ALGEBRAS AND APPLICATIONS

An Introduction to Group Rings

César Polcino Milies
and
Sudarshan K. Sehgal

Kluwer Academic Publishers

An Introduction to Group Rings

by

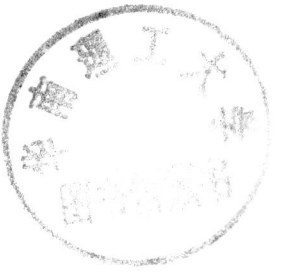
César Polcino Milies

Instituto de Matematica e Estatistica,
Universidade de São Paulo, São Paulo, Brasil

and

Sudarshan K. Sehgal

Department of Mathematical and Statistical Sciences,
University of Alberta, Edmonton, Canada



KLUWER ACADEMIC PUBLISHERS
DORDRECHT / BOSTON / LONDON

A C.I.P. Catalogue record for this book is available from the Library of Congress.

ISBN 1-4020-0238-6 (HB)
ISBN 1-4020-0239-4 (PB)

Published by Kluwer Academic Publishers,
P.O. Box 17, 3300 AA Dordrecht, The Netherlands.

Sold and distributed in North, Central and South America
by Kluwer Academic Publishers,
101 Philip Drive, Norwell, MA 02061, U.S.A.

In all other countries, sold and distributed
by Kluwer Academic Publishers,
P.O. Box 322, 3300 AH Dordrecht, The Netherlands.

Printed on acid-free paper

Printed in the Netherlands.

An Introduction to Group Rings

Algebras and Applications

Volume 1

The theory of rings, algebras and their representations has evolved into a well-defined subdiscipline of general algebra, combining its proper methodology with that of other disciplines and thus leading to a wide variety of applications ranging from algebraic geometry and number theory to theoretical physics and robotics.
Due to this, many recent results in these domains were dispersed in the literature, making it very hard for researchers to keep track of recent developments.
In order to remedy this, *Algebras and Applications* aims to publish carefully refereed monographs containing up-to-date information about progress in the field of algebras and their representations, their classical impact on geometry and algebraic topology and applications in related domains, such as physics or discrete mathematics.
Particular emphasis will thus be put on the state-of-the-art topics including rings of differential operators, Lie algebras and super-algebras, groups rings and algebras, C* algebras, Hopf algebras and quantum groups, as well as their applications.

Preface

Group rings are very interesting algebraic structures. Their importance became apparent after the work of T. Molien, G. Frobenius, I. Schur and H. Maschke in the beginning of the last century. The central role they play in group representation theory was established by E. Noether and R. Brauer in the period 1927-1929. Since then, group rings became an independent subject in their own right.

Besides the obvious relationship with group theory and ring theory, the study of group rings involves the theory of fields, linear algebra and algebraic number theory. It should be noted that group rings are also related to algebraic topology, homological algebra, and algebraic K-theory. More recently, they have found applications in algebraic coding theory. Hence, the theory of group rings provides a subject where many branches of algebra come to a rich interplay – which is especially suitable for a graduate course.

This book is intended as an introduction to the general theory and is addressed primarily to students who wish to learn these topics. It should take the reader from beginning to research level. Given the development that the area has already had, and the active state of research, a book with such an aim cannot be comprehensive. We do think, however, that after this course a student will feel motivated and prepared to read the several research level books, now in print, as well as research articles.

Since we tried to write a *course* rather than an exposition of the theory, we made an effort to provide the reader with motivations, a flavour of its historical development, a broad overview of the subject and a hint of its applications. In the beginning chapters we were careful to provide many details so that expressions such as "it is easy to see that" appear only when this is in fact the case. The final chapters are of a more advanced nature and often cover topics that so far have appeared only as articles in scientific journals. As we approach the present state of research, in later chapters, we expect the reader to be more at ease with the subject, so some details are left to his efforts. Even so, we do try to keep the book accessible. Whenever

possible, we offer new proofs for known results.

We assume only a minimum of prerequisites and, though the reader is expected to have some maturity in algebra - as acquired after a first year of graduate studies - we begin practically from scratch. Our first two chapters start from the definitions of groups and rings, respectively, and cover all the background on these two subjects that will be needed in the rest of the book. Due to the obvious limitations of time and space, however, we could not cover all the necessary background; elements of the theory of fields and linear algebra are the most obvious absences. The basic results on algebraic number theory that are needed are carefully stated in section 2.8, but no proofs are given.

In Chapter III we finally introduce group rings and many of the notions that will become the fundamental tools for the rest of the book. Chapters IV and V cover the basics of group representation theory and characters, and explore the connections between this theory and the structure of group algebras. In section 5.2, we use character theory to enter the discussion of the isomorphism problem. In particular, we use it to establish the normal subgroup correspondence and to show that a group determined by its character table is a solution of the isomorphism problem.

