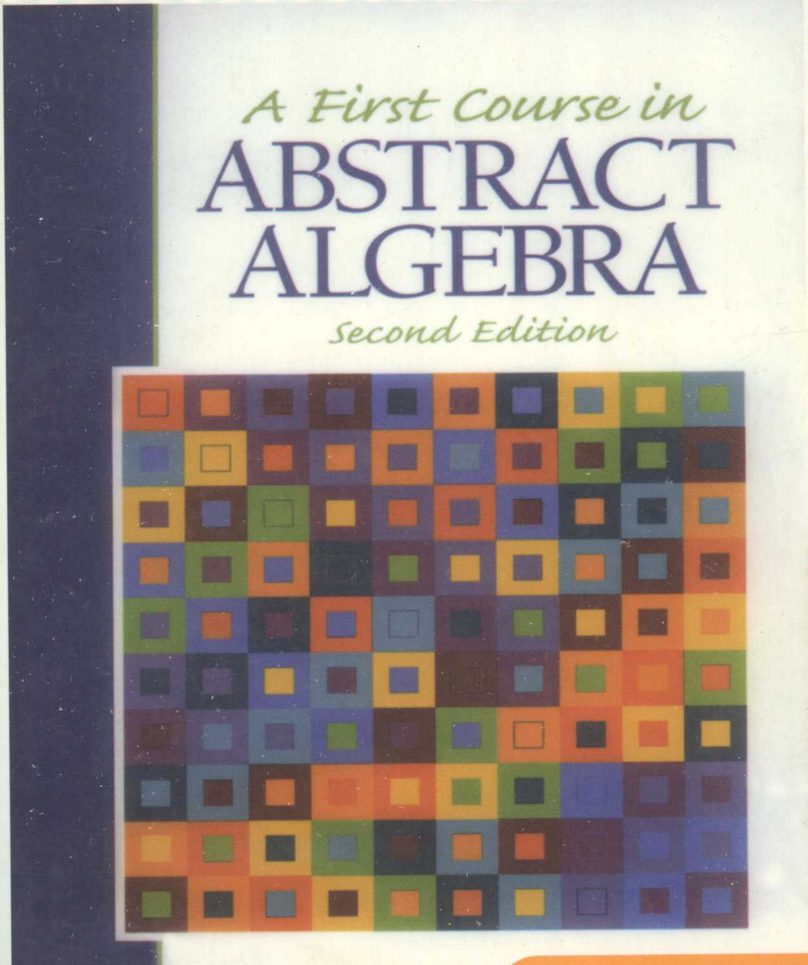
HZ BOOKS

PEARSON
Prentice Hall

经典原版书库

抽象代数基础教程

（英文版·第2版）



A First Course in

ABSTRACT ALGEBRA

Second Edition

JOSEPH J.

（美）Joseph J. Rotman 著

伊利诺伊大学

机械工业出版社
China Machine Press

经典原版书库

抽象代数基础教程

（英文版·第2版）

A First Course in Abstract Algebra

(Second Edition)

