国家精品课程主讲教材

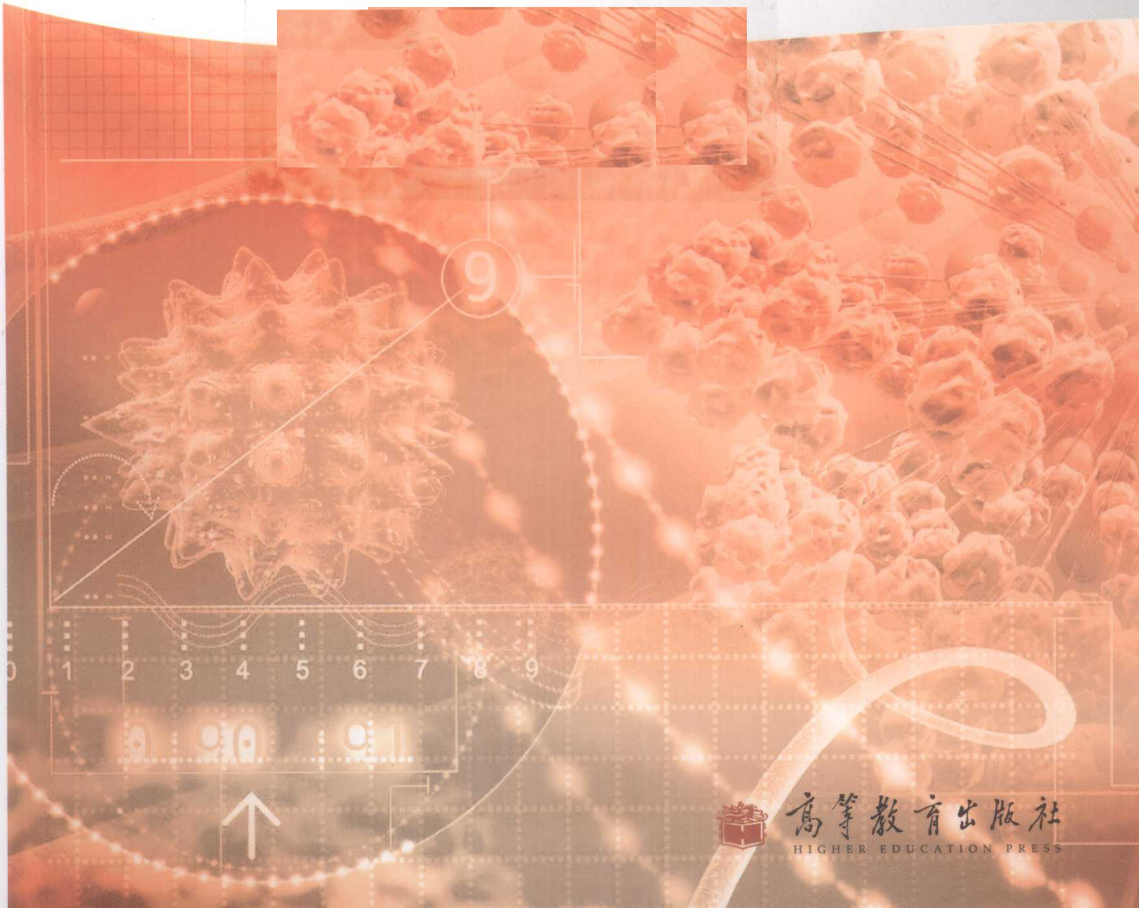
教育部高等理工教育教学改革与实践项目研究成果

《高等学校计算机科学与技术专业核心课程教学实施方案》规划教材

离散数学教程

A Course in Discrete Mathematics

王元元　等编著



高等教育出版社
HIGHER EDUCATION PRESS

国家精品课程主讲教材
教育部高等理工教育教学改革与实践项目研究成果
《高等学校计算机科学与技术专业核心课程教学实施方案》规划教材

离散数学教程

Lisan Shuxue Jiaocheng

王元元　沈克勤　李拥新　贺　汛　编著

高等教育出版社·北京
HIGHER EDUCATION PRESS　BEIJING

内容提要

本教程主要依据教育部计算机科学与技术教学指导委员会编制的《高等学校计算机科学与技术专业规范》和《高等学校计算机科学与技术专业核心课程教学实施方案》进行设计与定位，并针对综合性大学和工程类院校计算机科学与技术专业本科生进行选材与编撰。

本教程打破了传统离散数学教材几大模块分割的编写方式，突出知识的内在联系，强调理论的循序渐进、相互依存，从而更具有可读性和系统性。本教程不仅覆盖了集合论、数理逻辑、数论、组合论、图论、可计算性、抽象代数等基础理论部分，还包含了这些基本理论在粗糙集、模糊集、自动推理、智能搜索、加密技术等领域的应用，并涉及公理化集合论、数理逻辑形式系统、形式语言与自动机等相关理论。本教程以离散结构为建模对象，紧密联系计算机科学技术，特别强调应用能力、证明技术、计算思维的培养。

