Schaum's
题解精萃

抽象代数

ABSTRACT ALGEBRA

影印版

Deborah C. Arangno

重点概念精萃归纳

450 个精解例题

关键问题导引

课堂教学的良好辅助

读原版英文，学习基本理论和解题技巧

高等教育出版社
HIGHER EDUCATION PRESS

麦格劳－希尔国际出版公司
McGraw-Hill Inc.

Schaum's
题解精萃

抽象代数
ABSTRACT ALGEBRA

影印版

Deborah C. Arangno

高等教育出版社
Higher Education Press

麦格劳－希尔国际出版公司
McGraw-Hill Inc.

图字：01－2000－0540

内容简介

Schaum's丛书是由麦格劳－希尔(McGraw-Hill)国际出版公司出版的著名的系列教学辅助用书，涵盖了高等教育各类各门学科和课程。每本书都汇集了该门学科课程中的精髓内容，并对基本理论和基本概念作了简明精炼的归纳和总结，还提供了由美国众多经验丰富的资深教师和学者推荐、讲解透彻的精选例题和形式多样的各类习题。

本书根据Schaum's系列丛书中《抽象代数》原文影印出版。可供在校本科生、研究生以及社会各类科技人员参考使用。

Schaum's Outline of Theory and Problems of
ABSTRACT ALGEBRA

图书在版编目(CIP)数据

Schaum's题解精萃．抽象代数：英文/(美)阿拉贡(Arangno, D.)著．—北京：高等教育出版社，2000.6
ISBN 7－04－008755－3

Ⅰ.S… Ⅱ.阿… Ⅲ.抽象代数－高等学校－解题－英文 Ⅳ.G642.3－44

中国版本图书馆CIP数据核字(2000)第26681号

Schaum's题解精萃　抽象代数
Deborah C. Arangno

出版发行	高等教育出版社		
社　　址	北京市东城区沙滩后街55号	邮政编码	100009
电　　话	010－64054588	传　　真	010－64014048
网　　址	http://www.hep.edu.cn		
经　　销	新华书店北京发行所		
印　　刷	国防工业出版社印刷厂		
开　　本	850×1168　1/16	版　　次	2000年6月第1版
印　　张	15.25	印　　次	2000年6月第1次印刷
字　　数	410 000	定　　价	20.00元

出版说明

随着我国高等教育改革形势的发展,高等教育的人才培养模式及教学形式和教学方法正在发生重大变化,一个拓宽专业口径,实行弹性学习制度,允许分阶段完成学业,横向沟通、纵向衔接的教育体制正在逐步构建形成。为了促进高等教育的改革,活跃高等学校的教学工作,扩大学生的眼界,我们组织出版了这套"Schaum's题解精萃"。

"Schaum's丛书"是由麦格劳-希尔(McGraw-Hill)国际出版公司出版的著名的系列教学辅助用书,目前已出版了约700多个品种,涵盖了高等教育各类各门学科和课程。本套丛书的特点是:每本书都汇集了该门学科课程中的精髓内容,并对基本理论和基本概念作了简明精炼的归纳和总结;同时,还提供了由美国众多经验丰富的资深教师和学者推荐、讲解透彻的精选例题和形式多样的各类习题约2 000—4 000个。本套书在美国高等学校中颇具权威性,多年来持续畅销,目前在世界范围销售超过3 000万册。

我们从"Schaum's丛书"中经精心挑选,组合成"Schaum's题解精萃",以原版影印的形式介绍到国内,意在使学生在使用本书的同时,了解、熟悉相关学科和课程的英语专业词汇,提高英语专业阅读的速度和水平,锻炼使用英语学习、解题的能力。因为,当今时代,熟练掌握英语已成为21世纪人才必备的基本素质和能力。"Schaum's题解精萃"第一批影印书内容涉及理工科各基础学科,今后我们将陆续影印出版该系列其他学科的图书。

