

离散数学

王兵山 张 强 毛晓光



国防科技大学出版社

离 散 数 学

王兵山 张 强 毛晓光

国防科技大学出版社
· 长沙 ·

图书在版编目(CIP)数据

离散数学/王兵山,张强,毛晓光. —长沙:国防科技大学出版社,1998.8
ISBN 7-81024-491-4

- I. 离散数学
- II. ①王兵山②张强③毛晓光
- III. 离散数学—教材
- IV. O158

国防科技大学出版社出版发行
电话:(0731)4555681 邮政编码:410073
E-mail:gfkdcbs@public.cs.hn.cn
责任编辑:何 晋 责任校对:文 慧
新华书店总店北京发行所经销
国防科技大学印刷厂印装

*

开本:787×1092 1/16 印张:11.25 字数:260 千
1998年8月第1版第1次印刷 印数:1—3000册

*

定价:14.00 元

内 容 提 要

本书分 7 章系统介绍了集合论、数理逻辑、图论等离散数学最基本的内容,可作为计算机软件专业和硬件专业的“离散数学”课程教材,也可供从事计算机工作的科研人员、工程技术人员及其他有关人员参考。

前 言

随着计算机技术的发展,计算机的应用也日益广泛。除了一般的科学计算之外,它还深入到了组织管理、情报检索和社会的公共服务事业等各个方面。同时,计算机的理论也日臻完善,逐渐产生并形成了独立的计算机科学。因为计算机科学以研究计算机领域中的一些普遍规律为其主要任务,所以需要大量的近代数学作为工具。由于它所用的数学多具有“离散性”和“能行性”这两大特点,故而称之为“离散数学”。离散数学的内容一直随着计算机科学的发展而不断地扩充与更新。到目前为止,它包括的主要内容有:集合论、数理逻辑、抽象代数、图论、可计算性理论、自动机理论、组合学和离散概率论等等。

离散数学对计算机技术和计算机科学的发展,一直起着重大作用。在计算机产生之前,图灵在研究可计算性时于1936年提出了一个抽象机模型,即著名的图灵机,并证明了存在能存储程序的通用图灵机,这为1946年问世的第一台电子计算机奠定了理论基础。在计算机发展的初期,利用布尔代数理论研究开关电路从而建立了一门完整的数字逻辑理论,对计算机的逻辑设计起了很大作用。在近期,利用自动机理论研究形式语言和编译,利用谓词演算研究程序理论,利用代数结构研究编码理论,利用自动机和递归函数研究可计算性问题。此外,在计算机科学中普遍采用了离散数学中的基本概念、基本思想和方法。例如,集合论的概念和方法,抽象代数的概念和方法,在计算机科学的各个领域,到处都能碰到。所有这些都使离散数学在计算机科学中的地位和作用越来越重要,成了必不可少的理论工具。这就难怪有人把离散数学叫做“计算机数学”了。

本书是作者在国防科技大学计算机系长期讲授离散数学课程时而编写的,本次修订在王兵山、王长英、周贤林和何自强编著的《离散数学》(国防科技大学出版社,1985)前七章内容基础上作了较大变动。除对部分定义、定理、例题和习题的补充和修订以外,还对第五、六、七章的若干内容进行了重写。本书包括集合论、数理逻辑、图论等离散数学的最基本内容,抽象代数和组合学则在另一本书《抽象代数》中介绍,本书可作为计算机各专业离散数学课程的教材。

本次修订在进一步强调基本概念和基本方法的基础上,对原有内容进行了更新和补充,对某些较难较深的内容进行了简化或重新编写。例如,对数理逻辑中具有相当难度的命题符号化抽象给出了词性翻译的大致准则,并辅以典型例题说明符号化的一般思路;对自然推理系统中的定理证明,针对如何引入附加前提进行形式推理这一难点,结合大量例题给出了引入附加前提的基本原则,使学生能更好地掌握基本的形式证明方法;对不恰当的定义(如特征函数中的函数运算)进行了修正;将某些繁琐算法(如求网络最大流的算法等)改为易于理解、便于使用的操作方法,增强实用性;同时增补了大量例题和习题,以便于教学和自学。书中所有修订均经过三位作者的共同商讨,最后由王兵山统一审定。

