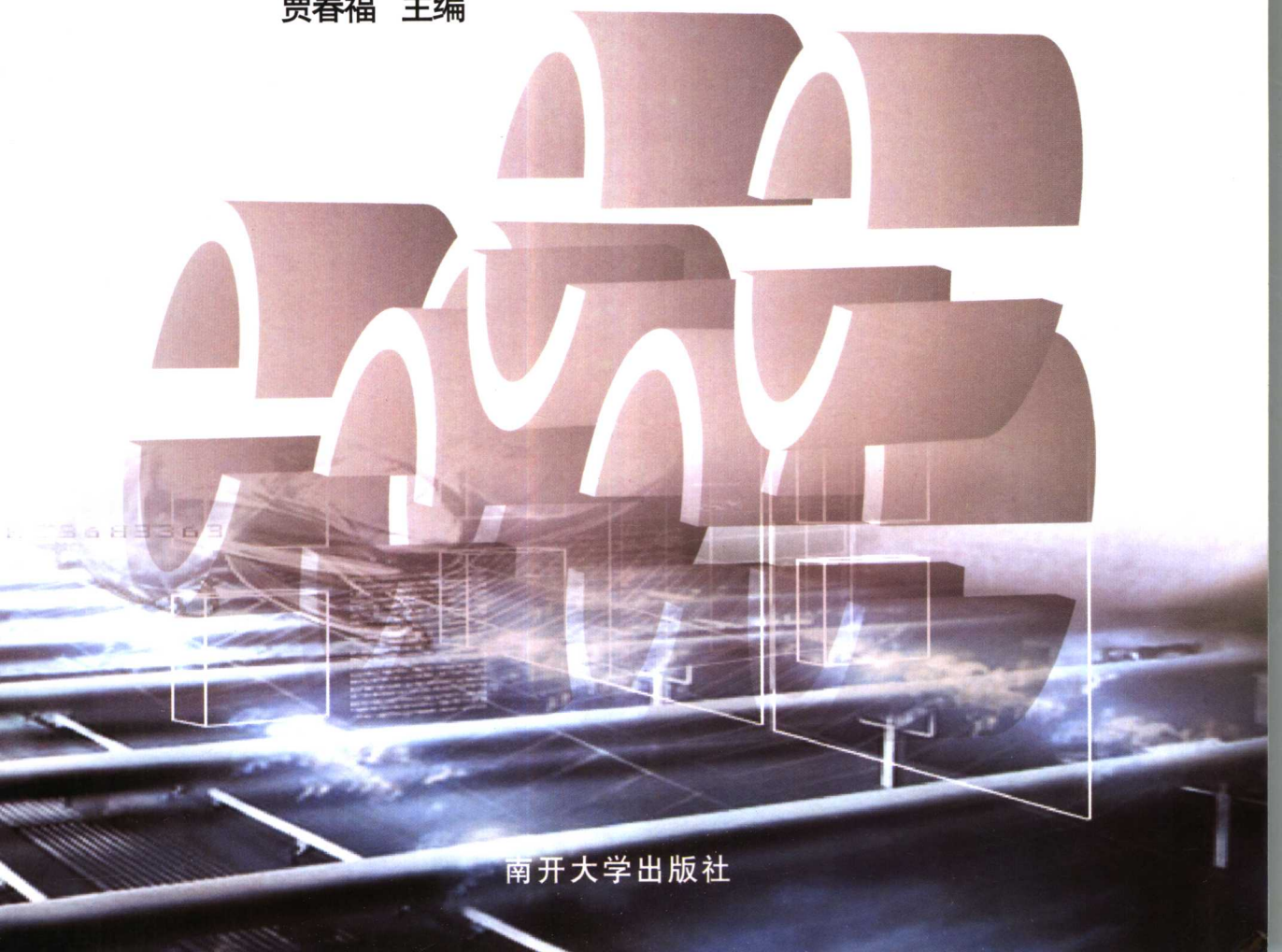
高等院校信息安全专业系列教材

信息安全数学基础

贾春福 主编



南开大学出版社

高等院校信息安全专业系列教材

信息安全数学基础

贾春福　主编

南开大学出版社
天津

内容简介

本书系统地介绍了信息安全理论与技术所涉及的数论、代数、椭圆曲线等数学理论基础。全书共分为5章：第1章是预备知识，介绍了书中内容所涉及的基础知识；第2章是数论基础，包括整数的因子分解，同余式，原根，二次剩余，连分数和素性检验等内容；第3章是代数系统基础，包括代数系统的基本概念，群、环、域的概念，一元多项式环和有限域理论初步等内容；第4章是椭圆曲线，包括椭圆曲线的预备知识，椭圆曲线，椭圆曲线上的离散对数等内容；第5章是反馈移位寄存器，包括反馈移位寄存器，分圆和本原多项式，m序列等内容。书中每章末都配有习题，以供学生学习和复习巩固所学内容。

本书是高等学校信息安全专业本科生的教材，也可作为信息科学技术类专业（如计算机科学技术、通信工程和电子科学技术等）本科生和研究生的教材，还可以供从事信息安全和其他信息技术工作的人员参考。

