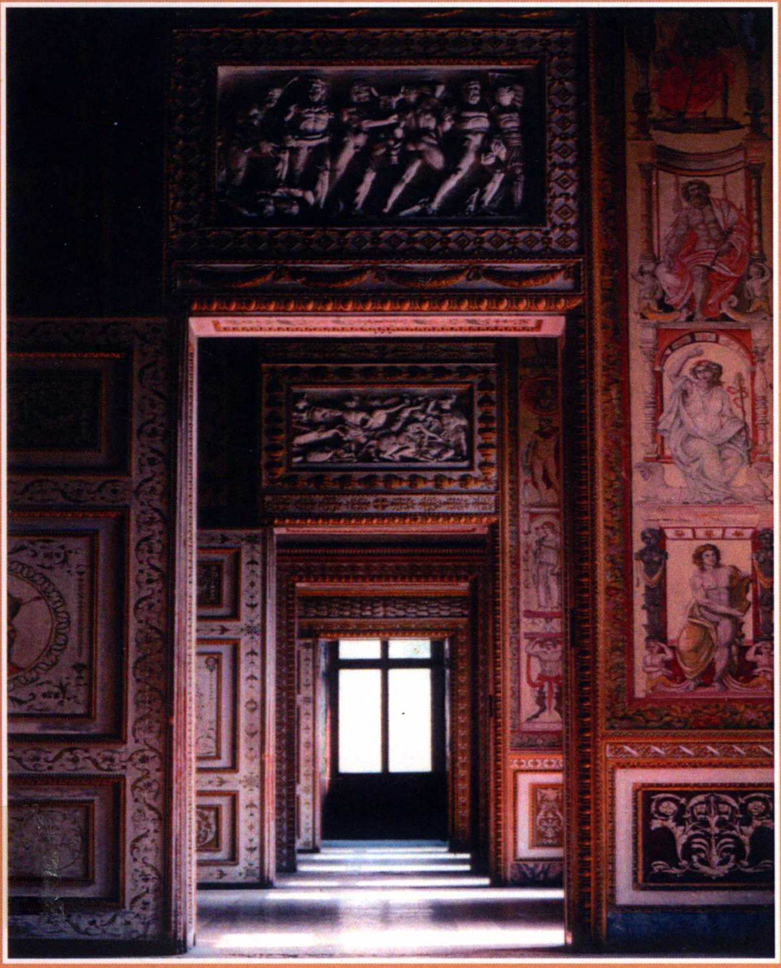
抽象代数

（第 3 版）

［美］I. N. 赫斯坦　著



WILEY

世界图书出版公司

ABSTRACT ALGEBRA

Third Edition

I. N. Herstein

Late Professor of Mathematics
University of Chicago

JOHN WILEY & SONS, INC.

图书在版编目（CIP）数据

抽象代数：第3版 = Abstract Algebra, 3rd Edition：英文 /（美）I. N. 赫斯坦（I. N. Herstein）著 . — 影印本 . — 北京：世界图书出版有限公司北京分公司，2019.6
ISBN 978-7-5192-6376-8

Ⅰ. ①抽… Ⅱ. ① I… Ⅲ. ①抽象代数—英文 Ⅳ. ① O153

中国版本图书馆 CIP 数据核字（2019）第113066号

中文书名	抽象代数（第3版）
英文书名	Abstract Algebra *Third Edition*
著　　者	［美］I. N. 赫斯坦（I. N. Herstein）
责任编辑	刘　慧　高　蓉
出版发行	世界图书出版有限公司北京分公司
地　　址	北京市东城区朝内大街137号
邮　　编	100010
电　　话	010-64038355（发行）　64033507（总编室）
网　　址	http://www.wpcbj.com.cn
邮　　箱	wpcbjst@vip.163.com
销　　售	新华书店
印　　刷	北京建宏印刷有限公司
开　　本	710 mm × 1000 mm　1/16
印　　张	16.5
字　　数	262千字
版　　次	2019年7月第1版
印　　次	2019年7月第1次印刷
版权登记	01-2019-1315
国际书号	ISBN 978-7-5192-6376-8
定　　价	69.00元

PREFACE TO THE THIRD EDITION

When we were asked to prepare the third edition of this book, it was our consensus that it should not be altered in any significant way, and that Herstein's informal style should be preserved. We feel that one of the book's virtues is the fact that it covers a big chunk of abstract algebra in a condensed and interesting way. At the same time, without trivializing the subject, it remains accessible to most undergraduates.

We have, however, corrected minor errors, straightened out inconsistencies, clarified and expanded some proofs, and added a few examples.

To resolve the many typographical problems of the second edition, Prentice Hall has had the book completely retypeset—making it easier and more pleasurable to read.

