21世纪高等学校计算机规划教材

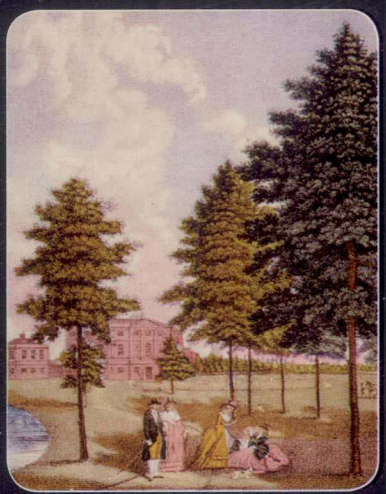
21st Century University Planned Textbooks of Computer Science

# 离散数学

## Discrete Mathematics

赵一鸣 阚海斌 吴永辉 编著

- 计算学科的重要数学基础
- 教学实践的多年系统总结
- 知识体系的完美提炼组合



名家系列

人民邮电出版社
POSTS & TELECOM PRESS

21世纪高等学校计算机规划教材

# 离散数学

Discrete Mathematics

赵一鸣 阚海斌 吴永辉 编著

名家系列

人民邮电出版社

北京

**图书在版编目（CIP）数据**

离散数学 / 赵一鸣，阚海斌，吴永辉编著. -- 北京
：人民邮电出版社，2011.9
21世纪高等学校计算机规划教材
ISBN 978-7-115-25305-7

Ⅰ. ①离… Ⅱ. ①赵… ②阚… ③吴… Ⅲ. ①离散数学－高等学校－教材 Ⅳ. ①O158

中国版本图书馆CIP数据核字(2011)第114376号

## 内 容 提 要

本书是复旦大学离散数学教材。全书介绍离散数学中的5个部分，即集合论、组合数学、图论、代数结构和数理逻辑的初步知识。在内容组织上，不但介绍基本内容、基本概念及其实际背景、各概念间的相互关系，而且强化了证明的思想和方法。

本书可作为高等院校计算机科学与技术、软件工程等专业的离散数学课程教材，也可以作为该课程的教学参考书。

21世纪高等学校计算机规划教材

**离散数学**

◆ 编　　著　赵一鸣　阚海斌　吴永辉
责任编辑　武恩玉

◆ 人民邮电出版社出版发行　　北京市崇文区夕照寺街14号
邮编　100061　　电子邮件　315@ptpress.com.cn
网址　http://www.ptpress.com.cn
三河市海波印务有限公司印刷

◆ 开本：787×1092　1/16
印张：16.75　　2011年9月第1版
字数：397千字　　2011年9月河北第1次印刷

ISBN 978-7-115-25305-7

定价：35.00元

**读者服务热线：(010)67170985　印装质量热线：(010)67129223**
**反盗版热线：(010)67171154**

# 前 言

离散数学是计算学科类重要的数学基础课之一，它是以离散（即非连续）对象的数量和空间关系为研究内容的若干个数学分支的总称，包括数理逻辑、近世代数、古典概率、组合学、图论、集合论、数论、自动机和形式语言、可计算性和可判定性、离散几何等。

18 世纪以前，数学基本上是研究**离散**对象的数量和空间关系的科学，而天文学（如行星轨道的研究）、物理学（如牛顿三大力学定律的研究）的发展，极大地推动了以微积分、数学物理方程、实复变函数论为代表的**连续**数学的发展。在这段时期内，除了近世代数（又称**抽象**代数）外，属于离散数学范围的组合数学、图论、数理逻辑等一直处于相对停滞状态。到了 20 世纪 50 年代，随着计算机的出现和计算机科学与技术的迅猛发展，才使得离散数学重新焕发青春。

从理论计算机科学（算法、可计算性、计算复杂性、程序正确性证明、自动编程等），计算机软件（数据结构、操作系统、数据库、软件工程等），人工智能（自动推理、机器学习）和系统结构设计（网络通信、分布式和并行计算系统）到计算机应用（模式识别，图像处理，信号处理，数据的压缩、编码和加密）以及如今成为关注热点的云计算和物联网，无一不以离散数学为基础，并为它提出了许多新的研究课题。通过本书的学习，读者将具有离散数学的基本知识和得到离散数学思维方法的训练，也可为今后长远发展，迎接未来计算学科的挑战获得必要的理论储备。

目前，计算学科类专业课程设置通常会另外单独设置概率统计类课程以及计算理论课程，因此本书只讲述离散数学中的 5 个部分，即集合论、组合数学、图论、代数结构和数理逻辑的初步知识。

本书编著者在系统总结使用由复旦大学计算机系朱洪等编写的《离散数学教程》教材的课堂教学实践，以及 10 年来课件改进体会的基础上，对相关知识点做了系统梳理，同时增加了部分实例，参照国外教材的先进理念，更多强调培养学生独立学习和思考能力。在图论部分，编著者不仅强调图论的基本内容、基本概念及其实际背景、各概念间相互关系，还强化了证明的思想和方法，以培养学生思维过程的数学化，以及通过图模型解决实际问题的能力。代数结构部分则强调了在计算机系统和编码技术中有着重要作用的本原元和本原多项式的内容，而数理逻辑则是通过引入泛代数，和代数部分一气呵成。

