DE GRUYTER

TEXTBOOK

Derek J. S. Robinson

ABSTRACT ALGEBRA

AN INTRODUCTION WITH APPLICATIONS

2ND EDITION

Derek J. S. Robinson

Abstract Algebra

An Introduction with Applications

2nd Edition

DE GRUYTER

Mathematics Subject Classification 2010
1201, 1301, 1501, 1601, 2001

Author
Prof. Dr. Derek J. S. Robinson
University of Illinois
Department of Mathematics
1409 West Green Street
Urbana IL 61801, USA
dsrobins@illinois.edu

The previous edition of this book was published with the title *An Introduction to Abstract Algebra*.

ISBN 978-3-11-034086-0
e-ISBN (PDF) 978-3-11-034087-7
e-ISBN (EPUB) 978-3-11-038560-1

Library of Congress Cataloging-in-Publication Data
A CIP catalog record for this book has been applied for at the Library of Congress.

Bibliographic information published by the Deutsche Nationalbibliothek
The Deutsche Nationalbibliothek lists this publication in the Deutsche Nationalbibliografie; detailed bibliographic data are available on the Internet at http://dnb.dnb.de.

Cover image: thinkstock
Typesetting: Tanovski Publ. Services, Leipzig, Sofia
Printing and binding: CPI books GmbH, Leck
♾ Printed on acid-free paper
Printed in Germany

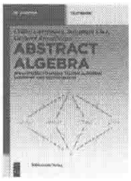
www.degruyter.com

Derek J. S. Robinson

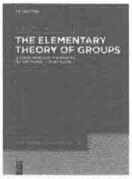
Abstract Algebra

De Gruyter Textbook

Also of Interest



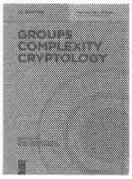
Abstract Algebra
Celine Carstensen, Benjamin Fine, Gerhard Rosenberger, 2011
ISBN 978-3-11-025008-4, e-ISBN 978-3-11-025009-1



The Elementary Theory of Groups
Benjamin Fine, Anthony Caglione, Alexei Myasnikov,
Gerhard Rosenberger, Dennis Spellman, 2014
ISBN 978-3-11-034199-7, e-ISBN (PDF) 978-3-11-034203-1,
e-ISBN (EPUB) 978-3-11-038257-0, Set-ISBN 978-3-11-034204-8

Journal of Group Theory
Christopher W. Parker, John S. Wilson (Editors in Chief),
6 issues per year
ISSN 1433-5883, e-ISSN 1435-4446

Discrete Mathematics and Applications
Andrei Zubkov (Editor in Chief), 6 issues per year
ISSN 0924-9265, e-ISSN 1569-3929



Groups Complexity Cryptology
Gerhard Rosenberger, Vladimir Shpilrain (Managing editors),
2 issues per year
ISSN 1867-1144, e-ISSN 1869-6104

In Memory of My Parents

Preface

The origins of algebra are usually traced back to Muhammad ben Musa al-Khwarizmi, who worked at the court of the Caliph al-Ma'mun in Baghdad in the early 9th Century. The word derives from the Arabic al-jabr, which refers to the process of adding the same quantity to both sides of an equation. The work of Arabic scholars was known in Italy by the 13th Century and a lively school of algebraists arose there. Much of their interest was centered on the solution of polynomial equations. This preoccupation of mathematicians lasted until the beginning of the 19th Century, when the possibility of solving the general equation of the fifth degree in terms of radicals was finally disproved by Ruffini and Abel.

This early work led to the introduction of some of the main structures of abstract algebra, groups, rings and fields. These structures have been studied intensively over the past two hundred years. For an interesting historical account of the origins of algebra the reader may consult the book by van der Waerden [17].

Until quite recently algebra was very much the domain of the pure mathematician, and applications were few and far between. But the situation has changed, in part as a result of the rise of information technology, where the precision and power inherent in the language and concepts of algebra have proved to be invaluable. Today many specialists in computer science and engineering, as well as physics and chemistry, routinely take courses in abstract algebra. The present work represents an attempt to meet the needs of both mathematicians and scientists who seek to acquire a knowledge of algebra and its applications.

