海外优秀数学类教材系列丛书

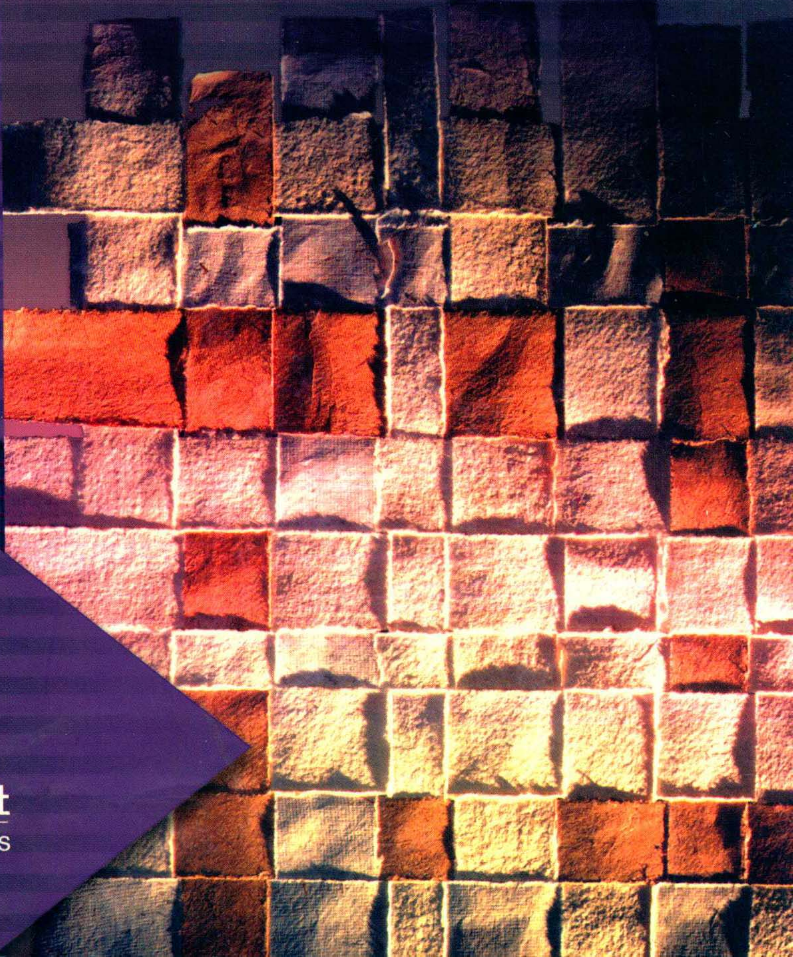
PEARSON
Prentice
Hall

影印版

Advanced Modern Algebra

抽象代数

□ Joseph J. Rotman



高等教育出版社
Higher Education Press

海外优秀数学类教材系列丛书

影印版

Advanced Modern Algebra

抽象代数

□ Joseph J. Rotman

University of Illinois at Urbana-Champaign

高等教育出版社
Higher Education Press

图书在版编目（CIP）数据

抽象代数＝Advanced Modern Algebra/（美）罗特曼（Rotman，J.J.）.—影印本.—北京：高等教育出版社，2004. 12
（海外优秀数学类教材系列丛书）
ISBN 7-04-015556-7

Ⅰ.抽… Ⅱ.罗… Ⅲ.抽象代数—高等学校—教材—英文 Ⅳ.0153

中国版本图书馆 CIP 数据核字（2004）第 112938 号

出版发行	高等教育出版社	**购书热线**	010－64054588
社　　址	北京市西城区德外大街 4 号	**免费咨询**	800－810－0598
邮政编码	100011	**网　　址**	http：//www.hep.edu.cn
总　　机	010－58581000		http：//www.hep.com.cn
经　　销	新华书店北京发行所		
印　　刷	北京外文印刷厂		
开　　本	787＊960　1/16	**版　　次**	2004 年 12 月第 1 版
印　　张	66.25	**印　　次**	2004 年 12 月第 1 次印刷
字　　数	600 000	**定　　价**	68.00 元