根据我们的教学实践，本书教学课时需要 102 学时。如果课时为 64～72 学时，可以考虑不讲下列内容：第 4.4 节“基数的比较”；第 8.6 节“图论模型初步”；第 11.1 节“连通度与块”；第 11.4 节“独立集、覆盖”；第 11.5 节“Petri 网”；第 14.5 节“整环与分式域”；第 15 章“域”和第 19.5 节“谓词演算的性

质”。如果课时为 48～54 学时，则除了不讲授上述内容之外，再删去第 11 章的其他内容，以及第 12.3 节“代数系统[Z;+, ·]”，第 14.3 节“多项式环”，第 18.4 节“一般逻辑系统”和第 18.5 节“命题演算的性质”。具体讲授内容可根据实际教学进度和各校实际情况做安排。本书也可以作为离散数学课程的参考教材。

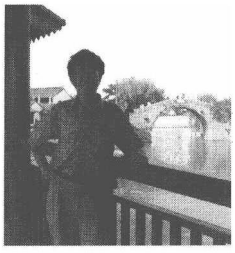
本书集合论和图论部分由吴永辉编写；近世代数部分由阚海斌编写；组合数学和数理逻辑部分由赵一鸣编写。赵一鸣最后对全书作了修改和审定。在本书编写过程中，朱洪提出了很多宝贵意见，彭超参与编写了组合数学的部分内容，人民邮电出版社的武恩玉编辑对本书的初稿提出了宝贵的修改建议，编著者在此对他们表示深深的感谢。

编　者

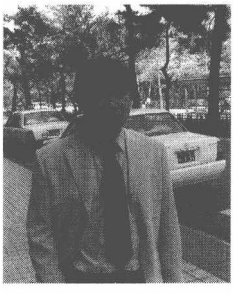
复旦大学

2011 年 4 月

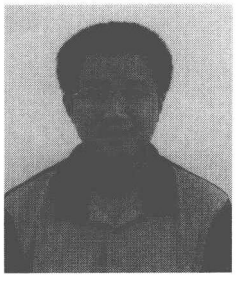
# 作者简介



**赵一鸣** 复旦大学毕业后留校，任计算机科学与技术专业、软件工程专业教师。现任复旦大学软件学院副院长，中国人工智能学会离散数学专业委员会副主任，全国高等学校计算机教育研究会常务理事，中国计算机学会教育专业委员会常委。多年来在密码和信息安全方面从事教学和研究工作。曾获教育部科技进步二等奖和国家级教学成果二等奖。长期主讲离散数学、信息安全原理等课程。



**阚海斌** 复旦大学毕业后留校，任计算机科学与技术专业教师。现任复旦大学计算机科学技术学院教授、博士生导师。2002 年 7 月—2006 年 1 月在日本北陆先端科学技术大学院大学（JAIST）的情报研究科工作，任助理教授（Assistant Professor），2006 年 2 月返回复旦大学工作。多年来在编码与信息论、信息安全方面从事教学和研究工作，发表 SCI 杂志论文 40 多篇。长期主讲离散数学、编码与信息论、密码学等课程。



**吴永辉** 复旦大学计算机科学技术学院副教授，ACM-ICPC 中国赛区指导委员会成员，复旦大学 ACM 程序设计竞赛队教练。自 2001 年起连续带队进入 ACM-ICPC 世界总决赛，并取得过世界第 6 名的佳绩。主要研究方向为数据库，长期主讲离散数学、数据结构等课程。

# 目 录

## Ⅰ 集合论概述



## Ⅱ 组合数学初步



## Ⅲ 图论

## Ⅳ 代数结构



## Ⅴ 数理逻辑

# I
# 集合论概述

集合论是现代数学的基础，已深入到各种科学和技术领域中，并被广泛地应用到了数学和计算机科学的各分支中。

德国的著名数学家、集合论的创始人康托尔（Cantor，1845—1918）于1874年在《数学杂志》上发表了关于集合论的第一篇论文，提出了“无穷集合”这个数学概念，开创了现代集合论的研究，为现代数学奠定了基础，但是在其理论中出现了悖论。为了解决集合论的悖论，并进一步解决集合论自身的问题，在20世纪初开始了集合论公理学的研究，它是数理逻辑的中心问题之一。

本书的集合论部分仅从集合的基本概念出发，完全避免使用集合的公理化方法，直观地介绍朴素集合论。这一部分从集合的基本概念和实例着手，对关系、函数、基数等进行讨论。

# 第 1 章 集合的基本概念

我们首先讨论一个问题：什么是集合？“一些教师”是不是集合？“复旦大学教师”又是不是集合？

所谓集合，就是具有共同性质的一些东西汇集成一个整体。复旦大学教师就是一个集合，组成这一集合的每个元素都具有共同性质：都是复旦大学教师。而“一些教师”就不是集合，因为我们无法确定其范围和性质。

