FUNDAMENTALS OF MODERN ALGEBRA

A Global Perspective

Robert G Underwood

World Scientific

FUNDAMENTALS OF MODERN ALGEBRA

A Global Perspective

$$\begin{tikzcd}
M \arrow[rr, "\phi"] \arrow[dr, "s"'] & & M' \\
& M/K \arrow[ur, dotted, "\psi"'] &
\end{tikzcd}$$

Robert G Underwood
Auburn University at Montgomery, USA

World Scientific

NEW JERSEY • LONDON • SINGAPORE • BEIJING • SHANGHAI • HONG KONG • TAIPEI • CHENNAI • TOKYO

Published by

World Scientific Publishing Co. Pte. Ltd.
5 Toh Tuck Link, Singapore 596224
USA office: 27 Warren Street, Suite 401-402, Hackensack, NJ 07601
UK office: 57 Shelton Street, Covent Garden, London WC2H 9HE

Library of Congress Cataloging-in-Publication Data
Names: Underwood, Robert G. (Robert Gene)
Title: Fundamentals of modern algebra : a global perspective / by Robert G. Underwood (Auburn University at Montgomery, USA).
Description: New Jersey : World Scientific, 2016. | Includes bibliographical references and index.
Identifiers: LCCN 2015040815| ISBN 9789814730280 (hardcover : alk. paper) | ISBN 9789814730297 (pbk. : alk. paper)
Subjects: LCSH: Algebra, Abstract--Textbooks. | Algebra--Textbooks.
Classification: LCC QA162 .U53 2016 | DDC 512--dc23
LC record available at http://lccn.loc.gov/2015040815

British Library Cataloguing-in-Publication Data
A catalogue record for this book is available from the British Library.

In-house Editor: Bai Li

Printed in Singapore by B & Jo Enterprise Pte Ltd

FUNDAMENTALS OF MODERN ALGEBRA

A Global Perspective

to my son, Andre

Preface

The purpose of this book is to provide a concise yet detailed account of fundamental concepts in modern algebra. The target audience for this book is first-year graduate students in mathematics, though the first two chapters are probably accessible to well-prepared undergraduates.

The book contains five chapters. In Chapter 1 we cover groups, subgroups, quotient groups, homomorphisms of groups, and group structure, including cyclic groups, the Structure Theorem for finitely generated Abelian groups, Cauchy's Theorem, and Sylow's Theorems. In Chapter 2 we consider rings, the group of units of a ring, ideals, quotient rings, and ring homomorphisms. Included also are sections on localizations and completions. In Chapter 3 we turn to modules. We begin with a review of both finite and infinite dimensional vector spaces, and then generalize to modules over PIDs and Noetherian rings. We include sections on projective modules, tensor products of modules, algebras, and the discriminant of modules over an integral domain. In Chapter 4 we define simple algebraic extensions of $\mathbb{Q}$ and introduce the Galois group of the splitting field of a monic irreducible polynomial over $\mathbb{Q}$. We state and prove the Fundamental Theorem of Galois Theory. We then follow with an introduction (essentially) to algebraic number theory: we include material on the ring of integers of an algebraic extension, the Noetherian propery of the ring of integers, Dedekind domains and unique factorization of ideals. In the final chapter (Chapter 5) we cover the basic theory of finite fields and linearly recursive sequences.

We begin each chapter with an overview of the material to be covered. At the end of each chapter we give an extensive list of exercises which range from basic applications of the theory, to problems designed to challenge the reader. We also include some "Questions for Further Study", which are advanced problems suitable for master's level research projects.

I would like to thank the fellow algebraists who read and commented on earlier drafts of the manuscript. Their suggestions, especially those regarding the organization of the sections, have been duly noted and incorporated into the book. My appreciation is also extended to E. H. Chionh and Li Bai, at World Scientific, who have skillfully guided me through the publication process. To my wife, Rebecca Brower, who is also an academic, and who certainly understands the challenge of a writing project of this sort, I thank you for your patience, kindness and companionship. Any finally, to my son Andre, to whom this book is dedicated, I thank you for understanding that although writing takes a lot of time, in the end it is a worthy endeavor.