本书如有缺页、倒页、脱页等质量问题，请到所购图书销售部门联系调换。
版权所有　侵权必究
物料号：15556－00

出版者的话

在我国已经加入WTO、经济全球化的今天，为适应当前我国高校各类创新人才培养的需要，大力推进教育部倡导的双语教学，配合教育部实施的“高等学校教学质量与教学改革工程”和“精品课程”建设的需要，高等教育出版社有计划、大规模地开展了海外优秀数学类系列教材的引进工作。

高等教育出版社和 Pearson Education，John Wiley & Sons，McGraw-Hill，Thomson Learning 等国外出版公司进行了广泛接触，经国外出版公司的推荐并在国内专家的协助下，提交引进版权总数100余种。收到样书后，我们聘请了国内高校一线教师、专家、学者参与这些原版教材的评介工作，并参考国内相关专业的课程设置和教学实际情况，从中遴选出了这套优秀教材组织出版。

这批教材普遍具有以下特点：(1) 基本上是近3年出版的，在国际上被广泛使用，在同类教材中具有相当的权威性；(2) 高版次，历经多年教学实践检验，内容翔实准确、反映时代要求；(3) 各种教学资源配套整齐，为师生提供了极大的便利；(4) 插图精美、丰富，图文并茂，与正文相辅相成；(5) 语言简练、流畅、可读性强，比较适合非英语国家的学生阅读。

本系列丛书中，有 Finney、Weir 等编的《托马斯微积分》（第10版，Pearson)，其特色可用“呈传统特色、富革新精神”概括，本书自20世纪50年代第1版以来，平均每四五年就有一个新版面世，长达50余年始终盛行于西方教坛，作者既有相当高的学术水平，又热爱教学，长期工作在教学第一线，其中，年近90的 G.B.Thomas 教授长年在 MIT 工作，具有丰富的教学经验；Finney 教授也在 MIT 工作达10年；Weir 是美国数学建模竞赛委员会主任。Stewart 编的立体化教材《微积分》（第5版，Thomson Learning）配备了丰富的教学资源，是国际上最畅销的微积分原版教材，2003年全球销量约40余万册，在美国，占据了约50%～60%的微积分教材市场，其用户包括耶鲁等名牌院校及众多一般院校。本系列丛书还包括 Anton 编的经典教材《线性代数及其应用》（第8版，Wiley）；Jay L. Devore 编的优秀教材《概率论与数理统计》（第5版，Thomson Learning）等。在努力降低引进教材售价方面，高等教育出版社做了大量和细致的工作，这套引进的教材体现了一定的权威性、

系统性、先进性和经济性等特点。

通过影印、翻译、编译这批优秀教材，我们一方面要不断地分析、学习、消化吸收国外优秀教材的长处，吸取国外出版公司的制作经验，提升我们自编教材的立体化配套标准，使我国高校教材建设水平上一个新的台阶；与此同时，我们还将尝试组织海外作者和国内作者合编外文版基础课数学教材，并约请国内专家改编部分国外优秀教材，以适应我国实际教学环境。

这套教材出版后，我们将结合各高校的双语教学计划，开展大规模的宣传、培训工作，及时地将本套丛书推荐给高校使用。在使用过程中，我们衷心希望广大高校教师和同学提出宝贵的意见和建议。

高等教育出版社高等理科分社联系电话：010-58581384，E-mail：xuke@hep.com.cn。

高等教育出版社

2004 年 4 月 20 日

To my wife

Marganit

and our two wonderful kids,

Danny and Ella,

whom I love very much

Preface

Algebra is used by virtually all mathematicians, be they analysts, combinatorists, computer scientists, geometers, logicians, number theorists, or topologists. Nowadays, everyone agrees that some knowledge of linear algebra, groups, and commutative rings is necessary, and these topics are introduced in undergraduate courses. We continue their study.