一般说来,阅读本书不需要具备高等数学知识,但希望读者具有一定的逻辑思维能力,且经过一定的数学训练。由于离散数学是一门数学,因此本书力求叙述严格,证明与推导的逻辑性强,思路清楚,使学生通过本课程的学习后能得到严格的逻辑推理与抽象思维能力的训练。

全书共分七章。前三章叙述朴素集合论的基本内容。第四章至第六章是数理逻辑,与其它离散数学教材不同的是,本书引入了比较严格的自然推理系统,以及在人工智能中应用广泛的艾尔布朗定理。第七章是图论,力求使定义和定理的叙述严格而明确。本书中习题数量较多,其中大部分是基本的,只要熟悉了教材的基本内容即可做出。但也有少数习题难度较大,需要一定的技巧才能做出,供学生选做。

本书的编写得到了国防科技大学计算机系、计算机软件教研室和国防科技大学出版社的大力支持,在此表示衷心的感谢。

本书虽经多次修订,难免仍然存在错误疏漏之处,望广大读者批评指正。

编 者

1998 年 4 月

目 录

第一章 集 合

§ 1.1 集合及其表示	1
§ 1.2 集合的运算	7
§ 1.3 自然数和归纳法	14
§ 1.4 笛卡儿乘积	20

第二章 二元关系

§ 2.1 关系	24
§ 2.2 关系矩阵与关系图	27
§ 2.3 逆关系	31
§ 2.4 关系的合成	33
§ 2.5 关系的闭包	36
§ 2.6 相容关系	41
§ 2.7 等价关系	44
§ 2.8 序关系	50

第三章 函 数

§ 3.1 部分函数	57
§ 3.2 函数的合成	61
§ 3.3 逆函数	64
§ 3.4 特征函数	67
§ 3.5 基数	69
§ 3.6 基数算术	74

第四章 命题逻辑

§ 4.1 命题和联结词	75
§ 4.2 合式公式	78
§ 4.3 等价和蕴含	83
§ 4.4 范式和判定问题	87

第五章 谓词逻辑

§ 5.1 变元、谓词和量词	92
§ 5.2 合式公式	98
§ 5.3 永真式	102
§ 5.4 永真式的判定	106

第六章 自然推理系统

§ 6.1 自然推理系统	110
--------------------	-----

§ 6.2 形式证明方法	116
第七章 图 论	
§ 7.1 图的基本概念	122
§ 7.2 子图和图的运算	126
§ 7.3 路径、回路和连通性	131
§ 7.4 欧拉图和哈密顿图	137
§ 7.5 图的矩阵表示	140
§ 7.6 树、有向树和有序树	145
§ 7.7 二部图	154
§ 7.8 平面图	157
§ 7.9 网络流	161
参考书目	
符 号 表	
索 引	

第一章 集 合

集合是现代数学中最重要的基本概念之一。

众所周知,在任何一种数学理论中,不可能对其中每个概念都严格定义。比如说,它的第一个概念就无法定义,因为已没有能用于定义这个概念的更原始的概念了。我们称这种不能严格定义的概念为该数学理论的原始概念,而称其余的概念为原始概念的派生概念。如在欧氏几何学中,“点”和“线”是原始概念,而“三角形”和“圆”则为派生概念。在这里,我们把“集合”就作为不能严格定义的原始概念。

本章主要介绍集合及其表示、集合的运算、自然数和归纳法。

§ 1.1 集合及其表示

因为集合是不能严格定义的原始概念,所以对它就只能给予直观描述。所谓集合,是由某些可以互相区分的任意对象,如数、变量、函数、符号、字母、数字、图、语句、程序或事件等等,汇集在一起所组成的一个整体。所涉及的各个对象,统称为元素。组成一个集合的各个对象,称为这个集合的元素或成员。

