B. Huppert N. Blackburn

Finite Groups II

B. Huppert N. Blackburn

Finite Groups II

Springer-Verlag
Berlin Heidelberg New York 1982

Bertram Huppert
Mathematisches Institut der Universität
Saarstraße 21
D-6500 Mainz

Norman Blackburn
Department of Mathematics
The University
GB-Manchester M13 9 PL

ISBN 3-540-10632-4 Springer-Verlag Berlin Heidelberg New York
ISBN 0-387-10632-4 Springer-Verlag New York Heidelberg Berlin

Library of Congress Cataloging in Publication Data. Huppert, Bertram, 1927–.
Finite groups II. (Grundlehren der mathematischen Wissenschaften; 242).
Bibliography: p. Includes index. 1. Finite groups. I. Blackburn, N. (Norman).
II. Title. III. Series. QA 171.B 577. 512'.22. 81-2287.
ISBN 0-387-10632-4. AACR 2

Typesetting: Asco Trade Typesetting Limited, Chai Wan, Hong Kong.
Printing and bookbinding: Konrad Triltsch, Würzburg
2141/3140-543210

Preface

From "Lohengrin", Richard Wagner

At the time of the appearance of the first volume of this work in 1967, the tempestuous development of finite group theory had already made it virtually impossible to give a complete presentation of the subject in one treatise. The present volume and its successor have therefore the more modest aim of giving descriptions of the recent development of certain important parts of the subject, and even in these parts no attempt at completeness has been made.

Chapter VII deals with the representation theory of finite groups in arbitrary fields with particular attention to those of non-zero characteristic. That part of modular representation theory which is essentially the block theory of complex characters has not been included, as there are already monographs on this subject and others will shortly appear. Instead, we have restricted ourselves to such results as can be obtained by purely module-theoretical means.

In Chapter VIII, the linear (and bilinear) methods which have proved useful in questions involving nilpotent groups are discussed. A major part of this is devoted to the classification of Suzuki 2-groups (see §7); while a complete classification is not obtained, the result proved is strong enough for an application to the determination of the Zassenhaus groups in Chapter XI. The standard procedure involves the use of Lie rings, and rather than attempting a theory of the connection between nilpotent groups and Lie rings, we give a number of applications to such topics as the length of the conjugacy classes of p-groups (§9), fixed point free automorphisms of nilpotent groups (§10), the restricted Burnside problem (§12) and automorphisms of p-groups (§13). In many of these considerations, the finiteness of the group is a relatively unimportant condition, and the last two of these applications depend on the Magnus-Witt theory of the lower central series of free groups, which is described in §11.

The ground-breaking investigations of P. Hall and G. Higman on the theory of p-soluble groups form the basis of Chapter IX. These arose from the restricted Burnside problem and led first to a solution for exponent 6 (see 1.15). Then however there followed far-reaching theorems for composite exponents (4.10, 4.13, 4.17). Besides various estimates of the p-length of a p-soluble group in terms of the structure of its Sylow p-subgroups (§5), we deal with some theorems about fixed point free automorphisms of soluble groups (§6). Finally we discuss the derived notion of p-stability, which will be of considerable use in Chapter X.

The three chapters in this volume are thus all concerned with relations between finite groups and linear algebra, but otherwise they are rather independent of one another, apart from occasional technical references, of course.

The authors must apologize for the length of time which readers have had to wait for this volume. They promise that Volume III will be available within a matter of months.

It is a great pleasure to thank the many colleagues who have helped us in the preparation of this volume and its successor. In this respect the second author must give pride of place to Philip Hall, who first stimulated his interest in the subject more than 25 years ago by combining patient encouragement of a naturally pessimistic student with lectures of a beauty which seems to be lost to subsequent generations. With the writing of the book the greatest help was given by W. Gaschütz and his associates in Kiel, where each year since 1967 our sketches were read and exhaustively studied. The participants in these discussions in the course of the years were H. Bender, D. Blessenohl, W. Caschütz, F. Gross, K. Johnsen, O.-U. Kramer, H. Laue, K.-U. Schaller and R. Schmidt. We are most grateful for the hospitality of the Mathematics Department in Kiel, without which this kind of work would not have been possible. Also we are indebted for financial assistance, enabling the two of us to meet reasonably often, to the National Science Foundation, the Alexander von Humboldt-Stiftung and the University of Manchester.

In the laborious proof-reading B. Hartley (Manchester), O. Manz, J. Pense and W. Willems (Mainz) all spent a great deal of time helping us, and we offer them our most sincere thanks. Also we thank the Manchester secretaries Kendal Anderson, Rosemary Horton and Patricia McMunn for the enormous amount of help they have given us with the typing and preparation of the manuscript.

