 0 & 2 & -1 \end{pmatrix}.$$

CASE i.  $p = 2$ . This time, there is only one block of defect 3. The defect group is the 2-Sylow subgroup  $H_2$ , and Theorem 87.29 asserts that  $N(H_2)$  also has exactly one block of defect 3. There are two 2-regular classes  $\mathfrak{C}_1$  and  $\mathfrak{C}_3$ . Besides the 1-representation, it is easily checked that the two-dimensional module  $\bar{Z}_3$  remains irreducible mod 2; otherwise all the matrices would have trace zero. The same trace argument shows that  $\bar{Z}_3$  appears as a composition factor of both  $\bar{Z}_4$  and  $\bar{Z}_5$ . For the decomposition matrix, we have

$$D = \begin{pmatrix} 1 & 0 \\ 1 & 0 \\ 0 & 1 \\ 1 & 1 \\ 1 & 1 \end{pmatrix},$$

and the Cartan matrix is

$$C = {}^t D D = \begin{pmatrix} 4 & 2 \\ 2 & 3 \end{pmatrix}.$$

Both the principal indecomposable modules have dimension 8, and one appears once and the other twice in the left regular module.

CASE ii.  $p = 3$ . The blocks are

- $B_1 = \{\zeta^{(1)}, \zeta^{(2)}, \zeta^{(3)}\}$  of defect 1,  
 $B_2 = \{\zeta^{(4)}\}$  of defect 0,  
 $B_3 = \{\zeta^{(5)}\}$  of defect 0.

The 3-regular classes are  $\mathfrak{C}_1, \mathfrak{C}_2, \mathfrak{C}_4, \mathfrak{C}_5$ . The irreducible  $\bar{K}$ -modules are  $\bar{Z}_1, \bar{Z}_2, \bar{Z}_4, \bar{Z}_5$ , and the matrices  $D$  and  $C$  are given by

$$D = Z_3 \begin{pmatrix} \bar{Z}_1 & \bar{Z}_2 & \bar{Z}_4 & \bar{Z}_5 \\ \hline Z_1 & \begin{matrix} 1 & 0 \\ 0 & 1 \end{matrix} & \begin{matrix} 0 & 0 \\ 0 & 0 \end{matrix} & \\ Z_2 & \begin{matrix} 1 & 1 \\ 0 & 0 \end{matrix} & \begin{matrix} 0 & 0 \\ 1 & 0 \end{matrix} & \\ \hline Z_4 & \begin{matrix} 0 & 0 \\ 0 & 0 \end{matrix} & \begin{matrix} 0 & 0 \\ 0 & 1 \end{matrix} & \\ Z_5 & \begin{matrix} 2 & 1 & 0 & 0 \\ 1 & 2 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{matrix} & & \end{pmatrix};$$

$$C = {}^t D D = \begin{pmatrix} 2 & 1 & 0 & 0 \\ 1 & 2 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

The defect group  $H_1$  of the block  $B_1$  is the 3-Sylow group, which is generated by any 3-cycle. We have

$$[N(H_1):1] = 6,$$

and  $N(H_1) \cong S_3$ . From the character table of  $S_3$  (see § 32), we see that  $S_3$  has exactly one block of defect one and no others, thus providing an illustration of Theorem 87.29.

## § 92. Literature on Applications to Group Theory

The applications of character theory to finite groups are still rather scattered, and we do not attempt to list all of them here. Our purpose is to indicate the different sorts of applications that have been achieved so far and to give references to a few of the major papers.

One of the most challenging problems in the theory of finite groups is the determination of the finite non-cyclic simple groups. Many of the results we quote have a bearing on this problem. For a general reference on the known simple groups, we cite Dieudonné [1], whose book contains references to the older literature as well as to the new developments concerning the finite analogues of the

simple Lie groups inaugurated by Chevalley's paper [2]. Our terminology in this section will follow that of Dieudonné [1].

### § 92A. Groups of a given order

Because of Burnside's  $p^aq^b$ -theorem (see § 34), the order of a non-cyclic simple group must contain at least three distinct primes. Brauer and Tuan [1] proved that if the order of a non-cyclic simple group is  $g = pqr^m$  where  $p, q, r$  are distinct primes, then  $g = 60$  or  $168$ . More generally, they proved that if  $G$  is a non-cyclic simple group of order  $pq^bg^*$  where  $p, q$  are primes and  $0 < g^* < p - 1$ , then  $G \cong PSL(2, p)$  with  $p = 2^m \pm 1$ ,  $p > 3$ , or  $G \cong PSL(2, 2^m)$ ,  $p = 2^m + 1$ ,  $p > 3$ .

Another result by Brauer ([10], §9) is that the only simple group of order  $4p^aq^b$ ,  $p, q$  primes,  $a \leq 2$ , is the alternating group  $A_5$  of order 60. The only simple groups of order  $3p^aq^b$ ,  $a \leq 2$ , are the groups  $A_5$  of order 60 and  $PSL(2, 7)$  of order 168.

Suzuki ([1], § 4) proved that if  $G$  is a finite simple group of order  $p_1^2p_2 \cdots p_n$  where the  $p_i$  are primes such that  $p_1 < p_2 < \cdots < p_n$ , then  $G \cong PSL(2, p_n)$ .

Feit [6] proved that a simple group of order  $4g'$  where  $g'$  is odd, with the property that any two Sylow 2-groups intersect in the identity element, is isomorphic to  $A_5$ .

A somewhat different sort of result was proved by Brauer ([11], II). Let  $G$  be an irreducible subgroup of  $GL(n, K)$  where  $K$  is the complex field, which has no normal subgroup of order  $p$ , where  $p$  is a prime. If the order of  $G$  is divisible by the prime  $p$  to the first power only, then  $p \leq 2n + 1$ . This improves for the case  $[G:1] \not\equiv 0 \pmod{p^2}$ , a theorem of H. Blichfeldt [1], who proved that  $p \leq (2n+1)(n-1)$ . For  $p = 2n + 1$ , Brauer proved that  $G \cong PSL(2, p)$ . Applications of this result were given in another paper on permutation groups (Brauer [12]). Using Brauer's work, Feit and Thompson [2] have recently proved the following result: Let  $G$  be a finite subgroup of  $GL(n, K)$ , and let  $p$  be a prime factor of  $[G:1]$  such that  $p > 2n + 1$ ; then the  $p$ -Sylow subgroup of  $G$  is an abelian normal subgroup.

Feit [4] proved the following result on permutation groups. Let  $G$  be a doubly transitive permutation group on  $m + 1$  letters such that no non-trivial permutation leaves three letters fixed. Suppose  $[G:1] = qm(m + 1)$ . Then either  $G$  contains a normal subgroup of

order  $m + 1$ , or  $m = p^e$  for some prime  $p$ . In the latter case,  $[S_p : [S_p, S_p]] < 4q^2$ , where  $S_p$  is the  $p$ -Sylow subgroup of  $G$ , and if  $S_p$  is abelian, there exists an exactly triply transitive permutation group  $G_0$  containing  $G$  such that  $[G_0 : G] \leq 2$ . The proof of this result is based on the theory of exceptional characters (see Chapter VI) and on an important paper by Zassenhaus [1] in which a characterization of exactly triply transitive permutation groups is given.

Other results on permutation groups have been given by Ito [6].

### § 92B. Characterizations of simple groups

Any attempt to determine all finite simple groups must rest on workable characterizations of the known ones. One of the first such characterizations is contained in a deep and fundamental paper by Suzuki [1]. It is known (M. Hall [2]) that if all the Sylow subgroups of a group  $G$  are cyclic, then  $G$  is solvable. Suzuki proved that if  $G$  is a non-solvable group of even order, whose  $p$ -Sylow subgroups are cyclic for odd primes  $p$ , and whose 2-Sylow subgroup is a dihedral group, then  $G$  contains a normal subgroup  $G_1$  such that  $[G : G_1] \leq 2$ , and  $G_1 \cong S \times L$  where  $S$  is solvable and  $L \cong PSL(2, p)$ . He proved also that a non-solvable group  $G$  having cyclic  $p$ -Sylow subgroups for odd primes  $p$ , and whose 2-Sylow subgroup is a generalized quaternion group, must contain a normal subgroup  $G_1$  such that  $[G : G_1] \leq 2$ , and  $G_1 \cong S \times T$  where  $S$  is solvable and  $T \cong SL(2, p)$  for some odd prime number  $p$ . The proof requires also a result from Brauer and Suzuki [1].

Another basic result<sup>†</sup> was proved by Brauer, Suzuki, and Wall [1]. They proved the following theorem: Let  $G$  be a finite group of even order such that  $G = [G, G]$ , and with the additional property that for any two cyclic subgroups  $A$  and  $B$  of even orders such that  $A \cap B \neq \{1\}$ , there exists a cyclic subgroup  $C$  of  $G$  which contains both  $A$  and  $B$ . Then  $G \cong PSL(2, q)$  for a prime power  $q \geq 4$ . Their proof uses the result of Zassenhaus [1].

We come now to some results that have been obtained characterizing simple groups of even order in which it is assumed that the centralizer of an involution (i.e., element of order two) has a given structure. Brauer and Fowler [1] proved that there exist only a finite number of simple groups in which the centralizer of an involution is isomorphic to a given group.

Suzuki ([3], I) proved that if  $G$  is a finite group of even order

---

<sup>†</sup> For an extension of this theorem see Gorenstein and Walter [1].

such that the centralizer of any involution in  $G$  is abelian, we have one of the following three possibilities: (1) the 2-Sylow subgroups of  $G$  are cyclic; (2) a 2-Sylow subgroup of  $G$  is a normal subgroup; or (3)  $G \cong L \times A$ , where  $L \cong SL(2, 2^n)$  and  $A$  is an abelian group of odd order.

The following result was obtained by Feit [6]: Let  $G$  be a non-cyclic simple group such that for any involution  $u$  belonging to a 2-Sylow subgroup  $S_2$  we have  $C(u) \subset C(S_2)$ . Then  $G \cong SL(2, 2^a)$  for some  $a > 1$ , and conversely, all the simple groups  $SL(2, 2^a)$  satisfy these conditions.

Suzuki and Brauer have carried their program one step farther to obtain the following characterizations of  $PSL(3, q)$ . Any involution of  $GL(3, 2^a)$  is conjugate to

$$U = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix}.$$

Let  $\Omega$  be the totality of  $3 \times 3$  matrices in  $GL(3, 2^a)$  commuting with  $U$ , and let  $\Sigma$  be the center of  $GL(3, 2^a)$ . Then the centralizer of any involution in  $PGL(3, 2^a)$  is isomorphic to  $\Omega/\Sigma$ . Suzuki proved ([3], II) that if  $G$  is a group of even order containing an involution  $t$  such that  $C(t) \cong \Omega/\Sigma$ , and if every involution in  $G$  is conjugate to  $t$ , then  $G \cong PGL(3, 2^a)$ ,  $a \geq 1$ , with one exception. The exceptional case occurs when the base field has two elements, and in this case we have  $G \cong PGL(3, 2)$  or  $G \cong A_6$ . A corresponding result can be obtained for the 3-dimensional unitary group over a finite field of characteristic 2 (Suzuki [7].)

The groups  $PSL(3, q)$  for odd  $q$  have been characterized by Brauer [25]. He announces the following result: Let  $G$  be a finite group containing an involution  $t$  such that (i)  $C(t) \cong GL(2, q)$ , (ii) if  $c \neq 1$  belongs to the center of  $C(t)$ , then  $C(c) = C(t)$ , and (iii)  $G = [G, G]$ . If  $q \equiv -1 \pmod{4}$ ,  $q \not\equiv 1 \pmod{3}$  and  $q \neq 3$ , then  $G \cong PSL(3, q)$ . If  $q = 3$  we have the additional case that  $G$  can be the simple Mathieu group of order 7912.

A characterization of  $PSL(n, p^n)$ ,  $n > 4$ , which does not make use of character theory, has been obtained by Walter [1].