This book can be used as a text for the first year of graduate algebra, but it is much more than that. It can also serve more advanced graduate students wishing to learn topics on their own; while not reaching the frontiers, the book does provide a sense of the successes and methods arising in an area. Finally, this is a reference containing many of the standard theorems and definitions that users of algebra need to know. Thus, the book is not only an appetizer, but a hearty meal as well.

Let me now address readers and instructors who use the book as a text for a beginning graduate course. If I could assume that everyone had already read my book, *A First Course in Abstract Algebra*, then the prerequisites for this book would be plain. But this is not a realistic assumption; different undergraduate courses introducing abstract algebra abound, as do texts for these courses. For many, linear algebra concentrates on matrices and vector spaces over the real numbers, with an emphasis on computing solutions of linear systems of equations; other courses may treat vector spaces over arbitrary fields, as well as Jordan and rational canonical forms. Some courses discuss the Sylow theorems; some do not; some courses classify finite fields; some do not.

To accommodate readers having different backgrounds, the first three chapters contain many familiar results, with many proofs merely sketched. The first chapter contains the fundamental theorem of arithmetic, congruences, De Moivre's theorem, roots of unity, cyclotomic polynomials, and some standard notions of set theory, such as equivalence relations and verification of the group axioms for symmetric groups. The next two chapters contain both familiar and unfamiliar material. "New" results, that is, results rarely taught in a first course, have complete proofs, while proofs of "old" results are usually sketched. In more detail, Chapter 2 is an introduction to group theory, reviewing permutations, Lagrange's theorem, quotient groups, the isomorphism theorems, and groups acting on sets. Chapter 3 is an introduction to commutative rings, reviewing domains, fraction fields, polynomial rings in one variable, quotient rings, isomorphism theorems, irreducible polynomials, finite fields, and some linear algebra over arbitrary fields. Readers may use "older" portions of these chapters to refresh their memory of this material (and also to see my notational choices); on the other hand, these chapters can also serve as a guide for learning what may have been omitted from an earlier course (complete proofs can be found in *A First Course in Abstract Algebra*). This format gives more freedom to an instructor, for there is a variety of choices for the starting point of a course of lectures, depending on what best fits the backgrounds of the students in a class. I expect that most instructors would begin a course somewhere in the middle of Chapter 2 and, afterwards, would continue from some point in the middle of Chapter 3. Finally, this format is convenient for the author, because it allows me to refer back to these earlier results in the midst of a discussion or a proof. Proofs in subsequent chapters are complete and are not sketched.

I have tried to write clear and complete proofs, omitting only those parts that are truly routine; thus, it is not necessary for an instructor to expound every detail in lectures, for students should be able to read the text.

When I was a student, Birkhoff and Mac Lane's *A Survey of Modern Algebra* was the text for my first algebra course, and van der Waerden's *Modern Algebra* was the text for my second course. Both are excellent books (I have called this book *Advanced Modern Algebra* in homage to them), but times have changed since their first appearance: Birkhoff and Mac Lane's book first appeared in 1941, and van der Waerden's book first appeared in 1930. There are today major directions that either did not exist over 60 years ago, or that were not then recognized to be so important. These new directions involve algebraic geometry, computers, homology, and representations (*A Survey of Modern Algebra* has been rewritten as Mac Lane–Birkhoff, *Algebra*, Macmillan, New York, 1967, and this version introduces categorical methods; category theory emerged from algebraic topology, but was then used by Grothendieck to revolutionize algebraic geometry).

Here is a more detailed account of the later chapters of this book.

Chapter 4 discusses fields, beginning with an introduction to Galois theory, the interrelationship between rings and groups. We prove the insolvability of the general polynomial of degree 5, the fundamental theorem of Galois theory, and applications, such as a proof of the fundamental theorem of algebra, and Galois's theorem that a polynomial over a field of characteristic 0 is solvable by radicals if and only if its Galois group is a solvable group.

Chapter 5 covers finite abelian groups (basis theorem and fundamental theorem), the Sylow theorems, Jordan–Hölder theorem, solvable groups, simplicity of the linear groups $\mathrm{PSL}(2, k)$, free groups, presentations, and the Neilsen–Schreier theorem (subgroups of free groups are free).