Finally our thanks are due to Springer-Verlag and to the typesetters and printers for their patience with us and for the excellent quality of the production of this book.

July, 1981

Bertram Huppert, Mainz
Norman Blackburn, Manchester

Index of Symbols

Aut $\mathfrak{X}$ XII
$S_p(\mathfrak{G})$ XII
$\gamma_n(\mathfrak{G})$ XII, 239
$\mathbf{O}_\pi(\mathfrak{G}), \mathbf{O}_{\pi_1,\ldots,\pi_n}(\mathfrak{G}), \mathbf{O}^\pi(\mathfrak{G})$ XIII, 407
$\mathfrak{G}^m$ XII
$\mathsf{A}\mathfrak{G}, \mathbb{Z}\mathfrak{G}, \mathsf{K}\mathfrak{G}$ XII
π' XIII
$\mathbf{H}(\mathsf{V})$ 12
$\mathbf{S}(\mathsf{V})$ 12
V_n 15
$\mathbf{Q}(\mathfrak{A})$ 33
$\mathbf{T}(\mathfrak{A})$ 35
$\mathsf{V}^{\mathfrak{G}}$ 44
${}^{\mathfrak{G}}\mathsf{V}$ 51
V^* 97
$\mathbf{R}(\mathfrak{S})$ 155
$\mathbf{L}(\mathfrak{S})$ 155
$\mathbf{S}_r(\mathfrak{A})$ 155
$\mathbf{S}_l(\mathfrak{A})$ 155
$\mathbf{An}_{\mathfrak{N}}(\mathsf{S}), \mathbf{An}_{\mathsf{V}}\mathbf{J}(\mathfrak{A})$ 155

$\mathsf{P}_{\mathfrak{G}}(\mathsf{V})$ 190
$\mathfrak{R}(\mathsf{V})$ 193
$\mathfrak{N}(\mathsf{V})$ 194
$\mathfrak{R}(\mathscr{B})$ 194
$\mathfrak{N}(\mathscr{B})$ 194
$\mathsf{K}^{\mathfrak{G}}_{\mathfrak{U}}$ 203
$\mathsf{A}^{\mathfrak{G}}_{\mathfrak{U}}$ 204
$\lambda_n(\mathfrak{G})$ 242
$\kappa_n(\mathfrak{G})$ 248
$A(n, \theta)$ 294
$l(\mathfrak{A})$ 318
g^n 320
$\mathsf{g}^{(n)}$ 323
ad x 338
$\mathsf{C}_{\mathsf{g}}(x)$ 338
$(\mathfrak{A}$ on $\mathfrak{B})$ 409
$e_p(\mathfrak{G})$ 449
$\tau_n(\mathfrak{G})$ 449
$e_p^*(\mathfrak{G})$ 449
$SA(2, p)$ 494

Terminology and Notation

In this volume, the same terminology and notation as in Volume 1 will be used, with the following exceptions.

1. The identity mapping on a set X will be denoted by 1_X.

2. The identity element of the group $\mathfrak{G}$ will be denoted by $1_{\mathfrak{G}}$ or 1.

3. By a *section* of a group $\mathfrak{G}$ is meant a group of the form $\mathfrak{H}/\mathfrak{K}$, where $\mathfrak{K} \trianglelefteq \mathfrak{H} \leq \mathfrak{G}$.

4. If $\mathfrak{X}$ is any algebraic system, **Aut** $\mathfrak{X}$ denotes the group of all automorphisms of $\mathfrak{X}$. The group of inner automorphisms of the group $\mathfrak{G}$ is denoted by **Inn** $\mathfrak{G}$.

5. The set of Sylow p-subgroups of the finite group $\mathfrak{G}$ will be denoted by $S_p(\mathfrak{G})$.

6. The *lower central series* (III, 2.2) of the group $\mathfrak{G}$ will be denoted by

$$\mathfrak{G} = \gamma_1(\mathfrak{G}) \geq \gamma_2(\mathfrak{G}) \geq \cdots \geq \gamma_n(\mathfrak{G}) \geq \cdots;$$

here $\gamma_n(\mathfrak{G}) = [\gamma_{n-1}(\mathfrak{G}), \mathfrak{G}]$ for $n > 1$.

7. If $\mathfrak{G}$ is a group and m is a positive integer, $\mathfrak{G}^m = \langle x^m | x \in \mathfrak{G} \rangle$. Thus $\mathfrak{G}^{mn} \leq (\mathfrak{G}^m)^n$.

8. Let A be a commutative ring with identity and let $\mathfrak{G}$ be a group. The *group-ring* of $\mathfrak{G}$ over A (I, 16.6) will be denoted by $\mathsf{A}\mathfrak{G}$.

