HZ BOOKS
华章教育

高等院校信息安全专业规划教材

信息安全数学基础

Essential Mathematics for Information Security

贾春福 钟安鸣 杨骏 编著

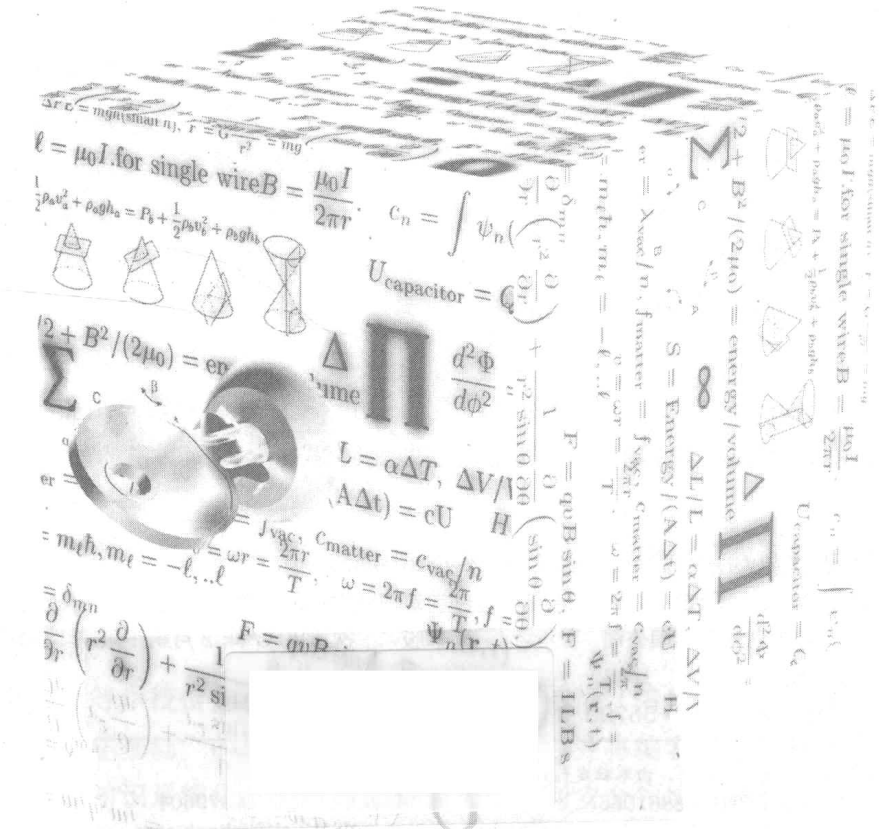
机械工业出版社
China Machine Press

高等院校信息安全专业规划教材

信息安全数学基础

Essential Mathematics for Information Security

贾春福 钟安鸣 杨骏 编著



机械工业出版社
China Machine Press

图书在版编目（CIP）数据

信息安全数学基础 / 贾春福，钟安鸣，杨骏编著 . —北京：机械工业出版社，2017.2
（高等院校信息安全专业规划教材）

ISBN 978-7-111-55700-5

I. 信… II. ① 贾… ② 钟… ③ 杨… III. 信息安全 – 应用数学 – 高等学校 – 教材
IV. ① TP309 ② O29

中国版本图书馆 CIP 数据核字（2016）第 324376 号

本书系统地介绍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 9 章：第 1 章是预备知识，介绍后续章节涉及的必要的数学基础知识；第 2 章至第 5 章是数论基础，包括整除、同余、次数与原根、二次剩余和素数检验以及整数分解等内容；第 6 章至第 8 章是代数基础，包括群、环、域的概念及其应用等内容；第 9 章是椭圆曲线，包括仿射空间和射影空间、椭圆曲线的基本性质、椭圆曲线上的离散对数等内容. 书中每节末都配有适量习题，以供学生复习和巩固书中所学内容.

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，可以供从事信息安全和其他信息技术工作的人员参考.

出版发行：机械工业出版社（北京市西城区百万庄大街 22 号　邮政编码：100037）
责任编辑：和　静　　责任校对：董纪丽
印　　刷：三河市宏图印务有限公司　　版　　次：2017 年 2 月第 1 版第 1 次印刷
开　　本：185mm × 260mm　1/16　　印　　张：15.5
书　　号：ISBN 978-7-111-55700-5　　定　　价：39.00 元

凡购本书，如有缺页、倒页、脱页，由本社发行部调换
客服热线：(010) 88378991　88361066　　投稿热线：(010) 88379604
购书热线：(010) 68326294　88379649　68995259　　读者信箱：hzjsj@hzbook.com

前言

计算机和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，也彻底改变了人们的生活和工作方式．与此同时，网络与信息安全问题也更多地受到关注，网络空间安全理论与技术已经成为当前最为重要的研究领域之一，网络空间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”是信息安全本科专业的基础课之一，对网络空间安全理论与技术（特别是网络空间安全的核心技术——密码技术）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．