Chapter 6 introduces prime and maximal ideals in commutative rings; Gauss's theorem that $R[x]$ is a UFD when R is a UFD; Hilbert's basis theorem, applications of Zorn's lemma to commutative algebra (a proof of the equivalence of Zorn's lemma and the axiom of choice is in the appendix), inseparability, transcendence bases, Lüroth's theorem, affine varieties, including a proof of the Nullstellensatz for uncountable algebraically closed fields (the full Nullstellensatz, for varieties over arbitrary algebraically closed fields, is proved in Chapter 11); primary decomposition; Gröbner bases. Chapters 5 and 6 overlap two chapters of *A First Course in Abstract Algebra*, but these chapters are not covered in most undergraduate courses.

Chapter 7 introduces modules over commutative rings (essentially proving that all R-modules and R-maps form an abelian category); categories and functors, including products and coproducts, pullbacks and pushouts, Grothendieck groups, inverse and direct limits, natural transformations; adjoint functors; free modules, projectives, and injectives.

Chapter 8 introduces noncommutative rings, proving Wedderburn's theorem that finite division rings are commutative, as well as the Wedderburn–Artin theorem classifying semisimple rings. Modules over noncommutative rings are discussed, along with tensor products, flat modules, and bilinear forms. We also introduce character theory, using it to prove Burnside's theorem that finite groups of order $p^m q^n$ are solvable. We then introduce multiply transitive groups and Frobenius groups, and we prove that Frobenius kernels are normal subgroups of Frobenius groups.

Chapter 9 considers finitely generated modules over PIDs (generalizing earlier theorems about finite abelian groups), and then goes on to apply these results to rational, Jordan, and Smith canonical forms for matrices over a field (the Smith normal form enables one to compute elementary divisors of a matrix). We also classify projective, injective, and flat modules over PIDs. A discussion of graded k-algebras, for k a commutative ring, leads to tensor algebras, central simple algebras and the Brauer group, exterior algebra (including Grassman algebras and the binomial theorem), determinants, differential forms, and an introduction to Lie algebra.

Chapter 10 introduces homological methods, beginning with semidirect products and the extension problem for groups. We then present Schreier's solution of the extension problem using factor sets, culminating in the Schur–Zassenhaus lemma. This is followed by axioms characterizing Tor and Ext (existence of these functors is proved with derived functors), some cohomology of groups, a bit of crossed product algebras, and an introduction to spectral sequences.

Chapter 11 returns to commutative rings, discussing localization, integral extensions, the general Nullstellensatz (using Jacobson rings), Dedekind rings, homological dimensions, the theorem of Serre characterizing regular local rings as those noetherian local rings of finite global dimension, the theorem of Auslander and Buchsbaum that regular local rings are UFDs.

Each generation should survey algebra to make it serve the present time.

It is a pleasure to thank the following mathematicians whose suggestions have greatly improved my original manuscript: Michael Barr, Daniel Bump, Heng Huat Chan, Ulrich Daepp, Boris A. Datskovsky, Keith Dennis, Vlastimil Dlab, Sankar Dutta, David Eisenbud, E. Graham Evans, Jr., Daniel Flath, Jeremy J. Gray, Daniel Grayson, Philllip Griffith, William Haboush, Robin Hartshorne, Craig Huneke, Gerald J. Janusz, Carl Jockusch, David Leep, Marcin Mazur, Leon McCulloh, Emma Previato, Eric Sommers, Stephen V. Ullom, Paul Vojta, William C. Waterhouse, and Richard Weiss.

Joseph Rotman

Etymology

The heading *etymology* in the index points the reader to derivations of certain mathematical terms. For the origins of other mathematical terms, we refer the reader to my books *Journey into Mathematics* and *A First Course in Abstract Algebra*, which contain etymologies of the following terms.

Journey into Mathematics:

π, algebra, algorithm, arithmetic, completing the square, cosine, geometry, irrational number, isoperimetric, mathematics, perimeter, polar decomposition, root, scalar, secant, sine, tangent, trigonometry.