9. Let $\mathfrak{G}$ be a finite group. The field K is called a *splitting field* of $\mathfrak{G}$ if $\mathsf{K}\mathfrak{G}/\mathbf{J}(\mathsf{K}\mathfrak{G})$ is the direct sum of complete matrix algebras over K, where $\mathbf{J}(\mathsf{K}\mathfrak{G})$ is the Jacobson radical of $\mathsf{K}\mathfrak{G}$. Thus by V, 11.2a), K is a splitting field of $\mathfrak{G}$ if and only if K is a splitting field of $\mathsf{K}\mathfrak{G}/\mathbf{J}(\mathsf{K}\mathfrak{G})$.

This definition is not the same as that given in V, 11.2b), but the two definitions reduce to the same thing when $|\mathfrak{G}|$ is not divisible by char K.

10. A $\mathsf{K}\mathfrak{G}$-module M is called *absolutely irreducible* if (i) M is irreducible and (ii) $\mathrm{Hom}_{\mathsf{K}\mathfrak{G}}(\mathsf{M}, \mathsf{M}) = \mathsf{K}$.

This definition is equivalent to that given in V, 11.8; this is proved in VII, 2.2.

11. The unit matrix will be denoted by I.

12. If π is a set of primes, the complementary set of primes is denoted

by π'; thus

$$\pi' = \{p \mid p \text{ is a prime, } p \notin \pi\}.$$

13. If π is a set of primes, the product of all the normal π-subgroups of the finite group $\mathfrak{G}$ is denoted by $\mathbf{O}_\pi(\mathfrak{G})$. Thus $\mathbf{O}_\pi(\mathfrak{G})$ is the *maximal normal π-subgroup* of $\mathfrak{G}$. Clearly $\mathbf{O}_\pi(\mathfrak{G})$ is a characteristic subgroup of $\mathfrak{G}$ and $\mathbf{O}_\pi(\mathfrak{G}/\mathbf{O}_\pi(\mathfrak{G})) = 1$.

More generally, suppose that $\pi_1, \pi_2, \ldots$ are sets of primes. We define a characteristic subgroup $\mathbf{O}_{\pi_1,\ldots,\pi_i}(\mathfrak{G})$ of $\mathfrak{G}$ by induction on i: for $i > 1$,

$$\mathbf{O}_{\pi_1,\ldots,\pi_i}(\mathfrak{G})/\mathbf{O}_{\pi_1,\ldots,\pi_{i-1}}(\mathfrak{G}) = \mathbf{O}_{\pi_i}(\mathfrak{G}/\mathbf{O}_{\pi_1,\ldots,\pi_{i-1}}(\mathfrak{G})).$$

Examples. a) The Fitting subgroup of $\mathfrak{G}$ is $\prod_p \mathbf{O}_p(\mathfrak{G})$.

b) If p is a prime, the *upper p-series* of $\mathfrak{G}$ (VI, 6.1) is

$$1 \le \mathbf{O}_{p'}(\mathfrak{G}) \le \mathbf{O}_{p',p}(\mathfrak{G}) \le \mathbf{O}_{p',p,p'}(\mathfrak{G}) \le \cdots.$$

c) The maximal p-nilpotent normal subgroup of $\mathfrak{G}$ is $\mathbf{O}_{p',p}(\mathfrak{G})$. For if $\mathfrak{N}$ is a normal p-nilpotent subgroup of $\mathfrak{G}$, the normal p-complement $\mathfrak{K}$ of $\mathfrak{N}$ is a characteristic p'-subgroup of $\mathfrak{G}$. Hence $\mathfrak{K} \trianglelefteq \mathfrak{G}$, $\mathfrak{K} \le \mathbf{O}_{p'}(\mathfrak{G})$, $\mathfrak{N}\mathbf{O}_{p'}(\mathfrak{G})/\mathbf{O}_{p'}(\mathfrak{G})$ is a normal p-subgroup and $\mathfrak{N} \le \mathbf{O}_{p',p}(\mathfrak{G})$.

14. If π is a set of primes, $\mathbf{O}^\pi(\mathfrak{G})$ is defined to be the intersection of all the normal subgroups $\mathfrak{N}$ of $\mathfrak{G}$ for which $\mathfrak{G}/\mathfrak{N}$ is a π-group. Thus $\mathfrak{G}/\mathbf{O}^\pi(\mathfrak{G})$ is the maximal π-factor group of $\mathfrak{G}$, and $\mathbf{O}^\pi(\mathfrak{G})$ is a characteristic subgroup of $\mathfrak{G}$.

Example. If $\mathfrak{G}$ is a p-nilpotent group, $\mathbf{O}^p(\mathfrak{G})$ is the normal p-complement of $\mathfrak{G}$.