Robert G. Underwood

Contents

Preface vii

1. Groups 1

1.1 Introduction to Groups 1
1.2 Subgroups 11
1.3 Homomorphisms of Groups 16
1.4 Group Structure 22
1.5 The Sylow Theorems 31
1.6 Exercises 35

2. Rings 41

2.1 Introduction to Rings 42
2.2 Polynomial Rings 48
2.3 The Group of Units of a Ring 53
2.4 Ideals 60
2.5 Quotient Rings and Ring Homomorphisms 70
2.6 Localization 78
2.7 Absolute Values and Completions 82
2.8 Exercises 93

3. Modules 101

3.1 Vector Spaces 102
3.2 Modules 109
3.3 Projective Modules 117
3.4 Tensor Products 122
3.5 Algebras 128

3.6 Discriminants 133
3.7 Exercises 140

4. Simple Algebraic Extension Fields 143

4.1 Simple Algebraic Extensions 144
4.2 Some Galois Theory 152
4.3 The Ring of Integers 158
4.4 The Noetherian Property of the Ring of Integers 169
4.5 Dedekind Domains 172
4.6 Unique Factorization of Ideals 178
4.7 Extensions of $\mathbb{Q}_p$ 181
4.8 Exercises 186

5. Finite Fields 191

5.1 Invented Roots 191
5.2 Finite Fields 193
5.3 Linearly Recursive Sequences 200
5.4 Exercises 212

Bibliography 215

Index 217

Chapter 1

Groups

In this chapter we introduce semigroups, monoids, and groups, give some basic examples of groups and discuss some of their elementary properties. We then consider subgroups, cosets and Lagrange's theorem, normal subgroups and the quotient group. We next turn to the basic maps between groups: homomorphisms and isomorphisms and their kernels. (Throughout this book, map = function.) We give the First, Second and Third Isomorphism theorems and the Universal Mapping Property for Kernels.

We close the chapter with the study of group structure, including generating sets for groups and subgroups and the notion of a cyclic group. From the cyclicity of the additive group of integers Z we obtain greatest common divisors, least common multiples, Bezout's Lemma and the Chinese Remainder Theorem. We state the structure theorem for finitely generated abelian groups. Regarding the structure of groups in general, we introduce G-sets, and give Cauchy's Theorem and Sylow's First, Second, and Third Theorems.

1.1 Introduction to Groups

In this section we define semigroups and monoids and give some examples, including the monoid of words on a finite alphabet. From semigroups and monoids, we develop the concept of a group, discuss finite, infinite and abelian groups, and prove some elementary properties of groups. We introduce examples of groups that we will appear throughout this book, including the additive group of integers, Z, the multiplicative group of non-zero real numbers, $\mathbb{R}^\times$ and the group of residue classes modulo n, Z_n. For further examples of groups we construct the 3rd and 4th dihedral groups, D_3, D_4 as the groups of symmetries of the equilateral triangle and the square, as well as the symmetric group on n letters, S_n.

* * *

Let S be a non-empty set of elements. The cartesian product on S is defined as $S \times S = \{(a, b) : a, b \in S\}$.

Definition 1.1. A **binary operation on** S is a function $B : S \times S \to S$; we denote the image of (a, b) by ab.

A binary operation is **commutative** if for all $a, b \in S$, $ab = ba$. A binary operation is **associative** if for all $a, b, c \in S$, $a(bc) = (ab)c$.

Definition 1.2. A **semigroup** is a set S together with an associative binary operation $S \times S \to S$.

Let S be a semigroup and let $a_1, a_2, a_3 \in S$. We define the product $a_1a_2a_3$ to be the common value of the expressions $(a_1a_2)a_3$ and $a_1(a_2a_3)$. For $n \geq 4$ we define the **product of elements** $a_1, a_2, \ldots, a_n \in S$ inductively to be

$$\prod_{i=1}^{n} a_i = \left(\prod_{i=1}^{n-1} a_i\right) a_n.$$

In defining $\prod_{i=1}^{n} a_i$ in this way we are asserting that we can insert parentheses into the product in any manner we choose without changing its value. For example, $a_1a_2a_3a_4$ is the common value of the expressions

$$(a_1a_2a_3)a_4,\ (a_1(a_2a_3))a_4,\ ((a_1a_2)a_3)a_4,\ a_1((a_2a_3)a_4),\ (a_1a_2)(a_3a_4),$$
$$a_1(a_2(a_3a_4)),\ a_1(a_2a_3)a_4,\ (a_1a_2)a_3a_4,\ a_1a_2(a_3a_4),\ a_1(a_2a_3a_4).$$

Definition 1.3. A **monoid** is a semigroup S in which there exists an element $e \in S$ with $ea = a = ae, \forall a \in S$. Such an element e is called an **identity element** for the monoid.

For example, the set of integers Z together with ordinary multiplication is a monoid with identity element $e = 1$ and the set of natural numbers $\mathbb{N} = \{1, 2, 3, \ldots\}$ together with ordinary addition is a semigroup. Note that $\mathbb{N}$ together with $+$ is not a monoid, however.

Here is an example of a monoid that is used in computer science. An **alphabet** Σ_0 is a non-empty set whose elements are the **letters** of the alphabet. A **word** is a finite sequence of letters in Σ_0. For a given alphabet Σ_0, let Σ_0^* denote the collection of all words formed from the alphabet Σ_0.

