de Gruyter Textbook

Derek J. S. Robinson

An Introduction to Abstract Algebra

Derek J. S. Robinson

An Introduction to Abstract Algebra

Walter de Gruyter
Berlin · New York 2003

Author
Derek J. S. Robinson
Department of Mathematics
University of Illinois at Urbana-Champaign
1409 W. Green Street
Urbana, Illinois 61801-2975
USA

Mathematics Subject Classification 2000: 12-01, 13-01, 16-01, 20-01

Keywords: group, ring, field, vector space, Polya theory, Steiner system, error correcting code

∞ Printed on acid-free paper which falls within the guidelines of the ANSI
to ensure permanence and durability.

Library of Congress Cataloging-in-Publication Data

Robinson, Derek John Scott.
An introduction to abstract algebra / Derek J. S. Robinson.
p. cm. – (De Gruyter textbook)
Includes bibliographical references and index.
ISBN 3-11-017544-4 (alk. paper)
1. Algebra, Abstract. I. Title. II. Series.
QA162.R63 2003
512'.02–dc21 2002041471

ISBN 3 11 017544 4

Bibliographic information published by Die Deutsche Bibliothek

Die Deutsche Bibliothek lists this publication in the Deutsche Nationalbibliografie;
detailed bibliographic data is available in the Internet at <http://dnb.ddb.de>.

Printed in Germany.
Cover design: Hansbernd Lindemann, Berlin.
Typeset using the author's TEX files: I. Zimmermann, Freiburg.
Printing and binding: Hubert & Co. GmbH & Co. KG, Göttingen.

de Gruyter Textbook
Robinson · An Introduction to Abstract Algebra

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 work was concerned with 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 modern abstract algebra, groups, rings and fields. These structures have been intensively studied 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 [15].

Until quite recently algebra was very much the domain of the pure mathematician; applications were few and far between. But all this has changed 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 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 are interested in acquiring a basic knowledge of algebra and its applications. On the other hand, this is not a book on applied algebra, or discrete mathematics as it is often called nowadays.

As to what is expected of the reader, a basic knowledge of matrices is assumed and also at least the level of maturity consistent with completion of three semesters of calculus. The object is to introduce the reader to the principal structures of modern 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 third or fourth year of study at a North American university and in their second or third year at a university in the United Kingdom.

There is more than enough material here for a two semester course in abstract algebra. If just one semester is available, Chapters 1 through 7 and Chapter 10 could be covered. The first two chapters contain some things that will be known to many readers and can be covered more quickly. In addition a good deal of the material in Chapter 8 will be familiar to anyone who has taken a course in linear algebra.

A word about proofs is in order. Often students from outside mathematics question the need for rigorous proofs, although this is perhaps becoming less common. One answer is that the only way to be certain 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, although on a first reading some of the more complex arguments could be omitted. 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.

This book 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 many colleagues for much good advice and lots of stimulating conversations: these have led to numerous improvements in the text. In particular I am most grateful to Otto Kegel for reading the entire text. However full credit for all errors and mis-statements belongs to me. Finally, I thank Manfred Karbe, Irene Zimmermann and the staff at Walter de Gruyter for their encouragement and unfailing courtesy and assistance.

Urbana, Illinois, November 2002 *Derek Robinson*

Contents

Chapter 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 at least to review the material to check notation and definitions. Because of its nature the pace of this chapter is brisker 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 a *proper* subset of B.

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 just one empty set; for if E and E' are two empty sets, then $E \subseteq E'$ and $E' \subseteq E$, so that $E = E'$. This unique empty set is written

$$\emptyset.$$

Some further standard sets with a reserved notation are:

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

which are respectively the sets of natural numbers $0, 1, 2, \ldots$, 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 (possibly 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

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

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

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

Properties of set operations. We list for future reference the fundamental properties of union, intersection and complement.

