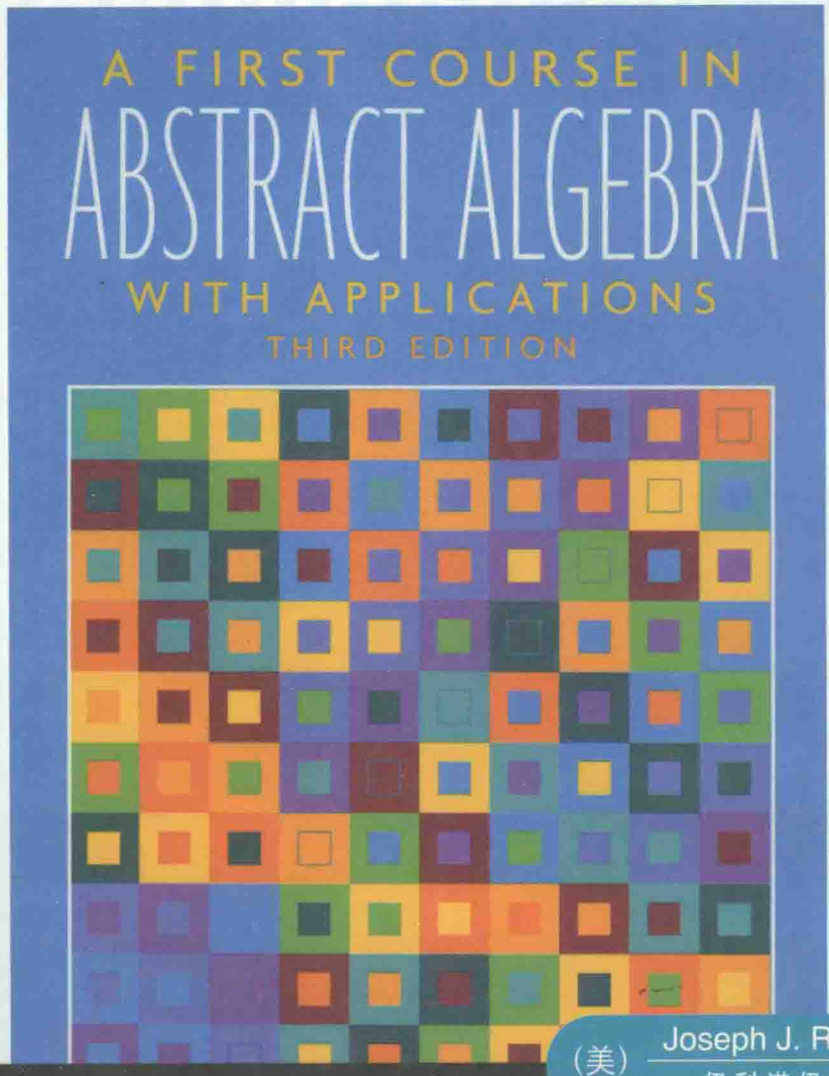
HZ BOOKS
PEARSON Prentice Hall

经 典 原 版 书 库

抽象代数基础教程

（英文版 · 第3版）



（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3版）

A First Course in Abstract Algebra
with Applications

(Third Edition)