15. If $\mathfrak{F}$ is a free group, a *group-basis* of $\mathfrak{F}$ is a subset X of $\mathfrak{F}$ such that X generates $\mathfrak{F}$ and any mapping of X into a group is the restriction of some homomorphism of $\mathfrak{F}$. Such a set always exists, by definition of a free group (I, 19.1).

Contents

Chapter VII. Elements of General Representation Theory 1

§ 1. Extension of the Ground-Field 4
§ 2. Splitting Fields 27
§ 3. The Number of Irreducible Modular Representations 32
§ 4. Induced Modules 44
§ 5. The Number of Indecomposable $K\mathfrak{G}$-Modules 63
§ 6. Indecomposable and Absolutely Indecomposable Modules .. 71
§ 7. Relative Projective and Relative Injective Modules 81
§ 8. The Dual Module 97
§ 9. Representations of Normal Subgroups 123
§10. One-Sided Decompositions of the Group-Ring 147
§11. Frobenius Algebras and Symmetric Algebras 165
§12. Two-Sided Decompositions of Algebras 174
§13. Blocks of *p*-Constrained Groups 184
§14. Kernels of Blocks 189
§15. *p*-Chief Factors of *p*-Soluble Groups 203
§16. Green's Indecomposability Theorem 223
Notes on Chapter VII 237

Chapter VIII. Linear Methods in Nilpotent Groups 238

§ 1. Central Series with Elementary Abelian Factors 239
§ 2. Jennings' Theorem 252
§ 3. Transitive Linear Groups 266
§ 4. Some Number-Theoretical Lemmas 270
§ 5. Lemmas on 2-Groups 275
§ 6. Commutators and Bilinear Mappings 286
§ 7. Suzuki 2-Groups 299
§ 8. Lie Algebras 316
§ 9. The Lie Ring Method and an Application 326
§10. Regular Automorphisms 349
§11. The Lower Central Series of Free Groups 366

§12. Remarks on the Burnside Problem 385
§13. Automorphisms of *p*-Groups 396
Notes on Chapter VIII 404

Chapter IX. Linear Methods and Soluble Groups 405

§1. Introduction 407
§2. Hall and Higman's Theorem B 419
§3. The Exceptional Case 429
§4. Reduction Theorems for Burnside's Problem 449
§5. Other Consequences of Theorem B 464
§6. Fixed Point Free Automorphism Groups 476
§7. *p*-Stability 492
§8. Soluble Groups with One Class of Involutions 503
Notes on Chapter IX 514

Bibliography 515

Index of Names 525

Index 527

Chapter VII

Elements of General Representation Theory

In Chapter V, classical representation theory was studied. This is the theory of the group-ring $K\mathfrak{G}$ and the $K\mathfrak{G}$-modules, where K is an algebraically closed field of characteristic 0. (Many theorems remain valid under the hypothesis that K is algebraically closed and that char K does not divide the order of $\mathfrak{G}$). In this case, $K\mathfrak{G}$ is semisimple and all $K\mathfrak{G}$-modules are completely reducible. For many purposes it is therefore sufficient to handle the irreducible representations.

In this chapter we shall study the group-ring $K\mathfrak{G}$ and the $K\mathfrak{G}$-modules when K is an arbitrary field. Thus we are concerned above all with the case when char $K = p$ and p is a prime divisor of the order of the group; for short we call this the *modular* case. In this case the Jacobson radical of $K\mathfrak{G}$ is non-zero and not all $K\mathfrak{G}$-modules are completely reducible. The number of isomorphism types of irreducible $K\mathfrak{G}$-modules is the p'-class number of $\mathfrak{G}$, as long as K is sufficiently large (§ 3). The irreducible modules are determined by $K\mathfrak{G}/\mathbf{J}(K\mathfrak{G})$, and the divergence of $K\mathfrak{G}$ from semisimplicity is determined by $\mathbf{J}(K\mathfrak{G})$. Unfortunately there is no general procedure known for the determination of $\dim_K \mathbf{J}(K\mathfrak{G})$. But by using the technique of lifting idempotents from the theory of algebras, certain facts about the direct decompositions of $K\mathfrak{G}$ into right ideals and two-sided ideals can be established (§ 10, 12). The decomposition of $K\mathfrak{G}$ into two-sided ideals leads to the theory of blocks and is central for the further development of the theory; unfortunately no general method for finding the number of blocks is known. More detailed assertions are made by taking into account the fact that the group-ring possesses a certain self-duality, namely, it is a symmetric algebra (§ 11). Among the consequences of this self-duality is the fact that projective and injective $K\mathfrak{G}$-modules are the same. If

$$K\mathfrak{G} = P_1 \oplus \cdots \oplus P_n$$

is a decomposition of $K\mathfrak{G}$ into indecomposable right ideals P_i, then all types of indecomposable projective $K\mathfrak{G}$-modules occur among the P_i.

