离 散 数 学

王兵山 王长英
周贤林 何自强 编

国防科技大学出版社

内 容 提 要

本书系统地介绍了离散数学各分支的基本内容。全书共分十四章，主要包括：集合论、数理逻辑、图论、原始递归函数、程序正确性验证、代数结构及其在计算机科学中的应用。它可作为计算机软件专业和硬件专业的“离散数学”课程的教材，供一学年教学之用。它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。

离 散 数 学

王兵山 王长英 周贤林 何自强 编

责任编辑 王金荣

装帧设计 侯 云

*

国防科技大学出版社 出版

湖 南 省 新 华 书 店 发 行

国防科技大学印刷厂印装

*

开本：787×1092 1/16 印张：20 6/16 字数：462千字

1985年6月第一版 1986年3月第二次印刷 印数：3,001—13,000 册

统一书号：15415·0002 定价：4.00 元

3.34

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中，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。

本书是作者为在国防科技大学计算机系讲授离散数学课程而编写的，这次付印做了修改和补充。它可以作为理工科院校计算机软件专业和硬件专业的教材，供一学年教学之用。

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，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。

全书共分十四章。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。第八章详细讨论了原始递归函数的性质，引进了递归函数，即能行可计算函数的概念。第九章讨论数理逻辑和集合论在计算机科学中的重要应用——程序正确性验证。第

十章至第十四章是代数结构及其在计算机科学中的应用，除了群和环的基本性质之外，还详细讨论了有限域，因为有限域的理论是编码理论的基础。

本书习题数量较多，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，供学习成绩好的学生选做，

武汉大学曾宪昌教授，中山大学麦卓文老师，国防科技大学宫德荣付教授审阅了全部书稿，并提出了修改意见，在此谨致谢意。

由于我们水平不高，加之时间仓促，错误疏漏之处一定不少，还望广大读者批评指正。

编　者

1984年11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……21

第二章　二元关系

§2.1　关系……25

§2.2　关系矩阵与关系图……29

§2.3　逆关系……33

§2.4　关系的合成……35

§2.5　关系的闭包……39

§2.6　相容关系……44

§2.7　等价关系……47

§2.8　序关系……53

第三章　函　数

§3.1　部分函数……62

§3.2　函数的合成……66

§3.3　逆函数……69

§3.4　特征函数……72

§3.5　基数……73

§3.6　基数算术……78

第四章　命题逻辑

§4.1　命题和联结词……80

§4.2　合式公式……83

§4.3　等价和蕴含……87

§4.4　范式和判定问题……92

第五章　谓词逻辑

§5.1　变元、谓词和量词……97

§5.2　合式公式…… 104

§5.3　永真式…… 108

§5.4　永真式的判定…… 111

第六章　自然推理系统

§6.1 自然推理系统…… 115
§6.2 形式推理关系的简化证明…… 121
第七章 图 论
§7.1 图的基本概念…… 125
§7.2 子图和图的运算…… 130
§7.3 路径、回路和連通性…… 134
§7.4 欧拉图和哈密顿图…… 141
§7.5 图的矩阵表示…… 144
§7.6 树、有向树和有序树…… 148
§7.7 二部图…… 157
§7.8 平面图…… 161
§7.9 网络流…… 164
第八章 原始递归函数
§8.1 原始递归函数的定义…… 170
§8.2 常用函数的原始递归性…… 173
§8.3 康托尔编码和哥德尔编码…… 181
§8.4 原始递归谓词…… 189
§8.5 部分递归函数的概念…… 194
§8.6 阿克曼函数…… 197
第九章 程序正确性验证
§9.1 流图程序…… 206
§9.2 霍尔的程序逻辑…… 215
§9.3 终止推断规则…… 219
第十章 代数结构
§10.1 代数运算…… 223
§10.2 代数结构…… 226
§10.3 同态与同构…… 227
§10.4 同余关系…… 230
§10.5 商代数和积代数…… 232
第十一章 半群、独异点和群
§11.1 半群和独异点…… 236
§11.2 群的基本性质…… 239
附录 初等数论中的某些结果…… 242
§11.3 子群和群的同态…… 244
§11.4 变换群与循环群…… 246
§11.5 不变子群、商群和群同态定理…… 250
第十二章 环和域
§12.1 具有两个二元运算的代数结构…… 256