(1.1.1) *Let A, B, C 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) $A - \left(\bigcup_{\lambda \in \Lambda} B_\lambda\right) = \bigcap_{\lambda \in \Lambda}(A - B_\lambda)$ *and* $A - \left(\bigcap_{\lambda \in \Lambda} B_\lambda\right) = \bigcup_{\lambda \in \Lambda}(A - B_\lambda)$ (*De Morgan's Laws*).[1]

The easy proofs of these results are left to the reader as an exercise: hopefully most of these properties will be familiar.

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

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 a_i's yields a different n-tuple. Therefore the total number of n-tuples is $|A_1| \cdot |A_2| \dots |A_n|$. □

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

$$P(A).$$

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

[1] Augustus De Morgan (1806–1871)

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

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 $B = \{a_j \mid 1 \le j \le n,\ i_j = 1\}$. It follows that the number of subsets of A equals the number of elements in $I \times I \times \cdots \times I$, (with n factors). By (1.1.2) we obtain $|P(A)| = 2^n = 2^{|A|}$. □

The power set $P(A)$, together with the operations $\cup$ and $\cap$, constitute 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:
(a) $(A - B) - C = A - (B \cup C)$.
(b) $A - (B - C) = (A - B) \cup (A \cap B \cap C)$.

4. 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:
(a) $A \oplus A = \emptyset$, $A \oplus B = B \oplus A$.
(b) $(A \oplus B) \oplus C = A \oplus (B \oplus C)$.
(c) $(A \oplus B) \cap C = (A \cap C) \oplus (B \cap C)$.

1.2 Relations, equivalence relations and partial orders

In mathematics it is often not sufficient to deal with the individual elements of a set since 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 will be clarified if we use a more suggestive notation: if $(a, b) \in R$, then a is said to be *related* to b by R and we write

$$a\ R\ b.$$

[2] George Boole (1815–1864)

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

Examples of relations. (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.

(ii) Let P be the set of points and L the set of 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. So R is the relation of incidence.

(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.

(a) R is *reflexive* if $a \, R \, a$ for all $a \in A$.

(b) R is *symmetric* if $a \, R \, b$ always implies that $b \, R \, a$.

(c) R is *antisymmetric* if $a \, R \, b$ and $b \, R \, a$ imply that $a = b$;

(d) 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*.

Examples. (a) Equality on a set is both an equivalence relation and a partial order.

(b) 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.

(c) If A is any set, the relation of containment $\subseteq$ is a partial order on the power set $P(A)$.

(d) 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 we 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 integer 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.

Example (1.2.1) In the equivalence relation (b) 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

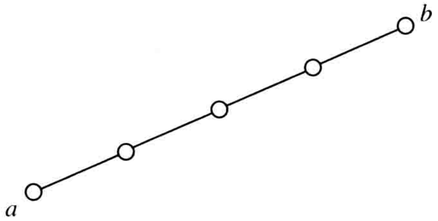
$$a \preceq b.$$

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. This can be visualized by drawing a picture of the poset called a *Hasse*[3]*diagram*. It consists of

[3] Helmut Hasse (1898-1979).

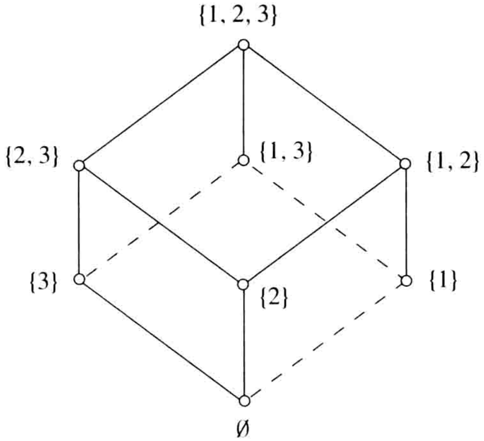
vertices and edges drawn in the plane, the vertices representing the elements of A. A sequence of upward sloping edges from a to b, as in the diagram below, indicates that $a \preceq b$, for example. Elements a, b not connected by such a sequence of edges do not satisfy $a \preceq b$ or $b \preceq a$. In order to simplify the diagram as far as possible, it is agreed that unnecessary edges are to be omitted.