As to what is expected of the reader, a basic knowledge of matrix algebra is assumed and also at least the level of mathematical maturity consistent with completion of three semesters of calculus. The objective is to introduce the reader to the principal structures of abstract algebra and to give an account of some of its more convincing applications. In particular there are sections on solution of equations by radicals, ruler and compass constructions, Polya counting theory, Steiner systems, orthogonal latin squares and error correcting codes. The book should be suitable for students in the final year of undergraduate or first year of (post)graduate studies at a university in North America or the United Kingdom.

The principal change to the book from the first edition is the addition of two new chapters. The first of these is an introduction to the theory of modules, a topic that combines the concepts of group and ring. Enough of the theory is developed to establish the structure theorem for finitely generated modules over principal ideal domains. Then applications to matrices and linear operators are presented. The second new chapter gives an introduction to tensor products, an essential tool in many advanced parts of algebra. Also Hilbert's Basis Theorem is proved and a more detailed account of Hall's theory of finite solvable groups is given. The original chapter on vector spaces has been modified by substituting an account of the theory of eigenvalues and eigenvectors of linear operators for the section on orthogonality. Some of these changes have inevitably had the effect of raising the level of abstraction in parts of the book. However, the original aim of making abstract algebra accessible to as many readers as possible is maintained in this edition.

Naturally the opportunity has been taken to correct errors and obscurities in the first edition. I am grateful to those readers who took the time and trouble to send in lists of corrections, and here particular thanks are due to Adolfo Ballester-Bolinches and Dieter Kilsch. Of course, as usual, full credit for all errors belongs to the author.

There is more than enough material here for a two semester course in abstract algebra. If just one semester is available, Chapters One through Eight and Chapter Eleven could be covered. The first two chapters contain topics that will be familiar to many readers and can be covered more quickly. In addition, a good deal of the material in Chapter Eight will not be new to a reader who has taken a first course in linear algebra. A word about proofs is in order. Sometimes students from outside mathematics question the need for mastering the art of rigorous proof, although this is perhaps becoming less common. One response is that the only way to be sure that a statement is correct, or that a computer program will always deliver the correct answer, is to prove it. As a rule complete proofs are given and they should be read. The first two chapters, which contain much elementary material, are a good place for the reader to develop and polish theorem proving skills. Each section of the book is followed by a selection of problems of varying degrees of difficulty.

The second edition of this book, like the first, is based on courses given over many years at the University of Illinois at Urbana-Champaign, the National University of Singapore and the University of London. I am grateful to my colleagues for good advice and many stimulating conversations: these have led to numerous improvements in the text. My thanks are due to Otto Kegel and Manfred Karbe for assistance with the first edition. In preparing this second edition I have been aided by Leonardo Milla and Friederike Dittberner at Walter de Gruyter, whose advice and assistance have greatly helped. Finally, I thank my family for their patience and encouragement, which are essential in a project such as this.

Derek Robinson

Urbana, Illinois,
November 2014

Contents

1 Sets, relations and functions

The concepts introduced in this chapter are truly fundamental and underlie almost every branch of mathematics. Most of the material is quite elementary and will be familiar to many readers. Nevertheless readers are encouraged to review the material and to check notation and definitions. Because of its nature the pace of this chapter is somewhat faster than in subsequent chapters.

1.1 Sets and subsets

By a *set* we shall mean any well-defined collection of objects, which are called the *elements* of the set. Some care must be exercised in using the term "set" because of Bertrand Russell's famous paradox, which shows that not every collection can be regarded as a set. Russell considered the collection C of all sets which are not elements of themselves. If C is allowed to be a set, a contradiction arises when one inquires whether or not C is an element of itself. Now plainly there is something suspicious about the idea of a set being an element of itself and we shall take this as evidence that the qualification "well-defined" needs to be taken seriously. A collection that is not a set is called a *proper class.*

Sets will be denoted by capital letters and their elements by lower case letters. The standard notation

$$a \in A$$

means that a is a element of the set A, or a *belongs* to A. The negation of $a \in A$ is denoted by $a \notin A$. Sets can be defined either by writing their elements out between braces, as in $\{a, b, c, d\}$, or alternatively by giving a formal description of the elements, the general format being

$$A = \{a \mid a \text{ has property } P\},$$

i.e., A is the set of all objects with the property P. If A is a finite set, the number of its elements is written

$$|A|.$$

Subsets. Let A and B be sets. If every element of A is an element of B, we write

$$A \subseteq B$$

and say that A is a *subset* of B, or that A *is contained* in B. If $A \subseteq B$ and $B \subseteq A$, so that A and B have exactly the same elements, then A and B are said to be *equal*,

$$A = B.$$

The negation of this is $A \neq B$. The notation $A \subset B$ is used if $A \subseteq B$ and $A \neq B$; then A is called a *proper* subset of B.