§12.2 有限域…… 263
附录 域上多项式的最高公因式…… 268
§12.3 有限域的结构…… 269
§12.4 有限域的表示…… 275
第十三章 格与布尔代数
§13.1 格及其性质…… 278
§13.2 格是一种代数…… 282
§13.3 特殊格…… 285
§13.4 布尔代数…… 288
§13.5 有限布尔代数的唯一性…… 294
§13.6 自由布尔代数…… 296
第十四章 代数结构在计算机设计中的应用
§14.1 剩余算术在计算机设计中的应用…… 302
§14.2 动态存贮器的置换联结…… 305
参考书目…… 311
符 号 表…… 311
索 引…… 314

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，而称其余的概念为它的派生概念。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”也作为这样的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，乃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，另一些素不是集合。

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

$\boldsymbol{Q}$——有理数的集合；

$\boldsymbol{N}$——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，则在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“$a\in A$”或“$A\ni a$”，并称为“a不属于A”或“A不含有a”。

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

定义 1.1.1 设A为任意一个集合，用$n(A)$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$\varnothing$表示。

在例1所列举的集合中，1)、2)和3)都是非空有限集（即为有限集，且不为空集的集合），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。但是，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

$$\boldsymbol{N}=\{0,1,2,\cdots\}$$
$$\boldsymbol{E}_{\upsilon}=\{0,2,4,\cdots\}$$
$$\boldsymbol{O}_{d}=\{1,3,5,\cdots\}$$

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，也可以是所含有的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

$x\in A$，当且仅当$P(x)$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，

$$\boldsymbol{N}_{m}=\{n|\,n\in\boldsymbol{N}\ \text{且}\ 0\leqslant n<m\}$$
$$\{1,2\}=\{x|\,x\in\boldsymbol{R}\ \text{且}\ x^{2}-3x+2=0\}$$

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$\boldsymbol{N}$，乃是数学归纳法的理论基础，在§1.3中还要详述，这里就不多说了。由于步骤iii) 在每次使用时都一样，毫无变化，所以常常省略不写，这并不是说没有这一步。

例3 设$k\in\boldsymbol{I}_{+}$，若用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为任意一个字母表，即一个由符号组成的非空有限集。我们称由Σ中的有限多个字母并置在一起所组成的字母串为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) $e\in\Sigma^*$;

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 α，$\beta\in\Sigma^+$，则 $\alpha\beta\in\Sigma^+$.

定理 1.1.1 设A，B和C为任意三个集合，则有

i) $\varnothing\subseteq A$;

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

定理 1.1.2 空集是唯一的。

证明 设 $\varnothing_1$ 和 $\varnothing_2$ 为任意两个空集。根据定理 1.1.1 知，$\varnothing_1\subseteq\varnothing_2$ 且 $\varnothing_2\subseteq\varnothing_1$. 所以$\varnothing_1=\varnothing_2$.

定义 1.1.3 设A为任意集合，令

$$\mathscr{P}(A)=\{x\mid x\subseteq A\}.$$

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

例 5 我们不难验证有

1) $\mathscr{P}(\varnothing)=\{\varnothing\}$;

2) $\mathscr{P}(\{a\})=\{\varnothing,\{a\}\}$;

3) $\mathscr{P}(\{a,b\})=\{\varnothing,\{a\},\{b\},\{a,b\}\}$.

定理 1.1.3 设A，B为任意两个集合，则有

i) $\varnothing\in\mathscr{P}(A)$;

ii) $A\in\mathscr{P}(A)$;

iii) 若$A\subseteq B$，则$\mathscr{P}(A)\subseteq\mathscr{P}(B)$;

iv) 若$A\subset B$，则$\mathscr{P}(A)\subset\mathscr{P}(B)$.

证明

i) 和 ii) 可由定理 1.1.1 和定义 1.1.3 直接推出。

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

iv) 因为$A\subset B$，所以 $A\subseteq B$ 且 $A\neq B$. 从而知道 $B\in\mathscr{P}(B)$ 且 $B\notin\mathscr{P}(A)$. 因

此，根据刚证明的 iii) 即知，$\mathscr{P}(A)\subset\mathscr{P}(B)$.

