离散数学原理之一

代数结构

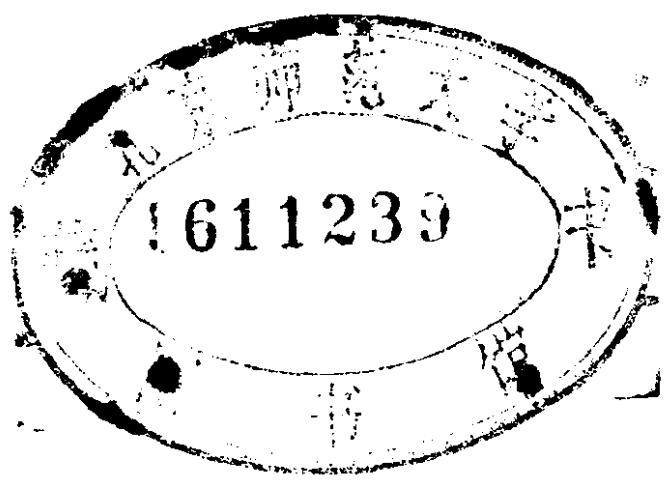
孙淑玲 编著

中国科学技术大学出版社

离散数学原理之一

代 数 结 构

孙淑玲　　编著



中国科学技术大学出版社

1990・合肥

代 数 结 构

孙淑玲 编著

*

中国科学技术大学出版社出版
（安徽省合肥市金寨路96号 邮政编码：230026）
安徽省金寨县印刷厂印刷
安徽省新华书店发行

*

开本：850×1168/32 印张6.125 字数157千
1991年12月第1版 1991年12月第1次印刷
印数 1—2500册
ISBN7-312-00304-4/O·98

〔皖〕第08号 定价：1.95元

内 容 简 介

本书是"离散数学原理"之一，它讲述代数结构的特性．在前四章中介绍了集合、映射、关系等基本概念以及初等数论知识；后四章介绍几种基本的代数系统——群、环、域、格的基本性质，其中强调的是代数结构本身(而不是结构中的元素)以及不同代数结构之间的相互联系．

本书可作为高等学校计算机系和无线电系基础课教材，也可供通讯、自动化等领域工程技术人员参考．

前　言

“代数结构”是计算机科学系开设的“离散数学”系列课程的第一个课程。它主要讲授计算机科学所需要的代数方面的基础知识，为今后学习和研究提供不可缺少的工具。

本书是在中国科学技术大学计算机科学系1978年的讲义基础上，经过十年教学实践不断修改完善而成的。

全书共有八章。

第一章是在学生高中代数的基础上将集合的运算和性质作一个系统地总结。特别介绍了集合的归纳定义，它在计算机科学中有着广泛的应用。

第二章讲述初等数论的基本知识.它不仅为后面学习群、环、域提供一些具体素材和实例，也为今后学习数字通讯、编码理论准备必要的知识。

在第三章、第四章中介绍关于映射和关系的知识，内容是标准的。

在后面的四章中分别讲述了几个基本的代数系统——群、环、域、格.由于学生不熟悉这部分所体现的近世代数的基本研究思想和方法，我们强调了代数结构本身(而不是该结构中的元素特性)以及不同代数结构之间的相互联系，并配有不同难度的例题。

该书每章后面均配有一定数量的习题。

在此，我向过去几年里对此书的前身提供意见的郑玉芳老师和许多学生表示谢意，并欢迎广大读者对此书给予更多的批评和指正。

孙淑玲

1991年1月

目　录

1 集　　合

集合是数学中最基本的概念，它已深入到各种科学和技术领域中，特别是应用于数学的各个分支中。本章的内容是在高中数学课所介绍的基础上略有提高，引入了幂集、积集概念以及计算机科学中常用的集合的归纳定义。

1.1 集合的基本概念

1.1.1 集　　合

集合是一些对象的总体。总体中的对象称之为集合的元素或成员。给定任意一个对象 x 以及集合 S，如果 x 是集合 S 的一个元素，我们将写成 $x\in S$。如果 x 不是集合 S 的一个元素，则写成 $x\notin S$。

