第 1 章 绪 论

计算机科学与技术学科是以数学和电子学科为基础发展起来的，该学科主要包含两方面的内容：一方面是研究计算机领域中的一些普遍规律，描述计算的基本概念与模型，其重点是描述现象，解释规律。另一方面是包括计算机硬件、软件（系统软件和应用软件）在内的计算系统设计和实现的工程技术。因此，我们称这个学科为计算机科学与技术学科。在科学的“发现自然规律”、“实验”和“计算”三个范型中，计算机科学与技术学科的研究与实践主要涉及实验范型和计算范型，这也表明，有些研究可以是以理论研究为主，有些研究可以是以实践为主。所以，对计算机科学与技术学科来说，理论和实践教学都是非常重要的，而其中的理论是基础。按照计算机科学与技术学科方法论的“抽象”、“理论”、“设计”三个过程来看，实际工作通过理论得到升华，而在理论指导下的设计（实现）才可能是理性的、高水平的。实际系统设计的突破往往等待理论上的突破——新理论的诞生。

简单地说，计算机科学与技术学科通过在计算机上建立模型并模拟物理过程来进行科学调查和研究，它系统地研究信息描述和变换算法，主要包括信息描述和变换算法的理论、分析、效率、实现和应用。

随着计算机科学与技术学科的发展，以及人们对该学科的认识的不断深化，我们认为，该学科的根本问题是：什么能被(有效地)自动化。

问题的计算机求解建立在高度抽象的基础上，问题的符号表示及处理过程的机械化、严格化等固有特性决定了数学是计算机科学与技术学科的重要基础之一，数学及其形式化描述以及严密的表达和计算，是计算机科学与技术学科所用的重要工具。建立物理符号系统并对其实施变换是计算机科学与技术学科进行问题描述和求解的重要手段。学科所要求的计算机问题求解的“可行性”限定了从问题抽象开始到根据适当理论的指导进行设计(实现)的科学实践过程；“可行性”所需要的“形式化”后呈现出的“离散

特征”，实质上限定了计算机科学与技术学科进行问题求解的重要特征。

本章简要回顾离散数学中学过的部分基本概念和方法，以使读者能够顺利地进行本书主要内容的学习。如果读者对这部分内容比较熟悉，建议快速地浏览 1.1～1.3 节，从而熟悉本书的符号使用方式和对问题的叙述方式。

另外，建议读者能较好地完成本章后面所列的习题，尤其是一些构造性的题目，以及关于语言的所有题目，因为它们对后续内容的学习是十分重要的。

本章的主要内容有两部分：一是有关集合、关系、图、证明方法的基本知识；另外讲述形式语言及其相关的基本概念。

1.1 集合的基础知识

集合论(set theory)是德国数学家康托(Geog Cantor)于 1874 年创立的，至今已经历了两个阶段：1908 年以前称为朴素集合论，又称为康托集合论。在朴素集合论中，存在着严重的集合悖论的问题。在朴素集合论刚出现时，人们认为找到了数学的基础，而集合悖论的发现使得人们无比沮丧，觉得数学失去了重要的基础，甚至有人认为以严密为重要特征的数学是不可靠的。为了避免集合悖论，哲墨罗（E. Zermelo)于 1908 年提出了第一个集合论公理系统，后经富兰科尔（A. A. Fraenkel）和斯库利姆(A. T. Skolem)的改进和补充,形成了 ZF 公理系统。同年，B. 罗素也给出了关于集合的型的层次理论——类型论。

无论如何，人们还是公认集合论在数学中占有非常重要的地位，它的基本概念已经渗透到许多领域。计算机科学与技术学科出现后，也将集合论作为其重要基础之一。计算机科学与技术领域中的大多数基本概念和理论几乎都采用了与集合论有关的术语来描述。

1.1.1 集合及其表示

集合是集合论中最原始的概念。我们只能给出它的非形式描述，以说明它的意义：一定范围内确定的，并且彼此可以区分的对象汇集在一起形成的整体叫作集合（set），简称为集。简单地说，集合是具有某种性质的对象的全体。构成集合的每一个对象称为这个集合的一个成员，它们可以是具体的东西，也可以是抽象的概念。通常称集合的成员为该集合的元素(element)。

例 1-1 集合的实际例子。

(1) 北京市的所有交通工具汇集在一起构成一个集合。

(2) 北京市的所有公共汽车是一个集合。

(3) 中国所有高等院校组成一个集合。

(4) 某高校的所有院系构成一个集合。

(5) 全体自然数构成一个集合；全体有理数构成一个集合；全体实数构成一个集合。

(6) 一个学校的所有班级的全体是一个集合；一个班的学生的全体是一个集合；一个学生的所有用品的全体是一个集合。

(7) 1,2,3,5,8,13 构成一个集合。

(8) 学生、教师构成一个集合。

显然，对象和集合之间有这样一种关系：该对象要么是该集合的一个元素，要么不是该集合的元素，两者必居其一。一个集合中的元素可能都在另一个集合中，也可能部分在另一个集合中。一个对象可以是某一个集合的元素，它本身也可以是一个集合。

通常我们用大写的英文字母 $A,B,C,\cdots$ 和大写的希腊字母 $\Gamma,\Sigma,\varnothing,\cdots$ 表示集合，用小写字母 $a,b,c,\cdots$ 表示集合的元素。例如，一般地，

