时代教育・国外高校优秀教材精选

（英文版・原书第2版）

代数学

Algebra

（印度）Vivek Sahai
Vikas Bist 著

机械工业出版社
CHINA MACHINE PRESS

时代教育·国外高校优秀教材精选

代 数 学

（英文版·原书第2版）

Algebra

机 械 工 业 出 版 社

本书是为研究生的代数学课程编写的教材，所选内容都是经典的，是学习近世代数必须具备的基本知识。全书语言精练，结构严谨，概念叙述清楚，定理证明简洁。

Original English Language title: Algebra, by Vivek Sahai &Vikas Bist.

ISBN 81-7319-516-1

北京市版权局著作权合同登记号：图字：01-2006-4960

图书在版编目(CIP)数据

代数学：英文版原书第2版/(印)萨哈(Sahai,V.)，比斯特(Bist,V.)著.—北京：机械工业出版社，2008.9

(时代教育:国外高校优秀教材精选)

ISBN 978-7-111-25074-6

Ⅰ.代… Ⅱ.①萨…②比… Ⅲ.代数—研究生—教材—英文 Ⅳ.015

中国版本图书馆CIP数据核字(2008)第137820号

机械工业出版社(北京市百万庄大街22号 邮政编码100037)

责任编辑：郑 玫 封面设计：鞠 杨

责任印制：洪汉军

北京铭成印刷有限公司印刷

2008年9月第1版第1次印刷

140mm×203mm·9.5印张·180千字

标准书号：ISBN 978-7-111-25074-6

定价：19.00元

凡购本书，如有缺页、倒页、脱页，由本社发行部调换

销售服务热线电话：(010)68326294

购书热线电话：(010)88379639 88379641 88379643

编辑热线电话：(010)88379722

封面无防伪标均为盗版

国外高校优秀教材审定委员会

主任委员：

杨叔子

委员（按姓氏笔画为序）：

丁丽娟	王先逵	王大康	白峰杉
石德珂	史荣昌	孙洪祥	朱孝禄
陆启韶	张润琦	张　策	张三慧
张福润	张延华	吴宗泽	吴　麒
宋心琦	李俊峰	佘远斌	陈文楷
陈立周	单辉祖	俞正光	赵汝嘉
郭可谦	翁海珊	龚光鲁	章栋恩
黄永畅	谭泽光	郭鸿志	

出版说明

随着我国加入WTO，国际间的竞争越来越激烈，而国际间的竞争实际上也就是人才的竞争、教育的竞争。为了加快培养具有国际竞争力的高水平技术人才，加快我国教育改革的步伐，国家教育部近来出台了一系列倡导高校开展双语教学、引进原版教材的政策。以此为契机，机械工业出版社陆续推出了一系列国外影印版教材，其内容涉及高等学校公共基础课，以及机、电、信息领域的专业基础课和专业课。

引进国外优秀原版教材，在有条件的学校推动开展英语授课或双语教学，自然也引进了先进的教学思想和教学方法，这对提高我国自编教材的水平，加强学生的英语实际应用能力，使我国的高等教育尽快与国际接轨，必将起到积极的推动作用。

为了做好教材的引进工作，机械工业出版社特别成立了由著名专家组成的国外高校优秀教材审定委员会。这些专家对实施双语教学做了深入细致的调查研究，对引进原版教材提出了许多建设性意见，并慎重地对每一本将要引进的原版教材一审再审，精选再精选，确认教材本身的质量水平，以及权威性和先进性，以期所引进的原版教材能适应我国学生的外语水平和学习特点。在引进工作中，审定委员会还结合我国高校教学课程体系的设置和要求，对原版教材的教学思想和方法的先进性、科学性严格把关。同时尽量考虑原版教材的系统性和经济性。

这套教材出版后，我们将根据各高校的双语教学计划，举办原版教材的教师培训，及时地将其推荐给各高校选用。希望高校师生在使用教材后及时反馈意见和建议，使我们更好地为教学改革服务。

机械工业出版社

序

本书是为研究生的代数学课程编写的教材，所选内容都是经典的，是学习近世代数必须具备的基础知识。全书语言精练，结构严谨，概念叙述清楚，定理证明简洁。除了正文叙述外，配有丰富的例题，基础题和比较复杂的题目都有，不仅可以帮助读者理解基本概念，而且进一步拓展了正文所述的性质及结果，每节后面还附有大量习题供读者巩固所学知识、进行练习，是一本很好的教科书。