习惯上称之为集合的东西，通常在数学上是可以接受的。例如：

1° “小于 4 的非负整数集合”是由四个元素组成的集合。这四个元素分别是 0，1，2，3。

2° “全体活着的中国人”是个集合。集合中元素的个数很多，但是有限的。由于生死的变化，要列出这个集合的成员是困难的。这种困难是实践上的，不是理论上的。

3° “大于等于 3 的整数集合”是个有无限多个元素的集合。要判断一个整数是否是它的元素很容易。

4° “在具有无限存贮量的计算机上，运行足够长的时间之后能停止运行的所有 Algol 60 程序组成了一个无限集合”。可计算

理论已经证明，判断任意程序是否是这个集合的元素的算法是不存在的。从而这个集合是不可判定的。

5° “全体大于 0，小于 1 的整数集合”。在这个集合中没有任何元素，我们称它为空集，并记为 $\varnothing$。

集合是以它的元素来表征的。一个有有限多个元素的集合可以用列出它的全部元素的方法来说明。这些元素用括号括起来，并且元素之间用逗号分开。一般集合用大写字母表示，集合元素用小写字母表示。当集合 A 中有有限多个元素时，用 $|A|$ 表示集合中的元素个数。特别对于空集 $\varnothing$，$|\varnothing|=0$。例如：

1° $A=\{a, b, c\}$，a, b, c 是集合 A 的元素，$|A|=3$。

2° $B=\{0, 2, 4, 6, 8\}$，B 是小于 10 的非负偶数集合。$|B|=5$。

集合，特别是有无限多个元素的集合，通常用指出集合中元素性质的方法来说明。例如，记 Z 是全体整数集合，

1° 全体偶数集合为 $\{x \mid \exists\, y\in Z, x=2y\}$。

2° 大于 10 的整数集合 $\{x \mid x\in Z$ 且 $x>10\}$。

3° 有理数集合 $Q=\{x/y \mid x, y\in Z$ 且 $y\neq 0\}$。

1.1.2 集合的相等

同一个集合可以有不同的表示法。例如，$A=\{-1, 1\}$，$B=\{x \mid x\in Z, x^2=1\}$，$C=\{x \mid x\in R, |x|=1\}$，其中 R 表示全体实数集合。这就产生了一个问题，即如何判断两个集合是同一个集合。

定义 1.1 给了两个集合 A 和 B，如果集合 A 中的每个元素都是集合 B 中的元素，反过来集合 B 的每个元素也都是集合 A 中的元素，那么称集合 A 与集合 B 相等，并记为 $A=B$。

用这个定义可直接验证上面的集合 A，B，C 是相等的集合，$A=B=C$。

定理 1.1 A, B, C 是任意集合，集合间的相等关系满足

1° **自反性** $A=A$.

2° **对称性** 若 $A=B$, 则 $B=A$.

3° **传递性** 若 $A=B$, $B=C$, 则 $A=C$.

证明 在定义 1.1 中，将 B 改成 A 以后显然成立，它说明 $A=A$. 又在定义 1.1 中，先说后一句话，再说前一句话，也就是说集合 B 的每个元素都是集合 A 中的元素，反过来集合 A 的每个元素也都是集合 A 中的元素，其意思与原来完全相同，所以当 $A=B$ 时，必有 $B=A$.

下面证明传递性. 已知 $A=B$，对于任何 $x\in A$，必有 $x\in B$. 又由 $B=C$，从 $x\in B$ 推出 $x\in C$. 反过来，由 $A=B$, $B=C$ 及相等关系的对称性推出 $B=A$, $C=B$. 对于任何 $x\in C$，由于 $C=B$，必有 $x\in B$. 又由 $B=A$ 从 $x\in B$ 推出 $x\in A$. 对照定义 1.1 知 $A=C$.

1.1.3 集合的包含

集合的相等与包含是集合间的两种最基本的关系. 现在定义两个集合的包含关系.

定义 1.2 **A 和 B 是两个集合. 如果集合 A 中的每个元素都是集合 B 中的元素，我们称集合 B 包含集合 A，而集合 A 叫做集合 B 的一个子集，表示成 $B\supseteq A$ 或 $A\subseteq B$.**

如果集合 B 包含集合 A，并且至少有一个元素属于集合 B 而不属于集合 A，我们称集合 B 真包含集合 A，而集合 A 叫做集合 B 的一个真子集.