Suzuki [4] raised the following question. Let  $S$  be a subset of a finite group  $H$ , and suppose that another group  $G$  contains  $H$  in such a way that for all  $s \in S$ ,  $C_G(s) \subset H$ . What can then be said about the structure of  $G$ ? In particular, for given  $S$  and  $H$ , are there in-

finitely many simple groups  $G$  satisfying the above condition? Suzuki settled the following special case of his problem. Let  $G$  be a finite group containing an element  $s$  of order 4, and suppose that  $C(s)$  coincides with the cyclic subgroup  $[s]$ . Then either  $G$  contains a normal subgroup of index 2 which does not contain  $s$ , or  $G$  contains an abelian normal subgroup  $G_0$  of odd order such that  $G/G_0$  is one of the following groups:  $SL(2, 3)$ ,  $SL(2, 5)$ ,  $PSL(2, 7)$ ,  $A_6$  or  $A_7$ .

See also Feit and Thompson [3], Gorenstein and Walter [1].

### §92C. Criteria for existence of normal subgroups

Here the idea is to show that groups of various sorts cannot be simple. In particular one would like to have results which assert that groups of odd order cannot be simple, in keeping with Burnside's conjecture that all finite groups of odd order are solvable.

We mention first a result by Brauer and Suzuki (see Suzuki [5], Brauer and Suzuki [1]) that, if a 2-Sylow subgroup of a finite group is a generalized quaternion group, then  $G$  contains a normal subgroup  $N$  of odd order such that the factor group  $G/N$  contains only one element of order 2.

Suzuki ([2]) proved that if  $G$  is a non-abelian finite group of odd order with the property that the centralizer of every element is abelian, then  $G$  cannot be simple. In their paper [1], Brauer, Suzuki, and Wall showed that the only simple groups of even order satisfying this condition are the groups  $SL(2, 2^a)$ ,  $a > 1$  (see also Feit [6]).

Suzuki's result was improved by Feit, M. Hall, and Thompson [1], who proved that, if  $G$  is a finite non-solvable group and if the centralizer of every non-identity element is nilpotent, then  $G$  is of even order.

Some extensions of the result of Frobenius given in §35 have been obtained by Feit ([1], [2]).

We conclude with the remark that besides the theory of characters and blocks, one method which overlaps the structure theory of groups and representation theory has played an important role in the proofs of some of the results stated in this section. The simplest case of the method comes from the observation that if  $M$  is a direct product of cyclic groups of order  $p$  for a fixed prime  $p$ , then  $M$  may be viewed as a vector space over the field of  $p$  elements, and the automorphisms of  $M$  may be viewed as linear transformations of this vector space. Some deep applications of this idea have been given by P. Hall and G. Higman [1], and their work indicates a promising direction for further applications of representation theory.

Additional references for this chapter are Berman [15], Brauer [29], Conlon [2, 3], Fong [4], Green [3, 4, 5], Iizuka and Nakayama [1], Morita [1a], Nagao [2], O'Reilly [1, 2], Reynolds [2, 4, 5], Rukolaine [1, 2], Srinivasan [1, 2], Suzuki [9, 10].

## Bibliography

Amitsur, S. A.

1. *Groups with representations of bounded degree, II.* Ill. J. Math. 5 (1961), 198-205.

Artin, E.

1. *Über eine neue Art von L-Reihen.* Hamb. Abh. 3 (1924), 89-108.
2. *Zur Arithmetik hyperkomplexer Zahlen.* Hamb. Abh. 5 (1927), 261-289.
3. *Zur Theorie der L-Reihen mit allgemeinen Gruppencharakteren,* Hamb. Abh. 8 (1931), 292-306.
4. *Algebraic numbers and algebraic functions.* Princeton University, New York University, 1950-1951.

Artin, E., Nesbitt, C., Thrall, R. M.

1. *Rings with minimum condition.* University of Michigan, Ann Arbor, 1944.

Asano, K.

1. *Einfacher Beweis eines Brauerschen Satzes über Gruppencharaktere.* Proc. Acad. Jap. 31 (1955), 501-503.

Asano, K., Shoda, K.

1. *Zur Theorie der Darstellungen einer endlichen Gruppe durch Kollineationen.* Comp. Math. 2 (1935), 230-240.

Azumaya, G.

1. *Corrections and supplementaries to my paper concerning Krull-Remak-Schmidt's theorem.* Nagoya Math. J. 1 (1950), 117-124.

Azumaya, G., Nakayama, T.

1. *Daisūgaku II (Algebra II).* Tokyo, 1954.

Baer, R.

1. *Abelian subgroups that are direct summands of every containing abelian group.* Bull. Am. Math. Soc. 46 (1940), 800-806.

Banaschewski, B.

1. *On the character ring of finite groups.* Can. J. Math. 15 (1963), 605-612.

Bashev, V. A.

1. *Representations of the  $Z_2 \times Z_2$  group in the field of characteristic 2.* Dokl. Akad. Nauk 141 (1961), 1015-1018.

Bass, H.

1. *Projective modules over algebras.* Ann. of Math. 73 (1961), 532-542.
2. *On the ubiquity of Gorenstein rings.* Math. Zeit. 82 (1963), 8-28.
3. *The Dirichlet unit theorem, induced characters and Whitehead groups of finite groups.* Topology 4 (1966), 391-410.

Berman, S. D.

1. *On the theory of representations of finite groups.* Dokl. Akad. Nauk 86 (1952), 885-888.

2. *On certain properties of integral group rings.* Dokl. Akad. Nauk 91 (1953), 7-9.
3. *On isomorphism of the centers of group rings of p-groups.* Dokl. Akad. Nauk 91 (1953), 185-187.
4. *On a necessary condition for isomorphism of integral group rings.* Dopovidi Akad. Nauk Ukrains. RSR (1953), 313-316.
5. *On the representations of the semi-direct product of two abelian groups.* Dokl. Akad. Nauk 98 (1954), 177-180.
6. *On the equation  $x^m = 1$  in an integral group ring.* Ukrains. Mat. Ž. 7 (1955), 253-261.
7. *Group algebras of abelian extensions of finite groups.* Dokl. Akad. Nauk 102 (1955), 431-434.
8. *p-adic ring of characters.* Dokl. Akad. Nauk 106 (1956), 583-586.
9. *The number of irreducible representations of a finite group over an arbitrary field.* Dokl. Akad. Nauk 106 (1956), 767-769.
10. *Generalized characters of finite groups.* Dopovidi Akad. Nauk Ukrains. RSR (1957), 112-115.
11. *Groups of which all representations are monomial.* Dopovidi Akad. Nauk Ukrains. RSR (1957), 539-542.
- 11a. *Characters of linear representations of finite groups over arbitrary fields.* Mat. Sb. 44 (86) (1958), 409-456.
12. *On Schur's index.* Uspehi Mat. Nauk 16 (1961), 95-100.
13. *On isomorphisms of group algebras of direct products of primary cyclic groups.* Dokl. Uzhgorod Univ. 4 (1961), 76-77.
14. *On representations of locally finite groups.* Dokl. Uzhgorod Univ. 4 (1961), 78-79.
15. *Generalized modular characters of finite groups.* Dokl. Uzhgorod Univ. 4 (1961), 80-81.
16. *Integer representations of finite groups.* Dokl. Akad. Nauk SSSR 152 (1963), 1286-1287.
17. *A contribution to the theory of integer representations of finite groups.* Dokl. Akad. Nauk SSSR 157 (1964), 506-508.

Berman, S. D., Bodí, A. A.

1. *P-blocks for some classes of groups* Dopovidi Akad. Nauk Ukrains. RSR 6 (1958), 606-609.

Berman, S. D., Gudivok, P. M.

1. *On integral representations of finite groups.* Dokl. Akad. Nauk SSSR 145 (1962), 1199-1201.
2. *On integral representations of finite groups.* Dokl. Uzhgorod Univ., ser. Phys.-Mat. Nauk, no. 5 (1962), 74-76.
3. *Indecomposable representations of finite groups over the ring of p-adic integers.* Izvestia Akad. Nauk SSSR 28 (1964), 875-910.

Bierberbach, L.

1. *Über einen Satz des Herrn C. Jordan in der Theorie der endlichen Gruppen linearer Substitutionen.* Sitzber. Preuss. Akad. Wiss. (1911),

231-240.

Blichfeldt, H.

1. *On the order of the linear homogeneous groups, I, II.* Trans. Am. Math. Soc. 4 (1903), 387-397; 5 (1904), 310-325.
2. *On imprimitive linear homogeneous groups.* Trans. Am. Math. Soc. 6 (1905), 230-236.

Bodi, A. A.

1. *Number of blocks of characters of a finite group with given defect.* Ukrains. Mat. Ž. 13 (1961), 136-141.

Boerner, H.

1. *Darstellungen von Gruppen.* Springer, Berlin, 1955.

Borevich, Z. I., Faddeev, D. K.

1. *Theory of homology in groups, I, II.* Proc. Leningrad Univ. 7 (1956), 3-39; 7 (1959), 72-87.
2. *Integral representations of quadratic rings.* Proc. Leningrad Univ. 19 (1960), 52-64.

Bourbaki, N.

1. *Algèbre.* Chap. III, "Algèbre multilinéaire," Hermann, Paris, 1948 (new edition, Paris, 1958).
2. *Algèbre.* Chap. VIII, "Modules et anneaux semi-simples," Hermann, Paris, 1958.

Brauer, R.

1. *Über Zusammenhänge zwischen arithmetischen und invariantentheoretischen Eigenschaften von Gruppen linearer Substitutionen.* Sitzber. Preuss. Akad. Wiss. (1926), 410-416.
2. *Untersuchungen über die arithmetischen Eigenschaften von Gruppen linearer Substitutionen, I, II.* Math. Zeit. 28 (1928), 677-696; 31 (1930), 737-747.
3. *Über Systeme hyperkomplexer Zahlen.* Math. Zeit., 30 (1929), 79-107.
4. *Über die Darstellungen von Gruppen in Galoischen Feldern.* Aci. Sci. Ind. No. 195, Paris, 1935.
5. *On modular and p-adic representations of algebras.* Proc. Nat. Acad. Sci. 25 (1939), 252-258.
6. *On the representations of groups of finite order.* Proc. Nat. Acad. Sci. 25 (1939), 290-295.
7. *On sets of matrices over a division ring.* Trans. Am. Math. Soc. 49 (1941), 502-548.
8. *On the Cartan invariants of groups of finite order.* Ann. of Math. 42 (1941), 53-61.
9. *On the connection between the ordinary and modular characters of groups of finite order.* Ann. of Math. 42 (1941), 926-935.
10. *Investigations on group characters.* Ann. of Math. 42 (1941), 936-958.
11. *On groups whose order contains a prime number to the first power, I, II.* Am. J. Math. 64 (1942), 401-420, 421-440.
12. *On permutation groups of prime degree and related classes of groups.*

- Ann. of Math. 44 (1943), 57-79.
13. *On the arithmetic in a group ring.* Proc. Nat. Acad. Sci. 30 (1944), 109-114.
  14. *On hypercomplex arithmetic and a theorem of Speiser.* Festschrift für Speiser, 233-245, Zurich, 1945.
  15. *On the representation of a group of order  $g$  in the field of the  $g$ -th roots of unity.* Am. J. Math. 67 (1945), 461-471.
  16. *On blocks of characters of groups of finite order, I, II.* Proc. Nat. Acad. Sci. 32 (1946), 182-186, 215-219.
  17. *On the Zeta-functions of algebraic number fields.* Am. J. Math. 69 (1947), 243-250.
  18. *On a conjecture by Nakayama.* Trans. Roy. Soc. Can. ser. III, sec. III, 40 (1947), 11-19.
  19. *On Artin's L-series with general group characters.* Ann. of Math. 48 (1947), 502-514.
  20. *Applications of induced characters.* Am. J. Math. 69 (1947), 709-716.
  21. *Representations of groups and rings.* Colloquium of the Amer. Math. Soc., Madison, Wisconsin, 1948 (mimeo. lecture notes).
  22. *Representations of groups of finite order.* Proc. Int. Cong. Math., vol. II, (1950), 33-36.
  23. *On the algebraic structure of group rings.* J. Math. Soc. Japan 3 (1951), 237-251.
  24. *A characterization of the characters of groups of finite order.* Ann. of Math. 57 (1953), 357-377.
  25. *On the structure of groups of finite order.* Proc. Int. Cong. Math. vol. I, (1954), 1-9.
  26. *Number theoretical investigations on groups of finite order.* Proc. Int. Symp. Alg. No. Theory, Japan (1955), 55-62.
  27. *Zur Darstellungstheorie der Gruppen endlicher Ordnung, I, II.* Math. Zeit. 63 (1956), 406-444; 72 (1959), 25-46.
  28. *A note on theorems of Burnside and Blichfeldt.* Proc. Am. Math. Soc. 15 (1964), 31-34.
  29. *Some applications of the theory of blocks of characters of finite groups. I, II.* J. of Algebra 1 (1964), 152-167; 307-334.

