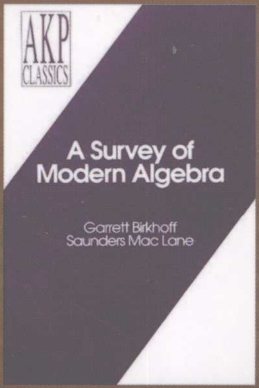
图灵原版数学·统计学系列 18

A Survey of Modern Algebra

近世代数概论

（英文版·第 5 版）

［美］ Garrett Birkhoff
Saunders Mac Lane 著



AKP CLASSICS

A Survey of Modern Algebra

Garrett Birkhoff
Saunders Mac Lane

人民邮电出版社
POSTS & TELECOM PRESS

图书在版编目（CIP）数据

近世代数概论：第 5 版：英文 /（美）伯克霍夫（Birkhoff, G.），（美）麦克莱恩（Mac Lane, S）著．—北京：人民邮电出版社，2007.8
（图灵原版数学·统计学系列）

ISBN 978-7-115-16231-1

Ⅰ．近…　Ⅱ．①伯…②麦…　Ⅲ．抽象代数－高等学校－教材－英文　Ⅳ．O153

中国版本图书馆 CIP 数据核字（2007）第 068017 号

内容提要

本书出自近世代数领域的两位科学巨匠之手，是一本经典的教材．全书共分为15章，内容包括：整数、多项式、实数、复数、矩阵代数、线性群、行列式和标准型、布尔代数和格、超限算术、环和理想、代数数域和伽罗华理论等．

本书曾帮助过几代人理解近世代数，至今仍是一本非常有价值的参考书和教材，适合数学专业及其他理工科专业高年级本科生和研究生使用．

图灵原版数学·统计学系列

近世代数概论（英文版·第 5 版）

◆ 著　　　［美］Garrett Birkhoff　Saunders Mac Lane
责任编辑　明永玲

◆ 人民邮电出版社出版发行　北京市崇文区夕照寺街 14 号
邮编　100061　电子函件　315@ptpress.com.cn
网址　http://www.ptpress.com.cn
北京铭成印刷有限公司印刷
新华书店总店北京发行所经销

◆ 开本：700 × 1000　1/16
印张：32
字数：612 千字　　2007 年 8 月第 1 版
印数：1– 3 000 册　　2007 年 8 月北京第 1 次印刷

著作权合同登记号　图字：01-2007-2132 号

ISBN 978-7-115-16231-1/TP

定价：69.00 元

读者服务热线：(010)88593802　印装质量热线：(010)67129223

Preface to the Fourth Edition

During the thirty-five years since the first edition of this book was written, courses in "modern algebra" have become a standard part of college curricula all over the world, and many books have been written for use in such courses. Nevertheless, it seems desirable to recall our basic philosophy, which remains that of the present book.

"We have tried throughout to express the conceptual background of the various definitions used. We have done this by illustrating each new term by as many familiar examples as possible. This seems especially important in an elementary text because it serves to emphasize the fact that the abstract concepts all arise from the analysis of concrete situations.

"To develop the student's power to think for himself in terms of the new concepts, we have included a wide variety of exercises on each topic. Some of these exercises are computational, some explore further examples of the new concepts, and others give additional theoretical developments. Exercises of the latter type serve the important function of familiarizing the student with the construction of a formal proof. The selection of exercises is sufficient to allow an instructor to adapt the text to students of quite varied degrees of maturity, of undergraduate or first year graduate level.

"Modern algebra also enables one to reinterpret the results of classical algebra, giving them far greater unity and generality. Therefore, instead of omitting these results, we have attempted to incorporate them systematically within the framework of the ideas of modern algebra.

"We have also tried not to lose sight of the fact that, for many students, the value of algebra lies in its applications to other fields: higher analysis, geometry, physics, and philosophy. This has influenced us in our emphasis on the real and complex fields, on groups of transformations as contrasted with abstract groups, on symmetric matrices and reduction to diagonal form, on the classification of quadratic forms under the orthogonal and Euclidean groups, and finally, in the inclusion of Boolean algebra, lattice theory, and transfinite numbers, all of which are important in mathematical logic and in the modern theory of real functions."

本书第5版是在1977年Macmillan出版的第4版基础上修订而成，保留了第4版序，未加新序.——编者注

In detail, our Chapters 1–3 give an introduction to the theory of linear and polynomial equations in commutative rings. The familiar domain of integers and the rational field are emphasized, together with the rings of integers modulò n and associated polynomial rings. Chapters 4 and 5 develop the basic algebraic properties of the real and complex fields which are of such paramount importance for geometry and physics.