本章并不是要讨论特定的集合，而是从抽象的角度讨论集合的基本概念：集合的表示、集合的子集、集合的运算，并简单地介绍集合论的悖论。

## 1.1 集合的表示

我们通常用大写字母表示集合，如 $S$，$A$ 等。构成一个集合中的那些对象称为该集合的元素，通常用小写字母或数字表示集合的元素。用 $a\in A$ 表示 $a$ 是集合 $A$ 的元素，读作 $a$ 属于 $A$。用 $a\notin A$ 表示 $a$ 不是集合 $A$ 的元素，读作 $a$ 不属于 $A$。

例如，所有整数全体构成的集合记为 $Z$，则 $3\in Z$，$-8\in Z$，$6.5\notin Z$。

集合中的元素可以是具体的事物，也可以是抽象的符号。集合有如下的表示方法。

（1）枚举法：通过列出集合中的所有元素来表示一个集合。例如，集合 $A$ 的元素为 1，3，5，7，9，则集合 $A$ 可表示为 $A=\{1, 3, 5, 7, 9\}$。

（2）特性刻画法（描述法）：通过描述集合中元素具有共同性质来表示一个集合。例如，集合 $A$ 的元素为 $x^2=1$ 的根，则集合 $A$ 表示为 $A=\{x \mid x^2-1=0\}$。一般来说，满足特性 $P$ 的元素组成的集合记为：$\{x|P(x)\}$，其中 $P(x)$是“$x$ 具有特性 $P$”的一个简写。

上述两种表示方法都是常用的，前者多用于元素个数较少的情况，后者多用于元素个数较多（或无限），并且各对象具有共同性质的情况。往往一个集合可以同时用上述两种方法表示，如$\{x \mid x^2-1=0\}$也可以表示成$\{1, -1\}$，$\{x \mid x$ 为小于或等于 7 的质数$\}$也可以表示成$\{1, 2, 3, 5, 7\}$。

（3）递归定义法：通过某规则的计算来定义集合中的元素，在此情况下，集合常称为递归定义的集合。我们将在第 4 章对这一方法做详细介绍。

不含有任何元素的集合称为空集，记为$\varnothing$或$\{\}$。如果在一个集合中元素个数有限，则称该集合为**有限集**，否则称该集合为**无限集**。有限集 $A$ 中的元素个数称为集合 $A$ 的基数（详见

第 4 章），记为$|A|$。例如，$A=\{x|x$ 是大于 1 小于 6 的质数$\}$，$|A|=3$。$A=\{x|x^2+1=0, x$ 为实数$\}$是空集$\varnothing$，$|A|=|\varnothing|=0$。

集合中的元素是不能重复出现的。由于一个集合完全由它的元素所确定，所以集合中的元素之间的次序是无关紧要的。例如，集合$\{a, b, c\}$与$\{b, a, c\}$是完全相同的集合。在特殊问题中，集合中元素可以重复出现，这种集合称为**多重集**，如$\{a, b, a, b, c\}$和$\{1, 2, 3, 1, 4\}$等。

一个集合也可以是其他集合的元素，以集合作为元素所组成的集合称为**集合族**。例如，$S=\{\{a, b\}, \{a, b, c\}, \{d, e\}\}$，$S$ 的元素$\{a, b\}$，$\{a, b, c\}$和$\{d, e\}$又都是集合，如集合$\{a, b, c\}$，其元素是 $a$，$b$ 和 $c$，而 $a$，$b$，$c$ 都不是集合 $S$ 的元素。又如，$S=\{\varnothing, \{\varnothing\}\}$的元素是$\varnothing$和$\{\varnothing\}$。必须注意$\varnothing$与$\{\varnothing\}$是不同的，$\{\varnothing\}$表示以$\varnothing$为元素的集合。

本书用 $I$ 或 $Z$ 表示整数集；$I^+$或 $Z^+$表示正整数集；$Q$ 表示有理数集；$Q^+$表示正有理数集；$Q^-$表示负有理数集；$R$ 表示实数集；$R^+$表示正实数集等。

# 1.2　集合的子集

我们可以用平面上封闭曲线包围点集的图形来表示集合，该图形称为文氏图（Venn Diagrams）。例如，集合 $A=\{1, 2, 3\}$的文氏图如图 1.1 所示。文氏图还能表示集合之间的相互关系，集合 $A$ 包含在集合 $B$ 中，如图 1.2 所示。

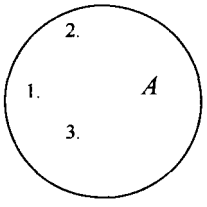


图 1.1

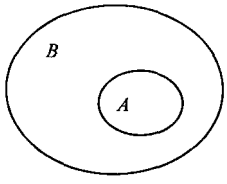


图 1.2

**定义 1.1**　设 $A$ 和 $B$ 是两个集合。$A$ 的每个元素都是 $B$ 的元素，则称 $A$ 是 $B$ 的**子集**，记为 $A\subseteq B$ 或 $B\supseteq A$，分别读作 $A$ 包含在 $B$ 中或 $B$ 包含 $A$。特别地，$A\subseteq A$。

