离散数学教程

徐秋亮　栾俊峰　卢　雷
王　慧　　赵合计
编著

山东大学计算机科学与技术学院

离散数学教程

徐秋亮　栾俊峰　卢　雷

编著

王　慧　　赵合计

山东大学计算机科学与技术学院

前　言

离散数学是现代数学的一个重要分支，是学习计算机科学与技术的重要基础课之一．离散数学的内容多而杂，合理选取是一个重要问题．国内教材一般由集合论、数理逻辑、图论、代数结构等 4 大块组成，有时增加一点初等数论、组合论、形式语言等．国外教材的内容差异较大，各有侧重且往往涵盖广泛、极为庞杂，不能很好地适应国内的教学体系．本书是在徐秋亮编著的《离散数学》（山东大学出版社，1993）的基础上修订、补充而成．比之原书增加了组合论、形式语言初步知识，删减了群的直积、环同态基本定理等较为抽象的内容，并在内容的表达等各方面进行了修订．本书是编者多年讲授此课的经验积累．

在本书的编写过程中，我们分析、比较了国内外各类教材及教学大纲，在内容选取、重点及难点内容的处理、定理证明的表述等方面，根据多年来的教学实践仔细斟酌，有一定的独到之处．本书以集合论、代数结构、数理逻辑、图论四大部分为主干，同时简单介绍组合论、形式语言的初步内容，可作为计算机科学与技术专业本科教材．讲完全书约需 140——160 学时，适当选取内容可适应本科生 72 学时——108 学时的教学需求．

本书第一、二篇及第三篇的第八章到第十一章由徐秋亮编写，第十二章到第十三章由栾俊峰编写，第四篇由徐秋亮、赵合计编写，第五篇由卢雷、王慧编写，最后由徐秋亮审阅全稿．

本书的如期印刷要感谢我们的学生——硕士研究生孔志刚、杨伟强、张鹏、蒋翰、尚久庆、张忠、柳欣、邹静、董贝贝等准确、漂亮的打字．

由于编者水平所限，书中定会有缺点或错误，欢迎读者批评指正．

编　者

2003 年 6 月

目　　录

第一篇 集合论

第二篇　代数结构

第三篇　图论与组合初步

第四篇　数理逻辑

第五篇　形式语言与自动机

第一篇　集合论

德国数学家G.Cantor在1874-1897年发表的一系列论文奠定了集合论的基础，从那以后，集合论的概念和结果被广泛地应用于数学的各个学科，使数学科学受到了深刻的影响. 到现在，集合论不但已成为几乎所有数学分支的基础，而且在计算机科学理论的研究中，也得到了卓有成效地应用.

在集合论的初创时期，Cantor是以所谓“朴素的”观点来看待集合的，尽管他已经建立起相当广泛而深刻的理论,但在他的理论基础上却存在着不可忽视的弱点，受到了各种批评和责难，同时也受到了集合论本身各种悖论的困扰. 这个时期的集合论称为朴素集合论.

为了填补Cantor理论基础的不足，从而维护Cantor理论. 在1908年，E.Zermelo开辟了公理集合论的研究方向，后经许多人的努力，形成了ZF系统、GB系统等公理系统.

本篇从集合的直观概念出发，介绍了集合论中的一些基本概念和基本理论，其中包括关系、函数、无限集等. 在我们的讨论中，将完全采用朴素集合论的观点，而避免公理化方法.

第一章 基本概念

§1 集　　合

集合是现代数学中的最基本概念，我们在此不对它做严格的定义，而只采用下述直观的说法.

一组明确的、互不相同的事物组成的整体称之为一个集合，组成集合的各个事物（个体）称为该集合的元素．例如，所有实数构成一个集合，0.3，1.5，2 都是该集合的元素，$\sqrt{-1}$ 则不然；26 个小写英文字母构成一个集合，a，b，c 都是该集合的元素β则不然．集合一般用大写字母 A，B，C，…，X，Y，Z 等表示，集合的元素一般用小写字母 a，b，c，…，x，y，z 等表示．当事物 a 是集合 A 的元素时，称 a 属于 A，记为 $a\in A$，当事物 a 不是集合 A 的元素时，称 a 不属于 A，记为 $a\notin A$.

例如，若将所有实数构成的集合记为 $\mathbf{R}$，则 $0.3\in\mathbf{R}$，$1.5\in\mathbf{R}$，$2\in\mathbf{R}$，$\sqrt{-1}\notin\mathbf{R}$；若将 26 个小写英文字母构成的集合记为 E，则 $a\in E$，$b\in E$，$c\in E$，$\beta\notin E$.

在对集合概念的描述中，要求构成集合的事物是“明确的”．这意味着某个事物是否属于某个集合是毫无含混余地的，即是说，对于给定的事物 a 和集合 A，$a\in A$ 与 $a\notin A$ 必定恰有一条成立．象较高的人、较远的星星、半径很大的圆等都不能构成集合．构成集合的事物又要是互不相同的，这意味着，在一个集合中，相同的事物只能算作一个.

为了讨论问题方便，我们还引入不含任何元素的集合，称为空集，记为$\varnothing$．空集与含有 n 个元素（n 为正整数）的集合称为有限（穷）集，不是有限集的集合称为无限（穷）集，有限集 A 中所含元素的个数记为$|A|$.

为了表示一个集合，最常用的方法有以下三种.

（1）全部列举法：写出集合的所有元素，并将它们放在花括号内．例如，由 a，b，c，d，四个字母组成的集合可记为 $\{a，b，c，d\}$，如果用 A 表示这个集合，则可记为

$$A=\{a，b，c，d\}$$

（2）部分列举法：列举集合的部分元素，其他元素可从列举的元素归纳出来，用省略号代替．例如，所有的自然数（包括 0）构成的集合可记为

$$\{0，1，2，\cdots\cdots\}$$

如果用 $\mathbf{N}$ 表示这个集合，则可记为

$$\mathbf{N}=\{0，1，2，\cdots\cdots\}$$

同样，由 0 到 1000 的所有整数构成的集合 A 可记作

$$A=\{0，1，2，\cdots，1000\}$$

（3）概括法：通过刻划集合的元素所满足的条件来描述集合．如果 A 是所有具有某种性质 P 的事物构成的集合，可以用以下形式表示

$$A=\{x\mid x \text{ 具有性质 } P\}$$

例如，所有素数构成的集合 P 可记为

$$P=\{x\mid x \text{ 是素数}\}$$

再如，方程 $ax^2+bx+c=0$ 的所有实根构成的集合 B 可记为

$$B=\{x|x \text{ 是实数}，ax^2+bx+c=0\}$$

注意：“$A=\{x|x$ 具有性质 $P\}$”与“$x\in A\Leftrightarrow x$ 具有性质 P”描述了同一个事实，以后经常用“$x\in A\Leftrightarrow x$ 具有性质 P”的形式定义集合 A．

为了使表达更加简明，我们常将这种表达方式稍作变形．

例如　　$P=\{x\mid x=3n，n \text{ 是整数}\}$．

通常写成　　$P=\{3n|n \text{ 是整数}\}$．

再如　　$Q=\{x\mid x=3n+7m，m，n \text{ 是正整数}\}$．

通常写成　　$Q=\{3n+7m|m，n \text{ 是正整数}\}$．

一个集合可以包含其它集合作为元素，例如 $\{a，\{b，c\}\}$ 中有两个元素 a 和 $\{b，c\}$，b 是 $\{b，c\}$ 的元素，但不是 $\{a，\{b，c\}\}$ 的元素．一个集合，如果其每个元素均为集合，则称之为集合族．例如 $\{\varnothing，\{a\}，\{b\}，\{a，b\}\}$ 就是一个集合族．

作为本节的结束，我们引入几个以后经常用到的集合符号．

（1）　用 **N** 表示所有自然数（包括 0）所组成的集合（简称自然数集）

（2）　用 **Z** 表示所有整数所组成的集合（简称整数集）

（3）　用 $\mathbf{N}^+$或 $\mathbf{Z}^+$表示所有正整数所组成的集合（简称正整数集）

（4）　用 **Q** 表示所有有理数所组成的集合（简称有理数集）

（5）　用 $\mathbf{Q}^+$表示所有正有理数所组成的集合（简称正有理数集）

（6）　用 **R** 表示所有实数所组成的集合（简称实数集）

（7）　用 $\mathbf{R}^+$表示所有正实数所组成的集合（简称正实数集）

今后，如果没有特别说明，符号 $\mathbf{N}$，$\mathbf{Z}$，$\mathbf{N}^+$，$\mathbf{Z}^+$，$\mathbf{Q}$，$\mathbf{Q}^+$，$\mathbf{R}$，$\mathbf{R}^+$总是表示上述集合．

习　题　一

1．下列事物全体能否构成集合？

（1）聪明的人．

（2）白兔子．

（3）某教室里的桌椅．

（4）$(0,1)$ 区间上的连续函数．

（5）有限集．

2．将下列集合表达为另一形式．

（1）$A=\{x|x\in N,\ 0\leqslant x\leqslant 50\}$．

（2）$A=\{x|x$ 是偶素数$\}$．

（3）$A=\{x|$存在 $n\in\boldsymbol{N}$，使 $x=5n+6\}$．

（4）$A=\varnothing$．

（5）$E=\{x|$存在 $r\in\boldsymbol{R}$ 使 $x=r^2\}$．

（6）$E=\{0,2,4,6,\cdots\cdots\}$．

§2 子　集

为了叙述的简捷，我们引入下面一些通用记号，这些记号将在本书中除第四篇以外的范围内较灵活、随意的使用．我们今后将用“$\forall x\in A$”表示“任取 $x\in A$”或“对于任意 $x\in A$”，“$\exists x\in A$”表示“存在 $x\in A$”，“$\exists|x\in A$”表示“存在唯一 $x\in A$”．设 P，Q 为两个论断，用“$P\Rightarrow Q$”表示“如果 P 则 Q”，“$P\Leftrightarrow Q$”表示“P 当且仅当 Q”．

定义 1　设 A，B 为两个集合，如果 A 的元素均是 B 的元素，则称 A 为 B 的子集或称 A 包含于 B（B 包含 A），记为 $A\subseteq B$ 或 $B\supseteq A$．即

$$A\subseteq B\Leftrightarrow \forall x\in A \text{ 必有 } x\in B$$

例如　$N\subseteq Z$

$$\{x|\,x(x\text{-}1)=0\}\subseteq\{x|\,x(x\text{-}1)(x\text{-}2)=0\}$$

$$\{\{a\},\{b,c\}\}\not\subseteq\{\{a,b\},\{c,d\}\}$$

这里，$A\not\subseteq B$ 表示 A 不是 B 的子集．

必须注意从属关系$\in$与包含关系$\subseteq$在概念上的区别．从属关系$\in$是个体（元素）与整体（集合）之间的关系，而包含关系$\subseteq$是整体（集合）与整体（集合）之间的关系．例如，考虑集合 $A=\{\{a,b\},b,c\}$．$\{a,b\}$ 作为一个个体出现在集合 A 中，故 $\{a,b\}\in A$，而 $\{a,b\}$ 作为一个事物构成的整体，其中的事物 a 不是集合 A 的元素，故 $\{a,b\}\not\subseteq A$；$\{b,c\}$ 作为一个个体，不出现在 A 中，故 $\{b,c\}\notin A$，而 $\{b,c\}$ 作为一个由事物构成的整体，其中各事物均出现在 A 中，故 $\{b,c\}\subseteq A$．

容易验证，集合的包含关系具有如下性质

1）$A\subseteq A$　　（反身性）

2）$A\subseteq B$，$B\subseteq C\ \Rightarrow\ A\subseteq C$　　（传递性）

对于任意集合 A，我们认为总有$\varnothing\subseteq A$．这样一来，$\varnothing$与 A 是 A 的两个必然的子集，我们称其为 A 的平凡子集．

定义 2　设 A，B 是两个集合，如果 $A\subseteq B$，$B\subseteq A$，则称 A 与 B 相等，记为 $A=B$，即

$$A=B\ \Leftrightarrow\ A\subseteq B\text{ 且 }B\subseteq A$$

例如　$\{a,b,c\}=\{c,a,b\}$

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

$\{x|x\in N,\ 1\leqslant x\leqslant 10\}=\{1,\ 2,\ 3,\ \cdots,\ 10\}$

$\{\{a\}\}\neq\{a\}$

定义 3　设 A,B 是两个集合，如果 $A\subseteq B$ 且 $A\neq B$，则称 A 为 B 的真子集，记为 $A\subset B$.