Chapter 6 introduces noncommutative algebra through its simplest and most fundamental concept: that of a group. The group concept is applied systematically in Chapters 7–10, on vector spaces and matrices. Here care is taken to keep in the foreground the fundamental role played by algebra in Euclidean, affine, and projective geometry. Dual spaces and tensor products are also discussed, but generalizations to modules over rings are not considered.

Chapter 11 includes a completely revised introduction to Boolean algebra and lattice theory. This is followed in Chapter 12 by a brief discussion of transfinite numbers. Finally, the last three chapters provide an introduction to general commutative algebra and arithmetic: ideals and quotient-rings, extensions of fields, algebraic numbers and their factorization, and Galois theory.

Many of the chapters are independent of one another; for example, the chapter on group theory may be introduced just after Chapter 1, while the material on ideals and fields (§§13.1 and 14.1) may be studied immediately after the chapter on vector spaces.

This independence is intended to make the book useful not only for a full-year course, assuming only high-school algebra, but also for various shorter courses. For example, a semester or quarter course covering linear algebra may be based on Chapters 6–10, the real and complex fields being emphasized. A semester course on abstract algebra could deal with Chapters 1–3, 6–8, 11, 13, and 14. Still other arrangements are possible.

We hope that our book will continue to serve not only as a text but also as a convenient reference for those wishing to apply the basic concepts of modern algebra to other branches of mathematics, including statistics and computing, and also to physics, chemistry, and engineering.

It is a pleasure to acknowledge our indebtedness to Clifford Bell, A. A. Bennett, E. Artin, F. A. Ficken, J. S. Frame, Nathan Jacobson, Walter Leighton, Gaylord Merriman, D. D. Miller, Ivan Niven, and many other friends and colleagues who assisted with helpful suggestions and improvements, and to Mrs. Saunders Mac Lane, who helped with the secretarial work in the first three editions.

Cambridge, Mass.
Chicago, Illinois

GARRETT BIRKHOFF
SAUNDERS MAC LANE

Contents

1

The Integers

1.1. Commutative Rings; Integral Domains

Modern algebra has exposed for the first time the full variety and richness of possible mathematical systems. We shall construct and examine many such systems, but the most fundamental of them all is the oldest mathematical system—that consisting of all the positive integers (whole numbers). A related but somewhat larger system is the collection **Z** of *all* integers $0, \pm 1, \pm 2, \pm 3, \cdots$. We begin our discussion with this system because it more closely resembles the other systems which arise in modern algebra.

The integers have many interesting algebraic properties. In this chapter, we will assume some especially obvious such properties as *postulates*, and deduce from them many other properties as logical consequences.

We first assume eight postulates for addition and multiplication. These postulates hold not only for the integers, but for many other systems of numbers, such as that of all rational numbers (fractions), all real numbers (unlimited decimals), and all complex numbers. They are also satisfied by polynomials, and by continuous real functions on any given interval. When these eight postulates hold for a system R, we shall say that R is a *commutative ring.*

Definition. *Let R be a set of elements $a, b, c, \cdots$ for which the sum $a + b$ and the product ab of any two elements a and b (distinct or not) of R are defined. Then R is called a* commutative ring *if the following postulates (i)–(viii) hold:*

(i) *Closure. If a and b are in R, then the sum $a + b$ and the product ab are in R.*

(ii) *Uniqueness. If $a = a'$ and $b = b'$ in R, then*

$$a + b = a' + b' \qquad \textit{and} \qquad ab = a'b'.$$

(iii) *Commutative laws. For all a and b in R,*

$$a + b = b + a, \qquad ab = ba.$$

(iv) *Associative laws. For all a, b, and c in R,*

$$a + (b + c) = (a + b) + c, \qquad a(bc) = (ab)c.$$

(v) *Distributive law. For all a, b, and c in R,*

$$a(b + c) = ab + ac.$$

(vi) *Zero. R contains an element 0 such that*

$$a + 0 = a \qquad \textit{for all } a \textit{ in } R.$$

(vii) *Unity. R contains an element $1 \neq 0$ such that*

$$a1 = a \qquad \textit{for all } a \textit{ in } R.$$

(viii) *Additive inverse. For each a in R, the equation $a + x = 0$ has a solution x in R.*

It is a familiar fact that the set $\mathbf{Z}$ of all integers satisfies these postulates. For example, the commutative and associative laws are so familiar that they are ordinarily used without explicit mention: thus $a + b + c$ customarily denotes the equal numbers $a + (b + c)$ and $(a + b) + c$. The property of zero stated in (vi) is the characteristic property of the number zero; and similarly, the property of 1 stated in (vii) is the characteristic property of the number one. Since these laws are formally analogous, we may say that 0 and 1 are the "identity elements" for addition and multiplication, respectively. The assumption $1 \neq 0$ in (vii) is included to eliminate trivial cases (otherwise the set consisting of the integer 0 alone would be a commutative ring).