例 1 以下是一些集合的例子:

- 1) 中国人的集合;
- 2) 中国的山与河的集合;
- 3) 1000 以内的素数的集合;
- 4) 方程 $x^2+x+1=0$ 的实根的集合;
- 5) 自然数(即非负整数)的集合;
- 6) 直线 $y=2x-5$ 上的点的集合。

在组成集合的对象中,也允许有集合,即允许把集合作为其它集合的元素。

例 2 在以下集合的元素中,有的就是集合:

- 1) 例 1 中列举的集合的集合;
- 2) 由 a, b 和自然数的集合一起所组成的集合。

对例 2 的 1),集合的每个元素都是集合;对例 2 的 2),集合的一些元素是集合,另一些元素不是集合。

通常,我们用大写拉丁字母 $A, B, C, \dots$ 表示集合,用小写拉丁字母 $a, b, c, \dots$ 表示元素。用以下字母表示固定集合:

Q ——有理数的集合;

N ——自然数的集合;

I ——整数的集合;
 R ——实数的集合;
 C ——复数的集合;
 E_v ——偶自然数的集合;
 O_d ——奇自然数的集合;
 N_m ——小于 m 的自然数的集合;
 I_+ ——正整数的集合;
 I_- ——负整数的集合;
 R_+ ——正实数的集合;
 R_- ——负实数的集合.

设 a 为任意一个对象, A 为任意一个集合. 在 a 和 A 之间有且仅有以下两种情况之一出现:

- (1) a 为 A 的元素, 记为“ $a \in A$ ”或“ $A \ni a$ ”, 并称为“ a 属于 A ”或“ A 含有 a ”;
- (2) a 不为 A 的元素, 记为“ $a \notin A$ ”或“ $A \not\ni a$ ”, 有时也记为“ $a \bar{\in} A$ ”或“ $A \bar{\ni} a$ ”, 并称“ a 不属于 A ”或“ A 不含有 a ”.

当 $a_1 \in A, a_2 \in A, \dots, a_n \in A$ 时, 常简写作 $a_1, a_2, \dots, a_n \in A$.

定义 1.1.1 设 A 为任意一个集合, $n(A)$ 表示 A 含有的元素的个数.

- i) 若 $n(A)=0$, 则称 A 为空集;
- ii) 若 $n(A)$ 为自然数, 则称 A 为有限集;
- iii) 若 $n(A)$ 为无穷大, 则称 A 为无限集;
- iv) 若 $n(A) \neq 0$, 则称 A 为非空集.

显然, 空集是不含有任何元素的有限集, 常用符号 $\emptyset$ 表示.

在例 1 所列举的集合中, 1)、2) 和 3) 都是非空有限集 (即不是空集的有限集), 4) 为空集, 而 5) 和 6) 都是无限集.

在上面列举的常用的重要集合中, 只有 N_m 为有限集, 其余的都是无限集.

定义 1.1.2 设 A, B 为任意两个集合.

- i) 若对每个 $a \in A$ 皆有 $a \in B$, 则称 A 为 B 的子集或 B 包含 A , 也称 B 为 A 的母集, 记为 $A \subseteq B$ 或 $B \supseteq A$.
- ii) 若 $A \subseteq B$ 且 $B \subseteq A$, 则称 A 和 B 相等, 记为 $A=B$; 否则, 称 A 和 B 不相等, 并记为 $A \neq B$.
- iii) 若 $A \subseteq B$ 且 $A \neq B$, 则称 A 为 B 的真子集或 B 真包含 A , 记为 $A \subset B$ 或 $B \supset A$.

由此可知, 两个集合相等, 仅指它们所含有的元素完全相同. 所以, 我们要想确定一个集合, 只需要确定: 哪些元素属于这个集合, 哪些元素不属于这个集合. 至于这些元素用什么方法描述或指定, 并无关紧要. 因此, 我们可以用种种不同的方法描述一个集合. 常用的方法有以下四种:

1) 列举法

依照任意一种次序, 不重复地列举出集合的全部元素, 并用一对花括号括起来. 例如 10 以内的素数的集合 $= \{2, 3, 5, 7\}$.