Further, each P_i has just one maximal submodule, namely $\mathsf{P}_i\mathsf{J}(\mathsf{K}\mathfrak{G})$, and P_i has just one minimal submodule S_i, which is isomorphic to $\mathsf{P}_i/\mathsf{P}_i\mathsf{J}(\mathsf{K}\mathfrak{G})$. Also P_i is determined to within isomorphism by S_i. Thus the top and bottom composition factors of P_i are known, but the complete composition structure of P_i can only rarely be determined. We therefore restrict ourselves to the investigation of the multiplicities of the composition factors of P_i. This yields the Cartan matrix C of $\mathsf{K}\mathfrak{G}$. The calculation of the elementary divisors of C from the centralizers of the p'-elements of $\mathfrak{G}$ is possible by deep theorems of Richard Brauer, which, however, will not be presented in this chapter.

In this way some information about the indecomposable projective $\mathsf{K}\mathfrak{G}$-modules can be obtained, but the general indecomposable $\mathsf{K}\mathfrak{G}$-module is almost unapproachable. If char $\mathsf{K} = p$, there is only a finite number of types of indecomposable $\mathsf{K}\mathfrak{G}$-modules if and only if the Sylow p-subgroups of $\mathfrak{G}$ are cyclic (§ 5). On the one hand this fact leads in the further development of the theory to the deep resulis of Brauer and Dade on groups with cyclic Sylow p-subgroups, but on the other hand it presents difficulties for the development of the general theory which have not yet been overcome.

In spite of these difficulties, some useful general facts about $\mathsf{K}\mathfrak{G}$-modules have been proved. Among these are the theory of the induced module and the reciprocity theorems (§ 4), the theorems of Clifford type about the relations between $\mathsf{K}\mathfrak{G}$-modules and $\mathsf{K}\mathfrak{N}$-modules for a normal subgroup $\mathfrak{N}$ of $\mathfrak{G}$ (§ 9) and the duality theory of $\mathsf{K}\mathfrak{G}$-modules (§ 8).

What are the aims of a general theory of group-rings? We mention here two lines of development.

(1) If $\mathfrak{G}$ is a p-soluble group, then the p-chief factors of $\mathfrak{G}$ yield irreducible $\mathsf{K}\mathfrak{G}$-modules in a natural way, where $\mathsf{K} = GF(p)$. (It is not very important that K need not be a splitting field for $\mathfrak{G}$, since the theory of the Schur index is trivial for finite fields.) On the one hand, one would like to know what place these representations, obtained so directly from the structure of $\mathfrak{G}$, have in the general theory (§ 15). On the other hand, abundant knowledge of irreducible $\mathsf{K}\mathfrak{G}$-modules of a given p-soluble group $\mathfrak{G}$ is often necessary for the construction of more complicated p-soluble groups.

(2) Another application is much better developed; analogously to local number theory there is a local theory of the characters of $\mathfrak{G}$ over $\mathbb{C}$. This is developed in the following way.

Let L be a field of characteristic 0 with a non-Archimedean valuation, let $\mathfrak{o}$ be the ring of integers in L, let $\mathfrak{p}$ be the maximal ideal of $\mathfrak{o}$ and let $\mathsf{K} = \mathfrak{o}/\mathfrak{p}$. We choose L large enough to be a splitting field for $\mathfrak{G}$. As in V, 12.5, each $\mathsf{L}\mathfrak{G}$-module may be regarded as obtained from an $\mathfrak{o}\mathfrak{G}$-module by extending the domain of coefficients. If M is an $\mathfrak{o}\mathfrak{G}$-module,

M/Mp can be made into a $K\mathfrak{G}$-module in a natural way. Thus the theory of $K\mathfrak{G}$-modules appears as a first approximation to the theory of $\mathfrak{o}\mathfrak{G}$-modules. If $\mathfrak{o}$ is supposed to be complete with respect to its valuation, then as in Hensel's lemma we can build up the $\mathfrak{o}\mathfrak{G}$-module from the $K\mathfrak{G}$-module by successive approximation. The result is a theory of characters in $\mathfrak{o}$ and thus a local representation theory for the prime p. Amongst other results this yields refinements of the classical orthogonality relations which have been drawn upon for the proofs of deep assertions about the structure of finite groups. The "local to global" step from the local theory to a theory of $D\mathfrak{G}$-modules, where D is a Dedekind ring, has been only partially successful up to now. The results thus obtained have played no part in the structure theory of finite groups.

The results of this chapter and the consequent modular representation theory are above all the work of Richard Brauer. Since 1936 he has systematically built up this theory and made it into a more and more delicate instrument for the investigation of finite groups.

We shall assume that the reader is familiar with the following simple facts about projective and injective modules. The proofs may be found in MACLANE [1]. Let $\mathfrak{R}$ be an arbitrary ring with 1.

