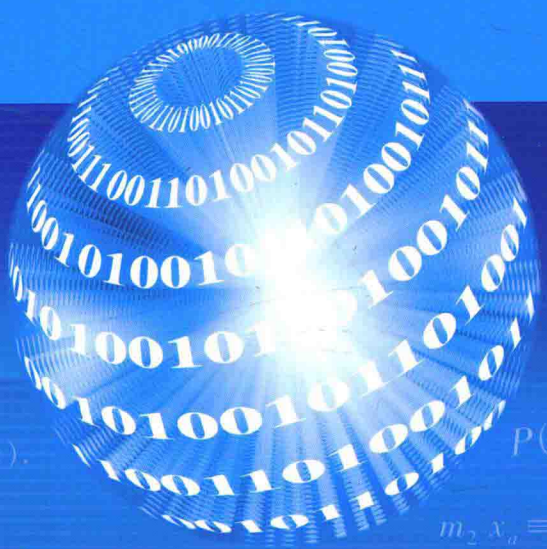
高等学校信息安全类专业系列教材

信息安全数学基础

（第2版）

◆贾春福　钟安鸣　赵源超　编著



$$a \equiv g^{\log_g a} (\bmod m).$$

$$P(n, n) = n!.$$

$$m_2 x_a \equiv m_2 x_n (\bmod m_1).$$

$$M_{S \circ R} = \begin{bmatrix} 0 & 1 & 0 \\ 1 & 1 & 1 \\ 0 & 0 & 0 \end{bmatrix}.$$

$$CP(n, r) = \frac{P(n, r)}{r} = \frac{n!}{r(n-r)!}.$$

清华大学出版社
http://www.tup.com.cn

北京交通大学出版社
http://www.bjtup.com.cn

高等学校信息安全类专业系列教材

信息安全数学基础

(第2版)

贾春福　钟安鸣　赵源超　编著

清华大学出版社
北京交通大学出版社
·北京·

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6章：第1章是预备知识，介绍了书中后面几章所涉及的基础知识；第2章和第3章是数论基础，包括整数的因子分解、同余式、原根、二次剩余、数论的应用等内容；第4章是代数系统，包括群、环、域的概念，一元多项式环和有限域理论初步等内容；第5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6章是线性反馈移位寄存器，包括反馈移位寄存器、分圆多项式和本原多项式、m序列等内容。书中每章末都配有适量习题，以供学生学习和复习巩固书中所学内容。

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，同时，也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,钟安鸣,赵源超编著. —2版. —北京:北京交通大学出版社:清华大学出版社, 2018.3

ISBN 978-7-5121-3486-7

Ⅰ.①信… Ⅱ.①贾… ②钟… ③赵… Ⅲ.①信息安全-应用数学-高等学校-教材 Ⅳ. ①TP309 ②O29

中国版本图书馆CIP数据核字(2018)第019559号

信息安全数学基础

XINXI ANQUAN SHUXUE JICHU

责任编辑：谭文芳

出版发行：清华大学出版社　邮编：100084　电话：010-62776969　http://www.tup.com.cn

北京交通大学出版社　邮编：100044　电话：010-51686414　http://www.bjtup.com.cn

印 刷 者：北京时代华都印刷有限公司

经　　销：全国新华书店

开　　本：185 mm×260 mm　印张：14　字数：358千字

版　　次：2018年3月第2版　2018年3月第1次印刷

书　　号：ISBN 978-7-5121-3486-7/TP·856

印　　数：1～1 000册　定价：38.00元

前 言

计算机与网络技术的飞速发展和广泛应用，极大地促进了社会的发展，也极大地改变了人们的生活和工作方式。与此同时，信息安全问题也更多地受到关注：信息安全理论与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了社会空前的重视。

“信息安全数学基础”是信息安全专业本科的专业基础课，对信息安全理论和技术的深入学习具有重要的意义。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 6 章：第 1 章是预备知识，介绍了书中所涉及的基础知识；第 2 章和第 3 章是数论基础，包括整数的因子分解、同余式、原根、二次剩余和数论的应用等内容；第 4 章是代数系统，包括群、环、域的概念，一元多项式环和有限域理论初步等内容；第 5 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 6 章是线性反馈移位寄存器，包括反馈移位寄存器、分圆多项式和本原多项式、m 序列等内容。书中每章末都配有适量的习题，供学生在学习和复习巩固书中所学内容时使用。

本书内容的选取，我们参照了“高等学校信息安全专业指导性专业规范（第二版）”中对“信息安全数学基础”相关教学内容和要求的阐述；并将多年来积累的实际教学经验融入其中，力求知识系统化、较好地覆盖信息安全领域所涉及的数学基础知识。对书中内容所涉及的基础预备知识做了简明扼要的介绍；书中所涉及的数学结论都给出了详细的证明；习题的配置着力于帮助学生巩固所学的内容和能力拓展。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、赵源超等编写，最后由贾春福统稿。李瑞琪、郑万通、王小璐、董奇颖、陈孟琪、李士佳、田美琦等对书中的内容进行了校对，在此表示感谢。另外，本书是南开大学教材资助项目，在此也表示衷心的感谢。