A First Course in Abstract Algebra:

affine, binomial, coefficient, coordinates, corollary, degree, factor, factorial, group, induction, Latin square, lemma, matrix, modulo, orthogonal, polynomial, quasicyclic, September, stochastic, theorem, translation.

Special Notation

$\mathbb{A}$	algebraic numbers
A_n	alternating group on n letters
$\mathbf{Ab}$	category of abelian groups
$\mathrm{Aff}(1, k)$	one-dimensional affine group over a field k
$\mathrm{Aut}(G)$	automorphism group of a group G
$\mathrm{Br}(k)$, $\mathrm{Br}(E/k)$	Brauer group, relative Brauer group
$\mathbb{C}$	complex numbers
$\mathbf{C}_\bullet$, $(\mathbf{C}_\bullet, d_\bullet)$	complex with differentiations $d_n : C_n \to C_{n-1}$
$C_G(x)$	centralizer of an element x in a group G
$D(R)$	global dimension of a commutative ring R
D_{2n}	dihedral group of order $2n$
$\deg(f)$	degree of a polynomial $f(x)$
$\mathrm{Deg}(f)$	multidegree of a polynomial $f(x_1, \ldots, x_n)$
$\det(A)$	determinant of a matrix A
$\dim_k(V)$	dimension of a vector space V over a field k
$\dim(R)$	Krull dimension
$\mathrm{End}_k(M)$	endomorphism ring of a k-module M
$\mathbb{F}_q$	finite field having q elements
$\mathrm{Frac}(R)$	fraction field of a domain R
$\mathrm{Gal}(E/k)$	Galois group of a field extension E/k
$\mathrm{GL}(V)$	automorphisms of a vector space V
$\mathrm{GL}(n, k)$	$n \times n$ nonsingular matrices, entries in a field k
$\mathbb{H}$	division ring of real quaternions
H_n, H^n	homology, cohomology
$\mathrm{ht}(\mathfrak{p})$	height of prime ideal
$\mathbb{I}_m$	integers modulo m
I or I_n	identity matrix
$\sqrt{I}$	radical of an ideal I
$\mathrm{Id}(A)$	ideal of a subset $A \subseteq k^n$
$\mathrm{im}\, f$	image of a function f
$\mathrm{irr}(\alpha, k)$	minimal polynomial of α over a field k
$\overline{k}$	algebraic closure of a field k

$K_0(R)$, $K_0(\mathcal{C})$	Grothendieck groups, direct sums
$K'(\mathcal{C})$	Grothendieck group, short exact sequences
$\ker f$	kernel of a homomorphism f
$lD(R)$	left global dimension of a ring R
$\mathrm{Mat}_n(k)$	ring of all $n \times n$ matrices with entries in k
$_R\mathbf{Mod}$	category of left R-modules
$\mathbf{Mod}_R$	category of right R-modules
$\mathbb{N}$	natural numbers $=$ {integers $n : n \geq 0$}
$N_G(H)$	normalizer of a subgroup H in a group G
$\mathcal{O}_E$	ring of integers in an algebraic number field E
$\mathcal{O}(x)$	orbit of an element x
$\mathrm{PSL}(n, k)$	projective unimodular group $= \mathrm{SL}(n, k)/\text{center}$
$\mathbb{Q}$	rational numbers
$\mathbf{Q}$	quaternion group of order 8
$\mathbf{Q}_n$	generalized quaternion group of order 2^n
$\mathbb{R}$	real numbers
S_n	symmetric group on n letters
S_X	symmetric group on a set X
$\mathrm{sgn}(\alpha)$	signum of a permutation α
$\mathrm{SL}(n, k)$	$n \times n$ matrices of determinant 1, entries in a field k
$\mathrm{U}(R)$	group of units in a ring R
$\mathrm{UT}(n, k)$	unitriangular $n \times n$ matrices over a field k
T	$\mathbb{I}_3 \rtimes \mathbb{I}_4$, a nonabelian group of order 12
tG	torsion subgroup of an abelian group G
$\mathrm{tr}(A)$	trace of a matrix A
$\mathbf{V}$	four-group
$\mathrm{Var}(I)$	variety of an ideal $I \subseteq k[x_1, \ldots, x_n]$
$\mathbb{Z}$	integers
$\mathbb{Z}_p$	p-adic integers
$Z(G)$	center of a group G
$Z(R)$	center of a ring R
$[G : H]$	index of a subgroup $H \leq G$
$[E : k]$	degree of a field extension E/k
$S \sqcup T$	coproduct of objects in a category
$S \sqcap T$	product of objects in a category
$S \oplus T$	external, internal direct sum
$K \times Q$	direct product
$K \rtimes Q$	semidirect product
$\sum A_i$	direct sum
$\prod A_i$	direct product
$\varprojlim A_i$	inverse limit
$\varinjlim A_i$	direct limit