本套书可供高等学校的理工科学生在学习各学科课程的同时,进行辅助学习和各类习题训练,有助于提高学生巩固学科基本知识和解题的综合能力,同时也可适用于各科教师在教学和辅导中参考。本套书同时还可作为在校本科生、研究生以及社会各类科技人员参加各类国际资格证书考试、国外留学考试(如GRE)等的适用参考书。

我们相信,本套书的出版,将会对我国高等院校的学生、教师们提供丰富多彩、形式多样、卓有成效的参考资料。

出版者

2000年4月

PREFACE

Intent

The theory and methods of higher algebras are used in many branches of mathematics and in the fields of engineering and science. The study of modern algebra helps equip the reader with the devices and the reasoning skills necessary to solve such problems as encountered in these diverse areas.

This book provides a unified perspective; it helps in the comprehension of abstract algebra for both the student and the professional alike, either for those applying the theory to other fields or as a tutorial review of the subject.

It is designed to: (1) compile the classic topics of the field into a single reference; (2) identify selected significant theorems as well as canonical examples and counter-examples; (3) recommend some classical problems, such as may be encountered in a traditional undergraduate or graduate course of study or in preparation for preliminary examinations; and (4) present the interrelation of topics, as a launching point for the reader's own efforts to unify the concepts and discover a cohesion among the myriad theorems, definitions, and structures—a "big picture."

The intended purpose of this book is as a digest of foundations and insights into introductory, general material. It is effective especially as a supplement to other texts and authorities: those other resources which, though exhaustive, traditionally make no overtures to present the big picture—the existence of which is the main goal of this outline.

For more robust and detailed treatments of the many topics condensed here, the reader is referred to authoritative texts, where motivations and elucidations, can be found.

Moreover, since this study is introductory, it will not undertake more specialized or advanced topics (such as projective algebras, number theory, lattice theory, non-associative algebras, etc.). Matrices and linear algebra are appropriately introduced in their natural context of non-commutative rings, and are generalized in Chapter 5, on vectors; however, you will not study the mechanics of matrices in minutiae here, so as to avoid overlap with a more complete development as can be found in Schaum's Outline on Linear Algebra. Similarly, although an introduction to Galois Theory is covered in Chapter 8, it is by no means an exhaustive treatment of the theory of numbers and equations, which is better studied as an independent course.

A list of recommended readings on various related topics is provided in the bibliography.

The emphasis of this reference is on the core entities of modern abstract algebra, and the powerful methods it employs, from which the other forms and structures can be intuitively and automatically derived, and which permits us such liberal interpretation so as to obtain the primitive forms with which we are already familiar.

This "top down" approach is preferable in the study of higher mathematics, while it provides a complete comprehension of the subject in context and *in toto.*

Format

The book roughly adheres to the following scheme: the *structural entities* of a given topic will be defined, and illustrated by examples; the *devices employed* in developing the theory will be reviewed; then the *structure and dynamics* will be described by citing or demonstrating significant results/theorems, as well as typical problems and exercises. In attempting to unify the myriad concepts and synthesize them for ease of comprehension, it relies on the abundant use of heuristics, especially in the form of "quick notes," which are topic overviews that serve as indispensable study aids, to make the esoteric material accessible and obvious at a glance. This rigorous digest of the subject helps to render it more palatable.

Notation

Conventional notation will be employed whenever possible. The reader who is unfamiliar with the notation encountered here may refer to the glossary for this purpose. For example, with respect to maps, the relation $f: x \to y$, is denoted $f(x) = y$ (in contrast with the notations $xf = y$, or $x^f = y$); also, the terms *monomorphic* (*one-to-one*), *epimorphic* (*onto*), and *isomorphic* (*one-to-one correspondence*), are used to mean "injective," "surjective," and "bijective." Also, we will denote the natural numbers, for example, by either $\mathcal{N}$ or $\mathcal{Z}^+$ interchangeably. Generalized sums and products will be represented by the notations $\sum$, $\prod$ respectively.

