安徽省高等学校“十一五”省级规划教材
安徽省高等学校省级精品课程教材

Abstract Algebra

抽象代数

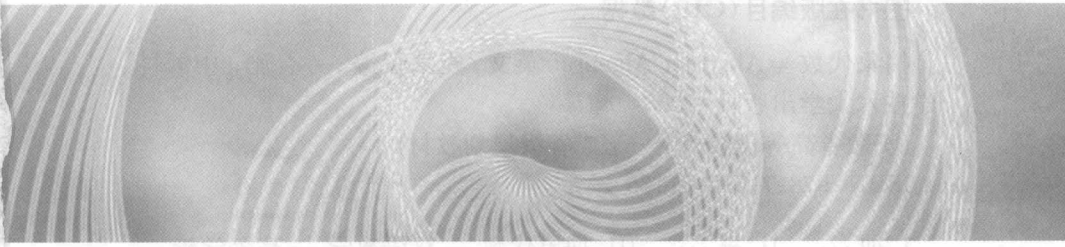
Zhu Jiagui
祝家贵／编

University of Science and Technology of China Press
中国科学技术大学出版社

安徽省高等学校“十一五”省级规划教材
安徽省高等学校省级精品课程教材

Abstract Algebra
抽象代数

祝家贵 / 编
Zhu Jiagui



中国科学技术大学出版社

内容简介

本书前 3 章包括近世代数的主要概念和基本结论, 并略有拓展. 第 4 章介绍模的基本理论及应用, 对主理想整环上有限生成模的分解理论只介绍主要结论, 而删去了部分定理的证明. 考虑到解题的困难, 在每章后精选了阅读材料以巩固基本理论和提高解题能力.

本书可以作为数学专业代数选修课教材, 也可以作为数学系本科生近世代数课程的教学参考书.

图书在版编目(CIP)数据

抽象代数 = Abstract Algebra: 英文 / 祝家贵编 .— 合肥: 中国科学技术大学出版社, 2008. 9

(安徽省高等学校“十一五”省级规划教材)

ISBN 978-7-312-01188-7

I. 抽 ··· II. 祝 ··· III. 抽象代数 — 双语教学 — 高等学校 — 教材 — 英文 IV.O153

中国版本图书馆 CIP 数据核字(2008)第 120956 号

精品课程网址 http://jpkc.wxc.edu.cn/2007/algebra/

中国科学技术大学出版社出版发行

安徽省合肥市金寨路 96 号, 230026

网址: http://press.ustc.edu.cn

安徽辉隆农资集团瑞隆印务有限公司印刷

全国新华书店经销

开本: 880 × 1 230 1/32 印张: 5.625 字数: 120 千

2008 年 9 月第 1 版 2008 年 9 月第 1 次印刷

定价: 15.00 元

前　言

随着我国高等教育改革步伐的不断加快，其人才培养模式、教学内容和教学方法都在发生重大变化，探索和研究应用型人才培养的课程体系和教学内容，是以培养应用型人才为主的高等学校的重要任务. 其次，由于对外开放的日益深入，外语作为信息交流的重要工具正在全方位地向日常工作渗透. 作为数学专业本科学生，在大学学习两年外语课以后，除了少数有志继续深造的以外，大部分对学习外语的用处感到茫然. 本书就是基于以上目的所做的一种尝试.

编者采用 Schaum 的题解精萃《抽象代数》(《Abstract Algebra》)，为我校数学与应用数学专业学生连续开设了 5 届选修课. 在学生学完高等代数和近世代数以后，我们把代数学的基本理论和基本概念作简明精练的归纳和总结，进一步拓展学科课程基本理论，对学生巩固学科基本知识和提高解题综合能力很有帮助；同时，使用外文原版教材，使学生在学习过程中，了解、熟悉《抽象代数》的英文词汇，促进了学生阅读专业英文书籍的速度和水平，使他们用英语学习、解题的能力得到了锻炼. 每届学生的调查问卷表明，该门课程的教学效果是很好的，学生收获较大.