(1) An $\mathfrak{R}$-module P is called *projective* if any diagram

$$\begin{tikzcd}
 & P \arrow[dl, dashed, "\gamma"'] \arrow[d, "\alpha"] & \\
V \arrow[r, "\beta"'] & W \arrow[r] & 0
\end{tikzcd}$$

can be completed by adding γ; more precisely, if V, W are $\mathfrak{R}$-modules, $\alpha \in \operatorname{Hom}_{\mathfrak{R}}(P, W)$, $\beta \in \operatorname{Hom}_{\mathfrak{R}}(V, W)$ and β is an epimorphism, there exists $\gamma \in \operatorname{Hom}_{\mathfrak{R}}(P, V)$ such that $\alpha = \gamma\beta$ (p. 20).

(2) An $\mathfrak{R}$-module is projective if and only if it is a direct summand of a free module. Any finitely generated projective $\mathfrak{R}$-module is a direct summand of a finitely generated free $\mathfrak{R}$-module (p. 21).

(3) If P is a projective $\mathfrak{R}$-module and

$$0 \to V \overset{\alpha}{\to} W \to P \to 0$$

is an exact sequence of $\mathfrak{R}$-modules, then there exists an $\mathfrak{R}$-submodule P' of W isomorphic to P such that $W = V\alpha \oplus P'$ (p. 24).

(4) If

$$0 \to U \to V \to W \to 0$$

is an exact sequence of $\mathfrak{R}$-modules and P is a projective $\mathfrak{R}$-module, then

$$0 \to \mathrm{Hom}_{\mathfrak{R}}(P, U) \to \mathrm{Hom}_{\mathfrak{R}}(P, V) \to \mathrm{Hom}_{\mathfrak{R}}(P, W) \to 0$$

is an exact sequence of Abelian groups. If $\mathfrak{R}$ is a K-algebra, this is an exact sequence of vector spaces over K (p. 24).

(5) Direct summands of projective modules are projective. Direct sums of projective modules are projective.

(6) An $\mathfrak{R}$-module J is called *injective* if any diagram

$$\begin{tikzcd}
 & J & \\
0 \arrow[r] & V \arrow[u, "\beta"] \arrow[r, "\alpha"] & W \arrow[ul, dashed, "\gamma"']
\end{tikzcd}$$

can be completed by adding γ; more precisely, if V, W are $\mathfrak{R}$-modules, $\alpha \in \mathrm{Hom}_{\mathfrak{R}}(V, W)$, $\beta \in \mathrm{Hom}_{\mathfrak{R}}(V, J)$ and α is a monomorphism, then there exists $\gamma \in \mathrm{Hom}_{\mathfrak{R}}(W, J)$ such that $\beta = \alpha\gamma$ (p. 92).

(7) An $\mathfrak{R}$-module J is injective if and only if any diagram

$$\begin{tikzcd}
 & J & \\
0 \arrow[r] & \mathfrak{S} \arrow[u, "\beta"] \arrow[r] & \mathfrak{R} \arrow[ul, dashed, "\gamma"']
\end{tikzcd}$$

can be completed by adding γ; here $\mathfrak{S}$ is a right ideal of $\mathfrak{R}$ (p. 92).

(8) An injective submodule of an $\mathfrak{R}$-module is a direct summand (p. 92).

(9) Direct summands of injective modules are injective. Direct sums of a finite number of injective modules are injective.

§ 1. Extension of the Ground-Field

In this section we consider the behaviour of group-rings and modules under extension of the ground field.

1.1 Definition. (V, 11.1) Suppose that the field L is an extension of the field K.

a) If $\mathfrak{A}$ is a K-algebra, then $\mathfrak{A} \otimes_K L$ becomes an L-algebra, multiplication being given by

$$(a_1 \otimes \lambda_1)(a_2 \otimes \lambda_2) = a_1 a_2 \otimes \lambda_1 \lambda_2$$

for all a_1, a_2 in $\mathfrak{A}$ and λ_1, λ_2 in L. We denote this algebra by $\mathfrak{A}_L$. If $\{a_1, \ldots, a_n\}$ is a K-basis of $\mathfrak{A}$ and

$$a_i a_j = \sum_{k=1}^{n} c_{ijk} a_k$$

with $c_{ijk} \in K$, then $\{a_1 \otimes 1, \ldots, a_n \otimes 1\}$ is an L-basis of $\mathfrak{A}_L$ and

$$(a_i \otimes 1)(a_j \otimes 1) = \sum_{k=1}^{n} c_{ijk}(a_k \otimes 1).$$

In particular $\dim_L \mathfrak{A}_L = \dim_K \mathfrak{A}$.