Abbreviations are often employed ("e.g." rather than "for example"; "i.e." instead of "that is ... "; w.r.t in place of "with respect to ... "; w.l.o.g. written as an abbreviation of "without loss of generality") and QED is employed to designate the completion of a proof (the demonstration of that which was to be shown). On the other hand, the customary symbols of mathematical logic are omitted in favor of the more familiar "such that", "given any", etc.

Again, the reader is referred to the glossary for unfamiliar symbols, and is encouraged to become acquainted with them, as they will most likely be encountered again in future study.

Credits

My most heartfelt gratitude goes to those who have been steadfast in their encouragement and those who have contributed in grooming the resulting work, especially Dr. Peter Winkler at Bell Labs, for his unwaivering faith in my efforts, the reviewer and copy editor for their expert critique of the manuscript, to Mary Loebig Giles for her extraordinary professional support and astute guidance, to the fine staff at Techset, and to Maria and Louis Arangno, for ... everything.

INTRODUCTION

Once principally a discipline devoted to such fundamental problems as the solution of polynomial equations, algebra has gained appreciation in modern times for the elegance, power and versatility provided by its axiomatic approach. Often the rigorous logical methods of algebra prove as significant as the general solutions to problems obtained by them. To wit, no longer are compass and ruler required to determine roots of polynomial equations, once Galois Theory had been articulated, and suddenly quantum theory and computer technology are made possible, ... entirely through the devices, structures and methods of abstract algebra. Indeed, its importance in other branches of mathematics is only recently being fully appreciated, even as the modern algebra itself matures, but its immediate use for the student is readily apparent in his or her continued study.

Algebra provides the formal language by which we can describe systems and relationships, both practical and theoretical—from solutions to puzzles to quantum physics. The student is better equipped to formulate problems, approach their solution, and master abstract material in every discipline, when acquainted with algebraic forms and strategies.

责任编辑　林云裳
封面设计　王凌波
责任印制　杨　明

CONTENTS

Chapter 1

Rudiments

This chapter is devoted to establishing the key concepts upon which the study of Algebra is based. All the branches of Algebra stem from a logical framework, as a natural consequence of some very basic and familiar tools, namely; set theory, maps, and operations. (For a reliable reference on general set theory, refer to Halmos, or to Schaum's Outline series on *Discrete Mathematics*, *College Algebra*, and *Set Theory and Related Topics*.)

All subsequent algebraic systems, from the most basic to the most sophisticated, will rely on the axiomatic approach used to develop the familiar basic arithmetical systems which we will review in this chapter.

We will examine the development of those ordinary number systems, and the properties they exhibit, because we can generalize the axiomatic approach used in their construction to obtain more abstract number systems which all adhere to the same basic principles and general forms. We will also review the devices and tools that relate basic structures (called sets); specifically, maps, relations and operations.

Finally included are two significant results of elementary algebra; the existence of greatest common divisors, and the Fundamental Theorem of Arithmetic (the Unique Factorization Theorem), which we will encounter in more advanced study (such as in our discussion of Principal Ideal Domains).

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 denoted by a capital letter, conventional representations of a set include:

  braces: $A = \{$Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, Saturday$\}$

  $B = \{a, b, c, \ldots\}$

  "set builder" notation: $A = \{x | x$ is a day of the week$\}$

  $B = \{x | x$ is a small case letter of the alphabet$\}$

- All objects satisfying the conditions of membership in a given set A (that is, all objects displaying the properties defined by set A), are called *elements* of A.

  Written $x \in A$, we say "x is an element of A," "x belongs to A," or "x lies in A."

  We write $x \notin A$ if x is not an element of A.

- Two sets A, B are said to be *equal* if they contain the same elements, in which case, we write $A = B$. (That is, when we state $A = B$ we mean $x \in A$ iff $x \in B$.)
- The set which contains no elements is called the *empty set*, or the "null set," and is written $\varnothing = \{\ \}$. If a set A is *non-empty*, we denote this as $A \neq \varnothing$.
- We take all sets under consideration as being subsets of a *universal set*, U, which may or may not be explicitly defined, but often is implied from its context, and is understood to be the greatest set $U \neq \varnothing$ which contains all the elements being discussed.
- Given sets A and B, if every element of B also is 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 A contains other elements besides those in B (that is, there exists $x \in A$, such that $x \notin B$), we specify that B is a *proper subset* of A, written $B < A$.
- The collection of all the subsets of a specified set A is called the *power set* of A, and is denoted $\mathscr{P}(A) = \{S | S \subseteq A\}$.