本书包括 5 章，第 1 章的内容包括最基础的集合、映射、等价关系、整数。

有关于群的一章(第 2 章)由定义和例子开始，包括 Lagrange、Cauchy 和 Sylow 的标准理论和应用。用单独的一节讨论对称群，目的是强调它在群理论中正例和反例的应用。本章详细讲解了可解群和幂零群，后面将在讲解域的一章中讨论求多项式的根时用到这些知识。此章最后以有限阿贝尔群和最小阶群理论结束。

关于环的一章(第 3 章)也以基本定义和大量环的例子开始，着重讲解了多项式环和形式幂级数环。用单独一节讲解整环中的因子分解，它引出了欧几里德域这一最基本的理想域和唯一的因式分解域。此章以 Noetherian 环上的一些结论结束，包括 Hilbert 基础理论。

有关模的一章(第 4 章)内容包括关于直和与正合序列的很多结论，扼要地介绍了环上的自由模和向量穿间。本章的最大特点是在理想域上的有限生成模的结构理论和它在阿贝尔群上的应用。

最后关于域的一章(第 5 章)以域扩张的概念开始，讨论了正

规扩张和可离扩张，也介绍了在分裂域和代数闭域上的结论，这些形成了 Galois 定理的基础。而后讨论了 Galois 定的基本理论，表明域理论与前面讨论的群理论的相互影响。然后构造了多项式的 Galois 理论，它能导出一般情况下五次方程在扩张下不可解。最后以域扩张的应用结束。

清华大学数学系
俞正光

Preface

This book is designed to serve as a text book on algebra for post-graduate students of Indian universities and for equivalent level abroad. The text has grown out of the one year course given by the authors at their respective universities. The subject matter is divided in five chapters. The contents of these chapters are standard and almost everything about the subject is developed that is essential for an introductory course on algebra. A fairly large number of examples are included to help the reader to understand the concepts involved as well as to explore further related results. The exercises at the end of each section are a mixed lot. These vary from the routine to the more complicated ones. The difficult ones do not start with a discouraging tag. It is the authors experience that students skip problems marked with some sort of tag. The book concludes with a short bibliography and an index.

In the first chapter, we include some fundamental results on sets, mappings, equivalence relations and integers, which are needed in subsequent chapters. An effort is made to make the book as much self contained as possible.

The chapter on groups begins with definitions and examples. It contains the standard theorems of Lagrange, Cauchy and Sylow, and their applications. Symmetric groups are discussed in a separate section highlighting their utility in generating examples and counter examples in group theory. An explicit description of solvable and nilpotent groups is given as these are required later in the chapter of fields while dealing with the solvability by radicals of the polynomials. The chapter concludes with structure theorems of finite abelian groups and classification of groups of small order.

The chapter on rings starts with the basic definitions and numerous examples of rings, with special attention to the ring of polynomials and the ring of formal power series. A section is devoted to study the factorization in integral domains, which leads to Euclidean domains, principal ideal domains and unique factorization domains. The chapter closes with some results on Noetherian rings, including the Hilbert's basis theorem.

The chapter on modules includes various results on direct sums and exact sequences. Free modules over a ring with identity are discussed and vector spaces are studied, in brief, as a special case. One of the main features of this chapter is the structure theorem of finitely generated modules over a principal ideal domain and its applications to abelian groups.

Finally, the chapter on fields opens with the definition of field extensions and discusses normal and separable extensions. Also, results on splitting fields and algebraically closed fields are presented. These form the ground work for Galois theory. The fundamental theorem of Galois theory is discussed and the interplay of field theory and the group theory is exhibited. Later, Galois groups of polynomials are constructed and it is shown that a quintic, in general, is not solvable by radicals. The chapter completes with some applications of field extensions which include the problem of constructibility of a regular n-gon and the Wedderburn's theorem.