为便于学生及时复习并巩固所学知识，本教程在每节后安排了大量习题；同时，为便于学有余力的学生进一步深造，每章后安排了一节阅读材料，以此来对本章所介绍的理论进行深入探讨，或进一步介绍技术的应用层面。

本教程不仅可用作高等学校计算机及相关专业本科生的离散数学课程教材，也可供相关工程技术人员阅读参考。

图书在版编目(CIP)数据

离散数学教程/王元元等编著. —北京：高等教育出版社，2010.7

ISBN 978-7-04-029465-1

Ⅰ. ①离… Ⅱ. ①王… Ⅲ. ①离散数学—高等学校—教材 Ⅳ. ①O158

中国版本图书馆 CIP 数据核字(2010)第 098326 号

出版发行	高等教育出版社	购书热线	010-58581118
社　　址	北京市西城区德外大街 4 号	咨询电话	400-810-0598
邮政编码	100120	网　　址	http://www.hep.edu.cn http://www.hep.com.cn
		网上订购	http://www.landraco.com http://www.landraco.com.cn
经　　销	蓝色畅想图书发行有限公司		
印　　刷	北京宏信印刷厂	畅想教育	http://www.widedu.com
开　　本	787×1092　1/16	版　　次	2010 年 7 月第 1 版
印　　张	24.75	印　　次	2010 年 7 月第 1 次印刷
字　　数	540 000	定　　价	36.00 元

本书如有缺页、倒页、脱页等质量问题，请到所购图书销售部门联系调换。

物料号　29465-00

前　言

教过多年的离散数学课程，也写过离散数学教材，但总觉得这门课程现有的一些教材内容过于“离散”，体系结构间的相互衔接不尽合理，知识模块的内在联系不够紧密。教学之余，笔者感到似乎需要一本系统性更强的离散数学教程，以更好地满足教学的需求。因此，笔者在传统内容的基础上对内容进行扩展梳理，试图做成这样一部“离散数学教程”：它首先把离散结构涉及的原始概念，诸如集合、命题、谓词、运算等，提炼出来作为全部学习内容的准备知识，为其后的各大组成模块作统一的铺垫；然后介绍离散结构形式化表示的理论，即逻辑代数和集合代数；再基于所有这些公共基础，由浅入深、由简单到复杂、由具体到抽象地依次推出各类离散结构及其数学模型。现在呈现在读者面前的，正是笔者努力想要达成的“离散数学教程”的雏形。它在选材和编排上的内在逻辑大致体现在以下图示中。

<table>
<tr><td colspan="4">抽象代数结构</td></tr>
<tr><td>计算模型
离散结构</td><td>图离散结构</td><td>关系函数
离散结构</td><td>整数离散
结构</td></tr>
<tr><td colspan="2">逻辑代数</td><td colspan="2">集合代数</td></tr>
<tr><td colspan="4">准 备 知 识</td></tr>
</table>

如果说本教程在教学内容系统性的改造上所做的工作还只是一种尝试，那么在教学内容广泛性的开拓上可以说是用心良苦了。本教程不仅覆盖了集合论、数理逻辑、数论、组合论、图论、可计算性、抽象代数等基础理论部分，还包含了这些基本理论在粗糙集、模糊集、自动推理、智能搜索、加密技术等领域的应用，并涉及公理化集合论、数理逻辑形式系统、形式语言与自动机等相关理论。为了教师和学生能更好地使用本教程，更加便捷地在这个浩瀚的知识海洋里选取适合的模块、章节，以便设计出具有自己所在院校及专业特色的离散数学课程，我们把教程的全部内容分为了如下三个层次。

(1) 基本内容，它们是教程的主体。运用本教程的教师，可以依据教育部计算机科学与技术教学指导委员会编制的《高等学校计算机科学与技术专业规范》和《高等学校计算机科学与技术专业核心课程教学实施方案》，以及所在学校的特色、定位，在基本内容中选取大部或全部内容进行教学。

(2) 推荐内容，其标题被标记了 * 号。教程的这部分内容理论上较为深入，理解上有些难度，推荐给使用本教程的教师，可视情况选作教学内容或课外讲座。

(3) 阅读材料,安排在教程每章的最后一节。它们或为相关理论的深入探讨,或为相关技术的重要应用,可用作学生的课外阅读指南,以利于他们巩固课堂上所学的知识,提升学习兴趣并培养探索精神。