列举法仅适用于所含有的元素个数不太多的有限集。

2) 部分列举法

依照任意一种次序,不重复地列举出集合的一部分元素。这部分元素要能充分体现出该集合的元素在上述次序下的构造规律,从而能够很容易地获得该集合中的任何一个未列举出的元素。未列举出的元素用“…”代替。然后,用一对花括号把已列举出的元素和“…”一起括起来。例如

$$N = \{0, 1, 2, \dots\}$$

$$E_v = \{0, 2, 4, \dots\}$$

$$O_d = \{1, 3, 5, \dots\}$$

部分列举法仅适用于元素的构造规律比较明显、简单的集合。它们可以是无限集,也可以是元素个数较多的有限集。

3) 命题法

用这种方法定义一个集合 A 时,要给出一个与 x 有关的命题 $P(x)$,使得

$$x \in A \text{ 当且仅当 } P(x) \text{ 为真}$$

并称 A 为“使 $P(x)$ 为真的 x 的集合”,记为

$$A = \{x | P(x)\} \text{ 或 } A = \{x: P(x)\}$$

例如,

$$N_m = \{n | n \in N \text{ 且 } 0 \leq n < m\}, m \in N$$

$$\{1, 2\} = \{x | x \in R \text{ 且 } x^2 - 3x + 2 = 0\}$$

4) 归纳定义法

用这种方法定义一个非空集合 A 时,一般包括以下三步:

i) 基本项

已知某些元素(常用 S_0 表示由这些元素组成的非空集合)属于 A (即 $S_0 \subseteq A$). 这是构造 A 的基础,并保证 A 不空。

ii) 归纳项

给出一组规则,从 A 中元素出发,依据这些规则所获得的元素,仍然都是 A 中的元素。这是构造 A 的关键步骤。

iii) 极小化

如果集合 $S \subseteq A$ 也满足 i) 和 ii), 则 $S = A$. 这说明, A 中每个元素都可以通过有限次使用 i) 和 ii) 来获得,它保证所构造出的集合 A 是唯一的。

用归纳定义法定义自然数集合 N , 乃是数学归纳法的理论基础,在 § 1.3 中还要详述。由于步骤 iii) 在每次使用时都一样,所以常常省略不写。但是这并不是说没有这一步。

例 3 设 $k \in I_+$. 若 A_k 表示能够被 k 整除的自然数的集合,则 A_k 可以用归纳定义法定义如下:

i) $0 \in A_k$;

ii) 若 $n \in A_k$, 则 $(n+k) \in A_k$.

例 4 设 Σ 为任意一个符号表,即一个由符号组成的非空有限集。我们称由 Σ 中的有

限多个符号并置在一起所组成的符号串为 Σ 上的字, 不含任何符号的空符号串称为空字, 用 ϵ 表示。若用 Σ^* 表示 Σ 上的字的集合, 则 Σ^* 可以用归纳定义法定义如下:

- i) $\epsilon \in \Sigma^*$;
- ii) 若 $\alpha \in \Sigma^*$ 且 $a \in \Sigma$, 则 $a\alpha \in \Sigma^*$.

若用 Σ^+ 表示 Σ 上的非空字的集合, 则 Σ^+ 可以用归纳定义法定义如下:

- i) $\Sigma \subseteq \Sigma^+$;
- ii) 若 $\alpha, \beta \in \Sigma^+$, 则 $\alpha\beta \in \Sigma^+$.

定理 1.1.1 若 A, B 和 C 为任意三个集合, 则有

- i) $\emptyset \subseteq A$;
- ii) $A \subseteq A$;
- iii) 若 $A \subseteq B$ 且 $B \subseteq C$, 则 $A \subseteq C$;
- iv) 若 $A \subset B$ 且 $B \subset C$, 则 $A \subset C$.