图书在版编目(CIP)数据

信息安全数学基础/贾春福主编. —天津：南开大学出版社，2006.5

（高等院校信息安全专业系列教材）

ISBN 7-310-02530-X

Ⅰ.信… Ⅱ.贾… Ⅲ.信息系统—安全技术—应用数学—高等学校—教材 Ⅳ.TP309

中国版本图书馆CIP数据核字(2006)第009409号

南开大学出版社出版发行

出版人：肖占鹏

地址：天津市南开区卫津路94号 邮政编码：300071

营销部电话：(022)23508339 23500755

营销部传真：(022)23508542 邮购部电话：(022)23502200

*

天津市宝坻区第二印刷厂印刷

全国各地新华书店经销

*

2006年5月第1版 2006年5月第1次印刷

787×1092毫米 16开本 13印张 323千字

定价：24.00元

如遇图书印装质量问题，请与本社营销部联系调换，电话：(022)23507125

前 言

随着信息技术的飞速发展，人们的生活和工作方式发生了极大的改变，计算机和通信网络已经渗透到了整个社会的各个领域。因此，信息安全问题也更多地受到关注：信息安全理论和技术已经成为信息科学与技术中极为重要的研究领域；信息安全专门人才的培养受到高度重视。

“信息安全数学基础”是新兴的“信息安全”本科专业的专业必修基础课，对信息安全理论和技术的深入学习和研究具有重要的意义。本书是在南开大学信息安全专业“信息安全数学基础”课程授课讲义的基础上整理而成的。全书共分为 5 章：第 1 章是预备知识，介绍了书中内容所涉及的基础知识；第 2 章是数论基础，包括整数的因子分解，同余式，原根，二次剩余，连分数和素性检验等内容；第 3 章是代数系统基础，包括代数系统的基本概念，群、环、域的概念，一元多项式环和有限域理论初步等内容；第 4 章是椭圆曲线，包括椭圆曲线的预备知识，椭圆曲线，椭圆曲线上的离散对数等内容；第 5 章是反馈移位寄存器，包括反馈移位寄存器，分圆和本原多项式，m 序列等内容。书中每章末都配有习题，以供学生学习和复习巩固所学内容时使用。

在本书的编写过程中，我们力求知识系统化、容易理解。对书中内容所涉及的基础预备知识作了简明扼要的介绍；书中所涉及的数学结论都给出了详细的证明；书中的内容力图较好地覆盖信息安全领域所涉及的数学基础知识；习题的配置着力于帮助学生巩固所学的内容。本书适合高等学校信息安全、计算机科学技术和通信工程等专业本科生和研究生使用，也可供相关领域的科研人员和技术人员参考。

本书由贾春福、钟安鸣、孙旭和段雪涛编写。高敏芬老师、杨峰、付玉冰、马勇和袁强等同学参与了书稿的校对工作，在此表示感谢。另外，本书是南开大学重点教材资助项目，在此对南开大学有关审批部门也表示衷心的感谢。

由于时间仓促，书中难免有疏漏和不当之处，敬请读者批评指正。

编 者

2005 年 9 月

目 录

第1章　预备知识

本章是与书中后面几章内容相关的预备知识的介绍，包括集合论基础、排列与组合和生成函数等内容.

1.1　集合论基础

集合论是德国著名数学家康托尔(Georg Cantor)于 19 世纪末创立的，称为朴素集合论，它是现代数学的基础. 20 世纪初，策梅罗(Zermelo)列出了第一个集合论的公理系统，在此基础上逐步形成了公理化集合论和抽象集合论，使该学科成为在数学中发展最快的一个分支. 现在，集合论观点已经渗透到了古典分析、泛函、概率和信息论等各个领域. 本节将介绍集合论的基础知识，包括集合与关系、集合运算、函数和基数的概念.

1.1.1 集合

1. 集合的概念

集合的概念是现代数学中最基本的概念之一. 一般来讲，把具有共同性质的一些事物汇集成一个整体，就形成一个**集合**. 这些事物称为**元素**或**成员**. 例如，所有 0 和 1 之间的实数，教室里的所有椅子，图书馆里的所有藏书都构成一个集合. 通常用大写英文字母 A, B, … 表示集合，小写英文字母 $a, b, \cdots$ 表示集合中的元素. 若元素 a 是集合 S 中的元素，则记作 $a \in S$，读作 a 属于 S，或 a 在 S 之中. 若元素 a 不是集合 S 中的元素，记作 $a \notin S$，读作 a 不属于 S，或 a 不在 S 之中.

对于一个集合 S，如果它是由有限个元素组成的，称 S 为**有限集**；否则称 S 为**无限集**.

集合通常有两种表示方法. 第一种方法是把集合中的元素列举出来，称作**列举法**. 例如

$$A = \{a, b, c, d\}, \quad B = \{1, 2, 3, \cdots\}.$$

第二种方法称为**叙述法**，即用一种规则来限定某个元素是否属于该集合. 例如

$$S_1 = \{x \mid x\text{是正整数}\}, \quad S_2 = \{x \mid x \in N \wedge x \leqslant 9\}, \quad S_3 = \{x \mid x \in R \wedge 5x^2 - 1 = 0\},$$

其中“$\wedge$”表示“且”.

定义 1.1.1　设 A, B 是任意两个集合，假如 A 的每一个元素都是 B 的成员，则称 A 为 B 的**子集**，记作 $A \subseteq B$ 或 $B \supseteq A$，读作 A **包含于** B，或 B **包含** A. 符号化表示为

$$A \subseteq B \Leftrightarrow (\forall x)(x \in A \rightarrow x \in B),$$

其中“$\forall$”表示“任意”，“$\Leftrightarrow$”表示命题“等价”，“$\rightarrow$”表示“蕴涵”(命题内).