Brauer, R., Feit, W.

1. *On the number of irreducible characters of finite groups in a given block.* Proc. Nat. Acad. Sci. 45 (1959), 361-365.

Brauer, R., Fowler, K. A.

1. *On groups of even order.* Ann. of Math. 62 (1955), 565-583.

Brauer, R., Hasse, H., Noether, E.

1. *Beweis eines Hauptsatzes in der Theorie der Algebren.* J. für Math. 167 (1931), 399-404.

Brauer, R., Nesbitt, C.

1. *On the modular representations of finite groups.* U. of Toronto Studies Math. Ser. # 4 (1937).

2. *On the regular representations of algebras.* Proc. Nat. Acad. Sci. 23 (1937), 236-240.
  3. *On the modular characters of groups.* Ann. of Math. 42 (1941), 556-590.
- Brauer, R., Reynolds, W. F.
1. *On a problem of E. Artin.* Ann. of Math. 68 (1958), 713-720.
- Brauer, R., Suzuki, M.
1. *On finite groups of even order whose 2-Sylow group is a quaternion group.* Proc. Nat. Acad. Sci. 45 (1959), 1757-1759.
- Brauer, R., Suzuki, M., Wall, G. E.
1. *A characterization of the one-dimensional unimodular projective groups over finite fields.* Ill. J. Math. 2 (1958), 718-745.
- Brauer, R., Tate, J.
1. *On the characters of finite groups.* Ann. of Math. 62 (1955), 1-7.
- Brauer, R., Tuan, H. F.
1. *On simple groups of finite order, I.* Bull. Am. Math. Soc. 51 (1945), 756-766.
- Burnside, W.
1. *On an arithmetical theorem connected with roots of unity, and its application to group characteristics.* Proc. London Math. Soc. (2) 1 (1904), 112-116.
  2. *On the complete reduction of any transitive permutation group and on the arithmetic nature of the coefficients in its irreducible components.* Proc. London Math. Soc. (2) 3 (1905), 239-252.
  3. *On the arithmetical nature of the coefficients in a group of linear substitution of finite order.* Proc. London Math. Soc. (2) 4 (1906), 1-9.
  4. *Theory of groups of finite order.* Second edition, Cambridge University Press, Cambridge, 1911.
- Cartan, H., Eilenberg, S.
1. *Homological Algebra.* Princeton University Press, Princeton, 1956, Chapter I.
- Chevalley, C.
1. *L'arithmétique dans les algèbres de matrices.* Act. Sci. Ind., No. 323, Paris, 1936.
  2. *Sur certains groupes simples.* Tôhoku Math. J. (2) 7 (1955), 14-66.
  3. *Fundamental concepts of algebra.* Academic Press, New York, 1956.
- Clifford, A. H.
1. *Representations induced in an invariant subgroup.* Ann. of Math. 38 (1937), 533-550.
- Cohn, J. A., Livingstone, D.
1. *On groups of order  $p^3$ .* Can. J. Math. 15 (1963), 622-624.
- Conlon, S. B.
1. *Twisted group algebras and their representations.* J. Austral. Math. Soc. 4 (1964), 152-173.
  2. *Certain representation algebras.* J. Austral. Math. Soc. 5 (1965), 83-99.
  3. *The modular representation algebra of groups with Sylow 2-subgroup  $Z_2 \times Z_2$ .*

- J. Austral. Math. Soc. 6 (1966), 76-88.
- Connell, I. G.
1. *On the group ring.* Can. J. Math. 15 (1963), 650-685.
- Curtis, C. W.
1. *Commuting rings of endomorphisms.* Can. J. Math. 8 (1956), 271-292.
  2. *Modules whose annihilators are direct summands.* Pacific J. Math. 8 (1958), 685-691.
  3. *Quasi-Frobenius rings and Galois theory.* Ill. J. Math. 3 (1959), 134-144.
  4. *A note on induced modules.* Can. J. Math. 13 (1961), 587-592.
- Curtis, C. W., Jans, J. P.
1. *On algebras with a finite number of indecomposable modules.* Trans. Amer. Math. Soc. 114 (1965), 122-132.
- Dade, E. C.
1. *Some indecomposable group representations.* Ann. of Math. (to appear).
  2. *Answer to a question of R. Brauer.* J. of Algebra 1 (1964), 1-4.
- DeLeeuw, K.
1. *Some applications of cohomology to algebraic number theory and group representations.* unpublished.
- Deskins, E.
1. *Finite abelian groups with isomorphic group algebras.* Duke Math. J. 23 (1956), 35-40.
  2. *A partial converse of a theorem of N. Ito.* Prelim. report, Am. Math. Soc. Notices 8 (Feb. 1961), 59.
- Deuring, M.
1. *Galoissche Theorie und Darstellungstheorie.* Math. Ann. 107 (1932), 140-144.
  2. *Algebren.* Springer, Berlin, 1935.
- Dickson, L. E.
1. *Modular theory of group characters.* Bull. Am. Math. Soc. 13 (1907), 477-488.
- Diederichsen, F. E.
1. *Über die Ausreduktion ganzzahliger Gruppendarstellungen bei arithmetischer Äquivalenz.* Hamb. Abh. 14 (1938), 357-412.
- Dieudonné, J.
1. *La géométrie des groupes classiques.* Springer, Berlin, 1955.
  2. *Remarks on quasi-Frobenius rings.* Ill. J. Math. 2 (1958), 346-354.
- Eckmann, B., Schopf, A.
1. *Über injective Moduln.* Archiv der Math. 4 (1953), 75-78.
- Eichler, M.
1. *Über die Idealklassenzahl total definiter Quaternionenalgebren.* Math. Zeit. 43 (1938), 102-109.
  2. *Über die Idealklassenzahl hyperkomplexer Zahlen.* Math. Zeit. 43 (1938), 481-494.
- Eilenberg, S., Nakayama, T.
1. *On the dimension of modules and algebras, II.* Nagoya Math. J. 9 (1955),

1-16.

Faddeev, D. K.

1. *On the semigroup of genera in the theory of integral representations.* Izvestia Akad. Nauk SSSR. 28 (1964), 475-478.

Feit, W.

1. *On a conjecture of Frobenius.* Proc. Am. Math. Soc. 7. (1956), 177-187.
2. *On the structure of Frobenius groups.* Can. J. Math. 9 (1957), 587-596.
3. *Characters of finite groups.* Mimeographed notes, Cornell University, 1958.
4. *On groups which contain Frobenius groups as subgroups.* Proc. Symp. Pure Math. vol. I (Finite Groups), Providence, (1959), 22-27.
5. *On a class of doubly transitive permutation groups.* Ill. J. Math. 4 (1960), 170-186.
6. *A characterization of the simple groups  $SL(2, 2^a)$ .* Am. J. Math. 82 (1960), 281-300.

Feit, W., Hall, M., Thompson, J. G.

1. *Finite groups in which the centralizer of any non-identity element is nilpotent.* Math. Zeit. 74 (1960), 1-17.

Feit, W., Thompson, J.

1. *On groups of odd order.* Mimeographed notes, 1960.
2. *On groups which have a faithful representation of degree less than  $(p - 1)/2$ .* Pacific Math. J. 4 (1961), 1257-1262.
3. *Solvability of groups of odd order.* Pacific J. Math. 13 (1963), 775-1029.

Fischer, B.

1. *Die Brauersche Charakterisierung der Charaktere endlicher Gruppen.* Math. Ann. 149 (1963), 226-231.

Fitting, H.

1. *Die Theorie der Automorphismenringe Abelscher Gruppen und ihr Analogon bei nicht kommutativen Gruppen.* Math. Ann. 107 (1932), 514-542.

Fong, P.

1. *Some properties of characters of finite solvable groups.* Bull. Am. Math. Soc. 66 (1960), 116-117.
2. *On the characters of  $p$ -solvable groups.* Trans. Am. Math. Soc. 98 (1961), 263-284.
3. *A note on splitting fields of representations of finite groups.* Ill. J. Math. 7 (1963), 515-520.
4. *A note on a conjecture of Brauer.* Nagoya Math. J. 22 (1963), 1-13.

Fong, P., Gaschütz, W.

1. *A note on the modular representations of solvable groups.* J. für Math. 208 (1961), 73-78.

Frame, J. S.

1. *The double cosets of a finite group.* Bull. Am. Math. Soc. 47 (1941), 458-467.

Frobenius, G.

1. Über Relationen zwischen den Charakteren einer Gruppe und denen ihrer Untergruppen. Sitzber. Preuss. Akad. Wiss. (1898), 501-515.
2. Über die Charaktere der alternierenden Gruppe. Sitzber. Preuss. Akad. Wiss. (1901), 303-315.
3. Über auflösbare Gruppen, IV. Sitzber. Preuss. Akad. Wiss. (1901), 1216-1230.
4. Über einen Fundamentalsatz der Gruppentheorie, II. Sitzber. Preuss., Akad. Wiss. (1907), 428-437.
5. Über den von L. Bieberbach gefundenen Beweis eines Satzes von C. Jordan. Sitzber. Preuss. Akad. Wiss. (1911), 241-248.

Frobenius, G., Schur, I.

1. Über die reellen Darstellungen der endlichen Gruppen. Sitzber. Preuss. Akad. Wiss. (1906), 186-208.
2. Über die Äquivalenz der Gruppen linearer Substitutionen. Sitzber. Preuss. Akad. Wiss. (1906), 209-217.

Frucht, R.

1. Darstellung Abelscher Gruppen durch Kollineationen. J. für Math. 166 (1931), 16-29.

Gallagher, P. X.

1. Group characters and commutators. Math. Zeit. 79 (1962), 122-126.

Gaschütz, W.

1. Zur Erweiterungstheorie der endlichen Gruppen. J. für Math. 190 (1952), 93-107.
2. Über den Fundamentalsatz von Maschke zur Darstellungstheorie der endlichen Gruppen. Math. Zeit. 56 (1952), 376-387.

Gelfand, I. M., Šapiro, Z. Ya.

1. Representations of the group of rotations in three-dimensional space and their applications. Uspehi Mat. Nauk (N.S.) (1952), 3-117; Am. Math. Soc. Translations, vol. 2, Series 2, Providence, 1956.

Giorgiutti, I.

1. Modules projectifs sur les algèbres de groupes finis. C. R. Acad. Sci. Paris 250 (1960), 1419-1420.

Gorenstein, D., Herstein, I. N.

1. Finite groups admitting a fixed-point-free automorphism of order 4. Am. J. Math. 83 (1961), 71-78.

Gorenstein, D., Hughes, D. R.

1. Triply transitive groups in which only the identity fixes four letters. Ill. J. Math. 5 (1961), 486-491.

Gorenstein, D., Walter, J. H.

1. On finite groups with dihedral 2-subgroups. Ill. J. Math. 6 (1962), 553-593.

Green, J. A.

1. On the indecomposable representations of a finite group. Math. Zeit. 70 (1959), 430-445.

- 1a. *On the converse to a theorem of R. Brauer.* Proc. Camb. Phil. Soc. 51 (1955), 237-239.
- 1b. *The characters of the finite general linear groups.* Trans. Amer. Math. Soc. 80 (1955), 402-447.
2. *A lifting theorem for modular representations.* Proc. Roy. Soc. London, 252A (1959), 135-142.
3. *Blocks of modular representations.* Math. Zeit. 79 (1962), 100-115.
4. *The modular representation algebra of a finite group.* Ill. J. Math. 6 (1962), 607-619.
5. *A transfer theorem for modular representations.* J. of Algebra 1 (1964), 73-84.

Gruenberg, K.

1. *The residual nilpotence of certain presentations of finite groups.* Archiv der Math. 13 (1962), 408-417.

Grün, O.

- 1 *Beiträge zur Gruppentheorie. II.* J. für Math. 186 (1948), 165-169.

Gudivok, P. M.

1. *Integral representations of groups of type  $(p,p)$ .* Dokl. Uzhgorod Univ., ser. Phys.-Mat. Nauk, no. 5 (1962), 73.
2. *On  $p$ -adic integral representations of finite groups.* Dokl. Uzhgorod Univ., ser. Phys.-Mat. Nauk, no. 5 (1962), 81-82.
3. *Representations of finite groups over certain local rings.* Dopovidi Akad. Nauk Ukrainsk. RSR (1964), 173-176.
4. *Representations of finite groups over quadratic rings.* Dokl. Akad. Nauk SSSR 159 (1964), 1210-1213.

