高等院校计算机专业教育改革推荐教材

计算机科学中的离散结构

王元元　张桂芸　编著

机械工业出版社
CHINA MACHINE PRESS

ISBN 7-111-12939-3/TP · 2896（课）

◎策划 胡毓坚
◎封面设计 旭洲企划 刘吉维

高等院校计算机专业教育改革推荐教材

基础知识模块
- 计算机电路与电子技术基础
- 信号系统与数字信号处理
- 计算机科学中的离散结构
- 计算机基础教程
- 数据结构与算法
- 操作系统简明教程
- 编译方法
- 计算机硬件技术基础
- 计算机网络技术
- 计算机专业英语

程序设计模块
- Windows 编程技术
- 新编 C 语言程序设计
- Visual Basic 6.0 程序设计
- 面向对象的程序设计与 Java 语言
- 面向对象程序设计基础
- 计算机网络程序设计
- 分布式对象技术

应用技术模块
- 数据库应用技术基础
- 计算机图形学
- 多媒体技术及其应用
- 因特网技术及其应用
- 人机交互教程
- 人工智能技术及其应用

软件工程模块
- 软件工程方法与实践
- ROSE 对象建模方法与技术
- 统一建模语言 UML 导论

实践模块
- 计算机网络实验教程
- 新编 C 语言学习指导与习题
- 面向对象的程序设计语言 C++ 实验教程
- 计算机硬件技术基础实验教程
- 信号系统与数字信号处理学习指导与实践

ISBN 7-111-12939-3
9 787111 129394 >

定价：28.00 元

地址：北京市百万庄大街22号 邮政编码：100037
联系电话：(010) 68326294 网址：http://www.cmpbook.com
E-mail:online@cmpbook.com

高等院校计算机专业教育改革推荐教材

计算机科学中的离散结构

王元元　张桂芸　编著

机械工业出版社

本书是按照教育部离散数学教学大纲，参考 ACM & IEEE CC2001 和 CCC2002（中国计算机科学与技术学科教程）的教改要求编写的。本书涵盖了经典的“离散结构”或“离散数学”课程的主要内容，包括集合论基础、逻辑代数、形式系统与形式推理、组合论基础、图论基础、关系与函数、计算理论基础和抽象代数学基础。具有内容系统全面、阐述浅显易懂、编排合理新颖、使用灵活方便的特点。

本书可用作高等院校计算机科学与技术专业及计算机软件学院本科生、专科生的离散数学课程的教材，以及毕业生考研复习用书；也可作为计算机教育工作者、相关专业技术人员的参考读物。

图书在版编目（CIP）数据

计算机科学中的离散结构/王元元，张桂芸编著.
—北京：机械工业出版社，2004.1
高等院校计算机专业教育改革推荐教材
ISBN 7-111-12939-3

Ⅰ. 计… Ⅱ. ①王…②张… Ⅲ. 离散数学—高等学校—教材 Ⅳ. 0158

中国版本图书馆 CIP 数据核字（2003）第 073748 号

机械工业出版社（北京市百万庄大街 22 号 邮政编码 100037）
策　　划：胡毓坚
责任编辑：时　静
责任印制：闫　焱

北京中加印刷有限公司印刷·新华书店北京发行所发行

2004 年 1 月第 1 版·第 1 次印刷
787mm×1092mm 1/16·19.75 印张·488 千字
0001—5000 册
定价：28.00 元

高等院校计算机专业教育改革推荐教材
编委会成员名单

编者的话

计算机科学技术日新月异的飞速发展和计算机科学技术专业教育的相对滞后，已是不争的事实。

有两个发人深省的现象：一是，由于非计算机专业的学生既具有一门非计算机专业的专业知识，又具有越来越高的计算机应用技术水平，从而使计算机专业的学生感受到一种强烈的冲击和压力；二是，创建软件学院的工作已有近两年的历史，但软件学院的计算机专业教育的定位仍在探讨之中。

我们认为计算机科学与技术专业（以下简称计算机专业）教育的改革势在必行，正确认识和划分计算机专业教育的层次，对该专业的教育改革无疑是一个非常重要的问题。我国的计算机专业教育主要分三个层次。一般说来，这三个层次通常分布在以下三类高等院校：

第一层次主要以具有计算机一级学科博士学位授予权的教育部属重点高等院校为代表（包括具有两个博士点的大学）。这一类大学本科着重培养理论基础比较坚实、技术掌握熟练、有一定研究和开发能力的计算机专业学科型人才，其中部分学生（约占本科生的10%）可攻读博士学位。

第二层次主要以具有一个计算机二级学科专业博士点的教育部属高等院校为代表。这一类高等院校本科着重培养有一定的理论基础、技术掌握比较熟练、有一定的研究或开发能力的计算机专业人才，其中一部分培养成学科型人才，另一部分培养成应用型人才，一小部分学生（约占本科生的5%）可攻读博士学位。

第三层次主要以具有计算机二级学科专业硕士点的省属高等院校为代表。这一类高等院校本科面向企业应用，侧重培养对计算机技术或部分计算机技术掌握比较熟练，有一定的开发、应用能力的计算机专业应用型人才，其中很小一部分学生（约占本科生的2.5%）可攻读博士学位。

国家教育部、计委批准的或省教育厅批准的示范性软件学院，就其培养目标和办学特色而言，分别与第二层次中应用型人才培养部分以及第三层次比较接近，但在如下方面有所不同：将软件工程课程作为专业教学重点，更加强调英语教学，更加重视实践能力培养，并对两者有更高的要求。

我们本着对高等院校的计算机专业状况的认识，主要面向与上述第二、第三两个层次对应的院校及与之相近的软件学院，总结多年的计算机专业的教改经验，在一定程度上融入了ACM& IEEE CC2001 和 CCC2002（中国计算机科学与技术学科教程）的教改思路，组织我国一直投身于计算机教学和科研的教师，编写了这套“高等院校计算机专业教育改革推荐教材”（以下简称“推荐教材”）。自然，“推荐教材”中所贯穿的改革思路和做法，也是针对上述第二、第三两个层次对应院校的计算机专业学生。这些思路和做法可概括成以下三句话：

- 适度调整电子技术基础、计算机理论基础和系统软件的教学内容。
- 全面强化计算机工具软件、应用软件的教学要求。
- 以应用为目标大力展开软件工程的教学与实践。

电子技术基础、计算机理论基础、系统软件教学关系到学生的基本素质、发展潜力和日后的应变能力。“推荐教材”在调整它们的教学内容时的做法是：适度压缩电子线路、数字

电路和信号系统的教学内容，变三门课程为两门，并插入数字信号处理的基础内容；合并“计算机组成原理”、“微型计算机接口技术”和“汇编语言”为“计算机硬件技术基础”一门课程；注意适当放宽“离散数学”课程的知识面，使之与 CCC2002 的要求基本接轨，但适度降低其深度要求；更新系统软件课程的教学内容，以开放代码的 Linux 作为操作系统原理的讲授载体，更加关注系统软件的实践性和实用性。

为了提高计算机专业人才的计算机应用能力，全面强化计算机工具软件、实用软件的教学要求是十分重要的，这也是上述改革思路的核心。为此，“系列教材”的做法是：强化程序设计技术，强化人机接口技术，强化网络应用技术。

为强化程序设计技术，“推荐教材”支持在单片机环境、微机平台、网络平台的编程训练；支持运用程序设计语言、程序设计工具以及分布式对象技术的编程训练。大大加强面向对象程序设计课程的组合（设计了三门课程：面向对象的程序设计语言 C++，面向对象的程序设计语言 Java 和分布式对象技术），方便教师和读者的选择。

为强化人机接口技术，“推荐教材”设计了“人机交互教程”，“计算机图形学”和“多媒体应用技术”等可供选择的、有层次特色的课程组合。

为强化网络应用技术，“推荐教材”设计了“计算机网络技术”，“计算机网络程序设计”，“计算机网络实验教程”和“因特网技术及其应用”等可供选择的、新颖丰富的课程组合。

将软件工程课程作为专业教学重点，以应用为目标大力展开软件工程的教学与实践，是“推荐教材”改革思路的又一亮点。为改变以往软件工程课程纸上谈兵的老毛病，“推荐教材”从工程应用出发，理论联系实际，突出建模语言及其实现工具的运用，设计了“软件工程的方法与实践”，“统一建模语言 UML 导论”和“ROSE 对象建模方法与技术”等可供选择的、创新独特的软件工程课程组合。对于各类软件学院，“推荐教材”的这一特色无疑是很有吸引力的。

强调实践也是计算机学科永恒的主题，对计算机应用专业的学生来说更是如此。重应用和重实践是“推荐教材”的一个整体特点。这一特点，一方面有利于解决本文开始所指出的计算机专业学生较之非计算机专业学生，在应用开发工作中上手慢的问题；另一方面，使计算机专业的学生能在更大范围内、更高层面上掌握计算机应用技术。这一特点正是许多高等院校计算机专业教育改革追求的一个目标，也是国家教育部倡导软件学院的初衷之一。

“推荐教材”由基础知识、程序设计、应用技术、软件工程和实践环节等五个模块组成。各模块有其对应的培养目标与功能，从而构架出一个创新的、完整的计算机应用专业的课程体系。模块化的设计，使各学校可根据学生及学校的特点做自由的选择和组合，既能达到本专业的总体要求，又能体现具有特色的个性发展。整套教材的改革脉络清晰，结构特色鲜明，值得各高等院校在改革教学内容、编制教学计划、挑选教材书目时借鉴和参考。当然，很多书目也适合很多相关学科的计算机课程用作教材。

“推荐教材”的组成模块和书目详见封底。显然它不能说是完备的（实践环节模块更是如此），其改革的思路、改革的举措也可能有值得探讨的地方。我们衷心希望得到计算机教育界同仁和广大读者的批评指正。

高等院校计算机专业教育改革推荐教材

编委会

前　言

“离散”与“连续”是数量关系中一对极为深刻的矛盾，它们之间的对立与统一是数学发展的重要原动力之一。“离散”是“连续”的否定，即“不连续”；而“连续”则是指事物、数量的一种属性，这种属性使它们容易被分割或结合，并且不会因分割或结合而丧失它们原有的本性。例如，实数是连续的，整数则是离散的；二次函数是连续的，二次函数值的计算则是离散的。

“离散结构”的研究对象是：离散数量关系以及离散系统结构的数学模型及建模方法。因而，讲授“离散结构”的课程又常称为“离散数学”

作为“离散数学”课程教材的《计算机科学中的离散结构》，其内容无疑应当包括两个方面的基础理论知识，这就是：研究计算机这一离散结构本身的数学模型及数学方法，以及研究计算机应用对象的离散结构的数学模型及建模方法。本教材由以下几个主要部分组成：

一、离散结构的研究中所需的基本数学知识：集合论基础和两个常用数学基本原理（第1、2两章）。

二、研究计算机离散结构本身的数学模型及数学方法。

1．作为计算机运算基础的逻辑代数（第3、4两章）。

2．作为计算机表示基础的形式化、形式系统技术（第5章）。

3．作为计算机科学中的“力学”，讨论计算机计算能力的计算理论（第12章）。

三、研究计算机应用对象的离散结构的数学模型及建模方法。

1．离散结构的计数模型及递归关系模型（第6、7两章）。

2．离散结构的图模型（第8、9两章）。

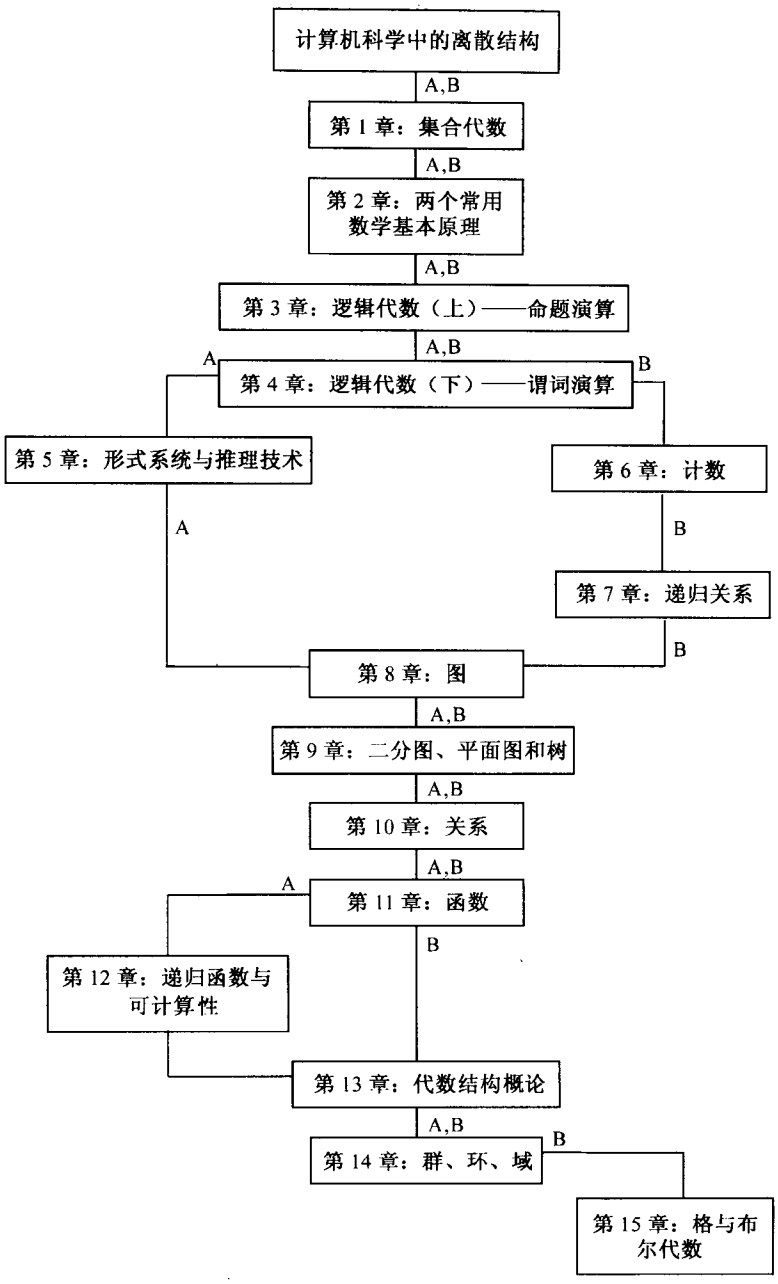
3．离散结构的一般关系模型及函数模型（第10、11两章）。

4．离散结构的抽象代数模型（第13、14、15三章）。

不难看出《计算机科学中的离散结构》完全覆盖了经典的“离散结构”或“离散数学”课程的主要内容，是一本适用于高等院校计算机科学与技术专业本科生、专科生，以及计算机软件学院本科生的“离散数学”课程的、充满改革气息的全新教材。

众所周知“离散数学”课程是计算机科学与技术专业的核心基础课程，IEEE&ACM 的 CC2001 教程以及 CCC2002（中国计算机科学与技术学科教程）更是以十分显著的方式强调了这一点。《计算机科学中的离散结构》的内容正是按照国家教委离散数学教学大纲，参考 CC2001 教程和 CCC2002 教程的教改要求进行选材和编排的。

由于离散数学课程所涉及的概念、方法和理论，大量地应用在计算机科学与技术专业的专业基础和专业课程中；它所提供的训练，十分有益于学生抽象概括能力、逻辑思维能力、归纳构造能力的提高，十分有益于学生严谨、规范、理论联系实际的科学态度的培养。因此，为加强计算机科学与技术的基础理论教学，适度拓宽离散数学课程的教学内容是可取的。在这一点上，《计算机科学中的离散结构》是一本很值得读者选择的教材，因其具有内容系统全面、阐述浅显易懂、编排合理新颖、使用灵活方便的特点。不准备讲授全部内容的教师，还可以根据本校的具体情况，按照以下两个思路来筛选素材（参见下图）：



一、希望注重计算机科学理论基础知识教学的，可选用 A 线路，即选择第 1 章、第 2 章、第 3 章、第 4 章、第 5 章、第 8 章、第 9 章、第 10 章、第 11 章、第 12 章、第 13 章、第 14 章依次讲授。

二、希望强调计算机应用技术基础知识教学的，可选用 B 线路，即选择第 1 章、第 2 章、第 3 章、第 4 章、第 6 章、第 7 章、第 8 章、第 9 章、第 10 章、第 11 章、第 13 章、第 14 章、第 15 章依次讲授。

《计算机科学中的离散结构》包含了大约可在 120 个学时内讲授的内容；如果选用 A

线路或选用 B 线路实施教学，那么可以在 80～100 学时内完成教学计划。如果全部或部分删除标记*的内容，那么完成教学计划的时数可控制在 60～70 学时。全书每一节的末尾编排了丰富的习题，难度也有一定的层次。

由于作者水平所限，书中疏漏、错误之处在所难免，敬请读者批评指正。

作　者

目　录

第1章 集合代数

集合理论是一门研究数学基础的学科，它试图从一个比“数”更简单的概念——集合（sets）出发，定义数及其运算，进而发展到整个数学。集合理论产生于 16 世纪末。当时，只是由于微积分学的需要，人们仅对数集进行了研究。19 世纪末，即 1876～1883 年间，康托尔（Georg Cantor 1845～1918 年，德国数学家）对任意元素的集合进行了系统的研究。康托尔被公认为集合理论的创始人。

人们称康托尔开创的集合理论为朴素集合论，因为他没有对集合论作完全公理化的描述，从而导致了理论的不一致（产生了悖论）。为弥补朴素集合理论的不足，本世纪初出现了各种公理化集合论体系，为数学奠定了一个良好的基础。更有意义的是，从此集合基本概念不断深入人心，被广泛地应用于数学理论和其他学科的基础研究和实际应用中，集合论的原理和方法成为名副其实的数学基本技术。基于本书的教学目的，本章主要讨论集合基本概念和集合运算，它与第 2 章一起，被视为全书学习所必备的最基本的数学知识和工具，在以后讨论的内容中将不断地运用它们。本章将不涉及公理化集合论体系。

事实上，集合不仅可用来表示数及其运算，更可以用于非数值信息及离散结构的表示和处理。像数据的删节、插入、排序，数据间关系的描述，数据的组织和查询都很难用传统的数值计算来处理，但可以用集合运算来实现。集合论被广泛应用在计算机科学中，如数据结构、操作系统、数据库、知识库、编译原理、形式语言、程序设计、人工智能、信息检索、计算机辅助设计等，这也是本章学习集合理论基础知识的目的。

1.1 集合的概念与表示

1.1.1 集合及其元素

在中学的数学课程中,大家对集合及其元素的意义已经有所了解，下面我们做些简要的回顾。

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。

严格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，在集合论中，集合是一个不作定义的原始概念（就像几何学中的点、线、面等概念）。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 1-1】

（1）“北洋大学全体学生”为一集合，组成这一集合的对象是北洋大学的学生。

（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，其组成对象是本书的汉字。

（4）“获 1988 年诺贝尔文学奖的作家”构成一个集合，尽管它只有一个对象——埃及作家纳吉布•马夫兹。“获 2002 年诺贝尔生理学或医学奖的科学家”构成一个集合，它包括英

国科学家悉尼·布雷内，美国科学家罗伯特·霍维茨，英国科学家约翰·苏尔斯顿三名成员。

（5）“解放军理工大学所有学员队”的集合，其组成对象是学员队，而不是学员，因为集合中的对象是整体识别的，尽管学员队又是学员的集合。

（6）“好书的全体”不构成集合，因为难以对每一本书的好坏作出确定的判断。

（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”组成一个集合。当在复数域上讨论时，它由两个对象组成；而当在实数域上讨论时，它不含有任何对象，是一个特定集合。

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，可以是任何具体的或抽象的客体，也可以还是集合，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 1-1（5）中的集合，以学员队集体为其元素；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，$\{a\}\neq\{\{a\}\}$，$\{\{a\}\}$是仅含$\{a\}$的单元素集。

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。

元素对于集合的隶属关系是集合理论的另一基本概念。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

$$a\notin A$$

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。这正是集合论对其元素的“确定性”要求。

1.1.2 集合的表示

集合的表示方式主要有以下三种：

（1）列举法：表示一个集合 A 时，将 A 中元素一一列举，或列出足够多的元素以反映 A 中成员的特征，其表示形式如

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

（2）描述法：表示一个集合 A 时，将 A 中元素的特征用一个性质来描述，其表示形式如

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

其中 $P(x)$表示“x 满足性质 P”或“x 具有性质 P”。$A=\{x\mid P(x)\}$ 或 $A=\{x:\ P(x)\}$ 的意义是：集合 A 由且仅由满足性质 P 的那些对象所组成，也就是说 $a\in A$ 当且仅当 a 满足性质 P（或 $P(a)$真）。

例 1-1 中的集合都是采用这种方式表示的。

（3）归纳法：将在 1.3 节中详细介绍。

【例 1-2】 以下是常常要用到的一些集合以及它们的表示。

（1）$\{0, 1\}=\{x \mid x=0 \text{ 或 } x=1\}$

（2）自然数集合 $N=\{0, 1, 2, 3, \cdots\}=\{x \mid x \text{ 是自然数}\}$

正整数集合 $I^{+}=\{1, 2, 3, \cdots\}=\{x \mid x \text{ 是正整数}\}$

（注意，这里我们所说的自然数集合与中学课本定义的自然数集合略有不同，它使自然数集合有别于正整数集合，自然数集合包括数 0，这是计算机科学的一个通常做法。）

（3）整数集合 $I=\{\cdots, -2, -1, 0, 1, 2, \cdots\}=\{x \mid x \text{ 是正整数，或零，或负整数}\}$

（4）偶整数集合 $E=\{\cdots, -4, -2, 0, 2, 4, \cdots\}=\{x \mid x \text{ 是偶数}\}$

$$=\{x \mid x \in I \text{ 且 } 2 \mid x\} \quad (2 \mid x \text{ 表示 2 整除 } x)$$

（5）前 n 个自然数的集合 $N_{\mathrm{n}}=\{0, 1, 2, \cdots, n-1\}$

$$=\{x \mid x \in N \text{ 且 } 0 \leqslant x<n\}$$

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

$$=\{x \mid x=N_{\mathrm{n}} \text{ 且 } n \in I^{+}\}$$

$$=\{N_n \mid \mathrm{n} \in I^{+}\}$$

定义 1-1 没有任何元素的特定集合称为**空集**，记为∅，即$\varnothing=\{\}=\{x \mid P(x)$恒假$\}$；由全体对象组成的集合称为**全集**，记为 U，即 $U=\{x \mid P(x)$恒真$\}$。

定义 1-2 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**（cardinatity）（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 1-3】 例 1-2 中（1）、（5）是有限集，其他为无限集。$|\{0, 1\}|=2$，$|\varnothing|=0$，$|\{\varnothing\}|=1$。故∅不同于$\{\varnothing\}$，前者是没有任何元素的集合，后者是恰含一个元素——空集的单元素集。

有些常用的集合通常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（或 Z）表示所有整数组成的集合，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，$Q+$ 表示所有正有理数组成的集合，$R-$ 表示所有负实数组成的集合，N_{n}表示前 n 个自然数的集合。

1.1.3 外延性公理与子集合

外延性公理是用于规定集合相等意义的重要约定。

外延性公理（extensionality axiom）：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，集合 A，B 满足 $A=B$，当且仅当对任意元素 x，x 属于 A 蕴涵 x 属于 B；反之，x 属于 B 蕴涵 x 也属于 A。

【例 1-4】 根据外延性公理有

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

因此，外延性公理事实上也确认了集合成员的“相异性”、“无序性”，及集合表示形式的多样性。

定义 1-3 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 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 $A\not\subset B$ 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。读者必须彻底弄清集合之间的子集关系和元素与集合之间的隶属关系这两个完全不同的概念。

【例 1-5】 $\{a, b\}\subseteq\{a, c, b, d\}$，$\{a, b, c\}\subseteq\{a, b, c\}$，$\{a\}\subseteq\{a, b\}$，但 $a\not\subset\{a, b\}$，只有 $a\in\{a, b\}$。不过存在这样两个集合，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 1-1 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，$A\subseteq A$。

证明 由外延性公理和子集定义立即可得。

定理 1-2 对任意集合 A，$A\subseteq U$。

此定理显然成立。

定理 1-3 设 A，B，C 为任意集合，若 $A\subseteq B$，$B\subseteq C$，则 $A\subseteq C$。

证明 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 的所有元素都是 C 的成员，故 $A\subseteq C$。

定理 1-4 对任何集合 A，$\varnothing\subseteq A$。

证明 假设$\varnothing\not\subset A$，即$\varnothing$不是集合 A 的子集，于是有元素 $x\in\varnothing$，但 $x\notin A$，而 $x\in\varnothing$与$\varnothing$是空集矛盾，因此$\varnothing\subseteq A$。

定理 1-5 空集是惟一的。

证明 设有空集$\varnothing_1$，$\varnothing_2$，据定理 1-4，应有$\varnothing_1\subseteq\varnothing_2$和$\varnothing_2\subseteq\varnothing_1$，从而由定理 1-1 知$\varnothing_1=\varnothing_2$。

定理 1-6 设 A 为一有限集合，$|A|=n$，那么 A 的子集个数为 2^n。

证明 集合 A 的子集有：没有元素的子集$\varnothing$，计 C_n^0 个（$C_n^0=1$）；恰含 A 中一个元素的子集计 C_n^1 个，恰含 A 中两个元素的子集计 C_n^2 个，…，恰含 A 中 n 个元素的子集计 C_n^n 个。因此 A 的子集个数为

$$C_n^0+C_n^1+\cdots+C_n^n=2^n$$

设集合 $A=\{1, \varnothing, \{1, 3\}\}$，则 A 有 $2^3=8$ 个子集，分别为：$\varnothing$，$\{1\}$，$\{\varnothing\}$，$\{\{1, 3\}\}$，$\{1, \varnothing\}$，$\{1, \{1, 3\}\}$，$\{\varnothing, \{1, 3\}\}$，$\{1, \varnothing, \{1, 3\}\}$。

定义 1-4 集合 A 称为集合 B 的**真子集**，如 $A\subseteq B$ 且 $A\neq B$。“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。

1.2 集合运算

集合运算指以集合为运算对象、以集合为值的运算。

本书中的符号“$\Leftrightarrow$”表示术语“当且仅当”（if and only if）。

1.2.1 并、交、差、补运算

并、交、差、补运算是集合最基本的运算。

定义 1-5 设 A，B 为任意集合。

（1）$A \cup B$ 称为 A 与 B 的**并集**（union set），定义为

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

$\cup$ 称为**并运算**。

（2）$A \cap B$ 称为 A 与 B 的**交集**（intersection set），定义为

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

$\cap$ 称为**交运算**。

（3）$A - B$ 称为 A 与 B 的**差集**（difference set），定义为

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

$-$ 称为**差运算**。

（4）$\overline{A}$ 称为 A 的**补集**（complement set），定义为

$$\overline{A} = U - A = \{x \mid x \notin A\}$$

$\overline{\ }$ 称为**补运算**，它是一元运算，是差运算的特例。

【例 1-6】 设 $U=\{0, 1, 2, 3, \cdots, 9\}$，$A=\{2, 4\}$，$B=\{4, 5, 6, 7\}$，$C=\{0, 8, 9\}$，$D=\{1, 2, 3\}$，则有

$A \cup B = \{2, 4, 5, 6, 7\}$，$A \cup B \cup C \cup D = U$

$A \cap B = \{4\}$，$A \cap C = \varnothing$

$A - B = \{2\}$，$B - A = \{5, 6, 7\}$，$A - C = \{2, 4\}$

$\overline{A} = \{0, 1, 3, 5, 6, 7, 8, 9\}$，$\overline{B} = \{0, 1, 2, 3, 8, 9\}$

定理 1-7 设 A，B，C 为任意集合，*代表运算 $\cup$ 或 $\cap$，那么

（1）$A * A = A$ （等幂律）

（2）$A * B = B * A$ （交换律）

（3）$A * (B * C) = (A * B) * C$ （结合律）

（4）$A \cup \varnothing = A$，　$A \cup U = U$

　　$A \cap \varnothing = \varnothing$，　$A \cap U = A$

（5）$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$　$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ （分配律）

（6）$A \cap (A \cup B) = A$　$A \cup (A \cap B) = A$ （吸收律）

证明 （1），（2），（3）由定义立得，（5），（6）的证明留给读者。现证（4）。

对任意 x，有

$$x \in A \cup \varnothing \Leftrightarrow x \in A \text{ 或 } x \in \varnothing$$
$$\Leftrightarrow x \in A \quad (x \in \varnothing \text{为假})$$

故 $A \cup \varnothing = A$。而

$$x \in A \cap \varnothing \Leftrightarrow x \in A \text{ 且 } x \in \varnothing$$
$$\Leftrightarrow x \in \varnothing \quad (x \in \varnothing \text{为假})$$

故 $A \cap \varnothing = \varnothing$。其余两式请读者补证。

定理 1-8 对任意集合 A，B，C 有

（1）$A - A = \varnothing$，$A - \varnothing = A$，$A - U = \varnothing$

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

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

证明 我们只证（2）中第一式，其余留给读者。

对任意 x，有

$$\begin{aligned} x\in A-(B\cup C) &\Leftrightarrow x\in A \text{ 且 } x\notin B\cup C \\ &\Leftrightarrow x\in A \text{ 且 } x\notin B \text{ 且 } x\notin C \\ &\Leftrightarrow (x\in A \text{ 且 } x\notin B) \text{且} (x\in A \text{ 且 } x\notin C) \\ &\Leftrightarrow (x\in A-B) \text{ 且} (x\in A-C) \\ &\Leftrightarrow x\in (A-B)\cap (A-C) \end{aligned}$$

故 $A-(B\cup C)=(A-B)\cap(A-C)$。

定理 1-9 对任意集合 A，B

（1）$\overline{\overline{A}}=A$，$\overline{U}=\varnothing$，$\overline{\varnothing}=U$

（2）$A\cup\overline{A}=U$，$A\cap\overline{A}=\varnothing$

（3）$\overline{A\cup B}=\overline{A}\cap\overline{B}$

$\overline{A\cap B}=\overline{A}\cup\overline{B}$

（4）$A-B=A\cap\overline{B}$

证明 （1），（2），（4）易证，现证（3）的第一式。

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

定理 1-10 对任意集合 A，B，C，D 有

（1）$A\subseteq A\cup B$

（2）$A\cap B\subseteq A$

（3）$A-B\subseteq A$

（4）$A\subseteq B$，$A-B=\varnothing$，$A\cup B=B$，$A\cap B=A$ 四命题等价。

（5）若 $A\subseteq B$，则 $\overline{B}\subseteq\overline{A}$。

证明 （1），（2），（3），（5）易证，我们仅证明（4）。

设（4）中四个命题为 P，Q，R，S，证明 $P\Rightarrow Q\Rightarrow R\Rightarrow S\Rightarrow P$（$\Rightarrow$ 表示“推出”），从而证实四命题等价。

（$P\Rightarrow Q$）：设 $A-B\neq\varnothing$，则有 $a\in A-B$，即 $a\in A$，但 $a\notin B$，这与 $A\subseteq B$ 矛盾。故 $A-B=\varnothing$。得证。

（$Q\Rightarrow R$）：为证 $A\cup B=B$，需证

1）$B\subseteq A\cup B$。但由定理 1-10 之（1），此已得证。

2）$A\cup B\subseteq B$。为此设 x 为 $A\cup B$ 中任一元素，从而 $x\in A$ 或 $x\in B$。当 $x\in B$ 时目的已达到。当 $x\in A$ 时，若 $x\notin B$，则 $x\in A-B$，此与 $A-B=\varnothing$ 矛盾。故 $x\in B$。总之，$A\cup B$ 中元素 x 必为 B 中元素，2）又得证。综合 1）、2）可知 $A\cup B=B$。

（$R\Rightarrow S$）：因 $A\cup B=B$，故

$$A\cap B=A\cap(A\cup B)=A \text{（吸收律）}$$

（$S \Rightarrow P$）：设 $A \cap B = A$。要证 $A \subseteq B$，现设 x 为 A 中任一元素。由 $A \cap B = A$，可得 $x \in A \cap B$ 从而知 $x \in B$。故 $A \subseteq B$ 得证。

定理 1-11 对任意集合 A，B，若它们满足

（1）$A \cup B = U$

（2）$A \cap B = \varnothing$

那么 $B = \overline{A}$。

证明
$$\begin{aligned} B &= B \cup \varnothing \\ &= B \cup (A \cap \overline{A}) \\ &= (B \cup A) \cap (B \cup \overline{A}) \\ &= U \cap (B \cup \overline{A}) \\ &= (A \cup \overline{A}) \cap (B \cup \overline{A}) \\ &= (A \cap B) \cup \overline{A} \\ &= \varnothing \cup \overline{A} \\ &= \overline{A} \end{aligned}$$

本定理的证明思路是利用已知等式进行推演，这种证明集合等式的方法简明，但难度有时较大。本定理还可直接用外延性公理来证，这种方法虽较繁锁，但思路清晰，易掌握。先证 $B \subseteq \overline{A}$。设 $x \in B$，由于 $A \cap B = \varnothing$，故 $x \notin A$，即 $x \in \overline{A}$，$B \subseteq \overline{A}$ 得证。再证 $\overline{A} \subseteq B$。设 $x \in \overline{A}$，则 $x \notin A$；由于 $A \cup B = U$，故必有 $x \in B$，$\overline{A} \subseteq B$ 又得证。因此 $B = \overline{A}$。

1.2.2 幂集运算和广义并、交运算

定义 1-6 对任意集合 A，$\rho(A)$ 称为 A 的**幂集**（power sets），定义为

$$\rho(A) = \{x \mid x \subseteq A\}$$

即 A 的全体子集组成的集合是 A 的幂集。

由于，$\varnothing \subseteq A$，$A \subseteq A$ 故必有 $\varnothing \in \rho(A)$，$A \in \rho(A)$。

【例 1-7】

（1）$A = \{a, b\}$ 时，$\rho(A) = \{\varnothing, \{a\}, \{b\}, \{a, b\}\}$。

（2）$A = \{0, \{1, 2\}\}$ 时，$\rho(A) = \{\varnothing, \{0\}, \{\{1, 2\}\}, \{0, \{1, 2\}\}\}$。

我们曾指出，当集合 A 的基数为 n 时，A 有 2^n 个子集，因此 $|\rho(A)| = 2^n$。

定理 1-12 设 A，B 为任意集合，$A \subseteq B$ 当且仅当 $\rho(A) \subseteq \rho(B)$。

证明 先证必要性。设 $A \subseteq B$，为证 $\rho(A) \subseteq \rho(B)$，又设 X 为 $\rho(A)$ 中任一元素，那么 $X \subseteq A$。由于 $A \subseteq B$，故 $X \subseteq B$，从而有 $X \in \rho(B)$。$\rho(A) \subseteq \rho(B)$ 得证。

再证充分性。设 $\rho(A) \subseteq \rho(B)$，反设 $A \subseteq B$ 不成立，那么至少有一元素 $a \in A$，但 $a \notin B$。考虑单元素集合 $\{a\}$，$\{a\} \in \rho(A)$，但 $\{a\} \notin \rho(B)$，与 $\rho(A) \subseteq \rho(B)$ 矛盾，$A \subseteq B$ 得证。

为了讨论广义的并、交运算，需要以下术语。

定义 1-7 若集合 C 的每个元素都是集合，则称 C 为**集合族**（collections）。若集合族 C 可表示为

$$C = \{S_d \mid d \in D\}$$

则称 D 为集合族的**标志集**（index set）。

【例 1-8】 $C = \{\{0\}, \{0, 1\}, \{0, 1, 2\}, \cdots\}$ 为一集合族，它没有标志集。若集合

族 $C=\{A_1, A_2, A_3, \cdots\}$,则 C 的标志集为正整数集 I^+；集合族 $C=\{S_{甲}, S_{乙}, S_{丙}\}$，则 C 的标志集为集合{甲，乙，丙}。

定义 1-8 设 C 为集合族，且 C 非空。

（1）$\bigcup C$ 称为 C 的**广义并**，定义为

$$\bigcup C=\{x: 有S使S\in C且x\in S\}$$

（2）$\bigcap C$ 称为 C 的**广义交**。定义为

$$\bigcap C\{x: 对所有\ S\in C\ 均有\ x\in S\}$$

（3）当集合族 $C=\{A_d \mid d\in D\}$ 时，$\bigcup C$ 和 $\bigcap C$ 可分别表示为

$$\bigcup C=\bigcup_{d\in D} A_d,\quad \bigcap C=\bigcap_{d\in D} A_d$$

当 D 为自然数集 N 时，它们又可分别表示为

$$\bigcup C=\bigcup_{d=0}^{\infty} A_d,\quad \bigcap C=\bigcap_{d=0}^{\infty} A_d$$

显然，当 $C=\{A, B\}$ 时，

$$\bigcup C=A\cup B,\quad \bigcup C=A\cap B$$

【例 1-9】

（1）当 $C=\{\{0\}, \{0, 1\}, \{0, 1, 2\}, \cdots\}$ 时，$\bigcup C=N$，$\bigcap C=\{0\}$。

（2）当 $C=\{S_1, S_2, S_3\}$ 时，

$$\bigcup C=\bigcup_{d\in\{1,2,3\}} S_d=\bigcup_{d=1}^{3} S_d=S_1\cup S_2\cup S_3$$

$$\bigcup C=\bigcap_{d\in\{1,2,3\}} S_d=\bigcap_{d=1}^{3} S_d=S_1\cap S_2\cap S_3$$

定理 1-13 对任意集合 A 和集合族 C，有

$$A\cap(\bigcup C)=\bigcup\{A\cap S: S\in C\}$$

$$A\cup(\bigcap C)=\bigcap\{A\cup S: S\in C\}$$

证明 我们只证第一式，第二式雷同。

设 x 为任一元素，

$$\begin{aligned} x\in A\cap(\bigcup C) &\Leftrightarrow x\in A并且有S\in C使得x\in S\\ &\Leftrightarrow 有S\in C使得(x\in A且x\in S)\\ &\Leftrightarrow 有S\in C使得x\in A\cap S\\ &\Leftrightarrow x\in\bigcup\{A\cap S: S\in C\} \end{aligned}$$

故 $A\cap(\bigcup C)=\bigcup\{A\cap S: S\in C\}$

定理 1-14 对任意集合 A 和集合族 C，有

$$A-(\bigcup C)=\bigcap\{A-S: S\in C\}$$

$$A-(\bigcap C)=\bigcup\{A-S: S\in C\}$$

证明 证第一式，第二式留给读者。

设 $x\in A-(\bigcup C)$，那么 $x\in A$，且对每一个 $S\in C$，$x\notin S$。于是，对每一 $S\in C$，$x\in A-S$，故 $x\in\bigcap\{A-S:S\in C\}$。反之，设 $x\in\bigcap\{A-S:S\in C\}$，则对每一 $S\in C$，均有 $x\in A-S$，从而 $x\in A$ 且对每一 $S\in C$，$x\notin S$，此即 $x\in A$ 而 $x\notin\bigcup C$，故 $x\in A-(\bigcup C)$。

两方面的证明证实 $A-(\bigcup C)=\bigcap\{A-S:S\in C\}$。

定理 1-14 的自然推论是定理 1-15。

定理 1-15 对任意集合族 C 有

$$(\bigcup C)^{-}=\bigcap\{S^{-}:S\in C\}$$

$$(\bigcap C)^{-}=\bigcup\{S^{-}:S\in C\}$$

定理 1-16 对任意集合 A, $\bigcup\rho(A)=A$。

证明 设 x 为任一元素，

$$\begin{aligned}x\in\bigcup\rho(A)&\Leftrightarrow\text{有}S\in\rho(A)\text{使得}x\in S\\&\Leftrightarrow\text{有}S\subseteq A\text{使得}x\in S\\&\Leftrightarrow x\in A\end{aligned}$$

故 $\bigcup\rho(A)=A$.

1.2.3 集合的笛卡儿积

定义 1-9 设 a,b 为任意对象，称集合$\{\{a\},\{a,b\}\}$为**二元有序组**，或**序偶**(ordered pairs)，简记为$<a,b>$。称 a 为$<a,b>$的**第一分量**，称 b 为**第二分量**。注意，第一、二分量可以相同。

***定理 1-17** 对任意序偶$<a,b>$，$<c,d>$，$<a,b>=<c,d>$当且仅当 $a=c$ 且 $b=d$。

证明 其充分性是显然的。

为证必要性，设 $<a,b>=<c,d>$，那么

$$\{\{a\},\{a,b\}\}=\{\{c\},\{c,d\}\}\tag{1-1}$$

$$\bigcup\{\{a\},\{a,b\}\}=\bigcup\{\{c\},\{c,d\}\}$$

$$\{a,b\}=\{c,d\}\tag{1-2}$$

以及

$$\bigcap\{\{a\},\{a,b\}\}=\bigcap\{\{c\},\{c,d\}\}$$

$$\{a\}=\{c\}\tag{1-3}$$

由式（1-2）和式（1-3）知 $a=c$，$b=d$。

因此，要充分注意$<a,b>$与$\{a,b\}$的区别，即当 $a\neq b$ 时，$<a,b>\neq<b,a>$，但$\{a,b\}=\{b,a\}$；$<a,a>\neq<a>$，但$\{a,a\}=\{a\}$

定义 1-10 定义 **n 元序组**$<a_1,\cdots,a_n>$：

$$<a_1,a_2>=\{\{a_1\},\{a_1,a_2\}\}$$

$$<a_1,a_2,a_3>=<<a_1,a_2>,a_3>$$

$$\vdots$$

$$<a_1,\cdots,a_n>=<<a_1,\cdots,a_{n-1}>,a_n>$$

本质上，n 元序组依然是序偶。a_i 称为 n 元序组的**第 i 分量**。

定理 1-18 对任意对象 $a_1,\cdots,a_n,b_1,\cdots,b_n$，有

$$<a_1, \cdots, a_n>=<b_1, \cdots, b_n>\text{当且仅当}\ a_1=b_1, \cdots, a_n=b_n$$

证明 略。

显然，序偶和 n 元序组都是集合，但由于它们的特殊结构，把次序赋予了有关对象，我们以后更多关心的是它们的这种“序特性”，而较少谈论定义它们的原有的集合结构细节。

定义 1-11 对任意集合 $A_1, A_2, \cdots, A_n$，$A_1\times A_2$，称为集合 A_1, A_2 的**笛卡尔积**（Cartesian product）。如下定义 $A_1\times A_2$ 和 $A_1\times A_2\times\cdots\times A_n$：

$$A_1\times A_2=\{<u, v>\mid u\in A_1, v\in A_2\}$$

而

$$A_1\times A_2\times A_3=(A_1\times A_2)\times A_3$$
$$\vdots$$
$$A_1\times A_2\times\cdots\times A_n=(A_1\times A_2\times\cdots\times A_{n-1})\times A_n$$

当 $A_1=A_2=\cdots=A_n=A$ 时，$A_1\times A_2\times\cdots\times A_n$ 简记为 A^n。

定理 1-19 对任意集合 $A_1, A_2, \cdots, A_n$，有

$$A_1\times A_2\times\cdots\times A_n=\{<<a_1, \cdots, a_{n-1}>, a_n>\mid a_1\in A_1,\cdots,a_n\in A_n\}$$

$<<a_1, \cdots, a_{n-1}\geqslant a_n>$常简记为$<a_1, \cdots, a_n>$本定理同样是易于证明的。

【例 1-10】 设 $A=\{1, 2\}$，$B=\{a, b, c\}$，$C=\{\varnothing\}$，R 为实数集，那么

（1）$A\times B=\{<1, a>, <1, b>, <1, c>, <2, a>, <2, b>, <2, c>\}$

$B\times A=\{<a, 1>, <b, 1>, <c, 1>, <a, 2>, <b, 2>, <c, 2>\}$

（2）$A\times B\times C=(A\times B)\times C=\{<1, a, \varnothing>, <1, b, \varnothing>, <1, c, \varnothing>,$
$<2, a, \varnothing>, <2, b, \varnothing>, <2, c, \varnothing>\}$

$A\times(B\times C)=\{<1, <a, \varnothing>>, <1, <b, \varnothing>>, <1, <c, \varnothing>>, <2, <a, \varnothing>>,$
$<2, <b, \varnothing>>, <2, <c, \varnothing>>\}$

（3）$A\times\varnothing=\varnothing\times A=\varnothing$

（4）$R^2=\{<u, v>\mid u, v\text{ 是实数}\}$，$R^2$ 为笛卡儿平面。显然 R^3 为三维笛卡儿空间。

我们注意到，一般地 $A\times B\neq B\times A$，$(A\times B)\times C\neq A\times(B\times C)$。此外，$\varnothing$也用来表示不含任何序组的笛卡儿积。

关于笛卡儿积有以下性质。

定理 1-20 设 A，B，C 为任意集合，*表示∪，∩或－运算，那么

$$A\times(B*C)=(A\times B)*(A\times C)$$

$$(B*C)\times A=(B\times A)*(C\times A)$$

证明 仅证明 $A\times(B\cup C)=(A\times B)\cup(A\times C)$ 和 $A\times(B-C)=(A\times B)-(A\times C)$

对任意 x，y，有

$$\begin{aligned}<x, y>\in A\times(B\cup C) &\Leftrightarrow x\in A\text{ 且 }y\in(B\cup C)\\ &\Leftrightarrow x\in A\text{ 且}(y\in B\text{ 或 }y\in C)\\ &\Leftrightarrow (x\in A\text{ 且 y}\in\text{B})\text{或}(x\in A\text{ 且 }y\in C)\\ &\Leftrightarrow <x, y>\in A\times B\text{ 或}<x, y>\in A\times C\\ &\Leftrightarrow <x, y>\in(A\times B)\cup(A\times C)\end{aligned}$$

为证第二式，设$<x, y>$为 $A\times(B-C)$中任一序偶，那么 $x\in A$，$y\in B$，$y\notin C$，从而

$<x, y>\in A\times B$，$<x, y>\notin A\times C$，即$<x, y>\in (A\times B)-(A\times C)$，$A\times(B-C)\subseteq(A\times B)-(A\times C)$得证。另一方面，设$<x, y>$为$(A\times B)-(A\times C)$中任一序偶，那么$<x, y>\in A\times B$，$<x, y>\notin A\times C$，从而 $x\in A$，$y\in B$，$y\notin C$（否则由于 $x\in A$，$<x, y>\in A\times C$），故可知 $y\in B-C$，$<x,y>\in A\times(B-C)$，于是$(A\times B)-(A\times C)\subseteq A\times(B-C)$得证。这就完成了$A\times(B-C)=(A\times B)-(A\times C)$的证明。

定理 1-21 对任意有限集合 A_1，…，A_n，有

$$|A_1\times\cdots\times A_n|=|A_1|*\cdots*|A_n| \quad \text{(其中*为数乘运算)}$$

这是十分直观的，证明省略。

***定理 1-22** 对任意非空集合 A，B，

(1) $\cup(\cup(A\times B))=A\cup B$

(2) $A\times B\subseteq\rho(\rho(A\cap B)$

证明 (1) $\cup(\cup(A\times B))$

$$=\cup(\cup\{<a,b>:a\in A\wedge b\in B\})$$

$$=\cup(\cup\{\{\{a\},\{a,b\}\}:a\in A\wedge b\in B\})$$

$$=\cup(\bigcup_{a\in A}\{\{a\}\}\cup\bigcup_{a\in A\wedge b\in B}\{\{a,b\}\})$$

$$=\cup(\{\{a\}:a\in A\}\cup\{\{a,b\}:a\in A\wedge b\in B\})$$

$$=\bigcup_{a\in A}\{a\}\cup\bigcup_{a\in A,b\in B}\{a,b\}$$

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

$$=A\cup B$$

(2) 设$<x, y>$为 $A\times B$ 中任一序偶，即 $x\in A$，$y\in B$。现需证

$$<x, y>=\{\{x\},\{x, y\}\}\in\rho(\rho(A\cup B))$$

由于$x\in A$，故 $\{x\}\in\rho(A\cup B)$；又由于$x\in A$，$y\in B$，故 $\{x, y\}\in\rho(A\cup B)$。因此，

$$\{\{x\},\{x, y\}\}\subseteq\rho(A\cup B)$$

即 $\{\{x\},\{x, y\}\}\in\rho(\rho(A\cup B))$。故$A\times B\subseteq\rho(\rho(A\cup B)$。

事实上，结论（1）、（2）对 A，B 为空集时也真。

1.3 集合归纳定义的意义

1.3.1 集合的归纳定义

我们已经提到集合有三种表示方式，其中之一是归纳定义（inductive definition）。现在介绍什么是归纳定义。

集合的归纳定义由三部分组成:

（1）基础条款：规定待定义集合以某些元素为其基本成员，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元素去进一步确定其他元素的规则。于是，可以从基本元素出发，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 1-11】 设 U 为整数集 I，现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 中没有别的元素。

许多关于形式语言（人工语言，例如计算机程序设计语言等）的概念及形式语言本身都是归纳定义的。

通常把一个非空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^+ 中没有别的元素。

如果用 λ 表示空字（即空符号串，对任何字 w，$\lambda w=w\lambda=w$），记 $\Sigma^+\cup\{\lambda\}=\Sigma^*$。当然也可以直接用归纳定义来规定 Σ^*。

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

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 w' 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。

【例 1-12】 设 Σ 为数字集 $D=\{0,1,2,\cdots,9\}$，那么 $\Sigma^+=D^+$ 可看作为全体自然数的集合。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（请读者归纳定义之）。L 之中所有字的字头中 a 的数目不少于 b 的数目，字尾中 a 的数目不多于 b 的数目。

最后一个例子说明归纳定义在计算机科学中有十分广泛的应用。

【例 1-13】 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：

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

3）若 $P1$，$P2$ 为 while 程序，则 $P1$，$P2$ 在 WP 中。

（3）终极条款（略）。

*1.3.2 集合定义的自然数

本章一开始就指出，集合论开创的初衷就是要为数学奠基,为此首先要在集合论中定义最基础的数学概念——自然数（它原本是不作定义的原始概念），即用集合来定义自然数。由于这一定义可用归纳定义的形式给出，因而正好成为一个归纳定义的生动的例子。

自然数是大家熟悉的。从本质上看，它们是满足下列特性的一列符号：

（1）它们中有一个为首的符号。

（2）每个符号都有且仅有一个直接的后继符号。

（3）为首的符号不是任何符号的直接后继符号。

（4）没有两个符号具有相同的直接后继符号。

（5）自然数仅指这列符号中的符号。

由于自然数的一切性质均可以从这五个特性推得，因此皮亚诺（Peano）用五条公理刻画自然数概念：

P1．至少有一个客体是自然数，它被记为 0。

P2．如果 n 是自然数，那么 n 必定恰有一个直接后继者，记为 n'。

P3．0 不是任何自然数的直接后继。

P4．如果自然数 m，n 的直接后继 m'，n'相同，那么 $m=n$。

P5．没有不满足上述条件的客体是自然数。

现在我们需要在集合论中，实实在在地拿出一列符号来，并使它们满足这五条公理，从而定义出自然数。

一种容易想到的定义自然数集 N 的方式是：

（1）$0\in N$。

（2）如果 $x\in N$，则 $x+1\in N$。

（3）终极条款。

但这一定义是不适当的。“0 为何物？集合否？”，“尚无自然数时，加 1 意义何在？”为了在集合论中定义自然数，首先要选择一个集合，例如∅，作为为首的自然数，并给∅起一个自然数名“0”。其次需确定一种集合运算，作为求直接后继的运算。

定义 1-12

（1）称空集∅为自然数，记为 0。

（2）称 A'为集合 A 的直接后继，如果

$$A'=A\cup\{A\}$$

【例 1-14】 $\{a,b\}'=\{a,b,\{a,b\}\}$

$$\varnothing'=\varnothing\cup\{\varnothing\}=\{\varnothing\}$$

$$\{\varnothing\}'=\{\varnothing\}\cup\{\{\varnothing\}\}=\{\varnothing,\{\varnothing\}\}$$

$$\{\varnothing,\{\varnothing\}\}'=\{\varnothing,\{\varnothing\},\{\varnothing,\{\varnothing\}\}\}$$

定义 1-13 归纳定义自然数集 N：

（1）基础条款：$\varnothing\in N$。

（2）归纳条款：如果$x\in N$，则$x'=x\cup\{x\}\in N$。

（3）终极条款（略）。

按照上述定义。自然数集N由下列元素组成：

$\varnothing$，$\{\varnothing\}$，$\{\varnothing,\{\varnothing\}\}$，$\{\varnothing,\{\varnothing\},\{\varnothing,\{\varnothing\}\}\}$，…

或

0，0′，0″，0‴，…

将它们依次表示为

0，1，2，3，…

这样定义的自然数，其表示形式是非常有趣的：

$1=\{0\}$，$2=\{0,1\}$，$3=\{0,1,2\}$，…，$n=\{0,1,2,\cdots,n-1\}$

这是因为$n=(n-1)\cup\{n-1\}$（当$n\neq 0$时）。

现在我们来证明，如上定义的自然数满足皮亚诺的5条公理。事实上只要证明它们满足P1～P4。

P1显然被满足，至少有$\varnothing$作为自然数0在N中。

为证P2，设n为一自然数。首先，n有后继$n'=n\cup\{n\}$。其次可证n'是惟一的，因为$n\cup\{n\}=\{0,1,2,\cdots,n\}$是惟一确定的集合。

为证P3，反设$\varnothing$是自然数n的后继。$n'=n\cup\{n\}$，从而$\varnothing=n\cup\{n\}$，但这是不可能的，因为右边至少有元素n。因此$\varnothing$不是任何自然数的后继。

为证P4，反设有自然数m，n，$m'=n'$，但是$m\neq n$。

由于$m'=n'$，$m\cup\{m\}=n\cup\{n\}$。因$m\neq n$，故总有元素$x\in m$，但$x\notin n$；或$x\in n$，但$x\notin m$。不妨设$x\in m$，但$x\notin n$。于是我们有$x\in m\cup\{m\}=n\cup\{n\}$，进而知$x\in n\cup\{n\}$。由于$x\notin n$，故$x\in\{n\}$，即$x=n$。这样便有$x=n\in m$。由$n\in m$可导出$m\neq n$，$m\notin n$。这与$m\cup\{m\}=n\cup\{n\}$矛盾，因为左边集合以$m$为元素，右边集合决无元素$m$。矛盾的导出表明$m=n$，P4得证。

有了自然数，便可以定义自然数集合上的运算和函数。关于这一点我们留待第11章讨论。

1.4 练习

1. 证明：如果$A\in\{\{b\}\}$，那么$b\in A$。

2. 用描述法表示下列集合：

（1）$A=\{1,3,5\}$

（2）$B=\{2,3,5,7,11,13,17,\cdots,89,97\}$

（3）$C=\{\{0\},\{1\},\{2\},\{3\},\cdots,\{9\}\}$

（4）全集U

3. 对任意对象a，b，c，d证明：

$\{\{a\},\{a,b\}\}=\{\{c\},\{c,d\}\}$当且仅当$a=c$且$b=d$

4. 指出下列集合序列的排列规律，并依此规律再写出两个后续集合：

$\varnothing$，$\{\varnothing\}$，$\{\varnothing,\{\varnothing\}\}$，$\{\varnothing,\{\varnothing\},\{\varnothing,\{\varnothing\}\}\}$，…

5. “如果$A\in B$，$B\in C$，那么$A\in C$”对任意对象A，B，C都成立吗？都不成立吗？举

例说明你的结论。

6. 确定下列各命题的真、假：

（1）$\varnothing \subseteq \varnothing$

（2）$\varnothing \in \varnothing$

（3）$\varnothing \subseteq \{\varnothing\}$

（4）$\varnothing \in \{\varnothing\}$

（5）$\{a, b\} \subseteq \{a, b, c, \{a, b, c\}\}$

（6）$\{a, b\} \in \{a, b, c, \{a, b, c\}\}$

（7）$\{a, b\} \subseteq \{\{a, b\}, \{\{a, b\}\}\}$

（8）$\{a, b\} \in \{\{a, b\}, \{\{a, b\}\}\}$

（9）对任意集合 A，B，C，若 $A \in B$，$B \subseteq C$ 则 $A \in C$。

（10）对任意集合 A，B，C，若 $A \in B$，$B \subseteq C$ 则 $A \subseteq C$。

（11）对任意集合 A，B，C，若 $A \subseteq B$，$B \in C$ 则 $A \in C$。

（12）对任意集合 A，B，C，若 $A \subseteq B$，$B \in C$ 则 $A \subseteq C$。

7. 指出下列各组集合中的集合的不同之处，列出每一集合的元素和全部子集：

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

（2）$\{a, b, c\}, \{a, \{b, c\}\}, \{\{a, b, c\}\}$

8. 设 A，B 为任意集合。证明：如果对任意的集合 C，$C \subseteq A$ 当且仅当 $C \subseteq B$，那么 $A = B$。

9. 证明定理 1-7 之（5）。

10. 证明定理 1-8 之（2）中的第二式。

11. 证明定理 1-9 之（4）。

12. 试以下列次序证明定理 1-10：

$$P \Rightarrow R \Rightarrow S \Rightarrow Q \Rightarrow P$$

13. 对任意集合 A，B，C，证明：

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

14. 对任意集合 A，B，C，证明：

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

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

（3）$(A - B) - C = A - (B - C)$ 当且仅当 $A \cap C = \varnothing$

（4）$(A - B) - C = (A - C) - (B - C)$

15. **证明** 对任意集合 A，B 下列命题等价，

（1）$A \subseteq B$

（2）$\overline{A} \cup B = U$

（3）$A \cap \overline{B} = \varnothing$

16. 设 $A = \{\varnothing\}$，$B = \{1, 2\}$，求 $\rho(\rho(\rho(A)))$，$\rho(\rho(B))$。

17. 对任意集合 A，B。求证：

（1）$A = B$ 当且仅当 $\rho(A) = \rho(B)$

（2）$\rho(A) \cap \rho(B) = \rho(A \cap B)$

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

18. 若 $C=\{\{x\}:x\in B\}$ 求 $\bigcup C$。

19. 对下列各 C，求 $\bigcup C$ 和 $\bigcap C$。

（1）$C=\{\varnothing\}$

（2）$C=\{\varnothing,\{\varnothing\}\}$

（3）$C=\{\{a\},\{b\},\{a,b\}\}$

（4）$C=\rho(\rho(N))$

20. 对任意非空集合族 $C1$，$C2$，证明：

（1）$(\bigcup C1)\cup(\bigcup C2)=\bigcup(C1\cup C2)$

（2）$(\bigcup C1)\cap(\bigcup C2)=\bigcup\{S1\cap S2:S1\in C1\text{且}S2\in C2\}$

（3）$(\bigcap C1)\cup(\bigcap C2)=\bigcap\{S1\cup S2:S1\in C1\text{且}S2\in C2\}$

（4）$(\bigcap C1)\cap(\bigcap C2)=\bigcap(C1\cup C2)$

21. 设 $A=\{1,2,3\}$，R 为实数集，请在笛卡儿平面上表示出 $A\times R$ 和 $R\times A$。

22. 以下各式是否对任意集合 A，B，C，D 均成立？试对成立的给出证明，对不成立的给出适当的反例。

（1）$(A-B)\times C=(A\times B)-(A\times C)$

（2）$(A\cap B)\times(C\cap D)=(A\times B)\cap(C\times D)$

（3）$(A-B)\times(C-D)=(A\times C)-(B\times D)$

（4）$(A\cup B)\times(C\cup D)=(A\times C)\cup(B\times D)$

23. 设 A，B，C，D 为任意集合，求证：

（1）若 $A\subseteq C,B\subseteq D$，那么 $A\times B\subseteq C\times D$。

（2）若 $C\neq\varnothing$，$A\times C\subseteq B\times C$，则 $A\subseteq B$。

（3）$(A\times B)-(C\times D)=((A-C)\times B)\cup(A\times(B-D))$

24. 归纳定义 Σ^*（$\Sigma^*=\Sigma^+\cup\{\lambda\}$），令 $\Sigma=\{a,b\}$。

25. 令 $\Sigma=\{a,b,c\}$，归纳定义：

（1）$L\subseteq\Sigma^*$，使 L 中所有字里都有字 ab 的出现，且所有含字 ab 的字全在 L 中。

（2）$L\subseteq\Sigma^*$，使 L 中所有字里都含有字符 a 和 b，且所有含字符 a，b 的字全在 L 中。

26. 归纳定义下列集合：

（1）十进制无符号整数集合，非零数不得以 0 为字头。

（2）十进制非负有穷小数。

（3）全体十进制有理数(分数)。

（4）二进制形式的非负偶数，非零数不得以 0 为字头

27. 数学表达式中允许出现的括号的嵌套和毗连所形成的括号串称为成形括号串。归纳定义成形括号串集合（假定它含有空括号串λ）。

28. 直接归纳定义形式语言中字尾的概念。

第 2 章　两个常用数学基本原理

本章和第 1 章都是今后学习的必要准备，它介绍两个最常用的数学基本原理：归纳原理和鸽笼原理。

2.1　归纳原理

归纳原理是一种重要的数学思想和证明技术，它广泛地应用在各种离散结构的数学证明中。

2.1.1　结构归纳原理

设集合 A 是归纳定义的集合，现欲证 A 中所有元素具有性质 P，即证：对任意 $x\in A$ 有 $P(x)$真。可进行如下证明：

（1）（归纳基础）证明归纳定义基础条款中规定的 A 的基本元素 x 均使 $P(x)$真。

（2）（归纳推理）证明归纳定义的归纳条款是“保性质 P 的”。即在假设归纳条款中已确定元素 $x_1,\cdots, x_n$ 使 $P(x_i)$真$(i=1,2,\cdots,n)$的前提下，证明用归纳条款中的操作 g 所生成元素 $g(x_1,\cdots, x_n)$依然有性质 P，即 $P(g(x_1,\cdots, x_n))$真。

归纳推理中的假设称为归纳假设。

由于 A 仅由（1）、（2）条款所确定的元素组成，因此当上述证明过程完成时，“A 中所有元素具有性质 P”得证。这种推理原理称为**归纳原理**，应用这一原理进行证明的方法称为**归纳法**（induction）。为区别于通常所说的“数学归纳法”，它又称为“结构归纳法”。数学归纳法是它的特例。

【例 2-1】回忆成形括号串集合（假定它含有空括号串λ）的定义（第 1 章练习之 27，为了视觉明晰，用括号[ ]代替括号（ ））

（1）（基础条款）空括号串λ是成形括号串。

（2）（归纳条款）如果 x,y 是成形括号串，那么$[x]$，xy 都是成形括号串。

（3）（终极条款）除有限次使用（1）、（2）条款确定的对象外，没有别的对象是成形括号串。

（A）证明：成形括号串中左括号数等于右括号数。

（B）证明：成形括号串的字头中，左括号数不少于右括号数。

证明（A）设 $L(x), R(x)$ 分别表示成形括号串 x 中的左、右括号数。

（1）（归纳基础）：$L(\lambda)=R(\lambda)=0$，命题成立。

（2）（归纳推理）：设 $L(x)=R(x)$，$L(y)=R(y)$，则

$$L([x])=L(x)+1=R(x)+1=R([x])，$$

$$L(xy)=L(x)+L(y)=R(x)+R(y)=R(xy)$$

因此对一切成形括号串 x，有 $L(x)=R(x)$。

（B）

（1）（归纳基础）：空成形括号串的字头的左括号数不少于右括号数显然真。

（2）（归纳推理）：设成形括号串 x，y 的字头中左括号数大于或等于右括号数，那么[x]的字头为“λ”或“[”或“[毗连 x 的字头”或“[x]”，而 x 的字头中左括号数大于或等于右括号数，因此[x]的字头，无论是“λ”或“[”或“[毗连 x 的字头”或“[x]”，其中的左括号数总大于或等于右括号数。

又 xy 的字头集合中包括 x 的字头以及 x 与 y 的字头毗连而成的字头。因为 x，y 的字头中左括号数大于或等于右括号数，而 x 中左括号数等于右括号数，因此 xy 的字头（无论是 x 的字头或 x 与 y 的字头毗连而成的字头）的左括号数也总大于或等于右括号数。

归纳完成，命题得证。

2.1.2 数学归纳原理

我们已经指出，数学归纳原理是上述结构归纳原理的特例，因为它只是在归纳定义的自然数集上进行归纳推理。读者在中学学习过的数学归纳法是数学归纳原理的最基本的形式。

数学归纳法的基本模式（第一数学归纳法）

用第一数学归纳法证明所有自然数具有性质 P 时，只要如下进行推理：

（1）归纳基础：证 $P(0)$真，即证明数 0 有性质 P。

（2）归纳过程：对任意 $k(\geq 0)$假设 $P(k)$真（归纳假设“k 满足性质 P”）时，推出 $P(k+1)$真（$k+1$ 也满足性质 P）。

（3）结论：所有自然数具有性质 P。

多米诺骨牌是数学归纳法基本模式的一个形象的释例。

【例 2-2】 用归纳法证明：对任意自然数 n 有

$$(0+1+2+\cdots+n)^2=0^3+1^3+2^3+\cdots+n^3$$

证明 （1）归纳基础：当 $n=0$ 时，$0^2=0^3$

（2）归纳过程：设当 $n=k$ 时，$(0+1+2+\cdots+k)^2=0^3+1^3+2^3+\cdots+k^3$,那么

当 $n=k+1$ 时，

$$\begin{aligned}(0+1+2+\cdots+k+k+1)^2&=0^3+1^3+2^3+\cdots+k^3+(k+1)^2+2(1+2+\cdots+k)(k+1)\\&=0^3+1^3+2^3+\cdots+k^3+(k+1)^2+k(k+1)^2\\&=0^3+1^3+2^3+\cdots+k^3+(k+1)^3\end{aligned}$$

归纳完成，命题得证。

对数学归纳法的这种基本模式，读者在中学已熟练掌握，这里不多举例了。下面仅对它的一些变形作些说明。

起始于任意自然数 n_0 的归纳证明模式

用第一数学归纳法证明所有大于或等于 n_0 的自然数具有性质 P 时，只要进行如下推理：

（1）归纳基础：证 $P(n_0)$真，即证明数 n_0 有性质 P。

（2）归纳过程：对任意 $k(\geq n_0)$假设 $P(k)$真（归纳假设“k 满足性质 P”）时，推出 $P(k+1)$真（$k+1$ 也满足性质 P）。

（3）结论：所有大于或等于 n_0 的自然数具有性质 P。

起始于多个值的归纳证明模式（例如起始于两个值，起始于更多个值的情况雷同）

用起始于 2 个值的第一数学归纳法证明所有自然数具有性质 P 时，只要如下进行推理：

（1）归纳基础：证 $P(0)$真，$P(1)$真，即证明数 0 和数 1 都有性质 P。

（2）归纳过程：对任意 $k(\geqslant 0)$假设 $P(k)$真（归纳假设“k 满足性质 P”）时，推出 $P(k+2)$真（$k+2$ 也满足性质 P）。

（3）结论：所有自然数具有性质 P。

【例 2-3】 证明用 3 分币和 5 分币可以组成 8 分以上的任何币值。

证明 对 8 分以上的币值 n 归纳。

因为 $8=3+5$，$9=3+3+3$，$10=5+5$，因此，当 n 为 8，9，10 时可用 3 分币及 5 分币组成。

设 $n=k$ 时命题真，即 k 可用 3 分币及 5 分币组成，需证 $n=k+3$ 时命题真，然而这是显然的,只要在组成 k 的 3 分币及 5 分币组合中新添一个 3 分币即可。

归纳完成，命题得证。

允许有参变数的归纳证明模式

设 $P(m,n)$为依赖自然数 m,n 的性质。为证 $P(m,n)$对一切自然数 m，n 均真时，可只对其中一个变元进行归纳，而将另一变元视为参变元。

【例 2-4】 设 f 是以自然数集为定义域的函数，满足

$$f(0,m)=m+1$$

$$f(n+1,m)=f(n,m^2)\cdot f(n,2nm)$$

求证：对任意 m，n，$f(n,m)>0$。

证明 对 n 归纳，把 m 看作参数。

当 $n=0$ 时，$f(0,m)=m+1>0$。

当 $n=k$ 时，设对任意 m 有 $f(k,m)>0$。那么，$n=k+1$ 时，

$$f(n,m)=f(k+1,m)=f(k,m^2)\cdot f(k,2km)$$

据归纳假设，$f(k,m^2)>0$，$f(k,2km)>0$，故 $f(k+1,m)>0$。

归纳完成，命题得证。

*有时待证命题虽只有一个变元，但变元所处的不同地位造成了归纳证明的困难。这时可以引人参数，“拆裂”变元进行证明。

【例 2-5】 求证：n 为不小于 3 的自然数时有 $n^{n+1}\geqslant(n+1)^n$。

在 $n=3$ 时易证，但归纳推理相当困难，因为同一变元 n 分处于底数和指数的位置，归纳假设 $k^{k+1}\geqslant(k+1)^k$ 难以利用。为此，我们将底数上 n 与指数上 n 拆裂开。即引入变元 u，去证明一个更加一般的结论：$u\geqslant n\geqslant 3$ 时有

$$nu^n\geqslant(u+1)^n \tag{2-1}$$

证明 对 n 归纳，视 u 为参数。

$n=3$ 时，u≥3，而

$$\begin{aligned}3u^3&=u^3+2uu^2\\&\geqslant u^3+6u^2\\&\geqslant u^3+3u^2+3u+1\end{aligned}$$

$$=(u+1)^3$$

因此 $n=3$ 时式（2-1）得证。

设 $n=k$ 时式（2-1）对一切 u≥3 成立，即 $ku^k \geqslant (u+1)^k$。那么 $n=k+1$ 时，

$$\begin{aligned} nu^n &= (k+1)u^{k+1} \\ &= (k+1)uu^k \\ &= (ku+u)u^k \\ &\geqslant (u+1)ku^k \qquad (\text{因 } u \geqslant n=k+1) \\ &\geqslant (u+1)(u+1)^k \qquad (\text{归纳假设 } ku^k \geqslant (u+1)^k) \\ &= (u+1)^{k+1} \end{aligned}$$

从而 $n=k+1$ 时式（2-1）亦成立。

式（2-1）由归纳法得证。在式（2-1）中令 $u=n$，即得 $n^{n+1} \geqslant (n+1)^n$。例 2-5 证毕。

强数学归纳法的证明模式（第二数学归纳法）

用第二数学归纳法证明所有自然数具有性质 P 时，只要进行如下推理：

（1）归纳基础：证 $P(0)$真，即证明数 0 有性质 P。

（2）归纳过程：对任意 $k(\geqslant 0)$假设 $P(i)$真，$k>i\geqslant 0$（归纳假设“0,1,…，k-1 均满足性质 P”）时，推出 $P(k)$真（k 也满足性质 P）。

（3）结论：所有自然数具有性质 P

【例 2-6】 有数目相等的两堆棋子(每一堆中棋子数目为 n)，甲、乙两人玩取棋子游戏。规定两人轮流取子，每次两人取子数相同，不能不取，也不能同时在两堆中取子，取得最后一枚棋子者为胜者。求证：后取者必胜。

证明 设甲为先取者。乙为后取者，对每一堆中棋子数目 n 归纳证明乙必胜。$n=1$ 时，两堆各有一枚棋子，甲必先从一堆中取走一枚，余下最后一枚必被乙取走，乙胜。

设 $n<k$ 时乙必胜。现证 $n=k$ 时乙亦必胜。

设第一轮取子时，甲从一堆中取走 r 枚棋子，余下 $k-r<k$ 枚棋子，那么，乙只要从另一堆棋子中也取走 r 枚棋子，亦留下 $k-r<k$ 枚棋子。若

（1）$r=k$，那么乙取到了最后一枚棋子，乙胜。

（2）$1<r<k$，那么 $0<k-r<k$。对留下的两堆棋子，每一堆为是 $k-r$ 枚，据归纳假设，在以后甲乙的搏奕中乙必胜，因此全局亦必是乙胜。

归纳完成，命题得证。

化归于数学归纳法的结构归纳

数学归纳法是结构归纳的特例，数学归纳法显然更易于掌握和运用。但我们要指出，许多结构归纳证明可以化归为数学归纳法，从而也变得易学易懂易表达。例如，可定义成形括号串中括号的嵌套和毗连的次数为括号串的秩，因而可对秩用数学归纳法证明例 2-1。在以后的学习中，我们会遇到这样的例子。

最后我们要强调，归纳证明的两个部分，归纳基础及归纳推理是缺一不可的，并且要注意归纳基础的充分性和归纳推理中“k”的任意性。

仅有归纳基础，没有归纳推理，即使对许多（乃至无穷多）情况已分别证明命题成立，仍不能据此作出一般化的结论。例如哥德巴赫猜想，已被大量数值验证，但仍不能称它在整个自然数集上为真。

仅有归纳推理，没有归纳基础，归纳证明也不能成立的。例如；仅作归纳推理可由 $k=k+1$（归纳假设），导出 $k+1=k+2$。从而得出 $n=n+1$ 的荒谬结论。

归纳基础的充分性是需严密关注的。

【例 2-7】 证明：对任何自然数，有 $2.5^n \geqslant n^2$。

证明 $n=0$ 时，$2.5^0=1 \geqslant 0=0^2$，故命题真。

设 $n=k$ 时命题真。现设 $n=k+1$，那么

$$2.5^{k+1}=2.5 \cdot 2.5^k > 2 \cdot 2.5^k = 2.5^k + 2.5^k \geqslant k^2 + k^2 \quad \text{（归纳假设）}$$

$$* \geqslant k^2 + 2k + 1 = (k+1)^2$$

归纳似已完成，但仔细的读者会发现，*标记的步骤是有疑问的，因为 $k^2 \geqslant 2k+1$ 只是在 $k \geqslant 3$ 时才成立，因而归纳基础只对 $n=0$ 进行是不充分的。因此，应对 $n=0$，$n=1$，$n=2$，$n=3$ 分别证明（作为归纳基础）后再进行上述归纳推理才对。（请读者补证）

归纳推理中，假定 $P(k)$真而证明 $P(k+1)$成立的过程中，k 必须是“任意的”。例 2-7 中，我们也是先考虑到 $k^2 \geqslant 2k+1$ 并非对任意 k 成立，才察觉归纳基础的不充分。下面的例子更好地说明了这一点。

【例 2-8】 下列命题和证明是错误的：

命题：任意 n 条直线必重合于同一条直线。

证明 $n=1$ 时显然命题真。

设 $n=k$ 时命题成立，即任意 k 条直线均重合于同一条直线。现考虑 $n=k+1$，即有 $k+1$ 条直线：l_1，l_2,…,l_k，l_{k+1}。据归纳假设，l_1，l_2,…，l_k，这 k 条直线必重合于同一条；l_2,…，l_k，l_{k+1} 这 k 条直线也必重合于同一条。由于这两组直线中有公共的成员，因此这两组直线事实上重合于同一条直线。归纳完成，命题证毕。

问题出在哪儿呢？出在 k 的任意性在推理中被忽略。不难看出，$k+1$（$n=2$）时，两组直线分别只含一条直线，它们不会有公共成员。

最后我们来讨论数学归纳原理的正确性。

在接受“自然数集合的任一非空子集都有最小元素”这一浅显事实的基础上，可以证明数学归纳原理的正确性。现应用反证法证明第一数学归纳法的正确性。假设我们已经完成以下推理：

（1）归纳基础：证 $P(0)$真，即证明数 0 有性质 P。

（2）归纳过程：对任意 $k(\geqslant 0)$假设 $P(k)$真（归纳假设“k 满足性质 P”）时，推出 $P(k+1)$真（$k+1$ 也满足性质 P）。

但是，并非所有自然数都有性质 P。那么不满足性质 P 的自然数组成一个自然数集合的非空子集，因而它有最小元素，设之为 k。显然 $k \neq 0$，并且 $k-1$ 一定具有性质 P，即 $P(k-1)$真，而 $P(k)$假。这是与已经证明的事实（2）矛盾的。因此，所有自然数都应有性质 P，也就是说第一数学归纳法是正确的。

2.2 鸽笼原理

鸽笼原理又名抽屉原理、狄里克雷原理（dirichlet principle），是一个十分基本、非常重

要、应用极其广泛的数学原理。它是解决数学中的一类存在性问题的基本工具，通常在组合数学中得到介绍。

可以用非常通俗的语言来表述鸽笼原理：当多于鸽笼的鸽子飞进笼子时，至少有两只鸽子进入同一个笼子。

2.2.1 鸽笼原理的基本形式

鸽笼原理基本形式一：如果把 $n+1$（n 是正整数）个对象放入 n 个盒子里，那么至少有一个盒子里放有两个或两个以上的对象。

这一原理的正确性是毋容置疑的，因为当每一个盒子中都少于两个对象时，盒子中对象的总数便不会超过 n 个，与前提相冲突。

鸽笼原理基本形式可略做加强，得出鸽笼原理形式二。

鸽笼原理基本形式二：m 只鸽子飞进 n 个笼子（m,n 是正整数），那么有一个笼子至少飞进了 $\left[\frac{m-1}{n}\right]+1$ 只鸽子。（$\left[\frac{m-1}{n}\right]$ 表示“$m-1$ 除以 n 的商的整数部分”）

证明 如果每只笼子飞进的鸽子都不多于 $\left[\frac{m-1}{n}\right]$，那么鸽子的总数将不多于 $n\cdot\left[\frac{m-1}{n}\right]$ 只，从而不多于 $m-1$ 只，与前提矛盾。

在鸽笼原理基本形式二中令 $m=n+1$，那么 $\left[\frac{m-1}{n}\right]+1=2$。这就是鸽笼原理基本形式一的结论。

一个简单的例子可以用来说明这两个形式的鸽笼原理：由 13 个人组成的集合中，至少有两个人生日的月份相同。由 60 个人组成的集合中，至少有 $\left[\frac{60-1}{12}\right]+1=5$ 个人生日的月份相同。

通过一些应用的例子来加深对这些原理的理解是再好不过的。

【例 2-9】 集合 M 由 10 个不同的十进制两位数所组成。试证明：必定存在 M 的两个不相交的非空真子集 A 和 B，使得 A 中的所有元素之和等于 B 中的所有元素之和。

证明 由于 M 共含有 10 个元素，因此 M 所有子集的总数是 $2^{10}=1024$ 个。除去空子集和 M 本身，M 的所有非空真子集的总数是 $2^{10}-2=1022$ 个。这些非空真子集的每一个都对应一个确定的数，即这一子集的所有元素的和。由于 M 由 10 个不同的十进制两位数所组成，于是这些和数中，最小的不会小于 10，最大的不会大于 $90+91+\cdots+99=945$。因此，这些和数中不同的至多有 $945-10+1=936$ 个。由于 1022 个和数只有 936 种取值可能，故必定有两个不同子集的和数相等，令它们是 $A1$，$B1$，并取 $A=A1-A1\cap B1$，$B=B1-A1\cap B1$。不难明白，A 和 B 是两个不相交的非空真子集，并且 A 中的所有元素之和等于 B 中的所有元素之和。

【例 2-10】 三维空间中有 9 个格点（各坐标均为整数的点）。证明：在所有格点的连线的中点之中，至少有一个也是格点。

证明 我们知道，格点的三个坐标的奇（用 1 表示）、偶（用 0 表示）状况只有 8 个：（0，0，

0)，(0，0，1)，(0，1，0)，(0，1，1)，(1，0，0)，(1，0，1)，(1，1，0)，(1，1，1)。因此，根据鸽笼原理基本形式一，9 个格点中至少有两个格点的坐标的奇、偶状况相同。设这两个格点的坐标是（a,b,c）和（a',b',c'），于是，它们之间连线的中点的坐标是$\left(\frac{a+a'}{2},\frac{b+b'}{2},\frac{c+c'}{2}\right)$。由于（$a,b,c$）和（$a',b',c'$）的奇、偶状况相同，$\left(\frac{a+a'}{2},\frac{b+b'}{2},\frac{c+c'}{2}\right)$中各坐标均为整数，故该点是一个格点。

【例 2-11】 从集合{1，2，…，200}中任选 101 个数。证明：无论怎样选取，在选取的这些数中，必定存在两个数，使得其中之一可以被另一个整除。

证明 我们知道，任何正整数都可以写成$2^k \cdot a$的形式，其中 k 是自然数，a 是奇数。对于集合{1，2，…，200}中的数，a 只能是 1，3，5，…，199 这 100 个数中的一个。于是，根据鸽笼原理基本形式一，在选取的 101 个数中，有两个数的上述表示形式中的 a 是相同的。即分别是$2^k \cdot a$，$2^j \cdot a$，它们之中自然有一个可以被另一个整除。

【例 2-12】 一位象棋大师用 11 周（77 天）的时间来准备一次大赛，他决定每天至少下一局棋。为了不至于太累，他又限定自己每一周下棋不多于 12 局。证明：存在连续的若干天，在这些天里，他恰好下了 21 局棋。

证明 设a_1是第一天下棋的局数，a_2是第一、第二两天下棋的局数，a_3是第一、第二、第三这三天下棋的局数，……，如此等等。由于每天至少下一局棋，因此序列a_1，a_2，a_3，…，a_{77}是严格递增的，即

$$1 \leqslant a_1 < a_2 < a_3 < \cdots < a_{77} \leqslant 12 \times 11 = 132$$

考虑序列a_1+21，a_2+21，a_3+21，…，$a_{77}+21$，应有

$$1 < a_1+21 < a_2+21 < a_3+21 < \cdots < a_{77}+21 \leqslant 132+21 = 153$$

我们注意到，a_1，a_2，a_3，…，a_{77}，a_1+21，a_2+21，a_3+21，…，$a_{77}+21$，这 154 个数分布在 1～153 这 153 个正整数当中。根据鸽笼原理基本形式一，它们中至少有两个数是相等的。又由于$i \neq j$时$a_i \neq a_j, a_i+21 \neq a_j+21$，因此有$i \neq j$使$a_i = a_j+21$。即有$i \neq j$使$a_i - a_j = 21$，这就是说，从第 $j+1$ 天到第 i 天这连续的 $i-j$ 天里，大师恰好下了 21 局棋。

【例 2-13】 取黑白围棋子 21 枚，黑白数目不限，排列成 3 行 7 列的长方形。求证：无论怎样排放，都可以从中找到一个长方形，使该长方形的四个角的棋子同色。

证明 设 21 枚棋子排成的长方形如下：

$$q_{11}, q_{12}, \cdots, q_{17}$$
$$q_{21}, q_{22}, \cdots, q_{27}$$
$$q_{31}, q_{32}, \cdots, q_{37}$$

由鸽笼原理基本形式二，$q_{11}, q_{12}, \cdots, q_{17}$中至少有$\left[\frac{7-1}{2}\right]+1=4$枚棋子同色，不妨设它们是$q_{11}, q_{12}, q_{13}, q_{14}$（黑子）。再考虑$q_{21}, q_{22}, q_{23}, q_{24}$，如果其中有两枚黑子，那么命题已成立；若不然，$q_{21}, q_{22}, q_{23}, q_{24}$中至少有三枚白子，不妨设它们是$q_{21}, q_{22}, q_{23}$。再考虑

q_{31},q_{32},q_{33}，这 3 枚棋子中必有$\left[\frac{3-1}{2}\right]+1=2$枚棋子同色，如果其中有两枚白子，那么与$q_{21},q_{22},q_{23}$中白子组成长方形白色的四角，满足命题要求；如果其中有两枚黑子，那么与$q_{11},q_{12},q_{13},q_{14}$中黑子组成长方形黑色的四角，满足命题要求。

*2.2.2 鸽笼原理的加强形式

鸽笼原理的加强形式一：如果把$q_1+q_2+\cdots+q_n-n+1$（q_i，n 是正整数）个对象放入 n 个盒子里，那么或者第一个盒子里至少有 q_1 个对象，或者第二个盒子里至少有 q_2 个对象，……，或者第 n 个盒子里至少有 q_n 个对象。

证明 如果第一个盒子里少于 q_1 个对象，并且第二个盒子里少于 q_2 个对象，……，并且第 n 个盒子里少于 q_n 个对象，那么所有盒子里的对象的总数就不会超过

$$(q_1-1)+(q_2-1)+\cdots+(q_n-1)=q_1+q_2+\cdots+q_n-n$$

这与前提相冲突。

更多使用的是如下的鸽笼原理的加强形式。

鸽笼原理的加强形式二：如果把$n(q-1)+1$个对象放入 n 个盒子里，那么至少有一个盒子里放入了 q 个或多于 q 个的对象。

只要在鸽笼原理的加强形式一中令$q_1=q_2=\cdots=q_n=q$，便可得到上述结论。

鸽笼原理的加强形式三：如果 n 个自然数$q_1,q_2,\cdots,q_n$的算术平均值

$$(q_1+q_2+\cdots+q_n)/n$$

大于（q-1），那么$q_1,q_2,\cdots,q_n$中至少有一个大于或等于 q。

由于$(q_1+q_2+\cdots+q_n)/n>q-1$，因此

$$q_1+q_2+\cdots+q_n\geqslant n(q-1)+1>n(q-1)$$

根据鸽笼原理的加强形式二，将$q_1+q_2+\cdots+q_n$分成 n 份$q_1,q_2,\cdots,q_n$，其中至少有一份大于或等于 q。

我们也通过一些例子来说明这些形式的鸽笼原理的意义和应用。

【例 2-14】 试证：$nm+1$ 个数组成的序列$a_1,a_2,\cdots,a_{nm+1}$中或者有一个长度为 $n+1$ 的递增子序列，或者有一个长度为 $m+1$ 的递减子序列。

证明 对序列$a_1,a_2,\cdots,a_{nm+1}$中的每一个a_x指定一个i_x，它表示序列中从a_x起的最长递增子序列的长度，应有 $nm+1$ 个这样的i_x。若存在$i_x\geqslant n+1$，那么命题得证。现反设它们均不大于 n。由于$\frac{nm+1}{n}>m$，据鸽笼原理的加强形式二，至少有 $m+1$ 个a_x具有相同的i_x值。现在我们来证明，具有相同i_x的 $m+1$ 个a_x组成一个递减子序列。即当a_{x1}，a_{x2}的i_{x1}，i_{x2}相等时，a_{x1}，a_{x2}随着 $x1$，$x2$ 的递增而递减。为此，反设 $x1<x2$,但$a_{x1}\leqslant a_{x2}$，那么$i_{x1}=i_{x2}+1$，这与i_{x1}，i_{x2}相等冲突。

命题得证。

【例 2-15】将两个同心圆盘 A，B 分别划分成 200 个全等的扇形。在 A 盘上任取 100 个扇形涂上红色，其余 100 个扇形涂上兰色。在 B 盘的 200 个扇形上随意地涂红色或兰色（每个扇形只涂一种颜色）。现将两盘中心对齐后叠在一起。证明：总可适当地转动 B 盘，使得两盘上具有 100 或更多对的相同颜色的扇形相互重叠在一起。

证明 我们知道将两盘中心对齐后叠在一起转动 B 盘时，可能出现的扇形对齐的局面有 200 种（每转动一个扇形出现一个局面）。考虑 B 盘的每一个扇形，它在 200 个局面中，与 A 盘上同色扇形重叠 100 次。因此，在所有 200 个局面中，两盘同色扇形重叠的总次数应当是 $100\times200=20000$；或者说在所有 200 个局面中，有 20000 对相同颜色的扇形相互重叠在一起。这 20000 对重叠扇形分布在 200 个局面里。每一个局面平均出现 $\left[\frac{20000}{200}\right]=100$ 对。根据鸽笼原理的加强形式三，必有一个局面拥有 100 或更多对的相同颜色的扇形相互重叠在一起。

2.3 练习

1. 证明：成形括号串的字尾中，右括号数不少于左括号数。
2. 用归纳法证明：当 $|A|=n$ 时，$|\rho(A)|=2^n$。
3. 设集合族 $C=\{A_1, \cdots, An\}$，用归纳法证明：

（1）$(\bigcup_{i=1}^{n} A_i)^- = \bigcap_{i=1}^{n} A_i^-$

（2）$(\bigcap_{i=1}^{n} A_i)^- = \bigcup_{i=1}^{n} A_i^-$

4. 用数学归纳法证明从 n 个不同元素中每次取出 r 个不同元素的排列数 A_n^r 为

$$A_n^r = n(n-1)(n-2)\cdots(n-r+1)$$

（提示：先用排列意义证明 $A_n^r = nA_{n-1}^{r-1}$，再进行归纳证明）。

5. 试判断 n 为何自然数时有 $2^n \geqslant n^2$，并用归纳法证明你的结论。
6. 求证：关于 x，y 的方程 $x+2y=n$ 的自然数解的组数为

$$r(n)=\frac{n+1}{2}+\frac{1+(-1)^n}{4}$$

（提示：考虑 $y=0$ 时解的组数及 $y\geqslant1$ 时解的组数。对 n 用起始于两个值的归纳）

7. 已知 e 为一常数，试确定 a，使得 $n\geqslant a$ 时有 $n!\geqslant e^n$，用归纳法证明你的结论。
8. 证明所有大于 1 的整数 n 均能用一个质数或若干个质数的积来表示。
9. 求证：对任意自然数 n，$(3+\sqrt{5})^n+(3-\sqrt{5})^n$ 能被 2^n 整除.
10. 下列证明是错误的，试指出错误所在。

求证：$\frac{n}{2}=\frac{n}{3}$ 对一切自然数均真。

证明：当 $n=0$ 时，显然 $\frac{n}{2}=\frac{n}{3}$。

设 $n<k$ 时命题成立，即 $\frac{0}{2}=\frac{0}{3}$，$\frac{1}{2}=\frac{1}{3}$，…，$\frac{k-1}{2}=\frac{k-1}{3}$。现对 $n=k$ 的情况进行证明。

这时

$$\frac{n}{2}=\frac{k}{2}=\frac{k-1}{2}+\frac{1}{2}=\frac{k-1}{3}+\frac{1}{3}\ （据归纳假设）=\frac{k}{3}=\frac{n}{3}$$

归纳完成，命题得证。

11．在接受“自然数集合的任一非空子集都有最小元素”这一事实的基础上，证明第二数学归纳法的正确性。

12．一个口袋里装有 12 个黑球和 12 个白球。问：一次至少取出多少个球时才能保证取出的球中有一个黑球和一个白球？一次至少取出多少个球时才能保证取出的球中有一对黑球？

13．（a）在边长为 2 的正方形中任取 5 个点，证明存在两个点，它们之间的距离不超过 $\sqrt{2}$。

（b）在边长为 1 的正三角形中任取 10 个点，证明存在两个点，它们之间的距离不超过 $\frac{1}{3}$。

（c）在边长为 1 的正方体内，任意给定 9 个点，证明存在两个点，它们之间的距离不超过 $\frac{\sqrt{3}}{2}$。

14．设 m 是一个取定的正整数，求证：任取 $m+1$ 个整数，其中至少有两个整数，它们的差是 m 的整数倍。

15．某个制造铁盘的工厂，由于设备和技术的原因只能将生产的盘子的重量控制在 a 克到（$a+0.1$）克之间。现在需要制成一对铁盘用于天平，它们的重量差不能超过 0.005 克。问该工厂至少要生产多少铁盘，才能保证得到一对符合要求的铁盘。

16．在 m 维空间中任意给定 n^m+1 个格点（各坐标均为整数的点，$n\geqslant 2$），求证：其中必定有两个格点 $P\ (x_1,\cdots,x_m)$，$Q\ (y_1,\cdots,y_m)$，使得点 $M\left(\frac{x_1-y_1}{n},\cdots,\frac{x_m-y_m}{n}\right)$ 也是一个格点。（提示：参考例 2-10，考虑各坐标 x 被 n 除的余数。）

17．一个学生用 37 天时间来准备考试。根据自己的经验他知道复习所需时间不会超过 60 小时，而他又希望每天至少复习一个小时。证明：不管如何安排每天的复习时数，总有连续的若干日，其间他恰好复习了 13 个小时。（提示：参考例 2-12）

18．证明在任意的六个人中，一定有三个人他们之间互相认识或互相不认识。

19．证明在加里福尼亚州（人口 2500 万）至少有 4 个人的姓前 3 个字母相同，并且他们的生日相同。

第3章　逻辑代数（上）——命题演算

逻辑学(logic)是研究人类推理过程的科学，数理逻辑（mathematical logic）则是用数学的方法来进行这一研究的一门数学学科，它的显著特征是符号化和形式化，即把逻辑学所涉及的“概念、判断、推理”用符号来表示，用公理体系（形式系统）来刻画，并基于符号形式的演算来描述推理过程的一般规律。数理逻辑又是计算机软件理论技术和硬件逻辑设计、人工智能等学科的重要理论基础。由于本书不能全面介绍数理逻辑学科，而只是介绍它的两个基础演算（命题演算和谓词演算），因此，本章和下一章被叫作**逻辑代数**。

早在 17 世纪，莱布尼兹（Leibniz）已经提出用代数的方法研究逻辑学的想法，但由于社会条件等原因，当时这一思想并未得到应有的重视。直到 19 世纪的中后期，布尔（Boole）和弗雷格（Frege）的天才工作“布尔代数”、“概念演算”，才真正翻开逻辑代数的辉煌篇章。1930 年 Godel 完全性定理的证明，使逻辑代数的基础得以完善，最终完成了数理逻辑形式系统的研究工作。数理逻辑与随后的计算理论的出现，为现代数字计算机的诞生奠定了重要的基础。近年来，现代逻辑学在计算机科学中的重要地位越来越被计算机专家所认识。著名的计算机软件设计大师戴克斯特拉（E.W.Dijkstra）曾经这样说：“我现在年纪大了，搞了这么多年软件，错误不知犯了多少，现在觉悟了。我想，假如我早年在数理逻辑上好好下点功夫的话，我就不会犯这么多的错误。不少东西逻辑学家早就说了，可我不知道。要是我能年轻 20 岁的话，就要回去学逻辑。”我国著名数理逻辑学家莫绍撰教授甚至说得更加直截了当：“事实上，程序设计或者就是数理逻辑，或者是用计算机语言书写的数理逻辑，或者是数理逻辑在计算机上的应用。”

在传统的形式逻辑中，先讨论概念，后讨论判断（即命题），最后讨论推理，这是因为由概念形成判断，由判断又形成推理。但是，这未必是一种好的次序安排。事实上，如果我们把推理作为研究的根本目标，先忽略判断的细节——概念，把判断看作不可分的整体——命题来讨论，也就是以命题演算入手，那么更便于对推理规律进行分析；而在此基础上，再引入概念的形式表示——谓词，讨论概念、关系的理论——谓词演算，把推理的研究引向更加深刻的层次，也不失为一种内容编排的选择。因此，本章先讨论命题、命题演算，第 4 章讨论谓词和谓词演算，而把两个演算的形式系统的介绍放在第 5 章。

3.1　命题与逻辑联结词

3.1.1　命题

逻辑学把“对确定的对象作出判断的陈述句”称作**命题**（propositions），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（我们也遵循此约定），这就是逻辑学的一个基本假设——排中律。非经典逻辑，如直觉主义逻辑、多值逻辑不接受排中律，本书对它们不作讨论。

【例 3-1】 考虑下列语句：

（1）雪是白的。

（2）2+2=5

（3）3 是偶数并且 4 也是偶数。

（4）陈胜、吴广起义的那天杭州下雨。

（5）第 28 届奥林匹克运动会开幕时北京天晴。

（6）大于 2 的偶数均可分解为两个质数的和（哥德巴赫猜想）。

（7）火星上有生物。

（8）好痛快啊！

（9）您去看电影吗？

（10）$x+y\leqslant 0$

（11）我只给那些不给自己刮胡子的人刮胡子。

（12）我说的这句话（例 3-1 之（12））假。

显然（1），（2），（3）都是命题，（1）为真命题，（2），（3）为假命题。事实上（4），（5），（6），（7）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是确定的。

（8），（9）不是陈述句，因此它们都不是命题。

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

（11）不是命题，因为当它成立时，将导出“我”既不能给自己刮胡子，又不能不给自己刮胡子的矛盾的结论。它是一个悖论（著名的理发师悖论）。即一种自相矛盾的病态语句，我们不承认此类语句为陈述句。

由于（12）对本身的真假作了否定的判断，从而对（12）真值的判定变得没有意义。当判定（12）真时，（12）对本身的判断成立，即（12）假；当判定（12）假时，（12）对本身的判断则不成立，即（12）真。它也是一个悖论。因此，（12）不是命题。

我们注意到，命题（1）～（7）中的（3）与其他命题不同，（3）实际上是由两个命题与一个连结词“并且”所组成的。命题（3）的真值不仅依赖于这两个组成它的命题，而且还依赖于这个连结词的意义。像这样的连结词称为**逻辑联结词**（logical connectives）或**命题联结词**。通常把不含有逻辑联结词的命题称为**原子命题**或**原子**（atoms），而把由原子命题和逻辑联结词共同组成的命题称为**复合命题**（compositive propositions）。

【例 3-2】 下列语句都是复合命题，其中带下划线的词为逻辑联结词：

（1）雪<u>不</u>是白的（并非雪是白的）。

（2）今晚我去商店<u>或者</u>去打球。

（3）他去了学校，<u>又</u>去了工厂。（用“又”表示逻辑联结词“并且”）

（4）你织布，我耕田。（用逗号表示逻辑联结词“并且”）

（5）<u>如果</u>有辆车，<u>那么</u>我去接你。

（6）偶数 a 是质数，<u>当且仅当</u> $a=2$（a 是常数）。

在命题的符号表示中，原子命题通常记为 p，q，r，s 等小写拉丁字母。f 表示恒假命题，t 表示恒真命题。

3.1.2 逻辑联结词

今后“联结词”一词均指逻辑联结词及其符号表示。逻辑代数中，重要的联结词有 5 个，它们已在例 3-2 中出现过。

否定词（negation）“并非”（not），用符号¬ 表示。设 p 表示一命题，那么¬ p 表示命题 p 的否定。p 真时¬ p 假，而 p 假时¬ p 真。¬ p 读作“并非 p”或“非 p”。今后我们用数 1 表示真值“真”，用数 0 表示真值“假”，用类似表 3-1 的所谓真值表来规定联结词的意义，描述复合命题的真值状况。表 3-1 规定了否定词¬ 的意义，表示¬ p 的真值状况。

表 3-1

p	¬ p
0	1
1	0

【例 3-3】 如果 p 表示命题“雪是白的”，那么“并非雪是白的”、“雪不是白的”应表示为¬ p，此时¬ p 为假，因为 p 为真。

当用否定词“并非”代替自然语言中的“不”时（或者反过来），应注意保持原语句的意义。例如 p 表示“整数都是自然数”时，¬ p 表示“并非整数都是自然数”或“整数不都是自然数”，而不是“整数都不是自然数”。

合取词(conjunction)“并且”（and），用符号∧表示。设 p，q 表示两命题，那么 $p\wedge q$ 表示合取 p 和 q 所得的命题，即 p 和 q 同时为真时 $p\wedge q$ 真，否则 $p\wedge q$ 为假。$p\wedge q$ 读作“p 并且 q”或“p 且 q”。合取词∧的意义和命题 $p\wedge q$ 的真值状况可由表 3-2 来刻画。

表 3-2

p	q	$p\wedge q$
0	0	0
0	1	0
1	0	0
1	1	1

【例 3-4】 如果 p 表示命题“你去了学校”q 表示命题“我去了工厂”，那么 $p\wedge q$ 表示命题“你去了学校并且我去了工厂”。$p\wedge q$ 为真，当且仅当你、我分别去了学校和工厂。

析取词（disjunction）“或”（or）用符号∨表示。设 p，q 表示两命题，那么 $p\vee q$ 表示 p 和 q 的析取，即当 p 和 q 有一为真时，$p\vee q$ 为真，只有当 p 和 q 均假时 $p\vee q$ 为假。$p\vee q$ 读作“p 或者 q”，“p 或 q”。析取词∨的意义及复合命题 $p\vee q$ 的真值状况由表 3-3 描述。

表 3-3

p	q	$p\vee q$
0	0	0
0	1	1
1	0	1
1	1	1

【例 3-5】 如果 p，q 分别表示“今晚我看书”和“今晚我去看电影”，那么 $p\vee q$ 表示“今晚我看书或者去看电影”。当我于当晚看了书，或者看了电影，或者既看了书又看了

电影时，$p \vee q$ 为真，只是在我既没看书也没看电影时 $p \vee q$ 为假。

注意，这里的“或”是可兼的，即当 p 和 q 都为真时，确认 $p \vee q$ 为真。在日常生活的某些场合下，“或”不同于上述意义。例如“人固有一死，或重于泰山，或轻于鸿毛”。其中的“或”是不可兼的，即当发现有人的死既重于泰山又轻于鸿毛时，上述论断被认为假。看来这里的“或”用 $\vee$ 表示不妥，可用表 3-4 规定的另一联结词“不可兼或” $\bar{\vee}$ 表示之。但是，像上述场合一样的许多场合下，不可兼或联结的两个命题事实上不可能同时为真，即表 3-4 的末行根本无需定义，这时用 $\vee$ 代替 $\bar{\vee}$ 就没有问题，并且能使语句的表示简化。例如“$a>0$ 或 $a=0$ 或 $a<0$”可表示为“$a>0 \vee a=0 \vee a<0$”，而不必多此一举地表示为“$a>0 \bar{\vee} a=0 \bar{\vee} a<0$”。

表 3-4

p	q	$p \bar{\vee} q$
0	0	0
0	1	1
1	0	1
1	1	0

蕴涵词（implication）“如果…，那么…”（if…then…），用符号→表示。设 p，q 表示两命题，那么 $p \to q$ 表示命题“如果 p，那么 q”。当 p 真而 q 假时，命题 $p \to q$ 为假，否则均认为 $p \to q$ 为真。$p \to q$ 中的 p 称为蕴涵前件，q 称为蕴涵后件。$p \to q$ 的读法较多，可读作“如果 p 则 q”，“p 蕴涵 q”，“p 是 q 的充分条件”，“q 是 p 的必要条件”，“q 当 p”，“p 仅当 q”等等。数学中还常把 $q \to p$，$\neg p \to \neg q$，$\neg q \to \neg p$ 分别叫做 $p \to q$ 的逆命题，否命题，逆否命题。蕴涵词→的意义及复合命题 $p \to q$ 的真值状况规定见表 3-5。

表 3-5

p	q	$p \to q$
0	0	1
0	1	1
1	0	0
1	1	1

【例 3-6】 如果用 p 表示“我有车”，q 表示“我去接你”，那么 $p \to q$ 表示命题“如果我有车，那么我去接你”。当我有车时，若我去接了你，这时诺言 $p \to q$ 真；若我没去接你，则诺言 $p \to q$ 假。当我没有车时，我无论去或不去接你均未食言，此时认定 $p \to q$ 为真是适当的。

表 3-5 规定的蕴涵词称为**实质蕴涵**(substantive implication)，因为它不要求 $p \to q$ 中的 p，q 有什么关系，只要 p，q 为命题，$p \to q$ 就有意义。例如“如果 $2+2=5$，那么雪是黑的”，就是一个有意义的命题，且据定义其值为“真”。蕴涵词的这种规定形式，在讨论数学问题和逻辑问题时是正确的、充分的、方便的。回忆定理 1-4“对任何集合 A，$\varnothing \subseteq A$”的证明：因为没有任何对象 x,$x \in \varnothing$（$x \in \varnothing$为假），故 $x \in \varnothing$蕴涵 $x \in A$ 为真，即$\varnothing \subseteq A$ 真。数学本来就是这样理解“蕴涵”一词的。

双向蕴涵词(two-way implication)“当且仅当”（if and only if），用符号↔表示之。设 p，q 为两命题，那么 $p \leftrightarrow q$ 表示命题“p 当且仅当 q”，“p 与 q 等价”，即当 p 与 q 同真值时 $p \leftrightarrow q$ 为真，否则为假。$p \leftrightarrow q$ 读作“p 双向蕴涵 q”，“p 当且仅当 q”，“p 等价于 q”。由于“当且

仅当”“等价”常在其他地方使用，因而用第一种读法更好些。

双向蕴涵词的意义及 $p\leftrightarrow q$ 的真值状况由表 3-6 给出。

表 3-6

p	q	$p\leftrightarrow q$
0	0	1
0	1	0
1	0	0
1	1	1

【例 3-7】 如果 p 表示命题“$\triangle ABC\cong\triangle A'B'C'$”，$q$ 表示命题“$\triangle ABC$ 与$\triangle A'B'C'$的三边对应相等”，那么 $p\leftrightarrow q$ 表示平面几何中的一个真命题，因为 p 真时 q 显然真，p 假时 q 亦必然假，故 p 与 q 同真值。若 q 表示命题“$\triangle ABC$ 与$\triangle A'B'C'$的三内角对应相等”，那么 $p\leftrightarrow q$ 不再是恒真的了，因 p 假时 q 未必为假。

以上介绍的是自然语言中五个最常用、最重要的联结词，还有其他联结词，有的可以直接用它们中的一个来表示，例如“也”“又”等同于“且”，“除非…，否则…”等同于“当且仅当”；有的则可以用它们中的若干个来表示，例如“不可兼或”$\overline{\vee}$，可用$\vee$，$\wedge$与$\neg$来表示，这一点是下一节要讨论的重要内容。

3.1.3 命题公式

符号化过程的最基本步骤是，用拉丁字母 p，q，r，s 等表示具体命题，用 f，t 表示两个特殊的常命题：常真命题和常假命题，p，q，r，s，f，t 统称为**命题常元**（proposition constant）。深入的讨论还需要引入**命题变元**（proposition variable）的概念，它们是以“真、假”或“1，0”为取值范围的变元，为简单计，命题变元仍用 p，q，r，s（但不使用 f，t）等表示。相同符号的不同意义，容易从上下文来区别，在未指出符号 p，q，r，s 等表示具体命题时，它们常被看作命题变元。

命题常元、变元及联结词是形式化描述命题及其推理的基本语言成分，用它们可以形式地描述更为复杂的命题。下面要引入更高一级的语言成分——命题公式。定义命题公式集合的方式是第一章介绍的归纳定义。

定义 3-1 归纳定义**命题公式**（proposition formula）：

（1）命题常元和命题变元是命题公式，也称为原子公式或原子。

（2）如果 A，B 是命题公式，那么（$\neg A$），（$A\wedge B$），（$A\vee B$），（$A\rightarrow B$），（$A\leftrightarrow B$）也是命题公式。

（3）只有有限步引用条款（1），（2）所组成的符号串是命题公式。

命题公式简称公式，常用大写拉丁字母 A，B，C 等表示。

有时会用到子公式的概念，B 称为公式 A 的**子公式**（sub formula），如果 B 是公式 A 中字母相互毗连的一部分，且 B 自身为一公式。

【例 3-8】 $(\neg(p\rightarrow(q\wedge r)))$是命题公式，但（$qp$），$p\rightarrow r$，$p_1\vee p_2\vee\cdots$均非公式。

为使公式的表示更为简练，我们作如下约定：

（1）公式最外层括号一律可省略。

（2）联结词的结合能力强弱依次为

$\neg$，($\wedge$，$\vee$)，$\rightarrow$，$\leftrightarrow$

($\wedge$，$\vee$)表示$\wedge$与$\vee$平等。

（3）结合能力平等的联结词在没有括号表示其结合状况时，采用左结合约定。

例如，$\neg p \rightarrow q \vee (r \wedge q \leftrightarrow s)$所表示的公式是

$$((\neg p) \rightarrow (q \vee ((r \wedge q) \leftrightarrow s)))$$

如果公式 A 含有命题变元 p_1，p_2，…，p_n，记为 $A(p_1,\cdots,p_n)$，并把联结词看作真值运算符，那么公式 A 可以看作是 $p_1,\cdots,p_n$ 的真值函数。对任意给定的 $p_1,\cdots,p_n$ 的一种取值状况，A 均有一个确定的真值。称每一取值状况为一个**指派**（assignments），用希腊字母α，β等表示，当 A 对取值状况α为真时，称指派α**弄真** A，或α是 A 的**弄真指派**，记为$\alpha(A)=1$；反之称指派α**弄假** A，或α是 A 的**弄假指派**，记为$\alpha(A)=0$。对一切可能的指派，公式 A 的取值状况可用表 3-7 来描述,这个表称为**真值表**（truth table）。当 $A(p_1,\cdots,p_n)$中有 k 个联结词时，公式 A 的真值表应为 2^n 行、$k+n$ 列（不计表头）。

【例 3-9】 作出公式$\neg (p \rightarrow (q \vee r))$的真值表。

表 3-7

p	q	r	$q \vee r$	$P \rightarrow (q \vee r)$	$\neg (p \rightarrow (q \vee r))$
0	0	0	0	1	0
0	0	1	1	1	0
0	1	0	1	1	0
0	1	1	1	1	0
1	0	0	0	0	1
1	0	1	1	1	0
1	1	0	1	1	0
1	1	1	1	1	0

表 3-7 即为所求。可见指派(0,0,0),(0,0,1),(0,1,0),(0,1,1) ,(1,0,1),(1,1,0)及(1,1,1)均弄假这一公式，而指派(1,0,0)弄真该公式。

3.1.4 语句的形式化

用我们已有的符号语言，可以将许多自然语言语句符号化，也称形式化。在这一小节里，我们用一些例子来说明，如何将语句形式化，以及如何理解形式化了的语句。

【例 3-10】 将下列语句形式化，并表示为命题公式：

（1）我和他既是弟兄又是同学。

可表示为 $p \wedge q$，其中

p：我和他是弟兄，q：我和他是同学。

（2）我和你之间至少有一个要去海南岛。

可表示为 $p \vee q$，其中

p：我去海南岛，q：你去海南岛。

（3）狗急跳墙。

可表示为 $p \rightarrow q$，其中

p：狗急了，q：狗跳墙。

（4）除非他来，否则我不同他谈判。

可表示为 $p \leftrightarrow q$，或$(p \rightarrow q) \wedge (\neg p \rightarrow \neg q)$，其中

p：他来，q：我与他谈判。

(有的学者认为此句应表示为：$q \rightarrow p$ 或$\neg p \rightarrow \neg q$，亦无不可。对“除非”的理解，仁者见仁，智者见智。)

（5）如果他没来见你，那么他或者是生病了，或者是不在本地。

可表示为$\neg p \rightarrow (q \vee \neg r)$，其中

p：他来见你，q：他生病，r：他在本地。

（6）如果袁翼和王虎不都是傻子，那么他们俩都不会去。

可表示为$\neg (p \wedge q) \rightarrow (\neg r \wedge \neg s)$，其中

p：袁翼是傻子，q：王虎是傻子，

r：袁翼会去，s：王虎会去。

（7）风雨无阻，我去北京。

可表示为$(p \wedge q \rightarrow r) \wedge (p \wedge \neg q \rightarrow r) \wedge (\neg p \wedge q \rightarrow r) \wedge (\neg p \wedge \neg q \rightarrow r)$，其中

p：天刮风，q：天下雨，r：我去北京。

（8）因为天下雨,所以地皮湿。

可表示为 $p \rightarrow q$，其中

p：天下雨，q：地皮湿。

从上述例子可以看出，语句形式化要注意以下几个方面：

- 要善于确定原子命题，不要把一个概念硬拆成几个概念，例如“弟兄”是一个概念，不要拆成“弟”和“兄”、“我和他是弟兄”是一个原子命题。
- 要善于识别自然语言中的联结词（有时它们被省略）。例如“风雨无阻，我去北京”一句，可理解为“不管是否刮风、是否下雨我都去北京”。
- 否定词的位置要放准确，如上例之（6）。
- 需要的括号不能省略，如上例之（7）；而可以省略的括号，在需要提高公式可读性时亦可不省略，如上例之（5），（6）。
- 语句的形式化未必是惟一的，如上例之（7），它还可以表示为

$$(p \wedge q \wedge r) \vee (p \wedge \neg q \wedge r) \vee (\neg p \wedge q \wedge r) \vee (\neg p \wedge \neg q \wedge r)$$

意指“四种情况必居其一,而每种情况下我都去北京”。它甚至可以更简单地表示为 r，意指“我去北京，不受其他任何因素的影响”。读者不久便会明白这些表示的逻辑等价性,也就是说它们实质的意义是一致的。

因果关系通常用蕴涵词来表示（如上例之（8）），这一点是有争议的，但在大多数场合下这样做都是没有问题的。

【例 3-11】 设 p 表示“α是偶数”，q 表示“α是奇数”，r 表示“α是质数”，s 表示“$\alpha=2$”，那么，可如下理解各命题公式：

（1）$p \vee q$（α是偶数或α是奇数）

（2）$p \wedge r \rightarrow s$（若α是偶质数，则$\alpha=2$）

（3）$p \rightarrow (r \rightarrow s)$（若α是偶数，那么当α是质数时，$\alpha=2$）

（4）$r \wedge \neg s \rightarrow q$（若α是不等于 2 的质数，则α为奇数）

（5）$\neg q \wedge \neg s \rightarrow \neg r$（若α不是奇数且$\alpha \neq 2$，则α不是质数）

（6）$\neg (q \vee s) \rightarrow \neg r$（若“α是奇数与$\alpha=2$之一真”不能成立，则α非质数）

（7）$r\rightarrow(q\vee s)$（若α是质数，则α是奇数与α=2之一真）

（8）$r\leftrightarrow q\vee s$（α是质数当且仅当α是奇数或α=2）

3.2 逻辑等价式和逻辑蕴涵式

由上节可知，一般命题公式的真值是随其所含有的命题变元的指派变化而变化的，但有一类特殊的命题公式，对于命题变元的任何指派，它的真值都是真，如$(p\rightarrow q)\leftrightarrow(\neg p\vee q)$。我们先来考虑这一类最重要的命题公式——重言式。

3.2.1 重言式

定义 3-2 命题公式 A 称为**重言式**（tautology），如果对 A 中命题变元的一切指派均弄真 A。因而重言式又称**永真式**。A 称为**可满足式**（satisfactable formula），如果至少有一个指派弄真 A，否则称 A 为**不可满足式**或**永假式**、**矛盾式**。

很显然，永真式是可满足式，非永真式未必是永假式，而当 A 是永真式（永假式）时，$\neg A$ 必为永假式（永真式）。

【例 3-12】 对任何公式 A，$A\vee\neg A$ 是重言式，$A\wedge\neg A$ 是矛盾式。这两个事实揭示人们通常的思维所遵循的逻辑排中律和矛盾律。对任何命题变元 p，p 与 $\neg p$ 都是可满足式。

可以用真值表来验证重言式，矛盾式和可满足式。

【例 3-13】 用真值表证明$(p\vee q)\wedge\neg p\rightarrow q$为重言式。

证明 建立待证公式的真值表（表 3-8），由表的最后一列可以看出，原式为重言式。

表 3-8

P	q	$P\vee q$	$\neg p$	$(p\vee q)\wedge\neg p$	$(p\vee q)\wedge\neg p\rightarrow q$
0	0	0	1	0	1
0	1	1	1	1	1
1	0	1	0	0	1
1	1	1	0	0	1

注意，用真值表验证重言式时，表中任何一列都不能省略，因为每一列的计算过程正是所需的证明过程。

3.2.2 重要的逻辑等价式和逻辑蕴涵式

定义 3-3 当命题公式 $A\leftrightarrow B$ 为永真式时，称 A **逻辑等价于** B，记为 $A\models\models B$，它又称为**逻辑等价式**(logically equivalent)。

因此，逻辑等价式 $A\models\models B$ 可以从两个角度去理解：

（1）$A\models\models B$ 表示断言“$A\leftrightarrow B$ 是重言式”。

（2）$A\models\models B$ 表示“A，B 等值”，或理解为“当 A 真时 B 亦真，当 A 假时 B 也假”，甚至理解为“由 A 真可推出 B 真，且由 B 真可推出 A 真”。

以下是一些重要的逻辑等价式，其中 A，B，C 表示任意命题公式：

E_1　$\neg\neg A\models\models A$　双重否定律

E_2　$A\vee A\models\models A$，$A\wedge A\models\models A$　幂等律

E_3	$A\vee B \models\!\dashv B\vee A$ ，$A\wedge B \models\!\dashv B\wedge A$	交换律
E_4	$(A\vee B)\vee C \models\!\dashv A\vee(B\vee C)$	结合律
	$(A\wedge B)\wedge C \models\!\dashv A\wedge(B\wedge C)$	结合律
E_5	$A\wedge(B\vee C) \models\!\dashv (A\wedge B)\vee(A\wedge C)$	分配律
	$A\vee(B\wedge C) \models\!\dashv (A\vee B)\wedge(A\vee C)$	
E_6	$\neg(A\vee B) \models\!\dashv \neg A\wedge\neg B$	德摩根律
	$\neg(A\wedge B) \models\!\dashv \neg A\vee\neg B$	
E_7	$A\vee(A\wedge B) \models\!\dashv A$	吸收律
	$A\wedge(A\vee B) \models\!\dashv A$	
E_8	$A\rightarrow B \models\!\dashv \neg A\vee B$	
E_9	$A\leftrightarrow B \models\!\dashv (A\rightarrow B)\wedge(B\rightarrow A)$	
E_{10}	$A\vee \mathrm{t} \models\!\dashv \mathrm{t}$，$A\wedge f \models\!\dashv f$	
E_{11}	$A\vee f \models\!\dashv A$，$A\wedge \mathrm{t} \models\!\dashv A$	
E_{12}	$A\vee\neg A \models\!\dashv \mathrm{t}$，$A\wedge\neg A \models\!\dashv f$	
E_{13}	$\neg \mathrm{t} \models\!\dashv f$，$\neg f \models\!\dashv \mathrm{t}$	
E_{14}	$A\wedge B\rightarrow C \models\!\dashv A\rightarrow(B\rightarrow C)$	
E_{15}	$A\rightarrow B \models\!\dashv \neg B\rightarrow\neg A$	
E_{16}	$(A\rightarrow B)\wedge(A\rightarrow\neg B) \models\!\dashv \neg A$	
E_{17}	$A\leftrightarrow B \models\!\dashv (A\wedge B)\vee(\neg A\wedge\neg B)$	

定义 3-4 当命题公式 $A\rightarrow B$ 为永真式时，称 A **逻辑蕴涵** B，记为 $A\models B$，它又称为**逻辑蕴涵式**（logically implication）。

同样，$A\models B$ 可作以下两种理解：

（1）$A\models B$ 表示语句“$A\rightarrow B$ 为永真式”。

（2）$A\models B$ 表示“弄真 A 的指派均弄真 B”，因而可理解为“由 A 真可推得 B 真”，或“由 B 假可推得 A 假”，但反之不然。

我们也列出一些十分重要的逻辑蕴涵式：

I_1	$A\models A\vee B$，$B\models A\vee B$
I_2	$A\wedge B\models A$，$A\wedge B\models B$
I_3	$A\wedge(A\rightarrow B)\models B$
I_4	$(A\rightarrow B)\wedge\neg B\models\neg A$
I_5	$\neg A\wedge(A\vee B)\models B$，$\neg B\wedge(A\vee B)\models A$
I_6	$(A\rightarrow B)\wedge(B\rightarrow C)\models A\rightarrow C$
I_7	$(A\rightarrow B)\wedge(C\rightarrow \mathrm{D})\models (A\wedge C)\rightarrow(B\wedge \mathrm{D})$
I_8	$(A\leftrightarrow B)\wedge(B\leftrightarrow C)\models A\leftrightarrow C$

当然，每一个逻辑等价式可看作两个逻辑蕴涵式，因为 $A \models\!\dashv B$ 指“$A\leftrightarrow B$ 永真”或“A，B 等值”，由此即知“$A\rightarrow B$ 与 $B\rightarrow A$ 均永真”，因而有 $A\models B$ 和 $B\models A$。

$A\models B$ 这一形式常被推广为 $\Gamma\models B$，其中 Γ 为公式集合，它表示：B 是 Γ 的逻辑结果，即弄真 Γ 中每一公式的指派均弄真 B。$\Gamma=\{A\}$ 时，它即表示 $A\models B$；当 Γ 为若干个公式的集合时，它可以看作是这若干个公式的合取逻辑蕴涵 B；当 $\Gamma=\varnothing$ 时，它记作 $\models B$，表示“B 永真”。

逻辑等价式与逻辑蕴涵式有如下明显性质。

定理 3-1 对任意命题公式 A，B，C，A'，B'，

（1）$A \models\!\models B$ 当且仅当 $\models A \leftrightarrow B$

（2）$A \models B$ 当且仅当 $\models A \rightarrow B$

（3）若 $A \models\!\models B$，则 $B \models\!\models A$

（4）若 $A \models\!\models B$，$B \models\!\models C$，则 $A \models\!\models C$

（5）若 $A \models B$，则 $\neg B \models \neg A$

（6）若 $A \models B$，$B \models C$，则 $A \models C$

（7）若 $A \models B$，$A \models\!\models A'$，$B \models\!\models B'$，则 $A' \models B'$

证明 由定义可立得（1），（2），（3），（4），（5），（6），（7）的证明，请读者自己完成。

定理 3-2 设 A 为永真式，p 为 A 中命题变元，$A(B/p)$表示将 A 中 p 的所有出现全部代换为公式 B 后所得的命题公式（称为 A 的一个**代入实例**），那么 $A(B/p)$亦为永真式。

这是明显的。由于 A 永真，A 的真值与 p 的取值状况无关，恒为 1，因此 $A(B/p)$的真值也恒为 1

定理 3-2 常被称为**代入原理**（rule of substitution），简记为 *RS*。

定理 3-3 设 A 为一命题公式，C 为 A 的子公式，且 $C \models\!\models D$。若将 A 中子公式 C 的某些（未必全部）出现替换为 D 后得到的公式记为 B，那么 $A \models\!\models B$。

这也是明显的。由于 C 和 D 等值，因而用 D 替换 C 不会改变 A 的真值，因此 B 与 A 等值。

定理 3-3 常被称为**替换原理**（rule of replacement）简记为 *RR*。

请注意 *RS* 与 *RR* 的区别，详见表 3-9。

表 3-9

	RS	*RR*
使用对象	任意永真式	任一命题公式
代换对象	任一命题变元	任一子公式
代换物	任一命题公式	任一与代换对象等价的命题公式
代换方式	代换同一命题变元的所有出现	代换子公式的某些出现
代换结果	仍为永真式	与原公式等价

现在我们已经有三种证明逻辑等价式及逻辑蕴涵式的方法。

（1）真值表法。为证 $A \models\!\models B$，$A \models B$，可用真值表分别证明 $A \leftrightarrow B$ 永真，$A \rightarrow B$ 永真。做法平凡，此不赘述。