例如，设 $\mathbf{N}$ 为自然数集，$\mathbf{Q}$ 为有理数集，$A=\{1,2,3\}$，$B=\{1\}$，则

$$A\subseteq\mathbf{N},\quad B\subseteq A,\quad B\subseteq\mathbf{N},\quad \mathbf{N}\subseteq\mathbf{Q}.$$

定义 1.1.2 如果集合 A 的每一个元素都属于 B，但集合 B 中至少有一个元素不属于 A，则称 A 为 B 的**真子集**，记作 $A\subset B$，读作 A **真包含于** B，或 B **真包含** A. 符号化表示为

$$A\subset B\Leftrightarrow A\subseteq B\wedge A\neq B,$$

$$A\subset B\Leftrightarrow(\forall x)(x\in A\rightarrow x\in B)\wedge(\exists x)(x\in B\wedge x\notin A).$$

例如，整数集是有理数集的真子集.

定义 1.1.3 设 A，B 是任意给定的两个集合，如果 $A\subseteq B$ 且 $B\subseteq A$，则称集合 A 和集合 B **相等**，记作 $A=B$. 符号化表示为

$$A=B\Leftrightarrow A\subseteq B\wedge B\subseteq A,$$

否则，称 A 与 B **不相等**，记作 $A\neq B$.

例如，若 $A=\{3,6,9\}$，$B=\{6,9,3\}$，$C=\{3,9\}$，则 $A=B$，$A\neq C$.

从这个例子中可以看出，集合中元素的排列顺序是无关紧要的.

定义 1.1.4 不含任何元素的集合称为**空集**，记作 $\varnothing$. 符号化表示为

$$\varnothing=\{x\mid p(x)\wedge\sim p(x)\},$$

其中 $p(x)$ 是任意谓词(谓词是用来描述客体的性质或关系的语句)，“$\sim$”表示“否”.

定理 1.1.1 对于任意一个集合 A，$\varnothing\subseteq A$.

证明 假设 $\varnothing\subseteq A$ 是假，则至少存在一个元素 x，使 $x\in\varnothing$ 且 $x\notin A$. 因为空集 $\varnothing$ 不包含任何元素，所以假设不成立. 定理得证.

由空集和子集的定义可知，对于每个非空集合 A，至少有两个不同的子集 A 和 $\varnothing$. 我们称 A 和 $\varnothing$ 是 A 的**平凡子集**.

定理 1.1.2 空集是唯一的.

证明 用反证法. 假设存在两个空集 $\varnothing_1$ 和 $\varnothing_2$. 因为空集被包含于每一个集合中，于是有

$$\varnothing_1\subseteq\varnothing_2\text{且}\varnothing_2\subseteq\varnothing_1,$$

故 $\varnothing_1=\varnothing_2$，即空集是唯一的.

定义 1.1.5 给定集合 A，由集合 A 的所有子集组成的集合称为集合 A 的**幂集**，记作 $\rho(A)$ 或 2^A，

$$\rho(A)=\{B\mid B\subseteq A\}.$$

例如，对于 $A=\{a,b,c\}$，我们有 $\rho(A)=\{\varnothing,\{a\},\{b\},\{c\},\{a,b\},\{b,c\},\{a,c\},\{a,b,c\}\}$.

定义 1.1.6 在一定范围内，如果所有集合均为某一集合的子集，则称该集合为**全集**，记作 E.

对于任一 $x\in A$，因为 $A\subseteq E$，故 $x\in E$. 符号化表示为

$$E=\{x\mid p(x)\vee\sim p(x)\},$$

其中 $p(x)$ 是任意谓词，“$\vee$”表示“或”.

全集是一个相对的概念，研究的问题不同，所取的全集也往往不同.

2. 集合运算

集合的运算就是以给定集合为对象，按照确定的规则得到另外一些集合. **文氏图**(Venn Diagram)可以直观、形象地表示集合间的关系及运算结果. 在文氏图中，通常用一个矩形表

示全集 E，然后在矩形的内部画一些圆(或其他封闭的曲线)，圆的内部代表集合，不同的圆代表不同的集合.

定义 1.1.7　设任意两个集合 A 和 B，由集合 A 和 B 的所有共同元素组成的集合 S，称为 A 和 B 的**交集**，记作 $A\cap B$. 显然

$$S=A\cap B=\{x\mid x\in A\wedge x\in B\}.$$

其文氏图如图 1.1.1 所示.

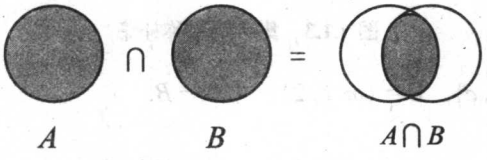


图 1.1.1　集合的交集

例 1.1.1　设 $A=\{0,2,a,7,c\}$，$B=\{r,m,0,c,2\}$，求 $A\cap B$.

解　$A\cap B=\{0,2,c\}$.

例 1.1.2　设 $A\subseteq B$，C 是任意集合，求证 $A\cap C\subseteq B\cap C$.

证明　由 $A\subseteq B$ 可知，若 $x\in A$，则 $x\in B$. 对于任意的 $x\in A\cap C$，由 $\cap$ 的定义，有 $x\in A$ 且 $x\in C$，即 $x\in B$ 且 $x\in C$，故 $x\in B\cap C$. 因此，$A\cap C\subseteq B\cap C$.