b) If V is an $\mathfrak{A}$-module, the vector space $V \otimes_K L$ becomes an $\mathfrak{A}_L$-module V_L if we put

$$(v \otimes \lambda_1)(a \otimes \lambda_2) = va \otimes \lambda_1 \lambda_2$$

for $v \in V$, $a \in \mathfrak{A}$ and $\lambda_1, \lambda_2 \in L$. We have $\dim_L V_L = \dim_K V$.

c) If $\mathfrak{A}$ is a K-algebra and $\mathfrak{B}$ is a K-subspace of $\mathfrak{A}$, there is an L-homomorphism ε of $\mathfrak{B} \otimes_K L$ into $\mathfrak{A} \otimes_K L$ in which $(b \otimes \lambda)\varepsilon = b \otimes \lambda$ ($b \in \mathfrak{B}$, $\lambda \in L$). We write im $\varepsilon = \mathfrak{B}_L$. Note that ε is a monomorphism, for if T is a K-basis of L, $\mathfrak{B} \otimes_K L = \bigoplus_{t \in T} \mathfrak{B} \otimes t$ and $\mathfrak{A} \otimes_K L = \bigoplus_{t \in T} \mathfrak{A} \otimes t$. If $\mathfrak{B}$ is a subring of $\mathfrak{A}$, $\mathfrak{B}_L$ is a subring of $\mathfrak{A}_L$; if $\mathfrak{B}$ is an ideal of $\mathfrak{A}$, $\mathfrak{B}_L$ is an ideal of $\mathfrak{A}_L$.

1.2 Lemma. *Suppose that* L *is an extension of the field* K.

a) *If* $\mathfrak{A}_1, \ldots, \mathfrak{A}_k$ *are* K*-algebras, then*

$$(\mathfrak{A}_1 \oplus \cdots \oplus \mathfrak{A}_k)_L \cong (\mathfrak{A}_1)_L \oplus \cdots \oplus (\mathfrak{A}_k)_L.$$

b) *If* $\mathfrak{A}$ *is a* K*-algebra and* $(\mathfrak{A})_m$ *is the complete matrix ring of degree* m *over* $\mathfrak{A}$, *then* $((\mathfrak{A})_m)_L \cong (\mathfrak{A}_L)_m$.

c) *If* $\mathfrak{A}$ *is a* K*-algebra and* $\mathfrak{I}$ *is a two-sided ideal of* $\mathfrak{A}$, *then* $(\mathfrak{A}/\mathfrak{I})_L \cong \mathfrak{A}_L/\mathfrak{I}_L$.

d) *If $\mathfrak{A}$ is a finite-dimensional* K*-algebra, then* $\mathbf{J}(\mathfrak{A})_{\mathsf{L}} \subseteq \mathbf{J}(\mathfrak{A}_{\mathsf{L}})$.

e) *If* V *and* W *are* $\mathfrak{A}$*-modules and* $\mathsf{V} \supseteq \mathsf{W}$, *then* $(\mathsf{V}/\mathsf{W}) \otimes_{\mathsf{K}} \mathsf{L}$ *and* $\mathsf{V}_{\mathsf{L}}/\mathsf{W}_{\mathsf{L}}$ *are isomorphic* $\mathfrak{A}_{\mathsf{L}}$*-modules.*

Proof. a) It is easily checked that there is an isomorphism α of $(\mathfrak{A}_1 \oplus \cdots \oplus \mathfrak{A}_k)_{\mathsf{L}}$ onto $(\mathfrak{A}_1)_{\mathsf{L}} \oplus \cdots \oplus (\mathfrak{A}_k)_{\mathsf{L}}$ such that

$$((a_1, \ldots, a_k) \otimes \lambda)\alpha = (a_1 \otimes \lambda, \ldots, a_k \otimes \lambda) \quad (a_i \in \mathfrak{A}_i, \lambda \in \mathsf{L}).$$

b) There is an isomorphism β for which

$$((a_{ij}) \otimes \lambda)\beta = (a_{ij} \otimes \lambda) \quad (a_{ij} \in \mathfrak{A}, \lambda \in \mathsf{L}).$$

c) There is an L-algebra epimorphism γ of $\mathfrak{A}_{\mathsf{L}}$ onto $(\mathfrak{A}/\mathfrak{J})_{\mathsf{L}}$ in which

$$(a \otimes \lambda)\gamma = (a + \mathfrak{J}) \otimes \lambda \quad (a \in \mathfrak{A}, \lambda \in \mathsf{L}).$$

If T is a K-basis of L, $\mathfrak{A}_{\mathsf{L}} = \bigoplus_{t \in \mathsf{T}} \mathfrak{A} \otimes t$, so $\ker \gamma = \mathfrak{J}_{\mathsf{L}}$.