另外,本教程特别强调对应用能力、证明技术、计算思维的培养。全书多数章节都独具匠心地安排了相关的应用课题,涉及人工智能、数据安全、计算模型等多个学科领域。全书以证明技术的教学贯穿始终,尤为注重基于逻辑表示的形式推演,以及基于逻辑定律的证明模式,包括引入假设的证明技术、分支证明技术、证伪证明技术等;除了对归纳法的证明模式、理论依据进行全面的分析与探讨之外,还将其大量运用于后续教学内容的演绎中;在图论和可计算理论中,重点介绍了构造性证明及其与归纳法、反证法证明的联合运用;对"鸽笼原理"、"对角线法"等常用证明技巧的灵活运用也给予了充分的关注。全书对离散结构及其数学模型进行了全面深入的介绍,期望给读者一个对计算思维的直观诠释。笔者以为,计算思维的核心价值在于对计算的"形式可表示性"、"结构可归约性"、"模型可构造性"、"能行可操作性"以及"操作可编码性"的理解与把握,而本教程的几乎全部内容恰恰正是围绕着这些主题循序渐进地展开的,以至于笔者有这样的冲动,给我们的《离散数学教程》添加一个鲜明而富有激情的副标题:走向计算思维的必由之路。

作为教材,本教程在每节后安排了为数不少的习题,有利于学生及时复习并巩固所学的知识,训练计算、推理的能力以及问题求解的能力。

本教程不仅可以用作高等学校计算机及相关专业本科生的离散数学课程教材,也可供相关工程技术人员阅读参考。笔者将向使用本教程实施教学的教师提供与本教程配套的教学用课件,以及习题的详细解答。笔者的联系方式为 yuanyuanwang0@gmail.com。

本教程采用了笔者以往编写的教材中的一些素材、例子和习题,由于这些内容较为经典、成熟,故未对它们作实质性的改写,特此敬告老读者。此外,北京大学的屈婉玲教授审阅了书稿,在此表示诚挚的感谢!限于笔者的专业造诣和教学水准,本教程中的错误和疏漏在所难免,不当之处敬请读者不吝指正。

作 者

2010 年 2 月 8 日于南京

目　录

第0章
准备知识

什么是离散数学？离散数学是研究离散数量关系和离散结构数学模型的数学分支的一个集成。“离散”是“连续”的否定，即“不连续”；“连续”则是事物、数量的一种属性，这种属性使得它们容易被分割或结合，并且不会因此而丧失它们原有的属性。举例来说，整数是离散的，实数则是连续的；马铃薯是离散的，马铃薯羹则是连续的。

与初等数学和高等数学不同，离散数学处理的对象不再局限于连续的实数，而对离散的整数情有独钟，甚至不再局限于“数”，而是要面对任意对象所组成的离散结构；离散数学关注的问题也不再局限于数的运算，而是任意对象的总体属性以及它们之间的关系和运算。本章是阅读全书的准备内容，因此，首先要介绍各个章节公共的基础——离散结构的原始概念，包括集合、命题、谓词、运算等；然后介绍在逻辑推理中常常涉及的最为简单的一个数学原理——鸽笼原理。

0.1 集合、命题、谓词和运算

0.1.1 集合

集合(sets)是一个十分常用的基本概念。在中学的数学课程中，读者对集合及其元素的意义已经有所了解。

集合是由确定的、互相区别的、并作整体识别的一些对象组成的总体。通常用{…}表示一个集合，其中…是集合中的对象，对象间用逗号分开。

确切地说这不是集合的定义，因为“总体”只是“集合”一词的同义反复。实际上，集合是一个未作定义的原始概念(就像几何学中的点、线、面等概念一样)。不过，上述关于集合概念的描述，有益于对它的内涵和外延作直观的理解和认识。

例 0.1

(1) “北京大学全体学生”为一集合，组成这一集合的对象是北京大学的学生。

(2) “全体正整数”为一集合，其组成对象是正整数。

(3) “本书中所有汉字”的集合，其组成对象是本书中的不同汉字。

(4) “获1921年诺贝尔物理学奖的科学家”构成一个集合，尽管它只有一个对象——爱因斯坦。

(5)“上海市市东中学所有班级”的集合,其组成对象是班级,而不是学生,因为集合中对象是整体识别的,尽管班级又是学生的集合。

(6)“好书的全体”不构成集合,因为难以对每一本书的好或不好作出确定的判断。

(7)“方程 $x(x^2-2x+1)=0$ 的所有根”组成一个集合,它只有一个对象 0 和一个(而不是两个)对象 1,因为集合中对象是相互区别的。

(8)“方程 $x^2+x+1=0$ 的根”在确定未知数 x 可取值的范围后组成一个集合。x 可取值范围是实数域时,该集合不含任何对象,是一个空的集合(一个人们特别指定的集合)。x 可取值范围是复数域时,该集合由两个对象组成。