Some special sets. A set with no elements at all is called an *empty set*. An empty set E is a subset of any set A; for if this were false, there would be an element of E that is not in A, which is certainly wrong. As a consequence, *there is exactly one empty set*: for if E and E' are two empty sets, then $E \subseteq E'$ and $E' \subseteq E$, so that $E = E'$. The unique empty set is written

$$\emptyset.$$

Some further standard sets with reserved notations are

$$\mathbb{N},\ \mathbb{Z},\ \mathbb{Q},\ \mathbb{R},\ \mathbb{C},$$

which are respectively the sets of natural numbers $0, 1, 2, \dots$, integers, rational numbers, real numbers and complex numbers.

Set operations. Next we recall the familiar set operations of union, intersection and complement. Let A and B be sets. The *union* $A \cup B$ is the set of all objects which belong to A or B, or possibly to both; the *intersection* $A \cap B$ consists of all objects that belong to both A and B. Thus

$$A \cup B = \{x \mid x \in A \text{ or } x \in B\},$$

while

$$A \cap B = \{x \mid x \in A \text{ and } x \in B\}.$$

It should be clear how to define the union and intersection of an arbitrary collection of sets $\{A_\lambda \mid \lambda \in \Lambda\}$; these are written

$$\bigcup_{\lambda \in \Lambda} A_\lambda \quad \text{and} \quad \bigcap_{\lambda \in \Lambda} A_\lambda,$$

respectively. The *relative complement* of B in A is

$$A - B = \{x \mid x \in A \text{ and } x \notin B\}.$$

Frequently one has to deal only with subsets of some fixed set U, called the *universal set*. If $A \subseteq U$, then the *complement* of A in U is

$$\bar{A} = U - A.$$

We list for future reference the fundamental properties of unions, intersections and complements: most of these should be familiar.

(1.1.1) *Let A, B, C, B_λ $(\lambda \in \Lambda)$ be sets. Then the following statements are valid:*

(i) $A \cup B = B \cup A$ *and* $A \cap B = B \cap A$, *(commutative laws).*

(ii) $(A \cup B) \cup C = A \cup (B \cup C)$ *and* $(A \cap B) \cap C = A \cap (B \cap C)$, *(associative laws).*

(iii) $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ *and* $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$, *(distributive laws).*

(iv) $A \cup A = A = A \cap A$.

(v) $A \cup \emptyset = A$, $A \cap \emptyset = \emptyset$.

(vi) $A - (\bigcup_{\lambda \in \Lambda} B_\lambda) = \bigcap_{\lambda \in \Lambda}(A - B_\lambda)$ *and* $A - (\bigcap_{\lambda \in \Lambda} B_\lambda) = \bigcup_{\lambda \in \Lambda}(A - B_\lambda)$, *(De Morgan's Laws).*[1]

The easy proofs of these results are left to the reader as an exercise.

Set products. Let $A_1, A_2, \dots, A_n$ be sets. By an *n-tuple* of elements from $A_1, A_2, \dots, A_n$ is to be understood a sequence of elements $a_1, a_2, \dots, a_n$ with $a_i \in A_i$. The n-tuple is usually written $(a_1, a_2, \dots, a_n)$ and the set of all n-tuples is denoted by

$$A_1 \times A_2 \times \cdots \times A_n.$$

This is the *set product* (or *cartesian product*) of $A_1, A_2, \dots, A_n$. For example $\mathbb{R} \times \mathbb{R}$ is the set of coordinates of points in the plane.

The following result is a basic counting tool.

(1.1.2) *If $A_1, A_2, \dots, A_n$ are finite sets, then*

$$|A_1 \times A_2 \times \cdots \times A_n| = |A_1| \cdot |A_2| \cdots |A_n|.$$

Proof. In forming an n-tuple $(a_1, a_2, \dots, a_n)$ we have $|A_1|$ choices for a_1, $|A_2|$ choices for $a_2, \dots, |A_n|$ choices for a_n. Each choice of an a_i yields a different n-tuple. Therefore the total number of n-tuples is $|A_1| \cdot |A_2| \cdots |A_n|$. □

The power set. The *power set* of a set A is the set of all subsets of A, including the empty set and A itself; it is denoted by

$$\mathcal{P}(A).$$

The power set of a finite set is always a larger set, as the next result shows.