$\mathbf{N}$—— 表示全体自然数集合

$\mathbf{Q}$—— 表示全体有理数集合

$\mathbf{R}$—— 表示全体实数集合

Σ——表示字母的集合

关于集合和元素，我们用如下的记法：

如果 a 是集合 A 的一个元素，则记为 $a\in A$，读作 a 属于 A，或者 A 含有 a；否则记为 $a\notin A$，读作 a 不属于 A，或者 A 不含 a。

例 1-2 集合与元素。

(1) $6\in\mathbf{N},1\in\mathbf{N},1.5\notin\mathbf{N},0.81\notin\mathbf{N}$。

(2) $4\in\mathbf{N},1.5\notin\mathbf{N},4\in\mathbf{Q},1.5\in\mathbf{Q},4\in\mathbf{R},1.5\in\mathbf{R}$。

(3) 设 U 是中国所有高等院校组成的集合，则有

清华大学 $\in U$，北京大学 $\in U$，北京工业大学 $\in U$

(4) 设北京工业大学表示该校所有院系组成的集合，则有

计算机学院 $\in$ 北京工业大学

集合可以用两种形式加以描述：

第一种形式称为列举法(listing)：将所有的元素逐一地列举在大括号 { } 中，读者能立即看出规律时，某些元素可用省略号表示。

例 1-3 集合的列举表示。

(1) $\{1,3,6,9,10\}$.

(2) $\{a,b,c,\cdots,z\}$.

(3) {本科生,硕士研究生,博士研究生,进修生}.

(4) {1.2,3,4,5,…}.

(5) {0.5.10.15,…,200}.

值得注意的是，在使用列举法时，集合中元素出现的先后顺序是没有意义的。例如,{1,3,6,9,10} 与{6,3,10,9,1} 表示的是同一个集合。

集合的第二种表示形式称为命题法（proposition）,其基本形式为

$$\{x \mid P(x)\}$$

其中 P 为谓词，表示此集合包括所有使 P 为真的 x。

例 1-4 集合的命题表示。

(1) $\{x \mid 0 \leqslant x \leqslant 200$ 且 $(\exists n \in N(n \cdot 5 = x))\}$.

(2) $\{x \mid 3x^2+8x+4=0\}$.

(3) $\{x \mid x \in [0.1]\}$.

(4) {x | x∈{本科生,硕士研究生,博士研究生,进修生}}.

在有的集合中，一个元素可以重复出现，这种集合称为多重集合。本书不考虑多重集合的问题，所提到的集合均不允许一个元素重复出现。

由有限个元素构成的集合叫作有限集（finite set），又称为有穷集。由无穷多个元素构成的集合叫作无穷集（infinite set）。这是一个直观的描述，作为一个思考题，读者可以根据定义 1-1 分别给有穷集和无穷集一个比较严格的定义。

定义 1-1 如果集合 A, B 之间有一个一一对应，则称它们具有相同的基数（cardinality）,通常用 $|A|$ 表示集合 A 的基数。

集合的基数又叫作集合的势。

对有穷集来说，它的基数就是它所包含的元素的个数。

例 1-5 有穷集合的基数。

(1) $|\{x \mid 0 \leqslant x \leqslant 200$ 且 $(\exists n \in N(n \cdot 5 = x))\}| = 41$。

(2) $|\{x \mid 3x^2+8x+4=0\}| = 2$.

(3) $|\{a,b,c,\cdots,z\}| = 26$.

(4) |{本科生，硕士研究生，博士研究生，进修生}|=4。

如果 $|A|=0$,则称 A 为空集（null set）,一般用 $\varnothing$ 表示。

无穷集可以分成可数集（countable infinite set 或 countable set）和不可数集（uncountable set）.

设 S 是一个无穷集，如果集合 S 与自然数集 N({1,2,3,4,…})具有相同的基数,则称 S 是可数无穷的集合，简称 S 是可数的 否则,称 S 是不可数集。

例如，整数集、有理数集是可数的，实数集是不可数的。实数集的不可数性质可以

用著名的对角线法（diagonalization）进行证明。在本书的后续章节中，有穷集和可数无穷集是我们讨论的主要对象。如果读者不了解对角线法，建议查阅相应的参考书，因为该方法是计算机科学中的一个非常重要的方法。

1.1.2 集合之间的关系

前面曾经提到，一个集合中的元素可能都在另一个集合中，也可能部分含在另一个集合中。一个对象可以是某一个集合的元素，它本身也可以是一个集合。这就是说，集合之间有着不同的关系，显然，这些关系是集合所表示的对象之间关系的一种抽象，这就是子集和相等的概念。

定义 1-2 设 A,B 是两个集合，如果集合 A 中的每个元素都是集合 B 的元素，则称集合 A 是集合 B 的子集(subset)，集合 B 是集合 A 的包集(container)。记作 $A\subseteq B$，也可记作 $B\supseteq A$。

$A\subseteq B$ 读作集合 A 包含在集合 B 中；$B\supseteq A$ 读作集合 B 包含集合 A。

由定义可知，$A\subset B$ 的充要条件是：对于 A 中的每一个元素 a，均有 $a\in B$。为了简洁起见，P_1 是 P_2 的充要条件记为

$$P_1\Leftrightarrow P_2$$

或者

$$P_2 \text{ iff } P_1$$

此外，今后还会经常地使用如下全程量词和存在量词：

“$\forall x\cdots$”表示“对所有的 $x\cdots$”；“$\exists x\cdots$”表示“存在一个 $x\cdots$”。

按照此约定，有

$A\subseteq B\Leftrightarrow \forall x\in A, x\in B$ 成立，

也就是

$A\subseteq B \text{ iff } \forall x\in A, x\in B$ 成立。

例 1-6 子集。

(1) $\{1,3,6,9,10\}\subseteq \mathbf{N}$。

(2) $\{a,b,c,\cdots,z\}\subseteq \{a,b,c,\cdots,z,A,B,C,\cdots,Z\}$.