定理 1.1.4 若A为有限集，则

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

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，即为C_m^i. 所以A的不同子集之总数$n(\mathscr{P}(A))$为

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

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） 设

$$\mathscr{S}=\{S\mid S \text{ 是集合且 } S\notin S\},$$

则$\mathscr{S}$不是集合。

证明 用反证法。

假定$\mathscr{S}$是集合，则有且仅有以下的两种情况之一出现：

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

ii) $\mathscr{S}\notin\mathscr{S}$. 这时由$\mathscr{S}$的定义知$\mathscr{S}\in\mathscr{S}$.

总之，恒有

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

这是一个矛盾。所以$\mathscr{S}$不可能是集合。

为了解决集合论中的悖论问题，人们从本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。这超出了本书的讨论范围，有兴趣的读者請参看有关著作。

由于例 6 中的$\mathscr{S}$，它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沒有意义？尽管集合论中的悖论产生的原因比较复杂，但在本书中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，够我们实际用的。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 的正整数倍数的集合。

2. 用命题法给出下列集合：

a) 不超过 100 的自然数的集合；

b) $\boldsymbol{E}_v$ 和 $\boldsymbol{O}_d$;

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) $\boldsymbol{E}_v$ 和 $\boldsymbol{O}_d$.

4. 确定下列集合中哪些是相等的:

$A=\{x|\ x$ 为偶数且 x^2 为奇数$\}$

$B=\{x|$ 有 $y\in \boldsymbol{I}$ 使 $x=2y\}$

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

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

$E=\{2x|\ x\in \boldsymbol{I}\}$

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

$G=\{x|\ x\in \boldsymbol{I}$ 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) $\varnothing\subseteq\varnothing$

b) $\varnothing\in\varnothing$

c) $\varnothing\subseteq\{\varnothing\}$

d) $\varnothing\in\{\varnothing\}$

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 $A\nsubseteq B$ 且 $B\nsubseteq \boldsymbol{C}$,则 $A\nsubseteq \boldsymbol{C}$.

b) 若 $A\in B$ 且 $B\nsubseteq \boldsymbol{C}$,则 $A\nsubseteq \boldsymbol{C}$.

c) 若 $A\subseteq B$ 且 $B\nsubseteq \boldsymbol{C}$,则 $A\nsubseteq \boldsymbol{C}$.

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

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

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) $\{\varnothing\}$

e) $\{\varnothing,\{\varnothing\}\}$

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

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

9. 给出下列集合的幂集：

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

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

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

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

§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

$$A\cup B=\{x\mid x\in A \text{ 或 } x\in B\}$$
$$A\cap B=\{x\mid x\in A \text{ 且 } x\in B\}$$
$$A-B=\{x\mid x\in A \text{ 且 } x\notin B\}$$
$$A\oplus B=(A\cup B)-(A\cap B)$$

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。我们还把差$U-A$称为A的补集，并用$\sim A$表示。

如果$A\cap B=\varnothing$，我们称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。

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

$$A\cup B=\{1,2,4,5\},$$
$$A\cap B=\{2\},$$
$$A-B=\{1,5\},$$
$$A\oplus B=\{1,4,5\},$$
$$\sim A=\{0,3,4\},$$
$$\sim B=\{0,1,3,5\}.$$

定理 1.2.1 设A，B和C为任意三个集合，则有

i) $A\subseteq A\cup B$且$B\subseteq A\cup B$;

ii) $A\cap B\subseteq A$且$A\cap B\subseteq B$;