（2）对指派进行讨论。为证 $A \models B$，只要证任意弄真 A 的指派都弄真 B（或证任一弄假 B 的指派均弄假 A）。为证 $A \models\!\models B$，可用此法同时证明 $A \models B$，$B \models A$。

（3）利用已知的永真式、逻辑等价式及逻辑蕴涵式和代入、替换原理进行推演。

【例 3-14】 试证对任意公式 A，B，C，有

$$(A \vee B) \rightarrow C \models\!\models (A \rightarrow C) \wedge (B \rightarrow C)$$

证明 先证$(A \vee B) \rightarrow C \models (A \rightarrow C) \wedge (B \rightarrow C)$。设$\alpha$为弄真$(A \vee B) \rightarrow C$ 的任一指派，那么

（a）$\alpha(A \vee B) = 0$。于是$\alpha(A) = \alpha(B) = 0$，从而$\alpha(A \rightarrow C) = \alpha(B \rightarrow C) = 1$，故$\alpha((A \rightarrow C) \wedge (B \rightarrow C)) = 1$。

（b）$\alpha(C)=1$，$\alpha(A\vee B)=1$。于是$\alpha(A\to C)=\alpha(B\to C)=1$，因而又有$\alpha((A\to C)\wedge(B\to C))=1$

据（a），（b）可知，α必弄真$(A\to C)\wedge(B\to C)$，因此，$(A\vee B)\to C \models (A\to C)\wedge(B\to C)$得证。

再证$(A\to C)\wedge(B\to C) \models (A\vee B)\to C$。为此设$\alpha$为弄假$(A\vee B)\to C$ 的任一指派，那么α $(A\vee B)=1$，$\alpha(C)=0$。当$\alpha(A)=1$，$\alpha(C)=0$ 时，$\alpha(A\to C)=0$，进而有$\alpha((A\to C)\wedge(B\to C))=0$；当$\alpha$ $(B)=1$，α $(C)=0$ 时，α $(B\to C)=0$，从而也有α $((A\to C)\wedge(B\to C))=0$，即$\alpha$弄假$(A\to C)\wedge(B\to C)$。于是$(A\to C)\wedge(B\to C) \models (A\vee B)\to C$ 得证。

总之，$(A\vee B)\to C \models\!\dashv (A\to C)\wedge(B\to C)$。

【例 3-15】 同例 3-14，试利用已知的永真式、逻辑等价式及逻辑蕴涵式和代入、替换原理进行推演。

证明 $(A\vee B)\to C$

$\models\!\dashv \neg(A\vee B)\vee C$　　对 E_8 用 RS

$\models\!\dashv (\neg A\wedge\neg B)\vee C$　　据 E_6 用 RR

$\models\!\dashv (\neg A\vee C)\wedge(\neg B\vee C)$　　对 E_5 用 RS

$\models\!\dashv (A\to C)\wedge(\neg B\vee C)$　　据 E_8 用 RR

$\models\!\dashv (A\to C)\wedge(B\to C)$　　据 E_8 用 RR

当然对于例 3-14，也可用真值表法来证明，请读者自行完成。

【例 3-16】 对任意公式 A，B，C，证明：

$$A\wedge B \models \neg A\to(C\to B)$$

证明 $A\wedge B \models B$　　据 I_2

$\models \neg C\vee B$　　对 I_1 用 RS

$\models C\to B$　　对 E_8 用 RS

$\models A\vee(C\to B)$　　对 I_1 用 RS

$\models \neg A\to(C\to B)$　　对 E_8 用 RS

*3.2.3 对偶原理

定义 3-5 设公式 A 仅含联结词$\neg$，$\wedge$，$\vee$，A^*为将 A 中符号$\wedge$，$\vee$，t，f 分别改换为$\vee$，$\wedge$，f，t 后所得的公式，那么称 A^*为 A 的**对偶**（dual）。

显然 A 与 A^*互为对偶，即$(A^*)^*=A$

【例 3-17】 $p\vee\neg p$ 与 $p\wedge\neg p$，$\neg p\vee q$ 与$\neg p\wedge q$，$(t\wedge p)\vee\neg q$ 与$(f\vee p)\wedge\neg q$ 均互为对偶。

下面两定理所描述的事实常称为**对偶原理**。

定理 3-4 设公式 A 中仅含命题变元 $p_1,\cdots,p_n$，及联结词$\neg$，$\wedge$，$\vee$，那么

$$A\models\!\dashv \neg A^*(\neg p_1/p_1,\ \cdots,\ \neg p_n/p_n) \tag{3-1}$$

这里，$A^*(\neg p_1/p_1,\ \cdots,\ \neg p_n/p_n)$表示在 A^*中对 p_1，$\cdots,p_n$ 分别作代入$\neg p_1$，$\cdots$，$\neg p_n$ 后所得的公式。

证明 我们用结构归纳法进行证明。

（1）（归纳基础）若 A 为原子公式，那么 A 为 p_1,p_2，$\cdots$，p_n，或t，f之一。由于

$p_i\models\!\dashv \neg\neg p_i$　（$i=1$，2，$\cdots n$）

$t\models\!\dashv \neg f\models\!\dashv \neg(t^*)$

$$f \models\!\models \neg t \models\!\models \neg (f^*)$$

因此，A 为原子公式时，式（3-1）成立。

（2）（归纳推理）当 A 为 $\neg A_1$，$A_1 \vee A_2$，$A_1 \wedge A_2$ 时，设 A_1，A_2 满足式（3-1）（归纳假设）。

（2.1）若 A 为 $\neg A_1$，那么

$$A \models\!\models \neg A_1 \models\!\models \neg (\neg A_1^* (\neg p_1 / p_1, \cdots, \neg p_n / p_n)) \quad \text{（归纳假设）}$$
$$\models\!\models \neg ((\neg A_1)^* (\neg p_1 / p_1, \cdots, \neg p_n / p_n))$$
$$\models\!\models \neg A^* (\neg p_1 / p_1, \cdots, \neg p_n / p_n)$$

（2.2）若 A 为 $A_1 \vee A_2$，那么

$$A \models\!\models A_1 \vee A_2 \models\!\models \neg A_1^* (\neg p_1 / p_1, \cdots, \neg p_n / p_n) \vee \neg A_2^* (\neg p_1 / p_1, \cdots, \neg p_n / p_n)$$
（归纳假设）
$$\models\!\models \neg (A_1^* (\neg p_1 / p_1, \cdots, \neg p_n / p_n) \wedge A_2^* (\neg p_1 / p_1, \cdots, \neg p_n / p_n))$$
$$\models\!\models \neg (A_1^* \wedge A_2^*)(\neg p_1 / p_1, \cdots, \neg p_n / p_n)$$
$$\models\!\models \neg (A_1 \vee A_2)^* (\neg p_1 / p_1, \cdots, \neg p_n / p_n)$$
$$\models\!\models \neg A^* (\neg p_1 / p_1, \cdots, \neg p_n / p_n)$$

（2.3）若 A 为 $A_1 \wedge A_2$，证明与（2.2）相仿，省略。

归纳完成，定理得证。

定理 3-5 设 A，B 为仅含联结词 $\neg$，$\wedge$，$\vee$ 和命题变元 $p_1, \cdots, p_n$ 的命题公式，且满足 $A \vdash B$，那么有 $B^* \vdash A^*$。进而当 $A \models\!\models B$ 时有 $A^* \models\!\models B^*$。常把 $B^* \vdash A^*$，$A^* \models\!\models B^*$ 称为 $A \vdash B$ 和 $A \models\!\models B$ 的**对偶式**。

证明 据定理 3-4 及题设 $A \vdash B$ 可知

$$\neg A^*(\neg p_1/p_1, \cdots, \neg p_n/p_n) \vdash \neg B^*(\neg p_1/p_1, \cdots, \neg p_n/p_n)$$

从而

$$B^*(\neg p_1/p_1, \cdots, \neg p_n/p_n) \vdash A^*(\neg p_1/p_1, \cdots, \neg p_n/p_n)$$

又据代入原理，有

$$B^*(\neg p_1/p_1, \cdots, \neg p_n/p_n)(\neg p_1/p_1, \cdots, \neg p_n/p_n)$$
$$\vdash A^*(\neg p_1/p_1, \cdots, \neg p_n/p_n)(\neg p_1/p_1, \cdots, \neg p_n/p_n)$$

即

$$B^*(\neg\neg p_1/p_1, \cdots, \neg\neg p_n/p_n) \vdash A^*(\neg\neg p_1/p_1, \cdots, \neg\neg p_n/p_n)$$

据 E_1 及替换原理即得 $B^* \vdash A^*$。

用对偶原理，可以从已知的永真式作出新的永真式，从已知的逻辑蕴涵式、逻辑等价式作出新的逻辑蕴涵式、逻辑等价式。

【例 3-18】 $A \vdash A \vee B$ 与 $A \wedge B \vdash A$，$A \vee (B \wedge C) \models\!\models (A \vee B) \wedge (A \vee C)$ 与 $A \wedge (B \vee C) \models\!\models (A \wedge B) \vee (A \wedge C)$ 互为对偶式。

当已知 $(p \wedge q) \vee (\neg p \vee (\neg p \vee q)) \models\!\models \neg p \vee q$ 时，可推得 $(p \vee q) \wedge (\neg p \wedge (\neg p \wedge q)) \models\!\models \neg p \wedge q$。

3.3 范式

我们已经知道，对众多的命题公式，可以依据它们之间的逻辑等价关系进行分类，使相

互逻辑等价的公式为一类。现在的问题是，是否可以在各类公式中分别选出一个公式作为各类的“代表”，而且使它们具有统一的规范形式呢？回答是肯定的。

3.3.1 析取范式和合取范式

在讨论范式以前，我们先介绍一些术语。

文字(letters)：指命题常元、变元及它们的否定，前者又称正文字，后者则称负文字。

析取子句(disjunctive clauses)：指文字或若干文字的析取。例如，p，$p\vee\neg q$，$\neg p\vee\neg q\vee r$。

合取子句(conjunctive clauses)：指文字或若干文字的合取。例如，$\neg p$，$\neg p\wedge\neg q$，$p\wedge\neg q\wedge r$。

互补文字对(complemental pairs of letters)：指形如 L，$\neg$ L（L 为文字）的一对字符。

很显然，析取子句恒真当且仅当子句中含有互补文字对；合取子句恒假当且仅当子句中含有互补文字对。

定义 3-6 命题公式 A' 称为公式 A 的**析取范式**（disjunctive normal form），如果

（1）$A' \models\!\models A$

（2）A' 为一合取子句或若干合取子句的析取。

【例 3-19】 $p\rightarrow q$ 的析取范式为$\neg p\vee q$（合取子句$\neg p$ 与 q 的析取）；$((p\rightarrow q)\wedge\neg p)\vee\neg q$ 的析取范式为$\neg p\vee(q\wedge\neg p)\vee\neg q$（合取子句$\neg p$，$q\wedge p$，$\neg q$ 的析取）。

定义 3-7 命题公式 A' 称为公式 A 的**合取范式**（conjunctive normal form）如果

（1）$A' \models\!\models A$

（2）A' 为一析取子句或若干析取子句的合取。

【例 3-20】 $p\rightarrow q$ 的合取范式为$\neg p\vee q$（析取子句），$((p\rightarrow q)\wedge\neg p)\vee\neg q$ 的合取范式为$(\neg p\vee t)\wedge(\neg p\vee\neg q)$(或$\neg p\vee\neg q$)。

利用逻辑等价式和代入、替换原理，可以求出任一公式的析取范式及合取范式。

【例 3-21】 求$\neg p\rightarrow\neg(p\rightarrow q)$的析取范式及合取范式。

$$\begin{aligned}\neg p\rightarrow\neg(p\rightarrow q) &\models\!\models p\vee\neg(\neg p\vee q)\\ &\models\!\models p\vee(p\wedge\neg q)(\models\!\models p)\text{析取范式}\\ &\models\!\models (p\vee p)\wedge(p\vee\neg q)\\ &\models\!\models p\wedge(p\vee\neg q)(\models\!\models p)\text{合取范式}\end{aligned}$$

合取范式和析取范式，可分别用于识别永真式和永假式。

【例 3-22】

（1）例 3-21 中的公式既非永真式，亦非永假式，因为它等价于 p。

（2）$(p\rightarrow(q\rightarrow r))\rightarrow((p\rightarrow q)\rightarrow(p\rightarrow r))$为永真式，因为

$$\begin{aligned}&(p\rightarrow(q\rightarrow r))\rightarrow((p\rightarrow q)\rightarrow(p\rightarrow r))\\ &\models\!\models\neg(\neg p\vee\neg q\vee r)\vee(\neg(\neg p\vee q)\vee(\neg p\vee r))\\ &\models\!\models (p\wedge q\wedge\neg r)\vee(p\wedge\neg q)\vee(\neg p\vee r)\\ &\models\!\models (p\wedge q\wedge\neg r)\vee((p\vee\neg p\vee r)\wedge(\neg q\vee\neg p\vee r))\\ &\models\!\models (p\wedge q\wedge\neg r)\vee(t\wedge(\neg q\vee\neg p\vee r))\\ &\models\!\models (p\wedge q\wedge\neg r)\vee(\neg q\vee\neg p\vee r)\end{aligned}$$

$\models (p\vee\neg q\vee\neg p\vee r)\wedge(q\vee\neg q\vee\neg p\vee r)\wedge(\neg r\vee\neg q\vee\neg p\vee r)$

$\models t\wedge t\wedge t$

$\models t$

（3）$(q\wedge(p\rightarrow\neg q)\rightarrow p)\wedge\neg(q\rightarrow p)$为永假式，因为

$(q\wedge(p\rightarrow\neg q)\rightarrow p)\wedge\neg(q\rightarrow p)$

$\models(\neg(q\wedge(\neg p\vee\neg q))\vee p)\wedge\neg(\neg q\vee p)$

$\models(\neg q\vee(p\wedge q)\vee p)\wedge(q\wedge\neg p)$

$\models(\neg q\wedge q\wedge\neg p)\vee(p\wedge q\wedge q\wedge\neg p)\vee(p\wedge q\wedge\neg p)$

$\models f\vee f\vee f$

$\models f$

由此可见，当一个公式的析（合）取范式的每一个合（析）取子句都至少含有一对互补文字，则该公式是永假（真）式，反之也成立。同时，我们看到：任一命题公式都可化为与其等价的析取范式和合取范式。其等价推演的方法步骤是：

第一步，消去公式中的联结词→和↔：

把公式中的$p\rightarrow q$化为$\neg p\vee q$；

把公式中的$p\leftrightarrow q$化为$(\neg p\vee q)\wedge(\neg q\vee p)$或$(p\wedge q)\vee(\neg p\wedge\neg q)$；

第二步，将否定联结词 ¬ 向内深入，使之只作用于命题变元或命题变元的否定，然后将$\neg\neg p$化为p；

第三步，利用分配律，将公式进一步化为所需要的范式。

应当指出，一公式的析取范式和合取范式都不是惟一的，例如

$p\vee(p\wedge\neg q)\models(p\wedge(q\vee\neg q))\vee(p\wedge\neg q)$

$\models(p\wedge q)\vee(p\wedge\neg q)\models p$

$p\wedge(p\vee\neg q)\models(p\vee(q\wedge\neg q))\wedge(p\vee\neg q)$

$\models(p\vee q)\wedge(p\vee\neg q)\models p$

因而$\neg p\rightarrow\neg(p\rightarrow q)$有析取范式 $p\vee(p\wedge\neg q)$，$(p\wedge q)\vee(p\wedge\neg q)$和 p，它又有合取范式 $p\wedge(p\vee\neg q)$，$(p\vee q)\wedge(p\vee\neg q)$及$p$。

另一方面，一公式的合取范式与析取范式又可能是同一的。例如，p 既是$\neg p\rightarrow\neg(p\rightarrow q)$的合取范式，又是它的析取范式。又如$\neg p\vee q$ 既可称为 $p\rightarrow q$ 的析取范式，又可称为它的合取范式。

上述两点不能不说是这种范式的缺点，因此，虽然它们在公式的规范形式上有很大的作用，但对于实现本节开头所说的目标是明显不足的。

3.3.2 主析取范式与主合取范式

定义 3-8 设 A 为恰含命题变元 $p_1,\cdots,p_n$ 的公式。公式 A' 称为 A 的**主析（合）取范式**（majordisjunctive（conjunctive）normal form）。如果 A' 是 A 的析（合）取范式，并且其每个合（析）取子句中 $p_1,\cdots,p_n$ 均恰出现一次。

据定义，例 3-21 中公式$\neg p\rightarrow\neg(p\rightarrow q)$的主析取范式是$(p\wedge q)\vee(p\wedge\neg q)$，而其主合取范式则应是$(p\vee q)\wedge(p\vee\neg q)$。

【例 3-23】 求公式$(p\wedge q)\vee r$的主析取范式及主合取范式。

$(p\wedge q)\vee r$

$\models\!\dashv (p\wedge q\wedge(r\vee\neg r))\vee((p\vee\neg p)\wedge(q\vee\neg q)\wedge r)$

$\models\!\dashv (p\wedge q\wedge r)\vee(p\wedge q\wedge\neg r)\vee(p\wedge q\wedge r)\vee(p\wedge\neg q\wedge r)\vee(\neg p\wedge q\wedge r)\vee(\neg p\wedge\neg q\wedge r)$

$\models\!\dashv (p\wedge q\wedge r)\vee(p\wedge q\wedge\neg r)\vee(p\wedge\neg q\wedge r)\vee(\neg p\wedge q\wedge r)\vee(\neg p\wedge\neg q\wedge r)$

此即所求的主析取范式。另外

$(p\wedge q)\vee r$

$\models\!\dashv (p\vee r)\wedge(q\vee r)$

$\models\!\dashv (p\vee(q\wedge\neg q)\vee r)\wedge((p\wedge\neg p)\vee q\vee r)$

$\models\!\dashv (p\vee q\vee r)\wedge(p\vee\neg q\vee r)\wedge(p\vee q\vee r)\wedge(\neg p\vee q\vee r)$

$\models\!\dashv (p\vee q\vee r)\wedge(p\vee\neg q\vee r)\wedge(\neg p\vee q\vee r)$

最后一式即为所求的主合取范式。

我们总结一下利用等价推演求公式的主析（合）取范式的方法步骤：

第一步：求出该公式的析（合）取范式；

第二步：简化各子句，除去范式中所有恒假（真）的合（析）取子句，即化掉含有互补文字对的合（析）取子句；同时，将合（析）取子句中同一文字的多个出现合并为一个；

第三步：对并非每一变元都出现的析（合）取范式中的合（析）取子句，利用 $p\models\!\dashv p\wedge t\models\!\dashv p\wedge(q\vee\neg q)$ 或 $p\models\!\dashv p\vee f\models\!\dashv p\vee(q\wedge\neg q)$ 把未出现的变元（q）补进来，并用分配律将其展开，最后得到给定公式的主析（合）取范式。

最后，我们要讨论指派与两种范式之间的联系。

很明显，要使主析取范式取值 1，只要使其某一个合取子句取值 1，从而需使这一子句中的每个文字都取值 1，即只要令正文字中命题变元取值 1，而令负文字中命题变元取值 0。换言之，由主析取范式的一个合取子句可确定一个原公式的弄真指派；反之，亦可由原公式的一个弄真指派确定其主析取范式中的一个合取子句。公式的弄真指派与主析取范式的合取子句是一一对应的。例如，例 3-23 中公式的主析取范式有五个合取子句，它们分别对应于公式的 5 个弄真指派：

$p\wedge q\wedge r$	1,1,1
$p\wedge q\wedge\neg r$	1,1,0
$p\wedge\neg q\wedge r$	1,0,1
$\neg p\wedge q\wedge r$	0,1,1
$\neg p\wedge\neg q\wedge r$	0,0,1

类似地，要使主合取范式取值 0，只要使其一个析取子句取值 0，从而需使析取子句中的每一文字取值 0，即令正文字中命题变元取值 0，而令负文字中命题变元取值 1。换言之，由主合取范式的一个析取子句可确定一个原公式的弄假指派；反之，亦可由原公式的一个弄假指派确定其主合取范式中的一个析取子句。公式的弄假指派与主合取范式的析取子句是一一对应的，只是对应方式刚好相反，正文字中变元都对应 0，负文字中变元都对应 1。例如，例 3-23 中公式的三个析取子句，如下对应于三个弄假指派：

$p\vee q\vee r$	0,0,0
$p\vee\neg q\vee r$	0,1,0
$\neg p\vee q\vee r$	1,0,0

由以上分析，我们可以进一步得到下述结论：

（1）每公式的主析取范式和主合取范式都是惟一确定的，因为任一公式的弄真指派及弄假指派是完全确定的。

（2）永真式，例如 $p\vee\neg p$，没有主合取范式，因为它没有弄假指派。永真式只有主析取范式，它包含所有可能的合取子句（$p\vee\neg p$ 的主析取范式为其自身），因为一切指派均弄真它。为讨论方便，约定永真式的主合取范式为 t。

（3）永假式，例如 $p\wedge\neg p$，没有主析取范式，因为它没有弄真指派。永假式只有主合取范式，它包含所有可能的析取子句（$p\wedge\neg p$ 的主合取范式为自身），因为一切指派均弄假它。为讨论方便，约定永假式的主析取范式为 f。

（4）n 个命题变元的主析取范式及主合取范式都有 2^{2^n} 个，因为不同的合取子句及析取子句都是 2^n 个，而两种主范式都是从 2^n 个子句中取若干个（0,1,…, 2^n 个）子句组成的（取 0 个子句组成 t 或 f）。我们知道 $C_{2^n}^{0}+C_{2^n}^{1}+\cdots+C_{2^n}^{2^n}=2^{2^n}$。从真值表的角度看也是如此。一张真值表（确定了弄真指派和弄假指派）恰对应一个主析（合）取范式。因此，n 个变元的真值表有多少种，便相应地有多少 n 个变元的主析（合）取范式。事实上，n 个变元的真值表必有 2^n 行，对应于 2^n 个可能的指派，而最后一列的每一行有 0，1 两个可能的值，因而这一列可能的取值状况有 2^{2^n} 种，从而生成 2^{2^n} 张不同的真值表。

（5）由于每一公式均有主析（合）取范式，因此，无限多的含 n 个变元的公式可以分作 2^{2^n}（有限）个类，每一类公式都逻辑等价于它们共同的主析（合）取范式。

*3.3.3 联结词的扩充与归约

据上小节的讨论知，n 个变元的真值表可以有 2^{2^n} 张，因而可以定义 2^{2^n} 个 n 元的真值函数或联结词。这就是说，我们可以规定 $2^{2^1}=4$ 个一元联结词，$2^{2^2}=16$ 个二元联结词，但迄今我们只讨论了一个一元联结词$\neg$ 和四个二元联结词$\wedge$，$\vee$，$\rightarrow$，$\leftrightarrow$。表 3-10 给出了四个一元联结词，其中$\triangle_1$，$\triangle_4$为常联结词，$\triangle_2$为幺联结词，$\triangle_3$是否定词，即对任意命题 p，

$$\triangle_1(p)\models f,\ \triangle_4(p)\models t,\ \triangle_2(p)\models p,\ \triangle_3(p)\models\neg p$$

表 3-10

p	$\triangle_1(p)$	$\triangle_2(p)$	$\triangle_3(p)$	$\triangle_4(p)$
0	0	0	1	1
1	0	1	0	1

表 3-11 给出了 16 个二元联结词，分别标记为$*_1,*_2,\cdots,*_{16}$。这里（p，q 为任意命题）

$*_1$和$*_{16}$是常联结词：

$$p*_1q\models f\ ,\ p*_{16}q\models \mathrm{t}$$

$*_4$和$*_6$是投影联结词：

$$p*_4q\models p,\ p*_6q\models q$$

$*_{11}$和$*_{13}$是二元否定词：

$$p*_{11}q\models\neg q\ ,\ p*_{13}q\models\neg p$$

$*_9$称为“**或非词**”，常用记号↓表示之，也称↓为**皮尔斯**（Peirce）记号：

$$p *_9 q \models\models p \downarrow q \models\models \neg (p \vee q)$$

$*_{15}$称为“**与非词**”，常用记号↑表示之，也称↑为悉非（Sheffer）记号：

$$p *_{15} q \models\models p \uparrow q \models\models \neg (p \wedge q)$$

$*_3$, $*_5$称为“**蕴涵否定词**”，常用记号 $\nrightarrow$ 表示：

$$p *_3 q \models\models p \nrightarrow q \models\models \neg (p \rightarrow q)$$

$$p *_5 q \models\models q \nrightarrow p \models\models \neg (q \rightarrow p)$$

$*_7$称为“**异或词**”，常用记号$\overline{\vee}$（或 ⊕）表示：

$$p *_7 q \models\models p \overline{\vee} q \models\models (p \vee q) \wedge \neg (p \wedge q) \models\models \neg (p \leftrightarrow q)$$

表 3-11

p q	$p *_1 q$	$p *_2 q$	$p *_3 q$	$p *_4 q$	$p *_5 q$	$p *_6 q$	$p *_7 q$	$p *_8 q$
0	0	0	0	0	0	0	0	0
1	0	0	0	0	1	1	1	1
0	0	0	1	1	0	0	1	1
1 1	0	1 合取词	0	1	0	1	0	1 析取词

p q	$p *_9 q$	$p *_{10} q$	$p *_{11} q$	$p *_{12} q$	$p *_{13} q$	$p *_{14} q$	$p *_{15} q$	$p *_{16} q$
0	1	1	1	1	1	1	1	1
0 1	0	0	0	0	1	1	1	1
0	0	0	1	1	0	0	1	1
1 1	0	1 等价词	0	1 蕴涵词	0	1 蕴涵词	0	1

上述讨论，一方面告诉我们可以将现有的 5 个联结词扩充得更多，另一方面又告诉我们，如果不增加变元个数，所有可能的扩充都不会带来实质性的收获，因为它们都可以用先前的 5 个来表示，我们将更清楚地说明这一点。

定义 3-9 称 n 元联结词 h 是用 m 个联结词 $g_1, g_2, \cdots, g_m$ 可表示的，如果

$$h(p_1, p_2, \cdots, p_n) \models\models A$$

而 A 中所含联结词仅取自 $g_1, g_2, \cdots, g_m$。

由于$\triangle_1 (p) \models\models p \wedge \neg p$，$\triangle_2 (p) \models\models p$，$\triangle_4 (p) \models\models p \vee \neg p$，因此一元联结词全都是¬，∧，∨可表示的。由上面的讨论，$*_1$，$*_3 \sim *_7$，$*_9$，$*_{11}$，$*_{13}$，$*_{15}$，$*_{16}$ 都是 ¬，∧，∨，→，↔可表示的。

定义 3-10 当联结词组$\{g_1, g_2, \cdots, g_m\}$可表示所有一元、二元联结词时，称其为**完备联结词组**（complete group of connectives）。

据以上讨论知，{¬，∧，∨，→，↔}是完备联结词组。更少的联结词是否可能组成完备联结词组呢？回答是肯定的。这就是说，对 5 个联结词还可以进行归约。

由于所有命题公式均可以化为析取范式或合取范式，因此，5 个联结词可以归约为 3 个：{¬，∧，∨}，从而{¬，∧，∨}是完备的联结词组。更进一步，由于∨与∧可利用 ¬ 来相互表示，即

$$p \vee q \models\models \neg (\neg p \wedge \neg q)$$

$$p \wedge q \models\models \neg (\neg p \vee \neg q)$$

因而{¬，∨}及{¬，∧}是两个完备联结词组。

此外，{¬，→}与{$\triangle_1$，→}也是两个完备的联结词组。为证明这一点，只要选取一个已知的完备联结词组（例如 {¬，∨}）去证明该组中的每一个联结词均可用¬，→或$\triangle_1$，→来表示。证明细节请读者补出。

【例 3-24】 证明或非词 ↓ 单独构成完备联结词组。

证明 我们用 ↓ 分别表示 ¬，∨ 中的每一个：

$$\neg p \models\models \neg (p \vee p) \models\models p \downarrow p$$

$$p \vee q \models\models \neg (\neg (p \vee q)) \models\models \neg (p \downarrow q) \models\models (p \downarrow q) \downarrow (p \downarrow q)$$

事实上与非词↑也是完备的，请读者证明之。

应当指出，存在不完备的联结词组，例如单一的析取词∨（合取词∧）不能构成完备联结词组。仅用 ∨（或∧）都不能构成永假式，因而不能表示一元联结词$\triangle_1$。

{∨，∧}也不是完备的，因为否定词¬ 无法用∨，∧来表示。¬ p 在 p 假时为真，而仅由 p 及∨，∧组成的公式在 p 假时均为假。

{¬，↔}也不是完备的，这可以如下证明：

（1）任一仅由 p，q，↔，¬ 组成的公式 $A(p,q)$，其可能的真值表只有 8 种（如表 3-12），每一表中弄真指派总是偶数个。

对 A 中联结词↔，¬ 的个数归纳证明（1）。

若 A 恰好是原子命题 p,q，其取值可能如表 3-12 之第 3，4 两列所示，各有两个弄真指派。

若 A 为 $A_1 \leftrightarrow A_2$ 或¬ A_1，设 A_1，A_2 只有表所示 8 种取值可能，易逐一计算验证，$A_1 \leftrightarrow A_2$，¬ A_1 的取值仍在这 8 种之列，弄真指派总为偶数个。

归纳完成。

（2）弄真 $p \vee q$ 的指派却为 3 个：（1，1），（1，0），（0，1），因此，$p \vee q$ 不可能同任何仅用 p,q, ↔,¬ 组成的公式等价，即∨不能用¬，↔来表示。

表 3-12

p q	$A(p,q)$							
	1	2	3	4	5	6	7	8
0 0	0	1	0	0	0	1	1	1
0 1	0	1	0	1	1	0	0	1
1 0	0	1	1	0	1	0	1	0
1 1	0	1	1	1	0	1	0	0

证明联结词组不完备还可用下述方法：选取一个已知的不完备联结词组（例如）{¬，↔}，证明这组联结词（甲）可表示待证联结词组（乙）中的每一个。如果成功，那么可确定待证联结词组（乙）不完备。因为不然的话，（乙）是完备的，会导出已知的不完备联结词组（甲）是完备的，产生矛盾。

3.4 练习

1．判断下列语句是否是命题，若是命题则请将其形式化：

（1）$a+b+c$

（2）$x>0$

（3）请进！

（4）离散数学是计算机科学与技术专业的基础课程。

（5）2009 年 7 月我们去意大利的米兰旅游。

（6）你是博士，但我是硕士。

（7）我今天或明天去泰山。

（8）我今天或明天去泰山的说法是谣传。

（9）我明天或后天去北京或天津。

（10）如果买不到飞机票，我不去海南岛。

（11）只要他出门，他必买书，不管他带的钱多不多。

（12）除非你陪伴我或代我雇辆车子，否则我不去。

（13）只要充分考虑，就可得到正确见解；必须充分考虑，才能得到正确见解。

（14）如果只有懂得希腊文才能了解柏拉图，那么我不了解柏拉图。

（15）不管你和他要不要这本书，我要。

（16）侈而惰者贫，而力而俭者富。（韩非：《韩非子・显学》）

（17）骐骥一跃，不能十步；驽马十驾，功在不舍；锲而舍之，朽木不折；锲而不舍，金石可镂。（荀况：《荀子・劝学》）

2．根据命题公式的定义和括号省略的约定，判定下列符号串是否为公式，若是，请给出它的真值表，并请注意这些真值表的特点：

（1）$\neg(p)$（p 为原子命题）

（2）$(p\vee qr)\rightarrow s$

（3）$(p\vee q)\rightarrow p$

（4）$p\rightarrow(p\vee q)$

（5）$p\wedge(p\rightarrow q)\rightarrow q$

（6）$p\wedge(p\rightarrow q)\wedge(p\rightarrow\neg q)$

（7）$\neg(p\vee q)\leftrightarrow\neg q\wedge\neg p$

（8）$\neg p\vee q\leftrightarrow(p\rightarrow q)$

（9）$(p\rightarrow q)\wedge(q\rightarrow r)\rightarrow(r\rightarrow p)$

（10）$(p\vee q\rightarrow r)\leftrightarrow(p\rightarrow r)\wedge(q\rightarrow r)$

3．给出弄真下列命题公式的指派：

（1）$((p\rightarrow q)\wedge q)\rightarrow\neg p$

（2）$((p\rightarrow q)\rightarrow r)\rightarrow((q\rightarrow p)\rightarrow r)$

（3）$((p\leftrightarrow q)\rightarrow r)\rightarrow((q\rightarrow p)\leftrightarrow r)$

（4）$\neg((p\vee q)\wedge r)\rightarrow(r\rightarrow p)$

4．在第 1 章里，定义广义交运算$\bigcap C=\{x:$对所有$S,$若$S\in C$则$x\in S)\}$时约定 C 非空。现依据实质蕴涵的定义，请判断，当 C 为空集时，$\bigcap C$ 应为什么集合？

*5．A 国的人只有两种，一种永远说真话，一种永远说假话。你来到 A 国，并在一个二叉路口不知如何走才能到达首都。守卫路口的士兵只准你问一个问题，而且他只答“是”或“不是”。你应该如何发问，才能从士兵处获知去首都的道路。

6. 试判定以下各式是否为重言式：

（1）$(p\rightarrow q)\rightarrow(q\rightarrow p)$

（2）$\neg p\rightarrow(p\rightarrow q)$

（3）$q\rightarrow(p\rightarrow q)$

（4）$p\wedge q\rightarrow(p\leftrightarrow q)$

（5）$(p\rightarrow q)\vee(r\rightarrow q)\rightarrow((p\vee r)\rightarrow q)$

（6）$(p\rightarrow q)\vee(r\rightarrow s)\rightarrow((p\vee r)\rightarrow(q\vee s))$

7. 试用真值表验证 E_6，E_8，E_{16}，E_{17}。

8. 不用真值表，用代入、替换原理证明 E_{16}，E_{17}。

9. 试用真值表验证 I_3，I_4，I_5，I_6。

10. 不用真值表，用代入、替换原理证明 I_7，I_8 。

11. 用三种不同方法证明下列逻辑等价式：

（1）$A\leftrightarrow B \dashv\vdash (A\wedge B)\vee(\neg A\wedge\neg B)$

（2）$A\rightarrow(B\rightarrow C) \dashv\vdash B\rightarrow(A\rightarrow C)$

（3）$A\rightarrow(A\rightarrow B) \dashv\vdash A\rightarrow B$

（4）$A\rightarrow(B\rightarrow C) \dashv\vdash (A\rightarrow B)\rightarrow(A\rightarrow C)$

12. 用三种不同方法证明下列逻辑蕴涵式：

（1）$A\wedge B \vdash A\leftrightarrow B$

（2）$(A\rightarrow B)\rightarrow A \vdash A$

（3）$A\rightarrow B \vdash ((A\leftrightarrow B)\rightarrow A)\rightarrow B$

（4）$(A\vee B)\wedge(A\rightarrow C)\wedge(B\rightarrow C) \vdash C$

*13. 验证下列逻辑等价式和逻辑蕴涵式，并写出它们的对偶式：

（1）$\neg(\neg A\vee\neg B)\vee\neg(\neg A\vee B) \dashv\vdash A$

（2）$(A\vee\neg B)\wedge(A\vee B)\wedge(\neg A\vee\neg B) \dashv\vdash \neg(\neg A\vee B)$

（3）$B\vee\neg((\neg A\vee B)\wedge A) \dashv\vdash \mathrm{t}$

（4）$\neg A\vee(\neg B\vee C) \vdash \neg(\neg A\vee B)\vee(\neg A\vee C)$

（5）$\neg(A\vee B)\vee C \vdash A\vee(\neg B\vee C)$

（6）$\neg(A\vee B) \vdash A\vee(\neg B\vee C)$

14. 求下列公式的析取范式、合取范式及主析取范式、主合取范式，并据主析（合）取范式直接确定该公式的弄真指派和该公式的弄假指派：

（1）$(\neg p\vee\neg q)\rightarrow(p\leftrightarrow\neg q)$

（2）$q\wedge(p\vee\neg q)$

（3）$p\vee(\neg p\rightarrow(q\vee(\neg q\rightarrow r)))$

（4）$(p\rightarrow(q\wedge r))\wedge(\neg p\rightarrow(\neg q\wedge\neg r))$

（5）$p\rightarrow(p\wedge(q\rightarrow r))$

15. 主析取范式的两个不同析取项可能在同一指派下均真吗？为什么？主合取范式的两个不同合取项可能在同一指派下均假吗？为什么？

16. 利用范式证明下列公式为永真式（证明合取范式的每一个合取项中含有互补文字、或其主析取范式中含有 2^n 个析取项，n 是公式中变元的个数）

（1）$(p\rightarrow q)\wedge p\rightarrow q$

（2）$((p\rightarrow q)\rightarrow(\neg p\rightarrow\neg q))\rightarrow((\neg q\rightarrow\neg p)\rightarrow(q\rightarrow p))$

（3）$(p\leftrightarrow q)\leftrightarrow((p\wedge q)\vee(\neg p\wedge\neg q))$

（4）$(p\leftrightarrow q)\leftrightarrow((r\wedge p)\leftrightarrow(r\wedge q))\wedge((r\vee p)\leftrightarrow(r\vee q))$

（5）$\neg(p\downarrow q)\leftrightarrow(\neg p\uparrow\neg q)$

（6）$\neg(p\uparrow q)\leftrightarrow(\neg p\downarrow\neg q)$

*17. 把公式$(p\rightarrow q)\leftrightarrow(\neg q\rightarrow\neg p)$变换为与之等价的、只含联结词↓或↑的公式。

*18. 求证$\{\neg,\rightarrow\}$及$\{\Delta_1,\rightarrow\}$都是完备联结词组。你还能找到恰由两个联结词组成的完备联结词组吗？

*19. 求证$\{\neg,\overline{\vee}\}$不是完备联结词组。

*20. 证明：联结词↓和↑满足交换律但不满足结合律。

*21. 化简下列各式：

（1）$p\overline{\vee}p$，（2）$p\overline{\vee}\mathrm{t}$，（3）$p\overline{\vee}f$

（4）$p\downarrow p$，（5）$p\downarrow\mathrm{t}$，（6）$p\downarrow f$

（7）$p\uparrow p$，（8）$p\uparrow\mathrm{t}$，（9）$p\uparrow f$

第4章　逻辑代数（下）——谓词演算

弗雷格（Frege）的天才著作《概念演算》，把我们引入到命题的内部。事实上，命题逻辑虽然可以形式化地描述一些人类思维的规律，并能够用来对命题公式进行一些代数变换。但是，命题逻辑以原子命题为最小的研究单位，不对原子命题的内部结构做深入研究，这无论在数学中还是在计算机科学中，都是不够的。例如，数学中常用的判断："$x>5$"，"实数的平方非负"等均无法用命题逻辑的形式来准确描述。对于推理机制的刻画，命题演算的不足就更加明显了。例如，下列逻辑学经典推理的正确性是人所共知的：

所有的人都是要死的
苏格拉底是人

苏格拉底是要死的

但是，命题演算却无法反映上述推理，因为这里的前提和结论都只能表示为原子命题，例如表示为 p，q，r。在命题演算系统中，无法由前提 p，q 推出结论 r，结论 r 也根本不是前提 p，q 的逻辑结果。

命题演算的不足当然是由于它忽略了命题内部的"细节"。原子命题内部究竟有些什么"细节"呢？弗雷格作了详尽的研究，我们借用上例加以说明。

这三个命题中涉及两个概念，它们表示事物的性质："是人"，"是要死的"，称之为**谓词**。它们还涉及两种主体："所有的人"，"苏格拉底"，称之为**个体**。前者表示一类个体的全部，这里使用了数量词"所有"，称之为**量词**。只有当这些细节都被清楚地表示出来，同时建立起它们之间逻辑关系的形式描述（例如，建立一条规则，表示一类个体都有的性质，此类个体中的每一个个体也具有这一性质），那么刻画类似本章引例的推理才是可能的。

本章的讨论就从谓词演算所涉及的这三种基本成分：个体、谓词和量词开始。

4.1　谓词演算基本概念

4.1.1　个体与个体域

谓词演算中把一切讨论对象都称为**个体**（individuals），它们可以是客观世界中的具体客体，也可以是抽象的客体，诸如数字、符号等。确定的个体常用 a，b，c 等小写字母或字母串表示。a，b，c 等小写字母或字母串称为**个体常元**（constants）。不确定的个体常用字母 x，y，z，u，v，w 等来表示，它们被称为个体**变元**（variables）。

谓词演算中把讨论对象——个体的全体称为**个体域**（domain of individuals），也就是我们在集合论中所说的全集，常用字母 D 表示，并约定任何 D 都至少含有一个成员。当讨论对象遍及一切客体时，个体域特称为**全总域**（universe），用字母 U 表示。例如，中学生在说"所有数的平方非负"时，实数集是个体域；而达尔文在写《物种起源》时，则以全体生物为个体域；也许哲学家更偏爱全总域，讨论常常会涉及多种类型个体，这时使用全总域也是

比较方便的。

当给定个体域时，常元表示该域中的一个确定的成员，而变元则可以取该域中的任何一个成员为其值。表示 D 上个体间运算的运算符与常元、变元组成所谓**个体项**（terms）。例如，$a+b$，x^2 等。

4.1.2 谓词与谓词填式

语句中表示个体性质或关系的语言成分（通常是谓语）称为**谓词**（predicate）。例如：

（1）“苏格拉底是人”中的“…是人”。

（2）“苏格拉底是要死的”中的“…是要死的”。

（3）“实数的平方非负”中的“…是实数”，“…是非负的”。

（4）“董旎生于青岛”中的“…生于…”。

（5）“3 小于 2”中的“…小于…”。

（6）“3+5=8”中的“…+…=…”。

这里，（1），（2），（3）中的谓词表示个体性质，（4），（5）中的谓词表示两个个体间的关系，（6）中的谓词表示 3 个个体间的关系。

我们看到，谓词携有可以放置个体的空位，当空位上填入个体后便产生一个关于这些个体的语句，它断言个体具有谓词所表示的性质或关系。通常把谓词所携空位的数目称为**谓词的元数**。例如上述例子中，（1），（2），（3）中的谓词是一元谓词，（4），（5）中的谓词是二元谓词，（6）中的谓词是三元谓词。

谓词演算中用携有空位的大写字母表示谓词(字母的选择是随意的,以方便记忆为好)。例如可用以下表示形式：

M（）表示“…是人”。

D（）表示“…是要死的”。

R（）表示“…是实数”。

NN（）表示“…是非负的”。

B（,）表示“…生于…”。

L（,）表示“…小于…”。

ADD（,,）表示“…+…=…”。

这种含空位的写法有一个明显的缺点，可读性差。因此常用变元来代替空位，例如可用 $M(x)$，$D(x)$，$R(x)$，$NN(x)$，$B(x,y)$，$L(x,y)$，$ADD(x,y,z)$ 表示上述 5 个谓词，它们被称为**谓词命名式**，简称谓词。这里，用什么变元是无关紧要的（当然，不同的空位应用不同的变元），并且这些变元仅仅作为谓词形式表示的一部分，没有独立的意义。

我们说过，当谓词的空位上填入个体后，便产生一个关于该个体的语句，这时它被称为**谓词填式**，例如：

M（socrates）表示“苏格拉底是人”。

D（socrates）表示“苏格拉底是要死的”。

$R(x)$ 表示“x 是实数”（这里 x 表示个体变元）。

$NN(y)$ 表示“y 是非负的”（这里 y 表示个体变元）。

B（Dongni，qingdao）表示“董旎生于青岛”。

L（3，2）表示“3 小于 2”。

ADD（3，5，8）表示“3+5=8”。

一般地，谓词填式 $P(t_1,\cdots,t_n)$表示:个体项 $t_1,\cdots,t_n$ 所代表的个体满足 n 元谓词 $P(x_1,\cdots,x_n)$。

应当注意，当空位处填入变元时，谓词命名式与谓词填式同形，但它们表示不同的意义。例如，R（x）作为命名式时，它只是 R（）的另一写法，与 x 无关，改为 R（y）意义照旧；R（x）作为填式时，它表示“x 所取值为实数”，改为 R（y）后其意义“y 所取值为实数”就完全不同了。在概念上认清这一点是十分重要的，但为了叙述的简明，只要不至于造成问题，我们不一一指明含有变元的谓词形式究竟是谓词命名式还是谓词填式，读者可通过上下文自行加以鉴别。

当谓词填式中所填个体都是常元时，它是一个命题，因而有确定的真值，例如 L（3，2）为假，ADD（3，5，8）为真。从这个意义上说，谓词是以个体域为定义域，以真值集为值域的映射。

一些复杂的性质和关系，可以用谓词和联结词复合的形式来描述，例如：

“x 是小于 100 的质数”可表示为

$$L(x,\ 100)\wedge P(x)\quad(L(x,\ 100)：x\text{ 小于 }100，P(x)：x\text{ 是质数})$$

“y 小于等于 3”可表示为

$$L(y,3)\vee E(y,3)\quad(E(y,3)：y\text{ 等于 }3)，或\ y\leqslant 3$$

“如果一个人生于北京，那么他不生于上海”可表示为

$$B(x,\text{beijing})\rightarrow\neg\ B(x,\text{shanghai})$$

“y 是非负实数当且仅当 y 大于等于零”可表示为

$$NN（y）\leftrightarrow 0\leqslant y$$

4.1.3 量词及其辖域

谓词演算中的**量词**（quantifiers）指数量词“所有”和“有”，分别用符号$\forall$和$\exists$来表示，分别称为**全称量词**和**存在量词**。为了用全称量词$\forall$和存在量词$\exists$分别表示个体域中所有个体和有些个体满足一元谓词 P，需引入一个变元，同时用作量词的指导变元（放在量词后）和谓词 P 的填式的变元：

$\forall xP(x)$ 读作“所有（任意，每一个）x 满足 $P(x)$”。表示个体域中所有的个体满足谓词 $P(x)$。

$\exists x\ P\ (x)$ 读作“有（存在，至少有一个）x 满足 $P(x)$”。表示个体域中至少有一个体满足谓词 $P(x)$。

下列关于量词的说明是重要的：

（1）上述变元是用 x 还是别的变元是无关紧要的，因为变元的更改并不改变语句的含义。因此，我们说量词的指导变元和量词“管辖”的谓词填式中的变元是可以**改名**（rename）的。

（2）量词不仅可用于谓词填式之前，还可用于复合的谓词表达式之前，这时应对该表达式使用括号。例如：

$\exists x\ (M(x)\wedge B(x))$ 表示“有的个体是人且是勇敢的”（$B(x)$：x 是勇敢的）。

$\forall x(L(x,2)\vee\neg\ L(x,2))$ 表示“所有的个体或者小于 2 或者不小于 2”。

$\forall x(M(x)\rightarrow D(x))$ 表示“所有个体中凡人者是要死的”，即“所有人都是要死的”。

当量词用于一谓词填式或复合的谓词表达式式时，该谓词或复合的谓词表达式称为量词的**辖域**（domains of quantifiers）。因此，量词的辖域或者是紧邻其右侧的那个谓词；或者是其右侧第一对括号内的表达式。

（3）量词的指导变元和量词辖域内的同名变元与通常谓词填式中的个体变元不同，因为它可以改名却不能取值代入，例如$\forall 5P(5)$，$\exists x^2\,P\,(x)$都是毫无意义的。因此，我们把$\forall xP(x)$和$\exists xP(x)$中变元称为**约束变元**（bound variables），而那些可以取值代入的变元则称为**自由变元**（free variables）。

综合（1），（3）可知，约束变元是形式记号的一部分，对它可以改名但不能代入。其实数学中常常使用这种约束变元作为数学符号的一部分。例如$\sum_{i=0}^{n} f(i)$中的变元 i，它只是 Σ记号的一部分，求和结果与 i 无关，对 i 可以改名（比如改为 j），但令 $i=2$，和式便失去意义。$\sum_{i=0}^{n} f(i)$中的 n 则是自由变元,，对 n 可作代入，例如，对 n 代入数字 2 时，和式是有意义的：

$$\sum_{i=0}^{2} f(i) = f(0)+f(1)+f(2)。$$

（4）对于一元谓词 $P(x)$，$\forall xP(x)$为一命题，它断言所有个体满足性质 $P(x)$，其真值已经确定。同理$\exists xP(x)$也是命题。特别是，当个体域中个体有穷时，例如 $D=\{a_1,\cdots,a_n\}$，$\forall xP(x)$的意义与命题 $P(a_1)\wedge\cdots\wedge P(a_n)$ 等同，而$\exists xP(x)$的意义与命题 $P(a_1)\vee\cdots\vee P(a_n)$ 等同。

【例 4-1】 （1）$\forall x(A(x)\rightarrow B(x))\vee C(x)$ 中$\forall x$ 的辖域是 $A(x)\rightarrow B(x)$，其中的 x 是约束变元；但 $C(x)$不在辖域内，其中的 x 则是自由变元；$\exists x\ A(x)\wedge B(x)$中$\exists$x 的辖域是 $A(x)$，其中 x 是约束变元，而 $B(x)$中 x 为自由变元。由于约束变元与自由变元同名，这类语句容易引起混乱，可以利用约束变元能够改名的特点来消除这种混乱。上述两例可改为

$$\forall y(A(y)\rightarrow B(y))\vee C(x)，\ \exists y\,A(y)\wedge B(x)。$$

（2）约定个体域为{0，1，2}，此时

$\forall y(y^2=y))$ 等价于 $0^2=0\wedge 1^2=1\wedge 2^2=2$，此为假。

$\exists y(y^2=y))$ 等价于 $0^2=0\vee 1^2=1\vee 2^2=2$，此为真。

4.1.4 谓词公式及语句的形式化

定义 4-1 归纳定义**谓词公式**（predicate forrmula），谓词公式又称合式公式，简称公式。

（1）谓词填式是公式，命题常元是公式（看作零元谓词），常称原子公式。

（2）如果 A，B 是公式，x 为任一变元，那么$(\neg A)$，$(A\rightarrow B)$，$(\forall xA)$，$(\exists x\ A)$（当使用 5 个联结词时还有$(A\wedge B)$，$(A\vee B)$，$(A\leftrightarrow B)$）都是公式。

（3）只有有限步使用（1），（2）条款所形成的符号串是公式。

括号省略原则同命题公式，并约定$(\forall xA)$，$(\exists x\,A)$中最外层括号也可省略。

【例 4-2】 $L(x,y)$，$\forall x(M(x)\rightarrow D(x))$，$\exists x\,A(x)\wedge B$，$\forall x\exists y(\,B(x,y)\wedge M(y))$，$\exists yL(3,2)\rightarrow\forall x\,L(x,2)$都是公式，其中$\forall x\exists y(\,B(x,y)\wedge M\,(y))$是$\forall x\,(\exists y(\,B(x,y)\wedge M(y)))$的简写。

注意，$\exists yL(3,2)$也是公式，尽管 $L(3,2)$中没有变元 y。$\exists yL(3,2)$被理解为 $L(3,2)$。一般地，

当 A 中无变元 x 时，$\forall xA$，$\exists x\,A$，均被看作与 A 相同。

当个体域给定，谓词公式中的谓词都有明确意义（关于个体域中个体的某个性质或关系），并且在谓词公式中自由变元均已取定个体时，谓词公式也就具有了确定的意义，成了关于个体域的一个断言，可判定其真值。

【例 4-3】 设 D 为实数域，$E(x,y)$表示 D 上关系“$x=y$”，$L(x,y)$：$x<y$ 那么

（1）$\forall x\,L(0,x^2+1)$ 真。

（2）$\exists xE(x^2-2x-1,0)$ 真。

（3）$\exists xE(x^2+x+1,0)$ 假。

（4）$\exists xE(x^2,y)$ 当 y 取非负实数时真，否则假。

当 D 改为复数域时，（1）为假，（2），（3）为真，（4）对 y 的一切可能取值为真，即$\forall y\,\exists xE(x^2,y)$真。为了使公式可读性更好，下文我们不再坚持谓词的前辍形式，允许常用的数学符号表示谓词，例如用 $x<y$ 代替 $L(x,y)$，$x^2=y$ 代替 $E(x^2,y)$。

（5）$\forall x\,\forall y\,(x+y=y+x)$ 真。

（6）$\exists x\,\exists y\,(x+y=x*y)$ (*表示数乘运算,下同) 真。

（7）$\forall x\,\exists y(x+y=0)$ 真。

（8）$\exists y\,\forall x\,(x+y=0)$ 假。

（9）$\exists y\,\forall x\,(x*y=0)$ 真。

（10）$\forall x\,\exists y(x*y=0)$ 真。

这里（5）是加法的交换律。（6）真，因为同时取 x,y 为 0 时，$x+y=x*y$。（7）是说“对任意 x 都有 y 使 $x+y=0$”，此为真，因为对任意 x，总可取 $y=-x$，使 $x+y=0$。但（8）则是说“有 y 对所有 x 均满足 $x+y=0$”，这不能成立，因为找不到这样的 y。由此可见，量词的次序不是无关紧要的。由于数零对任意 x 有 $x*0=0$，因此（9）成立。此时当然对任意 x 均可找到 y，使 $x*y=0$，因而（10）也成立。

作为本节的最后一个内容，我们来讨论用谓词公式将语句形式化的问题。先看几个例子。

【例 4-4】 设个体域是人类，试将下列语句译为谓词公式。

（1）有人勇敢，但不是所有的人都勇敢。

用 $B(x)$表示“x 勇敢”，它译为

$$\exists xB(x)\ \wedge\neg\ \forall x\,B(x)$$

（2）人人都不相互依靠，但互相帮助。

用 $R(x,y)$表示“x 依靠 y”，$H(x,y)$表示“x 帮助 y”，它译为

$$\forall x\forall y\neg\ R(x,y)\ \wedge\forall x\forall yH(x,y)$$

（3）我为人人，人人为我。

用 i 表示“我”，$S(x,y)$表示“x 为 y 服务”，它可译为

$$\forall xS(i,x)\ \wedge\forall xS(x,\mathrm{i})$$

（4）每个人都有人爱，但没有人为所有人爱。

用 $L(x,y)$表示“x 爱 y”，它可译为

$$\forall x\,\exists yL(y,x)\ \wedge\neg\ \exists y\,\forall x\,L(x,y)$$

（5）勇敢者未必都是成功者。

用 $B(x)$表示“x 是勇敢者”，$W(x)$表示“x 是成功者”，它可译为

$$\neg\,\forall x(B(x)\rightarrow W(x))\ \text{或}\ \exists x(B(x)\wedge\neg\,W(x))$$

从以上例子看出，语句形式化过程的三个关键问题是：

（1）准确地从语句中提取谓词，表示性质的谓语用一元谓词表示，表示关系的谓语用二元或更多元数的谓词来表示。

（2）准确地使用量词和确定量词的辖域，当辖域中多于一个谓词时必须注意联结词与括号的使用。

（3）准确地使用多个重叠的量词，其排列次序应与原语句意义一致。

上一例中，由于确定了个体域，使得语句的形式化变得简单了，但当语句中涉及不同类个体时，这一做法便不能奏效。因此在许多情况下，语句的形式化不针对某一特定域，而采用全总个体域，这给语句形式化带来了一点复杂性。首先，在讨论个体域的某个局部的所有个体或某些个体时，要使用把量词限于该局部的所谓“限定谓词”。例如，例 4-4 中都应使用限定谓词（$M(x)$：“…是人”）来限定量词的意义。其次，限定谓词与其他谓词之间应使用适当的联结词。当限定谓词用于限定全称量词时，它必须作为蕴涵词的前件加入；当限定谓词用于限定存在量词时，它必须作为合取词的合取项加入，即用

$$\forall x(A(x)\rightarrow\cdots)\ \text{和}\ \exists x(A(x)\wedge\cdots)$$

表示“所有满足 $A(x)$的东西都…”和“在满足 $A(x)$的东西中有满足 … 的个体”。这里 $A(x)$是限定谓词，将个体域暂时限定在满足 $A(x)$的那些个体上。例如，例 4-4 之（1）应译为

$$\exists x\,(M(x)\wedge B(x))\ \wedge\neg\,\forall x(M(x)\rightarrow B(x))$$

限定谓词 $M\,(x)$把论域限在了“人类”之上。例 4-4 之（4）应译为

$$\forall x(M(x)\rightarrow\exists y\,(M(y)\wedge L(y,x)))\ \wedge\neg\,\exists y\,(M(y)\wedge\forall x(M(x)\rightarrow L(x,y)))$$

限定谓词的上述联结方式是不可更改的。我们用$\exists x\ (M(x)\wedge B(x))$（有人勇敢）和$\forall x(M(x)\rightarrow D(x))$（所有人都是要死的）为例加以说明。

对全总个体域而言，“有人勇敢”即“有个体不仅是人而且勇敢”，$M(x)$与 $B(x)$合取是当然的；而“所有的人都是要死的”则是指“全总域中是人的那部分个体都是要死的”，即“若是人则要死”因而 $M\,(x)$与 $D\,(x)$是蕴涵关系。相反，如果我们用$\exists x(M(x)\rightarrow B(x))$表示“有人勇敢”，用$\forall x(M(x)\wedge D(x))$表示“所有人都是要死的”，那么它们与原语句的意义就完全不同了。“有人勇敢”一句原本对于个体域{3，秦桧}是假的，因为数 3 不是人，秦桧不勇敢。但$\exists x\,(M(x)\rightarrow B(x))$对个体域{3，秦桧}却为真，因为其中有非人的个体 3 使 $M(3)$假，从而 $M(3)\rightarrow B(3)$为真。更荒唐的是，$\forall x(M(x)\wedge D(x))$的意义是宇宙万物不仅都是人而且都要死，与“所有人都是要死的”毫无共同之处。

为了使读者更熟悉语句形式化，再列举一些例子。

【例 4-5】 将下列语句用谓词公式形式化：

（1）没有不犯错误的人。

$F(x)$：“x 犯错误”，$M(x)$同前，它译为

$$\neg\,\exists x(M(x)\wedge\neg\,F(x))\ \text{或}\ \forall x\,(M(x)\rightarrow F(x))$$

（2）凡是实数，或者大于零，或者等于零，或者小于零。

$R\,(x)$：“x 是实数”，它译为

$$\forall x(R(x)\rightarrow x<0\vee x=0\vee x>0)$$

（3）实数的加运算满足交换律。

$$\forall x\forall y(R(x)\wedge R(y)\rightarrow x+y=y+x)$$

（4）每人都有自己喜欢的水果，有人喜欢所有的水果。

$F(x)$：“x 是水果”，$M(x)$，$L(x,y)$同前，它译为

$$\forall x(M(x)\rightarrow\exists y\,(F(y)\wedge L(x,y)))\wedge\exists x\,(M(x)\wedge\forall y(F(y)\rightarrow L(x,y)))$$

（5）一个数是偶数当且仅当它可被 2 整除。

$E(x)$：“x 是偶数”，$D(x,y)$：“x 整除 y”，它可译为

$$\forall x(E(x)\leftrightarrow D(2,x)))$$

（6）并不是火车都比汽车跑得快，有的汽车比有的火车跑得快。

$A(x)$：“x 是汽车”，$T(x)$：“x 是火车”，$F(x,y)$：“x 比 y 跑得快”，它可译为

$$\neg\,\forall x\forall y(T(x)\wedge A(y)\rightarrow F(x,y))\wedge\exists x\exists y\,(A(x)\wedge T(y)\wedge F(x,y))$$

4.2 谓词演算永真式

4.2.1 谓词公式的真值规定

给定一个命题公式，要确定其真值状况是十分简单的，只要对其中命题变元的各种取值可能（指派）逐一进行计算。但是，对谓词公式问题就复杂得多。例如

（1）$\forall x(M(x)\rightarrow B(x))$

（2）$\exists x\,(f(x)=0)$

（3）$\exists x\,(ax^2+bx+c=0)\wedge y=1$

（1），（2），（3）是否为真，决定于讨论的个体域，决定于符号 M，B，f，a，b，c 的意义，以及自由变元 y 的取值。当个体域为人类，$M(x)$表示 x 是人，$B(x)$表示 x 是要死的，（1）为真；当个体域为实数集合，函数符号 f 表示的函数使得方程 $f(x)=0$ 有根，（2）为真；当个体域为实数集合，常元符号 a，b，c 表示的实数使得 $b^2-4ac\geqslant 0$，且变元 y 取值 1，（3）为真。

因此，谓词公式的真值不仅依赖于个体域，依赖于对公式中谓词符号、函数符号、常元符号所作的解释（即符号与个体域上具体的性质、关系、函数、对象间的映射，常用 I 表示一种解释。I 恒把命题常元解释为真值 0 或 1），还依赖于公式中各自由变元的取值状况。

【例 4-6】 分别给定个体域 $D_1=\{3,4\}$，$D_2=\{3,5\}$，以及解释 I_1、I_2，I_1 把 $P(x)$解释为“x 是质数”，I_2 把 $P(x)$解释为“x 是合数”时的情况，分别讨论 $P(x)$，$\exists yP(y)$ 和$\exists yP(y)\rightarrow P(x)$的真值。详见表 4-1。

表 4-1

个体域	$P(x)$	x	$P(x)$真值	$\exists y\,P(y)$真值	$\exists yP(y)\rightarrow P(x)$真值
D_1	x 是质数（I_1）	3	1	1	1
		4	0	1	0
	x 是合数（I_2）	3	0	1	0
		4	1	1	1
D_2	x 是质数（I_1）	3	1	1	1
		5	1	1	1
	x 是合数（I_2）	3	0	0	1
		5	0	0	1

因此，为了讨论谓词公式的真值，进而讨论谓词演算永真公式，我们需要下列多个层次的真值概念。

定义 4-2 给定个体域 D 及公式 A 中各谓词符号的解释 I，如果 A 中个体变元 $x_1,\cdots,x_n$ 分别取值 $u_1,\cdots,u_n$ 时 A 真，则称 **A 在 $u_1,\cdots,u_n$ 处真**；当 $x_1,\cdots,x_n$ 无论取 D 中怎样的个体 $u_1,\cdots,u_n$，A 在 $u_1,\cdots,u_n$ 处均真，则称 **A 在解释 I 下真**。

例如，例 4-6 中取个体域 D_2，I_1 把 $P(x)$解释为“x 是质数”时，$\exists yP(y)\rightarrow P(x)$在 3 处真，在 5 处真，从而它在 I_1 解释下真。I_2 把 P(x)解释为“x 是合数”时，$\exists yP(y)\rightarrow P(x)$在 3 处真，在 5 处真，从而它在 I_2 解释下也真。

定义 4-3 给定个体域 D，若公式 A 在每一解释 I 下均真，那么称 **A 在 D 上永真**。若公式 A 对任何个体域 D 均有 D 上永真，则称 A 为**永真式**，或称 A **永真**（valid）。A 永真仍记为 $\models A$。

对例 4-6 中个体域 D_2，虽然$\exists yP(y)\rightarrow P(x)$在 I_1 解释下真，在 I_2 解释下也真，仍不能说它在 D_2 上永真，因为容易找到一种解释使$\exists yP(y)\rightarrow P(x)$假。例如，把 $P(x)$解释为“$x=3$”，x 取值 5，那么$\exists yP(y)$为真，而 $P(5)$为假。

沿用命题演算中引入一些符号和称谓：

$A\models B$ 表示“$A\rightarrow B$”永真，称 A 逻辑蕴涵 B。$A\models B$ 当且仅当对任意个体域和解释，一切使 A 真的变元取值状况均使 B 亦真。$\Gamma\models A$ 同前，可作类似的定义。

$A\models\!\dashv B$ 表示“$A\leftrightarrow B$”永真，称 A 逻辑等价 B。$A\models\!\dashv B$ 当且仅当对一切域、解释和变元取值状况，A 与 B 都具有相同的真值。

【例 4-7】 公式 $\exists xP(x)\leftrightarrow\forall x\ P(x)$ 在只有一个元素的个体域 D 上，总是 D 上永真的，但当 D 多于一个成员时，它不再是 D 上永真了。公式$\forall x\ (P(x)\vee\neg P(x))$，$\forall x\ P(x)\rightarrow\exists xP(x)$都是永真式(注意，我们约定个体域不空)，因此可写为

$$\models\forall x\,(P(x)\vee\neg P(x)),\ \forall x\,P(x)\models\exists xP(x)$$

定义 4-4 公式 A 称为**可满足的**，如果对某一个体域、某一解释和变元的某一取值状况，A 在此处取值真。公式 A 不可满足时也称 A 为**永假式**。

例 4-6 中公式显然是可满足的。当公式 A 永真时，$\neg A$ 必定是永假式。

4.2.2 重要的谓词演算永真式

本小节首先指出一些基本的谓词演算永真式，通过一两个例子示范证明方法，但不逐个地对这些公式的永真性加以验证，它们的意义都是相当直观的。下文中 A，B，C 等表示任意的谓词公式。我们沿用命题演算中引入的一些符号和称谓：

$A\models B$ 表示“$A\rightarrow B$”永真，称 A 逻辑蕴涵 B。$A\models B$ 当且仅当对任意个体域和解释，一切使 A 真的变元取值状况均使 B 亦真。$\Gamma\models A$ 同前，可作类似的定义。

$A\models\!\dashv B$ 表示“$A\leftrightarrow B$”永真，称 A 逻辑等价 B。$A\models\!\dashv B$ 当且仅当对一切域、解释和变元取值状况，A 与 B 都具有相同的真值。

（1）所有重言式。首先，由于谓词演算中允许使用命题常元，因而谓词公式中仍包含命题公式，其中的重言式显然在谓词演算中仍然是永真式。

其次，当我们把命题演算中的重言式中的命题变元改为任意的谓词公式，都不会影响原式的永真性，从而它们也是谓词公式中的永真式。

【例 4-8】 $A(x)\rightarrow A(x)$

$A(x)\rightarrow(B(x)\rightarrow A(x))$

$(\neg A(x)\rightarrow\neg B(x))\rightarrow(B(x)\rightarrow A(x))$

都是永真式（这里 A，B 为任意谓词公式）。

（2）当 A 不含自由变元 x 时，

$$\forall x A \models\!\models A，\exists x A \models\!\models A$$

由于 A 与自由变元 x 无关，根据我们的约定两式显然成立。

（3）$\forall x A(x) \models A(x)$

$A(x) \models \exists x A(x)$

$\forall x A(x) \models \exists x A(x)$

它们的意义是十分清楚的。

（4）$\neg \exists x \neg A(x) \models\!\models \forall x A(x)$

$\neg \forall x \neg A(x) \models\!\models \exists x A(x)$

$\neg \exists x A(x) \models\!\models \forall x \neg A(x)$

$\neg \forall x A(x) \models\!\models \exists x \neg A(x)$

上述等价式的意义也是不难明白的，它们表明两个量词可相互表示，因此本质上可只用一个量词。此外，从形式上看，否定词$\neg$ 可以从量词外进入量词的辖域，也可从量词的辖域内提出到量词的辖域外，但要特别注意：在此过程中，量词需作相应的改变。

【例 4-9】 $\neg \exists x\forall y\forall z(x=y+z) \models\!\models \forall x\neg \forall y\forall z(x=y+z)$

$\models\!\models \forall x \exists y \neg \forall z (x=y+z)$

$\models\!\models \forall x \exists y\exists z (x\neq y+z)$

（5）当公式 B 中不含自由变元 x 时，有

$\forall x A(x)\vee B \models\!\models \forall x (A(x)\vee B)$

$\forall x A(x)\wedge B \models\!\models \forall x (A(x)\wedge B)$

$\exists x A(x)\vee B \models\!\models \exists x (A(x)\vee B)$

$\exists x A(x)\wedge B \models\!\models \exists x (A(x)\wedge B)$

【例 4-10】 $\exists x A(x)\wedge\exists y B(y) \models\!\models \exists x (A(x)\wedge\exists y B(y))$

$\models\!\models \exists x\exists y (A(x)\wedge B(y))$

$\forall x (x>0\vee 4<3) \models\!\models \forall x (x>0)\vee(4<3)$

$\models\!\models \forall x (x>0)$

（6）上一组永真式中的公式 B 若含自由变元 x，情况就要复杂一些。

$\forall x (A(x)\wedge B(x)) \models\!\models \forall x A(x)\wedge\forall x B(x)$

$\forall x A(x)\vee\forall x B(x) \models \forall x (A(x)\vee B(x))$

$\exists x (A(x)\wedge B(x)) \models \exists x A(x)\wedge\exists x B(x)$

$\exists x (A(x)\vee B(x)) \models\!\models \exists x A(x)\vee\exists x B(x)$

我们来证明第二式和第三式。

对任一个体域 D 和解释 I。若$\forall x\ A(x)\vee\forall x\ B(x)$真，那么或者（a）$\forall x\ A(x)$真，即对一切个体 $d\in D$，$A(d)$真，从而 $A(d)\vee B(d)$真，故有$\forall x\ (A(x)\vee B(x))$真。（b）$\forall x\ B(x)$真时，同理可证$\forall x\ (A(x)\vee B(x))$亦真。

相反的逻辑蕴涵却是不成立的。为证明这一点，我们只要举出一个个体域和一种解释，它们使$\forall x\,(A(x)\vee B(x))$真，却使$\forall x\,A(x)\vee\forall x\,B(x)$为假。令 D 为整数集，$A(x)$表示“x 是偶数”，$B(x)$表示“x 是奇数”。这时显然$\forall x\,(A(x)\vee B(x))$真，但$\forall x\,A(x)$假，$\forall x\,B(x)$也假，从而$\forall x\,A(x)\vee\forall x\,B(x)$假。

上文指出的证明逻辑蕴涵式“甲 $\models$乙”不能成立的方法十分重要，即只要给出一个个体域、一种解释和对自由变元（如果有的话）的一种赋值，它们使得“甲”为真，但使得“乙”为假。这种方法今后还会遇到，也可用来证明推理的无效。

第三式的讨论类似。若个体域 D 和解释 I 使$\exists x\,(A(x)\wedge B(x))$真，那么有 $d\in D$，使 $A(d)$，$B(d)$同时真，于是它们必使$\exists xA(x)\wedge\exists x\,B(x)$为真。与上面的反例一样，可说明$\exists xA(x)\wedge\exists x\,B(x)\models\exists x(A(x)\wedge B(x))$不能成立。因为“有整数是偶数”与“有整数是奇数”都是对的，但“有整数既是偶数又是奇数”则是荒谬的。

（7）$\forall x\,\forall yA(x,y)\dashv\vdash\forall y\,\forall x\,A(x,y)$

$\forall x\,\forall yA(x,y)\models\exists y\,\forall x\,A(x,y)$

$\exists y\,\forall xA(x,y)\models\forall x\,\exists y\,A(x,y)$

$\forall x\,\exists y\,A(x,y)\models\exists y\,\exists x\,A(x,y)$

$\exists x\,\exists y\,A(x,y)\dashv\vdash\exists y\,\exists x\,A(x,y)$

相邻的同名量词的次序无关紧要，不同名量词的次序是不可随意变更的，上面第三式指出的关系，我们已经在例 4-3 中看到过十分有说服力的例子。

（8）当 C 中无自由变元 x 时，

$\forall x(C\to A(x))\dashv\vdash C\to\forall x\,A(x)$

$\exists x(C\to A(x))\dashv\vdash C\to\exists x\,A(x)$

$\forall x\,(A(x)\to B(x))\models\forall x\,A(x)\to\forall x\,B(x)$

我们先来证明第一式。

$$\begin{aligned}\forall x(C\to A(x))&\dashv\vdash\forall x(\neg\,C\vee A(x))\\&\dashv\vdash\neg\,C\vee\forall x\,A(x)\\&\dashv\vdash C\to\forall x\,A(x)\end{aligned}$$

再来证明第三式。设个体域 D 和解释 I 下$\forall x\,(A(x)\to B(x))$真，即对任意 $d\in D$，$A(d)\to B(d)$真。为证$\forall xA(x)\to\forall xB(x)$在个体域 D 和解释 I 下真，设$\forall xA(x)$ 在域 D 和解释 I 下真，从而对任意 $d\in D$，$A(d)$均真。由 $A(d)\to B(d)$ 真及 $A\ (d)$真，可知对任意 $d\in D$，$B(d)$真，此即表明$\forall xB(x)$在域 D 解释 I 下真。第三式得证。该式之逆不成立。令 D 为整数集，$A\ (x)$，$B\ (x)$解释为“x 是偶数”和“x 是奇数”，这时$\forall xA(x)$假，从而$\forall xA(x)\to\forall x\,B(x)$真，但$\forall x(A(x)\to B(x))$假，因为“所有的偶数都是奇数”显然是荒谬的。

4.2.3 关于永真式的几个基本原理

在对谓词演算永真式进行等价变换时，常常要用到以下几个基本原理：代入原理，替换原理，对偶原理，改名原理等。

定义 4-5 设谓词公式 A 中含自由变元 x，设 t 为一个体项，且 t 中无自由变元为 A 中的约束变元，那么称 t **是在 A 中对 x 可代入的**，其代入实例记为 $A(t/x)$（代入的意义同前）。

由于约束变元可改名，因此总可对 A 中约束变元改名，使 t 成为对 x 是可代入的。

【例 4-11】 设公式 A 为$\exists y\ (x\neq y)$，它对多于一个元素的任何个体域都是真的。现对其中 x 作代入，只要代入的个体项 t 中不含 y，t 都是对 x 可代入的。否则却不然。例如取 t 为 y，代入后成为$\exists y\ (y \neq y)$，由于对变元的约束关系发生了变化，公式的意义完全不同了，成了一个永假式。如果有必要在$\exists y\ (x\neq y)$中对 x 代入 y，那么必须将$\exists y(x\neq y)$ 原有的约束变元 y 改名，例如改为$\exists z\ (x\neq z)$，再对 x 作代入，得到$\exists z(y\neq z)$。

定理 4-1 （**代入原理**）若 A 是永真式，那么对 A 中变元可代入的代入实例都是永真式。

由于 A 永真，因此它的取值与 A 中变元的取值无关，故其代入实例仍为永真式。

定理 4-2 （**替换原理**）设 A，D 为谓词公式，C 为 A 的子公式，且 $C \dashv\vdash D$。若 B 为将 A 中子公式 C 的某些出现（未必全部）替换为 D 后所得的公式，那么 $A \dashv\vdash B$。

证明参阅定理 3-3。

【例 4-12】 利用替换原理可由已知永真式导出其他永真式。

（1）由 4.2.2 节第（6）组第一式导出第四式。

证明 $\exists x\ (A(x)\vee B(x)) \dashv\vdash \exists x(\neg\ (\neg\ A(x)\wedge\neg\ B(x)))$

$\dashv\vdash \neg\ (\forall x(\neg\ A(x)\wedge\neg\ B(x)))$

$\dashv\vdash \neg\ (\forall x\neg\ A(x)\wedge\forall x\neg\ B(x))$

$\dashv\vdash \neg\ \forall x\neg\ A(x)\vee\neg\ \forall x\neg\ B(x)$

$\dashv\vdash \exists xA(x)\vee\exists x\ B(x)$

（2）可证对任意 $A(x)$，$B(x)$

$\exists x\ (A(x)\rightarrow B(x)) \dashv\vdash \forall xA(x)\rightarrow\exists x\ B(x)$

证明 $\exists x\ (A(x)\rightarrow B(x)) \dashv\vdash \exists x\ (\neg\ A(x)\vee B(x))$

$\dashv\vdash \exists x\neg\ A(x)\vee\exists x\ B(x)$

$\dashv\vdash \neg\ \forall xA(x)\vee\exists x\ B(x)$

$\dashv\vdash \forall xA(x)\rightarrow\exists x\ B(x)$

* **定义 4-6** 设 A 为仅含联结词$\neg$，$\vee$，$\wedge$的谓词公式，A^*为将 A 中符号$\vee$，$\wedge$，t，f，$\forall$，$\exists$分别换为$\wedge$，$\vee$，f，t，$\exists$，$\forall$后所得的公式，那么称 A^*为 A **的对偶式**。

注意，第三章中关于命题演算对偶式的一切讨论，即**对偶原理**，对于谓词演算都仍然成立，细节不赘。

【*例 4-13】 由对偶原理 $A \dashv\vdash \neg\ A^*(\neg\ p_1/p_1, \cdots, \neg\ p_n/p_n)$可立即推得$\neg\ \exists xp(x) \dashv\vdash \neg\ \neg\ \forall x\neg\ p(x) \dashv\vdash \forall x\neg\ p\ (x)$（4.2.2 节第（4）组永真式之第三式）。

利用“若 $A \vdash B$，则 $B^* \vdash A^*$”，可由 4.2.2 节第（6）组永真式的第二式$\forall x\ A(x)\vee\forall x\ B(x) \vdash\forall x\ (A(x)\vee B(x))$，直接导出第三式$\exists x\ (A(x)\wedge B(x)) \vdash\ \exists x\ A(x)\wedge\exists x\ B(x)$（或反之）。

利用“若 $A \dashv\vdash B$，则 $A^* \dashv\vdash B^*$”可由 4.2.2 节第（7）组永真式的第一式$\forall x\ \forall yA(x,y) \dashv\vdash \forall y\ \forall x\ A(x,y)$导出第五式$\exists x\ \exists\ y\ A(x,y) \dashv\vdash \exists y\ \exists\ x\ A(x,y)$（或反之）。

定理 4-3 （**改名原理**）若公式 $A(x)$中无自由变元 y，那么，

$\forall xA(x) \dashv\vdash \forall yA(y)$，$\exists xA(x) \dashv\vdash \exists yA(y)$

本定理由量词的意义立即可得。定理中对 $A\ (x)$的限制是不可忽略的。例如$\exists x\ (x \neq y)$与改名后的$\exists y(y \neq y)$显然不等价。

【例 4-14】 求证：对任意公式 $A(x,y)$，$\forall x\ \forall yA(x,y) \dashv\vdash \forall y\ \forall x\ A(y,x)$

证明 $\forall x\,\forall y A(x,y) \models\!\dashv \forall x\,\forall z\,A(x,z)$

$\models\!\dashv \forall y\,\forall z\,A(y,z)$

$\models\!\dashv \forall y\,\forall x\,A(y,x)$

在此过程的第一步中直接将 y 改为 x 是不行的，因为 $A(x,y)$中有自由变元 x（对$\forall yA(x,y)$而言），改名的前提得不到满足。

* 4.3 谓词公式的前束范式

在定理的机器证明中，需要消除谓词公式中的量词，因而需要将谓词公式中的量词前束化，即把公式中的量词均提取到公式的前部。

定义 4-7 公式 A' 称为公式 A 的**前束范式**（prenex normal forms），如果 $A \models\!\dashv A'$，且 A' 形如

$$Q_1x_1\cdots Q_nx_nB$$

其中 Q_1，…，Q_n 为量词$\forall$或$\exists$，B 称为**母式**，B 中无量词。当 B 为合取（析取）范式时，A' 称为 A 的**前束合取（析取）范式**。

对任何谓词公式均可作出其前束范式，因为我们总可以利用各组逻辑等价式将量词逐个移至公式的前部，其步骤是:

首先利用逻辑等价式将公式中联结词→，↔消除。

其次利用逻辑等价式将否定词¬ 深入到各原子公式之前。

最后，利用 4.2.2 节的第（5）组和第（6）组永真式将量词逐个移至公式前部。

应当注意，第（6）组第二、三两式不是逻辑等价式，$\forall x\,(A(x)\vee B(x)) \models \forall x\,A(x)\vee\forall x\,B(x)$，$\exists x\;A(x)\wedge\exists x\;B(x) \models \exists x\;(A(x)\wedge B(x))$ 都不能成立，因此，不能在化前束范式的过程中使用。然而对公式

$$\forall xA(x)\vee\forall x\,B(x),\quad \exists xA\,(x)\wedge\exists x\,B(x)$$

可如下将量词提出:

$\forall xA(x)\vee\forall x\,B(x) \models\!\dashv \forall xA(x)\vee\forall yB(y)$

$\models\!\dashv \forall x(A(x)\vee\forall yB(y))$

$\models\!\dashv \forall x\forall y\,(A(x)\vee B(y))$

类似地，可将$\exists xA(x)\wedge\exists x\,B(x)$化为等价的前束范式

$\exists xA(x)\wedge\exists x\,B(x) \models\!\dashv \exists xA(x)\wedge\exists y\,B(y)$

$\models\!\dashv \exists x(A(x)\wedge\exists yB(y))$

$\models\!\dashv \exists x\exists y(A(x)\wedge B(y))$

对于不同名量词的处理方式可仿此，例如:

$\forall xA(x)\wedge\exists x\,B(x) \models\!\dashv \forall xA(x)\wedge\exists yB(y)$

$\models\!\dashv \forall x(A(x)\wedge\exists yB(y))$

$\models\!\dashv \forall x\exists y\,(A(x)\wedge B(y))$

作上述处理时，要注意改名应满足的条件。

【例 4-15】 求以下两式的前束范式:

（1）$\forall xA(x)\rightarrow\exists x\,B(x)$

（2）$\forall x\forall y\,(\exists z(P(x,z)\wedge P(y,z))\rightarrow\exists z\,Q(x,y,z))$

解（1）$\forall xA(x)\rightarrow\exists x\,\mathrm{B}(x)\ \vDash\!\!\dashv\ \neg\,\forall xA(x)\vee\exists x\,B(x)$

$\vDash\!\!\dashv\ \exists x\neg\,A(x)\vee\exists x\,B(x)$

$\vDash\!\!\dashv\ \exists x(\neg\,A(x)\vee B(x))$

（或将母式表示为非范式的前束型 $\exists x(A(x)\rightarrow\mathrm{B}(x))$）

（2）$\forall x\forall y\,(\exists z(P(x,z)\wedge\mathrm{P}(y,z))\rightarrow\exists z\,Q(x,y,z))$

$\vDash\!\!\dashv\ \forall x\forall y\,(\neg\,\exists z(P(x,z)\wedge P(y,z))\vee\exists z\,Q(x,y,z))$

$\vDash\!\!\dashv\ \forall x\forall y\,(\forall z(\neg\,P(x,z)\vee\neg\,P(y,z))\vee\exists z\,Q(x,y,z))$

$\vDash\!\!\dashv\ \forall x\forall y\,(\forall z(\neg\,P(x,z)\vee\neg\,P(y,z))\vee\exists u\,Q(x,y,u))$

$\vDash\!\!\dashv\ \forall x\forall y\,\forall z\exists u\,(\neg\,P(x,z)\vee\neg\,P(y,z)\vee Q(x,y,u))$

（或 $\vDash\!\!\dashv\ \forall x\forall y\,\forall z\exists u\,(P(x,z)\wedge P(y,z)\rightarrow Q(x,y,u))$）

据以上讨论可知：

定理 4-4　（前束范式定理）对任意谓词公式均可作出其前束范式，进而作出其前束合取范式或前束析取范式。

4.4　练习

1．指出下列谓词公式中的量词及其辖域，指出各自由变元和约束变元，并回答它们是否是命题：

（1）$\forall x(P(x)\vee Q(x))\wedge R$（$R$ 为命题常元）

（2）$\forall x(P(x)\wedge Q(x))\wedge\exists xS(x)\rightarrow T(x)$

（3）$\forall x(\mathrm{P}(\mathrm{x})\rightarrow\exists y(B(x,y)\wedge Q(y))\vee T(y))$

（4）$P(x)\rightarrow(\forall y\exists x(P(x)\wedge B(x,y))\rightarrow P(x))$

2．对个体域{0，1}判定下列公式的真值，$E(x)$表示“x 是偶数”：

（1）$\forall x(E(x)\rightarrow\neg\,x=1)$

（2）$\forall x(E(x)\wedge\neg\,x=1)$

（3）$\exists x(E(x)\wedge x=1)$

（4）$\exists x(E(x)\rightarrow x=1)$

再将它们的量词消去，表示成合取或析取命题公式，鉴别你所确定的真值是否正确。

3．设整数集为个体域，判定下列公式的真值(*表示数乘运算)：

（1）$\forall x\,\exists y(x*y=x)$

（2）$\forall x\exists y\,(x*y=1)$

（3）$\forall x\,\exists y(x+y=1)$

（4）$\exists y\,\forall x\,(x*y=x)$

（5）$\exists y\,\forall x\,(x+y=1)$

4．量词$\exists!$表示“有且仅有”，$\exists!xP(x)$表示有且仅有一个个体满足谓词 $P(x)$。试用量词，$\forall$，$\exists$，等号“=”及谓词 $P(x)$，表示 $\exists!\ P\ (x)$，即写出一个通常的谓词公式使之与$\exists!xP\ (x)$具有相同的意义。

5．设个体域为整数集，试确定两个谓词 $P\,(x,y)$，分别使得下列两个蕴涵式假：

（1）$\forall x\,\exists!yP(x,y) \rightarrow \exists!y\forall x\,P(x,y)$

（2）$\exists!y\forall x\,P(x,y) \rightarrow \forall x\,\exists!yP(x,y)$

6．指定整数集的一个尽可能大的子集为个体域，使得下列公式为真：

（1）$\forall x(x>0)$

（2）$\forall x(x=5\vee x=6)$

（3）$\forall x\,\exists y(x+y=3)$

（4）$\exists y\,\forall x\,(x+y<0)$

7．以实数集为个体域，用谓词公式将下列语句形式化：

（1）如果两实数的平方和为零，那么这两个实数均为零。

（2）$f\,(x)$为一实函数当且仅当对每一实数 x 都有且只有一个实数 y 满足 $y=f\,(x)$（不得使用量词$\exists!$。“$f(x)$为实函数”可译为 $RF\,(f)$）。

8．用谓词公式将下列语句形式化：

（1）高斯是数学家，但不是文学家。

（2）没有一个奇数是偶数。

（3）一个数既是偶数又是质数，当且仅当该数为 2。

（4）有的猫不捉耗子，会捉耗子的猫便是好猫。

（5）党指向哪里，我们就奔向那里。

（6）发亮的东西不都是金子。

（7）不是所有的男人都至少比一个女人高，但至少有一个男人比所有的女人高。

（8）一个人如果不相信所有其他人，那么他也就不可能得到其他人的信任。

（9）君子坦荡荡，小人长戚戚。（孔子）

（10）谁要是游戏人生，他就一事无成；谁不能主宰自己，他就是一个奴隶。（歌德）

9．利用量词意义或利用已经证明了的永真式(逻辑蕴涵式，逻辑等价式)及几个基本原理，证明 4.2.2 节第（2）～（8）组永真式中尚未证明的各式。

10．证明下列逻辑蕴涵式及逻辑等价式（方法不限）：

（1）$\exists x\,P(x)\rightarrow\forall x\,Q(x) \vDash \forall x(A(x)\rightarrow Q(x))$

（2）$P(x)\wedge\forall x\,Q(x) \vDash \exists x\,(P(x)\wedge Q(x))$

（3）$\forall x\forall y(P(x)\vee Q(y)) \dashv\vDash \forall x\,P(x)\vee\forall y\,Q(y)$

（4）$\exists x\exists y(P(x)\wedge Q(y)) \dashv\vDash \exists x\,P(\mathrm{x})\wedge\exists y\,Q(y)$

（5）$\exists x\exists y(P(x)\rightarrow Q(y)) \dashv\vDash \forall x\,P(x)\rightarrow\exists y\,Q(y)$

（6）$\forall x\forall y(P(x)\rightarrow Q(y)) \dashv\vDash \exists x\,P(x)\rightarrow\forall y\,Q(y)$

11．试举出一个个体域及两种解释，分别证明第 2 题之（1）（2）的逆不能成立。

12．设个体域 $D=\{d_1,\cdots,d_n\}$，试用消去量词的方法证明下列基本逻辑等价式：

（1）$\neg\,\forall xA(x) \dashv\vDash \exists x\neg\,A(x)$

（2）$\forall xA(x)\wedge P \dashv\vDash \forall x(A(x)\wedge P)$（$P$ 为命题常元）

（3）$\forall xA(x)\vee\forall x\,B(x) \vDash\forall x(A(x)\vee\mathrm{B}(x))$

（4）$\exists xA(x)\vee\exists x\,B(x) \dashv\vDash \exists x(A(x)\vee B(x))$

*13．利用对偶原理“若 $A \dashv\vDash B$ 则 $A^* \dashv\vDash B^*$”及“若 $A \vDash B$，则 $B^* \vDash A^*$”，作出与 4.2.2 节（7）中各永真式相应的逻辑蕴涵式及逻辑等价式。

14. 用谓词公式写出 $\lim\limits_{x\to c} f(x)=k$ 的定义，并据此写出 $\lim\limits_{x\to c} f(x)\neq k$ 的意义（用自然语言叙述）。

15. 判别下列公式是否是可满足的，并说明理由：

（1）$\forall xP(x)\vee\exists y\neg P(y)$　　（2）$\forall xP(x)\wedge\exists y\neg P(y)$

（3）$\neg(P(a)\leftrightarrow\exists xP(x))$　　（4）$\neg(P(a)\wedge\exists xP(x))$

（5）$P(a)\rightarrow\neg\exists xP(x)$　　（6）$\forall xP(x)\rightarrow\neg P(a)$

16. 设个体域 $D=\{d_1,\cdots,d_n\}$，试用消去量词的方式证明：当 $A(x)$中无自由变元 y，$B(y)$中无自由变元 x 时，

$$\forall x\,\exists y\,(A(x)\wedge B(y))\models\exists y\forall x\,(A(x)\wedge B(y))$$

17. 求下列各式的前束合取范式：

（1）$\neg\,\forall x\,(A(x)\rightarrow\exists y\,B(y))$ ($A(x)$中无自由变元 y)

（2）$\forall x\,(A(x)\rightarrow\exists y\,B(x,y))$ ($A(x)$中无自由变元 y)

（3）$\forall x\forall y\,(\exists zA(x,y,z)\leftrightarrow\exists z\,B(x,y,z))$

（4）$\exists x(\neg\,\exists y\,A(x,y)\rightarrow(\exists z\,B(z)\rightarrow C(x)))$ ($A(x,y)$中无自由变元 z)

（5）$\neg\,\forall x(\exists yA(x,y)\rightarrow\exists x\forall y(\,B(x,y)\wedge\forall y(A(y,x)\rightarrow B(x,y))))$

*第 5 章　形式系统与推理技术

读者已经看到，逻辑代数的确揭示了人类思维的基本规律，例如 $\models A \vee \neg A$（排中律），$\models \neg (A \wedge \neg A)$（矛盾律），$A \wedge (A \rightarrow B) \models B$（假言推理），$A \rightarrow (B \wedge \neg B) \models \neg A$（归谬推理），$(A \vee B) \wedge (A \rightarrow C) \wedge (B \rightarrow C) \models C$（穷举推理）；逻辑代数还提供了真值计算、代入、替换、对偶等演算手段，可用于对其他思维规律的探求。但是，这与数理逻辑所追求的形式化、公理化的目标相去甚远。

20 世纪初，数理逻辑研究的一个重要目的在于建立一个严密的数学体系,来刻画人的思维的规律。这个体系以符号语言来表达；以若干表示最基本逻辑规律的公式（永真式）为基础，称为**公理**（axioms）；以若干可对公式进行重写的规则（确保由永真式重写出永真式），作为系统内公式变换的依据，称为**推理规则**（rules of reference）。系统内推演的全部依据是符号的形式，而不是别的任何东西，并且系统能导出且只能导出反映人们思维正确规律的永真式，进而成为人类进行逻辑推理的一个框架，它保证在前提正确的条件下，总得出正确的推理结果。这就是所谓数理逻辑的形式系统。

本章先推出一个经典简明的**谓词演算形式系统** FC（first order predicate calculus formal system），借以介绍形式系统的相关概念。然后较完整地讨论一个相对实用的形式系统——**自然推理系统**，也称**自然演绎系统**（natural deduction system），简记为 ND。

5.1　谓词演算形式系统 FC

5.1.1　FC 的基本构成

谓词演算形式系统 FC 由两个部分组成：（1）谓词演算形式系统 FC 的语言部分。（2）谓词演算形式系统 FC 的理论部分。

1．谓词演算形式系统 FC 的语言部分

FC 的符号表：

个体变元　$x, y, z, u, v, w, \cdots$

个体常元　$a, b, c, d, e, \cdots$

个体间运算符号（函数符）

$$f^{(n)}, g^{(n)}, h^{(n)}, \cdots$$

其中 n 为任一正整数，表示函数的元数。

谓词符号　$P^{(n)}, Q^{(n)}, R^{(n)}, S^{(n)}, \cdots$

其中 n 为非负整数，表示谓词的元数。当 $n=0$ 时谓词符退化为一个命题常元。

真值联结词　$\neg$，$\rightarrow$

量词　$\forall$　(把$\exists v$ 看作$\neg \forall v \neg$ 的缩写)

括号　(　，　)

FC 的更高一级的语言成分有“个体项”和“公式”。

个体项(terms，以下简称**项**)归纳定义如下：

（1）个体变元和个体常元是项。

（2）对任意正整数 n，如果 $f^{(n)}$为一 n 元函数符，t_1，…，t_n 为项，那么 $f^{(n)}(t_1,\cdots,t_n)$也是项。

（3）除有限次使用（1），（2）条款所确定的符号串外，没有别的东西是个体项。

合式公式(well found formula，以下简称**公式**)归纳定义如下：

（1）对任意非负整数 n，如果 $P^{(n)}$为一 n 元谓词符，t_1，…，t_n 为项，那么 $P^{(0)}$（命题常元）和 $P^{(n)}(t_1,\cdots,t_n)$（$n>0$）是公式。

（2）如果 A，B 为公式，v 为任一个体变元，那么$(\neg A)$，$(A\rightarrow B)$，$(\forall vA)$ (或$(\forall vA(v))$)均为公式。

（3）除有限次使用（1），（2）条款可确认为公式的符号串外，没有别的东西是公式。

公式中括号的省略原则同前。约束变元、自由变元及辖域等概念照旧。今后，我们常用大写拉丁字母 A，B，C，…表示任意公式，用 $A(v)$等表示公式 A 中含有自由变元 v；常用大写希腊字母 Γ 表示一个公式的集合，Γ 可以是空集合；用 Γ；A 表示在公式集合 Γ 中添入公式 A，即 $\Gamma\cup\{A\}$。

此外，我们还需要以下定义。

定义 5-1 设 $v_1,\cdots,v_n$ 是公式 A 中的自由变元，那么公式$\forall v_1\cdots\forall v_nA$(或$\forall v_1\cdots\forall v_nA(v_1,\cdots,v_n)$称为 A 的**全称封闭式**（generalization clusure）。A 不含自由变元时，A 的全称封闭式为其自身。

2．谓词演算形式系统 FC 的理论部分

FC 的公理系统包括以下公理（A，B，C 为任意公式）：

$A1.$ $A\rightarrow(B\rightarrow A)$

$A2.$ $(A\rightarrow(B\rightarrow C))\rightarrow((A\rightarrow B)\rightarrow(A\rightarrow C))$

$A3.$ $(\neg A\rightarrow\neg B)\rightarrow(B\rightarrow A)$

$A4.$ $\forall xA(x)\rightarrow A(t/x)$（$x$ 为任一变元，t 为对 x 可代入的项）。

$A5.$ $\forall x\,(A(x)\rightarrow B(x))\rightarrow(\forall xA(x)\rightarrow\forall x\,B(x))$（$x$ 为任一变元）。

$A6.$ $A\rightarrow\forall x\,A$（A 中无自由变元 x）。

$A7.$ 以上公式的全称封闭式都是 FC 的公理。

推理规则：$\dfrac{A,A\rightarrow B}{B}$(分离规则)。

$A1\sim A3$ 为命题演算的重言式，也是谓词演算的永真式。$A4\sim A7$ 是谓词演算的永真式。它们的永真性在第 3 章和第 4 章已经得到证实。

5.1.2 系统内的推理：证明与演绎

定义 5-2 公式序列 $A_1,A_2,\cdots,A_m$ 称为 A_m 的一个**证明**（proof），如果 A_i $(1\leqslant i\leqslant m)$或者是公理，或者由 $A_{j1}\cdots$，A_{jk}(j1,$\cdots$,$jk<$i)用推理规则推得。当这样的证明存在时，称 A_m 为系统的**定理**（theorems），记为 $\vdash_* A_m$,（*为所讨论的系统名），或简记为 $\vdash A_m$。

定义 5-3 设Γ为一公式集合。公式序列 A_1，A_2，…，A_m 称为 A_m 的以Γ为前提的**演绎**

（diduction），如果 A_i ($1 \leqslant i \leqslant m$)或者是 Γ 中公式，或者是公理，或者由 $A_{j1}\cdots,A_{jk}(j1,\cdots,jk<i)$ 用推理规则导出。当有这样的演绎时，A_m 称为 Γ 的**演绎结果**，记为 $\Gamma \vdash_* A_m$，（*为所讨论的系统名），或简记为$\Gamma \vdash A_m$。称Γ和Γ的成员为 A_m 的**前提**(hypothesis)。

显然，证明是演绎在 Γ 为空集时的特例。注意，$\vdash A_m$ 与 $\models A_m$ 是不同的，$\Gamma \vdash A_m$ 与 $\Gamma \models A_m$ 也是不同的，前者都是指形式系统内的推理关系（证明与演绎），而后者则是指公式的真值特性及真值间的逻辑关系。当然，它们之间应当是一致的，这正是我们建立形式系统所想要做到的。

例 5-1、例 5-2 和例 5-3 是 FC 系统内证明和演绎的例子。

【例 5-1】 证明：$\vdash_{FC} A \rightarrow A$

证明 其证明序列是

（1）$(A \rightarrow ((A \rightarrow A) \rightarrow A)) \rightarrow ((A \rightarrow (A \rightarrow A)) \rightarrow (A \rightarrow A))$　公理 *A*2

（2）$A \rightarrow ((A \rightarrow A) \rightarrow A)$　公理 *A*1

（3）$(A \rightarrow (A \rightarrow A)) \rightarrow (A \rightarrow A)$　对(1) (2)用分离规则

（4）$A \rightarrow (A \rightarrow A)$　公理 *A*1

（5）$A \rightarrow A$　对(3)(4)用分离规则

【例 5-2】 证明 $\vdash_{Fc} \neg B \rightarrow (B \rightarrow A)$。

证明 其证明序列是

（1）$\neg B \rightarrow (\neg A \rightarrow \neg B)$　公理 *A*1

（2）$(\neg A \rightarrow \neg B) \rightarrow (B \rightarrow A)$　公理 *A*3

（3）$((\neg A \rightarrow \neg B) \rightarrow (B \rightarrow A)) \rightarrow (\neg B \rightarrow ((\neg A \rightarrow \neg B) \rightarrow (B \rightarrow A)))$　公理 *A*1

（4）$\neg B \rightarrow ((\neg A \rightarrow \neg B) \rightarrow (B \rightarrow A))$　对(2)(3)用分离规则

（5）$(\neg B \rightarrow ((\neg A \rightarrow \neg B) \rightarrow (B \rightarrow A))) \rightarrow ((\neg B \rightarrow (\neg A \rightarrow \neg B)) \rightarrow (\neg B \rightarrow (B \rightarrow A)))$　公理 *A*2

（6）$(\neg B \rightarrow (\neg A \rightarrow \neg B)) \rightarrow (\neg B \rightarrow (B \rightarrow A))$　对(4)(5)用分离规则

（7）$\neg B \rightarrow (B \rightarrow A)$　对(1)(6)用分离规则

【例 5-3】 在 FC 中对任意公式 *A*，*B*，*C*，证明：

$\{A, B \rightarrow (A \rightarrow C)\} \vdash_F B \rightarrow C$

证明 其演绎序列为

（1）A　前提

（2）$B \rightarrow (A \rightarrow C)$　前提

（3）$A \rightarrow (B \rightarrow A)$　公理 *A*1

（4）$B \rightarrow A$　对(1) (3)用分离规则

（5）$(B \rightarrow (A \rightarrow C)) \rightarrow ((B \rightarrow A) \rightarrow (B \rightarrow C))$　公理 *A*2

（6）$(B \rightarrow A) \rightarrow (B \rightarrow C)$　对(2) (5)用分离规则

（7）$B \rightarrow C$　对(4) (6)用分离规则

5.1.3 FC 的重要性质

现在我们对 FC 的重要性质作一些讨论。

定理 5-1 （合理性，sondness）若公式 *A* 是系统 FC 的定理，则 *A* 为永真式。若 *A* 是公

式集 Γ 的演绎结果，那么 A 是 Γ 的逻辑结果。即

若 $\vdash_F A$，则 $\models A$。

若 $\Gamma \vdash_F A$，则 $\Gamma \models A$。

本定理的证明是容易的，因为

（1）易证公理 $A1$，$A2$，$A3$，$A4$，$A5$，$A6$，$A7$ 是永真的。

（2）易证分离规则是“保真”的，即当 A，$A\rightarrow B$ 真时，B 亦真。

从而由公理和分离规则逐步导出的公式是永真的；由Γ中公式、公理及分离规则导出的公式，在Γ中公式均真时也真。

合理性定理的逆否命题可表述为

若 $\Gamma \models A$ 不成立，则 $\Gamma \vdash_{FC} A$ 不成立。

因此，欲证 $\Gamma \vdash_{FC} A$ 不成立，只要找出一个个体域、一种解释和一种变元取值，它满足 Γ 的每一公式，但却弄假 A。也就是说，要证明由前提集合Γ推导出结论 A 的推理是无效的，只要举出一个反例（一个个体域、一种解释和一种变元取值），使得前提成立而结论不成立。

作为合理性定理的自然推论我们：

定理 5-2 FC 是一致的，即没有公式 A 使得 $\vdash_{FC} A$ 与 $\vdash_{FC} \neg A$ 同时成立。

证明 若不然，据合理性定理有 $\models A$ 和 $\models \neg A$，但这是不可能的。

更深入的研究表明，FC 还是完备的。

定理 5-3 （完备性，completeness）若公式 A 永真，则 A 必为 FC 的定理；若公式 A 是公式集Γ的逻辑结果，那么 A 必为 Γ 的演绎结果。即

若 $\models A$，那么 $\vdash_{FC} A$。

若 $\Gamma \models A$，那么 $\Gamma \vdash_{FC} A$。

本定理的证明是相当复杂的，略去。

由于{¬，→}是完备联结词组，并且由于全称量词∀可以表示存在量词∃，因此所有永真式均可用只含联结词¬，→和全称量词 ∀的形式来表示，从这个意义上说，在 FC 中可以推出前述系统中的一切永真式。这表明 FC 是一个成功和简化了的谓词演算形式系统。

关于系统 FC 的性质还有一些重要定理，它们被称为导出规则，可以用来简化系统内的推理。

定理 5-4 （演绎定理）对任意公式集Γ和公式 A，B，$\Gamma \vdash A\rightarrow B$ 当且仅当

$\Gamma;\ A \vdash B$

（当 $\Gamma=\varnothing$ 时，$\vdash A\rightarrow B$ 当且仅当 $\{A\} \vdash B$）

证明 设$\Gamma \vdash A\rightarrow B$ 的演绎序列是

$$A_1, A_2, \cdots, A_n(=A\rightarrow B)$$

那么可作出由Γ ；A 推出 B 的演绎：

$A_1, A_2, \cdots, A_n(=A\rightarrow B)$ ，A（前提），B（对 A_n, A 用分离规则）

反之，设Γ ；$A \vdash B$，其演绎是

$A_1, A_2, \cdots, A_{m-1}, A_m(=B)$

对演绎长度归纳证明 $\Gamma \vdash A\rightarrow B$。

（1）若 B 为公理或 Γ 中成员，那么可作出由 Γ 导出 $A\rightarrow B$ 的演绎如下：

$B\rightarrow(A\rightarrow B)$（公理 $A1$），B，$A\rightarrow B$（对前两式用分离规则）

（2）若 B 为 $A_i, A_j(=A_i\to B)$用分离规则推得：

由于 $i<m, j<m$，据归纳假设有 Γ 导出 A_i, A_j的两个演绎，分别记为

$$C_1, C_2, \cdots, C_r(=A\to A_i)$$

$$D_1, D_2, \cdots, D_l(=A\to A_j=A\to(A_i\to B))$$

用它们我们可以作出Γ导出 $A\to B$ 的演绎：

$C_1, C_2, \cdots, C_r, D_1, D_2, \cdots, D_l, (A\to(A_i\to B))\to((A\to A_i)\to(A\to B))$（公理 $A2$），$(A\to A_i)\to(A\to B)$（对前两式用分离规则），$A\to B$（对上式与 C_r用分离规则）

定理证毕。

【例 5-4】 证明：对任意公式 A，B，C，有

$$\vdash_{PC}(A\to B)\to((B\to C)\to(A\to C))$$

证明 根据演绎定理只需证

$$\{(A\to B), (B\to C), A\}\vdash C$$

（1）$A\to B$　　前提

（2）$B\to C$　　前提

（3）A　　前提

（4）B　　对（1），（3）用分离规则

（5）C　　对（2），（4）用分离规则

很明显，利用演绎定理使证明大大简化。

定理 5-5 （归谬定理）对任何公式集 Γ 和公式 A，B，若

$$\Gamma;\ A\vdash\neg B\ ,\ \Gamma;\ A\vdash B,$$

那么$\Gamma\vdash\neg A$。

由 $A\to(B\wedge\neg B)\models\neg A$（归谬推理）和完备性定理，本定理不难理解。

【例 5-5】 求证：对任何公式 A，有

$$\vdash\neg\neg A\to A\ \ \vdash A\to\ \neg\neg A$$

证明 据演绎定理，为证 $\vdash\neg\neg A\to A$，只需证明$\{\neg\neg A\}\vdash A$。由于

$$\{\neg\neg A, \neg A\}\vdash\neg\neg A\ 且\{\neg\neg A, \neg A\}\vdash\neg A$$

因此由归谬定理得$\{\neg\neg A\}\vdash A$。

由于已证 $\vdash\neg\neg A\to A$，故已有 $\vdash\neg\neg\neg A\to\neg A$。此外，$(\neg\neg\neg A\to\neg A)\to(A\to\neg\neg A)$ 为公理 $A3$，因而可用分离规则得 $\vdash A\to\ \neg\neg A$ 。

定理 5-6 （穷举定理）对任何公式集，公式 A，B，若$\Gamma;\ \neg A\vdash B$，$\Gamma;\ A\vdash B$，则 $\Gamma\vdash B$。

由$(A\vee B)\wedge(A\to C)\wedge(B\to C)\models C$（穷举推理）和完备性定理，本定理也不难理解。

【例 5-6】 对任何公式 A，B，C，求证

$$\vdash(A\to C)\to((B\to C)\to((\neg A\to B)\to C))$$

证明 据演绎定理，只需证$\{A\to C, B\to C, \neg A\to B\}\vdash C$

由于，$\{A\to C, B\to C, \neg A\to B, A\}\vdash C$ 是显然的，而且$\{A\to C, B\to C, \neg A\to B, \neg A\}\vdash C$ 也是易证的，因此由穷举定理即得欲证。

定理 5-7 （全称引入规则）对 F 中任一公式 A，变元 v，如果 $\vdash A$，那么 $\vdash\forall vA$。

证明 对 A 的证明序列长度 l 归纳。

$l=1$ 时 A 为公理，$\forall vA$ 为 A 的一个全称化（当 A 中有自由变元 v 时），仍为一公理；或者$\forall vA$ 由 A 及公理 $A6.A\rightarrow\forall vA$（当 A 中无自由变元 v 时）推得。总之此时有 $\vdash\forall vA$。

设 $l<k$ 时命题真，而 A 的证明序列是 $A_1,A_2,\cdots,A_k(=A)$。若 A_k 为公理，那么同上可证 $\vdash\forall vA$。若 A_k 由 A_i 与 $A_j(i,j<k)$用分离规则得出，那么 A_j 必为 $A_i\rightarrow A_k$ 形。据归纳假设，可知 $\vdash\forall vA_i$ 以及 $\vdash\forall v(A_i\rightarrow A_k)$。另一方面，我们有公理

$$\forall v(A_i\rightarrow A_k)\ \rightarrow(\forall vA_i\rightarrow\forall vA_k)$$

由它和$\forall v(A_i\rightarrow A_k)$用分离规则推出$\forall vA_i\rightarrow\forall vA_k$，对$\forall vA_i\rightarrow\forall vA_k$ 及$\forall vA_i$ 再次使用分离规则即得$\forall vA_k(=\forall vA)$。

归纳完成，$\vdash A$ 蕴涵 $\vdash\forall vA$ 得证。

定理 5-7 还可推广到演绎上来。

定理 5-8 （推广的全称引入规则）对 FC 的任何公式集Γ，公式 A 以及不在Γ的任一公式里自由出现的变元 v，如果$\Gamma\vdash A$，那么$\Gamma\vdash\forall vA$。

证明留给读者。需要强调指出的是，定理中的条件“v 不是 Γ 中任一公式的自由变元”是至关重要的，缺少这一要求，命题不能成立。例如我们知道

$$\{y=5\}\vdash y^2=25$$

但无论如何不能认为下式是正确的：

$$\{y=5\}\vdash\forall y(y^2=25)$$

本定理的数学背景是：当我们用一组与变元 v 无关的前提演绎出 $A(v)$，表明我们已对任意的 v 导出 $A(v)$，因而事实上我们已得到$\forall vA(v)$。若 Γ 中有 $B(v)$含自由变元 v，那么我们是在前提 $B(v)$之下演绎得 $A(v)$，故 v 并非是任意的，自然不能因此而得$\forall v\,A(v)$ 。

【例 5-7】 对任何公式 A，B 及任意变元 x 证明：

$$\forall x(A(x)\rightarrow B(x))\rightarrow(\exists xA(x)\rightarrow\exists x\,B(x))$$（$\exists$为$\neg\,\forall\neg$ 的简记符）

证明 据演绎定理只要证

$$\{\forall x(A(x)\rightarrow B(x)),\exists x\,A(x)\}\vdash\exists xB(x)$$

（1）$\forall x(A(x)\rightarrow B(x))$　　前提

（2）$\exists x\,A(x)$　　前提

（3）$\forall x(A(x)\rightarrow B(x))\rightarrow(A(x)\rightarrow B(x))$　　公理 $A4$

（4）$A(x)\rightarrow B(x)$　　对（1），（3）用分离规则

（5）$(A(x)\rightarrow B(x))\rightarrow(\neg\,B(x)\rightarrow\neg\,A(x))$　　重言式

（6）$\neg\,B(x)\rightarrow\neg\,A(x)$　　对（4），（5）用分离规则

（7）$\forall x(\neg\,B(x)\rightarrow\neg\,A(x))$　　定理 5-8

（8）$\forall x(\neg\,B(x)\rightarrow\neg\,A(x))\rightarrow(\forall x\neg\,B(x)\rightarrow\forall x\neg\,A(x))$　　公理 $A5$

（9）$\forall x\neg\,B(x)\rightarrow\forall x\neg\,A(x)$　　对（7），（8）用分离规则

（10）$(\forall x\neg\,B(x)\rightarrow\forall x\neg\,A(x))\rightarrow(\neg\,\forall x\neg\,A(x)\rightarrow\neg\,\forall x\neg\,B(x))$　　公理 $A3$

（11）$\neg\,\forall x\neg\,A(x)\rightarrow\neg\,\forall x\neg\,B(x)$　　对（9），（10）用分离规则

（12）$\exists xA(x)\rightarrow\exists x\,B(x)$　　$\exists x$ 是 $\neg\,\forall x\neg$ 的缩写

（13）$\exists x\,B(x)$　　对（2），（12）用分离规则

在许多场合下，使用存在量词是方便的，对 $\exists$ 有下列重要事实。

定理 5-9 （存在消除规则）设 A，B 为任意公式，变元 x 是公式 A、但不是公式 B 的自由变元，那么当 $\vdash \exists x A(x)$，$A(x) \vdash B$ 同时成立时，应有 $\vdash B$ 。

它也有一个推广形式。

定理 5-10 （推广的存在消除规则）设 Γ 为一公式集，A，B 为任意公式，变元 x 是 A 的自由变元，但不是 Γ 中任一公式以及公式 B 的自由变元那么当 $\Gamma \vdash \exists x A(x)$ ，$\Gamma \cup \{A(x)\} \vdash B$ 同时成立时，应有 $\Gamma \vdash B$ 。

证明 由$\Gamma \cup \{A(x)\} \vdash B$ 及演绎定理，得 $\Gamma \vdash A(x) \rightarrow B$。由于$\Gamma$中无自由变元 x，据定理 5-8 有$\Gamma \vdash \forall x(A(x) \rightarrow B)$ 。据例 5-7 及 $\Gamma \vdash \forall x(A(x) \rightarrow B)$，$\Gamma \vdash \exists x A(x)$，可得 $\Gamma \vdash \exists x B$。另一方面，由于 B 中无自由变元 x，$\neg B \rightarrow \forall x \neg B$ 为公理 $A6$，从而有$\neg \forall x \neg B \rightarrow B$ ，即 $\exists x B \rightarrow B$。据此与 $\Gamma \vdash \exists x A$ 即得 $\Gamma \vdash B$ 。

本定理之所以称为“存在指定规则”、“存在消除规则”，是因为它可以理解为：当有了演绎结果 $\exists x A(x)$后，便可将 $A(x)$看作附加的演绎前提（从而消除了量词），当由此推得与 x 无关的 B 时，可确认 B 为原前提的演绎结果，B 不再依赖于 A（仅仅依赖 $\exists x A$，从而仅依赖原前提）。这就像在数学论证中我们常常做的那样：当已经知道方程 $F(x)=0$ 有根时（即$\exists x\,(F(x)=0)$），不妨设有根 x_0，然后据 $F(x_0)=0$ 作进一步的推理。如果得出的结论与 x_0 无关，那么说明所得结论不依赖于“根是什么”，而仅依赖于“有根”这一事实。这就是说，这个结论是$\exists x\,(F(x)=0)$及原前提的演绎结果，“不妨设 $F(x_0)=0$”的证明过程是合理的。

5.2 自然推理形式系统 ND

对 FC 我们没有做过多的系统内部的推演，因为它过于复杂，例 5-1、例 5-2 和例 5-3 已充分显示出这一点。在 FC 中推演复杂的原因主要有两个：一是 FC 追求简洁，只用两个联结词、一个量词和一条推理规则；二是推理规则与人的日常推理特点没有联系。如果使用 5 个联结词、两个量词和多条推理规则，那么会使系统的描述能力更强、更自然。此外，如果模仿人的数学推理的常用手段，允许在推理中引入假设，将使得推理更加高效和便捷。人们常用的那些假设包括：

（1）为证 $A \rightarrow B$，常假设 A 而去证明 B，如果成功，则完成了 $A \rightarrow B$ 的证明（证明结果不再依赖假设 A）。

（2）为证 A，常假设$\neg A$ 而去证明可导出矛盾（假命题 f），如果成功，则完成了 A 的证明（证明结果不再依赖假设$\neg A$）。

（3）已证（或已知）$A \vee B$，欲证 C，常假设 A 和 B 分别去证明 C，如果都能成功，则完成了 C 的证明（证明结果不再依赖假设 A，也不依赖假设 B）。

（4）已证（或已知）$\exists v A(v)$，常假设 $A(v_0)$，去证明 C（它与 v_0 无关），如果能成功，则完成了 C 的证明（证明结果不再依赖假设 $A(v_0)$）。

如果说 F 是一个研究系统，那么 ND 可以说是一个应用系统。为了便于实际应用中对问题的描述，ND 采用五个真值联结词；为了便于推理，ND 采用少数公理，多数规则，并且把人的推理手段用推理规则加以体现，因而它被称为**自然推理系统**（Natural Deduction system），简记为 ND。

5.2.1 ND 的基本构成

自然推理系统 ND 的语言与 FC 大同小异，主要区别是 ND 中使用 5 个真值联结词。其推理部分与 FC 相去甚远。由于强调人的自然推理，ND 更注重演绎，它的公理表示为 $\Gamma \vdash \Phi$ 形，例如 用 $\Gamma; A \vdash A$ 代替 $A \to A$；其推理规则形如

$$\frac{\Gamma_1 \vdash \Phi_1, \Gamma_2 \vdash \Phi_2, \cdots, \Gamma_k \vdash \Phi_k}{\Gamma \vdash \Psi}$$

例如用 $\dfrac{\Gamma \vdash A \to B, \Gamma \vdash A}{\Gamma \vdash B}$ 取代分离规则。

ND 的理论部分组成如下。

公理模式只有一个

$$\Gamma; A \vdash A$$

推理规则模式为 18 个。

（1）假设引入规则

$$\frac{\Gamma \vdash B}{\Gamma; A \vdash B}$$

它源于重言式 $B \to (A \to B)$。规定了假设引入的合理性。

（2）假设消除规则

$$\frac{\Gamma; A \vdash B, \Gamma; \neg A \vdash B}{\Gamma \vdash B}$$

它源于重言式 $\neg A \to (A \to B)$ 上述两条规则反映了人在推理中常用的模式：分别情况进行证明。在假设 A 与 $\neg A$ 后均能导出 B，则 B 可推得（不依赖假设 A 或 $\neg A$）。

（3）$\vee$ 引入规则

$$\frac{\Gamma \vdash A}{\Gamma \vdash A \vee B}, \frac{\Gamma \vdash B}{\Gamma \vdash A \vee B}$$

它们源于重言式 $A \to A \vee B$ 和 $B \to A \vee B$。它们可以改用更强的形式

$$\frac{\Gamma; \neg B \vdash A}{\Gamma \vdash A \vee B}, \frac{\Gamma; \neg A \vdash B}{\Gamma \vdash A \vee B}$$

这是由于 $(\neg A \to B) \leftrightarrow A \vee B$ 为永真式。在自然推理中人们常用如下方式：“欲证 $A \vee B$，可设 $\neg A (\neg B)$ 而证 $B(A)$。

（4）$\vee$ 消除规则

$$\frac{\Gamma; A \vdash C, \Gamma; B \vdash C, \Gamma \vdash A \vee B}{\Gamma \vdash C}$$

这是重言式 $(A \vee B) \wedge (A \to C) \wedge (B \to C) \to C$ 的演绎表示形式，它也反映了数学推理中分别情况进行证明的思想。如果接受 $\Gamma \vdash A \vee \neg A$，那么假设消除规则只是本规则的特例。

（5）$\wedge$ 引入规则

$$\frac{\Gamma \vdash A, \Gamma \vdash B}{\Gamma \vdash A \wedge B}$$

它依据重言式 $A \to (B \to (A \wedge B))$。

（6）$\wedge$ 消除规则

$$\frac{\Gamma \vdash A \wedge B}{\Gamma \vdash A}, \quad \frac{\Gamma \vdash A \wedge B}{\Gamma \vdash B}$$

它们依据重言式 $A \wedge B \rightarrow A$，$A \wedge B \rightarrow B$。

（7）$\rightarrow$引入规则

$$\frac{\Gamma; A \vdash B}{\Gamma \vdash A \rightarrow B}$$

此即演绎定理。为证 $A \rightarrow B$，人们常以 A 为假设而证 B。

（8）$\rightarrow$消除规则

$$\frac{\Gamma \vdash A \rightarrow B, \Gamma \vdash A}{\Gamma \vdash B}$$

此即分离规则。

（9）$\neg$ 引入规则

$$\frac{\Gamma; A \vdash B, \Gamma; A \vdash \neg B}{\Gamma \vdash \neg A}, \quad \frac{\Gamma; A \vdash f}{\Gamma \vdash \neg A}$$

这一规则反映了数学推理的反证法的基本思想。为证$\neg A$，假设 A 导出矛盾 $B \wedge \neg B$。容易验证永真式$(A \rightarrow B) \wedge (A \rightarrow \neg B) \rightarrow \neg A$。

（10）$\neg$ 消除规则

$$\frac{\Gamma \vdash A, \Gamma \vdash \neg A}{\Gamma \vdash B}$$

它源于重言式 $A \rightarrow (\neg A \rightarrow B)$。

（11）$\neg\neg$ 引入规则

$$\frac{\Gamma \vdash A}{\Gamma \vdash \neg\neg A}$$

（12）$\neg\neg$ 消除规则

$$\frac{\Gamma \vdash \neg\neg A}{\Gamma \vdash A}$$

规则（11）与（12）源于重言式 $A \leftrightarrow \neg\neg A$。

（13）$\leftrightarrow$引入规则

$$\frac{\Gamma \vdash A \rightarrow B, \Gamma \vdash B \rightarrow A}{\Gamma \vdash A \leftrightarrow B}$$

（14）$\leftrightarrow$消除规则

$$\frac{\Gamma \vdash A \leftrightarrow B}{\Gamma \vdash A \rightarrow B}, \quad \frac{\Gamma \vdash A \leftrightarrow B}{\Gamma \vdash B \rightarrow A}$$

规则（13）、（14）源于重言式$(A \leftrightarrow B) \leftrightarrow (A \rightarrow B) \wedge (B \rightarrow A)$。

（15）$\forall$引入规则

$$\frac{\Gamma \vdash A}{\Gamma \vdash \forall v A} (v \text{ 在 } A \text{ 中无自由出现})$$

$$\frac{\Gamma \vdash A(v)}{\Gamma \vdash \forall v A(v)} (v \text{ 在 } \Gamma \text{ 中无自由出现})$$

本规则依据关于 FC 的公理 A6 和定理 5-8。这一规则反映了数学推理中的下述做法：为证$\forall vA(v)$，只要排除对变元 v 的任何限定（即与任一前提无关），不失一般性地证明对任意 v，$A(v)$均真。

（16）∀消除规则

$$\frac{\Gamma \vdash \forall vA(v)}{\Gamma \vdash A(t/v)} \ (t \text{ 对 } v \text{ 可代入})$$

它依据 FC 的公理$\forall xA(x)\rightarrow A(t/x)$（$x$ 为任一变元，t 为对 x 可代入的项）。

（17）∃引入规则

$$\frac{\Gamma \vdash A(t)}{\Gamma \vdash \exists vA(v/t)}$$

它依据永真式$A(t)\rightarrow\exists vA(v/t)$（这里 v/t 表示将项 t 的所有出现改为变元 v，t 对 v 可代入）。

（18）∃消除规则

$$\frac{\Gamma \vdash \exists vA(v) \ , \ \Gamma; A(e/v) \vdash C}{\Gamma \vdash C}$$