For $w \in \Sigma_0^*$, the **length of** w denoted by $l(w)$ is the number of letters in w. The **empty word** e is the (unique) word of length 0 in Σ_0^*. We endow Σ_0^* with a binary operation $\Sigma_0^* \times \Sigma_0^* \to \Sigma_0^*$ called **concatenation**. Concatenation (sometimes denoted as '$\cdot$') is defined as $x \cdot y = xy$, for $x, y \in \Sigma_0^*$. As the reader can easily verify, Σ_0^* together with concatenation is a monoid; the identity element is the empty word.

For example if $\Sigma_0 = \{a, b\}$, then $\{a, b\}^*$ consists of all finite sequences of a's and b's. The word $x = abbab \in \{a, b\}^*$ has length $l(x) = 5$. Moreover, if $y = bab$, then $x \cdot y = abbab \cdot bab = abbabbab$.

Definition 1.4. A **group** is a set G together with a binary operation $G \times G \to G$ for which

(i) the binary operation is associative,

(ii) there exists an element $e \in G$ for which $ea = a = ae$, for all $a \in G$,

(iii) for each $a \in G$, there exists an element $c \in G$ for which $ca = e = ac$.

An element e satisfying (ii) is an **identity element** for G; an element c satisfying (iii) is called an **inverse element** of a and is denoted by a^{-1}.

We note immediately that every group is a monoid. The converse is false, of course (see §1.6, Exercise 6).

There are many familiar examples of groups encountered in mathematics. For example, the set of integers Z, together with ordinary addition $+$ is a group, 0 plays the role of e, and $-a$ is the inverse of $a \in Z$. One easily shows that the set of rational numbers $\mathbb{Q}$ under ordinary addition and the set of real numbers $\mathbb{R}$ under ordinary addition are groups. The set of non-zero real numbers $\mathbb{R}^\times$ is a group under ordinary multiplication $\cdot$ with $e = 1$, and $a^{-1} = 1/a$. A further example is the **general linear group** $GL_n(\mathbb{R})$ consisting of invertible $n \times n$ matrices with entries in $\mathbb{R}$, together with matrix multiplication. Recalling some linear algebra, one has

$$GL_n(\mathbb{R}) = \{A \in Mat_n(\mathbb{R}) : \det(A) \neq 0\}.$$

In the case that $n = 1$, $GL_1(\mathbb{R}) = \mathbb{R}^\times$.

The **order** of a group G, denoted by $|G|$, is the number of elements in G. If $|G|$ is infinite, then G is an **infinite group**. All of the examples of groups given above are infinite groups. A group G is **finite** if $|G|$ is finite. In what follows we give an example of a finite group.

Let n, a be integers with $n > 0$. A **residue of a modulo n** is an integer r for which $a = nq + r$ for some $q \in Z$. For instance, if $n = 3$, $a = 8$, then 11 is a residue of 8 modulo 3 since $8 = 3(-1) + 11$, but so is 2 since $8 = 3(2) + 2$. The possible least non-negative residues of a modulo n are $0, 1, 2, \ldots, n-1$. The least non-negative residue of a modulo n is denoted as a **mod** n. For example, $8 \bmod 3 = 2$, but also note that $-3 \bmod 4 = 1$ and $11 \bmod 4 = 3 \bmod 4 = 3$. We say that two integers a, b are **congruent modulo** n if $a \bmod n = b \bmod n$ and we write $a \equiv b \bmod n$. Let a, n be integers with $n > 0$. Then n **divides** a, denoted by $n \mid a$, if there exists an integer k for which $a = nk$.

Proposition 1.1. *Let $a, b, n \in Z$, $n > 0$. Then $a \equiv b \bmod n$ if and only if $n \mid (a - b)$.*

Proof. To prove the "only if" part, assume that $a \equiv b \bmod n$. Then $a \bmod n = b \bmod n$, so there exist integers l, m for which $a = nm + r$ and $b = nl + r$ with $r = a \bmod n = b \bmod n$. Thus $a - b = n(m - l)$. For the "if" part, assume that $a - b = nk$ for some k. Then $(nm + a \bmod n) - (nl + b \bmod n) = nk$ for some $m, l \in Z$, so that n divides $a \bmod n - b \bmod n$. Consequently, $a \bmod n - b \bmod n = 0$, hence $a \equiv b \bmod n$. □

Proposition 1.1 can help us compute $a \bmod n$. For instance $-14 \bmod 17 = 3 \bmod 17 = 3$ since $17 \mid (-14 - 3)$. Likewise $-226 \bmod 17 = 12 \bmod 17 = 12$ since $17 \mid (-226 - 12)$.