定义 1.1 在给出子集定义的同时，还给出该定义的反面：若存在元素 $a\in A$，但 $a\notin B$，则 $A$ 不是 $B$ 的子集。

例如，$\{x|-1<x<2\}$，因 0.5 是该集合的元素，而不是整数集的元素，所以集合$\{x|-1<x<2\}$不是整数集 $Z$ 的子集。

**定义 1.2**　集合 $A$ 和 $B$ 的元素全相同，则称 $A$ 和 $B$ **相等**，记为 $A=B$；否则称 $A$ 和 $B$ **不相等**，记为 $A\neq B$。

**定理 1.1**　设 $A$ 和 $B$ 是两个集合，则 $A=B$ 当且仅当 $A\subseteq B$，并且 $B\subseteq A$。

**证明：** $\Rightarrow$因为 $A=B$，由定义 1.2，对任意的 $a\in A$，$a\in B$ 成立，因此有 $A\subseteq B$；同理，对任意的 $a\in B$，$a\in A$ 成立，因此 $B\subseteq A$。

$\Leftarrow$反之，若 $A\neq B$。因为集合 $A$ 和 $B$ 的元素不全相同，则 $A$ 中至少有一元素不在 $B$ 中，或者 $B$ 中至少有一元素不在 $A$ 中；如果 $A$ 中至少有一元素不在 $B$ 中，则与 $A\subseteq B$ 矛盾；如果 $B$

中至少有一元素不在 $A$ 中，则与 $B\subseteq A$ 矛盾。所以 $A\neq B$ 不可能成立。

**定义 1.3** 若 $A\subseteq B$，且 $A\neq B$，则称集合 $A$ 是集合 $B$ 的**真子集**，记为 $A\subset B$。也可以说，$A$ 是 $B$ 的子集，并且 $B$ 中至少有一个元素不属于 $A$。

例如，$\{a\}\subset\{a, b\}$。

注意，$\in$与$\subseteq$和$\subset$是完全不同的概念，$\in$表示元素与集合的属于关系，而$\subseteq$和$\subset$表示集合与集合的包含关系。

例如，$S_1=\{a\}$，$S_2=\{\{a\}\}$，$S_3=\{a, \{a\}\}$。则 $a\in S_3$，$S_1\subset S_3$，$\{a\}\in S_3$，$S_2\subset S_3$，$S_1\in S_3$，$S_1\in S_2$。

**定义 1.4** 在取定一个集合 $U$ 以后，对于 $U$ 的任意子集而言，称 $U$ 为**全集**。

全集是一个相对的概念。例如，实数集对于整数集、有理数集而言是全集，而整数集对于偶数集、奇数集而言也是全集。

**定理 1.2** 对于任何集合 $A$，必有（1）$\varnothing\subseteq A$，（2）$A\subseteq A$，（3）$A\subseteq U$。

**证明：**（1）用反证法证明，假设空集$\varnothing$不是集合 $A$ 的子集，则至少有一个元素 $x$，$x\in\varnothing$且 $x\notin A$。又根据空集的定义，$\varnothing$没有元素，所以对任何 $x$，必有 $x\notin\varnothing$，这样导致矛盾。因此空集是任何集合的子集，即$\varnothing\subseteq A$。

（2）、（3）证明集合 $A$ 是集合 $B$ 的子集，则由定义 1.1，对任何 $x\in A$，如果 $x\in B$，则 $A\subseteq B$ 成立。证明过程略。

对于集合 $A=\{1, 2, 3\}$，$\varnothing$，$\{1\}$，$\{2\}$，$\{3\}$，$\{1, 2\}$，$\{1, 3\}$，$\{2, 3\}$和$\{1, 2, 3\}$都是集合 $A$ 的子集。这些子集全体构成集合称为$\{1, 2, 3\}$的幂集。幂集定义如下。

**定义 1.5** 设 $A$ 是任意集合，$A$ 的所有子集所组成的集合称为集合 $A$ 的幂集，记为 $P(A)$，或记为 $2^A$，即 $P(A)=\{B|B\subseteq A\}$。

**例 1.1** 设 $A=\{a\}$，$P(A)=\{\varnothing, \{a\}\}$。

设 $A=\{a, b\}$，$P(A)=\{\varnothing, \{a\}, \{b\}, \{a, b\}\}$。

设 $A=\{a, b, c\}$，$P(A)=\{\varnothing, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, \{a, b, c\}\}$。

**定理 1.3** 设 $A$ 是有限集，则 $|P(A)|=2^{|A|}$。

**证明：**对于有限集合 $A$，设 $|A|=n$。从 $n$ 个元素中选取 $i$ 个元素有 $C(n, i)$种取法。所以$|P(A)|=C(n, 0)+C(n, 1)+C(n, 2)+\cdots+C(n, n)=(1+1)^n=2^n$，即$|P(A)|=2^{|A|}$。

# 1.3 笛卡儿积

**定义 1.6** 两个对象 $a$，$b$ 按一定次序组成一对，称为有序对，记为（$a$，$b$）。两个有序对相等记为$(a, b)=(c, d)$，当且仅当 $a=c$ 和 $b=d$ 同时成立。

例如：5<8 记为（5，8）；平面上的顶点坐标记为（$x$，$y$）；教师 $a$ 和学生 $b$ 的师生关系记为（$a$，$b$）。这些例子说明常用有序对来表示两个对象之间的关系。