(9)“坐标满足方程 $x^2+y^2=1$ 的平面直角坐标系中的点”组成一个集合。

(10)“满足方程 $x^2+y^2=1$ 的平面直角坐标系中的点的坐标”组成一个集合。

组成集合的对象称为集合的**成员**或**元素**(members)。

请注意,这里“对象”的概念是相当普遍的,可以是具体的客体也可以是抽象的客体;可以是单一的客体也可以是客体的序列(例如,点的坐标$<a,b>$为二元序列,又称序偶)、矩阵;甚至还可以又是集合,因为人们有时以集合为其讨论的对象,而又需涉及它们的一个总体——以集合为其元素的集合。例如,例 0.1(5)的集合,以班级集体为其元素;又如集合$\{1,\{1,2\},\{1\},2\}$,数 1,2 是它的成员,集合$\{1\}$和$\{1,2\}$也是它的成员。因此,尽管集合与其成员是两个截然不同的概念,但一个集合完全可以成为另一个集合的元素。因此必须注意,a 不同于$\{a\}$,前者为一对象 a,后者为仅含该对象 a 的单元素集合;同样,$\{a\}$不同于$\{\{a\}\}$,$\{\{a\}\}$是仅含$\{a\}$的单元素集。

人们还把所有成员均为集合的集合称作**集合族**(collections of sets)。

通常用大写拉丁字母 A,B,C 等表示集合,用小写字母 a,b,c 等表示集合中的元素。但是,由上可知,这种表示形式不是绝对的。a 作为 A 的元素时,并不排斥 a 作为集合的可能性。同样,集合 A 也可能是别的集合的元素。

当对象 a 是集合 A 的成员时,称 a **属于** A,记为

$$a\in A$$

当对象 a 不是集合 A 的成员时,称 a 不属于 A,记为

$$a\notin A$$

“$\in$”是对象与集合之间的基本关系。依据集合对象的确定性,对任何对象 a 和任何集合 A,或者 $a\in A$ 或者 $a\notin A$,两者必居其一,也只居其一。

集合理论约定,对任何对象、集合 A,$A\notin A$。它被称为**正规原理**(regularity principle)。

0.1.2 命题与谓词

命题(propositions)是另一个十分常用的基本概念。读者对此也许已非常熟悉,但对这一概念的重要性不会有任何异议。

逻辑学把“对确定事物作出判断的陈述句”称作**命题**,当判断正确或符合客观实际时,称该命题**真**(true),否则称该命题**假**(false)。“真、假”常被称为命题的**真值**。古典逻辑认为,命题或真、

或假，但不能兼而有之，这就是逻辑学的一个基本假设——排中律(我们也遵循此假设)。真值“真、假”常用数字“1,0”来表示。

例 0.2 考虑下列语句：

(1) 雪是白的。

(2) 2+2=5。

(3) 陈胜、吴广起义的那天杭州下雨。

(4) 第 30 届奥林匹克运动会开幕时伦敦天晴。

(5) 大于 2 的偶数均可分解为两个质数的和(哥德巴赫猜想)。

(6) 火星上有生物。

(7) 好痛快啊！

(8) 您身体好吗？

(9) 我说的这句话(例 0.2 之(9))假。

(10) $x\leqslant 0$。

显然(1),(2)都是命题，(1)为真命题，取真值 1，(2)为假命题，取真值 0。事实上(3),(4),(5),(6)也是命题，虽然它们的真值未必在现在或将来可以得知，但它们所作判断是否符合客观实际这一点被认为是确定的。

(7),(8)不是陈述句，因此它们都不是命题。

由于(9)对本身的真假作了否定的判断，从而对(9)真值的判定变得没有意义。当判定(9)真时，(9)对本身的判断成立，即(9)假；当判定(9)假时，(9)对本身的判断则不成立，即(9)真。它是一个悖论，一种病态的语句。我们约定悖论不是命题。

通常用小写拉丁字母 p,q,r 等表示命题，f 表示恒假的命题，t 表示恒真的命题。

(10)不是命题，因为习惯上 x 表示变元，它不是确定的对象，从而(10)没有确定的真值。只有当 x 取得确定的值时，(10)才成为命题，才有相应的真值。

$x\leqslant 0$ 虽然不是命题，但它是关于 x 的性质的一个判断，逻辑上称之为关于 x 的**断言**。事实上，还有关于多个对象间关系的断言，例如，$x^2+y^2=1$、$x+y=z$。