经过 5 年的教学实践，作为高等代数和近世代数的后

续课程，其特色得到了安徽省课程建设专家委员会的充分肯定，2007 年被评为省级精品课程. 鉴于国内目前尚未见到同名英文教材，我们以 Schaum 的题解精萃《Abstract Algebra》为蓝本，编写了这本教材. 内容安排是这样考虑的：前 3 章包括了目前近世代数的主要概念和基本结论，在复习和归纳的基础上稍微作了拓展，比如 Zorn 引理、Sylow 定理等. 第 4 章主要介绍模的基本理论及其应用，对主理想整环上有限生成模的分解理论，我们把整个结构体系介绍清楚，而删去部分定理的证明. 考虑到抽象代数解题的困难，我们在每章后面精选了部分阅读材料，有些是正文内容的扩充，以帮助学生巩固基本理论和提高解题能力. 如果用作选修课教材，各章教学时数与教学内容可以根据学生实际情况进行调整. 根据我们的经验，本书的内容可以在一学期（每周 3 学时）讲完. 此外，本书也可以作为数学系本科生近世代数课程的教学参考书.

安徽省教育厅将本书作为“十一五”省级规划教材建设立项. 在本书的试用过程中，数理系王修建老师提出了一些修改之处，并且细心地打印本书的初稿. 首都师范大学石生明教授和南京大学佟文廷教授在仔细审阅书稿后提出了许多具体的修改意见. 此外，本书还得到了国家自然科学基金（基金号: 10571153）的资助. 编者在此一并表示衷心的感谢!

限于编者的水平，书中一定有许多不足之处，敬请读者指正，从而使本书能不断得到完善.

编　者

2008 年 8 月

Special Notation

$|X|$ (cardinal) number of elements in a finite set X

$a|b$ a divides b

$\mathbb{C}$ set of all complex numbers

$\mathbb{N}$ set of all natural numbers $= \{\text{integers } n : n \geqslant 0\}$

$\mathbb{Q}$ set of all rational numbers

$\mathbb{R}$ set of all real numbers

$\mathbb{Z}$ set of all integers

$GL(V)$ all automorphisms of a vector space V

S_n symmetric group on n letters

S_X symmetric group on a set X

$\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$ integers modulo n

$\deg(f)$ degree of a polynomial $f(x)$

1_X identity function on a set X

$U(R)$ group of units in a ring R

$H < G$ H is a subgroup of a group G

$[G : H]$ index of a subgroup H in a group G

$\langle a \rangle$ principal ideal generated by a

$H \lhd G$ H is a normal subgroup of a group G

$\phi(n)$ Euler ϕ-function

$I \lhd R$ I is an ideal of a ring R

$N < M$ N is a submodule of a module M

$\text{glb}\{S, T\}$ the greatest lower bound of S and T

$\text{lub}\{S, T\}$ the least upper bound of S and T

$\gcd(a, b)$ the greatest common factor of a and b

$M_{m,n}(F)$ m-by-n matrices with entries from a field F

$Hom(R^{(m)}, R^{(n)})$ set of homomorphisms of $R^{(m)}$ into $R^{(n)}$

$\mathcal{T}(V)$ set of all subspaces of a vector space V

$L(V, W)$ set of all linear transformations from V to W

$L(V)$ set of all linear transformations on V

iff if and only if

Contents

Chapter 1 Rudiments

In this chapter, we briefly review some familiar materials of basic set theory, mappings, relations and operations. These materials are needed for the sequel and should be skimmed quickly.

1.1 Sets

Sets

Any collection of objects, whose properties are "well-defined" (that is, membership in the collection can be determined by the nature of the objects without ambiguity), is called a set. Usually we denote a set by a capital letter. For example,

$$A = \{a, b, c, \cdots\}$$
$$A = \{x \,|\, x \in \mathbb{R} \text{ and } x^2 < 1\}.$$

Any object in a given set A is called an element of A. We write $x \in A$ if x is an element of A, and $x \notin A$ if x is not an element of A.

Two sets A and B are defined to be equal, denoted by $A = B$, if they contain the same elements.

The set which contains no elements is called the empty set, and is written as $\varnothing$.

Given set A and B, if every element of B is also contained in A, then B is said to be itself contained in A, and is called a subset of A, written $B \subseteq A$. If $B \subseteq A$, but $B \neq A$, we say that B is a proper subset of A. If we wish to emphasize that B is a proper subset, we write $B \subsetneq A$.