这里 e 为Γ及公式 A，C 中均无出现的常元。它来源于人们在数学中常用的一条引进假设进行推理的规则：当我们有了$\exists vA(v)$后，便可将 $A(e)$看作附加的演绎前提，当得到与 e 无关的 C 时，可确认 C 已推出，即它并不依赖于 A 而成立。这就像数学证明中我们常做的那样：当推知方程 $F(x)=0$ 有根（即$\exists x(F(x)=0)$）时，可设这个根为 x_0（即 $F(x_0)=0$），然后再据此去证所需的结论，只要所证结论与 x_0 的性质（除 x_0 为 $F(x)=0$ 的根这一性质）无关，它就是有效的演绎结果。

5.2.2 ND 的系统内推理及性质

定义 5-4 在 ND 中，称 A 为Γ的**演绎结果**（deductive consequences），即$\Gamma \vdash_{ND} A$（以下将 ND 省略），如果存在序列

$$(\Gamma = \Gamma_1) \ \Gamma_1 \vdash A_1, \ \Gamma_2 \vdash A_2, \ \cdots, \ \Gamma_n \vdash A_n (\Gamma_n = \Gamma, A_n = A)$$

使得$\Gamma_i \vdash A_i (1 \leqslant i \leqslant n)$或者是公理，或者是$\Gamma_j \vdash A_j (j<i)$，或者是对$\Gamma_{j1} \vdash A_{j1}, \cdots, \Gamma_{jk} \vdash A_{jk} (j_1, \cdots, j_k<i)$使用推理规则导出的。称 A 为 ND 的定理，如果有$\Gamma \vdash A$ 且$\Gamma = \varnothing$。

下列例子可说明 ND 中的推演过程及风格。

【例 5-8】 证明：对任一 ND 的公式 A，$A\vee\neg A$ 为 ND 的定理。

（1）$A \vdash A$　　公理

（2）$A \vdash A\vee\neg A$　　∨引入规则（1）

（3）$\neg A \vdash \neg A$　　公理

（4）$\neg A \vdash A\vee\neg A$　　∨引入规则（3）

（5）$\vdash A\vee\neg A$　　假设消除规则（2）（4）

（这里“某某规则（a_1）…（a_n）”表示“对（a_1）…（a_n）诸式用某某规则”，下同）。

【例 5-9】 证明：对 ND 的任意公式 A，B：

（1）$\neg (A\vee B)\leftrightarrow\neg A\wedge\neg B$

（2）$\neg (A\wedge B)\leftrightarrow\neg A\vee\neg B$　　（德摩根律）

我们只证（1），把（2）的证明留给读者。

(i) $\neg(A\vee B), A\vdash A$	公理
(ii) $\neg(A\vee B), A\vdash A\vee B$	$\vee$引入规则 (i)
(iii) $\neg(A\vee B), A\vdash \neg(A\vee B)$	公理
(iv) $\neg(A\vee B)\vdash \neg A$	$\neg$ 引入规则 (ii) (iii)
(v) $\neg(A\vee B)\vdash \neg B$	(同理)
(vi) $\neg(A\vee B)\vdash \neg A\wedge\neg B$	$\wedge$引入规则(iv)(v)
(vii) $\vdash \neg(A\vee B)\rightarrow(\neg A\wedge\neg B)$	$\rightarrow$引入规则(vi)
(viii) $\neg A\wedge\neg B, A\vee B, A\vdash A$	公理
(ix) $\neg A\wedge\neg B, A\vee B, A\vdash \neg A\wedge\neg B$	公理
(x) $\neg A\wedge\neg B, A\vee B, A\vdash \neg A$	$\wedge$消除规则(ix)
(xi) $\neg A\wedge\neg B, A\vee B, A\vdash A\wedge\neg A$	$\wedge$引入规则(viii)(x)
(xii) $\neg A\wedge\neg B, A\vee B, B\vdash B$	(与(viii)同理)
(xiii) $\neg A\wedge\neg B, A\vee B, B\vdash \neg B$	(与(x)同理)
(xiv) $\neg A\wedge\neg B, A\vee B, B\vdash A\wedge\neg A$	$\neg$ 消除规则(xii)(xiii)
(xv) $\neg A\wedge\neg B, A\vee B\vdash A\vee B$	公理
(xvi) $\neg A\wedge\neg B, A\vee B\vdash A\wedge\neg A$	$\vee$消除规则(xi)(xiv)(xv)
(xvii) $\neg A\wedge\neg B, A\vee B\vdash A$	$\wedge$消除规则(xvi)
(xviii) $\neg A\wedge\neg B, A\vee B\vdash \neg A$	$\wedge$消除规则(xvi)
(xix) $\neg A\wedge\neg B\vdash \neg(A\vee B)$	$\neg$ 引入规则(xvii)(xviii)
(xx) $\vdash(\neg A\wedge\neg B)\rightarrow\neg(A\vee B)$	$\rightarrow$引入规则(xix)
(xxi) $\vdash \neg(A\vee B)\leftrightarrow(\neg A\wedge\neg B)$	$\leftrightarrow$引入规则(vii)(xx)

【例 5-10】 证明：对 ND 中的任意公式 A，B，有

$$\neg A\rightarrow B\vdash A\vee B, A\vee B\vdash \neg A\rightarrow B$$

证明 为简化过程缩短篇幅，对某些步骤作了省略。先证$\neg A\rightarrow B\vdash A\vee B$

(1) $\neg A\rightarrow B, \neg A\vdash B$	公理及$\rightarrow$消除规则
(2) $\neg A\rightarrow B, \neg A\vdash A\vee B$	$\vee$引入规则 (1)
(3) $\neg A\rightarrow B, A\vdash A\vee B$	公理及$\vee$引入规则
(4) $\neg A\rightarrow B\vdash A\vee\neg A$	例 5-8
(5) $\neg A\rightarrow B\vdash A\vee B$	$\vee$消除规则 (2) (3) (4)

再证 $A\vee B\vdash\neg A\rightarrow B$。

(1) $A\vee B, B, \neg A\vdash B$	公理
(2) $A\vee B, B\vdash \neg A\rightarrow B$	$\rightarrow$引入规则 (1)
(3) $A\vee B, A, \neg A\vdash B$	公理及$\neg$ 消除规则
(4) $A\vee B, A\vdash \neg A\rightarrow B$	$\rightarrow$引入规则 (3)
(5) $A\vee B\vdash A\vee B$	公理
(6) $A\vee B\vdash \neg A\rightarrow B$	$\vee$消除规则 (2) (4) (5)

容易证明，FC 的公理都是 ND 的定理。

【例 5-11】 对任意公式 A,B,C，有

(1) $\vdash A\rightarrow(B\rightarrow A)$

（2） $\vdash(A\to(B\to C))\to((A\to B)\to(A\to C))$

（3） $\vdash(\neg A\to\neg B)\to(B\to A)$

证明 （1）

（i） $A, B\vdash A$ 公理

（ii） $A\vdash B\to A$ →引入规则（i）

（iii） $\vdash A\to(B\to A)$ →引入规则（ii）

证明 （2）

（i） $A\to(B\to C),\ A\to B,\ A\vdash A$ 公理

（ii） $A\to(B\to C),\ A\to B,\ A\vdash A\to B$ 公理

（iii） $A\to(B\to C),\ A\to B,\ A\vdash A\to(B\to C)$ 公理

（iv） $A\to(B\to C),\ A\to B,\ A\vdash B$ →消除规则（i）（ii）

（v） $A\to(B\to C),\ A\to B,\ A\vdash B\to C$ →消除规则（i）（iii）

（vi） $A\to(B\to C),\ A\to B,\ A\vdash C$ →消除规则（iv）（v）

（vii） $\vdash(A\to(B\to C))\to((A\to B)\to(A\to C))$ →引入规则(运用 3 次)

证明 （3）

（i） $\neg A\to\neg B, B,\ \neg A\vdash B$ 公理

（ii） $\neg A\to\neg B, B,\ \neg A\vdash\neg A$ 公理

（iii） $\neg A\to\neg B, B, \neg A\vdash\neg A\to\neg B$ 公理

（iv） $\neg A\to\neg B, B,\ \neg A\vdash\neg B$ →消除规则(ii)(iii)

（v） $\neg A\to\neg B, B\vdash\neg\neg A$ ¬ 引入规则(i)(iv)

（vi） $\neg A\to\neg B, B\vdash A$ ¬¬ 消除规则（v）

（vii） $\vdash(\neg A\to\neg B)\to(B\to A)$ →引入规则(运用 2 次)

此外，FC 的公理 *A*5 在 ND 中可证明如下。

【例 5-12】 证明$\forall v(A(v)\to B(v))\to(\forall vA(v)\to\forall vB(v))$

证明 其演绎序列如下：

（1） $\forall v(A(v)\to B(v)), \forall vA(v)\vdash\forall vA\ (v)$ 公理

（2） $\forall v(A(v)\to B(v)), \forall vA(v)\vdash A(v)$ ∀消除规则（1）

（3） $\forall v(A(v)\to B(v)), \forall vA(v)\vdash\forall v\ (A(v)\to B(v))$ 公理

（4） $\forall v(A(v)\to B(v)), \forall vA(v)\vdash A(v)\to B(v)$ ∀消除规则（3）

（5） $\forall v(A(v)\to B(v)), \forall vA(v)\vdash B(v)$ →消除规则（2）（4）

（6） $\forall v(A(v)\to B(v)), \forall vA(v)\vdash\forall vB(v)$ ∀引入规则（5）

（7） $\forall v(A(v)\to B(v))\vdash\ \forall vA(v)\to\forall vB(v)$ →引入规则（6）

（8） $\vdash\ \forall v(A(v)\to B(v))\to(\forall vA(v)\to\forall vB(v))$ →引入规则（7）

FC 的公理 *A*4 由 ND 的 ∀ 消除规则保证，FC 的公理 *A*6 和公理 *A*7 由 ND 的 ∀ 引入规则保证。因此我们有

定理 5-11 FC 的公理均为 ND 的定理。

定理 5-12 FC 的定理均为 ND 的定理。

这是因为 FC 的公理均为 ND 的定理，FC 的分离规则就是 ND 的→消除规则。

于是，可以得到结论：

定理 5-13 ND 是合理的、完备的，即对任何 ND 中公式 A，$\Gamma \vdash_{ND} A$，当且仅当 $\Gamma \models A$。

ND 是合理的，它的公理和推理规则的合理性在我们给出系统时都已作出了说明。而 ND 的完备性可由 FC 的完备性以及定理 5-12 直接导出。

为了使读者对 ND 的系统内的推演更加熟悉，我们再介绍一些例子。

【例 5-13】 证明$\exists v A(v) \leftrightarrow \neg\, \forall v \neg\, A(v)$

证明 其演绎序列如下：

（1）$\exists v A(v), \forall v \neg\, A(v) \vdash \exists v A(v)$	公理
（2）$\exists v A(v), \forall v \neg\, A(v), A(c/v) \vdash A(c/v)$ (c 为新常元)	公理
（3）$\exists v A(v), \forall v \neg\, A(v), A(c/v) \vdash \forall v \neg\, A(v)$	公理
（4）$\exists v A(v), \forall v \neg\, A(v), A(c/v) \vdash \neg\, A(c/v)$	∀消除规则（3）
（5）$\exists v A(v), \forall v \neg\, A(v), A(c/v) \vdash B \wedge \neg\, B$($B$ 中 c 无出现)	¬ 消除规则（2）（4）
（6）$\exists v A(v), \forall v \neg\, A(v) \vdash B \wedge \neg\, B$	∃消除规则（1）（5）
（7）$\exists v A(v), \forall v \neg\, A(v) \vdash B$	∧消除规则（6）
（8）$\exists v A(v), \forall v \neg\, A(v) \vdash \neg\, B$	∧消除规则（7）
（9）$\exists v A(v) \vdash \neg\, \forall v \neg\, A(v)$	¬ 引入规则（7）（8）
（10）$\vdash \exists v A(v) \rightarrow \neg\, \forall v \neg\, A(v)$	→引入规则（9）

$\neg\, \forall v \neg\, A(v) \rightarrow \exists v A(v)$的证明留给读者完成。

本例可以看作是存在量词 ∃ 的定义式，也就是说，在 ND 中用一个量词并无不可。ND 中还有以下定理，我们在讨论公式的前束范式时已经运用过它们。

定理 5-14 设 $A(v)$为 ND 中公式，那么

（1）$\neg\, \forall v A(v) \dashv\vdash \exists v \neg\, A(v)$

（2）$\neg\, \exists v A(v) \dashv\vdash \forall v \neg\, A(v)$

证（2）。我们只证$\forall v \neg\, A(v) \vdash \neg\, \exists v A(v)$，另一方向的证明留给读者，（1）式的证明类似，省略。

（i）$\forall v \neg\, A(v), \exists v A(v), A(c/v) \vdash A(c/v)$（c 为新常元）	公理
（ii）$\forall v \neg\, A(v), \exists v A(v), A(c/v) \vdash \neg\, A(c/v)$	公理及∀消除规则
（iii）$\forall v \neg\, A(v), \exists v A(v), A(c/v) \vdash B \wedge \neg\, B$（$B$ 中无 c）	¬ 消除规则（i）（ii）
（iv）$\forall v \neg\, A(v), \exists v A(v) \vdash \exists v A(v)$	公理
（v）$\forall v \neg\, A(v), \exists v A(v) \vdash B \wedge \neg\, B$	∃消除规则（iii）（iv）
（vi）$\forall v \neg\, A(v), \exists v A(v) \vdash B$	∧消除规则（v）
（vii）$\forall v \neg\, A(v), \exists v A(v) \vdash \neg\, B$	∧消除规则（v）
（viii）$\forall v \neg\, A(v) \vdash \neg\, \exists v A(v)$	¬ 引入规则（vi）（vii）

定理 5-15 设 $A(v)$，B 为 ND 中公式，B 中无 v 的自由出现，那么

（1）$Qv(A(v) \vee B) \dashv\vdash Qv A(v) \vee B$

（2）$Qv(A(v) \wedge B) \dashv\vdash Qv A(v) \wedge B$

这里 Q 为 ∀ 或 ∃ 。

证明 我们只证（1）式中 Q 为∀的情况，其余证明读者可仿此完成。

（i）$\forall v(A(v) \vee B), \neg\, B, \neg\, A(v) \vdash A(v) \vee B$	公理
（ii）$\forall v(A(v) \vee B), \neg\, B, \neg\, A(v) \vdash (A(v) \vee B) \rightarrow (\neg\, A(v) \rightarrow B)$	例 5-10

（iii）$\forall v(A(v)\vee B),\neg B,\neg A(v)\vdash\neg A(v)\rightarrow B$　→消除规则（i）（ii）

（iv）$\forall v(A(v)\vee B),\neg B,\neg A(v)\vdash B$　→消除规则（公理）（iii）

（v）$\forall v(A(v)\vee B),\neg B,\neg A(v)\vdash\neg B$　公理

（vi）$\forall v(A(v)\vee B),\neg B\vdash\neg\neg A(v)$　¬ 引入规则（iv）（v）

（vii）$\forall v(A(v)\vee B),\neg B\vdash A(v)$　¬¬ 消除规则（vi）

（viii）$\forall v(A(v)\vee B),\neg B\vdash\forall vA(v)$　∀引入规则（vii）

（ix）$\forall v(A(v)\vee B)\vdash\neg B\rightarrow\forall vA(v)$　→引入规则（viii）

（x）$\forall v(A(v)\vee B)\vdash(\neg B\rightarrow\forall vA(v))\rightarrow(\forall vA(v)\vee B)$　例 5-11

（xi）$\forall v(A(v)\vee B)\vdash\forall vA(v)\vee B$　→消除规则（ix）（x）

另一方面，

（i）$\forall vA(v)\vdash A(v)$　∀消除规则（公理）

（ii）$\forall vA(v)\vdash A(v)\vee B$　∨引入规则（i）

（iii）$B\vdash A(v)\vee B$　∨引入规则（公理）

（iv）$\forall vA(v)\vee B\vdash\forall vA(v)\vee B$　公理

（v）$\forall vA(v)\vee B\vdash A(v)\vee B$　∨消除规则（ii）（iii）（iv）

（vi）$\forall vA(v)\vee B\vdash\forall v(A(v)\vee B)$　∀引入规则（v）

定理 5-16　设 $A(v)$，$B(v)$为 ND 中的任意公式，那么

（1）$\forall v(A(v)\wedge B(v))\dashv\vdash\forall vA(v)\wedge\forall vB(v)$

（2）$\exists v(A(v)\vee B(v))\dashv\vdash\exists vA(v)\vee\exists vB(v)$

本定理的证明是容易的，请读者自证。

定理 5-17　设 $A(v)$，$B(v)$为 ND 中的任意公式，那么

（1）$\forall vA(v)\vee\forall vB(v)\dashv\vdash\forall v\forall u(A(v)\vee B(u))$　（u 在 A 中无自由出现）

（2）$\exists vA(v)\wedge\exists vB(v)\dashv\vdash\exists v\exists u(A(v)\wedge B(u))$　（u 在 A 中无自由出现）

证明　（1）先证$\forall vA(v)\vee\forall vB(v)\vdash\forall v\forall u(A(v)\vee B(u))$。

（i）$\forall vA(v)\vee\forall vB(v)\vdash\forall vA(v)\vee\forall vB(v)$　公理

（ii）$\forall vA(v)\vee\forall vB(v),\forall vA(v)\vdash\forall vA(v)$　公理

（iii）$\forall vA(v)\vee\forall vB(v),\forall vA(v)\vdash A(v)$　∀消除规则（ii）

（iv）$\forall vA(v)\vee\forall vB(v),\forall vA(v)\vdash A(v)\vee B(\mathrm{u})$　∨引入规则（iii）

（v）$\forall vA(v)\vee\forall vB(v),\forall vA(v)\vdash\forall v\forall\mathrm{u}(A(v)\vee B(\mathrm{u}))$　对（iv）连续用两次∀引入规则

（vi）$\forall vA(v)\vee\forall vB(v),\forall vB(v)\vdash\forall v\forall\mathrm{u}(A(v)\vee B(\mathrm{u}))$　（同（i）-（iv））

（vii）$\forall vA(v)\vee\forall vB(v)\vdash\forall v\forall\mathrm{u}(A(v)\vee B(\mathrm{u}))$　∨消除规则（i）（v）（vi）

再证$\forall v\forall u(A(v)\vee B(u))\vdash\forall vA(v)\vee\forall vB(v)$。

（i）$\forall v\forall u(A(v)\vee B(u))\vdash\forall v(A(v)\vee\forall u\,B(u))$　定理 5-15

（ii）$\forall v\forall\mathrm{u}(A(v)\vee B(\mathrm{u}))\vdash\forall vA(v)\vee\forall u\,B(u)$　定理 5-15

（iii）$\forall v\forall u(A(v)\vee B(u)),\forall vA(v)\vdash\forall vA(v)\vee\forall uB(u)$　公理及∨引入规则

（iv）$\forall v\forall u(A(v)\vee B(u)),\forall u\,B(u)\vdash\forall u\,B(u)$　公理

（v）$\forall v\forall u(A(v)\vee B(u)),\forall u\,B(u)\vdash B(v)$　∀消除规则（iv）

（vi）$\forall v\forall u(A(v)\vee B(u)),\forall u\,B(u)\vdash\forall v\,B(v)$　∀引入规则（v）

（vii）$\forall v\forall u(A(v)\vee B(u)),\forall u\,B(u)\vdash\forall vA(v)\vee\forall vB(v)$　∨引入规则（vi）

（viii）$\forall v\forall u(A(v)\vee B(u))\vdash\forall vA(v)\vee\forall vB(v)$　　∨消除规则（ii）（iii）（vii）

（2）式的证明留给读者。

为了使读者进一步了解自然推理的应用层面，再介绍几个例子。

【例 5-14】 考虑下列问题。

已知事实：

（a）如果委员会拒绝通过新条令，那么罢工不结束，或者罢工持续一年并且商行董事长辞职。

（b）委员会拒绝通过新条令。

（c）罢工刚刚开始。

问题：罢工不结束吗？

解 首先将事实和问题形式化。

p：委员会拒绝通过新条令。

q：罢工结束。

r：商行董事长辞职。

s：罢工持续一年。

于是，问题的前提集合 $\Gamma=\{p\rightarrow(\neg q\vee(r\wedge s)),\ p,\ \neg s\}$ 。

要解答本问题，需确定在上述前提下可否推出结论$\neg q$，即 $\Gamma\vdash\neg q$ 是否成立。下列推理表明，答案是肯定的，$\Gamma\vdash\neg q$ 的演绎序列如下：

（1）$\Gamma\vdash p\rightarrow(\neg q\vee(r\wedge s))$　　公理

（2）$\Gamma\vdash p$　　公理

（3）$\Gamma\vdash\neg q\vee(r\wedge s)$　　→消除规则（1），（2）

（4）$\Gamma;\ \neg q\vdash\neg q$　　公理

（5）$\Gamma;\ r\wedge s\vdash\neg s$　　公理

（6）$\Gamma;\ r\wedge s\vdash\neg r\vee\neg s$　　∨引入规则（5）

（7）$\Gamma;\ r\wedge s\vdash(\neg r\vee\neg s)\rightarrow\neg(r\wedge s)$　　例 5-8，例 5-9

（8）$\Gamma;\ r\wedge s\vdash\neg(r\wedge s)$　　→消除规则（6），（7）

（9）$\Gamma;\ r\wedge s\vdash r\wedge s$　　公理

（10）$\Gamma;\ r\wedge s\vdash\neg q$　　¬ 消除规则（8），（9）

（11）$\Gamma\vdash\neg q$　　∨消除规则（3），（4），（10）

如果本例的问题改为“罢工结束吗？”，那么需要由前提 Γ 导出 q 。事实上这是不可能的。为了证明 $\Gamma\vdash q$ 不成立，我们只要证明 $\Gamma\models q$ 不成立（依据 ND 的完备性）。换言之，只要给出一种指派，使得 $\Gamma=\{p\rightarrow(\neg q\vee(r\wedge s)),\ p,\ \neg s\}$中的公式均为真，但使 q 为假。不难看出，这一指派应使得 p 为真，使得 q 为假，使得 s 为假。

【例 5-15】 将下列推理形式化，并判断推理是否正确。

前提：有的病人喜欢所有医生。

没有病人喜欢任何骗子

结论：没有医生是骗子。

解 令 $P(x)$：x 是病人。

$D(x)$：x 是医生。

$S(x)$：x 是骗子。

$L(x,y)$：x 喜欢 y。

以上推理表示为

$$\frac{\exists x(P(x)\wedge\forall y(D(y)\rightarrow L(x,y)))\quad \forall x(P(x)\rightarrow\forall y(S(y)\rightarrow\neg L(x,y)))}{\neg\exists x(D(x)\wedge S(x))}$$

上述推理是正确的，为证明这一点，只要证明推理的结论 $\neg\exists x(D(x)\wedge S(x))$，是前提的集合 $\Gamma=\{\exists x(P(x)\wedge\forall y(D(y)\rightarrow L(x,y))),\ \forall x(P(x)\rightarrow\forall y(S(y)\rightarrow\neg L(x,y)))\}$演绎的结果，亦即，要作出 $\Gamma\vdash\neg\exists x(D(x)\wedge S(x))$的演绎序列。

（1）$\Gamma\vdash\exists x(P(x)\wedge\forall y(D(y)\rightarrow L(x,y)))$ 公理

（2）$\Gamma\vdash\forall x(P(x)\rightarrow\forall y(S(y)\rightarrow\neg L(x,y)))$ 公理

（3）$\Gamma;\ \exists x(D(x)\wedge S(x))\vdash\exists x(D(x)\wedge S(x))$ 公理

（4）$\Gamma;\ \exists x(D(x)\wedge S(x));\ D(e)\wedge S(e)\vdash D(e)\wedge S(e)$ 公理

（5）$\Gamma;\exists x(D(x)\wedge S(x));\ D(e)\wedge S(e);\ P(e1)\wedge\forall y(D(y)\rightarrow L(e1,y))\vdash P(e1)\wedge\forall y(D(y)\rightarrow L(e1,y))$
公理

（6）$\Gamma;\ \exists x(D(x)\wedge S(x));\ D(e)\wedge S(e);\ P(e1)\wedge\forall y(D(y)\rightarrow L(e1,y))\vdash\forall y(D(y)\rightarrow L(e1,y))$
$\wedge$消除规则（5）

（7）$\Gamma;\ \exists x(D(x)\wedge S(x));\ D(e)\wedge S(e);\ P(e1)\wedge\forall y(D(y)\rightarrow L(e1,y))\vdash D(e)\rightarrow L(e1,e)$
$\forall$-消除规则（6）

（8）$\Gamma;\ \exists x(D(x)\wedge S(x));\ D(e)\wedge S(e)\ ;\ P(e1)\wedge\forall y(D(y)\rightarrow L(e1,y))\vdash D(e)$
$\wedge$消除规则（4）

（9）$\Gamma;\ \exists x(D(x)\wedge S(x));\ D(e)\wedge S(e)\ ;\ P(e1)\wedge\forall y(D(y)\rightarrow L(e1,y))\vdash L(e1,e)$
$\rightarrow$消除规则（7），（8）

（10）$\Gamma;\ \exists x(D(x)\wedge S(x));\ D(e)\wedge S(e);\ P(e1)\wedge\forall y(D(y)\rightarrow L(e1,y))\vdash P(e1)\rightarrow\forall y(S(y)\rightarrow\neg L(e1,y))$
$\forall$-消除规则+假设引入规则（2）

（11）$\Gamma;\ \exists x(D(x)\wedge S(x));\ D(e)\wedge S(e);\ P(e1)\wedge\forall y(D(y)\rightarrow L(e1,y))\vdash P(e1)$
$\wedge$规则消除（5）

（12）$\Gamma;\ \exists x(D(x)\wedge S(x));\ D(e)\wedge S(e);\ P(e1)\wedge\forall y(D(y)\rightarrow L(e1,y))\vdash\forall y(S(y)\rightarrow\neg L(e1,y))$
$\rightarrow$消除规则（10），（11）

（13）$\Gamma;\ \exists x(D(x)\wedge S(x));\ D(e)\wedge S(e);\ P(e1)\wedge\forall y(D(y)\rightarrow L(e1,y))\vdash S(e)\rightarrow\neg L(e1,e)$
$\forall$-消除规则（12）

（14）$\Gamma;\ \exists x(D(x)\wedge S(x));\ D(e)\wedge S(e);\ P(e1)\wedge\forall y(D(y)\rightarrow L(e1,y))\vdash S(e)$
$\wedge$消除规则+假设引入规则（4）

（15）$\Gamma;\ \exists x(D(x)\wedge S(x));\ D(e)\wedge S(e);\ P(e1)\wedge\forall y(D(y)\rightarrow L(e1,y))\vdash\neg L(e1,e)$
$\rightarrow$消除规则（13），（14）

（16）$\Gamma;\ \exists x(D(x)\wedge S(x));\ D(e)\wedge S(e);\ P(e1)\wedge\forall y(D(y)\rightarrow L(e1,y))\vdash f$
$\neg$ 消除规则（9），（15）

（17）$\Gamma;\ \exists x(D(x)\wedge S(x));\ D(e)\wedge S(e)\ \vdash f$ $\exists$ 消除规则（1），（5），（16）

（18）$\Gamma;\ \exists x(D(x)\wedge S(x))\vdash f$ $\exists$ 消除规则（3），（4），（17）

（19）$\Gamma \vdash \neg\, \exists x(D(x) \wedge S(x))$　　$\neg$ 引入规则（3），（18）

5.3 练习

1．什么是形式系统的证明和演绎？

2．在 FC 中对下列各式给出证明或演绎，其中 A，B，C 为任意公式（允许使用演绎定理和其他导出规则）。

（1）$\vdash (A \to B) \to ((\neg A \to \neg B) \to (B \to A))$

（2）$\vdash A \to (B \to (A \to B))$

（3）$\{A \to (A \to B)\} \vdash A \to B$

（4）$\{\neg A\} \vdash A \to B$

（5）$\{\neg \neg A\} \vdash A$

（6）$\{A \to B, \neg (B \to C) \to \neg A\} \vdash A \to C$

（7）$\vdash A \to \neg \neg A$

（8）$\vdash (B \to A) \to (\neg A \to \neg B)$

（9）$\vdash ((A \to B) \to A) \to A$

（10）$\vdash \neg (A \to B) \to (B \to A)$

3．证明关于 FC 的元定理：若 $\Gamma \vdash \neg A \to B$，$\Gamma$；$A \vdash C$，$\Gamma$；$B \vdash C$，则 $\Gamma \vdash C$。

4．证明：对任何公式 $A(x)$，$B(x)$，有

（1）$\vdash_{FC} \forall x(A(x) \to (B(x) \to A(x)))$

（2）$\vdash_{FC} \forall x\, A(x) \to \exists x A(x)$

（3）$\vdash_{FC} (\forall x \neg A(x) \to \exists x B(x)) \to (\neg \exists x B(x) \to \exists x A(x))$

5．指出下列 FC 中的演绎里的错误之处。

（1）$\exists x\, A(x,y)$	前提
（2）$\forall y \exists x\, A(x,y)$	对（1）用定理 2-5
（3）$\forall y \exists x\, A(x,y) \to \exists x\, A(x,x)$	公理
（4）$\exists x\, A(x,x)$	对（2），（3）用分离规则

6．模仿定理 5-7 的证明，给出定理 5-8 的证明。

7．在 ND 中证明下列各式，其中 A，B，C 为任意公式。

（1）$\vdash (A \to B) \to ((\neg A \to \neg B) \to (B \to A))$

（2）$\vdash A \to (B \to (A \to B))$

（3）$\{A \to (A \to B)\} \vdash A \to B$

（4）$\{\neg A\} \vdash A \to B$

（5）$\{\neg \neg A\} \vdash A$

（6）$\{A \to B, \neg (B \to C) \to \neg A\} \vdash A \to C$

（7）$\vdash A \to \neg \neg A$

（8）$\vdash (B \to A) \to (\neg A \to \neg B)$

（9）$\vdash ((A \to B) \to A) \to A$

（10）$\vdash \neg (A \to B) \to (B \to A)$

8．在 ND 中证明下列各式，其中 A，B，C 为任意公式。

（1）$\vdash ((A\to B)\to B)\to A\vee B$

（2）$\vdash A\wedge(B\vee C)\leftrightarrow(A\wedge B)\vee(A\wedge C)$

（3）$\vdash \neg(A\to B)\leftrightarrow(A\wedge\neg B)$

（4）$\vdash A\wedge B\leftrightarrow A\wedge(\neg A\vee B)$

（5）$\vdash (A\vee B)\wedge(\neg B\vee C)\to A\vee C$

9．证明下列推理是错误的(无效的)。

（1）$\{A\to B,\neg A\}\vdash\neg B$

（2）$\dfrac{A\wedge B\to C,\neg C}{\neg A\wedge\neg B}$

（3）
我有钱就买书
我买书必去淮海路
———————
我没去淮海路

10．试完成如下推理。

（1）如果今天下大雨，则马路上不好行走；如果马路难走，则我不去逛书店；如果我不去逛书店，则在家学习。所以，如果今天下大雨，则我在家学习。

（2）四位体操运动员 A，B，C，D 应邀参加表演赛。今知，如果 A 参加，则若 B 参加，C 一定参加；如果 D 参加，则 A 一定参加，B 也一定参加。可以推得：如果 D 参加，则 C 一定参加。

11．在 ND 中证明下列定理。

（1）$\vdash \forall x\,A(x)\to\neg\,\exists x\neg\,A(x)$

（2）$\vdash \neg\,\exists x\neg\,A(x)\to\forall x\,A(x)$

（3）$\vdash \forall x\neg\,A(x)\to\neg\,\exists xA(x)$

（4）$\vdash \forall x(A\to B(x))\leftrightarrow(A\to\forall x\,B(x))$（$A$ 中无自由变元 x）

（5）$\vdash \exists x(A\to B(x))\leftrightarrow(A\to\exists x\,B(x))$（$A$ 中无自由变元 x）

（6）$\vdash \forall x(A(x)\to B)\leftrightarrow(\exists x\,A(x)\to B)$（$B$ 中无自由变元 x）

（7）$\vdash \exists x(A(x)\to B)\leftrightarrow(\forall x\,A(x)\to B)$（$B$ 中无自由变元 x）

（8）$\vdash \forall x(A(x)\vee B(x))\to(\forall xA(x)\vee\exists x\,B(x))$

12．在 ND 中给出下列演绎的演绎序列。

（1）$\{\forall x(A(x)\to B(x)),\forall x(C(x)\to\neg\,B(x))\}\vdash\forall x(C(x)\to\neg\,A(x))$

（2）$\{\forall x(A(x)\vee B(x))\}\vdash\forall xA(x)\vee\exists x\,B(x)$

（3）$\{\forall x(A(x)\to(B(y)\wedge C(x))),\exists x\,A(x)\}\vdash B(y)\wedge\exists x\,(A(x)\wedge C(x))$

（4）$\{\exists x\,P(x)\to\forall x(P(x)\vee Q(x)\to R(x)),\exists x\,P(x),\exists x\,Q(x)\}\vdash\exists x\,\exists y(R(x)\wedge R(y))$

13．证明以下推理是无效的。

（1）$\dfrac{\forall x(A(x)\vee B(x))\quad\forall xA(x)}{\forall xB(x)}$

有的人是勇敢的人

（2）有的人是鲁莽的人

勇敢者是鲁莽的人

14．证明下列推理是有效的。

前提：每个非文科的一年级生都有辅导员。

小王是一年级生。

小王是理科生。

凡小王的辅导员都是理科生。

所有的理科生都不是文科生。

结论：至少有一个不是文科生的辅导员。

第6章 计 数

组合数学（combinatorial mathematics）是数学的一个分支，主要研究在给定模式下的可能配置，配置的存在性，配置的数目，配置的性质等等。我们已经介绍过的鸽笼原理常被列入组合数学范畴，它被用于可能配置的存在性讨论。计数（computing）是组合数学领域的重要课题，其主要任务是上述配置数目的计算技术的研究。高中阶段数学课程中的排列、组合及二项式定理等教学内容，皆属于计数这一范畴。计数技术广泛应用于事件概率的计算,以及计算机算法的复杂性研究。

6.1 计数基本原理

计数基本原理包括加法原理和乘法原理，是高中阶段数学课程中的学习内容，我们只作简要回顾。

6.1.1 加法原理和乘法原理

加法原理：若事件的有限集合 $S=S_1\cup\cdots\cup S_n$，且 $S_1,\cdots,S_n$ 两两不相交，那么

$$|S|=|S_1|+\cdots+|S_n|$$

也就是说，如果事件集合 S 可以分为两两不相交的子集 S_1，…，S_n，那么要对 S 中事件计数时，可对子集 S_1，…，S_n 分别计数，然后相加来求得。

加法原理的另一个说法是：n 个独立事件分别有 a_1，…，a_n 种方式发生，那么这 n 个事件之一发生的方式总计为 $a_1+\cdots+a_n$ 种。

乘法原理：若事件的有限集合 S 是依次取自有限集合 $S_1,\cdots,S_n$ 中事件的序列的集合，那么

$$|S|=|S_1|*\cdots*|S_n| \quad (*\text{表示数的乘法})$$

也就是说，如果集合 S 中的事件是由集合 S_1，…，S_n 中事件相继发生而形成的事件序列所构成，且 S_i 中每一事件的发生，可以导致 S_{i+1} 中所有事件的发生（$i=1$，2，…，$n-1$）。那么，对 S 中的事件序列计数时，可对集合 S_1，…，S_n 分别计数，然后相乘来求得。

乘法原理的另一个说法是：n 个独立事件分别有 a_1，…，a_n 种方式发生，那么这 n 个事件同时发生的方式总计为 $a_1\cdot\cdots\cdot a_n$ 种。

两个原理的正确性都是十分明显的。

【例 6-1】 （1）从上海直达天津可以乘坐汽车、火车和飞机旅行。已知每天汽车有 3 个班次，火车有 4 个班次，飞机有 2 个班次，问每天从上海直达到天津有多少种旅行方式？

（2）从上海直达天津可以乘坐汽车、火车和飞机旅行，已知汽车有 3 个班次，火车有 4 个班次，飞机有 2 个班次。从天津直达大连可以乘坐轮船和飞机旅行，已知轮船有 2 个班次，飞机有 3 个班次。问从上海经天津到大连有多少种旅行方式？

解 （1）从上海直达到天津有 $3+4+2=9$ 种旅行方式（加法原理）。

（2）从上海经天津到大连有 $9\times(2+3)=45$ 种旅行方式（加法原理和乘法原理）。

【例 6-2】 一家服装厂用 4 种式样，5 种颜色，8 种尺寸生产男式服装；用 6 种式样，5 种颜色，6 种尺寸生产女式服装，问这家服装厂共计生产男女服装多少种？

解 男式服装为

$$4\times5\times8=160\ (\text{种}) \qquad (\text{乘法原理})$$

女式服装为

$$6\times5\times6=180\ (\text{种}) \qquad (\text{乘法原理})$$

合计 160+180=340（种）（加法原理）。

6.1.2 包含排斥原理

我们注意到，在加法原理中，集合 $S_1,\cdots,S_n$ 两两不相交。若没有这一限制，那么 $|S|$ 的计算要复杂得多。

定理 6-1 考虑集合 S_1,S_2，$S=S_1\cup S_2$，那么

$$|S|=|S_1|+|S_2|-|S_1\cap S_2|$$

证明 由于 $|S_1|+|S_2|$ 是 S_1 元素个数与 S_2 元素个数之和，其中 S_1,S_2 的公共元素被两次计数，所以 $|S|=|S_1|+|S_2|-|S_1\cap S_2|$。

定理 6-2 考虑集合 $S_1,\cdots,S_n$，$S=S_1\cup\cdots\cup S_n$，那么

$$|S|=|S_1\cup\cdots\cup S_n|$$

$$=\sum_{i=1}^{n}|S_i|-\sum_{1\leqslant i<j\leqslant n}|S_i\cap S_j|+\sum_{1\leqslant i<j<k\leqslant n}|S_i\cap S_j\cap S_k|-\cdots+(-1)^{n+1}|S_1\cap\cdots\cap S_n|$$

证明 $n=1$ 时，左边 $=|S_1|$，右边 $=\sum_{i=1}^{1}|S_i|=|S_1|$。因此，等式成立。

$n=2$ 时，待证等式为

$$|S_1\cup S_2|=|S_1|+|S_2|-|S_1\cap S_2|$$

它正是定理 6-1。

设 $n=k$ 时，等式成立，现对 $n=k+1$ 论证。由于 $n=k+1$，那么

$$|S_1\cup\cdots\cup S_n|$$

$$=|S_1\cup\cdots\cup S_k\cup S_{k+1}|$$

$$=|S_1\cup\cdots\cup S_k|+|S_{k+1}|-|(S_1\cup\cdots\cup S_k)\cap S_{k+1}|$$

$$=\sum_{i=1}^{k}|S_i|-\sum_{1\leqslant i<j\leqslant k}|S_i\cap S_j|+\sum_{1\leqslant i<j<l\leqslant k}|S_i\cap S_j\cap S_l|-\cdots+(-1)^{k+1}|S_1\cap S_2\cap\cdots\cap S_k|+$$

$$+|S_{k+1}|-|(S_1\cap S_{k+1})\cup(S_2\cap S_{k+1})\cup\ldots(S_k\cap S_{k+1})|$$

$$=\sum_{i=1}^{k+1}|S_i|-\sum_{1\leqslant i<j\leqslant k}|S_i\cap S_j|+\sum_{1\leqslant i<j<l\leqslant k}|S_i\cap S_j\cap S_l|-\cdots+(-1)^{k+1}|S_1\cap S_2\cap\cdots\cap S_k|$$

$$-\Big(\sum_{i=1}^{k}|S_i\cap S_{k+1}|-\sum_{1\le i<j\le k}|S_i\cap S_j\cap S_{k+1}|+\sum_{1\le i<j<l\le k}|S_i\cap S_j\cap S_l\cap S_{k+1}|-\cdots+$$

$$+(-1)^{k+1}|S_1\cap S_2\cap\cdots\cap S_k\cap S_{k+1}|\Big)$$

$$=\sum_{i=1}^{k+1}|S_i|-\sum_{1\le i<j\le k+1}|S_i\cap S_j|+\sum_{1\le i<j<l\le k+1}|S_i\cap S_j\cap S_l|-\cdots+(-1)^{k+2}|S_1\cap S_2\cap\cdots\cap S_k\cap S_{k+1}|$$

归纳完成，命题得证。

定理 6-3 考虑集合 S_1,S_2，$S_1\cup S_2\subseteq S$，令 $S-S_1\cup S_2$ 为 $\overline{S_1\cup S_2}$ 或 $\overline{S_1}\cap\overline{S_2}$ 那么

$$|\overline{S_1}\cap\overline{S_2}|=|S|-(|S_1|+|S_2|)+|S_1\cap S_2|$$

定理 6-4 考虑集合 $S_1,\cdots,S_n$，已知 $S_1\cup\cdots\cup S_n\subseteq S$。现将 $S-(S_1\cup\cdots\cup S_n)$ 记为 $\overline{S_1\cup\cdots\cup S_n}$ 或 $\overline{S_1}\cap\cdots\cap\overline{S_n}$ 那么

$$|\overline{S_1}\cap\cdots\cap\overline{S_n}|$$

$$=|S|-\sum_{i=1}^{n}|S_i|+\sum_{1\le i<j\le n}|S_i\cap S_j|-\sum_{1\le i<j<k\le n}|S_i\cap S_j\cap S_k|+\cdots+(-1)^n|S_1\cap\cdots\cap S_n|$$

定理 6-4 就是人们常说的包含排斥原理（简称“容斥原理”）。它是定理 6-2 的明显推论。“容斥原理”的一个常用的说法是：用 $S_1,\cdots,S_n$ 分别表示集合 S 中具有性质 $P_1,\cdots,P_n$ 的元素的子集合，用 $\overline{S_1},\cdots,\overline{S_n}$ 分别表示集合 S 中不具有性质 $P_1,\cdots,P_n$ 的元素的子集合，那么，S 中不具有性质 P_1，不具有性质 $P_2,\cdots$，也不具有性质 P_n 的元素的个数是

$$|\overline{S_1}\cap\cdots\cap\overline{S_n}|$$

$$=|S|-\sum_{i=1}^{n}|S_i|+\sum_{1\le i<j\le n}|S_i\cap S_j|-\sum_{1\le i<j<k\le n}|S_i\cap S_j\cap S_k|+\cdots+(-1)^n|S_1\cap\cdots\cap S_n|$$

在上述公式中，如果诸 $|S_i|$ 都相等，记为 $N(1)$，诸 $|S_i\cap S_j|$ 都相等，记为 $N(2)$，诸 $|S_i\cap S_j\cap S_k|$ 都相等，记为 $N(3)$，……，如此等等，那么情况就简单得多。若令 $|\overline{S_1}\cap\cdots\cap\overline{S_n}|=N(0)$，$|S|=N$，我们有

$$N(0)=N-C(n,1)\cdot N(1)+C(n,2)\cdot N(2)-\cdots+(-1)^nC(n,n)\cdot N(n)$$

这个式子被称为**对称筛公式**。这里的 $C(n,i)$ 与中学数学中的 C_n^i 相同意义。

【例 6-3】 （1）试计算在集合{1，2，3，…，1000}中有多少元素至少能被 5，6，8 这三个数中的一个整除。

（2）试计算在集合{1，2，3，…，1000}中有多少元素不能被 5，6，8 这三个数中的任何一个整除。

解 集合{1，2，3，…，1000}中能被 5，6，8 这三个数整除的元素的集合分别是 S_5,S_6,S_8，那么（用 $[x]$ 表示 x 的整数部分。注意，一个数被若干个数同时整除当且仅当这个数被它们的最小公倍数整除。）

$$|S_5|=\left[\frac{1000}{5}\right]=200\quad,\quad|S_6|=\left[\frac{1000}{6}\right]=166\quad,\quad|S_8|=\left[\frac{1000}{8}\right]=125$$

$$|S_5 \cap S_6| = \left[\frac{1000}{30}\right] = 33,\quad |S_5 \cap S_8| = \left[\frac{1000}{40}\right] = 25,\quad |S_6 \cap S_8| = \left[\frac{1000}{24}\right] = 41$$

$|S_5 \cap S_6 \cap S_8| = \left[\frac{1000}{120}\right] = 8$ ，因此

（1）至少能被 5，6，8 这三个数中的一个整除的元素有

$$|S_5 \cup S_6 \cup S_8| = 200+166+125-33-25-41+8 = 400 \text{（个）}$$

（2）不能被 5，6，8 这三个数中的任何一个整除的元素有

$$|\overline{S_5} \cap \overline{S_6} \cap \overline{S_8}| = 1000-200-166-125+33+25+41-8 = 600 \text{（个）}$$

或

$$\overline{S_5} \cap \overline{S_6} \cap \overline{S_8}| = 1000-|S_5 \cup S_6 \cup S_8| = 1000-400 = 600 \text{（个）}$$

6.2 排列与组合

6.2.1 排列的计数

我们对中学课程中已经学习过的对象排列的计数作一个简要的回顾。

定义 6-1 用 P_n^r 或 $P(n,r)$ 表示“从 n 个元素的集合中每次取出 r 个元素进行有序排列时可得到的排列的总数”。P_n^r 或 $P(n,r)$ 简称为 **r-排列数**，$P(n,n)$ 简称为 **n-全排列数**。

定理 6-5 对任意正整数 n，r，$r \leqslant n$，从 n 个元素的集合中每次取出 r 个元素进行有序排列时可得到的排列的总数是：（约定 $n! = n(n-1)(n-2)\cdots 3 \cdot 2 \cdot 1$ ，$0!=1$）

$$P(n,r) = n(n-1)(n-2)\cdots(n-r+1) = \frac{n!}{(n-r)!}$$

特别地，$P(n,1) = n$，$P(n,n) = n!$

【例 6-4】 问有多少个大于 5400，又同时满足下列两个性质的整数：

（1）各位数字都不相同。

（2）数中不出现数字 2 与 7。

解 由于要求各位数字都不相同，并且数中不出现数字 2 与 7，因此满足条件的数只能是四位数、五位数、六位数、七位数和八位数。其中五位数、六位数、七位数和八位数的数目可以如下分别计算：第一位有非 0，2，7 的七种安排方法，其他各位则可从剩余的七个数字里再选取 i 个（i= 4，5，6，7）进行排列，因此它们的数目分别是

$$7 \cdot P(7,i),\ i = 4,5,6,7$$

而五位数、六位数、七位数和八位数的数的总数应当是

$$\sum_{i=4}^{7} 7 \cdot P(7,i) = 7\sum_{i=4}^{7} P(7,i) = 7 \times (7 \times 6 \times 5 \times 4 \times (1+3+6+6)) = 94080$$

另外，满足要求的四位数可如下计算：

千位数大于 5 的有 $3 \cdot P(7,3) = 630$ 个（千位数有 3 种排法，6，8，9，其余各位则可从剩余的 7 个数字里再选取 3 个来排列）。

千位数是 5，而百位数大于或等于 4 的有 $4 \cdot P(6,2) = 120$ 个（千位数确定，百位数有 4

种排法，4，6，8，9，其余各位则可从剩余的 6 个数字里再选取 2 个来排列）。

故满足上述两个性质的整数共计有

$$94080+630+120=94830\text{（个）}$$

本例中大量使用了加法原理，读者可以细细体会之。

以上所说的排列有人称之为线排列，而将以下的排列称之为**圆排列**：从 n 个元素的集合中每次取出 r 个元素，围绕一个圆周进行有序排列。这种排列的总数显然可以如下确定。

定理 6-6 对任意正整数 n，r，$r\leqslant n$，从 n 个元素的集合中每次取出 r 个元素，围绕一个圆周进行有序排列时可得到的排列的总数是：

$$\frac{P(n,r)}{r}=\frac{n!}{r(n-r)!}$$

特别地，全取 n 个元素的圆排列的数目是：$(n-1)!$。

证明 观察一个 r 个元素的圆排列，设想在圆排列的 r 个间隔处将其切断，每一个不同的切断均产生一个不同的线排列，换言之，一个圆排列对应 r 个线排列。因此，r 个元素的圆排列的总数应当等于 r 个元素的线排列的总数除以 r，即 $\frac{P(n,r)}{r}=\frac{n!}{r(n-r)!}$。

【例 6-5】 六位女士和六位先生围着一张圆桌聚餐，要求安排女士和先生交替就座。问：有多少可能的安排方案。

解 由于要求安排女士和先生交替就座，因此可以先安排六位女士坐下，两位之间留出一个空位，然后再安排先生就座。安排六位女士坐下（圆排列）的方案数是

$$\frac{P(6,6)}{6}=\frac{6!}{6}=5!=120\text{（种）}$$

由于已经有女士在位，安排先生在六个空位上就座时，就不再是圆排列了，因为原先被看成相同圆排列的六位先生的就座方式所产生的全体人员的圆排列是不同的。故安排先生在六个空位上就座的方案数是

$$6!=720$$

于是我们得到满足要求安排方案共计有

$$5!\cdot 6!=120\times 720=86400\text{（种）}$$

本例中主要使用了乘法原理，读者可以细细体会之。

6.2.2 组合的计数

组合的计数以及组合数的性质，在中学课程中也均有涉及，我们在作简要回顾的同时，适度地加以提高。

定义 6-2 用 C_n^r 或 $C(n,r)$ 表示“从 n 个元素的集合中每次取出 r 个元素（不进行有序排列）组成子集合的总数。C_n^r 或 $C(n,r)$ 简称为 **r-组合数**。

定理 6-7 对任意正整数 n，r，$r\leqslant n$，从 n 个元素的集合中每次取出 r 个元素组成子集合的总数是：

$$C(n,r)=\frac{P(n,r)}{r!}=\frac{n!}{r!(n-r)!}$$

特别地，$C(n,1)=n$，$C(n,n)=1$，约定 $C(n,0)=1$。

【例 6-6】 一个足球队有 15 名队员，其中 5 人能踢后场，8 人能踢前场，2 人既能踢后场又能踢前场。今需从中选取 7 名前锋和 4 名后卫参加比赛，问：有多少种不同的选法（只考虑队员的前后场特长组合，不考虑同一位置上的左右区别）。

解 把 15 人按其特长分为三个集合：S_1、S_2、S_3，S_1 由能踢后场的 5 人组成，S_2 由能踢前场的 8 人组成，S_3 既能踢后场又能踢前场的 2 人组成。分下列情况进行讨论：

（1）不用 S_3 人员的选法有 $C(8,7)\cdot C(5,4)=8\times 5=40$ (种)

（2）用 S_3 中一个人员的选法。

1）用 S_3 人员踢前锋的选法有 $C(8,6)\cdot C(5,4)=28\times 5=140$ (种)

2）用 S_3 人员踢后卫的选法有 $C(8,7)\cdot C(5,3)=8\times 10=80$ (种)

（3）用 S_3 中两个人员的选法。

1）用 S_3 中两个人员踢前锋的选法有 $C(8,5)\cdot C(5,4)=56\times 5=280$ (种)

2）用 S_3 中两个人员踢后卫的选法有 $C(8,7)\cdot C(5,2)=8\times 10=80$ (种)

3）用 S_3 中的一个人员踢后卫、另一个人踢前锋的选法有（注意这两个人可以互换位置）

$$2\cdot C(8,6)\cdot C(5,3)=2\times 28\times 10=560\text{ (种)}$$

因此，不同的选法共计有

$$40+140+80+280+80+560=1180\text{(种)}$$

本例中综合使用了加法原理和乘法原理。

组合数 $C(n,r)$ 有许多有趣的性质。

定理 6-8 对任意正整数 n，r，$r\leqslant n$，有

（1）$C(n,r)=C(n,n-r)$

（2）$C(n,r)=\dfrac{n}{r}C(n-1,r-1)$

两式均由定理 6-7 立即可得。

在介绍组合数 $C(n,r)$ 其他性质之前，我们回忆一下**牛顿二项式定理**：对任意正整数 n

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

定理 6-9 对任意正整数 n，有

（1）$\sum_{i=0}^{n}C(n,i)=2^n$。

（2）$\sum_{i=0}^{n}(-1)^iC(n,i)=0$。

证明 根据牛顿二项式定理：

$$2^n=(1+1)^n=C(n,0)+C(n,1)+\cdots+C(n,n)$$

$$0=(1-1)^n=C(n,0)-C(n,1)+\cdots+(-1)^nC(n,n)$$

定理 6-10 对于满足条件 $1\leqslant k\leqslant n-1$ 的任意正整数 k 和 n，有

$$C(n,k)=C(n-1,k)+C(n-1,k-1)$$

证明 等式的左边 $C(n,k)$ 表示从 n 个元素的集合中每次取出 k 个元素组成子集合的总数。我们从另外一个角度来考虑这些子集合。取定元素 a，这些子集合可以分为两类，（1）

不含元素 a 的 k 个元素组成的子集合，其个数是 $C(n-1,k)$；（2）必含元素 a 的 k 个元素组成的子集合，其个数是 $C(n-1,k-1)$。因此，$C(n,k)=C(n-1,k)+C(n-1,k-1)$。

6.3 重集的排列与组合

我们知道，集合是互相区别的对象的总体。而本节要讨论的**重集**则是允许多个相同的对象同时出现的对象总体。重集中的对象仍称为重集的**元素**，重集中相同元素的个数称为元素的**重数**。具有 n_1 个 a_1，n_2 个 a_2，…，n_m 个 a_m 的重集，称之为 $n(n=n_1+n_2+\cdots+n_m)$ 个元素的 m **元重集**，可以表示为

$$\{n_1 \cdot a_1, n_2 \cdot a_2, \cdots, n_m \cdot a_m\}$$

约定 $\infty \cdot a$ 表示 a 在重集中可出现任意多次，因此，重集 $\{\infty \cdot a_1, \infty \cdot a_2, \cdots, \infty \cdot a_m\}$ 中的所有元素均可以任意多次地出现。含有 $\infty \cdot a$ 的重集，称为**有无穷元素的 m 元重集**。

6.3.1 重集的排列

定义 6-3 **重集的 r-排列**是指从重集 $\{n_1 \cdot a_1, n_2 \cdot a_2, \cdots, n_m \cdot a_m\}$（其中各 n_i 可以是 ∞）中每次取出 r 个元素进行有序的排列，此时可得到的排列的总数称为 **r-排列数**。当 $r=n_1+n_2+\cdots+n_m$ 时，称此 r-排列为**全排列**，此时可得到的排列的总数称为**全排列数**。

定理 6-11 无穷重数的 m 元重集 $\{\infty \cdot a_1, \infty \cdot a_2, \cdots, \infty \cdot a_m\}$ 的 r-排列数是 m^r。

证明 无穷重数的 m 元重集 $\{\infty \cdot a_1, \infty \cdot a_2, \cdots, \infty \cdot a_m\}$ 的 r-排列的每一个位置上均可选取 m 个不同元素中的每一个，因此每一个位置上元素的排放法有 m 种，故而 r-排列数应当是 m^r。

【例 6-7】 （1）用 8 颗七彩的珠子串成长链，可以串出多少种不同的长链？（假定七彩的珠子取之不尽，并且不考虑链子的翻转）

（2）用 8 颗七彩的珠子串成环链，可以串出多少种不同的环链？（假定七彩的珠子取之不尽，并且不考虑链子的翻转）

解 （1）用 8 颗七彩的珠子串成长链，可以串出不同的长链

$$7^8 = 5764801 \text{（种）}$$

（2）用 8 颗七彩的珠子串成环链，可以串出不同的环链

$$7^8 \div 7 = 823543 \text{（种）}$$

注意：重集的圆排列与排列的关系可以参考普通集合的圆排列与排列的关系。本题中重集的一个 8-圆排列对应于重集的 7-排列。

定理 6-12 m 元重集 $\{n_1 \cdot a_1, n_2 \cdot a_2, \cdots, n_m \cdot a_m\}$ 的全排列数是

$$\frac{n!}{n_1! \cdot \cdots \cdot n_m!}$$

其中 $n=n_1+n_2+\cdots+n_m$。

证明 先从 n 个排列的位置中选取 n_1 个，放置元素 a_1，放置方法有 $C(n,n_1)$ 种，再从 $n-n_1$

个排列的位置中选取 n_2 个,放置元素 a_2，放置方法有 $C(n-n_1,n_2)$ 种，…，最后从 $n-n_1-n_2\cdots-n_{m-1}$ 个排列的位置中选取 n_m 个,放置元素 a_m，放置方法有 $C(n-n_1-\cdots-n_{m-1},n_m)$ 种。因此，m 元重集 $\{n_1\cdot a_1,n_2\cdot a_2,\cdots,n_m\cdot a_m\}$ 的全排列数是

$$C(n,n_1)\,C(n-n_1,n_2)\cdots C(n-n_1-\cdots-n_{m-1},n_m)$$

$$=\frac{n!}{n_1!(n-n_1)!}\,\frac{(n-n_1)!}{n_2!(n-n_1-n_2)!}\cdots\frac{(n-n_1-\cdots-n_{m-1})!}{n_m!(n-n_1-\cdots-n_m)!}$$

$$=\frac{n!}{n_1!\cdots n_m!}$$ （注意：$(n-n_1-\cdots-n_{m-1}-n_m)!=0!=1$）

【例 6-8】 一位秘书在某大厦（B）工作，该大厦在她家（H）东边 9 个街段，北边 7 个街段（如图 6-1 所示，图中线段表示街道）。假定她每天从家里到大厦去上班都不走回头路（即只向东和向北行走）。问她可以有多少种不同的走法？又若图中的 AC 段积水，使她无法通过，这时她又可以有多少种不同的走法？

解 为图 6-1 建立坐标系，H 点坐标为（0，0），B 点坐标为（9，7），A 点坐标为（4，3），C 点坐标为（5，3）。因为她只向东和向北行走，因此可以用 9 • E 表示她可选择的向东的九个街段，用 7 • N 表示她可选择的向北的七个街段。于是她的一种走法就对应于重集 {9 • E，7 • N}的一个全排列，故她可以有的不同的走法是

$$\frac{16!}{9!\cdot 7!}=11440\ （种）$$

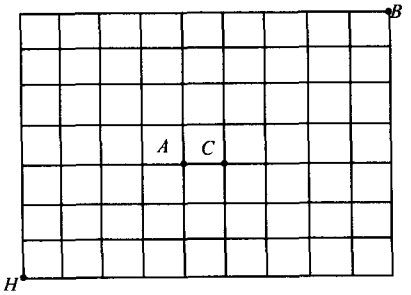


图 6-1

我们先来计算必经 AC 街段时她的走法总数，可以分为两个阶段来计算。从 A 到 H 的走法、从 C 到 B 的走法各有

$$\frac{7!}{4!\cdot 3!}=35\ （种），\quad \frac{8!}{4!\cdot 4!}=70\ （种）$$

因此，必经 AC 街段时她的走法总数是 $\frac{7!}{4!\cdot 3!}\times\frac{8!}{4!\cdot 4!}=35\times 70=2450$ （种）

若图中的 AC 段积水，使她无法通过，那么她的走法数目应当是

$$\frac{16!}{9!\cdot 7!}-\frac{7!}{4!\cdot 3!}\times\frac{8!}{4!\cdot 4!}=11440-2450=8990\ （种）$$

【例 6-9】 （1）问方程 $x_1+x_2+\cdots+x_m=r$ 有多少组自然数解？

（2）问方程 $x_1+x_2+\cdots+x_m=r$ 有多少组正整数解？

解 （1）考虑由 m–1 个 0 和 r 个 1 组成的 0，1 序列。我们把这样一个 0，1 序列看成

是 m–1 个 0 把 r 个 1 分成 m 组的一个分割：第一个 0 的左边的 1 看作为第一组 1，第一个 0 和第二个 0 之间的 1 看作为第二组 1，……，第 m–1 个 0 右边的 1 看作为第 m 组 1。这样，一个 0，1 序列的分割对应于方程的一组自然数解，反之，方程的一组自然数解也对应于一个这样的 0，1 序列分割。例如 $m=5$，$r=4$ 时，01011001 对应的方程 $x_1+x_2+x_3+x_4=4$ 的一组解是

$$x_1=0,x_2=1,x_3=2,x_4=0,x_5=1$$

因此，方程 $x_1+x_2+\cdots+x_m=r$ 自然数解的数目等同于重集 $\{(m-1)\cdot 0, r\cdot 1\}$ 的全排列数，即

$$\frac{(m-1+r)!}{(m-1)!\bullet r!}$$

（2）考虑 r 个 1 组成的 0，1 序列，用 $p_1,p_2,\cdots,p_{r-1}$ 来表示 r 个 1 之间的 r–1 个位置。取 $\{p_1,p_2,\cdots,p_{r-1}\}$ 中的 m–1 个，并在这些位置的每一个上插入一个 0。我们把得到的这样一个 0，1 序列看成是 m–1 个 0 把 r 个 1 分成 m 组的一个分割：第一个 0 的左边的 1 看作为第一组 1，第一个 0 和第二个 0 之间的 1 看作为第二组 1，……，第 m–1 个 0 右边的 1 看作为第 m 组 1。由于任意两个 0 之间至少有一个 1，因此，一个 0，1 序列的分割对应于方程的一组正整数解，反之，方程的一组正整数解也对应于一个这样的 0，1 序列分割。因此，方程 $x_1+x_2+\cdots+x_m=r$ 正整数解的数目等同于集合 $\{p_1,p_2,\cdots,p_{r-1}\}$ 的 $(m-1)$ –组合数：

$$C(r-1,m-1)$$

6.3.2 重集的组合

定义 6-4 **重集的 r-组合**是指从重集 $\{n_1\bullet a_1,n_2\bullet a_2,\cdots,n_m\bullet a_m\}$（其中各 n_i 可以是 ∞）中每次取出 r 个元素组成子重集，此时可得到的子重集的总数称为 **r-组合数**。

定理 6-13 无穷重数的 m 元重集 $\{\infty\bullet a_1,\infty\bullet a_2,\cdots,\infty\bullet a_{m-1},\infty\bullet a_m\}$ 的 r-组合数是 $C(m-1+r,r)$。

证明 m 元重集 $\{\infty\bullet a_1,\infty\bullet a_2,\cdots,\infty\bullet a_m\}$ 的 r-组合是 r 个元素组成子重集

$$\{x_1\bullet a_1,x_2\bullet a_2,\cdots,x_m\bullet a_m\},x_1+x_2+\cdots+x_m=r$$

因此，r-组合数与方程 $x_1+x_2+\cdots+x_m=r$ 的自然数解的数目相等，根据例 6-9（1），m 元重集 $\{\infty\bullet a_1,\infty\bullet a_2,\cdots,\infty\bullet a_m\}$ 的 r-组合数是

$$\frac{(m-1+r)!}{(m-1)!\bullet r!}=C(m-1+r,r)。$$

事实上，此结论对于 $n_1,n_2,\cdots,n_m$ 均不小于 r 的重集 $\{n_1\bullet a_1,n_2\bullet a_2,\cdots,n_m\bullet a_m\}$ 也成立。

定理 6-14 要求无穷重数的 m 元重集 $\{\infty\bullet a_1,\infty\bullet a_2,\cdots,\infty\bullet a_m\}$ 的 r-组合中 $a_1,a_2,\cdots,a_m$ 均至少选入一次的 r-组合数是 $C(r-1,m-1)$。

证明 无穷重数的 m 元重集 $\{\infty\bullet a_1,\infty\bullet a_2,\cdots,\infty\bullet a_m\}$ 的 r-组合是 r 个元素组成子重集

$$\{x_1\bullet a_1,x_2\bullet a_2,\cdots,x_m\bullet a_m\},x_1+x_2+\cdots+x_m=r$$

且 $x_1,x_2,\cdots,x_m$ 均为正整数，因此，r-组合数与方程 $x_1+x_2+\cdots+x_m=r$ 的正整数解的数目

相等，根据例 6-9（2），m 元重集$\{\infty \cdot a_1, \infty \cdot a_2, \cdots, \infty \cdot a_m\}$的 r-组合中$a_1, a_2, \cdots, a_m$均至少选入一次的 r-组合数是$C(r-1, m-1)$。

【例 6-10】 一家面包店卖 6 种面包，假如你要买 12 个面包，可以有多少种选择方案(假定各种面包的数量都大大超过 12 只)？假如你要买 12 个面包，且每种面包至少一只，可以有多少种选择方案？

解 第一问是一个求重集$\{\infty \cdot a_1, \infty \cdot a_2, \cdots, \infty \cdot a_6\}$的 12-组合数的问题。因此其解是

$$C(6-1+12,12)=C(17,12)=C(17,5)=\frac{17\times 16\times 15\times 14\times 13}{5\times 4\times 3\times 2}=6188 \text{（种）}$$

第二问则是求重集$\{\infty \cdot a_1, \infty \cdot a_2, \cdots, \infty \cdot a_6\}$的、每个元素至少取一个的 12-组合数的问题。因此其解是

$$C(12-1,6-1)=C(11,5)=\frac{11\times 10\times 9\times 8\times 7}{5\times 4\times 3\times 2}=462 \text{（种）}$$

【例 6-11】 设$S=\{1 \cdot a_1, 1 \cdot a_2, \cdots, 1 \cdot a_t, \infty \cdot a_{t+1}, \infty \cdot a_{t+2}, \cdots, \infty \cdot a_m\}$，求 S 的 r-组合数。

解 将 S 分为两个子集

$$S_1=\{1 \cdot a_1, 1 \cdot a_2, \cdots, 1 \cdot a_t\} \text{和} S_2=\{\infty \cdot a_{t+1}, \infty \cdot a_{t+2}, \cdots, \infty \cdot a_m\}$$

那么，S 的 r-组合可以如下构成：先从 S_1 中选出 i 个元素($i=0$，1，2，…，t)，再从 S_2 中选出 r–i 个元素。因此，S 的 r-组合数是

$$\sum_{i=0}^{t} C(t,i)\cdot C(m-t-1+r-i, r-i)$$

定理 6-13、例 6-10 和例 6-11 给出了一些情况比较特殊的重集的 r-组合数求解方法，更加一般的重集的 r-组合数求解方法要借助于容斥原理，我们只用一个例子来介绍这种方法的要领。

【例 6-12】 试计算重集$S=\{3 \cdot a, 4 \cdot b, 5 \cdot c\}$的 10-组合数。

解 考虑重集$T=\{\infty \cdot a, \infty \cdot b, \infty \cdot c\}$的所有 10-组合集合 K。令 P_1 表示性质：“T 的 10-组合中多于 3 个 a”，P_2 表示性质：“T 的 10-组合中多于 4 个 b”，P_3 表示性质：“T 的 10-组合中多于 5 个 c”。那么，S 的 10-组合数等于不具有性质 P_1，P_2，P_3 的 T 的 10-组合数。我们利用容斥原理来计算$S=\{3 \cdot a, 4 \cdot b, 5 \cdot c\}$的 10-组合数。将具有性质 P_1，P_2，P_3 的 T 的 10-组合数分别记为$|P_1|$，$|P_2|$，$|P_3|$；将同时具有性质 P_1 和 P_2，P_1 和 P_3，以及 P_2 和 P_3 的 T 的 10-组合数分别记为$|P_1 \cap P_2|$，$|P_1 \cap P_3|$，$|P_2 \cap P_3|$；将同时具有性质 P_1，P_2 和 P_3 的 10-组合数记为$|P_1 \cap P_2 \cap P_3|$，将同时不具有性质 P_1，P_2 和 P_3 的 10-组合数记为$\left|\overline{P_1} \cap \overline{P_2} \cap \overline{P_3}\right|$。

此外，$T=\{\infty \cdot a, \infty \cdot b, \infty \cdot c\}$的 10-组合数记为$|T|$。根据定理 6-11：

$|T|=\ C(3-1+10,10)=C(12,10)=66$

$|P_1|=\ C(3-1+6,6)=C(8,6)=28$（取定 4 个 a 后，再取 T 的一个 6-组合）

$|P_2|=\ C(3-1+5,5)=C(7,5)=21$（取定 5 个 b 后，再取 T 的一个 5-组合）

$|P_3|=\ C(3-1+4,4)=C(6,4)=15$（取定 6 个 c 后，再取 T 的一个 4-组合）

$|P_1 \cap P_2| = C(3-1+1,1) = C(3,1) = 3$（取定 4 个 a, 5 个 b 后，再取 T 的一个 1-组合）

$|P_1 \cap P_3| = C(3-1+0,0) = C(2,0) = 1$（取定 4 个 a, 6 个 c 后，再取 T 的一个 0-组合）

$|P_2 \cap P_3| = 0$（取定 5 个 b, 6 个 c 的 T 的 10-组合不存在）

$|P_1 \cap P_2 \cap P_3| = 0$（取定 4 个 a，5 个 b，6 个 c 的 T 的 10-组合不存在）

根据容斥原理：

$$\left|\overline{P_1} \cap \overline{P_2} \cap \overline{P_3}\right| = |T| - |P_1| - |P_2| - |P_3| + |P_1 \cap P_2| + |P_1 \cap P_3| + |P_2 \cap P_3| - |P_1 \cap P_2 \cap P_3|$$

$$= 66 - 28 - 21 - 15 + 3 + 1 + 0 - 0 = 6$$

这就是说，重集 $S = \{3 \cdot a, 4 \cdot b, 5 \cdot c\}$ 的 10-组合数为 6。

6.3.3 禁位排列的计数

定义 6-5 集合{1，2，3，…，n}的全排列，使得每个数 i 都不在第 i 位上，称这样的排列为{1，2，3，…，n}的一个**错置**。

定理 6-15 集合{1，2，3，…，n}的错置的总数（记为 D_n）是

$$D_n = n!\left(1 - \frac{1}{1!} + \frac{1}{2!} - \frac{1}{3!} + \cdots + (-1)^n \frac{1}{n!}\right)$$

约定 $D_0 = 1$。

证明 设 S 是{1，2，3，…，n}的全排列的集合，$|S| = n!$。令 P_i 表示性质："数 i 放置在排列的第 i 个位置上" ($i = 1, 2, \cdots, n$)。A_i 表示具有性质 P_i 的{1，2，3，…，n}的全排列的集合。由于集合{1, 2, 3, …, n}的错置的总数，就是同时不具有所有性质 P_i ($i = 1, 2, \cdots, n$)的{1，2，3，…，n}的全排列的总数，因此

$$D_n = \left|\overline{A_1} \cap \overline{A_2} \cap \cdots \cap \overline{A_n}\right|$$

可以用容斥原理来求解。

由于"数 i 放置在排列的第 i 个位置上"的排列数，等同于其余 $n-1$ 个数的全排列，因此

$$|A_i| = (n-1)!$$

而同时满足 P_i，P_j 的排列数，等同于其余 $n-2$ 个数的全排列，因此

$$|A_i \cap A_j| = (n-2)!$$

如此等等，一般地有

$$|A_{i1} \cap A_{i2} \cap \cdots \cap A_{ik}| = (n-k)!$$

故

$$D_n = \left|\overline{A_1} \cap \overline{A_2} \cap \cdots \cap \overline{A_n}\right|$$

$$= |S| - \sum_{i=1}^{n} |A_i| + \sum_{1 \leqslant i < j \leqslant n} |A_i \cap A_j| - \sum_{1 \leqslant i < j < k \leqslant n} |A_i \cap A_j \cap A_k| + \cdots + (-1)^n |A_1 \cap \cdots \cap A_n|$$

$$= n! - C(n,1)(n-1)! + C(n,2)(n-2)! - \cdots + (-1)^n C(n,n)\cdot 0!$$

$$= n! - \frac{n!}{1!} + \frac{n!}{2!} - \cdots + (-1)^n \frac{n!}{n!}$$

$$= n!(1 - \frac{1}{1!} + \frac{1}{2!} - \cdots + (-1)^n \frac{1}{n!})$$

D_n 的下列性质被称为它的“递推公式”。我们将在第 7 章来讨论这类递推公式。

定理 6-16 （1） $D_n = (n-1)(D_{n-2} + D_{n-1})$

（2） $D_n = nD_{n-1} + (-1)^n$

证明 （1）设{1，2，3，…，n}的一个错置是

$$a_1 a_2 \cdots a_k \cdots a_n$$

因为 $a_1 \neq 1$，所以 a_1 有 $n-1$ 种取法。设 $a_1 = i(2 \leqslant i \leqslant n)$，分两种情况来讨论：

1） $a_i = 1$。这时 $a_1 a_2 \cdots a_k \cdots a_n$ 取决于其余 $n-2$ 个数的错置，这些错置的数目是 D_{n-2}。

2） $a_i \neq 1$。这时 $a_1 a_2 \cdots a_k \cdots a_n$ 取决于其余 $n-1$ 个数的错置：“1 不可放置在第 i 位，其他各数 j 不可放置在第 j 位”，这些错置的数目是 D_{n-1}。因此，由加法原理和乘法原理

$$D_n = (n-1)(D_{n-2} + D_{n-1})$$

（2）容易明白 $D_0 = 1$，$D_1 = 0$，用它们和（1）不难得到本结论。

定义 6-6 集合{1，2，3，…，n}的全排列，使得每个数 i 都不紧邻在数 $i-1$ 的后面，把{1，2，3，…，n}的这样的禁位全排列的总数记为 Q_n。

定理 6-17 定义 6-6 中的集合{1，2，3，…，n}的禁位全排列总数

$$Q_n = n! - C(n-1,1)(n-1)! + C(n-1,2)(n-2)! - \cdots + (-1)^{n-1} C(n-1,n-1)1!$$

证明 设 S 是{1，2，3，…，n}的全排列的集合，$|S| = n!$。令 P_i 表示性质：“排列中数 $i+1$ 放置在数 i 的后面”（$i=1$，2，…，n）。A_i 表示具有性质 P_i 的{1，2，3，…，n}的全排列的集合。由于集合{1，2，3，…，n}的 Q_n，就是同时不具有所有性质 P_i（$i=1$，2，…，$n-1$）的{1，2，3，…，n}的全排列的总数，因此

$$Q_n = |\overline{A_1} \cap \overline{A_2} \cap \cdots \cap \overline{A_{n-1}}|$$

可以用容斥原理来求解。

由于“排列中数 $i+1$ 放置在数 i 的后面”的排列数，等同于其余 $n-2$ 个数与 i $(i+1)$的全排列，因此

$$|A_i| = (n-1)!$$

同理，同时满足 P_i，P_j 的排列数，等同于其余 $n-4$ 个数与 i $(i+1)$，与 j $(j+1)$的全排列，因此

$$|A_i \cap A_j| = (n-2)!$$

如此等等，一般地有

$$|A_{i1} \cap A_{i2} \cap \cdots \cap A_{ik}| = (n-k)!$$

故

$$Q_n = \left|\overline{A_1} \cap \overline{A_2} \cap \cdots \cap \overline{A_{n-1}}\right|$$

$$= |S| - \sum_{i=1}^{n-1} |A_i| + \sum_{1 \leqslant i < j \leqslant n-1} |A_i \cap A_j| - \sum_{1 \leqslant i < j < k \leqslant n-1} |A_i \cap A_j \cap A_k| + \cdots + (-1)^{n-1} |A_1 \cap \cdots \cap A_{n-1}|$$

$$= n! - C(n-1,1)(n-1)! + C(n-1,2)(n-2)!$$

$$- C(n-1,3)(n-3)! + \cdots + (-1)^{n-1} C(n-1,n-1) \cdot 1!$$

6.4 练习

1．学校为学生提供 3 门计算机硬件课程，4 门计算机程序设计语言课程。问

（1）如果学生可以且只可以在这两类课程中选一门课程，学生有多少选择方式？

（2）如果学生可以且只可以在这两类课程中各选一门课程，学生有多少选择方式？

2．在 1000 与 9999 之间有多少个数字互不相同的奇数？

3．用定理 6-2 证明定理 6-4。

4．（1）在例 6-3 中计算“至多可以被三个数中的两个整除的元素个数”。

（2）在例 6-3 中计算“恰被三个数都整除的元素个数”。

（3）在例 6-3 中计算“恰被三个数中的一个整除的元素个数”。

（4）把例 6-3 中（2）的要求改为“有多少元素不能被 3，5，6，8，这四个数中的任何一个整除”，试计算之。

5．某学院语言学系有 200 个学生，他们至少要选修德、英、法三种语言中的一种。已知在这些学生中有 90 人学德语，130 人学英语，84 人学法语，30 人学法语和德语，40 人学法语和英语，50 人学德语和英语。问同时学三种语言的学生有多少？仅学英语的学生有多少？

6．试计算在集合{1，2，3，…，10000}中有多少元素既不是完全平方数，也不是完全立方数，更不是完全四次方数？（提示：可以用$\left\lfloor \sqrt[n]{x} \right\rfloor$表示“对 x 的 n 次方根取整”）

7．某产品加工需要“甲、乙、丙、丁、戊”等五道工序。

（1）当规定工序丁必须紧接着工序丙安排加工，五道工序的安排方法有多少种？

（2）当规定工序乙必须安排在工序戊的前面加工，五道工序的安排方法有多少种？

8．今有 12 个人围着圆桌就座，如果其中有两个人不愿坐在相邻的位置上，问：有多少种不同的坐法？

9．从集合{1，2，3，…，300}中任取 3 个数，使得它们的和能被 3 整除。问有多少种取法？

10．一个俱乐部有 10 名男成员，12 名女成员，现从中选出 4 人组成一个委员会，若

（1）至少要有 2 名女的。

（2）除上述要求外，又指定 M，N 两女士不能同时入选。

那么，各有多少种不同的选法？

11．证明定理 6-8 (1)，(2)。

12．证明：对任意正整数 n，k，r，若 $r \leqslant k \leqslant n$，则

（1）$C(n,k)C(k,r) = C(n,r) + C(n-r,k-r)$

（2）$\sum_{i=1}^{n} i \cdot C(n,i) = n \cdot 2^{n-1}$

13. 如下分割集合 S：从集合 S 起，每一次都把多于一个元素的一个集合分成两个非空集合，直到所有集合都只有一个成员为止。问：有多少种不同的分割过程。（提示：可以考虑分割以后再合并的过程有多少种）

14. 从集合{1，2，…，n+1}中选出 3 个数组成三元序组<x，y，z>，使得 $x<z$，$y<z$。

（1）证明：当 $z=k+1$ 时，这样的三元序组的个数恰为 k^2 个($1\leqslant k\leqslant n$)。

（2）这样的三元序组可以依据 $x=y$，$x<y$,$y<x$ 分为三类，分别计算这三类三元序组的数目。

（3）根据（1）、（2）的计算，可以作出一个重要的恒等式。写出这个恒等式。

15. r 个有区别的球，放入 n 个有区别的盒子，盒子内球数不限，可以为 0。问：有多少不同的放置方法？

16. n 个有区别的球，放入 k 个有区别的盒子 B_1，B_2，…，B_k，要求在盒子 B_i 中放置 n_i 个球，$i=1$，2，…，k，且 $n=n_1+n_2+\cdots+n_k$。证明放置的不同方式有

$$\frac{n!}{n_1!\cdot\cdots\cdot n_k!}\text{（种）}$$

17. 节日期间某大楼要排成一行地悬挂 15 面彩旗。其中红、黄、蓝、绿、橙五种颜色各 3 面，问：

（1）这些彩旗有多少种不同的排列方法？

（2）若不允许有两面蓝旗相邻，又有多少种不同的排列方法？

18. n 个相同的球放入 r 个有标记的盒子中，（$r\leqslant n$）允许有盒子是空的。证明放置方法数为 $C(n-1+r,r)$。

19. 求方程 $x_1+x_2+x_3+x_4=14$ 的整数解，要求

（1）$0\leqslant x_1,x_2,x_3,x_4\leqslant 6$

（2）$1\leqslant x_1,x_2,x_3,x_4\leqslant 8$

20. n 个相同的球放入 r 个有标记的盒子中，（$r\leqslant n$）使得没有一个盒子是空的。证明放置方法数为 $C(n-1,r-1)$。

21. 两个十位数，如果重排其中的一个可以得到另外一个，那么称这两个十位数是“同码的”。问：有多少个同码的十位数。

22. 计算，由数字 1，1，2，3，3，4 可以组成多少个四位数。

23. 证明：把 x 个 1 和 y 个 0 排成一行（$x\leqslant y+1$），使得没有两个 1 相邻的排列数为 $C(y+1,x)$。

24. 一个面包店只剩下 6 个巧克力面包，7 个黄棕色面包和 3 个普通面包。这时要从这 16 个面包中任选 12 个装成一盒，问：有多少种不同的选法？

第7章 递归关系

在前一章的禁位排列的计数中我们曾指出，集合{1，2，3，…，n}的错置数D_n满足以下性质：

（1）$D_n=(n-1)(D_{n-2}+D_{n-1})$

（2）$D_n=nD_{n-1}+(-1)^n$

像（1）（2）这样的式子被称为**递归关系**（recurrence relations）式。递归关系式是指运用函数的前驱值来计算函数当前值的关系式。递归关系式在有些教科书上也称为递推关系式。例如，在（1）中，运用D_{n-1}，D_{n-2}可以计算D_n；在（2）中，运用D_{n-1}便可以计算D_n。我们还注意到，式（1）连同初值$D_0=1, D_1=0$，可以惟一地确定函数D_n。

定义 7-1 下列方程组

$$\begin{cases} H(0)=a_0 \\ H(1)=a_1 \\ \vdots \\ H(k-1)=a_{k-1} \\ H(n)+b_1H(n-1)+b_2H(n-2)+\cdots+b_kH(n-k)=0 \ (k\leqslant n, b_k\neq 0) \end{cases}$$

称为定义数列（自然数函数）$H(n)$的**常系数线性齐次递归式**(linear homogeneous recurrence relations with constant efficient)。若方程组的最后一式为

$$H(n)+b_1H(n-1)+b_2H(n-2)+\cdots+b_kH(n-k)=f(n)$$

那么，方程组称为定义数列（自然数函数）$H(n)$的**常系数线性非齐次递归式**（linear non homogeneous recurrence relations with constant efficient）。

递归关系式是求解组合数学问题的重要工具，几乎在所有的数学分支中都有重要应用，本教材的第 11 章将用它作为研究函数的重要手段。本章对递归关系式的研究的主要目的是：

（1）针对要求解的问题建立递归关系式。

（2）由递归关系式解出数列（自然数函数）的显式表示。

（3）利用递归关系式解决一些重要的计数问题。

7.1 一个重要的递归关系

我们从一个重要而且典型的递归关系式来开始本章的讨论。

13 世纪意大利数学家费波那契（Fibonacci）提出了一个有趣的兔子繁殖的问题：在一年的年初把一对刚出生的小兔子放进养殖场。小兔子满二个月后即可生育一对一雌一雄的小兔子。以后每隔一个月即可生育一对一雌一雄的小兔子。月复一月，问在一年后养殖场有多少对兔子？

用 $F(n)$ 表示在第 n 个月养殖场里兔子的对数，规定 $F(0)=0$ 表示初始时养殖场里没有兔子。那么

$F(1)=1$（为最初的兔子对数）

$F(2)=1$（仍为最初的兔子对数，即二月的兔子对数没增加）

$F(3)=1+1=2$（最初的兔子对数加上其后代，即为二月的一对加上一月兔子的后代）

$F(4)=2+1=3$（三月的 2 对加上二月兔子的后代）

$F(5)=3+2=5$（四月的 3 对加上三月 2 对的后代）

$\vdots$

$F(11)=55+34=89$（十月的 55 对加上九月 34 对的后代）

$F(12)=89+55=144$（十一月的 89 对加上十月 55 对的后代）

$F(13)=144+89=233$（十二月的 144 对加上十一月 89 对的后代）

一年后（12 个月后，即第 13 个月）养殖场共有兔子 233 对。于是人们把数列 $F(0)$，$F(1)$，$F(2)$，…，$F(n)$，…，称为**费波那契数列**，其中的每一个数也称**费波那契数**。不难发现费波那契数列满足下列递归关系式：

$$\begin{cases} F(0)=0 \\ F(1)=1 \\ F(n)=F(n-1)+F(n-2) \end{cases}$$

人们也把上述递归关系式叫做**费波那契递归关系**。

可以用以下方法求出费波那契数列的通项公式。

令 $F(n)=q^n$，$F(n-1)=q^{n-1}$，$F(n-2)=q^{n-2}$，$(n\geqslant 2)$，这里 q 是不等于零的数。那么

$$q^n=q^{n-1}+q^{n-2} \quad 或 \quad q^{n-2}(q^2-q-1)=0$$

因此，当且仅当 q 是二次方程 $x^2-x-1=0$ 的解时，$F(n)=q^n$ 是递归关系

$$F(n)=F(n-1)+F(n-2)$$

的解。由二次方程求根公式知 $x^2-x-1=0$ 的两个根是：

$$q_1=\frac{1+\sqrt{5}}{2} \quad , \quad q_2=\frac{1-\sqrt{5}}{2}$$

因此

$$F(n)=\left(\frac{1+\sqrt{5}}{2}\right)^n \quad 和 \quad F(n)=\left(\frac{1-\sqrt{5}}{2}\right)^n$$

都是 $F(n)=F(n-1)+F(n-2)$ $(n\geqslant 2)$ 的解。由于这一递归关系是线性齐次的，故而对任意常数 c_1,c_2，

$$F(n)=c_1\left(\frac{1+\sqrt{5}}{2}\right)^n+c_2\left(\frac{1-\sqrt{5}}{2}\right)^n$$

也都是 $F(n)=F(n-1)+F(n-2)$ $(n\geqslant 2)$ 的解，称为 $F(n)$ 的**通解**。此外，由于 $F(0)=0$，$F(1)=1$，代入递归式得

$$0=c_1+c_2$$

$$1=c_1\left(\frac{1+\sqrt{5}}{2}\right)+c_2\left(\frac{1-\sqrt{5}}{2}\right)$$

解这个方程组，又得

$$c_1=\frac{1}{\sqrt{5}}\quad,\quad c_2=\frac{-1}{\sqrt{5}}$$

最终我们有 $F(n)$ 的解，亦即费波那契数列的通项公式：

$$F(n)=\frac{1}{\sqrt{5}}\left(\frac{1+\sqrt{5}}{2}\right)^n-\frac{1}{\sqrt{5}}\left(\frac{1-\sqrt{5}}{2}\right)^n$$

若 $F(0)=a$，$F(1)=b$，那么由

$$a=c_1+c_2$$

$$b=c_1\left(\frac{1+\sqrt{5}}{2}\right)+c_2\left(\frac{1-\sqrt{5}}{2}\right)$$

可求 c_1,c_2 的解，因为上述方程组的系数行列式非零：

$$\begin{vmatrix}1 & 1\\ \dfrac{1+\sqrt{5}}{2} & \dfrac{1-\sqrt{5}}{2}\end{vmatrix}=-\sqrt{5}\neq 0$$

从而可以讨论一般意义下的费波那契数列。费波那契递归关系有许多的性质与应用见本章练习题 1～4，它是一个非常重要的递归关系。

【例 7-1】 集合{1，2，3，…，n}的子集称为是**交替的**，如果它的元素在按照上升次序排列时，是奇、偶交替地出现的，且第一个数是奇数。例如{1，4，7，8}和{1，2，3，…，n}是交替的，{2，4，5}和{1，3，4，6}都不是交替的。规定空集和奇数单元素子集是交替的。令 $f(n)$ 表示{1，2，3，…，n}的交替子集的数目。求解 $f(n)$。

解 先找出 $f(n)$ 的递归关系式。显然 $f(1)=2$，它的交替子集是{1}和∅。$f(2)=3$，它的交替子集是{1,2}，{1}和∅。

把{1，2，3，…，n}的所有子集分为两部分。第一部分是不含 n 的，即为{1,2,3,…,$n-1$}的所有子集，第二部分是包含 n 的，它可看成由{1，2，3，…，$n-1$}的每一个子集加进元素 n 以后所得到的子集。第一部分子集中的交替子集为 $f(n-1)$；第二部分子集中的交替子集，可以也只可以由{1，2，3，…，$n-2$}的交替子集并入{$n-1$, n}（交替子集末尾与 n 同奇偶时）、或{1，2，3，…，$n-2$}的交替子集并入{n}（交替子集末尾与 n 不同奇偶时）来构成，因此，其数目与{1，2，3，…，$n-2$}的交替子集数相同，也为 $f(n-2)$。故

$$f(n)=f(n-1)+f(n-2)$$

用上述递归关系式和 $f(1)=2=F(3)$，$f(2)=3=F(4)$ 可以得到

$$f(n)=F(n+2)$$

7.2 递归关系的求解

7.2.1 递归关系的迭代求解

由本章练习的第 1 题我们得到：递归关系式的迭代求解方法可以由以下两个步骤完成：

（1）利用递归关系式对关系式右边的表达式进行迭代，并推测解的公式。

（2）用数学归纳法证明得到的公式。

先用一个极其简单的例子给以说明。

【例 7-2】 平面上有 n 条两两相交的直线，又没有任何三条直线交于一点。问共有多少不同交点。（要求用递归关系式求解）

解 设已知的 $n(n\geqslant 2)$ 条直线的交点数目为 $h(n)$。如果增添第 $n+1$ 条直线，它与前 n 条直线相交产生新的 n 个交点，因此

$$h(n+1)=h(n)+n$$

此外，$h(2)=1$。现进行迭代计算

$$h(n+1)=h(n)+n=h(n-1)+n-1+n=h(n-2)+n-2+n-1+n=\cdots$$

$$=1+2+\cdots+(n-1)+n=\frac{n(n+1)}{2}$$

因此，$h(n)=\dfrac{n(n-1)}{2}$

用数学归纳法证明 $h(n)=\dfrac{n(n-1)}{2}$ $(n\geqslant 2)$。

归纳基础：$n=2$ 时，已知 $h(2)=1$，而 $\dfrac{n(n-1)}{2}=\dfrac{2\times 1}{2}=1$。

归纳推理：设 $h(k)=\dfrac{k(k-1)}{2}$，那么

$$h(n)=h(k+1)=h(k)+k=\frac{k(k-1)}{2}+k=\frac{k(k-1)+2k}{2}=\frac{k(k+1)}{2}=\frac{n(n-1)}{2}$$

归纳完成，证毕。

我们再讨论一个稍稍复杂的例子（通常称为河内塔（Hanoi）或汉诺塔问题）。

【例 7-3】 有三个木桩 A，B，C，在 A 木桩上有 n 个大小不等的圆盘，按照由小到大的次序叠放着，最大的圆盘放在最底下，木桩上的圆盘呈塔形。现需将这些圆盘逐个地从 A 木桩转移到 B 木桩，并依然按原来的由小到大的次序叠放，转移中可以利用 C 木桩，但要求在任何时候都保持让较大的圆盘在较小的圆盘之下。问：完成这样的一次转移，必须至少移动圆盘多少次。

解 令 $h(n)$ 为完成这样的一次转移至少必须移动圆盘的次数。容易知道，

$$h(0)=0,\quad h(1)=1,\quad h(2)=3$$

现求取 $h(n)$ 所满足的递归关系式。为了把 n 个圆盘从 A 木桩转移到 B 木桩，可以递归地将转移分为三个过程。

（1）将 $n-1$ 个圆盘从所在 A 木桩转移到 C 木桩，留下最大的圆盘。必须移动圆盘的次数是 $h(n-1)$。

（2）将最大的圆盘移至 B 木桩。必须移动圆盘的次数是 1 。

（3）将 $n-1$ 个圆盘从 C 木桩转移到 B 木桩。必须移动圆盘的次数是 $h(n-1)$。

因而

$$h(n)=2h(n-1)+1$$

作迭代计算

$$\begin{aligned}h(n)&=2h(n-1)+1\\&=2(2h(n-2)+1)+1=2^2h(n-2)+2+1\\&=2^2(2h(n-3)+1)+2+1=2^3h(n-3)+2^2+2+1\\&\vdots\\&=2^nh(0)+2^{n-1}+\cdots+2^2+2+1\\&=2^{n-1}+\cdots+2^2+2+1=2^n-1\end{aligned}$$

也就是说，$h(n)=2^n-1$

用归纳法证明这一结论。

归纳基础：$n=0$时，已知$h(0)=0$，而$2^n-1=2^0-1=0$

归纳推理：设$h(k)=2^k-1$，那么$n=k+1$时

$$h(n)=h(k+1)=2h(k)+1=2(2^k-1)+1=2^{k+1}-2+1=2^{k+1}-1=2^n-1$$

归纳完成，证毕。

通过上述两个例子的讲解，读者可以十分清楚地掌握递归关系式的迭代求解方法了。

7.2.2 常系数线性齐次递归关系的求解

在7.1中我们把形如

$$H(n)+b_1H(n-1)+b_2H(n-2)+\cdots+b_kH(n-k)=0$$

的递归关系式称为常系数线性齐次递归关系，并应用了一种十分特别的方法来求解常系数线性齐次递归关系的一个例子——费波那契递归关系式，这一方法称为常系数线性齐次递归关系求解的特征根方法。那里的方程$x^2-x-1=0$称为递归关系式

$$F(n)=F(n-1)+F(n-2)$$

的特征方程。一般地，称方程$x^k+b_1x^{k-1}+b_2x^{k-2}+\cdots+b_k=0$为递归关系式$H(n)+b_1H(n-1)+b_2H(n-2)+\cdots+b_kH(n-k)=0$的**特征方程**(characteristic equations)，其根称为它的**特征根**（characteristic roots）。在使用特征根方法时，我们运用了以下两个事实。

定理 7-1 设q是一个非零的实数或复数，那么，$H(n)=q^n$是递归关系式

$$H(n)+b_1H(n-1)+b_2H(n-2)+\cdots+b_kH(n-k)=0\quad(k\leqslant n,b_k\neq0)$$

的解当且仅当q是它的一个特征根。

证明 若$H(n)=q^n$是递归关系式的解，那么

$$q^n+b_1q^{n-1}+b_2q^{n-2}+\cdots+b_kq^{n-k}=0$$

$$q^{n-k}(q^k+b_1q^{kn-1}+b_2q^{k-2}+\cdots+b_k)=0$$

由于$q\neq0$，因此，$q^k+b_1q^{kn-1}+b_2q^{k-2}+\cdots+b_k=0$，也就是说$q$是它的特征方程$x^k+b_1x^{k-1}+b_2x^{k-2}+\cdots+b_k=0$的一个特征根。

另一方面，上述推理过程是可逆的，故定理得证。

定理 7-2 设$q_1,q_2,\cdots,q_k$是非零实数或复数，那么，

$$H(n)=c_1q_1^n+c_2q_2^n+\cdots+c_kq_k^n$$

($c_1,c_2,\cdots c_k$为确定的常数) 是递归关系式

$$H(n)+b_1H(n-1)+b_2H(n-2)+\cdots+b_kH(n-k)=0 \quad (k\leqslant n, b_k\neq 0)$$

的解当且仅当 $q_1,q_2,\cdots q_k$ 是它的 k 个不同的特征根。

证明 若 $H(n)=c_1q_1^n+c_2q_2^n+\cdots+c_kq_k^n$ 是递归关系式的解，其初始值

$$H(0)=a_0,\quad H(1)=a_1,\quad \cdots,\quad H(k)=a_k$$

那么，有关于 $c_1,c_2,\cdots c_k$ 的线性方程组

$$\begin{aligned}
a_0 &= c_1+c_2+\cdots+c_k\\
a_1 &= c_1q_1+c_2q_2+\cdots+c_kq_k\\
&\vdots\\
a_{k-1} &= c_1q_1^{k-1}+c_2q_2^{k-1}+\cdots+c_kq_k^{k-1}
\end{aligned}$$

由于它的系数矩阵的行列式（范德蒙,Vandermonde,行列式）

$$\begin{vmatrix}
1 & 1 & 1 & \cdots & 1\\
q_1 & q_2 & q_3 & \cdots & q_k\\
\vdots & \vdots & \vdots & \vdots & \vdots\\
q_1^{k-1} & q_2^{k-1} & q_3^{k-1} & \cdots & q_k^{k-1}
\end{vmatrix} \neq 0$$

线性方程组有确定解。换言之，$q_1,q_2,\cdots,q_k$ 是它的 k 个不同的特征根，当且仅当

$$H(n)=c_1q_1^n+c_2q_2^n+\cdots+c_kq_k^n \ (c_1,c_2,\cdots c_k\text{为确定的常数})$$

是递归关系式 $H(n)+b_1H(n-1)+b_2H(n-2)+\cdots+b_kH(n-k)=0$ 的解。

事实上，在 7.1 中这一定理已经得到了运用。我们再来看一个例子。

【例 7-4】 解下列递归关系式：

$H(0)=0, H(1)=1, H(2)=2$

$$H(n)=H(n-1)+9H(n-2)-9H(n-3) \quad (n\geqslant 3)$$

解 递归关系式的特征方程是

$$x^3-x^2-9x+9=0$$

解之，得三个根：$x_1=1,\ x_2=3,\ x_3=-3$，于是有递归关系式的通解

$$H(n)=c_1(1)^n+c_2(3)^n+c_3(-3)^n=c_1+c_2\,3^n+c_3(-3)^n$$

将初始值 $H(0)=0, H(1)=1, H(2)=2$ 代入，得到一方程组

$$\begin{aligned}
c_1+c_2+c_3 &= 0\\
c_1+3c_2-3c_3 &= 1\\
c_1+9c_2+9c_3 &= 2
\end{aligned}$$

解这个方程组得：$c_1=-\frac{1}{4}, c_2=\frac{1}{3}, c_3=-\frac{1}{12}$

因此，递归关系式的通解是

$$\begin{aligned}
H(n) &= -\frac{1}{4}+\frac{1}{3}\cdot 3^n-\frac{1}{12}(-3)^n\\
&= -\frac{1}{4}+3^{n-1}+\frac{1}{4}(-3)^{n-1}
\end{aligned}$$

【例 7-5】 某人有 $n(n\geqslant 1)$ 元钱，他每一天购买一次物品，或者买一元钱的甲物品，

或者买二元钱的乙物品，或者买二元钱的丙物品。问：此人有多少种方式花完这 n 元钱。

解 设花完这 n 元钱的方式有 $H(n)$ 种，那么，（1）他第一次购物买一元钱的甲物品的话，则花完余下的 $n-1$ 元有 $H(n-1)$ 种方式；（2）他第一次购物买二元钱的乙物品的话，则花完余下的 $n-2$ 元有 $H(n-2)$ 种方式；（3）他第一次购物买二元钱的丙物品的话，则花完余下的 $n-2$ 元有 $H(n-2)$ 种方式。因此

$$H(n)=H(n-1)+2H(n-2)\ \ (n\geqslant 3)$$

而且 $H(1)=1,\ H(2)=3$。利用特征根方法解之，可得

$$H(n)=\frac{1}{3}(2^{n+1}+(-1)^n)$$

但是，上述解法对于特征方程有重根的情况是无效的。

【例 7-6】 解下列递归关系式：

$$H(0)=1, H(1)=3$$

$$H(n)=4H(n-1)-4H(n-2)\ \ (n\geqslant 2)$$

解 递归关系式的特征方程是

$$x^2-4x+4=0$$

解之，得二个重根：$x_1=2,\ x_2=2$，于是有递归关系式的通解

$$H(n)=c_1 2^n+c_2 2^n=(c_1+c_2)2^n=c2^n$$

将初始值 $H(0)=1, H(1)=3$, 代入，得到一个矛盾方程组

$$c=1\quad ,\quad 2c=3$$

求解失败。

显然，必须改进上述方法，改进的依据是以下的定理。

定理 7-3 设 $q_1, q_2, \cdots, q_t$ 是非零实数或复数，它们是递归关系式

$$H(n)+b_1H(n-1)+b_2H(n-2)+\cdots+b_kH(n-k)=0\ \ (k\leqslant n, b_k\neq 0)$$

的特征方程的 $t(\leqslant k)$ 个不同的特征根，各有 $e_1, e_2, \cdots, e_t$ 重。那么该递归关系式的一般解是

$$H(n)=H_1(n)+H_2(n)+\cdots+H_t(n)$$

其中

$$H_i(n)=c_1q_i^n+c_2nq_i^n+\cdots+c_{e_i}n^{e_i}q_i^n\ \ (i=1,2,\cdots,t;\ c_1,c_2,\cdots c_{e_i}\text{为确定的常数})$$

定理的证明涉及范德蒙行列式的推广形式等知识，我们不作介绍，通过一些例子直观地诠释这一定理的意义。

【例 7-7】 （续例 7-6）根据定理 7-3，例 7-6 递归关系式的通解是

$$H(n)=H_1(n)=c_1 2^n+c_2 n2^n$$

将初始值 $H(0)=1, H(1)=3$, 代入，得到方程组

$$1=c_1\quad ,\quad 3=2c_1+2c_2$$

从而 $c_1=1$，$c_2=\frac{1}{2}$。故例 7-6 递归关系式的解是 $H(n)=2^n+2^{n-1}n$

【例 7-8】 解下列递归关系式：

$H(0)=1, H(1)=0, H(2)=1, H(3)=2$

$H(n)=-H(n-1)+3H(n-2)+5H(n-3)+2H(n-4)\ \ (n\geq 4)$

解 递归关系式的特征方程是

$$x^4+x^3-3x^2-5x-2=0$$

解之，得四个根：$x_1=-1,\ x_2=-1,\ x_3=-1, x_4=2$。于是有递归关系式的通解

$$H_1(n)=c_1(-1)^n+c_2n(-1)^n+c_3n^2(-1)^n$$

$$H_2(n)=c_4 2^n$$

因此

$$H(n)=c_1(-1)^n+c_2n(-1)^n+c_3n^2(-1)^n+c_4 2^n$$

将初始值 $H(0)=1, H(1)=0, H(2)=1, H(3)=2$ 代入，得到一方程组

$$\begin{aligned} c_1+c_4&=1\\ -c_1-c_2-c_3+2c_4&=0\\ c_1+2c_2+4c_3+4c_4&=1\\ -c_1-3c_2-9c_3+8c_4&=2 \end{aligned}$$

解这个方程组得

$$c_1=\frac{7}{9}, c_2=-\frac{1}{3}, c_3=0, c_4=\frac{2}{9}$$

因此，本题的解是

$$H(n)=\frac{7}{9}(-1)^n-\frac{1}{3}n(-1)^n+\frac{2^{n+1}}{9}$$

*7.2.3 一些特殊递归关系的求解

下文要讨论的一些特殊的递归关系包括：常系数线性非齐次递归关系的几种特殊情况，非常系数、非线性、非齐次递归关系以及联列递归关系的一些特殊例子，它们都没有一般的解法。

常系数线性非齐次递归关系（下简称非齐次递归关系）

$$H(n)+b_1H(n-1)+b_2H(n-2)+\cdots+b_kH(n-k)=f(n)$$

在 $f(n)$ 的一些特殊情况下是可解的，有时可以运用迭代求解方法，有时可以运用归约的方法，将它们化为常系数线性齐次递归关系。还有其他一些求解非齐次递归关系的方法，如运用特征根的方法，生成函数的方法等，但它们超出了本教材的既定范围。在此不予介绍。

实际上，本节例 7-2，例 7-3 就是用迭代求解方法求解非齐次递归关系的例子。

一般地，当 $f(n)$ 为一 n 的多项式或 a^n（a 为常数）时，可运用将非齐次递归关系归约为齐次递归关系的方法来求解。我们通过两个例子加以介绍。

【例 7-9】 解下列递归关系式：

$H(0)=2$

$$H(n)-2H(n-1)=n \quad (n\geqslant 1)$$

解 由 $H(n)-2H(n-1)=n$ 导出 $H(n+1)-2H(n)=n+1$，并将它们的等式两边对应相减，以消除等式右边的 n（或降低等式右边 n 的指数），可得

$$H(n+1)-3H(n)+2H(n-1)=1$$

由此再导出 $H(n)-3H(n-1)+2H(n-2)=1$，再将它们的等式两边对应相减，以消除等式右边的常数（或再降低等式右边 n 的指数），可得

$$H(n+1)-4H(n)+5H(n-1)-2H(n-2)=0$$

这已经是一个常系数线性齐次递归关系，我们已经有成熟的方法来求解。

（1）先由 $H(0)=2$ 和 $H(n)-2H(n-1)=n$ 求出 $H(1)=6$，$H(2)=15$。

（2）再求齐次递归式的特征方程和特征根：$x^3-4x^2+5x-2=0$，$x_1=2, x_2=1$，$x_3=1$。

（3）$H(n)$的通解是：$H(n)=c_1 2^n+c_2 n+c_3$

（4）利用上式及 $H(0)=2$，$H(1)=6$，$H(2)=15$，解得

$$c_1=\frac{5}{2}, c_2=-1, c_3=-2$$

最终求得 $H(n)=5\cdot 2^{n-1}-n-2$。

【例 7-10】 解下列递归关系式：

$$H(0)=1$$

$$H(n)-H(n-1)=a^{n-1} \quad (n\geqslant 1)$$

解 由 $H(n)-H(n-1)=a^{n-1}$ 可以得到

$$H(n-1)-H(n-2)=a^{n-2}$$

$$H(n-2)-H(n-3)=a^{n-3}$$

$$\vdots$$

$$H(2)-H(1)=a$$

$$H(1)-H(0)=a^0=1$$

将这些等式的两边对应相加得

$$H(n)-H(0)=a^{n-1}+a^{n-2}+\cdots+a+1$$

即

$$H(n)=1+\frac{a^n-1}{a-1}$$

非常系数、非线性递归关系式更无常规方法，但有些非常系数、非线性递归关系式也可以通过一定的转换，变成常系数线性齐次递归关系式，或变成常系数线性非齐次递归关系式的上述几种形式来求解。

【例 7-11】 解下列递归关系式：

（1）$G(0)=2$

$$G^2(n)-2G^2(n-1)=1 \quad (n\geqslant 1)$$

（2）$G(0)=273$

$$n\cdot G(n)+(n-1)\cdot G(n-1)=2^n \quad (n\geqslant 1)$$

（3）$G(0)=2$

$$G(n)-n\cdot G(n-1)=n! \quad (n\geqslant 1)$$

解 （1）令 $H(n)=G^2(n)$，则递归关系式变为

$$H(0)=4$$

$$H(n)-2H(n-1)=1 \quad (n\geqslant 1)$$

用迭代求解的方法解得 $H(n)=5\cdot 2^n-1$，因此 $G(n)=\sqrt{5\cdot 2^n-1}$ 。

（2）令 $H(n)=n\bullet G(n)$，则递归关系式变为

$$H(0)=0$$

$$H(n)+H(n-1)=2^n \quad (n\geqslant 1)$$

用非齐次递归关系式的特征根方法可解之，也可用迭代求解的方法解之。结果是

$$H(n)=\frac{2}{3}((-1)^{n+1}+2^n)$$

$$G(0)=273 \ ， \ G(n)=\frac{2}{3n}((-1)^{n+1}+2^n) \quad (n\geqslant 1)$$

（3）令 $H(n)=\frac{1}{n!}G(n)$，则递归关系式变为

$$H(0)=2$$

$$H(n)-H(n-1)=1 \quad (n\geqslant 1)$$

用迭代求解的方法解之。结果是

$$H(n)=n+2$$

$$G(0)=2 \ ， \ G(n)=n!(n+2) \quad (n\geqslant 1)$$

最后，我们给出一个联列递归关系求解的例子，使用的仍然是归约成常系数线性齐次递归关系式的方法。

【例 7-12】 在图 7-1 的长方形 *ACDB* 中，$AB:AC=\frac{1+\sqrt{5}}{2}$，在 *ABCD* 中作一个正方形 *AXYC*，证明长方形 *XBDY* 相似于 *ACDB*。如果同前继续在长方形 *XBDY* 中作正方形，并不断这样做，证明，每次所得长方形均相似于长方形 *ACDB*。

证明 设 $AC=1$，$AB=\frac{1+\sqrt{5}}{2}$，因此，$XB=\frac{1+\sqrt{5}}{2}-1=\frac{\sqrt{5}-1}{2}$，从而

$$BD:XB=1:\frac{\sqrt{5}-1}{2}=\frac{2}{\sqrt{5}-1}=\frac{1+\sqrt{5}}{2}=AB:AC$$

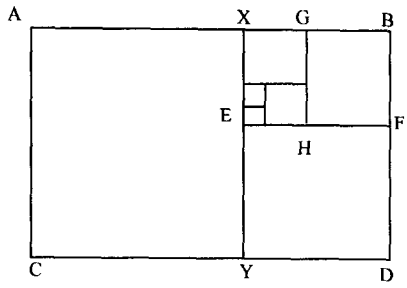


图 7-1

长方形 *XBDY* 相似于 *ACDB* 得证。

若用 $L(n)$ 表示第 n 个长方形的长边，用 $B(n)$ 表示第 n 个长方形的短边 $(n\geqslant 1)$，那么根据题意我们有

$$\begin{cases} L(n)=B(n-1) \\ B(n)=L(n-1)-B(n-1) \end{cases} \quad (n\geqslant 2)$$

以及初值 $\begin{cases} L(1)=\dfrac{1+\sqrt{5}}{2} \\ B(1)=1 \end{cases}$

由联列递归关系式可以得到

$$L(n)=B(n-1)=L(n-2)-B(n-2)=L(n-2)-L(n-1)$$

即

$$L(n)=L(n-2)-L(n-1) \quad (n\geqslant 3)$$

这是一个常系数线性齐次递归关系式，并有初值 $L(1)=\dfrac{1+\sqrt{5}}{2}$，$L(2)=1$。解这个递归关系式，得

$$L(n)=\left(\frac{3+\sqrt{5}}{2}\right)\left(\frac{\sqrt{5}-1}{2}\right)^{n} \quad , \quad B(n)=\left(\frac{3+\sqrt{5}}{2}\right)\left(\frac{\sqrt{5}-1}{2}\right)^{n+1}$$

从而

$$L(n)=\left(\frac{\sqrt{5}-1}{2}\right)L(n-1) \quad , \quad B(n)=\left(\frac{\sqrt{5}-1}{2}\right)B(n-1)$$

故 $L(n):B(n)=L(n-1):B(n-1)$，也就是说，每次所作长方形均相似于前次所作长方形，因而均相似于长方形 *ACDB*。

7.3 练习

1．用以下方式解下列递归关系式：先考虑前几个数值，并推测解的公式，然后用数学归纳法证明你得到的公式。

（1） $H(0)=1, H(n)=3H(n-1)$

（2） $H(0)=2, H(n)=H(n-1)-n+3$

（3） $H(0)=0, H(n)=-H(n-1)+1$

（4） $H(0)=0, H(1)=1, H(n)=4H(n-2)$

2．考虑一个$1\times n$的棋盘。假定我们对棋盘的每一个格子用红或蓝两种颜色之一去着色。令$g(n)(n=1,2,3\cdots)$表示“没有红色格子相邻的着色数目”。建立$g(n)$应满足的递归关系式，并求出$g(n)$的通项公式。

3．一楼梯有 n 级台阶，某人由下向上走。若每一步只能跨一级或两级楼梯，问他从地面走到第n级楼梯有多少种走法。

4．证明下列费波那契数列的性质：

（1） $F(0)+F(1)+F(2)+\cdots+F(n)=F(n+2)-1$

（2） $F(1)+F(3)+\cdots+F(2n-1)=F(2n)$

（3） $F(0)+F(2)+F(4)+\cdots+F(2n)=F(2n+1)-1$

5．平面上有 n 条两两相交的直线，又没有任何三条直线交于一点。问它们在平面上共分割出多少不同的区域。（要求用递归关系式求解）

6．用迭代的方法解以下递归关系式，并用数学归纳法证明你的结论。

（1） $h(0)=1$， $h(n)=3h(n-1)$

（2） $h(0)=1$， $h(n)=-h(n-1)+2$

（3） $h(0)=2$， $h(n)=h(n-1)-n+3$

（4） $h(0)=2$， $h(n)=(n+2)h(n-1)$

7．（1）设$h(n,k)$是集合$\{1,2,3,\cdots,n\}$的没有两个连续整数的k元素子集的个数。试建立$h(n,k)$所满足的递归关系。（提示：分别考虑数n被选入的k元素子集和数n不被选入的k元素子集）

（2）利用（1）和对n的数学归纳法证明

$$h(n,k)=C(n-k+1,k)$$

8．在信道上传输字母表$\{a,b,c\}$上的长度为n的字，且规定有两个a连续出现的字拒绝传输。试确定这个信道允许传输的字母表 $\{a,b,c\}$上长度为n的字共有多少个？

9．考察一个受控环境里细菌的繁殖问题。设$h(r)$表示第r天里细菌的数目。我们定义在第r天里细菌的增长率为$h(r)-2h(r-1)$。现设$h(0)=1$，约定$h(-1)=0$，如果已知增长率每天翻一番，求$h(r)$的解。

10．解下列递归关系式：

$$H(0)=0, H(1)=1, H(2)=1, H(3)=2$$

$$H(n)=5H(n-1)-6H(n-2)-4H(n-3)+8H(n-4)\ \ (n\geq 4)$$

11．解下列递归关系式：

$$H(0)=2$$

$$H(n)+2H(n-1)=n+1\ \ (n\geq 1)$$

12．解下列递归关系式：

$$H(0)=1$$

$$H(n)-H(n-1)=a^{n-1}+b^{n+1}\ \ (n\geq 1)$$

第8章 图

图论（graphic theory）是一门既古老又年轻的学科。说它古老，是因为早在 18 世纪初，学者们便已运用现在称之为图的工具来解决一些困难的问题；说它年轻，是因为直到 20 世纪中、后期，尤其是随着计算机科学与技术的发展，图的理论研究和应用研究才得到迅速广泛的重视，图论作为一个数学的分支，才真正确立了自己的地位。

图论的起源可以追溯到 1736 年，瑞士数学家欧拉（Euler）解决了当时很有名的哥尼斯堡七桥问题，并发表第一篇图论方向的论文。哥尼斯堡（后来的加里宁格勒）位于立陶宛的普雷格尔河畔。河中有两个小岛，河两岸及两个小岛之间由七座小桥相联（如图 8-la 所示）。当时城中居民提出了这样一个有趣的问题：游人是否可能从城市或小岛的一点出发，经由七座桥，并且只经由每座桥一次，然后回到原地。许多人久而不得其解，但欧拉却用一个十分简明而又很有代表性的方法——抽象为一张图（如图 8-1b 所示）解决了这一问题。并研究一般的图何时有这样的解。图 8-1b 中的小圆圈叫做结点，用以表示河两岸及两个小岛；结点间的线段或弧线叫做边，用以表示小桥，如果游人可以作出所要求的那种游历，那么必可从图的某一结点出发，经过每条边一次且仅经过一次后又回到原结点。这对每个结点而言，每进入一次，总相应地要离开一次，而每次离开不得重复同一条边，因而它应当与偶数条边相联结。由于图 8-1b 中并非每个结点都与偶数条边相联结，因此欧拉作出结论：游人不可能作出所要求的游历。

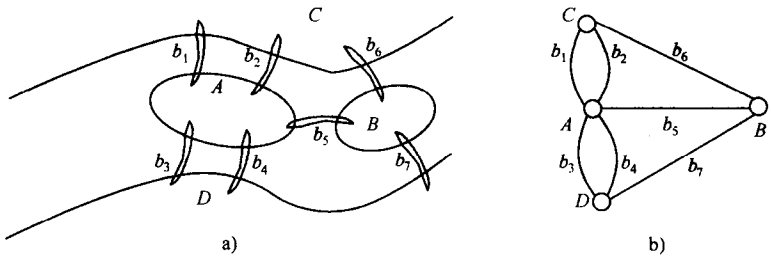


图 8-1

图 8-1b 是 8-1a 的抽象。我们看到，与几何图形不同，图 8-1b 中图形的结点位置、边的长短、形状无关紧要，人们只关心其中结点与边的联结关系。像这样由结点和联结结点的边所组成的离散结构及其直观表示形式就是本章和第 9 章要讨论的图。

我们现在所要研究的图，是建立和处理离散对象及其关系即离散结构模型的一个重要工具。在各类关系表示、运筹规划作业、网络技术研究、以及计算机程序流程分析中，都会遇到由这种“结点”和“边”组成的图。它在计算机科学及其应用的许多领域，如数据结构、操作系统、编译方法、人工智能、形式语言、网络理论、信息的组织与检索等，均起着重要作用。它广泛应用于生物学、心理学、遗传学、地理学、物理学、化学、经济学、社会学、语言学、控制论、运筹学等几乎所有的学科。

本章的任务是讨论图的基本概念及有关术语，研究图的最基本的性质。

8.1 图的基础知识

8.1.1 图的基本概念

定义 8-1 **图**（graph）G 由两个部分所组成：

（1）非空集合 $V(G)$，称为图 G 的结点集，其成员称为**结点或顶点**（nodes or vertices）。结点用拉丁字母或希腊字母来表示。

（2）多重集合 $E(G)$，称为图 G 的边集，其成员称为**边**(edges)。边用结点的序偶和结点的两元素多重集表示。结点序偶表示的边称为**有向边**（directed edges），两元素多重集表示的边称为**无向边**（indirected edges）。

当图的边均为有向边时，称该图为**有向图**（directed graph）；当图的边均为无向边时，称该图为**无向图**（indirected graph）。

以下图论术语是经常会用到的。

边 $e=<u,v>$时，称边 e **关联**端点 u，v,并称 u 为 e 的**起点**，v 为 e 的**终点**。边 $e=\{u,v\}$ 时，称边 e **关联**结点 u，v,并称 u，v 为 e 的**端点**，这时 u，v 为**相邻**（**接**）的结点。当 $u=v$ 时，$<u,v>$和$\{u,v\}$**均称为环**。

因此，图 G 常用二元序组$<V(G), E(G)>$，或$<V, E>$来表示。显然，图是一种离散数学结构。严格地说，图 8-1b 是一个图的直观表示，称为图的**图示**。

【例 8-1】

（1）图 8-1b 为一无向图的图示，可表示为

$$<\{A,B,C,D\},\{\{A,C\},\{A,C\},\{A,D\},\{A,D\},\{A,B\},\{C,B\},\{D,B\}\}>$$

（2）图 8-2 为一有向图的图示，可表示为

$$<\{v_1,v_2,v_3,v_4,v_5,v_6\},\{<v_1,v_1>,<v_2,v_3>,<v_3,v_2>,<v_3,v_4>,<v_1,v_4>,<v_5,v_5>\}>$$

定义 8-2 设图 G 为$<V, E>$。

（1）当 V 和 E 为有限集时，称 G 为**有限图**，否则称 G 为**无限图**。本书只讨论有限图。

（2）当边集合中至少有一个元素的重数不小于 2 时，称 G 为**重图**，否则称 G 为**单图**；重数不小于 2 的边称为**重边**，或**平行边**。

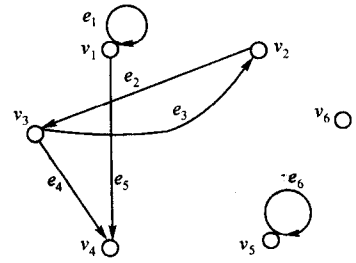


图 8-2

（3）无环和重边的无向图称为**简单图**。当 G 为有限简单图时，也常用（n，m）表示图 G，其中 $n=|V|$，$m=|E|$ 。

（4）任何两个不同结点间都有边关联的简单图，称为**完全图**。n 个顶点的完全图常记作 K_n。不是任何边的端点的结点称为**孤立结点**，仅由孤立结点构成的图（$E=\varnothing$）称为**零图**。

（5）当给 G 赋予映射 f：$V\to W$，或 g：$E\to W$，W 为任意集合，常为实数集的子集，此时称 G 为**赋权图**，用$<V,E,f>$或$<V,E,g>$或$<V,E,f,g>$表示之。$f(v)$称为结点 v 的**权**，$g(e)$称为边 e 的**权**。

【例 8-2】 图 8-1b 为重图，b_1，b_2 为重边。图 8-2 为有向图，e_1 为环，v_6 为孤立结点。

图 8-3a 为简单图，b 为完全图 K_5，c 为赋权图，$f(v_1)=7.3$，$g(e_1)=800$。

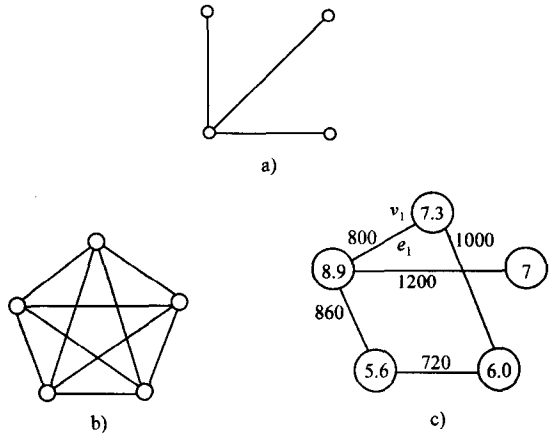


图 8-3

8.1.2 结点的度

结点所邻接的边的数目是图的性质的重要判据，这里给出有关的定义及性质。

定义 8-3 在无向图中，结点 v 的**度**（degree）$d(v)$是 v 作为边的端点的数目。在有向图中，结点 v 的**出度**是 v 作为有向边起点的数目，v 的**入度**是 v 作为有向边终点的数目。因此，结点 v 的度 $d(v)$是 v 的**出度** $d^+(v)$（out-degree）与**入度** $d^-(v)$（in-degree）的和。

【例 8-3】 图 8-4a 中，$d(v1)=5$，（注意：环 e 两次以结点 v_1 为端点）。图 8-4b 中 $d^+(v_1)=2$，$d^-(v_1)=3$，$d(v_1)=d^+(v_1)+d^-(v_1)=5$。

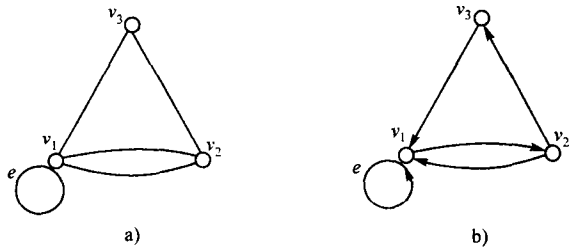


图 8-4

关于结点的度有下列性质。

定理 8-1 对任意图 G，设其边数为 m，顶点集为$\{v_1, v_2, \cdots, v_n\}$，那么

$$\sum_{i=1}^{n} d(v_i) = 2m \tag{8-1}$$

证明 当一边关联于两个不同结点时，它分别使两结点各增加一度；当一边为一环时，它给该结点增加两度，因此各结点的度的总和是边的数目的两倍。

当 G 为有向图时，式（8-1）可改写为

$$\sum_{i=1}^{n} d(v_i) = \sum_{i=1}^{n} d^+(v_i) + \sum_{i=1}^{n} d^-(v_i) = 2m$$

$$\sum_{i=1}^{n} d^+(v_i) = \sum_{i=1}^{n} d^-(v_i) = m$$

证明非常简单，此不赘述。

定理 8-2 图的奇数度顶点必为偶数个。

证明 反设某图有奇数个奇数度的顶点，那么它们的度的总和是奇数。由于其余顶点为偶数度的，从而其度的总和为偶数。于是，图的所有顶点的度数总和为奇数（奇数与偶数的和），与定理 8-1 矛盾。命题得证。