不难发现，一个断言常常涉及若干对象以及它们的性质或关系，前者是断言的“主语”，后者是断言的“谓语”。因此，逻辑学把断言中关于对象基本性质或相互关系的语言成分称为**谓词**。谓词通常用带有空位的大写拉丁字母(或字母串)来表示。例如，用 $P(\ )$ 表示“…小于等于零”，$QR(,)$ 表示“…与…的平方和等于 1”，$ADD(,,)$ 表示“…与…的和等于…”。为了增加可读性，数学家更愿意用变元去填满空位。例如，$P(x)$，$QR(x,y)$，$ADD(x,y,z)$ 分别读作“x 满足性质 P”，“x,y 满足关系 QR”，“x,y,z 满足关系 ADD”。含有 n 个空位(或变元)的谓词，称为 n **元谓词**。当谓词的空位或变元处填以确定的对象后，便可判别其真假，即可得到一个命题。

例 0.3

用一元谓词 $R(x)$ 表示性质“x 是实数”时，$R(3)$是一个真命题。

用二元谓词 $L(x,y)$ 表示关系“x 小于 y”时，$L(3,2)$是一个假命题。

用二元谓词 $B(x,y)$ 表示关系“x 生于 y”时，B(董青，青岛)表示命题“董青生于青岛”，其真假显然是确定的。

用三元谓词 $ADD(x,y,z)$表示关系“$x+y=z$”时，$ADD(3,5,8)$表示“$3+5=8$”，它是一个真命题。

一般地，n 元谓词 $P(x_1,\cdots,x_n)$填满对象后的表达式 $P(t_1,\cdots,t_n)$常称为**谓词填式**，表示对象序列 $t_1,\cdots,t_n$满足 n 元谓词 $P(x_1,\cdots,x_n)$，或对象序列 $t_1,\cdots,t_n$具有性质 P、或关系 P。

上文介绍的谓词，如 $P(x)$，$QR(x,y)$，$ADD(x,y,z)$都是所谓前置表示形式，即把谓词符号放在空位的前部。有些大家熟知的对象间的关系，把关系符号放在空位的中部，例如，$x\leqslant y$，$u\subseteq v$。其实它们也是谓词，只是使用中置形式来表示罢了。

0.1.3 集合的表示

集合的表示方式主要有以下三种：列举法、描述法和归纳法。

1. **列举法**：表示一个集合 A 时，可将 A 中元素一一列举在一个大括号中，或列出足够多的元素以反映 A 中成员的特征，其表示形如

$$A=\{a_1,a_2,\cdots,a_n\}\text{或 }A=\{a_1,a_2,a_3,\cdots\}$$

2. **描述法**：表示一个集合 A 时，将 A 中元素的特征性用一个谓词来描述，其表示形式如

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

$$B=\{<x_1,x_2,\cdots,x_n>\mid Q(x_1,x_2,\cdots,x_n)\}\quad\text{或}\quad B=\{<x_1,x_2,\cdots,x_n>:Q(x_1,x_2,\cdots,x_n)\}$$

其中$<x_1,x_2,\cdots,x_n>$表示 n 个对象的序列 $x_1,\cdots,x_n$。

上述 $P(x)$是一元谓词，表示“x 满足性质 P”或“x 具有性质 P”。$A=\{x\mid P(x)\}$的意义是：集合 A 由且仅由满足性质 P 的那些对象组成，也就是

$$a\in A\Leftrightarrow P(a)\text{真}\quad(a\text{ 满足性质 }P)$$

(符号⇔表示“当且仅当”，“if and only if”，下同。)

上述 $Q(x_1,\cdots,x_n)$是 n 元谓词，表示“有序对象组 $x_1,\cdots,x_n$满足关系 Q”或“$x_1,\cdots,x_n$具有关系 Q”。若用序列$<x_1,\cdots,x_n>$表示有序对象组，则 $B=\{<x_1,x_2,\cdots,x_n>\mid Q(x_1,x_2,\cdots,x_n)\}$的意义是：集合 B 由且仅由具有关系 Q 的那些序列组成，也就是

$$<a_1,\cdots,a_n>\in B\Leftrightarrow Q(a_1,\cdots,a_n)\text{真}\quad(a_1,\cdots,a_n\text{满足关系 }Q)$$

有时，对象的性质或关系需要用若干个谓词的联列来表示，在随后几章里我们将对此进行深入介绍。

集合理论约定，每一个谓词确定一个集合。它被称为**概括原理**。

例 0.4 以下是常常要用到的一些集合以及它们的表示。

(1) $\{0,1\}=\{x\mid TV(x)\}$，$TV(x)$表示“x 是真值”。

(2) 自然数集合 $\mathbf{N}=\{0,1,2,3,\cdots\}=\{x(NN(x)\}$，其中 $NN(x)$表示“x 是自然数”。

正整数集合 $\mathbf{I}_+=\{1,2,3,\cdots\}=\{x\mid IN(x)\}$，其中 $IN(x)$表示“x 是正整数”。

(3) 整数集合 $\mathbf{I}=\{\cdots,-2,-1,0,1,2,\cdots\}=\{x\mid INTEG(x)\}$，$INTEG(x)$表示“$x$ 是整数”。

