Representation Theory of Finite Groups and Associative Algebras

CHARLES W. CURTIS

IRVING REINER

REPRESENTATION THEORY OF FINITE GROUPS AND ASSOCIATIVE ALGEBRAS

CHARLES W. CURTIS
UNIVERSITY OF WISCONSIN
IRVING REINER
UNIVERSITY OF ILLINOIS

INTERSCIENCE PUBLISHERS
a division of John Wiley & Sons, New York, London

Library of Congress Catalog Card Number 62-16994

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 aknowledge 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

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 σ, τ is defined by

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

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

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

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

$$x \to x + au_0, \qquad a \text{ real},$$

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 $X = \{1, 2, \cdots, n\}$. Let $[\pi]$ denote the cyclic group generated by an element $\pi \in S_n$. We call π a *cycle* if X has only one non-trivial orbit relative to $[\pi]$. Each cycle π 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 $X_1, \cdots, X_m$ be the distinct orbits of $[\sigma]$. Define for each i, $1 < i < m$, a cycle π_i which acts in the same way as σ 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 π_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 τ_i. Then the $\{X_i'\}$ give the orbits of σ; hence they are just a rearrangement of the $\{X_i\}$. Permuting the $\{\tau_i\}$, we may assume $X_1' = X_1, \cdots, X_m' = X_m, q = m$. Then, for each i, $1 \leqq i \leqq m$, τ_i and π_i both act as σ 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 ρ; then π," 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

$$a_L: x \to ax , \qquad x \in G .$$

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

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

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

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

$$a_R: x \to xa , \qquad x \in G .$$

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

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

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,

$$G = x_1H \cup x_2H \cup \cdots \cup x_rH . \tag{2.2}$$

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:

$$[G: 1] = [G: H][H: 1] . \tag{2.3}$$

The one-to-one mapping $g \to g^{-1}$, $g \in G$, 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

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

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,

$$G = Hx_1K \cup \cdots \cup Hx_tK .$$

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

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

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

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

Thus α 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

$$i_a: x \to axa^{-1}, \qquad x \in G.$$

We have

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

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

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

This assertion is easily seen to be equivalent to the statement

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

and this, in turn, to the important relation

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

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

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

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 $f: G \to G'$ such that

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

Because of the manner in which multiplication in a factor group G/H is defined, it is clear that the mapping $x \to xH$ 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 $f: G \to G'$ 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

$$xH \to f(x)$$

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

$$K \to f(K) = K' , \qquad K = f^{-1}(K') .$$

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

$$G/K \cong G'/K' \cong (G/H)/(K/H) . \tag{2.6}$$

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

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

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

$$a \to i_a , \qquad a \in G ,$$

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

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