定理 8-3 自然数序列（$a_1,a_2,\cdots,a_n$）称为一个**度序列**，如果它是一个图的顶点的度的序列。（$a_1,a_2,\cdots,a_n$）为一个度序列，当且仅当 $\sum_{i=1}^{n} a_i$ 为一偶数。

证明 必要性由定理 8-1 立得。

为证充分性，设 $\sum_{i=1}^{n} a_i$ 为偶数，那么（$a_1,a_2,\cdots,a_n$）中的奇数必定是偶数个。建立 n 个顶点的图 G，使得

（1）当 a_i 为偶数 $2k$ 时，v_i 上恰有 k 个环。

（2）当 a_i 为奇数 $2k+1$，必有 a_j 为奇数（因为（$a_1,a_2,\cdots,a_n$）中的奇数有偶数个）。可使 v_i 上恰有 k 个环及一条非环的边，此边以顶点 v_j 为另一个端点。

由于为奇数的 a_i 是偶数个，上述构作过程是可行的。很显然，作得的图 G 满足 $d(v_i)=a_i$。

以下两个与度有关的术语是常用的。

定义 8-4 一度的顶点称为**悬挂点**（pendant nodes）。

定义 8-5 各顶点的度均相同的图称为**正则图**（regular graph）。各顶点度均为 k 的正则图称为 **k-正则图**。

当然，完全图都是正则图。

8.1.3 子图、补图及图同构

定义 8-6 设图 $G1=<V1, E1>$，$G2=<V2, E2>$，称 $G1$ 为 $G2$ 的**子图**（subgraph），如果 $V1\subseteq V2$，$E1\subseteq E2$。称 $G1$ 为 $G2$ 的**真子图**，如果 $G1$ 是 $G2$ 的子图，且 $G1$ 不同于 $G2$。称 $G1$ 为 $G2$ 的**生成子图**（spanning subgraph），如果 $G1$ 是 $G2$ 的子图，且 $V1=V2$。

定义 8-7 设无向图 $G1=<V1, E1>$，$G2=<V2, E2>$，如果 $V1=V2$，$E1\cap E2=\varnothing$，且 $<V1$（或 $V2$），$E1\cup E2>$ 是完全图，称 $G1$ 与 $G2$ 互为**补图**。

【例 8-4】 图 8-5a、b 都是 c 的真子图。图 8-5a、b 关于 c 互为**补图**，c 为完全图 K_5。

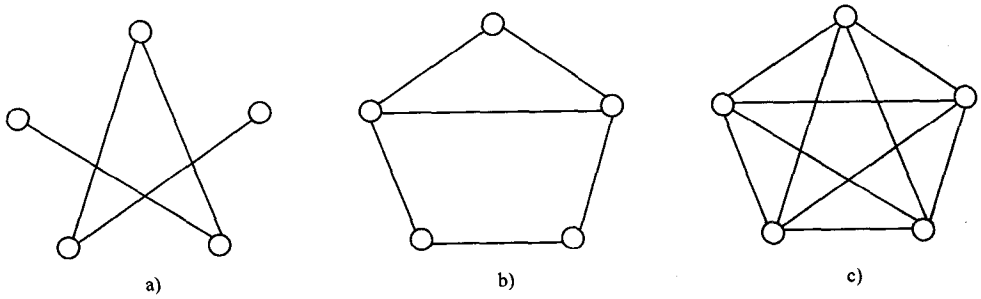


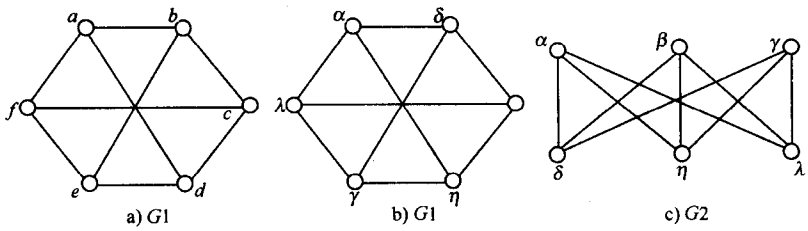
图 8-5

如果仅仅改变图的各顶点名及边名，或仅仅改变边的形状（不改变边对结点的关联关系），那么所得的图在本质上与原图没有区别。

定义 8-8 设 $G1=<V1, E1>$，$G2=<V2, E2>$为两个简单图，称 $G1$ 与 $G2$ **同构**（isomorphic），如果$|V1|=|V2|$，$|E1|=|E2|$，并且存在一种方式将 V1 中结点的名一一对应地置换为 $V2$ 中结点的名，可使置换得到的图 G_1'满足 $G_1'=G2$（即 $V_1'=V_2'$，$E_1'=E2$）。

【例 8-5】 （1）图 8-6a、c 表示的两图 $G1$，$G2$ 是同构的，因为可以如下将 $V1$ 中结点的名一一对应地置换为 $V2$ 中结点的名，可使得到的图 G_1'满足 $G_1'=G2$。其对应置换为：

$V1$	a	b	c	d	e	f
$V2$	α	δ	β	η	γ	λ

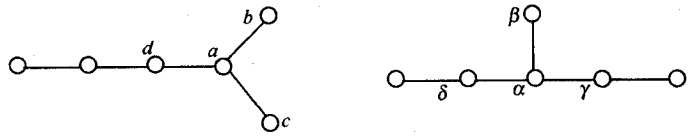


a) $G1$　　b) $G1$　　c) $G2$

图 8-6

（2）图 8-7 中 a，b 表示的两图 $G1$，$G2$ 不是同构的，定义 8-8 中所说“一一对应的置换”无法找到，因为这种一一对应的置换必定满足 a 置换为α（它们是两图中仅有的三度顶点），从而使 b，c，d 分别对应于β，γ，δ（或它们的另一排列），因而总有 $G1$ 中一个悬挂点对应于 $G2$ 中的一个二度结点，因而不可能使得 $G_1'=G2$。

本例指出了一个判断两图不同构的一种策略，即找出两图的一个根本的不同点，它在顶点名的置换中不可能被消除。



a) $G1$　　b) $G2$

图 8-7

8.2 路径、回路及连通性

8.2.1 路径与回路

定义 8-9 图 G 的顶点 v_1 到顶点 v_l 的**拟路径**（pseudo path）是指如下顶点与边的序列：

$$v_1,e_1,v_2,e_2,v_3,\cdots,v_{l-1},e_{l-1},v_l \tag{8-3}$$

其中 $v_1,v_2,v_3,\cdots,v_{l-1},v_l$ 为 G 的顶点，$e_1,e_2,\cdots,e_{l-1}$ 为 G 的边，且 $e_i(i=1,2,\cdots,l-1)$以 v_i 及 v_{i+1} 为端点，（对有向图 G，e_i 以 v_i 为起点，以 v_{i+1} 为终点），拟路径的边数 $l-1$ 称为该拟路径的

长度。当 e_i($i=1,2,\cdots,l-1$)各不相同时，该拟路径称为**路径**（walk），又当 $v_i(i=1,2,\cdots,l)$ 各不相同时(除 v_1 与 v_l)，则称此路径为**通路**（Path）。$v_1=v_l$ 的路径称为**闭路径**（closed walk）；$v_1=v_l$ 的通路称为**回路**（circuit）。

当讨论限于简单图或无平行边的有向图时，上述拟路径、路径、通路等可用顶点序列来表示，例如用（$v_1,v_2,v_3,\cdots,v_{l-1},v_l$）代替式（8-3）。

【例 8-6】

（1）在图 8-8a 的有向图中：

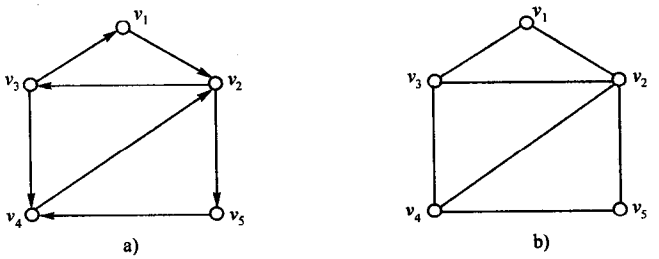


图 8-8

（v_1,v_2,v_3,v_1,v_2,v_5）为一拟路径，长度为 5。

（v_2,v_3,v_1,v_2,v_5,v_4）为一路径，长度为 5。

（v_2,v_3,v_4）为一通路，长度为 2。

（$v_2,v_3,v_1,v_2,v_5,v_4,v_2$）为一闭路径，长度为 6。

（v_2,v_3,v_1,v_2）为一回路，长度为 3。

（2）在图 8-8b 的无向图中：

（v_2,v_3,v_4,v_5）为一路径（它在 a 中不是路径），长度为 3。

（v_1,v_2,v_5,v_4,v_3,v_1）为一回路，长度为 5。

关于路径和回路有以下定理。

定理 8-4 在有 n 个顶点的图 G 中，如果有从顶点 u 到 v（$u\neq v$）的拟路径，那么从 u 到 v 必有路径，并且必有长度不大于 $n-1$ 的通路。

证明 不设一般性，设 G 为一简单图。若 G 有从 u 到 v 的拟路径（$u=v_1,v_2,v_3,\cdots,v_{l-1},v_l=v$），且没有 $v_i=v_j$（$i,j=1,2,\cdots,l$），那么它便是一条通路，且 $l\leqslant n-1$；若 G 的这一拟路径中有，$v_i=v_j$,则它可表示为

$$(u=v_1,v_2,\cdots,v_i,\cdots,v_i,\cdots,v_{l-1},v_l=v)$$

那么从中删去从 v_{i+1} 到第二个 v_i 之间的所有边及顶点，便得到一条从 u 到 v 的更短的拟路径

$$(u=v_1,v_2,\cdots,v_i,\cdots,v_{l-1},v_l=v)$$

然后重复上述讨论，直至没有边重复出现、没有顶点重复出现，从而得到从 u 到 v 的路径和长度不超过 $n-1$ 的通路。

完全类似地可以证明定理 8-5。

定理 8-5 在具有 n 个顶点的图 G 中，如果有从 v 到 v 的闭路径，那么必定有一条从 v 到 v 的长度不大于 n 的回路。

【例 8-7】

（1）图 8-8a 中有 v_2 到 v_4 的拟路径

$(v_2, v_3, v_1, v_2, v_5, v_4)$

因而可求得从 v_2 到 v_4 的长度为 2 ($\leqslant 4$)的通路 (v_2, v_5, v_4)。

（2）图 8-11b 中有经由 v_2 的闭路径

$(v_2, v_3, v_1, v_2, v_5, v_4, v_2)$

从而有经由 v_2 的长度为 3（$\leqslant 5$）的回路 (v_2, v_5, v_4, v_2)。

8.2.2 连通性

定义 8-10 称图中顶点 u 到 v 是**可达的**（accesible），如果 $u=v$，或者有一条 u 到 v 的路径。

定义 8-11 称无向图 G 是**连通的**（connected），如果对 G 的任何两个顶点 u，v，u 到 v 都是可达的。称有向图 G 是**强连通的**，如果 G 的任何两个顶点都是相互可达的；称有向图 G 是**单向连通的**，如果 G 的任何两个顶点中，至少从一个顶点到另一个顶点是可达的；称有向图 G 是**弱连通的**，如果 G 的有向边被看作无向边时是连通的。

定义 8-12 图 G'称为图 G 的**连通分支**（connected components），如果 G'是 G 的子图，G'是连通的，并且不存在 G 的真子图 G''，使 G''是连通的，且 G''以 G'为真子图。

【例 8-8】 图 8-9a 为一连通图，b 为含两个连通分支的不连通图，c 为弱连通图，d 为单向连通图，e 为强连通图。

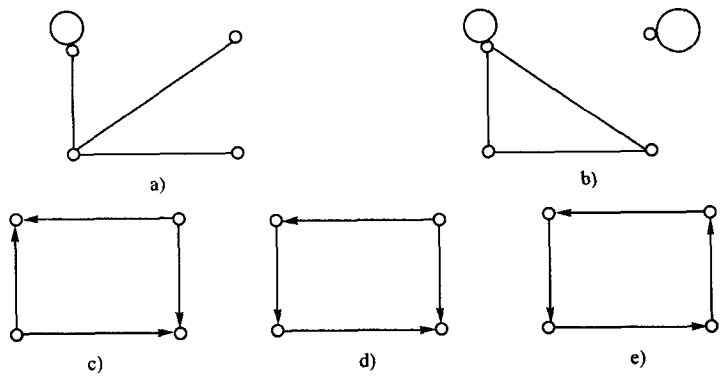


图 8-9

定义 8-13 设 G'为有向图 G 的子图，若 G'是强连通的（单向连通的、弱连通的），且 G 没有强连通（单向连通、弱连通）的真子图 G''，使 G'为其真子图，那么称 G'为 G 的一个**强分图**（**单向分图**、**弱分图**）。

【例 8-9】 在图 8-10 中：

强分图有：$<\{1,2,3\},\{e_0,e_2,e_3\}>$，$<\{4\},\varnothing>$，$<\{5\},\varnothing>$，$<\{6\},\varnothing>$，$<\{7,8\},\{e_7, e_8\}>$，$<\{9\},\varnothing>$

单向分图有：$<\{1,2,3,4,5\},\{e_0,e_1,e_2,e_3,e_4,e_5\}>$，$<\{5,6\},\{e_6\}>$，$<\{7,8\},\{e_7, e_8\}>$，$<\{9\},\varnothing>$

弱分图有：$<\{1,2,3,4,5,6\},\{e_0,e_1,e_2,e_3,e_4,e_5,e_6\}>$，$<\{7,8\},\{e_7, e_8\}>$，$<\{9\},\varnothing>$

关于无向图的连通性有下列定理。

定理 8-6 一个图 G 是不连通的，当且仅当 G 的顶点集 V 可以分成两个不交的非空子集 $V1$ 和 $V2$，使得任何边都不以 $V1$ 的一个顶点和 $V2$ 一个顶点为其两端点。

证明 充分性是显然的。

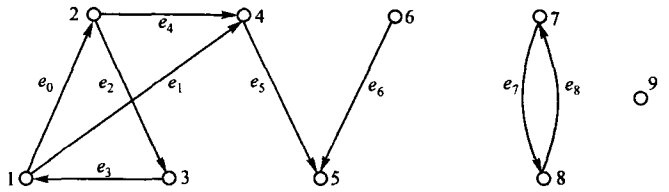


图 8-10

现证必要性。设 G 是不连通的，那么有 $v1$ 及 $v2$，$v2$ 到 $v1$ 是不可达的。令

$V1=\{v \mid v$ 到 $v1$ 是可达的$\}$

$V2=V-V1$

显然 $V1\neq\varnothing$，$V2\neq\varnothing$，因为 $v1\in V1$，$v2\in V2$。若有边的两端点分别在 $V1$ 和 $V2$ 中，那么该边在 $V2$ 中的端点到 $v1$ 是可达的了，这与 $V2$ 的定义冲突。

定理 8-7 如果图 G 有两个不同的奇数度的顶点 u，v，那么 u 到 v 必定是可达的。

证明 如果 u 到 v 不可达，那么 G 不是连通的，u 与 v 必分属于两个连通分支 $G1$，$G2$，而 $G1$，$G2$ 是 G 的子图，且都恰有一个奇数度顶点，这是不可能的（定理 8-2），因而 u 到 v 是可达的。

定理 8-8 若图 G 为具有 n 个顶点、k 个连通分支的简单图，那么 G 至多有 $\dfrac{(n-k)(n-k+1)}{2}$ 条边。

证明 设 G 的 k 个连通分支的顶点数分别是 n_1，n_2，…，n_k，从而，$n=n_1+n_2+\cdots+n_k$，$n_i\geqslant 1$。

由于各连通分支的边数不超过 $\dfrac{n_i(n_i-1)}{2}$（见本章练习之 3），因此 G 的边数 m 满足：

$$m\leqslant\frac{1}{2}\sum_{i=1}^{k}n_i(n_i-1)$$

$$=\frac{1}{2}(\sum_{i=1}^{k}n_i^2)-\frac{n}{2}$$

现证

$$(\sum_{i=1}^{k}n_i^2)\leqslant n^2-(k-1)(2n-k) \tag{8-4}$$

由于 $\sum_{i=1}^{k}(n_i-1)=n-k$，因此

$$(\sum_{i=1}^{k}(n_i-1))^2=n^2+k^2-2nk\geqslant\sum_{i=1}^{k}(n_i-1)^2=\sum_{i=1}^{k}n_i^2-2\sum_{i=1}^{k}n_i+k=\sum_{i=1}^{k}n_i^2-2n+k$$

从而

$$(\sum_{i=1}^{k}n_i^2)\leqslant n^2+(k^2-2nk+2n-k)=n^2-(k-1)(2n-k)$$

式（8-4）得证。于是

$$m\leqslant\frac{1}{2}(\sum_{i=1}^{k}n_i^2)-\frac{n}{2}\leqslant\frac{1}{2}(n^2-(k-1)(2n-k)-n)=\frac{1}{2}(n-k)(n-k+1)$$

定理得证。（本章练习第 7 题为此定理之特例）

* 8.2.3 连通度

连通图的连通程度也是不同的，有的很“脆弱”，有的则相反。为了讨论这一点，这小节引入割集和连通度的概念，我们的讨论限于简单无向图。

定义 8-14 设 S 为连通图 G 的顶点集 V 的子集，称 S 为 G 的**点割集**（cut-set of nodes），如果从 G 中删除 S 中的所有顶点（注：删除结点 v 时，同时要删掉关联 v 的所有边）后得到的图不连通，但 S 的任何真子集均无这一特性。当点割集为单元素集合 $\{v\}$ 时，v 称为**割点**（cut-nodes）。

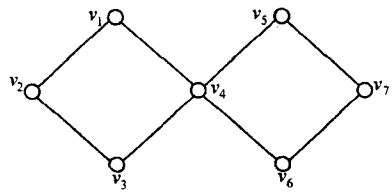


图 8-11

【例 8-10】 图 8-11 中的图有点割集$\{v_1, v_3\}$，$\{v_5, v_6\}$，v_4是割点，而$\{v_1, v_3, v_4\}$不是点割集。

定义 8-15 $\chi(G)$称为 G 的**点连通度**（node-connectivity），定义如下：

$$\chi(G)=\begin{cases}0 & \text{若}G\text{非连通图}\\ n-1 & \text{若}G\text{为}K_n\\ \min\{|S|: S\text{为点割集}\} & \text{若}G\text{连通，}G\neq K_n\end{cases}$$

例 8-10 的图的点连通度是 1。注意，依定义，单一孤立结点组成的图(K_1)的点连通度为零。

定义 8-16 设 S 为连通图 G 边集 E 的子集，称 S 为 G 的**边割集**（cut-set of edges），或**割集**，如果从 G 中删除 S 的所有边后所得的图是不连通的，但 S 的任何真子集均无这一特性。当割集为单元素集 $\{e\}$ 时，称 e 为**割边**（cut-edges）。

例 8-10 中图 8-11 有割集$\{\{v_1,v_2\},\{v_2,v_3\}\}$，$\{\{v_1,v_4\},\{v_3,v_4\}\}$等，它没有割边。$\{\{v_1,v_4\},\{v_3,v_4\},\{v_5,v_4\}\}$不是割集。

定义 8-17 $\lambda(G)$称为图 G 的**边连通度**（edge-connectivity），定义如下：

$$\lambda(G)=\begin{cases}0 & \text{当}G\text{非连通图时}\\ 0 & \text{当}G\text{为一孤立结点时}\\ \min\{|S|: S\text{为}G\text{的割集}\} & \text{否则}\end{cases}$$

例 8-10 中图 8-11 的边连通度为 2 。

很清楚，点（边）连通度是可使连通图不再连通需删去的顶点（边）的最少数目，它们的数值越小，图的连通性越脆弱。

令 $\delta(G)$表示图 G 中顶点度数的最小值（常称图 G 的最小度），则有以下定理。

定理 8-9 对任何简单无向图 G，$\chi(G)\leqslant\lambda(G)\leqslant\delta(G)$。

证明 若 G 为不连通图或单一孤立结点的图，那么据定义知：

$$\chi(G)=\lambda(G)=0\leqslant\delta(G) \text{ 或 } \chi(G)=\lambda(G)=\delta(G)=0。$$

若 G 为完全图 K_n，那么 $\chi(G)=\lambda(G)=\delta(G)=n-1$ 。

对其他情况，我们先证 $\lambda(G)\leqslant\delta(G)$。

由于度数最小的那个结点上关联的所有边被删除后，G 显然不再连通，因而 $\lambda(G)$至多是 $\delta(G)$，即 $\lambda(G)\leqslant\delta(G)$。

再证 $\chi(G)\leqslant\lambda(G)$。

当在 G 中删去构成割集的 $\lambda(G)$条边，则 G 不连通。现将这 $\lambda(G)$条边的每一条边上的一个端点删除，即删除 $\lambda(G)$个顶点，此时 G 亦必不连通，因此 G 的点连通度 $\chi(G)$不超过 $\lambda(G)$，即 $\chi(G) \leqslant \lambda(G)$。

定理 8-10 设 G 为 n 个顶点、m 条边的简单连通图，那么 $\lambda(G) \leqslant \frac{2m}{n}$。

证明 因为 $2m$ 是图 G 各顶点的度数总和，因此 n 个顶点中至少有一个顶点的度不超过 $\frac{2m}{n}$，故 G 的边连通度 $\lambda(G)$不超过 $\frac{2m}{n}$。

图 8-11 中的图 G 满足：

$$\frac{2m}{n} = 16/7 \geqslant \lambda(G) = 2$$

$$\chi(G) = 1 \leqslant \lambda(G) = 2 \leqslant \delta(G) = 2$$

8.3 欧拉图与哈密顿图

8.3.1 欧拉图及欧拉路径

定义 8-18 图 G 称为**欧拉图**（Euler graph），如果图 G 上有一条经过 G 的所有顶点、所有边的闭路径。图 G 称为**欧拉路径**（Euler walk），如果图 G 上有一条经过 G 所有顶点、所有边的路径。

本章一开头介绍的哥尼斯堡桥问题，现在可以这样来叙述：图 8-lb 是否为一欧拉图？

定理 8-11 无向图 G 为欧拉图当且仅当 G 连通，并且所有顶点的度都是偶数。有向图 G 为欧拉图，当且仅当 G 是弱连通的，并且每个顶点的出度与入度相等。

证明 这里仅对无向图立论，定理的后半部分仿此可证，不赘述。

设 G 为一欧拉图，那么 G 显然是连通的。另一方面，由于 G 本身为一闭路径，它每经过一个顶点一次，便给这一顶点增加度数 2，因而各顶点的度均为该路径经历此顶点的次数的两倍，从而均为偶数。

反之，设 G 连通，且每个顶点的度均为偶数，欲证 G 为一欧拉图。为此，对 G 的边数归纳。

当 $m=1$ 时，G 必定为单顶点的环，如图 8-14a 所示，显然这时 G 为欧拉图。

设边数少于 m 的连通图，在顶点度均为偶数时必为欧拉图，现考虑有 m 条边的图 G。设想从 G 的任一顶点出发，沿着边构画，使笔不离开图且不在构画过的边上重新构画。由于每个顶点都是偶数度，笔在进入一个顶点后总能离开那个顶点，除非笔回到了起点。在笔回到起点时，它构画出一条闭路径，记为 H。从图 G 中删去 H 的所有边，所得图记为 G'，G' 未必连通，但其各顶点的度数仍均为偶数（为什么？）。考虑 G'的各连通分支，由于它们都连通，顶点度数均为偶数，而边数均小于 m，因此据归纳假设，它们都是欧拉图。此外，由于 G 连通，它们都与 H 共有一个或若干个公共顶点（如图 8-12b 所示），因此，它们与 H 一起构成一个闭路径。这就是说，G 是一个欧拉图。

定理 8-12 无向图 G 为欧拉路径（非欧拉图），当且仅当 G 连通，并且恰有两个顶点的度是奇数。有向图 G 为欧拉路径（非欧拉图），当且仅当 G 连通，并且恰有两个顶点的入度

与出度不等，它们中一个的出度比入度多 1，另一个入度比出度多 1。

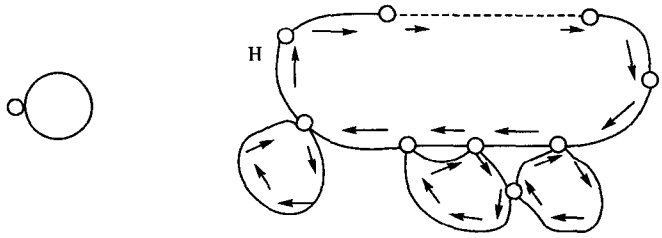


图 8-12

本定理的证明由定理 8-11 的证明很容易得到。

【例 8-11】

（1）由于图 8-1b 的四个顶点都是奇数度的，因此它既不是欧拉图也不是欧拉路径。这就是说，无论是否要求回到原地，不重复地走遍七桥是不可能的。

（2）奇数（大于 1）个顶点的完全图，k 为偶数时的 k-正则图都是欧拉图。

（3）一笔画游戏（笔不离开纸，不重复地画遍纸上图形的所有的边），实质上是一个欧拉图、欧拉路径的判定问题。图 8-13a 可以从一点出发一笔画所有边后回到起点；图 8-13b 可以一笔画所有边，但不能使笔回到起点；图 8-13c 则根本不可能一笔画所有边。

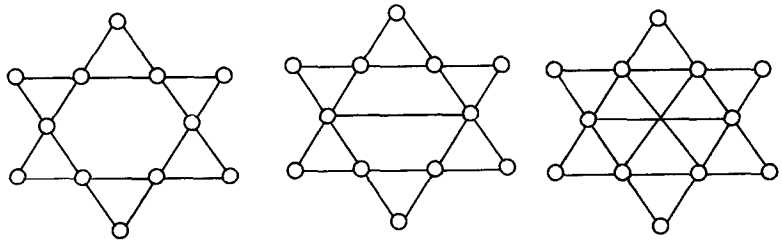


图 8-13

8.3.2 哈密顿图及哈密顿通路

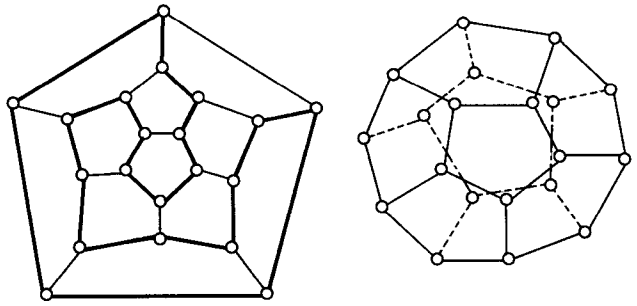
我们仅限于无向图讨论哈密顿图及哈密顿通路。

定义 8-19 图 G 称为**哈密顿图**（Hamilton graph），如果 G 上有一条经过所有顶点的回路（也称这一回路为哈密顿回路）。称无向图有**哈密顿通路**（非哈密顿图），如果 G 上有一条经过所有顶点的通路（非回路）。

【例 8-12】 图 8-14a 为一哈密顿图，图中粗线表示哈密顿回路。它是正十二面体（图 8-14b）的“平面投影”。哈密顿（爱尔兰数学家）1859 年提出一个名叫“周游世界”的游戏。问题是：能否遍历正 12 面体的每个顶点一次且仅一次后回到原地。

注意哈密顿图、哈密顿通路与欧拉图、欧拉路径之间的区别。它们之间几乎没有什么联系。有的图既是哈密顿图又是欧拉图，有的图只是哈密顿图不是欧拉图，有的图只是欧拉图不是哈密顿图，有的图则两者皆非。特别要留意的是，哈密顿图并不要求其哈密顿回路遍历

图的所有的边，仅仅要求遍历图的所有的顶点。



a)　　b)

图　8-14

至今没有一个像欧拉图的充要条件那样的“非平凡的”（不是定义的同义反复）关于哈密顿图、哈密顿通路的充分必要条件，但关于它们的充分性和必要性分别有一些研究成果。

定理 8-13　设图 G 为具有 n 个顶点的简单无向图，如果 G 的每一对顶点的度数之和都不小于 $n-1$，那么 G 中有一条哈密顿通路；如果 G 的每一对顶点的度数之和不小于 n，且 $n\geqslant 3$，那么 G 为一哈密顿图。

证明　先证 G 为一连通图。若不然，G 由若干连通分支所组成。令 $v1$，$v2$ 分属于连通分支 $G1$，$G2$；$G1$，$G2$ 各有 $n1$，$n2$ 个顶点。显然 $n1\leqslant n$，$n2\leqslant n$，于是 $\deg(v1)\leqslant n1-1$，$\deg(v2)\leqslant n2-1$，而 $\deg(v1)+\deg(v2)\leqslant n1+n2-2<n-1$，与题设矛盾。

为证 G 有哈密顿通路，只要在 G 中构作出一条长为 $n-1$ 的通路。为此令 P 为 G 中任意一条长为 $p-1$，$p<n$，的通路，设其顶点序列为 v_1，v_2，…，v_p。我们来扩充这一通路。

（1）如果有 $v\neq v_1$，v_2，…，v_p，它与 v_1 或 v_p 间有边相关联，那么可立即扩充 P 为长度为 p 的通路。

（2）如果 v_1，v_p 均只与原通路 P 上的顶点相邻，如下可证：G 中有一条包含 v_1，v_2，…，v_p，长度为 p 的回路。

如果 v_1 与 v_p 相邻，那么我们已经如愿。

如果 v_1 与 v_{i1}，v_{i2}，…，v_{ir} 相邻，$1<i_1$，i_2，…，$i_r<p$，考虑 v_p：

1）若 v_p 与 v_{i1-1}，v_{i2-1}，…，v_{ir-1} 之一，例如 v_{i1-1} 相邻，那么我们便可得到包含 v_1，v_2，…，v_p 的回路：（v_1，v_2，…，v_{i1-1}，v_p，v_{p-1}，…，v_{i1}，v_1）如图 8-15a 所示。

2）若 v_p 不与 v_{i1-1}，v_{i2-1}，…，v_{ir-1} 中任何一个相邻，那么 $\deg(v_p)\leqslant p-r-1$，因而

$$\deg(v_1)+\deg(v_p)\leqslant r+p-r-1=p-1<n-1$$

与题设矛盾，因此 2）不可能发生。

现考虑 G 中这条包含 v_1，v_2，…，v_p，长度为 p 的回路。由于已证 G 为一连通图且 $p\leqslant n-1$，故必有回路外顶点 v 与回路上顶点（例如 v_k）相邻，如图 8-15b 所示，那么我们可以得到一条长度为 p 的、包含 v_1，v_2，…，v_p 的通路：（v，v_k，v_{k-1}，…，v_1，v_{i1}，v_{i1+1}，…，v_p，v_{i1-1}，…，v_{k+1}），如图 8-15c 所示。

重复过程（1），（2）不断扩充通路 P，直至它的长度为 $n-1$，这时便得到 G 中的一条哈密顿通路。

定理的后半部分仿上可证。

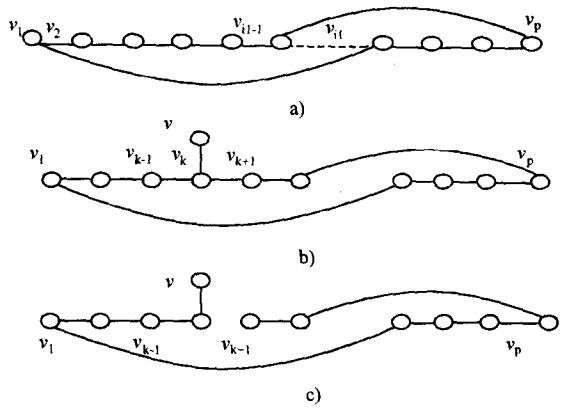


图 8-15

【例 8-13】 利用以上定理不难明白：

（1）顶点数目不少于 3 的完全图都是哈密顿图。

（2）每个顶点度数均不小于 $n/2$ 的图，特别地，k-正则图在 $k \geqslant n/2$ 时都是哈密顿图（n 为图的顶点数）。

注意，定理 8-13 给出的条件只是充分条件，不是必要条件。例如，形如六边形的图显然是哈密顿图，但它的任意两个顶点的度数和都是 4，小于 $n-1=5$ 。

另一个值得注意的问题是，哈密顿图中的哈密顿回路未必是惟一的。关于这一点，下面的定理说得更加深入。

定理 8-14 当 n 为不小于 3 的奇数时，K_n 上恰有 $\frac{n-1}{2}$ 条互相均无任何公共边的哈密顿回路。

证明 假设 K_n 的 n 个顶点如图 8-16 排成一个正（n-1）边形的顶点，它还给出了一条哈密顿回路（v_1，v_2，…，v_n，v_1）。

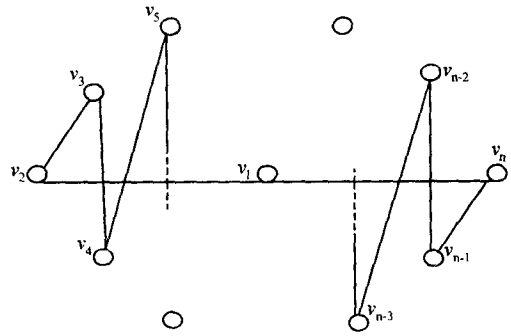


图 8-16

逆时针分别旋转图 8-18（顶点标记旋转时留在原地）$\frac{360^\circ}{n-1}$，$\frac{2\times 360^\circ}{n-1}$，…，$\frac{\frac{n-3}{2}\times 360^\circ}{n-1}$，各产生一条哈密顿回路，它们之间没有公共边。图 8-17 例示了 n=5 时的情

景，因此，合乎要求的哈密顿回路共有 $1+\frac{n-3}{2}=\frac{n-1}{2}$ 条。

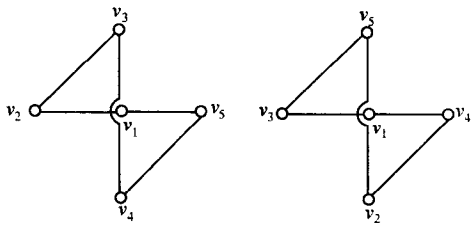


图 8-17

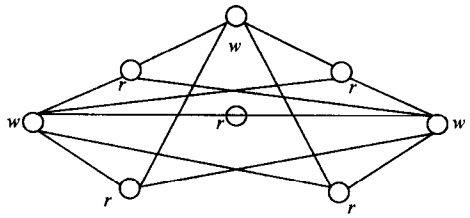


图 8-18

为了讨论哈密顿图和哈密顿通路存在的一个必要条件，以便鉴定非哈密顿图和不存在哈密顿通路的图，我们引入图着色概念，这一概念在今后的讨论中还会遇到。

定义 8-20 图 G 称为可 2-着色（2-chromatic），如果可用两种颜色给 G 的所有顶点着色，使每个顶点着一种颜色，而同一边的两个不同端点必须着不同颜色。

定理 8-15 设图 G 是可 2-着色的。如果 G 是哈密顿图，那么着两种颜色的顶点数目相等；如果 G 有哈密顿通路，那么着两种颜色的顶点数目之差至多为一。

证明 由于哈密顿回路、通路均经过图的所有顶点一次且仅一次，而它又是相间地通过两种颜色的顶点，因此定理的结论是明显的。

【例 8-14】 图 8-20 可 2-着色，r，w 分别表示顶点着红色和白色。由于图中红色顶点比白色顶点多 2 个，因此该图不是哈密顿图，也没有哈密顿通路。

注意，定理 8-15 只指出了哈密顿图和哈密顿通路存在的必要条件，它并不充分，很容易作出可 2-着色且两种颜色顶点数目相等的图，它却不是哈密顿图，例如图 8-19a 不是哈密顿图，b 中哈密顿通路也不存在，尽管它们都可 2-着色，且两种颜色的顶点数目符合要求。

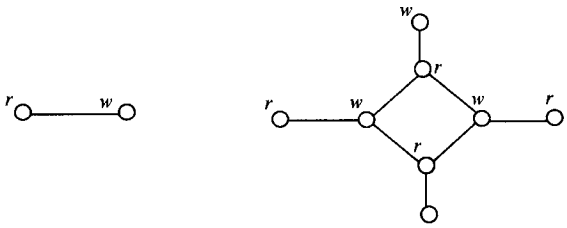
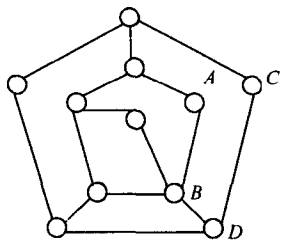


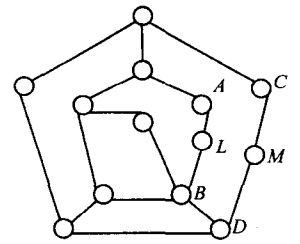
图 8-19

定理 8-15 用来判定某些图不是哈密顿图或没有哈密顿通路是方便的，就像例 8-14 表明的那样。但是，它要求图是可 2-着色的，这并不是任何图都能满足的。当一个图不可 2-着色时，不能运用定理 8-15 作判定。当然，在有些情况下我们可以施展一些手段。

【例 8-15】 图 8-20a 是不可 2-着色的，为了证明它不是哈密顿图，我们在边（A, B）及边（C, D）上添加新的顶点 L，M，得到图 8-20b，它是可 2-着色的，且红色结点比白色结点少(或反之)，因此可确认图 8-20b 没有哈密顿回路。进而可证明图 8-20a 也没有哈密顿回路。



a)



b)

图 8-20

若图 8-20a 有哈密顿回路，由于它经过顶点 C 和 A，因此亦必经边（C，D）和（A，B），因而经过顶点 L，M。这就是说，这条回路也是图 8-20b 的哈密顿回路，产生矛盾。

故图 8-20a 没有哈密顿回路。

众所周知，哈密顿图的理论是著名的货郎担问题的源头。

8.4 图的矩阵表示

图的图示虽然直观，但不便于计算机处理，本节要讨论图的另一种表示——矩阵表示，它显然有益于弥补这一不足。

8.4.1 邻接矩阵

邻接矩阵多用于有向图，但也适用于无向图。我们仅对无重边的有向图立论，其结论均可移植于简单无向图。

定义 8-21 设 $G=<V, E>$为一无重边的有向图。其中 $V=\{v_1,v_2,\cdots,v_n\}$，那么 $n\times n$ 矩阵 $A=[a_{ij}]$，

$$a_{ij}=\begin{cases}1 & \text{若}<v_i,v_j>\in E\\ 0 & \text{若}<v_i,v_j>\notin E\end{cases}$$

称为图 G 的邻接矩阵（adjacency matrix），记为 $A[G]$。

【例 8-16】

（1）零图的邻接矩阵为零矩阵。

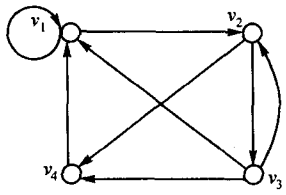
（2）一图的每个顶点以且仅以环为关联的边,那么该图的邻接矩阵为幺矩阵。

（3）无向图的邻接矩阵是对称矩阵。

（4）图 8-21a 的邻接矩阵为图 8-21b。

邻接矩阵可推广到有平行边的多重图和赋权图上，只要令矩阵分量 a_{ij} 为 v_i 到 v_j 的边的重数或边上的权值 $W(v_i,v_j)$，而当 v_i，v_j之间无边关联时，仍取 $a_{ij}=0$。

邻接矩阵有多种用途。它除了自身反映图的一些性质，例如图各顶点是否有环（对角线元素是否为 1），图的边是否成对出现（矩阵是否对称），图各顶点的出度和入度（矩阵的行和与列和）等等外，还能通过矩阵运算来探究图的更为深入的性质。



a)

$$\begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{pmatrix}$$

b)

图 8-21

以下设 A 为图 G 的邻接矩阵，$A=[a_{ij}]$，A^{T} 为 A 的转置矩阵，$\circ$为矩阵乘运算符。我们知道，若 $A\circ B=C$，$A=[a_{ij}]$，$B=[b_{ij}]$，$C=[c_{ij}]$，那么

$$c_{ij}=\sum_{k=1}^{n}a_{ik}b_{kj}$$

我们还用 A^l 表示 l 个矩阵 A 的乘积。

（1）令 $A^l=[a_{ij}^{(l)}]$，那么 $a_{ij}^{(l)}$ 的意义是：G 中从顶点 v_i 到 v_j 的长度为 l 的拟路径恰为 $a_{ij}^{(l)}$ 条。

在证明事实（1）之前，我们先用例 8-16 之（4）来验证这一结论。由计算得

$$A^3=\begin{pmatrix} 3 & 2 & 1 & 2 \\ 3 & 2 & 1 & 1 \\ 4 & 3 & 1 & 2 \\ 1 & 1 & 1 & 1 \end{pmatrix}$$

其中 $a_{31}^{(3)}=4$，而图 8-21 中 v_3 到 v_1 恰有四条长度为 3 的拟路径，它们是（v_3 ,v_1 ,v_1 ,v_1），（v_3 ,v_4 ,v_1 ,v_1），（v_3 ,v_2 ,v_4 ,v_1），（v_3 ,v_2 ,v_3 ,v_1）。

现对 l 归纳证明事实（1）。

$l=1$ 时，$A^l=A=[a_{ij}^{(1)}]=[a_{ij}]$，命题显然真。

设 $A^l=[a_{ij}^{(l)}]$中 $a_{ij}^{(l)}$ 对任意 i,j 均表示 v_i到 v_j的长度为 l 的拟路径条数。

考虑 $A^{l+1}=[a_{ij}^{(l+1)}]$。由矩阵乘积定义知

$$a_{ij}^{(l+1)}=\sum_{k=1}^{n}a_{ik}^{(l)}a_{kj}=a_{i1}^{(l)}a_{1j}+a_{i2}^{(l)}a_{2j}+\ldots+a_{in}^{(l)}a_{nj} \tag{8-5}$$

其中 $a_{ik}^{(l)}$ 表示从 v_i到 v_k有 $a_{ik}^{(l)}$ 条长度为 l 的拟路径。而

$$a_{kj}=\begin{cases}1 & \text{当}<v_k,v_j>\in E(\text{或}(v_i,v_j)\in E)\\ 0 & \text{当}<v_k,v_j>\notin E(\text{或}(v_i,v_j)\notin E)\end{cases}$$

$a_{ik}^{(l)}a_{kj}$ 表示从 v_i经由 v_k到 v_j的长度为 $l+1$ 的拟路径数目，因而和式（8-5）表明 $a_{ij}^{(l+1)}$ 是从 v_i到 v_j的长度为 $l+1$ 的拟路径的总条数。

归纳完成，（1）得证。

（2）令 $A\circ A^{\mathrm{T}}=[b_{ij}]$，那么 b_{ij} 的意义是：有 b_{ij} 个顶点 v，使得 v_i到 v，v_j到 v 都有边（两边交于 v）。因而 b_{ii} 表示顶点 v_i的出度。

仍用例 8-16 之（4）验证之。计算

$$A\circ A^{\mathrm{T}}=\begin{pmatrix}1&1&0&0\\0&0&1&1\\1&1&0&1\\1&0&0&0\end{pmatrix}\circ\begin{pmatrix}1&0&1&1\\1&0&1&0\\0&1&0&0\\0&1&1&0\end{pmatrix}=\begin{pmatrix}2&0&2&1\\0&2&1&0\\2&1&3&1\\1&0&1&1\end{pmatrix}$$

其中 $b_{31}=2$，而图 8-21 中正有两个顶点 v_1，v_2，使得 v_3 与 v_1 到它们都有边；$b_{33}=3$，而顶点 v_3 的出度恰为 3。

现证明事实（2）。根据矩阵乘积的定义：

$$b_{ij}=\sum_{k=1}^{n}a_{ik}a_{jk}$$

它等价于：有 b_{ij} 个 k 的值使 $a_{ik}a_{jk}=1$，有 b_{ij} 个 k 的值使 $a_{ik}=1$ 且 $a_{jk}=1$，有 b_{ij} 个顶点 v_k 使 v_i 到 v_k 有边且 v_j 到 v_k 也有边。

这正是事实（2）所表明的。

（3）令 $A^{\mathrm{T}}\circ A=[b_{ij}]$，那么 b_{ij} 的意义是：有 b_{ij} 个顶点 v，使得 v 到 v_i，v 到 v_j 都有边；因而 b_{ii} 表示顶点 v_i 的入度。

再用例 8-16 之（4）验证之。计算

$$A^{\mathrm{T}}\circ A=\begin{pmatrix}1&0&1&1\\1&0&1&0\\0&1&0&0\\0&1&1&0\end{pmatrix}\circ\begin{pmatrix}1&1&0&0\\0&0&1&1\\1&1&0&1\\1&0&0&0\end{pmatrix}=\begin{pmatrix}3&2&0&1\\2&2&0&1\\0&0&1&1\\1&1&1&2\end{pmatrix}$$

其中 $b_{31}=0$，而图 8-21 中确无到 v_3，v_1 均有边的顶点；$b_{44}=2$，而 v_4 的入度正是 2。

事实（3）的证明留给读者。

8.4.2 路径矩阵与可达性矩阵

设 n 个顶点的图 G 的邻接矩阵为 A，$\vee$ 及 $\wedge$ 表示如下定义的矩阵运算。若 $A=[a_{ij}]$，$C=[c_{ij}]$，则

$$A\vee C=[d_{ij}]\quad d_{ij}=a_{ij}\vee c_{ij}$$

$$A\wedge C=[e_{ij}]\quad e_{ij}=\bigvee_{k=1}^{n}(a_{ik}\wedge c_{kj})$$

这里 $\bigvee_{k=1}^{n}$ 为连续求 $\vee$ 运算的缩记符，以下 $\bigwedge_{k=1}^{n}$ 同此。

我们用 $A^{(m)}$ 表示 $A\wedge A\wedge\cdots\wedge A$（$m$ 个 A）。

考虑矩阵

$$B=A\vee A^{(2)}\vee\cdots\vee A^{(n)}$$

它的第 i，j 分量 $b_{ij}=1$ 当且仅当图 G 中有 v_i 到 v_j 的路径。B 称为图 G 的**路径矩阵**（walk matrix）。

令矩阵 $P=I\vee B$，其中 I 为（$n\times n$）么矩阵，称 P 为图 G 的**可达性矩阵**。

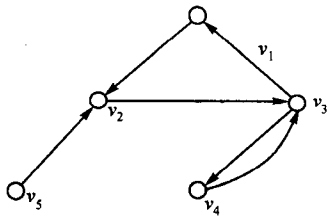


图 8-22

【例 8-17】 计算图 8-22 的路径矩阵 B 与可达性矩阵 P。

令该图邻接矩阵为 A，那么

$$A=\begin{pmatrix}0&1&0&0&0\\0&0&1&0&0\\1&0&0&1&0\\0&0&1&0&0\\0&1&0&0&0\end{pmatrix}\quad A^{(2)}=\begin{pmatrix}0&0&1&0&0\\1&0&0&1&0\\0&1&1&0&0\\1&0&0&1&0\\1&0&1&0&0\end{pmatrix}\quad A^{(3)}=\begin{pmatrix}1&0&0&1&0\\0&1&1&0&0\\1&0&1&1&0\\0&1&1&0&0\\1&0&0&1&0\end{pmatrix}$$

$$A^{(4)}=\begin{pmatrix}0&1&1&0&0\\1&0&1&1&0\\1&1&1&1&0\\1&0&1&1&0\\0&1&1&0&0\end{pmatrix}\quad A^{(5)}=\begin{pmatrix}1&0&1&1&0\\1&1&1&1&0\\1&1&1&1&0\\1&1&1&1&0\\1&0&1&1&0\end{pmatrix}$$

从而

$$B=A\vee A^{(2)}\vee A^{(3)}\vee A^{(4)}\vee A^{(5)}=\begin{pmatrix}1&1&1&1&0\\1&1&1&1&0\\1&1&1&1&0\\1&1&1&1&0\\1&1&1&1&0\end{pmatrix}$$

$$P=I\vee B=\begin{pmatrix}1&1&1&1&0\\1&1&1&1&0\\1&1&1&1&0\\1&1&1&1&0\\1&1&1&1&1\end{pmatrix}$$

P 说明图 8-22 是一个单向连通图，其中$\{v_1,v_2,v_3,v_4\}$构成一个强分图，$\{v_5\}$为另一强分图。

8.5 练习

1．想一想，一只昆虫是否可能从立方体的一个顶点出发，沿着棱爬行、要求它爬行过每条梭一次且仅一次，并且最终回到原地？为什么？

2．设想画一个图，它的 64 个顶点表示国际象棋棋盘的 64 个方格，顶点间的边表示:在这两个顶点表示的方格之间可以进行“马步”的行走。试指出其顶点有哪几类（依其度分类），每类各有多少个顶点。

3．证明：n 个顶点的简单图中不会有多于 $\frac{n(n-1)}{2}$ 条边。

4．证明：在任何 n ($n\geqslant 2$)个顶点的简单图中，至少有两个顶点具有相同的度。

5．图 8-23 是一个迷宫,其中数字表示通道和死胡同（包括目标）。请用一个图来表示这个迷宫（用结点表示通道和死胡同（包括目标），用边表示它们之间的可到达关系）。

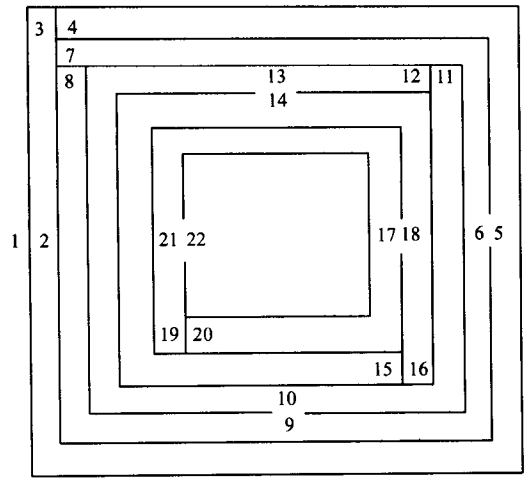


图 8-23

6．在晚会上有 n 个人，他们各自与自己相识的人握一次手。已知每人与别人握手的次数都是奇数，问 n 是奇数还是偶数。为什么？

7．n 个城市间有 k 条相互连接的直达公路。证明：当 $k>\frac{(n-1)(n-2)}{2}$ 时，人们便能通过这些公路在任何两个城市间旅行。

*8．（1）证明：序列（7，6，5，4，3，2，2），（7，6，5，4，3，3,2）以及（6，6，5，4，3，3，1）都不是简单图的度序列。

（2）若自然数序列（$d_1,d_2,\cdots,d_n$）满足 $d_1>d_2>\cdots>d_n$，那么当它为一简单图的度序列时必有

（a）$\sum_{i=1}^{n} d_i$ 为偶数；

（b）对任一 k，$1\leqslant k\leqslant n$，$\sum_{i=1}^{k} d_i \leqslant k(k-1)+\sum_{i=k+1}^{n}\min(k,d_i)$。

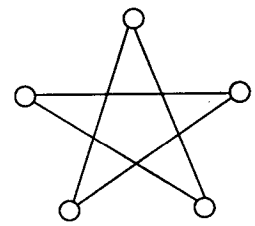


图 8-24

9．画出图 8-24 中图的补图及它的一个生成子图。

10．一个简单图，如果同构于它的补，则该图称为**自补图**。

（1）给出一个 4 个顶点的自补图。

（2）给出一个 5 个顶点的自补图。

（3）是否有 3 个顶点或 6 个顶点的自补图？

（4）证明一个自补图一定有 $4k$ 或 $4k+1$ 个顶点（k 为正整数）。

11．(1) 证明图 8-25 中 a 与 b 同构。

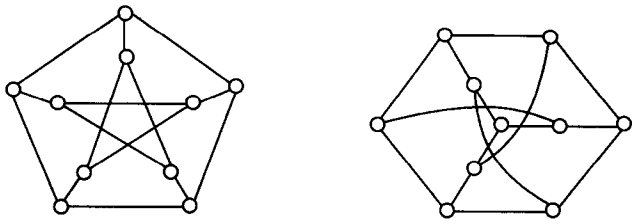


图 8-25

（2）给出所有不同构的 4 个结点的简单图的图示。

12. 证明定理 8-5。

13. 证明：在简单无向图 G 中，从结点 u 到结点 v，如果既有奇数长度的通路又有偶数长度的通路，那么 G 中必有一奇数长度的回路。

14. 证明：若简单无向图 G 是不连通的，那么 G 的补图 $\overline{G}$ 必定是连通的。

15. 给出图 8-26 中有向图的强分图，单向分图和弱分图。

16. 有 7 人 a，b，c，d，e，f，g 分别精通下列语言，问他们 7 人是否可以自由交谈（必要时借助他人作翻译）。

a 精通英语。

b 精通汉语和英语。

c 精通英语、俄语和意大利语。

d 精通日语和英语。

e 精通德语和意大利语。

f 精通法语、日语和俄语。

g 精通法语和德语。

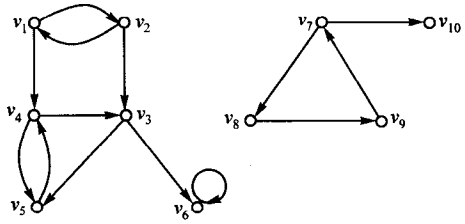


图 8-26

17. 证明：一个有向图是单向连通的，当且仅当它有一条经过每一结点的路径。

18. 称 $d(u,v)$为图 $G=<V,E>$中结点 u，v 间的距离：

$$d(u,v)=\begin{cases}0 & \text{当}u=v\\ \infty & \text{当}u\text{到}v\text{不可达}\\ u,v\text{间最短路径长度} & \text{否则}\end{cases}$$

$d(u_0,v_0)$称为图 G 的直径，如果 $d(u_0,v_0)=\max\{d(u,v)\mid u,v\in V\}$。试求图 8-27 中图的直径，$\chi(G)$，$\lambda(G)$，$\delta(G)$，并指出一个点割集和一个边割集。

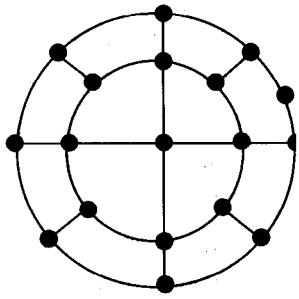


图 8-27

19. 顶点 v 是简单连通图 G 的割点，当且仅当 G 中存在两个顶点 $v1$，$v2$，使 $v1$ 到 $v2$ 的所有通路都经过顶点 v。试证明之。

20. 边 e 是简单连通图 G 的割边，当且仅当 e 不在 G 的任一回路上。试证明之。

21. 试用有向图描述下列问题的解：

某人 m 带一条狗 d，一只猫 c 和一只兔子 r 过河。m 每次游过河时只能带一只动物，而没人管理时，狗与兔子不能共处，猫和兔子也不能共处。问 m 怎样把三个动物带过河去？

（提示：用结点代表状态，状态用序偶$<S1, S2>$来表示，这里 $S1$，$S2$ 分别是左岸和右岸的人及动物集合，例如初始状态为$<\{m,d,c,r\}, \varnothing>$。

22. 有向图可以刻画一个系统的状态转换，例如用图 8-28 中的有向图可以描述识别 010*10 序列的状态转换系统。其中 S 为初始状态，在此读入序列，然后依序列中符号转入后续状态（读到 0 进入 $S1$，读到 1 进入 $S2$，如此等等）。$S4$ 表示读完序列 010*10 应进入的最后状态，$S5$ 表示读完一个非 010*10 序列应进入的最后状态。

试自行构作识别序列 01(10)*10 的有向图刻画的状态转换系统。

（上文中 w^*表示空字或重复任意多次 w 所得的字。）

23. 试作出四个图的图示，使第一个既为欧拉图又为哈密顿图；第二个是欧拉图而非哈密顿图；第三个是哈密顿图却非欧拉图；第四个既非欧拉图也非哈密顿图。

24. 像第 23 题要求的那样对欧拉路径和哈密顿通路作出四个图。

25. 问 n 为何种数值时，K_n 既是欧拉图又是哈密顿图。问 k 为何值时，k-正则图既是欧拉图又是哈密顿图。

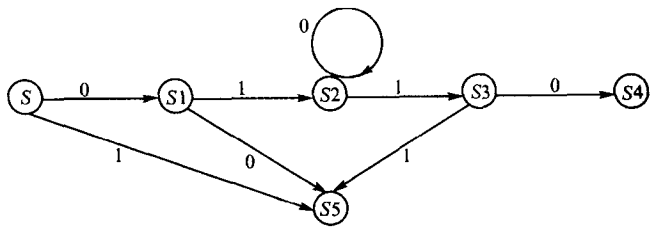


图 8-28

26. 证明：恰有两个奇数度顶点 u,v 的无向图 G 是连通的，当且仅当在 G 上添加边（u，v）后所得的图 G^*是连通的。

27. 试计算 K_n（$n \geq 3$）中不同的哈密顿回路共有多少条。

28. 十一个学生在一张圆桌旁共进晚餐，要求在每次晚餐上每个学生的邻座都与其他各次晚餐的邻座不同。问这样共进晚餐能安排多少次。

29. 判别图 8-29 中各图是否为哈密顿图，若不是，请说明理由，并回答它是否有哈密顿通路。

30. 证明：对哈密顿图 $G=<V, E>$删除 S（$\subseteq V$）中的所有顶点后，所得图 G'的连通分支数不大于$|S|$。

31. 设 G 为（n，m）图。证明：如果 $m \geq C_{n-1}^2+2$，那么 G 为哈密顿图（提示：运用定理 8-13）。

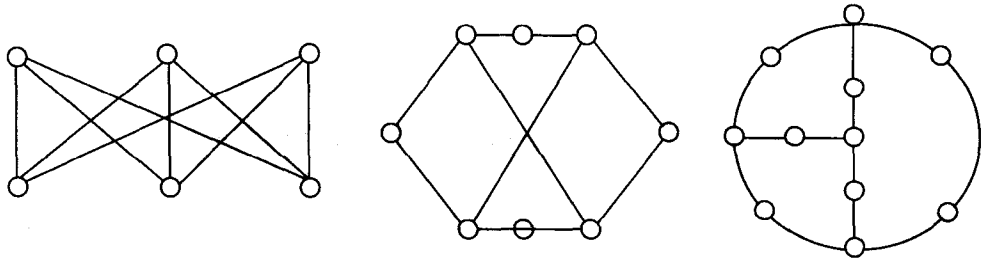


图 8-29

32. 设有 n（n 为偶数）个围成一圈跳舞的孩子，每个孩子都至少与其中 $\frac{n}{2}$ 个是朋友。试证明，总可安排得使每个孩子的两边都是他的朋友。

33. 对图 8-30 给出的有向图 G：

（1）计算它的邻接矩阵 A 及 A^2，A^3，A^4，说出从 v_1 到 v_4 的长度为 1，2，3，4 的拟路径各有多少条。

（2）计算 $A \circ A^T$，$A^T \circ A$，说出它们中第 2，3 分量及第 4，4 分量的意义。

（3）计算它的路径矩阵 B 及可达性矩阵 P，并从 P 说出 G 的各强分图。

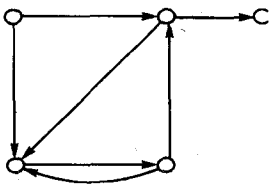


图 8-30

34. 如何利用邻接矩阵来识别它们对应的图是欧拉图？

35. 设 n 个顶点的有向图 G 是强连通的，说出 G 的路径矩阵、可达性矩阵的特点。

36. 设 A 为有向图 G 的邻接矩阵。证明：A^3 的对角线元素 $a_{ii}^{(3)}$ 表示经过顶点 v_i 的“三角形”的个数，即以 v_i 为一个顶点的 G 的子图 K_3 的个数。

第 9 章　二分图、平面图和树

本章将讨论几类在理论研究和实际应用中都有重要意义的无向图，它们是二分图、平面图和树。

9.1　二分图

9.1.1　二分图的基本概念

定义 9-1　无向图 $G=<V, E>$称为**二分图**（bipartite graph），如果有非空集合 X，Y 使 $X\cup Y=V$，$X\cap Y=\varnothing$，且对每一 $e\in E$，都有 $e=\{x, y\}$，$x\in X$，$y\in Y$。此时常用$<X, E, Y>$表示二分图 G。若对 X 中任一 x 及 Y 中任一 y 恰有一边 $e\in E$，使 $e=\{x, y\}$，则称 G 为**完全二分图**（complete bipartite graph）。当$|X|=m$，$|Y|=n$ 时，完全二分图 G 记为 $K_{m,n}$。

【例 9-1】　图 9-1a、b 为二分图，c 为完全二分图 $K_{3,3}$，d，e 不是二分图。

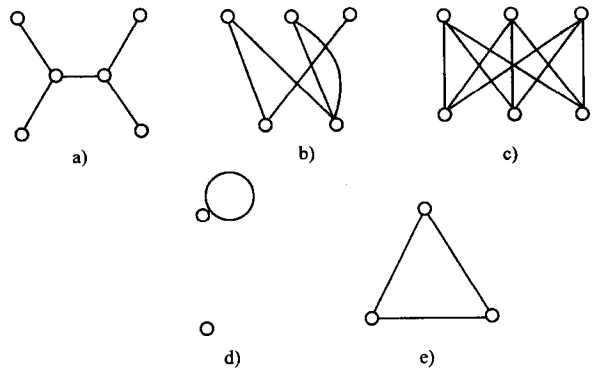


图　9-1

二分图的下列特征性是重要的。

定理 9-1　无向图 G 为二分图的充分必要条件是，G 至少有两个顶点，且其所有回路的长度均为偶数。

证明　先证必要性。

设 G 为二分图$<X, E, Y>$。由于 X，Y 非空，故 G 至少有两个顶点。若 C 为 G 中任一长度为 l 回路，令

$$C=(v_0,v_1,v_2,\cdots,v_{l-1},v_l=v_0)$$

其中诸 v_i ($i=0,1,\cdots,l$)必定相间出现于 X 及 Y 中，显然

$$\{v_0,v_2,v_4,\cdots,v_l=v_0\}\subseteq X$$

$$\{v_1,v_3,v_5,\cdots,v_{l-1}\}\subseteq Y$$

因此 l 必为偶数，从而 C 中有偶数条边。

再证充分性。

设 G 的所有回路具有偶数长度，并设 G 为连通图（不失一般性，若 G 不连通，则可对 G 的各连通分支作下述讨论）。

令 G 的顶点集为 V，边集为 E，现构作 X，Y，使$<X, E, Y>=G$。取 $v_0 \in V$，置

$X=\{v \mid v=v_0$或 v 到 v_0有偶数长度的通路$\}$

$Y=V-X$

X 显然非空。现需证 Y 非空，且没有任何边的两个端点都在 X 中或都在 Y 中。

若 v_0无相邻顶点，那么 X 中无其他顶点，由于$|V| \geqslant 2$，故至少还有一个顶点 v 在 Y 中；若 v_0有相邻顶点 v_1，那么 $v_1 \in Y$；故 Y 不空。

设有边$\{u, v\}$，使 $u \in X$，$v \in X$。那么，v_0到 u 有偶数长度的通路，或 $u=v_0$；v_0到 v 有偶数长度的通路，或 $v=v_0$。这样，无论何种情况，连同边$\{u, v\}$均有一条从 v_0到 v_0的奇数长度的闭的拟路径，在此闭的拟路径中一定存在奇数长度的回路（回忆定理 8-5 否则该闭路径的长度为偶数），与题设矛盾。故不可能有边$\{u, v\}$使 u, v 均在 X 中。

仿上可证“没有任何边的两个端点全在 Y 中”。

作为一种数学模型二分图是十分有用的，许多问题可以用它来刻画。例如“资源分配”、“工作安排”、“人员择偶”等等。但是，利用二分图分析解决这类问题时，还需要有关二分图的另一个概念——匹配。

9.1.2 匹配

定义 9-2 设 $G=<X, E, Y>$为二分图，$M \subseteq E$。称 M 为 G 的一个**匹配**（matching），如果 M 中任何两条边都没有公共端点。$M=\varnothing$时称 M 为空匹配。G 的所有匹配中边数最多的匹配称为**最大匹配**（maximal matching）。如果 $X(Y)$中任一顶点均为匹配 M 中边的端点，那么称 M 为 $X(Y)$-**完全匹配**(perfect matching)。若 M 既是 X-完全匹配又是 Y-完全匹配，则称 M 为 G 的**完全匹配**。

【例 9-2】 图 9-2 中各图的粗线表示匹配中的边（简称匹配边）。b 中匹配是最大的，$X=\{a,b,c\}$，匹配是 X-完全的，c 中匹配是 G 的完全匹配（从而也是最大的）。

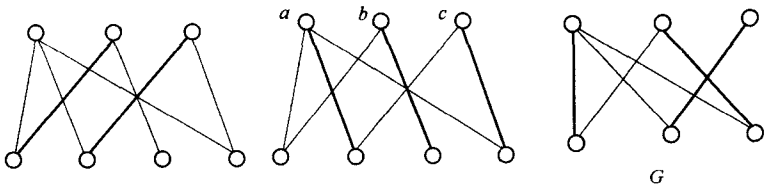


图 9-2

注意：最大匹配总是存在但未必惟一；$X(Y)$-完全匹配及 G 的完全匹配必定是最大的，但反之则不然；$X(Y)$-完全匹配未必存在。

为讨论最大匹配的求法及完全匹配的存在条件，需要下列术语。

定义 9-3 设 $G=<X, E, Y>$，M 为 G 的一个匹配。

（1）M 中边的端点称为 **M-顶点**，其他顶点称为**非 M-顶点**。

（2）G 中 v_k 到 v_l 的通路 P 称为**交替链**，如果 P 的起点 v_k 和终点 v_l 为非 M-顶点，而其边的序列中非匹配边与匹配边交替出现（从而首尾两边必为非匹配边，除顶点 v_k，v_l 以外各顶点均为 M-顶点）。特别地，当一边$\{v, v'\}$两端点均为非 M-顶点，通路$\{v, v'\}$亦称为交替链。

以下算法可把 G 中任一匹配 M 扩充为最大匹配，此算法被称为**匈牙利算法**：

（1）首先用（*）标记 X 中所有的非 M-顶点，然后交替进行步骤（2），（3）。

（2）选取一个刚标记（用（*）或在步骤（3）中用（y_i）标记）过的 X 中顶点，例如顶点 x_i，然后用（x_i）去标记 Y 中顶点 y，如果 x_i 与 y 为同一非匹配边的两端点，且在本步骤中 y 尚未被标记过。重复步骤（2），直至对刚标记过的 X 中顶点全部完成一遍上述过程。

（3）选取一个刚标记（在步骤（2）中用（x_i）标记）过的 Y 中结点，例如 y_i，用（y_i）去标记 X 中结点 x，如果 y_i 与 x 为同一匹配边的两端点，且在本步骤中 x 尚未被标记过。重复步骤（3），直至对刚标记过的 Y 中结点全部完成一遍上述过程。

（2），（3）交替执行，直到下述情况之一出现为止：

（Ⅰ）标记到一个 Y 中顶点 y，它不是 M-顶点。这时从 y 出发循标记回溯，直到（*）标记的 X 中顶点 x，我们求得一条交替链。设其长度为 $2k+1$，显然其中 k 条是匹配边，$k+1$ 条是非匹配边。

（Ⅱ）步骤（2）或（3）找不到可标记结点，而又不是情况（Ⅰ）。

（4）当（2），（3）步骤中断于情况（Ⅰ），则将交替链中非匹配边改为匹配边，原匹配边改为非匹配边（从而得到一个比原匹配多一条边的新匹配），回到步骤（1），同时消除一切现有标记。

（5）对一切可能，（2）和（3）步骤均中断于情况（Ⅱ），或步骤（1）无可标记结点，算法终止（算法找不到交替链）。

我们只用一个例子跟踪算法的执行，不打算证明算法的正确性。

【例 9-3】 用匈牙利算法求图 9-3 的一个最大匹配。

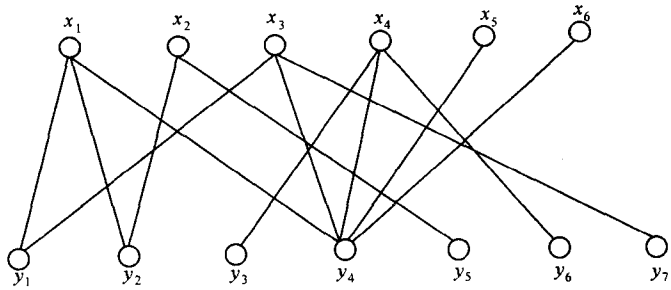


图 9-3

（1）置 $M=\varnothing$，对 x_1-x_6 标记（*）。

（2）找到交替链(x_1, y_1)（由标记（x_1），（*）回溯得），置 $M=\{\{x_1, y_1\}\}$。

（3）找到交替链(x_2, y_2)（由标记（x_2），（*）回溯得），置 $M=\{\{x_1, y_1\}, \{x_2, y_2\},\}$。

（4）找到交替链(x_3, y_1, x_1, y_4)（如图 9-4 所示。图中虚线表示非匹配边，细实线表示交替链中非匹配边，粗实线表示匹配边），因而得 $M=\{\{x_2, y_2\}, \{x_3, y_1\},\{x_1, y_4\}\}$。

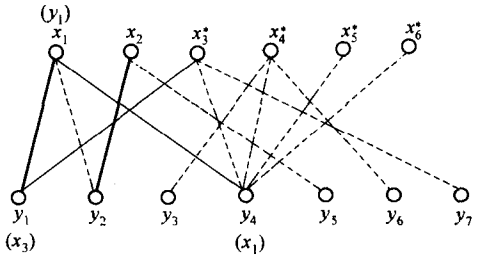


图 9-4

(5) 找到交替链(x_4, y_3)(由标记(x_4)，(*)回溯得)，置$M=\{\{x_2, y_2\}, \{x_3, y_1\}, \{x_1, y_4\}, \{x_4, y_3\}\}$。

(6) 找到交替链$(x_5, y_4, x_1, y_1, x_3, y_7)$(如图 9-5 所示，图中各种线段的意义同上)，因而得

$$M=\{\{x_2, y_2\}, \{x_4, y_3\}, \{x_5, y_4\}, \{x_1, y_1\}, \{x_3, y_7\}\}$$

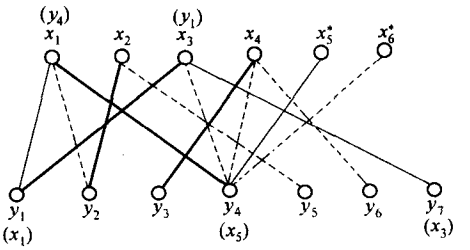


图 9-5

即为最大匹配(如图 9-6 所示)。

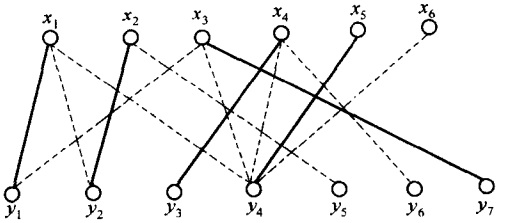


图 9-6

现在我们来讨论完全匹配的存在条件。为此，定义图 $G=<V, E>$的顶点子集 $S\subseteq V$ 的**相邻顶点集** $N(S)$(所有与 S 中顶点相邻的顶点组成的集合)：

$$N(S)=\{v \mid v\in V\wedge\exists u\exists e(u\in S\wedge e\in E\wedge e=\{u, v\})\}$$

或

$$N(S)=\{v \mid \exists u\exists e(u\in S\wedge e=\{u, v\})\}$$

定理 9-2 设图 $G=<X, E, Y>$。G 有 X-完全匹配的充分必要条件是：对每一 $S\subseteq X$ 有

$$|N(S)|\geqslant|S|$$

此定理是霍尔(Hall)于 1935 年证明的，通常称为霍尔婚姻定理。

证明 必要性是易证的。设 G 有 X-完全匹配

$$\{\{x_0, y_{i0}\}, \{x_1, y_{i1}\}, \cdots, \{x_m, y_{im}\}\} \quad (m=|X|)$$

其中诸 x_i 互不相同，诸 y_{ij} 也各不一样，因此对任一 $S\subseteq X$，S 中有多少元素，$N(S)$中至少也有同样多的元素，即$|N(S)|\geqslant|S|$。

现证充分性。

设 G 满足：对任一 $S\subseteq X$，$|N(S)|\geqslant|S|$，但 G 无 X-完全匹配。

作 G 的最大匹配 M，据假设，至少有顶点 $x\in X$，x 不是 M-顶点。用匈牙利算法求起始于 x 的所有交替链。由于 M 已是最大匹配，上述构作过程必定在步骤（3）中因情况（Ⅱ）停止，即它们都只能是末尾边为匹配边的链（暂称伪交替链）。用 Q 表示这些伪交替链上的顶点集合，易知，Q 中只有 x 不是 M-顶点。置

$S=Q\cap X$，$S'=Q\cap Y$（参阅图 9-7）

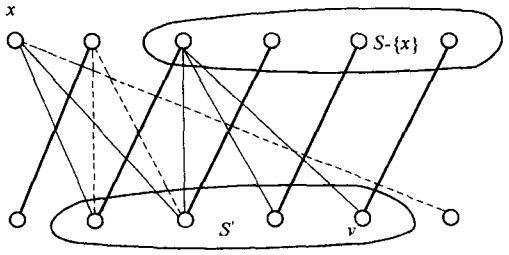


图 9-7

显然，$S-\{x\}$ 中顶点与 S' 中顶点一一对应，因此

$$|S'|=|S|-1$$

$$S'\subseteq N(S)$$

事实上 $N(S)=S'$，因为对每一 $y\in N(S)$，都有顶点 $u\in S=Q\cap X$（因而 $u\in Q$）使 $\{u,y\}$ 为一伪交替链中的边，从而 $y\in Q$，即 $y\in Q\cap Y=S'$ 之中。据以上讨论，

$$|N(S)|=|S'|=|S|-1$$

$$|N(S)|<|S|$$

与题设矛盾，因此 M 必是 X-完全匹配。

定理 9-2 证毕。对 Y-完全匹配有类似的结论，此不赘述。

【例 9-4】 k-正则二分图（$k>0$）有完全匹配。

证明 设 $G=<X,E,Y>$ 为 k-正则二分图，那么

$$k\cdot|X|=|E|=k\cdot|Y|$$

从而 $|X|=|Y|$。

设 S 为 X 的任一子集，E_1 为 S 中顶点所关联的边的集合，E_2 为 $N(S)$ 中顶点所关联的边的集合。据 $N(S)$ 的定义，$E_1\subseteq E_2$，于是

$$k\cdot|N(S)|=|E_2|\geqslant|E_1|=k\cdot|S|$$

$$|N(S)|\geqslant|S|$$

因此 G 有 X-完全匹配 M。

由于 $|X|=|Y|$，显然 M 也是 Y-完全匹配，故 G 有完全匹配。

9.2 平面图

9.2.1 平面图的基本概念

许多实际问题可以抽象为这样的模式：在一些表示客体的结点之间“布线”，以建立它

们之间的某种联系，要求这些线在一个平面上而又不相互交叠。这正是一个本节要讨论的图论问题。

例如，要在三个工作点 A，B，C 和三个原料库 L，M，N 之间建立各工作点到各原料库的传输线，问是否可能使这些线路互不相交？如果用结点表示工作点，用边表示传输线，那么上述问题便可描述为：图 $K_{3,3}$ 是否可以在一个平面上图示出来，而使图中各边除在端点处外均不相交？另外印刷线路板上的布线、交通道路的设计等都是此类问题。为了深入讨论这类问题，需要引入平面图的概念。

定义 9-4 无向图 G 称为**平面图**（planar graph），如果 G 可以在一个平面上图示出来，而使各边仅在顶点处相交。否则称 G 为**非平面图**。

【例 9-5】

（1）图 9-8 中除 e 外各图均为平面图。a，b 显然为平面图；c 为平面图，因为它可以图示如 d。

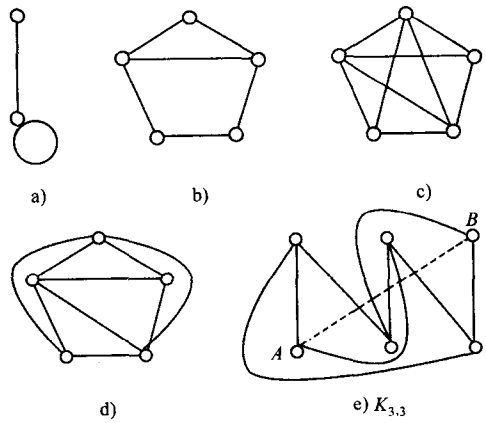


图 9-8

（2）$K_{3,3}$，K_5 都不是平面图。图 9-8e 中边（A，B）无论如何将与其他边相交（指不在顶点处相交，下同），因此 $K_{3,3}$ 非平面图。图 9-8d 中若再添边（非平行边和环）即为 K_5，这一新添加的边无论如何也将与其他边相交，因此 K_5 也不是平面图。当然这种解释不是严格证明，下文将给出严格证明。

$K_{3,3}$ 与 K_5 称为**库拉托夫斯基**（Kuratowski）**图**，它们有一些有趣的共同点：

（1）它们都是正则图。

（2）去掉一条边时它们都是平面图。

（3）$K_{3,3}$ 是边数最少的非平面简单图，K_5 是顶点数最少的非平面简单图，因而它们都是最基本的非平面图。

平面图除了有顶点、边的概念，还有面的概念，为简单计，只对平面连通图讨论。

定义 9-5 平面连通图中各边所界定的区域称为平面图的**面**（regions）。有界的区域称为**有界面**，无界的区域称为**无界面**。界定各面的闭的拟路径称为面的**边界**（boundary），它的长度称为面的**度**（degree）。

【例 9-6】 图 9-9 为一平面图，它共有 5 个面 r_1，r_2，r_3，r_4，r_5，其中 r_5 为无界面，其余为有界面，它们的边界分别是：

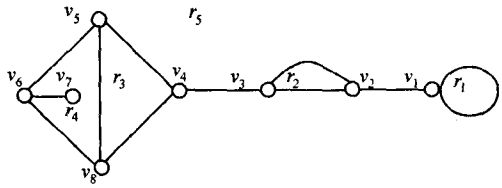


图 9-9

r_1：界定该面的闭的拟路径（v_1, v_1），度为 1。

r_2：界定该面的闭的拟路径（v_2, v_3, v_2），度为 2。

r_3：界定该面的闭的拟路径（v_4, v_5, v_8, v_4），度为 3。

r_4：界定该面的闭的拟路径（$v_5, v_6, v_7, v_6, v_8, v_5$），度为 5。

r_5：界定该面的闭的拟路径（$v_1, v_1, v_2, v_3, v_4, v_5, v_6, v_8, v_4, v_3, v_2, v_1$），度为 11。

下面常讨论平面简单图。显然平面简单图的所有有界面的度均不小于 3。

定义 9-6 称平面简单图 G 是**极大平面图**（maximal planar graph），如果在 G 中添加任一边（它不是环，也不是其他边的平行边）后所得的图均非平面图。

例 9-5 中图 9-8c 为极大平面图。

定理 9-3 极大平面图所有有界面都是 3 度的面，无界面也是 3 度的。即所有面的边界均为 K_3。

证明 反设极大平面图有 4 度的面，其边界为（v_1, v_2, v_3, v_4, v_1）。

若该面为无界面，那么可在无界面内联结（v_2, v_4）；若该面为有界面，那么可在有界面内联结（v_2, v_4）。联结后所产生的图均仍为平面图，这与平面图的极大性冲突。

定理 9-4 顶点个数 $n \geqslant 4$ 的极大平面图中，顶点的最小度数不少于 3 。

证明 设 v 是极大平面图 G 的任一顶点。考虑 $G-v$ 。$G-v$ 是一平面图，v 原在 $G-v$ 的一个面内。由于 G 为一简单图，$G-v$ 的这个面的边界上至少有 3 个顶点。由 G 的极大平面性，v 与这些顶点之间都有边关联，因此 v 至少是 3 度的顶点。

9.2.2 欧拉公式和库拉托夫斯基定理

在中学立体几何课程中，欧拉公式是指下列关于凸多面体的顶点数（n），棱数（m）及面数（r）之间的关系式：

$$n-m+r=2$$

我们设想把一个橡皮的凸四面体的底面剪破，从此撕开四面体，使其各面在同一平面中（参阅图 9-10），如果把撕破的面看作无界面，那么图 9-10b 便是一个连通平面图，它自然也满足上述关系式。这使我们自然地想到，对连通平面图是否依然有上述**欧拉公式**成立。回答是肯定的。

定理 9-5 设 G 为一平面连通图，n 为其顶点数，m 为其边数，r 为其面数，那么

$$n-m+r=2$$

证明 对边数 m 归纳。

当 $m=0$ 时 G 为一孤立顶点，因此 $n=1$，$m=0$，$r=1$（一无界面），从而 $n-m+r=2$。

设边数小于 m 的平面连通图均满足欧拉公式。现考虑 G（边数 $m>0$），在 G 中任意去掉一边 e 得到图 G'。下面对 e 的情况分别进行讨论（参见图 9-11）

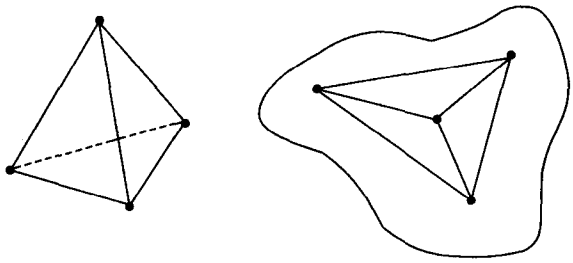


图 9-10

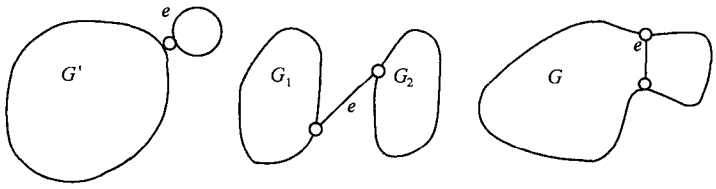


图 9-11

（1）e 为一环，那么 G'的顶点数、边数、面数分别是

$$n'=n\,,m'=m-1\,,r'=r-1$$

据归纳假设，$n'-m'+r'=2$。因而

$$n-(m-1)+r-1=2$$

即

$$n-m+r=2$$

（2）$\{e\}$为割集，不妨设 G'有两个连通分支 G_1，G_2。显然 $n_1+n_2=n'=n$，$m_1+m_2=m'=m-1$，$r_1+r_2=r'+1=r+1$。据归纳假设

$$n_1-m_1+r_1=2$$

$$n_2-m_2+r_2=2$$

从而

$$(n_1+n_2)-(m_1+m_2)+(r_1+r_2)=4$$

$$n-(m-1)+r+1=4$$

即

$$n-m+r=2$$

（3）e 关联 G 中两个顶点但$\{e\}$非割集，那么 G'的顶点数、边数和面数分别是

$$n'=n,\quad m'=m-1\,,\quad r'=r-1$$

据归纳假设，$n'-m'+r'=2$，从而

$$n-(m-1)+r-1=2$$

即

$$n-m+r=2$$

归纳完成，定理得证。

利用欧拉公式可以获得一系列有用的推论。

定理 9-6 如果平面连通图 G 的每个面的边界都具有长度 $l(l\geqslant 3)$，那么

$$m=\frac{l(n-2)}{l-2}$$

其中 m 为 G 的边数，n 为 G 的顶点数。

证明 设 G 有 k 个面。由于每一条边或者是两个面的边界，或者是一个面的两条边界（如图 9-9 中边$\{v_6, v_7\}$），因此

$$l\circ k=2\mathrm{m} \quad 或 \quad k=\frac{2m}{l}$$

将 k 代入欧拉公式，得

$$n-m+\frac{2m}{l}=2$$

解出 m 得

$$m=\frac{l(n-2)}{l-2}$$

定理 9-7 设 G 为一平面连通简单图，其顶点数 $n\geqslant 3$，其边数为 m，那么

$$m \leqslant 3n-6$$

证明 在 G 上添加边，使之成为一个极大平面图 G'。据定理 9-3，G'所有面的边界长度为 3，因此 G'的边数

$m'=\frac{3(n-2)}{3-2}=3n-6$，故

$$m\leqslant m'=3n-6$$

利用定理 9-7 可证明某些图是非平面图。

【例 9-7】 K_5 是非平面图。

证明 反设 K_5 为平面图，又 K_5 是连通简单图，那据定理 9-7，有

$$10 \leqslant 3\times 5-6=9$$

矛盾，故 K_5 非平面图。

定理 9-8 设 G 为一平面简单连通图，其顶点数 $n\geqslant 4$，边数为 m，且 G 不以 K_3 为其子图，那么

$$m \leqslant 2n-4$$

证明 由于 G 是不以 K_3 为子图的简单图，因此 G 的每个面的边界长度不小于 4。

同定理 9-6 之证明，G 的 k 个面的边界长度总和应为 $2m$，而根据题设又知 $4k$ 不超过这一总和，因此

$$4k \leqslant 2m \text{ 或 } k \leqslant \frac{m}{2}$$

据欧拉公式有

$$2=n-m+k \leqslant n-m+\frac{m}{2}=n-\frac{m}{2}$$

即

$$\mathrm{m}\leqslant 2n-4$$

定理 9-7 也可仿此定理的证明，请读者自行完成。利用定理 9-8 也可证明一些图是非平面图。

【例 9-8】 $K_{3,3}$ 是非平面图。

证明 设 $K_{3,3}$ 是平面图。显然 $K_{3,3}$ 不以 K_3 为其子图，又 K_5 是连通简单图，因而定理 9-8 适用之。于是

$$9 \leqslant 2\times 6-4=8$$

矛盾，故 $K_{3,3}$ 非平面图。

定理 9-9 顶点数 n 不少于 4 的平面连通简单图 G，至少有一个顶点的度数不大于 5。

证明 反设 G 的所有顶点的度数均大于 5，因而 G 的所有顶点的度数之和至少是 $6n$。若 m 为 G 的边数，那么据定理 9-7，有

$$3n-6 \geqslant m$$

$$6n-12 \geqslant 2m \geqslant 6n$$

矛盾，故 G 至少有一个顶点的度不超过 5。

应当指出，欧拉公式及其上述推论都只是平面连通图或平面连通简单图的必要条件，而不是它们的充分条件，因此只能用它们判别非平面图，不能用它们来识别平面图。那么，是否有关于平面图的判定定理呢？有，库拉托夫斯基定理给出了图为平面图的一个充分必要条件。

在介绍库拉托夫斯基定理之前，我们先引入两种对图的操作。

（1）对边 e 的**切割**操作。设 G 中有边 $e=\{u,v\}$，对边 e 作切割操作是指：

1）取消边 e。

2）增加顶点 w，以及边 $e1=\{u,w\}$，边 $e2=\{w,v\}$。

（2）对顶点 v 的**贯通**操作。设 G 中有二度顶点 v，它是 $e1=\{u,v\}$，$e2=\{v,w\}$的共同端点。对顶点 v 作**贯通**操作是指：

1）取顶点 v 以及边 $e1,e2$。

2）增加边 $e=\{u,w\}$ 。

切割与贯通是互逆的，两者常被称为图的**同胚**操作。

【例 9-9】 图 9-12a 为图 G，b、c 分别是边 e 切割和顶点 v 贯通操作的结果。

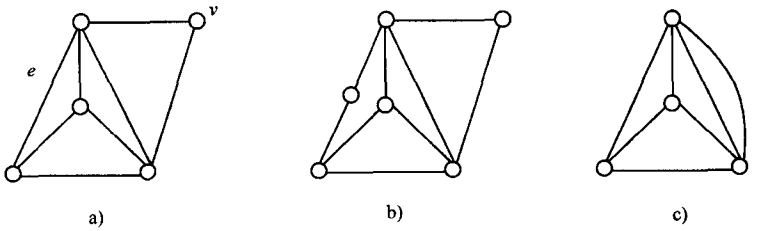


图 9-12

a) 图 G b) 边 e 切割 c) 顶点 v 贯通

定理 9-10 （库拉托夫斯基定理）图 G 是平面图，当且仅当对 G 或 G 的子图作任何同胚操作后所得图均不以 K_5 及 $K_{3,3}$ 为子图。

定理的证明略去。

【例 9-10】 图 9-13a 为一非平面图，因为 b 是 a 的子图。而 b 经同胚操作后为 c，此为 $K_{3,3}$。

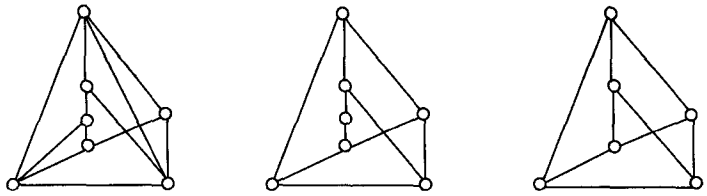


图 9-13

*9.2.3 着色问题

早在 19 世纪中期，英国数学家就提出了地图着色问题：给地图的各地域着色，要使相邻的地域具有不同的颜色，至少需要多少种颜色。显然，3 种颜色是不够的，例如图 9-14 中的 4 个地域至少要 4 种颜色才能作出满足上述要求的着色。另一方面，人们很快证明了，

5 种颜色是足够的。当时英国青年盖思里（Guthrie）提出，用 4 种颜色即可给地图着色，使相邻区域具有不同的颜色，但他未能加以证明。于是，这给后人留下了一个著名的难题——四色问题。

地图着色问题很明显可以用平面图的面着色来刻画。为了便于讨论，我们把平面图的面着色问题转换为同等的顶点着色问题。为此，需要下列的对偶图概念。

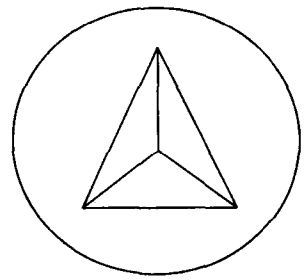


图 9-14

定义 9-7 对连通平面图 G 实施下列步骤所得到的图 G^*称为 G 的**对偶图**(dual of graph)：

（1）在 G 的每一个面 r_i 的内部作一个 G^*的顶点 v_i^*。

（2）若 G 中面 r_i 与 r_j 有公共边界，那么过边界的每一边 e_k 作关联 v_i^* 与 v_j^* 的一条边 e_k^*。e_k^* 与 G^*的其他边不相交。

（3）当 e_k 为面 r_i 的边界而非 r_i 与其他面的公共边界时，作 v_i^* 的一条环与 e_k 相交（且仅交于一处）。所作的环不与 G^*的边相交。

【例 9-10】 图 9-15b 是 a 的对偶图。b 中虚线部分表示原图 a，实线部分则是 a 的对偶图。

注意，当 G_1，G_2 为同构图的两种不同图示，那么它们的对偶图 G_1^* 与 G_2^* 不仅图示不同，而且可能是根本不同的图（不同构）。这就是说，一个图的对偶图未必是惟一的。

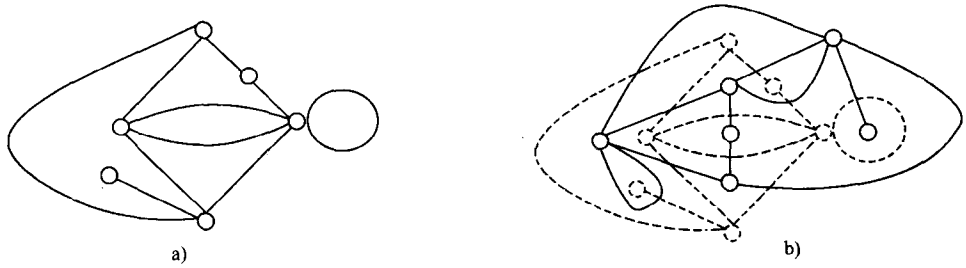


图 9-15

【例 9-11】 图 9-16a，b 中实线部分是两个同构的图（图示不同），a、b 中虚线部分分

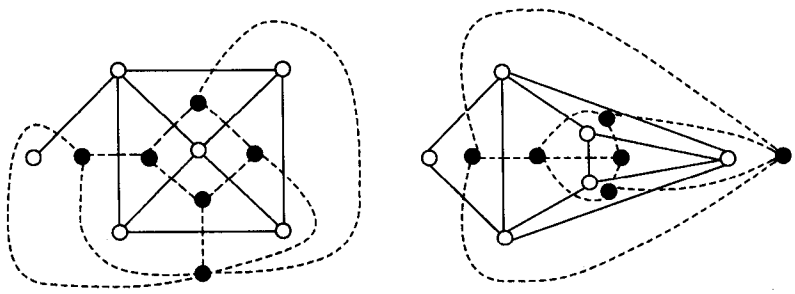
别表示它们的对偶图，这两个图是不同构的，a 中对偶图有 5 度顶点，b 中对偶图却没有。

对偶图有许多性质，我们关心的是：

（1）图 G 的面与 G^*的顶点一一对应，且 G 中面的度等于 G^*中对应顶点的度 。

（2）G 中两个面有公共边界，当且仅当 G^*中对应顶点之间有边关联。

（3）G 为平面图当且仅当 G^*为平面图。



a)　　b)

图 9-16

因此，对于图的面着色问题，可以通过研究其对偶图的顶点着色问题来解决。以下讨论图的顶点着色问题。先推广定义 8-20 中的 2-着色概念。

定义 9-8　无向图 G 称为**可 k-着色的**（k-chromatic），如果可用 k 种颜色给 G 的所有顶点着色，使每个顶点着一种颜色，而同一边的两个端点着不同颜色。

定理 9-11　任何无环平面图都是可 5-着色的。

证明　由于各连通分支可 5-着色当且仅当原图可 5-着色，由于平行边与着色问题无关，因此可只讨论平面连通简单图。

设 G 为任一平面连通简单图，顶点个数为 n。对 n 归纳。

当 $n \leqslant 5$ 时命题显然成立。

设 $n-1$ 个顶点的平面图都是可 5-着色的。考虑 n 个顶点的图 G。由定理 9-9，G 至少有一个顶点的度不大于 5，设 v_0 为这样一个顶点。令 $G' = G - v_0$，据归纳假设，G'可 5-着色。假定 G'已用红、黄、兰、白、黑 5 种颜色按要求着色，现将 v_0 及它所邻接的边（至多五条）放回原处（恢复图 G）。考虑 v_0 的着色。

（1）设 $\deg(v_0)<5$，那么只要取它相邻顶点所着颜色（至多 4 种）之外的一种颜色给 v_0 着色，便可完成对 G 的 5-着色。

（2）设 $\deg(v_0)=5$，若与 v_0 相邻的顶点用了少于 5 种颜色着色，便可完成对 G 的 5-着色。否则设 v_0 相邻顶点的着色状况如图 9-17 所示。

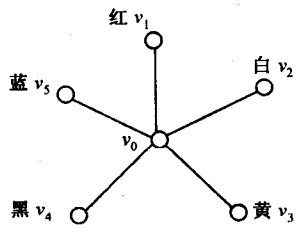


图 9-17

为叙述简明，令 RY 表示 $G-v_0$ 中所有着红、黄顶点的集合，BW 表示 $G-v_0$ 中所有着黑、白顶点的集合。考虑 RY 生成的 G 的子图 $G(RY)$。

若 v_1，v_3 分属于 $G(RY)$ 的两个不同的连通分支，那么只要将 v_1 所在分支的红、黄顶点的着色作一对换（从而 v_1 着黄色），便可给 v_0 着红色以完成对 G 的 5-着色。

若 v_1 和 v_3 同属于一个 G（RY）的连通分支，那么从 v_1 到 v_3 必有一条通路，其各顶点被红、黄两色相间着色。这条通路连同 v_0 便构成回路：

$$C:\ v_0, v_1, \cdots, v_3, v_0$$

C 把 BW 分成两部分，一部分在回路 C 之外，一部分在 C 之内。于是，BW 生成的 G 的子图也被分成了两个互不连通的部分，一部分在 C 外，一部分在 C 内，这就使 v_2，v_4 处于 BW 生成的 G 的子图的两个不同连通分支，同上将 v_2 所在分支作颜色对换，以便给 v_0 着上白色，完成对 G 的 5-着色。

归纳完成，定理得证。

9.3 树

树是一种极为简单而又非常重要的特殊图，它在计算机科学的算法设计、数据结构、网络技术、人工智能、软件工程、知识工程以及其他许多领域都有广泛的应用。

9.3.1 树的基本概念

定义 9-9 连通无回路的无向图称为**无向树**，简称为**树**（tree）。树中的悬挂点又称为**树叶**（leave），其他结点称为**分支点**（branched node）。单一孤立结点称为**空树**（null tree）。诸连通分支均为树的图称为**森林**（forest），树也是森林。

【例 9-13】 图 9-18a、b 为树，而 c 不是树，但 c 为森林。

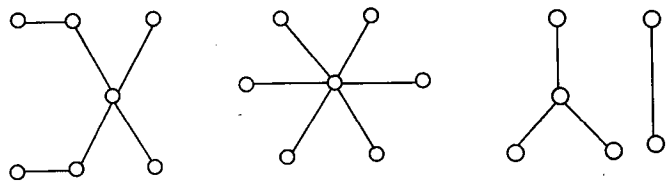


图 9-18

由于树无环也无重边（否则它有回路），因此树必定是简单图。树还有一些一目了然的性质，罗列如下，有的证明请读者完成。

定理 9-12 树和森林都是可 2-着色的，从而都是二分图。

定理 9-13 树和森林都是平面图，其面数为 1。

定理 9-14 设图 T 为一树，其顶点数、边数分别是 n, m，那么

$$n-m=1 \quad 或 \quad m=n-1$$

证明 因 T 为树，故 T 为连通平面图。据欧拉公式和 $n-m+1=2$，即 $n-m=1$。

定理 9-15 任何树都至少有两片叶。

证明 设 T 为任一树，其顶点数、边数分别为 n, m。又设 T 中至多只有一个顶点是叶，那么

$$2m=\sum_{i=1}^{n} deg\ (v_i) \geqslant 2(n-1)+1=2n-1$$

$$m \geqslant n-\frac{1}{2} > n-1$$

这与定理 9-14 矛盾。因此 T 至少有两片叶。

树还有下列 5 种等价定义形式。

定理 9-16 命题“(n, m) 图 T 为树”与下列 5 命题中的每一命题等价：

（1）T 无回路且 $m=n-1$ 。

（2）T 连通且 $m=n-1$ 。

（3）T 无回路，但任意添加边时，T 中产生惟一的一条回路。

（4）T 连通，但删去任一边时便不再连通（T 的每一边均为割边）。

（5）任意两个不同顶点之间有且仅有一条通路。

证明 记“T 为树”即“T 连通无回路”为命题（0）。为证（0）与（1），（2），（3），（4）（5）均等价，我们证

$$(0) \Rightarrow (1) \Rightarrow (2) \Rightarrow (3) \Rightarrow (4) \Rightarrow (5) \Rightarrow (0)$$

$(0) \Rightarrow (1)$ 这由定理 9-14 立得。

$(1) \Rightarrow (2)$ 设 T 无回路，$m=n-1$ ，欲证 T 连通。反设 T 有 k 个连通分支（$k \geqslant 2$），T_1，T_2，…，T_k，它们的顶点数分别是 $n_1, n_2, \cdots, n_k$，边数分别是 $m_1, m_2, \cdots, m_k$，显然

$$n=\sum_{i=1}^{k} n_i , \quad m=\sum_{i=1}^{k} m_i$$

$$m_i=n_i-1 \quad (i=1,2,\cdots,k)$$

于是

$$m=\sum_{i=1}^{k} m_i = \sum_{i=1}^{k} (n_i-1) = n-k < n-1$$

矛盾。因此 T 连通。

$(2) \Rightarrow (3)$ 设 T 连通且 $m=n-1$。先证 T 无回路，为此对 n 归纳。

$n=1$ 时显然 T 无回路，因这时 $m=n-1=0$。

设顶点数为 $n-1$ 的满足题设的图无回路，考虑顶点数为 n 的图 T。去掉 T 的一悬挂点（同定理 9-15 的证明可证，T 至少有两个悬挂点）构成 T'。显然 T' 仍连通，且 $m'=m-1=n-2=n'-1$，因此由归纳假设 T' 无回路。在 T' 上加回所删去的悬挂点得 T，故 T 亦无回路。

再证（3）的第二部分，设在 T 的顶点 v_i，v_j 间添加边 e。由于 T 连通，故原本有 v_i 到 v_j 的通路，此通路连同边 e 构成 $T \cup \{e\}$ 的一条回路。若此回路不惟一，那么去掉边 e 后 T 仍有回路，与以上证明冲突。这就是说，在 T 中添加任一边后，将产生惟一的一条回路。

$(3) \Rightarrow (4)$ 留给读者自行证明。

$(4) \Rightarrow (5)$ 留给读者自行证明。

$(5) \Rightarrow (0)$ 设 T 的任何两个顶点之间有且仅有一条通路，那么 T 显然连通。T 也是无回路的，否则 T 中有回路上顶点 v_i，v_j，使 v_i 到 v_j 有两条通路，与题设矛盾。

从以上特征性可以看出，树是“最小的连通图”，少一边便不连通；树又是“最大的无回路图”，多一边便有回路，因而树是以“最经济”的方式把其中各顶点连接起来的图。因此它可用作典型的数据结构，各类网络的主干网也通常都是树的结构。

9.3.2 生成树

由上面的讨论我们知道，树是一种结构“很优秀”，也是“最经济”的特殊图，但有的连通图不是树，而由树的特性使我们想到，一个连通图 G 的“最小连通生成子图”应当是一棵树，即生成子图构成的树。这棵树对图 G 很重要，我们常称为图 G 的生成树。

定义 9-10 图 T 称为无向图 G 的**生成树**（spanning tree），如果 T 为 G 的生成子图且 T 为树。

定理 9-17 任一连通图 G 都至少有一棵生成树。

证明 若 G 无回路，则 G 本身为一树。若 G 有回路。则删去回路上任一边 e，$G-e$ 仍连通。对 $G-e$ 重复上述讨论，直到得到 G 的无回路的连通子图——生成树。

由此可知，对于连通图 G 我们可以通过依次从回路中删边的方法得到其生成树，此方法常称为破圈法。不过，生成树通常是不惟一的。

【例 9-14】 图 9-19b、c 为图 a 的两棵生成树。

关于生成树，下面两个性质是容易理解的。

定理 9-18 设 G 为连通无向图，那么 G 的任一回路与任一生成树 T 的关于 G 的补 $G-T$，至少有一条公共边。

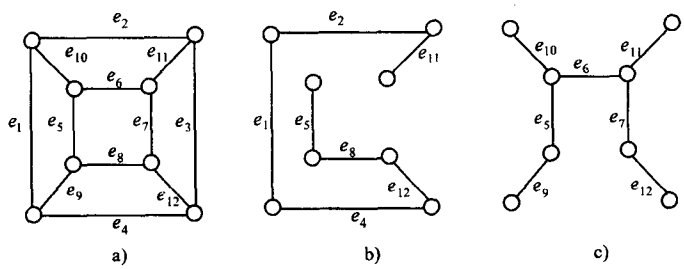


图 9-19

证明 设 C 为 G 的一回路，它和 G 的生成树 T 关于 G 的补 $G-T$ 无公共边，那么 C 是 T 的子图，从而树 T 中有回路，矛盾。

定理 9-19 设 G 为连通无向图，那么 G 的任一割集与任一生成树至少有一条公共边。

证明 设 S 为 G 的割集，但它和 G 的生成树 T 无公共边。那么，删去 G 中所有 S 的边后所得的图仍以 T 为子图，从而仍连通，这与 S 为割集矛盾。

联系到树的性质，我们想到，图的回路总可由一生成树上的一条路径及生成树外的一条边构成，而图的割集总可由生成树上的一条边与生成树外的若干条边组成。

定义 9-11 设 T 为图 G 的生成树，称 T 中的边为树枝（branch），称 $G-T$ 中的边为弦（chord）。对每一树枝 t，$T-t$ 分为两个连通分支 T_1，T_2，那么 t 及两端点分别在 T_1，T_2 中的弦组成 G 的一个割集，它被称为**枝 t-割集**（t-cut set）；而每一条弦 e 与 T 中的通路构成一回路，它被称为**弦 e-回路**（e-circuit）。

很显然，(n, m) 图 G 的任一生成树 T 恒有 $n-1$ 条边，$m-n+1$ 条弦；从而有 $n-1$ 个枝 t-割集，$m-n+1$ 个弦 e-回路（这里的 t 指任一树枝，e 指任一弦），它们分别称为**枝割集系**和**弦回路系**。

【例 9-15】 设 G 为图 9-19a，G 的生成树为图 9-19c，那么

（1）$e_5, e_6, e_7, e_9, e_{10}, e_{11}, e_{12}$，均为树枝，共 $8-1=7$ 枝。

（2）e_1, e_2, e_3, e_4, e_8 均为弦，共 $12-8+1=5$ 条。

（3）枝 e_5-割集是{ e_5, e_1, e_4, e_8 }

枝 e_6-割集是{ e_6, e_2, e_4, e_8 }

枝 e_7-割集是{ e_7, e_3, e_4, e_8 }

枝 e_9-割集是{ e_9, e_1, e_4 }

枝 e_{10}-割集是{ e_{10}, e_1, e_2 }

枝 e_{11}-割集是{ e_{11}, e_2, e_3 }

枝 e_{12}-割集是{ e_{12}, e_3, e_4 }

（4）弦 e_1-回路是（e_1, e_9, e_5, e_{10}）

弦 e_2-回路是（e_2, e_{10}, e_6, e_{11}）

弦 e_3-回路是（e_3, e_{11}, e_7, e_{12}）

弦 e_4-回路是（$e_4, e_9, e_5, e_6, e_7, e_{12},$）

弦 e_8-回路是（e_8, e_5, e_6, e_7）

现在我们来讨论枝割集系统与弦回路系统的关系。下列定理是一个准备。

定理 9-20 在连通无向图 G 中，任一回路与任一割集均有偶数条公共边。

证明 设 C 为 G 的任一回路，S 为 G 的任一割集，从 G 中删除 S 的所有边后得到两个互不连通的子图 G_1，G_2（如图 9-20 所示）。

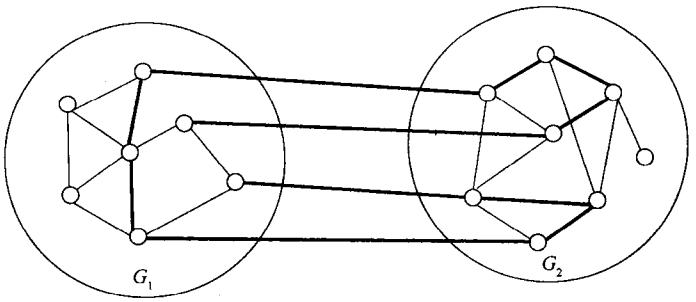


图 9-20

若回路 C 上的所有顶点都在 G_1（或 G_2）中，那么，C 和 S 无公共边，定理得证。

若回路 C 的一部分顶点在 G_1 中，另一部分在 G_2 中，那么 C 必定经过 S 中偶数条边（因 C 为回路，参阅图 9-20），故 C 与 S 有偶数条公共边。

定理 9-21 设 G 为一连通无向图，T 是 G 的生成树，$S=\{e_1, e_2, e_3, \cdots, e_k\}$ 为枝 e_1-割集，那么 e_1 必在弦 e_i-回路中（$i=2, 3, \cdots, k$），不在其他弦 e-回路中。（e_1 与弦 e_i-回路恰有两条公共边 e_1 和 e_i，而 e_1 与其他弦 e-回路无公共边。）

证明 设 C 为任一弦 e_i-回路（i=2，3,…，k），例如 C 为弦 e_2-回路，则 e_2 在 S 与 C 中。又据定理 9-20，C 与 S 有偶数条公共边。由于 S 中只有 e_1 为树枝，其余各边均为弦；而 C 中只有 e_2 为弦，其他各边均为树枝，所以只能还有 e_1 在 S 与 C 中。即 S 与 C 恰有两条公共边 e_1 和 e_2，因此 e_1 在弦 e_2-回路中。由于证明过程对一切 e_i（$i=2, 3, \cdots, k$）均成立，因此定理的前半部分得证。

为证定理后半部分，设 C 为弦 e-回路，而 $e \neq e_2, e_3, \cdots, e_k$。而 C 中只有 e 为弦，S 中 $e_2, e_3, \cdots, e_k$

为弦，故 $e \notin S$。由于 S 中只有 e_1 为树枝，其余各边均为弦；而 C 中只有 e 为弦，其他各边均为树枝，$e \notin S$，所以若 e_1 在 C 中，那么 C 与 S 只可能有一条公共边 e_1，此与定理 9-20 矛盾。因此，C 与 S 无公共边，即 $e_1 \notin C$。

定理 9-22 设 G 为一连通无向图，T 是 G 的生成树，$C=(e_1, e_2, \cdots, e_k)$ 为弦 e_1-回路，那么 e_1 必定在枝 e_i-割集中（$i=2, 3, \cdots, k$），不在其他任何枝 e-割集中。

证明请读者自行完成。

【例 9-15】 图 9-21 为一连通无向图 G，黑粗线描出了 G 的一棵生成树，虚线表示各个枝-割集。

考虑回路（d, a, b, e），它是弦 d-回路，因此，d 出现于枝 a-割集$\{a, c, d\}$、枝 b-割集$\{b, c, d\}$、枝 e-割集$\{e, d, f\}$中，但 d 不出现于枝 h-割集$\{h, g, f\}$和枝 i-割集$\{i, g, f\}$中。

考虑枝 b-割集$\{b, c, d\}$，b 出现于弦 c-回路（c, b, a）及弦 d-回路（d, a, b, e）中，但 b 不出现于弦 f-回路（f, e, h, i）和弦 g-回路（g, h, i）中。

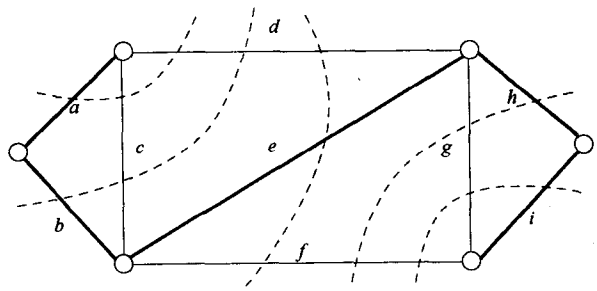


图 9-21

我们知道，一个连通图的生成树往往是不惟一的。而对于赋权图我们最关心的也是最有用的是所谓的最小生成树，下面我们来介绍它的概念及生成算法。

设 $G=<V, E, W>$为连通的边赋权图，W 为 E 到非负实数集的函数。设 T 为 G 的生成树，那么 T 中各边权之和 $W(T)=\sum_{e \in T} W(e)$ 称为生成树 T 的权，权最小的生成树称为**最小生成树**。

对赋权图求最小生成树的问题，在实际应用中是经常可遇到的。以下是求最小生成树的**克鲁斯克尔（Kruskal）算法**。

设连通边赋权图 G 有 n 个顶点 m 条边，并设

$$W(e_1)<W(e_2)<W(e_3)<\cdots<W(e_m)$$

（1）设置变量 k，A。置 k 为 1，置 A 为∅。

（2）若 G 的子图$<V, A \cup \{e_k\}>$不包含回路，那么置 A 为 $A \cup \{e_k\}$。

（3）当$|A|=n-1$ 时算法终止，否则置 k 为 $k+1$，回到步骤（2）。

算法的基本思想是，依边权从小到大的次序，逐边将它们放回到所关联的顶点上，但删去会生成回路的边，直至产生一个 $n-1$ 条边的无回路的子图。此法常形象地称为**避圈法**。算法是正确的。为证明这一点，我们先证明下列定理。

定理 9-23 设 G 是连通边赋权图，且各边的权互不相等。若 C 是 G 中的一条回路，那么 C 上权最大的边 e 必定不在 G 的最小生成树上。

证明 设 C 中权最大的边 e 在 G 的最小生成树 T 上。考虑枝 e-割集 S，S 与回路 C 有偶数条公共边，其中之一是 e，至少还有一条弦是公共边，记为 f。显然，f 在 C 中，$W(f)<W(e)$。现将 f 放入 T 中，构成 G 的子图 H，H 中仅有弦 f-回路。于是知 $H-e$ 为一生成树，且由于 $W(f)<W(e)$，可知 $W(H-e)<W(T)$，与 T 为最小生成树矛盾（参阅图 9-22）。

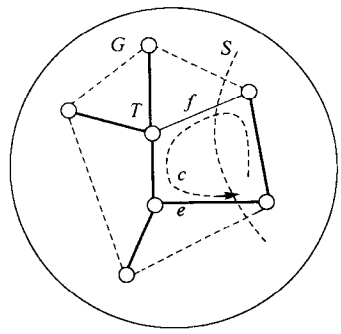


图 9-22

克鲁斯克尔算法是正确的，因为：

（1）算法产生的图无回路，且边数 $m=n-1$，据定理 9-16，此图为树。由于它含有 G 的所有 n 个顶点，因而是 G 的生成树。

（2）设算法生成的树 T 不是最小生成树，另有最小生成树 T'，那么至少有一边 e 在 T' 中而它不在 T 中。考虑关于生成树 T 的弦 e-回路，据算法实施过程知，e 是该回路中权最大的边。于是由定理 9-23，e 不会在 G 的最小生成树 T'中，矛盾。因此，算法生成的树是最小生成树。

最后我们指出两点：

（1）对于有边权相同的赋权图，克鲁斯克尔算法依然成立。若两条边的边权相同，这时无论怎样对它们顺序都一样。

（2）利用求生成树的破圈法也可求最小生成树，但其算法与避圈法相反。即依次从图的回路中删去边权最大的边，直至没有回路结束。若在某一回路中，两个边权相同且最大，这时可删去其中的任意一条。

9.3.3 根树

递归地定义根树的概念。

定义 9-12 树 T 称为**根树**（rooted tree），如果

（1）T 为一孤立结点 v_0。v_0 又被称为 T 的**树根**。

（2）T_1，T_2,…,T_k 为以 v_1，v_2,…，v_k 为树根的根树，T 由 T_1，T_2,…,T_k 及与 v_1，v_2,…，v_k 相邻的结点 v_0 所组成。v_0 称为 T 的**树根**。

定义 9-13 在定义 9-12 中：

（1）v_1，v_2,…，v_k 称为 v_0 的**儿子**，v_0 称为它们的**父亲**。v_i，v_j 同为一顶点 v 的儿子时，称它们为**兄弟**。

（2）顶点间的父子关系的合成称为顶点间的**祖孙关系**。即当 v_i 为 v_{i+1} $(i=1,2,\cdots,l-1)$的父亲时，v_1 是 v_l 的祖先，v_l 为 v_1 的**子孙**。

（3）根树 T 自身及以它的树根的子孙为根的根树（T 的子图），均称为 T 的**子树**（subtree），后者又称为 T 的**真子树**。

根树除有树的一般特性外，还有下列简明的性质。

根树的每个结点都是一棵子树的树根。

除了树根，根树中每结点均为某一结点的儿子；除了树叶，根树中每一结点均为某些结点的父亲。

树根到叶有惟一的通路，这样的通路中最长一条的长度称为**树高**。

为了图示能表明根树的树根和结点间的父子关系、兄弟关系，通常约定根树的图示中：

树根总画在树的顶部，同一顶点的儿子画在同一水平线上。

【例 9-16】 图 9-23 为一以 v_0 为根的根树，虚线框出部分为其一棵子树及该子树的子树。整个树的树高为 4。

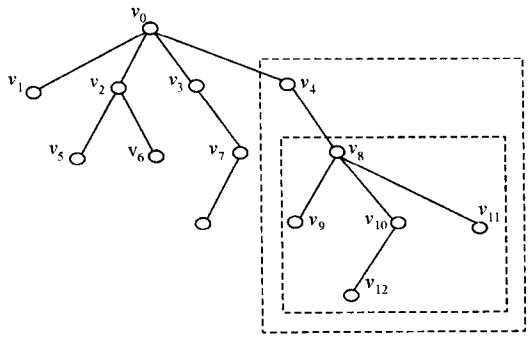


图 9-23

根树可用于表示很多种数据或逻辑关系，下面用一个例子说明这一点。

【例 9-18】 甲乙两人进行乒乓球赛，规定一方连胜两局或胜局首先达到 3 局者为胜方。问甲乙至少、至多要进行多少局比赛。

如果用分支结点表示一局比赛，用关联的两边表示胜负状况，标记甲的边表示甲胜，标记乙的边表示乙胜，那么可用一棵根树来描述比赛的各种可能进程，从而确定比赛至少要进行 2 局，至多要进行 5 局（见图 9-24）

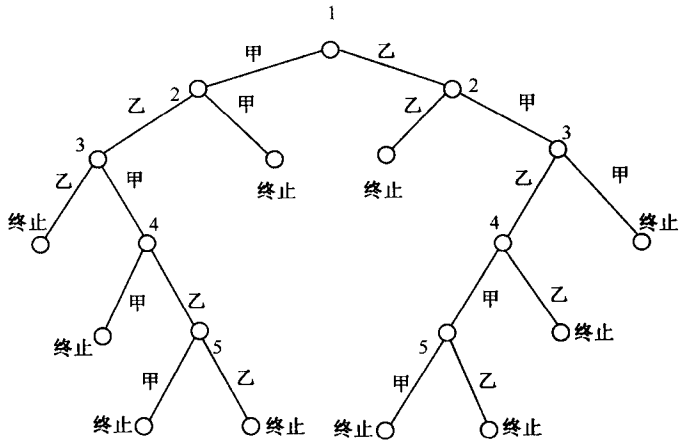


图 9-24

图 9-24 是一种特殊的根树，完全 2 元树，这是一种最为简单而又特别有用的根树。

定义 9-14 除了树叶外，每个结点都有两个儿子的根树称为**完全 2 元树**（binary tree）。

完全 2 元树有以下性质。

定理 9-24 完全 2 元树的顶点个数 n 必定是奇数。

证明 完全 2 元树中除树根的度为 2 外，其他顶点的度均为 3 或 1，因此完全 2 元树度

数总和为 $n-1$ 个奇数的和加 2。若 n 为偶数，则 $n-1$ 为奇数，从而树的度数的总和为奇数，但这是不可能的，因此 n 必为奇数。

定理 9-25 完全二元树中叶的数目 $l=\frac{n+1}{2}$，其中 n 为树的顶点数。

证明 设完全二元树 T 有 n 个顶点，l 片叶和 m 条边，那么除根和叶以外它有 $n-1-l$ 个分支结点，各为 3 度顶点，于是

$$m=\frac{2+3(n-l-1)+l}{2}=n-1$$

解出 l

$$l=\frac{n+1}{2}$$

定理 9-26 完全二元树高 h 满足

$$[\log_2(n+1)-1]\leqslant h\leqslant\frac{n-1}{2}$$

这里 n 为二元树的顶点个数，$[a]$表示 a 的取整运算，即小于等于 a 的最大整数。

证明 如果高为 h 的完全二元树的树根到每片树叶的通路长度均为 h，那么它的顶点数应是

$$2^0+2^1+2^2+\ldots+2^h=2^{h+1}-1$$

因此，对一般高为 h 的完全二元树其顶点数 $n\leqslant 2^{h+1}-1$，即 $2^{h+1}\geqslant n+1$，

因而 $h\geqslant\log_2(n+1)-1$，故

$$[\log_2(n+1)-1]\leqslant h$$

另一方面，如果高为 h 的完全二元树的每个分支结点的两个儿子中必有一个儿子是叶，那么它的顶点数应是$(h+1)+h$，而对一般高为 h 的完全二元树其顶点数 $n\geqslant(h+1)+h$，

故 $h\leqslant\frac{n-1}{2}$。

现在我们来讨论更一般的二元树，简称二元树。

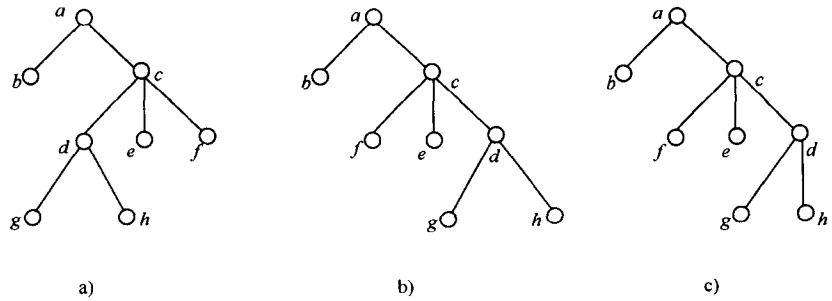
定义 9-15 每个结点都至多有两个儿子的根树称为**二元树**（quasibinary tree）。类似地，每个结点都至多有 n 个儿子的根树称为 **n 元树**。对各分支结点的诸儿子规定了次序（例如左兄右弟）的 n 元树称为 **n 元有序树**；若对各分支结点的已排序的诸儿子规定了在图示中的位置（例如左、中、右），那么该 n 元有序树又称 **n 元位置树**。2 元位置树各分支结点的左右儿子分别称为**左儿子**和**右儿子**。

【例 9-19】 图 9-25a、b、c 均为 3 元树。a、b 作为一般 3 元树是相同的，但作为 3 元有序树是不同的。b、c 作为一般 3 元树和 3 元有序树是相同的，但作为 3 元位置树是不同的。

我们用一个例子来指出一个重要的事实：任何 n 元有序树都可以用 2 元有序树来表示，即可对任何一 n 元有序树作一系列的变换，使之成为一棵 2 元位置树，从这一 2 元位置树中可得到原 n 元有序树的有关性质，甚至恢复出这一 n 元有序树。这对计算机很重要，因为计算机处理二元树是最方便的。

图 9-26a 为一 4 元有序树，为了表示为 2 元位置树，只要将每个分支结点的诸儿子中的大儿子（以左兄右弟为序）保留为其儿子（左儿子），而放弃其他儿子，令二儿子为大儿子