(4) 前 n 个自然数的集合 $\mathbf{N}_n=\{0,1,2,\cdots,n-1\}=\{x\mid NN(x)且\ x<n\}$，这里用到了两个谓词，要求它们同时被满足。

(5) 前 n 个自然数集合的集合$=\{\{0\},\{0,1\},\{0,1,2\},\cdots\}$

$$=\{\mathbf{N}_n\mid n\in\mathbf{I}_+\}$$

如上所见，有些常用的集合习惯用特定字母符号来表示。如：**N** 表示所有自然数组成的集合，**I** 表示所有整数组成的集合，$\mathbf{N}_n$ 表示前 n 个自然数的集合等。常见的还有，**Q** 表示所有有理数组成的集合，**R** 表示所有实数组成的集合，**C** 表示所有复数组成的集合，$\mathbf{Q}_+$ 表示所有正有理数组成的集合，$\mathbf{R}_-$ 表示所有负实数组成的集合，等等。

关于集合的下列概念无疑是十分基础的。

定义 0.1 没有任何元素的特定集合称为**空集**，记为$\varnothing$，即$\varnothing=\{\}=\{x\mid P(x)恒假\}$；由研究对象全体组成的集合称为**全集**，记为 $U=\{x\mid P(x)恒真\}$。

定义 0.2 空集和只含有有限多个元素的集合称为**有限集**(finite sets)，否则称为**无限集**(infinite sets)。有限集合中成员的个数称为集合的**基数**(cardinal number)(无限集合的成员个数，即无限集合的基数概念将在以后严格定义)。集合 A 的基数表示为$|A|$。

例 0.5 在例 0.4 中(1)(4)是有限集，其他为无限集。$|\{0,1\}|=2$，$|\mathbf{N}_n|=n$，$|\varnothing|=0$，$|\{\varnothing\}|=1$。

3. **归纳法**：集合的归纳法表示(也称**归纳定义** induction definition)就是用以下三个条款来确定集合。

(1) **基础条款**：规定待定义集合以某些对象为其成员，集合的其他元素可以从它们出发逐步确定。

(2) **归纳条款**：规定由已确定的集合成员去进一步确定其他成员的规则。于是，可以从基础条款确认的成员出发，反复运用这些规则来确认待定义集合的所有成员。

(3) **终极条款**：规定待定义集合只含有(1)，(2)条款所确定的成员。

条款(1)，(2)又称归纳表示或归纳定义的完备性条款，它们必须保证毫无遗漏地产生出待定义集合的全部成员；条款(3)又称归纳定义的纯粹性条款，它保证整个定义过程所规定的集合只包括满足要求的那些对象。

例 0.6 用归纳定义规定偶数集 E：

(1) 基础条款：$0\in E$。

(2) 归纳条款：若 $x\in E$，则 $x+2\in E$，$x-2\in E$。

(3) 终极条款：除有限次使用(1)，(2)条款确定的元素外，E 中没有别的对象。

计算机科学中，许多关于形式语言(人工定义的语言，例如程序设计语言)的概念及形式语言本身，都是归纳定义的。

通常把一个非空的符号集合称为**字母表**，常用Σ表示之，Σ上的字(即**符号串**)的概念可如下归纳定义。用Σ^+表示Σ上的字的集合。

(1) 基础条款：$\Sigma\subseteq\Sigma^+$。

(2) 归纳条款:若 $\xi\in\Sigma, w\in\Sigma^+$ 则 $\xi w\in\Sigma^+$。(这里 ξw 表示字符号 ξ 与字符串 w 的并置,或毗连,即自然连接。)

(3) 终极条款:除有限次使用(1),(2)条款确定的元素外,Σ^+ 中没有别的对象。

如果用 λ 表示**空字**(即空符号串,对任何字 w,$\lambda w=w\lambda=w$),令 $\Sigma^+\cup\{\lambda\}=\Sigma^*$。当然也可以用归纳定义来直接表示 Σ^*。