G'	commutator subgroup
G_x	stabilizer of an element x
$G[m]$	$\{g \in G : mg = 0\}$, where G is an additive abelian group
mG	$\{mg : g \in G\}$, where G is an additive abelian group
G_p	p-primary component of an abelian group G
$k[x]$	polynomials
$k(x)$	rational functions
$k[[x]]$	formal power series
$k\langle X\rangle$	polynomials in noncommuting variables
R^{op}	opposite ring
Ra or (a)	principal ideal generated by a
$R^{\times}$	nonzero elements in a ring R
$H \leq G$	H is a subgroup of a group G
$H < G$	H is a proper subgroup of a group G
$H \lhd G$	H is a normal subgroup of a group G
$A \subseteq B$	A is a submodule (subring) of a module (ring)B
$A \subsetneq B$	A is a proper submodule (subring) of a module (ring)B
1_X	identity function on a set X
1_X	identity morphism on an object X
$f : a \mapsto b$	$f(a) = b$
$\lvert X\rvert$	number of elements in a set X
${}_Y[T]_X$	matrix of a linear transformation T relative to bases X and Y
$\phi(n)$	Euler ϕ-function
χ_σ	character afforded by a representation σ
$a_1, \ldots, \widehat{a_i}, \ldots, a_n$	list $a_1, \ldots, a_n$ with a_i omitted
$\binom{n}{r}$	binomial coefficient
δ_{ij}	Kronecker delta $\delta_{ij} = \begin{cases} 1 & \text{if } i = j; \\ 0 & \text{if } i \neq j. \end{cases}$

Contents

1

Things Past

This chapter reviews some familiar material of number theory, complex roots of unity, and basic set theory, and so most proofs are merely sketched.

1.1 Some Number Theory

Let us begin by discussing mathematical induction. Recall that the set of ***natural numbers*** $\mathbb{N}$ is defined by

$$\mathbb{N} = \{\text{integers } n : n \geq 0\};$$

that is, $\mathbb{N}$ is the set of all nonnegative integers. Mathematical induction is a technique of proof based on the following property of $\mathbb{N}$:

Least Integer Axiom.[1] There is a smallest integer in every nonempty subset C of $\mathbb{N}$.

Assuming the axiom, let us see that if m is any fixed integer, possibly negative, then there is a smallest integer in every nonempty collection C of integers greater than or equal to m. If $m \geq 0$, this is the least integer axiom. If $m < 0$, then $C \subseteq \{m, m+1, \ldots, -1\} \cup \mathbb{N}$ and

$$C = \big(C \cap \{m, m+1, \ldots, -1\}\big) \cup \big(C \cap \mathbb{N}\big).$$

If the finite set $C \cap \{m, m+1, \ldots, -1\} \neq \varnothing$, then it contains a smallest integer that is, obviously, the smallest integer in C; if $C \cap \{m, m+1, \ldots, -1\} = \varnothing$, then C is contained in $\mathbb{N}$, and the least integer axiom provides a smallest integer in C.

Definition. A natural number p is ***prime*** if $p \geq 2$ and there is no factorization $p = ab$, where $a < p$ and $b < p$ are natural numbers.

[1] This property is usually called the *well-ordering principle*.