(美) Joseph J. Rotman
伊利诺伊大学 著

机械工业出版社
China Machine Press

本书版权登记号：图字：01-2006-1937

图书在版编目（CIP）数据

抽象代数基础教程（英文版 · 第3版）/（美）罗特曼（Rotman, J. J.）著. – 北京：机械工业出版社，2006.4

（经典原版书库）

书名原文：A First Course in Abstract Algebra: with Applications, Third Edition

ISBN 7-111-18842-X

Ⅰ. 抽… Ⅱ. 罗… Ⅲ. 抽象代数 – 英文 Ⅳ. O153

中国版本图书馆CIP数据核字（2006）第030237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

北京瑞德印刷有限公司印刷 · 新华书店北京发行所发行

2006年4月第1版第1次印刷

787mm × 1020mm 1/16 · 40印张

定价：75.00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

Preface to the Third Edition

A First Course in Abstract Algebra introduces number theory, groups, and commutative rings. Group theory was invented by Galois in the early 1800s, when he used groups to completely determine those polynomials whose roots can be found with generalizations of the quadratic formula. Nowadays, the language of group theory is the precise way to discuss various types of symmetry, both in geometry and elsewhere. Thus, besides introducing Galois's ideas, we classify certain planar designs called *friezes*, and we also apply group theory to solve some intricate counting problems (how many 6-beaded bracelets are there if each bead is either red, white, or blue?). Commutative rings provide the proper context in which to study number theory as well as many aspects of the theory of polynomials. Ideas such as greatest common divisor of integers and modular arithmetic extend effortlessly to polynomial rings in one variable. There are applications to public access codes, calendars, Latin squares, magic squares, and design of experiments. We then consider vector spaces with scalars in arbitrary fields (not just the reals), and this study allows us to solve the classical Greek problems involving ruler-compass constructions: trisecting an angle; doubling a cube; squaring a circle; constructing regular n-gons. Linear algebra over finite fields is applied to codes, showing how one can decode messages sent over a noisy channel (for example, photographs sent to Earth from other planets). The classical formulas finding the roots of cubic and quartic polynomials are proved, after which both groups and commutative rings are combined in proving Galois's theorem (polynomials whose roots are obtainable by such formulas have solvable Galois groups) and its corollary, Abel's theorem (there are polynomials of degree 5 whose roots cannot be found by a generalization of these formulas). This is only an introduction to Galois theory; readers wishing to learn more of this beautiful subject will have to see a more advanced text. Algebra is fascinating, and I hope that my enthusiasm for it is transmitted to my readers.

To accomodate readers having different backgrounds, this book contains more material than can be covered in a one- or two-semester course. The first four chapters contain all the results usually covered in a first year. But many sections need not be

covered in lectures, either because they are well known (induction, binomial theorem, complex numbers, linear algebra), they are not of primary importance, or they will be covered more thoroughly in more advanced courses. However, instructors may assign projects for interested students from these optional sections as well as from later chapters. Those readers whose appetites have been whetted by results in the first chapters may browse in the end of the book, which investigates groups and rings further. The chapter Groups II proves that finite abelian groups are direct products of cyclic groups, gives the existence (and significance) of large p-subgroups of finite groups, and classifies symmetry groups of friezes. The last chapter, an introduction to polynomials in several variables, includes Hilbert's basis theorem, varieties, Hilbert's *Nullstellensatz* for $\mathbb{C}[x_1, \ldots, x_n]$, and algorithmic methods associated with Gröbner bases. Thus, the last two chapters display some directions in which the earlier ideas have developed, and so they can serve as a reference for some algebra beyond the present courses.

Let me mention some new features of this edition.

- I have rewritten the text, making the exposition more smooth.
- In order that the reader know what is essential in the first five chapters, I have inserted a small arrow next to the most important sections, subsections, definitions, theorems, and examples.
- Chapters 2 and 3, which introduce groups and commutative rings, are essentially independent of one another. Thus, with very minor changes, it is possible to study groups first or to study commutative rings first.
- More linear algebra, over arbitrary fields, has been included. This allows me to include a new section on codes, which goes far enough to decode Reed-Solomon codes.
- There is a new section classifying frieze groups in the plane.
- Exercises.
  - (i) The previous edition had 414 exercises; this edition has 574 exercises.
  - (ii) Each exercise set begins with a multipart true-false question which reviews important items in its section.
  - (iii) Every exercise explicitly cited in the text is marked by *; moreover, every citation gives the page number on which the cited exercise appears.
  - (iv) Certain exercises, those marked by H, have hints in a section at the end of the book; thus, readers may consider problems on their own before reading the hints.

- One numbering system enumerates all lemmas, theorems, propositions, corollaries, and examples, so that finding back references is easy.

- There are several pages of Special Notation, giving page numbers where notation is introduced.

Today, abstract algebra is viewed as a challenging course; many bright students seem to have inordinate difficulty learning it. Certainly, students must learn to think in a new way. Axiomatic reasoning may be new to some; others may be more visually oriented. Some students have never written proofs; others may have once done so, but their skills have atrophied from lack of use. But none of these obstacles adequately explains the observed difficulties. After all, the same obstacles exist in beginning real analysis courses, but most students in these courses do learn the material, perhaps after some early struggling. However, the difficulty of standard algebra courses persists, whether groups are taught first, whether rings are taught first, or whether texts are changed. I believe that a major factor contributing to the difficulty in learning abstract algebra is that both groups and rings are introduced in the first course; as soon as a student begins to be comfortable with one topic, it is dropped to study the other. Furthermore, leaving group theory or commutative ring theory before significant applications are made gives students the false impression that the theory is either of no real value or, more likely, that it cannot be appreciated until some future indefinite time. Imagine a beginning analysis course in which both real and complex analysis are introduced in the first semester; would there be ample time to prove the intermediate value theorem and Liouville's theorem? If algebra is taught as a one-year (two-semester) course, there is no longer any reason to crowd both topics into the first course, and a truer, more attractive, picture of algebra is presented. This option is more practical today than it was in the past, for the many applications of abstract algebra have increased the numbers of interested students, many of whom work in other disciplines. Therefore, I have rewritten the text for two audiences. On the one hand, this new edition can serve as a text for those who prefer the currently popular arrangement of introducing both groups and rings in the first semester. There is ample material in the book so that it can serve as a text for a sequel course as well. On the other hand, the book can also serve as a text for a one-year course. There are many possible organizations; I suggest covering number theory and commutative rings in the first semester, and linear algebra and group theory in the second. Detailed syllabi for such courses are presented in the next section.