定义 1.1.8　设任意两个集合 A 和 B，所有属于 A 或属于 B 的元素组成的集合 S，称为 A 和 B 的**并集**，记作 $A\cup B$. 显然

$$S=A\cup B=\{x\mid x\in A\vee x\in B\}.$$

文氏图表示如图 1.1.2.

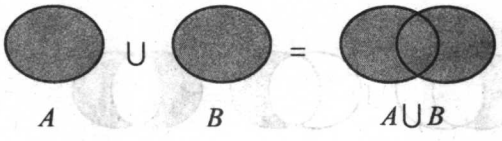


图 1.1.2　集合的并集

例 1.1.3　设 $A=\{a,2\}$，$B=\{2,m\}$，求 $A\cup B$.

解　$A\cup B=\{a,2,m\}$.

例 1.1.4　设 $A\subseteq B$，$C\subseteq D$，求证 $A\cup C\subseteq B\cup D$.

证明　对任意 $x\in A\cup C$，有 $x\in A$ 或 $x\in C$. 若 $x\in A$，则由 $A\subseteq B$，有 $x\in B$，故 $x\in B\cup D$. 若 $x\in C$，则由 $C\subseteq D$，有 $x\in D$，故 $x\in B\cup D$. 因此，$A\cup C\subseteq B\cup D$.

例 1.1.5　求证下列命题.

(1)　$A\subseteq B$，当且仅当 $A\cup B=B$；

(2)　$A\subseteq B$，当且仅当 $A\cap B=A$.

证明　(1) 若 $A\subseteq B$，则对任意的 $x\in A$，必有 $x\in B$. 又由于对任意的 $x\in A\cup B$，有 $x\in A$ 或 $x\in B$，故 $x\in B$，所以 $A\cup B\subseteq B$. 又 $B\subseteq A\cup B$，于是得到 $A\cup B=B$. 反之，若 $A\cup B=B$，因为 $A\subseteq A\cup B$，所以 $A\subseteq B$.

(2) 其证明过程与(1)类似.

定义 1.1.9　设任意两个集合 A 和 B，所有属于 A 而不属于 B 的一切元素组成的集合 S，称为 B 对 A 的**补集**，或称**对称补**，记作 $A-B$. 显然

$$S = A - B = \{x \mid x \in A \wedge x \notin B\} = \{x \mid x \in A \wedge \sim (x \in B)\}.$$

$A - B$ 也称为集合 A 和 B 的**差**. 文氏图表示见图 1.1.3.

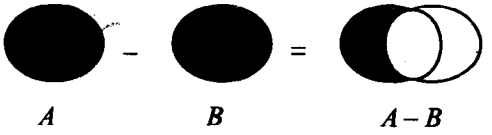


图 1.1.3 集合的对称补集

例 1.1.6 设 $A = \{a, 7, c\}$, $B = \{m, c, 2\}$, 求 $A - B$.

解 $A - B = \{a, 7\}$.

定义 1.1.10 设 E 为全集, 对任一集合 A 关于 E 的补集 $E - A$, 称为集合 A 的**绝对补**, 记作 $\sim A$. 显然

$$\sim A = E - A = \{x \mid x \in E \wedge x \notin A\}.$$

例 1.1.7 设 A, B 为任意两个集合, 则 $A - B = A \cap \sim B$.

证明 对于任意的 x, 有

$$x \in A - B \Leftrightarrow x \in A \wedge x \notin B \Leftrightarrow x \in A \wedge x \in \sim B \Leftrightarrow x \in A \cap \sim B,$$

所以 $A - B = A \cap \sim B$.

定义 1.1.11 设任意两个集合 A 和 B, A 和 B 的**对称差**为集合 S, 其元素或属于 A, 或属于 B, 但不能既属于 A 又属于 B, 记作 $A \oplus B$. 显然

$$S = A \oplus B = (A - B) \cup (B - A) = \{x \mid (x \in A \wedge x \notin B) \vee (x \in B \wedge x \notin A)\}.$$

文氏图表示如图 1.1.4 所示.

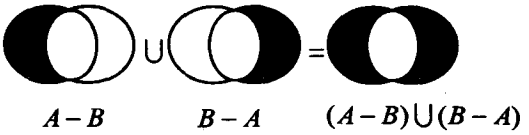


图 1.1.4 集合的对称差集

例 1.1.8 设 $A = \{4, 6, 8\}$, $B = \{1, 4, 8\}$, 求 $A \oplus B$.

解 $A \oplus B = \{1, 6\}$.

下面给出集合性质中最主要的几条定律.

定理 1.1.3 设 A, B, C 是全集 E 的任意子集.