当 $a\neq b$ 时，$(a, b)\neq(b, a)$，但集合$\{a, b\}=\{b, a\}$，也就是说，有序对$(a, b)$中 $a$，$b$ 是有次序的。$a$，$b$ 不一定来自同一集合。$a$，$b$ 可以相等，也可以不相等，$(a, a)$也是有意义的。有序对概念可以推广到 $n$ 个元素按一定次序组成有序 $n$ 元组，定义如下。

**定义 1.7** 设整数 $n>0$，$n$ 个对象的序列形如 $a_1$，$a_2$，…，$a_n$组成一组称为有序 $n$ 元组，记为（$a_1$，$a_2$，…，$a_n$），其中 $a_i$称为第 $i$ 个分量。两个有序 $n$ 元组相等当且仅当它们的每个

对应分量相等。

**定义 1.8**　两个集合 $A$ 和 $B$，定义 $A$ 和 $B$ 的笛卡儿积为 $A\times B=\{(a, b) \mid a\in A, b\in B\}$，又称 $A\times B$ 为 $A$ 和 $B$ 的**直积**。

**例 1.2**　设 $A=\{1, 2\}$，$B=\{x, y\}$，$C=\{a, b, c\}$，则

$A\times B=\{(1, x), (1, y), (2, x), (2, y)\}$；

$B\times A=\{(x, 1), (y, 1), (x, 2), (y, 2)\}$；

$A\times C=\{(1, a), (1, b), (1, c), (2, a), (2, b), (2, c)\}$；

$A\times A=\{(1, 1), (1, 2), (2, 1), (2, 2)\}$。

通常 $B\times A\neq A\times B$。

**定义 1.9**　设 $n$ 个集合 $A_1, A_2, \cdots, A_n$，$A_1, A_2, \cdots, A_n$ 的笛卡儿积为 $A_1\times A_2\times\cdots A_n=\{(a_1, a_2, \cdots, a_n) \mid a_i\in A_i, i=1, \cdots, n\}$。

例 1.2 中集合 $A$，$B$，$C$ 的笛卡儿积 $A\times B\times C=\{(1, x, a), (1, x, b), (1, x, c), (1, y, a), (1, y, b), (1, y, c), (2, x, a), (2, x, b), (2, x, c), (2, y, a), (2, y, b), (2, y, c)\}$。

若对所有 $i$，$A_i=A$，则 $A_1\times A_2\times\cdots\times A_n$ 记为 $A^n$。

# 1.4　集合的运算

设 $A$ 和 $B$ 是任意两个集合，通过下面的集合运算的定义可以得到新的集合。

**定义 1.10**　设 $A$ 和 $B$ 是两个集合，$U$ 是全集。

（1）$A$ 和 $B$ 的**并**，记为 $A\cup B$，它是由 $A$ 和 $B$ 中所有元素所组成的集合，即 $A\cup B=\{x|x\in A$ 或 $x\in B\}$。

（2）$A$ 和 $B$ 的**交**，记为 $A\cap B$，它是由 $A$ 和 $B$ 中公共元素所组成的集合，即 $A\cap B=\{x|x\in A$ 且 $x\in B\}$。

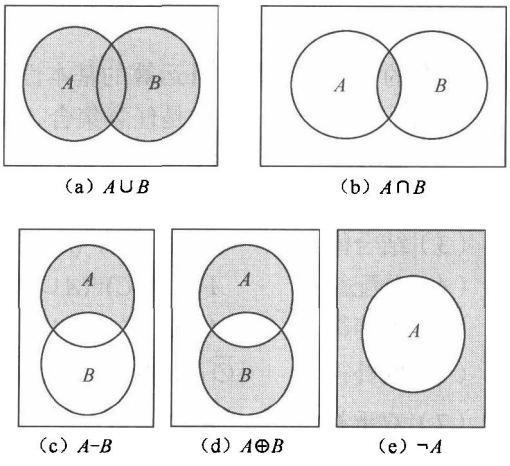
（3）$A$ 和 $B$ 的**差**，记为 $A-B$，它是由在 $A$ 中而不在 $B$ 中的元素所组成的集合，即 $A-B=\{x|x\in A$ 且 $x\notin B\}$。

（4）$A$ 和 $B$ 的**对称差**，记为 $A\oplus B$，$A\oplus B=(A-B)\cup(B-A)$。

（5）$A$ 的**补**，记为 $\overline{A}$ 或 $\neg A$，$\overline{A}=U-A$。

集合的并、交、差、对称差和补也分别称为集合的并运算、交运算、差运算、对称差运算和补运算。可用文氏图表示，如图 1.3 中的阴影部分。

**例 1.3**　设全集 $U=\{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$，$A=\{1, 2, 3, 4, 5\}$，$B=\{1, 2, 4, 6\}$，$C=\{7, 8\}$。则 $A\cup B=\{1, 2, 3, 4, 5, 6\}$，$A\cap B=\{1, 2, 4\}$，$A\cap C=\varnothing$，$A-B=\{3, 5\}$，$A-C=A$，$\overline{A}=\{6, 7, 8, 9, 10\}$，$\overline{B}=\{3, 5, 7, 8, 9, 10\}$。