(3) $\{a,b,c,\cdots,z\}\subseteq\{a,b,c,\cdots,z\}$.

(4) 对任意集合 S，$\varnothing\subseteq S, S\subseteq S$。

在此例中，(2)与(3)是有差别的，$\{a,b,c,\cdots,z,A,B,C,\cdots,Z\}$ 中除了含有 26 个小写英文字母外，还含有 26 个大写英文字母，而这 26 个大写英文字母在 $\{a,b,c,\cdots,z\}$ 中是没有的。直观上，$\{a,b,c,\cdots,z\}$ 是 $\{a,b,c,\cdots,z,A,B,C,\cdots,Z\}$ 的真正的子集。

定义 1-3 设 A,B 是两个集合，如果 $A\subseteq B$，且 $\exists x\in B$，但 $x\notin A$，则称 A 是 B 的真

子集(proper subset),记作 $A\subset B$。

例 1-7 真子集。

(1) $\{1,3,6,9,10\}\subset\mathbf{N}$。

(2) $\{a,b,c,\cdots,z\}\subset\{a,b,c,\cdots,z,A,B,C,\cdots,Z\}$。

(3) $\{-2\}\subset\{x|3x^2+8x+4=0\}$。(注意,$-2\in\{x|3x^2+8x+4=0\}$ 也成立,但这种写法表达的意义不同。)

(4) 对任意非空集合 S,$\varnothing\subset S$。

根据包含的定义,$\{a,b,c,\cdots,z\}$ 与 $\{a,b,c,\cdots,z\}$ 有互相包含、互为子集的关系,而且,对任意的集合 S,S 与 S 也有互相包含、互为子集的关系,因为它们实际是同一个集合。

定义 1-4 如果集合 A,B 含有的元素完全相同,则称集合 A 与集合 B 相等(equivalence),记作 $A=B$。

对于任意集合 A,B,C,我们不难得到如下结论:

(1) $A=B$ iff $A\subseteq B$ 且 $B\subseteq A$。

(2) 如果 $A\subseteq B$,则 $|A|\leqslant|B|$。

(3) 如果 $A\subset B$,则 $|A|\leqslant|B|$。

(4) 如果 A 是有穷集,且 $A\subset B$,则 $|B|>|A|$。

(5) 如果 $A\subseteq B$,则对 $\forall x\in A$,有 $x\in B$。

(6) 如果 $A\subset B$,则对 $\forall x\in A$,有 $x\in B$ 并且 $\exists x\in B$,但 $x\notin A$。

(7) 如果 $A\subseteq B$ 且 $B\subseteq C$,则 $A\subseteq C$。

(8) 如果 $A\subset B$ 且 $B\subset C$,则 $A\subset C$。

(9) 如果 $A=B$,则 $|A|=|B|$。

(10) 如果 $A\subset B$ 且 $B\subseteq C$,或者 $A\subseteq B$ 且 $B\subset C$,则 $A\subset C$。

1.1.3 集合的运算

某专业 2001 年招收了两个班的学生,其中一个班的学生用 C_1 表示,另一个班的学生用 C_2 表示,那么如何表示这两个班的学生呢?显然,这两个班的学生应该是 C_1 中的元素和 C_2 中的元素合并在一起构成的集合。为了解决类似的问题,和其他数学系统一样,我们在集合中引入若干种运算。当然,引入运算的最初目的是为了如上所提由已知集合获取新的集合,但是,除此之外,我们还能通过所引入的运算的特性,而达到获取相关集合的特性、简化所得公式等目的。

本节简单介绍集合的几个基本运算。

1. 并

定义 1-5　设 A,B 是两个集合，A 与 B 的并(union)是一个集合，该集合中的元素要么是 A 的元素，要么是 B 的元素，记作 $A\cup B$。

$$A\cup B=\{a\mid a\in A \text{ 或者 } a\in B\}$$

“$\cup$”为并运算符，$A\cup B$读作 A 并 B(A 与 B 的并)。

例 1-8　集合的并。

(1) 设 $A=\{1,3,5,7,\cdots\},B=\{2,4,6,8,\cdots\}$，则 $A\cup B=\{1,2,3,4,5,\cdots\}$.

(2) 设 $A=\{$红，黄，蓝，白$\},B=\{$紫，青，绿，橙，黑$\}$，则 $A\cup B=\{$紫，青，绿，橙，黑，红，黄，蓝，白$\}$.

(3) 设 $A=\{1,2,3,4,\cdots\},B=\{2,4,6,8,\cdots\}$，则 $A\cup B=\{1,2,3,4,5,\cdots\}$.

(4) 设 $A=\{$红，青，黄，蓝，绿，白$\},B=\{$紫，蓝，青，绿，橙，黑$\}$，则 $A\cup B=\{$紫，青，绿，橙，黑，红，黄，蓝，白$\}$。

对任意集合 A,B,C，不难证明以下结论：

(1) $A\cup B=B\cup A$.

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

(3) $A\cup A=A$。

(4) $A\cup B=A$ iff $B\subseteq A$.

(5) $\varnothing\cup A=A$.

(6) $|A\cup B|\leqslant|A|+|B|$.