The most basic properties of ideals in group rings are given in Chapter VI. Much more ground could have been covered here, as this aspect of the theory has been and continues to be extensively studied. Due to the introductory nature of the book, we decided to keep our treatment within narrow limits, but the reader can pursue the matter further, for example in Passman's book [126]. Chapter VII deals with several types of algebraic elements in group rings as a preparation for Chapter VIII, where we begin the study of the structure of the unit group.

In Chapter IX we discuss the isomorphism problem. In addition to the best known results, like the Whitcomb Theorem, that have already appeared in other books on the subject, we give Sandling's arguments showing that unit groups of finite rings, such as finite linear groups, are solutions of the isomorphism problem. We include a brief account of a recent counterexample due to Hertweck. This is followed by a discussion of the isomorphism problem in the modular case, giving a modified approach to results of Baginski on isomorphic group algebras of metacyclic p-groups over the field with p-elements. Finally, in Chapters X and XI, we return to the study of the structure of the unit group. We first discuss the existence of free subgroups of rank two in this group and then study some of its algebraic properties.

The exercises given at the end of most sections vary from routine to more challenging problems. Several of them are taken from published papers and

frequently come with hints. We also include the appropriate references in case the reader feels the need for a more detailed explanation.

We wish to thank our colleague Matthias Neufang for all the help he gave us so generously with our TEXnical problems.

It is a pleasure to acknowledge the generous support of our work by NSERC, Canada and FAPESP, Brazil. Finally, we are indebted to our friends A. Giambruno, G. Lee, Y. Li, G. Nebe, M. Parmenter and F. Szechtman who read various parts of the manuscript and made many excellent suggestions.

Edmonton and São Paulo

Summer 2001

Contents

Chapter 1

Groups

1.1 Basic Concepts

The famous memoir *Réflections sur la résolution algébrique des équations*, published by J.L. Lagrange in 1770, followed by papers of P. Ruffini and N.H. Abel, attracted the attention of working mathematicians to the concept of *permutations* (or *linear substitutions*, as they were called at that time). In his classical work of 1830, E. Galois was the first to consider groups and subgroups of permutations, using the term *group* in its modern sense - though restricted to permutations - and introducing such concepts as those of normal subgroup, solvable group, etc.

A. Cauchy was a pioneer in understanding the relevance of permutation groups as an independent subject. He wrote a series of interesting papers about them, in the period 1844-1846.

Influenced by Cauchy's work, A. Cayley recognized that the notion of a group could be formulated in a more abstract setting and gave the first definition of an *abstract group* in 1854 [22]. This paper is considered by several authors (e.g. N. Bourbaki [14] or M. Kline [83]) as the beginning of abstract group theory. It is a relatively short work, but it contains a number of important features:

- Gives an abstract definition of a group, in multiplicative notation.
- Introduces the *table* of an operation.
- Shows that there exist two non-isomorphic groups of order four, giving explicit examples.

- Shows that there exist two non-isomorphic groups of order six, one of them being commutative and the other isomorphic to S_3, the group of permutations of three elements.
- Shows that the order of every element is a divisor of the order of the group.

However, the paper attracted no attention at that time and, though many subsequent works were devoted to the subject, the interest was on applications rather than abstract theory. Especially noteworthy is the classical work of C. Jordan *Tratité des sustitutions et des équations algébriques*, published in 1870, where he organized the knowledge on the topic and added some fundamental new results. In particular, the notion of *isomorphism* and *homomorphism* of groups was explicitly stated there for the first time.

Finally, the definition of an abstract group that we use today was given by W.v. Dyck, a student of F. Klein, in 1883 [37] and a slightly different formulation was given in the same year by H. Weber [173] who later included this definition in his most influential 1886 book *Lehrbuch der Algebra.*

Several independent sets of axioms for abstract groups, which are minor variations of each other, were later given by E.V. Huntington, E.H. Moore and L.E. Dickson. The first book entirely devoted to group theory, W. Burnside's *The theory of groups of finite order*, was written in 1897.

Groups are one of the primary objects of interest in this book. In this chapter we recall some basic definitions and results, omitting the easy proofs.

Definition 1.1.1 *A* **group** *is a non-empty set G together with a binary operation (denoted below by $\cdot$) such that, for all $a, b, c \in G$, the following properties hold:*

(i) $(a \cdot b) \cdot c = a \cdot (b \cdot c)$,

(ii) There exists an element, that we shall denote by $1 \in G$, such that $a \cdot 1 = 1 \cdot a = a$,

(iii) There exists an element $a^{-1} \in G$, such that $a \cdot a^{-1} = a^{-1} \cdot a = 1$.