The system $\mathbf{Z}$ of all integers has another property which cannot be deduced from the preceding postulates. Namely, if $c \neq 0$ and $ca = cb$ in $\mathbf{Z}$, then necessarily $a = b$ (partial converse of (ii)). This property is not satisfied by real functions on a given interval, for example, though these form a commutative ring. The integers therefore constitute not only a commutative ring but also an *integral domain* in the sense of the following definition.

Definition. *An* integral domain *is a commutative ring in which the following additional postulate holds:*

(ix) *Cancellation law. If* $c \neq 0$ *and* $ca = cb$, *then* $a = b$.

The domain $\mathbf{Z}[\sqrt{2}]$. An integral domain of interest for number theory consists of all numbers of the form $a + b\sqrt{2}$, where a and b are ordinary integers (in $\mathbf{Z}$). In $\mathbf{Z}[\sqrt{2}]$, $a + b\sqrt{2} = c + d\sqrt{2}$ if and only if $a = c$, $b = d$. Addition and multiplication are defined by

$$(a + b\sqrt{2}) + (c + d\sqrt{2}) = (a + c) + (b + d)\sqrt{2}$$
$$(a + b\sqrt{2})(c + d\sqrt{2}) = (ac + 2bd) + (ad + bc)\sqrt{2}.$$

Uniqueness and commutativity are easily verified for these operations, while $0 + 0\sqrt{2}$ acts as a zero and $1 + 0\sqrt{2}$ as a unity. The additive inverse of $a + b\sqrt{2}$ is $(-a) + (-b)\sqrt{2}$. The verification of the associative and distributive laws is a little more tedious, while that of the cancellation law will be deferred to the end of §1.2.

1.2. Elementary Properties of Commutative Rings

In elementary algebra one often takes the preceding postulates and their elementary consequences for granted. This seldom leads to serious errors, provided algebraic manipulations are checked against specific examples. However, much more care must be taken when one wishes to reach reliable conclusions about whole families of algebraic systems (e.g., valid for *all* integral domains generally). One must be sure that all proofs use only postulates listed explicitly and standard rules of logic.

Among the most fundamental rules of logic are the three basic laws for equality:

Reflexive law: $a = a$.
Symmetric law: If $a = b$; then $b = a$.
Transitive law: If $a = b$ and $b = c$, then $a = c$, valid for all a, b, and c.

We now illustrate the idea of a formal proof for several rules valid in any commutative ring R.

Rule 1. $(a + b)c = ac + bc$, for all a, b, c in R.

This rule may be called the *right distributive law*, in contrast to postulate (v), which is the left distributive law.

Proof. For all a, b, and c in R:

1. $(a + b)c = c(a + b)$ (commutative law of mult.).
2. $c(a + b) = ca + cb$ (distributive law).
3. $(a + b)c = ca + cb$ (1, 2, transitive law).
4. $ca = ac,\ cb = bc$ (commutative law of mult.).
5. $ca + cb = ac + bc$ (4, uniqueness of addn.).
6. $(a + b)c = ac + bc$ (3, 5, transitive law).

Rule 2. For all a in R, $0 + a = a$ and $1 \cdot a = a$.

Proof. For all a in R:

1. $0 + a = a + 0$ (commutative law of addn.).
2. $a + 0 = a$ (zero).
3. $0 + a = a$ (1, 2, transitive law).

The proof for $1 \cdot a = a$ is similar.

Rule 3. If z in R has the property that $a + z = a$ for all a in R, then $z = 0$.

This rule states that R contains only one element 0 which can act as the identity element for addition.

Proof. Since $a + z = a$ holds for all a, it holds if a is 0.

1. $0 + z = 0$
2. $0 = 0 + z$ (1, symmetric law).
3. $0 + z = z$ (Rule 2 when a is z).
4. $0 = z$ (2, 3, transitive law).

In subsequent proofs such as this one, we shall condense the repeated use of the symmetric and transitive laws for equality.

Rule 4. For all a, b, c in R:

$$a + b = a + c \qquad \text{implies} \qquad b = c.$$

This rule is called the cancellation law for addition.