Gudivok, P. M., Drobotenko, V. S., Lichtman, A. I.

1. *On representations of finite groups over the ring of residue classes mod  $m$ .* Ukrainsk. Math. J. 16 (1964), 82-89.

Hall, M.

1. *A type of algebraic closure.* Ann. of Math. 40 (1939), 360-369.
2. *The theory of groups.* Macmillan, New York, 1959.

Hall, P.

1. *On a theorem of Frobenius.* Proc. London Math. Soc. (2) 40 (1936), 468-501.

Hall, P., Higman, G.

1. *On the  $p$ -length of  $p$ -soluble groups and reduction theorems for Burnside's problem.* Proc. London Math. Soc. (3) 6 (1956), 1-42.

Hasse, H.

1. *Zahlentheorie.* Akademie-Verlag, Berlin, 1949.

Hattori, A.

1. *Rank element of a projective module.* Nagoya Math. J. 25 (1965), 113-120.

Hecke, E.

1. *Vorlesungen über die Theorie der algebraischen Zahlen.* Akademische Verlag., Leipzig, 1923.

Heller, A.

1. *On group representations over a valuation ring.* Proc. Nat. Acad.

Sci. 47 (1961), 1194-1197.

Heller, A., Reiner, I.

1. *Indecomposable representations*. Ill. J. Math. 5 (1961), 314-323.
2. *Representations of cyclic groups in rings of integers*, I, II. Ann. of Math. 76 (1962), 73-92; 77 (1963) 318-328.
3. *Indecomposable representations of cyclic groups*. Bull. Am. Math. Soc. 68 (1962), 210-212.
4. *Grothendieck groups of orders in semisimple algebras*. Trans. Am. Math. Soc. 112 (1964), 344-355.
5. *Grothendieck groups of integral group rings*. Ill. J. Math. 9 (1965), 349-360.

Higman, D. G.

1. *Focal series in finite groups*. Can. J. Math. 5 (1953), 477-497.
2. *On modules with a group of operators*. Duke Math. J. 21 (1954), 369-376.
3. *Indecomposable representations at characteristic p*. Duke Math. J. 21 (1954), 377-381.
4. *Induced and produced modules*. Can. J. Math. 7 (1955), 490-508.
5. *On orders in separable algebras*. Can. J. Math. 7 (1955), 509-515.
6. *Relative cohomology*. Can. J. Math. 9 (1957), 19-34.
7. *On isomorphisms of orders*. Mich. Math. J. 6 (1959), 255-258.
8. *On representations of orders over Dedekind domains*. Can. J. Math. 12 (1960), 106-125.

Higman, D. G., MacLaughlin, J. E.

1. *Finiteness of class numbers of representations of algebras over function fields*. Mich. Math. J. 6 (1959), 401-404.

Higman, Graham

1. *The units of group rings*. Proc. London Math. Soc. (2) 46 (1940), 231-248.

Hochschild, G.

1. *Semi-simple algebras and generalized derivations*. Am. J. Math. 64 (1941), 677-694.
2. *Cohomology groups of an associative algebra*. Ann. of Math. 46 (1945), 58-67.
3. *Relative homological algebra*. Trans. Am. Math. Soc. 82 (1956), 246-269.

Hopkins, C.

1. *Rings with minimal condition for left ideals*. Ann. of Math. 40 (1939), 712-730.

Huppert, B.

1. *Monomiale Darstellung endlicher Gruppen*. Nagoya Math. J. 6 (1953), 93-94.

Iizuka, K.

1. *Note on blocks of group characters*. Kumamoto J. Sci. ser. A, 2 (1956), 309-321.
2. *On Osima's blocks of characters of groups of finite order*. Kumamoto J. Sci. ser. A, 4 (1960), 275-283.

3. *On Osima's blocks of group characters.* Proc. Japan Acad. 36 (1960), 392-396.
  4. *On the blocks and sections of finite groups.* Kumamoto J. Sci. ser. A, 5 (1960), 53-62.
  5. *On Brauer's theorem on sections in the theory of group characters.* Math. Zeit. 75 (1961), 299-304.
- Iizuka, K., Nakayama, T.
1. *A remark on orthogonality relations in finite groups.* Nagoya Math. J. 20 (1962), 185-194.
- Ikeda, M.
1. *A characterization of quasi-Frobenius rings.* Osaka Math. J. 4 (1952), 203-209.
  2. *On a theorem of Gaschütz.* Osaka Math. J. 5 (1953), 53-58.
- Ikeda, M., Nakayama, T.
1. *On some characteristic properties of quasi-Frobenius and regular rings.* Proc. Am. Math. Soc. 5 (1954), 15-19.
- Isaacs, I. M., Passman, D. S.
1. *Groups with representations of bounded degree.* Can. J. Math. 16 (1964), 299-309.
  2. *Groups whose irreducible representations have degrees dividing  $p^e$ .* Ill. J. Math. 8 (1964), 446-457.
- Ito, N.
1. *Some studies on group characters.* Nagoya Math. J. 2 (1951), 17-28.
  2. *On the degrees of irreducible representations of a finite group.* Nagoya Math. J. 3 (1951), 5-6.
  3. *On the characters of soluble groups.* Nagoya Math. J. 3 (1951), 31-48.
  4. *Note on A-groups.* Nagoya Math. J. 4 (1952), 79-81.
  5. *On a theorem of H. Blichfeldt.* Nagoya Math. J. 5 (1953), 75-78.
  6. *Zur Theorie der transitiven Gruppen vom Grad  $p$ , I, II.* Math. Zeit. 74 (1960), 299-301; 75 (1961), 127-135.
  7. *On transitive simple permutation groups of degree  $2p$ .* Math. Zeit. 78 (1962), 453-468.
- Jacobson, N.
1. *The theory of rings.* Am. Math. Soc., New York, 1943.
  2. *Lectures on abstract algebra II.* Van Nostrand, New York, 1952.
  3. *The structure of rings.* Am. Math. Soc., Providence, 1956.
- Jans, J. P.
1. *On the indecomposable representations of algebras.* Ann. of Math. 66 (1957), 418-429.
- Jenner, W. E.
1. *Block ideals and arithmetics of algebras.* Comp. Math. 11 (1953), 187-203.
  2. *On the class number of non-maximal orders in  $p$ -adic division algebras.* Math. Scand. 4 (1956), 125-128.
- Jennings, S. A.

1. *The structure of the group ring of a p-group over a modular field.* Trans. Am. Math. Soc. 50 (1941), 175-185.

Jones, A.

1. *Indecomposable integral representations.* Ph. D. thesis, University of Illinois, 1962.
2. *Groups with a finite number of indecomposable integral representations.* Mich. Math. J. 10 (1963), 257-261.
3. *Integral representations of the direct product of groups.* Can. J. Math. 15 (1963), 625-630.
4. *On representations of finite groups over valuation rings.* Ill. J. Math. 9 (1965), 297-303.

Jordan, C.

1. *Mémoire sur les équations différentielles linéaires à intégrale algébrique.* J. für Math. 84 (1878), 89-215.

Kaplansky, I.

1. *Modules over Dedekind rings and valuation rings.* Trans. Am. Math. Soc. 72 (1952), 327-340.

Kasch, F.

1. *Grundlagen einer Theorie der Frobeniuserweiterungen.* Math. Ann. 127 (1954), 453-474.

Kasch, F., Kneser, M., Kupisch, H.

1. *Unzerlegbare modulare Darstellungen endlicher Gruppen mit zyklischer p-Sylow-Gruppe.* Archiv der Math. 8 (1957), 320-321.

Kawada, Y.

1. *Cohomology in abstract unit groups.* Proc. Am. Math. Soc. 6 (1951), 12-15.

Kleppner, A.

1. *The structure of some induced representations.* Duke Math. J. 29 (1962), 555-572.

Knee, D. I.

1. *The indecomposable integral representations of finite cyclic groups.* Ph. D. thesis, M. I. T.. 1962.

Kneser, M.

1. *Einige Bemerkungen über ganzzahlige Darstellungen endlicher Gruppen.* Arch. der Math.

Kochendörffer, R.

1. *Über treue irreduzible Darstellungen endlicher Gruppen.* Math. Nachrichten 1 (1948), 25-39.
2. *Über den Multiplikator einer Gruppe.* Math. Zeit. 63 (1956), 507-513.

Kostant, B.

1. *A theorem of Frobenius, a theorem of Amitsur-Levitski and cohomology theory.* J. of Math. and Mech. 7 (1958), 237-264.

Krugljak, S. A.

1. *Representations of the (p,p) group over a field of characteristic p.* Dokl. Akad. Nauk. 153 (1963), 1253-1256.

Kurosh, A. G.

1. *Theory of groups*. Chelsea, New York, 1955.

Landau, E.

1. *Einführung in die elementare und analytische Theorie der algebraischen Zahlen und der Ideale*. Teubner, Leipzig, 1917.

Leahy, W. J.

1. *The classification of the indecomposable integral representations of the dihedral group of order  $2p$* . Ph. D. thesis M. I. T., 1962.

Ledermann, H.

1. *Introduction to the theory of finite groups*. 2nd ed., Oliver and Boyd, Edinburgh, 1953.

Lee, M. P.

1. *Integral representations of the dihedral group of order  $2p$* . Ph. D. thesis, University of Illinois, 1962.

Lee, M. P.

2. *Integral representations of dihedral groups*. Trans. Am. Math. Soc. 110 (1964), 213–231.

Lichtman, A. I.

1. *On group rings of  $p$ -groups*. Izvest. Akad. Nauk SSSR 27 (1963), 795–800.

Lomont, J. S.

1. *Applications of finite groups*. Academic Press, New York, 1959.

losey, G.

1. *On dimension subgroups*. Trans. Am. Math. Soc. 97 (1960), 474–486.
2. *On group algebras of  $p$ -groups*. Michigan Math. J. 7 (1960), 237–240.

Mackey, G. W.

1. *On induced representations of groups*. Am. J. Math. 73 (1951), 576–592.
2. *Symmetric and anti-symmetric Kronecker squares of induced representations of finite groups*. Am. J. Math. 75 (1953), 387–405.
3. *On multiplicity-free representations of finite groups*. Pacific J. Math. 8 (1958), 503–510.
4. *Unitary representations of group extensions, I*. Acta Math. 99 (1958), 265–311.

Malcev, A.

1. *On the representation of an algebra as a direct sum of its radical and a semi-simple subalgebra*. Dokl. Akad. Nauk 36 (1942), 42–45.

Mann, H.

1. *Über die Erzeugung von Gruppen durch Darstellungen von Untergruppen*. Mh. Math. Phys. 46 (1937), 74–83.
2. *Introduction to algebraic number theory*. Ohio State University Press, Columbus, 1955.

Maranda, J. M.

1. *On  $p$ -adic integral representations of finite groups*. Can. J. Math. 5 (1953), 344–355.
2. *On the equivalence of representations of finite groups by groups of automorphisms of modules over Dedekind rings*. Can. J. Math. 7 (1955),

516-526.

Maschke, H.

1. Über den arithmetischen Charakter der Coefficienten der Substitutionen endlicher linearer Substitutionsgruppen. *Math. Ann.* 50 (1898), 482-498.

Matuljauskas, A.

1. On integral representations of a cyclic group of order 4. *Litovsk. Mat. Sb.* 2 (1962).
2. Integral representations of a cyclic group of order 6. *Litovsk. Mat. Sb.* 2 (1962).
3. On the number of indecomposable representations of the group  $Z_8$ . *Litovsk Mat. Sb.* 3 (1963), 181-188.

Matuljauskas, A., Matuljauskene, M.

1. On integral representations of a group of type (3,3). *Litovsk. Mat. Sb.* 4 (1964), 229-233.

Miller, G. A., Blichfeldt, H., Dickson, L. E.

1. Theory and application of finite groups. 2nd ed., Stechert, New York, 1938.

Morita, K.