有时我们必须讨论某集合 A 的所有子集，这些子集全体作为一个整体又构成一个集合，该集合称为 A 的幂集.

定义 4　设 A 是一个集合，A 的所有子集构成的集合称为 A 的幂集，记为 $P(A)$或 2^A. 即 $P(A)=\{x|x\subseteq A\}$

例如，　$P(\{a,\ b\})=\{\varnothing,\ \{a\},\ \{b\},\ \{a,\ b\}\}$,　$P(\varnothing)=\{\varnothing\}$

$P(\{\varnothing\})=\{\varnothing,\ \{\varnothing\}\}$

定理 1　设A是有限集，则 $|2^A|=2^{|A|}$

证明　设 $|A|=n$，从 A 的 n 个元素中任取 i（$\leqslant n$）个元素共有 C_n^i 种取法，故 A 的包含 i 个元素的子集共有 C_n^i 个，因此，A 的所有子集共有 $C_n^0+C_n^1+\cdots\cdots+C_n^n=2^n$ 个. 即

$$|2^A|=2^{|A|}.$$ ▌

最后，我们给出一种对于有限集子集的编码方式.

设A＝$\{a_1,\ a_2,\ \cdots,\ a_n\}$，由集合的概念可知，$A$ 的元素之间不存在不言而喻的顺序，但我们可以任意规定一个顺序，具体地说，当我们写 $A=\{a_1,\ a_2,\ \cdots,\ a_n\}$ 时，就认为 A 的元素对应于序列 $a_1,\ a_2,\ \cdots,\ a_n$ 这个顺序.

设 $A_1\subseteq A$，对每个 $a_i\in A$，令

$$\delta_i=\begin{cases}0, & a_i\notin A_1\\ 1, & a_i\in A_1\end{cases}$$

则由 A_1 可以确定一个 n 位二进制数$\delta_1\delta_2\cdots\delta_n$，例如，设 $A=\{a,\ b,\ c,\ d\}$，$A_1=\{a,\ d\}$，$A_2=\{a,\ c\}$，则由 A_1 确定的二进制数为 1001，A_2 确定的二进制数为 1010，反之，给定一个 n 位二进制数$\delta_1\delta_2\cdots\delta_n$，不难确定与其对应的子集，这样就在 A 的子集与 n 位二进制数之间，建立了一一对应，若 $A_1\subseteq A$ 对应的二进制数为$\delta_1\delta_2\cdots\delta_n$，则 A_1 可记为 $B_{\delta_1\delta_2\cdots\delta_n}$，例如，设 $A=\{1,\ 2,\ 3,\ 4\}$，则 $B_{0110}=\{2,\ 3\}$，$B_{1001}=\{1,\ 4\}$. 为方便，可将二进制下标化为十进制书写，于是 $B_7=B_{0111}=\{2,\ 3,\ 4\}$，$B_4=B_{0100}=\{2\}$.

由有限集子集与二进制数的上述对应关系，也可看出，n 个元素的集合共有 2^n 个子集. 即$|2^A|=2^{|A|}$.

习　题　二

1．判断下列命题之正误.

（1）$\varnothing\subseteq\{\varnothing\}$.

（2）$\varnothing \in \{\varnothing\}$.

（3）$\{b, c\} \subseteq \{\{a, b\}, c\}$.

（4）$b \in \{\{a\}, \{b\}, \{b, c\}\}$

2．判断下列命题之正误，并证明你的结论.

（1）$A \in B, B \subseteq C \Rightarrow A \in C$.

（2）$A \in B, B \subseteq C \Rightarrow A \subseteq C$.

（3）$A \subseteq B, B \in C \Rightarrow A \in C$.

（4）$A \subseteq B, B \in C \Rightarrow A \subseteq C$.

（5）$A \in B, B \nsubseteq C \Rightarrow A \notin C$.

（6）$A \subseteq B, B \in C \Rightarrow A \notin C$.

3．求 $P(P(P(\varnothing)))$.

4．设 $A=\{a, \{a\}\}$，判断下列命题之正误.

（1）$\{a\} \in P(A)$，　　（2）$\{a\} \subseteq P(A)$

（3）$\{\{a\}\} \in P(A)$，　　（4）$\{\{a\}\} \subseteq P(A)$

5．试说明 $A \subseteq B$，$A \in B$ 能否同时成立.

§3　集合的运算

在本节中，我们给出最常用的五种集合运算，并研究它们的性质.

定义 1　设 A，B 是两个集合，由至少属于 A，B 之一的元素构成的集合称为 A 与 B 的并集，记为 $A \cup B$. 即

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

例如，设 $A=\{1, 2, 3\}$，$B=\{\{1\}, 2, 3, 4\}$

则

$A \cup B=\{1, 2, 3, 4, \{1\}\}$

$A \cup \varnothing=A$

$A \cup \{\varnothing\}=\{1, 2, 3, \varnothing\}$

定义 2　设 A，B 为两个集合，由既属于 A 又属于 B 的元素构成的集合称为 A 与 B 的交集，记为 $A \cap B$，即

$$A \cap B=\{x \mid x \in A, x \in B\}$$

例如，设　$A=\{a, b, c\}$，$B=\{\{a\}, b, c, \varnothing\}$，

则　　$A \cap B=\{b, c\}$

$B \cap \varnothing=\varnothing$

$B \cap \{\varnothing\}=\{\varnothing\}$

定义 3　设 A，B 是两个集合，如果 $A \cap B=\varnothing$，则称 A 与 B 是分离的或不交的；设 A 是一个集合族，如果 A 的元素是两两分离的，则称 A 为分离族.

例如，{1，2} 与 {3，4} 是分离的；{{a，b}，{d，c}，{f}} 是一个分离族.

定义 4　设 A，B 是两个集合，由属于 A 但不属于 B 的元素构成的集合称为 A 与 B 的差集，或称为 B 在 A 中的相对补集，记为 $A-B$. 即

$$A-B=\{x \mid x\in A，x\notin B\}$$

例如，设　$A=\{\{a\}，b，c\}$，$B=\{a，b，1，2\}$

则　　$A-B=\{\{a\}，c\}$　　$B-A=\{a，1，2\}$

人们讨论任何问题，总是在某个确定的基本集合中进行的，所考虑的集合均为该基本集合的子集，这个基本集合通常称为全集，用 U 表示. 例如，微积分是在实数范围内考虑问题的，所以实数集 R 可以作为全集；初等数论是在整数范围内考虑问题的，所以整数集 **Z** 可以作为全集.

以后，我们讨论集合时，总假定是在某个取定的全集 U 上进行的.

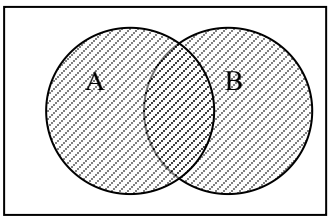
定义 5　集合 A 在全集 U 中的相对补集 $U-A$ 称为 A 的绝对补集，简称补集. 记为 $\sim A$. 即 $\sim A = U-A$.

例如，设全集 $U=\{a，b，c，\cdots，x，y，z\}$，则 $\sim\{a，b，c\}=\{d，e，f，\cdots，x，y，z\}$.

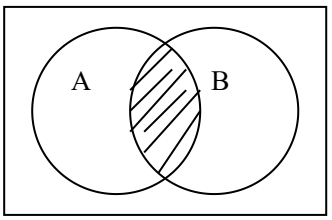
容易证明，对任意集合 A，B，有

$$A-B=A\cap\sim B$$

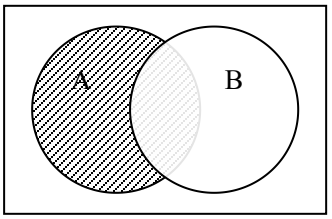
以上介绍的四种集合运算，可用如下图形直观、形象地表示.



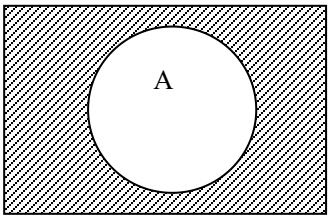
$A\cup B$



$A\cap B$



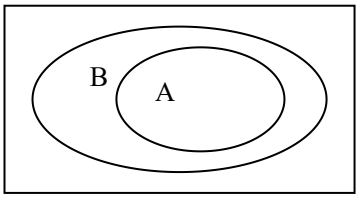
A-B



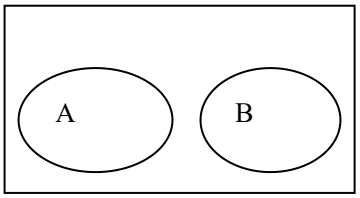
~A

这些图形称为 Venn 图，Venn 图是一种用平面点集表示一般集合的图示方法，利用

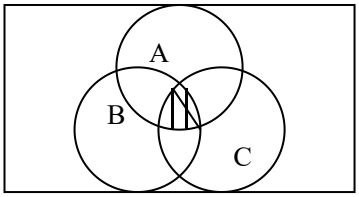
这种图示方法可以形象地表达集合之间的关系．下面我们再画出几个 Venn 图．



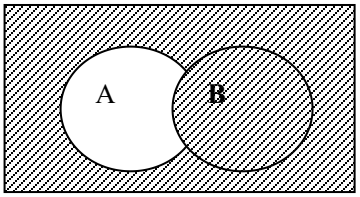
$A \subseteq B$



$A \cap B = \Phi$



$A \cap B \cap C$



$\sim A \cup B$

集合并、交、差、补四种运算的性质，可概括如下：

定理 1　设 A，B，C 为全集 U 的子集，则

（1）　$A \cup A = A$　　$A \cap A = A$　　（幂等律）

（2）　$A \cup B = B \cup A$　　$A \cap B = B \cap A$　　（交换律）

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

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

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

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

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

　　$\sim (A \cap B) = \sim A \cup \sim B$　　（De　Morgan 律）

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

（7）　$A \cup U = U$　　$A \cap \varnothing = \varnothing$　　（零律）

（8）　$A \cap U = A$　　$A \cup \varnothing = A$　　(单位律)

（9）　$A \cup \sim A = U$　　$A \cap \sim A = \varnothing$　　（补律）

（10）　$\sim (\sim A) = A$　　（反身律）

证明　这些性质大部分是明显的，现只给出（4）与（6）中第一式的证明，其他各式类似可证．

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

$\forall x \in A \cap (B \cup C)$，根据集合交的定义知，$x \in A$，$x \in B \cup C$，由 $x \in B \cup C$ 及集合并的定义知，$x \in B$ 或 $x \in C$，不妨设 $x \in B$，于是 $x \in A \cap B$，因此 $x \in (A \cap \mathrm{B}) \cup (A \cap C)$. 从

而

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

反之，$\forall x\in(A\cap B)\cup(A\cap C)$，根据集合并的定义知，$x\in A\cap B$ 或 $x\in A\cap C$，不妨设 $x\in A\cap B$，则 $x\in A$ 且 $x\in B$，由 $x\in B$ 可知 $x\in B\cup C$，再由 $x\in A$ 知 $x\in A\cap(B\cup C)$. 从而

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

总之，有 $A\cap(B\cup C)=(A\cap B)\cup(A\cap C)$

再证　　$\sim(A\cup B)=\sim A\cap\sim B$

$\forall x\in\sim(A\cup B)$，根据补集的定义，$x\notin A\cup B$[①]，因此，$x\notin A$，$x\notin B$，亦即 $x\in\sim A$，$x\in\sim B$，由此可知 $x\in\sim A\cap\sim B$. 从而

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

反之，$\forall x\in\sim A\cap\sim B$，根据交集的定义，$x\in\sim A$，$x\in\sim B$，即 $x\notin A$，$x\notin B$，于是，$x\notin A\cup B$，亦即 $x\in\sim(A\cup B)$.