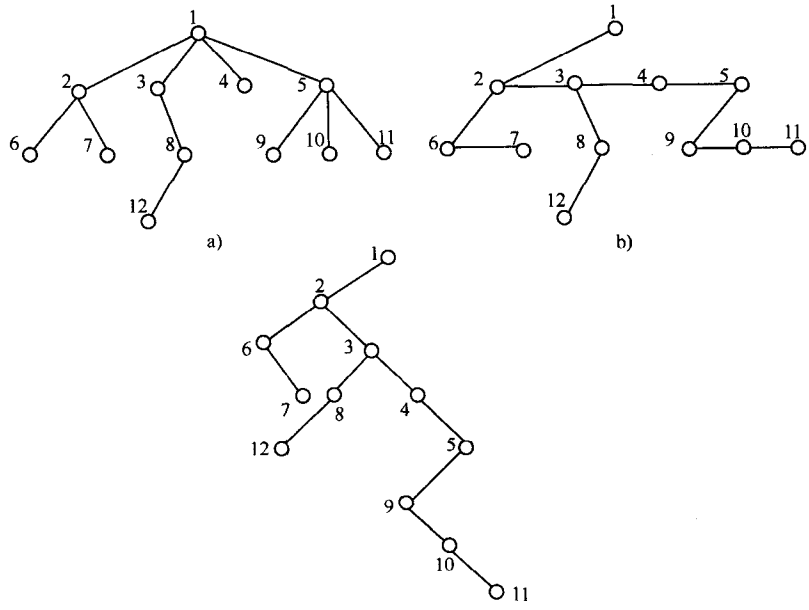
的右儿子，三儿子为二儿子的右儿子，如此等等，如图 9-26b 所示。9-26c 是按根树的约定画法重画图 9-26b 所得的、表示图 9-26a 的 2 元位置树。



a) b) c)

图 9-25

在作出的 2 元位置树中检索原 n 元有序树或恢复原 n 元有序树，只要把每一分支结点的左儿子看作它的大儿子，而将其右儿子看作它的弟兄，删去该分支结点到其右儿子的边，添加该分支结点的父结点到该分支结点的右儿子结点的边。



a) b)

c)

图 9-26

用类似的方法可用 2 元位置树来表示由 n 元有序树组成的森林（称为有序森林）。其做法是，将森林中的每一棵 n 元有序树表示为 2 元位置树，将它们的树根以父子方式连接起来，左父右子。图 9-27a 为一 3 棵有序树组成的有序森林，b、c 为表示 a 的 2 元位置树。

二元位置树被大量用于数据的表示，例如表示算术表达式及各种字符串。这时，常常需要遍访每一个结点，以下是三种遍访二元树的算法。

（1）先根算法（前序遍历法）。

1）访问二元树树根 r。

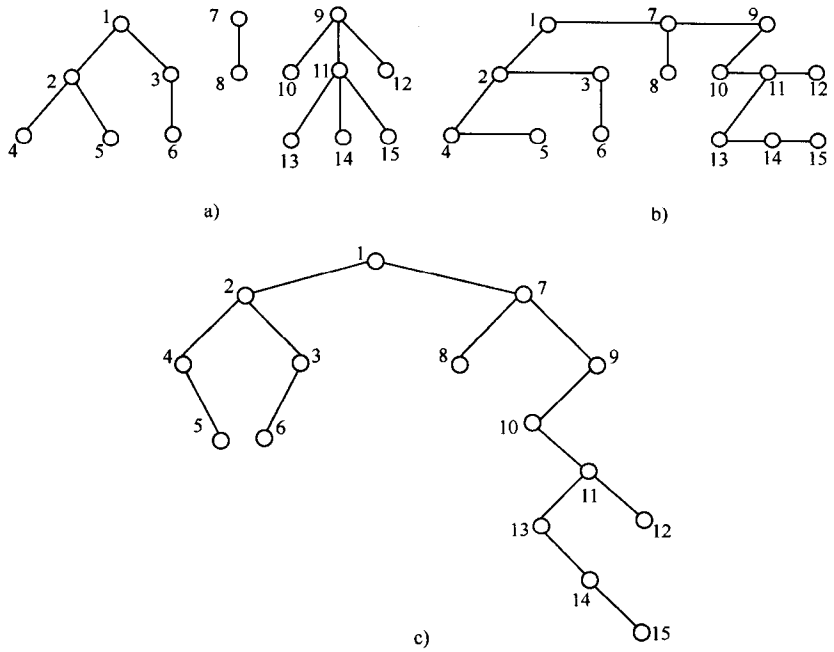


图 9-27

2）如果 r 有左儿子，那么又以先根算法遍访 r 的左子树（以 r 的左儿子为根的子树）。

3）如果 r 有右儿子，那么又以先根算法遍访 r 的右子树（以 r 的右儿子为根的子树）。

（2）中根算法（中序遍历法）。

1）如果二元树树根 r 有左儿子，那么又以中根算法遍访 r 的左子树。

2）访问二元树树根 r。

3）如果二元树树根 r 有右儿子，那么又以中根算法遍访 r 的右子树。

（3）后根算法（后序遍历法）。

1）如果二元树树根 r 有左儿子，那么又以后根算法遍访 r 的左子树。

2）如果二元树树根 r 有右儿子，那么又以后根算法遍访 r 的右子树。

3）访问二元树树根 r。

【例 9-20】 算术表达式 $\dfrac{a*(b+c)-d\uparrow 2}{a*(b-c)}$ 可以用图 9-28 中的 2 元树来表示。其中*表示数乘运算，↑表示指数运算，$d\uparrow 2=d^2$。分别用三种算法遍访这一 2 元树，可以得到三种符号串：

由先根算法得

$$/-*a+bc\uparrow d2*a-bc \tag{9-1}$$

由中根算法得

$$a*b+c-d\uparrow 2/a*b-c \tag{9-2}$$

由后根算法得

$$abc+*d2\uparrow -abc-*/ \tag{9-3}$$

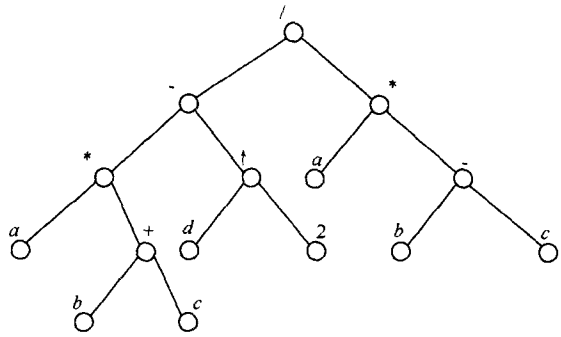


图 9-28

式（9-1）称为算术表达式的**前置表达式**（运算符都放置在运算数据之前），或称其为算术表达式的**波兰表示**。它的运算方式如式（9-4）所示，与原中置表达式的运算过程一致。由于波兰表示完全不依赖括号，所表示的运算又没有二义性，其优越性是显而易见的。

$$/-*a+bc\uparrow d2*a-bc \tag{9-4}$$

式（9-2）称为算术表达式的**中置表达式**（二元运算符都放置在运算数据之间）。由于遍访所得的表达式没有括号，而二元运算符又在运算数据之间，它所表示的运算过程的二义性就在所难免了。因此用中根算法遍访表示算术表达式的 2 元树是不适当的。

式（9-3）称为算术表达式的**后置表达式**（运算符都放置在运算数据之后），或称其为算术表达式的**逆波兰表示**。它的运算方式如式（9-5）所示，与波兰表示一样，逆波兰表示与原中置表达式的运算意义相一致。逆波兰表示也完全不依赖括号，所表示的运算也没有二义性。

$$abc+*d2\uparrow -abc-*/ \tag{9-5}$$

最后我们用两个应用根树解决实际问题的例子来结束本章的叙述。

【例 9-21】 有 10 个文件，分别用 10 个不同的正整数（2，4，5，7，8，10，12，13，15，16）作标记（称为它们的键值）。为了检索方便，可以把它们以根树的结构储存起来，使得每一个顶点上储存的文件的键值大于它的左子树上所有文件的键值，而小于它的右子树上所有文件的键值，如图 9-29 所示。

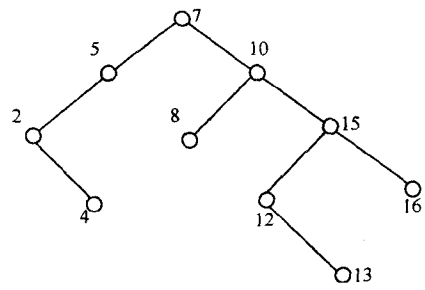


图 9-29

这时如果要检索一个文件，只要将其键值与树根的键值做比较，当它比树根的键值小时，便对左子树重复上述步骤；当它比树根的键值大时，便对右子树重复上述步骤。例如键值为 8 的文件，做两次比较便可找到。

【例 9-22】 有 8 枚硬币，其中恰有 1 枚是假币，假币比真币重。试用一架天平称出假币，使称量的次数尽可能地少。

图 9-30 描述了称量的策略，只要称两次便可测出假币。图中八个数字表示八个硬币，

结点处标记的两个集合，为一次称量中两盘所放的硬币，假币一定在一次称量中较低的盘中。

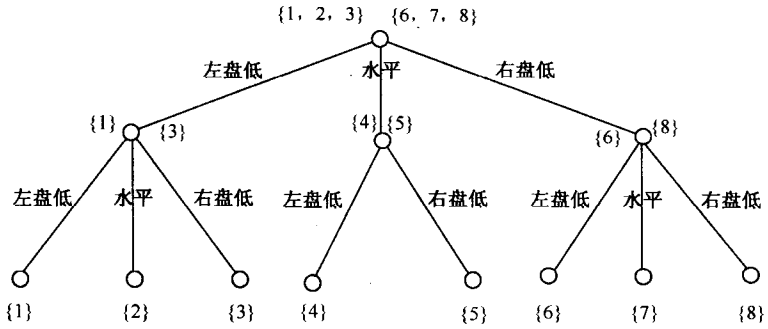


图 9-30

9.4 练习

1. 判别下列各图（图 9-31）是否为二分图，是否为完全二分图。

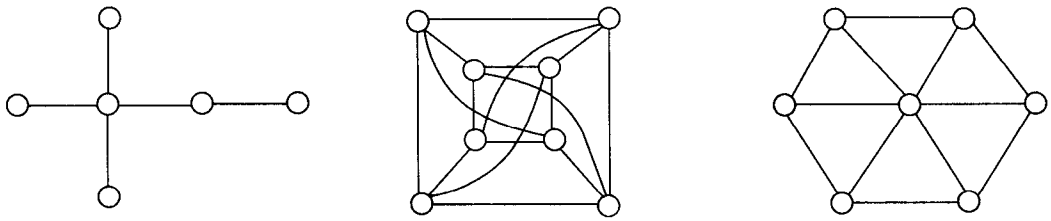


图 9-31

2. 六名间谍 a，b，c，d，e，f 被我捕获，他们分别懂得的语言是{汉语，法语，日语}，{德语，日语，俄语}，{英语，法语}，{汉语，西班牙语}，{英语，德语}，{俄语，西班牙语}，问至少用几个房间监禁他们，才能使同一房间的人不能互相直接对话。

3. 设（n, m）图 G 为二分图，证明 $m \leqslant \frac{n^2}{4}$。

4. 作一个二分图 $G=<X, E, Y>$，使它恰有 4！个 X-完全匹配 。

5. 用匈牙利算法求图 9-32 中二分图的最大匹配。

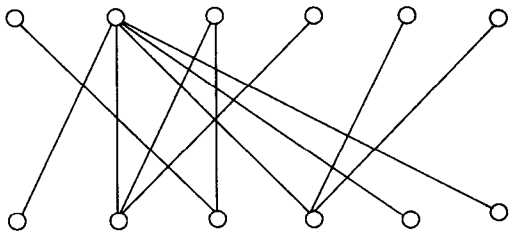


图 9-32

6. 某单位有 7 个岗位空缺，它们是 p_1，p_2,…,p_7 。应聘的 10 人 m_1，m_2,…,m_{10} 所适合的岗位分别是{p_1，p_5，p_6}，{p_2，p_6，p_7}，{p_3，p_4}，{p_1，p_5}，{p_6，p_7}，{p_3}，{p_2，p_3}，{p_1，p_3}，{p_1}，{p_5}。如何聘用可使落聘者最少。

7. 给出图 9-33 中各面的度，并作一与此图同构的图，使标记 2 的面在该图的图示中为一无界面。

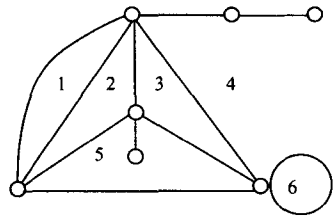


图 9-33

8. 证明定理 9-7，不直接引用定理 9-6。

9. 证明：有 n ($n\geqslant 3$)个顶点，r 个面的平面连通简单图满足

$$r \leqslant 2n-4$$

10. 证明：少于 30 条边的平面连通简单图至少有一个顶点的度不大于 4。

11. 证明：在有 6 个顶点和 12 条边的连通平面简单图中，每个面的度均为 3。

12. 设 G 为简单无向图，其顶点数 $n\geqslant 11$，证明 G 或 G 的补 $\overline{G}$ 是非平面图。

13. 证明图 9-34 中的图都是非平面图。

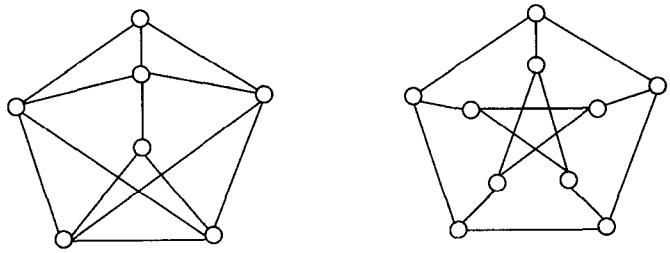


图 9-34

14. 作出图 9-33 的对偶图，再作出你在第一题中所作的平面图的对偶图，并比较这两个对偶图。

15. 如果一自对偶图有 n 个顶点、m 条边，证明：

$$m=2(n-1)$$

16. 平面图 G 称为是完全正则的，如果 G 的顶点的度都相等，并且 G 的面的度也相等。试作出一个完全正则图。

17. 证明：定理 9-9 的结论可加强为“至少有 3 个顶点的度数不大于 5”。

18. 给出一个平面图，使它是可 4-着色的，但不是可 3-着色的。

19. 证明：若图 G 的最大顶点度数是 d，那么 G 是可$(d+1)$-着色的。

20. 证明定理 9-12、定理 9-13。

21. 证明定理 9-16 之（3）$\Rightarrow$（4），（4）$\Rightarrow$（5）。

22.（1）试画出所有具有五个顶点的、不同构的树。

（2）描述恰有两片叶的树的特征，并证明你的描述是正确的。

23. 一棵树有两个 2 度顶点，一个 3 度顶点，三个 4 度顶点，问：它有几个 1 度的顶点。

24. 一棵树有 n_2 个 2 度顶点，有 n_3 个 3 度顶点，…，有 n_k 个 k 度顶点，问：它有几个 1 度的顶点。

25. 给出图 9-35 的最小生成树，并写出关于这一生成树的枝割集系和弦回路系。

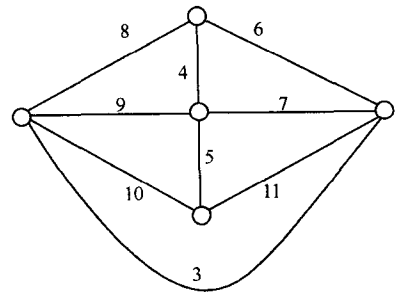


图 9-35

26. 判断下列断言的真假：

（1）连通无向图 G 的任何边，都是 G 的某一棵生成树的枝。

（2）连通无向图 G 的任何边，都是 G 的某一棵生成树的弦。

27. 设 G 为连通无向图，证明：

（1）G 的任一生成树 T 的关于 G 的补 $G-T$ 中不含有 G 的割集。

（2）G 的任一割集 S 的关于 G 的补 $G-S$（从 G 中删除所有 S 中的边）中不含有 G 的生成树。

28. 设 C 是连通无向图 G 的一条回路，a，b 是 C 中任意两条边。证明：存在 G 的割集 S，使得 S 与 C 仅以 a，b 为公共边。

29. T 是连通无向图 G 的生成树的充分必要条件是：T 是 G 的生成子图，且 T 有 $n-1$ 条边，这里 n 是 G 的顶点数。

30. 给出一个简明而又充分的条件，使得满足这一条件的平面连通边赋权图的最小生成树是惟一的。

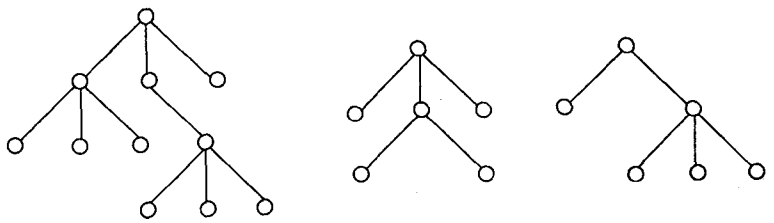
31.（1）用二元位置树表示命题公式

$$(A\rightarrow B)\wedge(\neg(C\vee B)\leftrightarrow\neg B)$$

注意，请将一元运算符的运算对象取做运算符结点的右儿子。

（2）用 3 种遍访算法遍访你作出的二元位置树，写出相应的线性表达式，并像式（9-4）、式（9-5）那样，用横线标出其波兰表示和逆波兰表示的运算进程。

32. 将图 9-36a 中的有序树及 b 中的有序森林，表示为 2 元位置树。



a) b)

图 9-36

33. 有 8 枚硬币，其中可能有 1 枚是假币（但假币不多于 1 枚），假币与真币重量不等。试用一架天平来称量，3 次称出假币或断言假币不存在，请用根树表示你的称量策略。

第10章 关 系

在日常生活和科学技术领域中，我们会经常碰到各种各样的具体“关系”。如：人与人之间有父子、兄弟、师生关系；两数之间有大于、等于、小于关系；电学中有电压、电阻与电流间的关系；元素与集合之间的属于关系；计算机科学中程序间的调用关系，程序执行过程中状态之间的转换关系，程序执行前变量取值状况和执行后变量取值状况的关系，文件与路径的关系……。宇宙万物之间存在着形形色色的联系，这种联系正是各门学科所关注的问题。关系概念应是对事物间多值依赖的一种描述，大家熟知的函数是关系的特例。有许多表述关系的数学模型，读者在高等代数中学习过的矩阵，我们在第 8、9 两章中介绍的图都是很好的例子。本章要讨论的是集合理论为刻画这种联系提供的最一般的数学模型——关系，它也是计算机科学中数据描述和信息处理的最常用的数学模型。集合理论中的关系本身也是一个集合，以具有那种联系的对象组合——“序组”（回忆定义 1-10）为其成员。换言之，在离散结构的表示中，关系不是通过描述其内涵来刻画事物间联系的，而是通过列举其外延(具有那种联系的对象组合全体)来描述这种联系。这使关系的研究可以方便地使用集合论的概念、运算及研究方法和研究成果。当然，这也使本章的学习依赖于对第 1 章知识的掌握。

需要指出，离散数学中的关系理论通常归入集合论的范畴，并不以个别的关系为主要对象，而是关注关系的一般特性、关系的分类等。

10.1 二元关系

10.1.1 关系的基本概念

下文由两个例子出发来导出关系的基本概念。回忆第 1 章介绍的集合笛卡儿积的概念。

【例 10-1】 设 $A=\{a, b, c, d, e, f\}$ 为学生的集合，$B=\{\alpha, \beta, \gamma, \delta\}$ 为可选修课程的集合，$C=\{2, 3, 4, 5\}$ 为学习成绩的集合。学生与课程之间存在着一种联系，不妨称之为“选修关系”；学生、课程和成绩之间也存在着一种联系，或许可叫做学生课程成绩关系。一种容易想到的方法是用具有这种联系的对象的有序元组的集合来表示这些关系。设学生 a 选修课程α，δ；学生 b 选修课程α, β；学生 c 和 f 选修课程 γ，学生 e 选修课程α，而学生 d 未选修任何课程。用 R 表示这种选修关系，那么 R 可表示为

$$R=\{<a,\alpha>, <a,\delta>, <b,\alpha>, <b,\beta>, <c,\gamma>, <e,\alpha>, <f,\gamma>\}$$

同样设学生 a 两门选修课α, δ成绩分别为 5 分和 4 分；学生 b 两门课α，β成绩均为 4 分，学生 c 选修课 γ成绩为 5 分，学生 f 选修课 γ成绩为 2 分。我们用 S 表示学生课程成绩关系，则 S 可表示为

$$S=\{<a,\alpha,5>, <a,\delta,4>, <b,\alpha,4>, <b,\beta,4>, <c,\gamma,5>, <e,\alpha,3>, <f,\gamma,2>\}$$

从上述例子可以看出，几个集合之间的关系，本质上取决于取自它们的元素所构成的有序元组的集合，因此我们如下定义关系：

定义 10-1 R 称为集合 A_1，A_2，…，A_{n-1} 到 A_n 的 n 元关系（n-ary relations），如果 R 是 $A_1\times A_2\times\cdots\times A_n$ 的一个子集。当 $A_1=A_2=\cdots=A_{n-1}=A_n$ 时，也称 R 为 A 上的 n 元关系。当 $n=2$ 时，称 R 为 A_1 到 A_2 的**二元关系**。A_1，A_2，…，A_{n-1} 到 A_n 的 n 元关系也可视为 $A_1\times A_2\times\cdots\times A_{n-1}$ 到 A_n 的二元关系。

今后，我们将主要研究二元关系。

由于关系是集合（只是以序组或序偶为元素），因此，所有集合的规定方式均适用于关系的确定。

【例 10-2】 自然数集上的相等关系 E_N，整除关系 D，小于关系 L 可分别用三种方法规定如下：

（1）$E_N=\{<0,0>,<1,1>,<2,2>,<3,3>,\cdots\}$（列举法）

（2）$D=\{<x,y>|x$ 整除 $y\}$（描述法）

（3）小于关系 L 归纳定义如下：（归纳法）

1）基础条款 $<0,1>\in L$

2）归纳条款若 $<x,y>\in L$，则

$$<x,y+1>\in L,<x+1,y+1>\in L$$

3）终极条款（略）

几个特殊的二元关系今后要常常提到：

$\varnothing\subseteq A\times B$，称$\varnothing$为 A 到 B 的**空关系**。

$A\times B\subseteq A\times B$，称 $A\times B$ 为 A 到 B 的**全关系**。

$E_A=\{<x,x>|x\in A\}$，称为 A 上**相等关系**（有的教科书称之为**恒等关系**，记作 I_A）。

$\varnothing$ 和 $A\times B$ 被称为关系似乎有点奇怪，其实不然。在实际应用中空关系和全关系是确实存在的。例如，正整数集合上“两数之和小于零”的关系（$R1=\{<x,y>|x+y<0\}$）是正整数集合上的空关系，而“两数之和大于零”的关系（$R2=\{<x,y>|x+y>0\}$）是正整数集合上的全关系。

定义 10-2 设 R 为 A 到 B 的二元关系。

（1）用 xRy 表示 $<x,y>\in R$，意为 x，y 有 R 关系（为可读性好，我们将在不同场合使用这两种表达方式中的某一种）。$\neg\, xRy$ 表示 $<x,y>\notin R$。

（2）称 Dom（R）为关系 R 的**定义域**（domain），

$$\text{Dom}(R)=\{x|x\in A\wedge\exists y(<x,y>\in R)\}$$

（3）称 Ran（R）为关系 R 的**值域**（range），

$$\text{Ran}(R)=\{y|y\in B\wedge\exists x(<x,y>\in R)\}$$

（4）称 A 为 R 的**前域**，B 为 R 的**陪域**。

【例 10-3】 设 $A=\{a,b,c,d,e,f\}$，$B=\{\alpha,\beta,\gamma,\delta\}$，

$$R=\{<b,\alpha>,<b,\beta>,<c,\beta>,<d,\gamma>,<f,\gamma>\}$$

那么如图 10-1 所示：

$$\text{Dom}(R)=\{b,c,d,f\},\ \text{Ran}(R)=\{\alpha,\beta,\gamma\}$$

图中各箭头分别表示 $bR\alpha$，$bR\beta$，$cR\beta$，$dR\gamma$，$fR\gamma$。

像图 10-1 这样的关系表示形式，称为**关系图**（graph of relation）。前域和陪域相同时，关系图可用一个更为简明的形式——有向图（回忆第 8 章）来表示。例如，图 10-2a～d 中的有向图分别表示 $A=\{1,2,3,4,5\}$ 上的空关系、相等关系、全关系和小于关系。

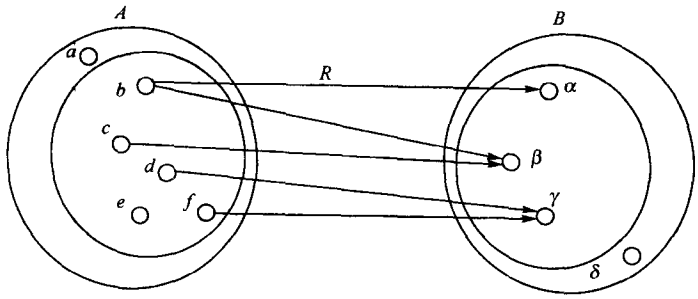


图 10-1

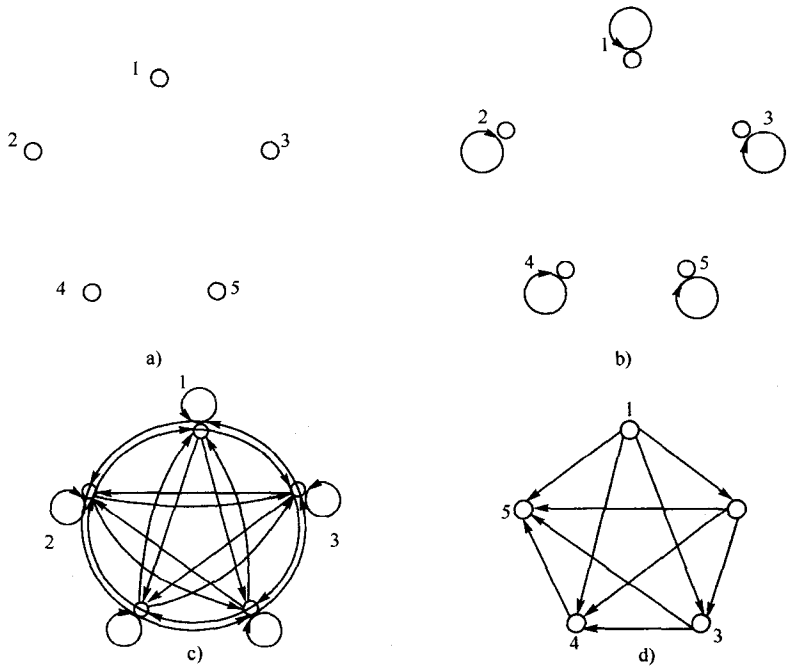


图 10-2

关系图直观清晰形象，是分析关系性质的方便形式，但是对它不便于进行运算。我们知道关系图是一个有向图，有向图又有一种便于运算的、直观鲜明的表示形式——矩阵，因此矩阵也被用于表示二元关系，称为**关系矩阵**（matrix of relation）。设 $R \subseteq A \times B$，$A=\{a_1, \cdots, a_m\}$，$B=\{b_1, \cdots, b_n\}$，那么 R 的关系矩阵 M_R 为一 $m \times n$ 矩阵，它的第 i，j 分量 c_{ij} 只取值 0 或 1，而

$c_{ij}=1$ 当且仅当 $a_i R b_j$；$c_{ij}=0$ 当且仅当 $\neg\, a_i R\, b_j$

例如图 10-1 所示关系 R 的关系矩阵为

$$M_R=\begin{bmatrix} 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

图 10-2 所示关系的关系矩阵分别是

$$M_{\phi}=\begin{bmatrix}0&0&0&0&0\\0&0&0&0&0\\0&0&0&0&0\\0&0&0&0&0\\0&0&0&0&0\end{bmatrix} \qquad M_{E_A}=\begin{bmatrix}1&0&0&0&0\\0&1&0&0&0\\0&0&1&0&0\\0&0&0&1&0\\0&0&0&0&1\end{bmatrix}$$

$$M_{A\times A}=\begin{bmatrix}1&1&1&1&1\\1&1&1&1&1\\1&1&1&1&1\\1&1&1&1&1\\1&1&1&1&1\end{bmatrix} \qquad M_{L_A}=\begin{bmatrix}0&1&1&1&1\\0&0&1&1&1\\0&0&0&1&1\\0&0&0&0&1\\0&0&0&0&0\end{bmatrix}$$

应当指出，关系图、关系矩阵的表示形式局限于关系的前域和陪域为有限集，而关系图主要用于前域和陪域相同的关系。

10.1.2 关系的基本运算

在讨论关系的基本运算之前，我们先给出关系相等的概念。

定义 10-3 称关系 R 和 S 相等，如果 R 与 S 有相同的前域和陪域，并且

$$\forall x\forall y\,(xRy\leftrightarrow xSy)$$

关系相等的条件中，前域和陪域相同的要求不是本质的，因为总可对其中一关系之前域或陪域作适当的扩充，而使两者具有相同的前域和陪域。这种域的改变不会改变 R 与 S 具有相同的序偶这一根本。因此，两个关系是否相等，本质上取决于两个关系作为序偶集合是否相等。

作为集合对关系作并、交、差、补运算是理所当然的，但为了运算结果作为关系的意义更明确，我们也要求运算对象应有相同的前域和陪域，从而运算结果是同一前域、陪域间的关系。同前所述，这一要求也只是技术上的。因此，在讨论关系运算时，我们有时忽略它们的前域和陪域。

设 R 和 S 为 A 到 B 的二元关系，其并、交、差、补运算定义如下：

$$R\cup S=\{<x,y>\mid xRy\vee xSy\}$$
$$R\cap S=\{<x,y>\mid xRy\wedge xSy\}$$
$$R-S=\{<x,y>\mid xRy\wedge\neg\, xSy\}$$
$$\bar{R}=A\times B-R=\{<x,y>\mid \neg\, xRy\}$$

当然，集合的并、交、差、补运算诸性质对关系的相应运算也成立。需要注意的是，作为关系时，补运算是对全关系而言的。

有限二元关系的并、交、差、补的矩阵可如下求取：

$M_{R\cup S}=M_R\vee M_S$（矩阵对应分量作逻辑析取运算）

$M_{R\cap S}=M_R\wedge M_S$（矩阵对应分量作逻辑合取运算）

$M_{R-S}=M_{R\cap\bar{S}}=M_R\wedge M_{\bar{S}}$

$M_{\bar{S}} = (M_S)^-$（矩阵各分量作逻辑非运算）

除了这些运算外，关系还有自己独特的运算，它们对于关系更为有意义。

定理 10-1 设 R 是 A 到 B 的关系，R 的**逆关系**或**逆**（converse）是 B 到 A 的关系，记为 $R^{\sim}$，规定为

$$R^{\sim} = \{<y,x> \mid xRy\}$$

这里“~”称为关系的**逆运算**。

很显然，对任意 $x \in A, y \in B$，

$$xRy \Leftrightarrow yR^{\sim}x$$

把 R 的关系图的所有有向边反转即可得到逆关系 $R^{\sim}$的关系图。

若 M_R 为 R 的关系矩阵，那么

$$M_{R^{\sim}} = M_R'$$（M'表示矩阵 M 的转置矩阵）

【例 10-4】 $E_A^{\sim} = E_A, \varnothing^{\sim} = \varnothing, (A \times B)^{\sim} = B \times A$；实数上的≤关系的逆是≥关系。

逆关系的下列性质是明显的。

定理 10-2 设 R 和 S 都是 A 到 B 的二元关系，*为 $\cap, \cup$ ，- 运算，那么

（1）$R^{\sim\sim} = R$

（2）$R^{-\sim} = R^{\sim-}$

（3）$(R*S)^{\sim} = R^{\sim}*S^{\sim}$

（4）$R \subseteq S$ 当且仅当 $R^{\sim} \subseteq S^{\sim}$

证明 （2）对任意 $x \in A, y \in B$

$$\begin{aligned} xR^{-\sim}y &\Leftrightarrow yR^{-}x \\ &\Leftrightarrow \neg(yRx) \\ &\Leftrightarrow \neg(xR^{\sim}y) \\ &\Leftrightarrow xR^{\sim-}y \end{aligned}$$

因此 $R^{-\sim} = R^{\sim-}$。

（3）我们仅证 $(R-S)^{\sim} = R^{\sim} - S^{\sim}$

对任意 $x \in A, y \in B$

$$\begin{aligned} <x,y> \in (R-S)^{\sim} &\Leftrightarrow <y,x> \in R-S \\ &\Leftrightarrow <y,x> \in R \wedge <y,x> \notin S \\ &\Leftrightarrow <x,y> \in R^{\sim} \wedge <x,y> \notin S^{\sim} \\ &\Leftrightarrow <x,y> \in R^{\sim} - S^{\sim} \end{aligned}$$

因此，$(R-S)^{\sim} = R^{\sim} - S^{\sim}$。

本例用已知等式进行证明更为简明：

$(R-S)^{\sim} = (R \cap S^{-})^{\sim} = R^{\sim} \cap S^{-\sim} = R^{\sim} \cap S^{\sim-} = R^{\sim} - S^{\sim}$。

其余证明留给读者，方法自便。

下面将要介绍的合成运算是最为重要的关系运算。

定义 10-4 设 R 为 A 到 B 的二元关系，S 为 B 到 C 的二元关系，那么 $R \circ S$ 为 A 到 C 的二元关系，称为关系 R 与 S 的**合成**（compositions）**关系**或**复合关系**，定义为

$$R \circ S = \{<x,z> \mid x \in A \wedge z \in C \wedge \exists y(y \in B \wedge xRy \wedge yRz)\}$$

或简单地

$$R°S=\{<x,z>\mid \exists y(xRy\wedge yRz)\}$$

这里°称为关系的**合成运算**或**复合运算**。

【例 10-5】

（1）兄弟关系和父子关系的合成是叔侄关系。设《红楼梦》中人物的兄弟关系为 R，父子关系为 S，那么

$R=\{<$贾宝玉，贾环$>$，$<$贾政，贾赦$>$，…$\}$

$S=\{<$贾政，贾宝玉$>$，$<$贾政，贾环$>$，$<$贾赦，贾琏$>$，…$\}$

从而$<$贾政，贾琏$>\in R°S$，贾政与贾琏有叔侄关系。

（2）设 $A=\{1,2,3,4,5\}$，$B=\{2,4,6\}$，$C=\{1,3,5\}$，$R\subseteq A\times B$，$S\subseteq B\times C$ 且

$R=\{<1,2>,<2,4>,<3,4>,<5,6>\}$

$S=\{<2,1>,<2,5>,<6,3>\}$

那么

$R°S=\{<1,1>,<1,5>,<5,3>\}\subseteq A\times C$

（3）设集合 $A=\{0,1,2,3,4\}$，R，S 均为 A 上二元关系，且

$R=\{<x,y>\mid x+y=4\}=\{<0,4>,<4,0>,<1,3>,<3,1>,<2,2>\}$

$S=\{<x,y>\mid y-x=1\}=\{<0,1>,<1,2>,<2,3>,<3,4>\}$

那么

$R°S=\{<4,1>,<1,4>,<3,2>,<2,3>\}=\{<x,z>\mid x+z=5\}$

$S°R=\{<0,3>,<1,2>,<2,1>,<3,0>\}=\{<x,z>\mid x+z=3\}$

$R°R=\{<0,0>,<4,4>,<1,1>,<3,3>,<2,2>\}=\{<x,z>\mid x-z=0\}$

$S°S=\{<0,2>,<1,3>,<2,4>\}=\{<x,z>\mid z-x=2\}$

$(R°S)°R=\{<4,3>,<1,0>,<3,2>,<2,1>\}=\{<x,z>\mid x-z=1\}$

$R°(S°R)=\{<4,3>,<3,2>,<2,1>,<1,0>\}=\{<x,z>\mid x-z=1\}$

从上例已可看出，一般地 $R°S\neq S°R$，即关系的合成运算不满足交换律。关系合成运算的下列性质是明显成立的。

定理 10-3 设 E_A，E_B 为集合 A，B 上的相等关系，$R\subseteq A\times B$，那么

（1）$E_A°R=R°E_B=R$

（2）$\varnothing°R=R°\varnothing=\varnothing$

证明 （1）为证 $E_A°R\subseteq R$，设$<x,y>\in E_A°R$，那么有 $u\in A$，使$<x,u>\in E_A$，$<u,y>\in R$。由$<x,u>\in E_A$ 知 $x=u$，因此$<x,y>\in R$。$E_A°R\subseteq R$ 得证。反之，设$<x,y>\in R$。由于$<x,x>\in E_A$，故$<x,y>\in E_A°R$，$R\subseteq E_A°R$ 得证。因此 $E_A°R=R$ 证毕 。同理可证 $R=R°E_B$。

（2）的证明留给读者。

关系合成运算进一步的性质由以下定理给出。

定理 10-4 设 R，S，T 均为 A 上二元关系，那么

（1）$R°(S\cup T)=(R°S)\cup(R°T)$

（2）$(S\cup T)°R=(S°R)\cup(T°R)$

（3）$R°(S\cap T)\subseteq(R°S)\cap(R°T)$

（4）$(S\cap T)°R\subseteq(S°R)\cap(T°R)$

（5）$R°(S°T)=(R°S)°T$

（6）$(R\circ S)^{\sim}=S^{\sim}\circ R^{\sim}$

证明 我们仅证明（1），（4），（5）另外三式的证明留给读者自行完成。

（1）对任意 $x,y\in A$，有

$$\begin{aligned}<x,y>\in R\circ(S\cup T) &\Leftrightarrow \exists u(<x,u>\in R\wedge<u,y>\in S\cup T)\\ &\Leftrightarrow \exists u(<x,u>\in R\wedge(<u,y>\in S\vee<u,y>\in T))\\ &\Leftrightarrow \exists u((<x,u>\in R\wedge<u,y>\in S)\vee(<x,u>\in R\wedge<u,y>\in T))\\ &\Leftrightarrow \exists u(<x,u>\in R\wedge<u,y>\in S)\vee\exists u(<x,u>\in R\wedge<u,y>\in T)\\ &\Leftrightarrow <x,y>\in R\circ S\vee<x,y>\in R\circ T\\ &\Leftrightarrow <x,y>\in R\circ S\cup R\circ T\end{aligned}$$

故（1）式真。

（4）对任意 $x,y\in A$，有

$$\begin{aligned}<x,y>\in(S\cap T)\circ R &\Leftrightarrow \exists u(<x,u>\in(S\cap T)\wedge<u,y>\in R)\\ &\Leftrightarrow \exists u(<x,u>\in S\wedge<x,u>\in T\wedge<u,y>\in R)\\ &\Leftrightarrow \exists u(<x,u>\in S\wedge<u,y>\in R\wedge<x,u>\in T\wedge<u,y>\in R)\\ &\Rightarrow \exists u(<x,u>\in S\wedge<u,y>\in R)\wedge\exists u(<x,u>\in T\wedge<u,y>\in R)\\ &\Leftrightarrow <x,y>\in(S\circ R)\wedge<x,y>\in(T\circ R)\\ &\Leftrightarrow <x,y>\in(S\circ R)\cap(T\circ R)\end{aligned}$$

故$(S\cap T)\circ R\subseteq(S\circ R)\cap(T\circ R)$。

（5）对任意 $x,y\in A$，有

$$\begin{aligned}<x,y>\in R\circ(S\circ T) &\Leftrightarrow \exists u(<x,u>\in R\wedge<u,y>\in S\circ T)\\ &\Leftrightarrow \exists u(<x,u>\in R\wedge\exists v(<u,v>\in S\wedge<v,y>\in T))\\ &\Leftrightarrow \exists v\exists u(<x,u>\in R\wedge<u,v>\in S\wedge<v,y>\in T)\\ &\Leftrightarrow \exists v(\exists u(<x,u>\in R\wedge<u,v>\in S)\wedge<v,y>\in T)\\ &\Leftrightarrow \exists v(<x,v>\in R\circ S\wedge<v,y>\in T)\\ &\Leftrightarrow <x,y>\in(R\circ S)\circ T\end{aligned}$$

故（5）式真。

注意，（3）、（4）两式中的$\subseteq$不能改为$=$，例如在(3)式中令 $R=\{<a,b>,<a,c>\}$，$S=\{<b,d>\}$，$T=\{<c,d>\}$ 时，$R\circ(S\cap T)=R\circ\varnothing=\varnothing$，而$(R\circ S)\cap(R\circ T)=\{<a,d>\}$。

（1）、（2）分别说明合成运算$\circ$对并运算$\cup$满足左、右分配律；而（3）、（4）说明合成运算$\circ$对交运算$\cap$左、右分配律都不满足；（5）说明合成运算$\circ$满足结合律。

由于关系合成运算有结合律，因此用“幂”表示集合上关系对自身的合成是适当的。我们规定 $R^0=E_A$（R 为 A 上二元关系），$R^n=\underbrace{R\circ\cdots\circ R}_{n}=R^{n-1}\circ R$。$R^n$ 满足下列性质：

定理 10-5 设 R 为 A 上二元关系，m，n 为自然数，那么

（1）$R^m\circ R^n=R^{m+n}$

（2）$(R^m)^n=R^{mn}$

可把 m 看作参数，对 n 进行归纳证明，不赘述。

定理 10-6 设集合 A 的基数为 n，R 是 A 上二元关系，那么存在自然数 i,j 使得 $R^i=R^j$，其中 $0\leqslant i<j\leqslant 2^{n^2}$。

证明 我们知道，当$|A|=n$时，A上不同二元关系共计2^{n^2}个（见本章练习第1题），令$K=2^{n^2}$，因此，在

$$R^0,\ R^1,\ R^2,\ \cdots,\ R^K$$

这$K+1$个关系中，至少有两个是相同的（鸽笼原理），即有$i,\ j,\ 0\leqslant i<j\leqslant 2^{n^2}$，使$R^i=R^j$。

关系合成运算比较复杂，借助关系图和关系矩阵来理解和计算是有益的。

【例10-6】

（1）$A=\{a_1,\ a_2,\ a_3,\ a_4,\ a_5\}$，$B=\{b_1,\ b_2,\ b_3,\ b_4,\ b_5\}$，$C=\{c_1,c_2,c_3,c_4\}$，$R\subseteq A\times B$，$S\subseteq B\times C$；且

$R=\{<a_2,\ b_1>,\ <a_2,b_2>,<a_3,\ b_3>,\ <a_4,\ b_3>,\ <a_5,\ b_4>\}$

$S=\{<b_3,\ c_2>,\ <b_4,\ c_1>,\ <b_4,\ c_4>\}$

$R\circ S=\{<a_3,c_2>,<a_4,c_2>,<a_5,c_1>,<a_5,c_4>\}$

它的关系图如图10-3a所示。

（2）$A=\{a,\ b,\ c,\ d,e\}$，R为A上二元关系，

$R=\{<a,\ c>,\ <a,\ e>,\ <b,\ a>,\ <c,\ b>,\ <c,\ d>\}$

$R^2=\{<a,\ b>,\ <b,\ c>,\ <b,\ e>,\ <a,\ d>,\ <c,\ a>\}$

R及R^2的关系图如图10-3b所示。

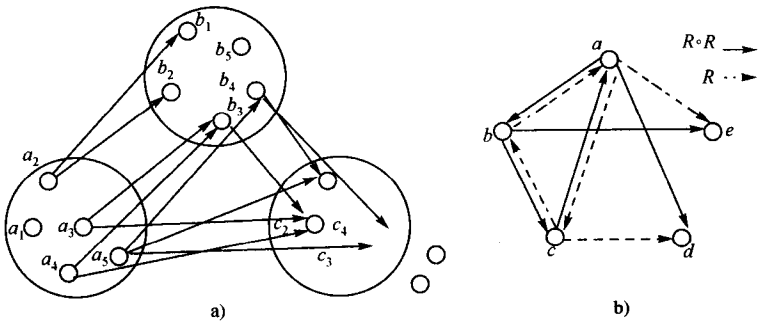


图 10-3

关于关系矩阵我们有下列结果。

定理10-7 设$A=\{a_1,\cdots,a_m\}$，$B=\{b_1,\cdots,b_n\}$，$C=\{c_1,\cdots,c_p\}$，$R\subseteq A\times B$，$S\subseteq B\times C$，$M_R=[r_{ij}]_{m\times n}$为R的关系矩阵，$M_S=[s_{ij}]_{n\times p}$为S的关系矩阵。那么，合成关系$R\circ S$的关系矩阵$M_{R\circ S}=[t_{ij}]$为一$m\times p$矩阵，其各分量t_{ij}可如下求取

$$t_{ij}=\bigvee_{k=1}^{n} r_{ik}s_{kj}\quad (i=1,\cdots,m;\ j=1,\cdots,p)$$

这里$\bigvee_{k=1}^{n} f(k)=f(1)\vee\cdots\vee f(n)$，$\vee$为逻辑析取运算。

证明 对$i=1,2,\ \cdots,m;\ j=1,2,\ \cdots,P$，

$$\begin{aligned} t_{ij}=1 &\Leftrightarrow \exists k\,(r_{ik}\cdot s_{kj}=1)\\ &\Leftrightarrow \exists k\,(r_{ik}=1\wedge s_{kj}=1)\\ &\Leftrightarrow \exists b_k\,(a_iRb_k\wedge b_kSc_j)\\ &\Leftrightarrow a_iR\circ Sc_j \end{aligned}$$

这表明$[t_{ij}]$的确为 $R\circ S$ 的关系矩阵$(m\times p)$。因此可定义

$$M_{R\circ S}=M_R \cdot M_S$$

其中 · 为特殊的矩阵乘，乘积各分量如上求得。

例 10-6 之（1）中 $R\circ S$ 的关系矩阵为

$$M_{RS}=\begin{bmatrix}0&0&0&0&0\\1&1&0&0&0\\0&0&1&0&0\\0&0&1&0&0\\0&0&0&1&0\end{bmatrix}\cdot\begin{bmatrix}0&0&0&0\\0&0&0&0\\0&1&0&0\\1&0&0&1\\0&0&0&0\end{bmatrix}=\begin{bmatrix}0&0&0&0\\0&0&0&0\\0&1&0&0\\0&1&0&0\\1&0&0&1\end{bmatrix}$$

· 乘与普通矩阵乘的不同在于，各分量计算中用 $\bigvee_{k=1}^{n}$ 代替 $\sum_{k=1}^{n}$ $(\bigvee_{k=1}^{n} f(k)=f(1)\vee\cdots\vee f(n))$。

10.1.3 关系的基本特性

本小节总假定关系是某一集合上的二元关系，因为任一 A 到 B 的关系 R 总可看作 $A\cup B$ 上的关系，它与 R 具有完全相同的序偶，用对它的讨论代替对 R 的讨论无损于问题的本质。

定义 10-5 设 R 是 A 上的二元关系。

称 R 是**自反的**（reflexive），如果对任意 $x\in A$，均有 xRx。即

R 自反 当且仅当 $\forall x\,(x\in A\rightarrow xRx)$

称 R 是**反自反的**（irreflexive），如果对任意 $x\in A$，xRx 均不成立。即

R 反自反 当且仅当 $\forall x\,(x\in A\rightarrow\neg\, xRx)$

称 R 是**对称的**（Symmetic），如果对任意 $x, y\in A$，xRy 蕴涵 yRx。即

R 对称 当且仅当 $\forall x\forall y\,(x, y\in A\wedge xRy\rightarrow yRx)$

称 R 是**反对称的**（antisymmetric），如果对任意 $x,y\in A$，xRy 且 yRx 蕴涵 $x=y$。即

R 反对称 当且仅当$\forall x\forall y\,(x, y\in A\wedge xRy\wedge yRx\rightarrow x=y)$

称 R 是**传递的**（transitive），如果对任意 $x, y, z\in A$，xRy 且 yRz 蕴涵 xRz。即

R 传递 当且仅当 $\forall x\forall y\forall z(x, y, z\in A\wedge xRy\wedge yRz\rightarrow xRz)$

【例 10-7】 设 $A=\{1, 2, 3\}$ 以下各关系 R_i（$i=1, 2, \cdots, 8$）均为 A 上二元关系。

（1）$R_1=\{<1, 1>, <1, 3>, <2, 2>, <3, 3>\}$ 是自反的，而 $R_2=\{<1, 3>, <3, 1>\}$ 不是自反的，是反自反的。存在既不自反也不反自反的二元关系，例如 $R_3=\{<1, 1>\}$。显然 A 上的$\varnothing$关系是反自反的，不是自反的。可是值得注意的是，当 $A=\varnothing$时（这时 A 上只有一个关系$\varnothing$），A 上空关系既是自反的，又是反自反的，因为 $A=\varnothing$使两者定义的前提恒假。

（2）$R_4=\{<1, 3>, <3, 1>, <1, 2>, <1, 1>\}$ 不是对称的；$R_5=\{<1, 2>, <2, 1>\}$ 是对称的；$R_6=\{<1, 2>, <1, 3>\}$ 是反对称的。其实 R_4 既不是对称的，也不是反对称的。特别有意思的是，存在既对称又反对称的二元关系，例如 A 上的相等关系 E_A 或任一 $R\subseteq E_A$。

（3）$R_7=\{<1, 2>, <2, 3>, <1, 3>, <3, 3>\}$ 是传递的，但 $R_7-\{<1, 3>\}$ 便不是传递的了。应当注意，A 上的空关系$\varnothing$，$R_8=\{<1, 2>\}$ 等是传递的，因为传递性

定义的前提对它们而言均为假。

（4）任何非空集合上的空关系都是反自反、对称、反对称、传递的；其上的相等关系是自反、对称、反对称、传递的；其上的全关系是自反、对称、传递的。

（5）正整数集合上的整除关系是自反、反对称、传递的；但整数集合上的整除关系有传递性，无自反性和反对称性。

三角形的相似、全等关系是自反、对称、传递的。

关系的基本特性与关系图、关系矩阵有怎样的联系？见表 10-1。

表 10-1

关系特性	关系图特征	关系矩阵特性
自反	每一结点处有一环	对角线元素均为 1
反自反	每一结点处均无环	对角线元素均为 0
对称	两结点间有方向相反的两边同时出现	矩阵为对称矩阵
反对称	两结点间没有方向相反的边成对出现	当分量 $c_{ij}=1(i\neq j)$时 $c_{ji}=0$
传递	如果结点 v_1, v_2间有边 v_1v_2；v_2, v_3间有边 v_2v_3，则结点 v_1, v_3间必有边 v_1v_3	（无鲜明特征）

关系的五大基本特性还可以用下列五个特征性加以刻画。

定理 10-8 设 R 为 A 上二元关系。

（1）R 自反当且仅当 $E_A\subseteq R$ 。

（2）R 反自反当且仅当 $E_A\cap R=\varnothing$。

（3）R 对称当且仅当 $R=R^{\sim}$。

（4）R 反对称当且仅当 $R\cap R^{\sim}\subseteq E_A$ 。

（5）R 传递当且仅当 $R^2\subseteq R$。

证明 （1）、（2）是明显的。

（3）设 R 对称，那么对任意 $x, y\in A$，有

$$\begin{aligned}<x, y>\in R &\Leftrightarrow <y, x>\in R \text{（R 对称）}\\ &\Leftrightarrow <x, y>\in R^{\sim}\end{aligned}$$

故 $R=R^{\sim}$。反之，设 $R=R^{\sim}$，为证 R 对称，又设有 xRy。由于 $R=R^{\sim}$，故 $xR^{\sim}y$，进而 yRx。R 对称证毕。

（4）设 R 反对称，那么对任意 $x, y\in A$，有

$$\begin{aligned}<x, y>\in R\cap R^{\sim} &\Leftrightarrow <x, y>\in R\wedge <x, y>\in R^{\sim}\\ &\Leftrightarrow <x, y>\in R\wedge <y, x>\in R\\ &\Rightarrow x=y \text{（}R\text{ 反对称）}\\ &\Leftrightarrow <x, y>\in E_A\end{aligned}$$

因此 $R\cap R^{\sim}\subseteq E_A$。反之，设 $R\cap R^{\sim}\subseteq E_A$。为证 R 反对称又设 xRy, yRx 。那么 $xRy, xR^{\sim}y$ 从而 $<x, y>\in R\cap R^{\sim}$，故 $<x, y>\in E_A, x=y$ 。R 反对称得证。

（5）设 R 传递，那么对任意 $x, y\in A$，有

$$\begin{aligned}<x, y>\in R^2 &\Leftrightarrow \exists u\,(<x, u>\in R\wedge <u, y>\in R)\\ &\Rightarrow \exists u\,(<x, y>\in R) \quad (R\text{ 传递})\\ &\Leftrightarrow <x, y>\in R\end{aligned}$$

故 $R^2 \subseteq R$ 。反之，设 $R^2 \subseteq R$。为证 R 传递，设有 xRy, yRz 。据此有 $x R^2 z$ 。由 $R^2 \subseteq R$，知 xRz。传递性得证。

已知某些关系同时具有某一性质，对它们作关系运算后的结果是否仍具有这一性质，是一个令人关注的问题。如果是，我们称该性质对这一运算**封闭**。现在我们来讨论五大特性对基本关系运算的封闭性。

定理 10-9 设 R，S 均为 A 上二元关系。

（1）五大特性对交运算均封闭。即若 R，S 有五大特性之一，则 $R \cap S$ 仍有此性质。

（2）自反、反自反、对称性对并运算封闭。

（3）反自反、对称、反对称性对差运算封闭。

（4）对称性对补运算封闭。

（5）五大特性对求逆运算均封闭。

（6）自反性对合成运算封闭，其他四大特性对合成运算均不封闭。

证明 （1）之“传递性对交运算封闭”。

设 R，S 传递。为证 $R \cap S$ 传递，设有 $x R \cap S y, y R \cap S z$,那么 $x Ry, xSy, yRz, ySz$ 。据 R，S 传递，可知 $x Rz, xSz$，从而 $xR \cap Sz$ 。故 $R \cap S$ 传递性得证。

（2）之“对称性对并运算均封闭”。

设 R，S 对称。为证 $R \cup S$ 对称，设 $xR \cup Sy$，那么 xRy 或 xSy。由 R，S 对称知 yRx 或 ySx，从而 $yR \cup Sx$。$R \cup S$ 对称性证完。

（3）之“反对称性对差运算均封闭”。

设 R，S 反对称。为证 $R-S$ 反对称，设 $x(R-S)y$ 且 $y(R-S)x$，因而 xRy，yRx，从而由 R 的反对称性得 $x=y$。这就完成了 $R-S$ 反对称的证明。

其实 $R-S$ 反对称与 S 反对称无关，只要 R 反对称，$R-S$ 一定反对称。反自反也如此。

（4）自证。

（5）之“传递性对求逆运算均封闭”。

设 R 传递。为证 $R^{\sim}$传递，设有 $xR^{\sim}y$，$y R^{\sim} z$ 。那么，yRx, zRy 。根据 R 的传递性又可得 zRx，即 $x R^{\sim} z$ 。$R^{\sim}$传递性得证。

（6）我们举例说明对称性、反对称性、传递性对合成运算均不封闭。

1）令 $R=\{<1,2>,<2,1>\}$，$S=\{<2,3>,<3,2>\}$，R, S 均对称，但 $R \circ S=\{<1,3>\}$不对称。

2）令 $R=\{<1,2>,<3,4>\}, S=\{<2,3>,<4,1>\}, R, S$ 均反对称，但 $R \circ S=\{<1,3>,<3,1>\}$不反对称。

3）同 2），R，S 均传递，但 $R \circ S$ 不传递。

10.1.4 关系特性闭包

在实际应用中，有时会遇到这样的问题，某一关系并不具有某种特性，但需要对它进行扩充，使它具有这种特性。而所进行的扩充又要求是最“经济”的。这种关系的扩充正是这一小节要讨论的关系特性闭包。

定义 10-6 设 R 是集合 A 上二元关系，称 R'为 R 的**自反闭包**（**对称闭包**，**传递闭包**），如果 R'满足：

（1）R'是自反（对称的，传递的）。

（2）$R \subseteq R'$。

（3）对 A 上任意关系 R''，若 R''满足（1）和（2），则 $R' \subseteq R''$。

R 的自反闭包、对称闭包和传递闭包分别记为 $r(R)$，$s(R)$，$t(R)$，也称 r，s，t 为闭包运算，它们作用于关系 R 后，分别产生包含 R 的、最小的自反、对称、传递的二元关系。这三个闭包运算也可据下述定理来规定。

定理 10-10 设 R 是集合 A 上的二元关系，那么

（1）$r(R) = E_A \cup R$

（2）$s(R) = R \cup R^{\sim}$

（3）$t(R) = \bigcup_{i=1}^{\infty} R^i$

证明 （1）$E_A \cup R$ 自反且 $R \subseteq E_A \cup R$ 是显然的。为证 $E_A \cup R$ 为自反闭包，还需证它的“最小性”。为此，令 R'自反，且 $R \subseteq R'$，欲证 $E_A \cup R \subseteq R'$。由于 R'自反，据定理 10-8（1），$E_A \subseteq R'$，连同 $R \subseteq R'$即得 $E_A \cup R \subseteq R'$。

（2）本式证明留给读者。

（3）首先 $R \subseteq \bigcup_{i=1}^{\infty} R^i$ 是显然的。

为证 $\bigcup_{i=1}^{\infty} R^i$ 传递，设 $<x, y> \in \bigcup_{i=1}^{\infty} R^i$，$<y, z> \in \bigcup_{i=1}^{\infty} R^i$ 那么有正整数 j，k，使 $<x, y> \in R^j$，$<y, z> \in R^k$，于是有 $<x, z> \in R^j \circ R^k = R^{j+k}$，从而 $<x, z> \in \bigcup_{i=1}^{\infty} R^i$，$\bigcup_{i=1}^{\infty} R^i$ 的传递性得证。

最后，令 R'传递，且 $R \subseteq R'$，需证 $\bigcup_{i=1}^{\infty} R^i \subseteq R'$。为此只要证：

对任意正整数 n，$R^n \subseteq R'$。对 n 归纳以证 $R^n \subseteq R'$。

$n = 1$ 时显然。

设 $R^k \subseteq R'$，欲证 $R^{k+1} \subseteq R'$。为此设 $<x, y> \in R^{k+1}$，那么有 u 使 $<x, u> \in R^k$，$<u, y> \in R$。据归纳假设及题设，知 $<x, u> \in R'$，$<u, y> \in R'$。但 R'是传递的，因此 $<x, y> \in R'$。$R^{k+1} \subseteq R'$证毕，归纳完成。（3）式得证。

【例 10-8】 设 $A = \{1,2,3\}$，$R_1 = \{<1,2>, <2,1>, <1,3>, <1,1>\}$，$R_2 = \{<1,2>, <2,1>\}$，$R_3 = \{<1,2>\}$，那么

$r(R_1) = \{<1,1>, <2,2>, <3,3>, <1,2>, <2,1>, <1,3>\}$，

$s(R_1) = \{<1,2>, <2,1>, <1,3>, <3,1>, <1,1>\}$

$t(R_1) = \{<1,2>, <2,1>, <1,1>, <2,2>, <1,3>, <2,3>\}$

$r(R_2) = \{<1,1>, <2,2>, <3,3>, <1,2>, <2,1>\}$，$s(R_2) = \{<1,2>, <2,1>\} = R_2$，

$t(R_2) = \{<1,2>, <2,1>, <1,1>, <2,2>\}$

$r(R_3) = \{<1,2>, <1,1>, <2,2>, <3,3>\}$，$s(R_3) = \{<1,2>, <2,1>\}$，$t(R_3) = \{<1,2>\} = R_3$

由闭包定义及上例可以看出：

定理 10-11 设 R 是集合 A 上任一关系，那么

（1）R 自反当且仅当 $R = r(R)$。

（2）R 对称当且仅当 $R=s(R)$。

（3）R 传递当且仅当 $R=t(R)$。

证明 （1）、（3）留给读者，现证（2）。

充分性由 $s(R)$定义立得。

为证必要性，设 R 对称，那么 $R=R^{\sim}$（据定理 10-8）。另一方面，$s(R)=R\cup R^{\sim}=R\cup R=R$（据定理 10-10），故 $s(R)=R$。

定理 10-12 设 R 是集合 A 上任一二元关系，那么

（1）如果 R 是自反的，那么 $s(R)$和 $t(R)$都是自反的。

（2）如果 R 是对称的，那么 $r(R)$和 $t(R)$都是对称的。

（3）如果 R 是传递的，那么 $r(R)$是传递的。

证明 （1）是显然的。

（2）由于 $r(R)^{\sim}=(E_A\cup R)^{\sim}=E_A^{\sim}\cup R^{\sim}=E_A\cup R=r(R)$，故 $r(R)$是对称的。

另外，由于对任意自然数 n，$(R^n)^{\sim}=(R^{\sim})^n$（据定理 10-4 之（6）），又由于 R 对称，故$(R^n)^{\sim}=R^n$。因此，对任意$<x,y>\in t(R)$，总有 i 使$<x,y>\in R^i$，从而$<y,x>\in(R^i)^{\sim}=R^i$，即$<y,x>\in t(R)$。故 $t(R)$对称。

（3）本式证明留给读者。请注意，R 传递并不保证 $s(R)$传递。例如 $R=\{<1,2>\}$是传递的，但是 $s(R)=\{<1,2>,<2,1>\}$却不是传递的。

定理 10-13 设 R 为集合 A 上的任一二元关系，那么

（1）$rs(R)=sr(R)$

（2）$rt(R)=tr(R)$

（3）$s(R)\subseteq ts(R)$

证明 （1）$sr(R)=s(E_A\cup R)=E_A\cup R\cup(E_A\cup R)^{\sim}$

$$=E_A\cup R\cup R^{\sim}=E_A\cup s(R)=rs(R)$$

（2）易证$(E_A\cup R)^n=E_A\cup\bigcup_{i=1}^{n}R^i$对一切正整数 n 均成立（本章练习之 17 题），于是

$$\begin{aligned}tr(R)&=t(E_A\cup R)\\&=\bigcup_{i=1}^{\infty}(E_A\cup R)^i\\&=\bigcup_{i=1}^{\infty}(E_A\cup\bigcup_{j=1}^{i}R^j)\\&=E_A\cup\bigcup_{i=1}^{\infty}R^i\\&=E_A\cup t(R)\\&=rt(R)\end{aligned}$$

（3）易证对任一闭包运算 Δ 和任意二元关系 R_1，R_2，如果 $R_1\subseteq R_2$，那么 $\Delta(R_1)\subseteq\Delta(R_2)$（本章练习之 21 题）；又据闭包定义，对任意二元关系 R 有 $R\subseteq s(R)$，故 $t(R)\subseteq ts(R)$，$st(R)\subseteq sts(R)$。由于 $ts(R)$是对称的（据定理 10-12），$sts(R)=ts(R)$。于是我们得到

$$st(R)\subseteq ts(R)$$

注意，（3）式中符号$\subseteq$不能用等号代替。例如$R\{<1,2>\}$时，$st(R)=\{<1,2>,<2,1>\}$，

而 $ts(R)=\{\langle 1,2\rangle,\langle 2,1\rangle,\langle 1,1\rangle,\langle 2,2\rangle\}$,$st(R)\neq ts(R)$。

从以上讨论可以看出，传递闭包的求取是很复杂的。但是，当集合 A 为有限集时，A 上二元关系的传递闭包的求取便可大大简化。

定理 10-14 设 R 为 A 上二元关系，$|A|=n$，那么 $t(R)=\bigcup_{i=1}^{n}R^i$。

证明 $\bigcup_{i=1}^{n}R^i\subseteq t(R)$是显然的。

为证 $t(R)\subseteq\bigcup_{i=1}^{n}R^i$，设$\langle x,y\rangle\in t(R)=\bigcup_{i=1}^{\infty}R^i$。那么可令 i_0 为“使$\langle x,y\rangle\in R^i$的最小 i 值”。现证 $i_0\leqslant n$。若不然，有 $i_0(>n)$个 A 中元素 $u_1,u_2,\cdots,u_{i_0}(=y)$，使得 $xRu_1,u_1Ru_2,\cdots,u_{i_0-1}Ry$（因$\langle x,y\rangle\in R^{i_0}$）。然而 A 中只有 n 个不同元素，因此 i_0 这个元素中至少有两个是相同的（鸽笼原理），不妨设 $u_k=u_j$，而 $k<j$，于是由

$$xRu_1,u_1Ru_2,\cdots,u_{k-1}Ru_k,u_jRu_{j+1},\cdots,u_{i_{0-1}}Ry$$

可推出$\langle x,y\rangle\in R^{i_0-(j-k)}$，这与 i_0 的最小性矛盾。故 $i_0\leqslant n$，进而知$\langle x,y\rangle\in\bigcup_{i=1}^{n}R^i$，$t(R)\subseteq\bigcup_{i=1}^{n}R^i$得证。定理 10-14 证毕。

10.2 等价关系

俗话说“物以类聚，人以群分”，那么这种分类的依据是什么呢？正是事物之间的关系。本节的目的就是要研究可用于对集合中元素进行分类的一种重要关系：等价关系。

10.2.1 等价关系与等价类

定义 10-7 称集合 A 上关系 R 是**等价关系**（equivalent relation），如果 R 为 A 上的自反、对称、传递的二元关系。

【例 10-9】

（1）三角形的相似关系、全等关系都是等价关系。

（2）住校学生的“同寝室关系”是等价关系。

（3）命题公式间的逻辑等价关系是等价关系。

（4）对任意集合 A，A 上的相等关系 E_A 和全关系 $A\times A$ 是等价关系。

（5）整数集上的“模 k 相等关系”（k 是正整数）是等价关系。模 k 相等用符号 $\equiv_k$ 表示，定义如下：

$$x\equiv_k y \text{ 当且仅当 } k|(x-y)\quad (k \text{ 整除 } x-y)$$

例如，$2\equiv_{12}14$，$-1\equiv_5 4$，$\equiv_k$ 关系为等价关系的证明留给读者。

定义 10-8 设 R 为集合 A 上的等价关系。对每一 $a\in A$，a 的**等价类**（equivalent class），记为$[a]_R$（或简单地记为$[a]$），指下列集合

$$[a]_R=\{x\mid x\in A\wedge xRa\}$$

a 称为$[a]_R$的**代表元素**。

【例 10-10】 设 R 为整数集上的$\equiv_5$关系，它有五个不同的等价类：

[0]= {…,-10,-5,0,5,10, …} = {x | 5 整除 x}，[1]= {…,-9,-4,1,6,11,…} = {x | 5 除 x 余 1}

[2]= {…,-8,-3,2,7,12,…} = {x | 5 除 x 余 2}，[3]= {…,-7,-2,3,8,13,…} = {x | 5 除 x 余 3}

[4]= {…,-6,-1,4,9,14,…} = {x | 5 除 x 余 4}

关于等价类的下列事实是十分显然的：

（1）对任何集合 A, E_A 有 $|A|$ 个不同的等价类，每个等价类都是单元素集。

（2）对任何集合 A，$A\times A$ 只有一个等价类——A（即每个元素的等价类全为 A）。

（3）对每一元素 $a\in A$，任何 A 上等价关系 R，$[a]_R\neq\varnothing$，因为 R 自反，恒有 $a\in[a]_R$。

（4）同一等价类可以有不同的代表元素，或者说，不同的元素，可能有相同的等价类。

关于等价类的进一步性质，在下列定理中给出。

定理 10-15 设 R 是集合 A 上的等价关系，那么，对任意 a, $b\in A$，

aRb 当且仅当 $[a]_R=[b]_R$

证明 设 aRb。为证 $[a]_R\subseteq[b]_R$，又设 $x\in[a]_R$，那么 xRa。又据 aRb 及 R 的传递性，有 xRb，从而 $x\in[b]_R$。$[a]_R\subseteq[b]_R$ 证得。同理可证 $[b]_R\subseteq[a]_R$。于是 $[b]_R=[a]_R$ 得证。

反之，设 $[a]_R=[b]_R$。由于 $a\in[a]_R$，故 $a\in[b]_R$，因而 aRb。

定理 10-16 设 R 是集合 A 上的等价关系，那么对任意 a，$b\in A$，或者 $[a]_R=[b]_R$ 或者 $[a]_R\cap[b]_R=\varnothing$。

证明 设 $[a]_R\cap[b]_R\neq\varnothing$，那么有 $x\in[a]_R\cap[b]_R$，从而有 xRa，xRb。据 R 的对称性又有 aRx，xRb。再用 R 的传递性，得 aRb。由定理 10-15 知 $[a]_R=[b]_R$。

定理 10-15、定理 10-16 告诉我们，对任何集合 A 上的等价关系 R，及对任意 a，$b\in A$，以下三个性质是等价的：

（1）aRb

（2）$[a]_R=[b]_R$

（3）$[a]_R\cap[b]_R\neq\varnothing$

10.2.2 等价关系与划分

定义 10-9 当非空集合 A 的子集族 π 满足下列条件时称为 A 的**划分**（partitions）：

（1）对任意 $B\in\pi$, $B\neq\varnothing$。

（2）$\cup\pi=A$。

（3）对任意 B，$B'\in\pi$，$B\neq B'$ 时，$B\cap B'=\varnothing$。

称 π 中元素为划分的**单元**。

我们约定 $A=\varnothing$ 时只有划分 $\varnothing$。

【例 10-11】 设 $A=\{1, 2, 3, 4\}$，那么下列集合为 A 的划分：

$\pi_1=\{\{1\}, \{2\}, \{3\}, \{4\}\}$

$\pi_2=\{\{1,3\}, \{2,4\}\}$

$\pi_3=\{\{3\}, \{1, 2, 4\}\}$

$\pi_4=\{\{1,2,3,4\}\}$

但下列集合不是 A 的划分：

$$\{\varnothing,\{1,2\},\{3,4\}\},\{\{1,3\},\{4\}\},\{\{1,2,3\},\{2,4\}\}$$

由定理 10-15 和定理 10-16 不难得出，A 上等价关系 R 的等价类的集合，构成 A 的一个划分，称为等价关系 R **对应的划分**。

定理 10-17 设 R 为集合 A 上的等价关系，那么 R 对应的 A 划分是$\{[x]_R \mid x\in A\}$。

反之，由集合的一个划分也可作出该集合上的一个等价关系。

定理 10-18 设 π 是集合 A 的一个划分，则如下定义的关系 R 为 A 上的等价关系：

$$R=\{<x,y>\mid \exists B(B\in \pi\wedge x\in B\wedge y\in B)\}$$

或者

$$R=\bigcup_{B\in\pi} B\times B=(\bigcup\{B\times B\mid B\in \pi\})$$

称 R 为 π 对应的等价关系。

证明是极为容易的，请读者完成之。

由等价关系作出其对应的划分，以及由划分作出其对应的等价关系，从它们的作法定义来看，划分与等价关系的这种对应是惟一确定的。事实上，可以证明，不可能有两个不同的等价关系对应同一个划分，也不可能有两个不同的划分对应同一个等价关系。下列定理给出的结论甚至更强。

定理 10-19 设 π 是集合 A 的划分，R 是 A 上等价关系，那么，对应 π 的等价关系为 R，当且仅当 R 对应的划分为 π。

证明 $A=\varnothing$ 时，只有∅划分和等价关系∅，结论显然成立。下文设 $A\neq\varnothing$ 。

先证必要性。设对应 π 的等价关系为 R，R 对应的划分为 π'，欲证 $\pi=\pi'$。为此对任一元素 $a\in A$，设 B，B'分别是 π， π'中含 a 的单元。那么，对 A 中任一元素 b，有

$$\begin{aligned} b\in B &\Leftrightarrow aRb \quad (R \text{ 是对应的等价关系})\\ &\Leftrightarrow b\in[a]_R\\ &\Leftrightarrow b\in B' \quad (\pi' \text{是 } R \text{ 对应的划分})\end{aligned}$$

这就是说 $B=B'$。由于 a 是 A 中任意元素，故可断定 $\pi=\pi'$。

再证充分性。设 R 对应的划分为 π， π对应的等价关系为 R'，欲证 $R=R'$。为此考虑 A 中任意元素 a，b，有

$$\begin{aligned} aRb &\Leftrightarrow b\in[a]_R\\ &\Leftrightarrow \exists B(B\in \pi\wedge[a]_R=B\wedge b\in B) \quad (\pi \text{ 为 } R \text{ 对应的划分})\\ &\Leftrightarrow \exists B(B\in \pi\wedge a\in B\wedge b\in B)\\ &\Leftrightarrow aR'b \quad (R' \text{为 } \pi \text{对应的等价关系})\end{aligned}$$

故 $R=R'$。

为深入讨论等价关系及划分，我们引入一些关于划分的新概念。

定义 10-10 设 π_1， π_2 为集合的两个划分。称 π_1 **细于** π_2，如果 π_1 的每一单元都包含于 π_2 的某个单元。π_1 **细于** π_2 表示为 $\pi_1\leqslant\pi_2$。 $\pi_1\leqslant\pi_2$ 且 $\pi_1\neq\pi_2$，则表示为 $\pi_1<\pi_2$，读作 π_1 **真细于** π_2。

【例 10-12】

（1）当$A=\{1,2,3,4\}$ 时，$\pi_1=\{\{1,2\},\{3\},\{4\}\}$ 细于$\pi_2=\{\{1,2,3\},\{4\}\}$；$\pi_3=\{\{1\},\{2\},\{3\},\{4\}\}$ 细于所有划分。而所有划分均细于 $\pi_4=\{\{1,2,3,4\}\}$。并且，π_1 真细于

π_2； π_3真细于 π_1。

（2）图 10-4 给出的两个 A 的划分 π， π'， π''细于 π。

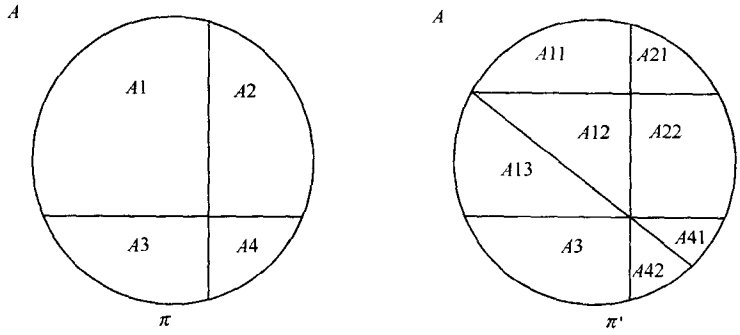


图 10-4

定理 10-20 设 R_1，R_2为集合 A 上的等价关系， π_1， π_2分别是 R_1，R_2所对应的划分，那么

$$R_1 \subseteq R_2 \text{当且仅当 } \pi_1 \leqslant \pi_2$$

证明 当 $A=\varnothing$时命题显然真。以下设 $A \neq \varnothing$。

先证必要性。设 $R_1 \subseteq R_2$，B_1为 π_1中任一单元，令 $B_1=[a]_{R1}$，$a \in A$。考虑$[a]_{R2}=B_2 \in \pi_2$。对任一 $b \in B_1$，有 $b\ R_1 a$，因 $R_1 \subseteq R_2$，从而有 $b\ R_2 a$，故 $b \in [a]_{R2}=B_2$。这就是说 $B_1 \subseteq B_2$，因而 $\pi_1 \leqslant \pi_2$。

再证充分性。设 $\pi_1 \leqslant \pi_2$，$x R_1 y$，那么有 π_1中单元 $B_1=[x]_R$，使 x，$y \in B_1$。由于 $\pi_1 \leqslant \pi_2$，故有 π_2中单元 B_2，使 $B_1 \subseteq B_2$；从而 x，$y \in B_2$，即 x，y 属同一个 R_2等价类。因此 $x\ R_2 y$。至此我们证得 $R_1 \subseteq R_2$。

本定理表明，越“小”（含有较少序偶）的等价关系对应越细的划分，反之亦然。很明显，最小的等价关系是相等关系，它对应于最细的划分（每一单元恰含一个元素，通常称为最大划分），最大的等价关系是全关系，它对应于最粗的划分（只有一个单元，通常称为最小划分）。

【例 10-13】 我们知道，$a \equiv_6 b$ 蕴涵 $a \equiv_2 b$ 和 $a \equiv_3 b$，因此模 6 相等关系对应的划分（六个单元）细于模 3 相等关系（三个单元）及模 2 相等关系对应的划分（二个单元）。容易证明，对任意整数 x，$[x]_6 \subseteq [x]_3$，$[x]_6 \subseteq [x]_2$（这里$[x]_k$表示模 k 相等关系的 x 的等价类——模 k 等价类）。

对于等价关系可作并、交运算，对于划分也有相应的运算。

***定义 10-11** 设 π_1， π_2是集合 A 的两个划分。称 $\pi_1 \cdot \pi_2$为 π_1和 π_2的**积划分**，它是满足下列条件的 A 的划分：

（1） $\pi_1 \cdot \pi_2$细于 π_1和 π_2。

（2）如果 A 的划分 π细于 π_1， π_2，则 π必细于 $\pi_1 \cdot \pi_2$。

这就是说， $\pi_1 \cdot \pi_2$是细于 π_1， π_2的最“粗”划分（类似于最大公约数）。

【例 10-14】 图 10-5 给出了一个积划分的直观例子。

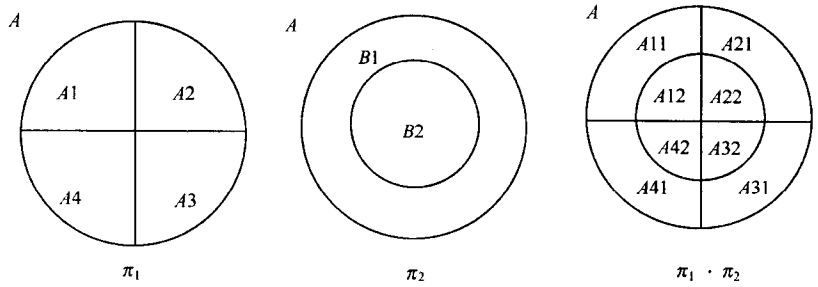


图 10-5

由本章练习第 25 题知，若 R_1，R_2 为 A 上等价关系，则 $R_1 \cap R_2$ 也是 A 上等价关系。

定理 10-21 设 π_1，π_2 为集合的划分，$R1$，$R2$ 分别为 π_1，π_2 对应的等价关系。那么 $\pi_1 \cdot \pi_2$ 是等价关系 $R1 \cap R2$ 所对应的划分。

证明 首先，$R1 \cap R2 \subseteq R1$，$R1 \cap R2 \subseteq R2$，因此 $R1 \cap R2$ 对应的划分必细于 π_1，π_2（定理 10-20）。

其次，假设有 π，$\pi \leqslant \pi_1$，$\pi \leqslant \pi_2$，而 π 对应于等价关系 R，那么据定理 10-20，$R \subseteq R1$，$R \subseteq R2$，因而 $R \subseteq R1 \cap R2$，故 R 对应的划分 π 必细于 $R1 \cap R2$ 所对应的划分。

综上所述，$R1 \cap R2$ 所对应的划分即为 π_1 与 π_2 的积划分 $\pi_1 \cdot \pi_2$。

由于积划分被 $R1 \cap R2$ 惟一确定，因此对任意划分 π_1，π_2，其积划分 $\pi_1 \cdot \pi_2$ 是惟一确定的。

定义 10-12 设 π_1，π_2，是集合 A 上的划分，$\pi_1 + \pi_2$ 称为 π_1，π_2 的**和划分**，它是满足下列条件的 A 的划分：

（1）π_1 细于 $\pi_1 + \pi_2$，π_2 细于 $\pi_1 + \pi_2$。

（2）若有 A 的划分 π，π_1 细于 π，π_2 细于 π，那么 $\pi_1 + \pi_2$ 细于 π。

这就是说，和划分 $\pi_1 + \pi_2$ 是“粗于” π_1，π_2 的最细划分（类似于最小公倍数）。

【例 10-15】 图 10-7 给出了一个和划分的直观例子。

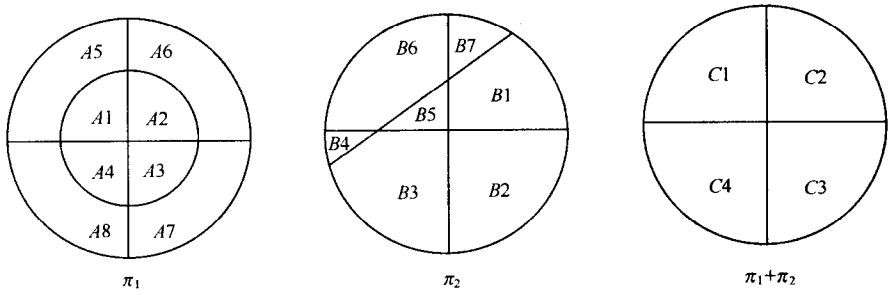


图 10-6

一个自然的猜想是，对应于 π_1，π_2 的等价关系的并对应于 $\pi_1 + \pi_2$。然而两个等价关系的并未必是等价关系，猜想并不成立。不过，我们有一个十分接近的结论，也是在意料之中的。

定理 10-22 设 $R1$ 和 $R2$ 是集合 A 的划分 π_1，π_2 所对应的等价关系，那么 $t(R1 \cup R2)$ 是对应于和划分 $\pi_1 + \pi_2$ 的 A 上的等价关系。

证明 $t(R1 \cup R2)$为 A 上的等价关系是明显的。现证 $\pi_1 + \pi_2$对应于 $t(R1 \cup R2)$。

由于 $R1 \subseteq t(R1 \cup R2)$，$R2 \subseteq t(R1 \cup R2)$，因此 $R1$，$R2$ 对应的划分 π_1，π_2细于 $t(R1 \cup R2)$对应的划分。另一方面，设划分 π满足 $\pi \leqslant \pi_1$，$\pi_2 \leqslant \pi$，它对应于等价关系 R。那么 $R1 \subseteq R$，$R2 \subseteq R$，进而 $R1 \cup R2 \subseteq R$，$t(R1 \cup R2) \subseteq t(R)$。由于 R 传递，$t(R) = R$，因此 $t(R1 \cup R2) \subseteq R$，故 $t(R1 \cup R2)$对应的划分细于 R 对应的划分 π。

以上讨论表明。$t(R1 \cup R2)$所对应的划分正是 π_1与 π_2的和划分 $\pi_1 + \pi_2$。

由于 π_1，π_2 的和划分被它们所对应的等价关系的并的传递闭包惟一确定。因此对任何划分 π_1，π_2，它们的和划分是惟一确定的。

【例 10-16】 令 $R1$ 为模 2 相等关系，$R2$ 为模 3 相等关系。那么 $R1$，$R2$ 对应的划分分别是

$$\pi_1 = \{[0]_2, [1]_2\}$$

$$\pi_2 = \{[0]_3, [1]_3, [2]_3\}$$

令 $R3$ 为模 6 相等关系，$R4$ 为模 1 相等关系，那么 $R3$，$R4$ 对应的划分分别是

$$\pi_3 = \{[0]_6, [1]_6, [2]_6, [3]_6, [4]_6, [5]_6\}$$

$$\pi_4 = \{[0]_1\}\{I\} \quad (I \text{为整数集})$$

我们来证明 π_3是 π_1，π_2的积划分，π_4为 π_1，π_2的和划分。

对任何整数 x，y，有

$$\begin{aligned} xR3y &\Leftrightarrow x \equiv_6 y \\ &\Leftrightarrow \exists m\,(x-y=6m) \\ &\Leftrightarrow \exists m\,(x-y=2m) \wedge \exists m\,(x-y=3m) \\ &\Leftrightarrow xR1y \wedge xR2y \\ &\Leftrightarrow x\,(R1 \cap R2)y \end{aligned}$$

于是 $R3 = R1 \cap R2$，π_3是 π_1与 π_2的积划分。

为证 $\pi_4 = \pi_1 + \pi_2$，只要证 $R4 = t(R1 \cup R2)$。由于对任何整数 x，y 都有 $xR4y$（因恒有整数 m，使 $x-y=m \cdot 1$，从而 $x \equiv_1 y$），因此只要证，对任何整数 x，y，均有$<x, y> \in t(R1 \cup R2)$。为此，令 $x-y=i$。若 i 是偶数，则有整数 m，使 $x-y=2m$，从而$<x, y> \in R1 \subseteq t(R1 \cup R2)$；若 i 是奇数，则有整数 m，使 $x-y=m \cdot 2+3$。于是可取整数 $u=y+3$，使 $x-u=m \cdot 2$，$u-y=3$。这样$<x, u> \in R1$，$<u, y> \in R2$，亦即$<x, y> \in R1 \circ R2$。由于$R1 \circ R2 \subseteq (R1 \cup R2)^2 \subseteq t(R1 \cup R2)$，因此$<x, y> \in t(R1 \cup R2)$。

综上所述，$R4 = t(R1 \cup R2)$，$\pi_4 = \pi_1 + \pi_2$。

最后我们介绍一个常用的术语。

定义 10-13 设 R 为集合 A 上的等价关系，那么称 A 的划分$\{[a]_R | a \in A\}$为 A 的 R **商集**（quotient sets），记为 A/R。

显然，A 的每一划分 π均为 A 的一个商集，可称划分的和与积为商集的和与积，从而

$$A/(R1 \cap R2) = A/R1 \cdot A/R2,\ A/t(R1 \cup R2) = A/R1 + AR/2。$$

10.3 序关系

事物之间的次序常常是事物群体的重要特征，决定事物之间次序的还是事物间的关系。

本节的目的则是要研究可用以对集合中元素进行排序的关系类——序关系。

10.3.1 序关系和有序集

定义 10-14 设 R 是集合 A 上的二元关系，称 R 为**序关系**（ordered relations），如果 R 是自反、反对称、传递的。如果集合 A 上有序关系 R，则称 A 为**有序集**（ordered sets），用序偶$<A, R>$表示之。

很容易判定，数集上的≤关系为一典型的序关系。因此为简明，我们今后用记号≤表示一般的序关系，从而$<A, \leqslant>$表示一般的有序集。

【例 10-17】

（1）实数集 R 上的“≤关系”为一序关系，$<R, \leqslant>$表示一个有序集。实数集 R 上的“≥关系”也是序关系，<R, ≥>也表示一个有序集。

（2）集合 A 的幂集 $\rho(A)$上的“$\subseteq$ 关系”为序关系，$<\rho(A), \subseteq>$为一有序集。

（3）正整数集合上的整除关系为一序关系，$<I_+, |>$为一有序集。

我们可对序关系的关系图作简化。

（1）由于序关系自反，各结点处均有环，约定全部省去。

（2）由于序关系反对称且传递，关系图中任何两个不同结点之间不可能有相互到达的边或通路，因此可约定边的向上方向为箭头方向，即若 $a \leqslant b$, 则将结点 a 画在结点 b 之下，省略全部箭头。

（3）由于序关系传递，我们还可将由传递关系可推定的边也省去，即若 $a \leqslant b, b \leqslant c$，则肯定应有 $a \leqslant c$，但省略 a 到 c 的有向边。

经过这种简化的序关系图称为**哈斯**（Hasse）**图**。哈斯图既表示一个序关系，又表示一个有序集。

例如，表示集合 $\rho(\{a,b\})$上的集合包含关系的关系图，可如图 10-7 作简化。

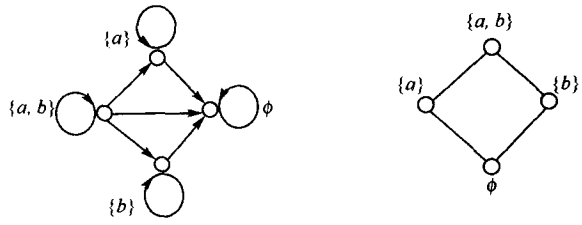
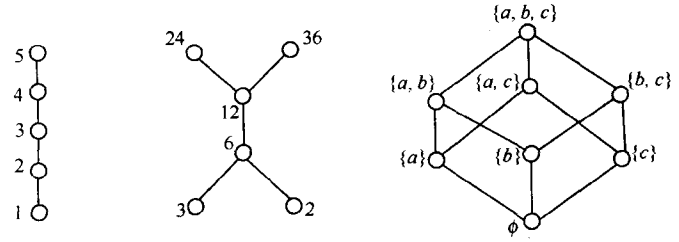


图 10-8

【例 10-18】 图 10-8a、b、c 分别表示有序集



a) b) c)

图 10-8

$<\{1,2,3,4,5\}, \leqslant>, <\{2,3,6,12,24,36\}, |>, <\rho(A), \subseteq>(A=\{a,b,c\})$

利用序关系可对有序集合中元素进行比较或排序。$a \leqslant b$ 时，称 a **先于或等于** b，a 小于或等于 b；$\neg(a \leqslant b)$ 且 $\neg(b \leqslant a)$ 时，称 a，b **不可比较或不可排序**。在排序中，有的元素处于特殊的地位。

定义 10-15 设$<A, \leqslant>$为有序集，$B \subseteq A$。

（1）称 b 为 B 的**最小元**（least element），如果 $b \in B$ 且对每一 $x \in B$，$b \leqslant x$。即

b 为 B 之最小元 $\Leftrightarrow b \in B \wedge \forall x (x \in B \rightarrow b \leqslant x)$

（2）称 b 为 B 的最大元（greatest element），如果 $b \in B$，并且对每一 $x \in B$，$x \leqslant b$。即

b 为 B 之**最大元** $\Leftrightarrow b \in B \wedge \forall x (x \in B \rightarrow x \leqslant b)$

（3）称 b 为 B 的**极小元**（minimal element），如果 $b \in B$，并且没有 $x \in B$，$x \neq b$，使得 $x \leqslant b$。即

b 为 B 之极小元 $\Leftrightarrow b \in B \wedge \neg \exists x (x \in B \wedge x \neq b \wedge x \leqslant b)$

（4）称 b 为 B 的**极大元**（maximal element），如果 $b \in B$，并且没有 $x \in B$，$x \neq b$，使得 $b \leqslant x$。即

b 为 B 之极大元 $\Leftrightarrow b \in B \wedge \neg \exists x (x \in B \wedge x \neq b \wedge b \leqslant x)$

【例 10-19】 有序集$<\{a, b, c, d, e, f, g, h\}, \leqslant>$，由图 10-9 中哈斯图给出。

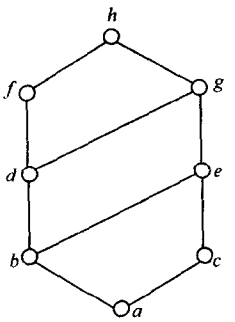


图 10-9

（1）$B=\{b, d, e, g\}$

B 的最大元为 g。

B 的极大元为 g。

B 的最小元为 b。

B 的极小元也为 b。

（2）$B=\{b, c, d, e, f, g\}$

B 无最大元和最小元。

B 的极大元是 f, g；极小元是 b, c。

（3）$B=\{a, c, d\}$

B 无最大元，其最小元为 a。

B 的极大元为 c, d，极小元为 a。

（4）$B=\{d, e\}$

B 无最大元，也无最小元。

B 的极大元是 d, e，极小元也是 d, e。

定理 10-23 设$<A, \leqslant>$为有序集，$B \subseteq A$。

（1）若 b 为 B 的最大（最小）元，则 b 为 B 的极大（极小）元。

（2）若 B 有最大（最小）元，则 B 的最大（最小）元惟一。

（3）若 B 为有限集，则 B 的极大元、极小元恒存在。

证明 （1）由定义或用反证法易得。

（2）设 b_1，b_2 为 B 的最大（最小）元，那么 $b_1 \leqslant b_2$ 且 $b_2 \leqslant b_1$。由$\leqslant$的反对称性即得 $b_1 = b_2$。

（3）设 $B=\{b_1, b_2, \cdots, b_n\}$，对 n 归纳。

当 $n=1$ 时，B 中仅有一个元素，它既是极大元，也是极小元。当 $n=2$ 时，设 $B=\{b_1, b_2\}$。那么，$b_1 \leqslant b_2$ 时 b_1 为极小元，b_2 为极大元；$b_2 \leqslant b_1$ 时 b_2 为极小元，b_1 为极大元；$\neg(b_1 \leqslant b_2)$

且¬（$b_2 \leqslant b_1$）时，b_1，b_2同为极大元，也同为极小元。

设$n=k$时命题真。若$n=k+1$，B＝{ b_1,b_2，…,b_k,b_{k+1} }。据归纳假设，{ b_1,b_2，…,b_k}有极大元 b_i，极小元 b_j。又据归纳基础，{b_i,b_{k+1}}有极大元，它显然是 B 的极大元；{b_j,b_{k+1}}有极小元，它显然是 B 的极小元。

归纳完成，（3）得证。

值得注意的是，最大元、最小元未必存在，极大元、极小元对有限集虽必存在，但却未必惟一。

定义 10-16 设<A, ≤>为有序集，$B \subseteq A$。

（1）称 a 为 B 的上界（upper bound）。如果$a \in A$，且对每一$x \in B$，$x \leqslant a$，即

a 为 B 的上界 $\Leftrightarrow a \in A \wedge \forall x\,(x \in B \rightarrow x \leqslant a)$

（2）a 称为 B 的下界（lower bound），如果$a \in A$，且对每一$x \in B$，$a \leqslant x$，即

a 为 B 的下界 $\Leftrightarrow a \in A \wedge \forall x\,(x \in B \rightarrow a \leqslant x)$

（3）a 称为 B 的最小上界或上确界（least upper bound），如果 a 是 B 的所有上界的集合的最小元。

（4）a 称为 B 的最大下界或下确界（greatest lower bound），如果 a 是 B 的所有下界的集合的最大元。

【例 10-19】 （续）

（1）当 B＝{ b, c, d, e, g}时，B 有上界 g,h，下界 a；最小上界 g，最大下界 a。

（2）当 B＝{ b, e, d, f }时，B 有上界 h，下界 b，a；最小上界 h，最大下界 b。

【例 10-20】 图 10-10 中的哈斯图表示一有序集。考虑集合 $B=\{h, i\}$，它有上界 j，k，但无最小上界；它有下界 f, g, b, c, d, e, a，但没有最大下界。当 B＝{ b, c, d, e}时，它有上界 h，I, j, k，无最小上界；它没有下界和最大下界。

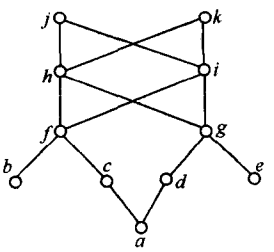


图 10-10

定理 10-24 设<A, ≤>为有序集，$B \subseteq A$。

（1）若 b 为 B 之最大元（最小元），则 b 必为 B 最小上界（最大下界）。

（2）若 b 为 B 之上（下）界，且$b \in B$，则 b 必为 B 的最大（最小）元。

（3）如果 B 有最大下界（最小上界），则最大下界（最小上界）惟一。

证明极易，略。

注意，上、下界未必存在，存在时又未必惟一。即使在有上界、下界时，最小上界和最大下界也未必存在。

有序集中链和反链的概念是十分有趣的。

定义 10-17 设<A, ≤>为有序集，$B \subseteq A$。称 B 为 A 上的链（chain），如果 B 中任何两个元素都是可比较的，即

$$\forall x \forall y(x,y \in B \rightarrow x \leqslant y \vee y \leqslant x)$$

称 B 为**反链**（antichain），如果 B 中任何两个不同元素都是不可比较的，即

$$\forall x \forall y(x,y \in B \wedge x \neq y \rightarrow \neg\,(x \leqslant y) \wedge \neg\,(y \leqslant x))$$

$|B|$称为**链或反链的长度**。

【例 10-21】 图 10-11 的哈斯图中有链$\{a, c, f, h, j\}$，$\{a, d, g, h, j\}$，$\{e, g, h, k\}$，$\{b, f\}$，$\{b\}$等。有反链$\{b, c, d, e\}$，$\{f, g\}$，$\{h, i\}$，$\{j, k\}$，$\{a, e\}$，$\{c, g\}$，$\{b\}$等。

定理 10-25 设$<A, \leqslant>$为一有限的有序集，且 A 中最长的链的长度为 n，那么 A 有一划分，使划分有 n 个单元，且每一单元为一反链。

证明 对 n 归纳。

当 $n=1$ 时，A 中没有任何两个不同元素有$\leqslant$关系，因此 A 本身既为一链，又为一反链，因此划分$\{A\}$即合要求。

设 $n=k$ 时命题成立。现令 $n=k+1$。

设 M 为 A 中所有极大元素的集合。由于 A 为有限集，因此 M 必为一非空的反链（极大元之间是不可比较的）。考虑有序集$<A-M, \leqslant>$，它不可能有长度为 n 的链（否则 A 中链的长度将超过 n，关于这一点请读者思考），因而$<A-M, \leqslant>$中最长链的长度应当为 $n-1=k$。据归纳假设，$A-M$ 有 k 个单元的划分，且每个单元为一反链。这 k 个反链连同反链 M，恰构成 A 的 $k+1$ 个单元组成的划分。归纳完成。

定理 10-26 设$<A, \leqslant>$为一有序集，$|A|=mn+1$。那么，A 中或者有 $m+1$（$n+1$）个元素组成的反链，或者有 $n+1$（$m+1$）个元素组成的链。

证明 回忆第 2 章，鸽笼原理之例 2-14。若 A 中链的长度不超过 n（m），那么据定理 10-25，A 中必有长度为 $m+1$（$n+1$）个元素的反链，否则$|A|\leqslant mn$。

【例 10-22】 设 C 是 7 个集合组成的集合族。由于集合之间的包含关系是序关系，而 $7=2\times3+1$，因此这 7 个集合中或者有 3（4）个集合 $A1$，$A2$，$A3$，（$A4$），满足 $A1\subseteq A2\subseteq A3$（$\subseteq A4$），或者有 4（3）个集合，其间两两互不包含。

如果将序关系中自反的要求改为反自反，就得到另一类重要的次序关系。

定义 10-18 称 R 为集合 A 上的**半序关系**（partially ordered relation），如果 R 反自反且传递。$<A, R>$称为**半序集**（poset）。

定义中省去了对 R 的“反对称”要求，因为 R 反自反且传递明显蕴涵 R 的反对称性。（本章练习第 11 题之（2））

有关有序集的讨论，大多可以适用于半序集。

* 10.3.2 良基性与良序集，完备序集

定义 10-19 设$<A, R>$为有序集（或半序集）。

（1）称$<A, R>$是**良基的**（well founded），如果 A 的任何非空子集都有关于 R 的极小元。

（2）称$<A, R>$是**全序的**（totally ordered），如果对任意的 x，$y\in A$，或者 xRy 或者 yRx；即 A 为一链。

（3）称$<A, R>$为**良序集**（well ordered set），如果$<A, R>$是全序的、良基的。

显然，若$<A, R>$为有限的全序集，那么它一定是良基的，从而为良序集。

关于良基性我们有定理 10-27。

定理 10-27 设$<A, \leqslant>$是有序集，那么下列两命题等价：

（1）$<A, \leqslant>$是良基的。

（2）不存在关于$\leqslant$的无穷降链，即不存在 A 的无穷子集$\{a_1, a_2, a_3, \cdots\}$，使得

$$\cdots \leqslant a_3 \leqslant a_2 \leqslant a_1$$

证明 （1）蕴涵（2）是明显的。若（2）不成立，那么无穷降链的存在就破坏了良基性。

反之，若（2）成立，欲证（1）。反设（1）不真。即有一 A 的某个非空子集 B 无极小元。由定理 10-24（3），则 B 是无限集。现取 $a_0 \in B$，由于 a_0 非极小元，有 $a_1 \in B$，使 $a_1 \leqslant a_0$。再对 a_1 如此重复，必可作出 $\{a_0, a_1, a_2, \cdots\} \subseteq B \subseteq A$，而

$$\cdots \leqslant a_2 \leqslant a_1 \leqslant a_0$$

这是一个无穷降链，与题设矛盾。

【例 10-23】

（1）设 R 为实数集，那么 $<R, \leqslant>$ 是全序的，但不是良基的。

（2）设 C 为非空集合族。因 C 上的“隶属关系”是一半序关系，$<C, \in>$ 是良基的（据定理 10-27）。

（3）$<N, \leqslant>$ 为良序集（N 为自然数集）。

若一集合为有序集（或半序集）且是良基的，那么可对该集施行归纳法。

设 $<A, \leqslant>$ 是良基的，欲证 $\forall x(x \in A \rightarrow P(x))$，可如下归纳地进行：

（1）证明 A 的所有极小元满足性质 P（归纳基础）。

（2）对任意非极小元 $x \in A$，设所有 y，$y \neq x$，$y \leqslant x$，满足 P，证明 x 也满足 P（归纳步骤）。

定理 10-28 设 $<A, \leqslant>$ 为一良基集，P 为一元谓词，若已对 $<A, \leqslant>$ 及 P 完成上述归纳过程，那么 $\forall x\,(x \in A \rightarrow P(x))$。

证明 设已对 $<A, \leqslant>$，P 完成了归纳过程的两个步骤，但有 $x \in A$ 使 $P(x)$ 假。令

$$S = \{x \mid x \in A \wedge \neg\, P(x)\}$$

显然，$S \neq \varnothing$。由于 $<A, \leqslant>$ 良基，S 中有极小元，记为 s。因而所有 $y, y \neq s, y \leqslant s$, 均不在 S 中，从而均满足 $P(x)$，故 s 也满足 $P(x)$（据归纳过程），矛盾。矛盾表明假设不能成立，$\forall x(x \in A \rightarrow P(x))$ 真。

本定理表明，对良基集运用归纳法是适当的。由于 $<N, \leqslant>$ 为良序集——良基集的特例，因此，本定理也证明了数学归纳法的正确性。

以下我们讨论有序集的又一特例。

定义 10-20 有序集 $<A, \leqslant>$ 称为是**完备的**（complete），如果

（1）A 有最小元，常记为 $\perp_A$ 或 $\perp$。

（2）A 中每一链 K 均有最小上界（上确界）。

【例 10-24】 设 B 为一集合，那么 $<\rho(B), \subseteq>$，为一完备序集。其中 $\varnothing$ 为最小元 $\perp$，对每一链 $\{B_1, B_2, B_3, \cdots\} = K$，$\cup K \subseteq B$ 总存在，$\cup K$ 为 K 的最小上界。

定理 10-29 具有最小元，且仅含有有穷链的有序集是完备的。

证明是显然的。

【例 10-25】 在真值集 $\{0, 1\}$ 中加入元素 ω，称为无定义值，并在 $\{0, 1, \omega\}$ 上定义偏序 $\leqslant$：

$a \leqslant b$ 当且仅当 $a = \omega$ 或 $a = b$

显然 $<\{0, 1, \omega\}, \leqslant>$ 为一完备序集，它在计算机形式语义学中有重要应用。

像例 10-25 中那样，在一已知集合（原本无序）中引入最小元，并如上定义序关系，所构成的有序集或半序集称为**平序集**（flat ordered set）或**平半序集**（flat partial ordered set）。

定义 10-21 设$\{<A_i, R_i>|i\in D\}$为一有序集合族（D 为标记集），如下定义笛卡儿（尔）积$\prod_{i\in D}A_i$上的关系 R：对任意 t，$s\in\prod_{i\in D}A_i$，有

$$tRs \text{ 当且仅当 } p_i(t)R_ip_i(s)$$

这里 $p_i(s)$，$p_i(t)$表示 s 和 t 的第 i 分量。

容易证明（本章练习第 50 题）$<\prod_{i\in D}A_i, R>$为一序关系。

定理 10-30 若有序集合族$\{<A_i, R_i>|i\in D\}$中的每一个都是完备的，那么$<\prod_{i\in D}A_i, R>$(R 如上定义)也是完备的。

证明 设$\perp_i$为各 A_i的最小元（$i\in D$），那么对一切 $i\in D$，$p_i(t)=\perp_i$的$\prod_{i\in D}A_i$中元素 t，显然是$<\prod_{i\in D}A_i, R>$中的最小元。

设 K 是$<\prod_{i\in D}A_i, R>$的一个链。据 R 的定义，K 中所有元素的第 i 分量构成一个$<A_i, R_i>$中的链 K_i ($i\in I$)。引用它们的完备性，对每一 i 有 K_i的最小上界，记为 $\sup K_i$，显然满足下列条件的$\prod_{i\in D}A_i$中元素 t 为 K 的最小上界：对每一 $i\in D$，

$$p_i(t)=\sup K_i$$

因此$<\prod_{i\in D}A_i, R>$为完备序集。

*10.3.3 全序集、良序集的构造

容易看出，以下算法可以把任一有限的有序集改造为全序集，从而成为一良序集。

设$<A, \leqslant>$为一非空有限有序集，如下构造$<A, \leqslant'>$，使之为全序集，且保持对任何 $a, b\in A$ 有

$$\text{若 } a\leqslant b, \text{ 则 } a\leqslant' b$$

（1）置 B 为 A，置 A 为$\varnothing$。

（2）取 B 中任一极小元（$B\neq\varnothing$时总存在）。例如 x，作为 A 的一个元素。即置 B 为 $B-\{x\}$，置 A 为 $A\cup\{x\}$。

（3）若 $B\neq\varnothing$，回到（2），否则停止。

（4）依 A 中元素进入先后定义序关系$\leqslant'$，即

$$a\leqslant' b \text{ 当且仅当 } a \text{ 先于 } b \text{ 进入 } A, \text{ 或 } a=b$$

显然$<A, \leqslant'>$为一全序集（从而为一良序集）。上述过程常称为**拓扑排序算法**。

此外，从已有的全序集、良序集出发，可以构造新的全序集和良序集。

首先，可用良序集$<N, \leqslant>$，来构造一个良序整数的良序集$<I, \leqslant_I>$。为此，我们在 N 和 I 之间建立起一种对应：

N:	0	1	2	3	4	5	6	7…
I:	0	-1	1	-2	2	-3	3	-4…

然后对 I 定义序关系$\leqslant_I$：对任意整数 m，n。

$$m\leqslant_I n \text{ 当且仅当} |m|<|n| \vee (|m|=|n| \wedge m\leqslant n)$$

如上定义的关系$\leqslant_I$显然是全序的。$<I, \leqslant_I>$的任一非空子集 S 的$\leqslant_I$关系最小元可如此求得：求出 N 的子集 $S'=\{|x| \mid x\in S\}$及其最小元 x_0。若$-x_0\in S$，则$-x_0$为 S 的$\leqslant_I$最小元；若$-x_0\notin S$，则 x_0为 S 的$\leqslant_I$最小元。

由良序集$<N,\leqslant>$构作良序集$<N\times N, \leqslant_{NN}>$，的方式同上。$\leqslant_{NN}$ 可如下定义：对任意自然数 x，y，x'，y'，有

$$<x,y>\leqslant_{NN}<x',y'>\text{当且仅当 } x<x'\vee (x=x'\wedge y\leqslant y')$$

类似地可用全序集$<I, \leqslant_I>$构作全序集$<I\times I, \leqslant_{II}>$,$\leqslant_{II}$ 的定义与$\leqslant_{NN}$ 的定义相仿，但是应当注意$\leqslant_{II}$不是良序。

处理非数值信息时，字典序和标准序是十分重要的，它们可以用定义在字母表上的良序来构作。

定义 10-22 设Σ为一字母表，$<\Sigma,\leqslant>$为一良序集，那么Σ^*上的关系$\leqslant_{字}$称为Σ^*上的**字典序**（lexicographically ordered relation），定义如下：对任意 x，$y\in\Sigma^*$，有

$$x\leqslant_{字} y \text{ 当且仅当}(x \text{ 为 } y \text{ 字头})\vee(x=w\xi w'\wedge y=w\zeta w''\wedge\xi\neq\zeta\wedge\xi\leqslant\zeta)$$

$$(\xi,\zeta\in\Sigma, w,w',w''\in\Sigma^*)$$

容易证明$\leqslant_{字}$为一全序，不赘述。但字典序不是良序。设$\Sigma=\{a,b\}$，$\lambda\leqslant a\leqslant b$ 那么Σ^*的子集 $S=\{b, ab, aab, aaab, \cdots\}$无$\leqslant_{字}$最小元。

定义 10-23 设Σ为一字母表，$<\Sigma,\leqslant>$为一良序集，那么Σ^*上的关系$\leqslant_{标}$称为Σ^*上的**标准序**（normally ordered relation），定义如下：对任意 x，$y\in\Sigma^*$，有

$$x\leqslant_{标} y \text{ 当且仅当}|x|<|y|\vee(|x|=|y|\wedge x\leqslant_{字} y)\ (|w|\text{表示字 } w \text{ 的字长})$$

标准序为全序关系是容易明白的，事实上它还是一个良序关系。设 S 为Σ^*的任一子集。令 $S_0=\{x \mid x \text{ 为 } S \text{ 中字长最短的字}\}$，显然，$S_0$为相同字长的字的集合，它必定为有限集。$S_0$的$\leqslant_{字}$最小元即为 S 的$\leqslant_{标}$最小元。

【例 10-26】 设$\Sigma=\{a,b\}$，$\lambda\leqslant a\leqslant b$，那么

（1）依字典序排列Σ^*如下：

$$\lambda, a, aa, aaa, \cdots, ab, aab, aaab, \cdots, b, ba, baa, baaa, \cdots$$

（2）依标准序排列如下：

$$\lambda, a, b, aa, ab, ba, bb, aaa, aab, aba, abb, baa, bab, bba, bbb, \cdots$$

10.4 练习

1．设 A,B 为集合，$|A|=n, |B|=m$。

（1）问 A 到 B 的二元关系共多少个？

（2）问 A 上二元关系共多少个？

（3）问 A 上的三元关系共多少个？

2．设 $A=\{0,1,2,3,4,5\}$，$B=\{1,2,3\}$，用列举法描述下列关系，并作出它们的关系图及关系矩阵：

（1）$R_1=\{<x, y>|x\in A\cap B\wedge y\in A\cap B\}$

（2）$R_2=\{<x, y>|x\in A\wedge y\in B\wedge x=y^2\}$

（3）$R_3=\{<x, y>|x\in A\wedge y\in A\wedge x+y=5\}$

（4）$R_4=\{<x,y>|x\in A\wedge y\in A\wedge\exists k(x=k\cdot y\wedge k\in N\wedge k<2)\}$

3．对下列 N 上的关系 R 作出归纳定义，并证明（依归纳定义）：$x\in R_3$。

（1）$R=\{<u,v>|u=2v\}, x=<6,3>$

（2）$R=\{<u,v,w>|u+v=w\}, x=<1,1,2>$

（3）$R=\{<u,v>|u\neq v\rightarrow u=v\}, x=<3,3>$

4．设 R, S 为集合 A 上任意关系，证明：

（1）$\mathrm{Dom}(R\cup S)=\mathrm{Dom}(R)\cup\mathrm{Dom}(S)$

（2）$\mathrm{Ran}(R\cap S)\subseteq\mathrm{Ran}(R)\cap\mathrm{Ran}(S)$

5．设 $A=\{a,b,c,d\}$，A 上二元关系 R_1，R_2 分别为

$$R_1=\{<b,b>,<b,c>,<c,a>\}$$

$$R_2=\{<b,a>,<c,a>,<c,d>,<d,c>\}$$

计算 $R_1\circ R_2$，$R_2\circ R_1$，R_1^2，R_2^2。

6．设 R_1，R_2 为 $A=\{0,1,2,3,4\}$ 上的关系：

$$R_1=\{<i,j>|j=i+1\vee j=\frac{i}{2}\}$$

$$R_2=\{<i,j>|i=j+2\}$$

计算 $R_1\circ R_2$，$R_2\circ R_1$，R_1^2，R_2^2。

7．图 10-11 给出了关系 R 的关系图，试求最小的 i，j，使 $i<j$，而 $R^i=R^j$。

8．设 R_1,R_2,R_3,R_4,R_5 都是整数集上的关系，且

$xR_1y\Leftrightarrow x\cdot y>0$

$xR_2y\Leftrightarrow|x-y|=1$

$xR_3y\Leftrightarrow x+y=10$

$xR_4y\Leftrightarrow x|y$

$xR_5y\Leftrightarrow x=y^k$（$k$ 是整数）

用 Y(yes)和 N(no)填写表 10-2。

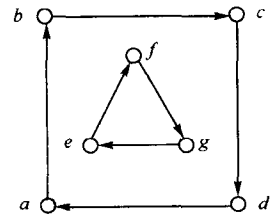


图 10-11

表 10-2

	自　反	反 自 反	对　称	反 对 称	传　递
R_1					
R_2					
R_3					
R_4					
R_5					

9．（1）设 R 是 A 上的二元关系，R 自反（反自反，对称，反对称，传递），$B\subseteq A$，试问 $R\cap B\times B$ 是否依然是自反（反自反，对称，反对称，传递）的。

（2）试举例说明：反对称性与传递性对并运算不封闭。

（3）试举例说明：自反性与传递性对差运算不封闭。

（4）试举例说明：自反性、反自反性、反对称性和传递性对求补运算均不封闭。

10. 设 R 是 A 上关系，如下定义 R 的三个性质（定义表达式中 $x\in A,y\in A,z\in A$ 省略）：

R 是循环的$\Leftrightarrow\forall x\forall y\forall z(xRy\wedge yRz\rightarrow zRx)$

R 有欧几里得性质$\Leftrightarrow\forall x\forall y\forall z(xRy\wedge xRz\rightarrow yRz)$

R 有菱形性质$\Leftrightarrow\forall x\forall y\forall z(xRy\wedge xRz\rightarrow\exists w\,(yRw\wedge zRw))$

证明：

（1）如果 R 自反且循环，则 R 对称且传递。

（2）如果 R 自反且有欧几里得性质，那么 R 是对称的。

（3）如果 R 对称且有欧几里得性质，那么 R 是传递的。

（4）如果 R 对称且传递，那么 R 具有欧几里得性质。

（5）如果 R 自反且具有欧几里得性质，那么 R 具有菱形性质。

11.（1）有人说：如果 R 对称且传递，那么 R 必自反，因为由 R 对称可知 xRy 蕴涵 yRx，而由 R 传递及 xRy，yRx，可知 xRx 。

（2）有人说：如果 R 反自反且传递，那么 R 必定是反对称的，因为若 R 不反对称可知有 $x\neq y$ 使 xRy 且 yRx，而由 R 传递及 xRy，yRx，可导出 xRx，从而得到矛盾。

你认为他们的结论和理由能够成立吗？为什么？

12. 证明：当关系 R 传递且自反时，$R^2=R$。

13. 证明：若集合 A 上关系 $R1$，$R2$，满足 $R1\subseteq R2$，那么对任一 A 上关系 $R3$，有

$$R1\circ R3\subseteq R2\circ R3$$

$$R3\circ R1\subseteq R3\circ R2$$

14. 设 R 为集合 A 上任一关系，求证对一切正整数 n，有

$$(E_A\cup R)^n=E_A\cup\bigcup_{i=1}^{n}R^i$$

15. 称 A 上关系 R 是**反传递**的，如果

$$\forall x\forall y\forall z\,(xRy\wedge yRz\rightarrow\neg\,xRz)$$

证明：R 是反传递的当且仅当 $R^2\cap R=\varnothing$

16. 设 $A=\{1,2,3,4,5\}$，A 上关系 $R=\{<1,2>,<3,4>,<2,2>\}$，$S=\{<4,2>,<2,5>,<3,1>,<1,3>\}$。试求 $R\circ S$ 的关系矩阵。

17. 设 $A=\{1,2,3,4\}$，A 上关系 $R=\{<1,4>,<3,1>,<3,2>,<4,3>\}$。求各 R 的幂的关系矩阵。

18. $<$ ，$\leqslant$ ，$\neq$，$\varnothing$，E_I 分别表示整数集 I 上的“小于关系”、“小于等于关系”、“不等关系”、“空关系”和“相等关系”，求：

（1）$r(<)$ ，$s(<)$，$t(<)$

（2）$r(\leqslant)$，$s(\leqslant)$，$t(\leqslant)$

（3）$r(\neq)$，$s(\neq)$，$t(\neq)$

（4）$r(\varnothing)$，$s(\varnothing)$，$t(\varnothing)$

（5）$r(E_I)$，$s(E_I)$，$t(E_I)$

19. 设 $R1$，$R2$ 为 A 上关系，$R1\subseteq R2$，求证：

（1）$r(R1)\subseteq r(R2)$

（2）$s(R1) \subseteq s(R2)$

（3）$t(R1) \subseteq t(R2)$

20. 设 $R1$，$R2$ 为 A 上关系，证明

（1）$r(R1 \cup R2) = r(R1) \cup r(R2)$

（2）$s(R1 \cup R2) = s(R1) \cup s(R2)$

（3）$t(R1 \cup R2) \supseteq t(R1) \cup t(R2)$

（4）对 $t(R1 \cup R2) = t(R1) \cup t(R2)$举出反例。

21. $t(R) = \bigcup_{i=1}^{n} R^i$ 中 n 是不可减小的。试举出 n 个元素的集合 A 及 A 上的关系 R，使 R，R^2，R^3，…，R^n是两两不交的（交为空），以说明这一点。

22. “找出三个元素的集合 A 和 A 上关系 R，使 R，R^2，R^3，R^4两两不等”是可能的吗？如可能请具体作出，并说明这一现象与 $t(R) = \bigcup_{i=1}^{n} R^i$不矛盾。

23. 设 R 为集合 A 上任一关系，$R^+ = t(R)$, $R^* = R^+ \cup E_A$，求证：

（1）$(R^+)^+ = R^+$

（2）$R \circ R^* = R^+ = R^* \circ R$

（3）$(R^*)^* = R^*$

24. 设 $A = \{1, 2, 3, 4\}$，问 A 上共有多少等价关系？

25. 设 R_1，R_2，…，R_n均为 A 上等价关系，证明$\bigcap_{i=1}^{n} R_i$ 也是 A 上等价关系。

并举例说明 R_1，R_2 为 A 上等价关系，而 $R1 \cup R2$ 不一定是 A 上等价关系。

26. 设∑为一字母表，R 为∑*上的二元关系，且满足

$$xRy \text{ 当且仅当 } \exists u\,(u \in \Sigma^* \wedge xu = uy)$$

证明：R 为∑*上的等价关系。

27. 设 R 为 A 上二元关系，称 R 为**连续的**，如果对每一 $a \in A$ 均有 $b \in A$ 使 aRb。

证明：当 R 连续、对称、传递时，R 为等价关系。

28. 求证：R 为等价关系当且仅当 R 是自反的和循环的。

29. 令 $C = \{a+bi \mid a,b \text{ 为实数}, a \neq 0\}$，定义 C 上关系 R：

$$(a+bi)R\,(c+di) \text{ 当且仅当 } ac > 0$$

证明：R 为等价关系，并利用复平面说明 R 所对应的划分。

30. 设 R 为 A 上二元关系，且 Dom $(R) = A$。若 $R \circ R^{\smile} \circ R = R$，证明 $R \circ R^{\smile}$和 $R^{\smile} \circ R$ 都是 A 上的等价关系。

31. 设 R 为 A 上的等价关系，证明：

$$R^{\smile} \circ R = R \circ R^{\smile} = R^{\smile}$$

32. 设$\{A_1, \cdots, A_m\}$为集合 A 的划分，证明：对任意集合 B，$\{A_1 \cap B, A_2 \cap B, \cdots, A_m \cap B\} - \{\varnothing\}$必为集合 $A \cap B$ 的划分。

33. 设 $A = \{1, 2, 3, 4, 5, 6\}$，A 有划分

$\pi_1 = \{\{1, 2, 3\}, \{4, 5, 6\}\}$

$\pi_2 = \{\{1, 2\}, \{3, 4\}, \{5, 6\}\}$

求 $\pi_1 \cdot \pi_2$，$\pi_1 + \pi_2$，及 π_1，π_2, $\pi_1 \cdot \pi_2$, $\pi_1 + \pi_2$所对应的等价关系。

34．试给出一个整数集合上的等价关系，使其所对应的划分恰由两个单元所组成，而每个单元都是整数集合的无穷子集。

35．设 $R1$ 表示整数集上模 $k1$ 相等关系，$R2$ 表示模 $k2$ 相等关系，π_1，π_2 分别是 $R1$，$R2$ 对应的划分。

（1）证明：π_1 细于 π_2 当且仅当 $k1$ 是 $k2$ 的倍数。

（2）当 $k1$ 是 $k2$ 的倍数时，求 $\pi_1 \cdot \pi_2$，$\pi_1 + \pi_2$。

36．设整数集上关系 $R1$，$R2$，$R3$ 分别是$\equiv_3$，$\equiv_5$，$\equiv_6$ 关系，试写出 $R1$，$R2$，$R3$ 对应的划分 π_1, π_2, π_3，并计算 $\pi_1 \cdot \pi_2, \pi_1 \cdot \pi_3, \pi_1 + \pi_2, \pi_1 + \pi_3$。

37．设 R 是集合 A 上的一个等价关系，$\{A_1, A_2, \cdots, A_k\}$为 A 的子集族，且对任意 $x, y \in A$ 满足

$$xRy \Leftrightarrow \exists i(1 \leqslant i \leqslant k \wedge x \in A_i \wedge y \in A_i)$$

问：可否断定$\{A_1, A_2, \cdots, A_k\}$为 A 的一个划分，若可以，请证明它确为 A 的划分；若不可，请补充适当条件，以使上述断言成立。

38．设 R，S 为 A 上的两个等价关系，且 $R \subseteq S$。定义 A/R 上的关系 R/S：

$$<[x],[y]> \in R/S \text{ 当且仅当} <x, y> \in S$$

证明：R/S 为 A/R 上的等价关系。

39．列表（表 10-3）区分有序集$<A, \leqslant>$的子集 B 上的最大、最小元，极大、极小元，上界、下界和上确界、下确界。

表 10-3

b 是 B 的…	定　义	$b \in B$ 否	存 在 性	唯 一 性
最大元				
最小元				
极大元				
极小元				
上　界				
下　界				
上确界				
下确界				