The power axiom asserts that for every set A the class $\mathcal{P}(A)$ of all subsets of A is itself a set.

$$\mathcal{P}(A) = \{S \mid S \subseteq A\}$$

is called the power set of A.

Operations on Sets

Let $\{A_i \mid i \in I\}$ be a family of sets indexed by (the nonempty set) I. Its union and intersection are defined to be respectively the sets

$$\bigcup_{i \in I} A_i = \{x \mid x \in A_i \text{ for some } i \in I\}$$

and

$$\bigcap_{i \in I} A_i = \{x \mid x \in A_i \text{ for every } i \in I\}.$$

If $I = \{1, 2, \cdots, n\}$, we write $A_1 \cup A_2 \cup \cdots \cup A_n$ in place of $\bigcup_{i \in I} A_i$ and similarly for intersections. If $A \cap B = \varnothing$, A

and B are said to be disjoint.

If A and B are sets, the relative complement of B in A is the subset of A :

$$A - B = \{x \mid x \in A \text{ and } x \notin B\}.$$

If all the sets under consideration are subsets of some fixed set U (called the universal set), then $U - A$ is denoted A^C and called simply the complement of A. Clearly, if $A \subseteq B$, then $A^C \supseteq B^C$.

The Properties of Operations

(1) Idempotent law:

$$A \cup A = A, \ A \cap A = A;$$

Involution law:

$$(A^C)^C = A;$$

(2) Commutative laws:

$$A \cup B = B \cup A, \ A \cap B = B \cap A;$$

Associative laws:

$$A \cup (B \cup C) = (A \cup B) \cup C,$$

$$A \cap (B \cap C) = (A \cap B) \cap C;$$

Distributive laws:

$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C),$$

$$A \cup (B \cap C) = (A \cup B) \cap (A \cup C);$$

(3) DeMorgan's laws:

(i) $(A \cup B)^C = A^C \cap B^C$, $(A \cap B)^C = A^C \cup B^C$;

(ii) $A - (B \cup C) = (A - B) \cap (A - C)$,

$A - (B \cap C) = (A - B) \cup (A - C)$.

Partitions of a Set

Let $A_i \subseteq A (i = 1, 2, \cdots, n)$, and $A_i \cap A_j = \varnothing (i \neq j)$. If $\bigcup_{i=1}^{n} A_i = A$, we say $\{A_i\}_{i=1,2,\cdots,n}$ is a partition of A.

Cartesian Product

Suppose that A and B are two sets, the set

$$A \times B = \{(x, y) \mid x \in A \text{ and } y \in B\}$$

is called the Cartesian product of A and B.

If

$$(a, b), (a', b') \in A \times B,$$

we define $(a, b) = (a', b')$ if and only if $a = a'$ and $b = b'$.

Example 1 The plane

$$\mathbb{R}^2 = \mathbb{R} \times \mathbb{R} = \{(x, y) \mid x, y \in \mathbb{R}\}.$$

In general, if $\{A_i \mid i \in I\}$ is a family of sets indexed by a (nonempty) set I. The cartesian product of the sets A_i is the set of all maps $f : I \to \bigcup_{i \in I} A_i$ such that $f(i) \in A_i$ for all $i \in I$ and is denoted by $\prod_{i \in I} A_i$.

1.2 Mappings

Maps

Let A and B be sets. If there is a method f of associating a unique element of B with each element of A, we say that f is a map, or a mapping from A into B and denote $f : A \to B$ or $A \xrightarrow{f} B$. We represent the element in B which is associated with a given element of A by the notation $b = f(a)$.

If $f : A \to B$ is a map, the set

$$\{(a, b) \in A \times B \mid b = f(a)\}$$

is called the graph of the map f. Given a map $f : A \to B$, we refer to the set A as the domain, and to the set B as the co-domain.

The map which associates every element of a set A with itself is called the identity map, denoted by "$1_A : A \to A$, via $1_A(x) = x$, for all $x \in A$."