从而　　$\sim A\cap\sim B\subseteq\sim(A\cup B)$

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

定理中的结论（3）说明，在 $(A\cup B)\cup C$ 与 $(A\cap B)\cap C$ 中，可以省去括号写成 $A\cup B\cup C$，$A\cap B\cap C$ 而不会引起混乱. 一般地，可以用归纳法证明，对集合 A_1，A_2，…，A_n 按任意组合方式进行求并（或交）运算所得的结果总是相同的，因此，符号 $A_1\cup A_2\cup\cdots\cup A_n$ 与 $A_1\cap A_2\cap\cdots\cap A_n$ 是有意义的.

设 J 是一个非空集合，对于 J 的每个元素 a，我们都唯一给定一个集合 A_a（对不同的 a，相应的 A_a 可能相同），则所有这些 A_a 构成一个集合族，这个集合族可记为 $A=\{A_a|a\in J\}$. 其中 J 称为指标集. 当 $J=\{1,2,\cdots,n\}$ 时，$A=\{A_1,A_2,\cdots,A_n\}$. 当 $J=\{1,2,3,\cdots\}$ 时，$A=\{A_1,A_2,\cdots\}$，这时，称 A 的元素 A_1，A_2，A_3，……为一列集.

利用以上集合族的记法，集合并、交运算的概念很容易推广到任意多个集合的情形.

定义 6　设 $A=\{A_i\mid i\in J\}$ 是一个集合族，至少属于 $A_i\,(i\in J)$ 之一的元素构成的集合称为所有 A_i（$i\in J$）的并，记为 $\bigcup\limits_{i\in J}A_i$，即

$$\bigcup_{i\in J}A_i=\{x|\exists i\in J\text{使}x\in A_i\}$$

当 $J=\{1,2,\cdots,n\}$ 时，$\bigcup\limits_{i\in J}A_i$ 常记为 $\bigcup\limits_{i=1}^{n}A_i$，当 $J=\{1,2,\cdots\}$ 时，$\bigcup\limits_{i\in J}A_i$ 常记为 $\bigcup\limits_{i=1}^{\infty}A_i$.

[①]因为 $x\in U$ 总是成立的，所以在讨论问题时，通常将“$x\in U$”的叙述略去. 下同.

根据以上定义容易证明

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

从而，$\bigcup_{i=1}^{n} A_i = A_1 \cup A_2 \cup \cdots\cdots \cup A_n$. 仿此，也记 $\bigcup_{i=1}^{\infty} A_i = A_1 \cup A_2 \cup A_3 \cup \cdots\cdots$.

定义 7　设 $A=\{ A_i \mid i \in J \}$ 是一个集合族，属于每一个 $A_i (i \in J)$ 的元素构成的集合称为所有 $A_i (i \in J)$ 的交，记为 $\bigcap_{i \in J} A_i$，即

$$\bigcap_{i \in J} A_i = \{x \mid x \in A_i, \forall i \in J\}$$

当 $J=\{1, 2, \cdots, n\}$ 时，$\bigcap_{i \in J} A_i$ 常记为 $\bigcap_{i=1}^{n} A_i$，当 $J=\{1, 2, \cdots\}$ 时，$\bigcap_{i \in J} A_i$ 常记为 $\bigcap_{i=1}^{\infty} A_i$.

与并集的情况类似地，有

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

从而 $\bigcap_{i=1}^{n} A_i = A_1 \cap A_2 \cap \cdots\cdots \cap A_n$，　并记 $\bigcap_{i=1}^{\infty} A_i = A_1 \cap A_2 \cap A_3 \cdots\cdots$.

定理 1 中的许多性质，可以推广到任意多个集合的情况.

定理 2　设 $A=\{ A_i \mid i \in J \}$ 是一个集合族，B 是一个集合，则

（1）　$B \cap (\bigcup_{i \in J} A_i) = \bigcup_{i \in J} (B \cap A_i)$

$B \cup (\bigcap_{i \in J} A_i) = \bigcap_{i \in J} (B \cup A_i)$

（2）　$\sim \bigcup_{i \in J} A_i = \bigcap_{i \in J} \sim A_i$

$\sim \bigcap_{i \in J} A_i = \bigcup_{i \in J} \sim A_i$

证明　先证（1）中的第一式：$B\cap(\bigcup_{i\in J}A_i)=\bigcup_{i\in J}(B\cap A_i)$

$\forall x\in B\cap(\bigcup_{i\in J}A_i)$，则 $x\in B$，　$x\in\bigcup_{i\in J}A_i$，由 $x\in\bigcup_{i\in J}A_i$ 知，$\exists i_0\in J$ 使 $x\in A_{i_0}$　再由 $x\in B$ 得，$x\in B\cap A_{i_0}$，所以　$x\in\bigcup_{i\in J}(B\cap A_i)$，

因此　$B\cap(\bigcup_{i\in J}A_i)\subseteq\bigcup_{i\in J}(B\cap A_i)$.

反之，$\forall x\in\bigcup_{i\in J}(B\cap A_i)$，$\exists i_0\in J$ 使 $x\in B\cap A_{i_0}$，于是 $x\in B$，　$x\in A_{i_0}$，从而 $x\in\bigcup_{i\in J}A_i$，$x\in B\cap(\bigcup_{i\in J}A_i)$.

因此　$\bigcup_{i\in J}(B\cap A_i)\subseteq B\cap(\bigcup_{i\in J}A_i)$.

总之，$B\cap(\bigcup_{i\in J}A_i)=\bigcup_{i\in J}(B\cap A_i)$.

（1）中第二式类似可证.

再证（2）中第一式：$\sim\bigcup_{i\in J}A_i=\bigcap_{i\in J}\sim A_i$

$\forall x\in\sim\bigcup_{i\in J}A_i$，$x\notin\bigcup_{i\in J}A_i$，故对任意 $i\in J$，$x\notin A_i$，即 $x\in\sim A_i$，　$\forall i\in J$.　因此 $x\in\bigcap_{i\in J}\sim A_i$.所以，$\sim\bigcup_{i\in J}A_i\subseteq\bigcap_{i\in J}\sim A_i$.

反之，$\forall x\in\bigcap_{i\in J}\sim A_i$，则 $x\in\sim A_i$，　$\forall i\in J$. 即 $x\notin A_i$，　$\forall i\in J$. 所以 $x\notin\bigcup_{i\in J}A_i$，于是 x $\in\sim\bigcup_{i\in J}A_i$，因此，$\bigcap_{i\in J}\sim A_i\subseteq\sim\bigcup_{i\in J}A_i$.

总之，$\sim\bigcup_{i\in J}A_i=\bigcap_{i\in J}\sim A_i$.

（2）中的第二式类似可证.　▌

在讨论了上面各种常用的集合运算之后，我们再来引进一种新的运算.

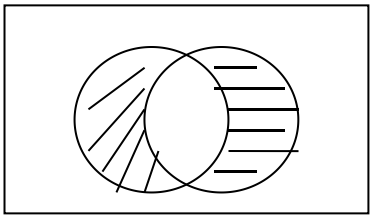
定义 8　设 A，B 为两个集合，A 与 B 的对称差 $A\oplus B$ 定义如下

$$A\oplus B=（A-B）\cup（B-A）$$

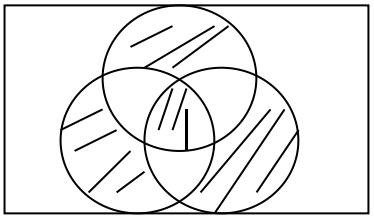
例如，设 $A=\{\{a\}，b，\{b\}，c\}$，$B=\{a，b，c\}$

则　　$A\oplus B=\{\{a\}，\{b\}，a\}$

$A\oplus B$ 与 $（A\oplus B）\oplus C$ 的 venn 图如下图所示.



$A\oplus B$



$(A\oplus B)\oplus C$

定理 3　设 A，B 为两个集合，则

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

证明留作习题. ▌

定理 4　设 A，B，C 是三个集合，则

（1）　$A\oplus A=\varnothing$

（2）　$A\oplus B=B\oplus A$

（3）　$(A\oplus B)\oplus C=A\oplus(B\oplus C)$

证明　（1）、（2）式是显然的，现考虑（3）式. 根据定理 3，我们有

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

而
$$(A\oplus B)\cap\sim C=[(A\cap\sim B)\cup(\sim A\cap B)]\cap\sim C$$
$$=(A\cap\sim B\cap\sim C)\cup(\sim A\cap B\cap\sim C)$$
$$\sim(A\oplus B)\cap C=\sim[(A\cap\sim B)\cup(\sim A\cap B)]\cap C$$
$$=[(\sim A\cup B)\cap(A\cup\sim B)]\cap C$$
$$=[(\sim A\cap\sim B)\cup(B\cap A)]\cap C$$
$$=(\sim A\cap\sim B\cap C)\cup(A\cap B\cap C)$$

因此，
$$(A\oplus B)\oplus C=(A\cap\sim B\cap\sim C)\cup(\sim A\cap B\cap\sim C)$$
$$\cup(\sim A\cap\sim B\cap C)\cup(A\cap B\cap C)$$

又，
$$A\oplus(B\oplus C)=(B\oplus C)\oplus A$$
$$=(B\cap\sim C\cap\sim A)\cup(\sim B\cap C\cap\sim A)$$
$$\cup(\sim B\cap\sim C\cap A)\cup(B\cap C\cap A)$$

从而
$$A\oplus(B\oplus C)=A\oplus(B\oplus C)$$

习题三

1．设 A，B，C 为全集 U 的子集，设 $A\cap B=A\cap C$，　$\sim A\cap B=\sim A\cap C$，证明 $B=C$.

2．设 $A=\{a,\ b,\ \{a,\ b\},\ \varnothing\}$，试求

（1）$A-\{a,\ b\}$；　（2）$A-\varnothing$ ；（3）$A-\{\varnothing\}$；

（4）$\{\{a,\ b\}\}-A$；（5）$\varnothing-A$；（6）$\{\varnothing\}-A$.

3．设 A，B，C 为任意集合，试用集合运算性质证明下列各式.

（1）$(A-B)-C=A-(B\cup C)$.

（2）$(A-B)-C=(A-C)-B$.

（3）$(A-B)-C=(A-C)-(B-C)$.

4．设 A，B 是两个集合

（1）若 $A-B=B$，则 A 与 B 有什么关系？

（2）若 $A-B=B-A$，则 A 与 B 有什么关系？

5. 设 $A=\{A_i\mid i\in J\}$ 是一个集合族，其中，$J=\{1,2,\cdots,n\}$，证明 $\bigcup\limits_{i=1}^{n}A_i=(\bigcup\limits_{i=1}^{n-1}A_i)\cup A_n$.

6．证明定理 3.

7．设 A，B，C 为任意集合，证明

（1）若 $A\subseteq B$，则 $A\cup B=B$，$A\cap B=A$.

（2）若 $A\subseteq$ B，则 $\sim B\subseteq\sim A$.

§ 4　有序 n 元组与笛卡尔积

在一个集合中，元素之间是没有先后次序的，比如 $\{a,\ b\}=\{b,\ a\}$，但有时元素之间的次序是重要的，必须给予区别．因此我们下面引入“有序对”的概念．通俗地说，两个有先后次序的事物构成的整体称为一个有序对，a 在先、 b 在后构成的有序对记为 $\langle a,\ b\rangle$[①]，a 称为该有序对的第一元素（第一分量），b 称为该有序对的第二元素（第二分量）．例如，平面上点的坐标（x，y）就是一个实数有序对．一般说来 $\langle a,\ b\rangle\neq\langle b,\ a\rangle$.