It has been pointed out to us that some instructors would find it useful to have the Symmetric Group S_n and the cycle notation available in Chapter 2, in order to provide more examples of groups. Rather than alter the arrangement of the contents, thereby disturbing the original balance, we suggest an alternate route through the material, which addresses this concern. After Section 2.5, one could spend an hour discussing permutations and their cycle decomposition (Sections 3.1 and 3.2), leaving the proofs until later. The students might then go over several past examples of finite groups and explicitly set up isomorphisms with subgroups of S_n. This exercise would be motivated by Cayley's theorem, quoted in Section 2.5. At the same time, it would have the beneficial result of making the students more comfortable with the concept of an isomorphism. The instructor could then weave in the various subgroups of the Symmetric Groups S_n as examples throughout the remainder of Chapter 2. If desired, one could even introduce Sections 3.1 and 3.2 after Section 2.3 or 2.4.

Two changes in the format have been made since the first edition. First, a Symbol List has been included to facilitate keeping track of terminology. Second, a few problems have been marked with an asterisk (*). These serve as a vehicle to introduce concepts and simple arguments that relate in some important way to the discussion. As such, they should be read carefully.

Finally, we take this opportunity to thank the many individuals whose collective efforts have helped to improve this edition. We thank the reviewers: Kwangil Koh from North Carolina State University, Donald Passman from the University of Wisconsin, and Robert Zinc from Purdue University. And, of course, we thank George Lobell and Elaine Wetterau, and others at Prentice Hall who have been most helpful.

Barbara Cortzen
David J. Winter

PREFACE TO THE FIRST EDITION

In the last half-century or so abstract algebra has become increasingly important not only in mathematics itself, but also in a variety of other disciplines. For instance, the importance of the results and concepts of abstract algebra play an ever more important role in physics, chemistry, and computer science, to cite a few such outside fields.

In mathematics itself abstract algebra plays a dual role: that of a unifying link between disparate parts of mathematics and that of a research subject with a highly active life of its own. It has been a fertile and rewarding research area both in the last 100 years and at the present moment. Some of the great accomplishments of our twentieth-century mathematics have been precisely in this area. Exciting results have been proved in group theory, commutative and noncommutative ring theory, Lie algebras, Jordan algebras, combinatorics, and a host of other parts of what is known as abstract algebra. A subject that was once regarded as esoteric has become considered as fairly down-to-earth for a large cross section of scholars.

The purpose of this book is twofold. For those readers who either want to go on to do research in mathematics or in some allied fields that use algebraic notions and methods, this book should serve as an introduction—and, we stress, only as an introduction—to this fascinating subject. For interested readers who want to learn what is going on in an engaging part of modern mathematics, this book could serve that purpose, as well as provide them with some highly usable tools to apply in the areas in which they are interested.

The choice of subject matter has been made with the objective of introducing readers to some of the fundamental algebraic systems that are both interesting and of wide use. Moreover, in each of these systems the aim has been to arrive at some significant results. There is little purpose served in studying some abstract object without seeing some nontrivial consequences of the study. We hope that we have achieved the goal of presenting interesting, applicable, and significant results in each of the systems we have chosen to discuss.

As the reader will soon see, there are many exercises in the book. They are often divided into three categories: easier, middle-level, and harder (with an occasional very hard). The purpose of these problems is to allow students to test their assimilation of the material, to challenge their mathematical ingenuity, to prepare the ground for material that is yet to come, and to be a means of developing mathematical insight, intuition, and techniques. Readers should not become discouraged if they do not manage to solve all the problems. The intent of many of the problems is that they be tried—even if not solved—for the pleasure (and frustration) of the reader. Some of the problems appear several times in the book. Trying to do the problems is undoubtedly the best way of going about learning the subject.

We have strived to present the material in the language and tone of a classroom lecture. Thus the presentation is somewhat chatty; we hope that this will put the readers at their ease. An attempt is made to give many and revealing examples of the various concepts discussed. Some of these examples are carried forward to be examples of other phenomena that come up. They are often referred to as the discussion progresses.

We feel that the book is self-contained, except in one section—the second last one of the book—where we make implicit use of the fact that a polynomial over the complex field has complex roots (that is the celebrated *Fundamental Theorem of Algebra* due to Gauss), and in the last section where we make use of a little of the calculus.

We are grateful to many people for their comments and suggestions on earlier drafts of the book. Many of the changes they suggested have been incorporated and should improve the readability of the book. We should like to express our special thanks to Professor Martin Isaacs for his highly useful comments.

We are also grateful to Fred Flowers for his usual superb job of typing the manuscript, and to Mr. Gary W. Ostedt of the Macmillan Company for his enthusiasm for the project and for bringing it to publication.

With this we wish all the readers a happy voyage on the mathematical journey they are about to undertake into this delightful and beautiful realm of abstract algebra.

I.N.H.