(a) $A\cup B$　(b) $A\cap B$　(c) $A-B$　(d) $A\oplus B$　(e) $\neg A$

图 1.3

若 $A \cap B=\varnothing$，则称 $A$ 和 $B$ 不相交。由定义 1.10，集合的差和交之间的关系为

$$A-B=A \cap \overline{B}$$

利用集合运算的性质和集合相等的概念，我们可以对集合运算表达式的相等进行验证。由定理 1.1，两个集合相等的充要条件是这两个集合互为子集；即，左式 $\subseteq$ 右式，右式 $\subseteq$ 左式。所以可以根据定义 1.1，由对任意的 $x \in$ 左式推出 $x \in$ 右式，再由对任意的 $x \in$ 右式推出 $x \in$ 左式，来证明两个集合运算表达式相等。下面先介绍几个例子。

**例 1.4** 证明 $A \cap (B \cup C)=(A \cap B) \cup (A \cap C)$。

**证明：** 先证明左式 $\subseteq$ 右式，即 $A \cap (B \cup C) \subseteq (A \cap B) \cup (A \cap C)$。

对任意的 $x \in A \cap (B \cup C)$，根据定义 1.4，则 $x \in A$ 并且 $x \in B \cup C$，即 $x \in A$，并且 $x \in B$ 或者 $x \in C$。如果 $x \in B$，则 $x \in A \cap B$；如果 $x \in C$，则 $x \in A \cap C$；所以 $x \in (A \cap B) \cup (A \cap C)$，则 $A \cap (B \cup C) \subseteq (A \cap B) \cup (A \cap C)$。

再证明 $(A \cap B) \cup (A \cap C) \subseteq A \cap (B \cup C)$。同理，对任意的 $x \in (A \cap B) \cup (A \cap C)$，根据定义 1.4，$x \in A \cap B$ 或者 $x \in A \cap C$；则 $x \in A$ 并且 $x \in B$，或者 $x \in A$ 并且 $x \in C$；即 $x \in A$，并且 $x \in B$ 或者 $x \in C$，所以 $x \in A \cap (B \cup C)$，则 $(A \cap B) \cup (A \cap C) \subseteq A \cap (B \cup C)$。

所以，$A \cap (B \cup C)=(A \cap B) \cup (A \cap C)$。 □

**例 1.5** 若 $A \subseteq B$，则 $(A \cap B)=A$，$A \cup B=B$。

**证明：** 若 $A \subseteq B$，对任意的 $x \in A$，有 $x \in B$，所以 $x \in A \cap B$；则 $A \subseteq A \cap B$；另一方面 $A \cap B \subseteq A$；因此 $(A \cap B)=A$。

对任意的 $x \in A \cup B$，则 $x \in A$ 或者 $x \in B$。若 $x \in A$，因为 $A \subseteq B$，则 $x \in B$，所以 $A \cup B \subseteq B$；另一方面 $B \subseteq A \cup B$；因此 $A \cup B=B$。 □

**例 1.6** 证明 $\overline{A \cap B}=\overline{A} \cup \overline{B}$。

**证明：** 先证明 $\overline{A \cap B} \subseteq \overline{A} \cup \overline{B}$。

对任意 $x \in \overline{A \cap B}$，$x \notin A \cap B$，即 $x \notin A$ 或 $x \notin B$，故 $x \in \overline{A}$ 或 $x \in \overline{B}$，因此 $x \in \overline{A} \cup \overline{B}$。

再证明 $\overline{A} \cup \overline{B} \subseteq \overline{A \cap B}$。

对任意 $x \in \overline{A} \cup \overline{B}$，$x \in \overline{A}$ 或 $x \in \overline{B}$，如果 $x \notin \overline{A \cap B}$，则 $x \in A \cap B$，即 $x \in A$ 且 $x \in B$，与 $x \in \overline{A}$ 或 $x \in \overline{B}$ 矛盾，所以 $x \in A \cap B$。

因此 $\overline{A \cap B}=\overline{A} \cup \overline{B}$。 □

集合的并、交、差和补运算的基本性质概括如下。

**定理 1.4** 设 $A$，$B$，$C$ 是任意集合，$U$ 是全集，下列等式成立。

（1）幂等律　$A \cup A=A$　　$A \cap A=A$

（2）交换律　$A \cup B=B \cup A$　　$A \cap B=B \cap A$

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

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

（5）恒等律　$A \cup U=U$　$A \cap U=A$　$A \cup \varnothing=A$　$A \cap \varnothing=\varnothing$

（6）取补律　$\overline{\varnothing}=U, \overline{U}=\varnothing, A \cup \overline{A}=U, A \cap \overline{A}=\varnothing$

（7）双重补　$\overline{\overline{A}}=A$

（8）狄·摩根律　$\overline{A \cup B}=\overline{A} \cap \overline{B}, \overline{A \cap B}=\overline{A} \cup \overline{B}$