定义 1　两个有序对 $\langle x,\ y\rangle$ 与 $\langle u,\ v\rangle$，当其元素依次对应相等时，我们称这两个有序对相等，记为 $\langle x,\ y\rangle=\langle u,\ v\rangle$，即

$$\langle x,\ y\rangle=\langle u,\ v\rangle\Leftrightarrow x=u,\ y=v$$

一般地，n 个有确定次序的事物构成的整体称为一个有序 n 元组，事物 $a_1,a_2,\cdots,a_n$

[①] $\langle a,\ b\rangle$ 的形式定义为：$\langle a,\ b\rangle=\{a,\{a,b\}\}$.

组成的有序 n 元组记为〈$a_1,a_2,\cdots,a_n$〉，其中，$a_i(1\le i\le n)$ 称为第 i 个元素（或第 i 个分量）.

定义 2　两个有序 n 元组〈$a_1,a_2,\cdots,a_n$〉与〈$b_1,b_2,\cdots,b_n$〉，当其元素依次对应相等时，称这两个有序 n 元组相等，记为〈$a_1,a_2,\cdots,a_n$〉＝〈$b_1,b_2,\cdots,b_n$〉，即

$$\langle a_1,a_2,\cdots,a_n\rangle=\langle b_1,b_2,\cdots,b_n\rangle \Leftrightarrow a_1=b_1,\cdots,a_n=b_n$$

利用以上有序对及有序 n 元组的概念，我们可以定义一种新的集合运算——笛卡尔积.

定义 3　设 A，B 为两个集合，集合

$$A\times B=\{\langle x,y\rangle \mid x\in A,y\in B\}$$

称为 A 与 B 的笛卡尔积.

例如，设 $A=\{a,b\}$，$B=\{1,2\}$，$C=\{a\}$，则

$A\times B=\{\langle a,1\rangle,\langle a,2\rangle,\langle b,1\rangle,\langle b,2\rangle\}$

$B\times A=\{\langle 1,a\rangle,\langle 2,a\rangle,\langle 1,b\rangle,\langle 2,b\rangle\}$

$(A\times B)\times C=\{\langle\langle a,1\rangle,a\rangle,\langle\langle a,2\rangle,a\rangle,\langle\langle b,1\rangle,a\rangle,\langle\langle b,2\rangle,a\rangle\}$

$A\times(B\times C)=\{\langle a,\langle 1,a\rangle\rangle,\langle a,\langle 2,a\rangle\rangle,\langle b,\langle 1,a\rangle\rangle,\langle b,\langle 2,a\rangle\rangle\}$

$A\times\varnothing=\varnothing$

$A\times\{\varnothing\}=\{\langle a,\varnothing\rangle,\langle b,\varnothing\rangle\}$

由以上例子不难看出，笛卡尔积不满足交换律，不满足结合律，但我们有

定理 1　设 A，B，C 为三个集合，则有

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

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

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

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

证明

（1）$\forall\langle x,y\rangle\in A\times(B\cup C)$，则 $x\in A$，$y\in B\cup C$，因此，$y\in B$ 或 $y\in C$，若 $y\in B$ 则 $\langle x,y\rangle\in A\times B$，若 $y\in C$，则 $\langle x,y\rangle\in A\times C$，总之，不论何种情况均有 $\langle x,y\rangle\in(A\times B)\cup(A\times C)$，所以 $A\times(B\cup C)\subseteq(A\times B)\cup(A\times C)$.

反之，$\forall\langle x,y\rangle\in(A\times B)\cup(A\times C)$，则 $\langle x,y\rangle\in A\times B$ 或 $\langle x,y\rangle\in A\times C$，若 $\langle x,y\rangle\in A\times B$，则 $x\in A$，$y\in B$，即知 $y\in B\cup C$，从而 $\langle x,y\rangle\in A\times(B\cup C)$. 同理可证，当 $\langle x,y\rangle\in A\times C$ 时也有 $\langle x,y\rangle\in A\times(B\cup C)$. 因此 $(A\times B)\cup(A\times C)\subseteq A\times(B\cup C)$.

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

（2）$\forall\langle x,y\rangle\in A\times(B\cap C)$，则 $x\in A$，$y\in B\cap C$，因此 $y\in B$，$y\in C$，故有

$\langle x, y\rangle \in A\times B$，$\langle x, y\rangle \in A\times C$，所以 $\langle x, y\rangle \in (A\times B)\cap(A\times C)$. 即知 $A\times(B\cap C)\subseteq(A\times B)\cap(A\times C)$.

反之，$\forall\ \langle x, y\rangle \in (A\times B)\cap(A\times C)$，则 $\langle x, y\rangle \in A\times B$ 且 $\langle x, y\rangle \in A\times C$，因此 $x\in A$，$y\in B$，$y\in C$，所以 $y\in B\cap C$，从而 $\langle x, y\rangle \in A\times(B\cap C)$，故知 $(A\times B)\cap(A\times C)\subseteq A\times(B\cap C)$

总之，$A\times(B\cap C)=(A\times B)\cap(A\times C)$.

（3），（4）的证明完全类似，略. ▌

利用有序 n 元组的概念，类似可定义多个集合的笛卡尔积.

定义 4　设 $A_1, A_2, \cdots, A_n$ 为 n 个集合，集合

$$A_1\times A_2\times\cdots\times A_n=\{<a_1, a_2, \cdots, a_n>\mid a_i\in A_i, i=1,2,\cdots,n\}$$

称为 $A_1, A_2, \cdots, A_n$ 的笛卡尔积.

例如，设 $A=\{a_1, a_2\}$，$B=\{b\}$，$C=\{c\}$，

则　$A\times B\times C=\{\langle a_1, b, c\rangle, \langle a_2, b, c\rangle\}$

$B\times A\times C=\{\langle b, a_1, c\rangle, \langle b, a_2, c\rangle\}$

对任意集合 A，　$A\times A\times\cdots\times A$（$n$ 个）常记为 A^n.

定理 2　设 $A_1, A_2, \cdots, A_n$ 是有限集，则

$$|A_1\times A_2\times\cdots\times A_n|=|A_1|\cdot|A_2|\cdots|A_n|$$

证明　$a_1\in A_1$ 有 $|A_1|$ 种选取方式，$a_2\in A_2$ 有 $|A_2|$ 种选取方式，……，$a_n\in A_n$ 有 $|A_n|$ 种选取方式，因此，利用乘法法则，有序 n 元组 $\langle a_1, a_2, \cdots, a_n\rangle$（其中 $a_n\in A_i$）共有 $|A_1|\cdot|A_2|\cdots|A_n|$ 种选取方式，即

$$|A_1\times A_2\times\cdots\times A_n|=|A_1|\cdot|A_2|\cdots|A_n|$$ ▌

习题四

1．设 $A=\{0, 1\}$，$B=\{1, 2\}$，求 $A\times B$，$B\times A$，$\varnothing\times A$，$A\times\varnothing$.

2．设 $A=\{a, b\}$，求 $P(A)\times A$.

3．证明 $A\times B=\varnothing \Leftrightarrow A=\varnothing$ 或 $B=\varnothing$.

4．已知 $A\times B=C\times D$，是否一定有 $A=C$ ？说明理由.

§5　多重集

在集合的概念中，我们要求集合元素是互不相同的，即是说任意两个元素都是可以相互区别的，同一个符号只能表示一个元素，这样，{a，a，b} = {a，b} 是具有两个元素的集合．但是，在许多问题中，对某些具有同样特征的事物不加区别更为方便．例如，设有 3 个红球、2 个白球和 1 个黑球，将这 6 个球放入袋中，由 6 个人来摸，摸着红球的上山，摸着白球的下海，摸着黑球的看家，这时红球之间、白球之间是毫无差别的，不需要区分．一般地，如果有一组事物，其中可以有某些事物不加区别（或说某些事物可重复出现多次，且出现几次就看作是几个事物），这组事物构成的整体就称为一个多重集．

例如，事物 a，a，b 构成一个多重集 {a，a，b}，该多重集中有 3 个元素，其中 a 出现 2 次．又如，3 个红球、2 个白球和 1 个黑球构成一个多重集 {红球，红球，红球，白球，白球，黑球}，该多重集有 6 个元素．为方便，{a，a，b} 可记为 {2•a，b}，{红球，红球，红球，白球，白球，黑球} 可记为 {3•红球，2•白球，黑球}，{b，b，b，a，a，…} 可记为 {3•b，∞•a} 等等．在一个多重集 A 中，元素 a 出现的次数（既可以是正整数，也可以是∞或 0）称为 a 在 A 中的重复度，记为 $M_A(a)$．例如，令 A = {b，b，c，a，a，…}，则 $M_A(a)=\infty$，$M_A(b)=2$，$M_A(c)=1$，$M_A(d)=0$．显然，一个多重集 A，如果任何事物在 A 中的重复度只能为 1 和 0，则该多重集就是一个通常意义下的集合．

定义 1　设 A，B 是两个多重集，A 与 B 的并 $A\cup B$ 是一个多重集，使得任一元素在 $A\cup B$ 中的重复度等于该元素在 A，B 中重复度的最大值，即

$$M_{A\cup B}(x)=\max\{M_A(x),\ M_B(x)\}$$

例如，设 A = {a，a，a，c，d，d}，B = {a，a，b，c，c}，则

$$\mathrm{A}\cup\mathrm{B}=\{a,\ a,\ a,\ b,\ c,\ c,\ d,\ d\}$$

定义 2　设 A，B 是两个多重集，A 与 B 的交 $A\cap B$ 是一个多重集，使得任一元素在 $A\cap B$ 中的重复度等于该元素在 A，B 中重复度的最小值，即

$$M_{A\cap B}(x)=\min\{M_A(x),\ M_B(x)\}$$

例如，对于 A = {a，a，a，c，d，d}　B = {a，a，b，c，c}，

$$A\cap B=\{a,\ a,\ c\}$$

为了定义多重集的差，先引入如下“非负差”运算：设 m，n 是两个整数，m 与 n 的“非负差” $m\dot{-}n$ 定义如下：

$$m \dot{-} n = \begin{cases} m-n, & m \geq n \\ 0, & m < n \end{cases}$$

定义 3　设 A，B 是两个多重集，A 与 B 的差 $A-B$ 是一个多重集，使得任一元素在 $A-B$ 中的重复度等于该元素在 A 中重复度与其在 B 中重复度的非负差，即

$$M_{A-B}(x) = M_A(x) \dot{-} M_B(x)$$

例如，设 $A=\{a, a, a, b, b, c, d, d, e\}$，$B=\{a, a, b, b, b, c, c, d, d, f\}$，则

$$A-B=\{a, e\}$$

最后，我们引入两个多重集的和，这个概念在通常的集合运算中是没有的.

定义 4　设 A，B 是两个多重集，A 与 B 的和 $A+B$ 是一个多重集，使得任一元素在 $A+B$ 中的重复度等于该元素在 A，B 中重复度的和，即

$$M_{A+B}(x) = M_A(x) + M_B(x)$$

例如，设 $A=\{a, a, b, c, c\}$，$B=\{a, b, b, d\}$

则　　$A+B=\{a, a, a, b, b, b, c, c, d\}$

习题五

1．设 $A=\{\infty \cdot a, 4 \cdot b, c, 2 \cdot d\}$，$B=\{3 \cdot a, 2 \cdot b, 4 \cdot c, d\}$

求　$A \cup B$，$A \cap B$，$A-B$，$A+B$.

