


Marshall Hall, Jr.

THE THEORY OF GROUP

ALGEBRA

TOPICS IN MATHEMATICS

Preface

HE present volume is intended to serve a dual purpose. The first ten chapters are meant to be the basis for a course in Group Theory, and exercises have been included at the end of each of these chapters. The last ten chapters are meant to be useful as optional material in a course or as reference material. When used as a text, the book is intended for students who have had an introductory course in Modern Algebra comparable to a course taught from Birkhoff and MacLane's *A Survey of Modern Algebra*. I have tried to make this book as self-contained as possible, but where background material is needed references have been given, chiefly to Birkhoff and MacLane.

Current research in Group Theory, as witnessed by the publications covered in *Mathematical Reviews* is vigorous and extensive. It is no longer possible to cover the whole subject matter or even to give a complete bibliography. I have therefore been guided to a considerable extent by my own interests in selecting the subjects treated, and the bibliography covers only references made in the book itself. I have made a deliberate effort to curtail the treatment of some subjects of great interest whose detailed study is readily available in recent publications. For detailed investigations of infinite Abelian groups, the reader is referred to the appropriate sections of the second edition of Kurosch's *Theory of Groups* and Kaplansky's monograph *Infinite Abelian Groups*. The monographs *Structure of a Group and the Structure of its Lattice of Subgroups* by Suzuki and *Generators and Relations for Discrete Groups* by Coxeter and Moser, both in the *Ergebnisse* series, are recommended to the reader who wishes to go further with these subjects.

This book developed from lecture notes on the course in Group Theory which I have given at The Ohio State University over a period of years. The major part of this volume in its present form was written at Trinity College, Cambridge, during 1956 while I held a Fellowship from the John Simon Guggenheim Foundation. I give my thanks to the Foundation for the grant enabling me to carry out this work and to the Fellows of Trinity College for giving me the privileges of the College.

I must chiefly give my thanks to Professor Philip Hall of King's College, Cambridge, who gave me many valuable suggestions on the preparation of my manuscript and some unpublished material of his own. In recognition of his many kindnesses, this book is dedicated to him.

I wish also to acknowledge the helpfulness of Professors Herbert J. Ryser and Jan Koringa and also Dr. Ernest T. Parker in giving me their assistance on a number of matters relating to the manuscript.

Marshall Hall, Jr.
Columbus, Ohio

Content

1	Introduction	6	1.3	Definitions for groups and some related systems	8
1.1	Algebraic laws	6			
1.2		6			
				Index	10

1 Introduction

1.1 Algebraic laws



LARGE PART of algebra is concerned with systems of elements which, like numbers, may be combined by addition or multiplication or both. We are given a system whose elements are designated by letters a, b, c, \dots . We write $S = S(a, b, c, \dots)$ for this system. The properties of these systems depend upon which of the following basic laws hold:

Laws	Addition	Multiplication
Closure laws	A_0 : Addition is well defined	M_0 : Multiplication is well defined
Associative laws	A_1 : $(a + b) + c = a + (b + c)$	M_1 : $(ab)c = a(bc)$
Commutative laws	A_2 : $a + b = b + a$	M_2 : $ba = ab$
Zero and unit	A_3 : $\exists 0, \exists 0 + a = a + 0 = a, \forall a$	M_3 : $\exists 1, \exists 1a = a1 = a, \forall a$
Negatives and Inverses	A_4 : $\forall a, \exists -a, \exists (-a) + a = a + (-a) = 0$	M_4 : $\forall a \neq 0, \exists a^{-1}, \exists (a^{-1})a = a(a^{-1}) = 1$
Distributive laws	D_1 : $a(b + c) = ab + ac$ D_2 : $(b + c)a = ba + ca$	

Table 1.1 Algebraic laws.

Note: A_0 means that, for every ordered pair of elements $a, b \in S$, $a + b = c$ exists and is a unique element of S . Also, M_0 means that, $ab = d$ exists and is a unique element of S .

Definition 1.1.1 Field and Ring

A system satisfying all these laws is called a field. A system satisfying $A_0, A_1, A_2, A_3, A_4, M_0, M_1$ and D_1, D_2 is called a ring.

The parallelism between addition $A_0 - A_4$ and multiplication $M_0 - M_4$ is exploited in the use of logarithms, where the basic correspondence between them is given by the law:

$$\log(xy) = \log(x) + \log(y).$$

In general an n -ary operation in a set S is a function $f = f(a_1, \dots, a_n)$ of n arguments (a_1, \dots, a_n) which are the elements of S and whose values $f(a_1, \dots, a_n) = b$ is a unique element of S when f is defined for these arguments. If, for every choice of a_1, \dots, a_n in S , $f(a_1, \dots, a_n)$ is defined, we say that the operation f is *well defined* or that the set S is *closed* with respect to the operation f .

In a field F , the addition and multiplication are well-defined binary operations, while the inversion operation $f(a) = a^{-1}$ is a unary operation defined for every element except zero.

1.2

Mappings



VERY FUNDAMENTAL CONCEPT of modern mathematics in that of a *mapping* of a set S into a set T .

Definition 1.2.1 Mapping

A *mapping* α of a set S into a set T is a rule which assigns to each x of the set S a unique y of the set T .

Symbolically we write this either of the notations:

$$\alpha : x \longrightarrow y \quad \text{or} \quad y = (x)\alpha.$$

The element y is called the *image* of x under α . If every y of the set T is the image of at least one x in S , we say that α is a mapping of S onto T .

The mapping of a set into (or onto) itself are of particular importance. For example a rotation in a plane may be regarded as a mapping of the set of points in the plane onto itself. Two mappings α and β of a set S into itself may be combined to yield a third mapping of S into itself, according to the following definition.