A very familiar poset is the power set of a set A with the partial order $\subseteq$, i.e. $(P(A), \subseteq)$.

Example (1.2.2) Draw the Hasse diagram of the poset $(P(A), \subseteq)$ where $A = \{1, 2, 3\}$.

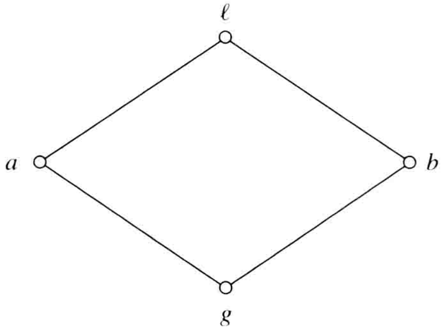
This poset has $2^3 = 8$ vertices, which can be visualized as the vertices of a cube (drawn in the plane) standing on one vertex.



Partially ordered sets are important in algebra since they can provide a useful representation of substructures of algebraic structures such as subsets, subgroups, subrings etc..

A partial order $\preceq$ on a set A is called a *linear order* if, given $a, b \in A$, either $a \preceq b$ or $b \preceq a$ holds. Then $(A, \preceq)$ is called a *linearly ordered set* or *chain*. The Hasse diagram of a chain is a single sequence of edges sloping upwards. Obvious examples of chains are $(\mathbb{Z}, \leq)$ and $(\mathbb{R}, \leq)$ where $\leq$ is the usual "less than or equal to". Finally, a linear order on A is called a *well order* if each non-empty subset X of A contains a *least* element a, i.e., such that $a \preceq x$ for all elements $x \in X$. For example, it would seem clear that $\leq$ is a well order on the set of all positive integers, although this is actually an axiom, the Well-Ordering Law, which is discussed in Section 2.1.

Lattices. Consider a poset $(A, \preceq)$. If $a, b \in A$, then a *least upper bound* (or lub) of a and b is an element $\ell \in A$ such that $a \preceq \ell$ and $b \preceq \ell$, and if $a \preceq x$ and $b \preceq x$, with x in A, then $\ell \preceq x$. Similarly a *greatest lower bound* (or glb) of a and b is an element $g \in A$ such that $g \preceq a$ and $g \preceq b$, while $x \preceq a$ and $x \preceq b$ imply that $x \preceq g$. Part of the Hasse diagram of $(A, \preceq)$ is the lozenge shaped figure



A poset in which each pair of elements has an lub and a glb is called a *lattice*. For example, $(P(S), \subseteq)$ is a lattice since the lub and glb of A and B are $A \cup B$ and $A \cap B$ respectively.

The composite of relations. Since a relation is a subset, two relations may be combined by forming their union or intersection. However there is a more useful way of combining relations called *composition*: let R and S be relations between A and B and between B and C respectively. Then the *composite relation*

$$S \circ R$$

is the relation between A and C defined by $a \; S \circ R \; c$ if there exists $b \in B$ such that $a \; R \; b$ and $b \; S \; c$.

For example, assume that $A = \mathbb{Z}$, $B = \{a, b, c\}$, $C = \{\alpha, \beta, \gamma\}$. Define relations $R = \{(1, a), (2, b), (4, c)\}$, $S = \{(a, \alpha), (b, \gamma), (c, \beta)\}$. Then $S \circ R = \{(1, \alpha), (2, \gamma), (4, \beta)\}$.

In particular one can form the composite of any two relations R and S on a set A. Notice that the condition for a relation R to be transitive can now be expressed in the form $R \circ R \subseteq R$.

A result of fundamental importance is the associative law for composition of relations.

(1.2.3) *Let R, S, T be relations between A and B, B and C, and C and D respectively. Then $T \circ (S \circ R) = (T \circ S) \circ R$.*