证明类似例 1.5、例 1.6 的证明。

**例 1.7**　证明（$A\cap B$）-（$A\cap C$）=$A\cap$（$B-C$）。

证明：$(A\cap B)-(A\cap C)=(A\cap B)\cap(\overline{A\cap C})$

$=(A\cap B)\cap(\overline{A}\cup\overline{B})=((A\cap B)\cap\overline{A})\cup((A\cap B)\cap\overline{C})$

$=\varnothing\cup(A\cap(B\cap\overline{C}))$

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

$=A\cap(B-C)$

**例 1.8**　证明 $A\oplus B=$（$A\cup B$）-（$A\cap B$）。

证明：$A\oplus B=(A-B)\cup(B-A)$

$=(A\cap\overline{B})\cup(B\cap\overline{A})$

$=((A\cap\overline{B})\cup B)\cap((A\cap\overline{B})\cup\overline{A})$

$=((A\cup B)\cap(\overline{B}\cup B))\cap((A\cup\overline{A})\cap(\overline{B}\cup\overline{A}))$

$=(A\cup B)\cap\overline{(B\cap A)}=(A-B)\cup(B-A)$　□

集合并、交可以推广到多个集合中去（见习题）。

**定义 1.11**　设集合 $A_1$，$A_2$，…，$A_n$，定义：

$A_1\cup A_2\cup\cdots\cup A_n=\{x|$至少有某个 $i$，$1\leqslant i\leqslant n$，$x\in A_i\}$，称为 $A_1$，$A_2$，…，$A_n$ 的并，记为 $\bigcup_{i=1}^{n}A_i$。

$A_1\cap A_2\cap\cdots\cap A_n=\{x|$对于所有的 $i$，$1\leqslant i\leqslant n$，$x\in A_i\}$，称为 $A_1$，$A_2$，…，$A_n$ 的交，记为 $\bigcap_{i=1}^{n}A_i$。

一般情况下，对于多个集合的运算，除对并（交）有结合律、交换律成立以外，还有如下定律。

设 $n$ 个集合 $A_1$，$A_2$，…，$A_n$ 和集合 $B$，则有

（1）分配律

$B\cap(A_1\cup A_2\cup\cdots\cup A_n)=(B\cap A_1)\cup(B\cap A_2)\cup\cdots\cup(B\cap A_n)$

$B\cup(A_1\cap A_2\cap\cdots\cap A_n)=(B\cup A_1)\cap(B\cup A_2)\cap\cdots\cap(B\cup A_n)$

（2）狄·摩根律

$$\overline{\bigcup_{i=1}^{n}A_i}=\bigcap_{i=1}^{n}\overline{A_i}$$

$$\overline{\bigcap_{i=1}^{n}A_i}=\bigcup_{i=1}^{n}\overline{A_i}$$

## 1.5　罗 素 悖 论

1874 年康托尔发表了一篇题为《关于所有实代数所组成集合的一个性质》的论文，开创了现代集合论的研究。随后，康托尔以他一系列杰出的工作为集合论奠定了基础，使集合论成为现代数学的一个重要的分支。然而，从康托尔创立集合论的时候起，就有一个既基本又明显的问题一直困惑着数学家们：集合论研究的对象是集合，可是集合是什么呢？我们在前面所提到的集合的概念是“具有共同性质的一些东西汇集成一个整体”，这是凭直观经验建

立起来的，一般称为朴素集合论。在朴素集合论中，似乎用不着为“集合”下一个严格的定义。但随着数学的发展，单凭直观经验建立起来的集合概念存在着问题，早在 1895 年康托尔就已经察觉到这一点，他和其他的一些数学家曾经举出不少例子指明朴素集合论将导致矛盾，其中最著名的例子是英国哲学家和数学家罗素（Russell，1872—1970）在 1901 年给出的，在数学史上称为罗素悖论。

在讨论悖论和罗素悖论之前，首先给出命题的概念。所谓命题，是指能区别真假的陈述语句。例如，“我是学生”和“今天不下雨”是命题，因为它们是能判别真假的陈述语句。而“祝你一帆风顺!”和“你明天下午出去吗？”这类祈使句和疑问句就不是命题。

所谓悖论，是指对于命题 $Q$，如果从 $Q$ 为真，可以推导出 $Q$ 为假，又从 $Q$ 为假可以推导出 $Q$ 为真，我们就说命题 $Q$ 是一个悖论。显然，如果从命题 $P$ 可引出一个命题 $Q$，而 $Q$ 是一个悖论，那么 $P$ 也是一个悖论。

在介绍罗素悖论之前，我们先介绍两个悖论：说谎悖论和理发师悖论。它们都是通俗而有趣的，能够帮助我们理解罗素悖论。

说谎悖论是一个古代的通俗悖论。有一个人断言：“我正在说谎”。我们要问：这个人是在说谎还是在讲真话?