  Observe that the empty set and the entire set A itself are elements of the power set of A.

EXAMPLE 1

(*a*) Given the set $A = \{a, b, c\}$, we can define its power set, $\mathscr{P}(A) = \{\varnothing, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, A\}$.
(*b*) $\mathscr{P}(\varnothing) = \{\varnothing\}$.

Operations on Sets

- Given sets A and B we define the following operations:
  - The *union* of sets A, B is defined as the set of all elements contained in *either A or B* (which does not preclude the possibility that there may exist elements in common to both sets); denoted by $A \cup B = \{x | x \in A \text{ or } x \in B\}$.

    We can also define the general union of sets $A_1, A_2, A_3, \ldots, A_n$, as $\bigcup_{i=1,\ldots,n} A_i$. (Note: "union" is the set theoretic equivalent of the logical "either/or", i.e., the logical sum.)
  - The *intersection* of sets A, B is defined as the set of all elements contained in *both A and B*; denoted by $A \cap B = \{x | x \in A \text{ and } x \in B\}$. (Note: "intersection" is the set theoretic equivalent of the logical "both/and", i.e., the logical difference.)
- We say the sets A, B are **disjoint** if their intersection is empty, that is $A \cap B = \varnothing$.
  - The *complement* of B in A is defined as the set of all elements which lie exclusively in A but not also in B; denoted $A - B = \{x | x \in A, x \notin B\}$.

    Conversely, the *complement* of A in B is defined as the set of all elements which lie in B but not also in A; denoted $B - A = \{x | x \in B, x \notin A\}$.

    Given a universal set U which contains both A and B, the complement of A is defined with respect to all the elements of U, denoted by $A^c \equiv A' = U - A = \{x \in U | x \notin A\}$. (The reader should verify also, that if a set A is a subset of B then $B^c \subseteq A^c$.)
- The following laws apply to the operations of the union and intersection of sets:

  Idempotent law: (*i*) $A \cup A = A$

  (*ii*) $A \cap A = A$

  Involution law: $(A^c)^c = A$

  In Exercise 1.1.1, we also prove:

Theorem 1.1.1 Laws of Operations with Sets:

(*i*) Commutative laws of $\cup$ and $\cap$:

$$A \cup B = B \cup A$$
$$A \cap B = B \cap A$$

(*ii*) Associative laws of $\cup$ and $\cap$:

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

(*iii*) Distributive laws:

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

The complementation of sets is governed by DeMorgan's Laws (illustrated in Example 9), which we demonstrate in Exercise 1.1.2:

Theorem 1.1.2 DeMorgan's Laws: Given (non-empty) sets A, B, C as subsets of a universal set U, the following laws of complementation hold:

(*i*) $(A \cup B)^c = A^c \cap B^c$
$(A \cap B)^c = A^c \cup B^c$

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

(These laws of set operations can also be reviewed in the Schaum's Outlines previously mentioned.)

- If two sets A, B have no elements in common, that is, their intersection is empty ($A \cap B = \varnothing$), we say they are *disjoint*; in which case, also, we observe that $A - B = A$, $B - A = B$, etc.
- If $A \cap B = A \cup B$, then $A = B$. This implies that $A = B = A \cap B = A \cup B$. That is, sets are equal if their union and intersection agree, in which case we can also write $A - B = \varnothing = B - A$.
- If two sets can be placed in one-to-one correspondence with each other, they are said to be "cardinally equivalent," that is, they have the same *cardinality*. (See section 1.2.1 for further discussion of one-to-one correspondences as maps between sets.)

EXAMPLE 2 Any set which can be placed in one-to-one correspondence with the set $\{1, 2, 3\}$ has precisely cardinality 3.