下面将集合的并推广到多个和无穷多个集合上。

定义 1-5′　设 $A_1,A_2,\cdots,A_n$ 是 n 个集合，则它们的并

$$A_1\cup A_2\cup\cdots\cup A_n=\{a\mid \exists i.1\leqslant i\leqslant n,\text{使得 } a\in A_i\}$$

可记为 $\bigcup_{i=1}^{n}A_i$。

设 $A_1,A_2,\cdots,A_n,\cdots$是一个集合的无穷序列，则它们的并

$$A_1\cup A_2\cup\cdots\cup A_n\cup\cdots=\{a\mid \exists i,i\in N,\text{使得 } a\in A_i\}$$

可记为 $\bigcup_{i=1}^{\infty}A_i$。

当一个集合的元素都是集合时，我们将这样的集合称为集族。设 S 是一个集族，则 S 中的所有元素的并为

$$\bigcup_{A\in S}A=\{a\mid \exists A\in S,a\in A\}$$

2. 交

定义 1-6 设 A,B 是两个集合，A 与 B 的交(intersection)是一个集合，该集合是由既属于 A，又属于 B 的所有元素组成，记作 $A\cap B$。

$$A\cap B=\{a\mid a\in A \text{ 且 } a\in B\}$$

如果 $A\cap B=\varnothing$，则称 A 与 B 不相交。

“$\cap$”为交运算符，$A\cap B$ 读作 A 交 B(A 与 B 的交)。

例 1-9 集合的交。

(1) 设 $A=\{1,3,5,7,\cdots\},B=\{2,4,6,8,\cdots\}$，则 $A\cap B=\varnothing$.

(2) 设 $A=\{a\mid a$ 是哈尔滨工业大学 7742 班的来自于南方的同学$\}$，$B=\{a\mid a$ 是哈尔滨工业大学 7742班的当过工人或者农民的同学$\}$，则 $A\cap B=\{a\mid a$ 是哈尔滨工业大学 7742班的来自于南方的并且当过工人或者农民的同学$\}$.

(3) 设 $A=\{1,2,3,4,\cdots\},B=\{2,4,6,8,\cdots\}$，则 $A\cap B=\{2,4,6,8,\cdots\}=B$。

(4) 设 $A=\{$红，青，黄，蓝，绿，白$\}$，$B=\{$紫，蓝，青，绿，橙，黑$\}$，则 $A\cap B=\{$青，蓝，绿$\}$.

对任意集合 A,B,C，不难证明以下结论：

(1) $A\cap B=B\cap A$.

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

(3) $A\cap A=A$.

(4) $A\cap B=A$ iff $A\subseteq B$.

(5) $\varnothing\cap A=\varnothing$.

(6) $|A\cap B|\leqslant\min\{|A|,|B|\}$.

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

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

(9) $A\cap(A\cup B)=A$。

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

根据交的基本定义，读者可以用与定义 1-5′类似的方式将集合的交推广到多个和无穷多个集合上。

3. 差

定义 1-7 设 A,B 是两个集合，A 与 B 的差(difference) 是一个集合，该集合是由属于 A，但不属于 B 的所有元素组成，记作 $A-B$。

$$A-B=\{a\mid a\in A \text{ 且 } a\notin B\}$$

“ $-$ ”为减(差)运算符，$A-B$ 读作 A 减 B(A 与 B 之差)。

例 1-10 集合的差。

(1) 设 $A=\{1,3,5,7,\cdots\}$，$B=\{2,4,6,8,\cdots\}$，则 $A-B=A$。

(2) 设 $A=\{a \mid a$ 是哈尔滨工业大学 7742 班的来自于南方的同学$\}$，$B=\{a \mid a$ 是哈尔滨工业大学 7742 班的当过工人或者农民的同学$\}$，则 $A-B=\{a \mid a$ 是哈尔滨工业大学 7742 班的来自于南方的并且没有当过工人或者农民的同学$\}$.

(3) 设 $A=\{1,2,3,4,\cdots\}$，$B=\{2,4,6,8,\cdots\}$，则 $A-B=\{1,3,5,7,\cdots\}$.

(4) 设 $A=\{$红，青，黄，蓝，绿，白$\}$，$B=\{$紫，蓝，青，绿，橙，黑$\}$，则 $A-B=\{$红，黄，白$\}$.

(5) 设 $A=\{1,2,3,4\}$，$B=\{2,4,6,8,\cdots\}$，则 $A-B=\{1,3\}$.

(6) 设 $A=\{1,2,3,4\}$，$B=\{6,7,8,9,\cdots,200\}$，则 $A-B=\{1,2,3,4\}$.

对任意集合 A,B,C，不难证明以下结论：

(1) $A-A=\varnothing$.

(2) $A-\varnothing=A$.

(3) $A-B \neq B-A$.

(4) $A-B=A$ iff $A \cap B=\varnothing$.

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

(6) $|A-B| \leqslant |A|$.

定义 1-8 设 A,B 是两个集合，A 与 B 的对称差(symmetric difference)是一个集合，该集合由属于 A 但不属于 B，以及属于 B 但不属于 A 的所有元素组成，记作 $A \oplus B$。

$$A \oplus B = \{a \mid a \in A \text{ 且 } a \notin B \text{ 或者 } a \notin A \text{ 且 } a \in B\}$$

显然，对集合 A,B，有

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

“ ④ ”为对称差运算符，$A \oplus B$ 读作 A 对称减 B(A 与 B 的对称差)。

4. 笛卡儿积

定义 1-9 设 A,B 是两个集合，A 与 B 的笛卡儿积（Cartesian product ）是一个集合，该集合由所有这样的有序对(a,b)组成，其中 $a \in A, b \in B$，记作 $A \times B$。

$$A \times B = \{(a,b) \mid a \in A \text{ 且 } b \in B\}$$

“ $\times$ ”为集合的笛卡儿积运算符，$A \times B$ 读作 A 叉乘 B(A 与 B 的笛卡儿积）。

例 1-11 集合的笛卡儿积。

(1) 设 $A=\{1,3,5,7,\cdots\}$，$B=\{2,4,6,8,\cdots\}$，则

$A \times B=\{(a,b) \mid a$ 是任意的正奇数，b 是任意的正偶数$\}$.