第二章　关　　系

§1　关系的概念

不论在日常生活中或在数学中，我们都经常遇到“关系”这个概念，如父子关系，同学关系，等于关系，小于关系，属于关系，函数关系等等．本节将给关系概念建立一个数学定义．为了启发，先看两个例子．

设有 A，B 两个男人和 x，y，z 三个男孩，其中 A 是 x，y 的父亲，B 是 z 的父亲，为了表示这五人之间的父子关系，我们按父在先子在后的次序将 A，B 与 x，y，z 配对，从而得到三个有序对 $\langle A, x\rangle$，$\langle A, y\rangle$，$\langle B, z\rangle$．这三个有序对作为一个整体构成一个集合 FS.

$$FS=\{\langle A, x\rangle, \langle A, y\rangle, \langle B, z\rangle\}$$

于是，A，B，x，y，z 五人间的父子关系完全由有序对集合 FS 刻划：

$$u, w \text{ 满足父子关系} \Leftrightarrow \langle u, w\rangle \in FS$$

我们不考虑关系的内涵或语义，就将“这五人之间父子关系”抽象为集合 FS.

以下是关系的数学定义．

定义 1　一个有序对的集合 R 称为一个二元关系，简称关系．当 $R\subseteq A\times B$ 时，称 R 为 A 到 B 的关系，当 $R\subseteq A\times A$ 时，称 R 为 A 上的关系．

对任意关系 R，若 $\langle x, y\rangle \in R$，称 x，y 具有关系 R（或 x，y 满足关系 R），记为 xRy；若 $\langle x, y\rangle \notin R$，称 x，y 不具有关系 R（或 x，y 不满足关系 R），记为 $x\not R y$.

例如，$R_1=\{\langle x, y\rangle \mid x, y \text{ 是人且 } x \text{ 是 } y \text{ 的父亲}\}$

$$R_2=\{\langle x, y\rangle \mid x, y\in \mathbf{Z},\ \exists k\in \mathbf{N}^+ \text{ 使 } x=y+k\}$$

$$R_3=\{\langle A, B\rangle \mid A, B \text{ 是集合}, x\in A\Rightarrow x\in B\}$$

R_1，R_2，R_3 均是有序对集合即关系，可分别理解为人类的父子关系，整数集上的大于关系，全集的幂集 $P(\mathrm{U})$上的包含关系．

定义 2　设 R 为 A 到 B 的关系，R 中所有有序对的第一元素构成的集合称为该关系的定义域，记为 $\mathrm{dom}R$，即

$$\mathrm{dom}R=\{x\mid \exists y\in B \text{，使 } \langle x, y\rangle \in R\}$$

R 中所有有序对的第二元素构成的集合称为该关系的值域，记为 ran$R$，即

$$\text{ran}R=\{y\mid \exists x\in A \text{ 使 } \langle x,y\rangle \in R\}$$

例 1　设 $S=\{\langle 1,2\rangle,\langle 3,3\rangle,\langle 3,4\rangle\}$，则 dom$S=\{1,3\}$ ran$S=\{2,3,4\}$.

设 $S=\{\langle x,x^2\rangle \mid x\in\mathbf{R}\}$，$\mathbf{R}$ 为实数集，则 dom$S=\mathbf{R}$，ran$S=\{x\mid x\in\mathbf{R},x\geqslant 0\}$

关系作为一个有序对的集合，可以进行集合的各种运算.

例 2　设 $A=\{1,2,\cdots,6\}$，L 表示 A 上的小于等于关系，

$L=\{\langle x,y\rangle \mid x,y\in A,x\leqslant y\}$，$D$ 表示 A 上的平方关系，

$D=\{\langle x,y\rangle \mid x,y\in A,y=x^2\}$，则

$$\begin{aligned}L=\{&\langle 1,1\rangle,\langle 1,2\rangle,\langle 1,3\rangle,\langle 1,4\rangle,\langle 1,5\rangle,\langle 1,6\rangle,\\&\langle 2,2\rangle,\langle 2,3\rangle,\langle 2,4\rangle,\langle 2,5\rangle,\langle 2,6\rangle,\\&\langle 3,3\rangle,\langle 3,4\rangle,\langle 3,5\rangle,\langle 3,6\rangle,\\&\langle 4,4\rangle,\langle 4,5\rangle,\langle 4,6\rangle,\\&\langle 5,5\rangle,\langle 5,6\rangle,\\&\langle 6,6\rangle\}\end{aligned}$$

$$D=\{\langle 1,1\rangle,\langle 2,4\rangle\}$$

$$L\cup D=L,\quad L\cap D=D,$$

$$\begin{aligned}L-D&=\{\langle x,y\rangle \mid x,y\in A,x\leqslant y,y\neq x^2\}\\&=\{\quad\langle 1,2\rangle,\langle 1,3\rangle,\langle 1,4\rangle,\langle 1,5\rangle,\langle 1,6\rangle,\\&\quad\langle 2,2\rangle,\langle 2,3\rangle,\quad\langle 2,5\rangle,\langle 2,6\rangle,\\&\quad\langle 3,3\rangle,\langle 3,4\rangle,\langle 3,5\rangle,\langle 3,6\rangle,\\&\quad\langle 4,4\rangle,\langle 4,5\rangle,\langle 4,6\rangle,\\&\quad\langle 5,5\rangle,\langle 5,6\rangle,\\&\quad\langle 6,6\rangle\}\end{aligned}$$

定义 3　设 A 是任意集合，令

$$I_A=\{\langle x,x\rangle \mid x\in A\}$$

称 I_A 为 A 上的恒等（相等）关系，当不引起混乱时，I_A 也简记为 I.

我们已经知道，A 到 B 的关系 R 是 $A\times B$ 的一个子集，在 A，B 都是有限集的情况下，为了表达的直观或处理的方便，有时利用图形或矩阵来表示关系.

首先，考虑关系的图形表示，分两种情形讨论.

（一）R 是 A 上的关系，$A=\{a_1,a_2,\cdots,a_n\}$. A 的每个元素 a_i 用圆点表示，称为顶

点 a_i，当 $a_i R a_j$ 时，画一条自 a_i 到 a_j 的有向弧，特别地，当 $a_i R a_i$ 时，画一条从 a_i 出发回到 a_i 的封闭弧，该弧称为自环．这样得到的图形称为 R 的关系图．

例 3　设 $A=\{1, 2, 3, 4, 5\}$，R 是 A 上的关系，$R=\{\langle 1,1\rangle, \langle 2,2\rangle, \langle 2,1\rangle, \langle 1,2\rangle, \langle 2,3\rangle, \langle 4,5\rangle, \langle 5,5\rangle, \langle 5,4\rangle\}$，则 R 的关系图如图 1.1

（二）R 是 A 到 B 的关系，　其中，A，B 是两个有限集，$A=\{a_1, a_2, \cdots, a_m\}$，$B=\{b_1, b_2, \cdots, b_n\}$，用圆点表示 A，B 的元素，并分别画在平面上，当 $a_i R b_j$ 时，做一条自 a_i 向 b_j 的有向弧，这样得到的图也称为 R 的关系图．

例 4　设 $A=\{1, 2, 3\}$，$B=\{a, b\}$，R 是 A 到 B 的关系，$R=\{\langle 1, a\rangle, \langle 1, b\rangle, \langle 2, a\rangle, \langle 3, b\rangle\}$，则 R 的关系图如图 1.2

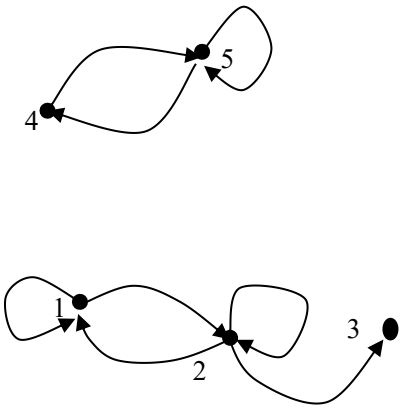


图 1.1

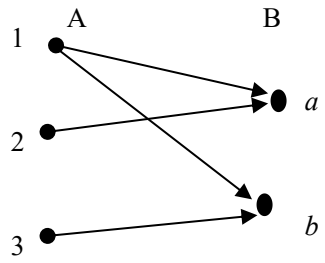


图 1.2

例 5　设 $A=\{a, b, c, d\}$，R 为 A 上的关系，$R=\{\langle a, a\rangle, \langle a, b\rangle, \langle b, a\rangle, \langle c, c\rangle\}$，则 R 的关系图为如图 1.3.

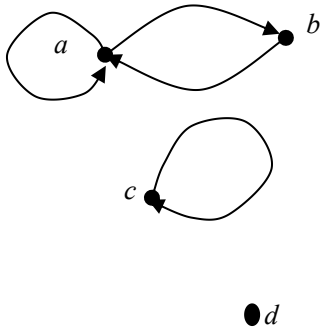


图 1.3

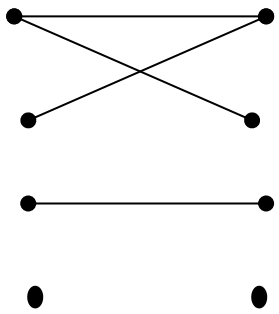


图 1.4

当然，R 也可看成是 A 到 A (即 A 上) 的关系，按第二种情形处理，这时，R 的关系图如图 1.4 所示.

今后如无特别说明，集合 A 上关系 R 的关系图总是指第一种形式的关系图.

现在再来讨论关系矩阵.

先看一个例子.

设 $A=\{1, 2, 3\}$，$B=\{a, b, c, d\}$，R 是 A 到 B 的关系，

$R=\{\langle 1, a\rangle, \langle 1, b\rangle, \langle 2, a\rangle, \langle 2, d\rangle, \langle 3, b\rangle\}$，则 R 可用下表表示：

	a	b	c	d
1	∨	∨		
2	∨			∨
3		∨		

该表可抽象为如下矩阵：

$$\begin{pmatrix} 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \end{pmatrix}$$

一般地，设 $A=\{a_1, a_2, \cdots, a_m\}$，$B=\{b_1, b_2, \cdots, b_n\}$ 是两个有限集，R 是 A 到 B

的关系，R 的关系矩阵 M_R 是一个 $m\times n$ 矩阵，

$$M_R=(r_{ij})_{m\times n}，\text{其中 } r_{ij}=\begin{cases}0, & x_i\not R y_j\\ 1, & x_iRy_j\end{cases}\quad i=1,2,\cdots,m\qquad j=1,2,\cdots,n$$

例 6　设 $A=\{a，b，c\}$，$B=\{1，2，3，4\}$，R 是 A 到 B 的关系，$R=\{\langle a，1\rangle，\langle a，2\rangle，\langle a，4\rangle，\langle b，3\rangle，\langle b，4\rangle\}$ 则 R 的关系矩阵 M_R 为

$$M_R=\begin{array}{c}\\ a\\ b\\ c\end{array}\begin{array}{c}\begin{array}{cccc}1 & 2 & 3 & 4\end{array}\\ \begin{pmatrix}1 & 1 & 0 & 1\\ 0 & 0 & 1 & 1\\ 0 & 0 & 0 & 0\end{pmatrix}\end{array}$$

习题一

1．设 $R_1=\{\langle x^2，x\rangle\mid x\in\mathbf{R}\}$，$R_2=\{\langle x，x^2\rangle\mid x\in\mathbf{R}\}$，$R_1$，$R_2$ 的定义域、值域各是什么？

2．设 $|A|=n$，A 上共有多少个不同的关系？

3．设 $S=\{\langle\langle x，y\rangle，\langle u，w\rangle\rangle\mid x，y，u，w\in\mathbf{N}，(x-u)^2+(y-w)^2\leqslant 25\}$　问 S 是否是关系？若是，S 是哪个集合到哪个集合的关系？

4．设 $A=\{a，b，c\}$，$B=\{a，b，c，d，e\}$，$S=\{\langle a，a\rangle，\langle a，b\rangle，\langle c，d\rangle，\langle b，d\rangle\}$ 是 A 到 B 的关系，写出 S 的关系矩阵，并画出其关系图.

5．设 $A=\{a，b，c，d，e\}$，$S=\{\langle a，a\rangle，\langle a，b\rangle，\langle c，d\rangle，\langle b，d\rangle\}$ 是 A 上的关系，写出 S 的关系矩阵并画出其关系图.

§2　关系性质

在本节中，只讨论任意集合 A 上的关系，我们先给出以下定义.

定义 1　设 R 是 A 上的关系.