d) By V, 2.4a), $\mathbf{J}(\mathfrak{A})$ is nilpotent. Suppose that $\mathbf{J}(\mathfrak{A})^n = 0$. Then $(\mathbf{J}(\mathfrak{A})_{\mathsf{L}})^n = 0$. Thus $\mathbf{J}(\mathfrak{A})_{\mathsf{L}}$ is a nilpotent ideal of $\mathfrak{A}_{\mathsf{L}}$. Hence by V, 2.4b), $\mathbf{J}(\mathfrak{A})_{\mathsf{L}} \subseteq \mathbf{J}(\mathfrak{A}_{\mathsf{L}})$.

e) The proof is similar to that of c). **q.e.d.**

1.3 Examples. Suppose that L is an extension of the field K.

a) We have $(\mathsf{K}\mathfrak{G})_{\mathsf{L}} \cong \mathsf{L}\mathfrak{G}$.

By 1.1a), $(\mathsf{K}\mathfrak{G})_{\mathsf{L}}$ has the L-basis $\{g \otimes 1 \mid g \in \mathfrak{G}\}$ and

$$(g_1 \otimes 1)(g_2 \otimes 1) = g_1 g_2 \otimes 1.$$

Hence the mapping α of $(\mathsf{K}\mathfrak{G})_{\mathsf{L}}$ into $\mathsf{L}\mathfrak{G}$ given by

$$\left(\sum_{g \in \mathfrak{G}} g \otimes \lambda_g\right)\alpha = \sum_{g \in \mathfrak{G}} \lambda_g g \quad (\lambda_g \in \mathsf{L})$$

is an L-algebra isomorphism of $(\mathsf{K}\mathfrak{G})_{\mathsf{L}}$ onto $\mathsf{L}\mathfrak{G}$.

b) By 1.2a) and b), for

$$\mathfrak{A} \cong \bigoplus_{i=1}^{k} (\mathsf{K})_{n_i},$$

we get immediately

$$\mathfrak{A}_{\mathsf{L}} \cong \bigoplus_{i=1}^{k} (\mathsf{L})_{n_i}.$$

In the following lemma, some elementary facts about fields are collected for later use.

1.4 Lemma. a) *Suppose that* $0 \neq f \in \mathsf{K}[t]$ *and* L *is an extension field of* K. *Let* $f = \prod_{i=1}^{r} g_i^{m_i}$ *be the decomposition of* f *in* $\mathsf{L}[t]$ *with pairwise non-associated irreducible polynomials* g_i. *Then*

$$(\mathsf{K}[t]/f\mathsf{K}[t])_{\mathsf{L}} \cong \mathsf{L}[t]/f\mathsf{L}[t] \cong \bigoplus_{i=1}^{r} \mathsf{L}[t]/g_i^{m_i}\mathsf{L}[t].$$

b) *Suppose* $\mathsf{K} = GF(q)$ *and* $\mathsf{L}_i = GF(q^{n_i})$ $(i = 1, 2)$. *Let* d *be the greatest common divisor and* k *the least common multiple of* n_1 *and* n_2. *Then*

$$\mathsf{L}_1 \otimes_{\mathsf{K}} \mathsf{L}_2 \cong GF(q^k) \oplus \cdots \oplus GF(q^k),$$

with d *direct summands on the right.*

c) *Let* L_1 *be a separable extension of* K *and* L_2 *any extension of* K. *Then*

$$\mathsf{L}_1 \otimes_{\mathsf{K}} \mathsf{L}_2 \cong \mathsf{F}_1 \oplus \cdots \oplus \mathsf{F}_r,$$

where the fields F_i *are separable extensions of* L_2.

Proof. a) We have

$$\begin{aligned}(\mathsf{K}[t]/f\mathsf{K}[t])_{\mathsf{L}} &\cong (\mathsf{L} \otimes_{\mathsf{K}} \mathsf{K}[t])/(\mathsf{L} \otimes_{\mathsf{K}} f\mathsf{K}[t]) \qquad \text{(by 1.2c))}\\ &\cong \mathsf{L}[t]/f\mathsf{L}[t],\end{aligned}$$

The mapping α of $\mathsf{L}[t]$ into $\bigoplus_{i=1}^{r} \mathsf{L}[t]/g_i^{m_i}\mathsf{L}[t]$ given by

$$h\alpha = (h + g_1^{m_1}\mathsf{L}[t], \ldots, h + g_r^{m_r}\mathsf{L}[t]) \quad (h \in \mathsf{L}[t])$$

is obviously an L-algebra homomorphism, and $h \in \ker \alpha$ if and only if $g_i^{m_i}$ divides h for all $i = 1, \ldots, r$. Thus $\ker \alpha = f\mathsf{L}[t]$. By the Chinese remainder theorem for the principal ideal ring $\mathsf{L}[t]$, the system of congruences