（美）Joseph J. Rotman 著
伊利诺伊大学

机械工业出版社
China Machine Press

本书版权登记号：图字：01-2004-3686

图书在版编目（CIP）数据

抽象代数基础教程（英文版·第2版）/（美）罗特曼（Rotman, J. J.）著. –北京：机械工业出版社，2004.7

（经典原版书库）

书名原文：A First Course in Abstract Algebra, Second Edition

ISBN 7-111-14688-3

Ⅰ. 抽… Ⅱ. 罗… Ⅲ. 抽象代数–教材–英文 Ⅳ. O153

中国版本图书馆CIP数据核字（2004）第057878号

机械工业出版社（北京市西城区百万庄大街22号 邮政编码 100037）

责任编辑：迟振春

北京牛山世兴印刷厂印刷·新华书店北京发行所发行

2004年7月第1版第1次印刷

787mm ×1092mm 1/16 · 34.25印张

印数：0 001-3 000册

定价：49.00元

凡购本书，如有倒页、脱页、缺页，由本社发行部调换

本社购书热线：（010）68326294

Special Notation

$\|X\|$	number of elements in a finite set X
$a \mid b$	the integer a is a divisor of the integer b
$\mathbb{C}$	complex numbers
$\mathrm{GF}(q)$	finite field having q elements
$\mathbb{F}_q$	finite field having q elements
$\mathbb{N}$	natural numbers $= \{\text{integers } n : n \geq 0\}$
$\mathbb{Q}$	rational numbers
$\mathbb{R}$	real numbers
$\mathbb{Z}$	integers
A_n	alternating group on n letters
D_{2n}	dihedral group of order $2n$
$\mathrm{GL}(V)$	all automorphisms of a vector space V
$\mathrm{GL}(n, k)$	all $n \times n$ nonsingular matrices with entries in a field k
$\mathrm{SL}(n, k)$	all $n \times n$ matrices of determinant 1 with entries in a field k
$\mathrm{UT}(n, k)$	unitriangular $n \times n$ matrices over a field k
$\mathbf{Q}$	quaternion group of order 8
S_n	symmetric group on n letters
S_X	symmetric group on a set X
$\mathbf{V}$	four-group
$\mathbb{Z}_m$	integers modulo m
$\mathrm{Frac}(R)$	fraction field of a domain R
G'	commutator subgroup
$Z(G)$	center of a group G
$\mathrm{sgn}(\alpha)$	signum of a permutation α
$\deg(f)$	degree of a polynomial $f(x)$
$\det(A)$	determinant of a matrix A
E	identity matrix
1_X	identity function on a set X
δ_{ij}	Kronecker delta $\delta_{ij} = \begin{cases} 1 & \text{if } i = j \\ 0 & \text{if } i \neq j \end{cases}$

To my two wonderful kids,
Danny and Ella,
whom I love very much

Preface to the First Edition

A First Course in Abstract Algebra introduces three related topics: number theory (division algorithm, greatest common divisors, unique factorization into primes, and congruences), group theory (permutations, Lagrange's theorem, homomorphisms, and quotient groups), and commutative ring theory (domains, fields, polynomial rings, homomorphisms, quotient rings, and finite fields). The final chapter combines the preceding chapters to solve some classical problems: angle trisection, squaring the circle, doubling the cube, construction of regular n-gons, and impossibility of generalizing the quadratic, cubic, and quartic formulas to polynomials of higher degree. Such results make it clear that mathematics is, indeed, one subject whose various areas do bear one on the other.

A complicating factor, permeating introductory courses, is that this may be one of the first times students are expected to read and write proofs. This book is my attempt to cover the required topics, to give models of proofs, and to make it all enjoyable.

There is enough material here for a two-semester course, even though many readers may be interested in only one semester's worth. All the "usual suspects" are assembled here, however, and I hope that instructors will be able to find those theorems and examples they believe to be appropriate for a first course. When teaching a one-semester course, one must skip parts of the text; however, it is often possible simply to state and use theorems whose proofs have been omitted. For example, if the discussion of generalized associativity is omitted, one can safely cite the laws of exponents; if the proof of Gauss's lemma is omitted, one can quote it and still derive irreducibility criteria for polynomials in $\mathbb{Q}[x]$. ...

I do not enjoy reading introductory chapters of books that consist wholly of "tools" needed for understanding subsequent material. By the Golden Rule, I do not inflict such greetings on my readers. Rather than beginning with a discussion of logic, sets, Boolean operations, functions, equivalence relations, and so forth, I introduce such tools as they are needed. For example, functions and bijections are introduced with permutation groups; equivalence relations are introduced in Chapter 3 to construct fraction fields of domains (I recognize that this late entry of equivalence relations and equivalence classes may annoy those who prefer introducing quotient groups with them; however, I feel that readers first meeting cosets and quotient groups do not need the extra baggage of an earlier discussion of equivalence classes). The first section of Chapter 1 does introduce an essential tool, induction, but induction also serves there as a vehicle to introduce more interesting topics such as primes and De Moivre's theorem.