40．图 10-12 为一有序集$<A, R>$的哈斯图。

（1）下列命题哪些为真？

aRb，dRa，cRd，cRb，bRe，aRa，eRa；

（2）恢复 R 的关系图。

（3）指出 A 的最大、最小元（如果有的话），极大、极小元。

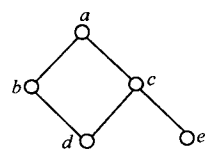


图 10-12

（4）求出子集 $B1=\{c,d,e\}$，$B2=\{b,c,d\}$，$B3=\{b,c,d,e\}$的上界、下界，上确界、下确界（如果有的话）。

41．对下列每一条件构造满足该条件的有限集和无限集各一个。

（1）非空有序集，其中有子集没有最大元素。

（2）非空有序集，其中有子集有下确界，但它没有最小元素。

（3）非空有序集，其中有一子集存在上界，但它没有上确界。

42. 图 10-13 给出了 4 个关系图。请指出哪些是序关系图，哪些是全序关系图，哪些是良序关系图，并对序关系图画出对应的哈斯图。

43. 下列集合中哪些是半序集合，哪些是有序集合，哪些是全序集合，哪些是良序集合？

（1）$<\rho(N), \subseteq>$　　（2）$<\rho(N), \subset>$

（3）$<\rho\{a\}, \subseteq>$　　（4）$<\rho(\varnothing), \subseteq>$

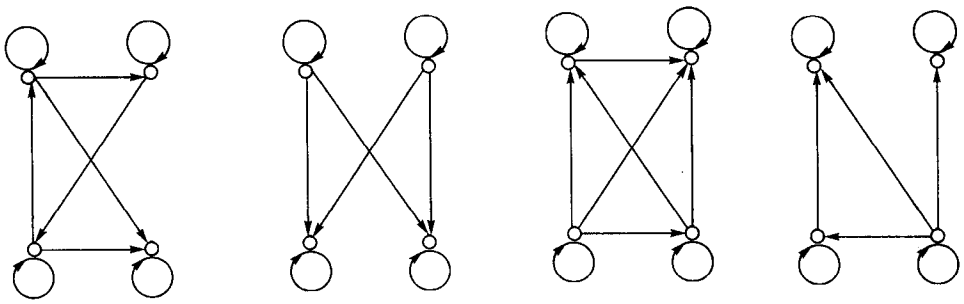


图　10-13

44. 证明：当 R 为 A 上的序关系（全序关系）时，$R^{\sim}$亦为 A 上的序关系（全序关系）。用反例说明，R 为 A 上良序关系并不蕴涵 $R^{\sim}$为 A 上良序关系。

45. 证明：定理 10-25 的证明中，有序集 $\langle A-M, \leqslant\rangle$ 不可能有长度为 n 的链。

46. 设 x，y 为自然数，$<x, y>$决定的矩形是指笛卡尔直角坐标系第一象限四点$<0, 0>$，$<x, 0>$，$<0, y>$，$<x, y>$所构成的矩形。证明：第一象限五点$<x1, y1>$，$<x2, y2>$，$<x3, y3>$，$<x4, y4>$，$<x5, y5>$所决定的五个矩形中，或者有三个矩形 $R1$，$R2$，$R3$，使 $R1$ 在 $R2$ 内，$R2$ 又在 $R3$ 内；或者有三个矩形，它们中没有任何一个矩形包含在另一个之中（见图 10-14 提示，利用定理 10-26）。

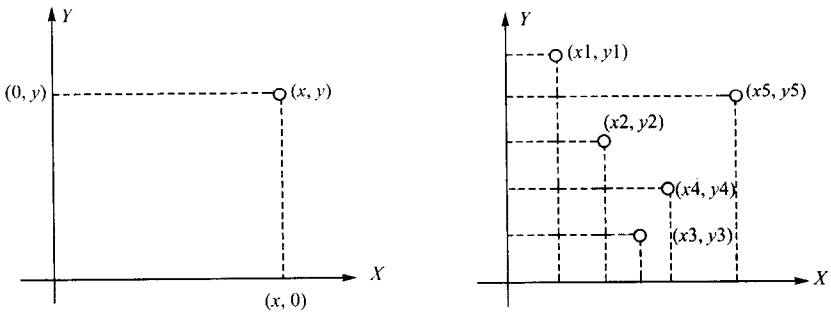


图　10-14

47. 证明：10.3.3 中定义的关系$\leqslant_{II}$不是良序。

48. 设 R 是集合 S 上的关系，$S' \subseteq S$，定义 S' 上的关系 R'如下：

$$R' = R \cap (S' \times S')$$

确定下述各断言的真假：

（1）如果 R 传递，则 R'传递。

（2）如果 R 为序关系，则 R'也是序关系。

（3）如果$<S, R>$为全序集，则$<S', R'>$，也是全序集。

（4）如果$<S, R>$为良序集，则$<S', R'>$，也是良序集。

49．设$<A, \leqslant>$为一有限全序集，$|A| \geqslant 2$，R 是 $A \times A$ 上的关系，根据 R 下列各定义，确定$<A \times A, R>$是否为半序集、有序集、全序集或良序集。设 x，y，u，v 为 A 中任意元素。

（1）$<x, y>R<u, v> \Leftrightarrow x \leqslant u \wedge y \leqslant v$

（2）$<x, y>R<u, v> \Leftrightarrow x \leqslant u \wedge x \neq u \vee (x = u \wedge y \leqslant v)$

（3）$<x, y>R<u, v> \Leftrightarrow x \leqslant u$

（4）$<x, y>R<u, v> \Leftrightarrow x \leqslant u \wedge x \neq u$

50．证明：$\{<A_i, R_i> | i \in D\}$中所有有序集的笛卡儿积$<\prod_{i \in D} A_i, R>$为有序集。R 由定义 10-21 确定。

51．设 K 是$<R, \leqslant>$的子集，R 为实数集，$\leqslant$为小于等于关系。证明 u 是 K 的上确界，当且仅当以下两个条件得到满足：

（1）对每一 $k \in K$，$k \leqslant u$。

（2）对任意正数ε，存在 $y \in K$，使 $u - \varepsilon \leqslant y$。

52．设$<M, R>$，$<M, S>$为两链（全序集）。问：在什么条件下$<M, R \circ S>$也为一链。

*53．证明：$<\rho(N), \subseteq>$不是良基的。

*54．证明：$<\rho_f(N), \subseteq>$是良基的，其中 $\rho_f(N) = \{X | X \subseteq N \wedge X$ 为有限集$\}$。

第11章 函 数

函数是大多数读者耳熟能详的一个重要概念。在初中数学中，'函数定义为“对自变量每一确定值都有一确定的值与之对应”的因变量；在高中数学中，函数又被定义为两个集合的元素之间的映射。现在，我们要对后一个定义作进一步的深化，像处理关系那样，用一个集合来具体规定映射，称这个集合为函数，从而将函数归结为集合、归结为关系的特例来研究。

函数概念是最基本的数学概念之一，也是最重要的数学工具。本章除了介绍离散对象之间的函数关系的一般概念、表示形式和主要性质外，还将介绍函数在无限集合理论研究中的许多应用。连同今后第12章的讨论，读者将会清晰地看到，离散对象之间的函数关系在计算机科学研究中极其重要的地位。事实上，函数概念在以后的所有各章（第12章至第15章）里都将扮演重要的角色。

11.1 函数及函数的合成

这一小节介绍离散对象之间函数（偏函数）关系的一般概念、表示形式和函数之间的合成运算（操作）。

11.1.1 函数的基本概念

定义 11-1 设 X，Y 为集合，称 f 为 X 到 Y 的**函数**（functions），记为 f：$X\to Y$，如果 f 为 X 到 Y 的关系（$f\subseteq X\times Y$），且对每一 $x\in X$，都有惟一的 $y\in Y$，使 $<x,y>\in f$。当 $X=X_1\times\cdots\times X_n$ 时，称 f 为 n 元函数。函数也称**映射**（mapping）或**变换**（transformation）。

换言之，函数是特殊的关系，它满足

（1）前域与定义域重合。

（2）若 $<x,y>\in f$，$<x,y'>\in f$，则 $y=y'$（单值性）。

根据函数的上述第二个特性，人们常把 $<x,y>\in f$ 或 xfy 这两种关系表示形式，在 f 为函数时改为 $y=f(x)$。这时称 x 为**自变元**，y 为函数在 x 处的**值**；也称 y 为 x 的**像点**，x 为 y 的**源点**。注意，函数的上述表示形式不适用于一般关系，因为对关系 R，可能有 $<x,y_1>\in R$，$<x,y_2>\in R$，但 $y_1\neq y_2$。若采用 $y_1=R(x)$，$y_2=R(x)$的表示方法，将产生 $y_1=R(x)=y_2$ 的矛盾。

【例 11-1】

（1）任意集合 A 上的相等关系 E_A 为一函数，常称为**恒等函数**（identical functions，也常用 I_A 表示之），因为 $E_A(x)=x$（对任意 $x\in A$）。

（2）自然数集合上的二倍关系为一函数，若用 f 表示这一关系，那么 $f:N\to N$，$y=f(x)=2x$。

（3）自然数集合上的整除关系不是函数，因为 $0\in N$，而对任意 $x\in N$，0 不整除 x。即使在正整数集合上，整除关系仍不是函数，因为有 $x\in N$，例如 2，2|4，2|8，但 $4\neq 8$。

（4）当 $X=\varnothing$时，X 到 Y 的空关系为一函数，称为空函数。当 $X\neq\varnothing$时，X 到 Y 的空关系不是一个函数。

（5）$Add:N\to N$，$y=Add\,(x1,x2)\ =x1+x2$ 为自然数集上的二元加函数。

通常用以下三种方法规定函数：

（1）列表法：由于函数具有“单值性”，即对任一自变量有惟一确定的函数值，因此可将其序偶排列成一个表，将自变量与函数值一一对应起来。列表法一般适用于定义域为有限集合的情况。

（2）图标法：用笛卡儿平面上点的集合表示函数。图标法一般适用于定义域有限的情况。

（3）解析法：用等式 $y=f(x)$表示函数，这时可认为 $y=f(x)$为函数的“命名式”，有别于“y 是 f 在 x 处的值”。$y=f(x)$的这种意义的双重性，与谓词表达式类似，读者可依据上下文加以区别。

【例 11-2】 设 $A=\{-3, -2, -1, 0, 1, 2, 3\}$，$f$: $A\to A$ 为绝对值函数，即 $y=|x|$，它可以用三种方法规定如下：

（1）列表法：

x	-3	-2	-1	0	1	2	3
$f(x)$	3	2	1	0	1	2	3

（2）图标法：（见图 11-1）

（3）解析法：

$$y=|x|=\begin{cases} x & x\geqslant 0 \\ -x & x<0 \end{cases}$$

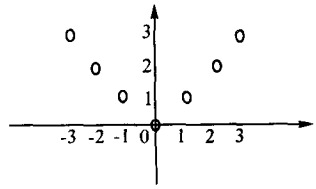


图 11-1

事实上，还可以递归地定义函数。关于这一点，稍后再细谈，我们还将用几乎整整一章（第 12 章）来讨论递归定义的函数。

由于函数归结为关系，因而函数相等的概念、函数包含概念，也便归结为关系相等的概念及关系包含概念。

定义 11-2 设 f:$A\to B$，g:$C\to D$，称函数 f 等于 g，记为 $f=g$，如果 $A=C$，$B=D$，且对每一 $x\in A$，$f(x)=g(x)$。

称函数 f 包含于 g，记为 $f\subseteq g$，如果 $A\subseteq C$，$B=D$，且对每一 $x\in A$，$f(x)=g(x)$。

定义中 $B=D$ 的要求不是本质的，或者说是无关紧要的。

定理 11-1 设 $|X|=m$，$|Y|=n$，那么 $\{f\mid f: X\to Y\}$ 的基数为 n^m。即共有 n^m 个 X 到 Y 的函数。

证明 设 $X=\{x_1,\cdots,x_m\}$，$Y=\{y_1,\cdots,y_n\}$，那么每一个 $f: X\to Y$ 由一张如下的表来规定：

x	x_1	x_2	…	x_m
$f(x)$	y_{i1}	y_{i2}	…	y_{im}

其中 y_{i1}，y_{i2}，…，y_{im} 为取自 y_1，y_2，…，y_n 的允许元素重复的排列，这种排列总数为 n^m 个。因此，上述形式的表恰有 n^m 张，恰对应全部 n^m 个 X 到 Y 的函数。

由于上述缘故，A 到 B 的全体函数的集合常用记号 B^A 表示之，即

$$B^A=\{f\mid f: A\to B\}$$

特别地 A^A 表示 A 上函数的全体。目前在计算机科学中，也用 $A\to B$ 替代 B^A。

关于函数的下列术语和记号是常用的。

定义 11-3 设 $f: X \to Y$，$A \subseteq X$，称 $f'(A)$ 为 A 的**映像**（image），定义为

$$f'(A) = \{y \mid \exists x (x \in A \wedge y = f(x))\}$$

显然，f' 为 $\rho(X)$ 到 $\rho(Y)$ 的函数，且

$$f'(\varnothing) = \varnothing, f'(X) = \mathrm{Ran}(f), f'(\{x\}) = \{f(x)\} \ (x \in A)$$

关于 f' 的下列事实是容易掌握的。

定理 11-2 设 $f: X \to Y$，对任意 $A \subseteq X$，$B \subseteq X$，有

（1）$f'(A \cup B) = f'(A) \cup f'(B)$

（2）$f'(A \cap B) \subseteq f'(A) \cap f'(B)$

（3）$f'(A) - f'(B) \subseteq f'(A - B)$

证明 （1）对任一 $y \in Y$，有

$$\begin{aligned} y \in f'(A \cup B) &\Leftrightarrow \exists x (x \in A \cup B \wedge y = f(x)) \\ &\Leftrightarrow \exists x ((x \in A \wedge y = f(x)) \vee (x \in B \wedge y = f(x))) \\ &\Leftrightarrow \exists x (x \in A \wedge y = f(x)) \vee \exists x (x \in B \wedge y = f(x)) \\ &\Leftrightarrow y \in f'(A) \vee y \in f'(B) \\ &\Leftrightarrow y \in f'(A) \cup f'(B) \end{aligned}$$

因此 $f'(A \cup B) = f'(A) \cup f'(B)$。

（2），（3）的证明请读者完成。注意，（2），（3）中的包含符号不能用等号代替。下例是一明证。

【例 11-3】 设 $X = \{a,b,c,d\}$，$Y = \{1,2,3,4,5\}$，$f: X \to Y$，如图 11-2 所示。那么

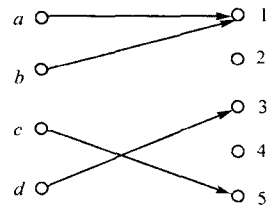


图 11-2

$$f'(\{a\}) = \{1\}, f'(\{b\}) = \{1\}, f'(\{a\}) \cap f'(\{b\}) = \{1\}$$

$$f'(\{a\}) - f'(\{b\}) = \varnothing$$

$$f'(\{a\} \cap \{b\}) = f'(\varnothing) = \varnothing, f'(\{a\} - \{b\}) = f'(\{a\}) = \{1\}$$

$$f'(\{a\} \cap \{b\}) \subset f'(\{a\}) \cap f'(\{b\})$$

$$f'(\{a\}) - f'(\{b\}) \subset f'(\{a\} - \{b\})$$

注意，不少书籍上 $f'(A) = \{f(x) \mid x \in A\}$ 的写法是不适当的，因为这意味着

$$f(x) \in f'(A) \Leftrightarrow x \in A$$

但它是与 f' 的定义不合的，由 $f(x) \in f'(A)$ 并不能确定 $x \in A$。上例中 $f(b) = 1 \in f'(\{a\})$，但 $b \notin \{a\}$。

*11.1.2 函数概念的拓广

在实际应用中常常遇到这样一种情况，g 为 X 到 Y 的关系，又是 A 到 Y 的函数，$A \subseteq X$，且对某些 $x \in X - A$，$g(x)$ 没有意义，但是却又需要在 X 上讨论 g。为此人们引入偏函数概念来拓广函数的意义。

定义 11-4 设 $f \subseteq X \times Y$，称 f 为 X 到 Y 的一个**偏函数**（partial functions），如果 f 满足下列条件：对任意 $x \in X$，$y1$，$y2 \in Y$，若 $\langle x, y1 \rangle \in f$，$\langle x, y2 \rangle \in f$，则 $y1 = y2$。

换言之，偏函数的定义从函数的定义中取消了定义域等于前域的要求，保留了单值性要求。对于 $x \in X$，若无 $y \in Y$，使 $\langle x, y \rangle \in f$ 时，称 f 在 x 处**无定义**。

据定义 11-4 可知，一切函数均为偏函数，但反之不然。当 f 为偏函数却非函数时，称 f

为**真偏函数**。

【例 11-4】

（1）$y=f(x)=\sqrt{x}$，$y=g(x1,x2)=\dfrac{x1}{x2}$ 规定的 f，g 都是实数集合上的真偏函数。

（2）当 $Y=\varnothing$，$X\neq\varnothing$ 时，X 到 Y 的空关系为一真偏函数。

（3）下列 Pascal 程序也定义了一个真偏函数：

```
function f (x:integer) : integer
var y : integer
begin
y :=1
while(x< >0)
    begin
    x :=x − 2
    y :=y * 2
    end
f :=y
end
```

容易明白

$$f(x)=\begin{cases}2^{\frac{x}{2}} & x\text{为非负偶数}\\ \text{无定义} & \text{否则}\end{cases}$$

在作函数理论研究时，可以直接讨论偏函数，但更多的是使用扩充和限制，将真偏函数转化为函数来加以讨论。

定义 11-5 设 f 为 A 到 Y 的偏函数，g 为 X 到 Y 的偏函数，$A\subseteq X$，且对每一 $x\in A$，$f(x)=g(x)$（即 $f\subseteq g$），那么称偏函数 g 为 f 的**扩充**（extention），称偏函数 f 为 g 在 A 上的**限制**（restriction），特记为 $f\upharpoonright_A$。

如果 f 为一真偏函数，那么当对 f 的每一无定义处规定一个值（补充定义），可构造出 f 的一个扩充，它是一个函数。反之，如果 g 为一真偏函数，那么将 g 限制在它前域有定义的子集上，同样可构造一个函数。

【例 11-5】 对例 11-4（1）中 $y=f(x)=\sqrt{x}$，$y=g(x1,x2)=\dfrac{x1}{x2}$ 规定：

$f(x)=0$ 当 $x<0$；$g(x1,0)=\dfrac{x1}{0}=0$

后所得的 f，g 均为实数集上的函数。反之，将 f 限制于非负实数集合，将 g 限制于非零实数集合，都可以得到相应的函数。

显然，当 f 为 g 的扩充时，g 为 f 的限制。当 f 为 X 到 Y 的函数，$A\subseteq X$ 时，

$$f'(A)=\mathrm{Ran}\,(f\upharpoonright_A)$$

下面的例子表明，限制不仅可以由真偏函数产生函数，还可以使某些函数的某些问题的讨论成为可能。

【例 11-6】

（1）例 11-4 中偏函数 f，g 的限制

$$f\upharpoonright_{R+\cup\{0\}},\quad g\upharpoonright_{R\times R-\{0\}}$$

都是函数。

（2）令函数$f=\{<\varnothing,a>,<\{\varnothing\},a>\}$，那么

$$f\upharpoonright_{\varnothing}=\varnothing,f\upharpoonright_{\{\varnothing\}}=\{<\varnothing,a>\},f\upharpoonright_{\{\{\varnothing\}\}}=\{<\{\varnothing\},a>\},$$

后两个限制的逆仍为函数，但$f^{\sim}$不是函数。

（3）实数集上的三角函数在一定区间上的限制，对于反三角函数的讨论是至关重要的。arcsin，arccos，arctg，arcctg，其实都不是 sin,cos,tg,ctg 的反函数（它们不可能有反函数），而是$\sin\upharpoonright_{[-\pi/2,\pi/2]}$，$\cos\upharpoonright_{[0,\pi]}$，$\mathrm{tg}\upharpoonright_{[-\pi/2,\pi/2]}$，$\mathrm{ctg}\upharpoonright_{[0,\pi]}$的反函数。

11.1.3 函数的合成

作为关系，函数合成的讨论是顺理成章的。

定义 11-6 设$f:X\to Y$，$g:Y\to Z$，那么称$f\circ g$为函数f和g的合成函数。

$f\circ g$为X到Z的一个关系是显然的，但它是否是X到Z的函数呢？也就是说，定义 11-6 是否是良定的呢？下述定理作了肯定的回答。

定理 11-3 设$f:X\to Y$，$g:Y\to Z$，那么合成关系$f\circ g$为X到Z的函数。

证明 首先证明 Dom($f\circ g$)=X。对任一$x\in X$，有$y\in Y$，使$<x,y>\in f$；对这一y，有$z\in Z$，使得$<y,z>\in g$，因此$<x,z>\in f\circ g$。故$x\in$ Dom($f\circ g$)。Dom ($f\circ g$)=X得证。

再证$f\circ g$的单值性。设对x有$z1,z2$，使$<x,z1>\in f\circ g$，$<x,z2>\in f\circ g$。那么有$y1,y2$，使$<x,y1>\in f$，$<y1,z1>\in g$，$<x,y2>\in f$,$<y2,z>\in g$。由于f为函数，知$y1=y2$；又因g为函数，得知$z1=z2$。$f\circ g$为X到Z的函数得证。

我们注意到$<x,z>\in f\circ g$意指：有y使$<x,y>\in f$，$<y,z>\in g$，即$y=f(x)$，$z=g(y)=g(f(x))$，因而

$$f\circ g\,(x)=g(f(x))$$

这就是说，当f,g为函数时，它们的合成函数作用于自变量的次序刚好与合成的原始记号的顺序相反。为了改变这种不自然，在讨论函数时，函数f与g的合成写作$g\circ f$（而不把它们看作关系的合成而写作$f\circ g$），从而对任意$x\in$ Dom(f)，有

$$g\circ f\,(x)=g(f(x))$$

我们约定，函数f与g合成时，只有当函数f的陪域与函数g的定义域相同时，它们的合成$g\circ f$才有意义。当这一条件不满足时，可利用函数g的限制与扩充来弥补。

【例 11-7】

（1）设$X=\{a,b,c,d\}$，$Y=\{\alpha,\beta,\gamma,\delta\}$，$Z=\{a,b,c\}$，$f:X\to Y$，$g:Y\to Z$，由图 11-3a、b 分别给出，那么，图 11-3c 表示$g\circ f$。由于$Z\neq X$，$f\circ g$是没有意义的，但$Z\subset X$，g与$f\upharpoonright_Z$的合成$f\upharpoonright_Z\circ g$为一$Y$到$Y$的函数，由图 11-3d 给出。

（2）设f，g均为实函数，$f(x)=2x+1$，$g(x)=x^2+1$，那么

$$f\circ g(x)=f(g(x))=2(x^2+1)+1=2x^2+3$$

$$g\circ f(x)=g(f(x))=(2x+1)^2+1=4x^2+4x+2$$

$$f\circ f(x)=f(f(x))=2(2x+1)+1=4x+3$$

$$g\circ g(x)=g(g(x))=(x^2+1)^2+1=x^4+2x^2+2$$

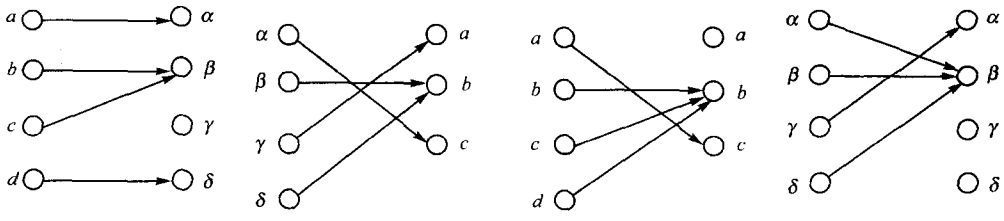


图 11-3

a) f b) g c) $g\circ f$ d) $f\uparrow_Z\circ g$

同关系的合成运算一样，函数的合成运算不满足交换律，但满足结合律，即

设 $f:X\to Y$，$g:Y\to Z$，$h:Z\to D$，则

$$h\circ(g\circ f)=(h\circ g)\circ f$$

因对任意 $x\in \mathrm{Dom}(f)$，有

$$\begin{aligned} h\circ(g\circ f)(x) &= h((g\circ f)(x)) \\ &= h(g(f(x)) \\ &= (h\circ g)(f(x)) \\ &= (h\circ g)\circ f(x) \end{aligned}$$

函数合成的下列性质是明显的：

对 $f:X\to Y$，

$$f\circ E_X=E_Y\circ f=f$$

由于函数的合成满足结合律，n 个函数 f 的合成可记为 f^n，常称为 f 的 n 次**迭代**。显然

$$\begin{cases} f^0(x)=x \\ f^{n+1}(x)=f(f^n(x)) \end{cases}$$

【例 11-8】

（1）设 f 为 N 上的后继函数，即 $f(x)=x+1$，那么 $f^y(x)=x+y$。这表明，当把合成运算强化地运用于变元（合成次数），它就成为一种有力的构造新函数的手段。

（2）设 $f:X\to X$，$X=\{a,b,c\}$。若 $f(a)=b$，$f(b)=b$，$f(c)=c$，那么 $f^2=f$。这时常称 f 是等幂的。

11.1.4 函数的递归定义

有了函数合成这一工具，我们便可以来讨论另一重要的构造函数的手段，即函数的递归定义。首先，函数既然是关系，又是序偶的集合，就可以用归纳的方式来定义。

例如自然数集上的二元加函数 Add（三元关系）可归纳定义如下：

（1）（基础条款）$<0,0,0>\in \mathrm{Add}$

（2）（归纳条款）若 $<x,y,z>\in \mathrm{Add}$，那么

$$<x+1,y,z+1>\in \mathrm{Add}$$

$$<x,y+1,z+1>\in \mathrm{Add}$$

（3）（终极条款）略。

注意，归纳过程中，后继函数被用作了已知函数。

如果再把上述条款改写成等式，便得到一组由已知的被定义函数值计算未知的被定义函数值的等式：

$$\begin{cases} Add(0,0)=0 \\ Add(x+1,y)=Add(x,y)+1 \\ Add(x,y+1)=Add(x,y)+1 \end{cases}$$

如果又将 x 看作参数，那么它们又可以改写为

$$\begin{cases} Add(x,0)=x \\ Add(x,y+1)=Add(x,y)+1 \end{cases} \tag{11-1}$$

式（11-1）称为二元加函数 A 的**递归定义式**。像式（11-1）这样，给出被定义函数在某些自变量处的值（所谓初值），又给出由已知的被定义函数值逐步计算未知的被定义函数值的规则，来规定一个函数的方式，称为函数的**递归定义**（recursive definitions）。

【例 11-9】 下列函数都是递归定义的：

（1）字长函数 l：$\Sigma^*\to N$。

$$\begin{cases} l(\lambda)=0 \\ l(w\xi)=l(w)+1 \quad (w\in\Sigma^*,\xi\in\Sigma) \end{cases}$$

（2）麦卡锡（McCarthy）91 函数 Mc：$N\to N$。

$$\begin{cases} \mathrm{Mc}(x)=x-10 & \text{当 } x>100 \\ \mathrm{Mc}(x)=Mc(Mc(x+11)) & \text{当 } x\leqslant 100 \end{cases}$$

（可证：当 $x\leqslant 100$ 时，$\mathrm{Mc}(x)=91$）

由上述例子可以看出，递归定义方式相当有力而又复杂，这就产生了一个问题，是否递归定义方式总能确定一个函数呢？回答是否定的。

【例 11-10】 设 $\Sigma=\{a,b,c\}$，Σ^+ 如下归纳地定义：

（1）$\Sigma\subseteq\Sigma^+$

（2）若 $w1\in\Sigma^+$，$w2\in\Sigma^+$，那么 $w1w2\in\Sigma^+$。

（3）略。

现递归地定义 f：$\Sigma^+\to N$ 如下：

$$\begin{cases} f(a)=2,f(b)=1,f(c)=0 \\ f(w1w2)=f(w1)^{f(w2)} \end{cases}$$

那么

$$f(abc)=f(ab)^{f(c)}=f(a)^{f(b)\cdot f(c)}=2^0=1$$

$$f(abc)=f(a)^{f(bc)}=f(a)^{f(b)^{f(c)}}=2^1=2$$

因而 f 不是一个函数。

问题出在哪儿呢？出在 Σ^+ 的归纳定义上。当归纳条款允许由不同方式从已知元素产生新元素时（abc 可由 $w1=ab$，$w2=c$ 及 $w1=a$，$w2=bc$ 两种方式生成），于该归纳定义之集合上建立的递归定义未必能确定一个函数。由于自然数的归纳定义无上述弊病，因此例 11-9 所定义的函数都是适当的。我们容易明白，下述最常用的、最基本的、自然数集上函数的递归定义方式是适当的，即当已知 h 为自然数集上的函数时，它如下所定义的 f 也是自然数集

上的函数：

$$\begin{cases} f(0)=a \\ f(x+1)=h(x,f(x)) \end{cases}$$

计算理论的研究表明，递归定义是很强的一种函数定义手段。从若干简单的函数：后继函数、恒等函数、投影函数（$p_k\ (x_1, \cdots, x_n)=x_k,\ k=1,2, \cdots, n$）出发，可以用合成操作、求最小根操作和递归定义方式，构造出所有自然数集上的可计算函数，这是我们下一章要讨论的主题（参阅第 12 章）。

11.2 特殊函数类

11.2.1 单射的、满射的和双射的函数

如果从函数的最基本性质出发，可以讨论单射的、满射的和双射的函数类。

定义 11-7 设 f：$X\to Y$。

（1）称 f 为 X 到 Y 的**单射函数**，或**单射**（injection）、**内射**、**入射**，如果对任意 $x1$，$x2\in X$，$x1\neq x2$ 蕴涵 $f(x1)\neq f(x2)$。单射函数也称一对一的函数。

（2）称 f 为 X 到 Y 的**满射函数**，或**满射**（surjection），如果对任意 $y\in Y$，均有 $x\in X$，使 $y=f(x)$，即 $\mathrm{Ran}(f)=Y$。满射函数也称映上的函数。

（3）称 f 为 X 到 Y 的**双射函数**，或**双射**（bejection），如果 f 既是 X 到 Y 的单射，又是 X 到 Y 的满射。双射函数也称一一对应。

图 11-4 说明了这三类函数之间的关系。注意，既非单射又非满射的函数是大量存在的。

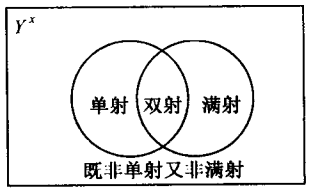


图 11-4

【例 11-11】 实数集上的指数函数 $y=2^x$ 是单射而非满射，多项式函数 $y=x^3-x$ 是满射而非单射，一次函数 $y=kx+b$ $(k\neq 0)$ 都是双射，但二次函数 $y=ax^2+bx+c$ $(a\neq 0)$既非单射，又非满射。

关于单射的、满射的和双射的函数有下列性质。

定理 11-4 设 f：$X\to Y$，g：$Y\to Z$，那么

（1）如果 f 和 g 是单射的，则 $g\circ f$ 也是单射。

（2）如果 f 和 g 是满射的，则 $g\circ f$ 也是满射的。

（3）如果 f 和 g 是双射的，则 $g\circ f$ 也是双射的。

证明 （1）设 $x1$，$x2\in X$，$x1\neq x2$，由于 f 为单射，故 $f(x1)\neq f(x2)$；又因为 g 也是单射，所以 $g(f(x1))\neq g(f(x2))$即 $g\circ f(x1)\neq g\circ f(x2)$。$g\circ f$ 为单射得证。

（2）为证 $g\circ f$ 为满射，设 z 为 Z 中任一元素。由于 g 为满射，因而有 $y\in Y$ 使 $g(y)=z$。对于这一 y，由于 f 为满射，又必有 $x\in X$ 使 $y=f(x)$。于是我们找到 x，使 $g(f(x))=z$，即 $g\circ f(x)=z$。$g\circ f$ 为满射得证。

（3）由（1），（2）立得。

本定理之逆是不能成立的。图 11-5a 中 $g\circ f$ 是单射，但 g 并非单射；b 中 $g\circ f$ 为满射，但 f 不是满射。

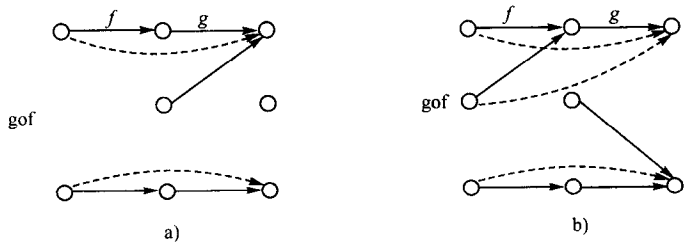


图 11-5

定理 11-4 之逆的一个弱形式是成立的。

定理 11-5 设 f：$X\to Y$，g：$Y\to Z$，那么

（1）若 $g\circ f$ 是单射，则 f 是单射。

（2）若 $g\circ f$ 是满射，则 g 是满射。

（3）若 $g\circ f$ 是双射，则 f 是单射，g 是满射。

证明 （1）设 $g\circ f$ 是单射，而 f 并非单射。那么有 $x1$，$x2\in X$，虽 $x1\neq x2$，但 $f(x1)=f(x2)$，从而

$$g\circ f(x1)=g(f(x1))=g(f(x2))=g\circ f(x2)$$

与 $g\circ f$ 为单射矛盾。因此 f 为单射。

（2），（3）的证明留给读者。

双射函数无疑是最为重要的一类函数。作为例子，我们介绍一种常见的双射函数——置换。

定义 11-8 设 X 为有限集，p：$X\to X$ 为一双射，那么称 p 为 X 上的**置换**（permutation）。当

$|X|=n$ 时，称 p 为 **n 次置换**。

置换常用一种特别的形式来表示。设 $X=\{a_1,\cdots,a_n\}$，那么

$$p=\begin{pmatrix}a_1,a_2,\ldots,a_n\\ a_{i1},a_{i2},\ldots,a_{in}\end{pmatrix}$$

表示一个 X 上的 n 次置换，它满足

$$p(a_j)=a_{ij}$$

X 上的恒等函数显然为一置换，称为么置换，用 i 表示之。

由于习惯上把置换的合成写得与一般函数合成次序相反，因而置换的合成的书写又回到了关系合成的书写次序。这种“返祖”的原因是，置换的表示方式与关系的序偶集合表示形式接近，这种书写次序便于进行合成运算。

显然，对任一集合 X 上的任一置换 p，有

$$p\circ i=i\circ p=\mathrm{p}$$

【例 11-12】 设 $X=\{1,2,3,4\}$，$p1,p2$ 为 X 上置换，

$$p1=\begin{pmatrix}1&2&3&4\\2&4&1&3\end{pmatrix},\quad p2=\begin{pmatrix}1&2&3&4\\3&4&2&1\end{pmatrix}$$

那么

$$p1\circ p2=\begin{pmatrix}1&2&3&4\\2&4&1&3\end{pmatrix}\circ\begin{pmatrix}1&2&3&4\\3&4&2&1\end{pmatrix}=\begin{pmatrix}1&2&3&4\\4&1&3&2\end{pmatrix}$$

$$p2\circ p1=\begin{pmatrix}1&2&3&4\\3&4&2&1\end{pmatrix}\circ\begin{pmatrix}1&2&3&4\\2&4&1&3\end{pmatrix}=\begin{pmatrix}1&2&3&4\\1&3&4&2\end{pmatrix}$$

$$p1\circ p2(2)=p2(p1(2))=p2(4)=1$$

$$p2\circ p1(2)=p1(p2(2))=p1(4)=3$$

* 11.2.2 规范映射、单调映射和连续映射

如果同等价关系、序关序一起讨论函数，那么规范映射、单调映射和连续映射是不可遗忘的，因为它们在抽象代数等诸多领域中有重要的应用，也可用于构作新的等价关系、划分和有序集。

定义 11-9 设 f：X→Y，称关系 ker(f)为函数 f 的核（kernel），定义为

$$\ker(f)=\{<x1,x2>\mid x1,x2\in X,\ \text{且}\ f(x1)=f(x2)\}$$

图 11-6 直观地说明了 $X/\ker(f)$的意义。

关于函数 f 的核 $\ker(f)$有如下的结论：

定理 11-6 设 f：$X\to Y$，那么 $\ker(f)$为 X 上的等价关系。

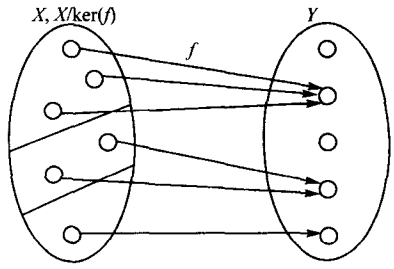


图 11-6

此定理的证明很容易，请读者自行完成。

于是我们可得到 X 的划分 $X/\ker(f)$。

定理 11-7 对任意函数 f：$X\to Y$，存在一个双射 h：$X/ker(f)\to Ran(f)$。

证明 作 h：$X/\ker(f)\to Ran(f)$，使得对任一 $X/\ker(f)$中的单元$[x]$(x 的等价类)

$$h([x])=f(x) \tag{11-2}$$

可证 h 为一函数。因若 $h([x])=f(x)$，$h([x])=f(x')$，那么 x，$x'\in[x]$；据 $X/\ker(f)$的定义，$f(x)=f(x')$，h 满足单值性。

现证 h 为单射。设 $h([x])=h([y])$，那么 $f(x)=f(y)$，因此$<x,y>\in\ker(f)$，故$[x]=[y]$。

h 为满射明显（读者自证）。

定理 11-7 中双射 h 常称为**规范映射**（canonical mapping）。规范映射在代数结构的讨论中有十分重要的地位。

定理 11-8 对任意函数 f：$X\to Y$，存在三个函数，g：$X\to X/\ker(f)$，h：$X/\ker(f)\to\text{Ran}(f)$，$k$：$\text{Ran}(f)\to Y$，使 g 为满射，h 为双射，k 为单射，且$f=k\circ h\circ g$。

证明 令

$g(x)=[x]$　　（对任意 x∈X）

$h([x])=f(x)$（对任意$[x]\in X/\ker(f)$）

$k(y)=y$（对任意 $y\in\text{Ran}(f)$）

于是对任一 $x\in X$，

$$k\circ h\circ g(x)=k\circ h([x])=k(f(x))=f(x)$$

图 11-7 直观地反映了定理 11-8 的含义。

与有序集相关的重要函数类是所谓单调映像和连续映射。

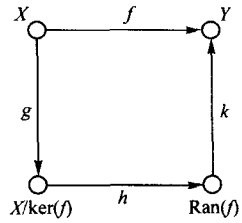


图 11-7

定义 11-10 设$<X, \leqslant_1>$，$<Y, \leqslant_2>$为有序集，称函数 f: $X\to Y$ 为 X 到 Y 的**单调映射**（monotonic mapping），如果对任意 $x1$，$x2\in X$ 满足

$$x1\leqslant_1 x2 \text{ 蕴涵 } f(x1)\leqslant_2 f(x2)$$

称 f 为 X 到 Y 的**严格单调映射**（monotonic mapping）如果对任意 $x1$，$x2\in X$，它满足

$$x1\leqslant_1 x2\wedge x1\neq x2 \text{ 蕴涵 } f(x1)\leqslant_2 f(x2)\wedge f(x1)\neq f(x2)$$

定理 11-9 设$<X, \leqslant_1>$，$<Y, \leqslant_2>$为有序集，f: $X\to Y$，g: $Y\to Z$ 为单调映射，那么 $g\circ f$ 为 X 到 Z 的单调映射。

证明是极容易的，请读者完成。

定理 11-10 设$<X, \leqslant_1>$，$<Y, \leqslant_2>$为有序集，$L\subseteq X$ 为 X 中的$\leqslant_1$链，f: $X\to Y$ 为单调映射，那么 $f'(L)$为 Y 中的$\leqslant_2$链。

证明同样是简单的。

定义 11-11 设$<X, \leqslant_1>$，$<Y, \leqslant_2>$为完备序集，称 f: $X\to Y$ 为**连续映射**（continuous mapping），如果对 X 中每一$\leqslant_1$链 L，$f'(L)$的上确界 $\sup f'(L)$存在且等于 $f(\sup L)$($\sup L$ 为 L 的上确界)。

定理 11-11 设$<X, \leqslant_1>$，$<Y, \leqslant_2>$为完备序集。若 f: $X\to Y$ 为连续映射，那么 f 必为 X 到 Y 的单调映射。

证明 设 $x1$, $x2\in X$，$x1\leqslant_1 x2$，$\sup\{x1, x2\}=x2$。由于 f 为连续映射，$\{f(x1)=y1, f(x2)=y2\}$ 有上确界，且 $\sup\{y1, y2\}=f(\sup\{x1, x2\})=f(x2)=y2$，故 $y1\leqslant_2 y2$。因此 f 必为单调映射。

定理 11-12 设$<X, \leqslant_1>$，$<Y, \leqslant_2>$为完备序集，f: $X\to Y$ 为单调映射，若对每一链 $L\subseteq X$，总有

$$f(\sup L)\leqslant_2 \sup f'(L) \tag{11-3}$$

那么 f 是一连续映射。

证明 首先，由定理 10-10 知 $f'(L)$为 Y 中$\leqslant_2$链，因此 $\sup f'(L)$在 Y 中存在（Y 为完备的）。另外，对任意 $x\in L$，我们有 $x\leqslant_1 \sup L$，从而据 f 单调性得

$$f(x)\leqslant_2 f(\sup L)$$

这表明 $f(\sup L)$是 $f'(L)$的一个上界，因此

$$\sup f'(L)\leqslant_2 f(\sup L) \tag{11-4}$$

式（11-3）与式（11-4）蕴涵 $f(\sup L)=\sup f'(L)$，这就是说 f 是连续的。

定理 11-13 设$<X, \leqslant_1>$，$<Y, \leqslant_2>$，$<Z \leqslant_3>$均为完备序集，f :$X\to Y$, g : $Y\to Z$ 都是连续映射，那么 $g\circ f$: $X\to Z$ 也是连续映射。

证明请读者来完成。

11.3 函数的逆

函数作为关系可以求取它的逆。对 f: $X\to Y$，$f^{\sim}\subseteq Y\times X$ 为 f 的逆关系，那么是否 $f^{\sim}$一定

是 Y 到 X 的函数呢？回答是否定的。容易知道，当 f 不是单射时，则 $f^{\sim}$ 无法满足单值性，而当 f 不是满射时，无法满足 $\mathrm{Dom}(f^{\sim})=Y$。因此，当 f 不是双射时，$f^{\sim}$ 就不再是一个函数了。但是，

定理 11-14 若 f：$X\to Y$ 为一双射，则关系 f 的逆关系 $f^{\sim}$ 为 Y 到 X 的函数，记为 f^{-1}，且 f^{-1}：$Y\to X$ 也为一双射。

证明 我们只证 f^{-1} 为一函数，而把 f^{-1} 为单射和满射的证明留给读者。

由于 f 为满射，因此对每一 $y\in Y$，有 $x\in X$，使 $f(x)=y$，从而 $<y,x>\in f^{-1}$，这表明 $\mathrm{Dom}(f^{-1})=Y$。为证 f^{-1} 的单值性，设 $y\in Y$，且 $<y,x1>\in f^{-1}$，$<y,x2>\in f^{-1}$，从而 $f(x1)=y=f(x2)$。据 f 的单射性，有 $x1=x2$。f^{-1} 的单值性证毕。故 f^{-1} 为 Y 到 X 的一个函数。

当 f 为一双射函数时，称 f^{-1} 为 f 的**逆函数**（inverse functions），称 f 是**可逆的**。

关于逆函数，下列事实是明显的。

定理 11-15 若 f：$X\to Y$ 是可逆的，那么

（1）$(f^{-1})^{-1}=f$

（2）$f^{-1}\circ f=E_X$，$f\circ f^{-1}=E_Y$

证明 （1）由定理 11-14 知 f^{-1} 为一双射，因而 f^{-1} 也是可逆的。故 $(f^{-1})^{-1}=(f^{-1})^{\sim\sim}=f$。

（2）设 x 为 X 中任一元素，$f(x)=y$，那么 $x=f^{-1}(y)$。由于 $f^{-1}\circ f(x)=f^{-1}(f(x))=f^{-1}(y)=x$，故 $f^{-1}\circ f=E_X$。同理可证 $f\circ f^{-1}=E_Y$。

定理 11-16 设 f：$X\to Y$，g：$Y\to Z$ 都是可逆的，那么 $g\circ f$ 也是可逆的，且

$$(g\circ f)^{-1}=f^{-1}\circ g^{-1}$$

证明留作练习。

我们已经强调，非双射函数不是可逆的，它没有逆函数。但是，对某些这样的函数，仍可找到与 f^{-1} 有相近性质的函数 g，使得

$$g\circ f=E_X \quad \text{或者} \quad f\circ g=E_Y$$

（但 g 不能使两者同时成立）。

定义 11-12 设 f：$X\to Y$，g：$Y\to X$，称 g 为 f 的**左逆函数**（或**左逆**，left inverses），如果

$$g\circ f=E_X$$

称 g 为 f 的**右逆函数**（或**右逆**,right inverses），如果

$$f\circ g=E_Y$$

【例 11-13】 设 $f1$：$X1\to Y1$，$f2$：$X2\to Y2$，$f3$：$X3\to Y3$，如图 11-8 所示。那么 $f1$ 有左逆函数 $g1$，$f2$ 有右逆函数 $g2$，$f3$ 既无左逆，又无右逆。

$g1$，$g2$ 如图 11-9 所示。

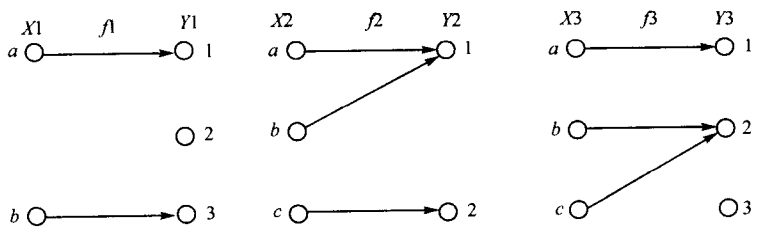


图 11-8

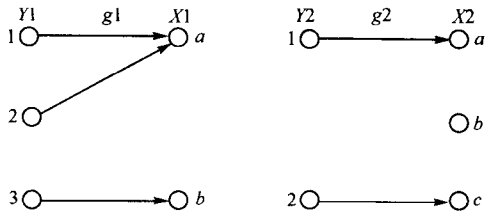


图 11-9

从例子中可以看出，$g1$ 不是 $f1^{-1}$，$g2$ 不是 $f2^{-1}$，$g1$，$g2$ 也不是惟一的。

怎样的函数有左逆函数，怎样的函数有右逆函数呢？下列定理作出了回答。

定理 11-17 设 f：$X\to Y$。

（1）f 有左逆当且仅当 f 为一单射。

（2）f 有右逆当且仅当 f 为一满射。

证明 （1）先证必要性。设 f 有左逆 g，使得 $g\circ f=Ex$。已知 Ex 为单射，据定理 11-5 之（1）f 为一单射。

再证充分性。设 f 为一单射，现构作函数 g：$Y\to X$ 如下：对于任一 $y\in Y$，

$$g(y)=\begin{cases}x & \text{有}x\in X\text{使}f(x)=y\\ a(\text{任意}a\in X) & \text{无}x\in X\text{使}f(x)=y\end{cases}$$

由于 f 为单射，g 的定义是适当的。对任一 $x\in X$，设 $f(x)=y$，由 g 的定义，则 $g(y)=x$，从而 $g\circ f(x)=g(f(x))=g(y)=x$，故 $g\circ f=E_X$，g 为 f 的左逆。

（2）先证必要性。设 f 有右逆函数 g，使得 $f\circ g=E_Y$。已知 E_Y 为满射，据定理 11-5 之（2），f 为满射。

再证充分性。设 f 为一满射，现构作函数 g：$Y\to X$ 如下：对于任一 $y\in Y$，

$$g(y)=\begin{cases}x & \text{有惟一}x\in X\text{使}f(x)=y\\ x_0(\text{任一满足}f(x)=y\text{的根}) & \text{否则}\end{cases}$$

对于任一 $y\in Y$，由于 f 为满射，总有 $x\in X$，使 $y=f(x)$，从而总有上两种 x 之一，例如 x_0，使 $g(y)=x_0$，于是 $f\circ g(y)=f(g(y))=f(x_0)=y$。因此 $f\circ g=E_Y$，g 为 f 的右逆。

左逆、右逆、逆函数之间的关系如下。

定理 11-18 设 f：$X\to Y$，那么下列三命题等价：

（1）f 可逆，即 f 有逆函数 f^{-1}。

（2）存在函数 g：$Y\to X$，g 既为 f 的左逆，又为 f 的右逆。

（3）f 既有左逆，又有右逆。

证明 （1）蕴涵（2）是明显的，取 g 为 f^{-1}。（2）蕴涵（3）更是显然的。由（3）及定理 11-17 可知，f 既是单射，又是满射，因此 f 为双射，从而可逆，故（1）可由（3）推得。

我们看到，对双射函数可以讨论它们的逆函数，对单射和满射可以讨论它们的左逆或右逆函数。现在我们引入逆象的概念，对任意函数均可进行这一讨论。

定义 11-13 设 f：$X\to Y$，$A\subseteq Y$，定义

$$f''(A)=\{x\mid f(x)\in A\}$$

称 $f''(A)$ 为 A 的逆像（inverse image）。

显然 $f''(A)\subseteq X$，它表示像点恰好落在 A 中的那些源点的集合。常用 $f^{-1}(A)$ 代替 $f''(A)$。

屈从于习惯，我们也采用这一表示，但应注意，这里f^{-1}并非指f的逆函数（可能f根本无逆函数）。当f^{-1}作用于一个Y的子集A时，约定无异于$f''(A)$，即A的逆像。

关于逆像有下列结论。

定理 11-19 设f: $X\to Y$，那么

（1）$f^{-1}(Y)=f^{-1}(\mathrm{Ran}(f))=X$

（2）若$A\subseteq B\subseteq Y$，则$f^{-1}(A)\subseteq f^{-1}(B)$

（3）若$A\subseteq Y$，则$f'(f^{-1}(A))\subseteq A$

（4）若$A\subseteq X$，则$A\subseteq f^{-1}(f'(A))$

证明 （1），（2）请读者自证。

（3）设y为$f'(f^{-1}(A))$中任一元素，那么有$x\in f^{-1}(A)$使$y=f(x)$。又据$x\in f^{-1}(A)$，知有$y_0\in A$，使$y_0=f(x)$。由于f为函数，故$y=y_0\in A$。至此，$f'(f^{-1}(A))\subseteq A$得证。

（4）设$x\in A$，那么有$y\in Y$，使$y=f(x)$，从而$y\in f'(A)$。据逆像定义，$x\in f^{-1}(f'(A))$。由x的任意性知$A\subseteq f^{-1}(f'(A))$。

本定理（3），（4）的结论中，$\subseteq$号不可更换为等号，请读者自行举例说明之。

定理 11-20 设f: $X\to Y$，那么

$$X/\ker(f)=\{C\mid \exists y\,(y\in Y\wedge f^{-1}(\{y\})=C)\}$$

证明 只需证等式两边的划分对应于同一等价关系。

$X/\ker(f)$对应于等价关系$\ker(f)$，即对任意$x1, x2\in X$（见定义 11-9），

$\langle x1, x2\rangle\in\ker(f)$ 当且仅当$f(x1)=f(x2)$

设待证等式右边对应于等价关系R，那么对任意$x1, x2\in X$，

$\langle x1, x2\rangle\in R$ 当且仅当有单元C，$x1, x2\in C$。

当且仅当有$y\in Y$，使$y=f(x1)=f(x2)$

当且仅当$f(x1)=f(x2)$

当且仅当$\langle x1, x2\rangle\in\ker(f)$

所以，$\ker(f)=R$定理 11-20 得证。

*11.4 有限集和无限集

利用函数概念对无限集进行研究是集合理论的一个重要部分，将它选为离散数学课程的一部分内容，目的是使读者对无限集概念有一个正确的认识，并借此加深对函数概念的理解，提高正确运用函数工具的能力，获得一些特定的研究方法（如“对角线法”）。

在第 1 章里，我们只是直观地描述了有限集、无限集的概念，但这样的描述是会引起问题的。著名的伽利略悖论正说明了这一点。一家有无穷多个房间的旅店，规定每间房住一位旅客，并已客满。当日又有一位旅客来投宿，店主竟欣然接纳。他让一号房旅客住二号房，让二号房旅客住三号房，……如此等等，腾出的一号房让新来旅客去住。用集合论的语言来表述这一“悖论”，无疑是说无限集$I_+=\{1, 2, 3, \cdots\}$与$N=\{0, 1, 2, \cdots\}$具有同样多的元素，即$|I_+|=|N|$。可是 N 明明白白地比I_+多一个元素“0”！这表明，依靠直观讨论无限集显然是行不通的。因此必须严格地定义有限集和无限集。

本章我们先讨论有限集、无限集的意义，然后再指出形式地描述元素“多少”概念的最

好工具是函数，并给出常见无限集的基数规定及其大小比较。

11.4.1 有限集、可数集与不可数集

定义 11-14 集合 A 称为**有限集**，如果存在集合$\{0, 1, 2, \cdots, n-1\}$（自然数 n）到 A，或 A 到集合$\{0, 1, 2, \cdots, n-1\}$的双射；否则称 A 为**无限集**。

【例 11-14】

（1）$A=\{a_0, a_1, a_2, \cdots, a_{n-1}\}$为一有限集，因为 a_i（$i=0, 1, 2, \cdots, n-1$）即为$\{0, 1, 2, \cdots, n-1\}$到 A 的一个双射。

（2）自然数集 N 为无限集。

为证明这一点，反设 N 为有限集，即存在$\{0, 1, 2, \cdots, n-1\}$到 N 的双射，记为 f。现令 $n_0=\sum_{i=0}^{n-1} f(i)+1 \in N$。显然，对每一 $i=0, 1, 2, \cdots, n-1$，恒有 $f(i)<n_0$，这就是说 f 不是满射，矛盾。因此 N 不是有限集,是无限集。

关于有限集和无限集的下列性质是十分简单明了的。

定理 11-21 任何有限集的任意子集为有限集。

证明 设 A 为有限集，因而有双射 f，自然数 n，

$$f: \{0, 1, 2, \cdots, n-1\} \to A$$

因此 $A=\{f(0), f(1), f(2), \cdots, f(n-1)\}$。若 $A1$ 为 A 的任一子集，那么 $A1=\{f(a_0), f(a_1), f(a_2), \cdots, f(a_{k-1})\}$，$k \leqslant n$。$a_0, a_1, a_2, \cdots, a_{k-1}$为 $\{0, 1, 2, \cdots, n-1\}$ 中的不同成员。将序列 $a_0, a_1, a_2, \cdots, a_{k-1}$ 看作 $\{0, 1, 2, \cdots, k-1\}$ 到 $\{a_0, a_1, a_2, \cdots, a_{k-1}\}$ $(=A2)$的双射，记为 a_i，那么

$$f\uparrow_{A2} \circ a_i: \{0, 1, 2, \cdots, k-1\} \to A1$$

为一双射，因此 A 为有限集。

定理 11-22 任何含有无限子集的集合必定是无限集。

本定理是定理 11-21 的逆否命题。

对无限集还可作进一步的分类。

定义 11-15 集合 A 称为**可数无限集**（countable infinite sets），如果存在双射 $f: N \to A$（或双射 $f: A \to N$）。其他无限集称为不可数无限集。有限集和可数无限集统称为**可数集**（countable sets）。因此，不可数集即不可数无限集。

显然，自然数集合 N 为可数无限集，N 的任何子集均为可数集。

【例 11-15】

（1）I_+为可数无限集，因为 $f(x)=x+1$ 为 N 到 I_+的双射。

（2）非负偶数集以及正奇数集均为可数无限集，因为 $f(x)=2x$，$f(x)=2x+1$ 分别为 N 到非负偶数集以及正奇数集的双射。

定理 11-23 整数集为可数无限集。

证明 建立函数 $f: I \to N$（I 为整数集）

$$f(x)=\begin{cases} 2x & \text{当 } x>0 \\ 0 & \text{当 } x=0 \\ 2(-x)-1 & \text{当 } x<0 \end{cases}$$

易知f为一双射（证明略），因此I为可数无限集。

其实，有理数集也是可数无限集，为证明这一点，我们先证明一个更一般的结论。为此需要下列术语。

定义 11-16 称集合 A 是**可枚举的**（recursively enumerable），如果存在满射f：$N\to A$。f被称为**枚举函数**。

定理 11-24 非空集合A是可数集当且仅当A是可枚举的。

证明 先证必要性。设A是非空可数集。当A为可数无限集时，有双射f：$N\to A$，因此A是可枚举的。当A为有限集时，有自然数及双射f：$\{0, 1, 2, \cdots, n-1\}\to A$。现取$a\in A$，扩充$f$为$g$：$N\to A$，

$$g(x)=\begin{cases} f(x) & 0\leqslant x\leqslant n-1 \\ a & x\geqslant n \end{cases}$$

显然g为N到A的满射，因此A是可枚举的。

再证充分性。设A是可枚举的，其枚举函数为f。如果A为有限集，则显然A是可数集；若A为无限集，构作双射g：$N\to A$，

$$g(x)=\begin{cases} f(0) & x=0 \\ f(k) & x\neq 0, k\text{为使}f(k)\neq g(0), g(1), \cdots, g(x-1)\text{的最小值} \end{cases}$$

显然g为单射。为证g为满射，令a为A中任一元素。据f意义，可知有k使$f(k)=a$，且可取k为这样的数中的最小者，那么不难由g的定义看出，$g(0), g(1), \cdots, g(k+1)$中至少有一等同于$f(k)$，即有$x\leqslant k+1$，使$g(x)=f(k)=a$。$g$构造成功，表明$A$仍为可数集。（图 11-10 给出了$g$构造的直观。）

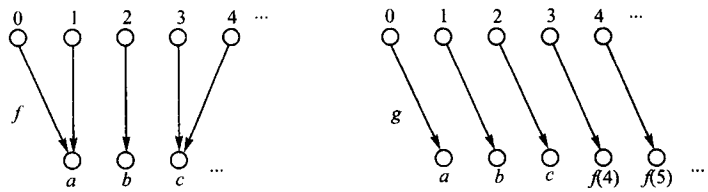


图 11-10

有了定理 11-24，许多关于可数集的结论就容易建立了。

定理 11-25 有理数集是可数集。

证明 为简明计，我们只证正有理数集Q_+是可数的，有理数集Q可数的结论可由本定理及定理 11-26 推得。

我们知道$Q_+=\{n/m \mid m,n\text{是正整数}\}$，它可用图 11-11 所示方式排列，并如该图中箭头所示来枚举，枚举函数f：$N\to Q$定义如下：

$$f(0)=\frac{1}{1}\quad f(1)=\frac{1}{2}\quad ,\ f(2)=\frac{2}{1}\ ,\ f(3)=\frac{1}{3}\ ,\ f(4)=\frac{2}{2}\ ,\ \cdots$$

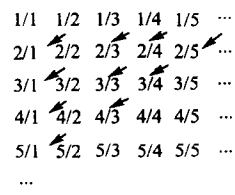


图 11-11

更形式地，可如下确定：

$$f(x)=\frac{n}{m}$$

$$x=\frac{(n+m-2)(n+m-1)}{2}+n-1 \qquad (11\text{-}5)$$

由于方程（11-5）对任一自然数 x，关于 n，m 的解是惟一确定的（请读者自行证明），因此 f 为一满射，从而 Q_+可枚举，Q_+为可数集。

定理 11-26 可数个可数集的并集是可数的。

证明 不失一般性，设这可数个可数集均非空，且为

$$A_0=\{a_{00},a_{01},a_{02},\cdots\}$$
$$A_1=\{a_{10},a_{11},a_{12},\cdots\}$$
$$A_2=\{a_{20},a_{21},a_{22},\cdots\}$$
$$\vdots$$

当 A_i 为有限集 $\{a_{i0},a_{i1},a_{i2},\cdots,a_{ik}\}$时，令

$$a_{ik}=a_{i(k+1)}=a_{i(k+2)}=\cdots$$

从而可像图 11-12 那样排列并枚举$\bigcup_{i=1}^{\infty}A_i$ 的元素：

$$a_{00},a_{01},a_{02},\cdots$$
$$a_{10},a_{11},a_{12},\cdots$$
$$a_{20},a_{21},a_{22},\cdots$$
$$\vdots$$

因此$\bigcup_{i=1}^{\infty}A_i$ 是可枚举的，因而是可数集。

定理 11-27 如果 A 是有限集，B 是可数集，那么 A 到 B 的全体函数的集合 B^A 为可数集。

证明 若 A，B 中有一为∅，则定理显然成立。现设 A，B 均非空，$|A|=n$，B 有枚举函数：$f:N\to B$。

对每一正整数 k 定义函数集合 G_k，

$$G_k=\{g\mid g\in B^A\wedge g'(A)\subseteq f'(\{0,1,\cdots,k-1\})\}$$

即 $G_k=\{f(0),f(1),f(2),\cdots,f(k-1)\}^A$，$|G_k|=k^n$ 换言之，G_k 为一有限集（可数集）。

由于 $B^A=\bigcup_{k=1}^{\infty}G_k$，即 B 为可数多可数集的并集，因此 B 是可数集。

众多的无限集都是可数集，是否还有不可数集？回答是肯定的。

定理 11-28 实数集的子集[0，1]区间是不可数集。

证明 反设[0，1]为可数集，f 为其任一枚举函数。由于[0，1]中实数均可表示为十进制无限小数（循环或不循环无限小数，0 表示为，0．000…，1 表示为 0．999…），因此[0，1]中实数可如下列出：

$$f(0)\quad 0.x_{00}x_{01}x_{02}x_{03}\cdots$$
$$f(1)\quad 0.x_{10}x_{11}x_{12}x_{13}\cdots$$
$$f(2)\quad 0.x_{20}x_{21}x_{22}x_{23}\cdots$$
$$\vdots$$
$$f(n)\quad 0.x_{n0}x_{n1}x_{n2}x_{n3}\cdots$$
$$\vdots$$

这里 $x_{nj}\,(n,j=0,1,2,\cdots)$为第 n 个小数的第 j 个数字。现构作实数 $y=0.y_0y_1y_2\cdots$使得

$$y_i=\begin{cases}1 & x_{ii}\neq 1\\ 2 & x_{ii}=1\end{cases}$$

显然 $y\in[0,1]$，且对于任一 n，$y\neq f(n)$，因为至少 $y_i\neq x_{ii}$ 这就是说 f 不是满射，矛盾。矛盾表明，[0，1]不可能有枚举函数，从而是不可数集。

上述定理的证明方法，就是著名的“康脱对角线法”，这一方法在可计算性理论中有广泛的应用。

11.4.2 无限集的特性

利用定义 11-14 来判定无限集是不方便的，于是人们找出了一个无限集的特征性：**每个无限集总与自己的一个真子集一一对应**。利用这一特征性来判定一个集合是否为无限集就方便得多了。例如，自然数集 N 有真子集 E（非负偶数集），N 与 E 有一一对应 $f(x)=2x$；又如实数集 R 与其真子集 R_+（正实数集）一一对应，因 $f(x)=2^x$ 中 f 为 R 到 R_+ 的一个双射；这表明 N 与 R 为无限集。

为证明上述特征性，需要下列事实。

定理 11-29 任何无限集合均含有一可数无限子集。

证明 设 A 为任一无限集，显然 $A\neq\varnothing$，可设 $a_0\in A$。考虑 $A_1=A-\{a_0\}$，A_1 仍为无限集，又有 $a_1\in A$。考虑 $A_2=A_1-\{a_1\}$，A_2 依然为无限集，同样有 $a_2\in A_2$，……如此等等。

令 $B=\{a_0,a_1,a_2,\cdots\}$，显然 $B\subseteq A$，且对任一自然数 n，总有 $a_n\in B$，因而可类似例 11-14 之（2）证明 B 为可数无限集。

有了定理 11-29 便可建立无限集的下列特征性。

定理 11-30 集合 A 为无限集，当且仅当存在 A 的真子集 $A0$ 及双射函数 f：$A\to A0$。

证明 先证必要性。设 A 为无限集，据定理 11-29，A 有可数无限子集 $B=\{a_0,a_1,a_2,\cdots\}$。令 $A0=A-\{a_0\}\subset A$。定义函数 f：$A\to A0$：

$$f(x)=\begin{cases}x & x\notin B\\ a_{i+1} & x=a_i\in B(i=0,1,2,\mathrm{n})\end{cases}$$

容易看出 f 为一双射。

再证充分性。设 $A0\subset A$，且有 f：$A\to A0$ 为一双射。若 A 为有限集，那么由 $A0\subset A$ 知 f 为双射是不可能的。故 A 为无限集。

我们指出，定理 11-29、定理 11-30 依赖于集合论的选择公理。

* **选择公理**（choice axiom）对任何一个非空集合族 $A=\{A_d\mid d\in D\}$，总有集合 B，使 B 与诸 A_d 的交均为单元素集合。常称 B 为 A 的代表元素集。

对于有限集合族，选择公理无疑是适当的；但对于非有限集合族，选择公理是否适当是有争议的，但多数数学家认为集合论应当接受选择公理。

定理 11-29 事实上默认集合族有代表集 B，从而默认选择公理。

由于有定理 11-30，可以用上述特征性作为无限集的定义，这一定义在接受选择公理的前提下与定义 11-14 等价。

11.4.3 有限集和无限集的基数

基数概念是刻画集合元素多少的极为重要的概念，但对于无限集而言，由于它可以同自己的一个真子集一一对应（这一特性充分地反映了无限集的本质），因此利用直观的“多少”概念来定义无限集的基数是行不通的。就本书的宗旨而言，详尽严格地给出基数的一般定义似又过于复杂。因此，我们在这一节里只给出有限集、可数无限集以及不可数无限集中“连续统”的基数意义，而回避对基数作一般的定义。

定义 11-17 称集合 A 的**基数**(cardinal number)为 n(n 为自然数)，如果有双射 $f:\{0,1,2,\cdots,n-1\}\to A$，或双射 $f: A\to\{0,1,2,\cdots,n-1\}$。记为 $|A|=n$。

显然，集合 A 为有限集，当且仅当它以自然数为其基数，即存在自然数 n 使 $|A|=n$。可以说 n 是集合 A 的元素个数。

定义 11-18 称集合 A 的基数为 $\aleph_0$，如果有双射 $f: N\to A$，或双射 $f: A\to N$，N 为自然数集。记为 $|A|=\aleph_0$。

因此，自然数集及一切可数无限集的基数均为 $\aleph_0$。

定义 11-19 称集合 A 的基数为 C，如果有双射 $f: [0,1]\to A$，或双射 $f: A\to[0,1]$。记为 $|A|=C$。具有基数 C 的集合常称为**连续统**（continuum）。

定理 11-31 实数集上的任何闭区间 $[a,b]$，开区间 (a,b) $(a<b)$，以及实数集本身都是连续统。

证明 建立双射 $f: [0,1]\to[a,b]$

$$f(x)=(b-a)x+a$$

因此

$$|[a,b]|=|[0,1]|=C$$

为证 $|(a,b)|=C$，先证 $|(0,1)|=C$，然后同上可证 $|(a,b)|=|(0,1)|=C$。为此建立双射 $g: [0,1]\to(0,1)$，使

$$g(x)=\begin{cases}\dfrac{1}{2} & x=0\\ \dfrac{1}{n+2} & x=\dfrac{1}{n}\quad (n=1,2,\cdots)\\ x & \text{否则}\end{cases}$$

（g 的图示在图 11-12 中给出）因此 $|[0,1]|=|(0,1)|=C$。

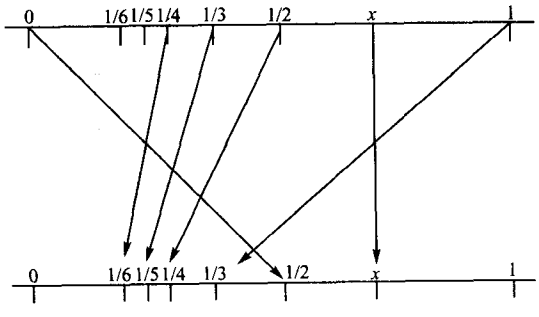


图 11-12

为证$|R|=C$，建立双射 h：$(0,1)\to R$，

$$h(x)=\frac{\frac{1}{2}-x}{x(1-x)}$$

因此$|R|=|(0,1)|=C$。

f，g 为双射请读者自行验证。现证 h 为一双射。首先，对任实数 y，方程 $y=\dfrac{\frac{1}{2}-x}{x(1-x)}$ 同解于 $yx^2-(y+1)x+1/2=0$，由于$(y+1)^2-4y\times 1/2=y^2+1>0$，因而该方程总有解，即 h 为满射。其次该方程的两根

$$x_1=\frac{y+1+\sqrt{y^2+1}}{2},\quad x_2=\frac{y+1-\sqrt{y^2+1}}{2}$$

中，$x_1\notin(0,1)$，因此只有 x_2 为其解，也就是说 h 为一单射。

也许有人会问，是否所有集合都以自然数 n、$\aleph_0$ 和 C 之一作为其基数呢？事实不然。例如，$\rho(R)$（R 为实数集）不以 C 为基数，更不以$\aleph_0$和自然数为其基数，需另外加以确定。为了作更深入的讨论，我们引人基数大小的概念。

11.4.4 基数比较

我们已经指出，表示集合元素“多少”的基数并不限于：自然数，$\aleph_0$ 和 C，还存在着其他集合和表示它们元素“多少”的别的基数，只是为了简化，我们不讨论一般的基数概念。但是，为了对基数有一个总体的认识，以下要讨论基数大小的概念。

定义 11-20 设 A，B 为任意集合。

（1）称 A，B 基数**相等**，记为$|A|=|B|$，如果有双射 f：$A\to B$ 或双射 f：$B\to A$。

（2）称 A 的基数**小于等于** B 的基数，记为$|A|\leqslant|B|$，如果有单射 f：$A\to B$ 或满射 f：$B\to A$。

（3）称 A 的基数**小于** B 的基数，记为$|A|<|B|$，如果$|A|\leqslant|B|$，且$|A|\neq|B|$。

显然，上述定义与我们前面对有限集、可数无限集及连续统的基数规定是一致的。对任何自然数 m，n，若 $m\leqslant n$，则

$$|\{0,1,2,\cdots,m-1\}|\leqslant|\{0,1,2,\cdots,n-1\}|$$

对任意自然数 n，$n<\aleph_0$，即 $|\{0,1,2,\cdots,n-1\}|<|\{0,1,2,3,\cdots\}|$；而$\aleph_0<C$，即 $|\{0,1,2,3,\cdots\}|<|R|$。

关于基数相等及不等关系有下列事实。

定理 11-32 基数相等关系为一等价关系，即对任何集合 A，满足：

（1）$|A|=|A|$。

（2）若$|A|=|B|$，则 $|B|=|A|$。

（3）若$|A|=|B|$，$|B|=|C|$，则 $|A|=|C|$。

由定义 11-20 及双射性质立得。

本定理表明，全体集合可以依赖集合间的基数相等关系来进行划分，每一等价类为两两基数相等（其元素一一对应）的集合族。因而可以说，基数是一等价类中诸成员——集合的

一个共同特性的抽象。

定理 11-33 对任意集合 A，B，C，

（1）$|A| \leqslant |A|$。

（2）若$|A| \leqslant |B|$，$|B| \leqslant |C|$，则 $|A| \leqslant |C|$。

请读者自行证明本定理。

定理 11-34 对任意集合 A，B，或者$|A| < |B|$，或者$|A| = |B|$，或者$|B| < |A|$，且任意两者都不能兼而有之。

本定理常称为基数三歧性定理，它的证明依赖于选择公理，我们略去这一证明，有兴趣的读者可参阅文献 2。

定理 11-35 对任意集合 A，B，如果$|A| \leqslant |B|$，$|B| \leqslant |A|$，那么$|A| = |B|$。

证明 设$|A| \neq |B|$，那么根据基数三歧性定理，或者$|A| < |B|$，或者$|B| < |A|$，且不能兼而有之。

若$|A| < |B|$，那么$|B| < |A|$不成立，且$|A| \neq |B|$，于是与$|B| \leqslant |A|$矛盾。

若$|B| < |A|$，那么$|A| < |B|$不成立，且$|A| \neq |B|$，于是又与$|A| \leqslant |B|$矛盾。

$|A| = |B|$得证。

定理 11-33、定理 11-34 和定理 11-35 表明，基数的≤关系为一全序关系。定理 11-35 在基数讨论中应用广泛。

定理 11-36 $\rho(N)$（N 为自然数集）为连续统。

证明 利用定理 11-35 证明本命题，为此要建立单射 f：$\rho(N) \to [0, 1]$，单射 g：$[0, 1] \to \rho(N)$以便证明，$|\rho(N)| \leqslant C, C \leqslant |\rho(N)|$。

定义$f: \rho(N) \to [0, 1]$如下：对每一 $S \subseteq N$

$$f(S) = 0.x_0x_1x_2x_3\cdots \text{（十进制小数）}$$

其中

$$x_i = \begin{cases} 1 & i \in S \\ 0 & i \notin S \end{cases}$$

（例如$f(\varnothing) = 0.000\cdots$，$f(N) = 0.111\cdots$，$f(\{0, 2\}) = 0.10100\cdots$）显然 f 为单射。

定义 g：$[0, 1] \to \rho(N)$如下：对每一[0，1]中数的二进制表示（如果这种表示不惟一，则取定其中之一）$0.x_0x_1x_2x_3\cdots$（x_i 为 0 或 1）：

$$g(0.x_0x_1x_2x_3) = \{i \mid x_i = 1\}$$

易知，g 也是单射。定理得证。

注意，上述证明中，对 f 的定义不可用二进制表示的实数 $0.x_0x_1x_2x_3\cdots$，

因为

$$f(\{0\}) = 0.1000\cdots = 0.0111\cdots = f(\{1,2,3,\cdots\})$$

从而 f 便不是单射。另外，应注意 g 不是满射。例如 1/2，只能取一种二进制表示方式，当它确定表示为 0.1000…时，$g(0.1000\cdots) = \{0\}$，从而不可能有 x 使 $g(x) = \{1, 2, 3, 4, \cdots\}$，因为只有在 $x = 0.0111\cdots$时才有这一结果，而 0.0111…是 1/2 的另一二进制表示形式。

现在我们来讨论上一小节末提出的问题，看看究竟是些什么集合具有不同于自然数、$\aleph_0$ 和 C 的基数。

定理 11-37 $\aleph_0$ 是最小的无限集基数，即没有无限集 A，使 $|A| < \aleph_0$。

证明 设 A 为一无限集，那么据定义 11-22，有可数无限集 B，$B \subseteq A$，从而有单射 $f: B \to A$，$f(x)=x$。因此 $|B| \leqslant |A|$，即 $\aleph_0 \leqslant |A|$，据基数三歧性 $|A| < \aleph_0$ 不能成立。

本定理表明，不存在基数大于所有自然数而又小于 $\aleph_0$ 的集合。

定理 11-38 对任一基数 α，总存在集合，其基数 β 大于 α，即 $\alpha < \beta$。

证明 设以 α 为基数的集合为 A，令 $\rho(A)$ 的基数为 β，欲证 $\alpha < \beta$，即 $|A| < |\rho(A)|$。

显然 $|A| \leqslant |\rho(A)|$，因为如下定义的函数 $f: A \to \rho(A)$，明显为一单射：对每一 $x \in A$，$f(x)=\{x\}$

现证 $|A| \neq |\rho(A)|$。若不然，有双射 g：$A \to \rho(A)$，使得对每一 $x \in A$，$g(x) \subseteq A$。定义集合

$$S=\{x \mid x \notin g(x)\}$$

当然 $S \subseteq A$。由于 g 为满射，有 $y \in A$，使得 $g(y)=S$。考虑 $y \in S$ 与否，得知

$$\begin{aligned} y \in S &\Leftrightarrow y \in \{x \mid x \notin g(x)\} \\ &\Leftrightarrow y \notin g(y) \\ &\Leftrightarrow y \notin S \end{aligned}$$

矛盾。因此 g 不存在。$|A| \neq |\rho(A)|$ 得证。

如果我们把 $|\rho(A)|$ 记为 $2^{|A|}$（这对于有限集 A 是成立的），那么

（1）对有限集 A，当 $|A|=n$ 时，$|\rho(A)|=2^n$。

（2）对可数无限集 A，$|A|=\aleph_0$，那么 $|\rho(A)|=2^{\aleph_0}$

由于 $|\rho(N)|=C$（定理 11-36），且对任何可数无限集 A

$$|\rho(A)|=|\rho(N)|$$

因此

$$2^{\aleph_0}=C$$

（3）对连续统 A，$|A|=C$，那么

$$|\rho(A)|=2^C$$

这是一个大于 C，$\aleph_0$ 和一切自然数的基数。

（4）据定理 7-18，可以断定还有集合以 2^{2^C}，$2^{2^{2^C}}$，…为基数。因此，我们已知的基数由小到大可排列为

$$0,\ 1,\ 2,\ 3,\ \cdots,\ \aleph_0,\ C(2^{\aleph_0}),\ 2^C,\ 2^{2^C},\ 2^{2^{2^C}},\ \cdots$$

我们已经知道，在自然数与 $\aleph_0$ 之间不可能还有别的基数，那么，是否有集合，其基数大于 $\aleph_0$ 而小于 C 呢？即 $\aleph_0$ 与 C 之间是否另有基数呢？同样的，在 C 与 2^C 之间，在 2^C 与 2^{2^C} 之间，……，是否另有基数呢？这是一个至今尚未解决的理论问题。著名的连续统假设及广义连续统假设断言：它们之间均无其他基数。这些假设没有得到证明，也没有得到否证；但是它们被证明与现行集合论系统是一致的、独立的，即用现行集合论公理不可能证明它们，也不可能证明它们的否定。

11.5 练习

1. 指出图 11-13 中各关系是不是函数，并说明理由。

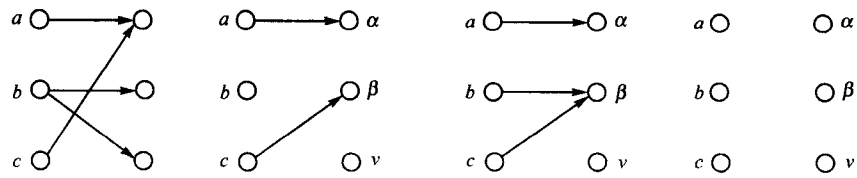


图 11-13

2. 指出下列各关系是否为 A 到 B 的函数：

（1）$A=B=N$

$R=\{<x,y>|\ x\in A\wedge y\in B\wedge x+y<10\}$

（2）$A=B=R$（实数集）

$S=\{<x,y>|\ x\in A\wedge y\in B\wedge y=x^2\}$

（3）$A=\{1,2,3,4\}$，$B=A\times A$

$R=\{<1,<2,3>>,<2,<3,4>>,<3,<1,4>>,<4,<2,3>>\}$

（4）$A=\{1,2,3,4\}$，$B=A\times A$

$S=\{<1,<2,3>>,<2,<3,4>>,<3,,<2,3>>\}$

3. 设 f：$X\to Y$，g：$X\to Y$，求证：

（1）$f\cap g$ 为 X 到 Y 的函数当且仅当 $f=g$。

（2）$f\cup g$ 为 X 到 Y 的函数当且仅当 $f=g$。

4. 设 f 为一函数，g 为一函数，求证：

（1）$f\cap g$ 是以 Dom $(f\cap g)$为定义域的一个函数。

（2）$f\cup g$ 是以 Dom $(f\cup g)$为定义域的函数当且仅当对每一 $x\in \mathrm{Dom}(f)\cap \mathrm{Dom}(g)$，$f(x)=g(x)$。

5. 设 f 和 g 为函数，且 $f\subseteq g$，Dom $(g)\subseteq$ Dom (f)。证明 $f=g$ 。

6.（1）用数学归纳法证明 $n^n<2^{n^2}$

（2）考虑一集合上关系与函数的数目上的差异，再证（1），不用归纳法。

7. 证明定理 11-2 之（2），（3）。

8. 设 $f:X\to Y$，$A\subseteq B\subseteq X$，求证 $f(A)\subseteq f(B)$。

9. 令 $f=\{<\varnothing,\{\varnothing,\{\varnothing\}\}>,<\{\varnothing\},\varnothing>\}$为一函数。计算 $f(\varnothing)$，$f(\{\varnothing\})$，$f'(\varnothing)$，$f'(\{\varnothing\})$，$f'(\{\varnothing,\{\varnothing\}\})$以及 $f\upharpoonright_{\varnothing}$，$f\upharpoonright_{\{\varnothing\}}$，$f\upharpoonright_{\{\varnothing,\{\varnothing\}\}}$。

10. 设 f：$X\to Y$，$A\subseteq X$，$B\subseteq X$，求证：

（1）$f\upharpoonright_A=f\cap(A\times \mathrm{Ran}(f))$

（2）$f\upharpoonright_{A\cup B}=f\upharpoonright_A\cup f\upharpoonright_B$

11. 令 $B^{[A]}=\{f|f$ 为 A 到 B 的偏函数$\}$，问：集合 A 和 B 满足什么条件时

$$B^A=B^{[A]}$$

12. 考虑下列实数集上的函数：

$$f(x)=2x^2+1,\ g(x)=-x+7,\ h(x)=2^x,\ k(x)=\sin x$$

求 $g\circ f$，$f\circ g$，$f\circ f$，$g\circ g$，$f\circ h$，$f\circ k$，$k\circ h$ 的解析式。

13. 设 $X=\{0,1,2\}$，请找出 X^X 中满足下列各式的所有函数。

（1）$f^2(x)=f(x)$（f 等幂）

（2）$f^2(x)=x$（f^2 为恒等函数）

（3）$f^3(x)=x$（f^3为恒等函数）

14. 设f：$X\to Y$，g：$Y\to Z$，$A\subseteq X$，求证：

$$(g\circ f)'(A)=g'(f'(A))$$

15. 设$A\neq\varnothing$，A，B，C为集合。

（1）求$A^{\varnothing}$，$\varnothing^{A}$，$\varnothing^{\varnothing}$。

（2）证明：若$A\subseteq B$，则$A^C\subseteq B^C$。

16. 设f：$X\to Y$，X，Y为有限集合。

（1）若$|X|<|Y|$，f可能是满射吗？为什么？

（2）若$|X|>|Y|$，f可能是单射吗？为什么？

（3）若$X=\varnothing$，f可能是单射吗？可能是满射吗？

（4）X与Y满足什么条件时，f可能是满射？单射？双射？

（5）思考你对（4）给出的条件，在X，Y为无限集时还适用吗？

17. 证明定理 11-5 之（2），（3）。

18. 证明：存在一个从集合X到它的幂集$\rho(X)$的一个单射。

19. 例 11-9 之（1）中定义的字长函数l: $\Sigma^*\to N$，在Σ满足什么条件时为一双射函数？

20. 设f：$X\to Y$，$A\subseteq X$。

（1）证明：若f为一单射，则$f\upharpoonright_A$亦为一单射。

（2）设f为一满射。给出一个关于A的条件，使它是使$f\upharpoonright_A$为满射的充分必要条件。

21. 对下列每对集合X，Y构造一个X到Y的双射函数。

（1）$X=N$，$Y=N-\{0\}$

（2）$X=\rho(\{a,b,c\})$，$Y=\{0,1\}^{\{a,b,c\}}$

（3）$X=R_+$，$Y=R$（R为实数集，R_+为正实数集）

（4）$X=N$，$Y=I$

22. 设h为X上函数，证明下列条件中（1）与（2）等价，（3）与（4）等价。

（1）h为一单射。

（2）对任意X上函数f，g，$h\circ f=h\circ g$蕴涵$f=g$。

（3）h为一满射。

（4）对任意X上函数f，g，$f\circ h=g\circ h$蕴涵$f=g$。

23. 设$A=\{1,2,3\}$，作出全部A上的置换，并以三个函数值组成的字的字典序排列这些置换。试计算$p_2\circ p_3$，$p_3\circ p_3$，$p_3\circ p_2$，并求x，使得$p_3\circ p_x=p_x\circ p_3=i$。

24. 设f：$X\to Y$满足$f^2(x)=x$证明f为一双射。

*25. 设f：$A\to B$，g：$A\to C$，证明：存在函数h：$B\to C$，使$g=h\circ f$，当且仅当$\ker(f)\subseteq\ker(g)$。

*26. 设$<X,\leqslant_1>$，$<Y,\leqslant_2>$为有序集，f：$X\to Y$为单调映射。问：如何定义$X/\ker(f)$上的关系≤，使之满足：

（1）≤为$X/\ker(f)$上的序关系。同时

（2）映射g：$X\to X/\ker(f)$是单调映射。

*27. 对下列函数分别说出它们所导出的商集和规范映射：

（1）$f1$：$N\to N$，$f1(x)=x+1$

（2）$f2: I\to I, f2(x)=\begin{cases}0 & x\text{为偶数}\\ 1 & x\text{为奇数}\end{cases}$

28．完成定理 11-14 的证明。

29．证明定理 11-16。

30．证明定理 11-19 之（1），（2），并用实例说明，（3），（4）中的$\subseteq$号不可更换为等号。

31．下列函数为实数集上的函数，如果它们可逆，请求出它们的逆函数；否则，对它们作适当的限制后，求出这一限制的逆函数。

（1）$y=3x+1$

（2）$y=x^3-1$

（3）$y=x^2-2x$

（4）$y=\tan x+1$

32．置换的逆函数称为逆置换。请给出一个由已知置换求其逆置换的简明算法。

33．设 $A=\{1,2,3,4\}$，$B=\{1,2\}$，

（1）试定义一函数 f：$A\to A$，使 $f\neq E_A$，但 $f=f^{-1}$。

（2）试定义一函数 f：$A\to B$，使 f 非双射，但有四个右逆函数 g。

（3）设 f：$B\to A$，f 为一单射，问 f 最多可能有几个左逆函数 g。

34．设 f：$X\to Y$，A，B 为 Y 的子集，证明：

（1）$f^{-1}(A\cup B)=f^{-1}(A)\cup f^{-1}(B)$

（2）$f^{-1}(A\cap B)=f^{-1}(A)\cap f^{-1}(B)$

（3）$f^{-1}(A-B)=f^{-1}(A)-f^{-1}(B)$

35．试作一函数 f：$N\to N$，使之恰有两个右逆。

36．证明：若函数 f：$N\to N$ 有多于一个的左逆，那么它必有无穷多个左逆。

37．用定义 11-14 证明：

（1）两个有限集的并集为有限集。

（2）两个有限集的笛卡尔积为有限集。

（3）[0，1]区间为无限集。

38．设 A，B 为可数集，证明：

（1）$A\cup B$ 为可数集（不用定理 11-16）。

（2）$A\times B$ 为可数集（不用定理 11-26）。

39．证明所有 0，1 序列（包括无穷序列）所组成的集合为不可数集。

40．证明自然数集的幂集为不可数集（提示：利用题 39）。

41．应用定理 11-30 但不用例 11-16 证明：若 A 为无限集，B 为任一集合，那么 $A\cup B$ 亦为无限集.。

42．在定理 11-28 的证明中，假如[0，1]中实数用二进制小数来表示，即 f(x)中 $x_{n0}, x_{n1}, x_{n2}, x_{n3}\cdots$均为 0 或 1，而 $y=0.y_0y_1y_2\cdots$中诸 y_i 定义如下：

$$y_i=\begin{cases}1 & x_{ii}=0\\ 0 & x_{ii}=1\end{cases}$$

那么，证明过程是否仍能成立，为什么？

43．设 f：$A\to B$ 为一满射。

（1）当 A 为无限集时，B 是否一定为无限集？

（2）A 为可数集时，B 是否一定为可数集？

44. 设 f: $A \to B$ 为一单射。

（1）A 为无限集时，B 是否一定为无限集？

（2）A 为可数集时，B 是否一定为可数集？

45. 利用定理 11-30 证明：

（1）当 A 为无限集时，$\rho(A)$为无限集。

（2）当 A 为无限集，$B \neq \varnothing$时，$A \times B$ 为无限集。

（3）当 A 为无限集，$B \neq \varnothing$时，A^B 为无限集。

46. 证明：A 为无限集，当且仅当对 A 上的任意函数 f，恒有 A 的非空真子集 B，使得 $f(B) \subseteq B$。

47. 设字母表 $\Sigma = \{a, b\}$，证明 $|\Sigma^*| = \aleph_0$。

48. 证明：任意开区间 (a, b) $(a < b)$的基数为 C。

第 12 章　递归函数集与可计算性

本章既是第 11 章的自然延伸，又是相对独立的一个部分。本章介绍自然数集合上的一类重要函数——递归函数（又称可计算函数），它们与计算机科学技术有着十分紧密的联系。递归函数理论（或可计算理论）是十分重要的基础理论，被人誉为计算机科学中的“力学”。事实上，它还有相当广泛的应用。基于课程的局限，我们不讨论这个理论的全部，只介绍可计算函数集合的两种描述。

“可计算函数”是一个直观的概念，它的内涵无法在数学的范畴内严格定义，人们只能说某函数直觉上是可计算的。如果严谨些，也许可以说某函数（1）用人的某些约定俗成的计算规则可计算；（2）用某种计算模型可计算；或者（3）用某个计算程序可计算。研究的成果表明，从这三个角度来看可计算函数的集合，它们竟是同一个集合,也就是我们即将要讨论的递归函数集。于是，计算理论的创始人图灵（Turing）和丘奇（Church）便把这个函数集合叫做“可计算函数集”，绝大多数数学家和计算机科学家都认同这个定义。我们就从（1）、（2）这两个角度来认识“可计算函数集”。

我们约定，本章讨论的函数（或偏函数）全部以自然数集合为其定义域（或前域）和陪域，也称它们为**数论函数**。由于，我们会较多地谈论真偏函数（其定义域是自然数集合的真子集），因而有时会把以自然数集合为定义域的数论函数特称为**“全函数”**。还有一点需要指出，下文会较多地运用多元函数，这样做读起来有些麻烦，但对函数的深入理解是有好处的。许多场合下它们也只是一元函数的简单推广，可以简化为一元函数去理解。

通过本章的学习，不仅可以对“可计算函数”的概念有所了解，进而从本质上认识计算机的计算能力，还可以学习许多重要函数的构造方法，对于将来学习和掌握函数式程序设计及其语言是大有裨益的。

12.1　初等函数集

12.1.1　初等函数

我们先来认识一些最简单的、最直观地可计算的、被人们称之为本原函数的函数。

本原函数：

（1）一元**后继函数** $S(x)$

$$S(x)=x+1$$

（2）n 元**常值函数** $C_m^{(n)}(x_1,\cdots,x_n)$

$$C_m^{(n)}(x_1,\cdots,x_n)=m$$ （m 为一确定的自然数，n 为确定的正整数）

（3）n 元**投影函数** $p_m^{(n)}(x_1,\cdots,x_n)$（$m\leqslant n$，$m$，$n$ 为正整数）

$$p_m^{(n)}(x_1,\cdots,x_n)=x_m$$

它们的可计算性是明显的，也是可以约定的。

下列对函数的**操作**（operater，它们以函数为对象，产生的结果仍然是函数）是大家已经熟悉的。

（1）函数的**合成操作**。

设 $f(x_1,\cdots,x_n)$ 为 n 元函数，$g_1(y_1,\cdots,y_m)$，…，$g_n(y_1,\cdots,y_m)$，是 n 个 m 元函数，那么

$$f(g_1(y_1,\cdots,y_m),\cdots,g_n(y_1,\cdots,y_m))$$

称为 $f(x_1,\cdots,x_n)$ 与 $g_1(y_1,\cdots,y_m),\cdots,g_n(y_1,\cdots,y_m)$ 的**复合函数**，这一过程称为函数的**合成操作**。

不难理解，当函数 $f(x_1,\cdots,x_n)$ 与 $g_1(y_1,\cdots,y_m)$，…，$g_n(y_1,\cdots,y_m)$ 都可计算时，复合函数 $f(g_1(y_1,\cdots,y_m),\cdots,g_n(y_1,\cdots,y_m))$ 也可认定是可计算的 。

（2）函数的**迭加操作**。

设 $f(x,x_1,\cdots,x_{n-1})$ 为 n 元函数，定义

$$\begin{aligned} g(u,x_1,\cdots,x_{n-1}) &= \sum_{i\leqslant u} f(i,x_1,\cdots,x_{n-1}) \\ &= f(0,x_1,\cdots,x_{n-1}) + f(1,x_1,\cdots,x_{n-1}) + \cdots + f(u,x_1,\cdots,x_{n-1}) \end{aligned}$$

称 $\sum_{x\leqslant u}$ 为**迭加操作**。（$\sum_{x\leqslant u}$ 就是大家熟悉的 $\sum_{x=0}^{u}$，下同）

很显然，当函数 $f(x,x_1,\cdots,x_{n-1})$ 可计算时，函数 $\sum_{i\leqslant u} f(i,x_1,\cdots,x_{n-1})$ 也可认定是可计算的。

（3）函数的**迭乘操作**。

设 $f(x,x_1,\cdots,x_{n-1})$ 为 n 元函数，定义

$$\begin{aligned} g(u,x_1,\cdots,x_{n-1}) &= \prod_{x\leqslant u} f(x,x_1,\cdots,x_{n-1}) \\ &= f(0,x_1,\cdots,x_{n-1}) \cdot f(1,x_1,\cdots,x_{n-1}) \cdot \cdots \cdot f(u,x_1,\cdots,x_{n-1}) \end{aligned}$$

称 $\prod_{x\leqslant u}$ 为**迭乘操作**。

同样，当函数 $f(x,x_1,\cdots,x_{n-1})$ 可计算时，函数 $\prod_{x\leqslant u} f(x,x_1,\cdots,x_{n-1})$ 也可认定是可计算的 。

定义 12-1 归纳定义**初等函数**（elementary functions）**集**：

（1）本原函数是初等函数。

（2）二元差函数（注意它与算术减的区别）

$$x \overset{*}{-} y = \begin{cases} 0 & \text{当 } x\leqslant y \\ x-y & \text{当 y<x，这里的 - 是通常的算术减} \end{cases}$$

是初等函数。

（3）如果 $f(x_1,\cdots,x_n)$ 与 $g_1(y_1,\cdots,y_m)$，…，$g_n(y_1,\cdots,y_m)$ 都是初等函数，那么它们的合成 $f(g_1(y_1,\cdots,y_m),\cdots,g_n(y_1,\cdots,y_m))$ 也是初等函数。

（4）如果 $f(x,x_1,\cdots,x_{n-1})$ 是初等函数,那么

$$g(u,x_1,\cdots,x_{n-1}) = \sum_{x\leqslant u} f(x,x_1,\cdots,x_{n-1})$$

$$g(u,x_1,\cdots,x_{n-1}) = \prod_{x\leqslant u} f(x,x_1,\cdots,x_{n-1})$$

也是初等函数。

（5）只有有限次使用上述条款确定的函数是初等函数。

（请注意，这里的初等函数不同于高等数学或数学分析中初等函数的概念）

下面我们来看看，如此定义的初等函数集合会含有哪些函数，初等函数集合能有多大。

【例 12-1】 下列函数都是初等函数，等式的右边是它们的构作过程。

（1）**二元乘函数** $x\cdot y$

$x\cdot y=\sum_{i\leqslant x} C_y^{(1)}(i)\overset{*}{-}y$（注意：$i$ 从 0 到 x 共取 $x+1$ 个值）

（2）**二元加函数** $x+y$

$x+y=(x+1)\cdot(y+1)\overset{*}{-}x\cdot y\overset{*}{-}1$

（3）**逆符号函数** $\overline{sg(x)}=\begin{cases}0 & \text{当 } x>0\\ 1 & \text{当 } x=0\end{cases}$

$\overline{sg(x)}=1\overset{*}{-}x$

（4）**符号函数** $sg(x)=\begin{cases}1 & \text{当 } x>0\\ 0 & \text{当 } x=0\end{cases}$

$sg(x)=1\overset{*}{-}\overline{sg(x)}$

（5）**绝对差函数** $x\Delta y=\begin{cases}x\overset{*}{-}y & \text{当 } y\leqslant x\\ y\overset{*}{-}x & \text{当 } x<y\end{cases}$

$x\Delta y=(x\overset{*}{-}y)+(y\overset{*}{-}x)$

（6）**商取整函数** $\left[\frac{x}{y}\right]$（约定 $y=0$ 时 $\left[\frac{x}{y}\right]=0$）

$\left[\frac{x}{y}\right]=sg(y)\cdot\sum_{i\leqslant x}\overline{sg}(y\cdot(i+1)\overset{*}{-}x)$（$sg(y)$ 的引入是上述约定的需要）

（7）**指数函数** x^y

$$x^y=\left[\frac{\prod\limits_{i\leqslant y}C_x^{(1)}(i)}{x}\right]$$（注意：i 从 0 到 y 共取 $y+1$ 个值）

（8）**求小函数** $\min(x,y)$

$$\min(x,y)=x\overset{*}{-}(x\overset{*}{-}y)$$

（9）**求大函数** $\max(x,y)$

$$\max(x,y)=x+(y\overset{*}{-}x)$$

（10）**剩余函数** $rs(x,y)$（表示 x 除以 y 所得的余数，当 $y=0$ 时，约定 $rs(x,y)=x$）

$$rs(x,y)=x\overset{*}{-}\left(y\cdot\left[\frac{x}{y}\right]\right)$$（前有约定 $y=0$ 时 $\left[\frac{x}{y}\right]=0$）

（11）**平方根取整函数** $sq(x)$（表示 x 的算术平方根的整数部分）

$$sq(x)=\left[\sqrt{x}\right]=\left(\sum_{i\leqslant x}\overline{sg}(i^2\overset{*}{-}x)\right)\overset{*}{-}1$$（$\sum\limits_{i\leqslant x}\overline{sg}$ 像是一个“计数器”）

（12）**平方根剩余函数** $E(x)$（x 与不大于它的最大的完全平方数的差）

$$E(x)=x\overset{*}{-}sq^2(x)$$

（13）**阶乘函数** $x!$

$$x!=\prod_{i\leqslant x-1}(i+1)$$

（14）**相等性函数** $eq(x,y)=\begin{cases}1 & \text{当 } x=y\\ 0 & \text{当 } x\neq y\end{cases}$

$$eq(x,y)=\overline{sg}(x\Delta y)$$

12.1.2 初等谓词

为了进一步讨论初等函数，我们引入初等谓词的概念。

定义 12-2 n 元谓词 $P(x_1,\cdots,x_n)$ 称为初等谓词（elementary predicates），如果它的特征函数 $x_P(x_1,\cdots,x_n)$ 为初等函数。

下列谓词都是初等谓词。

$x=y$	它的特征函数是 $eq(x,y)=\overline{sg}(x\Delta y)$
$x\leqslant y$	它的特征函数是 $\overline{sg}(x\overset{*}{-}y)$
$x<y$	它的特征函数是 $sg(y\overset{*}{-}x)$

$y|x$　　“y 整除 x”（约定：0 整除 x 当且仅当 $x=0$）它的特征函数是 $eq(rs(x,y),0)$，为简明计，将其记为 $div(y,x)$，于是得到“计算 x 的因子数”的初等函数：$ndiv(x)=\sum_{i\leqslant x} div(i,x)$，注意 $ndiv(0)=0$

$\Pr(x)$（x 是质数）　　它的特征函数是 $eq(ndiv(x),2)$

关于初等谓词，还有以下重要结论。

定理 12-1　初等谓词集合关于命题联接词封闭。即当 $P(x_1,\cdots,x_n)$，$Q(x_1,\cdots,x_n)$ 为 n 元初等谓词，那么

$$\neg P(x_1,\cdots,x_n),\ P(x_1,\cdots,x_n)\vee Q(x_1,\cdots,x_n),\ P(x_1,\cdots,x_n)\wedge Q(x_1,\cdots,x_n)$$

$$P(x_1,\cdots,x_n)\to Q(x_1,\cdots,x_n),\ P(x_1,\cdots,x_n)\leftrightarrow Q(x_1,\cdots,x_n)$$

均为初等谓词。

证明　设 $P(x_1,\cdots,x_n)$，$Q(x_1,\cdots,x_n)$ 为 n 元初等谓词，$P(x_1,\cdots,x_n)$，$Q(x_1,\cdots,x_n)$ 的特征函数分别是，$\chi_P(x_1,\cdots,x_n)$ 和 $\chi_Q(x_1,\cdots,x_n)$。现只需证 $\neg P(x_1,x_2,\cdots,x_n)$ 和 $P(x_1,\cdots,x_n)\vee Q(x_1,\cdots,x_n)$ 为初等谓词，因为我们知道联结词组 $\{\neg,\vee\}$ 是完备的。由于

$$\chi_{\neg P}(x_1,\cdots,x_n)=\overline{sg}(\chi_P(x_1,\cdots,x_n))$$

$$\chi_{P\vee Q}(x_1,\cdots,x_n)=\max(\chi_P(x_1,\cdots,x_n),\chi_Q(x_1,\cdots,x_n))$$

而 $\chi_P(x_1,\cdots,x_n)$，$\chi_Q(x_1,\cdots,x_n)$ 已知是初等函数，因此 $\chi_{\neg P}(x_1,\cdots,x_n)$，$\chi_{P\vee Q}(x_1,\cdots,x_n)$ 是初等函数，进而 $\chi_{P\wedge Q}(x_1,\cdots,x_n)$，$\chi_{P\to Q}(x_1,\cdots,x_n)$，$\chi_{P\leftrightarrow Q}(x_1,\cdots,x_n)$，都是初等函数。命题得证。

定义 12-3　把形如 $\forall x(x\leqslant t\to P(x)),\exists x(x\leqslant t\wedge P(x))$ 的谓词公式简记为

$$\forall x\leqslant tP(x)\ \text{和}\ \exists x\leqslant tP(x)$$

并称 $\forall x\leqslant t$ 和 $\exists x\leqslant t$ 为**受限量词**（bounded quantifires）。

定理 12-2　初等谓词集合关于受限量词封闭。即当 $P(x)$，$Q(x)$ 为 n 元初等谓词，那么

$$\forall x\leqslant tP(x)\ \text{和}\ \exists x\leqslant tP(x)$$

均为初等谓词。

证明　设 $P(x)$，$Q(x)$ 为 n 元初等谓词，$P(x)$，$Q(x)$ 的特征函数分别是，$\chi_P(x)$ 和 $\chi_Q(x)$。那么 $\forall x\leqslant tP(x)$ 和 $\exists x\leqslant tP(x)$ 的特征函数应分别是

$$\prod_{i\leqslant t}\chi_P(i),\quad sg(\sum_{i\leqslant t}\chi_P(i))$$

由于 $\chi_P(x)$ 是初等函数，因此 $\forall x\leqslant tP(x)$ 和 $\exists x\leqslant tP(x)$ 的特征函数也是初等函数。

定理 12-3　设 $P_i(x_1,\cdots,x_n)$，$i=1,2,\cdots,m$，为 n 元初等谓词，且它们两两不同时为真；$f_i(x_1,\cdots,x_n)$，$i=1,2,\cdots,m,m+1$，为 n 元初等函数。那么，如下定义（也称凑合定义，definition by case）的函数 $h(x_1,\cdots,x_n)$ 是初等函数：

$$h(x_1,\cdots,x_n)=\begin{cases} f_1(x_1,\cdots,x_n) & \text{当 } P_1(x_1,\cdots,x_n)\text{真} \\ \quad\vdots & \\ f_m(x_1,\cdots,x_n) & \text{当 } P_m(x_1,\cdots,x_n)\text{真} \\ f_{m+1}(x_1,\cdots,x_n) & \text{否则} \end{cases}$$

证明 设 $\chi_{P_i}(x_1,\cdots,x_n)$ 是 $P_i(x_1,\cdots,x_n)$ 的特征函数，$i=1,2,\cdots,m$，它们都是初等函数。那么

$$h(x_1,\cdots,x_n)=f_1(x_1,\cdots,x_n)\cdot\chi_{P_1}(x_1,\cdots,x_n)+\cdots+f_m(x_1,\cdots,x_n)\cdot\chi_{P_m}(x_1,\cdots,x_n)+$$
$$f_{m+1}(x_1,\cdots,x_n)\cdot\prod_{i\leqslant m}\overline{sg}(\chi_{P_i}(x_1,\cdots,x_n))$$

不难看出，$h(x_1,\cdots,x_n)$ 是初等函数。

作为特例，可有：

定理 12-4 下列判定函数 $\mathrm{con}(x,y,s,t)$ 是初等函数：

$$\mathrm{con}(x,y,s,t)=\begin{cases} s & \text{当 } x=y \\ t & \text{当 } x\neq y \end{cases}$$

为进一步讨论初等函数和初等谓词，我们引入受限摹状操作。

定义 12-4 $\mu_{t\leqslant y}$ 称为**受限摹状操作**（或受限最小根操作，bounded minimalization operater）。对任一 $n+1$ 元谓词 $P(x_1,\cdots,x_n,t)$，$\mu_{t\leqslant y}P(x_1,\cdots,x_n,t)$ 定义一函数 $h(x_1,\cdots,x_n,y)$，其值为：使 $P(x_1,\cdots,x_n,t)$ 为真的、不大于 y 的、最小的 t；当这样的 t 不存在时，约定其值为 y。即

$$h(x_1,\cdots,x_n,y)=\begin{cases} t_0 & \text{使}P(x_1,\cdots,x_n,t_0)\text{真的最小值且}t_0\leqslant y \\ y & \text{否则} \end{cases}$$

定理 12-5 若 $n+1$ 元谓词 $P(x_1,\cdots,x_n,t)$ 是初等谓词，那么

$$h(x_1,\cdots,x_n,y)=\mu_{t\leqslant y}P(x_1,\cdots,x_n,t)$$

是初等函数。

证明 我们考虑简化了的情况，即证明

$$h(y)=\mu_{t\leqslant y}P(t)$$

是初等函数。其中 $P(t)$ 是初等谓词，令其特征函数为 $\chi_P(t)$，因而是初等函数。由于

$$h(y)=\mu_{t\leqslant y}P(t)=\mu_{t\leqslant y}(\chi_P(t)=1)=\sum_{k\leqslant x}\prod_{i\leqslant k}\overline{sg}(\chi_P(t))\overset{*}{-}\prod_{i\leqslant x}\overline{sg}(\chi_P(t))$$

$h(y)=\mu_{t\leqslant y}P(t)$ 是初等函数得证。

$\mu_{t\leqslant y}P(x_1,\cdots,x_n,t)$ 的直观可计算性是容易理解的。计算可以如此进行：依次计算 $P(x_1,\cdots,x_n,0)$，$P(x_1,\cdots,x_n,1),\cdots,P(x_1,\cdots,x_n,y)$，第一个使 $P(x_1,\cdots,x_n,t)$ 为真的 t 即为其值，否则取 y 为其值。

现在，我们可以借助初等谓词、凑合定义、受限摹状操作来确定以下函数是初等函数。（续例 12-1 中的 14 后）

（15）$npr(x)$ 表示不大于 x 的质数的数目，那么

$$npr(x)=\sum_{i\leqslant x}\chi_{\Pr}(i)$$

其中 $\Pr(x)$ 是初等谓词“x 是质数”。

（16）p_n 表示函数 $p(n)$：“第 n 个质数”，即 $p_1=2$，$p_2=3$，$p_3=5$，…，约定 $p_0=0$。那么

$$p_n=\begin{cases}0 & \text{当 } n=0\\ \mu_{i\leqslant A}(\Pr(i)\wedge npr(i)=n) & \text{当 } n\neq 0\end{cases}$$

其中 $A=2^{2^n}$，因为有数论结果：“第 n 个质数不大于 2^{2^n}”。

（17）$ep_n(x)$ 表示“x 的质因子分解式中第 n 个质数的指数”。例如，$ep_2(90)=2$，$ep_4(90)=0$，因为 $90=2\cdot 3^2\cdot 5$。那么

$$ep_n(x)=\begin{cases}0 & n=0\\ \mu_{t\leqslant x}(\neg(p_n^{t+1}\mid x)) & n\neq 0\end{cases}$$

其中 $\neg(p_n^{t+1}\mid x)$ 表示“p_n^{t+1} 不整除 x”。

有了以上几个函数，便可以用初等函数来表示正整数的质因子分解式：

$$n=\prod_{t\leqslant npr(n)-1}p_{t+1}^{ep_{t+1}(n)}\quad（\text{n 是正整数}）$$

通过以上讨论，我们看到，初等函数集合已经相当大，它包括了大多数人们熟悉的数论函数。很显然，初等函数都是全函数，都是直觉上可计算的函数。

12.2 原始递归函数集

上一节我们指出初等函数集相当大，初等函数也都是可计算的。那么，是否所谓可计算函数集合就是初等函数集呢？回答是否定的。

12.2.1 初等函数集的不足

考虑如下定义的诸函数。令 $f(x)=2^x$，用 f^n 表示 n 个 f 的合成，并约定 $f^0(x)=x$，$f^{n+1}(x)=f(f^n(x))$。现令 $k(n,x)=f^n(x)$，那么

$$k(0,x)=f^0(x)=x$$

$$k(1,x)=f^1(x)=2^x$$

$$k(2,x)=f^2(x)=2^{2^x}$$

$$\vdots$$

很明显，$k(n,x)=f^n(x)$ 是可计算的（$f(x)=2^x$ 是可计算的），但它不是初等函数。用两个定理来交代这件事情。

定理 12-6 对任一 n 元初等函数 $h(x_1,\cdots,x_n)$，都存在适当的 n,x，使得对一切 $x_1,\cdots,x_n$，

有

$$h(x_1,\cdots,x_n)\leqslant k(n,x) \quad (k(n,x)\text{ 如上定义})$$

证明 若初等函数 $h(x_1,\cdots,x_n)$ 为本原函数时

$$S(x)=x+1\leqslant k(1,x)$$

$$C_m^{(n)}(x_1,\cdots,x_n)=m\leqslant k(m,x)$$

$$p_m^{(n)}(x_1,\cdots,x_n)=x_m\leqslant k(0,x_m)$$

若初等函数 $h(x_1,\cdots,x_n)$ 为 $x_1\overset{*}{-}x_2$

$$x_1\overset{*}{-}x_2\leqslant x_1\leqslant k(0,x_1)$$

若初等函数 $h(x_1,\cdots,x_n)$ 为 $\sum\limits_{i\leqslant x_1} r(i,x_2,\cdots,x_n)$，而 $r(i,x_2,\cdots,x_n)$ 是初等函数。根据归纳假设，对任一 $i\leqslant x_1$，有 n，x，使 $r(i,x_2,\cdots,x_n)\leqslant k(n,x)$，取这些 $k(n,x)$ 中的最大者 $k(n_0,x_0)$，那么对一切 $i,x_2,\cdots,x_n$ 有

$$r(i,x_2,\cdots,x_n)\leqslant k(n_0,x_0)$$

于是

$$h(x_1,x_2,\cdots,x_n)=\sum_{i\leqslant x_1} r(i,x_2,\cdots,x_n)\leqslant(x_1+1)k(n_0,x_0)\leqslant k(n_0,x_0+x_1)$$

若初等函数 $h(x_1,\cdots,x_n)$ 为 $\prod\limits_{i\leqslant x_1} r(i,x_2,\cdots,x_n)$，而 $r(i,x_2,\cdots,x_n)$ 是初等函数。根据归纳假设，对任一 $i\leqslant x_1$，有 n，x，使 $r(i,x_2,\cdots,x_n)\leqslant k(n,x)$，取这些 $k(n,x)$ 中的最大者 $k(n_0,x_0)$，那么对一切 $i,x_2,\cdots,x_n$ 有

$$r(i,x_2,\cdots,x_n)\leqslant k(n_0,x_0)$$

于是

$$h(x_1,x_2,\cdots,x_n)=\prod_{i\leqslant x_1} r(i,x_2,\cdots,x_n)\leqslant k^{x_1+1}(n_0,x_0)\leqslant k(n_0,x_0\cdot x_1)$$

归纳完成，定理证毕。

定理 12-7 设 $k(n,x)=f^n(x)$，$f(x)=2^x$，那么 $k(n,x)=f^n(x)$ 不是初等函数。

证明 反设 $k(n,x)$ 是初等函数，那么 $k(n,x)+1$ 也是初等函数。根据定理 11-6，存在 n_0,x_0，使之对一切 n,x 有

$$k(n,x)+1\leqslant k(n_0,x_0)$$

取 $n=n_0,x=x_0$，于是

$$k(n_0,x_0)+1\leqslant k(n_0,x_0)$$

矛盾，定理得证。

读者也许会问，$k(n,x)=f^n(x)$ 究竟与“一般的 f 的 n 次合成”有什么区别呢？请注意 $k(n,x)=f^n(x)$ 中的 n 是一个函数的变元，不是参数、更不是常数。n 确定时 $f^n(x)$ 只是 f 的 n 次合成，因此它是初等函数；$k(n,x)=f^n(x)$ 中 n 是函数的变元，这是它不再是初等函数的

根本原因。

如果用读者容易理解的所谓递归式来定义 $k(n,x)=f^n(x)$ 似乎应该更容易明白些：

$$\begin{cases} k(0,x)=f^0(x)=x \\ k(n+1,x)=f(f^n(x))=f(k(n,x)) \end{cases}$$

这正是我们下文要深入讨论的关键所在。

12.2.2 原始递归式

我们常常看到有人用以下等式组来定义或计算阶乘函数：

$$\begin{cases} 0!=1 \\ (n+1)!=(n+1)\cdot n! \end{cases}$$

它描述了一种计算过程，其特点是：计算一个函数的现行值时要使用这个函数的已知值，因而被称为递归计算。上述等式组就是我们要讨论的原始递归式的一种形式。

定义 12-5 设 $g(x_1,\cdots,x_n)$，$h(x_1,\cdots,x_n,u,v)$ 分别是已知的 n 元和 $n+2$ 元函数，那么下列定义函数 $f(x_1,\cdots,x_n,x_{n+1})$ 的等式组称为定义 f 的**原始递归式**（primitive recursions）：

$$\begin{cases} f(x_1,\cdots,x_n,0)=g(x_1,\cdots,x_n) \\ f(x_1,\cdots,x_n,y+1)=h(x_1,\cdots,x_n,y,f(x_1,\cdots,x_n,y)) \end{cases}$$

或简单地

$$\begin{cases} f(0)=g \quad (g\text{是常数}) \\ f(y+1)=h(y,f(y)) \end{cases}$$

原始递归式有一种最简单的形式：

$$\begin{cases} f(0)=g \quad (g\text{是常数}) \\ f(y+1)=h(f(y))=\cdots=h^{y+1}(g) \end{cases}$$

称为**复迭式**，定理 12-7 中的 $k(n,x)=f^n(x)$ 就是用复迭式定义的。

原始递归式是否良定呢？即给定 $g(x_1,\cdots,x_n)$，$h(x_1,\cdots,x_n,u,v)$ 是否总能惟一地确定函数 $f(x_1,\cdots,x_n,x_{n+1})$ 满足这一等式组呢？回答是肯定的。我们不对这一结论进行证明，直觉地理解应当没有什么困难。下文是几个用原始递归式定义的函数。

用投影函数和后继函数定义二元加函数：

$$\begin{cases} x+0=x \\ x+(y+1)=(x+y)+1 \end{cases}$$

用常函数和二元加函数定义二元乘函数：

$$\begin{cases} x\cdot 0=0 \\ x\cdot(y+1)=(x\cdot y)+x \end{cases}$$

用常函数和二元乘函数定义二元指数函数：

$$\begin{cases} x^0=1 \\ x^{y+1}=x^y\cdot x \end{cases}$$

12.2.3 原始递归函数

现归纳地定义原始递归函数集合。

定义 12-6

（1）本原函数：后继函数、常值函数和投影函数是原始递归函数。

（2）如果 $g_1(x_1,\cdots,x_n)$，…，$g_m(x_1,\cdots,x_n)$，$h(x_1,\cdots,x_m)$ 是原始递归函数，那么，复合函数 $h(g_1(x_1,\cdots,x_n)$，…，$g_m(x_1,\cdots,x_n))$ 也是原始递归函数。

（3）如果 $g(x_1,\cdots,x_n)$，$h(x_1,\cdots,x_n,u,v)$ 是原始递归函数，那么原始递归式

$$\begin{cases} f(x_1,\cdots,x_n,0)=g(x_1,\cdots,x_n) \\ f(x_1,\cdots,x_n,y+1)=h(x_1,\cdots,x_n,y,f(x_1,\cdots,x_n,y)) \end{cases}$$

定义的函数 $f(x_1,\cdots,x_n,x_{n+1})$ 也是原始递归函数。

（4）只有有限步使用上述条款生成的函数才是原始递归函数。

在 12.2.1 中引入的函数 $k(n,x)=f^n(x)$ 不是初等函数，但它显然是原始递归函数。我们有更为重要的结论：

定理 12-8 初等函数集合是原始递归函数集合的真子集。

证明 由于上述函数 $k(n,x)=f^n(x)$ 的存在，只需证明初等函数集合是原始递归函数集合的子集。为此，对初等函数集合的组成进行归纳。

显然，本原函数是原始递归函数。

为证 $x\overset{*}{-}y$ 是原始递归函数，先证 $x\overset{*}{-}1$ 是原始递归函数。$x\overset{*}{-}1$ 可用原始递归式定义如下：

$$\begin{cases} 0\overset{*}{-}1=0 \\ (x+1)\overset{*}{-}1=x \end{cases}$$

因此 $x\overset{*}{-}1$ 是原始递归函数。而

$$\begin{cases} x\overset{*}{-}0=x \\ x\overset{*}{-}(y+1)=(x\overset{*}{-}y)\overset{*}{-}1 \end{cases}$$

因而 $x\overset{*}{-}y$ 是原始递归函数。

设用迭加操作定义的初等函数（为简明将参变元省去）

$$g(u)=\sum_{x\leqslant u} f(x)$$

其中 $f(x)$ 是初等函数。根据归纳假设，$f(x)$ 是原始递归函数。那么 $g(u)$ 可用原始递归式定

义如下：

$$\begin{cases} g(0)=f(0) \\ g(x+1)=g(x)+f(x+1) \end{cases}$$

因此 $g(u)=\sum_{x\leqslant u} f(x)$ 也是原始递归函数。

若用迭乘操作定义 $g(u)=\prod_{x\leqslant u} f(x)$，那么它的原始递归性仿此可证。

归纳完成，定理得证。

原始递归函数还有许多重要性质。例如：

定理 12-9 设 $f(x)$是原始递归函数，那么用它和受限摹状操作定义的函数

$$g(x)=\mu_{i\leqslant x}(f(i)=0)$$

也是原始递归函数。

证明 回忆受限摹状操作定义和定理 12-5 的证明。$\mu_{i\leqslant x}(f(i)=0)$ 等于使 $f(i)=0$ 的最小的 i，如果这样的 i 不存在，它取值 x。因此

$$g(x)=\mu_{i\leqslant x}(f(i)=0)=\sum_{k\leqslant x}\prod_{i\leqslant k} sg(f(i))\dot{-}\prod_{i\leqslant x} sg(f(i))$$

这表明 $g(x)$ 是原始递归函数。

定理 12-10 设 $f_1(x)$，…，$f_k(x)$ 是原始递归函数，$g(x)$ 定义如下，

$$g(x)=\begin{cases} f_1(x) & \text{当 } x=a_1 \\ \vdots & \\ f_k(x) & \text{当 } x=a_k \\ 0 & \text{否则} \end{cases}$$

那么，$g(x)$也是原始递归函数。

请读者自己证明。

定义 12-7 n 元谓词 $P(x_1,x_2,\cdots,x_n)$ 称为**原始递归谓词**（primitive recursive predicates），如果它的特征函数$\chi_P(x_1,x_2,\cdots,x_n)$ 为原始递归函数。

显然，所有初等谓词都是原始递归谓词。关于原始递归谓词的以下性质是容易证明的（与初等谓词同类性质的证明相仿）。

定理 12-11 原始递归谓词集合对命题联结词、受限量词封闭。

定理 12-12 设 $P_i(x_1,\cdots,x_n)$，$i=1,2,\cdots,m$，为 n 元原始递归谓词，且它们两两不同时为真；$f_i(x_1,\cdots,x_n)$，$i=1,2,\cdots,m,m+1$，为 n 元原始递归函数。那么，如下凑合定义的函数 $h(x_1,\cdots,x_n)$ 也是原始递归函数：

$$h(x_1,\cdots,x_n)=\begin{cases} f_1(x_1,\cdots,x_n) & \text{当 } P_1(x_1,\cdots,x_n)\text{真} \\ \vdots & \\ f_m(x_1,\cdots,x_n) & \text{当 } P_m(x_1,\cdots,x_n)\text{真} \\ f_{m+1}(x_1,\cdots,x_n) & \text{否则} \end{cases}$$

定理 12-13 若 $n+1$ 元谓词 $P(x_1,\cdots,x_n,t)$ 是原始递归谓词，那么

$$h(x_1,\cdots,x_n,y)=\mu_{t\leqslant y}P(x_1,\cdots,x_n,t)$$

是原始递归函数。

请读者自行证明本定理。

原始递归函数都是全函数，也都是直觉上可计算的函数。

以上讨论表明，原始递归函数集合是一个更大的直觉上可计算的函数集合。人们已经很难找出一个直觉上可计算的全函数，而又使它不是一个原始递归函数。那么，是否可以断言，原始递归函数集合正是我们要想知道的那个可计算的函数集合呢？回答又是否定的。

12.3 递归函数集

我们已经指出，原始递归函数集合已经相当广大，以至于要作出一个可计算的非原始递归的全函数，已非一件易事，但这样的函数是确实存在的，著名的阿克曼（Ackerman）函数就是十分重要的一个。

12.3.1 阿克曼函数及其性质

定义 12-8 称下列等式组定义的函数 $A(x,y)$ 为**阿克曼函数**。

$$\begin{cases}A(0,y)=y+1\\A(x+1,0)=A(x,1)\\A(x+1,y+1)=A(x,A(x+1,y))\end{cases}$$

阿克曼函数在直觉上是可计算的。

【例 12-2】 计算 $A(2,2)$。

$$\begin{aligned}A(2,2)&=A(1,A(2,1))\\&=A(1,A(1,A(2,0)))\\&=A(1,A(1,A(1,1)))\\&=A(1,A(1,A(0,A(1,0))))\\&=A(1,A(1,A(0,A(0,1))))\\&=A(1,A(1,3))\\&=A(1,A(0,A(1,2)))\\&=A(1,A(0,A(0,A(1,1))))\\&=A(1,A(0,A(0,3)))\\&=A(1,5)\\&=A(0,A(0,A(1,3)))\\&=A(0,A(0,5))\\&=7\end{aligned}$$