SYMBOL LIST

$a \in S$	a is an element of the set S, 3
$a \notin S$	a is not an element of the set S, 3
$S \subset T$, $T \supset S$	S is a subset of the set T, 3
$S = T$	The sets S and T are equal (have the same elements), 4
$\emptyset$	The empty set, 4
$A \cup B$	The union of the sets A and B, 4
$A \cap B$	The intersection of the sets A and B, 4
$\{s \in S \mid s \text{ satisfies } P\}$	The subset of elements of S satisfying P, 4
$A - B$	The difference of the sets A and B, 4
A'	The complement of A, 5
(a, b)	Ordered pair consisting of a, b (see also below), 5
$A \times B$	The Cartesian product of A and B, 5
$\mathbb{R}$	The set of real numbers, 8
$f: S \to T$	Function from the set S to the set T, 8
$f(s)$	Image of the element s under the function f, 8
$i: S \to S$, i_S	The identity function on S, 9
$f^{-1}(t)$	Inverse image of t under f, 10
$f^{-1}(A)$	Inverse image of a subset A of T under $f: S \to T$, 10
$f \circ g$, fg	Composition or product of functions f and g, 11, 18
$A(S)$	Set of 1-1 mappings from a set S to S, 16
S_n	Symmetric group of degree n, 16, 109
$n!$	n factorial, 17
$\mathbb{Z}$	Set of integers, 21
$O(s)$	Orbit of s relative to mapping f, 21

$\mathbb{N}$	Set of positive integers, 21
$m \mid n$	m divides n, 22
$m \nmid n$	m does not divide n, 22
(a, b)	Greatest common divisor of a, b (see also above), 23
$\mathbb{C}$	Set of complex numbers, 32
$i, -i$	Square roots of -1, 32
$z = a + bi$	Complex number z with real part a and imaginary part b, 32
$\bar{z} = a - bi$	Conjugate of complex number $z = a + bi$, 32
$1/z$	Inverse of the complex number z, 33
$\lvert z\rvert$	Absolute value of complex number z, 34
$r(\cos\theta + i\sin\theta)$	Polar form of a complex number, 35
θ_n	Primitive nth root of unity, 36, 42
$\mathbb{Q}$	Set of rational numbers, 42
E_n	Group of nth roots of unity, 42
$\lvert G\rvert$	Order of the group G, 42
$C(a)$	Centralizer of a in G, 53, 102
(a)	Cyclic group generated by a, 53
$Z(G)$	Center of group G, 53
$a \sim b$	a is equivalent to b in a specified sense, 57
$a \equiv b \bmod n$	a is congruent to b modulo n (long form), 57
$a \equiv b(n)$	a is congruent to b modulo n (short form), 57
$[a]$	Class of all b equivalent to a, 58
$\mathrm{cl}(a)$	Conjugacy class of a, 58, 101
$o(a)$	Order of element a of a group, 60
$i_G(H)$	Index of H in G, 59
$\mathbb{Z}_n$	Set of integers mod n, 61
U_n	Group of invertible elements of $\mathbb{Z}_n$, 62
$\varphi(n)$	Euler φ function (phi function), 62
Hb	Right coset of subgroup H, 58
aH	Left coset of subgroup H, 64
$G \simeq G'$	Group G is isomorphic to group G', 68
$\varphi(G)$	Image of homomorphism, 70
$\mathrm{Ker}\,\varphi$	Kernel of the homomorphisms φ, 70, 140
$N \lhd G$	N is a normal subgroup of G, 72
G/N	Quotient of a group G by a subgroup N, 78
AB	Product of subsets A, B of a group, 79
$G_1 \times G_2 \times \dots \times G_n$	Direct product of $G_1, G_2, \dots, G_n$, 93
$\begin{pmatrix} a & b & \dots & c \\ u & v & \dots & w \end{pmatrix}$	Permutation sending a to u, b to $v, \dots, c$ to w, 110
$(a, b, \dots, c)$	Cycle sending a to $b, \dots, c$ to a, 111
A_n	Alternating group of degree n, 121, 215
$\alpha_0 + \alpha_1 i + \alpha_2 j + \alpha_3 k$	Quaternion, 131
$\det x$	Determinate of the 2×2 matrix x, 136