全书分为 4 部分，共包括 9 章内容：

第一部分：预备知识（第 1 章），介绍书中后续章节所涉及的基本概念和基础知识，包括集合、关系、函数、映射与势以及拓扑空间等．

第二部分：数论基础（第 2 至 5 章），介绍数论的基本内容，包括整除（整数的因子分解）、同余、原根与指数、二次剩余以及数论的应用等内容．

第三部分：抽象代数基础（第 6 至 8 章），分别介绍群、环、域的概念和知识，以及初等伽罗瓦理论和有限域理论．

第四部分：椭圆曲线（第 9 章），介绍椭圆曲线的算术理论，包括仿射空间和射影空间、Weierstrass 方程与椭圆曲线、椭圆曲线上的群结构、有限域上的椭圆曲线和椭圆曲线上的离散对数等内容．

书中每节末都配有适量的习题，供学生在复习和巩固书中所学内容时使用．习题包括 A、B 两组：A 组主要用于巩固学生在课堂上所学的内容和知识，B 组主要用于拓展学生的知识和技能．

本书依据《高等学校信息安全专业指导性专业规范》（清华大学出版社，2014）中关于“信息安全数学基础”的相关教学要求选取内容，并将编者多年积累的实际教学经验融入其中，力求知识系统化，能较好地覆盖网络空间安全领域所涉及的数学基础知识．书中所涉及的基础知识都进行了介绍，其中的数学结论都给出了详细的证明；书中所配的习题着力于帮助学生巩固所学的内容和拓展能力．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、钟安鸣和杨骏编写. 高敏芬老师、李瑞琪、梁爽、吕童童、田美琦、程晓阳和郑万通等参与了书稿的阅读和校对. 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

2016 年 10 月于南开园

教学建议

教学章节	教学要求	课时
第 1 章 预备知识	• 掌握集合的相关概念及其运算定律 • 掌握关系的相关概念，重点掌握等价关系的定义 • 掌握映射和函数的相关概念，重点掌握单射、满射和双射的定义 • 了解集合势的定义以及映射与势之间的关系 • 了解度量空间和拓扑空间的相关概念	2
第 2 章 整　除	• 掌握整除和带余除法的相关定义 • 掌握最大公因子和互素的定义，掌握欧几里得除法的相关定理及其应用 • 掌握算术基本定理的内容及其应用 • 了解完全数、费马数和梅森素数的概念	4
第 3 章 同　余	• 掌握同余的概念以及相关性质、剩余系和剩余类的相关概念 • 掌握欧拉函数的概念、欧拉定理和费马小定理的内容，重点掌握欧拉定理的使用，了解欧拉定理在密码学中的应用 • 掌握扩展欧几里得算法的内容，了解威尔逊定理 • 掌握线性同余方程、孙子定理以及线性同余方程组的解法 • 了解高次同余方程的概念以及解法	6
第 4 章 原根与指数	• 掌握次数的概念和性质 • 掌握原根的概念和性质 • 掌握离散对数和 n 次剩余的概念以及相关性质 • 了解本章内容在密码学中的应用	6
第 5 章 二次剩余	• 掌握二次剩余的概念和性质 • 掌握勒让德符号的定义、高斯引理和二次互反律的内容和应用 • 掌握雅可比符号的定义以及应用	6
第 6 章 群	• 掌握群、子群的相关定义以及性质 • 掌握循环群、置换群的相关定义以及性质 • 掌握陪集、商群的定义和相关性质以及拉格朗日定理的内容 • 掌握同态、同构的相关概念和定理，重点掌握群的同态基本定理	10
第 7 章 环	• 掌握环的相关概念，重点掌握环上的一元多项式、多项式环以及环上的同态和同构等概念 • 掌握理想和商环的相关概念，重点掌握环上的同态基本定理 • 掌握唯一析因环、主理想整环、欧几里得环的相关概念以及性质 • 掌握素理想和极大理想的概念以及相关性质，重点掌握环构造域的方法	10

（续）

教学章节	教学要求	课时
第 8 章 域	• 掌握域上多项式的相关概念以及性质 • 了解域的代数扩张的相关知识 • 了解分裂域、自同构、正规扩张的相关知识 • 初步了解伽罗瓦理论 • 掌握有限域的相关概念，重点掌握有限域的构造，了解有限域的相关性质	10
第 9 章 椭圆曲线	• 了解仿射空间和射影空间的概念，掌握仿射平面和射影平面的概念 • 初步了解代数曲线的基本知识 • 掌握 Weierstrass 方程的概念、椭圆曲线的概念以及相关性质 • 掌握椭圆曲线上的群结构的相关概念、椭圆曲线上的点加运算，重点掌握有限域上的椭圆曲线的点加运算 • 了解椭圆曲线上的离散对数问题以及本章内容在密码学中的应用	10

目录

Chapter 1

第1章 预备知识

集合、关系、函数、映射、势和拓扑空间等概念是构成近代数学体系的基础内容，也是信息安全专业“信息安全数学基础”课程的基本概念和基础知识．本章将介绍这些朴素的概念，为后续章节的学习做必要的知识准备．