Lucknow
February 2002

VIVEK SAHAI
VIKAS BIST

Notations

$\mathbf{A}$	set of algebraic numbers
$\mathbf{C}$	set of complex numbers
$\mathbf{N}$	set of nonnegative integers
$\mathbf{Q}$	set of rational numbers
$\mathbf{Q}^+$	set of positive rational numbers
$\mathbf{R}$	set of real numbers
$\mathbf{R}^+$	set of positive real numbers
$\mathbf{Z}$	set of integers
$\mathbf{Z}^+$	set of positive integers
$n\mathbf{Z}$	set of integers which are multiples of n
$\mathbf{Z}_n$	set of integers modulo n
$x \in A$	x is an element of the set A
$x \notin A$	x is not an element of the set A
$A \cup B$	union of sets A and B
$A \cap B$	intersection of sets A and B
$A \setminus B$	difference of B in A
$B \subseteq A$	B is a subset of A
$B \subsetneq A$	B is a proper subset of A
$A \times B$	cartesian product of A and B
$\|A\|$	cardinality of A
$f: A \to B$	f is a mapping from A to B
$a \mapsto b$	a is mapped to b
$\mathrm{Im}\,(f)$	image under the mapping f
$\varphi(n)$	Euler's phi-function
$\langle X \rangle$	generated by X
$o(x)$	order of x
$H \leq G$	H is a subgroup of G
$H < G$	H is a proper subgroup of G
Ha, $H + a$	right coset of H in G
aH, $a + H$	left coset of H in G
$\|G : H\|$	index of H in G
$N \lhd G$	N is a normal subgroup of G
G/N	factor group of G by N
S_n	symmetry group on n letters
A_n	alternating group on n letters
D_n	dihedral group of order n

$\ker \phi$	kernel of the homomorphism ϕ
$G \simeq \bar{G}$	G is isomorphic to $\bar{G}$
$\prod_{i=1}^{n} G_i$	direct product of $G_1, \ldots, G_n$
$\oplus \sum_{i=1}^{n} G_i$	direct sum of $G_1, \ldots, G_n$
G', $[G, G]$	commutator subgroup of G
$N_G(X)$	normalizer of X in G
$C_G(X)$	centralizer of X in G
$\zeta(G)$	centre of G
$\mathrm{Aut}\,(G)$	group of automorphisms of G
$\mathrm{Inn}\,(G)$	group of inner automorphisms of G
$H \,\mathrm{char}\, G$	H is a characteristic subgroup of G
$U(R)$	group of units of a ring R
$\mathrm{char}\,(R)$	characteristic of ring R
R/I	factor ring of R by I
$f(x)$	polynomial in indeterminate x
$\deg(f(x))$	degree of $f(x)$
$\mathrm{cont}(f(x))$	content of $f(x)$
$R[x]$	ring of polynomials
$R[[x]]$	ring of formal power series
$K(x)$	field of fractions of $K[x]$
$K((x))$	field of fractions of $K[[x]]$
$R[x_1, \ldots, x_n]$	ring of polynomials in n indeterminates
$a \vert b$	a divides b
$\gcd(a, b)$	greatest common divisor of a and b
UFD	unique factorization domain
PID	principal ideal domain
$\mathrm{rank}_R(M)$	rank of M over R
$\mathrm{Ann}\,(X)$	annihilator of X
$\dim_K(V)$	dimension of V over K
$\mathrm{Hom}_R(M, N)$	set of all R-module homomorphisms from M to N
$\mathrm{End}_R(M)$	set of all R-module endomorphisms on M
$K \prec F$	F is an extension field of field K
$[F : K]$	degree of F over K
$\min(u, K)$	minimal polynomial of u over K
$\mathrm{Mon}_K(E, F)$	set of all K-monomorphisms from E to F
$\Phi_n(x)$	n-th cyclotomic polynomial

目　　录

Contents

Chapter 1

Preliminaries

In this chapter we briefly discuss the basic concepts which we assume that the reader is familiar with. The purpose of this chapter is to review some results that are needed for the sequel, and to establish certain notations that will be used throughout this book.

1.1 Sets and Mappings

Our approach to sets is quite informal. By a **set** we mean a collection of objects which are called the **elements** of the set. If A is a set and x is an element of A, we write $x \in A$; if x is not an element of A, we write $x \notin A$. A set A is **finite** if it has finitely many elements. Otherwise A is said to be **infinite**. A set B is called a **subset** of A, if every element of B is an element of A; in this case we write $B \subseteq A$. Two sets A and B are **equal**, written as $A = B$, if $A \subseteq B$ and $B \subseteq A$. A subset B of A is **proper** if $B \subseteq A$ and $B \neq A$, denoted by $B \subsetneq A$. The **empty set** $\emptyset$ is a set with no elements. Clearly the empty set is a subset of every set.

