

离散数学概论

周丽珍 编著

冶金工业出版社

离散数学概论

周丽珍 编著

北 京
冶 金 工 业 出 版 社
2008

内 容 简 介

本书从集合论、代数学、图论、数理逻辑、丢番图方程五个方面介绍了离散数学的基础知识。

本书可作为各级各类高等院校与各级各类职业技术培训学校数论、自控、电子、电气、计算机、仪器仪表、暖通、建筑物理等专业的参考书,也可供有关专业的科技工作者使用。

图书在版编目(CIP)数据

离散数学概论/周丽珍编著. —北京:冶金工业出版社, 2008. 1
ISBN 978-7-5024-4432-7

I. 离… II. 周… III. 离散数学—概论 IV. 0158

中国版本图书馆CIP数据核字(2008)第016266号

出 版 人 曹胜利

地 址 北京北河沿大街嵩祝院北巷39号, 邮编100009

电 话 (010)64027926 电子信箱 postmaster@cnmip.com.cn

责任编辑 张 卫 张爱平 美术编辑 李 心 版式设计 张 青

责任校对 王永欣 责任印制 丁小晶

ISBN 978-7-5024 4432-7

北京印刷一厂印刷; 冶金工业出版社发行; 各地新华书店经销

2008年1月第1版, 2008年1月第1次印刷

850mm×1168mm 1/32; 10.125印张; 275千字; 310页; 1 2000册

25.00元

冶金工业出版社发行部 电话: (010)64044283 传真: (010)64027893

冶金书店 地址: 北京东四西大街46号(100711) 电话: (010)65289081

(本书如有印装质量问题, 本社发行部负责退换)

前 言

离散数学是现代数学的重要组成部分,由多个数学分支组成;每个分支从不同角度研究离散量结构及其相互关系。离散数学研究对象的数量是有限的(或可数的),这些数学分支既相对独立又密切联系。阐述每个数学分支的特点与各个数学分支之间的关系是本书的基本目的,读者通过本书可以初步了解离散数学的概貌。由于篇幅所限,难免挂一漏万,因此读者可以根据具体情况进行选择、取舍。

本书从集合论、代数学、图论、数理逻辑、丢番图方程五个方面介绍了离散数学的基础知识。

本书可以作为各级各类高等院校与各级各类职业技术培训学校数控、自控、电子、电气、计算机、仪器仪表、暖通、建筑物理等专业的参考书,也可供有关专业的科技工作者使用。

在著述过程中易中给予了始终如一的鼓励,为本书的最终形成倾注了大量的心力,我深深地感激!

囿于作者的水平,书中会有一些不妥之处,恳请读者不吝赐教。

作 者

目 录

I 集 合 论

1 基本概念	1
1.1 集合与元素	1
1.2 集合运算	2
1.2.1 包含关系	2
1.2.2 基本运算	3
1.3 集合的极限	7
1.4 直积	10
2 关系与映射	12
2.1 关系定义	12
2.2 映射定义	14
2.3 关系矩阵和关系图	17
2.4 序关系与等价关系	18
3 集合的势	23
3.1 基数概念	23
3.2 皮亚诺公理	24
3.3 ω 递归	24
3.4 势	27
4 点集	32
4.1 距离空间	32

4.2	收敛点列	37
4.3	欧氏空间中的点集	39
4.4	基本定理	45
4.5	零集	48
4.5.1	p 进小数	48
4.5.2	康托尔集	50
4.5.3	直线上的零集	52

I 代 数 学

5	代数系统	55
5.1	代数系统定义	55
5.2	同态与同构	58
5.3	商代数系统	61
6	群	63
6.1	群定义	63
6.2	子群和陪集	66
6.3	群同态定理	71
6.4	集合上的变换群	77
6.5	置换群和循环群	79
7	环与域	87
7.1	环定义和域定义	87
7.2	多项式环	92
7.3	环和域的特征	93
7.4	扩域	96
7.5	有序环和有序域	99
7.6	交错代数	103