阿克曼函数有许多有趣的性质。

定理 12-14 对任意 x,y，$A(x,y)>y$。

证明 先对 x 归纳。

归纳基础 1：$x=0$ 时，$A(x,y)=A(0,y)=y+1>y$。

归纳过程 1：设 $A(x,y)>y$，要证 $A(x+1,y)>y$。为此再对 y 归纳。

归纳基础 2：$y=0$ 时，$A(x+1,y)=A(x+1,0)=A(x,1)>1>0=y$。

归纳过程 2：设 $A(x+1,y)>y$，要证 $A(x+1,y+1)>y+1$。由于

$$\begin{aligned}A(x+1,y+1)&=A(x,A(x+1,y))\\&>A(x+1,y)\ (\text{由归纳假设 } A(x,y)>y)\\&\geqslant A(x,y)+1\\&>y+1\ (\text{由归纳假设 } A(x+1,y)>y)\end{aligned}$$

这样，双层归纳完成，定理得证。

定理 12-15 对任意 x,y，$A(x,y+1)>A(x,y)$。

证明 对 x 归纳。

归纳基础：$x=0$ 时，$A(x,y+1)=A(0,y+1)=y+2>y+1=A(x,y)$。

归纳过程：设 $A(x,y+1)>A(x,y)$，要证 $A(x+1,y+1)>A(x+1,y)$。而

$$A(x+1,y+1)=A(x,A(x+1,y))>A(x+1,y)\ (\text{据定理 11-4})$$

归纳完成，定理得证。

定理 12-16 对任意 x，若 $s>t$，那么 $A(x,s)>A(x,t)$

这一定理是定理 12-15 的直接推论。

定理 12-17 对任意 x,y，$A(x+1,y)\geqslant A(x,y+1)$。

证明 对 y 归纳。

归纳基础：$y=0$ 时，$A(x+1,y)=A(x+1,0)=A(x,1)=A(x,y+1)$。

归纳过程：设 $A(x+1,y)\geqslant A(x,y+1)$，要证 $A(x+1,y+1)\geqslant A(x,y+2)$。由于

$$A(x+1,y)\geqslant A(x,y+1)\geqslant y+2\ (\text{由归纳假设和定理 12-14})$$

于是

$$A(x+1,y+1)=A(x,A(x+1,y))\geqslant A(x,y+2)$$

归纳完成，定理得证。

定理 12-18 对任意 x,y，$A(x,y)\geqslant x$。

用定理 12-17 和简单的归纳法即可证明：

$$A(x,y)\geqslant A(0,x+y)=x+y+1>x$$

证明细节请读者补充。

定理 12-19 对任意 x,y，$A(x+1,y)>A(x,y)$。

证明

$$\begin{aligned}A(x+1,y)&=A(x,A(x+1,\overset{*}{y-1}))\\&>A(x,A(x,y))\qquad(\text{据定理 12-17 和定理 12-16})\\&>A(x,y)\end{aligned}$$

定理 12-20 对任意 y，若 $s>t$，那么 $A(s,y)>A(t,y)$。

这一定理是定理 12-19 的直接推论。

定理 12-21 对任意 x,y，$A(x+2,y)>A(x,2y)$。

对 y 归纳进行证明，与以上定理的证明雷同。

定理 12-22 阿克曼函数不是原始递归函数。

利用上述阿克曼函数的性质证明本定理并不十分困难，但篇幅相当大，我们不介绍这个证明了，有兴趣的读者可以在相关文献查阅[7]。重要的是，出现了一个可计算的非原始递归函数，这迫使人们去进一步探索可计算函数集合的奥秘。

12.3.2 μ-递归式

可计算的非原始递归函数存在，迫使我们要扩大原始递归函数集合，扩大的方式看来也只能是采用更加有力的操作。一个可供的选择是：将已经使用过的受限摹状操作加强为不受限的摹状操作——摹状操作（最小根操作）。

定义 12-9 摹状操作 μ_t 是作用于 $n+1$ 元谓词 $P(t,x_1,\cdots,x_n)$ 生成如下 n 元（偏）函数 $f(x_1,\cdots x_n)$ 的操作：

$$\mu_t P(t,x_1,\cdots,x_n)=f(x_1,\cdots,x_n)=\begin{cases}t_0 & t_0\text{是使}P(t,x_1,\cdots,x_n)\text{真的最小值}\\ \uparrow(\text{无定义}) & \text{使}P(t,x_1,\cdots,x_n)\text{真的}t\text{不存在}\end{cases}$$

注意：

（1）摹状操作生成的 f 未必是全函数，完全可能是一个真偏函数。本章下文中的函数一词常指偏函数（全函数或真偏函数）

（2）以下常对形如 $g(t,x_1,\cdots,x_n)=0$（其中 g 为全函数）的 $P(t,x_1,\cdots,x_n)$ 用摹状操作，因而也常说 μ_t 是作用于 $n+1$ 元函数的操作。

【例 12-3】

（1） $\mu_t(t+x=0)=f(x)=\begin{cases}0 & \text{当}x=0\\ \uparrow & \text{当}x\neq 0\end{cases}$

（2）用 $\left[\frac{y}{x}\right]^*$ 表示人们日常使用的求商取整函数，它与我们先前定义的 $\left[\frac{y}{x}\right]$ 的不同之处在于，当 $x=0$ 时 $\left[\frac{y}{x}\right]^*$ 无定义，而 $\left[\frac{y}{x}\right]=0$。$\left[\frac{y}{x}\right]^*$ 可用摹状操作来定义：

$$\left[\frac{y}{x}\right]^*=\mu_t(1\overset{*}{-}sg((t+1)\overset{*}{x}-y)=0)$$

（3）受限摹状操作可以用摹状操作以及初等函数来表示：

$$\mu_{x\leqslant y}(f(u,x)=0)=\mu_x(f(u,x)\cdot\overline{sg}(eq(x,y))=0)$$

$$\mu_{x\leqslant y}(P(u,x))=\mu_x(P(u,x)\vee x=y)$$

12.3.3 递归函数集（μ-递归函数集）

定义 12-10 归纳定义**μ-递归函数集**。μ-递归函数集也称**递归函数集**。

（1）本原函数：后继函数、常值函数和投影函数是μ-递归函数。

（2）如果 $f(x_1,\cdots,x_n)$ 与 $g_1(y_1,\cdots,y_m)$，…，$g_n(y_1,\cdots,y_m)$ 都是μ-递归函数，那么它们

的合成 $f(g_1(y_1,\cdots,y_m),\cdots,g_n(y_1,\cdots,y_m))$ 也是μ-递归函数。

（3）如果 $g(x_1,\cdots,x_n)$，$h(x_1,\cdots,x_n,u,v)$ 是μ-递归函数，那么原始递归式

$$\begin{cases} f(x_1,\cdots,x_n,0)=g(x_1,\cdots,x_n) \\ f(x_1,\cdots,x_n,y+1)=h(x_1,\cdots,x_n,y,f(x_1,\cdots,x_n,y)) \end{cases}$$

定义的函数 $f(x_1,\cdots,x_n,x_{n+1})$ 也是μ-递归函数。

（4）如果 g 是 $n+1$ 元μ-递归全函数，那么由 g 和摹状操作定义的函数 f

$$f(x_1,\cdots,x_n)=\mu_t(g(t,x_1,\cdots,x_n)=0)$$

也是μ-递归函数。

（5）只有有限步使用上述条款生成的函数才是μ-递归函数。

需要对这一定义做些说明。

（a）显然原始递归函数都是μ-递归函数。

（b）定义中的条款（4）可能生成真偏函数，因此条款（2），（3）中的函数 g, h 可能也不是全函数。这并不影响条款（2），（3）的使用，只是此时它们生成的也不是全函数（我们约定当函数的变目无定义时，其函数值也无定义）。

（c）定义要求摹状操作 μ_t 必须作用于全函数，这是为了讨论的简化。

（d）直观上μ-递归函数是可计算的。如果μ-递归函数 f 是由条款（4）生成，那么，为了计算 $f(x_1,\cdots,x_n)$，只要逐个计算 $g(0,x_1,\cdots,x_n)$，$g(1,x_1,\cdots,x_n)$，$g(2,x_1,\cdots,x_n)$，…，直至发现 t，使得 $g(t,x_1,\cdots,x_n)=0$，否则计算将不会终止，$f(x_1,\cdots,x_n)$ 无定义。

如此作出的递归函数集是否能如愿以偿呢？

定理 12-23 阿克曼函数是μ-递归函数，因此原始递归函数集是μ-递归函数集的真子集。

本定理的证明比较复杂，超出了本教材的要求，略去。

丘奇-图灵论题：可计算函数集等同于递归函数集（μ-递归函数）。

由于可计算函数集没有形式定义，这个论题不是一条定理，它是丘奇、图灵给出的一个假设，也可以说这是丘奇、图灵给出的可计算函数的定义。该假设已经提出半个多世纪，至今尚未有人给出反例。即没有人找到一个直觉可计算的函数，它不是递归函数；也没有人对递归函数的可计算性提出任何异议。

事实上，这一假设提出还有另一个有力的背景。图灵提出了一种重要的计算模型——图灵机，它简单得让人无法否认使用它计算的能行性，它又强大得足以模拟现有的所有计算模型。人们称用图灵机可计算的函数为图灵可计算函数。一个人们意料之中而又十分精妙的事实被证明：图灵可计算函数集等同于递归函数集。下一节我们要对图灵机作一个简单的介绍。

*12.4 图灵机与可计算函数集

12.4.1 图灵机

图灵机（Turing Machines）是一种理想机，一种计算模型。最基本的图灵机由一根假设两端可无限延长的**带**（读写的载体）和一个具有**读写头**的**控制器**所组成（见图 12-1）。带起着与存储器类似的作用，它被划分成大小相同的方格，每一方格上可由读写头书写一个给定字母表上的符号，或保持空白，并且约定空白的方格用“0”表示，数 0 用符号“1”表示，

而自然数 n 则用 $n+1$ 个 1 的毗连来表示。控制器可在带上左右移动，在此过程中，读写头每经过一个方格便访问之，读出方格上的符号，同时根据读得的符号，由控制器依据自己的**状态**决定是否改写该符号（改写为 0 即表示抹去方格上的原符号），决定读写头继续移动的方向，决定控制器自身要进入的后继状态。控制器的状态是根据计算目的事先设计而定的，常用字母 $q_0, q_1, q_2, \cdots$ 来表示，q_0 常表示初始状态。

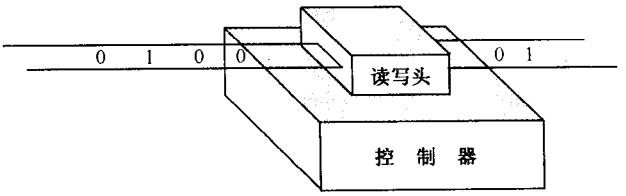


图 12-1

图灵机的运行过程可以如下简单地描述。机器最初有一根记录着表示**输入**的符号序列的带，称为**初始带**，带上某一特定的方格被置于读写头之下，这时带上的符号串连同读写头位置标识符“_”称为**初始带形**（或输入带形）。控制器先处于**初始状态** q_0。机器从初始状态和初始带形出发，依据机器控制器内设定的“程序”（一张**状态转换表**，简称**状态表**）运行：由读写头当前读得符号和控制器当前状态，确定如何改写这一符号，读写头向哪个方向移动一格，控制器进入哪个后续状态。这样一个系列的操作，称为图灵机运行的一步。当运行终止时，其带形称为**终止带形**，带上的符号串便是这次计算的**输出**；当运行无休止地进行下去时，称机器对本输入**无定义**。

从以上描述可以看出，决定一台图灵机的是那张状态转换表。图 12-2 是一台简单图灵机的状态转换表。表中 q_0，1 对应的分量 $0Rq_1$，表示机器处状态 q_0 并读得 1 时，要将读得的符号 1 改写为 0（即抹去 1 成为空格），同时读写头右移一格（R，L 表示右移和左移），控制器进入状态 q_1。表中 q_2，0 对应的分量 $0Lq_3$，表示机器处状态 q_2 并读得 0 时，读得的符号 0（空格）保持不变，同时读写头左移一格，控制器进入状态 q_3。表中 q_0，0 和 q_2，1 无对应的分量，表示机器在这两种情况下停止运行。

当前状态	读得符号	
	0	1
q_0		$0Rq_1$
q_1	$1Rq_2$	$1Rq_1$
q_2	$0Lq_3$	
q_3	$0Rq_0$	$1Lq_3$

图 12-2

除了状态转换表，还有一种直观地描述图灵机的方法——**状态转换图**（简称**状态图**），一种有向加权图。图 12-3a 是一台图灵机的状态图，它与 图 12-2 表示的图灵机等同。这里每一个结点表示一个状态，结点中标记的是进入这一状态时读写头的移动方向。每一条有向边表示一步运行，有向边起始结点是这一步的起始状态，有向边到达结点是这一步的后继状态（用没有到达结点的边表示停机），边上标记的是这一步对符号的改写，标记 x/y 表示将 x 改写为 y。

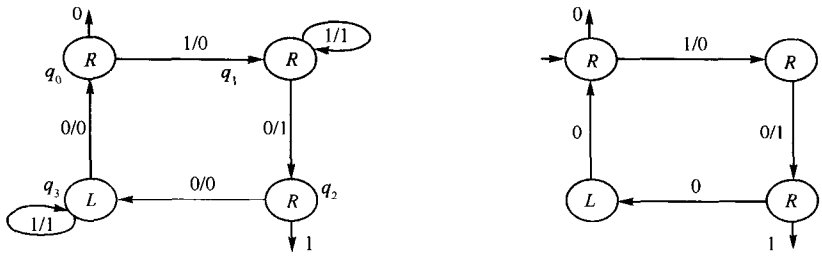


图 12-3

图 12-3b 是 图 12-3a 的简化形式（以后我们主要使用这种简化形式）。它与原图的不同在于：省去了结点状态的标记，用一个只有终点的有向边表示起始状态 q_0；用标记 x 代替 x/x，表示保持原符号 x 不变；省去了表示既不改变状态，也不改写符号的运行的边（标记 x/x 的环）。

【例 12-4】 假定上述图灵机具有初始带形 $\underline{1}1100011$，如 图 12-4（a）所示。第一个 1 下面的横线表示读写头的初始位置。开始运行后，第一步依 q_0，1 相应分量 $0Rq_1$ 运行，即把 1 抹去，向右移动读写头并使控制器进入状态 q_1。第二步依 q_1，1 相应分量 $1Rq_1$ 运行，即保留 1，向右移动读写头并使控制器仍处于状态 q_1。第三步重复上一步的操作，如此等等，直至读写头越过第一个**幺段**（由连续的 1 组成的符号段。仿此，**s 段**指连续的 s 组成的符号段）。这时，控制器仍处于状态 q_1，读写头读出的符号为 0，从而图灵机依 q_1，0 相应分量 $1Rq_2$ 运行，即把 0 改写为 1，向右移动读写头并使控制器进入状态 q_2（这时带形如 图 12-4（b）所示）。现在机器据 q_2，0 相应分量 $0Lq_3$ 运行。此后，机器据 q_3，1 相应分量 $1Lq_3$ 向左移动越过第一个幺段，直至读写头向左遇到第一个 0。于是机器又依 q_3，0 相应分量 $0Rq_0$ 运行，使带形变得如 图 12-4（c）所示，而控制器回到状态 q_0。此时机器又从头开始下一轮运行，直至达到 图 12-4（d）所示带形。如此往复，每一轮循环恰好使第一个幺段右移一格。等到第一个幺段与第二个幺段相毗连时，带形应如图 12-4（e）所示，控制器处于状态 q_2，读写头访问符号 1，于是图灵机停机。读者也许想象得到，这大概是一台加法机。

下面介绍几个重要的图灵机。

1．拷贝机

拷贝机是指能把初始带型中的某个幺段（或一般的 s 段）拷贝到某个指定位置的图灵机。我们约定待拷贝的幺段用 A 标记，指定位置用 B 标记。图 12-5 是一台拷贝机。

(a) … 00$\underline{1}$1100011100 …
(b) … 000111$\underline{0}$01100 …
(c) … 000$\underline{1}$11001100 …
(d) … 0000111$\underline{0}$1100 …
(e) … 000001111$\underline{1}$100 …

图 12-4

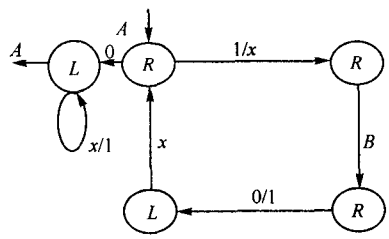


图 12-5

它的运行过程可如下描述：

（1）将待拷贝幺段的左边第一个 1 用新符号 x 替代。

（2）右移到 *B* 右边的第一个空格处写下 1。

（3）折返到左边，直到读写头访问到 *x* 时向右移动一格。

（4）如果读写头访问 1，又用 *x* 替代之，返回（2）；否则执行（5）。

（5）左移，将 *x* 改回为 1，访问 A 时停机。

图 12-6 是拷贝机的一个运行实例的带形演变进程。（a）是初始带形，（e）是输出带形。

2. 匹配机

匹配机是指能用于判断两个幺段的长度（即 1 的数目）是否相等的图灵机，也就是计算相等性函数的图灵机。

我们约定待判断的两个幺段用 *A*，*B* 标记。图 12-7 是一台匹配机。其中虚线部分的功能和拷贝机大体一样。拷贝机机理弄清楚了，匹配机也就不难理解了。

(a) … *A*11101100*B*00000 …
(b) … *Ax*1101100*B*10000 …
(c) … *Axx*101100*B*11000 …
(d) … *Axxx*01100*B*11100 …
(e) … *A*11101100*B*11100 …

图 12-6

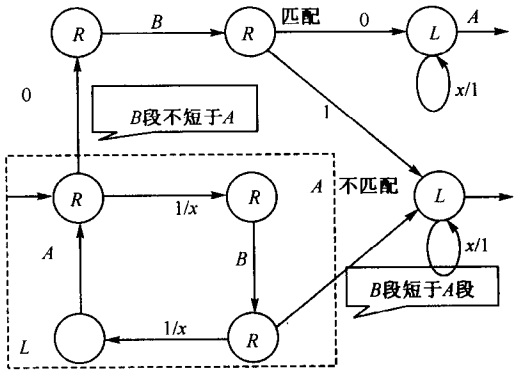


图 12-7

3. 段代换机

段代换机是指能用标准带型中的某个幺段去代换另一个幺段的图灵机。标准带型要求各个幺段间用一个 0 间隔，最右边的幺段毗邻至少两个 0。段代换机要求代换过程中不能改变原来两个幺段的“环境”。约定 B 标记代换段，C 表示被代换段。设初始带形是 图 12-8（a），其输出带形应当是 图 12-8（c）。

图 12-9 是一台段代换机。

它的运行过程可以分为两个阶段。第一阶段中，首先右移到最右边一个幺段，向左折返时变每一幺段的第一个 1 为 0，将遇到的 0 改为 1，使 *C* 段右边部分带形左移了一格，却将 *C* 段中的 1 抹去一个（如图 12-8（b）所示）。只要 *C* 段中还有 1，重复这一过程，可将 *C* 段中的 1 全部抹去（如图 12-8（c）所示）。第二阶段中，在将 *B* 标记的幺段拷贝到 *C* 右侧时，同时不断地右移原 *C* 标记幺段右边部分的带形（如 图 12-8（d）所示）。

(a) … *B*11111010111C11101011100…
(b) … B11111010111*C*1101011100…
(c) … *B*11111010111*C*01011100…
(d) … *B*11111010111C11111010111100…

图 12-8

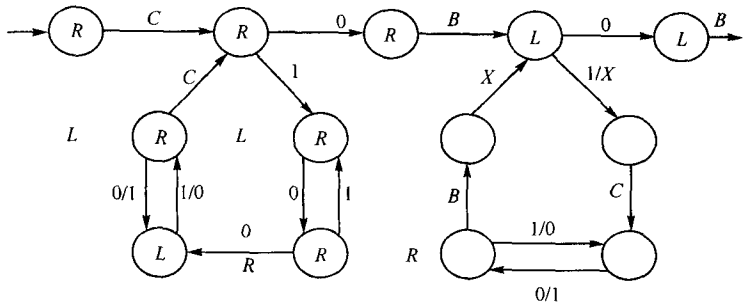


图 12-9

12.4.2 图灵可计算函数

定义 12-11 $f(x_1,\cdots x_n)$称为**图灵可计算函数**，如果存在一台图灵机，它对输入带形

$$\cdots 0\underline{0}\overline{x_1}0\overline{x_2}0\overline{x_3}0\cdots 0\overline{x_n}0\cdots$$

以下列输出带形停机

$$\cdots 0\underline{0}\overline{f(x_1,x_2,\cdots,x_n)}0\cdots$$

其中$\overline{y}$表示由 $y+1$ 个 1 组成的幺段，表示数零的幺段是“1”。我们约定，当图灵机不停机或者不能以指定形式停机时，表示 $f(x_1,\cdots,x_n)$ 对输入 $x_1,\cdots,x_n$ 无定义。

【例 12-5】 图 12-10a 是计算二元加函数的图灵机，图 12-10b 是计算二元单向减函数的图灵机。单向减函数定义如下

$$x\underline{\Delta}y=\begin{cases}x\overset{*}{-}y & \text{当 } x\geqslant y\\ \uparrow & \text{否则}\end{cases}$$

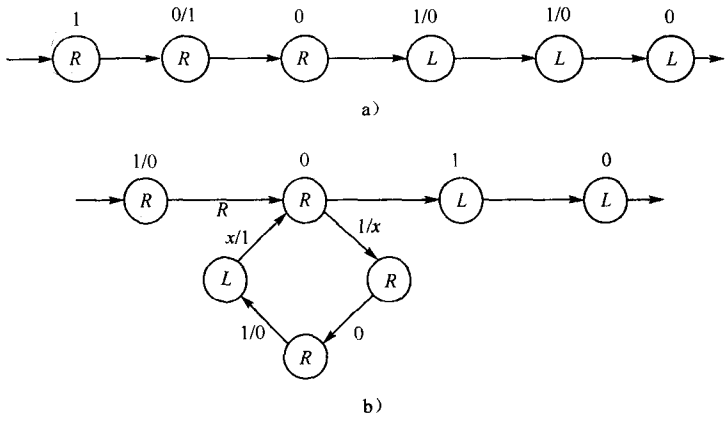


图 12-10

定理 12-24 本原函数：后继函数、常值函数和投影函数是图灵可计算函数。

证明 图 12-10a、b、c 分别是可计算后继函数 $S(x)=x+1$、常值函数 $C_m^{(n)}(x_1,\cdots,x_n)=m$

和投影函数 $p_m^{(n)}(x_1,\cdots,x_n)=x_m$ 的图灵机。

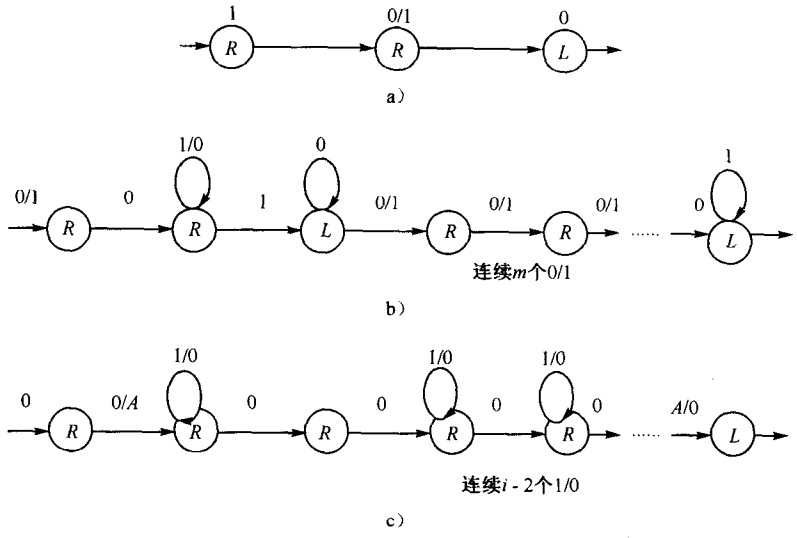


图 12-11

定理 12-25 如果 $g_1(x_1,\cdots,x_n)$，…，$g_m(x_1,\cdots,x_n)$，$h(x_1,\cdots,x_m)$ 是图灵可计算函数,那么，复合函数 $h(g_1(x_1,\cdots,x_n)$，…，$g_m(x_1,\cdots,x_n))$ 也是图灵可计算函数。

证明 计算 $h(g_1(x_1,\cdots,x_n)$，…，$g_m(x_1,\cdots,x_n))$ 的图灵机可如下设计。

将输入符号串 $\underline{0}\overline{x_1}0\overline{x_2}0\overline{x_3}0\cdots0\overline{x_n}0$ 拷贝 $m-1$ 份，从最右边的那一段开始，逐个计算 $g_m(x_1,\cdots,x_n)$，…，$g_1(x_1,\cdots,x_n)$。然后对

$$\cdots0\underline{0}\overline{g_1(x_1,x_2,\cdots x_n)}0\overline{g_2(x_1,x_2,\cdots x_n)}0\cdots0\overline{g_m(x_1,x_2,\cdots x_n)}0\cdots$$

计算 $h(g_1(x_1,\cdots,x_n)$，…，$g_m(x_1,\cdots,x_n))$。（注意：$g_1(x_1,\cdots,x_n)$，…，$g_m(x_1,\cdots,x_n)$，$h(x_1,\cdots,x_m)$ 是图灵可计算的，至于计算这些函数的图灵机如何联结成计算 $h(g_1(x_1,\cdots,x_n)$，…，$g_m(x_1,\cdots,x_n))$ 的图灵机的细节，我们不作详解）。

定理 12-26 如果 $g(x_1,\cdots,x_n)$，$h(x_1,\cdots,x_n,u,v)$ 是图灵可计算函数，那么原始递归式

$$\begin{cases} f(x_1,\cdots,x_n,0)=g(x_1,\cdots,x_n) \\ f(x_1,\cdots,x_n,y+1)=h(x_1,\cdots,x_n,y,f(x_1,\cdots,x_n,y)) \end{cases}$$

定义的函数 $f(x_1,\cdots,x_n,x_{n+1})$ 也是图灵可计算函数。

证明 设计算 $g(x_1,\cdots,x_n)$ 和 $h(x_1,\cdots,x_n,u,v)$ 的图灵机是 $T1$ 和 $T2$。计算 $f(x_1,\cdots,x_n,x_{n+1})$ 的图灵机 T 可如下设计。

T 首先将输入符号串 $\underline{0}\overline{x_1}0\overline{x_2}0\overline{x_3}0\cdots0\overline{x_n}0\ \ \overline{x_{n+1}}\ 0$ 改写为

$$0\overline{x_1}0\overline{x_2}0\cdots0\overline{x_n}0\ \ \overline{x_{n+1}}\ 0\ \overline{x_1}0\overline{x_2}0\cdots0\overline{x_n}0\ \ \overline{x_{n+1}-1}\ 0\cdots\cdots\underline{0}\overline{x_1}0\overline{x_2}0\cdots0\overline{x_n}0\ \ \overline{0}\ \ 0$$

用 T1 和 $\underline{0}\overline{x_1}0\overline{x_2}0\overline{x_3}0\cdots0\overline{x_n}0\ \ \overline{0}\ 0$ 计算出 $0\overline{g(x_1,\cdots,x_n)}0$；然后用 $T2$

依据 $\underline{0}\overline{x_1}0\overline{x_2}0\cdots0\overline{x_n}0\ \ \overline{1}\ \ 0\overline{g(x_1,\cdots,x_n)}0$ 计算出 $0\overline{f(x_1,\cdots,x_n,1)}0$

依据 $\underline{0}\overline{x_1}0\overline{x_2}0\cdots0\overline{x_n}0\ \ \overline{2}\ \ 0\overline{f(x_1,\cdots,x_n,1)}0$ 计算出 $0\overline{f(x_1,\cdots,x_n,2)}0$

⋮

依据 $\underline{0}\overline{x_1}0\overline{x_2}0\cdots0\overline{x_n}0\ \ \overline{x_{n+1}-1}\ \ 0\overline{f(x_1,\cdots,x_n,x_{n+1}-1)}0$ 计算出 $0\overline{f(x_1,\cdots,x_n,x_{n+1})}0$

图灵机 T 如何由图灵机 $T1$ 和 $T2$ 联结而成的细节仍然略去。

定理 12-27 如果 $g(x_0,\cdots,x_{n-1},x_n)$ 是 $n+1$ 元图灵可计算全函数，那么由 g 和摹状操作定义的函数 $f(x_1,\cdots,x_n)$，

$$f(x_1,\cdots,x_n)=\mu_t(g(t,x_1,\cdots,x_n)=0)$$

也是图灵可计算函数。

证明 设计算 $g(x_0,x_1,\cdots,x_n)$ 的图灵机为 $T1$，那么计算 $f(x_1,\cdots,x_n)$ 的图灵机 T 可以如下设计：

T 首先将输入带形 $\underline{0}\overline{x_1}0\overline{x_2}0\overline{x_3}0\cdots0\overline{x_n}0$ 改写为 $\underline{0}\ \overline{0}\ 0\ \overline{x_1}0\overline{x_2}0\overline{x_3}0\cdots0\overline{x_n}0$，用 $T1$ 计算之，由于 g 为全函数，$T1$ 必定停机，判定其值是否为 0，若是，$f(x_1,\cdots,x_n)=0$；若不然，将 $\underline{0}\ \overline{0}\ 0\ \overline{x_1}0\overline{x_2}0\overline{x_3}0\cdots0\overline{x_n}0$ 改写为 $\underline{0}\ \overline{1}\ 0\ \overline{x_1}0\overline{x_2}0\overline{x_3}0\cdots0\overline{x_n}0$，再用 $T1$ 计算之，判定其值是否为 0，若是，$f(x_1,\cdots,x_n)=1$；若不然将 $\underline{0}\ \overline{1}\ 0\ \overline{x_1}0\overline{x_2}0\overline{x_3}0\cdots0\overline{x_n}0$ 改写为 $\underline{0}\ \overline{2}\ 0\ \overline{x_1}0\overline{x_2}0\overline{x_3}0\cdots0\overline{x_n}0$，再用 $T1$ 计算之，……，如此不断计算直至 $T1$ 以输出 $\underline{0}\ \overline{0}\ 0$ 停机；若 $T1$ 永不以输出 $\underline{0}\ \overline{0}\ 0$ 停机，那么 T 对于输入 $\underline{0}\overline{x_1}0\overline{x_2}0\overline{x_3}0\cdots0\overline{x_n}0$ 不停机，即 $f(x_1,\cdots,x_n)$ 对于 $x_1,\cdots,x_n$ 无定义。

定理 11-28 递归函数（μ-递归函数）都是图灵可计算函数。

定理 11-23 至定理 11-27 已经归纳地证明了本定理。

事实上，我们还有如下定理：

定理 12-29 图灵可计算函数都是递归函数（μ-递归函数）。

定理的证明超出了本教材的要求，略去。

最后要回答的问题是：是否所有函数都是图灵可计算的呢？当然不是。

定理 12-30 存在函数是图灵机不可计算的。

本定理的证明也超出了本教材的要求。不过，我们可以粗略地给出这样一个函数的描述。

学者们的研究表明，可以给所有的图灵机编号。他们进而断言：判断图灵机是否对其输入最终停机的函数是不可计算的。即没有任何图灵机可计算如下定义的函数（停机函数）$h(t,x_1,\cdots,x_n)$（t 为任意图灵机编号）：

$$h(t,x_1,\cdots,x_n)=\begin{cases}1 & \text{编号为 } t \text{ 的图灵机对输入 } x_1,\cdots,x_n \text{ 最终停机}\\ 0 & \text{否则}\end{cases}$$

学者们还证明了它同样不是一个递归函数。它在直觉上是可计算的吗？你若觉得“是可计算的”，就请拿出计算的方法；你若认同丘奇-图灵论题，那么就不要去徒劳地寻找这个方法了。像这样不可计算的函数（非递归函数）不仅存在，而且其数量大大地多于可计算函数（递归函数）。又例如，判断一段程序代码（它们也是可以被编号的）是否是病毒的函数也是不可计算的。要了解非递归函数的问题，读者只有去详细学习可计算理论了[8]。

至此，事情已经十分清楚

递归函数集＝图灵可计算函数集 ⊆ 直觉可计算的函数集合

而人们至今并没有找到更强的生成函数的操作，没有找到更强的计算模型，也没有找到直觉可计算的函数不属于递归函数集和图灵可计算函数集，那么自然就有理由假设

递归函数集＝图灵可计算函数集＝直觉可计算的函数集合

从而有理由用递归函数集和图灵可计算函数集来定义可计算函数的集合。因此，大多数数学家和计算机科学家认同**丘奇-图灵论题**也就不足为奇了。

由于整数可以归结为自然数，有理数可以用“整数对”去表示，而实数又可以用有理数去逼近，因此，现代数字计算机可以计算的函数本质上都是递归函数（图灵可计算函数）；非递归函数则是计算机不可计算的。

12.5 习题

1. 什么是初等函数集？
2. 试说明例 12-1 中 14 个初等函数的构作过程的正确性。
3. 试说明（15）～（17）这三个初等函数的构作过程的正确性。
4. 试证明下列函数是初等函数。

（1） $g_1(m,n)=\sum_{i=n}^{m} f(i)$ （$f(i)$是初等函数）

（2） $g_2(m,n)=\prod_{i=n}^{m} f(i)$ （$f(i)$是初等函数）

（3） $g_3(n)=$ “n 中不同质因子的个数”（相同的只算一个）

（4） $g_4(n)=$ “n 中质因子的个数”（相同的重复计算）

（5） $g_5(n)=$ “m，n 的最大公约数”

（6） $g_6(n)=$ “m，n 的最小公倍数”

5. 试说明定理 12-5 的证明中以下等式的正确性：

$$h(y)=\mu_{t\leqslant y}P(t)=\mu_{t\leqslant y}(\chi_P(t)=1)=\sum_{k\leqslant x}\prod_{i\leqslant k}\overline{sg}(\chi_P(t))\overset{*}{-}\prod_{i\leqslant x}\overline{sg}(\chi_P(t))$$

6. 用归纳法证明：“第 n 个质数不大于 2^{2^n}。（提示：$p_1\cdot p_2\cdot\cdots\cdot p_{n-1}+1$ 的任一质因子都不小于 p_n）

7. 令 $f(x)=2^x$，用 f^n 表示 n 个 f 的合成，并约定 $f^0(x)=x$，$f^{n+1}(x)=f(f^n(x))$。现令 $g(n,x)=f^n(x)$。计算 $g(5,x),g(3,4)$，并指出这个函数在哪个方面让你觉得惊讶。

8. 说说为什么在用原始递归式定义 $x\overset{*}{-}y$ 前要先定义 $x\overset{*}{-}1$。

9. 请仔细推敲在定理 12-6 的证明中的两个不等式，

$$h(x_1,x_2,\cdots,x_n)=\sum_{i\leqslant x_1} r(i,x_2,\cdots,x_n)\leqslant(x_1+1)g(n_0,x_0)\leqslant g(n_0,x_0+x_1)$$

$$h(x_1,x_2,\cdots,x_n)=\prod_{i\leqslant x_1} r(i,x_2,\cdots,x_n)\leqslant g^{x_1+1}(n_0,x_0)\leqslant g(n_0,x_0\cdot x_1)$$

的证明。

10. 详细分析定理 12-9 的证明中以下等式的正确性：

$$\mu_{i\leqslant x}(f(i)=0)=\sum_{k\leqslant x}\prod_{i\leqslant k}sg(f(i))\overset{*}{-}\prod_{i\leqslant x}sg(f(i))$$

11. 证明定理 12-10。

12. 用原始递归式和其他初等函数定义下列函数：

（1） $f_1(x)=\left[\sqrt{x}\right]$

（2） $f_3(x)=p_n(x)$

13. 证明原始递归函数都是全函数。

14. 证明定理 12-13。

15. 什么是递归函数集？

16. 试计算 $A(1,n)$， $A(2,n)$， $A(3,n)$， $A(4,n)$。

17. 证明定理 12-16。

18. 利用例 12-3 之（1）的启发，用摹状操作定义一个 n 元的空函数 $\varnothing(x_1,\cdots x_n)$，即对 $x_1,\cdots x_n$ 的一切可能取值， $\varnothing(x_1,\cdots x_n)$ 均无定义。

19. 试用摹状操作定义函数

（1） $f_1(x)=\left[\sqrt{x}\right]$

（2） $f_2(x)=\begin{cases}g^{-1}(x) & \text{当 } x\in Ran(g)\\ \uparrow & \text{否则}\end{cases}$ （g 是一个双射全函数）

20. 设 f 是三元原始递归函数，g 定义为

$$g(x,y)=\mu_t(f(x,y,t)=0)$$

（1）若 $h(x)=\mu_y(g(x,y)=0)$，此时称 h 为μ-递归函数是否妥当？为什么？

（2）证明下列函数 h 是μ-递归函数：

$$h(x)=\begin{cases}\mu_y(g(x,y)=0) & \text{当有}y\text{使}g(x,y)=0\\ \uparrow & \text{否则}\end{cases}$$

21. 试求 图 12-12 中的状态表所确定的图灵机的简化的状态转换图。

	0	1
q_0	$1Rq_0$	$0Lq_2$
q_1	$0Lq_0$	$0Rq_1$
q_2	$1Lq_1$	

图 12-12

22. 考虑 图 12-12 中的状态转换图表示的图灵机：

（1）写出对下列初始带形机器运行时的带形变化：

（a）… 0 0 0 0 0 0 0 0 0 0 0 0 …

（b）… 0 1 1 1 0 1 1 1 1 0 0 …

（2）对下列初始带形机器将如何运行？何时停机？停机时读写头位置如何？

… 0$\underline{0}$1111101110 …

（3）请修改 图 12-13 中的状态转换图，使它表示的图灵机对（2）中输入带形运行停机时，读写头位置回到初始位置。

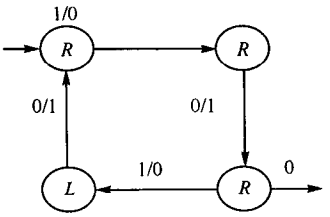


图 12-13

23. 考虑 图 12-14 中的状态转换图表示的图灵机：

（1）写出对下列初始带形机器运行时的带形变化：

（a）… 000000$\underline{0}$00000 …

（b）… 0$\underline{0}$010010110 …

（2）试叙述能使该机最终停机的初始带形应具备的条件。

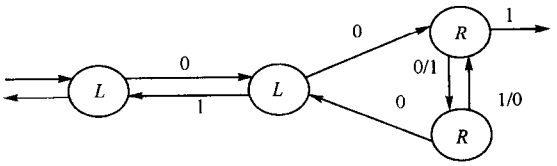


图 12-14

24. 试设计一台图灵机（简化的状态转换图），使它在一根只有一个 1 其余均为空格的初始带形上的任意一处启动，最终在读写头访问那个 1 时停机，而停机时带上的其余部分仍为空格。

25. 试设计一台计算二元加函数的图灵机（简化的状态转换图），使它对初始带形 … $\underline{0}$ $\bar{x}$ 0 $\overline{y}$ 0 0 …计算运行后以下列输出带形停机：

… $\underline{0}$ $\bar{x}$ 0 $\overline{y}$ 0 $\overline{x+y}$ 0 0…

26. 设 $T1$ 是计算函数 $g(x)$的图灵机，试简要描述计算下列函数的图灵机应当如何设计。

（1） $f(x)=\sum_{i\leqslant x} g(i)$

（2） $f(x)=\prod_{i\leqslant x} g(i)$

第 13 章　代数结构概论

读者回忆所接触过的数学结构，包括连续的或离散的，总是在研究对象（自然数、实数、多项式、矩阵、命题、集合乃至图）的集合上定义种种运算（加、减、乘；与、或，非；并、交、补），然后讨论这些对象及运算的有关性质。细心的读者也许已经发现，它们中不无雷同之处。例如，数与多项式对于代数运算有相当一致的特性；命题对于“与、或、非”运算和集合对于“并、交、补”运算甚至可以作统一的描述。这就使人们自然地想到，可以作进一步抽象的研究，不管对象集合的具体特性，也不管对象集合上运算的具体意义，主要讨论这些数学结构的一般特性，并按研究对象集合的特性和运算所遵循的一般定律（如结合律、交换律、分配律等），对这些数学结构进行分类研究。这就是本篇要介绍的**抽象代数学**（abstract algebra）的基本内容，抽象代数学又名近世代数学。

在抽象代数学中，上述由对象集合及运算组成的数学结构被称为**代数结构**（algebra structures）。本章要引进代数结构的一般概念，介绍代数结构研究的主要手段，而把对各种类型的代数结构的深入讨论留在以后两章进行。

13.1　代数结构

13.1.1　代数结构的意义

运算是特定集合上的函数，是代数结构的灵魂。在对代数结构的意义作一般的描述之前，先给出代数结构中的运算的定义，以及有关运算定律的意义。

定义 13-1　称$*$为集合 S 上的 **n 元运算**（operaters），如果$*$为 S^n 到 S 的一个函数。以下$*$常用以表示二元运算，$*(x, y)$常记为 $x*y$；Δ常用以表示一元运算。对二元运算$*$，$*'$：

称$*$运算满足**结合律**，若

$$\forall x\forall y\forall z(x,y,z\in S\rightarrow x*(y* z)=(x*y)*z)$$

称$*$运算满足**交换律**，若

$$\forall x\forall y(x,y\in S\rightarrow x*y= y*x)$$

称$*$运算对$*'$运算满足**分配律**，若

$$\forall x\forall y\forall z(x,y,z\in S\rightarrow x*(y*'z)=(x*y)*'(x*z)\wedge(y*'z)*x=(y*x)*'(z*x))$$

【例 13-1】

（1）加法、乘法运算是自然数集、整数集、有理数集、实数集上的二元运算，减法是整数集、有理数集、实数集上的二元运算。但是除法却不是这些数集上的二元运算。加法、乘法满足结合律、交换律；乘法对加法、实数集上的减法满足分配律。减法运算不满足结合律、交换律。

（2）表 13-1 规定了集合$\{a, b, c\}$上的一个二元运算，这类表称为**运算表**。

表 13-1

*	a	b	c
a	a	b	c
b	b	c	c
c	c	c	c

定义 13-2 **代数结构**是由以下三个部分组成的数学结构：

（1）非空集合 S，称为代数结构的**载体**。

（2）载体 S 上的若干运算。

（3）一组刻画载体上各运算所满足性质的公理。

事实上条款（2）一旦给定，条款（3）也就同时确定，因此条款（3）不是必须的。代数结构常用一个多元序组$<S, \Delta, *, \cdots>$来表示，其中 S 是载体，Δ，$*$，…为各种运算。有时为了强调 S 中有某些元素的地位特殊，也可将这些元素列入多元序组的末尾。

【例 13-2】

（1）以自然数集 N 为载体，数加运算“+”为二元运算组成一代数结构，记为$<N, +>$。

（2）以全体 2×2 实数矩阵组成的集合 M 为载体，矩阵乘“∘”为二元运算，组成一代数结构，记为$<M, \circ>$。

（3）以集合 A 的幂集 $\rho(A)$为载体，以集合并、交、补为其二元运算和一元运算组成一代数结构，记为$<\rho(A), \cup, \cap, \bar{}>$。有时为了突出集合 A 及空集∅在 $\rho(A)$中的特殊地位，也可将这一代数结构记为$<\rho(A), \cup, \cap, \bar{}, A, \varnothing>$。

（1），（2），（3）均称为**具体代数结构**，其运算所满足的公理是众所周知的，因此上文未加以列出。

（4）设 S 为一非空集合，$*$为 S 上满足结合律、交换律的二元运算，那么$<S, *>$为代数结构，称为一个**抽象代数结构**，即一类具体代数结构的抽象。例如$<N, +>$，$<\rho(A), \cup>$，$<\rho(A), \cap>$都是$<S, *>$的具体例子；$<M, \circ>$则不是$<S, *>$的具体例子，因为矩阵乘“∘”不满足交换律。

13.1.2 代数结构的特殊元素

我们已经提及，在一些代数结构中某些元素对所涉及的运算具有特殊的性质，因而在代数结构中具有特殊的地位。

定义 13-3 元素 e 称为代数结构$<S, *>$的（关于运算$*$的）幺元（identity elements），如果 $e \in S$ 且对任意元素 $x \in S$ 有

$$x*e = e*x = x$$

元素 $e_r \in S(e_l \in S)$称为（关于运算$*$的）**右幺元**（**左幺元**），如果 $e_r(e_l)$对任意元素 $x \in S$ 满足

$$x*e_r = x \quad (e_l*x = x)$$

【例 13-3】

（1）$<N, +>$中的数零 0，$<\rho(A), \cup>$中的∅，以及$<\rho(A), \cap>$中的集合 A，分别是这三个代数结构的关于运算+，∪，∩的幺元，因为对任意 $x(\in N, \in \rho(A))$，

$$x+0=0+x=x, x\cup\varnothing=\varnothing\cup x=x, x\cap A=A\cap x=x$$

（2）设 $S=\{a, b, c\}$，S 上运算*由运算表 13-2 给出，那么 a，b，c 都是$<S, *>$的左幺元，它没有右幺元和幺元。注意，左、右幺元，幺元都未必存在，但左、右幺元却可能同时存在、或存在多个。

表 13-2

*	a	b	C
a	a	b	C
b	a	b	C
c	a	B	C

定理 13-1 代数结构$<S, *>$有关于*运算的幺元，当且仅当它同时有关于*运算的左幺元和右幺元。

证明 由于幺元必是左幺元和右幺元，因此必要性显然成立。

为证充分性，设 e_r，e_l 为$<S, *>$的左、右幺元，那么

$$e_r=e_l * e_r=e_l$$

因此 $e_r(e_l)$即幺元。

定理 13-2 任何含有关于*运算幺元的代数结构$<S, *>$，其所含幺元是惟一的。

证明 设$<S, *>$有幺元 $e1$，$e2$，那么

$$e1=e1*e2=e2$$

故幺元是惟一的。

定义 13-4 元素 O 称为代数结构$<S, *>$（关于*运算）的**零元**（zero），如果 $O\in S$ 且对任意 $x\in S$ 有

$$x * O = O * x = O$$

元素 $O_r\in S(O_1\in S)$称为**左零元**（**右零元**），如果 $O_r(O_l)$满足:对一切 $x\in S$，

$$x * O_r = O_r \quad (O_l * x = O_l)。$$

【例 13-4】

（1）$<N, \cdot>$（$\cdot$ 为数乘运算）中的自然数 0，$<\rho(A), \cup>$中的集合 A，$<\rho(A), \cap>$中的$\varnothing$，分别是这三个代数结构的关于运算 $\cdot$，$\cup$，$\cap$ 的零元。

$$x\cdot 0=0\cdot x=0,\ x\cap\varnothing=\varnothing\cap x=\varnothing,\ x\cup A=A\cup x=A$$

（2）设 $S=\{a, b, c\}$，S 上*运算由运算表 13-3 确定，那么 b 是右零元，a 是幺元。

表 13-3

*	a	b	C
a	a	b	C
b	b	b	C
c	c	b	B

我们注意到，代数结构中关于同一运算可能同时有幺元和零元，甚至可能有这样的元素，它关于同一运算既是左（右）幺元，又是右（左）零元，例如表 13-3 第一行（不计表头）改为三个 a 时，那么*运算有左零元 a 和右幺元 a。

定理 13-3 代数结构$<S, *>$有关于*运算的零元，当且仅当它同时有关于*运算的左零元和右零元。

定理 13-4 任何含有关于*运算零元的代数结构$<S, *>$，其所含零元是惟一的。

两定理的证明留给读者。

我们强调指出：

（1）左、右幺元，幺元，左、右零元，零元都是代数结构的常元。

（2）左、右幺元，幺元，左、右零元，零元都是依赖于代数结构中的运算的。例如，在代数结构$<N,+,\cdot>$中，0 关于数加+是幺元，关于数乘·是零元；1 关于·是幺元，关于+则既非幺元又非零元。又如在代数结构$<\rho(A),\cup,\cap,\bar{},A,\varnothing>$中，$\varnothing$是关于$\cup$的幺元，是关于$\cap$的零元；$A$ 是关于$\cup$的零元，又是关于$\cap$的幺元。

（3）今后，在不致造成混淆时，特殊元素是关于什么运算的不再一一指出，但当代数结构中有两个或两个以上的运算时仍将对此作出申明。这时，常常出现这样的情况，一个运算与数加的性质接近，另一个运算与数乘的性质接近，为了简明、直观，我们把前一种运算叫做加法运算，关于它的幺元、零元称为加法幺元、加法零元；常把后一种运算叫做乘法运算，关于它的幺元、零元称为乘法幺元，乘法零元。例如，可称$\varnothing$为$<\rho(A),\cup,\cap,\bar{},A,\varnothing>$的加法幺元、乘法零元，称 A 为$<\rho(A),\cup,\cap,\bar{},A,\varnothing>$的乘法幺元、加法零元。

定义 13-5 设代数结构$<S, *, e>$中 e 为幺元，x, y 为 S 中元素，若 $x*y=e$，那么称 x 为 y 的**左逆元**，y 为 x 的**右逆元**。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}；但当运算被称为“加法运算”（记为+）时，x 的逆元可记为 $-x$。

【例 13-5】

（1）代数结构$<N,\cdot>$（·为数乘）只有数 1 有逆元 1，$<N,+>$（+为数加）只有数 0 有逆元零。总之，任何代数结构其幺元恒有逆元，逆元为其自身。

（2）代数结构$<I,+,\cdot>$（I 为整数集，+，·同上）的每个元素均有加法逆元，但除 1 以外的数都没有乘法逆元．对任意 $x\in I, x$ 的逆元是 $-x$。

（3）代数结构$<Q,+,\cdot>$（Q 为有理数集）中每个元素 x，都有加法逆元 $-x$，除 0 以外的每个元素 x 都有乘法逆元 $x^{-1}=1/x$。

（4）代数结构$<\rho(A),\cup>$中每个元素 B（$B\neq\varnothing$）均无逆元；$<\rho(A),\cap>$中每个元素 B（$B\neq A$）均无逆元。

（5）代数结构$<A^A,\circ>$（其中 $A^A=\{f\mid f: A\to A\}$，$\circ$为函数的合成运算）中，恒等函数 E_A 为幺元，从而 A 中所有双射函数都有逆元，所有单射函数都有左逆元，所有满射函数都有右逆元。回忆定理定理 11-17。

定理 13-5 设$<S,*>$有幺元 e，零元 O；并且$|S|\geqslant 2$，那么 O 无左（右）逆元。

证明 首先，$O\neq e$，否则 S 中另有元素 a，a 非幺元和零元，从而

$$O=O*a=e*a=a$$

矛盾，$O\neq e$ 得证。

若 O 有左（右）逆元 x，那么

$$O=x*\ O\ (O*x)=e$$

与 $O\neq e$ 矛盾，故 O 无左（右）逆元。

定理 13-6 设$<S,*>$有幺元 e，且运算*满足结合律，那么当 S 中元素 x 有左逆元 l 及

右逆元 r 时，$l=r$，它们就是 x 的逆元。

证明 由题设知

$$l=l*e=l*(x*r)=(l*x)*r=e*r=r$$

从而 $l=r$ 是 x 的逆元。

定理 13-6 的一个简单推论是:运算满足结合律的代数结构中，任何元素的逆元是惟一的。

注意，元素的逆元并非代数结构的常元，它不仅依赖运算，而且还依赖于各别的元素。

例如，$<Q, +, \cdot>$中，5 的加法逆元是 -5，乘法逆元是 $\frac{1}{5}$；而 -2 的加法逆元是 2，乘法逆元是 $-\frac{1}{2}$。

当一个代数结构中每一元素都有逆元时，可以认为该代数结构中定义了一个一元求逆运算。

与逆元概念密切相关的是可约性概念。

定义 13-6 称$<S, *>$中元素 a 是**可约的**（cancelable），如果 a 满足:对任意 $x, y\in S$

$$a*x=a*y \text{ 蕴涵 } x=y \tag{13-1}$$

$$x*a=y*a \text{ 蕴涵 } x=y \tag{13-2}$$

当 a 满足（13-1）时，也称 a 是**左可约的**，当 a 满足（13-2）时，也称 a 是**右可约的**。

定理 13-7 若$<S, *>$中*运算满足结合律，且元素 a 有逆元（左逆元，右逆元），那么 a 必定是可约的（左可约的，右可约的）。

证明 设 a 的逆元为 a^{-1}，那么由 $a*x=a*y$ 及 $x*a=y*a$ 可得

$$a^{-1}*(a*x)=a^{-1}*(a*y),\quad (x*a)*a^{-1}=(y*a)*a^{-1}$$

即

$$(a^{-1}*a)*x=(a^{-1}*a)*y,\quad x*(a*a^{-1})=y*(a*a^{-1})$$

均可推得 $x=y$。因此，a 是可约的。

定理 13-7 之逆并不成立。例如$<N, +>$中，任一非零元素 a 均满足式（13-1）与（13-2），但 a 无逆元。

13.1.3 子代数结构

定义 13-7 设 S 上有 n 元运算$*(n=1, 2, \cdots)$，$S'\subseteq S$，称***运算对 S'封闭**（closed），如果对任意元素 $x_1, x_2, \cdots, x_n\in S'$，$*(x_1, x_2, \cdots, x_n)\in S'$。

【例 13-6】 设 E 为非负偶数集，O 为正奇数集，那么定义于 N 上的数加运算对 E 封闭，对 O 不封闭，数乘运算对 E 和 O 都封闭。

定义 13-8 称$<S', *>$为代数结构$<S, *>$的**子代数结构**，或**子代数**（subalgebra），如果

（1）$S'\subseteq S$

（2）运算*对 S'封闭。

常把$<S, *>$叫做$<S, *>$的**平凡子代数**；若 S 含幺元 e，那么也把$<\{e\}, *>$叫做$<S, *, e>$的**平凡子代数**。

据定义，子代数必为一代数结构，*运算所满足的公理显然仍能得到满足。应当注意的是，由于 S'只是 S 的子集，S 中关于*运算的特殊元素，S'中未必仍然具有。

【例 13-7】 对$<N, +>$而言，非负偶数集 E，$<E, +>$为其子代数；正奇数集 O，

$<O, \cdot>$为其子代数；$<N, +>$，$<\{0\}, +>$为其平凡子代数。$<O, +>$不构成其子代数。

13.2 同态、同构及同余

同态映射、同构映射及同余关系（等价关系）以及序关系是研究代数结构的重要工具。同态映射与同构映射是研究所有代数结构所不可或缺的；同余关系在群、环、域的研究中十分重要，而序关系则是格和布尔代数的基本要素。由于等价关系和序关系读者已经熟悉，本节只讨论同态映射、同构映射及同余关系。

13.2.1 同态与同构

由于我们只讨论含一元运算、二元运算的代数结构，因此下文（直至本章末）常用$<S,\Delta,*>$表示一个一般的代数结构；其中 Δ 表示一元运算，$*$表示二元运算。为简明计，有时也仅用载体 S 表示一个代数结构。

定义 13-9 设$<S,\Delta,*>$及$<S',\Delta',*'>$均为代数结构，称函数 h：$S\to S'$为（代数结构 S 到 S'的）同态映射，或同态（homomorphism），如果对 S 中任何元素 a，b，

$$h(\Delta a) = \Delta'(h(a)) \tag{13-3}$$

$$h(a*b) = h(a)*' h(b) \tag{13-4}$$

当同态 h 为单射时，又称 h 为**单一同态**；当 h 为满射时，又称 h 为**满同态**；当 k 为双射时，又称 h 为**同构映射**，或**同构**（isomorphism）。当两个代数结构间存在同构映射时，也称这两个代数结构同构。当 h 为$<S,\Delta,*>$到$<S,\Delta,*>$的同态（同构）时，称 h 为 S 的**自同态**（**自同构**）。

式（13-3）和（13-4）被称为同态 h 的**保运算性**。

【例 13-8】

（1）设 f: $R\to R$ 为 $f(x)=2^x$（R 为实数集）那么，f 为$<R,+>$到$<R,\cdot>$的同态。因为对任意实数 x，y，

$$f(x+y) = 2^{x+y} = 2^x \cdot 2^y = f(x)\cdot f(y)$$

由 f 的定义还可知 f 为单一同态。

但是当 f：$R\to R_+$为 $f(x)=2_x$（R_+为正实数集），那么 f 为$<R,+>$到$<R_+,\cdot>$的同构映射，换言之$<R,+>$与$<R_+,\cdot>$同构。

（2）设 h：$\Sigma^*\to N$ 为 $h(w)=\|w\|$，这里Σ为一非空字母表，$\|w\|$表示字 w 的长度，那么 h 为$<\Sigma^*, 毗连>$到$<N, +>$的同态，因为对任何字 u，$v\in\Sigma^*$，

$$h(uv) = \|uv\| = \|u\| + \|v\| = h(u) + h(v)$$

（uv 表示字 u，v 的毗连）由 h 的定义可知，h 为一满同态。

如果 $|\Sigma|=1$（例如$\Sigma=\{a\}$），那么上述 h 为$<\Sigma^*, 毗连>$到$<N, +>$的同构映射。

（3）设 g：$R\to R$ 为 $g(x)=kx$（k 为常实数），那么 g 为$<R,+>$到$<R,+>$的自同态，因为对任何实数 x，y，

$$g(x+y) = k(x+y) = kx + ky = g(x) + g(y)$$

并且在 $k\neq 0$ 时，g 为自同构。

识别和证明两个代数结构是否同构是十分重要的代数学基本技能。

【例 13-9】

（1）设 $N_4=\{0,1,2,3\}$，$f: N_4\to N_4$ 定义如下：

$$f(x)=\begin{cases}x+1 & \text{当} x+1<4\\ 0 & \text{当} x+1=4\\ x+1-4 & \text{当} x+1>4\end{cases}$$

令 $F=\{f^0, f^1, f^2, f^3\}$，其中 f^0 为 N_4 上恒等函数。易证$<F,\circ>$为一代数结构，且 $f^i\circ f^j=f^{i+_4 j}$（这里$\circ$为函数合成运算，$+_4$为模 4 加运算，见本章练习第 12 题）。

试证$<F,\circ>$与$<N_4,+_4>$同构。

证明 建立双射 $h: F\to N_4$，使

$$h(f^i)=i\ (i=0,1,2,3);$$

由于对任何 $f^i, f^j\in F$，

$$h(f^i\circ f^j)=h(f^{i+_4 j})=i+_4 j=h(f^i)+_4 h(f^j)$$

故 h 为一同构映射，$<F,\circ>$与$<N_4,+_4>$同构得证。

（2）证明代数结构$<N,+>$与$<N,\cdot>$不同构。

证明 反设$<N,+>$与$<N,\cdot>$同构，f为任一同构映射。

不失一般性，设有 n，$n\geqslant 2$，$f(n)$为一质数 p。于是

$$p=f(n)=f(n+0)=f(n)\cdot f(0) \tag{13-5}$$

$$p=f(n)=f(n-1+1)=f(n-1)\cdot f(1) \tag{13-6}$$

据式（13-5），$f(n)=1$ 或 $f(0)=1$；据式（13-6），$f(n-1)=1$ 或 $f(1)=1$。总之，至少在两处 f 的值为 1，这与 f 为同构映射（双射）冲突．因此$<N,+>$与$<N,\cdot>$不同构。

为了进一步讨论同态的性质，我们引入同态像的概念。

定义 13-10 设 h 为代数结构$<S,\Delta,*>$到$<S',\Delta',*'>$的同态映射，那么称 $h(S)$为 h 的**同态像**（image under homomorphism）。

定理 13-8 设 h 为代数结构$<S,\Delta,*>$到$<S',\Delta',*'>$的同态，那么同态像 $h(S)$与 Δ'，$*'$构成$<S',\Delta',*'>$的一个子代数。

证明 只要证 $h(S)$对运算 Δ'，$*'$封闭。为此设 a'，b'为 $h(S)$中任意两个元素，且 $h(a)=a'$，$h(b)=b'$。那么

$$\Delta'(a')=\Delta'(h(a))=h(\Delta(a))\in h(S)$$

$$a'*'b'=h(a)*'h(b)=h(a*b)\in h(S)$$

故 $h(S)$对运算 Δ'，$*'$封闭，$<h(S),\Delta',*'>$为 S'的子代数。

h 的同态像有时也指子代数$<h(S),\Delta',*'>$。很显然，h 为单射时$<S,\Delta,*>$与同态像$<h(S),\Delta',*'>$同构，这使我们想到，同态像应同$<S,\Delta,*>$有许多共同的性质。

定理 13-9 设 h 是代数结构$<S,*_1,*_2>$到$<S',*_1',*_2'>$的同态，h 的同态像为$<h(S),*_1',*_2'>$（这里$*_1,*_2,*_1',*_2'$均为二元运算），那么

（1）当运算$*$（指$*_1$或$*_2$，下同）满足结合律、交换律时，同态像中运算$*'$也满足结合律、交换律；当运算$*_1$对$*_2$满足分配律时，同态像中运算$*_1'$对$*_2'$也满足分配律。

（2）如果$<S,*_1,*_2>$关于$*$有幺元 e 或零元 O，那么$<h(S),*_1',*_2'>$中有关于$*'$的幺元 $h(e)$或零元 $h(O)$。

（3）如果$<S, *_1,*_2>$中元素 x 有关于$*$的逆元 x^{-1}，那么$<h(S),*_1',*_2'>$中元素 $h(x)$有关于$*'$的逆元 $h(x^{-1})$。

证明 证明是平凡的。

需要强调指出，上述定理的结论都只对同态像有效，决不能随意扩大到$<S', *_1',*_2'>$上，下面将有例子说明这一点。当然，在 h 为满同态时，由于 $h(S)=S'$，而代数结构中的幺元、零元都是惟一的，一个元素的逆元也是惟一的，因此，对满同态定理 13-9 的结论在$<S', *_1',*_2'>$上也能成立。

【例 13-10】

（1）在命题代数$<\{0,1\},\wedge,\vee>$与集合代数$<\rho(A), \cap, \cup>$（$A \neq \varnothing$）之间可建立下列同态映射 h：$\rho(A)\to\{0,1\}$，令 a 为 A 中某一元素：

$$h(B)=\begin{cases}1 & \text{当} a\in B\\ 0 & \text{当} a\notin B\end{cases}$$

（请读者自行验证 h 的保运算性。）

很显然，$h(\varnothing)=0$，$h(A)=1$，h 为一满同态，并且 h 把 $\rho(A)$分成两部分，一部分是含 a 的子集，另一部分是不含 a 的子集．我们将看到，当把这两部分看成两个整体时，集合代数便像是“凝聚”成了命题代数，这种“凝聚”作用正是同态研究的意义之一。

（2）如果将 h 改为 h：$\{0,1\}\to\rho(A)$，使

$$h(0)=\varnothing,\ h(1)=A$$

那么，可以看到集合代数的子代数$<\{\varnothing,A\},\cap,\cup>$与命题代数同构的。

（3）设 $A=\{a, b, c, d\}$，令 $h:\{0,1\}\to\rho(A)$满足

$$h(0)=\{a\},\ h(1)=\{a, b\}$$

那么可证 h 仍为一同态映射，$\{a\}$是$<h(\{0,1\}),\cap, \cup>$的关于$\cup$运算的幺元，$\{a, b\}$则是它的零元，但它们都不是$<\rho(A), \cap, \cup>$的关于$\cup$运算的幺元和零元。

下面我们要讨论同态核的概念。

定义 13-11 如果 h 为代数结构$<S,*>$到$<S',*'>$的同态，并且 S'中有幺元 e'，那么称下列集合为**同态 h 的核**（kernel of homomorphism），记为 $K(h)$。

$$K(h)=\{x\mid x\in S\wedge h(x)=e'\}$$

关于同态核我们有以下定理。

定理 13-10 设 h 为代数结构$<S,*>$到$<S',*'>$的同态，如果 $K(h)\neq\varnothing$，那么$<K(h),*>$为$<S,*>$的子代数。

证明 只要证 $K(h)$对$*$运算封闭。为此设 x, y 为 $K(h)$中任意元素，于是 $h(x)=h(y)=e'$。考虑

$$h(x*y)=h(x)*'h(y)=e'*'e'=e'$$

因此 $x*y\in K(h)$，故$<K(h),*>$为$<S,*>$的子代数。

至此我们看到，围绕同态映射 h 有两个子代数，一个是$<S',*'>$的子代数$<h(S),*'>$，另一个是$<S,*>$的子代数$<K(h),*>$。

注意不要混淆同态核与定义 11-9 中的函数核的概念。同态 h 的核 $K(h)$是 h 作为函数的核 Ker(h)（一个等价关系）所导出的划分中的一个单元：$\{x\mid h(x)=e'\}$。

【例 13-11】 设 $A=\{a, b, c\}$，h 为例 13-10 中确定的同态，据该例要求取 A 中元素

a。由于<{0,1}，∧，∨>中关于运算∨的幺元为 0，因此

$$K(h)=\{\varnothing,\{b\},\{c\},\{b,c\}\}$$

而

$$\rho(A)/\mathrm{Ker}(h)=\{\{\{a\},\{a,b\},\{a,c\},\{a,b,c\}\},\{\varnothing,\{b\},\{c\},\{b,c\}\}\}$$

显然 $K(h)$对∩，∪运算封闭。

13.2.2 同余关系

简单地说，同余关系是相等关系的推广，是具有“保运算”性质的等价关系。

定义 13-12 设～为代数结构<S, Δ,*>的载体 S 上的等价关系，称～为 S 上关于一元运算 Δ 的**同余关系**（congruence relations），如果对 S 中任何元素 a，b，

$$a\sim b \text{ 蕴涵 } \Delta a\sim\Delta b \tag{13-7}$$

称～为 S 上关于二元运算*的同余关系，如果对 S 中任何元素 a，b，c，d

$$a\sim b,\ c\sim d \text{ 蕴涵 } a*c\sim b*d \tag{13-8}$$

当～关于<S, Δ,*>中一元运算 Δ、二元运算*均为同余关系时，便称～为<S, Δ,*>上的同余关系，等价类$[x]_\sim$则又称为**同余类**。

【例 13-12】

（1）相等关系显然是所有代数结构上的同余关系。因此，可以说同余关系是相等关系的一种推广。

（2）可证模 k 相等关系是关于整数运算的同余关系。因此，也可以说同余关系是模 k 相等关系（数论中也称模 k 同余关系）的推广。

设整数 x, y, u, v 满足 $x=y(\mathrm{mod}\ k)$，$u=v(\mathrm{mod}\ k)$，那么 $x-y=nk$, $u-v=mk$（n, m 为整数），于是

$$(x+u)-(y+v)=(n+m)k$$

故 $x+u=y+v(\mathrm{mod}\ k)$。

为证 $xu=yv(\mathrm{mod}\ k)$，将 $x=y+nk$ 与 $u=v+mk$ 两边分别相乘，于是有

$$xu-yv=ymk+vnk+nmk^2$$

$$xu-yv=(ym+vn+nmk)k$$

由于 $ym+vn+nmk$ 为整数，$xu=yv(\mathrm{mod}\ k)$得证。

模 k 相等关系关于整数集上的减运算和一元减运算（添负号运算）也是同余关系，请读者自行验证。

（3）集合 $S=\{a, b, c, d\}$，S 上的等价关系～由图 13-1a 所示的划分确定，S 上的一元运算 Δ 及二元运算*分别由表 13-4 和表 13-5 给定。

表 13-4

x	Δx
a	C
b	D
c	a
d	b

表 13-5

*	a	b	c	d
a	a	b	c	c
b	b	a	c	d
c	c	c	a	b
d	c	d	b	a

那么等价关系～关于 Δ，*均为同余关系，我们把繁琐的验证略去，用图 13-1b、c 作为直观说明。

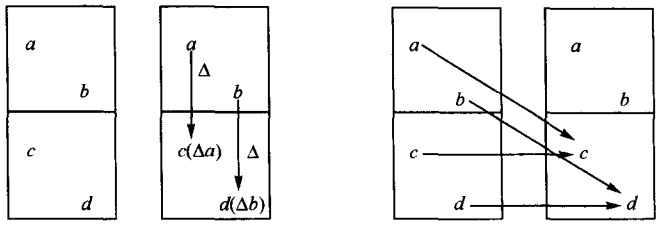


图 13-1

（4）据（1）的讨论可知，模 k 相等关系是代数结构$<I,+,\cdot>$上的同余关系。

在同余关系的定义中，式（13-8）还可以改为:对 S 中任意元素 a, b, c：

$$a\sim b \text{ 蕴涵 } a*c\sim b*c \text{ 且 } c*a\sim c*b \tag{13-9}$$

我们来证明式（13-8）与式（13-9）等价。

由于 $c\sim c$，式（13-8）蕴涵式（13-9）是显然的。

现设式（13-9）真，并设 $a\sim b$，$c\sim d$。据式（13-9）及 $a\sim b$，有 $a*c\sim b*c$。又据式（13-9）及 $c\sim d$，有 $b*c\sim b*d$. 于是 $a*c\sim b*d$。式（13-8）得证。

由第 11 章的讨论我们已经知道函数 h：$S\to S'$导出 S 上的一个等价关系，现在我们要指出，如果 h 是$<S, \Delta,*>$到$<S', \Delta',*'>$的同态映射，那么 h 导出的 S 上的等价关系必定是$<S, \Delta,*>$上的同余关系。

定理 13-11 设 h 是$<S, \Delta,*>$到$<S', \Delta',*'>$的同态映射，那么 Ker(h)确定的 S 上的等价关系～是代数结构$<S, \Delta,*>$上的同余关系。回忆定义 11-9，Ker(h)确定的 S 上的等价关系～如下定义：对任意 $x, y\in S$，

$$x\sim y \text{ 当且仅当 } h(x)=h(y)$$

证明 关系～显然是等价关系、为证～为$<S, \Delta,*>$上的同余关系，需证～满足式（13-7）和式（13-9）。

设 a，b，c 为 S 中任意元素:

（1）若 $a\sim b$，那么 $h(a)=h(b)$；从而 $\Delta(h(a))=\Delta(h(b))$，因 h 为一同态映射，故 $h(\Delta a)=h(\Delta b)$。因而 $\Delta a\sim\Delta b$。式（13-7）证毕。

（2）若 $a\sim b$，那么 $h(a)=h(b)$；从而对任意 S 中元素 c

$$h(a)*'h(c)=h(b)*'h(c)$$

$$h(a*c)=h(b*c)$$

因此 $a*c\sim b*c$。$c*a\sim c*b$ 同理可证。（13-9）也证毕。

【例 13-13】 设 Q 为有理数集（既约分数的集合），F 为 $\frac{n}{m}$ 形分数集合，其中 m, n 是整数，$m\neq 0$。注意 Q 是 F 的真子集，因为 F 中可以有 $\frac{1}{2}$，$\frac{2}{4}$，$\frac{3}{6}$，…，但是，对应地在 Q 中只有一个有理数 $\frac{1}{2}$。在代数结构$<F,-,+>$和$<Q,-,+>$之间建立同态 h:对每一 $\frac{n}{m}\in F$

$$h\left(\frac{n}{m}\right)=n \text{ 除以 } m \text{ 的商（即约去 } n, m \text{ 的公因子）}$$

易证 h 为一同态，且对于任意 m, n, m', n'

$$h\left(\frac{n}{m}\right)=h\left(\frac{n'}{m'}\right) \text{当且仅当 } m\cdot n'=m'\cdot n$$

因此 h 导出 F 上的一个同余关系～：

$$\left(\frac{n}{m}\right)\sim\left(\frac{n'}{m'}\right) \text{当且仅当 } h\left(\frac{n}{m}\right)=h\left(\frac{n'}{m'}\right) \text{ 当且仅当 } m\cdot n'=m'\cdot n \tag{13-10}$$

事实上，～关系即为（非既约或既约的）分数间的相等关系。

*13.3 商代数

子代数概念为我们由已知代数结构作新的代数结构提供了一条思路。而本节则要介绍，由已知代数结构构造新的代数结构的一个主要手段。

本节仍沿用对$<S,\Delta,*>$的约定，$S/\sim$表示 S 上等价关系～所导出的商集（划分）、即

$$S/\sim\ =\{[x]_\sim \mid x\in S\}$$

定义 13-13 设 S 上等价关系～为$<S, \Delta,*>$上的同余关系。定义 $S/\sim$上一元运算@和二元运算⊙如下，对任意 $x, y\in S$，

$$@\ ([x])=[\Delta x]$$

$$[x]\odot[y]=[x*y]$$

那么代数结构$<S/\sim, @, \odot>$称为$<S, \Delta, *>$的关于～的**商代数**（quotient algebra）。

为确认$<S/\sim, @, \odot>$为一代数结构，只要确认@和⊙运算上述定义是适当的（良定的）。即：@，⊙确为 S/～的运算。为此，只要确认对任意 $S/\sim$中元素[x]，[y]，@（[x]），[x]⊙[y]都是惟一地确定的。事实上，Δ，*运算的良定性，以及等价类的惟一确定性保证了这一点，从而保证了@和⊙运算定义的良定性。

定理 13-12 设$<S/\sim, @, \odot>$为$<S, \Delta,*>$的关于～的商代数，那么

（1）若*运算满足结合律、交换律，那么⊙运算也满足结合律、交换律。

（2）若*运算有幺元 e（零元 0），那么⊙以[e]为幺元（以[0]为零元）。

（3）若 $x\in S$ 有关于*运算的逆元 x^{-1}，那么[x]有关于⊙运算的逆元$[x^{-1}]$。

定理的证明是极简单的，请读者自行完成。

回忆第 11 章中规范映射 $f: S\to S/\sim$的定义

$$f(x)=[x]_\sim$$

定理 13-13 设～为$<S, \Delta,*>$上的同余关系，那么规范映射 $f: S\to S/\sim$为$<S, \Delta,*>$到其商代数$<S/\sim, @, \odot>$的一个同态。

证明 设 x, y 为 S 中任意元素，那么

$$f(\Delta(x))=[\Delta(x)]=@[x]=@f(x)$$

$$f(x*y)=[x*y]=[x]\odot[y]=f(x)\odot f(y)$$

规范映射 f 为一同态得证。

显然，上述规范映射还是<S, Δ,*>到<$S/\sim$，@，⊙>的满同态，并且，当<S, Δ,*>有幺元 e（零元 0）时，<$S/\sim$，@，⊙>定有幺元 $f(e)=[e]$（零元 $f(0)=[0]$）。

我们知道，当 h 为<S, Δ, *>到<S', Δ', *'>的同态时，由 h 导出了<S, Δ, *>上的一个同余关系，而本定理则告诉我们，这个同余关系反过来又导出了一个<S, Δ, *>到<$S/\sim$，@，⊙>的同态，它被称为**自然同态**。它们之间的关系如图 13-2 所示。

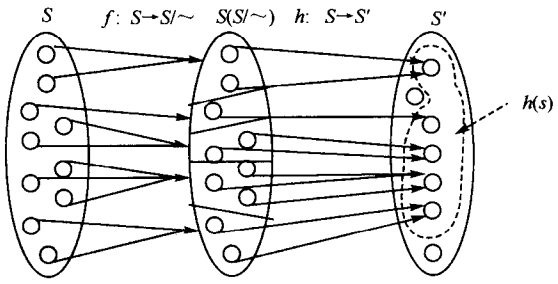


图 13-2

图 13-2 还提示我们考虑商代数和同态像之间的关系，前者是同态 h 在 S 上导出的代数结构，后者是 h 在 S'上导出的代数结构，而且两者的载体具有相同数目的元素。

定理 13-14 设 h 为<S, Δ,*>到<S', Δ',*'>的同态，～为 h 导出的<S, Δ,*>的同余关系，那么，商代数<$S/\sim$，@，⊙>与同态像<$h(S)$, Δ',*'>同构。（回忆定理 11-7）。

证明 定义函数 $i: S/\sim \to h(S)$，对任意元素$[x]\in S/\sim$，

$$i([x])=h(x)$$

为证 i 是良定的，即 i 确为一函数，设$[x]=[y]$，需证 $i([x])=i([y])$。由于$[x]=[y]$，故 $y\in[x]$，因而 $h(y)=h(x)$（据～的定义），因此 $i([x])=i([y])$得证。

i 显然是满射。为证 i 为单射，设$[x]\neq[y]$，需证 $i([x])\neq i([y])$。反设 $i([x])=i([y])$，从而 $h(x)=h(y)$，进而有 $y\in[x]$，$[x]=[y]$，矛盾。

最后，我们要证明映射 i 是保运算的，即 i 为一同态。设$[x]$，$[y]$为 $S/\sim$中任意元素，那么

$$\begin{aligned}
i(@([x])) &= i([\Delta(x)]) && (@\text{的定义})\\
&= h(\Delta(x)) && (i\text{ 的定义})\\
&= \Delta'(h(x)) && (h\text{ 为同态})\\
&= \Delta'(i[x]) && (i\text{ 的定义})\\
i([x]\odot[y]) &= i([x*y]) && (\odot\text{的定义})\\
&= h(x*y) && (i\text{ 的定义})\\
&= h(x)*'h(y) && (h\text{ 为同态})\\
&= i([x])*'i([y])
\end{aligned}$$

因此 i 为一同态。

综上所述，i 确系<$S/\sim$，@，⊙>到<$h(S)$，Δ',*'>的一个同构映射。因此，同态 h 导出的商代数与同态像导出的子代数同构。

由于规范映射 f 为 S 到 $S/\sim$的映射，i 为 $S/\sim$到 $h(S)$的映射，因此 h 可看作是 f 与 i 的合成 $i\circ f$，即对任一 $x\in S$，

$$h(x) = i([x]) = i(f(x)) = i \circ f(x)$$

三者的关系如图 13-3 所示。

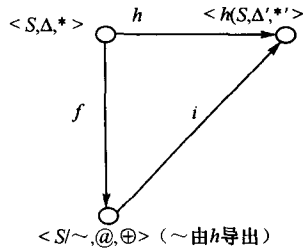


图 13-3

【例 13-14】 考虑代数结构$<I, -, +>$，其中$-$是整数集 I 上的一元添负号运算。定义函数 h，$h: I \to \{0,1,2,3,4\}$，使得对任意 $x \in I$，

$h(x)$ =（5 除 x 所得的余数）$= x \pmod 5$

易证 h 为$<I, -, +>$到$<N_5, -_5, +_5>$的同态。这里$+_5$ 为模 5 加运算，而对每一 $x \in N_5$

$$-_5 x = \begin{cases} 5-x & \text{当} x \neq 0 \\ 0 & \text{当} x = 0 \end{cases}$$

不难证明 h 导出的$<I, -, +>$上的同余关系～即为模 5 相等关系，即

$$x \sim y \text{ 当且仅当 } x = y \pmod 5$$

如果我们将[0]，[1]，[2]，[3]，[4]简记为$\bar{0}$，$\bar{1}$，$\bar{2}$，$\bar{3}$，$\bar{4}$，那么商代数$<I/\sim, \ominus, \oplus>$可表示为$<\{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}\}, \ominus, \oplus>$，其中$\ominus$，$\oplus$定义如下：对任意 x，$y \in I/\sim$，

$$\ominus \bar{x} = \overline{-_5 x}$$

$$\bar{x} \oplus \bar{y} = \overline{x +_5 y}$$

据以上讨论知，$<\{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}\}, \ominus, \oplus>$与$<N_5, -_5, +_5>$同构。因此，通常用对$<N_5, -_5, +_5>$的讨论来取代模 k 相等关系等价类上运算的讨论。

13.4 练习

1. 给出三个上文未涉及的代数结构。

2. 设 $S = \{a, b, c, d, e\}$，S 上运算$*$由表 13-6 给定：

表 13-6

*	A	b	c	d	e
a	a	b	c	b	d
b	b	c	a	e	c
c	c	a	b	b	a
d	b	e	b	e	d
e	d	b	a	d	c

（1）计算$(a*b)*c$ 和 $a*(b*c)$，由计算结果可否断定$*$运算满足结合律？

（2）计算$(b*d)*c$ 和 $b*(d*c)$，由计算结果可否断定$*$运算满足结合律？

（3）运算满足交换律吗？为什么？

3. 已知 S 上运算$*$满足结合律与交换律，证明：对 S 中任意元素 a，b，c，d 有

$$(a*b)*(c*d) = ((d*c)*a)*b$$

4. 已知 S 上运算$*$满足结合律，并且满足:若 $x*y = y*x$，则 $x = y$。试证明：对一切 $x \in S$ 有 $x*x = x$（此种元素称为等幂元素，因而上述$<S, *>$所有元素都是等幂元素）。

5. 设集合 S 有 n 个元素，问可定义多少个 S 上的二元运算，可定义多少个 S 上的满足交换律的二元运算。

6. 完成下列运算表（表 13-7），使之定义的运算$*_1$, $*_2$满足结合律:

表 13-7

$*_1$	a	b	c	d		$*_2$	a	b	C	d
a	a	b	c	d		a	b	a	C	d
b	b	a	d	c		b	b	a	C	d
c	c	d	a	b		c				
d						d	d	c	C	d

7. S 及其 S 上的运算$*$如下定义。问各种定义下$*$运算是否满足结合律、交换律，$<S, *>$中是否有幺元、零元，S 中哪些元素有逆元，哪些元素没有逆元?

（1）S 为 I（整数集），$x*y=x-y$

（2）S 为 I（整数集），$x*y=x+y-xy$

（3）S 为 Q（有理数集），$x*y=\dfrac{x+y}{2}$

（4）S 为 N（自然数集），$x*y=2^{xy}$

（5）S 为 N（自然数集），$x*y=\max(x, y)$ $(\min(x, y))$

（6）S 为 N（自然数集），$x*y=x$

8. 证明定理 13-3，定理 13-4。

9. 下列断言正确吗？为什么？

（1）代数结构中的幺元与零元总不相等。

（2）一代数结构中可能有三个右幺元，而只有一个左幺元。

（3）代数结构中可能有一个元素，它既是左零元，又是右幺元。

（4）幺元总有逆元。

（5）用 a^n 表示 n 个 a 的积：$\underbrace{a*a*\cdots*a}_{n}$，那么当$<S, *>$中有元素 a 时，a^n（$n=1$, 2, 3, …）均在 S 中。

（6）如果 $S'\subseteq S$，运算$*'$为$*$在 $S'\times S'$上的限制，那么代数结构$<S', *'>$为$<S, *>$的子代数。

10. 设 $A=\{a, b\}$，S 为 A^A，即 $S=\{f1, f2, f3, f4\}$，诸 f 由表 13-8 给定。

表 13-8

x	$f1(x)$	$f2(x)$	$f3(x)$	$f4(x)$
a	a	a	b	B
b	a	b	a	B

（1）给出 S 上函数复合运算$\circ$的运算表。

（2）$<S, \circ>$ 是否有幺元、零元?

（3）$<S, \circ>$中哪些元素有逆元，逆元是什么?

11．对例 13-1 之（1），（2），（3）中给出的代数结构分别说出一个非平凡的子代数。

12．记集合{0，1，2，…，$k-1$}（k 为正整数）为 N_k，定义 N_k 上的模 k 加运算 $+_k$ 和模 k 乘运算 $\times_k$：

$$x +_k y = \begin{cases} x+y & \text{当 } x+y<k \\ x+y-k & \text{当 } x+y \geqslant k \end{cases}$$

$$x \times_k y = xy - \left[\frac{xy}{k}\right]k$$

其中 $\left[\frac{xy}{k}\right]$ 表示商 $\frac{xy}{k}$ 的整数部分。

考虑代数结构 $<N_6,+_6>$，$<N_6,\times_6>$，$<N_6,+_6,\times_6>$。问下列集合及集合上的运算是否构成以上三代数结构的子代数：

（1）$\{0,2\},+_6$；$\{0,2\},\times_6$

（2）$\{0,3\},+_6$；$\{0,3\},\times_6$

（3）$\{0,2,4\},+_6$；$\{0,2,4\},\times_6$

（4）$\{0,1\},+_6$；$\{0,1\},\times_6$

（5）$\{0,1,3,5\},+_6$；$\{0,1,3,5\},\times_6$

13．证明：$f:R_+ \to R$，$f(x)=\log_2 x$ 为代数结构 $<R_+,\cdot>$ 到 $<R,\cdot>$ 的同态（这里 R_+ 为正实数集，R 为实数集，$\cdot$ 为数乘运算）。它是否为一同构映射？为什么？

14．设 $f: N \to \{0,1\}$ 定义如下：

$$f(n)=\begin{cases} 1 & \text{当} n=2^k (k\text{是自然数}) \\ 0 & \text{否则} \end{cases}$$

证明：f 为代数结构 $<N,\cdot>$ 到 $<\{0,1\},\cdot>$ 的同态。它是单一同态，满同态吗？

15．设 $A=\{a,b,c\}$。问代数系统 $<\{\varnothing,A\},\cup,\cap>$ 和 $<\{\{a,b\},A\},\cup,\cap>$ 是否同构？

16．假定 h 是 $<S,*>$ 到 $<S',*'>$ 的同态，试举例说明

（1）$<h(S),*'>$ 的幺元（零元），可能不是 $<S',*'>$ 的幺元（零元）。

（2）$<h(S),*'>$ 的成员的逆元，可能不是它在 $<S',*'>$ 中的逆元。

17．设 f，g 都是 $<S,*>$ 到 $<S',*'>$ 的同态，并且 $*$ 与 $*'$ 运算均满足交换律和结合律，证明：如下定义的函数 $h: S \to S'$

$$h(x)=f(x)*'g(x)$$

是 $<S,*>$ 到 $<S',*'>$ 的同态。

18．设 f，g 分别是 $<S,*>$ 到 $<S',*'>$ 的同态和 $<S',*'>$ 到 $<S'',*''>$ 的同态，证明：$g\circ f$ 是 $<S,*>$ 到 $<S'',*''>$ 的同态。

19．证明：恰有 i 个映射 $f: N_i \to N_i$，使得

（1）$f(0)=0$。

（2）f 为 $<N_i,+_i>$ 到 $<N_i,+_i>$ 的同态。

（提示：f 具有以下形式：$f(x)=px(\mathrm{mod}\ i)$，$p=0,1,2,\cdots,i-1$）

20．（1）以 $<N_3,+_3>$ 为例，给出所有满足第 19 题要求的同态 f。

（2）给出所有满足$f(0)=0$的$<N_2,+_2>$到$<N_3,+_3>$的同态f。

（3）给出所有满足$f(0)=0$的$<\mathrm{N},+>$到$<N_3,+_3>$的同态f。

21．对例 13-12 中分数集 F 证明：如下定义的 F 上的等价关系～是$<F,-,+>$（这里，-为一元添负号运算）上的同余关系：

$$\frac{n}{m}\sim\frac{n'}{m'}\text{ 当且仅当 }m'n=mn'$$

22．定义分数集 F 上的一元运算 Δ：

$$\Delta\left(\frac{n}{m}\right)=\frac{n}{m^2}$$

证明：第 21 题中定义的等价关系～不是$<F,\Delta>$上的同余关系.

23．对下列每一关系，证明或否证它是$<I,+>$上的同余关系（这里 I 为整数集合）：

（1）$x\sim y$ 当且仅当 $x\geqslant y$。

（2）$x\sim y$ 当且仅当 $(x<0\wedge y<0)\vee(x\geqslant 0\wedge y\geqslant 0)$。

（3）$x\sim y$ 当且仅当 $|x-y|<0$。

（4）$x\sim y$ 当且仅当 $x=y=0\vee(x\neq 0\wedge y\neq 0)$。

24．证明：代数结构$<S,*>$上的两个同余关系的交仍为$<S,*>$上的同余关系。

25．对例 13-13 中代数结构$<F,-,+>$建立其商代数$<F/\sim,\ominus,\oplus>$，其中～为式（13-10）所确定的同余关系。证明$<F/\sim,\ominus,\oplus>$与$<Q,-,+>$同构。

26．设$<S,\Delta_1,\Delta_2>$中 $S=\{a,b,c,d,e\}$，两个一元运算由下列运算表定义：

x	a	b	c	d	e
$\Delta_1(x)$	d	c	d	b	a
$\Delta_2(x)$	c	b	a	c	e

另设 R 为 S 上等价关系，R 对应于划分π：

$$\pi=\{\{a,c\},\{b,e\},\{d\}\}$$

（1）试证 R 为$<S,\Delta_1,\Delta_2>$上的同余关系。

（2）作出$<S,\Delta_1,\Delta_2>$的商代数 S/R。

27．令 $h:N\to N$ 为$<N,+>$到$<N,+>$的同态，对任何 $x\in N$，$h(x)=kx$（k 为给定自然数）。试描述 h 所导出的同余关系～，构作$<N,+>$的商代数$<N/\sim,\oplus>$，并证明它与$<N,+>$同构。

28．令 $h:I\to N$ 为$<I,\cdot>$到$<N,\cdot>$的同态，对任何 $x\in I$，$h(x)=x^2$。试描述 h 所导出的同余关系～，构作$<I,\cdot>$的商代数$<I/\sim,\odot>$，并证明它与$<N,\cdot>$同构。

29．证明定理 13-12。

第14章　群、环、域

本章主要讨论传统抽象代数的主要内容，即讨论典型的三类代数结构：群、环、域。作为它们的共同基础，我们先介绍最简单的代数结构——半群。

14.1　半群

14.1.1　半群及独异点

在第 13 章里我们看到，运算的结合律是代数结构应当满足的最基本的性质，因为没有运算的结合律，连幺元、零元的惟一性都保证不了，因此，运算具有结合律的代数结构可以说是最基本的代数结构。

定义 14-1　称代数结构$<S, *>$为**半群**（semigroups），如果$*$运算满足结合律。当半群$<S, *>$含有关于$*$运算的幺元，则称它为**独异点**（monoid），或**含幺半群**。

【例 14-1】　$<I_+, +>$，$<N, \cdot>$，$<\Sigma^*$，并置$>$都是半群，后两个又是独异点。

半群及独异点的下列性质是明显的。

定理 14-1　设$<S, *>$为一半群，那么

（1）$<S, *>$的任一子代数都是半群，称为$<S, *>$的**子半群**。

（2）若独异点$<S, *, e>$的子代数含有幺元 e，那么它必为一独异点，称为$<S, *, e>$的**子独异点**。

证明是十分简单的。

定理 14-2　设$<S, *>$，$<S', *'>$是半群，h 为 S 到 S'的同态，这时称 h 为**半群同态**。对半群同态有

（1）同态像$<h(S), *'>$为一半群。

（2）当$<S, *>$为独异点时，则$<h(S), *'>$为一独异点。

利用第 13 章的知识可立即得到这些结论。

定理 14-3　设$<S, *>$为一半群，那么

（1）$<S^S, \circ>$为一半群，这里 S^S 为 S 上所有一元函数的集合，$\circ$为函数的合成运算。

（2）存在 S 到 S^S 的半群同态。

证明　(1) 是显然的。

为证（2）定义函数 $h: S \to S^S$：对任意 $a \in S$

$$h(a) = f_a$$

$f_a: S \to S$ 定义如下：对任意 $x \in S$，

$$f_a(x) = a * x$$

现证 h 为一同态．对任何元素 $a, b \in S$。

$$h(a*b) = f_{a*b} \tag{14-1}$$

而对任何 $x\in S$，

$$f_{a*b}(x)=a*b*x=f_a(f_b(x))=f_a\circ f_b(x)$$

故 $f_{a*b}=f_a\circ f_b$，由此及式（14-1）即得

$$h(a*b)=f_{a*b}=f_a\circ f_b \quad =h(a)\circ h(b)$$

定理 14-3 被称为半群表示定理。它表明，任一半群都可以表示为（同态于）一个由其载体上的函数的集合及函数合成运算所构成的半群。这里$<S,*>$同构于$<h(S),\circ>$，后者是$<S^S,\circ>$的一个子代数。

*14.1.2 自由独异点

定义 14-2 称独异点$<S,*,e>$为**自由独异点**（free monoid），如果有 $A\subseteq S$ 使得

（1）$e\notin A$。

（2）对任意 $u\in S$，$x\in A$，$u*x\neq e$。

（3）对任意 u，$v\in S$，$x,y\in A$，若 $u*x=v*y$，那么 $u=v$，$x=y$。

（4）S 由 A 生成，即 S 中元素或者为 e，或者为 A 的成员，或者为 A 的成员的“积”：

$$a_{i1}*a_{i2}*\cdots*a_{ik} \qquad (a_{i1},a_{i2},\cdots,a_{ik}\in A)$$

集合 A 称为 S 的**生成集**。

【例 14-2】 $<N,+,0>$，$<\Sigma^*$，并置$>$都是自由独异点。它们的生成集分别为{1}和Σ。

由定义中条款（4）与（3）可知，自由独异点的元素除幺元外，均可表示为生成集中元素的“积”的形式，且这种表示形式是惟一确定的。

顺便指出，当半群$<S,*>$有生成集 $A=\{a\}$时，称$<S,*>$为**循环半群**（cyclic semigroups）。$<N,+,0>$是循环半群。

在自由独异点上可递归地定义函数。

定理 14-4 设$<S,*,e>$为一自由独异点，A 为它的生成集，$g:S\times A\times M\to M$ 为一已知函数，m 为 M 中已知元素，那么下列等式组定义了一个 S 到 M 的函数 f：

$$\begin{cases} f(e)=m \\ f(w*x)=g(w,x,f(w)) \end{cases}$$

其中 $w\in S$，$x\in A$。

定理表明的事实是清楚的，由于 S 中元素可以惟一地表示为生成集元素的积，f 的值被这组等式惟一地确定。与定义在自然数上的递归函数一样，递归地定义在 S 上的函数 $f:S\to M$ 是良定的（参见 11.1.4）。

定理 14-5 设$<S,\bullet,e1>$和$<T,*,e2>$为两个自由独异点，A，B 分别为它们的生成集，且$|A|=|B|$，那么$<S,\bullet,e1>$和$<T,*,e2>$同构。

证明 设 $g:A\to B$ 为一双射，据定理 14-4，可定义函数 $f:S\to T$：

$$\begin{cases} f(e1)=e2 \\ f(w\bullet x)=f(w)*g(x) \end{cases}$$

其中 $w\in S$，$x\in A$。

对 g^{-1} 运用定理 14-4，可定义函数 $h:T\to S$：

$$\begin{cases} h(e2)=e1 \\ h(w*x)=h(w)\cdot g^{-1}(x) \end{cases}$$

其中 $w\in T$，$x\in B$。

以下证明：对任一 $w\in S, h(f(w))=w$，（对任一 $w\in T, f(h(w))=w$），因而 $f^{-1}=h$，$h^{-1}=f$，f 和 h 均为双射。

归纳证明 $h(f(w))=w$。

$w\in A=e1$ 时，$h(f(e1))=h(e2)=e1$。

对 $w\cdot x$，设 $h(f(w))=w$

$$\begin{aligned} h(f(w\cdot x)) &= h(f(w)*g(x)) \\ &= h(f(w))\cdot g^{-1}(g(x)) \\ &= w\cdot x \text{（据归纳假设 } h(f(w))=w\text{）} \end{aligned}$$

同理可证 $f(h(w))=w$。

为证 f 为同构映射，还需证明 f 保运算，即证明：对任何 u，$v\in S$，$f(u\cdot v)=f(u)*f(v)$。对 v 归纳如下：

$$f(u\cdot e1)=f(u)=f(u)*e2=f(u)*f(e1)$$

设 $f(u\cdot v)=f(u)*f(v)$，那么对任一 $x\in A$

$$\begin{aligned} f(u\cdot v\cdot x) &= f(u\cdot v)*g(x) \\ &= f(u)*f(v)*g(x) \\ &= f(u)*(f(v)*g(x)) \\ &= f(u)*f(v\cdot x) \end{aligned}$$

归纳完成。f 确为$<S,\cdot,e1>$到$<T,*,e2>$的同构映射。

本定理说明：

（1）自由独异点完全取决于它的生成集。

（2）所有有穷生成集生成的自由独异点无异于一个语言$<\Sigma^*$，并置$>$。

*14.1.3 高斯半群

先熟悉几个讨论高斯半群所需要的术语。

定义 14-3 设$<S,*>$为一半群，那么

（1）当$*$满足交换律时，称$<S,*>$为**交换半群**（commutative semigroups）。

（2）当 S 中元素均可约时，称 S 为**可约半群**（cancelable semigroups）。

（3）称 S 中元素 a 是 b 的**因子**（factor），如果有 S 中元素 c，d，使 $b=a*c$，$b=d*a$。

（4）在可约交换独异点$<S,\cdot,e>$中，若 a 是 b 的因子，同时 b 又是 a 的因子，那么称 a，b **相伴**（correlate）。

显然，可约交换独异点中的相伴关系是自反的，对称的，传递的，因而它是一个等价关系。还有进一步的事实如下。

定理 14-6 设$<S,*,e>$为可约交换独异点，那么 S 中相伴关系～为$<S,*,e>$上同余关系。

证明 已知～为 S 上等价关系，现证：对 S 中任意元素 a，b，c，$a\sim b$ 蕴涵 $a*c\sim b*c$。

设 $a\sim b$，因而有 $d1$，$d2$，使

$$a = b*d1 = d1*b;\ \ b = a*d2 = d2*a$$

于是

$$a*c = b*d1*c = (b*c)*d1 = d1*(b*c)$$
$$b*c = a*d2*c = (a*c)*d2 = d2*(a*c)$$

因此 $a*c$ 与 $b*c$ 相伴，即 $a*c \sim b*c$。

定理 14-7 设$<S,*,e>$为可约交换独异点。

（1）S 中元素 a，b 相伴，当且仅当有可逆元 c（c 有逆元），使 $a = b*c$。

（2）S 中所有可逆元构成一个相伴类（相伴关系等价类）。

（3）S 的相伴类具有相同的基数。

证明 （1）先证充分性。

设 $a = b*c$，c 为可逆元，那么 $b = a*c^{-1}$，又因*运算可交换，故 a 与 b 相伴。

再证必要性。设 a，b 相伴，因而有 c，d，使 $a = b*c$，$b = a*d$。进而 $a = a*d*c$，$b = b*c*d$。于是由 S 可约，有 $c*d = d*c = e$，即 c 可逆。我们证得 $a = b*c$，c 可逆。

（2）设 inv (S)为 S 中所有可逆元的集合，它不空（至少有元素 e），令 $a \in \text{inv}(S)$。现证 $[a]_\sim = \text{inv}(S)$。

由（1）$[a]_\sim = \{b \mid \exists c\ (b = a*c \wedge c \in \text{inv}(S))\}$，由于 a，c 可逆，b 亦可逆（$b*(c^{-1}*a^{-1}) = (c^{-1}*a^{-1})*b = e$），故$[a]_\sim \subseteq \text{inv}(S)$。

另一方面，若 $b \in \text{inv}(S)$，则 $b*b^{-1} = a*a^{-1}$，从而 $b = a*(a^{-1}*b)$，$a = b*(b^{-1}*a)$，故 $a \sim b$，$b \in [a]_\sim$。这就是说 $\text{inv}(S) \subseteq [a]_\sim$。

（3）为证本事实，只需证 $|\text{inv}(S)| = |[a]_\sim|$（$a$ 为 S 中任一元素）。

由于$[a]_\sim = \{b \mid \exists c\ (b = a*c \wedge c \in \text{inv}(S))\}$，建立映射 $h: [a]_\sim \to \text{inv}(S)$，对任一 $x \in [a]_\sim$，

$$h(x) = h(a*c_x) = c_x\ (c_x \text{可逆})$$

可证 h 确为一映射。当 $x = y$ 时，$a*c_x = a*c_y$，从而 $c_x = c_y$。

可证 h 为一单射。设 $c_x = c_y$，那么 $a*c_x = a*c_y$，从而 $x = y$。

还可证 h 为满射。对任何 $c \in \text{inv}(S)$，取 $x = a*c \in [a]_\sim$，$h(x) = h(a*c) = c$。

因此 $|\text{inv}(S)| = |[a]_\sim|$。

据定义 13-13、定理 13-12 及以上结果，我们有以下定理。

定理 14-8 可约交换独异点$<S, *, e>$的商半群$<S/\sim, *, [e]_\sim>$（$\sim$为相伴关系）为一可约交换独异点，且$|S/\sim| = |S/[e]_\sim|$。

【例 14-3】 $<I-\{0\}, \cdot, 1>$是可约交换独异点，inv $(I) = \{-1, 1\}$，它的其他相伴类有 $\{-2,2\}$，$\{-3,3\}, \cdots$。它的商半群为$<\{\{-1,1\}, \{-2,2\}, \{-3,3\}, \cdots\}, \odot, \{-1,1\}>$，其中$\odot$运算规定如下：

$$[x]_\sim \odot [y]_\sim = [x \cdot y]_\sim$$

或

$$\{-x, x\} \odot \{-y, y\} = \{-x \cdot y, x \cdot y\}$$

注意$<I, \cdot, 1>$不是可约的，因为 0 不可约。

定义 14-4 设$<S,*, e>$为可约交换独异点。若 a 是 S 中不可逆元素，且除了 a 及所有可逆元为其因子外没有别的因子，那么称 a 为**既约元**，否则称 a 为**可约元**。

这就是说，S 中元素可以分为三类：可逆元，可约元和既约元。

在例 14-3 中 -1，1 是可逆元，$-2, 2, -3, 3, -5, 5, \cdots, -p, p$（$p$ 为质数）为既约元，其他元素为可约元。

定义 14-5 可约交换独异点$<S,*, e>$称为**高斯半群**（Gauss semigroup），如果 S 中不可逆元素均可分解为若干个（有限个）既约元素的积，且这种分解在相伴意义下是惟一的，即若 a 有两个分解

$$a = p_1 * p_2 * \cdots * p_r = q_1 * q_2 * \cdots * q_s$$

则 $r = s$，且（适当变换运算次序）总可使 p_i 与 q_i 相伴。

【例 14-4】

（1）$<I-\{0\}, \cdot, 1>$为高斯半群。例如

$$24 = 2 \cdot 2 \cdot 2 \cdot 3 = (-2) \cdot 2 \cdot 2 \cdot (-3)$$

2 与 2，-2 均相伴，3 与 -3 也相伴。

（2）令 $S = \{a + b\sqrt{5}\, i \mid a, b$ 为整数且不同时为零$\}$，那么$<S, \cdot, 1>$为可约交换独异点（请读者自证），但它不是高斯半群，因为 9 有两种分解：

$$9 = 3 \cdot 3 = \left(2 + \sqrt{5}i\right) \cdot \left(2 - \sqrt{5}i\right)$$

但 3 与 $2+\sqrt{5}\, i$ 不相伴（请读者自行验证：①$3, 2+\sqrt{5}\, i, 2-\sqrt{5}\, i$ 均为既约元。②3 与 $2+\sqrt{5}\, i$ 不相伴）。

14.2 群

群是抽象代数学研究的最重要的代数结构类，也是应用最为广泛的代数结构类。以后将要深入研究的代数结构环和域也都是以群为基础的。

14.2.1 群及其基本性质

定义 14-6 称代数结构$<G, *>$为**群**（groups），如果

（1）$<G, *>$为一半群。

（2）$<G, *>$中有幺元 e。

（3）$<G, *>$中每一元素都有逆元。

也可以说，群是每个元素都可逆的独异点。群的载体常用字母 G 表示，因而字母 G 也常用于表示群。

定义 14-7 设$<G, *>$为一群。

（1）若*运算满足交换律，则称 G 为**交换群**或**阿贝尔群**（Abel group）。阿贝尔群又称**加群**，常表示为$<G, +>$（这里的+不是数加，而泛指可交换二元运算。回忆：*常被称为乘）。加群的幺元常用 0 来表示，常用 $-x$ 来表示 x 的逆元。

（2）G 为有限集时，称 G 为**有限群**（finite group），此时 G 的元素个数也称 G 的**阶**（order）；否则，称 G 为**无限群**（infinite group）。

【例 14-5】

（1）$<I, +>$（整数集与数加运算）为一阿贝尔群（加群），数 0 为其幺元。$<N,+>$不是群。因为所有非零自然数都没有逆元。

（2）$<Q_+, \cdot>$（正有理数与数乘）为一阿贝尔群，1 为其幺元。$<Q, \cdot>$不是群，因为数 0 无逆元。

（3）$<N_k, +_k>$为一 k 阶阿贝尔群，数 0 为其幺元。

（4）设 P 为集合 A 上全体双射函数的集合，$\circ$为函数合成运算。那么$<P, \circ>$为一群。A 上恒等函数 E_A 为其幺元。$<P, \circ>$一般不是阿贝尔群。

（5）上一节里我们指出，$<\text{inv}(S), *>$为独异点$<S, *>$的子独异点。事实上$<\text{inv}(S), *>$为一群。它常被称为半群的可逆元群。

群的下列基本性质是十分明显的。

定理 14-9 设$<G, *>$为群，那么

（1）G 有惟一的幺元，G 的每个元素恰有一个逆元。

（2）关于 x 的方程 $a*x=b$，$x*a=b$ 都有惟一解。

（3）G 的所有元素都是可约的。

（4）当 $G \neq \{e\}$时，G 无零元。

（5）幺元是 G 的惟一的等幂元素。

证明（1），（2），（3）是十分明显的。

（4）若 G 有零元，那么由定理 13-5 它没有逆元，与 G 为群矛盾（注意，$G=\{e\}$时，e 既是幺元，又是零元）。

（5）设 G 中有等幂元 x，那么

$$x*x=x \quad \text{或} \quad x*x=x*e$$

约去 x 得 $x=e$。

由于群的所有元素都有逆元，因此可认为群上定义了一元求逆运算“-1”。关于求逆运算有以下定理。

定理 14-10 对群$<G, *>$的任意元素 a，b，

（1）$(a*b)^{-1}=b^{-1}*a^{-1}$

（2）$(a^r)^{-1}=(a^{-1})^r$（记为 a^{-r}）（r 为自然数）

证明（1）$(a*b)*(b^{-1}*a^{-1})=a*(b*b^{-1})*a^{-1}=e$

$$(b^{-1}*a^{-1})*(a*b)=b^{-1}*(a^{-1}*a)*b=e$$

因此 $a*b$ 的逆元为 $b^{-1}*a^{-1}$，即$(a*b)^{-1}=b^{-1}*a^{-1}$。

（2）对 r 归纳。

$r=0$，1 时命题显然真。设$(a^r)^{-1}=(a^{-1})^r$，即$(a^{-1})^r$是 a^r 的逆元。那么，

$$a^{r+1}*(a^{-1})^{r+1}=a^r*(a*a^{-1})*(a^{-1})^r=a^r*(a^{-1})^r=e$$

$$(a^{-1})^{r+1}*a^{r+1}=(a^{-1})^r*(a^{-1}*a)*a^r=(a^{-1})^r*a^r=e$$

故 a^{r+1} 的逆元为$(a^{-1})^{r+1}$，即$(a^{r+1})^{-1}=(a^{-1})^{r+1}$。归纳完成，（2）得证。

据定理 14-10，在群中可引入“负指数幂”的概念，容易证明定理 14-11。

定理 14-11 对群$<G, *>$的任意元素 a，b，及任何整数 m，n，

（1）$a^m*a^n=a^{m+n}$

（2）$(a^m)^n=a^{mn}$

证（1）当 n 是自然数时，对 n 归纳（视 m 为参数）。

当 $n=0$ 时，显然

$$a^m * a^n = a^m * a^0 = a^m * e = a^{m+0}$$

当 $n = k+1$ 时，设 $a^m * a^k = a^{m+k}$

$$a^m * a^n = a^m * a^{k+1} = a^m * (a^k * a) = (a^m * a^k) * a = a^{m+k} * a = a^{m+k+1} = a^{m+n}$$

当 n 是负整数时，$a^m * a^n = (a^{-m})^{-1} * (a^{-n})^{-1}$。由于 $-m$，$-n$ 均为正整数，故

$$a^m * a^n = (a^{-m})^{-1} * (a^{-n})^{-1} = (a^{-n} * a^{-m})^{-1} = (a^{-(n+m)})^{-1} = a^{m+n}$$

（2）当 n 是自然数时，对 n 归纳（视 m 为参数）。

当 $n = 0$ 时，显然

$$(a^m)^n = (a^m)^0 = e = a^{m\times 0}$$

当 $n = k+1$ 时，设 $(a^m)^k = a^{mk}$

$$(a^m)^n = (a^m)^{k+1} = (a^m)^k * a^m = (a^{mk}) * a^m = a^{mk+m} = a^{m(k+1)} = a^{mn}$$

当 n 是负整数时，由于 $-n$ 均为正整数，故

$$(a^m)^n = ((a^m)^{-n})^{-1} = (a^{m\times(-n)})^{-1} = a^{-(m\times(-n))} = a^{mn}$$

定理得证。

如果我们用 aG 和 Ga 分别表示下列集合

$$aG = \{a*g \mid g \in G\},\quad Ga = \{g*a \mid g \in G\}$$

那么我们有以下定理。

定理 14-12 设$<G, *>$为一群，a 为 G 中任意元素，那么

$$aG = G = Ga$$

特别地，当 G 为有限群时，*运算的运算表的每一行（列）都是 G 中元素的一个全排列。

证明 $aG \subseteq G$ 是显然的。

设 $g \in G$，那么 $a^{-1}*g \in G$，从而 $a*(a^{-1}*g) \in aG$，即 $g \in aG$。因此 $Ga \subseteq G$。

$aG = G$ 得证。$Ga = G$ 同理可证。

这一事实的一个明显推论是：当 G 为有限群时，*运算的运算表的每一行（列）都是 G 中元素的一个全排列。从而有限群$<G, *>$的运算表中没有一行（列）上有两个元素是相同的。因此，当 G 为 1，2，3 阶群时，*运算都只有一个定义方式（即，不计元素记号的不同，只有一张定义*运算的运算表，如表 14-1 所示），于是可以说，1，2，3 阶的群都只有一个。

表 14-1

*	e
e	e

*	e	a
e	e	a
a	a	e

*	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

对群还可以讨论元素的阶，这是一个十分重要和非常有用的概念。

定义 14-8 设$<G, *>$为群，$a \in G$，称 a 的**阶**（order）为 n，如果 $a^n = e$，且 n 为满足此式的最小正整数。上述 n 不存在时，称 a 有**无限阶**。

【例 14-6】

（1）任何群 G 的幺元 e 的阶为 1，且只有幺元 e 的阶为 1。

（2）$<I, +>$中整数 $a \neq 0$ 时，a 有无限阶。

（3）$<N_6,+_6>$中 1 的阶是 6；2 的阶是 3；3 的阶是 2；4 的阶是 3；5 的阶是 6。

关于元素的阶有以下性质。

定理 14-13 有限群 G 的每个元素都有有限阶，且其阶数不超过群 G 的阶数 $|G|$。

证明 设 a 为 G 的任一元素，考虑

$$e=a^0,a^1,a^2,\cdots,a^{|G|}$$

这 $|G|+1$ 个 G 中元素。由于 G 中只有 $|G|$ 个元素，因此，根据鸽笼原理，它们中至少有两个是同一元素，不妨设

$$a^r=a^s \qquad (0\leqslant r<s\leqslant |G|)$$

于是 $a^{s-r}=e$，因此 a 有有限阶，且其阶数至多是 $s-r$，不超过群 G 的阶数 $|G|$。

定理 14-14 设$<G,*>$为群，G 中元素 a 的阶为 k，那么，$a^n=e$ 当且仅当 k 整除 n。

证明 先证充分性。

设 $a^k=e$，k 整除 n，那么 $n=kr$（r 为整数）。因为 $a^k=e$，所以 $a^n=a^{kr}=(a^k)^r=e^r=e$。

再证必要性。

设 $a^n=e$，$n=mk+r$，其中 m 为 n 除以 k 的商，r 为余数，因此 $0\leqslant r<k$。于是

$$e=a^n=a^{mk+r}=a^{mk}*a^r=a^r$$

因此，由 k 的最小性得 $r=0$，k 整除 n。

定理 14-15 设$<G,*>$为群，a 为 G 中任一元素，那么 a 与 a^{-1} 具有相同的阶。

证明 只要证 a 具有阶 n 当且仅当 a^{-1} 具有阶 n。由于逆元是相互的，即 $(a^{-1})^{-1}=a$，同此只需证：当 a 具有阶 n 时，a^{-1} 也具有阶 n。

设 a 的阶是 n，a^{-1} 的阶是 m。由于

$$(a^{-1})^n=(a^n)^{-1}=e^{-1}=e$$

故 $m\leqslant n$。又因为

$$a^m=((a^{-1})^m)^{-1}=e^{-1}=e$$

故 $n\leqslant m$。因此，$n=m$。

14.2.2 子群、陪集和拉格朗日定理

定义 14-9 设$<G,*>$为群。称$<H,*>$为 G 的**子群**（subgroups），如果$<H,*>$为 G 的子代数，且$<H,*>$为一群。

子群有下列特征性。

定理 14-16 设$<G,*>$为群，那么$<H,*>$为$<G,*>$子群的充分必要条件是

（1）G 的幺元 $e\in H$。

（2）若 $a,b\in H$，则 $a*b\in H$。

（3）若 $a\in H$，则 $a^{-1}\in H$。

证明 先证必要性。

设 H 为子群。那么（2）是显然的（因 H 为子代数）。为证（1），设$<H,*>$的幺元为 e'，那么 $e'*e'=e'$。由于在 G 中只有 e 是等幂元，故 $e'=e$，$e\in H$ 得证。为证（3）设$<H,*>$中任一元素 a 的 H 中逆元为 b，那么 $a*b=b*a=e$，由逆元的惟一性，b 就是 a 在 G 中的逆元，即 $b=a^{-1}\in H$。

充分性是明显的。事实上只要条件（2），（3）便可使$<H,*>$为$<G,*>$子群，因为

H 不空时条件（2）、（3）蕴涵条件（1）。因此，可用（2）、（3）来判别非空子集 H 是否构成 G 的子群$<H, *>$。

显然，对任何群 G，$<\{e\}, *>$及$<G, *>$均为其子群，它们被称为**平凡子群**，其他子群则称为**非平凡子群或真子群**。

【例 14-7】

（1）群$<N_6, +_6>$有非平凡子群

$$<\{0,3\}, +_6>\text{和}<\{0,2,4\}, +_6>$$

（2）设 $E \subseteq I$, E 为偶数集。那么$<E,+>$为$<I,+>$的子群，但$<N,+>$不是$<I,+>$的子群。

对于有限群，子群的判别更为简单。

定理 14-17 设$<G, *>$为有限群，那么当 G 的非空子集 H 对*运算封闭时，$<H, *>$即为 G 的子群。

证明 由于 G 为有限群，H 必为有限集。设 $|H| = r, a \in H$。考虑

$$a^1, a^2, \cdots, a^{r+1}, \cdots$$

它们都在 H 中（H 对*运算封闭），因此必定有 $a^i = a^j$（$0 \leqslant i < j \leqslant r+1$），从而 $a^{j-i} = e$，故 $e \in H$。

若 $H = \{e\}$，$<H, *>$为 G 的子群得证。

若 $H \neq \{e\}$，设 a 为 H 中任一不同于 e 的元素。同上可证，有 $k \geqslant 2$ 使 $a^k = e$，从而有

$$a * a^{k-1} = a^{k-1} * a = e$$

因此，$a^{k-1} = a^{-1} \in H$。

据定理 14-16，$<H, *>$为 G 的子群得证。

由于我们采用的上述证明方法仅仅依赖 H 的有限性，可见本定理可加强为

设$<G, *>$为群，H 为 G 的非空有限子集，且 H 对*运算封闭，那么$<H, *>$为$<G, *>$的子群。

和子群概念直接相关的是陪集的概念。

定义 14-10 设$<H, *>$为$<G, *>$的子群，那么对任一 $g \in G$，称 gH 为 H 的**左陪集**（left coset）称 Hg 为 H 的**右陪集**（right coset）。这里

$$gH = \{g * h \mid h \in H\},\quad Hg = \{h * g \mid h \in H\}$$

关于左（右）陪集我们有以下定理。

定理 14-18 设$<H, *>$为$<G, *>$的子群，那么

（1）当 $g \in H$ 时，$gH = H$（$Hg = H$）。

（2）对任意 $g \in G$，$|gH| = |H|$（$|Hg| = |H|$）。

证明（1）由定理 14-12 立得。

为证（2），只要证 H 与 gH 之间存在双射。定义函数 $f: H \to gH$ 如下:对任何一 $h \in H$，

$$f(h) = g * h$$

设 $h1 \neq h2$，那么 $f(h1) = g * h1, f(h2) = g * h2$，若 $f(h1) = f(h2)$，那么由可约性即得 $h1 = h2$，与 $h1 \neq h2$ 矛盾。f 为单射得证，f 为满射是显然的，因此 f 为双射。$|gH| = |H|$ 得证。同理可证 $|Hg| = |H|$。

定理 14-19 设$<H, *>$为$<G, *>$的子群，$a, b \in G$，那么，或者 $aH = bH$（$Ha = Hb$），或者 $aH \cap bH := \varnothing$（$Ha \cap Hb = \varnothing$）。

证明 设 $aH \cap bH \neq \varnothing$，那么有 $h1$，$h2 \in H$ 使得 $a*h1 = b*h2$。于是 $a = b*h2*h1^{-1}$。

为证 $aH \subseteq bH$，设 $x \in aH$。那么有 $h3 \in H$，使得 $x = a*h3 = b*(h2*h1^{-1}*h3) \in bH$。$aH \subseteq bH$ 得证。

同理可证 $bH \subseteq aH$。于是 $aH = bH$ 得证。对于右陪集 Ha，Hb，同上可证平行的命题。

由于对每一元素 $g \in G$，$g \in gH$（$g \in Hg$），$gH \subseteq G$（$Hg \subseteq G$），因此据以上讨论可以看出，子群 H 的全体左（右）陪集构成 G 的一个划分，且划分的各单元与 H（亦即陪集 eH，He）具有同样数目的元素。由此可导出下列重要的**拉格朗日定理**（Lagrange theorem）。

定理 14-20 设$<H, *>$为有限群$<G, *>$的子群，那么 H 的阶整除 G 的阶。

证明 由以上讨论知 $|G| = k|H|$，其中 k 为不同左（右）陪集的数目。定理得证。

注意，拉格朗日定理之逆不能成立。因此，据此定理只可判别一子代数“非子群”，却不可用它来判别一子代数“是子群”。

拉格朗日定理可用于证明下列事实：

（1）有限群$<G, *>$中任何元素的阶均为 G 的阶的因子。

设 a 为 G 中任一元素，a 的阶为 r。那么$<\{e, a, a^2, \cdots, a^{r-1}\}, *>$必为 G 的 r 阶子群，因此 r 整除 $|G|$。

（2）质数阶的群没有非平凡子群。

利用陪集还可定义陪集等价关系。

定义 14-11 设$<H, *>$为群$<G, *>$的子群。定义 G 上 H **的左（右）陪集等价关系**～。对任意 $a, b \in G$

$$a \sim b \text{ 当且仅当 } a, b \text{ 在 } H \text{ 的同一左（右）陪集中}$$

显然，～确为一等价关系。关于～有下列事实。

定理 14-21 设～为群 G 上 H 的左（右）陪集等价关系，那么

$$a \sim b \text{ 当且仅当 } a^{-1}*b \in H$$

证明 设 $a \sim b$，则有 $g \in G$，使 a，$b \in gH$，因而有 $h1$，$h2 \in H$，使得 $a = g*h1$，$b = g*h2$。于是

$$a^{-1}*b = (g*h1)^{-1}*(g*h2) = h1^{-1}*h2 \in H$$

反之，设 $a^{-1}*b \in H$，即有 $h \in H$ 使 $a^{-1}*b = h$。因而 $b = a*h \in aH$。而 $a \in aH$ 显然，故 a，b 在同一左陪集 aH 中，$a \sim b$ 真。

对右陪集等价关系同理可证上述定理。

*14.2.3 正规子群、商群和同态基本定理

定义 14-12 设$<H, *>$为群$<G, *>$的子群，称 H 为**正规子群**（normal subgroup），如果对任一 $g \in G$，

$$gH = Hg$$

显然，当 G 为阿贝尔群时，G 的任何子群都是正规子群。

我们知道，G 的子群 H 的左（右）陪集全体构成 G 的划分，从而导出 G 上的一个等价关系。那么当 H 为正规子群时情况将如何呢？

定理 14-22 设$<H, *>$为群$<G, *>$的正规子群，那么 H 的左（右）陪集等价关系～为$<G, *>$上的同余关系。

证明 只需证：对任意 $a,b,c\in G$

$$a\sim b \text{ 蕴涵 } a*c\sim b*c,\ c*a\sim c*b$$

设 $a\sim b$，那么 $a^{-1}*b\in H$，从而有 $h\in H$ 使 $h=a^{-1}*b$，或 $b=a*h$。又由于 $aH=Ha$，故有 $h1\in H$，使 $b=h1*a$。于是有 $h2\in H$ 使 $b*c=h1*(a*c)=(a*c)*h2$（亦因$(a*c)H=H(a*c)$），进而$(a*c)^{-1}*(b*c)=h2\in H$。因此 $a*c\sim b*c$。同理可证 $c*a\sim c*b$。$\sim$为$<G,*>$上的同余关系得证。

据定义 13-12，可作出群 G 的商代数$<G/\sim,\odot>$。由于$\sim$为正规子群 H 导出的等价关系，有时它也被记为$<G/H,\odot>$，其中 $G/H=G/\sim=\{gH\mid g\in G\}$（或$\{Hg\mid g\in G\}$），$\odot$运算定义如下:对任意 $g1,g2\in G$

$$[g1]\odot[g2]=[g1*g2]$$

亦即

$$g1H\odot g2H=(g1*g2)H \text{ 或 } Hg1\odot Hg2=H(g1*g2)$$

定理 14-23 群 G 的上述商代数结构$<G/H,\odot>$为一群。

证明 据定理 13-12，只要证：

（1）$eH(=H)$为关于$\odot$运算的幺元。事实上，对任意 $g\in G$

$$gH\odot eH=(g*e)H=gH=eH\odot gH$$

（2）对每一 gH 有关于$\odot$运算的逆元。事实上，对任意 $g\in G$

$$gH\odot g^{-1}H=(g*g^{-1})H=H=g^{-1}H\odot gH$$

【例 14-8】 不难明白，$H=\{0,3\}$时$<H,*>$为群$<N_6,+_6>$的正规子群。由于它们都是加群，我们把左右陪集分别表示为 $a+H$，$H+a$。于是 H 有左右陪集如下：