(2) 设 $A=\{1,2,3,4\}$, $B=\{$红,绿,青$\}$,则

$A\times B=\{(1$,红$),(1$,绿$),(1$,青$),(2$,红$),(2$,绿$),(2$,青$),(3$,红$),(3$,绿$),(3$,青$),(4$,红$),(4$,绿$),(4$,青$)\}$.

(3) 设 $A=\{1,2,3,4\}$,则

$A\times A=\{(1,1),(1,2),(1,3),(1,4),(2,1),(2,2),(2,3),(2,4),(3,1),(3,2),(3,3),(3,4),(4,1),(4,2),(4,3),(4,4)\}$.

(4) 设楼上、楼下共有两个开关控制同一个电灯，开关的状态有两种：开、关。设此状态集为集合 A:$A=\{$开,关$\}$，则系统开关的状态可用如下集合表示：

$A\times A=\{$(开,开),(开,关),(关,开),(关,关)$\}$.

对任意集合 A,B,C，不难证明以下结论：

(1) $A\times B\neq B\times A$.

(2) $(A\times B)\times C\neq A\times(B\times C)$.

(3) $A\times A\neq A$.

(4) $A\times\varnothing=\varnothing$.

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

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

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

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

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

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

(11) 当 A,B 为有穷集时,$|A\times B|=|A||B|$。

5. 幂集

定义 1-10 设 A 是一个集合,A 的幂集(power set)是一个集合,该集合由 A 的所有子集组成,记作 2^A.

$$2^A=\{B\mid B\subseteq A\}$$

2^A 读作 A 的幂集。

例 1-12 集合的幂集。

(1) 设 $A=\{1,2,3\}$,则 $2^A=\{\varnothing,\{1\},\{2\},\{3\},\{1,2\},\{1,3\},\{2,3\},\{1,2,3\}\}$.

(2) 设有红、绿、黄、白四种不同颜色的标志，问这些标志的不同取法有哪些？

为解决此问题，设 $A=\{$红,绿,黄,白$\}$,则

$2^A=\{\varnothing,\{$红$\},\{$绿$\},\{$黄$\},\{$白$\},\{$红,绿$\},\{$红,黄$\},\{$红,白$\},\{$绿,黄$\},\{$绿,白$\},\{$黄,白$\},\{$红,黄,白$\},\{$红,绿,白$\},\{$红,绿,黄$\},\{$绿,黄,白$\},\{$红,绿,黄,白$\}\}$.

2^A 中的每个元素对应一种取法，共有 16 种取法。例如，{红，绿}表示取红、绿两个标志；{红，绿，黄，白}表示取全部标志；$\varnothing$ 表示什么标志都不取。

对任意集合 A,B，不难证明以下结论：

(1) $\varnothing \in 2^A$.

(2) $\varnothing \subseteq 2^A$.

(3) $\varnothing \subset 2^A$.

(4) $2^{\varnothing}=\{\varnothing\}$.

(5) $A \in 2^A$.

(6) 如果 A 是有穷集，则 $|2^A|=2^{|A|}$.

(7) $2^{A\cap B}=2^A \cap 2^B$.

(8) 如果 $A \subseteq B$，则 $2^A \subseteq 2^B$。

6. 补集

在实际工作和生活中，我们都会在一定的范围内讨论问题，我们把讨论问题的范围叫作论域。如果集合 A 是论域 U 上的一个集合，则 $A \subseteq U$。在这里对集合的讨论均限于对 U 上的集合的讨论。

定义 1-11 设 A 是论域 U 上的一个集合，A 的补集(complementary set)是一个集合，该集合由在 U 中，但不在 A 中的所有元素组成，记作 $\overline{A}$。

$$A=U-A$$

补集又叫作余集。有的书上使用其他符号表示补运算，如 C_U. ~. $\overline{A}$ 读作 A(关于论域 U)的补集(U 中子集 A 的补集)。

例 1-13 集合的补集。

设 $U=\{1,2,3,4,5\}, A=\{4,2\}$，则 $\overline{A}=\{1,3,5\}$.

设 U 是论域，A,B 是 U 上的集合，则有下列结论：

(1) $\varnothing=U$。

(2) $U=\varnothing$.

(3) 如果 $A \subset B$，则 $\overline{B} \subseteq \overline{A}$。

(4) $A \cup \overline{A}=U$。

(5) $A \cap \overline{A}=\varnothing$.