(1) 幂等律 $A \cup A = A$

$A \cap A = A$

(2) 交换律 $A \cup B = B \cup A$

$A \cap B = B \cap A$

$A \oplus B = B \oplus A$

(3) 结合律 $(A \cup B) \cup C = A \cup (B \cup C)$

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

$(A \oplus B) \oplus C = A \oplus (B \oplus C)$

(4) 分配律　$A\cup(B\cap C)=(A\cup B)\cap(A\cup C)$

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

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

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

(5) 同一律　$A\cup\varnothing=A$

$A\cap E=A$

$A-\varnothing=A$

$A\oplus\varnothing=A$

(6) 零律　$A\cup E=E$

$A\cap\varnothing=\varnothing$

(7) 互补律　$A\cup\sim A=E$

$A\cap\sim A=\varnothing$

$\sim E=\varnothing$

$\sim\varnothing=E$

(8) 吸收律　$A\cup(A\cap B)=A$

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

(9) 摩根定律　$\sim(A\cup B)=\sim A\cap\sim B$

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

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

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

(10) 双重否定律　$\sim(\sim A)=A$

(11) $A\oplus A=\varnothing$　$A-A=\varnothing$　$A\cap B\subseteq A$　$A\cap B\subseteq B$

(12) $A\subseteq A\cup B$　$B\subseteq A\cup B$　$A-B\subseteq A$　$A-B=A\cap\sim B$

(13) $A\oplus B=(A-B)\cup(B-A)=(A\cup B)-(A\cap B)=(A\cap\sim B)\cup(\sim A\cap B)$

对于上面的集合基本定律，下面以例题的形式证明其中的一部分，其余留给读者完成.

例 1.1.9　证明幂等律 $A\cup A=A$.

证明　对于任意的 x，有

$$x\in A\cup A\Leftrightarrow x\in A\vee x\in A\Leftrightarrow x\in A,$$

所以 $A\cup A=A$.

例 1.1.10　证明交换律 $A\cap B=B\cap A$.

证明　对于任意的 x，有

$$x\in A\cap B\Leftrightarrow x\in A\wedge x\in B\Leftrightarrow x\in B\wedge x\in A\Leftrightarrow x\in B\cap A,$$

所以 $A\cap B=B\cap A$.

例 1.1.11　证明分配律 $A\cap(B\cup C)=(A\cap B)\cup(A\cap C)$.

证明　对于任意给定的 x，有

$$\begin{aligned}x\in A\cap(B\cap C)&\Leftrightarrow x\in A\wedge x\in(B\cup C)\\&\Leftrightarrow x\in A\wedge(x\in B\vee x\in C)\\&\Leftrightarrow(x\in A\wedge x\in B)\vee(x\in A\wedge x\in C)\\&\Leftrightarrow(x\in A\cap B)\vee(x\in A\cap C)\\&\Leftrightarrow x\in(A\cap B)\cup(A\cap C)\end{aligned}$$

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

例 1.1.12 证明吸收律 $A\cup(A\cap B)=A$.

证明 $A\cup(A\cap B)=(A\cap E)\cup(A\cap B)=A\cap(E\cup B)=A\cap E=A$.

例 1.1.13 证明摩根定律 $\sim(A\cup B)=\sim A\cap\sim B$.

证明

$$\sim(A\cup B)=\{x\mid x\in\sim(A\cup B)\}=\{x\mid x\notin A\cup B\}=\{x\mid x\notin A\wedge x\notin B\}$$
$$=\{x\mid(x\in\sim A)\wedge(x\in\sim B)\}=\sim A\cap\sim B$$

例 1.1.14 证明分配律 $A\cap(B-C)=(A\cap B)-(A\cap C)$.

证明 由于

$$A\cap(B-C)=A\cap(B\cap\sim C)=A\cap B\cap\sim C,$$

又

$$\begin{aligned}(A\cap B)-(A\cap C)&=(A\cap B)\cap\sim(A\cap C)\\&=(A\cap B)\cap(\sim A\cup\sim C)\\&=(A\cap B\cap\sim A)\cup(A\cap B\cap\sim C)\\&=\varnothing\cup(A\cap B\cap\sim C)\\&=A\cap B\cap\sim C\end{aligned}$$

故可知 $A\cap(B-C)=(A\cap B)-(A\cap C)$.

1.1.2 关系

关系的概念在日常生活中是普遍存在的，如师生关系、朋友关系、同学关系等. 在数学上，关系可以表达集合中元素间的联系. 在介绍关系的概念以前，我们首先介绍一下序偶和笛卡儿积的概念.

定义 1.1.12 由两个具有给定次序的个体 x 和 y（允许 $x=y$）所组成的序列，称为**序偶**，记作 $<x, y>$. 其中 x 称为**第一分量**，y 称为**第二分量**.

序偶可以看作是具有两个元素的集合，但它与一般集合不同的是，序偶具有确定的次序. 例如，在集合中 $\{a, b\}=\{b, a\}$，但对于序偶 $<a, b>\neq<b, a>$.

定义 1.1.13 设 $<a, b>$, $<x, y>$ 是两个序偶，则 $<a, b>=<x, y>$ 当且仅当 $a=x$ 且 $b=y$.

定义 1.1.14 由 n 个具有给定次序的个体 $a_1, a_2, \cdots, a_n$ 组成的序列，称为**有序 n 元组**，记作 $<a_1, a_2, \cdots, a_n>$.

有序 n 元组的实质依然是序偶，可将其表示为

$$<a_1, a_2, \cdots, a_n>=<<a_1, a_2, \cdots, a_{n-1}>, a_n>=\cdots=<<<\cdots<<a_1, a_2>, a_3>, \cdots>, a_{n-1}>, a_n>,$$

其中 a_i 称为第 i 个分量. $<a_1, a_2, \cdots, a_n>=<b_1, b_2, \cdots, b_n>$ 当且仅当 $a_i=b_i$ $(i=1, 2, \cdots, n)$.