EXAMPLE 3 The set of even integers has the same cardinality as the set of odd integers.

EXAMPLE 4 Any set which has the cardinality of the natural numbers, $\mathcal{N}$, referred to as "aleph-0" ($\aleph_0$), is said to be "countable."

EXAMPLE 5 Any set which has the cardinality of the real numbers, $\Re$, referred to as "aleph-1" ($\aleph_1$), is said to be "uncountable."

EXAMPLE 6 The set given in Example 1, $A = \{a, b, c\}$, has cardinality 3, hence its power set, $\mathcal{P}(A) = \{\varnothing, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, A\}$, has cardinality $2^3 = 8$.

EXAMPLE 7 In general, if a set A has cardinality n, then its power set has cardinality 2^n.

Venn diagrams

- Venn diagrams (Fig. 1-1) provide a pictorial representation of sets A, B within a given universal set U.

  Inspection of such an illustration of sets helps us to visually identify and describe the regions containing elements resulting from operations between those sets, as depicted in the following examples.

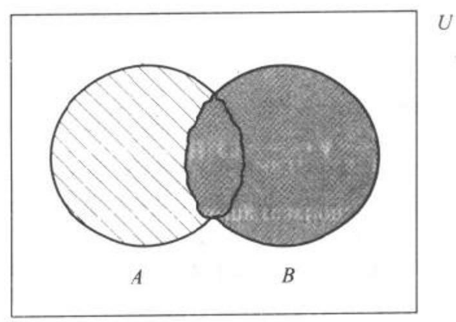

Fig. 1-1

EXAMPLE 8 Figure 1-2 shows examples of Venn diagrams in illustrating operations between sets:

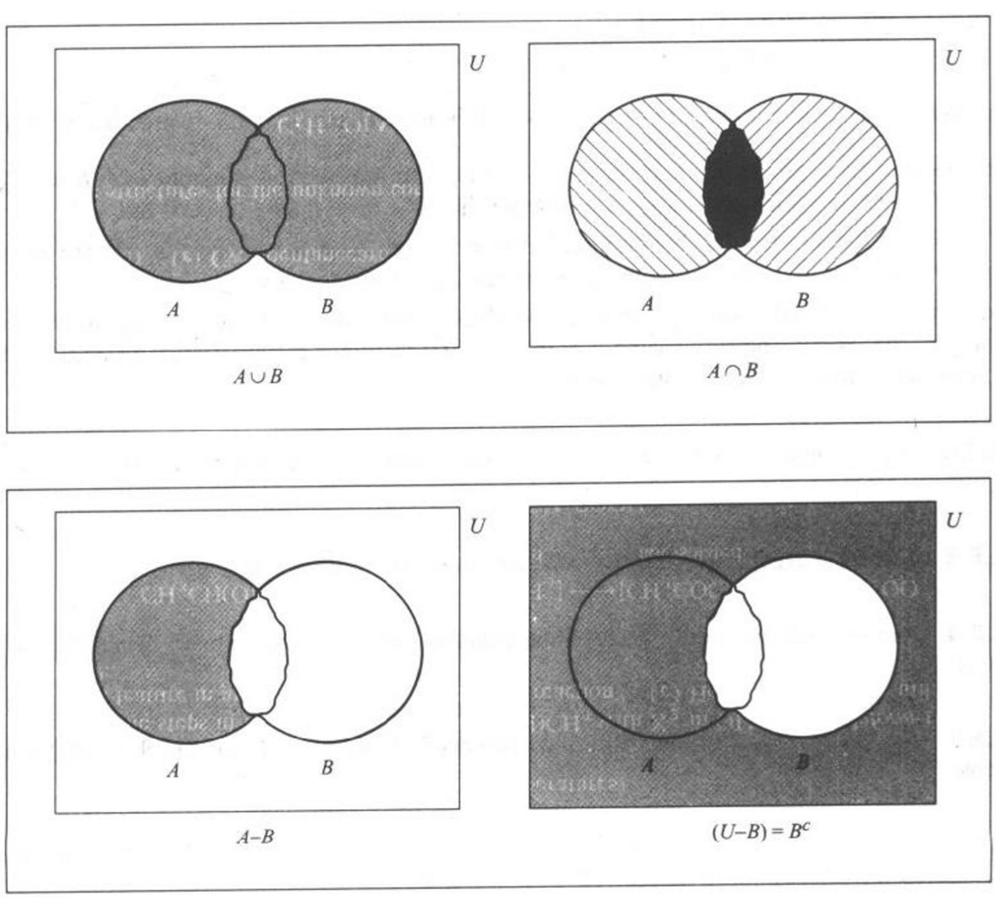

Fig. 1-2

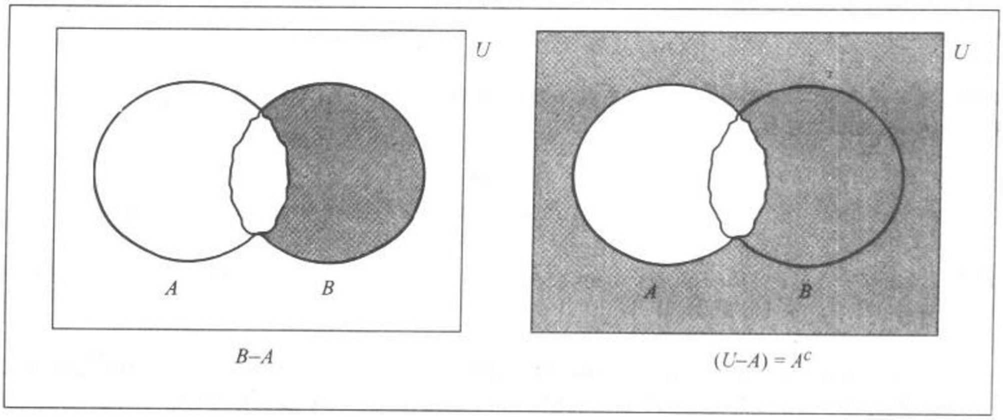

Fig. 1-2 *(Cont.)*

EXAMPLE 9 An example of DeMorgan's First Law (Fig. 1-3).

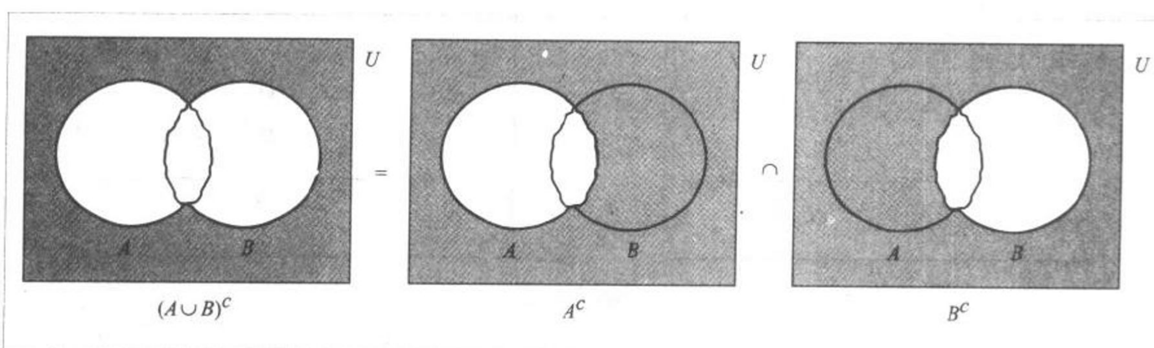

Fig. 1-3

Important Note: Be cautious not to mistake the use of Venn diagrams as proof of a claim; such diagrams are intended to be heuristic only, to serve to illustrate the operations involved.

Partition of a Set

- A set $\{A_i\}_{i=1,\ldots,n}$ of non-empty subsets of a given set A, which are *pair-wise disjoint*, and whose union equals all of A, is called a *partition* of A.