1.1 集合

1．集合的概念

集合论是德国数学家康托尔（Georg 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，德国数学家策梅罗（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，使该学科成为数学领域中发展较快的一个分支．

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，甚至包括很多我们已经非常熟悉的概念，如整数、实数和函数等，都可以用集合表示．此外，集合概念的引入，也使得我们能够摆脱一些具体要求的束缚，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6章等后续章节中得到较多的体现．现在，集合论观点已经渗透到了现代代数学、几何学、分析学、概率论和信息论等各个领域．本节将介绍集合论的基础知识，从而引入后续的集合与关系、集合运算、函数和等势的概念及规则．

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**，而这些事物称为**元素**或**成员**．例如，所有0和1之间的实数，坐标平面中的所有点，所有整数，

整数中的所有素数，实数域上的所有连续函数，等等.

我们通常用大写英文字母 A，B，…表示集合，用小写英文字母 a，b，…表示集合中的元素.

若元素 a 是集合 S 中的元素，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所有元素列举出来，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

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

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

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

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

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

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

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

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

例如，整数集 $\mathbb{Z}$ 是有理数集 $\mathbb{Q}$ 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 $A\neq B$.

几乎在数学的所有分支中，都会经常遇到需要证明两个集合相等的问题，请注

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，我们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，我们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），“~”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，对于每一个非空集合 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

$$\varnothing_1\subseteq\varnothing_2$$

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，即

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

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”.

需要说明的是，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　设有任意两个集合 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.

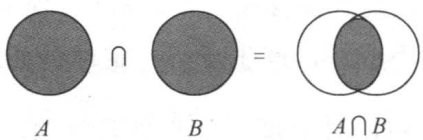


图 1.1.1　集合的交集

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　设有任意两个集合 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.

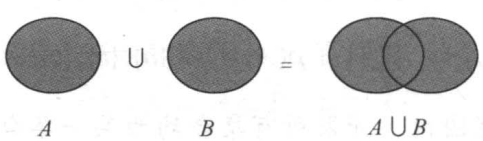


图 1.1.2　集合的并集

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 $A\cup B\subseteq B$，因为 $A\subseteq A\cup B$，所以 $A\subseteq B$.

（2）其证明过程与（1）类似，留给读者完成. ◀

定义 1.1.9　设有任意两个集合 A 和 B，所有属于 A 而不属于 B 的元素组成的集合 S，称为集合 B 对 A 的**补集**，或称集合 B 对 A 的**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.

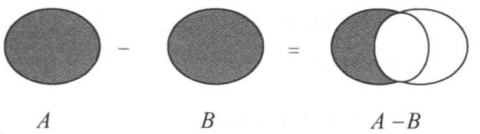


图 1.1.3　集合的对称补集

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　设有任意两个集合 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.

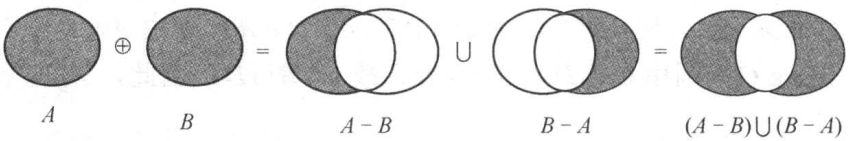


图 1.1.4　集合的对称差集

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）$A\subseteq A\cup B$　$B\subseteq A\cup B$　$A-\bar{B}\subseteq A$　$A-B=A\cap\sim B$

（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，其余的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 $A\cup(A\cap B)=A$.

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 $A\cap(B-C)=(A\cap B)-(A\cap C)$. ◀

习题 1.1

A 组

1.（1）设 $A=\{a,\{a\}\}$，下列各式成立吗？

$\{a\}\in\rho(A)$；$\{a\}\subseteq\rho(A)$；$\{\{a\}\}\in\rho(A)$；$\{\{a\}\}\subseteq\rho(A)$.

（2）若 $A=\{a,\{b\}\}$，（1）中的各式成立吗？

2. 设 $E=\{1,2,3,4,5\}$，$A=\{1,4\}$，$B=\{1,2,5\}$，$C=\{2,4\}$，求

（1）$A\cap\sim B$；

（2）$(A\cup B)\cap(A\cup C)$；

（3）$\sim(A\cup B)$；

（4）$\rho(A)-\rho(C)$.

3. 证明集合运算定律（定理 1.1.3）中的其余部分.

B 组

4. 设 A，B，C 是任意三个集合，证明下列各式：

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

（2）$A\cap(B\oplus C)=(A\cap B)\oplus(A\cap C)$.

1.2　关系

关系的概念在日常生活中是普遍存在的. 在数学中，关系用来表达集合中元素间的联系. 在介绍关系的概念之前，我们首先介绍一下序偶和笛卡儿积的概念.

定义 1.2.1　由两个具有给定次序的元素 x 和 y（允许 $x=y$）所组成的序列，称为**序偶**或**数对**，记作$<x,y>$. 其中称 x 为**第一分量**，称 y 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，$<a,b>\neq<b,a>$.