如果他在说谎，这表明他的断言“我正在说谎”是谎话，也就是说他在讲真话。所以我们得出这样一个结论，如果他是说谎，那么他是讲真话（即没有说谎）。

另一方面，如果他讲真话，这表明他的断言“我正在说谎”是真话，也就是说他正说谎话，所以我们得出如下结论：如果他是讲真话，那么他在说谎（即没有讲真话）。

通过以上分析我们看到，以命题出现的断言“我正在说谎”就是一个悖论，因为我们无法断言它的真假。

1918 年罗素给出了理发师悖论：在一个村子里，有一个理发师宣布他给而且只给村子里所有自己不替自己理发的人理发。现在要问：谁给这个理发师理发?

如果理发师是由别人来给他理发，也就是说理发师自己不替自己理发，那么按照理发师自己所说的，这位理发师应该给他自己理发。

另一方面，如果理发师是由自己来给自己理发，那么按照理发师自己所说的，这个理发师不能给自己理发。

因此这也是一个悖论：理发师由别人来给他理发，不行；理发师由自己来给自己理发，也不行。

下面介绍罗素悖论。罗素悖论是相当简单的，一点也用不到集合论的专门知识。

罗素将集合分成两类：一类是集合 $A$ 本身是 $A$ 的一个元素，即 $A\in A$；如所有不是苹果的东西组成的集合，这个集合本身就不是苹果，所以它是这个集合自身的元素。另一类是集合 $A$ 本身不是 $A$ 的一个元素，即 $A\notin A$；如 26 个英语字母组成的集合，由于这个集合本身不是一个字母，所以这个集合不是它自身的元素。

由罗素的分类，我们构造一个集合 $S$：$S=\{A|A\notin A\}$。也就是说，$S$ 是由满足条件 $A\notin A$ 的那些集合 $A$ 组成的一个新的集合。我们要问：$S$ 是不是它自己的一个元素？即 $S\in S$，还是 $S\notin S$?

如果 $S\notin S$，因为集合 $S$ 由所有满足条件 $A\notin A$ 的集合组成，由于 $S\notin S$，所以 $S$ 满足对于集合 $S$ 中元素的定义，即 $S$ 是集合 $S$ 的元素，也就是说 $S\in S$。

如果 $S\in S$，因为 $S$ 中任一元素 $A$ 都有 $A\notin A$，又由于 $S\in S$，根据集合 $S$ 的规定，可知 $S$ 不

是集合 $S$ 的元素，也就是说 $S \notin S$。

这样，便得到了矛盾：既不是 $S \in S$，也不是 $S \notin S$。这个悖论就是著名的罗素悖论。

罗素悖论的出现，说明朴素集合论有问题，从而使数学的基础发生了动摇，引起了一些著名数学家的极大重视。在现代数学中，为了防止这类悖论的出现，产生各种公理化的集合论和不同的学派，这里不做介绍了。

## 习　　题

1.1　设 $A$，$B$，$C$ 是集合，判断下列命题真假。如果为真，给出证明；如果为假，给出反例。

（1）$A \notin B$，$B \in C \Rightarrow A \in C$。

（2）$A \notin B$，$B \notin C \Rightarrow A \notin C$。

（3）$A \in B$，$B \notin C \Rightarrow A \notin C$。

（4）$A \subset B$，$B \notin C \Rightarrow A \notin C$。

（5）$a \in A$，$A \subset B \Rightarrow a \in B$。

1.2　设 $A$，$B$ 是全集 $U$ 的子集，若 $A \subseteq B$，证明 $B-(B-A)=A$。

1.3　设 $A$，$B$，$C$ 是全集 $U$ 的任意子集。

（1）若 $A \cap B = A \cap C, \overline{A} \cap B = \overline{A} \cap C$，证明 $B = C$。

（2）若 $(A \cap C) \subseteq (B \cap C), (A \cap \overline{C}) \subseteq (B \cap \overline{C})$，证明 $A \subseteq B$。

1.4　（1）　设 $A \subseteq B$，$C \subseteq D$。

是否一定成立 $(A \cup C) \subseteq (B \cup D)$？

是否一定成立 $(A \cap C) \subseteq (B \cap D)$？

（2）$W \subset X$，$Y \subset Z$。

是否一定成立 $(W \cup Y) \subset (X \cup Z)$？

是否一定成立 $(W \cap Y) \subset (X \cap Z)$？

1.5　要使下列等式成立，集合 $A$ 和 $B$ 之间应满足什么条件？

（1）$\overline{B} \subseteq \overline{A}$。

（2）$\overline{A} \cap B = \varnothing$。

（3）$\overline{A \cup B} = \overline{B}$。

（4）$A-B=B$。

（5）$A-B=B-A$。

（6）$A \oplus B=B-A$。

1.6　证明：$A \times B=\varnothing$，当且仅当 $A$ 或 $B$ 为 $\varnothing$。

1.7　（1）已知 $A \subseteq C$，$B \subseteq D$，求证 $A \times B \subseteq C \times D$。

（2）已知 $A \times B \subseteq C \times D$，问是否有 $A \subseteq C$，$B \subseteq D$？

1.8　设 $A$ 是 $U$ 的子集，试求 $A \oplus A, A \oplus \overline{A}, U \oplus A$ 以及 $\varnothing \oplus A$。

1.9　对于下列命题，如果为真，则给出证明；否则给出反例。设 $A$，$B$ 和 $C$ 是全集 $U$ 的任意子集。