$H(F)$	Ring of quaternions over F, 136
$R \oplus S$	Direct sum of rings R, S, 146
(a)	Ideal generated by a in a commutative ring, 145
$F[x]$	Polynomial ring over the field F, 152
$\deg p(x)$	Degree of polynomial $p(x)$, 153
$(g(x))$	Ideal generated by $g(x)$ in a polynomial ring, 157
$g(x) \mid f(x)$	Polynomial $g(x)$ divides $f(x)$, 157
$R[x]$	Polynomial ring over ring R, 163
$F(x)$	Field of rational functions in x over F, 177
$v \in V$	Vector v in a vector space V, 180
αv	Scalar α times vector v, 180
$\alpha_1 v_1 + \ldots + \alpha_n v_n$	Linear combination of vectors $v_1, \ldots, v_n$, 181
$\langle v_1, v_2, \ldots, v_n \rangle$	Subspace spanned by $v_1, v_2, \ldots, v_n$, 181
$V \oplus W$	Direct sum of vector spaces V, W, 181
$\dim_F(V)$	Dimension of V over F, 186
$U + W$	Sum of subspaces U, W of V, 190
$[K : F]$	Degree of K over F, 191
$F[a]$	Ring generated by a over F, 196
$F(a)$	Field extension obtained by adjoining to a to F, 196
$E(K)$	Field of algebraic elements of K over F, 198
$f'(x)$	Formal derivative of polynomial $f(x)$, 227
$\phi_n(x)$	nth cyclotomic polynomial, 230

ABSTRACT ALGEBRA

Cover Photograph: Charnley Residence, entryway.
Photo by © Nick Merrick/Hedrich-Blessing

This book was typeset in 10/12 Times Ten Roman by University Graphics, Inc.

The paper in this book was manufactured by a mill whose forest management programs include sustained yield harvesting of it timberlands. Sustained yield harvesting principles ensure that the number of trees cut each year does not exceed the amount of new growth.

Library of Congress Cataloging in Publication Data

Herstein, I. N.
Abstract algebra / I.N. Herstein. — 3rd ed.
p. cm.
Includes index.
ISBN 0-471-36879-2
1. Algebra, Abstract. I. Title
QA162.H47 1995 95-21470
512'.02—dc20 CIP

To Biška

目　录

1

THINGS FAMILIAR AND LESS FAMILIAR

1. A FEW PRELIMINARY REMARKS

For many readers this book will be their first contact with abstract mathematics. The subject to be discussed is usually called "abstract algebra," but the difficulties that the reader may encounter are not so much due to the "algebra" part as they are to the "abstract" part.

On seeing some area of abstract mathematics for the first time, be it in analysis, topology, or what-not, there seems to be a common reaction for the novice. This can best be described by a feeling of being adrift, of not having something solid to hang on to. This is not too surprising, for while many of the ideas are fundamentally quite simple, they are subtle and seem to elude one's grasp the first time around. One way to mitigate this feeling of limbo, or asking oneself "What is the point of all this?," is to take the concept at hand and see what it says in particular cases. In other words, the best road to good understanding of the notions introduced is to look at examples. This is true in all of mathematics, but it is particularly true for the subject matter of abstract algebra.

Can one, with a few strokes, quickly describe the essence, purpose, and background for the material we shall study? Let's give it a try.

We start with some collection of objects S and endow this collection with an algebraic structure by assuming that we can combine, in one or several ways (usually two), elements of this set S to obtain, once more, elements of this set S. These ways of combining elements of S we call *operations* on S.

Then we try to condition or regulate the nature of S by imposing certain rules on how these operations behave on S. These rules are usually called the *axioms* defining the particular structure on S. These axioms are for us to define, but the choice made comes, historically in mathematics, from noticing that there are many concrete mathematical systems that satisfy these rules or axioms. We shall study some of the basic axiomatic algebraic systems in this book, namely *groups*, *rings*, and *fields*.

Of course, one could try many sets of axioms to define new structures. What would we require of such a structure? Certainly we would want that the axioms be consistent, that is, that we should not be led to some nonsensical contradiction computing within the framework of the allowable things the axioms permit us to do. But that is not enough. We can easily set up such algebraic structures by imposing a set of rules on a set S that lead to a pathological or weird system. Furthermore, there may be very few examples of something obeying the rules we have laid down.

Time has shown that certain structures defined by "axioms" play an important role in mathematics (and other areas as well) and that certain others are of no interest. The ones we mentioned earlier, namely groups, rings, and fields, have stood the test of time.

A word about the use of "axioms." In everyday language "axiom" means a self-evident truth. But we are not using everyday language; we are dealing with mathematics. An axiom is not a universal truth—but one of several rules spelling out a given mathematical structure. The axiom is true in the system we are studying because we have forced it to be true by hypothesis. It is a license, in the particular structure, to do certain things.

We return to something we said earlier about the reaction that many students have on their first encounter with this kind of algebra, namely a lack of feeling that the material is something they can get their teeth into. Do not be discouraged if the initial exposure leaves you in a bit of a fog. Stick with it, try to understand what a given concept says, and most importantly, look at particular, concrete examples of the concept under discussion.

PROBLEMS

1. Let S be a set having an operation $*$ which assigns an element $a * b$ of S for any $a, b \in S$. Let us assume that the following two rules hold:

1. If a, b are any objects in S, then $a * b = a$.
2. If a, b are any objects in S, then $a * b = b * a$.

Show that S can have at most one object.