Proof. By postulate (viii) there is for the element a an element x with $a + x = 0$. Then

1. $x + a = a + x = 0$ (comm. law addn., trans. law).
2. $x = x, a + b = a + c$ (reflexive law, hypothesis).
3. $x + (a + b) = x + (a + c)$ (2, uniqueness of addn.).
4. $b = 0 + b = (x + a) + b$
   $= x + (a + b) = x + (a + c)$
   $= (x + a) + c = 0 + c = c.$

(Supply the reason for each step of 4!)

RULE 5. For each a, R contains one and only one solution x of the equation $a + x = 0$.

This solution is denoted by $x = -a$, as usual. The rule may then be quoted as $a + (-a) = 0$. As customary, the symbol $a - b$ denotes $a + (-b)$.

Proof. By postulate (viii), there is a solution x. If y is a second solution, then $a + x = 0 = a + y$ by the transitive and symmetric laws. Hence by Rule 4, $x = y$. Q.E.D.

RULE 6. For given a and b in R, there is one and only one x in R with $a + x = b$.

This rule asserts that subtraction is possible and unique.

Proof. Take $x = (-a) + b$. Then (give reasons!)

$$a + x = a + ((-a) + b) = (a + (-a)) + b = 0 + b = b.$$

If y is a second solution, then $a + x = b = a + y$ by the transitive law; hence $x = y$ by Rule 4. Q.E.D.

RULE 7. For all a in R, $a \cdot 0 = 0 = 0 \cdot a$.

Proof.

1. $a = a,\ a + 0 = a$ (reflexive law, postulate (vi)).
2. $a(a + 0) = aa$ (1, uniqueness of mult.).
3. $aa + a \cdot 0 = a(a + 0) = aa$ (distributive law, etc.).
   $= aa + 0$
4. $a \cdot 0 = 0$ (3, Rule 4).
5. $0 \cdot a = a \cdot 0 = 0$ (comm. law mult., 4)

RULE 8. If u in R has the property that $au = a$ for all a in R, then $u = 1$.

This rule asserts the uniqueness of the identity element 1 for multiplication. The proof, which resembles that of Rule 3, is left as an exercise.

RULE 9. For all a and b in R, $(-a)(-b) = ab$.

A special case of this rule is the "mysterious" law $(-1)(-1) = 1$.

Proof. Consider the triple sum (associative law!)

1. $[ab + a(-b)] + (-a)(-b) = ab + [a(-b) + (-a)(-b)]$.

By the distributive law, the definition of $-a$, Rule 7, and (vi),

2. $$\begin{aligned} ab + [a(-b) + (-a)(-b)] &= ab + [a + (-a)](-b) \\ &= ab + 0(-b) = ab. \end{aligned}$$

For similar reasons,

3. $$\begin{aligned} [ab + a(-b)] + (-a)(-b) &= a[b + (-b)] + (-a)(-b) \\ &= a \cdot 0 + (-a)(-b) = (-a)(-b). \end{aligned}$$

The result then follows from 1, 2, and 3 by the transitive and symmetric laws for equality. Q.E.D.

Various other simple and familiar rules are consequences of our postulates; some are stated in the exercises below.

Another basic algebraic law is the one used in the solution of quadratic equations, when it is argued that $(x + 2)(x - 3) = 0$ means either that $x + 2 = 0$ or that $x - 3 = 0$. The general law involved is the assertion

$$\text{(1)} \qquad \text{if} \quad ab = 0, \qquad \text{then either} \quad a = 0 \quad \text{or} \quad b = 0.$$

This assertion is not true in all commutative rings. But the proof is immediate in any integral domain D, by the cancellation law. For suppose that the first factor a is not zero. Then $ab = 0 = a \cdot 0$, and a may be cancelled; whence $b = 0$. Conversely, the cancellation law follows from this assertion (1) in any commutative ring R, for if $a \neq 0$, $ab = ac$ means that $ab - ac = a(b - c) = 0$, which by (1) makes $b - c = 0$. We therefore have

Theorem 1. *The cancellation law of multiplication is equivalent in a commutative ring to the assertion that a product of nonzero factors is not zero.*

Nonzero elements a and b with a product $ab = 0$ are sometimes called "divisors of zero," so that the cancellation law in a commutative ring R is equivalent to the assumption that R contains no divisors of zero.