例如，偶数集合是整数集合的真子集. 集合 $\{1, 2, 3, 4\}$ 是集合 $\{x|x\in Z \text{ 且 } 0<x<5\}$ 的子集，但不是真子集.

定理 1.2 **A, B, C 是任意集合. 集合间的包含关系满足**

1° **自反性** $A\subseteq A$.

2° **反对称性** 若 $A\subseteq B$ 且 $B\subseteq A$，则 $A=B$.

3° **传递性** 若 $A\subseteq B$ 且 $B\subseteq C$，则 $A\subseteq C$.

证明 1°，3°的证明留作习题。这里只证 2°。

若 $A\subseteq B$ 且 $B\subseteq A$，由集合包含的定义知集合 A 中的每个元素都是集合 B 中的元素，并且集合 B 中的每个元素都是集合 A 中的元素。这正是集合 A 与集合 B 相等的定义，从而得出 $A=B$。

定理 1.3 **对于任何集合** A，$\varnothing\subseteq A$。

证明 用反证法。假设空集 $\varnothing$ 不是某个集合 A 的子集，那么至少有一个元素 x，$x\in\varnothing$ 且 $x\notin A$。而 $\varnothing$ 是空集，它没有任何元素，即对任何 x 必有 $x\notin\varnothing$。产生矛盾，故不可。由此得出 $\varnothing$ 是任何集合 A 的子集。

由定理 1.3 知空集 $\varnothing$ 是唯一的。这是因为假若 $\varnothing_1$ 和 $\varnothing_2$ 都是空集。因为 $\varnothing_1$ 是空集，得出 $\varnothing_1\subseteq\varnothing_2$。因为 $\varnothing_2$ 是空集，得出 $\varnothing_2\subseteq\varnothing_1$。由集合包含关系的反对称性知 $\varnothing_1=\varnothing_2$。

在研究一个特定问题时，假设有一个足够大的集合使一切集合都包含在它之中。这个足够大的集合称之为万有集合，并记为 U。对于任意集合 A 均有 $A\subseteq U$。

1.1.4 幂　　集

A，B，…是集合，把它们放在一起构成一个新的集合$\{A, B, \cdots\}$。这种集合以集合作为元素称为集族。集族通常用花写字母 $\mathscr{A}$，$\mathscr{B}$，…表示。

一个集合的全部子集构成的集族叫做该集合的幂集。若 $A=\{a, b, c\}$，A 的幂集 $\mathscr{P}(A)$ 是有 8 个元素的集族。

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

定理 1.4 A **是有限集合**，$|\mathscr{P}(A)|=2^{|A|}$。

证明 A 是有限集合，$|A|=n$。A 的 i 元子集的个数就是从 n 个元素中选取 i 个不同元素的方法数 $C_n^i\left(=\dfrac{n!}{i!(n-i)!}\right)$，这里 i 可以取 0，1，…，n 这 $n+1$ 个值。

$$|\mathscr{P}(A)|=C_n^0+C_n^1+\cdots+C_n^n。$$

在二项式定理

$$(x+y)^n = C_n^0 x^n y^0 + C_n^1 x^{n-1} y + \cdots + C_n^n x^0 y^n$$

中，令 $x=y=1$，于是有 $2^n = C_n^0 + C_n^1 + \cdots + C_n^n$。从而 $|\mathscr{P}(A)| = 2^n = 2^{|A|}$。

1.1.5 积　　集

定义 1.3　对于正整数 n，有序 n 数组 $(a_1, a_2, \cdots, a_n)$ 是以 a_i 为第 i 个分量的 n 个对象的序列。

两个有序 n 数组是相等的，当且仅当它们的每个分量都是相等的。

定义 1.4　n 个集合 $A_1, A_2, \cdots A_n$ 的积集 $A_1 \times A_2 \times \cdots \times A_n$ 是由全体有序 n 数组 $(a_1, a_2, \cdots, a_n)$ 构成的集合，其中 $a_i \in A_i$，$1 \leqslant i \leqslant n$。

特别地，若 $A_1 = A_2 = \cdots = A_n = A$ 时，记 $A_1 \times A_2 \times \cdots \times A_n$ 为 A^n。