Definition 1.2.2 Product of Mappings

Given two mappings α, β , of a set S into itself, we define a third mapping γ of S into itself by the rule: If $y = (x)\alpha$ and $z = (y)\beta$, then $z = (x)\gamma$. The mapping γ is called the product of α and β , and we write $\gamma = \alpha\beta$.

Here, since $y = (x)\alpha$ is unique and $z = (y)\beta$ is unique, $z = [(x)\alpha]\beta = (x)\gamma$ is defined for every x of S and is a unique element of S .

Theorem 1.2.1

The mappings of a set S into itself satisfy M_0 , M_1 , and M_3 if multiplication is interpreted to be the product of mappings.

Proof: It has already been noted that M_0 is satisfied. Let us consider M_1 . Let α, β, γ be three given mappings. Take any element x of S and let $y = (x)\alpha$, $z = (y)\beta$ and $w = (x)\gamma$. Then $(x)[(\alpha\beta)\gamma] = z(\gamma) = w$, and $(x)[\alpha(\beta\gamma)] = y(\beta\gamma) = w$. Since both mappings, $(\alpha\beta)\gamma$ and $\alpha(\beta\gamma)$, give the same image for every x in S , it follows that $(\alpha\beta)\gamma = \alpha(\beta\gamma)$.

As for M_3 , let 1 be the mapping such that $(x)1 = x$ for every x in S . Then 1 is a unit in the sense that for every mapping α , $\alpha 1 = 1\alpha = \alpha$.

In general, neither M_2 nor M_4 holds for mappings. But M_4 holds for an important class of mappings, namely, the one-to-one mappings of S onto itself.

Definition 1.2.3 One-to-one Mappings

A mapping α of a set S onto T is said to be one-to-one (which we will frequently write $1-1$) if every element of T is the image of exactly one element of S . We indicate such a mapping by the notation: $\alpha : x \mapsto y$, where x is an element of S and y is an element of T . We say that S and T have the same cardinal number of elements.

Theorem 1.2.2

The one-to-one mappings of a set S onto itself satisfy M_0, M_1, M_3 and M_4 .

Proof: Since theorem 1.2.1 covers M_0, M_1 and M_3 , we need only verify M_4 . If $\alpha : x \mapsto y$ is a one-to-one mapping of S onto itself, then by definition, for every y of S there is exactly one x of S such that $y = (x)\alpha$. This assignment of a unique x to each y determines a one-to-one mapping $\tau : y \mapsto x$ of S onto itself. From the definition of τ we see that $(x)(\alpha\tau) = x$ for every x in S and $y(\tau\alpha) = y$ for every y in S . Hence, $\alpha\tau = \tau\alpha = 1$, and τ is a mapping satisfying the requirements for α^{-1} in M_4 .

We call a one-to-one mapping of a set onto itself a *permutation*. When the given set is finite, a permutation may be written by putting the elements of the set in a row and their images below them. Thus $\alpha = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ and $\beta = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$ are two permutations of the set $S(1, 2, 3)$. Their product is defined to be the permutation $\alpha\beta = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$. Note that the product rule for permutations given here is obtained by multiplying from left to right. Some authors define the product so that multiplication is from right to left.

1.3 Definitions for groups and some related systems



WE see that, as single operations, the laws governing addition and multiplication are the same. Of these, all but the commutative law are satisfied by the product rule for the one-to-one mappings of a set onto itself. The law obeyed by these one-to-one mappings are those which we shall use to define a group.

Definition 1.3.1 First Definition of a Group

A group G is a set of elements $G(a, b, c, \dots)$ and a binary operation call “product” such that:

G_0 . Closure Law. For every ordered pair a, b of elements of G , the product $ab = c$ exists and is a unique element of G .

G_1 . Associative Law. $(ab)c = a(bc)$.

G_2 . Existence of Unit. An element 1 exists such that $1a = a1 = a$ for every a of G .

G_3 . Existence of Inverse. For every a of G there exists an element a^{-1} of G such that $a^{-1}a = aa^{-1} = 1$.

These laws are redundant. We may omit one-half of G_2 and G_3 , and replace them by:

G_2^* . An element 1 exists such that $1a = a$ for every a of G .

G_3^* . For every a of G there exists an element x of G such that $xa = 1$.

We can show that these in turn imply G_2 and G_3 . For a given a let

$$xa = 1 \quad \text{and} \quad yx = 1$$

by G_3^* . Then we have

$$ax = 1(ax) = (yx)(ax) = y[x(ax)] = y[1x] = yx = 1,$$

so that G_3 is satisfied. Also,

$$a = 1a = (ax)a = a(xa) = a1,$$

so that G_2 is satisfied.

The uniqueness of the unit 1 and of an inverse a^{-1} are readily established (see Ex. 13). We could, of course, also replace G_2 and G_3 by the assumption of the existence of 1 and x such that: $a1 = a$ and $ax = 1$. But if we assume that they satisfy $a1 = a$ and $xa = 1$, the situation is slightly different.

There are a number of ways of bracketing an ordered sequence $a_1a_2\cdots a_n$ to give it a value by calculating a succession of binary products. For $n = 3$ there are just two ways of bracketing, namely, $(a_1a_2)a_3$ and $a_1(a_2a_3)$, and the associative law asserts the equality of these two products. An important consequence of the associative law is the *generalized associative law*.

All ways of bracketing an ordered sequence $a_1a_2\cdots a_n$ to give it a value by calculating a succession of binary products yield the same value.

It is a simple matter, using induction on n , to prove that the generalized associative law is a consequence of the associative law (see Ex. 1).

Another definition may be given which does not explicitly postulate the existence of the unit.

Index