定义 1.1.15 设 $A_1, A_2, \cdots, A_n$ 是任意给定的 n 个集合，若有序 n 元组 $<a_1, a_2, \cdots, a_n>$ 的第一个分量是取自集合 A_1 里的元素，第二个分量是取自集合 A_2 里的元素，$\cdots$，第 n 个分量是取自集合 A_n 里的元素，则由所有这样的有序 n 元组所组成的集合称为集合 $A_1, A_2, \cdots, A_n$ 的**笛卡儿积**，并用 $A_1\times A_2\times\cdots\times A_n$ 表示，即

$$A_1\times A_2\times\cdots\times A_n=\{<a_1, a_2, \cdots, a_n>\mid a_i\in A_i,\ i=1,2,\cdots,n\}.$$

特别地，两个集合的笛卡儿积可以叙述为：任意给定两个集合 A 和 B，若序偶的第一个分量是 A 的元素，第二个分量是 B 的元素，则所有这样的序偶的集合称为 A 和 B 的笛卡儿积或直积，记作 $A\times B$，即

$$A\times B=\{<x,y>\mid x\in A\wedge y\in B\}.$$

例 1.1.15　设 $A=\{0,1\}$，$B=\{a,b\}$，$C=\varnothing$，则

$$A\times B=\{<0,a>,<0,b>,<1,a>,<1,b>\},$$
$$B\times A=\{<a,0>,<a,1>,<b,0>,<b,1>\},$$
$$A\times A=\{<0,0>,<1,1>,<1,0>,<0,1>\},$$
$$B\times B=\{<a,a>,<b,b>,<a,b>,<b,a>\},$$
$$A\times C=\varnothing,$$
$$C\times A=\varnothing.$$

显然，$A\times B\neq B\times A$，即笛卡儿积不满足交换律.

例 1.1.16　设 $A=\{1\}$，$B=\{a,b\}$，$C=\{x,y\}$，则

$$(A\times B)\times C=\{<<1,a>,x>,<<1,a>,y>,<<1,b>,x>,<<1,b>,y>\},$$
$$A\times(B\times C)=\{<1,<a,x>>,<1,<a,y>>,<1,<b,x>>,<1,<b,y>>\}.$$

显然，$(A\times B)\times C\neq A\times(B\times C)$，即笛卡儿积不满足结合律.

定理 1.1.4　笛卡儿积的性质如下：

(1) 交换律不成立，即当 $A\neq B$ 时，$A\times B\neq B\times A$.

(2) 结合律不成立，即 $(A\times B)\times C\neq A\times(B\times C)$.

(3) 下列分配律是成立的：

① $A\times(B\cup C)=(A\times B)\cup(A\times C)$；

② $A\times(B\cap C)=(A\times B)\cap(A\times C)$；

③ $(A\cup B)\times C=(A\times C)\cup(B\times C)$；

④ $(A\cap B)\times C=(A\times C)\cap(B\times C)$；

⑤ $A\times(B-C)=(A\times B)-(A\times C)$；

⑥ $(A-B)\times C=(A\times C)-(B\times C)$.

(4) 若 $C\neq\varnothing$，则 $A\subseteq B\Leftrightarrow(A\times C\subseteq B\times C)\Leftrightarrow(C\times A\subseteq C\times B)$.

(5) 设 A,B,C,D 是四个非空集合，则 $A\times B\subseteq C\times D$ 当且仅当 $A\subseteq C$ 且 $B\subseteq D$.

例 1.1.17　证明分配率 $A\times(B\cup C)=(A\times B)\cup(A\times C)$.

证明　对任意的 $<x,y>$，有

$$\begin{aligned}<x,y>\in A\times(B\cup C)&\Leftrightarrow x\in A\wedge y\in(B\cup C)\\&\Leftrightarrow x\in A\wedge(y\in B\vee y\in C)\\&\Leftrightarrow(x\in A\wedge y\in B)\vee(x\in A\wedge y\in C)\\&\Leftrightarrow<x,y>\in A\times B\vee<x,y>\in A\times C\\&\Leftrightarrow<x,y>\in(A\times B)\cup(A\times C)\end{aligned}$$

所以

$$A\times(B\cup C)=(A\times B)\cup(A\times C).$$

例 1.1.18　证明分配率 $(A\cap B)\times C=(A\times C)\cap(B\times C)$.

证明　对任意的 $<x,y>$，有

$$\begin{aligned}<x,y>\in(A\cap B)\times C &\Leftrightarrow x\in(A\cap B)\wedge y\in C\\ &\Leftrightarrow(x\in A\wedge x\in B)\wedge y\in C\\ &\Leftrightarrow(x\in A\wedge y\in C)\wedge(x\in B\wedge y\in C)\\ &\Leftrightarrow<x,y>\in A\times C\wedge<x,y>\in B\times C\\ &\Leftrightarrow<x,y>\in(A\times C)\cap(B\times C)\end{aligned}$$

所以

$$(A\cap B)\times C=(A\times C)\cap(B\times C).$$

例 1.1.19 设 A,B,C 是三个任意集合，且 $C\neq\varnothing$，则 $A\subseteq B$ 当且仅当 $A\times C\subseteq B\times C$.

证明 先证必要性. 设 $A\subseteq B$ 成立，则对任意的 x，若 $x\in A$，则必有 $x\in B$. 现对任意的$<x,y>$，有

$$<x,y>\in A\times C\Leftrightarrow x\in A\wedge y\in C\Rightarrow x\in B\wedge y\in C\Leftrightarrow<x,y>\in B\times C,$$

所以 $A\times C\subseteq B\times C$.