例如，$A=\{1, 2\}$，$B=\{m, n\}$，$C=\{0\}$．$D=\varnothing$，那么

$$A \times B = \{(1, m), (1, n), (2, m), (2, n)\},$$
$$A \times C = \{(1, 0), (2, 0)\},$$
$$C \times A = \{(0, 1), (0, 2)\},$$
$$A \times D = \varnothing.$$

注意，这里 $A \times C \neq C \times A$。

定理 1.5　A, B 是两个有限集合，$|A \times B| = |A| \cdot |B|$。

证明　从集合 A 中任取一个元素 a 作为第一分量，从集合 B 中任取一个元素 b 作为第二分量构成的有序 2 数组 (a, b) 是 $A \times B$ 的一个元素。a 与 b 的不同取法构成不同的有序 2 数组。从集合 A 中选取一个元素有 $|A|$ 种方法，从集合 B 中选取一个元素有 $|B|$ 种方法。它们可以构成 $|A| \cdot |B|$ 个不同的 2 数组。于是 $|A \times B| = |A| \cdot |B|$。

同理可以证明 $|A_1 \times A_2 \times \cdots \times A_n| = |A_1| \cdot |A_2| \cdot \cdots \cdot |A_n|$。

1.2 集合的运算

我们在前一节谈到集合间的一些联系，如包含，子集等，各种不同集合的进一步联系是通过集合上的各种运算显示出来的。

定义 1.5 **集合 A 与 B 的并，交，差集 $A\cup B$，$A\cap B$，$A-B$ 分别为**

$$A\cup B=\{x|x\in A \text{ 或 } x\in B\},$$
$$A\cap B=\{x|x\in A \text{ 且 } x\in B\},$$
$$A-B=\{x|x\in A \text{ 且 } x\notin B\}.$$

由定义看出 $A\cup B$ 是由或是在集合 A 中，或是在集合 B 中的元素组成的。$A\cap B$ 是由集合 A 和集合 B 的公共元素组成的。$A-B$ 是由在集合 A 中且不在集合 B 中的元素组成的。若取 A 为万有集合 U，$U-B$ 称为集合 B 的补集，并记为 $\bar{B}$。不难看出

$$\bar{B}=\{x|x\in U \text{ 且 } x\notin B\}=\{x|x\notin B\}.$$

例如，$A=\{0,1,2\}$，$B=\{1,2,3\}$，$U=\{x|x\in Z \text{ 且 } x\geqslant 0\}$。

$A\cup B=\{0,1,2,3\}$，

$A\cap B=\{1,2\}$，

$A-B=\{0\}$，$B-A=\{3\}$。

$\bar{A}=U-A=\{x|x\in Z \text{ 且 } x\geqslant 3\}$。

定理 1.6 **对于任意集合 A，$A\cup\bar{A}=U$，$A\cap\bar{A}=\varnothing$。**

证明 由并与交运算的定义

$A\cup\bar{A}=\{x|x\in A \text{ 或 } x\in\bar{A}\}=\{x|x\in A \text{ 或 } x\notin A\}=U$。

$A\cap\bar{A}=\{x|x\in A \text{ 且 } x\in\bar{A}\}=\{x|x\in A \text{ 且 } x\notin A\}=\varnothing$。

例 1 证明 $\bar{A}\subseteq\bar{B}$ 当且仅当 $B\subseteq A$。

证明 用反证法证明必要性。假设 $B\subseteq A$ 不成立，那么至少存在一个元素 $x_0\in B$ 且 $x_0\notin A$，从而 $x_0\in\bar{A}$。另一方面 $x_0\in B$，故 $x_0\notin\bar{B}$。这就是说，至少存在一个元素 x_0，使 $x_0\in\bar{A}$ 且 $x_0\notin\bar{B}$，与 $\bar{A}\subseteq\bar{B}$ 相矛盾，故不可。于是仅当 $B\subseteq A$ 时有 $\bar{A}\subseteq\bar{B}$。

可用类似的方法证明充分性.

例 2 证明 $\overline{A\cap B}=\bar{A}\cup\bar{B}$.