证明 我们只证 i), 其余的留作练习。

用反证法。假定 $\emptyset \subseteq A$ 不成立, 则必存在某个 $a \in \emptyset$ 使 $a \in A$, 但 $a \in \emptyset$ 与 $\emptyset$ 为空集(即 $\emptyset$ 不含有任何元素)矛盾。

定理 1.1.2 空集是唯一的。

证明 设 $\emptyset_1$ 和 $\emptyset_2$ 为任意两个空集。根据定理 1.1.1 知, $\emptyset_1 \subseteq \emptyset_2$ 且 $\emptyset_2 \subseteq \emptyset_1$. 所以 $\emptyset_1 = \emptyset_2$.

定义 1.1.3 设 A 为任意集合。若令

$$\mathcal{P}(A) = \{x | x \subseteq A\},$$

则称 $\mathcal{P}(A)$ 为 A 的幂集(A 的幂集有时也记为 2^A , 即 $2^A = \mathcal{P}(A)$)。

例 5 我们不难验证有

- 1) $\mathcal{P}(\emptyset) = \{\emptyset\}$;
- 2) $\mathcal{P}(\{a\}) = \{\emptyset, \{a\}\}$;
- 3) $\mathcal{P}(\{a, b\}) = \{\emptyset, \{a\}, \{b\}, \{a, b\}\}$.

定理 1.1.3 若 A, B 为任意两个集合, 则有

- i) $\emptyset \in \mathcal{P}(A)$;
- ii) $A \in \mathcal{P}(A)$;
- iii) 若 $A \subseteq B$, 则 $\mathcal{P}(A) \subseteq \mathcal{P}(B)$;
- iv) 若 $A \subset B$, 则 $\mathcal{P}(A) \subset \mathcal{P}(B)$.

证明

i) 和 ii) 可由定理 1.1.1 和定义 1.1.3 直接推出。

iii) 若 $x \in \mathcal{P}(A)$, 则 $x \subseteq A$. 因为 $A \subseteq B$, 所以 $x \subseteq B$. 因此 $x \in \mathcal{P}(B)$. 从而知道 $\mathcal{P}(A) \subseteq \mathcal{P}(B)$ 成立。

iv) 因为 $A \subset B$, 所以 $A \subseteq B$ 且 $A \neq B$. 从而知道 $B \in \mathcal{P}(B)$ 且 $B \notin \mathcal{P}(A)$. 因此, 根据刚证明的 iii) 即知, $\mathcal{P}(A) \subset \mathcal{P}(B)$.

定理 1.1.4 若 A 为有限集, 则

$$n(\mathcal{P}(A)) = 2^{n(A)}.$$

证明 设 $n(A)=m$. 因为对每个不大于 m 的自然数 i , A 的恰有 i 个元素的子集个数, 为从 m 个不同的元素中每次取出 i 个元素的不同组合数, 即 C_m^i . 所以 A 的不同子集之总数 $n(\mathcal{P}(A))$ 为

$$\begin{aligned} n(\mathcal{P}(A)) &= C_m^0 + C_m^1 + \cdots + C_m^m \\ &= (1+1)^m \\ &= 2^m \\ &= 2^{n(A)} \end{aligned}$$

最后, 我们指出, 前面给予集合的直观描述不能当做集合的严格定义, 因为它不能避免逻辑上的矛盾。这可由下面著名的罗素(B. Russell)悖论来说明。

例 6(罗素悖论) 若设

$$\mathcal{S} = \{S | S \text{ 是集合且 } S \notin S\},$$

则 $\mathcal{S}$ 不是集合。

证明 用反证法。

假定 $\mathcal{S}$ 是集合, 则有且仅有以下的两种情况之一出现:

- i) $\mathcal{S} \in \mathcal{S}$. 这时由 $\mathcal{S}$ 的定义知 $\mathcal{S} \notin \mathcal{S}$;
- ii) $\mathcal{S} \notin \mathcal{S}$. 这时由 $\mathcal{S}$ 的定义知 $\mathcal{S} \in \mathcal{S}$.