Giving the etymology of mathematical terms is rarely done in mathematics texts. 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 trigonometric terms *tangent* and *secant* are good names for those knowing some Latin, but they are obscure otherwise (see a discussion of their etymology on page 32). 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 why should some theorems be called flowers? A plausible explanation is that it was common, in ancient Rome, to give flowers as a gratuity, 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. I believe that etymology of terms is worthwhile (and interesting!), for it often aids understanding by removing unnecessary obscurity.

In addition to thanking again those who helped me with the first two editions, I give special thanks to George Bergman for his many suggestions as well as for his generosity in allowing me to use many interesting exercises. I also thank Chris Heil, for pointing out subtle errors I had not discovered, and Iwan Duursma for his help with the new section on coding. Finally, I thank William Chin, Joel S. Foisy, Robert Friedman, Blair F. Goodlin, Zahid Hasan, Ilya Kapovich, Dieter Koller, Fatma Irem Koprulu, Mario Livio, Thomas G. Lucas, Leon McCulloh, Arnold W. Miller, Charles H. Morgan, Jr., Chuang Peng, Eric Schmutz, Brent B. Solie, Paul Weichsel, and John Wetzel.

George Lobell was with Prentice Hall until this edition was essentially complete. He consistently gave me sage advice about its content and style, and my book is significantly better now than it would have been without him. I am happy to thank him for his guidance.

Joseph Rotman
rotman@math.uiuc.edu

Suggested Syllabi

Here are some one-semester courses using this text, where a semester consists of about 45 one-hour lectures (hour lectures are usually 50 minutes in length; Paul Halmos noted that a ***microcentury***, one millionth of a century, is about 52.6 minutes). We give five syllabi. The first, Table 1, is a "standard" syllabus designed for the currently popular course organization: a one-semester course which introduces both groups and rings. This syllabus has three topics: Chapter 1: number theory; Chapter 2: groups; Chapter 3: commutative rings. It is possible to invert the order of topics and treat commutative rings before groups, for I have rewritten Chapters 2 and 3 so that they are now essentially independent of one another. As an aside, I disagree with today's received wisdom that expounding groups first is more efficient than doing rings first; in spite of Chapter 3's mentioning almost no group theory, its present version is about the same length as its versions in previous editions.

Either of the second two syllabi, Tables 2 and 3, may be used for a sequel course (there is ample material in the text which can be used to create other sequel courses as well).

My own ideas about teaching abstract algebra have changed. I now think that the best presentation is a year-long two-semester course in which only one of groups or rings is taught in the first semester. Moreover, I recommend such a course whose first semester covers number theory and commutative rings, and whose second semester covers linear algebra and group theory. Tables 4 and 5 are syllabi for such a course. (Of course, I recognize merit in arguments advocated by those who prefer to discuss groups first. A one-year course using this text and organized about this choice should be easy to design.) I think that doing commutative rings first is more natural. As one passes from $\mathbb{Z}$ to $k[x]$, one can watch arithmetic results and proofs generalize to polynomials. If the second semester begins with linear algebra, then the discussion of groups takes on more significance, for matrix groups, with their geometric context, are another source of concrete examples of groups in addition to groups of permutations.