Axiom of Choice

Theorem 1.2.1 *For any set A, there is a mapping $\phi : \mathcal{P}(A) \to A$ (called the "choice function"), such that if S is a nonempty subset of A, then $\phi(S) \in S$.*

Example 1 Let $A = \{a, b\}$. Then the non-trivial sub-

sets of A are $A_1 = \{a\}, A_2 = \{b\}, A_3 = \{a, b\}$. By the Axiom of choice, we can define two different "choice" functions

$$\phi_1 = \{(A_1, a), (A_2, b), (A_3, a)\}$$

and

$$\phi_2 = \{(A_1, a), (A_2, b), (A_3, b)\}.$$

Note Axiom of choice is equivalent to Zorn's lemma.

Composite Maps

Given sets A, B, C, and maps $f : A \to B$, $g : B \to C$, we define a composite map as

$$g \circ f = \{(a, g(f(a))) \mid a \in A\}.$$

Theorem 1.2.2 (1) *Composition is associative: if* $f : A \to B$, $g : B \to C$ *and* $h : C \to D$ *are maps, then*

$$h \circ (g \circ f) = (h \circ g) \circ f.$$

(2) *If* $f : A \to B$, *then* $1_B \circ f = f \circ 1_A = f$.

Classification of Maps

Given a map $f : A \to B$, then for each $a \in A$, there is a unique $b \in B$ such that $f(a) = b$. If $S \subseteq A$, the image of S under f (denoted $f(S)$) is the set $\{f(s), s \in S\}$. The set $f(A)$ is called the image of f and is denoted $\mathrm{Im} f$. If $T \subseteq B$, the inverse image of T under f (denoted $f^{-1}(T)$) is the set

$$\{a \in A \mid f(a) \in T\}.$$

The following facts can be easily verified:

for $S \subset A$, $f^{-1}(f(S)) \supset S$;

for $T \subset B$, $f(f^{-1}(T)) \subset T$;

for any family $\{T_i \mid i \in I\}$ of subsets of B,

$$f^{-1}\left(\bigcup_{i\in I} T_i\right) = \bigcup_{i\in I} f^{-1}(T_i),$$

$$f^{-1}\left(\bigcap_{i\in I} T_i\right) = \bigcap_{i\in I} f^{-1}(T_i).$$

(1) Injection

f is called an injection if, whenever a and a' are distinct elements of A, then $f(a) \neq f(a')$. Equivalently, f is injective if, for every pair $a, a' \in A$, we have "$f(a) = f(a')$ implies $a = a'$" .

(2) Surjection

f is called a surjection if, for each $b \in B$, there is some $a \in A$ such that $f(a) = b$. Equivalently, f is surjective if $\mathrm{Im}f = B$.

(3) Bijection

f is called a bijection if it is both injection and surjection.

There are other names for these maps. Injections are often called monomorphisms, surjections are often called epimorphisms, and bijections are often called one-to-one correspondences.

Theorem 1.2.3 *If $f : A \to B, g : B \to C$ are both epimorphisms, then $g \circ f$ is also an epimorphism.*

Inverse Maps

A map $f : A \to B$ has an inverse if there is a map $g : B \to A$ with $g \circ f = 1_A$ and $f \circ g = 1_B$.

Theorem 1.2.4 (1) *If $f : A \to B$ and $g : B \to A$ are maps such that $g \circ f = 1_A$, then f is injective and g is surjective.*

(2) *A map $f : A \to B$ has an inverse $g : B \to A$ if and only if f is a bijection.*

Proof (1) Suppose that $f(a) = f(a')$, apply g to obtain $g(f(a)) = g(f(a'))$, that is, $a = a'$, and so f is injective. For each $a \in A$, since $a = g(f(a))$, we know that there is a $b = f(a) \in B$ such that $g(b) = a$, and so g is surjective.

(2) If f has an inverse g, then part (1) show that f is both injective and surjective, and $g \circ f = 1_A$ and $f \circ g = 1_B$. Assume that f is a bijection. For each $b \in B$, there is $a \in A$ with $f(a) = b$ since f is surjective, and this element is unique because f is injective. Defining $g(b) = a$ gives a map whose domain is B, and it is plain that g is the inverse of f. □

Note If a map $f : A \to B$ is a bijection, then it has exactly one inverse. The inverse of f is denoted by f^{-1}.

Example 2 Let $A = \mathbb{R}$ and $B = \mathbb{R}^+$, and let

$$f : A \to B$$

be given by $f(x) = \mathrm{e}^x$. Then f is a bijection, and its inverse