8 格论	109
8.1 格定义	109
8.2 格性质	112
8.3 特殊格	117
8.4 布尔代数和纽曼代数	121
9 多重线性代数	127
9.1 对偶空间	127
9.2 多重线性变换	129
9.3 线性空间的张量积与直和	132
9.4 张量代数和外代数	136
9.5 $E(V)$ 的线性变换和对偶	145
10 李代数	148
10.1 李代数定义	148
10.2 单李代数和半单李代数	153
10.3 嘉当内积	157

Ⅲ 图 论

11 图的基本概念	161
11.1 图定义	161
11.2 路与回路	166
11.3 图代数	170
11.3.1 图运算	170
11.3.2 图的矩阵表示	171
11.3.3 图的线性空间	179
11.3.4 图同构和图同调	180

12 特殊图	183
12.1 欧拉图和哈密顿图	183
12.2 平面图	189
12.2.1 平面图定义	189
12.2.2 库拉托夫斯基定理	192
12.3 对偶图	193
13 树	204
13.1 树定义	204
13.2 生成树	207
13.3 二叉树	209
13.4 生成树的生成	212
13.5 优美树	219

IV 数理逻辑

14 命题逻辑	223
14.1 命题	223
14.2 命题逻辑的形式化	226
14.3 范式	238
14.4 命题演算和集合	245
14.5 命题逻辑的公理系统	246
15 谓词逻辑	251
15.1 谓词和量词	251
15.2 谓词逻辑的形式化	254
15.3 谓词逻辑的公理系统	258
15.4 范式	262

16 Herbrand 定理	264
16.1 公理化理论的基本思想	264
16.2 判定问题	265
16.3 Herbrand 定理的证明	266

V 丢番图方程

17 贝尔方程	275
17.1 贝尔方程的基本解	275
17.1.1 一次不定方程	275
17.1.2 勾股数	277
17.1.3 贝尔方程的解	278
17.2 方程 $x^2 - Dy^2 = M$ 解的结构	283
18 二次域和不定方程	285
18.1 O_K 的理想类数	285
18.2 三角和	288
18.3 实二次域与贝尔方程	298
18.4 费尔马方程	301
参考文献	305
术语索引	306

I 集 合 论

1 基 本 概 念

1.1 集合与元素

集合(简称集)是数学最基本的概念之一,但是至今没有一个公认的集合定义,更多的是采用描述的方法说明集合的含义。集合就是由确定的、互不相同的事物组成的整体,整体中的事物称为元素;集合中的元素数量可以是有限的,也可以是无限的。元素数量有限的集合称为有限集合,反之称为无限集合。如某学校的全体教师组成一个集合,教师就是该集合的元素;所有自然数组成一个集合,自然数就是该集合的元素。

表示集合有两种方法:

(1)列举法 举出集合中的全部元素,元素之间用逗号分开,用大括号括起来。

设 A 是以 a, b, c, d, e 为元素的集合,表示成 $A = \{a, b, c, d, e\}$;
设 B 是以所有自然数为元素的集合,表示成 $B = \{1, 2, 3, \dots\}$ 。

(2)描述法 用集合中元素的性质表示集合。

设 A 表示法国人组成的集合, A 中元素的性质就是法国人,表示成 $A = \{x | x \text{ 为法国人}\}$;设 $Q(x)$ 为集合 B 中元素 x 的性质,表示成 $B = \{x | Q(x)\}$ 。

关于集合的表示方法须注意三点:

(1)集合中的元素是各不相同的,如 $\{a, b\}$ 中 $a \neq b$;

(2)集合中的元素没有顺序规定,如 $\{a, b\} = \{b, a\}$;

(3)两种集合表示法有时可以互换,如 $\{2, 4, 6, \dots\} = \{x | x \text{ 为偶自然数}\}$ 。

元素和集合的关系是个体与整体的关系,通常用大写字母代表集合,以小写字母代表元素。若 a 是集合 A 的元素,则记作 $a \in A$,

读作“ a 属于 A ”;若 a 不是集合 A 的元素,则记作 $a \notin A$,读作“ a 不属于 A ”。

1.2 集合运算

1.2.1 包含关系

定义1.1 设 A, B 为集合,若属于 A 的元素也都属于 B ,则称 A 是 B 的一个子集合,或者称 B 包含 A ,记作 $A \subseteq B$ 或 $B \supseteq A$ 。