再证充分性. 设 $A\times C\subseteq B\times C$ 成立，因为 $C\neq\varnothing$，故存在 $y\in C$. 对于任意的 x，有

$$x\in A\Rightarrow x\in A\wedge y\in C\Leftrightarrow<x,y>\in A\times C\Rightarrow<x,y>\in B\times C\Leftrightarrow x\in B\wedge y\in C\Rightarrow x\in B,$$

其中“$\Rightarrow$”表示“蕴涵”（命题间），所以 $A\subseteq B$. 证毕.

例 1.1.20 设 A,B,C,D 是四个非空集合，则 $A\times B\subseteq C\times D$ 当且仅当 $A\subseteq C$ 且 $B\subseteq D$.

证明 先证必要性. 设 $A\times B\subseteq C\times D$ 成立，则对任意的 $x\in A$ 和 $y\in B$，有

$$x\in A\wedge y\in B\Leftrightarrow<x,y>\in A\times B\Rightarrow<x,y>\in C\times D\Leftrightarrow x\in C\wedge y\in D,$$

所以 $A\subseteq C$ 且 $B\subseteq D$.

再证充分性. 设 $A\subseteq C$ 且 $B\subseteq D$ 成立，则对任意的 $x\in A$ 和 $y\in B$，有

$$<x,y>\in A\times B\Leftrightarrow x\in A\wedge y\in B\Rightarrow x\in C\wedge y\in D\Leftrightarrow<x,y>\in C\times D,$$

所以 $A\times B\subseteq C\times D$. 证毕.

定义 1.1.16 设 $A_1,A_2,\cdots,A_n$ 是任意给定的集合，笛卡儿积 $A_1\times A_2\times\cdots\times A_n$ 的任何一个子集 R 称为 $A_1,A_2,\cdots,A_n$ 上的一个 ***n* 元关系**. 特别地，设 A,B 是任意两个集合，则笛卡儿积 $A\times B$ 的任意一个子集 R 称为从集合 A 到集合 B 的一个**二元关系**，$<a,b>\in R$ 也可表示为 aRb.

例如，设 $A=\{1,2,3\}$，$B=\{a,b\}$，则

$$A\times B=\{<1,a>,<1,b>,<2,a>,<2,b>,<3,a>,<3,b>\},$$

$A\times B$ 的任意一个子集都是一个关系，如 $R_1=\{<1,a>\}$，$R_2=\{<2,a>,<3,b>\}$等都是从 A 到 B 的关系.

对于有限集合上的二元关系 R 除了可用序偶集合表示外，还可以用矩阵（叫作**关系矩阵**）表示. 设 $A=\{a_1,a_2,\ldots,a_m\}$，$B=\{b_1,b_2,\ldots,b_n\}$，R 为从 A 到 B 的一个二元关系，则对应于关系 R 的关系矩阵为 $\boldsymbol{M}_R=[r_{ij}]_{m\times n}$，其中

$$r_{ij}=\begin{cases}1, & \text{当}<a_i,b_j>\in R\\ 0, & \text{当}<a_i,b_j>\notin R\end{cases}\quad(i=1,2,\cdots,m;\ j=1,2,\cdots,n).$$

例如在上例中，R_1 和 R_2 对应的关系矩阵分别为

$$M_{R_1}=\begin{bmatrix}1&0\\0&0\\0&0\end{bmatrix},\qquad M_{R_2}=\begin{bmatrix}0&0\\1&0\\0&1\end{bmatrix}.$$

定义 1.1.17　设 R 是从集合 A 到集合 B 的一个二元关系，则由 R 中所有序偶的第一个分量组成的集合称为 R 的**定义域**，记作 $D(R)$，由 R 中所有序偶的第二个分量组成的集合称为 R 的**值域**，记作 $V(R)$，即

$$D(R)=\{a\mid a\in A\wedge(\exists b)(<a,b>\in R)\},$$
$$V(R)=\{b\mid b\in B\wedge(\exists a)(<a,b>\in R)\},$$

显然，$D(R)\subseteq A$，$V(R)\subseteq B$.

例 1.1.21　设 $A=\{1,2,3,4\}$，求 A 到 A（或称 A 上）的整除关系，并求相应的定义域和值域.

解　整除关系 $R=\{<1,1>,<1,2>,<1,3>,<1,4>,<2,4>,<4,4>\}$，

定义域 $D(R)=\{1,2,4\}$，

值域 $V(R)=\{1,2,3,4\}$.

定义 1.1.18　设 R 是从集合 A 到集合 B 的一个二元关系，若 $R=\varnothing$，则称 R 为**空关系**，若 $R=A\times B$，则称 R 为**全域关系**.

定义 1.1.19　设 I_X 是集合 X 上的二元关系，如果 $I_X=\{<x,x>\mid x\in X\}$，则称 I_X 为 X 中的**恒等关系**.

例如，设 $A=\{1,2,a\}$，则 A 中的恒等关系为

$$I_X=\{<1,1>,<2,2>,<a,a>\}.$$

空关系，全域关系，恒等关系都是唯一的.

有了表达关系的各种方法，下面就可以对关系做进一步的讨论. 我们特别注意的是在集合 X 上的二元关系 R 的一些特殊性质.