Several results that are not usually included in a first course have been included just because they are interesting and accessible applications; they should not be presented in class because they are designed for curious readers only. In Chapter 1 on number theory, congruences are used to find on which day of the week a given date falls. In Chapter 2 on groups, the group of motions of the plane is used to describe symmetry of planar figures, the affine group is used to prove theorems of plane geometry, and a counting lemma is applied to solve some difficult combinatorial problems. In Chapter 3 on rings, we construct finite fields, and then we use them to construct complete sets of orthogonal Latin squares. The (fourth) chapter is both a dessert and an appetizer. After a short discussion of vector spaces and dimension (which reinforces the categorical viewpoint of objects and morphisms), we show how modern algebra solves several classical problems of geometry. After giving the quadratic, cubic, and quartic formulas, we present an analogy between symmetry groups of figures and Galois groups, and we prove the theorem of Abel and Ruffini that there is no generalization of the classical formulas to higher degree polynomials. This discussion can serve as an introduction to Galois Theory.

Since Birkhoff and Mac Lane created this course half a century ago, there has been mild controversy about the order of presentation: should the exposition of groups precede that of rings, or should rings be done first (Birkhoff and Mac Lane do rings first). There are arguments on both sides and, after being a rings first man for a long time, I have come to believe that it is more reasonable to do groups first. The definition of group is very simple, and permutation groups offer an immediate nontrivial example. Many elementary properties of rings are much simpler once one has studied groups. Indeed, the very definition of a ring is more palatable once one has seen groups. As a second example, the quotient group construction can be used to construct quotient rings (since rings are additive abelian groups and ideals are normal subgroups), but the quotient ring construction cannot be used directly in constructing quotient groups. Thus, discussing groups first is more efficient than the alternative. Finally, whenever I have taught rings first, I have found an initial confusion in the class about the relation of general rings to the particular ring $\mathbb{Z}$ of integers. There is a need to develop some arithmetic properties of $\mathbb{Z}$, and bouncing back and forth between commutative rings and $\mathbb{Z}$ creates an unnecessary difficulty for many students. In particular, students become unsure about which properties of $\mathbb{Z}$ may be assumed and which need proof. The organization here avoids this problem by separating these two subjects by group theory.

Giving the etymology of mathematical terms is rarely done. Let me explain, with an analogy, why I have included derivations of many terms. There are many variations of standard poker games and, in my poker group, the dealer announces the game of his choice by naming it. Now some names are better than others. For example, "Little Red" is a game in which one's smallest red card is wild; this is a good name because it reminds the players of its distinctive feature. On the other hand, "Aggravation" is not such a good name, for though it is, indeed, suggestive, the name does not distinguish this particular game from several others. Most terms in mathematics have been well chosen; there are more red names than aggravating ones. An example of a good name is *even* permutation, for a permutation is even if it is a product of an even number of transpositions. Another example of a good term is the *parallelogram law* describing vector addition. But many good names, clear when they were chosen, are now obscure because their roots are either in another language or in another discipline. The term *mathematics* is obscure only because most of us do not know that it comes from the classical Greek word meaning "to learn." The term *corollary* is doubly obscure; it comes from the Latin word meaning "flower," but what do flowers have to do with theorems? A plausible explanation is that it was common, in ancient Rome, to give flowers as gifts, and so a corollary is a gift bequeathed by a theorem. The term *theorem* comes from the Greek word meaning "to watch" or "to contemplate" (*theatre* has the same root); it was used by Euclid with its present meaning. The term *lemma* comes from the Greek word meaning "taken" or "received;" it is a statement that is taken for granted (for it has already been proved) in the course of proving a theorem. On the other hand, I am not too fond of the mathematical terms *normal* and *regular* for, in themselves, they convey no specific meaning. Since the etymology of terms often removes unnecessary obscurity, it is worthwhile (and interesting!) to do so.