1. Duality for modules and its applications to the theory of rings with minimum condition. *Science reports of the Tokyo Kyoiku Daigaku, Section A*, vol. 6, No. 150, (1958), 83-142.
2. On group rings over a modular field which possess radicals expressible as principal ideals. *Sci. Rep. Tokyo Bunrika Daigaku* 4 (1951), 177-194.
2. On algebras for which every faithful representation is its own second commutator. *Math. Zeit.* 69 (1958), 429-434.

Morita, K., Kawada, Y., Tachikawa, H.

1. On injective modules. *Math. Zeit.* 68 (1957), 217-226.

Morita, K., Tachikawa, H.

1. Character modules, submodules of a free module, and quasi-Frobenius rings. *Math. Zeit.* 65 (1956), 414-428.

Murnaghan, F.

1. The theory of group representations. Johns Hopkins, Baltimore, 1938.

Nagai, O.

1. Note on Brauer's theorem of simple groups. *Osaka Math. J.* 4 (1952), 113-120.
2. Supplement to Note on Brauer's theorem of simple groups, I, II. *Osaka Math. J.* 5 (1953), 227-232; 11 (1959), 147-152.
3. On simple groups related to permutation groups of prime degree. *Osaka Math. J.* 8 (1956), 107-117.

Nagao, H.

1. A remark on the orthogonality relations in the representation theory of finite groups. *Can. J. Math.* 11 (1959), 59-60.
2. A proof of Brauer's theorem on generalized decomposition numbers. *Nagoya Math. J.* 22 (1963), 73-77.

Nagao, H., Nakayama, H.

1. *On the structure of  $M_0$ - and  $M_u$ -modules.* Math. Zeit. 59 (1953), 164-170.
- Nakayama, T.
  1. *Some remarks on regular representations, induced representations, and modular representations.* Ann. of Math. 39 (1938), 361-369.
  2. *On Frobenius algebras, I, II.* Ann. of Math. 40 (1939), 611-633; 42 (1941), 1-21.
  3. *On some modular properties of irreducible representations of a symmetric group, I, II.* Jap. J. Math. 17 (1940), 165-184, 411-423.
  4. *On two topics in the structural theory of rings.* Proc. Int. Cong. Math. (1950), vol. II, New York, 1952.
  5. *A theorem on modules of trivial cohomology over a finite group.* Proc. Japan Acad. 32 (1956), 373-376.
  6. *On modules of trivial cohomology over a finite group.* Ill. J. Math. 1 (1957), 36-43.
  7. *On modules of trivial cohomology over a finite group II.* Nagoya Math. J. 12 (1957), 171-176.

Nakayama, T., Nesbitt, C.

1. *Symmetric algebras.* Ann. of Math. 39 (1938), 659-668.

Nakayama, T., Osima, M.

1. *Note on blocks of symmetric groups.* Nagoya Math. J. 2 (1951), 111-117.

Nakayama, T., Shoda, K.

1. *Über die Darstellung einer endlichen Gruppe durch halblineare Transformationen.* Jap. J. Math. 12 (1935), 109-122.

Nazarova, L. A.

1. *Integral representations of Klein's four-group.* Dokl. Akad. Nauk 140 (1961), 1011-1014.
2. *Integral representations of the alternating group of degree 4.* Ukrain. Math. J. 15 (1963).

Nazarova, L. A., Roiter, A. V.

1. *Integral representations of the symmetric group of third degree.* Ukrain. Math. J. 14 (1962), 271-288.

Nesbitt, C.

1. *Relations between the coefficients of the modular representations of groups.* Bull. Am. Math. Soc. 44 (1938), 40.

2. *Regular representations of algebras.* Ann. of Math. 39 (1938), 634-658.

Nesbitt, C., Scott, W. M.

1. *Matrix algebras over an algebraically closed field.* Ann. of Math. 44 (1943), 147-160.

Nesbitt, C., Thrall, R. M.

1. *Some ring theorems with applications to modular representations.* Ann. of Math. 47 (1946), 551-567.

Noether, E.

1. *Hyperkomplexe Größen und Darstellungstheorie.* Math. Zeit. 30 (1929), 641-692.

2. *Nichtkommutative Algebra.* Math. Zeit. 37 (1933), 513-541.

Novikov, P. S.

1. *On periodic groups.* Dokl. Akad. Nauk 127 (1959), 749-752.

Nunke, R. J.

1. *Modules of extensions over Dedekind rings.* Ill. J. Math. 3 (1959), 222-241.

O'Reilly, M. F.

1. *On the modular representation algebra of metacyclic groups.* J. London Math. Soc. 39 (1964), 267-276.
2. *On the semisimplicity of the modular representation algebra of a finite group.* Ill. J. Math. 9 (1965), 261-276.

Osima, M.

1. *On the representations of groups of finite order.* Math. J. Okayama Univ. 1 (1952), 33-61.
2. *On the Schur relations for the representations of a Frobenius algebra.* J. Math. Soc. Japan 4 (1952), 1-13.
3. *On the induced characters of a group.* Proc. Japan Acad. 28 (1952), 243-248.
4. *Supplementary remarks on the Schur relations for a Frobenius algebra.* J. Math. Soc. Japan 5 (1953), 24-28.
5. *On the induced characters of groups of finite order.* Math. J. Okayama Univ. 3 (1953), 47-64.
6. *Notes on blocks of group characters.* Math. J. Okayama Univ. 4 (1955), 175-188.
7. *On some properties of group characters, I.* Proc. Japan Acad. 36 (1960), 18-21.
8. *On some properties of group characters, II.* Math. J. Okayama Univ. 10 (1960), 61-66.

Passman, D. S.

1. *On groups with enough finite representations.* Proc. Am. Math. Soc. 14 (1963), 782-787.

Perlis, S., Walker, G.

1. *Abelian group algebras of finite order.* Trans. Am. Math. Soc. 68 (1950), 420-426.

Pollard, H.

1. *Theory of algebraic numbers.* John Hopkins, Baltimore, 1950.

Pu, L. C.

1. *Integral representations of nonabelian groups of order pq.* Mich. Math. J. 12 (1965), 231-246.

Rayna, G.

1. *On the classification of modules over finite groups.* Ph.D. thesis, Princeton Univ., 1965.

Reiner, I.

1. *Maschke modules over Dedekind rings.* Can. J. Math. 8 (1956), 329-334.
2. *Integral representations of cyclic groups of prime order.* Proc. Am. Math. Soc. 8 (1957), 142-146.

3. *On the class number of representations of an order.* Can. J. Math. 11 (1959), 660-672.
4. *The non-uniqueness of irreducible constituents of integral group representations.* Proc. Am. Math. Soc. 11 (1960), 655-657.
5. *The behavior of integral group representations under ground ring extension.* Ill. J. Math. 4 (1960), 640-651.
6. *The Schur index in the theory of group representations.* Mich. Math. J. 8 (1961), 39-47.
7. *The Krull-Schmidt theorem for integral group representations.* Bull. Am. Math. Soc. 67 (1961), 365-367.
8. *Indecomposable representations of non-cyclic groups.* Mich. Math. J. (to appear).
9. *Failure of the Krull-Schmidt theorem for integral representations.* Mich. Math. J. (to appear).
10. *Extensions of irreducible modules.* Mich. Math. J. 10 (1963), 273-276.
11. *The number of irreducible modular representations of a finite group.* Proc. Am. Math. Soc. 15 (1964), 810-812.
12. *The integral representation ring of a finite group.* Mich. Math. J. 12 (1965), 11-22.
13. *Nilpotent elements in rings of integral representations.* Proc. Am. Math. Soc. 17 (1966), 270-273.

Reynolds, W. F.

1. *Modular representations of finite groups.* Report, Summer Inst. Finite Groups, Pasadena, 1960, 181-217.
2. *Blocks and normal subgroups of finite groups.* Nagoya Math. J. 22 (1963), 15-32.
3. *Projective representations of finite groups in cyclotomic fields.* Ill. J. Math. 9 (1965), 191-198.
4. *Block idempotents of twisted group algebras.* Proc. Am. Math. Soc. 17 (1966), 280-282.
5. *A generalization of Brauer characters.* Trans. Am. Math. Soc. 119 (1965), 333-351.

Rim, D. S.

1. *Modules over finite groups.* Ann. of Math. 69 (1959), 700-712.
2. *On projective class groups.* Trans. Am. Math. Soc. 98 (1961), 459-467.

Robinson, G. de B.

1. *Representation theory of the symmetric group.* Univ. of Toronto Press, Toronto, 1961.

Roiter, A. V.

1. *Integral representations of cyclic groups of the fourth order.* Proc. Leningrad Univ. 19 (1960), 65-74.
2. *Categories with division and integral representations.* Dokl. Akad. Nauk SSSR 153 (1963), 46-48.
3. *On categories of representations.* Ukrains. Math. J. 15 (1963), 448-452.

Roquette, P.

1. *Arithmetische Untersuchung des Charakters eines endlichen Körpers.* J. für Math. 190 (1952), 148-168.
2. *Realisierung von Darstellungen endlicher nilpotenter Gruppen.* Archiv. der Math. 9 (1958), 241-250.

Rosenberg, A.

1. *Blocks and centres of group algebras.* Math. Zeit. 76 (1961), 209-216.

Rosenberg, A., Zelinsky, D.

1. *Annihilators.* Port. Math. 20 (1961), 53-65.

Rukolaine, A. V.

1. *On the degrees of the modular representations of  $p$ -solvable groups.* Vestnik Leningrad Univ. 19 (1962), 41-48.
2. *Some arithmetic properties of modular characters of  $p$ -solvable groups.* Izvestia Akad. Nauk SSSR 28 (1964), 571-582.

Rutherford, D. E.

1. *Substitutional analysis.* Edinburgh University Press, Edinburgh, 1948.

Sah, C. H.

1. *Existence of normal complements and extensions of characters in finite groups.* Ill. J. Math. 6 (1962), 282-291.

Schilling, O. F. G.

1. *Über die Darstellungen endlicher Gruppen.* J. für Math. 174 (1936), 188.

Schur, I.

1. *Über die Darstellung der endlichen Gruppen durch gebrochene lineare Substitutionen.* J. für Math. 127 (1904), 20-50.
2. *Neue Begründung der Theorie der Gruppencharaktere.* Sitzber. Preuss. Akad. Wiss. (1905), 406-432.
- 2a. *Zur Theorie der vertauschbaren Matrizen.* J. für Math. 130 (1905), 66-76.
3. *Arithmetische Untersuchungen über endliche Gruppen linearer Substitutionen.* Sitzber. Preuss. Akad. Wiss. (1906), 164-184.
4. *Untersuchungen über die Darstellung der endlichen Gruppen durch gebrochene lineare Substitutionen.* J. für Math. 132 (1907), 85-137.
5. *Beiträge zur Theorie der Gruppen linearer homogener Substitutionen.* Trans. Am. Math. Soc. 10 (1909), 159-175.
6. *Über die Darstellung der symmetrischen und der alternierenden Gruppen durch gebrochene lineare Substitutionen,* J. für Math. 139 (1911), 155-250.
7. *Über Gruppen periodischer Substitutionen.* Sitzber. Preuss. Akad. Wiss. (1911), 619-627.
8. *Über Gruppen linearer Substitutionen mit Koeffizienten aus einem algebraischen Zahlkörper.* Math. Ann. 71 (1911), 355-367.
9. *Einige Bemerkungen zu der vorstehenden Arbeit des Herrn A. Speiser.* Math. Zeit. 5 (1919), 6-10.

Scott, W. M.

1. *Matrix algebras over an algebraically closed field.* Ann. of Math. 43 (1942), 534-553.

Sehgal, S. K.