Theorem 1 can be used to prove the cancellation law for the domain $\mathbf{Z}[\sqrt{2}]$ defined at the end of §1.1, as follows. Suppose that $\mathbf{Z}[\sqrt{2}]$ included divisors of zero, with

$$(a + b\sqrt{2})(c + d\sqrt{2}) = (ac + 2bd) + (ad + bc)\sqrt{2} = 0.$$

By definition, this gives $ac + 2bd = 0$, $ad + bc = 0$. Multiply the first by d, the second by c, and subtract; this gives $b(2d^2 - c^2) = 0$, whence either $b = 0$ or $c^2 = 2d^2$. If $b = 0$, then the two preceding equations give $ac = ad = 0$, so either $a = 0$ or $c = d = 0$ by Theorem 1. But the first alternative, $a = 0$, would imply that $a + b\sqrt{2} = 0$ (since $b = 0$); the second that $c + d\sqrt{2} = 0$—in neither case do we have divisors of zero.

There remains the possibility $c^2 = 2d^2$; this would imply $\sqrt{2} = c/d$ rational, whose impossibility will be proved in Theorem 10, §3.7.

If one admits that $\sqrt{2}$ is a real number, and that the set of all real numbers forms an integral domain R, then one can very easily prove that $\mathbf{Z}[\sqrt{2}]$ is an integral domain, by appealing to the following concept of a subdomain.

Definition. *A* subdomain *of an integral domain D is a subset of D which is also an integral domain, for the same operations of addition and multiplication.*

It is obvious that such a subset S is a subdomain if and only if it contains 0 and 1, with any element a its additive inverse, and with any two elements a and b their sum $a + b$ and product ab.

Exercises

In each of Exercises 1–5 give complete proofs, supporting each step by a postulate, a previous step, one of the rules established in the text, or an already established exercise.

1. Prove that the following rules hold in any integral domain:
   (a) $(a + b)(c + d) = (ac + bc) + (ad + bd)$,
   (b) $a + [b + (c + d)] = (a + b) + (c + d) = [(a + b) + c] + d$,
   (c) $a + (b + c) = (c + a) + b$,
   (d) $a(bc) = c(ab)$,
   (e) $a(b + (c + d)) = (ab + ac) + ad$,
   (f) $a(b + c)d = (ab)d + a(cd)$.

2. (a) Prove Rule 8. (b) Prove $1 \cdot 1 = 1$,
(c) Prove that the only "idempotents" (i.e., elements x satisfying $xx = x$) in an integral domain are 0 and 1.

3. Prove that the following rules hold for $-a$ in any integral domain:
(a) $-(-a) = a$, (b) $-0 = 0$,
(c) $-(a + b) = (-a) + (-b)$, (d) $-a = (-1)a$,
(e) $(-a)b = a(-b) = -(ab)$.

4. Prove Rule 9 from Ex. 3(d) and the special case $(-1)(-1) = 1$.

5. Prove that the following rules hold for the operation $a - b = a + (-b)$ in any integral domain:
(a) $(a - b) + (c - d) = (a + c) - (b + d)$,
(b) $(a - b) - (c - d) = (a + d) - (b + c)$,
(c) $(a - b)(c - d) = (ac + bd) - (ad + bc)$,
(d) $a - b = c - d$ if and only if $a + d = b + c$,
(e) $(a - b)c = ac - bc$.

6. Are the following sets of real numbers integral domains? Why?
(a) all even integers, (b) all odd integers, (c) all positive integers,
(d) all real numbers $a + b5^{1/4}$, where a and b are integers,
(e) all real numbers $a + b9^{1/4}$, where a and b are integers,
(f) all rational numbers whose denominators are 1 or a power of 2.

7. (a) Show that the system consisting of 0 and 1 alone, with addition and multiplication defined as usual, except that $1 + 1 = 0$ (instead of 2) is an integral domain.
(b) Show that the system which consists of 0 alone, with $0 + 0 = 0 \cdot 0 = 0$, satisfies all postulates for an integral domain except for the requirement $0 \neq 1$ in (vii).

8. (a) Show that if an algebraic system S satisfies all the postulates for an integral domain except possibly for the requirement $0 \neq 1$ in (vii), then S is either an integral domain or the system consisting of 0 alone, as described in Ex. 7(b).
(b) Is $0 \neq 1$ used in proving Rules 1–9?

9. Suppose that the sum of any two integers is defined as usual, but that the product of any two integers is defined to be zero. With this interpretation, which ones among the postulates for an integral domain are still satisfied?

10. Find two functions $f \not\equiv 0$ and $g \not\equiv 0$ such that $fg \equiv 0$.

1.3. Properties of Ordered Domains

Because the ring **Z** of all ordinary integers plays a unique role in mathematics, one should be aware of its special properties, of which the commutative and cancellation laws of multiplication are only two. Many other properties stem from the possibility of listing the integers in the usual order

$$\cdots -4, -3, -2, -1, 0, 1, 2, 3, 4, \cdots.$$