定义1.2 设 A, B 为集合,若 A 的所有元素都在 B 中且 B 的所有元素都在 A 中,则称集合 A 与集合 B 相等,记作 $A = B$;也就是若 $A \subseteq B$ 且 $B \subseteq A$,则称 $A = B$ 。

定义1.3 设 A, B 为集合,若 $A \subseteq B$ 且 $A \neq B$,则称 A 为 B 的真子集合,记作 $A \subset B$ 。

不含任何元素的集合称为空集,记为 $\emptyset$;以集合为元素的集合称为集族,如 $\{\emptyset\}$ 为一个集族, $\{\text{中国人}\} = \{\{\text{北京人}\}, \{\text{台湾人}\}, \{\text{香港人}\}, \{\text{上海人}\}, \{\text{澳门人}\}, \{\text{西藏人}\}, \{\text{新疆人}\}, \{\text{内蒙古人}\}, \{\text{湖南人}\} \dots\}$ 。

例1.1 设 $A = \{1, 2, 3, 4, 5, 6, 7, 8\}$ 、 $B = \{1, 3, 5, 7\}$,判断 A, B 的关系。

解:显然 $B \subset A$,如图 1-1 所示,这种图示法称为文氏图。

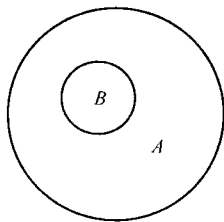


图 1-1

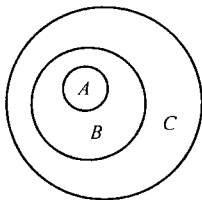


图 1-2

例 1.2 已知集合 $A = \{\text{等边三角形}\}$ 、 $B = \{\text{等腰三角形}\}$ 、 $C = \{\text{三角形}\}$,判断 A, B, C 的关系。

解: $A \subset B \subset C$, 如图 1-2 所示。

例 1.3 问集合 $X = \{x | x \text{ 为方程 } x^2 + 1 = 0 \text{ 的实根}\}$, 是否为空集?

解: 因为 $x^2 + 1 = 0$ 无实根, 所以 X 为空集, 即 $X = \emptyset$ 。

例 1.4 设 $A = \{a, b, c\}$, 求出 A 的所有子集。

解: A 的所有子集为 $\emptyset, \{a\}, \{b\}, \{c\}, \{a, b\}, \{b, c\}, \{c, a\}, \{a, b, c\}$ 。显然 A 本身也是 A 的子集。若集合 A 有 n 个元素, 则 A 的所有子集合共有 2^n 个; 事实上, 从 A 中任取 l 个元素, 共有 C_n^l 个取法, 形成 C_n^l 个子集, 于是有

$$C_n^0 + C_n^1 + C_n^2 + \cdots + C_n^l + \cdots + C_n^n = (1+1)^n = 2^n$$

共 2^n 个子集合。

1.2.2 基本运算

定义 1.4 由集合 A 与集合 B 的所有元素组成的集合称为 A 、 B 的并集, 记作 $A \cup B$, $A \cup B = \{x | x \in A \text{ 或 } x \in B\}$, 如图 1-3 所示。

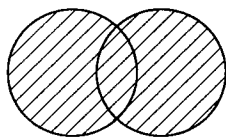


图 1-3

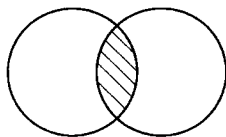


图 1-4

定义 1.5 由集合 A 与集合 B 的公共元素组成的集合称为 A 、 B 的交集, 记作 $A \cap B$, $A \cap B = \{x | x \in A \text{ 且 } x \in B\}$ 。