(6) $B=A \Leftrightarrow A \cup B=U$ 且 $A \cap B=\varnothing$。

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

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

其中(7),(8)是著名的 De Morgan 公式的简单形式。

1.2 关　　系

具有某种性质的一些对象可以组成一个集合。这就是说，集合描述的是事物。但世界上的事物是运动的、变化的，它们既相互区别，又相互联系。我们用关系这一个概念来反映对象（集合元素）之间的联系和性质。

1.2.1 二元关系

我们希望关系能够表达集合中元素之间的联系和性质。实际上，关系的概念正是建立在日常生活中关系的基础上，用来抽象地表达这些关系的。例如，一个班的同学中存在有同龄、同乡、成绩好、兴趣不同等各种关系。集合 $\{1,3,4,8\}$ 和集合 $\{0,3,5,7\}$ 的元素之间存在大于、大于等于、小于等关系。下面先从通常意义下的大于、小于关系的描述开始，逐步给出二元关系的描述。

集合 $\{1,3,4,8\}$ 和集合 $\{0,3,5,7\}$ 的元素之间存在的小于关系有

$$1<3,1<5,1<7,3<5,3<7,4<5,4<7.$$

存在的大于关系有

$$1>0,3>0,4>0,4>3,8>0,8>3,8>5,8>7.$$

现在将小于关系换一种表示方法，如 $1<3$ 表示成 $(1,3)$，这样我们可以将集合 $\{1,3,4,8\}$ 和集合 $\{0,3,5,7\}$ 的元素之间存在的小于关系表示为

$$\{(1,3),(1,5),(1,7),(3,5),(3,7),(4,5),(4,7)\}.$$

这是一个集合，我们将其记作 $R_<$。类似地，可以将集合 $\{1,3,4,8\}$ 和集合 $\{0,3,5,7\}$ 的元素之间存在的大于关系表示为

$$\{(1,0),(3,0),(4,0),(4,3),(8,0),(8,3),(8,5),(8,7)\}.$$

并记为 $R_>$。显然，

$$R_<\subseteq\{1,3,4,8\}\times\{0,3,5,7\},R_>\subseteq\{1,3,4,8\}\times\{0,3,5,7\}.$$

可见，集合 $\{1,3,4,8\}$ 到集合 $\{0,3,5,7\}$ 的不同的二元关系实际上是 $\{1,3,4,8\}\times\{0,3,5,7\}$ 的不同子集，而“$1<3,1<5,1<7,3<5,3<7,4<5,4<7$”和 $\{(1,3),(1,5),(1,7),(3,5),(3,7),(4,5),(4,7)\}$ 只是表现形式不同罢了。于是，我们有

定义 1-12　设 A,B 是两个集合，任意的 $R\subseteq A\times B$，R 是 A 到 B 的二元关系（binary relation）。

$(a,b)\in R$，表示 a 与 b 满足关系 R，按照中缀形式，也可表示为 aRb。A 称为定义域（domain），B 称为值域（range）。当 $A=B$ 时，则称 R 是 A 上的二元关系。

定义 1-13　设 R 是 A 上的二元关系，有

(1) 如果对任意一个 $a\in A$,有$(a,a)\in R$,则称 R是自反的(reflexive)。

(2) 如果对任意一个 $a\in A$,有$(a,a)\notin R$,则称 R 是反自反的 (irreflexive)。

(3) 如果对任意的 $a,b\in A$, 当$(b,a)\in R$ 时,必有$(a,b)\in R$,则称 R 是对称的(symmetric).

(4) 如果对任意的 $a,b\in A$,当$(b,a)\in R$和$(a,b)\in R$ 同时成立时, 必有 $a=b$,则称 R是反对称的(asymmetric)。

(5) 如果对任意的 $a,b,c\in A$,当$(a,b)\in R$和$(b,c)\in R$ 同时成立时, 必有$(a,c)\in R$,则称 R 是传递的(transitive) .

条件(1),(3),(5) 合并在一起叫作关系的三歧性。

例 1-14 关系的性质。

(1) “=”关系是自反的、对称的、传递的。

(2) “>”,“<”关系是反自反的、传递的。

(3) “≥”,“≤”关系是自反的、反对称的、传递的。

(4) 集合之间的包含关系是自反的、反对称的、传递的。

(5) 整数集上的模 n 同余关系是自反的、对称的、传递的。

(6) 通常意义下的父子关系是反自反的、非传递的。

(7) 通常意义下的兄弟关系是反自反的、传递的。

(8) 通常意义下的祖先关系是反自反的、传递的。

1.2.2 等价关系与等价类

定义 1-14 如果集合 A 上的二元关系 R 是自反的、对称的、传递的,则称 R 是等价关系(equivalence relation)。

例如,实数集上的“=”关系,整数集上的模 n 同余关系,通常意义下的“在同一个学校工作”的关系,“户口在同一个省、市”的关系等都是等价关系。

在“在同一个学校工作”的限制下,我们将全国的教师分成不同的集合,每个集合对应一所学校。按照不考虑兼职问题和其他的类似“不在册”等问题的假设,每个教师在且仅在一个学校对应的集合中。而在“户口在同一个省、市”的限制下,我们将全国人民分成不同的集合,每个集合对应一个省、市。按照我国现行的户籍制度,每个人在且仅在一个省、市对应的集合中。由此,我们可以考虑利用集合 S上的等价关系 R 将 S划分成若干个等价类。

定义 1-15 设 R是集合 S上的等价关系,则满足如下要求的 S 的划分$S_1,S_2,S_3,\cdots,S_n$称为 S 关于 R 的等价划分,S_i 称为等价类(equivalence class)。

(1) $S=S_1\cup S_2\cup S_3\cup\cdots\cup S_n\cup\cdots$。

(2)如果 $i\neq j$,则 $S_i\cap S_j=\varnothing$。

(3)对任意的 i,S_i 中的任意两个元素 a,b,aRb 恒成立。

(4)对任意的 $i,j,i\neq j$,S_i 中的任意元素 a 和 S_j 中的任意元素 b,aRb 恒不成立。

我们把 R 将 S 分成的等价类的个数称为 R 在 S 上的指数(index)。有时候,R 可将 S 分成有穷多个等价类,此时称 R 具有有穷指数;有时候,R 可将 S 分成无穷多个等价类,此时称 R 具有无穷指数。