1. *On P. Hall's generalization of a theorem of Frobenius.* Proc. Glasgow Math. Assoc. 5 (1962), 97-100.
- Shimura, G.
1. *On an ideal in the center of a Frobenius algebra.* Sci. Papers Coll. Gen. Ed. Tokyo 2 (1952), 117-124.
- Shiratani, K.
1. *On the characters and character rings of finite groups.* Mem. Kyusyu Univ. Ser. A, no. 2, 11 (1957), 99-115.
- Shoda, K.
1. *Über die monomialen Darstellungen einer endlichen Gruppe.* Proc. Phys.-Math. Soc. Jap. (3) 15 (1933), 249-257.
- Snapper, E.
1. *Completely indecomposable modules.* Can. J. Math. 1 (1949), 125-152.
- Solomon, L.
1. *The Schur index.* Ph. D. thesis, Harvard University, 1958.
  2. *The representation of finite groups in algebraic number fields.* J. Math. Soc. Japan 13 (1961), 144-164.
  3. *On Schur's index and the solutions of  $G^n = 1$  in a finite group.* Math. Zeit. 78 (1962), 97-115.
- Speiser, A.
1. *Zahlentheoretische Sätze aus der Gruppentheorie.* Math. Zeit. 5 (1919), 1-6.
  2. *Die Theorie der Gruppen von endlicher Ordnung.* 3rd ed., Berlin, 1937.
- Srinivasan, B.
1. *A note on blocks of modular representations.* Proc. Cambridge Phil. Soc. 60 (1964), 179-182.
  2. *The modular representation ring of a cyclic  $p$ -group.* Proc. London Math. Soc. (3) 14 (1964), 677-688.
- Steinberg, R.
1. *Complete sets of representations of algebras.* Proc. Am. Math. Soc. 13 (1962), 746-747.
- Steinitz, E.
1. *Rechteckige Systeme und Moduln in algebraischen Zahlenkörpern, I, II.* Math. Ann. 71 (1911), 328-354; 72 (1912), 297-345.
- Suprunenko, D. A.
1. *On irreducible nilpotent matrix groups.* Mat. Sb. (N.S.) 77 (1954), 501-512.
- Suzuki, M.
1. *On finite groups with cyclic Sylow subgroups for all odd primes.* Am. J. Math. 77 (1955), 657-691.
  2. *The nonexistence of a certain type of simple group of odd order.* Proc. Am. Math. Soc. 8 (1957), 686-695.
  3. *On characterizations of linear groups, I, II.* Trans. Am. Math. Soc. 92 (1959), 191-204, 205-219.
  4. *On finite groups containing an element of order four which commutes*

*only with its powers.* Ill. J. Math. 3 (1959), 255-271.

5. *Applications of group characters.* Proc. Symp. Pure Math. vol. I (Finite Groups), Providence, 1959, 88-99.
6. *Applications of group characters.* Report, Summer Inst. Finite Groups, Pasadena, 1960, 256-263.
7. *Finite groups with nilpotent centralizers.* Trans. Am. Math. Soc. 99 (1961), 425-470.
8. *On characterizations of linear groups, III.* Nagoya Math. J. (to appear).
9. *On a finite group with a partition.* Archiv. der Math. 12 (1961), 241-254.
10. *On the existence of a Hall normal subgroup.* J. Math. Soc. Japan 15 (1963),

Swan, R.

1. *Projective modules over finite groups.* Bull. Am. Math. Soc. 65 (1959), 365-367.
2. *Induced representations and projective modules.* University of Chicago, 1959. Mimeographed notes.
3. *The p-period of a finite group.* Ill. J. Math. 4 (1960), 341-346.
4. *Induced representations and projective modules.* Ann. of Math. 71 (1960), 552-578.
5. *Projective modules over group rings and maximal orders.* Ann. of Math. 76 (1962), 55-61.
6. *The Grothendieck ring of a finite group.* Topology 2 (1963), 85-110.

Tachikawa, H.

1. *On algebras of which every indecomposable representation has an irreducible one as the top or the bottom Loewy constituent.* Math. Zeit. 75 (1961), 215-227.

Takahashi, S.

1. *Arithmetic of group representations.* Tôhoku Math. J. (second series) 11 (1959), 216-246.
2. *On rational characters of a finite group.* Can. J. Math. (to appear).
3. *Some properties of the group ring over rational integers of a finite group.* Pacific J. Math. (to appear).

Taketa, K.

1. *Über die Gruppen, deren Darstellungen sich sämtlich auf monomiale Gestalt transformieren lassen.* Proc. Jap. Imp. Acad. 6 (1930), 31-33.

Tamaschke, O.

1. *S-Ringe und verallgemeinerte Charaktere auf endlichen Gruppen.* Math. Zeit. 84 (1964), 101-119.
2. *S-rings and the irreducible representations of finite groups.* J. of Algebra 1 (1964), 215-232.

Taussky, O.

1. *Matrices of rational integers.* Bull. Am. Math. Soc. 66 (1960), 327-345.

Thrall, R. M.

1. *Modular representations induced by ordinary representations.* Bull. Am. Math. Soc. 50 (1944), 335.

2. *Some generalizations of quasi-Frobenius algebras.* Trans. Am. Math. Soc. 64 (1948), 173-183.
- Troy, A.
- Integral representations of cyclic groups of order  $p^2$ .* Ph. D. thesis, University of Illinois, 1961.
- Tuan, H. F.
- On groups whose orders contain a prime to the first power.* Ann. of Math. 45 (1944), 110-140.
- Tucker, P.
- On the reduction of induced representations of finite groups.* Ph. D. thesis, University of Wisconsin, 1961.
  - On the reduction of induced representations of finite groups.* Am. J. Math. 84 (1962), 400-420.
  - Note on the reduction of induced representations.* Am. J. Math. 85 (1963), 53-58.
  - Endomorphism ring of an induced module.* Mich. Math. J. 12 (1965), 197-202
- van der Waerden, B. L.
- Gruppen von linearen Transformationen.* New York, 1948.
  - Modern Algebra.* vols. I, II. Ungar, New York, 1949.
- Walter, J. H.
- On the characterization of linear and projective linear groups, I, II.* Trans. Am. Math. Soc. 100 (1961), 481-529; 101 (1961), 107-123.
  - Note on the radical of a group algebra.* Proc. Camb. Phil. Soc. 54 (1957), 128-130.
  - Group algebras with central radicals.* Proc. Glasgow Math. Assoc. 5 (1962), 103-106.
  - Group algebras with radicals of square zero.* Proc. Glasgow Math. Assoc. 5 (1962), 158-159.
- Wedderburn, J. H. M.
- Lectures on matrices.* Am. Math. Soc., New York, 1934.
- Weyl, H.
- Commutator algebra of a finite group of collineations.* Duke Math. J. 3 (1937), 200-212.
  - The classical groups.* Princeton University Press, Princeton, 1939.
  - Algebraic theory of numbers.* Princeton University Press, Princeton, 1940.
  - Symmetry,* Princeton University Press, Princeton, 1952.
- Wielandt, H.
- Über die Existenz von Normalteilern in endlichen Gruppen.* Math. Nachrichten 18 (1958), 274-280.
- Wigner, E. P.
- Group theory and its applications to the quantum mechanics of atomic spectra.* Academic Press, New York. 1959.
- Witt, E.
- Über die Kommutativität endlicher Schiefkörper.* Hamb. Abh. 8 (1930),

413.

2. *Die algebraische Struktur des Gruppenringes einer endlichen Gruppe über einem Zahlenkörper.* J. für Math. 190 (1952), 231-245.

Zariski, O., Samuel, P.

1. *Commutative Algebra, vol. I.* van Nostrand, Princeton, 1958.

Zassenhaus, H.

1. *Kennzeichnung endlicher linearer Gruppen als Permutationsgruppen,* Hamb. Abh. 11 (1936), 17-40.
2. *Über endliche Fastkörper.* Hamb. Abh. 11 (1936), 187-220.
3. *Neuer Beweis der Endlichkeit der Klassenzahl bei unimodularer Äquivalenz endlicher ganzzahliger Substitutionsgruppen.* Hamb. Abh. 12 (1938), 276-288.
4. *The theory of groups.* 2nd ed., Chelsea, New York, 1949.

Zassenhaus, H., Reiner, I.

1. *Equivalence of representations under extensions of local ground rings.* Ill. J. Math. 5 (1961), 409-411.

# Index

## A

Abelian groups, 10-13  
Abelian group of ideal classes, 112  
Abelian normal subgroup of  $G$ , 236  
Absolute irreducibility, 202  
Absolutely irreducible  $KG$ -modules, 214-215, 292  
Algebra over a field, 43  
    tensor products of, 71-73  
Algebraic integers, 102-107  
    definition of, 103  
Algebraic number, norm of, 131-133  
Algebraic number theory, 91-154  
Algebras, over algebraically closed fields, 203  
    Frobenius, 409-452  
    representations of, 38-49  
Algorithm used in  $S_n$ , 197  
Annihilator, 97, 395  
Artin theorem of induced characters, 279-282, 550  
Ascending central series, 15  
Ascending chain condition, 55  
Associative non-degenerate bilinear form, 415, 424  
Associativity of the tensor product, 67  
Automorphism, 5  
Averaging over a finite group, 42, 420

## B

Balanced map, 60-61  
Base field, separable extensions of, 459-463  
Basis, 52, 381

$B$ -equivalent modules, 568-570  
Bilinear mapping, definition of, 59  
Binding function, 504, 520  
    definition of, 500  
Binding system, 500  
Blichfeldt's theorem, 348, 356  
Block, 378, 604-611  
    belonging to the same, 379-380  
    defect of, 611-618  
    of defect 0, 611-613  
    direct sum of, 379  
    of  $KG$ , 604  
    number of characters belonging to, 643-645  
Block distribution of classes, 635-638  
Block idempotents, 604  
Block theory for groups with normal  $p$ -subgroups, 627-635  
Bounded representation type, definition of, 431  
Brauer character, 588  
    of  $T$ , 589  
Brauer-Feit theorem, 643-645  
Brauer-Nesbitt theorem, 215-216, 585-586, 611-614  
Brauer-Suzuki theorem, 276-278  
Brauer theorem, 591-592, 602, 642-643  
Brauer theorem on induced characters, 283-292, 294  
Brauer theorem on splitting fields, 292-295  
 $B$ -source, definition of, 438  
Burnside's criterion for solvable groups, 239-241  
Burnside theorem, 182, 232-233  
    analogue of, 233  
Burnside theorem of linear groups, 251-252

## C

- Canonical homomorphism, 6  
 Canonical invariants determined uniquely by  $M$ , 513  
 Cartan invariants, 590-598  
 Cartan matrix, 593  
 Cauchy sequence, 119  
 Center of the group, 6  
 Central idempotents, 172, 233-239  
 Centralizer, 8  
 Centralizer of  $H$  in  $G$ , 10  
 Centralizer of an  $R$ -module, 53  
 Centralizers of modules over symmetric algebras, 440-448  
 Central series, ascending, 15  
 Character,  
     afforded by a module, 209-210  
     of a direct sum, 211  
     of  $G$  constant on  $S$ , 243  
 Characteristic polynomial,  
     of  $A$ , 207-209  
     of a matrix, 207  
 Characteristic roots, 207  
 Characteristic subgroup, 7-8  
 Characters, exceptional, 275  
 Characters, generalized, 272  
     linear, 272  
     one-dimensional, 272  
 Characters, induced, 265-311  
 Characters, product of, 211  
 Characters, rational, 279-283  
     definition of, 279  
 Character table of a group, as determined by constants, 237-238  
 Character tables, 224-228  
     of  $A_4$ , 226  
     of  $A_5$ , 238  
     of  $S_3$ , 225-226  
     of  $S_4$ , 226-228  
 Chinese remainder theorem, 112-113, 303  
 Class equation, 8  
 Classes of finite-dimensional algebras over  $K$ , 440  
 Class function, 210, 241, 266  
 Class number of a field, 126  
 Clifford's theorem, 343-344  
 Coboundaries, definition of, 521  
 Cocycles, definition of, 521  
 Cohomology group, definition of, 521  
 Cohomology theory of associative algebras, 486  
 Column permutations, 191, 193-194, 197  
 Commutative law for finite skewfields, 458-459  
 Commutator subgroup, 15  
 Commuting unitary matrices, 256, 257-259  
 Complete field with respect to a valuation, 120  
 Completely primary ring, 371-372  
 Completely reducible matrix representation, 40  
 Completely reducible modules, 86-90, 163-173  
     definition of, 86  
 Completely reducible representation, 39  
 Completely reducible set of linear transformations, 254-255  
 Component of  $M$ , definition of, 409  
 Composition factors, 15, 77, 375, 378-379  
 Composition factors of  $M$ , sum of the characters of, 211  
 Composition series, 14-15, 76-81, 368, 373-374  
     definition of, 77  
     equivalent, 77  
     length, 77