例 1.5 设 $A = \{a, b, e\}$, $B = \{b, e, d\}$, 求 $A \cup B$, $A \cap B$ 。

解: $A \cup B = \{a, b, d, e\}$, $A \cap B = \{b, e\}$ 。

例 1.6 设 $A = \{x | x > 1\}$, $B = \{x | x \leq 2\}$, 求 $A \cap B$ 。

解: $A \cap B = \{x | 1 < x \leq 2\}$ 。

定理 1.1 交并运算性质:

(1) 交换性

$$A \cup B = B \cup A \quad A \cap B = B \cap A$$

(2) 结合性

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

(3)分配性

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

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

(4)幂等性

$$A \cup A = A \cap A = A$$

(5)吸收性

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

证明分配性 $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$

先证 $A \cup (B \cap C) \subseteq (A \cup B) \cap (A \cup C)$

取

$$x \in A \cup (B \cap C)$$

有

$$x \in A \quad \text{或} \quad x \in B \cap C$$

当 $x \in A$ 时,推出

$$x \in A \cup B \quad \text{以及} \quad x \in A \cup C$$

得

$$x \in (A \cup B) \cap (A \cup C)$$

即

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

当 $x \in B \cap C$ 时,推出

$$x \in B \quad \text{且} \quad x \in C$$

得

$$x \in A \cup B \quad \text{且} \quad x \in A \cup C$$

$$x \in (A \cup B) \cap (A \cup C)$$

即

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

再证

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

取

$$x \in (A \cup B) \cap (A \cup C)$$

有

$$x \in A \cup B \quad \text{且} \quad x \in A \cup C$$

进一步, $x \in A$ 或 $x \in B$ 且 $x \in A$ 或 $x \in C$

$$x \in A \cup (B \cap C)$$

即

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

故

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

定义 1.6 设 A, B 为集合, 称由属于 A 而不属于 B 的元素组成的集合为 B 对 A 的相对补集, 记作 $A - B$ (或 $A \setminus B$), $A - B = \{x \mid$

$x \in A$ 且 $x \notin B$ }, 如图 1-5 所示。

定义 1.7 设 E 为给定的集合, 若限定讨论的集合都是 E 的子集, 则称 E 为全集。

定义 1.8 设 E 为全集, $A \subseteq E$, 称 A 对 E 的相对补集为 A 的绝对补集, 记作 $E \setminus A$ 或 $\bar{A}$, $\bar{A} = \{x | x \in E \text{ 且 } x \notin A\}$, 如图 1-6 所示。

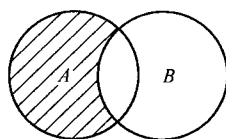


图 1-5

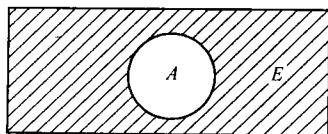


图 1-6

有时将相对补集称为差集, 绝对补集称为补集。补集运算法则:

- (1) $A - B = A \cap \bar{B}$;
- (2) $\overline{A \cup B} = \bar{A} \cap \bar{B}$ $\overline{A \cap B} = \bar{A} \cup \bar{B}$;
- (3) $A - (B \cup C) = (A - B) \cap (A - C)$
 $A - (B \cap C) = (A - B) \cup (A - C)$;
- (4) $\overline{\emptyset} = E$ $\bar{E} = \emptyset$ 。

根据空集 $\emptyset$ 、全集 E 的定义可以得到

$$\begin{aligned} A \cup \emptyset &= A & A \cap \emptyset &= \emptyset \\ A \cup E &= E & A \cap E &= A \end{aligned}$$

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

证明: 因为

$$\begin{aligned} A - (B \cup C) &= A \cap \overline{(B \cup C)} = (A \cap \bar{B}) \cap (A \cap \bar{C}) \\ &= (A \cap \bar{B}) \cap (A \cap \bar{C}) = (A - B) \cap (A - C) \end{aligned}$$

所以

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

例 1.8 证明 $A \cup (B \cap A) = A$ 。

证明: 因为

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

$$= A \cap (E \cup B) = A \cap E = A \quad (E \text{ 为全集})$$

所以

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

定义 1.9 设 A, B 为集合, 称属于 A 而不属于 B , 或属于 B 而不属于 A 的所有元素组成的集合为 A 与 B 的对称差, 记作 $A \oplus B$, 即 $A \oplus B = (A - B) \cup (B - A)$, 如图 1-7 所示。