（1）　如果对任意 $x\in A$，均有 xRx，则称 R 是自反的.

（2）　如果当 xRy 时，必有 yRx，则称 R 是对称的.

（3）　如果当 xRy，yRz 时，必有 xRz，则称 R 是传递的.

（4）　如果对任意 $x\in A$，均有 $x\not R x$，则称 R 是反自反的.

（5） 如果当 xRy，yRx 时，必有 $x=y$，则称 R 是反对称的.

例如，实数集上的“小于等于”关系是自反的、传递的、反对称的；平面上三角形的“全等”关系是自反的、对称的、传递的.

例 1 设 $A=\{1,2,3,4\}$，R_1，R_2，R_3，R_4 是 A 上的关系，

$R_1=\{\langle 1,1\rangle,\langle 2,2\rangle,\langle 2,3\rangle,\langle 3,2\rangle,\langle 4,4\rangle\}$

$R_2=\{\langle 1,2\rangle,\langle 4,1\rangle,\langle 4,2\rangle\}$

$R_3=\{\langle 1,2\rangle,\langle 2,3\rangle,\langle 1,3\rangle,\langle 3,4\rangle\}$

$R_4=\{\langle 1,1\rangle,\langle 2,2\rangle,\langle 3,3\rangle,\langle 4,4\rangle\}$

我们指出以上关系所具有的性质. R_1 是对称的，R_2 是传递的、反对称的、反自反的，R_3 是反对称的、反自反的，R_4 是自反的、对称的、传递的、反对称的.

在上节我们已经看到，有限集上的关系可以用关系图和关系矩阵表示，这时关系的各个性质必然会反映到关系图和关系矩阵上来，不难看出以下结论.

（1） 关系 R 是自反的 $\Leftrightarrow$ 关系图上每一点都有一自环 $\Leftrightarrow$ 关系矩阵对角元全为 1 .

（2） 关系 R 是对称的 $\Leftrightarrow$ 关系图中不同顶点间的弧线成对出现，其中一条弧的起、终点分别为另一条弧的终、起点 $\Leftrightarrow$ 关系矩阵是对称的.

（3） 关系 R 为反自反的 $\Leftrightarrow$ 关系图中不存在自环 $\Leftrightarrow$ 关系矩阵中对角元全为零.

（4） 关系 R 为反对称的 $\Leftrightarrow$ 关系图中任意两点间至多有一条弧 $\Leftrightarrow$ 关系矩阵中关于对角线的对称元不同时为 1

例 2 设 R 是 $\{1,2,3,4\}$ 上的关系，

其关系矩阵如下

$$\begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \end{pmatrix} 1$$

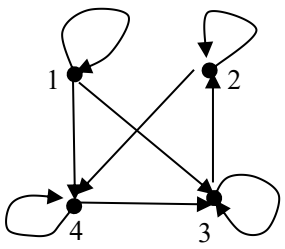


图 2.1

则由关系矩阵不难画出其关系图（图 2.1）.

由关系图和关系矩阵均可看出，R 是自反的、反对称的，但不是对称的和反自反的. 又从关系图中不难发现，$4R3$，$3R2$ 但 $4\not R2$，故 R 不是传递的.

习题二

1．设 $A=\{1,2,3,4\}$，R 是 A 上的关系，指出关系 R 的性质.

（1） $R=\{\langle 1,1\rangle,\langle 2,2\rangle\}$

（2） $R=\{\langle 1,2\rangle,\langle 2,1\rangle,\langle 1,1\rangle,\langle 3,1\rangle,\langle 1,3\rangle\}$

（3） $R=\{\langle 1,2\rangle,\langle 3,4\rangle\}$

（4） $R=\{\langle 1,2\rangle,\langle 2,1\rangle,\langle 1,1\rangle,\langle 2,2\rangle,\langle 3,3\rangle,\langle 4,4\rangle\}$

2．设 $A=\{1,2,3,4\}$，求出一个 A 上的关系 R，使

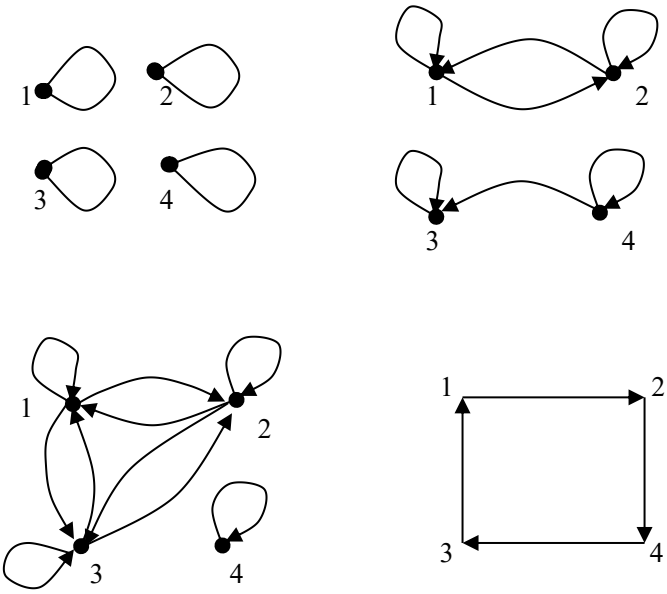
（1） R 既是对称的又是反对称的.

（2） R 既不是对称的，又不是反对称的.

（3） R 是传递的.

（4） R 既不是自反的又不是反自反的.

3．设 $A=\{1,2,3,4\}$，A 上关系 R 由如下关系图确定，问 R 具有哪些性质？



4．设 R 是 A 上的非空关系，证明：如果 R 是反自反的、对称的，则必不是传递的.

§3　复合关系与逆关系

关系作为有序对的集合可以进行集合的并、交、差等各种运算，现在我们再引进一种对关系来说更为重要的运算——关系的复合.

设 R，S 是两个关系，xRy，ySz，则通过元素 y，x 与 z 之间便产生了某种关系，x 与 z 所具有的这种关系就称为 R 与 S 的复合关系.

定义 1　设 R 是从 A 到 B 的关系，S 是从 B 到 C 的关系，如下 A 到 C 的关系

$\{\langle a,c\rangle \mid a\in A,\ c\in C,\ \exists b\in B$ 使 $\langle a,b\rangle\in R,\langle b,c\rangle\in S\}$

称为 R 与 S 的复合（关系），记为 $R\circ S$. 由 R, S 求出 $R\circ S$ 的过程称为关系的复合.

例如，若 MS 是“母子关系”，$MS=\{\langle x, y\rangle \mid x$ 是 y 的母亲，y 是男性$\}$，HW 是“夫妻关系”，$HW=\{\langle x, y\rangle \mid x$ 是 y 的丈夫$\}$，则 $MS\circ HW=\{\langle x, z\rangle \mid \exists y$ 使 $\langle x, y\rangle \in MS$，$\langle y, z\rangle \in HW\}$ 是“婆媳关系”.

例 1　设 R，S 均为 $A=\{1, 2, 3, 4\}$ 上的关系，$R=\{\langle 1, 2\rangle, \langle 2, 3\rangle, \langle 2, 4\rangle\}$，$S=\{\langle 1, 2\rangle, \langle 2, 1\rangle, \langle 3, 3\rangle, \langle 3, 2\rangle\}$，则

$$R\circ S=\{\langle 1, 1\rangle, \langle 2, 3\rangle, \langle 2, 2\rangle\}$$

$$S\circ R=\{\langle 1, 3\rangle, \langle 1, 4\rangle, \langle 2, 2\rangle, \langle 3, 3\rangle, \langle 3, 4\rangle\}$$

由复合关系的定义不难看出，关系的复合运算不满足交换律，事实上，当 $R\circ S$ 有意义时，$S\circ R$ 未必有意义，即使 $R\circ S$ 与 $S\circ R$ 均有定义，也未必有 $R\circ S=S\circ R$，例如，在例 1 中就有 $R\circ S\neq S\circ R$，但可以证明，关系的复合满足结合律.

定理 1　设 R 是 A 到 B 的关系，S 是 B 到 C 的关系，H 是 C 到 D 的关系，则

$$(R\circ S)\circ H=R\circ (S\circ H)$$

证明　$\forall \langle a, d\rangle \in (R\circ S)\circ H$，根据复合关系的定义，存在 $c\in C$，使

$$\langle a, c\rangle \in R\circ S, \langle c, d\rangle \in H$$

由 $\langle a, c\rangle \in R\circ S$ 又知，存在 $b\in B$ 使 $\langle a, b\rangle \in R$，$\langle b, c\rangle \in S$. 因为 $\langle b, c\rangle \in S$，$\langle c, d\rangle \in H$，所以 $\langle b, d\rangle \in S\circ H$，又因为 $\langle a, b\rangle \in R$　因此 $\langle a, d\rangle \in R\circ (S\circ H)$，于是有

$$(R\circ S)\circ H\subseteq R\circ (S\circ H)$$

同理可证

$$R\circ (S\circ H)\subseteq (R\circ S)\circ H$$

从而

$$(R\circ S)\circ H = R\circ (S\circ H)$$

▌

特别地，设 R 是 A 上的关系，则

$$(R\circ R)\circ R=R\circ (R\circ R)$$

因此记号 $R\circ R\circ R$ 有意义，推而广之，记号 $R\circ R\circ \cdots \circ R$（共 n 个）有意义

定义 2　设 R 是 A 上的关系，$n\in \mathbf{N}$，R 的 n 次幂 R^n 定义如下

（1）　R^0 是 A 上的恒等关系，即 $R^0=I_A$

（2）　$R^n=R^{n-1}\circ R=R\circ R\circ \cdots \circ R$（共 n 个）　　$n\geqslant 1$

据此定义及关系复合运算的结合律，可用数学归纳法证明如下定理

定理 2　设 R 是 A 上的关系，

（1）　$R^m\circ R^n=R^{m+n}$

（2）　$(R^m)^n=R^{mn}$　　$\forall m, n\in \mathbf{N}$

（3） $\langle x, y\rangle \in R^m$（$m \geqslant 2$）当且仅当 存在 $x_1, x_2, \cdots, x_{m-1} \in A$ 使

$$\langle x, x_1\rangle \in R, \langle x_1, x_2\rangle \in R, \cdots, \langle x_{m-1}, y\rangle \in R$$

证明留作习题. ▌

对有限集之间的关系，可利用关系矩阵计算复合关系.

设 R 是 A 到 B 的关系，S 是 B 到 C 的关系，其中 A，B，C 均为有限集，不妨设 $A=\{a_1, a_2, \cdots, a_m\}$，$B=\{b_1, b_2, \cdots, b_n\}$，$C=\{c_1, c_2, \cdots, c_p\}$，记 R，S 以及 $R \circ S$ 的关系矩阵分别为 $M_R=(r_{ik})_{m\times n}$，$M_S=(s_{kj})_{n\times p}$，$M_{R\circ S}=(x_{ij})_{m\times p}$，则

$$\begin{aligned} x_{ij}=1 &\Leftrightarrow <a_i, c_j> \in R\circ S \\ &\Leftrightarrow \exists k, 1\leq k\leq n \text{ 使 } <a_i, b_k>\in R, <b_k, c_j>\in S \\ &\Leftrightarrow \exists k, 1\leq k\leq n \text{ 使 } r_{ik}=1, s_{kj}=1 \\ &\Leftrightarrow \exists k, 1\leq k\leq n \text{ 使 } r_{ik}\wedge s_{kj}=1 \\ &\Leftrightarrow \bigcup_{k=1}^{n}(r_{ik}\wedge s_{kj})=1 \quad \text{（注：这里的符号}\bigcup\text{ 表示逻辑“或”）} \end{aligned}$$

因此，有

$$x_{ij}=\bigcup_{k=1}^{n}(r_{ik}\wedge s_{kj}) \qquad i=1, 2, \cdots, m,\ j=1, 2, \cdots, p$$

$M_{R\circ S}$ 的元素 x_{ij} 的计算公式，完全类似于矩阵乘积 $M_R \cdot M_S$ 的元素的计算公式，只是将其中的数量加法与乘法分别换为逻辑加（$\vee$）和逻辑乘（$\wedge$）. 因而，与复合关系的符号相对应，以上计算公式得到的矩阵将写成 $M_R \circ M_S$，于是 $M_{R\circ S}=M_R \circ M_S$.