If, in addition, the following property is satisfied

$$a \cdot b = b \cdot a,$$

then the group is said to be **abelian** *or* **commutative**.

If the set G is finite, then the number of elements of G is called the **order** *of G and is denoted by $|G|$.*

Groups form a very important category of mathematical objects, and there are many examples that are certainly familiar to the reader. As an illustration, we list a few.

Example 1.1.2

The set $\mathbf{Z}$ of rational integers; the set $\mathbf{Q}$ of rational numbers, the set $\mathbf{R}$ of real numbers and the set $\mathbf{C}$ of complex numbers, with the ordinary operation of addition, are examples of groups, all of which are also commutative. Furthermore, if we denote by $\mathbf{Q}^*$, $\mathbf{R}^*$ and $\mathbf{C}^*$ the sets obtained from the previous ones *excluding the element 0*, then these sets, with the ordinary operation of multiplication are also examples of abelian groups. The set $\mathbf{Z}^*$ of integers without 0, is not a group under multiplication since no integer, except 1 and -1, has a multiplicative inverse.

The set $\mathbf{Z}_m = \{\overline{0}, \overline{1}, \ldots, \overline{m-1}\}$ of integers modulo m, with addition defined by $\overline{a+b} = \overline{a} + \overline{b}$ is an abelian group. Also, defining multiplication by $\overline{a \cdot b} = \overline{a} \cdot \overline{b}$ it follows that $\mathbf{Z}_m^*$ is a group under multiplication if and only if the modulus m is a prime number (see Exercise 3).

Example 1.1.3

Let K be a field. The reader is probably already familiar with this concept: if not, he can think of K in what follows as being either $\mathbf{Q}, \mathbf{R}$ or $\mathbf{C}$. Fields will be introduced formally in Definition 2.1.2. Then, the set $GL(n, K)$ of all $n \times n$ invertible matrices with entries in K, with the usual multiplication of matrices, is a group, which is not commutative if $n > 1$. It is called the *full linear group of $n \times n$ matrices over K*.

Example 1.1.4 External direct product

Let $G_1, G_2, \ldots, G_n$ be groups. We consider the set

$$G_1 \dot{\times} G_2 \dot{\times} \cdots \dot{\times} G_n = \{(a_1, a_2, \ldots, a_n) \ : \ a_i \in G_i, 1 \leq i \leq n\},$$

with multiplication defined componentwise:

$$(a_1, a_2, \ldots, a_n) \cdot (b_1, b_2, \ldots, b_n) = (a_1 \cdot b_1, a_2 \cdot b_2, \ldots, a_n \cdot b_n).$$

This set, with the operation above, is a group. It is called the **(external) direct product** of the groups $G_1, G_2, \ldots, G_n$. The direct product is abelian if and only if each direct factor $G_i, 1 \leq i \leq n$, is abelian.

Our next example is of particular interest. Historically, this was the first example of a group to be discovered and it was introduced because of its

applications to the theory of equations. The development of research on this particular class of groups eventually led to the formulation of the general concept.

Example 1.1.5 The symmetric group

Let M be a finite set. We recall that a bijective map of M onto itself is called a *permutation* of M. Clearly, the identical mapping is a permutation and both the composition of two permutations and the inverse of a permutation are permutations. Hence, it follows easily that the set of all permutations of a given set M is a group with respect to composition of mappings. It is usually denoted by S_M and called the **symmetric group on** M.

If $M = \{1, 2, \ldots, n\}$ then S_M is called the *symmetric group of degree* n and is denoted by S_n. Given an element $\psi \in S_n$, if we set $i_k = \psi(k), 1 \leq k \leq n$, we can represent ψ in the form:

$$\psi = \begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ i_1 & i_2 & i_3 & \cdots & i_n \end{pmatrix},$$

a notation introduced by A. Cauchy in 1845 [21, vol. 1, pp. 64 - 90]. Using this notation, we can represent the inverse of ψ as

$$\psi^{-1} = \begin{pmatrix} i_1 & i_2 & i_3 & \cdots & i_n \\ 1 & 2 & 3 & \cdots & n \end{pmatrix}.$$

Given, for instance,

$$\phi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 2 & 4 & 1 \end{pmatrix} \text{ and } \psi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 4 & 5 & 3 \end{pmatrix},$$

we have that $\phi \circ \psi(1) = \phi(2) = 5$. Computing the images of the other numbers in a similar way, we obtain that

$$\phi \circ \psi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 3 & 4 & 1 & 2 \end{pmatrix}.$$

In the same manner we get

$$\psi \circ \phi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 3 & 1 & 5 & 2 \end{pmatrix}.$$

This simple computation shows that, in general, symmetric groups are not commutative. Actually, the reader can check that S_n is commutative if and only if $n \leq 2$.