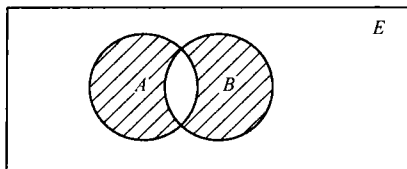


图 1-7

如设 $A = \{1, 2, 3, 4, 5\}$, $B = \{3, 4, 5, 6, 7, 8\}$, 有 $A \oplus B = \{1, 2, 6, 7, 8\}$ 。依对称差定义知道:

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

$$(2) A \oplus \emptyset = A \quad A \oplus A = \emptyset.$$

此外对称差运算还有结合性、分配性。

定义 1.10 设 A 为集合, 称由 A 的全部子集组成的集合为 A 的幂集, 记作 $\rho(A)$ 或 2^A , 即 $\rho(A) = 2^A = \{a \mid a \subseteq A\}$ 。

在不发生混淆的情况下, $\rho(A)$ 可写成 ρA 。由定义 1.10 得到 $\rho(\emptyset) = \{\emptyset\}$, $\rho(\{\emptyset\}) = \{\emptyset, \{\emptyset\}\}$ 。幂集运算的性质为:

$$(1) \text{若 } A \subseteq B, \text{ 则 } \rho(A) \subseteq \rho(B); \text{ 或若 } \rho(A) \subseteq \rho(B), \text{ 则 } A \subseteq B;$$

$$(2) \rho(A) \cup \rho(B) \subseteq \rho(A \cup B);$$

$$(3) \rho(A \cap B) = \rho(A) \cap \rho(B);$$

$$(4) \rho(A - B) \subseteq [\rho(A) - \rho(B)] \cup \{\emptyset\}.$$

证明: $\rho(A) \cup \rho(B) \subseteq \rho(A \cup B)$

设

$C \in \rho(A) \cup \rho(B)$, 推出

$$C \in \rho(A) \quad \text{并有} \quad C \subseteq A$$

或

$$C \in \rho(B) \quad \text{并有} \quad C \subseteq B$$

得

$$C \subseteq A \cup B \quad \text{即} \quad C \in \rho(A \cup B)$$

故 $\rho(A) \cup \rho(B) \subseteq \rho(A \cup B)$

最后略述多重集合的概念。上述的集合均由不同元素组成；如果允许集合内出现相同的元素，如 $\{a, a, b, c, c, e\}$ ，那么称之为多重集合。设 E 为全集，全集中元素在某个多重集合中出现的次数为该元素的重复度。如 $E = \{a, b, c, d\}$ 时 $A = \{a, a, a, b, b\}$ 中的 a 的重复度为 3， b 的重复度为 2， c, d 的重复度为“0”。于是通常所说的集合内的元素的重复度为 1 或 0，为多重集合的特殊情况。多重集合的概念可用于图论、组合数学中。一般的集合是指非多重集合。

1.3 集合的极限

设 $\{A_n\}$ 为集列，作两个新集合：

$$A^o = \{x \mid \text{有无限多个 } n, \text{ 使 } x \in A_n\}$$

$$A_\sigma = \{x \mid \text{除有限个 } n, \text{ 其余有 } x \in A_n\}$$

定义 1.11 A^o 称为集列 $\{A_n\}$ 的上极限集，记作 $\varlimsup_{n \rightarrow \infty} A_n$ ； A_σ 称为集列 $\{A_n\}$ 的下极限集，记作 $\varliminf_{n \rightarrow \infty} A_n$ ；当 $\varlimsup_{n \rightarrow \infty} A_n = \varliminf_{n \rightarrow \infty} A_n = \lim_{n \rightarrow \infty} A_n$ 时称之为集列 $\{A_n\}$ 的极限集，称集列 $\{A_n\}$ 收敛。