It is a pleasure to thank Dan Grayson, Heini Halberstam, David G. Poole, Ed Reingold, and John Wetzel for their suggestions. I also thank the Hebrew University of Jerusalem for the hospitality given me as I completed my manuscript. I thank the several reviewers who carefully read my manuscript and made valuable suggestions. They are Daniel D. Anderson, University of Iowa; Michael J. J. Barry, Allegheny College; Brad Shelton, University of Oregon; Warren M. Sinnott, Ohio State University; and Dalton Tarwater, Texas Tech University. And I thank George Lobell, who persuaded me to develop and improve my first manuscript into the present text.

Joseph J. Rotman

Preface to the Second Edition

I was reluctant to accept Prentice Hall's offer to write a second edition of this book. When I wrote the first edition several years ago, I assumed the usual assumption: All first courses in algebra have essentially the same material, and so it is not necessary to ask *what* is in such a book, but rather *how* it is in it. I think that most people accept this axiom, at least tacitly, and so their books are almost all clones of one another, differing only in the quality of the writing. Looking at the first version of my book, I now see many flaws; there were some interesting ideas in it, but the book was not significantly different from others. I could improve the text I had written, but I saw no reason to redo it if I were to make only cosmetic changes.

I then thought more carefully about what an introduction to algebra ought to be. When Birkhoff and Mac Lane wrote their pioneering *A Survey of Modern Algebra* about 60 years ago, they chose the topics that they believed were most important, both for students with a strong interest in algebra and those with other primary interests in which algebraic ideas and methods are used. Birkhoff and Mac Lane were superb mathematicians, and they chose the topics for their book very well. Indeed, their excellent choice of topics is what has led to the clone producing assumption I have mentioned above. But times have changed; indeed, Mac Lane himself has written a version of *A Survey of Modern Algebra* from a categorical point of view. [I feel it is too early to mention categories explicitly in this book, for I believe one learns from the particular to the general, but categories are present implicitly in the almost routine way homomorphisms are introduced as soon as possible after introducting algebraic systems.] Whereas emphasis on rings and groups is still fundamental, there are today major directions which either did not exist in 1940 or were not then recognized to be so important. These new directions involve algebraic geometry, computers, homology, and representations. One may view this new edition as the first of a two volume sequence. This book, the first volume, is designed for students beginning their study of algebra. The sequel, designed for beginning graduate students, is designed to be independent of this one. Hence, the sequel will have a substantial overlap with this book, but it will go on to discuss some of the basic results which lead to the most interesting contemporary topics. Each generation should survey algebra to make it serve the present time.

When I was writing this second edition, I was careful to keep the pace of the exposition at its original level; one should not rush at the beginning. Besides rewriting and rearranging theorems, examples, and exercises that were present in the first edition, I have added new material. For example, there is a short subsection on euclidean rings which contains a proof of Fermat's Two-Squares Theorem; and the Fundamental Theorem of Galois Theory is stated and used to prove the Fundamental Theorem of Algebra: the complex numbers are algebraically closed.

I have also added two new chapters, one with more group theory and one with more commutative rings, so that the book is now more suitable for a one-year course (one can also base a one-semester course on the first three chapters). The new chapter on groups proves the Sylow theorems, the Jordan-Hölder theorem, and the fundamental theorem of finite abelian groups, and it introduces free groups and presentations by generators and relations. The new chapter on rings discusses prime and maximal ideals, unique factorization in polynomial rings in several variables, noetherian rings, varieties, and Gröbner bases. Finally, a new section contains hints for most of the exercises (and an instructor's solution manual contains complete solutions for all the exercises in the first four chapters).

In addition to thanking again those who helped me with the first edition, it is a pleasure to thank Daniel D. Anderson, Andrew Bremner, Aldo Brigaglia, E. Graham Evans, Daniel Flath, William Haboush, Dan Grayson, Christopher Heil, Gerald J. Janusz, Carl Jockusch, Jennifer D. Key, Steven L. Kleiman, David Leep, Emma Previato, Juan Jorge Schaffer, and Thomas M. Songer for their valuable suggestions for this book.