- Conjugate character, 304, 630, 641-643  
 $p$ , 641
- Conjugate classes, 8-10, 190 of  $G$ , 187 in  $S_n$ , 10
- $K$ -Conjugate elements, 306
- Conjugate ideal, 125
- Conjugate representation, 471
- Content of a polynomial, 106-107, 118
- Contragredient module, 318
- Contragredient representation, 318
- Convergent sequence, 120
- Coordinate functions, 182
- Cyclic group, 34-35 of prime order, 506-515
- Cyclic module, 52, 97-99
- Cyclotomic fields, 135, 136, 137, 138-144, 265
- Cyclotomic polynomial, 137
- Cyclic  $p$ -Sylow subgroup, 431
- D**
- Decomposable  $G$ -module, 519
- Decomposable module, definition of, 81, 496-497
- Decomposition matrix, definition of, 591
- Decomposition numbers, 590, 591, 592, 593, 594-598 definition of, 591
- Dedekind domain, 108 modules over, 144-155
- Defect of a block, 611-618
- Defect of a class, 618
- Defect group of a block, 618, 623
- Defect group of a class, 618
- Defect groups, 618-634
- Degree of  $\mu$ , 272
- Degree of a representation, 30
- Degrees of the irreducible projective representations of  $G$ , 364
- Degrees of the irreducible representations of a finite group  $G$ , 236
- de Leeuw-Reiner theorem, 529-530
- Derived series, 16
- Descending chain condition, 55
- Determinantal divisor, 96
- Determinant ideal, 566
- Determinant of a linear transformation, 29
- Deuring-Noether theorem, 200, 538
- Diagonal subgroup, 315
- Diagram, 191, 197
- Dickson corollary, 439-440, 601
- Diederichsen-Reiner theorem, 508, 509, 510-514
- Dihedral group, 22, 334, 339, 342  $D_6$  of order 12, 646-648 of order 10, 238
- Direct product external, 11 internal, 11 of matrices, 69
- Discrete valuation, 116
- Discriminant of a field, 143
- Disjoint cycles, 2-3
- Disjoint modules, 328
- Disjoint orbits, 337
- Divisible module, 386-387
- Division algebra, 180
- Double centralizer property, 175-177, 403, 405
- Double centralizer theorem, 405-406
- Double cosets, 4-5
- Doubly transitive, 7
- Doubly transitive permutation group, 230-231
- Dual bases, 423

Dual module, 317, 394  
 Dual space, 316-317

**E**

Eckmann-Schopf theorem, 390-391  
 Eisenstein criterion, 140  
 Elementary divisors, 599  
     of  $G$ , 12  
     of a matrix, 101-102  
 Elementary divisor theorem, 12-13,  
     264, 403  
 Elementary subgroup, 284, 302, 476  
 Enveloping algebra, 464  
     definition of, 43  
 Equivalence  
     of induced modules, 328-329  
     integral, 494, 515  
      $P$ -integral, 531-542  
     of a representation, 30  
 Equivalent composition series, 77  
 Equivalent ideals, 125-126  
 Equivalent matrices, 94  
 Equivalent representations, 515  
     definition of, 494  
 Equivalent valuations, 117  
 Exact sequence, 381  
 Exceptional characters, 275  
 Existence of normal subgroups in a  
     group, 241-250  
 Exponent of a group, 37, 292  
 Extension, 381  
     of an algebra, 488  
     of a ground field, 198-206  
     of a group, 23  
     of an ideal, 133-134  
     of a module, 486  
 External direct product, 11  
 External direct sum, 11, 52

**F**

Factor commutator group, 16  
 Factor groups, 3-8  
 Factor module, 53  
 Factor set, 349, 488  
 Factors of the normal series, 14  
 Faithful irreducible representation,  
     232  
 Faithful module, 178  
 Faithful representation, 279  
 Field, class number of, 126  
 Field of  $P$ -adic numbers, 121  
 Field of scalars of a vector space,  
     extension of, 70-71  
 Finite abelian groups 10-13, 36-38  
 Finite-dimensional algebra, 188  
     over an algebraically closed field,  
     181-182  
     injective modules for, 409-413  
 Finite dimensional over  $K$ , 157-158  
 Finite group, representation of, 30  
 Finitely generated module, 52, 381  
 Finitely generated periodic subgroup,  
     252-254  
 Finite nilpotent group, 356  
 Finite periodic subgroup, 251-252  
 Finite representation type  
     definition of, 431  
     group algebras of, 431-435  
 Finite subgroups of rotation group  $O_3$   
     in three-dimensional Euclidean  
     space, 329-330  
 First regular representation, 413  
 Fractional ideal, 107, 125-126, 146, 150  
 Free (left)  $R$ -module, 52  
 Frobenius algebras, 367, 409-452, 459-  
     463  
     definition of, 413  
     dual bases of, 423

- generalization of the orthogonality relations, 419  
 injective and projective modules for, 420-426  
 multiplicity relations for, 418, 419, 420  
 Frobenius algebras over perfect fields, general multiplicity theorem for, 419  
 Frobenius reciprocity theorem, 271, 279, 327, 333, 477  
 Frobenius-Schur theorem, 183, 184, 185, 186  
 Frobenius theorem, 179-190, 242, 295-301  
 Frobenius-Wielandt theorem, existence of normal subgroups in a group, 241-250  
*F*-trace, 477

**G**

- Gaschutz-Ikeda-Higman theory, 453, 461  
 Gaschutz-Ikeda operator, 481  
 Gaschutz's theorem, 421  
 generalization of, 426, 427, 428, 429, 430  
 Ikeda's generalization of, 425-426

Generalized character, 272

- lying in  $K$ , 311  
 ring of, 285

Generalized decomposition numbers, 638-641  
 definition of, 638

Generalized derivation, definition of, 487

Generalized induction theorem, 301-311

Generalized quaternion groups, 23, 334, 339-340, 342

General linear group, 28

Generators, set of, 381

Genus, 567-578

definition of, 570

*G*-equivalence, 1

( $G, H$ )-injective, 427

Global theory of projective modules, 550-558

*G*-module, definition of, 559, 567

Grothendieck rings, 550

Ground field, extension of, 198, 199, 200-206

Group algebra, 43-44

of finite representation type, 431-435

Group character

definition of, 210

theory of, 207-264

Group of a given order, 651-652

Group representations, 38-49

Group of rotations of the cube, 331-333

Group ring, 44

units in, 262-264

Group whose Sylow groups are cyclic, 334

**H**

Hall theorem, 301

Height, 644

Heller theorem, 542

Hermitian form, 49, 254

Holomorph, 22

Homogeneous components, 345, 347-348

Homomorphism, 6-7

Hyper-elementary subgroup, 302

## I

Ideal in an algebraic number field, 107  
 Ideal classes, 123-135, 130, 146  
 Ideals, 107-115  
   extensions of, 133-134  
   fractional, 107  
   inverse, 109  
   maximal, 107  
   norm of, 123-124  
   prime, 107-108, 110-112  
   product of, 109  
   proper, 108, 110  
   sum of, 109  
 Idempotent element, 164  
 Idempotents, 160-161  
   orthogonal set of, 165  
 Ikeda's generalization of Gaschütz's theorem, 425-426  
 Imprimitive modules, 346-348  
   definition of, 346  
 Imprimitivity system, 346  
 Indecomposability, 12, 81  
 Indecomposable cyclic submodule, 98  
 Indecomposable  $G$ -module, 519  
 Indecomposable integral representations of a cyclic group of square-free order, 581  
 Indecomposable integral representations of the dihedral group of order  $2p$ , 581  
 Indecomposable modules, 81-86, 578-581  
   definition of, 81, 497  
   vertex and source of, 435-440  
 Indecomposable two-sided ideal, 378-379  
 Index of  $D$ , definition of, 458  
 Index of  $H$  in  $G$ , 4

Induced characters, 265-311  
   Artin's theorem of, 279-282  
   Brauer's theorem of, 283-292  
   definition of  $\mu^G$ , 265-266  
 Induced matrix representation, 314  
 Induced modules, 73-75, 314-323  
   equivalence of, 328-329  
   irreducibility of, 328-329  
   definition of  $M^G$ , 73  
 Induced monomial representation, 314, 329  
 Induced representations, 73-75, 313-365  
 Induction, transitivity of, 267  
 Induction theorem, generalized, 301-311  
 Inertia group, 346, 631  
 Injective hull, definition of, 389  
 Injective modules, 384-393, 410-411  
   definition of, 385-386  
   for a finite-dimensional algebra, 409-413  
   for a Frobenius algebra, 420-426  
   relative, 426-430  
 Inner binding function, 504, 520  
   definition of, 501  
 Inner generalized derivation, definition of, 487  
 Inner product of characters, 222-223, 270  
 Inner tensor product, 315  
 Integers, algebraic, 102-107  
 Integral domain, 91  
 Integral ideal, 107, 111-114, 153-154  
 Integrally closed, 106  
 Integral representations, theory of, 493-578  
 Internal direct product, 11  
 Internal direct sum, 51  
 Intertwine, 198-199  
 Intertwining number, 319-320, 375

- Intertwining number theorem, 323-328, 340-342  
proof of, 327
- Invariance, 2
- Invariant, 319-320
- Invariant factors, 94, 151
- Invariant factor theorem, 12-13, 150-153, 403  
for matrices, 94-97  
for modules, 97-98
- Inverse different, definition of, 525
- Inverse ideal, 109
- Invertible element, 28
- Irreducibility of induced modules, 328-329
- Irreducible  $G$ -module, 519
- Irreducible submodules of the tensor space  $V$ , 449
- Irreducible matrix representation, 40
- Irreducible modules, 76  
absolute irreducibility of, 202  
for particular groups, 313  
restriction to normal subgroups, 342-346
- Irreducible monomial representation, 347
- Irreducible representation, 39  
of a direct product, 189-190  
of a nilpotent group, 355-358  
products of, 231-233  
projective representation, 349  
of the symmetric group, 190, 191, 192-198
- Irreducible tensor representations of  $GL(V)$ , 449-452
- Ito's theorem, 365
- Jordan-Hölder theorem, 15, 79, 506
- Jordan theorem on linear groups, 250-262  
proof of, 258-262
- Jordan-Zassenhaus theorem, 494, 558-563  
for the case when  $M$  is absolutely irreducible, 573  
proof of, 559-563
- K**
- Kasch-Kneser-Kupisch theorem, 433-434
- $K$ -character of  $G$ , 476
- $K$ -conjugate character, 304
- $K$ -conjugate elements, 306
- $K$ -elementary subgroup, 302, 476
- $K$ -equivalent representations, 515
- Kernel of an extension of a module, 486
- $K$ -homomorphisms, 26
- $K$ -linear transformations, 26
- Kronecker or direct product of matrices, 69
- Krull-Schmidt theorem, 83-85, 201-202, 373, 383, 403-404, 414, 432, 437  
applied to  $G$ -modules, 542  
applied to  $G^*$ -modules, 540-541, 548
- L**
- Left  $A$ -module, 47
- Left annihilator, 395
- Length of the composition series, 77
- Left cosets, 3-4
- J**
- Jones theorem, 579-580

Left  $G$ -module, 46  
 Left ideals, 50  
 Left minimum condition, 157  
 Left multiplication, 3  
 Left noetherian ring, 55, 56  
 Left regular module, 48, 50  
 Left  $R$ -modules, definition of, 50  
 Left socle, definition of, 394  
 Levi-Malcev theorem for Lie algebras, 486  
 Lifting idempotents, 545  
 Linear character, 272, 362  
     on  $\bar{A}$ , 606  
 Linear groups, Jordan, Burnside, and Schur theorems, 250-262  
 Linearly dependent set of functions, 182  
 Linear transformations, 26-30  
     definition of, 26  
 Linked, 378  
 Local theory of projective modules, 542-550

**M**

Mackey theorem, 323-328, 341-342, 353-355  
 Maranda's theorem, 539-540, 568-570  
 Maschke's theorem, 41, 88, 355, 423, 501  
     matrix analogue of, 501-502  
 Matrices, equivalent, 94  
     invariant factor theorem, 94-97  
 Matrices over a field, 27  
 Matrix, characteristic polynomial, 207  
 Matrix, trace of, 207  
 Matrix representation, 30  
     afforded by an  $A$ -module, 47  
     afforded by a representation space, 31