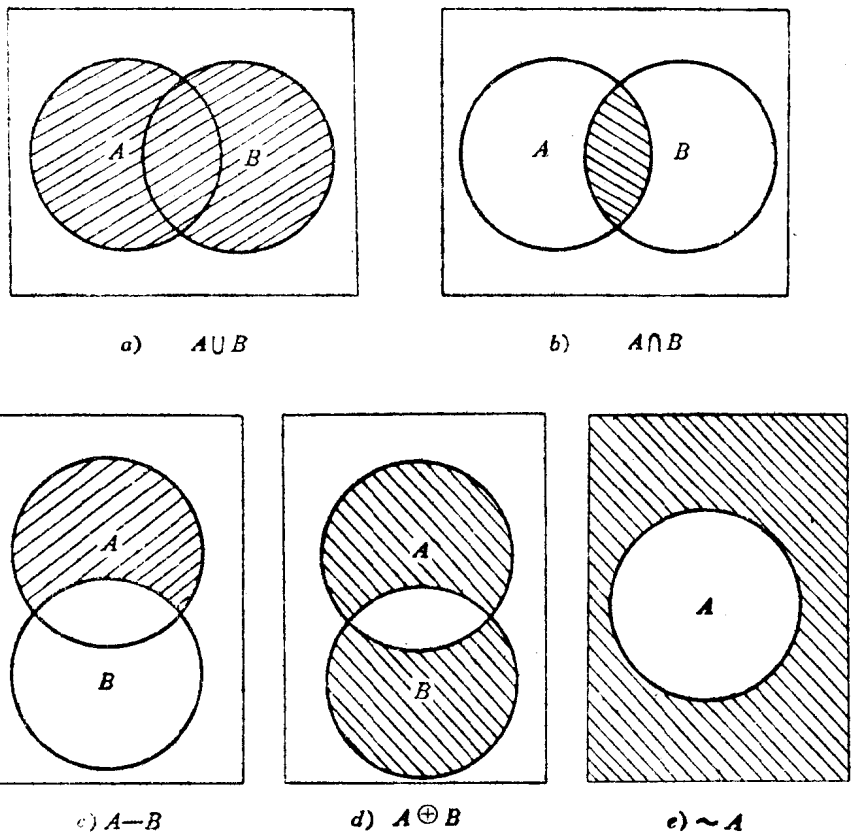
iii) $A-B\subseteq A$;

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$A\subseteq B\cap C$.



a) $A\cup B$　　b) $A\cap B$

c) $A-B$　　d) $A\oplus B$　　e) $\sim A$

图 1.2.1 集合运算的文氏图

这个定理的证明很容易，留作练习。

定理 1.2.2 设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) 这可由定理 1.2.1 的 ii) 直接推得。

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

$A\cup\varnothing=A$

$A\cap U=A$

6) 零律

$A\cup U=U$

$A\cap\varnothing=\varnothing$

7) 互补律

$A\cup\sim A=U$

$A\cap\sim A=\varnothing$

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)

$\sim U=\varnothing$

$\sim\varnothing=U$

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$x\in U$，则$x\in A$当且仅当$x\notin\sim A$. 但$x\notin\sim A$当且仅当$x\in\sim(\sim A)$。因此，$x\in A$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$x\notin A\cup B$，但$x\notin A\cup B$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$\sim(A\cup B)=\sim A\cap\sim B$中的$A$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$(A\cup B)\cap(A\cup C)\subseteq A\cup(B\cap C)$.

总结以上的结果，就得到

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

若用$\sim A$，$\sim B$和$\sim C$分别代替上式中的A，B和C即可得到

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

根据德·摩尔根律和对合律，由上式可得到

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

和

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

所以

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

我们下面来推广求两个集合的并和交的运算。为此，我们称完全以集合为元素的集合为集类，并常用字母$\mathscr{A}$，$\mathscr{B}$，$\mathscr{C}$，……表示。

定义 1.2.2 设$\mathscr{B}$为任意集类。

i）称集合$\{x\mid$有$B\in\mathscr{B}$使$x\in B\}$为$\mathscr{B}$的广义并，并记为$\bigcup\mathscr{B}$；

ii）若$\mathscr{B}\neq\varnothing$，则称集合$\{x\mid$若$B\in\mathscr{B}$，则$x\in B\}$为$\mathscr{B}$的广义交，并记为$\bigcap\mathscr{B}$.

在公理化的集合论中已经证明，定义 1.2.2 给出的$\bigcup\mathscr{B}$和$\bigcap\mathscr{B}$都是集合，而且所附加的条件也都是必不可少的。对此，我们就不再深入地讨论了。

下面我们再引进一些关于广义并和广义交的常用记号

1) 若$\mathscr{B}=\{B_0, B_1,\cdots,B_m\}$，则记

$$\bigcup\mathscr{B}=B_0\cup B_1\cup\cdots\cup B_m=\bigcup_{i=0}^{m}B_i$$

$$\bigcap\mathscr{B}=B_0\cap B_1\cap\cdots\cap B_m=\bigcap_{i=0}^{m}B_i$$

2) 若$\mathscr{B}=\{B_i\mid i\in N\}$，则记