And so here is edition two; my hope is that it makes modern algebra accessible to beginners, and that it will make its readers want to pursue algebra further.

Joseph J. Rotman

Contents

1

Number Theory

1.1 Induction

There are many styles of proof, and mathematical induction is one of them. We begin by saying what mathematical induction is not. In the natural sciences, ***inductive reasoning*** is the assertion that a freqently observed phenomenon will always occur. Thus, one says that the Sun will rise tomorrow morning because, from the dawn of time, the Sun has risen every morning. This is not a legitimate kind of proof in mathematics, for even though a phenomenon has been observed many times, it need not occur forever.

Inductive reasoning is valuable in mathematics because seeing patterns in data often helps in guessing what may be true in general. On the other hand, inductive reasoning is not adequate for proving theorems. Before we see examples, let us make sure that we agree on the meaning of some standard terms.

Definition. An ***integer*** is one of $0, 1, -1, 2, -2, 3, \ldots$.

Definition. An integer d is a ***divisor*** of an integer n if $n = da$ for some integer a. An integer $n \geq 2$ is called ***prime***[1] if its only positive divisors are 1 and n; otherwise, n is called ***composite***.

[1] One reason the number 1 is not called a prime is that many theorems involving primes would otherwise be more complicated to state.

An integer $n \geq 2$ is composite if it has a factorization $n = ab$, where $a < n$ and $b < n$ are positive integers; the inequalities are present to eliminate the uninteresting factorization $n = n \times 1$. The first few primes are 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, . . . ; that this sequence never ends is proved in Corollary 1.27.

Consider the assertion, for n a positive integer, that

$$f(n) = n^2 - n + 41$$

is always prime. Evaluating $f(n)$ for $n = 1, 2, 3, \ldots, 40$ gives the numbers

$$\begin{aligned}&41, 43, 47, 53, 61, 71, 83, 97, 113, 131,\\ &151, 173, 197, 223, 251, 281, 313, 347, 383, 421,\\ &461, 503, 547, 593, 641, 691, 743, 797, 853, 911,\\ &971, 1033, 1097, 1163, 1231, 1301, 1373, 1447, 1523, 1601.\end{aligned}$$

It is tedious, but not very difficult, to show that every one of these numbers is prime (see Proposition 1.3). Inductive reasoning predicts that *all* the numbers of the form $f(n)$ are prime. But the next number, $f(41) = 1681$, is not prime, for $f(41) = 41^2 - 41 + 41 = 41^2$, which is, obviously, composite. Thus, inductive reasoning is not appropriate for mathematical proofs.

Here is an even more spectacular example (which I first saw in an article by W. Sierpinski). Recall that ***perfect squares*** are numbers of the form n^2, where n is an integer; the first few perfect squares are 1, 4, 9, 16, 25, 36, ... For each $n \geq 1$, consider the statement

$$S(n)\colon 991n^2 + 1 \text{ is not a perfect square.}$$

The nth statement, $S(n)$, is true for many n; in fact, the smallest number n for which $S(n)$ is false is

$$\begin{aligned} n &= 12, 055, 735, 790, 331, 359, 447, 442, 538, 767\\ &\approx 1.2 \times 10^{28}.\end{aligned}$$

(The original equation, $m^2 = 991n^2 + 1$, is an example of ***Pell's equation***—an equation of the form $m^2 = pn^2 + 1$, where p is prime—and there is a way of calculating all possible solutions of it. An even more spectacular example of Pell's equation involves the prime $p = 1{,}000{,}099$; the smallest n for which $1{,}000{,}099n^2 + 1$ is a perfect square has 1116 digits.) The most generous estimate of the age of the earth is 10 billion (10,000,000,000) years, or 3.65×10^{12} days, a number insignificant when compared to 1.2×10^{28}, let alone 10^{1115}. If, starting from the Earth's very first day, one verified statement $S(n)$ on the nth day, then there would be today as much evidence of the general truth of these statements as there is that the Sun will rise tomorrow morning. And yet some of the statements $S(n)$ are false!