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

2017 年 12 月于南开园

符 号 表

符 号	含 义
$\mathbf{N}$	自然数集
$\mathbf{Z}$	整数集
$\mathbf{Q}$	有理数集
$\mathbf{R}$	实数集
$\mathbf{C}$	复数集
$\mathbf{Z}_m$	整数的模 m 剩余类集
$\mathbf{F}_p$	当 p 为素数时，$\mathbf{Z}_p$ 的专有表示形式
$m\mathbf{Z}$	整数 m 的整数倍构成的集合
$\mathbf{Z}[x]$	整数环 $(\mathbf{Z},+,\times)$ 上的一元多项式集
$\mathbf{Z}_m[x]$	$\mathbf{Z}_m$ 上的一元多项式集
$\mathbf{GF}(p)$	元素数为 p 的有限域
$\bmod n$	模 n 运算
$\gcd(m,n)$	整数 m,n 的最大公因子
$\mathrm{lcm}(m,n)$	整数 m,n 的最小公倍数
$\deg(f(x))$	多项式 $f(x)$ 的次数

目　录

第1章 预备知识

在当前的信息安全专业的课程体系中，由于“信息安全数学基础”课程涉及的一些数学基础知识在前期的“高等数学”等课程中介绍得较少，本书将对相关的这部分内容进行一些补充，以便读者能够顺利地阅读书中后续的各个章节.

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、关系和函数的基本概念、排列与组合及生成函数等内容.

1.1 集合、关系和函数

集合论是德国著名数学家康托尔(Cantor)于19世纪末创立的，康托尔当时建立的集合论称为朴素集合论. 20世纪初，策梅罗(Zermelo)给出了第一个集合论的公理系统，并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.

集合论是现代数学的基础，通俗地讲，数学所研究的一切概念都可以用集合来定义，甚至包括很多已经非常熟悉的概念，如整数、实数和函数等，都可以用集合加以表示. 此外，集合概念的引入，也使得我们能够摆脱具体数系的束缚，建立和研究很多抽象的数学概念和对象，从而得到很多抽象层次上的具有更多普遍含义的结论，这一点将在本书的第4章得到较多的体现. 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、函数和等势的概念和规则.

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，…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

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

其中“$\wedge$”表示“并且”.

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

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

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

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

或

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

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 $A\neq B$.

数学的所有分支中都会经常遇到需要证明两个集合相等的问题，注意，这个定义就是证明两个集合相等的关键所在，一般的证明步骤总结如下：

第一步，从集合 A 中任意选择一个元素，都能够证明这个元素也属于集合 B，根据定义 1.1.1，可以推得 $A\subseteq B$；

第二步，从集合 B 中任意选择一个元素，都能够证明这个元素也属于集合 A，根据定义 1.1.1，可以推得 $B\subseteq A$；

第三步，根据定义 1.1.3，可以推得 $A=B$.

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

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，产生矛盾. 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$\varnothing$. 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

$$\varnothing_1\subseteq\varnothing_2$$

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$A=\{a, b, c\}$，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的集合为对象，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.

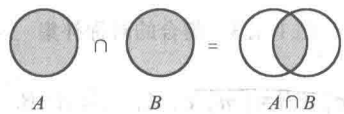


图 1.1.1 集合的交集

[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 所示.

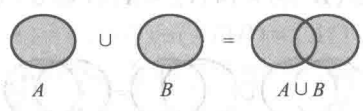


图 1.1.2 集合的并集

[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**. 文氏图表示如图 1.1.3 所示.

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 $\sim A$ 或者 $\overline{A}$. 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.

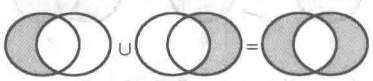


图 1.1.4 集合的对称差集

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

解 $A \oplus B=\{1, 6\}$.

下面给出集合运算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 $A \cup (B \cap C)=(A \cup B) \cap (A \cup C)$

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

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

(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, 其余留给读者作为习题完成.

[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

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

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

[例 1.1.12] 证明吸收律, 即 $A\cup(A\cap B)=A$.

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

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

[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, 首先介绍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, 有$\{a, b\}=\{b, a\}$, 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$b=y$.

注意，这个定义告诉我们证明两个序偶相等的关键在于，分别证明两个位置上的对应元素分别相等.

定义 1.1.14 由n个具有给定次序的个体a_1, a_2, …, 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

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

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, …, 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，…，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, …, 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

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

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] 证明分配律$(A\cap B)\times C=(A\times C)\cap(B\times C)$.

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, …, 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. 如果一个二元关系是从集合 A 到其自身的关系，则这样的二元关系称为集合 A 上的关系.

例如，设 $A=\{1, 2, 3\}$, $B=\{a, b\}$，则

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

$$B\times B=\{<a, a>, <a, b>, <b, a>, <b, b>\}$$

$A\times B$ 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；$R_3=\{<a, a>, <a, b>, <b, b>\}$ 是集合 B 上的一个二元关系.

对于有限集合上的二元关系 R 除了可以用序偶集合表示外，还可以用矩阵(通常称作**关系矩阵**)表示. 设 $A=\{a_1, a_2, \cdots, a_m\}$, $B=\{b_1, b_2, \cdots, b_n\}$, 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

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

例如，在上例中，R_1 和 R_2 对应的关系矩阵分别为

$$\boldsymbol{M}_{R_1}=\begin{bmatrix}1 & 0\\ 0 & 0\\ 0 & 0\end{bmatrix}$$

和

$$\boldsymbol{M}_{R_2}=\begin{bmatrix}0 & 0\\ 1 & 0\\ 0 & 1\end{bmatrix}.$$

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关系 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关系 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 上的整除关系，并求相应的定义域和值域.

解 整除关系 $R=\{<1, 1>, <1, 2>, <1, 3>, <2, 2>, <1, 4>, <3, 3>, <2, 4>, <4, 4>\}$，对应此整除关系 R 的定义域

$$D(R)=\{1, 2, 3, 4\},$$

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