证明 证明的思路是先证明 $\overline{A\cap B}\subseteq\bar{A}\cup\bar{B}$，再证明 $\bar{A}\cup\bar{B}\subseteq\overline{A\cap B}$，利用集合间包含关系的反对称性得到 $\overline{A\cap B}=\bar{A}\cup\bar{B}$.

下面我们先证 $\overline{A\cap B}\subseteq\bar{A}\cup\bar{B}$:

任取 $x\in\overline{A\cap B}$，由补运算的定义知 $x\notin A\cap B$，即 $x\in A$ 与 $x\in B$ 不能同时成立. 由此得出 $x\notin A$ 或 $x\notin B$. 再由集合并运算的定义知 $x\in\bar{A}\cup\bar{B}$. 这里 x 是 $\overline{A\cap B}$ 的任意元素，故 $\overline{A\cap B}\subseteq\bar{A}\cup\bar{B}$.

再证 $\bar{A}\cup\bar{B}\subseteq\overline{A\cap B}$:

任取 $x\in\bar{A}\cup\bar{B}$，由并运算的定义知 $x\in\bar{A}$ 或 $x\in\bar{B}$. 因 $A\cap B\subseteq A$，从上例知 $\bar{A}\subseteq\overline{A\cap B}$. 当 $x\in\bar{A}$ 时，必有 $x\in\overline{A\cap B}$. 同样因 $A\cap B\subseteq B$，从上例知 $\bar{B}\subseteq\overline{A\cap B}$. 当 $x\in\bar{B}$ 时，必有 $x\in\overline{A\cap B}$. 综上分析知 $\bar{A}\cup\bar{B}$ 的每个元素都是 $\overline{A\cap B}$ 的元素. 即 $\bar{A}\cup\bar{B}\subseteq\overline{A\cap B}$. **证毕**

定理 1.7 对任意集合 A，B，C 下面等式成立:

1° $A\cup B=B\cup A$，$A\cap B=B\cap A$.

2° $A\cup(B\cup C)=(A\cup B)\cup C$，$A\cap(B\cap C)=(A\cap B)\cap C$.

3° $A\cup(B\cap C)=(A\cup B)\cap(A\cup C)$，

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

4° $A\cup\varnothing=A$，$A\cap U=A$.

5° $A\cup\bar{A}=U$，$A\cap\bar{A}=\varnothing$.

证明 5°已在定理 1.6 中证明. 其余的均可由集合并，交运算的定义直接证明.

定理 1.8 下面三个关于集合 A 和 B 的命题是相互等价的.

1° $A\subseteq B$，

2° $A\cup B=B$，

3° $A\cap B=A$。

证明 我们的证明方法是通过证明 1°⇒2°⇒3°⇒1° 来说明它们是等价的。

首先证明 1°⇒2°：

已知 $A\subseteq B$，A 的每个元素都是 B 中的元素，从集合并运算的定义知

$$A\cup B=\{x|x\in A\text{ 或 }x\in B\}=\{x|x\in B\}=B。$$

再证明 2°⇒3°：

已知 $A\cup B=B$，等式两边同时与 A 求交仍然相等，然后再定理 1.7 中的诸性质

$$\begin{aligned}A\cap B&=A\cap(A\cup B)\\&=(A\cup\varnothing)\cap(A\cup B)&&4°\\&=A\cup(\varnothing\cap B)&&3°\\&=A\cup((\varnothing\cap B)\cup\varnothing)&&4°\\&=A\cup((B\cap\varnothing)\cup(B\cap\bar{B}))&&1°,\ 5°\\&=A\cup(B\cap(\varnothing\cup\bar{B}))&&3°\\&=A\cup(B\cap\bar{B})&&1°,\ 4°\\&=A\cup\varnothing&&5°\\&=A。&&4°\end{aligned}$$

最后证明 3°⇒1°：

已知 $A\cap B=A$，任取 $x\in A\cap B$，由集合交运算的定义知 $x\in A$ 且 $x\in B$，特别注意到 $x\in B$. 由 x 的任意性，得到 $A\cap B\subseteq B$。将 $A\cap B=A$ 代入即是所求的结果 $A\subseteq B$。

对集合的运算可以用 Venn 图直观地表示。在图 1 中用矩形表示万有集合 U，圆表示集合 A，B，C。