Matrix with respect to a basis, 27  
 Maximal ideal, 107  
 Maximal related extension, definition of, 389-390  
 Maximal submodule, 77  
 Maximum principle, 56, 88-89  
 Metabelian groups, 357  
 Metacyclic group  $G$ , definition of, 333-334  
 Metacyclic groups, representations of, 333-340  
 $M$ -group, 357-358  
 Minimal left ideal, definition of, 163  
 Minimal submodule, 77  
 Minimum polynomial of a matrix, 179  
 Möbius inversion formulas, 136-137  
 Möbius  $\mu$ -function, 136  
 Möbius transform, 136  
 Modular character, 588  
 Modular representation, 532, 583-584  
     associated with  $T$ , 584  
 Modules,  
     over Dedekind domains, 144-155  
     indecomposable, 81-86  
     injective, 384-393  
     invariant factor theorem for, 97-98  
     over orders, 515-531  
     over principal ideal domains, 91-102  
     projective, 380-384  
     over quasi-Frobenius rings, 403-408  
     tensor product of, 211  
 Modules, principal indecomposable, 367-377  
     classification into blocks, 377-380  
     definition of, 369  
 Monic polynomial, 102-103  
 Monomial representation, 314, 321, 355-358  
 Morita-Tachikawa theorem, 397-398  
 Multiplicity-free representations, 340-342

- Multiplicity relations for Frobenius algebras, 418-420  
 Multiplicity theorem for Frobenius algebras over perfect fields, 419  
 Multiplier, 359

**O****N**

- Nagao-Nakayama theorem, 412-413  
 Natural homomorphism, 6  
 Natural mapping, 53  
 $n$ -dimensional right vector space, 173-175  
 Nilpotent element, 159-160  
 Nilpotent groups, 14-17  
     irreducible representations of, 355-358  
 Nilpotent ideal, 160-162  
 Noether-Deuring theorem, 200-202  
 Noetherian module, 55  
 Noetherian ring, 55, 106  
 Non-Archimedean valuation, 116  
 Non-degenerate bilinear form, associative, 415, 424  
 Non-degenerate pairing, 397  
 Non-semi-simple rings, 367-408  
 Non-singularity of the Cartan matrix, 550, 602  
 Norm, 127  
 Norm of an algebraic number, 131-133  
 Normalized factor set, 361  
 Normalizer of  $H$  in  $G$ , 10  
 Normal series, 14  
     factors of, 14  
 Normal subgroup, 5  
     criteria for existence of, 654, 241-250  
     restriction of irreducible modules, 342-346  
 Norms of ideals, 123-135

- Nucleus, 442  
 Numerical bounds, 645-646
- Octahedral groups, 329-333  
 One-character, 222  
 One-dimensional characters, 272  
 One-dimensional representations, 36-38  
 One-representation, 222  
 Orbits, 1-3  
 Order, 97, 516  
 Order of cyclotomic polynomial, 137  
 Order ideal, 96, 563-567  
     of  $M$ , definition of, 564  
 Orders, modules over, 515-531  
 Orthogonal idempotents, 165, 369  
 Orthogonality relations, 217-224, 300, 304, 598-604  
     simple applications of, 224-233  
 Orthogonality relations for Frobenius algebras, 419  
 Orthogonal set of idempotents, 165  
 Osima theorem, 610  
 Outer tensor product, 315

**P**

- $P$ -adic integers, 117  
 $P$ -adic number field, 121  
 $P$ -adic numbers, valuations, 115-123  
 $P$ -adic valuation, definition of, 116-117  
 Pairing, 396-397  
 Pairwise relatively prime, 112  
 Pairwise relatively prime integral ideals, 112-113  
 Partially ordered set, 89, 385  
 Partition of  $n$ , 9-10, 190

- p*-elementary divisors, 599  
*p*-elementary subgroup, 284-285  
 Perfect field, 376-377  
     definition of, 464  
 Periodic of bounded period, 250  
 Periodic group, 250  
 Permutation groups, 1-3, 228-231  
 Permutation matrix, 31-34  
 Permutation representations, 31, 314  
*p*-group, 8-9  
*P*-integral elements of a field, 117  
*P*-integral equivalence, 531-542  
*p*-irregular, 584  
*P<sup>k</sup>*-modular representation of *G* of  
     degree *m*, definition of, 532  
 Polynomial, content of, 106-107, 118  
 Positive definite hermitian form, 49,  
     254  
*p*-part, 477  
*p*-rank for a matrix *X* over *Z*, 591  
*p*-regular, 283-284, 584  
*p*-regular classes, 288  
*p*-regular components, 284  
 Primary component, 11  
 Prime ideal, 107-108, 110-112, 124-  
     125  
 Primitive idempotent, 172, 369  
 Primitive *n*th root of 1, 136-138  
 Primitive polynomial, 103  
 Principal character, 222  
 Principal ideal, 113-114  
 Principal ideal domain, 91  
     modules over, 91-102  
 Principal indecomposable modules,  
     367-377, 410  
     classification into blocks, 377-380  
     definition of, 369  
 Product of characters, 211  
 Product of ideals, 109  
 Product modules, 267-269  
 Product of modules, 211  
 Products of irreducible representa-  
     tions, 231-233  
 Projection, 41-42  
 Projections associated with a given  
     direct sum decomposition, 54  
 Projective class group, 557  
 Projective *G*-module, as determined by  
     its behavior mod *p*, 543-547  
 Projective module, 148-149, 380-384,  
     409  
     for a Frobenius algebra, 420-426  
     global theory, 550-558  
     local theory, 542-550  
     relative, 426-430  
 Projective relative to *H*, 427  
 Projective representations, 348-355  
     definition of, 349  
     irreducible, 349  
     Schur's theory of, 358-365  
 Proper ideal, 108, 110  
*p*-singular, 284, 288, 584  
*p*-singular component, 284  
*p*-Sylow subgroup, 17-20  
     of *G*, 239-241  
 Pure submodule, 100

**Q**

- Quasi-Frobenius algebras, 413-420  
     definition of, 413  
 Quasi-Frobenius rings, 367, 393-403  
     definition of, 395-396  
     modules over, 403  
*Q*-elementary subgroups, 302  
*Q*-equivalent, definition of, 494

**R**

- Radical, definition of, 162

- Radical of a ring with minimum condition, 159-163
- Rank, 93
- Rank of a module, 145
- Rational characters, 279-283  
definition, 279
- R*-basis, 52
- Realizable matrix representation, 293
- Realizable in a subfield, 464
- Reduced regular module, 404
- Reducible, 519
- Reducible matrix representation, 40
- Reducible module, 77
- Reducible representation, 39
- Regular matrix representation, 32-34
- Regular module with respect to the pairing  $\tau$ , 442
- Regular representation, 32
- Reiner-Nakayama theorem, 542-543, 550-551
- Reiner theorem, 574-578
- Related extension. definition of, 389-390
- Relative homological algebra, 420
- Relatively prime, 112
- R*-endomorphisms, 53
- Representation-group, definition of, 361
- Representations  
of an algebra, 45  
of  $G$  by matrices with entries in a ring  $R$ , 493  
induced, 313-365  
of metacyclic groups, 333-340  
multiplicity free, 340-342
- Representations, projective, 348-355  
definition of, 349  
irreducible, 349  
Schur's theory of, 358-365
- Representation space, 30
- R*-equivalent representations, 515
- Restriction to normal subgroups of irreducible modules, 342-346
- R*-free, 52
- R*-homomorphism, 53
- Right annihilator, 395
- Right cosets, 3-4
- Right ideals, 50
- Right minimum condition, 157
- Right regular module, 50
- Right socle, definition of, 394
- Ring of generalized characters, 272, 285
- Rings, non-semi-simple, 367-408
- Ring with minimum condition  
definition of, 157  
radical of, 159-163
- R*-linear combination, 52
- Roquette's simplification of proof of Brauer's theorem, 301
- R*-order, definition of, 516
- Rotations of the cube, group of, 331-333
- Row permutations, 191, 197
- R*-reducible, 519
- R*-torsion-free, 52

## S

- Schur index, 292-295, 453, 463-479  
computation of, 470-471  
definition of, 293
- Schur index of  $U$  with respect to  $k$ ,  
definition of, 466
- Schur's lemma, 80, 181, 350, 475  
converse of, 189
- Schur theorem, 24, 249, 361-362
- Schur theorem of linear groups, 250-262  
proof of, 252-258
- Schur's theory of projective representations, 358-365
- Second regular representation, 413

- Semi-direct products, 21-23  
 Semi-simple, 162  
 Semi-simple ring  $R$ , simple components of, 170  
 Semi-simple rings, 163-173  
 Separability, intrinsic criterion for, 481-485  
 Separable algebras, 453-492  
     definition of, 480  
 Separable extensions of the base field, 459-463  
 Sequence, exact, 381  
 Series, composition, 76-81  
 Set of generators, 381  
 Simple components, 170  
 Simple groups, characterizations of, 652-654  
 Simple ring, 168-169  
     structure of, 173-179  
 Skewfield, 167-168, 173-175  
 Skew symmetric tensors, 452  
 Socle, definition of, 394  
 Solvable groups, 14-17  
 Solvable groups, Burnside's criterion for, 239-241  
 Source, definition of, 438  
 Source and vertex of an indecomposable module, 435-440  
 Split extension, 23-24, 381, 486, 488  
 Split factor set, definition of, 489  
 Splitting fields, 265, 453-492  
     for an algebra, 202, 455  
     Brauer's theorem on, 292-295  
     cyclotomic, 135-144  
     for division algebras, 453-459  
     for a group, 203  
     for simple algebras, 453-459  
 Splitting field theorem for characteristic  $p$ , proof of, 474-475  
 Square-free order group, 334  
 $(S, R)$ -bimodule over the rings  $R$  and  $S$ , 66  
 Subalgebra, 43  
 Subgroups, 3-8  
 Subgroup theorem, 324-325, 437  
 Submodule, 50  
 Subordinates, 622, 628  
 Subsets of a ring, 158-159  
 Sum of ideals, 109  
 Swan theorem, 543-550, 552-558  
 Sylow subgroups, 17-21  
 Symmetric algebra, 401  
     definition of, 440  
 Symmetric algebras, centralizers of modules over, 440-448  
 Symmetric group  
     irreducible representations of, 190-198  
      $S_4$ , 648-650  
 Symmetric tensors, 452  
 Symmetry operator, 450  
 System of imprimitivity, 346

## T

- Table, 191, 197  
 Tensor product, 59-76  
     of algebras over a field, 71-73  
     of modules, 62, 313  
     representation, 69  
     of two induced modules, 323, 325  
     of vector spaces, 67-70  
 Tensor product theorem, 323-328  
     proof of, 325-326  
 Tensor space  $V$ , 449  
 Tetrahedral groups, 329-333  
 Torsion-free, 92  
 Torsion-free element, 97  
 Torsion-free element of  $R$ -module, definition of, 564  
 Torsion-free module, 97  
 Torsion module, 97, 564

- Totally ordered set, definition of, 385  
 Trace of a matrix, 29, 207  
 Transitive, 2  
 Transitive imprimitive module, 346-347  
 Transitive permutation representation, 321  
 Transitivity of induction, 267  
 Transpose, 317  
 Transpose matrix, 317  
 Trivial orbit, 2  
 Two-sided ideal, indecomposable, 378
- U**
- Unimodular matrix, 93  
 definition of, 494  
 over  $R$ , 515  
 Unique factorization domain, 91  
 Unit, 28  
 Unitary basis, 254  
 Unitary group, 49, 254  
 Unitary matrix, 255-256  
 Unitary transformation, 49, 256-258  
 Units in a group ring, 262-264  
 Upper bound of a subset, definition of, 385
- V**
- Valuation, 116  
 $P$ -adic numbers, 115-123
- Valuation ring, 117  
 Value group of a valuation, 116  
 Van der Monde determinant, 34, 105  
 Vertex, definition of, 438  
 Vertex and source of an indecomposable module, 435-440
- W**
- Wedderburn-Malcev theorem, 377, 485-492  
 proof of, 491-492  
 Wedderburn's theorem, 403, 453, 458, 475  
 Wedderburn structure theorem, 157, 175-178, 188-189  
 Wielandt-Frobenius theorem, permutation groups, 246-247  
 Wielandt theorem, 242, 247-248  
 Witt-Bermann induction theorem, 302-311, 475
- Z**
- Zassenhaus-Reiner theorem, 538-539  
 Zassenhaus theorem, 563  
 $Z$ -composition factors, 498  
 $Z$ -composition series, 498  
 $Z$ -equivalent, definition of, 494  
 $ZG$ -module, definition of, 494  
 $Z$ -irreducible, definition, 497  
 Zorn's lemma, 385  
 $Z$ -reducible, definition of, 497