For $n > 0$ consider the set $J = \{0, 1, 2, 3, \ldots, n-1\}$ of least non-negative residues modulo n. Note that $a = a \bmod n, \forall a \in J$. On J we define a binary operation $+_n$ as follows: for $a, b \in J$,

$$a \bmod n +_n b \bmod n = (a + b) \bmod n.$$

Then $+_n$ gives J the structure of a group, known as the **group of residue classes modulo** n. We denote this group by Z_n; Z_n is a finite group of order $|Z_n| = n$. For example, $Z_4 = \{0, 1, 2, 3\}$ and one has $1 +_4 2 = 3$, $3 +_4 2 = 1$, and so on.

One nice feature of a small finite group is that all possible group products can be arranged in a finite table in which the elements of the group are listed across the top as labels of the columns and down the left side as labels of the rows. For elements a, b in finite group G, the (a, b)th entry in the table is ab. This table is the **group table** for finite group G. For instance, the group table for Z_4 is

$+_4$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

We can construct a new group from a finite set of groups. Let $S_1, S_2, \ldots, S_k$ be a finite collection of sets. Then the **cartesian product** $\prod_{i=1}^{k} S_i$ is the collection of all k-tuples $\{(a_1, a_2, \ldots, a_k) : \ a_i \in S_i\}$.

Proposition 1.2. *Let G_i, $i = 1, \ldots, k$, be a finite collection of groups. Then the cartesian product $\prod_{i=1}^{k} G_i$ is a group under the binary operation defined as*

$$(a_1, a_2, \ldots, a_k) \cdot (b_1, b_2, \ldots, b_k) = (a_1 b_1, a_2 b_2, \ldots, a_k b_k),$$

where $a_i b_i$ is the image of (a_i, b_i) under the binary operation $B_i : G_i \times G_i \to G_i$ of the group G_i, $1 \le i \le k$.

Proof. We show that the conditions of Definition 1.4 hold. Clearly the binary operation on the cartesian product is associative; for an identity element we take $e = (e_1, e_2, \ldots, e_k)$ where e_i is an identity in G_i. Lastly, for each k-tuple $(a_1, a_2, \ldots, a_k)$ one has $(a_1, a_2, \ldots, a_k)^{-1} = (a_1^{-1}, a_2^{-1}, \ldots, a_k^{-1})$. □

The group $\prod_{i=1}^{k} G_i$ of Proposition 1.2 is the **direct product group**.

As an illustration we consider the group $Z \times Z$ in which the binary operation is given as $(m_1, m_2) + (n_1, n_2) = (m_1 + n_1, m_2 + n_2)$. For another example, we take $Z_2 \times Z_3$; here for instance, $(0, 1) + (1, 2) = (1, 0)$. Note that $|Z_2 \times Z_3| = 6$.

In any group the identity and the inverse of an element are unique.

Proposition 1.3. *Let G be a group. Then there exists a unique element e for which $ea = a = ae$, and for each $a \in G$, there exists a unique element a^{-1} for which $a^{-1}a = e = aa^{-1}$.*

Proof. Suppose there are two identities e_1 and e_2. Then with e_1 acting on the left, $e_1e_2 = e_2$. Also, with e_2 acting on the right, $e_1e_2 = e_1$. Thus $e_1 = e_2$.

Now suppose there exist two inverses a_1^{-1} and a_2^{-1} for a given element $a \in G$. Then $a_1^{-1}a = e = a_2^{-1}a$. Now multiplying on the right by a_1^{-1} yields $a_1^{-1} = a_2^{-1}$. □

Since $(ab)(b^{-1}a^{-1}) = e = (ab)(ab)^{-1}$, uniqueness of the inverse yields the **rule for inverses of products** in a group, that is: $(ab)^{-1} = b^{-1}a^{-1}$.

In a group the binary operation is by definition associative. It may or may not be commutative.

Definition 1.5. A group for which the binary operation is commutative is an **abelian** group.

For example, the residue class group Z_n is an abelian group, as are Z, $\mathbb{Q}$, and $\mathbb{R}$.

The easiest example of a non-abelian group is $GL_2(\mathbb{R})$. In this group, for example, we have

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \neq \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

For a finite non-abelian group, we consider the 3rd order **dihedral group**, which is denoted by D_3. The elements of D_3 are the six "symmetries" of the equilateral triangle $\triangle ABC$ (Figure 1.1) and consist of three clockwise rotations of 0°, 120°, and 240° about the center O of the triangle, represented by the elements ρ_0, ρ_1, ρ_2, together with three reflections through the perpendicular lines ℓ_1, ℓ_2, ℓ_3, represented by the elements μ_1, μ_2, μ_3, respectively. It is critical to realize that the rotations move the vertices of the triangle, yet the perpendicular lines remain fixed and do not move with the rotation of the triangle.