$0+H=H+0=H:\{0,3\}$（$=3+H=H+3$）

$1+H=H+1\quad:\{1,4\}$（$=4+H=H+4$）

$2+H=H+2\quad:\{2,5\}$（$=5+H=H+5$）

$<N_6,+_6>$有商群$<\{\{0,3\},\{1,4\},\{2,5\}\},\oplus>$，而$(a+H)\oplus(b+H)=(a+b)+H$。例如：

$$\{1,4\}\oplus\{2,5\}=(1+H)\oplus(2+H)=3+H=\{0,3\}$$

由第 13 章我们已经知道同余关系与同态映射之间的密切联系，为了弄清正规子群及其导出的陪集同余关系与同态映射之间的联系，我们再来讨论群之间的同态映射——群同态。

定理 14-24 设 h 为群$<G_1,*_1,e_1>$到群$<G_2,*_2,e_2>$的同态映射，那么 $h(e_1)=e_2$。

证明 因为 $h(e_1)=h(e_1*_1e_1)=h(e_1)*_2h(e_1)$，所以 $h(e_1)=e_2$（G_2中只有 e_2是等幂元）。

因此，据定理 13-9，上述同态映射的同态像$<h(G_1),*_2,e_2>$为$<G_2,*_2,e_2>$的子群。

定理 14-25 设 h 为群$<G_1,*_1>$到群$<G_2,*_2>$的同态映射，那么 h 的核 $K(h)$构成$<G_1,*_1>$的正规子群。（为简明计，以下用 K 表示 $K(h)$）

证明 根据定理 13-10 及上述定理 14-24，可知$<K,*_1>$为$<G_1,*_1>$的子群。

现对任一 $g\in G$，证明 $gK=Kg$。为此，设 $x\in gK$，那么有 $k\in K$，使得 $x=g*_1k$。考虑到

$$h(g*_1k*_1g^{-1})=h(g)*_2e_2*_2h(g^{-1})=e_2$$

故 $g*_1k*_1g^{-1}\in K$。令 $g*_1k*_1g^{-1}=k'$，于是

$$k'*_1g=g*_1k=x,\ x\in Kg$$

$gK\subseteq Kg$ 得证。同理可证 $Kg\subseteq gK$。因此 $gK=Kg$ 证毕。

根据定理 13-14，我们便可得到重要的同态基本定理。

定理 14-26 设 h 为群$<G_1, *_1>$到群$<G_2, *_2>$的同态映射，$K = K(h)$，那么商群$<G/K, \odot>$与同态像$<h(G_1), *_2>$同构。

【例 14-9】 设 h 为群$<N_6, +_6>$到群$<N_3, +_3>$的同态映射，使得

$$h(x) = 2x \ (\text{mod}3)$$

即

$$h(0) = h(3) = 0,\ h(1) = h(4) = 2,\ h(2) = h(5) = 1$$

于是 $K = K(h) = \{0,3\}$，$<K, +_6>$为$<N_6, +_6>$的正规子群。正如例 14-8 指出的那样，

$$<N_6/\mathrm{K}, \oplus> = <\{\{0,3\},\{1,4\},\{2,5\}\}, \oplus>$$

它同构于$<N_3, +_3>$，同构映射 $i: N_6/K \to N_3$ 满足

$$i(\{0,3\}) = 0,\ i(\{2,5\}) = 1, i(\{1,4\}) = 2$$

14.3 循环群和置换群

在这一节里我们要介绍两种重要的群：循环群和置换群。

14.3.1 循环群

回忆循环半群的概念。

定义 14-13 称<G，*>为**循环群**（cyclic group），如果 G 为群，且 G 中存在元素 g，使 G 以$\{g\}$为生成集，即 G 的任何元素都可表示为 g 的幂（约定 $e = g^0$）。这时 g 称为循环群 G 的**生成元**（generater）。

【例 14-10】

（1）$<I,+>$为循环群，1 或（-1）为其生成元。

（2）令 $A = \{2^i \mid i \in I\}$，那么$<A, \cdot>$（$\cdot$ 为数乘）是循环群，2 是生成元。

（3）$<N_5, +_5>$为循环群，1，2，3，4 都可以是生成元。

关于循环群的下列性质是明显的。

定理 14-27 设$<G, *>$为循环群，g 为生成元，那么

（1）G 为阿贝尔群。

（2）G 的 h 同态像是以 $h(g)$为生成元的循环群。

（3）G 为无限循环群时必同构于$<I,+>$。

（4）G 为有限循环群时，必有

$$G = \left\{e, g, g^2, \cdots, g^{n-1}\right\}$$

其中 $n = |G|$，也是 g 的阶。从而 n 阶循环群必同构于$<N_n,+_n>$。

证明（1），（2），（3）的证明留给读者，下面证明（4）。

由于 G 为有限群，g 有有限阶，设为 r，$r \leqslant |G| = n$。易证$\left\{e, g, g^2, \cdots, g^{r-1}\right\}$为 G 的子群（只要证其每一元素 g^i 有逆元 g^{r-i}）。现证

$$G \subseteq \left\{e, g, g^2, \cdots, g^{r-1}\right\}$$

从而知 $n=r$，$G=\left\{e, g, g^2, \cdots, g^{n-1}\right\}$。

设有 $g^k \in G$，但 $g^k \notin \left\{e, g, g^2, \cdots, g^{r-1}\right\}$。令 $k=mr+t$，其中 m 为 r 除 k 的商，t 为剩余，$0 \leqslant t < r$，于是

$$g^k = g^{mr+t} = g^{mr} * g^t = g^t$$

这就是说 $g^t \notin \left\{e, g, g^2, \cdots, g^{r-1}\right\}$，$0 \leqslant t < r$，矛盾。因此 $G=\left\{e, g, g^2, \cdots, g^{r-1}\right\}$，命题得证。

本定理（3），（4）告诉我们，循环群本质上只有两种，一种同构于$<I,+>$，另一种同构于$<N_k, +_k>$，弄清了$<I,+>$与$<N_k, +_k>$，也便弄清了所有无限的和有限的循环群。

此外我们还有以下定理。

定理 14-28 循环群的子群都是循环群。

证明 设$<G, *>$为 g 生成的循环群，$<H, *>$为其子群。当然，H 中元素均可表示为 g^r 形。

（1）若 $H=\{e\}$，显然 H 为循环群。

（2）若 $H \neq \{e\}$，那么 H 中有 $g^i (i \neq 0)$。由于 H 为子群，H 中必还有 g^{-i}。因此，不失一般性，可设 i 为正整数，并且它是 H 中元素的最小正整数指数。现证 H 为 g^i 生成的循环群。

设 g^j 为 H 中任一元素。令 $j=mi+r$，其中 m 为 i 除 j 的商，r 为剩余，$0 \leqslant r < i$。于是

$$g^j = g^{mi+r} = g^{mi} * g^r$$

$$g^r = g^{-mi} * g^j$$

由于 g^j，$g^{-mi} \in H$，（因 $g^{mi} \in H$），故 $g^r \in H$，根据 i 的最小性，$r=0$，从而 $g^j = g^{mi} = (g^i)^m$，H 为循环群，证毕。

根据上述定理，立即可以推得以下定理。

定理 14-29 设$<G, *>$为 g 生成的循环群。

（1）若 G 为无限群，则 G 有无限多个子群，它们分别由 $g^0, g^1, g^2, g^3, \cdots$生成。

（2）若 G 为有限群，$|G|=n$，且 n 有因子 $k_1, k_2, k_3, \cdots, k_t$，那么 G 有 r 个循环子群，它们分别由 $g^{k_1}, g^{k_2}, g^{k_3}, \cdots$ 生成（注意这 r 个子群中可能有相同者）。

【例 14-11】

（1）$<I, +>$有循环子群：

$<\{0\}, +>$，$<\{0, 2, -2, 4, -4, \cdots\}, +>$，$<\{0, 3, -3, 6, -6, \cdots\}, +>$，$<\{0, 4, -4, 8, -8, \cdots\}, +>$，$\cdots$，$<I, +>$

（2）$<N_6, +_6>$有循环子群：

$<\{0\}, +_6>$，$<\{0,2,4\}, +_6>$，$<\{0,3\}, +_6>$，$<N_6, +_6>$

*14.3.2 置换群

回忆第 11 章定义 11-8，我们称有限集上的双射函数为**置换**。置换有独特的表示方式。

【例 14-12】 设 $A=\{1,2\}$，那么 A 上有两个置换：

$$p_1 = \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix} \qquad p_2 = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}$$

当 $A=\{1,2,3\}$ 时，A 上有 6 个置换：

$$p_1=\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}\qquad p_2=\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}\qquad p_3=\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}$$

$$p_4=\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}\qquad p_5=\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}\qquad p_6=\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}$$

一般地，$A=\{a_1, a_2, \cdots, a_n\}$ 时，A 上有 $n!$ 个置换。置换 p 满足 $p(a_i)=a_{ji}$ 时，可表示为

$$\begin{pmatrix}a_1&a_2&\cdots&a_n\\a_{j1}&a_{j2}&\cdots&a_{jn}\end{pmatrix}$$

置换的合成运算通常用记号$\circ$表示之，对置换的独特表示形式计算它们的合成时，可像计算两个关系的合成那样来进行。例如

$$p_5\circ p_2=\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}\circ\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}=\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}$$

因此，应当注意

$$(p_i\circ p_j)(x)=p_j(p_i(x))$$

对于置换的合成运算而言，A 上置换的全体中有幺元——恒等函数，又称**幺置换**，且每一置换都有逆置换，因此置换全体构成一个群。

定义 14-14 将 n 个元素的集合 A 上的置换全体记为 S，那么称群$<S,\circ>$为 n 次**对称群**（symmetric group），它的子群又称为 n 次**置换群**（permutation group）。

【例 14-13】 令 $A=\{1,2,3\}$，那么 $S_3=\{p_i \mid i=1,2,3,4,5,6\}$，（$p_i$ 如例 14-12 给定）。其中 p_1 为幺置换，$p_2^{-1}=p_2$，$p_3^{-1}=p_3$，$p_4^{-1}=p_4$，$p_5^{-1}=p_6$。$<S_3,\circ>$为三次对称群。

从另一个角度也可得到这个群。

设正三角形的三个顶点由 1，2，3 所标记（如图 14-1 所示）。考虑以三角形中心 o 为轴的旋转σ_0，σ_1，σ_2，（旋转 0°，旋转 120°，旋转 240°），以及以直线 l_1，l_2，l_3 的翻转（σ_3，σ_4，σ_5）。显然，每次旋转和翻转都对应于三角形顶点的一个置换，对应关系如下：

σ_0（旋转 0°）　$p_1=\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}$

σ_1（旋转 120°）　$p_5=\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}$

σ_2（旋转 240°）　$p_6=\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}$

σ_3（绕 l_3 翻转）　$p_2=\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}$

σ_4（绕 l_2 翻转）　$p_3=\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}$

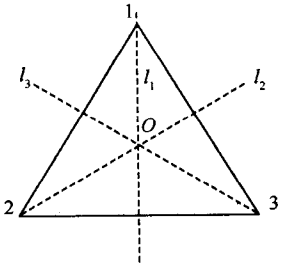


图　14-1

σ_5（绕 l_1 翻转）　　$p_4=\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}$

不难看出<{σ_0，σ_1，σ_2，σ_3，σ_4，σ_5},∘>构成一群（其中∘为旋转或翻转操作的合成），它同构于<S_3,∘>。

【例 14-14】　令 $A=\{1,2,3,4\}$，$S_4=\{p \mid p$ 为 A 上置换$\}$，因此，<S_4，∘>为四次对称群。

再来考虑由 1，2，3，4 标记 4 个顶点的正方形（如图 14-2 所示）的旋转和翻转，它们又各对应于 A 上的一个置换：

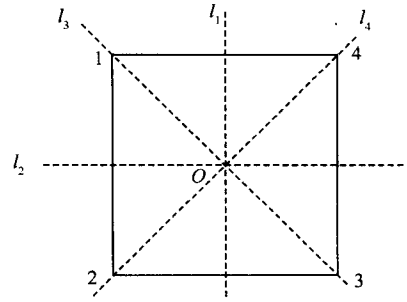


图　14-2

σ_0（旋转 0°）　　$p_1=\begin{pmatrix}1&2&3&4\\1&2&3&4\end{pmatrix}$

σ_1（旋转 90°）　　$p_2=\begin{pmatrix}1&2&3&4\\2&3&4&1\end{pmatrix}$

σ_2（旋转 180°）　　$p_3=\begin{pmatrix}1&2&3&4\\3&4&1&2\end{pmatrix}$

σ_3（旋转 270°）　　$p_4=\begin{pmatrix}1&2&3&4\\4&1&2&3\end{pmatrix}$

σ_4（绕 l_1 翻转）　　$p_5=\begin{pmatrix}1&2&3&4\\4&3&2&1\end{pmatrix}$

σ_5（绕 l_2 翻转）　　$p_6=\begin{pmatrix}1&2&3&4\\2&1&4&3\end{pmatrix}$

σ_6（绕 l_3 翻转）　　$p_7=\begin{pmatrix}1&2&3&4\\1&4&3&2\end{pmatrix}$

σ_7（绕 l_4 翻转）　　$p_8=\begin{pmatrix}1&2&3&4\\3&2&1&4\end{pmatrix}$

设Σ为这 8 种旋转、翻转操作的集合，∘为操作的合成运算，那么易证<Σ，∘>为群。∘的运算表见表 14-2。

表　14-2

∘	σ_0	σ_1	σ_2	σ_3	σ_4	σ_5	σ_6	σ_7
σ_0	σ_0	σ_1	σ_2	σ_3	σ_4	σ_5	σ_6	σ_7
σ_1	σ_1	σ_2	σ_3	σ_0	σ_7	σ_6	σ_4	σ_6
σ_2	σ_2	σ_3	σ_0	σ_1	σ_5	σ_4	σ_7	σ_5
σ_3	σ_3	σ_0	σ_1	σ_2	σ_6	σ_7	σ_5	σ_4
σ_4	σ_4	σ_6	σ_5	σ_7	σ_0	σ_2	σ_1	σ_3
σ_5	σ_5	σ_7	σ_4	σ_6	σ_2	σ_0	σ_3	σ_1
σ_6	σ_6	σ_5	σ_7	σ_4	σ_3	σ_1	σ_0	σ_2
σ_7	σ_7	σ_4	σ_6	σ_5	σ_1	σ_3	σ_2	σ_0

因此$<\{p_1, p_2, \cdots, p_6\}, \circ>$也为群，它是$<S_4, \circ>$的子群。一个 4 次的 8 阶置换群（它不是 4 次对称群。4 次对称群有 24 个置换。

对置换群稍作推广便有变换群的概念。

定义 14-15 任意集合上的双射函数称为**变换**。

定义 14-16 对任意集合 A 定义集合 S

$$S = \{f \mid f \in A^A \wedge f \text{为双射}\}$$

那么群$<S, \circ>$及其子群称为**变换群**，其中$\circ$为函数的合成运算。

像定理 14-3 那样，可以证明下列群表示定理。

定理 14-30 每个群均同构于一个变换群，特别地，每一个有限群均同构于一个置换群。

证明 设$<G, *>$为任一群，对 G 中每一元素 a，定义双射函数 $f_a: G \to G$ 如下。

$$f_a(x) = a*x$$

（请读者自行证明 f_a 确为双射）令

$$F = \{f_a \mid a \in G\}$$

现证$<F, \circ>$为群（$\circ$为函数合成运算）。

（1）F 对$\circ$运算封闭。

设 $f_a \in F$，$f_b \in F$，那么 $a \in G$，$b \in G$。考虑 $f_a \circ f_b$：对任意 $x \in G$，

$$f_a \circ f_b(x) = f_a(f_b(x)) = a*b*x = f_{a*b}(x)$$

即 $f_a \circ f_b = f_{a*b}$。由于 a，$b \in G$，$f_{a*b} \in F$，故 $f_a \circ f_b \in F$。

（2）$\circ$运算显然满足结合律。

（3）$\circ$运算有幺元 $f_e \in F$。

（4）F 中每一元素 f_a 均有逆元 $f_{a^{-1}}$。这是因为由 $a \in G$ 知 $a^{-1} \in G$，从而 $f_{a^{-1}} \in F$，并且对任意 $x \in G$，$f_a \circ f_{a^{-1}}(x) = a*a^{-1}*x = x = e*x = f_e(x)$，即 $f_a \circ f_{a^{-1}} = f_e$。

再证$<G, *>$与$<F, \circ>$同构。为此定义函数 $h: G \to F$，使得对任一 $x \in G$，$h(x) = f_x$。显然 h 为双射（请读者自证）。另仿（1）可证 h 保运算，即对 G 中任意元素 x, y，有

$$h(x*y) = f_{x*y} = f_x \circ f_y = h(x) \circ h(y)$$

14.4 环

半群和群都是只含有一个二元运算的代数结构，从这一节起我们要讨论含有两个二元运算的代数结构环和域，首先讨论“环”。

14.4.1 环和整环

未作特别说明时，下文中符号+，$\cdot$ 表示满足结合律的一般二元运算，分别称为**加**、**乘**运算（未必是数加和数乘），并对它们沿用数加、数乘的术语及运算约定，例如，a，b 的积表示为 ab，n 个 a 的和 $a+\cdots+a$ 表示为 na，n 个 a 的积表示为 a^n 等。

定义 14-17 称代数结构$<R, +, \cdot>$为环（ring），如果

（1）$<R, +>$是阿贝尔群（或加群）。

（2）$<R, \cdot>$是半群。

（3）乘运算对加运算可分配，即对任意元素 $a, b, c \in R$，

$$a(b+c)=ab+ac,\ (b+c)a=ba+ca$$

【例 14-15】

（1）$<I,+,\cdot>$（I 为整数集，$+,\cdot$ 为数加与数乘运算）为一环；$<Q,+,\cdot>$（Q 为有理数集，$+,\cdot$ 为数加与数乘运算）为一环。

（2）$<N_k,+_k,\times_k>$为环，因为我们已知$<N_k,+_k>$为加群，$<N_k,\times_k>$为半群，此外，

$$\begin{aligned}a\times_k(b+_kc)&=a\times_k((b+c)\bmod k)\\&=(a(b+c)(\bmod k))(\bmod k)\\&=(a(b+c))(\bmod k)\\&=(ab+ac)(\bmod k)\\&=ab(\bmod k)+_kac(\bmod k)\\&=a\times_kb+_ka\times_kc\end{aligned}$$

（其中 $x(\bmod k)$表示 x 除以 k 的剩余）且同理可证$(b+_kc)\times_k a=b\times_k a+_k c\times_k a$。

（3）所有整数分量的 $n\times n$ 方阵集合 M_n 与矩阵加运算（+）及矩阵乘运算（$\circ$）构成一环，即，$<M_n,+,\circ>$为环。

（4）所有实系数多项式（以 x 为变元）的集合 $R[x]$与多项式加，乘运算构成环，即$<R[x],+,\cdot>$为环。

（5）$<\{0\},+,\cdot>$（其中 0 为加法幺元、乘法零元）为一环，称为零环。（其他环至少有两个元素）。

（6）$<\{0,e\},+,\cdot>$（其中 0 为加法幺元、乘法零元，e 为乘法幺元）为一环。

环有下列基本性质，这些性质与有理数十分一致。

定理 14-31 设$<R,+,\cdot>$为环，0 为加法幺元，那么对任意 $a,b,c\in R$

（1）$0a=a0=0$（加法幺元必为乘法零元）。

（2）$(-a)b=a(-b)=-ab$（$-a$ 表示 a 的加法逆元，下同）。

（3）$(-a)(-b)=ab$。

（4）若用 $a-b$ 表示 $a+(-b)$，则

$$(a-b)c=ac-ab,\ c(a-b)=ca-cb$$

证明（1）$0=a0+(-a)0=a(0+0)+(-a)0=a0+a0+(-a)0=a0$

同理可证 $0a=0$。

（2）$(-a)b=ab+(-ab)+(-a)b=(a+(-a))b+(-ab)=0b+(-ab)=-ab$

同理可证 $a(-b)=-ab$。

（3）仿（2）可证。

（4）$(a-b)c=(a+(-b))c=ac+(-b)c=ac+(-bc)=ac-bc$

同理可证 $c(a-b)=ca-cb$。

注意，$<R,+,\cdot>$中乘运算未必满足交换律，也未必有幺元（但一定有零元）。

定义 14-18 环$<R,+,\cdot>$中 $\cdot$ 运算满足交换律时，称 R 为**交换环**（commutative rings），当 $\cdot$ 运算有幺元时，称 R 为**含幺环**（ring with unity）。

例 14-15 中（1），（2），（4）是含幺交换环，（3）是含幺环。

环不仅必有乘法零元，还可能有下述所谓零因子。

定义 14-19 设$<R,+,\cdot>$为环，若有非零元素 a，b 满足 $ab=0$，则称 a，b 为 R 的**零**

因子（divisor of 0），并称 R 为**含零因子环**，否则称 R 为**无零因子环**。

【例 14-16】 在环$<N_6,+_6,\times_6>$中，0 是零元，2，3 为零因子，因为 $2\times_6 3=0$。在环$<M_2,+,\circ>$中有零因子

$$\begin{pmatrix}1 & -1\\ -1 & 1\end{pmatrix} \text{ 和 } \begin{pmatrix}1 & -1\\ -1 & 1\end{pmatrix}$$

因为

$$\begin{pmatrix}1 & -1\\ -1 & 1\end{pmatrix}\circ\begin{pmatrix}1 & 1\\ 1 & 1\end{pmatrix}=\begin{pmatrix}0 & 0\\ 0 & 0\end{pmatrix}$$

它是矩阵加的幺元。

关于零因子我们有以下定理。

定理 14-32 设$<R,+,\cdot>$为环，那么 R 为无零因子环当且仅当 R 满足可约性（即 R 中所有非零元素均可约）。

证明 设 R 无零因子，且 $ab=ac$，$a\neq 0$。那么 $ab-ac=0$，$a(b-c)=0$。a 和 $b-c$ 不是零因子，因此或者 $a=0$ 或者 $b-c=0$ 。因为 $a\neq 0$，故 $b-c=0$，即 $b=c$。a 可约得证。

反之，设对任意元素 x，y，z，$x\neq 0$，由 $xy=xz$，可推得 $y=z$。欲证 R 无零因子。反设 R 中有零因子 b，c，$b\neq 0$，$c\neq 0$，但 $bc=0$。于是 $bc=b0$，据可约性得 $c=0$，矛盾。因此 R 无零因子。

定义 14-20 设$<R,+,\cdot>$不是零环。称 R 为**整环**（1ntegra1 domain），如果$<R,+,\cdot>$是含么、交换、无零因子坏。

显然，上文中的$<I,+,\cdot>$是整环，$<N_6,+_6,\times_6>$及$<M_2,+,\circ>$不是整环。注意$<\{0\},+,\cdot>$也不是整环，它是零环。

*14.4.2 子环和理想

定义 14-21 设$<R,+,\cdot>$为环，称代数结构$<S,+,\cdot>$为 R 的**子环**（subring），如果

（1）$<S,+>$为$<R,+>$的子群（正规子群）。

（2）$<S,\cdot>$为$<R,\cdot>$的子半群。

显然，当$<S,+,\cdot>$为$<R,+,\cdot>$的子代数系统，并且 S 对（关于+的）求逆运算“－”封闭，那么$<S,+,\cdot>$为$<R,+,\cdot>$的子环。另外，由于乘对加的分配律在$<S,+,\cdot>$中沿袭下来，因此子环必定是环。

定义 14-22 设$<D,+,\cdot>$为环$<R,+,\cdot>$的子环。称$<D,+,\cdot>$为 R 的**理想子环**，简称**理想**（ideals），如果对任意的 $r\in R$，$d\in D$，有 $rd\in D$，$dr\in D$。当 $D=R$ 或 $D=\{0\}$时，称$<D,+,\cdot>$为$<R,+,\cdot>$**平凡理想**。

【例 14-17】 $<E,+,\cdot>$（E 为偶数集），$<\{0,2,4\},+_6,\times_6>$分别为环$<I,+,\cdot>$，$<N_6,+_6,\times_6>$的理想。环$<M_2,+,\circ>$有子环$<P,+,\circ>$

$$P=\left\{\begin{pmatrix}a & 0\\ b & 0\end{pmatrix}:a,b\in I\right\}$$

但它不是理想，因为$\begin{pmatrix}a & 0\\ b & 0\end{pmatrix}\circ\begin{pmatrix}1 & 1\\ 1 & 1\end{pmatrix}=\begin{pmatrix}a & a\\ b & b\end{pmatrix}\notin P$。

关于环的理想我们有以下定理。

定理 14-33 设$<D1,+,\cdot>$，$<D2,+,\cdot>$为环$<R,+,\cdot>$的理想，那么

（1）$<D1\cap D2,+,\cdot>$为$<R,+,\cdot>$的理想。

（2）$<D1+D2,+,\cdot>$为$<R,+,\cdot>$的理想。其中$D1+D2=\{d1+d2\mid d1\in D1\wedge d2\in D2\}$。

证（1）的证明留给读者。

（2）先证$<D1+D2,+,\cdot>$为 R 的子环。为此只要证 $D1+D2$ 对于减运算封闭，对乘运算也封闭（为什么？参阅本章练习第 19 题）。

设$x,y\in D1+D2, x=d1+d2, y=d1'+d2'$，那么

$$x-y=(d1-d1')+(d2-d2')\in D1+D2$$

$$x\cdot y=(d1+d2)\cdot(d1'+d2')$$

$$=d1d1'+d1d2'+d2d1'+d2d2'$$

由于 $D1$，$D2$ 为理想，$d1d1'\in D1$，$d1d2'\in D1$，$d2d1'\in D2$，$d2d2'\in D2$，因此$x\cdot y=(d1d1'+d1d2')+(d2d1'+d2d2')\in D1+D2$。

再证对任何$r\in R$，$d\in D1+D2$，有$rd\in D1+D2$，$dr\in D1+D2$。设$d=d1+d2$，那么

$$rd=r(d1+d2)=rd1+rd2\in D1+D2$$

同理可证$dr\in D1+D2$。

因此，$<D1+D2,+,\cdot>$为$<R,+,\cdot>$的理想。

定理 14-34 设 h 为环$<R1,+,\cdot>$到环$<R2,+,\cdot>$的同态，那么

（1）$<h(R1),+,\cdot>$为$<R2,+,\cdot>$的子环。

（2）$<K(h),+,\cdot>$为 $R1$ 的理想。

证（1）可由定理 13-9 立得。

（2）将 $K(h)$记为 K。我们已知$<K,+>$为阿贝尔群（定理 14-25）。现只要证：

1）K 对 $\cdot$ 运算封闭。

现设$k1$，$k2\in K$，那么$h(k1\cdot k2)=h(k1)\cdot h(k2)=0\cdot 0=0$，因此$k1\cdot k2\in K$。

2）对任何$r\in R1$，$k\in K$，有$rk\in K$，$kr\in K$。

由于

$$h(rk)=h(r)\cdot h(k)=h(r)\cdot 0=0=0\cdot h(r)=h(k)\cdot h(r)=h(kr)$$

故$rk\in K$，$kr\in K$。

因此 K 为 $R1$ 的理想。

理想在环中的地位与正现了群在群中的地位相当，我们可以在环中讨论理想（亦即环的加法正规子群）的陪集及陪集等价关系。

定理 14-35 设$<D,+,\cdot>$为环$<R,+,\cdot>$的理想，作$<R,+>$的正规子群$<D,+>$的（加法）陪集等价关系～，它是$<R,+,\cdot>$上的同余关系。

证明 由上一节的讨论我们已经知道，关系～为$<R,+>$的同余关系。为证～为$<R,+,\cdot>$的同余关系，只要对任意 a，b，$c\in R$ 证明：

$$a\sim b \text{ 蕴涵 } ac\sim bc,\ ca\sim cb$$

现设$a\sim b$，那么$a\in b+D$，即有$d\in D$，使得$a=b+d$。由于$ac=(b+d)c=bc+dc$，$dc\in D$（D 为理想），因此$ac\in bc+D$，$ac\sim bc$。同理可证$ca\sim cb$。

综上所述，D 的陪集等价关系～为$<R,+,\cdot>$上的同余关系。

据定义 13-13，可构作环$<R, +, \cdot>$的商的代数$<R/\sim, \oplus, \odot>$。据定理 13-12，$<R/\sim, \oplus, \odot>$也是一个环，称为 R 的**商环**（quotient ring）。这里运算$\oplus$，$\odot$的意义如下所述：

$$(a+D)\oplus(b+D) = (a+b)+D$$
$$(a+D)\odot(b+D) = (ab)+D$$

上述由理想 D 导出的商环也可记为$<R/D, \oplus, \odot>$。

读者一定想到了同态基本定理。

定理 14-36 设 h 为环$<R1, +, \cdot>$到环$<R2, +, \cdot>$的同态，$K = K(h)$，那么 K 导出的商环$<R1/K, \oplus, \odot>$与同态像$<h(R1), +, \cdot>$同构。

本定理由定理 13-14 及以上讨论立即可得。

【例 14-18】 证明：环$<N_6, +_6, \times_6>$关于理想$<\{0, 3\}, +_6, \times_6>$的商环$<N_6/\{0, 3\}, \oplus, \odot>$，与环$<N_3, +_3, \times_3>$同构。

证明 定义函数 $h: N_6 \to N_3$，使

$$h(0) = h(3) = 0$$
$$h(1) = h(4) = 1$$
$$h(2) = h(5) = 2$$

易证 h 为同态，{0,3}为同态核，同态像即为$<N_3, +_3, \times_3>$。据定理 14-36，$<N_6/\{0, 3\}, \oplus, \odot>$与$<N_3, +_3, \times_3>$同构。

上述证明也可通过列出 $\oplus$，$\odot$的运算表来完成。令[0]={0, 3}，[1] = {1, 4}，[2] = {2, 5}，那么 $N_6/\{0, 3\}$上$\oplus$，$\odot$运算由表 14-3 确定。

表 14-3

$\oplus$	[0]	[1]	[2]	$\odot$	[0]	[1]	[2]
[0]	[0]	[1]	[2]	[0]	[0]	[0]	[0]
[1]	[1]	[2]	[0]	[1]	[0]	[1]	[2]
[2]	[2]	[0]	[1]	[2]	[0]	[2]	[1]

注意，$[x] \oplus [y] = [x+y]$，$[x] \odot [y] = [xy]$，它们同 N_3 上运算$+_3, \times_3$的运算表相一致。

*14.5 域和有限域

定义 14-23 称$<F, +, \cdot>$为**域**（fields），如果$<F, +, \cdot>$为一环，且$<F-\{0\}, \cdot>$为阿贝尔群。

由于群无零因子（为什么？），因此域必定是整环。事实上，域也可定义为每个非零元素都有乘法逆元的整环。

【例 14-19】 $<Q, +, \cdot>$为域，但$<I, +, \cdot>$不是域，因为在整数集中整数没有乘法逆元。$<N_5, +_5, \times_5>$为域，1 的逆元是 1，4 的逆元是 4，2 和 3 互为逆元。但$<N_6, +_6, \times_6>$不是域，它甚至不是整环，同为它有零因子，例如 2，3，它们没有乘法逆元。

域有以下基本性质。

定理 14-37 $<N_p, +_p, \times_p>$为域当且仅当 p 为质数。

证明 设 p 不是质数，那么由上例可知 N_p 有零因子（p 的因子），故$<N_p,+_p,\times_p>$不是域。

反之，当 p 为质数时，可证 N_p 中所有非零元素都有$\times_p$运算的逆元，从而含么交换环$<N_p,+_p,\times_p>$为域。

设 q 是 N_p 中任一非零元素，那么 q 与 p 质。据数论事实，有整数 m，n 使

$$mp+nq=1$$

从而

$$(mp+nq)(\mathrm{mod}\ p)=1$$

即

$$mp(\mathrm{mod}\ p)+_p nq(\mathrm{mod}\ p)=1$$

$$0+n(\mathrm{mod}\ p)\times_p q(\mathrm{mod}\ p)=1，或\ n(\mathrm{mod}\ p)\times_p q=1$$

因此，q 有逆元 $n(\mathrm{mod}\ p)$。

定理得证。

定理 14-38 有限整环都是域。

证明 设$<R，+，\cdot>$为有限整环，由于$<R，\cdot>$为有限含幺元交换半群，据定理 14-17 的证明，$<R，\cdot>$为阿贝尔群，因而$<R，+，\cdot>$为域。

定理 14-39 设$<F,+,\cdot>$为域，那么 F 中的非零元素在$<F，+>$中有相同的阶。

证明 当$<F，+>$中每个元素都是无限阶时，定理当然真。当$<F，+>$中有非零元素 a 具有有限阶 n，欲证$<F，+>$中任一元素 b 的阶亦必是 n。

设 b 的阶为 m。事实上$(nb)\cdot a=b\cdot(na)=0$，而 F 无零因子，且 $a\neq 0$。故 $nb=0$，因此 b 的阶 m 不超过 n（a 的阶）。

另一方面，由于$(ma)\cdot b=a\cdot(mb)=0$，而 F 无零因子，且 $b\neq 0$。可知 $ma=0$，因此 a 的阶 n 不超过 m（b 的阶）。

故 a 的阶等于 b 的阶。

定义 14-24 域$<F,+,\cdot>$中非零元素关于运算+的阶称为域 F 的**特征数**。

【例 14-20】 $<N_5,+_5,\times_5>$的特征数为 5，$<Q,+,\cdot>$特征数为∞。事实上，所有数域（实数域、复数域）都以∞为其特征数。

定理 14-40 域的特征数或为质数，或为∞。

证明 只要证域的特征数非∞时必定为质数。设域$<F,+,\cdot>$的特征数为 n，欲证 n 为质数。若 n 不是质数，那么有整数 $p,q,1<p,q<n$，使得 $n=pq$。设 a 为 F 中非零元素，那么

$$0=na=pqa=(pe)\cdot(qa)$$

其中 e 为$\cdot$运算的幺元。由于 F 无零因子，$pe\neq 0$，（e 的阶为 n），因此 $qa=0$，与 a 的阶为 n 矛盾。故 n 为质数。

下面要给出子域的概念。

定义 14-25 设$<F,+,\cdot>$为域。$<S,+,\cdot>$为 F 的子环，且$<S,+,\cdot>$为一域，那么称 S 为 F 的子域（subfields）。

【例 14-21】 设 R，C 分别表示实数集和复数集，那么域$<Q,+,\cdot>$是域$<R,+,\cdot>$，$<C,+,\cdot>$的子域。

根据本章练习第 19 题，不难看出下列子域的判定法则是正确的。

定理 14-41 设$<F, +, \cdot>$为域，$F' \subseteq F$，且F'至少有两个元素。那么$<F', +, \cdot>$为$<F, +, \cdot>$的子域当且仅当F'满足下列条件：

（1）对任意$a, b \in F'$，$a \neq b$，有$a - b \in F'$（从而$<F', +>$为$<F, +>$的子群）。

（2）对任意$a, b \in F', a \neq b$，有$ab^{-1} \in F'$（从而$<F'-\{0\}, \cdot>$为$<F-\{0\}, \cdot>$的子群）。

利用这一定理立即可得以下定理。

定理 14-42 设$<F1, +, \cdot>$，$<F2, +, \cdot>$都是域$<F, +, \cdot>$的子域，那么$<F1 \cap F2, +, \cdot>$也是域F的子域。

每个域都有子域，例如自身——平凡子域，许多域还有真子域——非自身的子域（例如例 14-25 中的$<R, +, \cdot>$，$<C, +, \cdot>$有真子域$<Q, +, \cdot>$。有趣的是，域作为环时都没有非平凡的理想子环，即除了$<\{0\}, +, \cdot>$和自身以外没有别的理想子环。

定理 14-43 含么非零交换环$<F, +, \cdot>$为域，当且仅当F没有非平凡的理想。

证明 设$<F, +, \cdot>$为域，$<D, +, \cdot>$为任一非零理想，欲证$D = F$。为此只要证$F \subseteq D$。设$a \in D$，$a \neq 0$，那么$a^{-1} \in F$。据理想定义$aa^{-1} = e \in D$。设x为F中任一元素，那么$xe \in D$，即$x \in D$。$F \subseteq D$得证，从而$D = F$。

反之，设F没有非平凡理想，欲证$<F, +, \cdot>$为域。为此只要证，F中每一非零元都有乘法逆元。设$a \in F$，$a \neq 0$。考虑

$$F' = \{ba + ma \mid b \in F,\ m \text{ 是整数}\}$$

可证$<F', +, \cdot>$为$<F, +, \cdot>$的理想且$F' \neq \{0\}$。据题设$F' = F$，于是$e \in F'$，即有$b \in F$，整数m使$ba + ma = e$，亦即$(b + me)a = e$。因此a有逆元$(b + me)$。$<F, +, \cdot>$为域得证。

既然域$<F, +, \cdot>$只有两种理想——零理想和自身F，那么域作为环时的商环也只有两个。容易知道，这两个商环中$<F/\{0\}, \oplus, \otimes>$与$<F, +, \cdot>$同构。而$<F/F, \oplus, \otimes>$与零环$<\{0\}, +, \cdot>$同构。于是，根据同态基本定理，域$F$的同态像或者同构于$F$本身，或者同构于零环。

利用同态，我们再来证明一个重要结果。

定理 14-44 设$<F, +, \cdot>$为域，那么当F的特征数为质数p时，F包含一个与$<N_p, +_p, \times_p>$同构的子域；当F的特征数为∞时，F包含一个与$<Q, +, \cdot>$同构的子域。

证明 当F的特征数为质数p时，定义函数$\lambda: I \to F$使得对任何$n \in I$（I为整数集），

$$\lambda(n) = n(\mathrm{mod}\ p)e \text{（}e \text{ 为 } F \text{ 中乘法幺元）}$$

易证λ为环$<I, +, \cdot>$到$<F, +, \cdot>$的同态映射，而同态核$K(\lambda) = \{\cdots, -2p, -p, 0, p, 2p, \cdots\}$，记为$K$（因$\lambda(ip) = ip(\mathrm{mod}\ p) = 0$）。另一方面，$\lambda$的同态像为

$$< \{0, e, 2e, \cdots, (p-1)e\}, +, \cdot > \text{（注意 } e \text{ 的阶为 } p\text{）}$$

据同态基本定理，商环$<I / K, \oplus, \otimes>$同构于有限域$< \{0, e, 2e, \cdots, (p-1)e\}, +, \cdot >$，从而$<N_p, +_p, \times_p>$同构于$F$的一个子域。

当F的特征数为∞时，建立函数λ：$Q \to F$，使得对任意$m/n \in Q$（m，n互质，$n \neq 0$），

$$\lambda(m/n) = (ne)^{-1}(me)$$

易证λ是良定的，且为单射。另外

$$\lambda((m/n)(s/t)) = \lambda((ms)/(nt)) = (nte)^{-1}(mse)$$

$$\lambda(m/n) \cdot \lambda(s/t) = (ne)^{-1}(me) \cdot (te)^{-1}(se) = (nte)^{-1}(mse)$$

故$\lambda((m/n)(s/t)) = \lambda(m/n) \cdot \lambda(s/t)$

$$\lambda((m/n) + (s/t)) = \lambda((mt + ns)/(nt)) = (nte)^{-1}((mt + ns)e)$$

$$\lambda(m/n) + \lambda(s/t) = (ne)^{-1}(me) + (te)^{-1}(se)$$

$$= (nte^2)^{-1}(mte^2) + (nte^2)^{-1}(nse^2)$$

$$= (nte)^{-1}((mt + ns)e)$$

故$\lambda((m/n) + (s/t)) = \lambda(m/n) + \lambda(s/t)$。

这就是说，λ 为$<Q, +, \cdot>$到$<F, +, \cdot>$的一个单一同态。同态像为

$$<\{(ne)^{-1}(me) \mid m, n \text{ 互质}, n \neq 0\}, +, \cdot>$$

由于$<Q, +, \cdot>$为域，从而λ同态像也为域，且为$<F, +, \cdot>$的子域。以上证明说明 F 确有一个子域与 Q 同构。

本定理表明，任何一个域都必然包含域$<Q, +, \cdot>$或$<N_p, +_p, \times_p>$（同构意义下）。因此，可以说$<Q, +, \cdot>$，$<N_p, +_p, \times_p>$（p 为质数）是一些最小的域。

有限域在密码理论中有重要的应用。

我们知道，在 p 为质数时$<N_p, +_p, \times_p>$为域，它们是极为重要的有限域，域的元素个数与元素的阶数相同，均为质数 p。那么，是否还有元素个数不是质数的有限域呢?有。

【例 14-22】 令 $F = \{0, e, a, a^2\}$，其中 $a^2 \neq a$, $a^3 = e$。因此$<F, \cdot>$构成一循环群，因而也是阿贝尔群。表 14-4 给出$<F, +>$中的运算 + 的定义。

表 14-4

+	0	e	a	a^2
0	0	e	a	a^2
e	e	0	a^2	a
a	a	a^2	0	e
a^2	a^2	a	e	0

容易验证$<F, +>$也是阿贝尔群。也可验证乘运算对加运算是可分配的。于是$<F, +, \cdot>$为四个元素的一个域。

阶数不是质数的有限群有何特征呢？

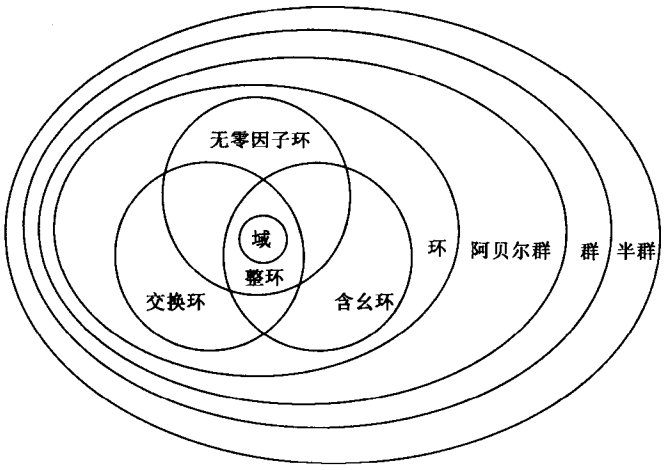
设有限域$<F, +, \cdot>$的特征数为质数 p，从而其每个元素都是 p 阶的。据拉格朗日定理，F 的阶数应当是 p 的倍数。事实上我们有

定理 14-45 有限域中元素个数等于其特征数的正整数方幂。

定理 14-46 对任一质数 p 及任一正整数 n，有阶（元素个数）为 p^n 的有限域 F。

它的逆也真，即对任一有限域 F，总有质数 p 和正整数 n，使得 $|F| = p^n$。我们略去它们定理的证明，读者可参阅文献 10。

作为本章的小结,我们用一个图直观地向读者展示本书已介绍过的重要的代数结构之间的关系，详见图 14-3。



（环就其+运算而言是群，域就其+,·运算而言都是群）

图 14-3

14.6 练习

1．证明：含幺半群的可逆元素集合构成一子半群，即＜inv（S），$*$＞为半群＜S，$*$＞的子半群。

2．设＜S，$*$＞为一半群，$z\in S$ 为左（右）零元。证明：对任一 $x\in S$，$x*z(z*x)$亦为左（右）零元。

3．设＜S，$*$＞为一半群，a，b，c 为 S 中给定元素证明：若 a，b，c 满足

$$a*c=c*a,\quad b*c=c*b$$

那么，$(a*b)*c=c*(a*b)$。

4．设＜$\{a,b\}$,$*$＞为一半群，且 $a*a=b$，证明：

（1）$a*b=b*a$

（2）$b*b=b$

5．代数结构＜$\{a,b,c,d\}$,$*$＞中运算$*$如表 14-5 规定。

表 14-5

*	a	b	c	d
a	a	b	c	d
b	b	c	d	a
c	c	d	a	b
d	d	a	b	c

（1）已知$*$运算满足结合律，证明＜$\{a,b,c,d\}$,$*$＞为一循环独异点。

（2）把$\{a,b,c,d\}$中各元素写成生成元的幂。

6．证明：循环半群必定是交换半群（参阅定义 14-3 之（1））。

7．证明：独异点元素可逆当且仅当它是幺元的因子（参阅定义 14-3 之（3））。

8．设<S，$*$>为一半群，且对任意 $x, y \in S$，若 $x \neq y$ 则 $x*y \neq y*x$。

（1）求证 S 中所有元素均为等幂元（a 称为等幂元，如果 $a*a=a$）。

（2）对任意元素 x，$y \in S$，

$$x*y*x=x,\quad y*x*y=y$$

*9．设<S，$*$>为一半群，且 S 中有元素 a，使得对于任意 $x \in S$，均有 S 中元素 u，v 满足

$$a*u=v*a=x$$

证明：<S，$*$>为一独异点。（提示：考虑 $x=a$ 时的 u 和 v。）

*10．问<I,+,0>是否为自由独异点？为什么？问<S,+,0>是否为自由独异点？为什么？其中 $S \subseteq N$（自然数集）归纳定义如下：

（1）0,4,6∈S。

（2）如果 $x, y \in S$ 则 $x+y \in S$。

（3）S 中元素仅此而已。

11．设<G，$*$>为群。若在 G 上定义运算○，使得对任何元素 x, $y \in G$，$x \circ y = y*x$。证明：<G，○>也是群。

12．设<S，$*$>是有限交换独异点，且 S 可约，即对任意 $a,b,c \in S, a*b = a*c$ 蕴涵 $b=c$。证明<S，$*$>为一阿贝尔群。

13．设<G，$*$>为一群。证明：

（1）若对任意 $a \in G$ 有 $a^2=e$，则 G 为阿贝尔群。

（2）若对任意 a，$b \in G$ 有 $(a*b)^2=a^2*b^2$，则 G 为阿贝尔群。

14．设 a 是群中的无限阶元素，证明：当 $m \neq n$ 时，$a^m \neq a^n$。

15．设<G，$*$>为群，$|G|$为偶数。证明 G 中必定有二阶的元素，且二阶元素的个数为奇数。

16．求证：有限群中阶大于 2 的元素个数必为偶数。

17．设 p 为质数。求证：在阿贝尔群中，若 a，b 的阶都是 p 的方幂，那么 $a*b$ 的阶也必是 p 的方幂。

18．设<G，$*$>为群，定义集合 $S=\{x \mid x \in G \wedge \forall y(y \in G \rightarrow x*y=y*x)\}$。证明：<$S$，$*$>为<$G$，$*$>的子群。

19．设<G，$*$>为群，H 为 G 的非空子集。证明：<H，$*$>为<G，$*$>的子群当且仅当对任意元素 a，$b \in H$ 有 $a*b^{-1} \in H$。

20．设<$H1$，$*$>，<$H2$，$*$>都是群<G，$*$>的子群，求证：

（1）<$H1 \cap H2$，$*$>为<G，$*$>的子群。

（2）<$H1 \cup H2$，$*$>为<G，$*$>的子群当且仅当 $H1 \subseteq H2$ 或 $H2 \subseteq H1$。

21．证明：对有限群<G，$*$>中任意元素 a，有 $a^{|G|}=e$。

22．求证：一个子群的左陪集元素的逆元组成这个子群的一个右陪集。

23．设 p 为质数，证明 p^n 阶的群中必有 p 阶的元素，从而必有 p 阶的子群（n 为正整数）。

*24．设<H，$*$>为群<G，$*$>的子群，求证：H 为正规子群当且仅当对任何元素 $g \in G$ 有

$$g^{-1}Hg \subseteq H$$

25. 设<G，>为一偶数阶的群。<H，*>是群<G，*>的子群，且 $|H| = |G|/2$。证明：<H，*>为正规子群。

26. 设<G，*>为群，$f: G \to G$ 为一同态映射。证明:对任一元素 $a \in G$，$f(a)$的阶不大于 a 的阶。

27. 证明定理 14-27 之（1），（2），（3）。

28. 一个质数阶的群必定是循环群，并且它的不同于幺元的每个元素均可作生成元。

29. 设 d 整除 n，证明：n 阶循环群必有 d 阶子群（拉格朗日定理之逆对循环群成立）。

30. 求证：任意群<G，*>可以表为若干阿贝尔群的并，即<G，*>有若干子群<S，*>，它们是交换群，且其载体诸 S 的并为 G。

31. 设<G，*>为循环群，<H，*>为其正规子群。证明：商群<G/H，⊙>亦为一循环群。

*32. 求置换群<S_3, ∘>中各元素的阶，并求出下列置换所生成的子群：

$$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$$

33. 设<R,+,0>为加群，R 上定义运算 • ，对任意 $a, b \in R$, $a \cdot b = 0$。证明：<R, +, • >为一环。

34. 设代数系统<I，⊕，⊗>中运算⊕，⊗定义如下：对任何整数 a，$b \in I$

$$a \oplus b = a + b - 1,\quad a \otimes b = a + b - a \cdot b$$

（这里+，·分别是数加和数乘）证明<I，⊕，⊗>是含么交换环。

35. 问<$\{5x \mid x \in I\}$，+，• >（+，• 分别为数加和数乘）是否为环？是否为整环？

36. 设环<R，+，• >中有元素 a，b，它们有乘法逆元 a^{-1}，b^{-1}，且 $ab = ba$。求证：

（1）$ab^{-1} = b^{-1}a$

（2）$a(-b) = (-b)a$

37. 若环<R，+，• >中每一元素 a 均满足 $a^2 = a$，那么 R 被称为布尔环。证明

（1）对布尔环中每一元素 a 有 $a+a=0$。

（2）布尔环是交换环。

（3）当 $|R|>2$ 时布尔环决不是整环。

*38. 请给出两个含零因子环。

39. 设环<R，+，• >中<R，+>为循环群，求证：R 是交换环。

*40. 设<D，+，• >是含么环<R，+，• >的理想，幺元 $e \in D$，求证 $D = R$。

41. 设 $F = \{a + b\sqrt{2} \mid a, b$ 为有理数$\}$，证明：<F, +, • >为域（这里+，• 为数加和数乘运算）。

42. 当 p 为质数时，问域<N_p, $+_p$, $\times_p$>的特征数为何？域<N_{p^2}, +, •>的特征数又为何？

43. 证明：在特征数为 p（p 为质数）的域里，对任何元素 a，b，有

（1）$(a+b)^p = a^p + b^p$

（2）$(a-b)^p = a^p - b^p$

（3）$(ne)^p = ne$（e 为域的乘法幺元，n 为正整数）

44. 证明：域与其每个子域具有相等的特征数。

45. 求证：高斯数域$<\{a+bi \mid a, b$ 为有理数$\}, +, \cdot>$是复数域的真子域。

46. 在例 14-24 给出的四元素域中解下列方程组：

$$\begin{cases} x+ay=0 \\ ax+y=e \end{cases}$$

第 15 章　格与布尔代数

本章要讨论另外两种代数结构——格与布尔代数，它们之间有密切的联系，但与代数结构群、环、域有重要的区别，其基本不同之处是：格与布尔代数的载体都是一个有序集（回忆第 10 章中的有序集概念）。这里，载体上序关系的建立及其与代数运算之间的联系是讨论的要点。格与布尔代数在代数学、逻辑理论研究，以及在电子技术的实际应用中都有重要的地位。

15.1　格

15.1.1　格——有序集

格是一种特殊的有序集，因此我们先从有序集的角度出发讨论格的概念。

在讲述关系的那一章里，已经对有序集的子集引入了上确界和下确界的概念，但我们知道，并非每个子集都有上确界或下确界，例如在图 15-1 中两个哈斯图所示的有序集里，$\{a, b\}$ 没有上确界，$\{c, d\}$没有下确界。不过，当某子集的上、下确界存在时，这个上、下确界是惟一确定的。

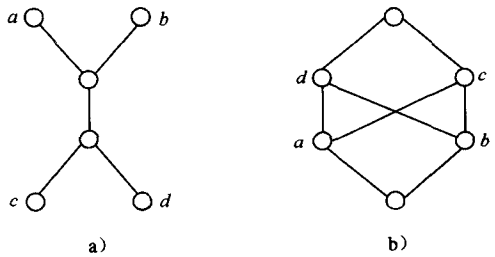


图　15-1

定义 15-1　称有序集$<L, \leqslant>$为**格**（lattice），如果 L 的任何两个元素的子集都有上确界和下确界。

通常用 $a \vee b$ 表示$\{a, b\}$的上确界，用 $a \wedge b$ 表示$\{a, b\}$的下确界，$\vee$和$\wedge$分别称为**保联**（join）和保交（meet）运算。由于对任何 a，b，$a \vee b$ 及 $a \wedge b$ 都是 L 中确定的成员，因此 $\vee$，$\wedge$均为 L 上的运算。

【例 15-1】

（1）对任意集合 A，有序集$<\rho(A), \subseteq>$为格，其中集合的并、交运算即为其保联、保交运算，即

$$B \vee C = B \cup C,\ B \wedge C = B \cap C$$

（2）设 I_+表示正整数集，| 表示 I_+上整除关系，那么$<I_+, |>$为格，其中保联、保交

运算即为求两正整数最小公倍数和最大公约数的运算，即

$$m\vee n=\mathrm{lcm}\,(m,\ n),\ m\wedge n=gcd\,(m,\ n)$$

（3）全序集（链）$<L,\ \leqslant>$都是格，其中保联、保交运算可如下规定：对任何 $a,\ b\in L$。

$$a\vee b=\begin{cases}a & b\leqslant a\\ b & a\leqslant b\end{cases},\ a\wedge b=\begin{cases}a & a\leqslant b\\ b & b\leqslant a\end{cases}$$

（4）设 P 为命题公式集合，当指定逻辑等价关系 $\dashv\vdash$ 为相等关系时，逻辑蕴涵关系 $\vdash$ 为 P 上的序关系，从而$<P,\vdash>$为格，对任何命题公式 A，B，$A\vee B=A\vee B$，$A\wedge B=A\wedge B$（等式右边的$\vee$，$\wedge$为“逻辑或”及“逻辑与”运算）。

（5）图 15-2 中的哈斯图 a～c 所表示的有序集是格，d、e，及图 15-1a、b 所表示的有序集不是格。

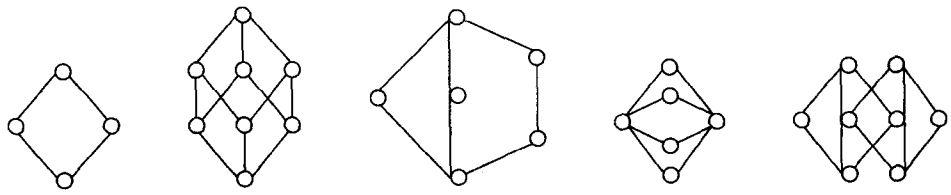


图 15-2

（6）设 R 为一环，$S(R)$表示 R 的理想的集合，那么$<S(R),\ \subseteq>$构成格。对任何理想 $D1$，$D2$，

$$D1\vee D2=D1+D2$$
$$D1\wedge D2=D1\cap D2$$

现设$\geqslant$表示序关系$\leqslant$的逆关系，那么据逆关系的性质可知：$a\geqslant b$ 意即 $b\leqslant a$。容易证明定理 15-1。

定理 15-1 当$<L,\ \leqslant>$为格时，$<L,\ \geqslant>$亦为格，且它的保联、保交运算$\vee^{\sim}$，$\wedge^{\sim}$对任意 $a,\ b\in L$ 满足

$$a\vee^{\sim}b=a\wedge b,\ a\wedge^{\sim}b=a\vee b$$

于是，我们有下列对偶原理。

定理 15-2 A 为格$<L,\ \leqslant>$上的真表达式，当且仅当 A^*为$<L,\ \geqslant>$上的真表达式，这里 A^*称为 A 的对偶式，即将 A 中符号$\vee$，$\wedge$，$\leqslant$分别改为$\wedge$，$\vee$，$\geqslant$后所得的公式。

对比命题演算、集合代数中所述对偶定理，不难理解上述定理的意义。

【例 15-2】 格$<\rho(S),\ \subseteq>$中的真表达式 $A\cap B\subseteq A$ 有对偶真表达式 $A\cup B\supseteq A$。格$<P,\ \vdash>$中真表达式 $p\wedge q\vdash q$ 有对偶真表达式 $q\vdash p\vee q$。

下文深入地讨论格的性质，注意，有时给出的两个真表达式是对偶的。

定理 15-3 设$<L,\ \leqslant>$为格，那么对 L 中任何元素 $a,\ b,\ c$，有

（1）$a\leqslant a\vee b$，$b\leqslant a\vee b$

$a\wedge b\leqslant a$，$a\wedge b\leqslant b$

（2）若 $a\leqslant b$，$a\leqslant c$，则 $a\leqslant b\vee c$

若 $b\leqslant a$，$c\leqslant a$，则 $b\wedge c\leqslant a$

（3）若 $a\leqslant b$，$c\leqslant d$，则 $a\vee c\leqslant b\vee d$，$a\wedge c\leqslant b\wedge d$

（4）若 $a\leqslant b$，则 $a\vee c\leqslant b\vee c$，$a\wedge c\leqslant b\wedge c$。

证明（1），（2）由运算$\wedge$，$\vee$的定义立即可得。

（3）设 $a\leqslant b$，$c\leqslant d$，我们只证 $a\vee c\leqslant b\vee d$，将 $a\wedge c\leqslant b\wedge d$ 的证明留给读者。

由（1）$b\leqslant b\vee d$，$d\leqslant b\vee d$，于是 $a\leqslant b\vee d$，$c\leqslant b\vee d$（由$\leqslant$的传递性）。于是由（2）得 $a\vee c\leqslant b\vee d$。

（4）这是（3）的特例。

定理 15-4 设$<L$，$\leqslant>$为格，那么对 L 中任意元素 a，b，c，有

（1）$a\vee a=a$，$a\wedge a=a$　　（幂等律）

（2）$a\vee b=b\vee a$，$a\wedge b=b\wedge a$　　（交换律）

（3）$a\vee(b\vee c)=(a\vee b)\vee c$

$a\wedge(b\wedge c)=(a\wedge b)\wedge c$　　（结合律）

（4）$a\wedge(a\vee b)=a$，$a\vee(a\wedge b)=a$　　（吸收律）

证明（1），（2）是显然的。

（3）证 $a\wedge(b\wedge c)=(a\wedge b)\wedge c$，另一式请读者自证。

因为

$$(a\wedge b)\wedge c\leqslant a\wedge b\leqslant a$$
$$(a\wedge b)\wedge c\leqslant a\wedge b\leqslant b$$
$$(a\wedge b)\wedge c\leqslant c$$

从而$(a\wedge b)\wedge c\leqslant b\wedge c$，进而$(a\wedge b)\wedge c\leqslant a\wedge(b\wedge c)$。同理可证

$$a\wedge(b\wedge c)\leqslant(a\wedge b)\wedge c$$

由$\leqslant$的反对称性，（3）式得证 。

（4）显然，$a\wedge(a\vee b)\leqslant a$；另一方面，由于

$$a\leqslant a，\ a\leqslant a\vee b$$

故而

$$a\leqslant a\wedge(a\vee b)$$

于是有

$$a\wedge(a\vee b)=a$$

$a\vee(a\wedge b)=a$ 的证明留给读者.

本定理给出了格的本质属性，我们将看到，格的其他性质都是它们的逻辑结果，包括有序关系$\leqslant$的性质。

格还有下列性质：

定理 15-5 设$<L$，$\leqslant>$为格，那么对 L 中任意元素 a，b，c，有

（1）$a\leqslant b$ 当且仅当 $a\wedge b=a$ 当且仅当 $a\vee b=b$。

（2）$a\vee(b\wedge c)\leqslant(a\vee b)\wedge(a\vee c)$。

（3）$a\leqslant c$ 当且仅当 $a\vee(b\wedge c)\leqslant(a\vee b)\wedge c$。

证明（1）首先设 $a\leqslant b$，那么 $a\leqslant a\wedge b$；另一方面 $a\wedge b\leqslant a$ 是已知成立的。因此有 $a\wedge b=a$。

再设 $a=a\wedge b$，那么 $a\vee b=(a\wedge b)\vee b$，即 $a\vee b=b$（由吸收律）。

最后，设 $b=a\vee b$，那么由 $a\leqslant a\vee b$ 立得 $a\leqslant b$。

至此，（1）中的三个命题的等价性得证。

（2）首先 $a\leqslant a\vee b$，$a\leqslant a\vee c$，故 $a\leqslant(a\vee b)\wedge(a\vee c)$。其次因为

$$b\wedge c\leqslant b\leqslant a\vee b,\ b\wedge c\leqslant c\leqslant a\vee c$$

从而有 $b\wedge c\leqslant(a\vee b)\wedge(a\vee c)$。由两者即得

$$a\vee(b\wedge c)\leqslant(a\vee b)\wedge(a\vee c)$$

（3）设 $a\leqslant c$，那么 $a\vee c=c$，代入（2）式即得

$$a\vee(b\wedge c)\leqslant(a\vee b)\wedge c$$

反之，设 $a\vee(b\wedge c)\leqslant(a\vee b)\wedge c$。由于

$$a\leqslant a\vee(b\wedge c),\ (a\vee b)\wedge c\leqslant c$$

因此有 $a\leqslant c$。

15.1.2 格代数

这一小节将从代数结构的角度出发来讨论格，也就是说，按第 13 章的方式，把格定义为载体和满足特定公理的运算组成的代数结构，并用读者熟悉的抽象代数研究工具讨论之。

定义 15-2 设 L 为一非空集合，$\vee$，$\wedge$ 为 L 上的两个二元运算，称$<L,\ \vee,\ \wedge>$为**格代数**，或简单地称为**格**，如果$<L,\ \vee,\ \wedge>$中运算$\vee$，$\wedge$满足幂等律、交换律、结合律和吸收律（见定理 15-4）。

现在要证明，这里定义的格正是定义 15-1 中所说的格，为此，需要在$<L,\ \vee,\ \wedge>$上定义序关系$\leqslant$，使得对任意 a，$b\in L$，$a\vee b$ 为$\{a,\ b\}$的上确界，$a\wedge b$ 为$\{a,\ b\}$的下确界（依据序$\leqslant$）。从而使定理 15-3 成立。

定义 L 上$\leqslant$关系如下；对任意 a，$b\in L$，

$$a\leqslant b \text{ 当且仅当 } a\wedge b=a$$

（1）可证$\leqslant$为 L 上序关系。

1）因为 $a\wedge a=a$，故 $a\leqslant a$。自反性得证。

2）设 $a\leqslant b$，$b\leqslant c$，那么 $a\wedge b=a$，$b\wedge c=b$，于是

$$a\wedge c=(a\wedge b)\wedge c=a\wedge(b\wedge c)=a\wedge b=a$$

故 $a\leqslant c$。传递性得证。

3）设 $a\leqslant b$，$b\leqslant a$，那么 $a\wedge b=a$，$b\wedge a=b$。由于 $a\wedge b=b\wedge a$。故 $a=b$。反对称性得证。

（2）可证 $a\leqslant b$ 当且仅当 $a\vee b=b$。

设 $a\leqslant b$，那么 $a\wedge b=a$，从而$(a\wedge b)\vee b=a\vee b$，由吸收律即得 $b=a\vee b$。

反之，设 $a\vee b=b$，那么 $a\wedge(a\vee b)=a\wedge b$，由吸收律可知 $a=a\wedge b$，即 $a\leqslant b$。

（3）可证 $a\vee b$ 为$\{a,\ b\}$的上确界。

由吸收律 $a\wedge(a\vee b)=a$，$b\wedge(a\vee b)=\mathrm{b}$，可知 $a\leqslant a\vee b$，$b\leqslant a\vee b$，因而 $a\vee b$ 为$\{a,b\}$的上界。

设 c 为$\{a,\ b\}$任一上界，即 $a\leqslant c$，$b\leqslant c$，那么，$a\vee c=\mathrm{c}$，$b\vee c=c$，于是

$$a\vee c\vee b\vee c=c\vee c$$

亦即 $a\vee b\vee c=c$，故 $a\vee b\leqslant c$。这表明 $a\vee b$ 为$\{a, b\}$的上确界。

（4）仿上可证 $a\wedge b$ 为$\{a, b\}$的下确界。细节留给读者补出。

格作为代数结构，自然可以讨论它的特殊常元的存在性，讨论它的子格以及其上同态、同构映射等。

定义 15-3 格$<L, \vee, \wedge>$称为**完全格**（complete lattice），如果 L 的所有非空子集都有上确界和下确界。

设 $S\subseteq L$，那么 S 的上确界记为 $\vee S$ 或 $\underset{a\in S}{\vee} a$，$S$ 的下确界记为 $\wedge S$ 或 $\underset{a\in S}{\wedge} a$。$L$ 的上确界记为 1，L 的下确界记为 0。

定理 15-6 设$<L, \vee, \wedge>$为完全格，那么 0 为$\vee$运算么元、$\wedge$运算零元；1 为$\wedge$运算么元、$\vee$运算零元.

证明 由定义知：对 L 中任意元素 a 有 $0\leqslant a\leqslant 1$，从而

$$0\vee a=a\vee 0=a,\quad 0\wedge a=a\wedge 0=0$$

$$1\vee a=a\vee 1=1,\quad 1\wedge a=a\wedge 1=a$$

有限格总是完全格，这是极易想到的。无限格中是否有完全格呢？例 15-1 中（1）（其中 A 为无限集时），（4），（5）是完全格，但（2）不是完全格。下面的定理可用于完全格的判定和证伪。

定理 15-7 有序集$<L, \leqslant>$为完全格的充分必要条件是：存在 L 的上确界 1，并且 L 的每一非空子集有下确界。

证明 必要性是显然的。

为证充分性，只要证 L 的任一非空子集都有上确界。

设 $S\subseteq L$，$S\neq\varnothing$。考虑 S 的上界集合 B。由于 $1\in B$ 是显然的，因此 $B\neq\varnothing$。据题设，B 有下确界，记为 b，现证 b 为 S 的上确界。

b 当然是 S 的上界，因为 $b\in B$。另设 a 是 S 的任一上界，那么 $a\in B$，因而 $b\leqslant a$。这就是说，b 是 S 的上确界。

我们不打算重复叙述子格、格同态、格同构的定义，这有点儿例行公事的意味。简单地说，格的子代数即为子格，两个格之间有同态、同构映射，则称这两个格同态、同构。下面是有关这几个概念的例子和事实。

【例 15-3】

（1）令 $S_n=\{x\mid x$ 为 n 的因子$\}$，那么对任何正整数 n，$<S_n$，lcm，gcd$>$为格，且为$<I_+$，lcm，gcd$>$的子格（lcm，gcd 分别为求最小公倍数和最大公约数运算）。

（2）设$<L, \vee, \wedge>$为格，那么对任一 $a\in L$，$<\{a\}, \vee, \wedge>$为格 L 的子格。

（3）格$<L, \vee, \wedge>$的子格显然为格，但由 $S\subseteq L$，$<S, \vee, \wedge>$为格，并不可断定$<S, \vee, \wedge>$为格 L 的子格。图 15-3 中哈斯图表示一个格 L。设 $L1=\{O, a, b, c\}$，那么$<L1, \vee, \wedge>$为 L 的子格。设 $L2=\{O, a, b, d\}$，那么$<L2, \vee, \wedge>$为格，但它不是 L 的子格。（为什么？）

（4）设格 $L1=<\{1, 2, 3\}, \leqslant>$，$L2=<\rho(\{1, 2, 3\}), \subseteq>$，它们的哈斯图在图 15-4 中给出。

定义函数 f: $\{1, 2, 3\}\to\rho(\{1, 2, 3\})$

$$f(x)=\{y\mid y\leqslant x\}$$ （图中虚线标出）

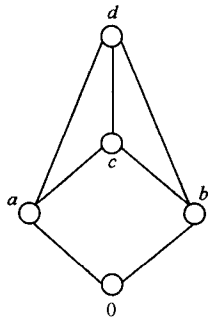


图 15-3

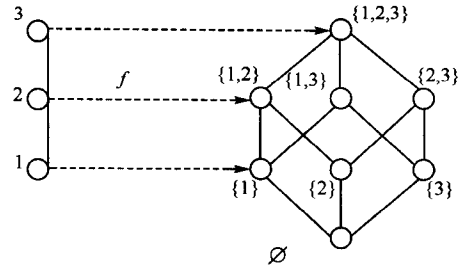


图 15-4

那么由于

$$f(x\vee y)=f(\max(x,y))$$
$$=\{z\mid z\leqslant\max(x,y)\}$$
$$=\{z\mid z\leqslant x\}\cup\{z\mid z\leqslant y\}$$
$$=f(x)\cup f(y)$$
$$f(x\wedge y)=f(\min(x,y))$$
$$=\{z\mid z\leqslant\min(x,y)\}$$
$$=\{z\mid z\leqslant x\}\cap\{z\mid z\leqslant y\}$$
$$=f(x)\cap f(y)$$

因此，f为 $L1$ 到 $L2$ 的同态。

（5）具有 1 个，2 个，3 个元素的格，分别同构于元素个数相同的链。4 个元素的格必同构于图 15-5 中给出的 2 个格之一；5 个元素的格必同构于图 15-6 中的 5 个格之一。

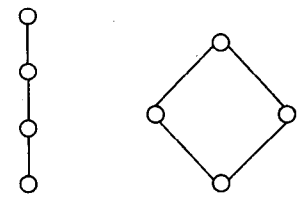


图 15-5

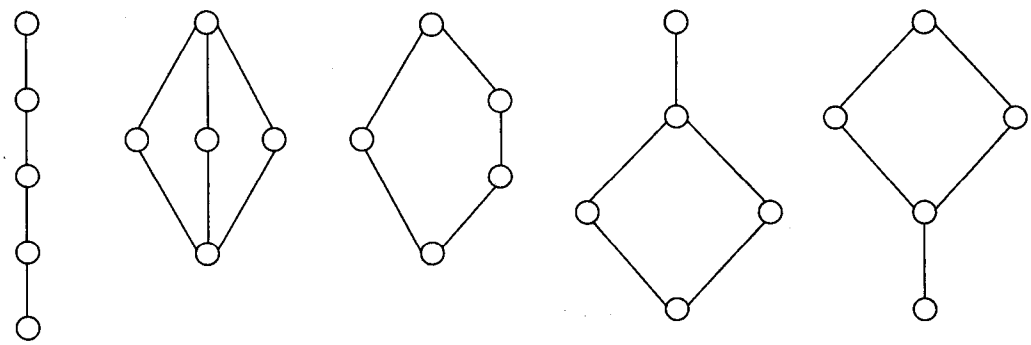


图 15-6

定理 15-8 设$<L,\vee,\wedge>$为格，$a\in L$，令

$$L_a=\{x\mid x\in L\text{ 且 }x\leqslant a\},\quad M_a=\{x\mid x\in L\text{ 且 }a\leqslant x\}$$

那么$<L_a,\vee,\wedge>$，$<M_a,\vee,\wedge>$都是 L 的子格。

证明 为证$<L_a,\vee,\wedge>$为子格，只要证 L_a对运算$\vee$，$\wedge$封闭。设 x，y 为 L_a中任意

元素，那么，$x\leqslant a$，$y\leqslant a$，从而 $x\vee y\leqslant a$，$x\wedge y\leqslant a$，即 $x\vee y\in L_a$，$x\wedge y\in L_a$。

仿此可证$<M_a, \vee, \wedge>$为 L 的子格。

定理 15-9 设$<L, \vee, \wedge>$，$<L', \vee', \wedge'>$为两个格，f 为 L 到 L'的同态，那么对任意 a，$b\in L$，$a\leqslant b$ 蕴涵 $f(a)\leqslant' f(b)$。即同态是保序的。

证明 因为 $f(a)\vee' f(b)=f(a\vee b)=f(a)$（$a\leqslant b$），故 $f(a)\leqslant' f(b)$。

注意，本定理的逆不成立。

【例 15-4】 已知 $L_1=<\{1, 2, 3, 4, 6, 12\}, |>$（|为整除关系）和 $L_2=<\{1, 2, 3, 4, 6, 12\}, \leqslant>$（$\leqslant$为整数大小关系）都是格，函数 $f(x)=x$ 显然是保序的，但 f 不是 L_1 到 L_2 的同态. 因为 $f(2\vee_1 3)=f(6)=6$，但 $f(2)\vee_2 f(3)=2\vee_2 3=3$，因此 $f(2\vee_1 3)\neq f(2)\vee_2 f(3)$。（$\vee_1$ 为 L_1 上保联运算，$\vee_2$ 为 L_2 上保联运算。）

对于同构映射我们却有以下定理：

定理 15-10 设$<S, \leqslant>$，$<S', \leqslant'>$均为格，f 为 S 到 S'的双射，那么 f 为 S 到 S'的同构映射，当且仅当对任意 a，$b\in S$，

$$a\leqslant b\Leftrightarrow f(a)\leqslant' f(b) \tag{15-1}$$

证明 设 f 为 S 到 S'的同构映射，那么

（1）当 $a\leqslant b$ 时，由定理 15-9 已知 $f(a)\leqslant' f(b)$。

（2）当 $f(a)\leqslant' f(b)$时，$f(a)\wedge' f(b)=f(a)$，亦即 $f(a\wedge b)=f(a)$。由于 f 为双射，$a\wedge b=a$。因此 $a\leqslant b$。

$a\leqslant b\Leftrightarrow f(a)\leqslant' f(b)$得证。

反之，设对任意 a，$b\in S$，式（15-1）成立。现令 $a\wedge b=c$，$f(a)\wedge' f(b)=f(d)$。由于 $c\leqslant a$，$c\leqslant b$，$f(a\wedge b)=f(c)$，而且 $f(c)\leqslant' f(a)$，$f(c)\leqslant' f(b)$，可知

$$f(c)\leqslant' f(a)\wedge' f(b)=f(d)$$

另一方面，由于 $f(d)=f(a)\wedge' f(b)\leqslant' f(a)$，$f(d)=f(a)\wedge' f(b)\leqslant' f(b)$，因而有 $d\leqslant a$，$d\leqslant b$，$d\leqslant a\wedge b$，进而又有 $f(d)\leqslant' f(a\wedge b)=f(c)$。

由于 $f(c)\leqslant' f(d)$且 $f(d)\leqslant' f(c)$，故 $f(c)=f(d)$，即 $f(a\wedge b)=f(a)\wedge' f(b)$。

仿上可证 $f(a\vee b)=f(a)\vee' f(b)$。

f 为 S 到 S'的同构得证。

15.1.3 分配格和模格

对于具有两个运算的代数结构，人们自然要关心这两个运算之间是否成立分配律。

定义 15-4 称格$<L, \vee, \wedge>$为**分配格**（distributive lattice）。如果它满足分配津，即对任意 $a, b, c\in L$，

$$a\wedge(b\vee c)=(a\wedge b)\vee(a\wedge c) \tag{15-2}$$

$$a\vee(b\wedge c)=(a\vee b)\wedge(a\vee c) \tag{15-3}$$

【例 15-5】

（1）例 15-1 中（1），（2），（3），（4）及（5）都是分配格。

（2）图 15-7 中两个格都不是分配格。因为在（a）中，

$$b\wedge(c\vee d)=b\wedge a=b$$

$$(b\wedge c)\vee(b\wedge d)=e\vee e=e$$

但 $b \neq e$。

在（b）中，

$$c \wedge (b \vee d) = c \wedge a = c$$
$$(c \wedge b) \vee (c \wedge d) = e \vee d = d$$

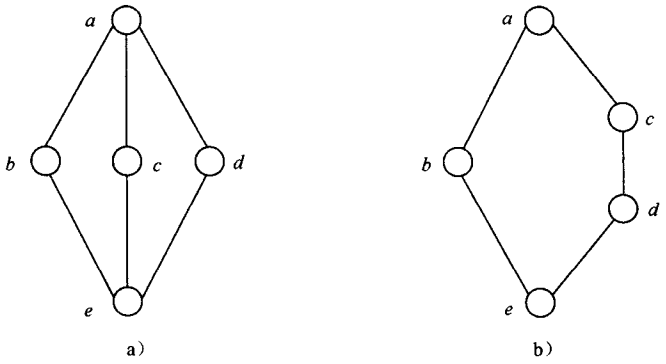


图 15-7

但 $c \neq d$。

事实上，式（15-2）、式（15-3）中可去掉一式，因为在格中，式（15-2）等价于式（15-3）。我们来证明这个事实。

设 a，b，c 为格$<L, \vee, \wedge>$中任意元素，那么

$$\begin{aligned} a \vee (b \wedge c) &= (a \vee (a \wedge c)) \vee (b \wedge c) \\ &= a \vee ((a \wedge c) \vee (b \wedge c)) \\ &= a \vee ((a \vee b) \wedge c) \qquad \text{（由式（15-2））} \\ &= (a \vee b) \wedge a) \vee ((a \vee b) \wedge c) \\ &= (a \vee b) \wedge (a \vee c) \qquad \text{（由式（15-2））} \end{aligned}$$

这正是式（15-3）。因此，式（15-2）蕴涵式（15-3）。反之，

$$\begin{aligned} a \wedge (b \vee c) &= (a \wedge (a \vee c)) \wedge (b \vee c) \\ &= a \wedge ((a \vee c) \wedge (b \vee c)) \\ &= a \wedge ((a \wedge b) \vee c) \qquad \text{（由式（15-3））} \\ &= ((a \wedge b) \vee a) \wedge ((a \wedge b) \vee c) \\ &= (a \wedge b) \vee (a \wedge c) \qquad \text{（由式（15-3））} \end{aligned}$$

这正是式（15-2），因此式（15-3）蕴涵式（15-2）。

（注意，上述事实不能引用对偶原理来证，因为式（15-2）和式（15-3）都不是关于格的真命题。）

有的格虽不能满足分配律。但它们可以有条件地满足分配律，这就是模格。

定义 15-5 称格$<L, \vee, \wedge>$为**模格**（moduler lattice），如果对任意元素 a，b，$c \in L$，它满足：

$$a \leqslant c \text{ 蕴涵 } a \vee (b \wedge c) = (a \vee b) \wedge c$$

或

$a \leqslant c$ 蕴涵 $a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c)$

【例 15-6】

（1）例 15-5 中（2）的两个格都不是分配格，其中的（a）是模格，而（b）连模格也不是，因为尽管 $d \leqslant c$，但是

$$d \vee (b \wedge c) = d \vee a = a$$
$$(d \vee b) \wedge c = a \wedge c = c$$

$a \neq c$。

（2）例 15-1 中（6）为模格。设 $D1$，$D2$，$D3$ 为环 R 的理想，$D1 \subseteq D3$，那么可证

$$D1 + (D2 \cap D3) = (D1 + D2) \cap D3$$

设 $x \in D1 + (D2 \cap D3)$，那么 $x = d1 + d$，其中 $d1 \in D1$，$d \in D2$，$d \in D3$。于是

$d1 + d \in D1 + D2$，$d1 + d \in D3$（因 $D1 \subseteq D3$，$D3$ 为理想）

故 $x \in (D1 + D2) \cap D3$。$D1 + (D2 \cap D3) \subseteq (D1 + D2) \cap D3$ 得证。

$(D1 + D2) \cap D3 \subseteq D1 + (D2 \cap D3)$的证明请读者完成。

以上讨论表明，格可以分为分配格与非分配格两类，而非分配格中又有模格及非模格之分。

作为本节的结束，我们来讨论分配格与模格的两个性质。

定理 15-11 设$<L, \vee, \wedge>$为分配格，那么对 L 中任意元素 a，b，c，有

$a \wedge b = a \wedge c$ 并且 $a \vee b = a \vee c$ 当且仅当 $b = c$

证明 充分性是显然的。

现证必要性。由于

$$(a \wedge b) \vee c = (a \wedge c) \vee c = c \qquad （因 a \wedge b = a \wedge c）$$
$$(a \wedge b) \vee c = (a \vee c) \wedge (b \vee c)$$
$$= (a \vee b) \wedge (b \vee c) \qquad （因 a \vee c = a \vee b）$$
$$= b \vee (a \wedge c)$$
$$= b \vee (a \wedge b) \qquad （因 a \wedge b = a \wedge c）$$
$$= b$$

故 $b = c$。

定理 15-12 格$<L, \vee, \wedge>$为模格的充分必要条件是：对 L 中任意元素 a，b，c，若 $b \leqslant c$，$a \vee b = a \vee c$，$a \wedge b = a \wedge c$，则 $b = c$。

证明 先证必要性。

设$<L, \vee, \wedge>$为模格，且 $b \leqslant c$，$a \vee b = a \vee c$，$a \wedge b = a \wedge c$，那么，

$$b = b \vee (a \wedge b)$$
$$= b \vee (a \wedge c)$$
$$= (b \vee a) \wedge (b \vee c)$$
$$= (c \vee a) \wedge (b \vee c)$$
$$= c \vee (a \wedge b)$$
$$= c \vee (a \wedge c)$$
$$= c$$

再证充分性。

为证$<L, \vee, \wedge>$为模格，设$b \leqslant c$，需证$c \wedge (b \vee a) = b \vee (c \wedge a)$。

首先，据定理 15-5 之（3），由$b \leqslant c$可知

$$b \vee (c \wedge a) \leqslant c \wedge (b \vee a) \tag{15-4}$$

由此

$$\begin{aligned} c \wedge a &= (c \wedge a) \wedge a \\ &\leqslant (b \vee (c \wedge a)) \wedge a \\ &\leqslant (c \wedge (b \vee a)) \wedge a \qquad \text{（由式（15-4））} \\ &= c \wedge a \end{aligned}$$

于是

$$(b \vee (c \wedge a)) \wedge a = (c \wedge (b \vee a)) \wedge a = c \wedge a \tag{15-5}$$

同样可以证明（请读者完成）

$$(b \vee (c \wedge a)) \vee a = (c \wedge (b \vee a)) \vee a = b \vee a \tag{15-6}$$

因此，由题设及式（15-4）～（15-6）即得

$$c \wedge (b \vee a) = b \vee (c \wedge a)$$

$<L, \vee, \wedge>$为模格得证。

15.2 布尔代数

这一节讨论一种特殊的格——布尔代数。从有界格和有补格谈起。

15.2.1 有界格和有补格

定义 15-8 格$<L, \vee, \wedge>$称为**有界格**（bounded lattice），如果 L 中既有上确界 1，又有下确界 0。0，1 称为 L 的界（bound）。

【例 15-7】

（1）完全格都是有界格。

（2）有限格都是有界格。

（3）例 15-1 中（1），（4），（5）及（6）所规定的格都是有界格。

（4）有界格未必是完全格。令 Q [0，1] 为 [0，1] 区间中全体有理数的集合，定义 Q [0，1] $\times Q$ [0，1] 上的序关系$\leqslant^2$

$$<x, y> \leqslant^2 <u, v> \text{当且仅当 } x \leqslant u \text{ 且 } y \leqslant v。$$

显然$<Q$ [0，1] $\times Q$ [0，1]，$\leqslant^2>$为格，$\vee$与$\wedge$分别定义为：

$$<x, y> \vee <u, v> = <\max(x, u), \max(y, v)>$$

$$<x, y> \wedge <u, v> = <\min(x, u), \min(y, v)>$$

这是一个有界格，界为$<0, 0>$与$<1, 1>$，但它不是完全格，因为它有子集

$$\{<0, x> \mid x \in \{0.4, 0.41, 0.414, \cdots\}\}$$

（其中 0.4，0.41，0.414，…为$\sqrt{2}-1$的近似逼近序列），该子集在 Q [0，1] 中没有上确界。

定义 15-7 设$<L, \vee, \wedge>$为有界格，a 为 L 中一元素，称 b 为 a 的**补元**或**补**（complements），如果

$$a \vee b = 1, \quad a \wedge b = 0$$

应当注意补元的下列特点。

（1）补元是相互的，即 b 是 a 的补元，那么 a 也是 b 的补元。

（2）0 和 1 互为补元。

（3）并非有界格中每个元素都有补元，而一个元素的补元也未必惟一。图 15-8a 中除 0，1 之外没有元素有补元；图 15-8b 中元素 a，b，c 两两互为补元；图 15-8c 中 c 有补元 a，b，而 a，b 的补元同为 c。

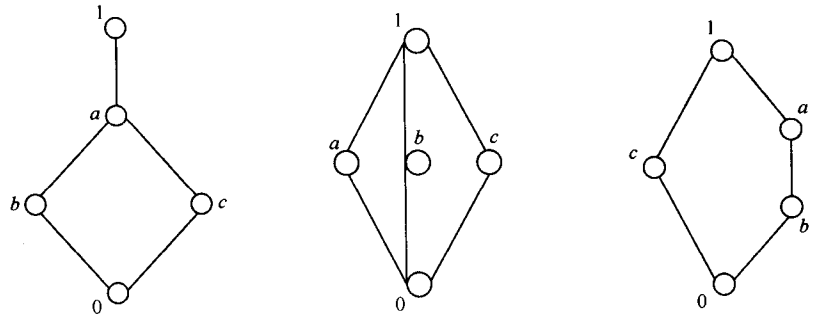


图 15-8

定义 15-8 有界格$<L, \vee, \wedge>$称为有**补格**（complemented lettice），如果 L 中每个元素都有补元。

【例 15-8】

（1）图 15-8a 不是有补格，b 和 c 是有补格。

（2）多于两个元素的链都不是有补格。

关于有补格有下列事实：

定理 15-13 有补格$<L, \vee, \wedge>$中元素 0，1 的补元是惟一的。

证明 已知 0，1 互为补元。设 a 也是 1 的补元，那么 $a \wedge 1 = 0$，即 $a = 0$。因此 1 的补元仅为 0。同样可证 0 的补元仅为 1。

定理 15-14 有补分配格中每一元素的补元都是惟一的。因此，有补分配格中一元素 a 的补可用 a'来表示。

证明 设$<L, \vee, \wedge>$为有补分配格，a 为 L 中任一元素，b，c 都是 a 的补元，那么

$$a \wedge b = 0 = a \wedge c,\quad a \vee b = 1 = a \vee c$$

据定理 15-11，$b = c$，因此 a 只有惟一补元 a'。

作为定理 15-14 的推论，显然有以下定理：

定理 15-15 对有补分配格中每一元素 a，有

$$(a')' = a$$

定理 15-16 设$<L, \vee, \wedge>$为有补分配格，那么对 L 中任意元素 a，b，有

（1）$(a \vee b)' = a' \wedge b'$

（2）$(a \wedge b)' = a' \vee b'$

证明 由于

$$(a\vee b)\wedge(a'\wedge b')=(a'\wedge b)\wedge b'=0$$
$$(a\vee b)\vee(a'\wedge b')=(a\vee b\vee a')\wedge(a\vee b\vee b')=1$$

因此 $a'\wedge b'$为 $a\vee b$ 的补元。由补元的惟一性得知：

$$(a\vee b)'=a'\wedge b'$$

同样可证（2），请读者完成之。

定理 15-17 对有补分配格的任何元素 a，b，有

$$a\leqslant b \text{ 当且仅当 } a\wedge b'=0 \text{ 当且仅当 } a'\vee b=1$$

定理的证明留作练习。

15.2.2 布尔代数的意义

人们把有补分配格称为**布尔代数**（Boolean algebra）。其实我们也可以用少数的几个特征性来定义布尔代数。

定义 15-9 代数系统$<B$，$\vee$，$\wedge>$（$\vee$，$\wedge$为 B 上二元运算）称为**布尔代数**，如果 B 满足下列条件：

（1）运算$\vee$，$\wedge$满足交换律。

（2）$\vee$运算对$\wedge$运算满足分配律，$\wedge$运算对$\vee$运算也满足分配律。

（3）B 有$\vee$运算幺元 1 和$\wedge$运算零元 0，$\wedge$运算幺元和$\vee$运算零元 1。

（4）对 B 中每一元素 a，均存在元素 a'，使

$$a\vee a'=1,\quad a\wedge a'=0$$

为证定义 15-9 定义的布尔代数的确是有补分配格，只要证定义 15-9 中的代数系统$<B$，$\vee$，$\wedge>$为格，进而由（2），（3），（4）可断定 B 为有补分配格。

为证 B 为格。据定义 15-2，只要证 B 满足幂等律、结合律和吸收律。

B 满足幂等律。因为对任意 $a\in B$，

$$a=a\wedge 1=a\wedge(a\vee a')=(a\wedge a)\vee(a\wedge a')=a\wedge a$$

B 满足吸收律。因为对 B 中任何元素 a，b，

$$\begin{aligned}a\vee(a\wedge b)&=(a\wedge 1)\vee(a\wedge b)\\&=a\wedge(1\vee b)\\&=a\end{aligned}$$

$$\begin{aligned}a\wedge(a\vee b)&=(a\vee 0)\wedge(a\vee b)\\&=a\vee(0\wedge b)\\&=a\end{aligned}$$

B 满足结合律。因为对 B 中任意元素 a，b，c，可如下证明 $a\vee(b\vee c)=(a\vee b)\vee c$，从而对偶地可证 $a\wedge(b\wedge c)=(a\wedge b)\wedge c$。令

$$N=a\vee(b\vee c),\quad M=(a\vee b)\vee c,$$

那么

$$a\wedge N=a\wedge(a\vee(b\vee c))=a$$

$$\begin{aligned}a\wedge M&=a\wedge((a\vee b)\vee c)\\&=(a\wedge(a\vee b))\vee(a\wedge c)\\&=a\vee(a\wedge c)=a\end{aligned}$$

故

$$a \wedge N = a \wedge M \tag{15-7}$$

$$\begin{aligned} a' \wedge N &= a' \wedge (a \vee (b \vee c)) = a' \wedge (b \vee c) \\ &= (a' \wedge b) \vee (a' \wedge c) \\ a' \wedge M &= a' \wedge ((a \vee b) \vee c) \\ &= (a' \wedge (a \vee b)) \vee (a' \wedge c) \\ &= (a' \wedge b) \vee (a' \wedge c) \end{aligned}$$

故

$$a' \wedge N = a' \wedge M \tag{15-8}$$

由式（15-7）和（15-8）得

$$(a \wedge N) \vee (a' \wedge N) = (a \wedge M) \vee (a' \wedge M)$$

即

$$\begin{aligned} (a \vee a') \wedge N &= (a \vee a') \wedge M \\ N &= M \end{aligned}$$

$a \vee (b \vee c) = (a \vee b) \vee c$ 得证。

布尔代数通常用序组$<B, \vee, \wedge, ', 0, 1>$来表示。其中'为一元求补运算。这并不意味着布尔代数至少有两个不同元素，当 B 只有一个元素 0 时，可以认为$<\{0\}, \vee, \wedge, ', 0>$仍为布尔代数，这时它被称为退化了的布尔代数。

【例 15-9】

（1）在$<B, \vee, \wedge, ', 0, 1>$中取 $B=\{0, 1\}$，得$<\{0, 1\}, \vee, \wedge, ', 0, 1>$为一布尔代数。

（2）对任意集合 A，$<\rho(A), \cup, \cap, \bar{}, \varnothing, A>$（其中 $\bar{}$ 为一元求补集的运算）。

（3）$<P, \vee, \wedge, \neg, f, t>$为布尔代数。这里 P 为命题公式集，$\vee$，$\wedge$，$\neg$ 为析取、合取、否定等真值运算，f，t 分别为永假命题、永真命题。

（4）设 B_n 为由真值 0，1 构成的 n 元序组组成的集合，即

$$B_n = \{<a_1, a_2, \cdots, a_n> \mid a_i=0 \text{ 或 } a_i = 1, i=1, 2, \cdots, n\}$$

在 B_n 上定义运算（以下用 a 表示$<a_1, a_2, \cdots, a_n>$，0 表示$<0, 0, \cdots, 0>$，1 表示$<1, 1, \cdots, 1>$）

$a \vee b = <a_1 \vee b_1, a_2 \vee b_2, \cdots, a_n \vee b_n>$

$a \wedge b = <a_1 \wedge b_1, a_2 \wedge b_2, \cdots, a_n \wedge b_n>$

$\neg a = <\neg a_1, \neg a_2, \cdots, \neg a_n>$

那么，$<B_n, \vee, \wedge, \neg, 0, 1>$为一布尔代数，常称为**开关代数**。

同样可以讨论子布尔代数概念以及布尔代数间的同态——布尔同态的概念。

定义 15-10 称$<A, \vee, \wedge, ', 0, 1>$为布尔代数$<B, \vee, \wedge, ', 0, 1>$的**子代数**，如果 $A \subseteq B$，且$<A, \vee, \wedge, ', 0, 1>$为布尔代数。

事实上我们有以下定理。

定理 15-18 设$<B, \vee, \wedge, ', 0, 1>$为布尔代数，$A \subseteq B$ 且 A 含有元素 0，1，对运算$\vee$，$\wedge$，'封闭，那么$<A, \vee, \wedge, ', 0, 1>$为 B 的子代数。

证明是十分简单的，不赘述。

【例 15-10】

（1）对任何布尔代数$<B, \vee, \wedge, ', 0, 1>$ 恒有子布尔代数$<B, \vee, \wedge, ', 0, 1>$和$<\{0, 1\}, \vee, \wedge, ', 0, 1>$，它们被称为 B 的平凡子布尔代数。

（2）图 15-9 给出一个布尔代数，它有子代数$<\{0, 1, a, a'\}, \vee, \wedge, ', 0, 1>$和$<\{0, 1, a, a', b, b'\}, \vee, \wedge, ', 0, 1>$等。

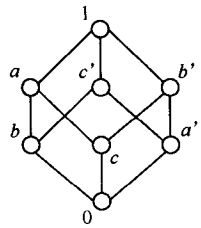


图 15-9

定义 15-11 设 $h: A \to B$ 为布尔代数$<A, \vee, \wedge, ', 0, 1>$到布尔代数$<B, \vee, \wedge, ', 0, 1>$的同态映射，即对任何元素 a，b，

$$h(a \vee b) = h(a) \vee h(b) \tag{15-9}$$

$$h(a \wedge b) = h(a) \wedge h(b) \tag{15-10}$$

$$h(a') = (h(a))' \tag{15-11}$$

那么称 h 为 A 到 B 的**布尔同态**。

定理 15-19 设 h 为布尔代数$<A, \vee, \wedge, ', 0, 1>$到布尔代数$<B, \vee, \wedge, ', 0, 1>$的布尔同态，那么

$$h(0) = 0, \quad h(1) = 1$$

证明 $h(0) = h(0 \wedge 0') = h(0) \wedge h(0') = h(0) \wedge (h(0))' = 0$

$h(1) = h(1 \vee 1') = h(1) \vee h(1') = h(1) \vee (h(1))' = 1$

如果定义仅满足式（15-9）和（15-10）两式的映射 h 为布尔同态，那么上述定理不真，但此种 h 是$<A, \vee, \wedge, ', 0, 1>$到$<h(A), \vee, \wedge, ', h(0), h(1)>$的布尔同态，因为易见 $h(0)$为 $h(A)$上$\vee$运算么元，$h(1)$为 $h(A)$上$\wedge$运算么元，且

$$h(a) \wedge h(a') = h(0)$$

$$h(a) \vee h(a') = h(1)$$

从而 $h(a') = (h(a))'$。

以上讨论表明，当 h 为满射时，式（15-11）可省，并且有定理 15-20。

定理 15-20 设 h 为布尔代数$<A, \vee, \wedge, ', 0, 1>$到格$<B, \vee, \wedge>$的格同态（仅保$\vee$，$\wedge$运算），那么当 h 为满射时$<B, \vee, \wedge>$为一布尔代数。

*15.2.3 布尔代数表示定理

为了介绍重要的布尔代数表示定理，先给出下列概念：

定义 15-12 设$<B, \vee, \wedge, ', 0, 1>$为布尔代数，$\leqslant$为 B 作为格时的序关系，$x<y$ 表示 $x \leqslant y$ 且 $x \neq y$。称 B 中元素 a **盖着**（covering）b，如果 $b<a$，但没有 B 中元素 c，使 $b<c$，$c<a$。

a 盖着 b，当且仅当哈斯图中 a 在 b 的上方，且 a，b 间有一边相关联。

定义 15-13 布尔代数中盖着元素 0 的元素称为该布尔代数的**原子**（atoms）.

关于布尔代数的原子我们有以下定理。

定理 15-21 元素 a 是布尔代数$<B, \vee, \wedge, ', 0, 1>$的原子，当且仅当 $a \neq 0$ 且对 B 中任何元素 x

$$x \wedge a = a \text{ 或 } x \wedge a = 0 \tag{15-12}$$

证明 设 a 是原子，显然 $a \neq 0$。另设 $x \wedge a \neq a$。由于 $x \wedge a \leqslant a$，故 $0 \leqslant x \wedge a$，$x \wedge a < a$. 据

原子的定义，有 $x \wedge a = 0$。

反之，设 $a \neq 0$，且对任意 $x \in B$，式（15-12）成立。若 a 不是原子，那么必有 $b \in B$，使 $0 < b < a$。于是，$b \wedge a = b$。因为 $b \neq 0$，$b \neq a$，故 $b \wedge a = b$ 与式（15-12）矛盾。a 只能是原子。

定理 15-22 设 a 是布尔代数$<B, \vee, \wedge, ', 0, 1>$的原子，$x$ 为 B 中任一元素，那么 $a \leqslant x$ 或 $a \leqslant x'$，但不兼而有之。

证明 由于 a 为原子，因此有式（15-12）成立。

当 $x \wedge a = a$ 时，$a \leqslant x$。当 $x \wedge a = 0$ 时，令 $x' \wedge a = b$，于是$(x \wedge a) \vee (x' \wedge a) = 0 \vee b$，即$(x \vee x') \wedge a = b$，$a = b$，故 $x' \wedge a = a$，因而 $a \leqslant x'$（亦可由定理 15-17 直接推得）。

若 $a \leqslant x$，$a \leqslant x'$同时成立，那么 $a \wedge a \leqslant x \wedge x'$，即 $a \leqslant 0$，与 a 为原子矛盾。

本定理说明，布尔代数结构如下：

（1）有一个处于最“低层”的子集——原子的集合。

（2）依每个原子可以将布尔代数的非零元素分为两类，一类与该原子可比较，另一类与该原子不可比较。

定理 15-23 设$<B, \vee, \wedge, ', 0, 1>$为一有限布尔代数，那么对于 B 中任一非零元素 x，恒有一原子 $a \in B$，使 $a \leqslant x$。

证明 若 x 为原子，则命题已得证。

若 x 不是原子，那么必有 $y \in B$，$0 < y < x$。对 y 重复上面的讨论。

由于 B 有限，上述过程中产生的元素序列满足

$$0 < \cdots < z < y < x$$

其中必有一原子（否则此序列无限长）。定理得证。

定理 15-24 设 $a1$，$a2$ 为布尔代数$<B, \vee, \wedge, ', 0, 1>$中任意两个不相同的原子，那么 $a1 \wedge a2 = 0$.

证明 由原子的性质可知：$a1 \wedge a2 \neq a1$，$a1 \wedge a2 \neq a2$（否则 $a1 < a2$ 或 $a2 < a1$），若 $a1 \wedge a2 \neq 0$，那么

$$0 < a1 \wedge a2 < a1,\quad 0 < a1 \wedge a2 < a2$$

与 $a1$，$a2$ 为原子矛盾，故 $a1 \wedge a2 = 0$。

本定理也可叙述为：若原子 $a1$，$a2$ 满足 $a1 \wedge a2 \neq 0$，那么 $a1 = a2$。

定理 15-25 设$<B, \vee, \wedge, ', 0, 1>$为有限布尔代数，$x$ 为 B 中任一非零元素，a_1，a_2，…，a_k为满足 $a_i \leqslant x$（$i = 1, 2, \cdots, k$）的所有原子，那么

$$x = a_1 \vee a_2 \vee \cdots \vee a_k \quad (x \text{ 的原子表示})$$

证明 为简明计，令 $y = a_1 \vee a_2 \vee \cdots \vee a_k$。

由于 $a_i \leqslant x$（$i = 1, 2, \cdots, k$），因此 $y \leqslant x$。

欲证 $x \leqslant y$。据定理 15-17，只要证 $x \wedge y' = 0$。现反设 $x \wedge y' \neq 0$，从而有原子 a 使得

$$0 < a \leqslant x \wedge y', \text{ 进而有 } a \leqslant x,\ a \leqslant y'$$

由于 $a \leqslant x$，a 为原子，因此 a 为 a_1，a_2，…，a_k 之一，故 $a \leqslant y$。据定理 15-23，$a \leqslant y$ 和 $a \leqslant y'$不可能同时成立。这使我们从反面证得 $x \wedge y' = 0$，即 $x \leqslant y$。

$x = y = a_1 \vee a_2 \vee \cdots \vee a_k$得证。

定理 15-25 中非零元素 x 的原子表示形式

$$x = a_1 \vee a_2 \vee \cdots \vee a_k$$

是惟一的。我们可以证明之。

设 x 可表示为

$$x = a_1 \vee a_2 \vee \cdots \vee a_k,\quad x = b_1 \vee b_2 \vee \cdots \vee b_j \quad (b_1, b_2, \cdots, b_j \text{亦为原子})$$

由于$\{a_1, a_2, \cdots, a_k\}$为所有小于等于 x 的原子的集合，而 $b_i \leqslant x$ $(I = 1, 2, \cdots, j)$。因此

$$\{b_1, b_2, \cdots, b_j\} \subseteq \{a_1, a_2, \cdots, a_k\}$$

若 $j = k$，那么$\{b_1, b_2, \cdots, b_j\} = \{a_1, a_2, \cdots, a_k\}$，定理得证。若 $j < k$，那么必有 a_i 不同于所有 b_h $(h = 1, 2, \cdots, j)$。于是据定理 15-24，由

$$a_i \wedge (b_1 \vee b_2 \vee \cdots \vee b_j) = a_i \wedge (a_1 \vee a_2 \vee \cdots \vee a_k)$$

可推得

$$0 = a_i$$

矛盾。这就是说 $j < k$ 是不可能的。从而 $j = k$，命题得证。

现在我们来证明布尔代数表示定理。

定理 15-26 设$<B, \vee, \wedge, ', 0, 1>$为有限布尔代数，$A(\subseteq B)$为 B 中所有原子的集合，那么 B 同构于布尔代数$<\rho(A), \cup, \cap, ^-, \varnothing, A>$。

证明 定义映射 h：$B \to \rho(A)$，使得对任意 $x \in B$，

$$h(x) = \begin{cases} \varnothing & \text{当 } x = 0 \\ \{a : a \in A \wedge a \leqslant x\} & \text{当 } x \neq 0 \end{cases}$$

首先证明 h 为一双射。

对任一 $C \in \rho(A)$，令 $C = \{a_1, a_2, \cdots, a_k\} \subseteq A$。取

$$x = a_1 \vee a_2 \vee \cdots \vee a_k$$

那么 $h(x) = C$。h 为满射得证。

设 $x, y \in B$，$x \neq y$，那么 $x \leqslant y$ 不成立或 $y \leqslant x$ 不成立。不失一般性，设 $x \leqslant y$ 不成立。据定理 15-17，$x \wedge y' \neq 0$，从而有原子 $a \leqslant x \wedge y'$，进而 $a \leqslant x$，$a \leqslant y'$，而 $a \leqslant y$ 不成立。这表明，$a \in h(x)$，$a \notin h(y)$。因此，$h(x) \neq h(y)$。h 为单射也得证。

接着要证明 h 保运算，即 h 满足式（15-9）、式（15-10）和式（15-11）。

设 x，y 为 B 中任意两个元素，它们的原子表示分别是

$$x = a_1 \vee a_2 \vee \cdots \vee a_k \qquad y = b_1 \vee b_2 \vee \cdots \vee b_p$$

于是

$$\begin{aligned} h(x) &= \{a_1, a_2, \cdots, a_k\} \\ h(y) &= \{b_1, b_2, \cdots, b_p\} \\ h(x \vee y) &= h(a_1 \vee a_2 \vee \cdots \vee a_k \vee b_1 \vee b_2 \vee \cdots \vee b_p) \\ &= \{a_1, a_2, \cdots, a_k, b_1, b_2, \cdots, b_p\} \\ &= h(x) \cup h(y) \\ h(x \wedge y) &= h((a_1 \vee a_2 \vee \cdots \vee a_k) \wedge (b_1 \vee b_2 \vee \cdots \vee b_p)) \\ &= h(\vee_{1 \leqslant i \leqslant k, 1 \leqslant j \leqslant p} a_i \wedge b_j) \\ &= \bigcup_{1 \leqslant i \leqslant k, 1 \leqslant j \leqslant p} h(a_i \wedge b_j) \end{aligned}$$

由于

$$a_i \wedge b_j = a_i \text{（当 } a_i = b_j \text{）} \quad a_i \wedge b_j = 0 \text{（当 } a_i \neq b_j \text{）}$$

故

$$\begin{aligned} h(x \wedge y) &= \bigcup_{1 \leqslant i \leqslant k, 1 \leqslant j \leqslant p} \{h(a_i) : a_i = b_j\} \\ &= \bigcup_{1 \leqslant i \leqslant k, 1 \leqslant j \leqslant p} \{\{a_i\} : a_i = b_j\} \\ &= \{a_1, a_2, \cdots, a_k\} \cap \{b_1, b_2, \cdots, b_p\} \\ &= h(x) \cap h(y) \end{aligned}$$

$h(x') = (h(x))^-$ 证明如下：

对任意原子 $a \in A$，

$a \in h(x')$ 当且仅当 $a \leqslant x'$

当且仅当 $\neg\, a \leqslant x$（定理 15-22）

当且仅当 $a \notin h(x)$

当且仅当 $a \in (h(x))^-$

h 为布尔同构证完，定理得证。

本定理说明，有限布尔代数与集合代数同构，从而它总是恰含 2^n 个元素，其中 n 正是它的原子的数目。

这一定理对载体为无限集的布尔代数不能成立。

【例 15-11】 图 15-10 是定理 15-28 的一个例子。图 15-10a 表示以{a，b，c}为原子集的布尔代数，它共有 $2^3=8$ 个元素，各元素均已表示为原子表示形式（除了 0 和 1）。

图 15-10b 为布尔代数<$\rho(\{a, b, c\})$，∪，∩，$^-$，0，1>。图 15-10a 与图 15-10b 的同构是一目了然的。

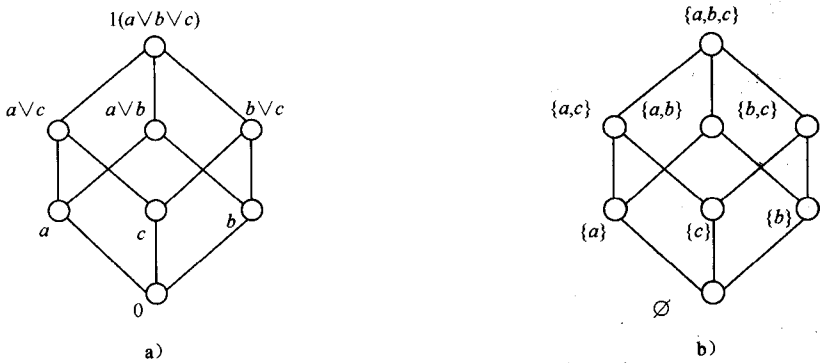


图 15-10

*15.2.4 布尔表达式与布尔函数

布尔代数中的布尔表达式、布尔函数的范式表示及简化，无论在理论研究和实际应中都有十分重要的意义，本小节介绍这两个概念。

定义 15-14 设<B，∨，∧，'，0，1>为布尔代数，如下递归地定义 B 上**布尔表达式**

（Boolean expressions）：

（1）布尔常元和布尔变元（取值于 B 的常元和变元）是布尔表达式。布尔常元常用 a，b，c 等字母表示，布尔变元常用 x，y，z 等字母表示。

（2）如果 e，$e1$，$e2$ 为布尔表达式，那么（e'），（$e1 \vee e2$），（$e1 \wedge e2$）也是布尔表达式。

（3）除有限次使用条款（1），（2）生成的表达式是布尔表达式外，没有别的是布尔表达式。

为了省略括号，我们约定运算'的优先级高于运算∨，∧，并约定表达式最外层括号省略。

常用 $f(x_1, x_2, \cdots, x_n)$，$g(y_1, y_2, \cdots, y_m)$等分别表示含有 n 个变元 x_1，x_2，…，x_n 的 n 元布尔表达式和含有 m 个变元 y_1，y_2，…，y_m 的 m 元布尔表达式。

给定布尔表达式并确定其中变元的取值后，该表达式对应于一个确定的 B 的元素——布尔表达式的值（对应于变元所取值）。因此有下列定义：

定义 15-15 布尔表达式 $f(x_1, x_2, \cdots, x_n)$所定义的函数 $f: B \to B$ 称为**布尔函数**（Booleanl functions）。

【例 15-12】 设$<\{0, a, b, 1\}$，∨，∧，'，0，1$>$为布尔代数，其上有表达式

$$f(x1, x2) = (x1' \vee a) \wedge x2$$

$$g(x1, x2, x3) = (x1 \wedge x2 \wedge x3)' \vee (x1 \wedge x2' \wedge x3')$$

$$f(1, b) = (1' \vee a) \wedge b = a \wedge b = 0$$

$$\begin{aligned} g(a, b, 0) &= (a \wedge b \wedge 0)' \vee (a \wedge b' \wedge 0') \\ &= 0' \vee (a \wedge a \wedge 1) \\ &= 1 \end{aligned}$$

像在命题代数中那样，可以讨论布尔表达式的范式。

定义 15-16 布尔表达式

$$\alpha_1 \wedge \alpha_2 \wedge \cdots \wedge \alpha_n$$

称为 n 个变元的**极小项**，其中α_i为变元 x_i 或 x_i'，而表达式

$$\alpha_1 \vee \alpha_2 \vee \cdots \vee \alpha_n$$

称为 n 个变元的**极大项**，其中α_i为变元 x_i 或 x_i'。

显然，n 个变元的极小项和极大项各有 2^n 个，我们分别用

$$m_0, m_1, \cdots, m_{e(n)}$$

$$M_0, M_1, \cdots, M_{e(n)} \qquad (e(n) = 2^n - 1)$$

来表示它们，它们满足下列性质：

（1）$m_i \wedge m_j = 0$；$M_i \vee M_j = 1$ $\quad (i \neq j)$

（2）$\bigvee_{i=0}^{e(n)} m_i = 1$，$\bigwedge_{i=0}^{e(n)} M_i = 0$

定义 15-17 布尔表达式 $f(x_1, x_2, \cdots, x_n)$的主析取范式和主合取范式分别指下列布尔表达式：

$$(a_0 \wedge m_0) \vee (a_1 \wedge m_1) \vee \cdots \vee (a_{e(n)} \wedge m_{e(n)}) \qquad (15\text{-}13)$$

$$(a_0 \vee M_0) \wedge (a_1 \vee M_1) \wedge \cdots \wedge (a_{e(n)} \vee M_{e(n)}) \qquad (15\text{-}14)$$

其中 a_i 为布尔常元，m_i 与 M_i 分别是极小项与极大项，且两式对 x_1，x_2，…，x_n 一切的可能取值均与 $f(x_1, x_2, \cdots, x_n)$ 等值。

求取主析取范和主合取范式的方法与命题演算中介绍的方法大体相同（参见第 3 章第 3 节）：

（1）将布尔常元看作变元，作同样的处理。

（2）利用德摩根律将运算符号'深入到每个变元（常元）上。

（3）利用分配律展开。

（4）构成极小项或极大项缺少变元 x 时，用添合取项（$x \vee x'$）或析取项（$x \wedge x'$）来处理。

（5）计算合并常元，变元和表达式（只要可能，这一步骤可随时进行）。

【例 15-12】 布尔代数 $<\{0, a, b, 1\}, \vee, \wedge, ', 0, 1>$ 上的布尔函数

$$f(x1, x2) = ((a \wedge x1) \vee (b \vee x1)') \wedge (x1 \vee x2)$$

的主析取范式可以如下求取：

$$\begin{aligned} f(x1, x2) &= ((a \wedge x1) \vee (b' \wedge x1')) \wedge (x1 \vee x2) \\ &= ((a \wedge x1) \wedge (x1 \vee x2)) \vee ((b' \wedge x1') \wedge (x1 \vee x2)) \\ &= (a \wedge x1) \vee (a \wedge x1 \wedge x2) \vee (b' \wedge x1' \wedge x1) \vee (b' \wedge x1' \wedge x2) \\ &= (a \wedge x1) \vee (b' \wedge x1' \wedge x2) \\ &= (a \wedge x1) \wedge (x2 \vee x2') \vee (b' \wedge x1' \wedge x2) \\ &= (a \wedge x1 \wedge x2) \vee (a \wedge x1 \wedge x2') \vee (a \wedge x1' \wedge x2) \end{aligned}$$

它的主合取范式可如下求取：

$$\begin{aligned} f(x1, x2) &= ((a \wedge x1) \vee (b' \wedge x1')) \wedge (x1 \vee x2) \\ &= ((a \wedge x1) \vee b') \wedge ((a \wedge x1) \vee x1') \wedge (x1 \vee x2) \\ &= (a \vee b') \wedge (b' \vee x1) \wedge (a \vee x1') \wedge (x1 \vee x2) \\ &= a \wedge (a \vee x1) \wedge (a \vee x1') \wedge (x1 \vee x2) (b' = a) \\ &= a \wedge (x1 \vee x2) \\ &= (a \vee x1 \vee x2) \wedge (a \vee x1 \vee x2') \wedge (a \vee x1' \vee x2) \wedge (a \vee x1' \vee x2') \wedge (x1 \vee x2) \\ &= (x1 \vee x2) \wedge (a \vee x1 \vee x2') \wedge (a \vee x1' \vee x2) \wedge (a \vee x1' \vee x2') \end{aligned}$$

从定义 15-17 可以看出，$<B, \vee, \wedge, ', 0, 1>$ 的不同的 n 元主析取范式和主合取范式分别是 $|B|^{2^n}$ 个，因为在式（15-13）和式（15-14）中，a_0，a_1，…，$a_{e(n)}$（$e(n) = 2^n - 1$）各有 $|B|$ 种取值可能。这就表明，B 上不同的 n 元布尔函数至多是 $|B|^{2^n}$ 个。因此应当注意并非所有的 B^n 到 B 的函数都是布尔函数，B^n 到 B 的函数共有 $|B|^{|B^n|}$ 个。只是在 $B = \{0, 1\}$ 时两者数目相同，正像我们在命题演算中看到的那样，n 元真值函数与 n 元主析取（合取）范式的个数相同，都是 2^{2^n} 个。另一点值得注意的是，式（15-13）中 a_0，a_1，…，$a_{e(n)}$ 均取 0 时，该式值为 0，因此 0 的主析取范式常简单地规定为 0。它表示常函数 $f(x_1, x_2, \cdots, x_n) = 0$。式（15-14）中 a_0，a_1，…，$a_{e(n)}$ 均取值 1 时，该式值为 1，因此 1 的主合取范式常简单地规定为 1。它表示常函数 $f(x_1, x_2, \cdots, x_n) = 1$。

15.3 练习

1. 对格 L 中任意元素 a，b，c，d，证明：

（1）$a\leqslant b$，$a\leqslant c$ 当且仅当 $a\leqslant b\wedge c$。

（2）$a\leqslant c$，$b\leqslant c$ 当且仅当 $a\vee b\leqslant c$。

（3）若 $a\leqslant b\leqslant c$，$d\wedge c=a$，则 $d\wedge b=a$。

（4）若 $a\leqslant b\leqslant c$，$d\wedge a=c$，则 $d\wedge b=c$。

（5）$(a\wedge b)\vee(a\wedge c)\leqslant a\wedge(b\vee c)$。

（6）$(a\wedge b)\vee(c\wedge d)\leqslant(a\vee c)\wedge(b\vee d)$。

2. 令 $x<y$ 表示 $x\leqslant y$ 且 $x\neq y$，对格 L 中任意元素 a，b，证明：$a\wedge b<a$ 且 $a\wedge b<b$ 当且仅当 a 与 b 是不可比较的，即 $a\leqslant b$，$b\leqslant a$ 都不能成立。

3. 求证：有序集$<L$，$\leqslant>$为完全格的充分必要条件是：L 有下确界，且 L 的每一子集有上确界。

4. 问开区间（0，1）中的有理数集合按有理数的大小排序是否构成完全格？闭区间［0，1］呢？

5. 证明：定义 12-2 中 L 满足幂等律的要求是多余的，即由交换律、结合律和吸收律可导出它满足幂等律。

6. 设格 $L1$ 与 $L2$ 同态，求证：若 $L1$ 有幺元（零元），那么 $L2$ 也有幺元（零元）。

7. 证明：格 L 的两个子格的交仍为 L 的子格。

8. 设 a，b 为格 L 中的两个元素，证明：$S=\{x\mid x\in L$ 且 $a\leqslant x\leqslant b\}$可构成 L 的一个子格。

9. 设 f 为格 $L1$ 到格 $L2$ 的同态映射，证明：f 的同态像是 $L2$ 的子格。

10. 完成定理 15-8 中$<M_a$，$\vee$，$\wedge>$为子格的证明。

11. 设$<L$，$\vee$，$\wedge>$为分配格，a 为 L 中一确定元素。定义函数 $f:L\to L$；$g:L\to L$，使得对任一 $x\in L$，

$$f(x)=x\wedge a,\quad g(x)=x\vee a$$

求证：f，g 都是 L 上的自同态，从而它们的像都是 L 的子格。

12. 证明：在分配格中有

（1）$a\wedge\bigvee_{i=1}^{m}b_i=\bigvee_{i=1}^{m}(a\wedge b_i)$

（2）$a\vee\bigwedge_{i=1}^{m}b_i=\bigwedge_{i=1}^{m}(a\vee b_i)$

13. 图 15-11 中各哈斯图是否表示有补格？

14. 证明：在有界分配格中，拥有补元的所有元素可以构成一个子格。

15. 设$<L$，$\vee$，$\wedge>$为有补分配格，a，b 为 L 中任意元素，证明：

$$b'\leqslant a'\text{当且仅当 }a\wedge b'=0\text{ 当且仅当 }a'\vee b=1$$

16. 证明下列布尔恒等式；

（1）$(a\wedge b)\vee(a\wedge b')\vee(a'\wedge b)=a\vee b$

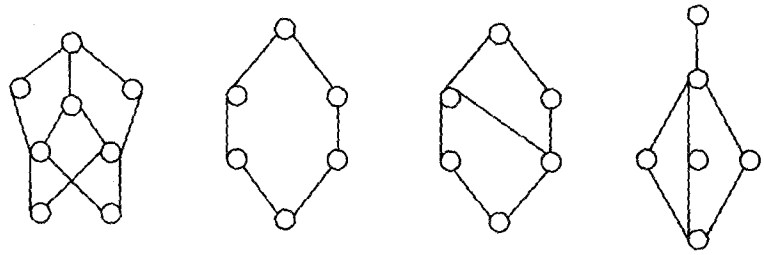


图 15-11

（2）$(a\wedge c)\vee(a'\wedge b)\vee(b\wedge c)=(a\wedge c)\vee(a'\wedge b)$

（3）$(a\vee b')\wedge(b\vee c')\wedge(c\vee a')=(a'\vee b)\wedge(b'\vee c)\wedge(c'\vee a)$

（4）$(a\wedge b)\vee(a'\wedge c)\vee(b'\wedge c)=(a\wedge b)\vee c$

17. 化简下列布尔表达式：

（1）$(1\wedge a)\vee(0\wedge a')$

（2）$(a\wedge b)\vee(a'\wedge b\wedge c,)\vee(b\wedge c)$

（3）$((a\wedge b')\vee c)\wedge(a\vee b')\wedge c$

（4）$(a\wedge b)'\vee(a\vee b)'$

18. 设 a，b 为布尔代数 B 中任意元素，求证：

$$a=b \text{ 当且仅当}(a\wedge b')\vee(a'\wedge b)=0$$

19. 设 a，b，c，d 为布尔代数 B 中任意元素，求证：当 $c\vee a=b$，$c\wedge a=0$，$d\vee a=b$，$d\wedge a=0$ 时有 $b\wedge a=a$，$b\wedge c=c$，$c=d$。

20. 设 h 是布尔代数 $B1$ 和 $B2$ 的格同态（即仅满足式（15-9）和式（15-10）），同时 $h(0)=0$，$h(1)=1$。证明：h 是 $B1$，$B2$ 之间的布尔同态。

21. 设$<B$，$\vee$，$\wedge$，'，0，1$>$为布尔代数，定义 B 上环和运算$\oplus$：对任意 a，$b\in B$，

$$a\oplus b=(a\wedge b')\vee(a'\wedge b)$$

（1）证明：$<B$，$\oplus>$为一阿贝尔群。

（2）证明：$<B$，$\oplus$，$\wedge>$）为一含幺交换环。

*22. 设$<B$，$\vee$，$\wedge$，'，0，1$>$为布尔代数，$a\in B$。称 a 是**极小的**，如果 $a\neq 0$ 且对于任意 $x\in B$，有

$$x\leqslant a \text{ 蕴涵 } x=a \text{ 或 } x=0$$

证明：a 是极小的当且仅当 a 是原子。

*23. 不利用布尔代数表示定理，证明：没有恰含 3 个元素的布尔代数。

参 考 文 献

1 本教程研究组．中国计算机科学与技术学科教程 2002．北京：清华大学出版社，2002

2 Azriel Levy．Basic Set Theory．Springer-Verlag , 1979

3 王元元．计算机科学中的现代逻辑学．北京：科学出版社，2001

4 王元元等．组合数学原理及题解．台北：台湾中央图书出版社，1999

5 Narsingh Deo．Graph Theory With Applications and Computer Science．Prentice-Hall , Inc. 1974

6 王元元，张桂芸．离散数学导论．北京：科学出版社，2002

7 王元元．可计算性引论．南京：东南大学出版社，1990

8 张立昂等译．计算理论导引．北京：机械工业出版社，2000

9 冯克勤等．近世代数引论．合肥：中国科学技术大学出版社，1988

10 Fraleigh J . B．A First Course in Abstract Algebra , Addison-wesley Publishing Company , 1982

[General Information]
书名=计算机科学中的离散结构
作者=王元元　张桂芸编著
页数=302
SS号=11157756
DX号=
出版日期=2004年01月第1版
出版社=机械工业出版社