如果 $L\subseteq\Sigma^*$,那么符号串集合 L 称为 Σ 上的一个**形式语言**(formal languages)。

例 0.7 设 Σ 为数字集 $D=\{0,1,2,\cdots,9\}$,那么 $\Sigma^+=D^+$ 可看作全体自然数的集合。当 $\Sigma=\{a,b\}$ 时,$\Sigma^*=\{\lambda, a, b, aa, ab, ba, bb,\cdots\}$。$L=\{\lambda, ab, aabb, aaabbb,\cdots\}\subseteq\Sigma^*$,$L$ 为 Σ 上的一个语言(请读者用归纳定义直接表示之)。

字头、字尾的概念也是形式语言中常用的。它们也可以归纳地定义。先定义字 w 的字头的概念:

(1) 基础条款:λ 是 w 的字头。

(2) 归纳条款:若 w' 为 w 的字头,$w=w'\xi w''$(其中 $\xi\in\Sigma$, $w', w''\in\Sigma^*$),那么 $w'\xi$ 也是 w 的字头。

(3) 终极条款(略)。

当 w' 为 w 的字头,$w=w'w''$,则称 w'' 为 w 的字尾。对字尾也可以直接作归纳定义。

最后一个例子说明归纳定义在计算机科学中的应用。

例 0.8 假定我们已经规定了"变元集"、"算术表达式集"、"条件语句集",现归纳定义"while 程序集",记为 WP。

(1) 基础条款:$V\leftarrow E$ 在 WP 中,其中 V 为变元,E 为算术表达式。

(2) 归纳条款:

(2.1) 若 C 为条件语句,P1,P2 为 while 程序,则 `if C then P1 else P2 end if` 在 WP 中。

(2.2) 若 C 为条件语句,P 为 while 程序,则 `while C do P end while` 在 WP 中。

(2.3) 若 P1,P2 为 while 程序,则 P1,P2 在 WP 中。

(3) 终极条款(略)。

0.1.4 外延性原理与子集合

除了正规原理和概括原理,集合理论的另一个重要约定是外延性原理,用于规定集合相等的意义,是描述集合本质的核心原理。

外延性原理(extensionality principle):集合 A 和集合 B 相等,当且仅当它们具有相同的元素。也就是说,对任意集合 A,B,$A=B$ 当且仅当属于 A 的元素也属于 B;反之,属于 B 的元素也属于 A。

例 0.9 根据外延性原理,

$$\{0,1\}=\{1,0\}=\{x \mid x(x^2-2x+1)=0\}=\{x\mid x=1 \text{ 或 } x=0\}$$

因此,外延性原理事实上也确认了集合成员的"相异性"、"无序性",以及集合表示形式的多

样性。

定义 0.3 集合 A 称为集合 B 的**子集合**(或子集,subsets),如果 A 的每一个元素都是 B 的元素,即,若元素 x 属于 A,那么 x 也属于 B。

A 是 B 的子集,表示为 $A\subseteq B$(或 $B\supseteq A$),读作"A 包含于 B"(或"B 包含 A")。A 不是 B 的子集用 $A\not\subseteq B$ 来表示。

集合之间的子集关系或包含关系是集合之间最重要的关系之一。读者必须十分清楚集合之间的子集关系和元素与集合之间的隶属关系,这是两个完全不同的概念。

例 0.10 $\{a,b\}\subseteq\{a,c,b,d\}$,$\{a,b,c\}\subseteq\{a,b,c\}$,$\{a\}\subseteq\{a,b\}$,但 $a\not\subset\{a,b\}$,只有 $a\in\{a,b\}$。注意,存在这样两个集合,其中一个既是另一个的子集、又是它的元素。例如,$\{1\}\in\{1,\{1\}\}$,且 $\{1\}\subseteq\{1,\{1\}\}$。

关于子集关系我们有以下定理和定义。

定理 0.1 对任意集合 A,B,$A=B$ 当且仅当 $A\subseteq B$ 且 $B\subseteq A$。特别地,对任意集合 A,$A\subseteq A$。

证 由外延性原理和子集定义立即可得。

定理 0.2 对任意集合 A,$A\subseteq U$。

此定理显然成立。

定理 0.3 设 A,B,C 为任意集合,若 $A\subseteq B$,$B\subseteq C$,则 $A\subseteq C$。

证 设 x 为 A 中任一元素. 由于 $A\subseteq B$,因此 $x\in B$;又因为 $B\subseteq C$,故 $x\in C$。这就是说,A 中的所有元素都是 C 的元素,故 $A\subseteq C$。

定理 0.4 对任何集合 A,$\varnothing\subseteq A$。

证 假设 $\varnothing\not\subset A$,即 $\varnothing$ 不是集合 A 的子集,于是至少有一元素 $x\in\varnothing$,但 $x\notin A$,而 $x\in\varnothing$ 与 $\varnothing$ 的定义矛盾,因此 $\varnothing\subseteq A$。