例 2 设 $A=\{1, 2, 3\}$，$B=\{2, 3, 4\}$，$C=\{1, 2, 3, 4\}$，R_1 是 A 到 B 的关系，R_2 是 B 到 C 的关系，其关系矩阵分别为：

$$M_{R_1}=\begin{array}{c} \\ 1 \\ 2 \\ 3 \end{array}\!\!\begin{array}{c} \begin{array}{ccc} 2 & 3 & 4 \end{array} \\ \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 0 & 1 & 1 \end{bmatrix} \end{array} \qquad M_{R_2}=\begin{array}{c} \\ 2 \\ 3 \\ 4 \end{array}\!\!\begin{array}{c} \begin{array}{cccc} 1 & 2 & 3 & 4 \end{array} \\ \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{bmatrix} \end{array}$$

则 $$M_{R_1\circ R_2}=\begin{bmatrix}1&0&1\\0&1&1\\0&1&1\end{bmatrix}\circ\begin{bmatrix}1&0&0&0\\0&0&0&1\\0&1&1&0\end{bmatrix}=\begin{array}{c}\\2\\3\\4\end{array}\begin{array}{c}\begin{matrix}1&2&3&4\end{matrix}\\\begin{bmatrix}1&1&1&0\\0&1&1&1\\0&1&1&1\end{bmatrix}\end{array}$$

设 R 是 A 到 B 的关系，如果将 R 中每个有序对的两个分量均交换位置，便可得到一个从 B 到 A 的关系，这个关系称为关系 R 的逆.

定义 3　设 R 是 A 到 B 的关系，则

$$\{\langle y,x\rangle \mid \langle x,y\rangle \in R\}$$

称为 R 的逆，记为 R^{-1}.

例如，体育比赛中“战胜”关系的逆为“负于”关系，实数集上小于关系的逆为大于关系.

由定义 3 可见，将 R 的关系图中弧线反向，即得到 R^{-1} 的关系图，将 R 的关系矩阵 M_R 转置，即得到 R^{-1} 的关系矩阵，即 $M_{R^{-1}}=(M_R)^T$.

定理 3　设 R 是 A 到 B 的关系，则

（1）　$\mathrm{dom}\,R^{-1}=\mathrm{ran}\,R$　　$\mathrm{ran}\,R^{-1}=\mathrm{dom}\,R$

（2）　$(R^{-1})^{-1}=R$

读者自证. ▌

定理 4　设 R 是 A 到 B 的关系，S 是 B 到 C 的关系，则有 $(R\circ S)^{-1}=S^{-1}\circ R^{-1}$

证明　$<c,a>\in(R\circ S)^{-1}\Leftrightarrow<a,c>\in R\circ S$

$\Leftrightarrow\exists b\in B$使$<a,b>\in R,<b,c>\in S$

$\Leftrightarrow\exists b\in B$使$<b,a>\in R^{-1},<c,b>\in S^{-1}$

$\Leftrightarrow<c,a>\in S^{-1}\circ R^{-1}$

即有 $(R\circ S)^{-1}=S^{-1}\circ R^{-1}$. ▌

习题三

1. 设 A 是一个集合，$\varnothing$，$A\times A$ 分别称为 A 上的空关系与全关系. 证明：如果 R 是 A 上的空或全关系，则 $R^2=R$.

2. 证明集合 A 上的关系 R 是传递的，当且仅当 $R^2 \subseteq R$.

3. 设 R_1 是从 A 到 B 的关系，R_2，R_3 是从 B 到 C 的关系，证明

（1） $R_1 \circ (R_2 \cup R_3) = (R_1 \circ R_2) \cup (R_1 \circ R_3)$

（2） $R_1 \circ (R_2 \cap R_3) \subseteq (R_1 \circ R_2) \cap (R_1 \circ R_3)$

4. 若 A 是具有 n 个元素的有限集，R 是 A 上的关系，证明：存在 s 和 t，使 $R^s = R^t$，其中，$0 \le s < t \le 2^{n^2}$.

5. 设 S 为 A 上的关系，证明如果 S 是自反的和传递的，则 $S \circ S = S$.

6. 证明定理 2 .

7. 证明定理 4 中的（2），（3）.

8. 设 $A = \{a, b, c, d\}$，R 为 A 上的关系，$R = \{\langle a, b\rangle, \langle a, c\rangle, \langle b, c\rangle, \langle c, b\rangle\}$，求 R^n，$n = 0, 1, 2, 3\cdots$

§ 4　关系的闭包

在我们讨论问题时，往往希望某关系 R 满足一定性质，当 R 不满足所希望的性质时，有时需要在 R 上添加某些元素，构造一个具有所要求性质，且包含 R 的新关系 R' . 当然，在这个过程中我们应该添加尽量少的元素.

定义 1　设 R 是 A 上的关系，如果 A 上的关系 R' 满足如下条件：

（1） R' 是传递的（或自反的、对称的）

（2） $R' \supseteq R$

（3） 若 S 是传递的（或自反的、对称的）且 $S \supseteq R$，则必有 $S \supseteq R'$.

则称 R' 是 R 的传递闭包（自反闭包、对称闭包、）记为 $t(R)$（或 $r(R)$，$s(R)$）.

定义中的（1）、（2）说明 R' 是包含 R 的传递（自反、对称）关系，（3）则说明 R' 是这种关系中“最小的”.

显然，若 R 是传递的，则 $t(R) = R$，若 R 是自反的，则 $r(R) = R$，若 R 是对称的，则 $s(R) = R$，反之亦然.

定理 1　设 R 是集合 A 上的关系，I_A 为 A 上的恒等关系，则 $r(R) = R \cup I_A$.

证明　只需验证 $R \cup I_A$ 满足自反闭包定义中的诸条件即可.

（1） $\forall x \in A$，则 $\langle x, x\rangle \in I_A$，故 $\langle x, x\rangle \in R \cup I_A$ 因此，$R \cup I_A$ 是自反的.

（2） 显然 $R \subseteq R \cup I_A$.

（3） 假设 S 是 A 上的自反关系，且 $S \supseteq R$，往证 $S \supseteq R \cup I_A$.

$\forall \langle a, b\rangle \in R \cup I_A$，有 $\langle a, b\rangle \in R$ 或 $\langle a, b\rangle \in I_A$.

若〈a，b〉$\in R$，则由$S\supseteq R$得〈a，b〉$\in S$

若〈a，b〉$\in I_A$，则$a=b$．由S的自反性得〈a，b〉$\in S$

由此证得$S\supseteq R\cup I_A$.

所以$r(R)=R\cup I_A$. ▌

定理 2　设R是集合A上的关系，则$s(R)=R\cup R^{-1}$

证明　只需验证$R\cup R^{-1}$满足$s(R)$定义中的诸条件即可．

（１）、（２）留给读者，下证（３）．

假设S是A上的对称关系，且$S\supseteq R$，往证$S\supseteq R\cup R^{-1}$．$\forall$〈x，y〉$\in R\cup R^{-1}$，　有〈x，y〉$\in R$或〈x，y〉$\in R^{-1}$．若〈x，y〉$\in R$，则由$S\supseteq R$知〈x，y〉$\in S$．若〈x，y〉$\in R^{-1}$，则〈y，x〉$\in R$，由$S\supseteq R$知，〈y，x〉$\in S$．又由S的对称性，〈x，y〉$\in S$.

因此，总有〈x，y〉$\in S$，从而证得$S\supseteq R\cup R^{-1}$，这样就证明了$s(R)=R\cup R^{-1}$.

定理 3　设R是集合A上的关系，则$t(R)=\bigcup_{i=1}^{\infty}R^i=R^1\cup R^2\cup\cdots$

证明　记$R^+=\bigcup_{i=1}^{\infty}R^i$，只需验证$R^+$满足$t(R)$定义中的诸条件即可．

（１）首先证明R^+是传递的．设〈a，b〉$\in R^+$，〈b，c〉$\in R^+$，则由R^+的定义知必存在正整数m，n，　使〈a，b〉$\in R^m$，〈b，c〉$\in R^n$．因此〈a，c〉$\in R^m\circ R^n=R^{m+n}$．　故〈a，c〉$\in R^+$，即知R^+是传递的．

（２）$R^+\supseteq R$显然成立．

（３）假设S是传递的，且$S\supseteq R$，往证$S\supseteq R^+$.

$\forall$〈x，y〉$\in R^+$，必存在正整数m，使〈x，y〉$\in R^m$，因此有x_1，x_2，…，$x_{m-1}\in A$，使〈x，x_1〉，〈x_1，x_2〉，…，〈x_{m-1}，y〉$\in R$．由于$S\supseteq R$，故知

〈x，x_1〉，〈x_1，x_2〉，…，〈x_{m-1}，y〉$\in S$.

因为S是传递的，所以有〈x，y〉$\in S$，即证得$S\supseteq R^+$．从而知$t(R)=R^+$. ▌

在应用中，R^+经常作为传递闭包的标准记号使用．

对于有限集A，若$|A|=n$，则A上共有2^{n^2}个关系，于是R的所有幂次中最多有2^{n^2}个互不相同者，因此，在

$$R^1，R^2，\cdots，R^{2^{n^2}}，R^{2^{n^2}+1}$$

中，必会出现重复．从而$R^+=\bigcup_{i=1}^{2^{n^2}}R^i$，进一步地，有

定理 4　设 A 为有限集，$|A|=n$，R 为 A 上的关系，则 $R^+=\bigcup_{i=1}^{n} R^i$

证明　显然 $\bigcup_{i=1}^{n} R^i \subseteq R^+$，下证 $R^+ \subseteq \bigcup_{i=1}^{n} R^i$.

$\forall \langle x, y\rangle \in R^+$，必存在正整数 m，使 $\langle x, y\rangle \in R^m$，若 $m \leqslant n$，则 $\langle x, y\rangle \in \bigcup_{i=1}^{n} R^i$

下面考虑 $m>n$ 的情况．由于 $\langle x, y\rangle \in R^m$，故必存在 $x_1, x_2, \cdots, x_{m-1}$，使

$$xRx_1,\ x_1Rx_2,\ \cdots,\ x_{m-1}R\,x_m \qquad (1)$$

其中 $x_m=y$.

由于 $|A|=n<m$，故在 $x_1, x_2, \cdots, x_m$ 中必有相同者，即存在 $1 \leqslant i<j \leqslant m$，使 $x_i=x_j$. 于是，序列（1）可以写成

$$xRx_1,\ \cdots,\ x_{i-1}Rx_i,\ x_iRx_{i+1},\ \cdots,\ x_{j-1}R_j,\ x_jRx_{j+1},\ \cdots,\ x_{m-1}R\,x_m$$

将 $x_iRx_{i+1}, \cdots, x_{j-1}R_j$，一段删去，得

$$xRx_1,\ \cdots,\ x_{i-1}Rx_i,\ \ x_iRx_{j+1},\ \cdots,\ x_{m-1}R\,x_m$$

如果上序列中的项数仍多于 n 项，同上进行处理，直到序列中项数不超过 n 项．这样我们得到如下序列

$$xRx_1',\ x_1'Rx_2'\ \cdots\ x_{k-1}'Rx_m \quad k \leq n$$

因此 $\langle x, x_m\rangle \in R^k$，即 $\langle x, y\rangle \in R^k$，由于 $k \leqslant n$ 故 $\langle x, y\rangle \in \bigcup_{i=1}^{n} R^i$. 由此证得 $R^+ \subseteq \bigcup_{i=1}^{n} R^i$ ，

从而 $R^+=\bigcup_{i=1}^{n} R^i$. ▌

例 1　设 $A=\{a, b, c, d\}$，R 为 A 上的关系，其关系图如图 4.1 所示，下面利用关系矩阵来求 R^+.