(1.1.3) *If A is a finite set, then* $|\mathcal{P}(A)| = 2^{|A|}$.

Proof. Let $A = \{a_1, a_2, \dots, a_n\}$ with distinct a_i's. Also put $I = \{0, 1\}$. Each subset B of A is to correspond to an n-tuple $(i_1, i_2, \dots, i_n)$ with $i_j \in I$. Here the rule for forming the n-tuple corresponding to B is this: $i_j = 1$ if $a_j \in B$ and $i_j = 0$ if $a_j \notin B$. Conversely, every n-tuple $(i_1, i_2, \dots, i_n)$ with $i_j \in I$ determines a subset B of A, defined by $B = \{a_j \mid 1 \leq j \leq n, i_j = 1\}$. It follows that the number of subsets of A equals the number of elements in $I \times I \times \cdots \times I$, where the number of factors is n. By (1.1.2) we obtain $|\mathcal{P}(A)| = 2^n = 2^{|A|}$. □

[1] Augustus De Morgan (1806–1871)

The power set $\mathcal{P}(A)$, together with the operations $\cup$ and $\cap$, constitutes what is known as a *Boolean*[2] *algebra*; such algebras have become very important in logic and computer science.

Exercises (1.1)

(1) Prove as many parts of (1.1.1) as possible.

(2) Let A, B, C be sets such that $A \cap B = A \cap C$ and $A \cup B = A \cup C$. Prove that $B = C$.

(3) If A, B, C are sets, establish the following:
 (i) $(A - B) - C = A - (B \cup C)$.
 (ii) $A - (B - C) = (A - B) \cup (A \cap B \cap C)$.

(4) Let A and B be finite sets. Prove that $|\mathcal{P}(A \times B)| = |\mathcal{P}(A)|^{|B|}$.

(5) Let A and B be finite sets with more than one element in each. Prove that $|\mathcal{P}(A \times B)|$ is larger than both $|\mathcal{P}(A)|$ and $|\mathcal{P}(B)|$.

(6) The *disjoint union* $A \oplus B$ of sets A and B is defined by the rule $A \oplus B = A \cup B - A \cap B$, so its elements are those that belong to exactly one of A and B. Prove the following statements:
 (i) $A \oplus A = \emptyset$, $A \oplus B = B \oplus A$.
 (ii) $(A \oplus B) \oplus C = A \oplus (B \oplus C)$.
 (iii) $(A \oplus B) \cap C = (A \cap C) \oplus (B \cap C)$.

(7) If A and B be finite sets, show that $|\mathcal{P}(A \cup B)| = \frac{|\mathcal{P}(A)| \cdot |\mathcal{P}(B)|}{|\mathcal{P}(A \cap B)|}$.

1.2 Relations, equivalence relations, partial orders

In mathematics it is often not sufficient to deal with the individual elements of a set: for it may be critical to understand how elements of the set are related to each other. This leads us to formulate the concept of a relation.

Let A and B be sets. Then a *relation R between A and B* is a subset of the set product $A \times B$. The definition is clarified by use of a suggestive notation: if $(a, b) \in R$, then a is said to be *related* to b by R and we write

$$a \; R \; b.$$

The most important case is of a relation R between A and itself; this is called *a relation on the set A*.

Example (1.2.1)

(i) Let A be a set and define $R = \{(a, a) \mid a \in A\}$. Thus $a_1 \; R \; a_2$ means that $a_1 = a_2$ and R is the relation of equality on A.

[2] George Boole (1815–1864)

(ii) Let P be the set of all points and L the set of all lines in the plane. A relation R from P to L is defined by: $p \; R \; \ell$ if the point p lies on the line ℓ.
(iii) A relation R on the set of integers $\mathbb{Z}$ is defined by: $a \; R \; b$ if $a - b$ is even.

The next result confirms what one might suspect, that a finite set has many relations.

(1.2.1) *If A is a finite set, the number of relations on A equals* $2^{|A|^2}$.

For this is the number of subsets of $A \times A$ by (1.1.2) and (1.1.3).