  Specifically, we say that A is the "disjoint union" of those subsets, denoted by $A = \overline{\bigcup}_{i=1,n} A_i$, (since $A_i \cap A_j = \emptyset$ for each pair of indices, $i \neq j$).

EXAMPLE 10 If $\{B, C\}$ is a partition of a set A, then $B \cup C = A$, and $B \cap C = \emptyset$. Observe moreover, that:

- $B - C = B$
- $C^c = A - C = B$ $\qquad$ $C^c = A - C = B$
- $B^c \cup C^c = A$

There exist more than one partition of a given set.

(*Note*: This is an important concept not only in the study of Algebra, but also in Analysis and Topology.)

Cartesian Product

- Given two sets A and B, we define the *Cartesian product*, $A \times B$, to be the set of ordered pairs (x, y) such that $x \in A$, and $y \in B$.

  Specifically, we write the product set as $A \times B = \{(x, y) | x \in A; y \in B\}$

  We note that elements (a, b), $(a', b') \in A \times B$ are "equal" if and only if $a = a'$ and $b = b'$.

EXAMPLE 11 Let $A = \{1, 2\}$, $B = \{3, 4\}$; then $A \times B = \{(1, 3), (1, 4), (2, 3), (2, 4)\}$, which is distinct from the product set $B \times A = \{(3, 1), (4, 1), (3, 2), (4, 2)\}$.

Note: We can represent these sets of ordered pairs as points in the real plane (which is itself the product set $\mathfrak{R} \times \mathfrak{R}$), using the Cartesian coordinate system, as shown in Fig. 1-4.

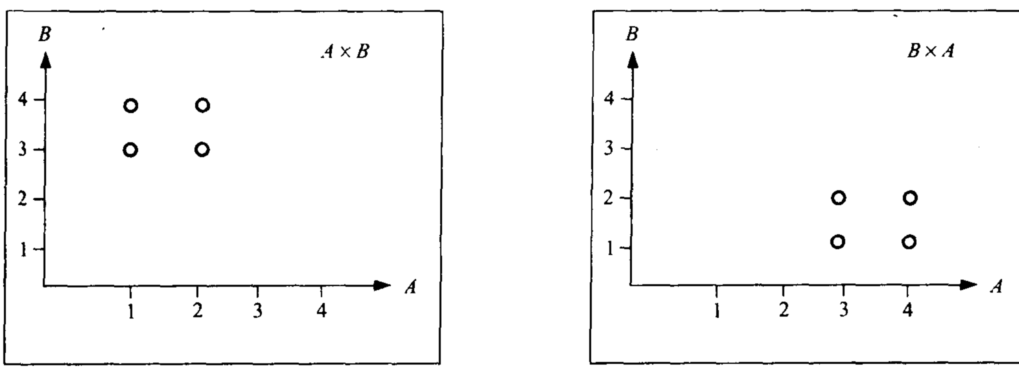

Fig. 1-4

EXAMPLE 12 Given sets $A = \{x | 0 \leq x \leq 4\}, B = \{y | y = x\}$, then $A \times B$ can be represented by the graph in Fig. 1-5.

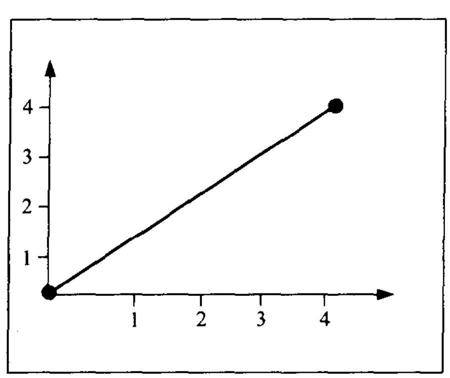

Fig. 1-5

Note: Our familiar representation of "functions," to be examined in the next section, relies on this construct of the Cartesian product of sets, and moreover, we are already acquainted with a geometric interpretation of functions defined over the real numbers $\mathfrak{R}$ as "graphs" on the real plane, $\mathfrak{R} \times \mathfrak{R}$, i.e., as subsets of that greater product set, using "Cartesian coordinates."