Definition: Let A and B be sets. Then:
(*i*) $A \cup B = \{\, x \mid x \in A \text{ or } x \in B \,\}$, called the **union** of A and B;
(*ii*) $A \cap B = \{\, x \mid x \in A \text{ and } x \in B \,\}$, called the **intersection** of A and B;
(*iii*) $A \setminus B = \{\, x \mid x \in A \text{ and } x \notin B \,\}$, called the **difference** of B in A.

Sets A and B are **disjoint** if $A \cap B = \emptyset$. It is easy to verify that $A \subseteq B$ if and only if $A \cup B = B$; and $A \subseteq B$ if and only if $A \cap B = A$.

We say that a set $\wedge$ is an **index set** of the family $\mathcal{F}$ of sets if for every $\alpha \in \wedge$, there is a set A_α in the family. The index set can be finite or infinite. Let $\{A_\alpha\}_{\alpha\in\wedge}$ be a family of sets indexed by $\wedge$. Then

$$\cup_{\alpha\in\wedge} A_\alpha = \{\, x \mid x \in A_\alpha \text{ for some } \alpha \in \wedge \,\}$$

and

$$\cap_{\alpha\in\wedge} A_\alpha = \{\, x \mid x \in A_\alpha \text{ for all } \alpha \in \wedge \,\}$$

are the union and intersection of the sets A_α respectively. The sets $\{A_\alpha\}_{\alpha\in\wedge}$ are said to be **mutually disjoint** if for $A_\alpha \neq A_\beta$, $A_\alpha \cap A_\beta = \emptyset$. The reader should verify the following statements:

$$A \cap (\cup_{\alpha\in\wedge}\ A_\alpha) = \cup_{\alpha\in\wedge}(A \cap A_\alpha);$$

$$A \cup (\cap_{\alpha\in\wedge}\ A_\alpha) = \cap_{\alpha\in\wedge}(A \cup A_\alpha);$$

$$A \setminus (\cup_{\alpha\in\wedge}\ A_\alpha) = \cap_{\alpha\in\wedge}(A \setminus A_\alpha);$$

$$A \setminus (\cap_{\alpha\in\wedge}\ A_\alpha) = \cup_{\alpha\in\wedge}(A \setminus A_\alpha).$$

Let A and B be sets. The **cartesian product** of A and B is a set

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

The elements of $A \times B$ are called **ordered pairs**. If either A or B is empty, then $A \times B = \emptyset$.

Definition: A mapping (or **map** or **function**) from a set A to a set B is a triple (A, B, f) such that:
(i) $f \subseteq A \times B$;
(ii) to each $a \in A$, there exists a unique $b \in B$ such that $(a, b) \in f$. We denote this element b by $f(a)$.
In this case, we shall frequently say that f is a mapping from A to B, and we write $f\colon A \to B$. The set A is called the **domain** of f and the set B is called the **codomain** of f.

Let $f\colon A \to B$ and $X \subseteq A$. The **direct image** of X under f is the set

$$f(X) = \{\, f(x) \mid x \in X \,\}.$$

Clearly, $f(X) \subseteq B$. In particular, if $X = A$, then $f(A)$ is also known as the **image** of f and is also denoted by $\mathrm{Im}\,(f)$. If $Y \subseteq B$, the **inverse image** of Y under f is the set

$$f^{-1}(Y) = \{\, a \in A \mid f(a) \in Y \,\}.$$

If $Y = \{y\}$, a **singleton set**, we write $f^{-1}(y)$ for $f^{-1}(\{y\})$. Clearly, if $b \in B \setminus f(A)$, then $f^{-1}(b) = \emptyset$.

A mapping $f\colon A \to B$ is **surjective** or **onto** if $f(A) = B$. Equivalently, $f\colon A \to B$ is surjective if to each $b \in B$ there is $a \in A$ such that $f(a) = b$. If $f\colon A \to B$ is such that for $x, y \in A$, $f(x) = f(y)$ implies that $x = y$, then f is called **injective** or **one-one**. A mapping which is injective as well as surjective is known as a **bijective** or **one-one onto** mapping.

Let $f\colon A \to B$ be a mapping. Let A_1, A_2 be subsets of A and B_1, B_2 be subsets of B. The reader should verify the following statements:

(i) if $A_1 \subseteq A_2$, then $f(A_1) \subseteq f(A_2)$;

(ii) if $B_1 \subseteq B_2$, then $f^{-1}(B_1) \subseteq f^{-1}(B_2)$;

(iii) $f(A_1 \cup A_2) = f(A_1) \cup f(A_2)$;