定理 0.5 空集是唯一的。

证 设有任意空集 $\varnothing_1$,$\varnothing_2$。据定理 0.4,应有 $\varnothing_1\subseteq\varnothing_2$ 和 $\varnothing_2\subseteq\varnothing_1$,从而由定理 0.1 知 $\varnothing_1=\varnothing_2$。

定义 0.4 如果 $A\subseteq B$ 且 $A\neq B$,那么,集合 A 称为集合 B 的**真子集**。"A 是 B 的真子集"记为 $A\subset B$。

显然,空集 $\varnothing$ 是所有非空集合的真子集。

0.1.5 运算

无论是初等数学,还是高等数学,在讨论某些对象的集合时,我们常常会涉及该集合中对象之间的运算。例如,中小学的加法、乘法、减法、除法,大学的多项式乘法、矩阵转置运算,等等。让我们简单回顾这些所谓运算的基本概念和常见性质。

定义 0.5 分别称 Δ,$*$ 为集合 A 上的一元、二元**运算**(operating),如果 Δ,$*$ 分别是对单元素和序偶的操作,并且对任意 $x,y\in A$,其操作结果,记为 $\Delta(x)$,$x*y$,是集合 A 中唯一确定的元素。

这一定义告诉我们，运算是一种“确定的”、“封闭的”操作，即操作结果是唯一的，并且仍然在原来的集合中。如果从初等数学中函数的概念出发来看问题，运算只是特定的函数。

读者在以往的学习中对运算的一些性质已经有不少的经验了。

定义 0.6 设 $*$，$*'$为集合 A 上的二元运算，

(1) 如果对 A 中的任意元素 x,y,z 有 $x*(y*z)=(x*y)*z$，那么称 $*$ 运算满足**结合律**；

(2) 如果对 A 中的任意元素 x,y,z 有 $x*y=y*x$，那么称 $*$ 运算满足**交换律**；

(3) 如果对 A 中的任意元素 x,y,z 有 $x*(y*'z)=(x*y)*'(x*z)$，那么称 $*$ 运算对 $*'$ 运算满足**分配律**。

例 0.11 我们知道，求相反数运算是实数集合上的一元运算，加运算、乘运算是实数集合上的二元运算。实数和多项式的加运算、乘运算都满足结合律和交换律；乘运算对加运算都满足分配律。但矩阵乘法只满足结合律，并不满足交换律。

注意，按照定义 0.5，除法不是实数集合上的运算。尽管如此，并不曾影响初等数学对除法的讨论，人们只是将它的应用范围加以限制，不允许零作除数；或者在零作除数时作出特别的规定，例如约定 $x\div 0=0$。除法更不是整数集合上的运算，但人们适当改变其定义后，也可成为十分有意义的运算，在下一节中我们便会用到它，而第 4 章将详细讨论这种被称为“取整除”的运算。

定义 0.7 设 $*$ 为集合 A 上的二元运算，如果 $e\in A$，且对任意元素 $x\in A$ 有 $x*e=e*x=x$，那么，称元素 e 为集合 A 的关于运算 $*$ 的**幺元**(identity elements)。

定义 0.8 设 $*$ 为集合 A 上的二元运算，如果 $o\in A$，且对任意 $x\in A$ 有 $x*o=o*x=o$，那么，称元素 o 为集合 A 的关于运算 $*$ 的**零元**(zero elements)。

例 0.12 0 是实数集合上关于加运算的幺元、关于乘运算的零元；1 是实数集合上关于乘运算的幺元。零矩阵是关于矩阵加法的幺元、关于矩阵乘法的零元；单位矩阵是关于矩阵乘法的幺元。

注意，某元素是否是所在集合的幺元或零元，不仅取决于所在的集合，还取决于所关注的运算。

定理 0.6 设 $*$ 为集合 A 上的二元运算，那么集合 A 的关于运算 $*$ 的幺元是唯一的。

证 设 A 有关于运算 $*$ 的幺元 e_1,e_2，那么

$$e_1=e_1*e_2=e_2$$

故幺元是唯一的。

定理 0.7 设 $*$ 为集合 A 上的二元运算，那么集合 A 的关于运算 $*$ 的零元是唯一的。

请读者自行证明之。

定义 0.9 设 $*$ 为集合 A 上的二元运算，e 为幺元，x,y 为 A 中元素，若 $x*y=y*x=e$，那么称 $x(y)$ 为 $y(x)$ 的**逆元**(inverse elements)。x 的逆元通常记为 x^{-1}。

例 0.13 我们知道，非零实数集合上，1 是乘法的幺元，因此，每个非零实数 x 都有自己的乘法逆元 x^{-1}。实数集合上，0 是加法的幺元，因此，每个实数 x 都有自己的加法逆元 $-x$(注意，这