Section	Topics	Hours
1.3	Division algorithm, euclid lemma, euclidean algorithm	3
1.4	Fundamental theorem of arithmetic	1
1.5	Congruences, Fermat, Chinese remainder theorem	3
2.1	Functions	1
2.2	Permutations	4
2.3	Groups and examples	2
2.4	Subgroups and Lagrange's theorem	2
2.5	Homomorphisms	2
2.6	Quotient groups and isomorphism theorems	4
2.7	Group actions	4
2.8	Burnside counting (skim)	1
3.1	Commutative rings and subrings	1
3.2	Fields	1
3.3	Polynomial rings $R[x]$	1
3.4	Homomorphisms	2
3.5	From numbers to polynomials	3
3.6	Unique factorization for polynomials	1
3.7	Irreducibility (skim)	2
3.8	Quotient rings and finite fields	3

Table 1: Standard One-Semester Syllabus: 41 Hours

Section	Topics	Hours
4.1	Vector spaces and dimension	5
4.1	Gaussian elimination	3
4.2	Euclidean constructions	3
4.3	Linear transformations	4
4.4	Determinants and eigenvalues	2
4.5	Coding	6
5.1	Classical formulas	2
5.2	Solvability by radicals	4
5.2	Translation into group theory	4
5.3	Epilog	1
6.1	Finite abelian groups	3
6.2	Sylow theorems	3

Table 2: Second Semester, Syllabus A: 40 Hours

Section	Topics	Hours
4.1	Vector spaces and dimension	5
4.1	Gaussian elimination	3
4.2	Euclidean constructions	3
4.3	Linear transformations	4
4.4	Determinants and eigenvalues	2
6.1	Finite abelian groups	3
6.2	Sylow theorems	3
6.3	Symmetry groups of friezes (skim)	3
7.1	Prime ideals and maximal ideals	1
7.2	Unique factorization	3
7.3	Noetherian rings	2
7.4	Varieties	6

Table 3: Second Semester: Syllabus B: 38 Hours

Section	Topics	Hours
1.3	Division algorithm, euclid lemma, euclidean algorithm	4
1.4	Fundamental theorem of arithmetic	1
1.5	Congruences, Fermat, Chinese remainder theorem	4
2.1	Functions	1
3.1	Commutative rings and subrings	2
3.2	Fields	1
3.3	Polynomial rings $R[x]$	2
5.1	Classical formulas	2
3.4	Homomorphisms	2
3.5	From numbers to polynomials	4
3.6	Unique factorization for polynomials	2
3.7	Irreducibility	3
3.8	Quotient rings and finite fields	4
3.9	Latin squares, magic squares, projective planes (skim)	1
7.1	Prime ideals and maximal ideals	1
7.2	Unique factorization (skim)	1
7.3	Noetherian rings (skim)	1
7.4	Varieties (skim)	3

Table 4: One-Year Version, Semester I: 39 Hours

Section	Topics	Hours
4.1	Vector spaces	5
4.1	Gaussian elimination	3
4.2	Euclidean constructions	3
4.3	Linear transformations	4
4.4	Eigenvalues	2
4.5	Coding (skim)	3
2.2	Permutations	4
2.3	Groups and examples	2
2.4	Subgroups and Lagrange's theorem	2
2.5	Homomorphisms	2
2.6	Quotient groups and isomorphism theorems	4
2.7	Group actions	4
2.8	Burnside counting (skim)	1
6.1	Finite abelian groups (skim)	1
6.2	Sylow theorems (skim)	1
6.3	Ornamental symmetry (skim)	1

Table 5: One-Year Version, Semester II: 42 Hours

To the Reader

The essential sections, subsections, theorems, definitions, and examples in the first five chapters have a small arrow in the margin next to them (some things, though interesting, are not as important as others).

Exercises in a text have two main functions: to reinforce the reader's grasp of the material, and to provide puzzles whose solutions give a certain pleasure. Therefore, the serious reader should attempt *all* the exercises (many are not difficult).

There are two special notations associated to exercises. An asterisk, as in *2.44, means that this exercise is cited elsewhere in the text. For example, the citation reads "Exercise 2.44 on page 146." The letter H, as in H 2.47, means that there is a hint to Exercise 2.47 in the Hints section at the back of the book. Neither of these notations indicates the relative difficulty of an exercise.

Most exercise sets begin with a multipart question labeled "True or false with reasons." If one of the parts is the statement, "The fourth roots of unity are i and $-i$," then the correct answer is, "False; 1 is also a fourth root of unity." The declaration "False" must be supported by a concrete example. If another statement is "$2 + 4 + \cdots + 100 = 50 \times 51$," then the correct response is "True; using Proposition 1.6, we have

$$2 + 4 + \cdots + 100 = 2[1 + 2 + \cdots + 50] = 2\left[\tfrac{1}{2}(50 \times 51)\right] = 50 \times 51."$$

The declaration 'True" must be supported either by a "one-line proof" using results proved in the text or by a short argument from first principles.

Special Notation

Set Theory and Number Theory

Group Theory

Commutative Rings and Linear Algebra

Contents