The concept of a relation on a set is evidently a very broad one. In practice the relations of greatest interest are those which have special properties. The most common of these are listed next. Let R be a relation on a set A.

(i) R is *reflexive* if $a \; R \; a$ for all $a \in A$.
(ii) R is *symmetric* if $a \; R \; b$ always implies that $b \; R \; a$.
(iii) R is *antisymmetric* if $a \; R \; b$ and $b \; R \; a$ imply that $a = b$;
(iv) R is *transitive* if $a \; R \; b$ and $b \; R \; c$ imply that $a \; R \; c$.

Relations which are reflexive, symmetric and transitive are called *equivalence relations*; they are of fundamental importance. Relations which are reflexive, antisymmetric and transitive are also important; they are called *partial orders*. Here are some examples of relations of various types.

Example (1.2.2)
(i) Equality on a set is both an equivalence relation and a partial order.
(ii) A relation R on $\mathbb{Z}$ is defined by: $a \; R \; b$ if and only if $a - b$ is even. This is an equivalence relation, but it is not a partial order.
(iii) If A is any set, the relation of containment $\subseteq$ is a partial order on the power set $P(A)$.
(iv) A relation R on $\mathbb{N}$ is defined by $a \; R \; b$ if a divides b. Here R is a partial order on $\mathbb{N}$.

Equivalence relations and partitions. The structure of an equivalence relation on a set will now be analyzed. The essential conclusion will be that an equivalence relation causes the set to split up into non-overlapping non-empty subsets.

Let E be an equivalence relation on a set A. First of all define the *E-equivalence class* of an element a of A to be the subset

$$[a]_E = \{x \mid x \in A \text{ and } x \; E \; a\}.$$

By the reflexive law $a \in [a]_E$, so

$$A = \bigcup_{a \in A} [a]_E$$

and A is the union of all the equivalence classes.

Next suppose that the equivalence classes $[a]_E$ and $[b]_E$ both contain an element x. Assume that $y \in [a]_E$; then $y \; E \; a$, $a \; E \; x$ and $x \; E \; b$, by the symmetric law. Hence $y \; E \; b$ by two applications of the transitive law. Therefore $y \in [b]_E$ and we have proved that

$[a]_E \subseteq [b]_E$. By the same reasoning $[b]_E \subseteq [a]_E$, so that $[a]_E = [b]_E$. It follows that distinct equivalence classes are disjoint, i.e., they have no elements in common.

What has been shown so far is that the set A is the union of the E-equivalence classes and that distinct equivalence classes are disjoint. A decomposition of A into disjoint non-empty subsets is called a *partition* of A. Thus E determines a partition of A.

Conversely, suppose that a partition of A into non-empty disjoint subsets A_λ, $(\lambda \in \Lambda)$, is given. We would like to construct an equivalence relation on A corresponding to the partition. Now each element of A belongs to a unique subset A_λ; thus we may define $a\ E\ b$ to mean that a and b belong to the same subset A_λ. It follows immediately from the definition that the relation E is an equivalence relation; what is more, the equivalence classes are just the subsets A_λ of the original partition. We summarize these conclusions in:

(1.2.2)

(i) *If E is an equivalence relation on a set A, the E-equivalence classes form a partition of A.*

(ii) *Conversely, each partition of A determines an equivalence relation on A for which the equivalence classes are the subsets in the partition.*

Thus the concepts of equivalence relation and partition are in essence the same. In the equivalence relation (ii) above there are two equivalence classes, the sets of even and odd integers; of course these form a partition of $\mathbb{Z}$.

Partial orders. Suppose that R is a partial order on a set A, i.e., R is a reflexive, antisymmetric, transitive relation on A. Instead of writing $a\ R\ b$ it is customary to employ a more suggestive symbol and write

$$a \preceq b.$$

The pair $(A, \preceq)$ then constitutes a *partially ordered set* (or *poset*).

The effect of a partial order is to impose a hierarchy on the set A. When the set is finite, this can be visualized by drawing a picture of the poset called a *Hasse*[3] *diagram*. It consists of vertices and edges drawn in the plane, the vertices representing the elements of A. A sequence of upwardly sloping edges from a to b, as in the diagram below, indicates that $a \preceq b$. Elements a, b not connected by such a sequence of edges do not satisfy $a \preceq b$ or $b \preceq a$. In order to simplify the diagram as far as possible, it is

[3] Helmut Hasse (1898–1979)