例 1.9 设集列 $\{A_n\}$ 为

$$A_{2n} = M \quad A_{2n-1} = N \quad (n=1, 2, 3, \dots)$$

求 $\varlimsup_{n \rightarrow \infty} A_n$ 和 $\varliminf_{n \rightarrow \infty} A_n$ 。

解： $\varlimsup_{n \rightarrow \infty} A_n = M \cup N$ $\varliminf_{n \rightarrow \infty} A_n = M \cap N$ 。

例 1.10 设集列 $\{A_n\}$ 为 $A_n = [0, n]$ ，求 $\varlimsup_{n \rightarrow \infty} A_n$ 和 $\varliminf_{n \rightarrow \infty} A_n$ 。

解： $\varlimsup_{n \rightarrow \infty} A_n = \varliminf_{n \rightarrow \infty} A_n = [0, +\infty]$ 。

例 1.11 设

$$A_1 = [0, 1] \quad A_2 = \left[0, \frac{1}{2}\right] \quad A_3 = \left[\frac{1}{2}, 1\right]$$

$$A_4 = \left[0, \frac{1}{3}\right] \quad A_5 = \left[\frac{1}{3}, \frac{2}{3}\right] \quad A_6 = \left[\frac{2}{3}, 1\right] \quad \dots$$

求 $\varlimsup_{n \rightarrow \infty} A_n$ 和 $\varliminf_{n \rightarrow \infty} A_n$ 。

解: $\overline{\lim}_{n \rightarrow \infty} A_n = [0, 1]$ $\lim_{n \rightarrow \infty} A_n = \emptyset$.

定理 1.2 对上、下极限集有:

$$(1) \overline{\lim}_{n \rightarrow \infty} A_n \supset \lim_{n \rightarrow \infty} A_n;$$

$$(2) \overline{\lim}_{n \rightarrow \infty} A_n = \bigcap_{n=1}^{\infty} \bigcup_{l=n}^{\infty} A_l;$$

$$(3) \lim_{n \rightarrow \infty} A_n = \bigcup_{n=1}^{\infty} \bigcap_{l=n}^{\infty} A_l.$$

证明: (2) 任取 $x \in \overline{\lim}_{n \rightarrow \infty} A_n$, 由定义知有无限多个 A_n 含有 x , 设为 $A_{n_1}, A_{n_2}, A_{n_3}, \dots$ 含有 x , 且 $n_1 < n_2 < n_3 < \dots$, 于是对任意正整数 m , 有

$n_i > m$, 使 $x \in A_{n_i} \subseteq \bigcup_{l=m}^{\infty} A_l$, 得

$$x \in \bigcap_{m=1}^{\infty} \bigcup_{l=m}^{\infty} A_l$$

反之, 若 $x \in \bigcap_{m=1}^{\infty} \bigcup_{l=m}^{\infty} A_l$, 则对每个 n , 均有

$$x \in \bigcup_{l=n}^{\infty} A_l$$

就是有 $n_i \geq n, x \in A_{n_i}$, 所以 x 必在无限多个 A_n 中, 即

$$\overline{\lim}_{n \rightarrow \infty} A_n = \bigcap_{n=1}^{\infty} \bigcup_{l=n}^{\infty} A_l$$

反演原理 若关于集合的并、交、补运算的某一关系式成立, 将式中的记号 $\cup, \cap, \subset, \supset$ 对应地换成 $\cap, \cup, \supset, \subset$, 式中出现的等号不变, 且把式中每个集合换成它的补集合, 则得到的关系式也成立。

定义 1.12 若集列 $\{A_n\}$ 满足 $A_n \subseteq A_{n+1}$, 则称 $\{A_n\}$ 为递增集列; 若集列 $\{A_n\}$ 满足 $A_n \supseteq A_{n+1}$, 则称 $\{A_n\}$ 为递减集列。递增集列和递减集列统称为单调集列。

定理 1.3 单调集列一定收敛, 且

$$(1) \text{ 当 } \{A_n\} \text{ 为递增集列时, } \lim_{n \rightarrow \infty} A_n = \bigcup_{n=1}^{\infty} A_n;$$