总之, 恒有

$$\mathcal{S} \in \mathcal{S} \text{ 当且仅当 } \mathcal{S} \notin \mathcal{S}$$

这是一个矛盾。所以 $\mathcal{S}$ 不可能是集合。

为了解决集合论中的悖论问题, 人们从 20 世纪初就开始了公理化集合论的研究, 并提出了集合论的种种公理系统。这超出了本书的范围, 有兴趣的读者请参看有关著作。

由于例 6 中的 $\mathcal{S}$ 符合我们给予集合的直观描述, 但又不是集合, 这不免会引起人们的怀疑: 我们给予集合的直观描述还有没有意义? 尽管集合论中的悖论产生的原因比较复杂, 但在本书和计算机科学中所涉及的集合, 都不会引出悖论, 所以我们给予集合的直观描述还是有意义的。这也正是我们以朴素集合论为满足的原因。

习 题 1.1

1. 用列举法给出下列集合:
 - a) 小于 5 的非负整数的集合;
 - b) 10 到 20 之间的素数的集合;
 - c) 不超过 65 的 12 之正整数倍数的集合。
2. 用命题法给出下列集合:
 - a) 不超过 100 的自然数的集合;
 - b) E_v 和 O_d ;
 - c) 10 的整倍数的集合。
3. 用归纳定义法给出下列集合:
 - a) 允许有前 0 的十进制无符号整数的集合;
 - b) 不允许有前 0 的十进制无符号整数的集合;

- c) 允许有前 0 和后 0 的有有限小数部分的十进制无符号实数的集合;
- d) 不允许有前 0 的二进制无符号偶数的集合;
- e) E_v 和 O_d ;
- f) 集合 $\{0, 1, 4, 9, 16, 25, \dots\}$.

4. 确定下列集合中哪些是相等的:

$$A = \{x \mid x \text{ 为偶数且 } x^2 \text{ 为奇数}\}$$

$$B = \{x \mid \text{有 } y \in I \text{ 使 } x = 2y\}$$

$$C = \{1, 2, 3\}$$

$$D = \{0, 2, -2, 5, -3, 4, -4\}$$

$$E = \{2x \mid x \in I\}$$

$$F = \{3, 3, 2, 1, 2\}$$

$$G = \{x \mid x \in I \text{ 且 } x^3 - 6x^2 - 7x - 6 = 0\}$$

5. 确定下列关系中哪些是正确的, 并简单说明理由。

a) $\emptyset \subseteq \emptyset$

b) $\emptyset \in \emptyset$

c) $\emptyset \subseteq \{\emptyset\}$

d) $\emptyset \in \{\emptyset\}$

e) $\{a, b\} \subseteq \{a, b, c, \{a, b, c\}\}$

f) $\{a, b\} \in \{a, b, c, \{a, b, c\}\}$

g) $\{a, b\} \subseteq \{a, b, \{\{a, b\}\}\}$

h) $\{a, b\} \in \{a, b, \{\{a, b\}\}\}$

6. 设 A, B 和 C 为集合。证明或用反例推翻以下的各个命题:

a) 若 $A \in B$ 且 $B \in C$, 则 $A \in C$.

b) 若 $A \in B$ 且 $B \in C$, 则 $A \in C$.

c) 若 $A \subseteq B$ 且 $B \in C$, 则 $A \in C$.

d) 若 $A \in B$ 且 $B \in C$, 则 $A \in C$.

7. 若 A, B 为集合, 则 $A \subseteq B$ 与 $A \in B$ 能同时成立吗? 请证明你的结论。

8. 列举出下列集合中每个集合的所有子集:

a) $\{1, 2, 3\}$

b) $\{1, \{2, 3\}\}$

c) $\{\{1, \{2, 3\}\}\}$

d) $\{\emptyset\}$

e) $\{\emptyset, \{\emptyset\}\}$

f) $\{\{1, 2\}, \{2, 1, 1\}, \{2, 1, 1, 2\}\}$

g) $\{\{\emptyset, 2\}, \{2\}\}$

9. 给出下列集合的幂集:

a) $\{a, \{b\}\}$

b) $\{1, \emptyset\}$

$$c) \{x, y, z\}$$

$$d) \{\emptyset, a, \{a\}\}$$

$$e) \mathcal{P}(\{\emptyset\})$$

10. 设 $\mathcal{P}(A) = \mathcal{P}(B)$. 证明 $A = B$.