As a final example, let us consider the following statement, known as ***Goldbach's conjecture***: Every even number $m \geq 4$ is a sum of two primes. (It would be foolish to demand that all odd numbers be sums of two primes. For example, let us show that 27 is not the sum of two primes. Otherwise, $27 = p + q$, where p and q are primes. Now one of the summands must be even (for the sum of two odds is even); as $p = 2$ is the only even prime, it follows that $q = 25$, which is not prime.)

No one has ever found a counterexample to Goldbach's Conjecture, but neither has anyone ever proved it. At present, the conjecture has been verified for all even numbers $m < 10^{13}$ by H. J. J. te Riele and J.-M. Deshouillers. It has been proved by J.-R. Chen (with a simplification by P. M. Ross) that every sufficiently large even number m can be written as $p + q$, where p is prime and q is "almost" a prime; that is, q is either a prime or a product of two primes. Even with all of this positive evidence, however, no mathematician will say that Goldbach's Conjecture must, therefore, be true for all even m.

We have seen what (mathematical) induction is not; let us now discuss what induction is. Suppose one has a list of statements

$$S(1), S(2), \dots, S(n), \dots,$$

one for each positive integer n. Having determined that many statements on this list are true, one may guess that every $S(n)$ is true. Induction is a technique of proving that *all* the statements $S(n)$ on the list are, indeed, true. For example, the reader may check that $2^n > n$ for many values of n, but is this inequality true for every positive integer n? We will soon prove, using induction, that this is so.

Our discussion is based on the following property of positive integers (usually called the *Well Ordering Principle*).

Least Integer Axiom. There is a smallest integer in every nonempty collection C of positive integers.

Saying that C is *nonempty* merely means that there is at least one integer in the collection C. Although this axiom cannot be proved (it arises in analyzing what integers are), it is certainly plausible. Consider the following procedure. Check whether 1 belongs to C; if it does, then it is the smallest integer in C. Otherwise, check whether 2 belongs to C; if it does, then 2 is the smallest integer; if not, check 3. Continue this procedure until one bumps into C; this will occur eventually because C is nonempty.

Remark. The Least Integer Axiom holds for the set of nonnegative integers as well as for the set of positive integers: any nonempty collection C of the nonnegative integers contains a smallest integer. If C contains 0, then 0 is the smallest integer in C; otherwise, C is actually a nonempty collection of positive integers, and the original axiom now applies to C. ◀

We begin by recasting the Least Integer Axiom.

Proposition 1.1 (Least Criminal). *Let $S(1), S(2), \ldots, S(n), \ldots$ be statements, one for each integer $n \geq 1$. If some of these statements are false, then there is a first false statement.*

Proof. Let C be the collection of all those positive integers n for which $S(n)$ is false; by hypothesis, C is nonempty. The Least Integer Axiom provides a smallest integer m in C, and $S(m)$ is the first false statement. •

This seemingly innocuous proposition is useful.

Theorem 1.2. *Every integer $n \geq 2$ is either a prime or a product of primes.*

Proof. Were this not so, there would be "criminals," that is, integers $n \geq 2$ neither prime nor a product of primes; a least criminal m is the smallest such integer. Since m is not a prime, it is composite; there is thus a factorization $m = ab$ with $2 \leq a < m$ and $2 \leq b < m$ (since a is an integer, $1 < a$ implies $2 \leq a$). Since m is the least criminal, both a and b are "honest," i.e.,

$$a = pp'p'' \cdots \text{ and } b = qq'q'' \cdots,$$

where the factors p and q are primes. Therefore,

$$m = ab = pp'p'' \cdots qq'q'' \cdots$$

is a product of (at least two) primes, which is a contradiction. •