例 1-15 等价类。

(1)“=”关系将自然数集 N 分成无穷多个等价类:$\{1\},\{2\},\{3\},\{4\},\cdots$。

(2)非负整数集上的模 5 同余关系将 $\{0,1,2,3,\cdots\}$ 分成 5 个等价类:

$\{0,5,10,15,20,\cdots\}$

$\{1,6,11,16,21,\cdots\}$

$\{2,7,12,17,22,\cdots\}$

$\{3,8,13,18,23,\cdots\}$

$\{4,9,14,19,24,\cdots\}$

(3)某计算机学院 2001 年招收本科生 420 名,分成 12 个班,按同班同学的关系划分,这 420 个同学分成 12 个等价类,每个等价类对应一个班。

值得注意的是,给定集合 S 上的一个等价关系 R,R 就确定了 S 的一个等价类。当给定另一个不同的等价关系时,它会确定 S 的一个新的等价类。

例如,令 $S=\{1,2,3,4\}$,通常意义下的“=”将 S 分成 4 个等价类:$\{1\},\{2\},\{3\},\{4\}$。如果取 $R=\{(1,1),(2,1),(1,2),(2,2),(3,3),(3,4),(4,3),(4,4)\}$,则 R 将 S 分成两个等价类:$\{1,2\},\{3,4\}$。

1.2.3 关系的合成

在日常生活中,关系是可以合成的。例如,“父子”关系,“父女”关系就可以合成为“祖孙女”关系。张宏是张春的父亲,张春是张燕的父亲,所以,张宏是张燕的爷爷。形式上,可以描述为

(张宏,张春)∈父子

(张春,张燕)∈父女

(张宏,张燕)∈祖孙女

这就是说,关系“父子”与“父女”合成关系“祖孙女”,这个合成要求“父子”在前;“父女”在后。显然;“父女”在前;“父子”在后是无法合成的。而“父女”在前;“母子”在后是可以合成的。

定义 1-16 设 $R_1\subseteq A\times B$ 是 A 到 B 的关系,$R_2\subseteq B\times C$ 是 B 到 C 的关系,则 R_1 与

R_2 的合成(composition) $R_1 \circ R_2$ 是 A 到 C 的关系。

$$R_1 \circ R_2 = \{(a,c) \mid \exists (a,b) \in R_1 \text{ 且 } (b,c) \in R_2\}$$

为了方便起见，约定在今后的叙述中，如果意义明确，关系的合成运算符“ ”可以省略不写，如 $R_1 \circ R_2$ 可以写成 R_1R_2。

例 1-16 设 R_1, R_2 是集合 $\{1,2,3,4\}$ 上的关系，其中

$R_1 = \{(1,1),(1,2),(2,3),(3,4)\}$，

$R_2 = \{(2,4),(4,1),(4,3),(3,1),(3,4)\}$，

(1) $R_1R_2 \neq R_2R_1$。

(2) $(R_1R_2)R_3 = R_1(R_2R_3)$。 （结合律）

(3) $(R_1 \cup R_2)R_3 = R_1R_3 \cup R_2R_3$。 （右分配律）

(4) $R_3(R_1 \cup R_2) = R_3R_1 \cup R_3R_2$。 （左分配律）

(5) $(R_1 \cap R_2)R_3 \subseteq R_1R_3 \cap R_2R_3$。

(6) $R_3(R_1 \cap R_2) \subseteq R_3R_1 \cap R_3R_2$。

1.2.4 递归定义与归纳证明

在后续章节中，我们会用到一些递归定义及相关的表示方法。利用它们能够很方便地表达一些对象，也能够比较容易地处理相应方式下定义出来的对象，包括算法和证明。我们先介绍递归定义。

递归定义(recursive definition)又称为归纳定义(inductive definition)，我们用它来定义一个集合。通常一个集合的递归定义由三部分组成：

(1)基础（basis）：它指出某一些对象是该集合的元素，定义了该集合的最基本的元素，使得被定义的集合是非空的。

(2)归纳（induction）：它指出用集合中的元素来构造集合的新元素的规则。归纳的形式一般为：如果 a, b, c, …, d 是被定义集合的元素，则用某种运算、函数或者组合方法对这些元素进行处理后所得的结果也是集合中的元素。

(3)极小性限定：指出一个对象是所定义的集合中的元素的充要条件是该对象可以通过有限次地使用基础和归纳条款中所给的规定构造出来。

上述三条中的前两条会因定义的对象不同而不同，但第三条基本上是一样的。所以，在许多时候，我们只强调对第一条和第二条的叙述，而省略对第三条的叙述，这通常是不会引起误解的。

例 1-17 著名的斐波那契（Fibonacci）数的定义：

(1) 基础：0 是第一个斐波那契数，1 是第二个斐波那契数。

(2) 归纳：如果 n 是第 i 个斐波那契数，m 是第 $i+1$ 个斐波那契数，则 $n+m$ 是第 $i+2$ 个斐波那契数，这里 i 为大于等于 1 的正整数。