§ 1.2 集合的运算

通常, 在我们讨论某类问题时, 往往有一个固定的集合, 它含有我们所涉及的全部元素。我们称这个固定集合为全集或空间, 并常用 U 表示。这时, 其余的集合就都是全集 U 的子集。有时, 我们并不具体指明全集是什么, 但总是假定所涉及的每个集合都是全集的一个子集。

定义 1.2.1 设 A, B 为任意两个集合。令

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

$$A \cap B = \{x | x \in A \text{ 且 } x \in B\}$$

$$A - B = \{x | x \in A \text{ 且 } x \notin B\}$$

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

我们分别称 $A \cup B, A \cap B, A - B$ 和 $A \oplus B$ 为 A 与 B 的并、交、差和对称差。我们还把 $U - A$ 称为 A 的补集, 并用 $\sim A$ 表示。

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

对集合的运算, 我们可以用文氏图(见图 1.2.1)直观地表示。图中阴影区表示运算的结果。

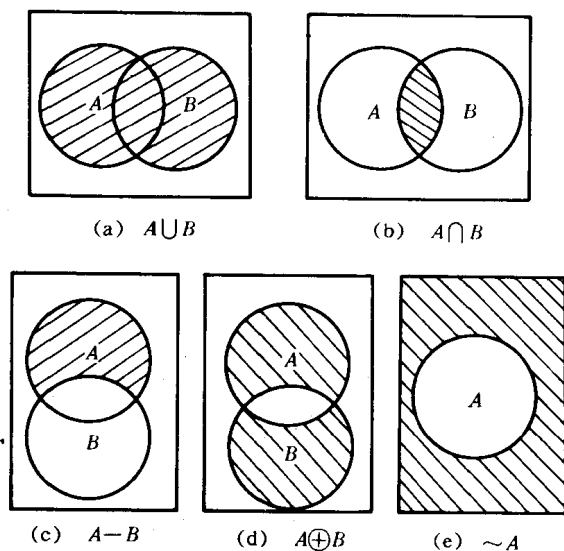


图 1.2.1 集合运算的文氏图

例 1 若取 $U = \{0, 1, 2, 3, 4, 5\}$, $A = \{1, 2, 5\}$ 及 $B = \{2, 4\}$ 时, 则有
 $A \cup B = \{1, 2, 4, 5\}$,

$$\begin{aligned}
 A \cap B &= \{2\}, \\
 A - B &= \{1, 5\}, \\
 A \oplus B &= \{1, 4, 5\}, \\
 \sim A &= \{0, 3, 4\}, \\
 \sim B &= \{0, 1, 3, 5\}.
 \end{aligned}$$

定理 1.2.1 设 A, B 和 C 为任意三个集合。

- i) $A \subseteq A \cup B$ 且 $B \subseteq A \cup B$;
- ii) $A \cap B \subseteq A$ 且 $A \cap B \subseteq B$;
- iii) $A - B \subseteq A$;
- iv) $A - B = A \cap \sim B$;
- v) 若 $A \subseteq B$, 则 $\sim B \subseteq \sim A$;
- vi) 若 $A \subseteq C$ 且 $B \subseteq C$, 则 $A \cup B \subseteq C$;
- vii) 若 $A \subseteq B$ 且 $A \subseteq C$, 则 $A \subseteq B \cap C$;

这个定理的证明很容易, 留作练习。

定理 1.2.2 若 A, B 为任意两个集合, 则以下条件互相等价:

- i) $A \subseteq B$;
- ii) $A \cup B = B$;
- iii) $A = A \cap B$.