Given a permutation $\psi \in S_n$, and a positive integer k, $1 \leq k \leq n$, we say that ψ *moves* k if $\psi(k) \neq k$ and, in the opposite case, we say that ψ *fixes* k.

An element $\psi \in S_n$ is called a **cycle of length k** if there exist k distinct positive integers $a_1, a_2, \ldots, a_k$, in $M = \{1, 2, \ldots, n\}$ such that

$$\psi(a_1) = a_2,\ \psi(a_2) = a_3,\quad \ldots\quad ,\psi(a_{k-1}) = a_k,\ \psi(a_k) = a_1,$$

and $\psi(a) = a$ for any other element $a \in M$.

To simplify notations, a cycle as above is denoted as $\psi = (a_1, a_2, \ldots, a_k)$. For example, if we talk of the the cycle $\alpha = (2, 3, 5, 7)$ of S_8 we actually mean the permutation:

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 1 & 3 & 5 & 4 & 7 & 6 & 2 & 8 \end{pmatrix}.$$

As a convention, we shall consider the identity mapping to be a cycle of length 1. Cycles of length 2 have a special name, they are called **transpositions**. Two cycles $\alpha = (a_1, a_2, \ldots, a_k)$ and $\beta = (b_1, b_2, \ldots, b_s)$ are called *disjoint* if the sets $\{a_1, a_2, \ldots, a_k\}$ and $\{b_1, b_2, \ldots, b_s\}$ are disjoint.

We claim that *the order of the symmetric group of degree n is n!*. In fact, an element of S_n is determined by specifying the images of each of the elements $1, 2, \ldots, n$ in M. To count the number of elements in S_n it will suffice to count the numbers of possible choices for the images.

Since the image of 1 can be any of the elements in M, we have exactly n possible choices for it. Once the image of 1 has been chosen, for the image of 2 we can choose any of the remaining elements of M, so we have $n - 1$ choices. In the same way, we shall have $n-2$ possible images for 3 and so on. It follows that there are $n(n-1)(n-2)\cdots 2 \cdot 1 = n!$ different permutations of M.

Definition 1.1.6 *A nonempty subset H of a group G is called a* **subgroup** *of G if it is closed under the operation of G (i.e., for every pair of elements $a, b \in H$, we have that $ab \in H$) and H, with the restriction of the operation of G, is itself a group.*

There are several familiar examples of subgroups; for instance, $\mathbf{Q}^*$ is a subgroup of $\mathbf{R}^*$ which, in turn, is a subgroup of $\mathbf{C}^*$. For any multiplicative group G the subsets $\{1\}$ and G are subgroups of G called the *trivial* subgroups of G.

Example 1.1.7 Cyclic subgroups

Let a be an element of a group G. For an integral exponent, we define the *powers* of a by:

$$a^n = \begin{cases} \underbrace{a \cdot a \cdots a}_{n \text{ times}} & \text{if } n > 0 \\ \underbrace{a^{-1} \cdot a^{-1} \cdots a^{-1}}_{|n| \text{ times}} & \text{if } n < 0 \\ 1 & \text{if } n = 0\,. \end{cases}$$

Since $a^m \cdot a^n = a^{m+n}$, it follows immediately that the set

$$\langle a \rangle \;=\; \{a^n \;:\; n \in \mathbf{Z}\}$$

is a subgroup of G, which is called **the cyclic subgroup of G generated by a.**

If this group is finite, then there exist distinct integers n, m such that $a^n = a^m$. Hence $a^{n-m} = a^{m-n} = 1$. The least positive integer n such that $a^n = 1$ is called the **order of a** and is denoted $o(a)$. If $\langle a \rangle$ is infinite, then we say that a is an element of **infinite order.**

If there exists an element a in G such that $G = \langle a \rangle$, then we say that G is a **cyclic group** and that a is a **generator** of G. Notice that $o(a) = |\langle a \rangle|$.

Example 1.1.8 Subgroups generated by a subset

Let X be a nonempty subset of a group G. We define the **subgroup generated by X** as the intersection of all the subgroups of G containing X. Notice that this family of subgroups is nonempty, since at least G itself belongs to it and that the intersection of this family is, in fact, a subgroup (see *Exercise*13). This subgroup will be denoted by $\langle X \rangle$.

We leave, as an exercise, the task of proving that

$$\langle X \rangle \;=\; \{x_1^{\varepsilon_1} \cdots x_k^{\varepsilon_k} \;:\; x_i \in X,\; \varepsilon_i = \pm 1,\; k \geq 1\} \cup \{1\}.$$

If $\langle X \rangle = G$, then we say that X is a **set of generators** of G. If X is finite, then we say that G is a **finitely generated** group.

To give more examples, we introduce some new groups.

Definition 1.1.9 *Given a field K, we define:*