(3) 只有满足(1)和(2)的数才是斐波那契数。

根据上述定义，我们从第一个斐波那契数开始，将这些数依次排列，就构成了斐波那契数列：

0,1,1,2,3,5,8,13,21,34,55, …

例 1-18 我们可以按下列方法定义算术表达式：

(1) 基础：常数是算术表达式，变量是算术表达式。

(2) 归纳：如果 E_1,E_2 是表达式，则 $+E_1,-E_1,E_1+E_2,E_1-E_2,E_1*E_2,E_1/E_2,E_1**E_2$,Fun($E_1$)是算术表达式，其中 Fun 为函数名，$E_1*E_2$ 表示 E_1 与 E_2 的乘积，E_1**E_2 表示 E_1 的 E_2 次幂。

(3) 只有满足(1)和(2)的表达式才是算术表达式。

下面用递归方式定义关系的 $n(n\geqslant 0)$ 次幂。

定义 1-17 设 R 是 S 上的二元关系，则 R^n 如下递归定义：

(1) $R^0=\{(a,a)\mid a\in S\}$

(2) $R^i=R^{i-1}\circ R(i=1,2,3,4,5,\cdots)$。

递归定义提供了一种良好的定义方式，使得集合中元素的构造规律明确地表现出来，这也给集合性质的归纳证明提供了良好的基础。归纳法证明与递归定义相对应，由三步组成：

(1) 基础：证明该集合的最基本的元素具有性质 P。

(2) 归纳：证明如果被定义集合的元素 $a,b,c,\cdots,d$ 具有性质 P，则用某种运算、函数或者组合方法对这些元素进行处理后所得的结果也具有性质 P.

(3) 由归纳法原理，集合中的所有元素具有性质 P——集合具有性质 P。

例 1-19 对有穷集合 A，证明 $|2^A|=2^{|A|}$.

证明：设 A 为一个有穷集合，现施归纳于 $|A|$。

(1) 基础：当 $|A|=0$ 时，由幂集定义，$2^A=\{\varnothing\}$，从而 $|2^A|=|\{\varnothing\}|=1$，而 $2^{|A|}=2^0=1$。所以有 $|2^A|=2^{|A|}$ 对 $|A|=0$ 成立。

(2) 归纳：假设 $|A|=n$ 时结论成立，这里 $n\geqslant 0$，往证当 $|A|=n+1$ 时结论成立。

为此，不妨设 $A=B\cup\{a\}$，这里 $a\notin B$，即

$$|A|=|B\cup\{a\}|=|B|+|\{a\}|=|B|+1$$

由幂集的定义知

$$2^A=2^B\cup\quad C\cup\{a\}\mid C\in 2^B\}$$

由于 $a\notin B$,所以

$$2^B\cap\{C\cup\{a\}\mid C\in 2^B\}=\varnothing$$

由 $\{C\cup\{a\}\mid C\in 2^B\}$ 的构造方法知道,可以按如下方法构造一个一一对应 $f:\{C\cup\{a\}\mid C\in 2^B\}\to 2^B$,使

$$f(C\cup\{a\})=C$$

所以

$$|\{C\cup\{a\}\mid C\in 2^B\}|=|2^B|$$

故

$$\begin{aligned}|2^A|&=|2^B\cup\{C\cup\{a\}\mid C\in 2^B\}|\\&=|2^B|+|\{C\cup\{a\}\mid C\in 2^B\}|\\&=|2^B|+|2^B|\\&=2|2^B|\end{aligned}$$

显然,$|B|=n$,由归纳假设知

$$|2^B|=2^{|B|}$$

从而有

$$|2^A|=2|2^B|=2\times 2^{|B|}=2^{|B|+1}=2^{|A}$$

这就是说,结论对 $|A|=n+1$ 成立。

(3)由归纳法原理,结论对任意有穷集合成立。

例 1-20 表达式的前缀形式是指将运算符写在前面,后跟相应的运算对象。如 $+E_1$ 的前缀形式为 $+E_1$,E_1+E_2 的前缀形式为 $+E_1E_2$,E_1*E_2 的前缀形式为 $*E_1E_2$,E_1**E_2 的前缀形式为 $**E_1E_2$,$\mathrm{Fun}(E_1)$ 的前缀形式为 $\mathrm{Fun}E_1$。证明例 1-18 所定义的表达式可以用这里定义的前缀形式表示。

证明:设 E 为例 1-18 所定义的表达式,现在对 E 中所含的运算符(包括函数引用)的个数实施归纳。为了叙述方便,设 E 中含 n 个运算符。

(1)基础:当 $n=0$ 时,表达式为一个常数或者变量,结论显然成立。

(2)归纳:假设 $n\leqslant k$ 时结论成立,这里 $k\geqslant 0$,往证当 $n=k+1$ 时结论成立。

由于 E 中含有 $k+1$ 个运算符,所以 E 必是如下形式之一:

① 当 $E=+E_1$ 时,我们知道 E_1 中的运算符的个数为 k,由归纳假设,E_1 有对应的前缀形式 F_1,从而 E 的前缀形式为 $+F_1$。

② 当 $E=-E_1$ 时,用与①相同的方式进行讨论,可得 E 的前缀形式为 $-F_1$。

③ 当 $E=E_1+E_2$ 时,E_1 和 E_2 中所含的运算符的个数分别小于等于 k,由归纳假设 E_1,E_2 对应的前缀形式分别为 F_1,F_2,从而 E 的前缀形式为 $+F_1F_2$。

④ 对 $E=E_1-E_2$,$E=E_1*E_2$,$E=E_1/E_2$,$E=E_1**E_2$ 的情况进行类似的讨论,它们对应的前缀形式分别为:$-F_1F_2$,$*F_1F_2$,$/F_1F_2$,$**F_1F_2$。