证明

i) $\Rightarrow$ ii) 任取 $x \in A \cup B$, 则 $x \in A$ 或 $x \in B$. 但因 $A \subseteq B$, 所以总有 $x \in B$. 这表明 $A \cup B \subseteq B$. 再根据定理 1.2.1 的 i) 即得到 $A \cup B = B$.

ii) $\Rightarrow$ iii) 任取 $x \in A$, 则 $x \in A \cup B$. 但因 $A \cup B = B$, 所以 $x \in B$. 因此 $x \in A \cap B$. 这表明 $A \subseteq A \cap B$. 再根据定理 1.2.1 的 ii) 即得到 $A = A \cap B$.

iii) $\Rightarrow$ i) 任取 $x \in A$, 则 $x \in A \cap B$, 所以 $x \in B$. 这表明 $A \subseteq B$.

关于集合运算的一些基本定律, 我们列举如下:

1) 幂等律

$$A \cup A = A$$

$$A \cap A = A$$

2) 结合律

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

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

3) 交换律

$$A \cup B = B \cup A$$

$$A \cap B = B \cap A$$

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) 同一律

- $$A \cup \emptyset = A$$
- $$A \cap U = A$$
- 6) 零律
- $$A \cup U = U$$
- $$A \cap \emptyset = \emptyset$$
- 7) 互补律
- $$A \cup \sim A = U$$
- $$A \cap \sim A = \emptyset$$
- 8) 吸收律
- $$A \cup (A \cap B) = A$$
- $$A \cap (A \cup B) = A$$
- 9) 德·摩尔根(De Morgan)律
- $$\sim(A \cup B) = \sim A \cap \sim B$$
- $$\sim(A \cap B) = \sim A \cup \sim B$$
- 10) 对合律
- $$\sim(\sim A) = A$$
- 11) $\sim U = \emptyset$
- $$\sim \emptyset = U$$

这些定律的证明并不难。下面我们仅以对合律、分配律和德·摩尔根律为例来说明一般的证明方法。

先证对合律。

对任意的 $x \in U$, 因为 $x \in A$ 当且仅当 $x \notin \sim A$, $x \notin \sim A$ 当且仅当 $x \in \sim(\sim A)$, 所以, $x \in A$ 当且仅当 $x \in \sim(\sim A)$. 这表明 $\sim(\sim A) = A$.

再证德·摩尔根律。

对任意的 $x \in U$, 因为 $x \in \sim(A \cup B)$ 当且仅当 $x \notin A \cup B$, $x \notin A \cup B$ 当且仅当 $x \notin A$ 且 $x \notin B$, 即 $x \in \sim A$ 且 $x \in \sim B$, 所以 $x \in \sim(A \cup B)$ 当且仅当 $x \in \sim A \cap \sim B$. 这表明 $\sim(A \cup B) = \sim A \cap \sim B$.

当用 $\sim A$ 和 $\sim B$ 分别代替刚证明的 $\sim(A \cup B) = \sim A \cap \sim B$ 中之 A 和 B 时, 就得到

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

但由对合律知道 $A \cap B = \sim(\sim A) \cap \sim(\sim B)$, 所以

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

最后, 我们来证分配律。

因为 $A \subseteq A \cup B$ 且 $A \subseteq A \cup C$, 所以 $A \subseteq (A \cup B) \cap (A \cup C)$. 因为 $B \cap C \subseteq B \subseteq A \cup B$ 且 $B \cap C \subseteq C \subseteq A \cup C$, 所以 $B \cap C \subseteq (A \cup B) \cap (A \cup C)$. 因此得到

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

另一方面, 任取 $x \in (A \cup B) \cap (A \cup C)$, 则 $x \in A \cup B$ 且 $x \in A \cup C$. 如果 $x \notin A$, 则由 $x \in A \cup B$ 知 $x \in B$, 由 $x \in A \cup C$ 知 $x \in C$, 所以 $x \in B \cap C$. 从而知道, 总有 $x \in A$ 或 $x \in B \cap C$, 即 $x \in A \cup (B \cap C)$. 这表明 $(A \cup B) \cap (A \cup C) \subseteq A \cup (B \cap C)$.