定义 1.1.20　设 R 是集合 X 上的二元关系，如果对于任意的 $x\in X$，有 xRx，则称二元关系 R 是**自反的**，即

$$R\text{ 在 }X\text{ 上自反}\Leftrightarrow(\forall x)(x\in X\rightarrow xRx).$$

定义 1.1.21　设 R 是集合 X 上的二元关系，如果对于任意的 $x\in X$，都有 $<x,x>\notin R$，则称 R 为**反自反的**，即

$$R\text{ 在 }X\text{ 上反自反}\Leftrightarrow(\forall x)(x\in X\Rightarrow<x,x>\notin R).$$

例 1.1.22　设 $X=\{1,2,3\}$，给出 X 上的几个自反关系和反自反关系.

解　由定义可知

$$R_1=\{<1,1>,<2,2>,<3,3>,<1,3>,<2,3>\},$$
$$R_2=\{<1,1>,<2,2>,<3,3>,<1,2>\},$$
$$R_3=\{<1,1>,<2,2>,<3,3>,<3,2>\}$$

都是 X 上的自反关系. 另外，X 上的全域关系和恒等关系也都是自反关系. 而

$$R_4=\{<1,2>,<1,3>,<2,3>\},$$
$$R_5=\{<3,2>\}$$

都是反自反关系.

$$R_6=\{<1,1>,<1,3>,<3,2>\},$$

$$R_7 = \{<3, 2>, <3, 3>\}$$

既不自反，也不反自反.

定义 1.1.22 设 R 是集合 X 上的二元关系，对于任意的 $x, y \in X$，若有 xRy 时，就有 yRx，则称集合 X 上的二元关系 R 是**对称的**，即

$$R \text{ 在 } X \text{ 上对称} \Leftrightarrow (\forall x)(\forall y)(x \in X \wedge y \in X \wedge xRy \rightarrow yRx).$$

例如，在同一班级学习的同学关系是对称的，平面上三角形的相似关系是对称的，即若三角形 A 和三角形 B 相似，则 B 就相似于 A.

例 1.1.23 设 $A = \{2, 3, 5, 7\}$，$R = \{<x, y> | \frac{x-y}{2} \text{是整数}\}$，证明 R 在 A 上是自反和对称的.

证明 因为对任意 $x \in A$，$\frac{x-x}{2} = 0$，即 $<x, x> \in R$，所以 R 是自反的. 又设 $x, y \in A$，如果 $<x, y> \in R$，即 $\frac{x-y}{2}$ 是整数，则 $\frac{y-x}{2}$ 也必是整数，即 $<y, x> \in R$，因此 R 是对称的.

定义 1.1.23 设 R 是集合 X 上的二元关系，对于任意的 $x, y \in X$，若有 xRy，yRx，就有 $x = y$，则称 R 在 X 上是**反对称的**，即

$$R \text{ 在 } X \text{ 上反对称} \Leftrightarrow (\forall x)(\forall y)(x \in X \wedge y \in X \wedge xRy \wedge yRx \rightarrow x = y).$$

例如，$A = \{1, 2, 3\}$，$S = \{<1, 1>, <2, 2>, <3, 3>\}$，则 S 在 A 上是对称的也是反对称的. 若 $S = \{<1, 2>, <1, 3>, <3, 1>\}$，则 S 既不是对称关系，也不是反对称关系.

定义 1.1.24 设 R 是集合 X 上的二元关系，对于任意的 $x, y, z \in X$，若有 xRy，yRz，就有 xRz，称关系 R 在 X 上是**传递的**，即

$$R \text{ 在 } X \text{ 上传递} \Leftrightarrow (\forall x)(\forall y)(\forall z)(x \in X \wedge y \in X \wedge z \in X \wedge xRy \wedge yRz \rightarrow xRz).$$

例如，在实数集合中关系 $<$，$>$ 和 $=$ 关系，都是传递的. 又如，设 A 是人的集合，R 是 A 上的二元关系，若 $<a, b> \in R$ 当且仅当 a 是 b 的祖先，则显然祖先关系 R 是传递的.

定义 1.1.25 设 R 是集合 X 上的二元关系，若 R 是自反、对称和传递的，则称 R 为 X 上的**等价关系**.

常见的等价关系有同一班级中的同学关系、直线间的平行关系等. 其主要意义在于它证实了应用抽象的一般原理的正确性，即在某些性质等价的个体中产生等价类，对全体的等价类进行分析往往比对全体本身进行分析更简单.

二元关系是以序偶为元素的集合，所以它们也可以进行集合的运算，如交、并、补等而产生新的集合. 当然关系也可以进行一些其他的运算，如复合运算、逆运算、幂运算等.

定义 1.1.26 设 R 为 X 到 Y 的关系，S 为 Y 到 Z 的关系，则 $S \circ R$ 称为 R 和 S 的**复合关系**，即

$$S \circ R = \{<x, z> | x \in X \wedge z \in Z \wedge (\exists y)(y \in Y \wedge <x, y> \in R \wedge <y, z> \in S)\}.$$

所谓关系的复合运算或合成运算就是求 R 和 S 的复合关系 $S \circ R$. 例如，设 R 是人群中的父子关系，则 R 与 R 的复合关系就是祖孙关系.

复合运算是关系的二元运算，它能够由两个关系生成一个新关系，并且可以依次类推. 例如，R 是从 X 到 Y 的关系，S 是从 Y 到 Z 的关系，P 是从 Z 到 W 的关系，于是 $(R \circ S) \circ P$ 和 $R \circ (S \circ P)$ 都是从 X 到 W 的关系. 容易证明 $(R \circ S) \circ P = R \circ (S \circ P)$，因此关系的复合运算是可结合的.