由于 $M_R=$

	a	b	c	d
a	0	1	0	0
b	0	0	1	0
c	0	0	0	1
d	1	0	0	0

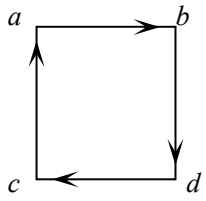


图 4.1

故 $M_{R^2}=M_R\circ M_R=\begin{bmatrix}0&1&0&0\\0&0&1&0\\0&0&0&1\\1&0&0&0\end{bmatrix}\circ\begin{bmatrix}0&1&0&0\\0&0&1&0\\0&0&0&1\\1&0&0&0\end{bmatrix}=\begin{bmatrix}0&0&1&0\\0&0&0&1\\1&0&0&0\\0&1&0&0\end{bmatrix}$

$M_{R^3}=M_{R^2}\circ M_R=\begin{bmatrix}0&0&1&0\\0&0&0&1\\1&0&0&0\\0&1&0&0\end{bmatrix}\circ\begin{bmatrix}0&1&0&0\\0&0&1&0\\0&0&0&1\\1&0&0&0\end{bmatrix}=\begin{bmatrix}0&0&0&1\\1&0&0&0\\0&1&0&0\\0&0&1&0\end{bmatrix}$

$M_{R^4}=M_{R^3}\circ M_R=\begin{bmatrix}0&0&0&1\\1&0&0&0\\0&1&0&0\\0&0&1&0\end{bmatrix}\circ\begin{bmatrix}0&1&0&0\\0&0&1&0\\0&0&0&1\\1&0&0&0\end{bmatrix}=\begin{bmatrix}1&0&0&0\\0&1&0&0\\0&0&1&0\\0&0&0&1\end{bmatrix}$

故知 $t(R)=R^1\cup R^2\cup R^3\cup R^4$ 的关系矩阵为 $M_{R^4}=\begin{bmatrix}1&1&1&1\\1&1&1&1\\1&1&1&1\\1&1&1&1\end{bmatrix}$

因此 $R^+=A\times A$

定理 5　设 R 是集合 A 上的关系，

（1）若 R 是自反的，则 $s(R)$和 $t(R)$都是自反的.

（2）若 R 是对称的，则 $r(R)$和 $t(R)$都是对称的.

（3）若 R 是传递的，则 $r(R)$是传递的.

证明留作习题. ▌

习题四

1. 设 R_1 和 R_2 是集合 A 上的二元关系，且 $R_1\subseteq R_2$，证明

（1）$r(R_1)\subseteq r(R_2)$

（2）$s(R_1)\subseteq s(R_2)$

（3）$t(R_1)\subseteq t(R_2)$

2. 证明定理 5 .

3. R_1 和 R_2 是集合 A 上的二元关系，证明

（1）$r(R_1 \cup R_2)=r(R_1)\cup r(R_2)$

（2）$s(R_1 \cup R_2)=s(R_1)\cup s(R_2)$

（3）$t(R_1 \cup R_2) \supseteq t(R_1)\cup t(R_2)$

用反例说明一般来讲 $t(R_1 \cup R_2) \neq t(R_1)\cup t(R_2)$.

4. 设 $A=\{a, b, c, d\}$，R 是 A 上的二元关系，$R=\{\langle a, b\rangle, \langle b, a\rangle, \langle b, c\rangle, \langle c, d\rangle\}$，求 R 的自反闭包，对称闭包和传递闭包.

§ 5　等价关系与集合的划分

本节将介绍一种特殊关系——等价关系，它在以后的内容中起着非常重要的作用.

定义 1　设 R 是集合 A 上的关系，如果 R 是自反的、对称的、传递的，则称 R 为 A 上的等价关系，对等价关系 R，当 aRb 时，称 a 等价于 b.

等价关系通常用符号“～”表示.

例如，数的相等关系，集合的相等关系，三角形的相似关系，矩阵的合同关系等都是等价关系.

例 1　设 $a=\{a, b, c\}$，R 为 A 上的关系，其关系图如图 5.1，则 R 为等价关系.

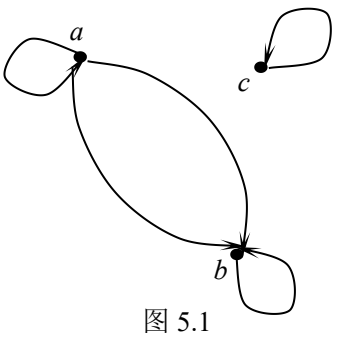


图 5.1

现在我们来给出一个重要的等价关系，为此，引入下列术语.

设 s，t 是两个整数，如果存在整数 q，使 $s=qt$，则称 t 整除 s，记为 $t \mid s$，这时也称 t 是 s 的因数，s 是 t 的倍数.

现设 m 是一个正整数，定义整数集 $\mathbf{Z}$ 上的关系 R_m 如下：

$$iR_mj \Leftrightarrow m \mid i-j \qquad \forall i, j \in \mathbf{Z}$$

称 R_m 为整数集 $\mathbf{Z}$ 上的模 m 同余关系，iR_mj 常记为 $i \equiv j \mod m$，这时说 i，j 关于模 m 同余. 当不引起混乱时，$i \equiv j \mod m$ 也简记为 $i \equiv j$. 显然，$i \equiv j \mod m$ 意味着用 m 分别去除 i，j 得到的余数相同.

以后我们还将用（a，b）表示 a 与 b 的最大公因数，[a，b] 表示 a 与 b 的最小公倍数.

例 2　对任意正整数 m，整数集 $\mathbf{Z}$ 上的模 m 同余关系为等价关系.

事实上，$\forall i \in \mathbf{Z}$，则 $i-i=0\,m$，故 $m \mid (i-i)$，即　$i \equiv i \mod m$，模 m 同余关系是自反的.

$\forall i, j \in \mathbf{Z}$，若 $i \equiv j \mod m$，即 $m \mid (i-j)$，不妨令 $i-j=qm$，则 $j-i=-qm$，于是 $m \mid (j-i)$，即 $j \equiv i \mod m$，模 m 同余关系是对称的.

$\forall i, j, k \in \mathbf{Z}$，若 $i \equiv j \mod m$，$j \equiv k \mod m$，即 $m \mid (i-j)$，$m \mid (j-k)$，

不妨令 $i-j=q_1m$，$j-k=q_2m$，则 $i-k=i-j+j-k=q_1m+q_2m=(q_1+q_2)m$，
即有　$m\mid(i-k)$，亦即 $i\equiv k \bmod m$，模 m 同余关系是传递的.

总之，模 m 同余关系是等价关系.

例 3　设 R_1，R_2 为 A 上的等价关系，则 $R_1\cap R_2$，$(R_1\cup R_2)^+$为 A 上的等价关系.

$R_1\cap R_2$ 是等价关系的证明留作习题，下证 $(R_1\cup R_2)^+$是等价关系.

由传递闭包的定义，$(R_1\cup R_2)^+$ 必为传递的，故只需证明它是自反的，对称的. 由于 R_1 是等价关系，故必为自反的，因此，$\forall x\in A, \langle x, x\rangle \in R_1$, 从而，$\langle x, x\rangle \in R_1\cup R_1\subseteq(R_1\cup R_2)^+$. 所以$(R_1\cup R_2)^+$是自反的.

为证$(R_1\cup R_2)^+$是对称的，有上节定理 5，只要证明$(R_1\cup R_2)$对称即可.
设 $\langle x, y\rangle \in(R_1\cup R_2)$，则 $\langle x, y\rangle \in R_1$ 或 $\langle x, y\rangle \in R_2$. 因为 R_1，R_2 均为等价关系，故必是对称的. 所以 $\langle y, x\rangle \in R_1$ 或 $\langle y, x\rangle \in R_2$. 因而必有 $\langle y, x\rangle \in(R_1\cup R_2)$. 从而$(R_1\cup R_2)$是对称的. 总之，$(R_1\cup R_2)^+$ 是等价关系.

定义 2　设 R 是 A 上的等价关系，$a\in A$. 一切与 a 等价的元素构成的 A 的子集，叫做 a 的 R-等价类，记为$[a]_R$，或简记为 $[a]$. 即

$$[a]_R=\{x\mid x\in A，xRa\}$$

a 称为$[a]_R$的代表元.

对于 A 上等价关系 R，每个元素 $a\in A$ 均可产生一个等价类 $[a]$，所有这些等价类作为一个整体又构成一个集合，对此引入下述定义.

定义 3　设 R 是 A 上的等价关系，R 的所有等价类构成的集合，称为 A 对 R 的商集，记为 A/R，即 $A/R=\{[a]\mid a\in A\}$.

例 4　设 $A=\{a，b，c\}$，R 为例 1 中的关系，则

$[a]=[b]=\{a，b\}$，$[c]=\{c\}$，$A/R=\{\{a，b\}，\{c\}\}$.

例 5　对于正整数 m，考虑整数集上的模 m 同余关系，由例 2 已知它为等价关系，现考虑其等价类 $[i]$. 设 $i\in\mathbf{Z}$，则

$$\begin{aligned}[i]&=\{j\mid j\in\mathbf{Z}，j\equiv i \bmod m\}\\&=\{j\mid j\in\mathbf{Z}，m\mid j-i\}\\&=\{j\mid j\in\mathbf{Z}，\exists k\in\mathbf{Z}\text{ 使 }j-i=km\}\\&=\{j\mid \exists k\in\mathbf{Z}，j=km+i\}\\&=\{km+i\mid k\in\mathbf{Z}\}\end{aligned}$$

特别地

$$[0]=\{km\mid k\in\mathbf{Z}\}=\{\cdots，-2m，-m，0，m，2m，\cdots\}$$

$$[1]=\{km+1\mid k\in\mathbf{Z}\}=\{\cdots，-2m+1，-m+1，1，m+1，2m+1，\cdots\}$$

$$\cdots\cdots$$

$$[r]=\{km+r\mid k\in\mathbf{Z}\}=\{\cdots，-2m+r，-m+r，r，m+r，2m+r，\cdots\}$$

$$\cdots\cdots$$

$$[m-1]=\{km+(m-1)\mid k\in\mathbf{Z}\}$$

$$=\{\cdots,\ -m-1,\ -1,\ m-1,\ 2m-1,\ 3m-1,\ \cdots\}$$

对于任何 $i\in\mathbf{Z}$，设

$$i=qm+r \qquad 0\leqslant r<m$$

则
$$\begin{aligned}[i]&=[qm+r]=\{km+qm+r \mid k\in\mathbf{Z}\}\\&=\{(k+q)m+r \mid k\in\mathbf{Z}\}\\&=\{lm+r \mid l\in\mathbf{Z}\}\\&=[r]\end{aligned}$$

从而 $[i]\in\{[0],[1],\cdots,[m-1]\}$

因此 $\mathbf{Z}/R_m=\{[i] \mid i\in\mathbf{Z}\}=\{[0],[1],\cdots,[m-1]\}$

$[i]\in\mathbf{Z}/R_m$ 通常称作 i 所在的模 m 剩余类．$\mathbf{Z}/R_m$ 则称作模 m 剩余类集，用符号 $\mathbf{Z}_m$ 表示．

现在研究关于等价类的性质．

定理 1　设 R 是 A 上的等价关系，则

（1）　$a\in[a]$

（2）　$[a]=[b] \Leftrightarrow aRb$

（3）　$[a]\cap[b]=\varnothing \Leftrightarrow a\not R b$

证明

（1）由于 aRa，故 $a\in[a]$．

（2）充分性．假设 aRb，要证 $[a]=[b]$.

$\forall x\in[a]$，必有 xRa，故由 aRb 及 R 的传递性知 xRb，故 $x\in[b]$.

因此 $[a]\subseteq[b]$，同理 $[b]\subseteq[a]$，从而　$[a]=[b]$.

必要性．假设 $[a]=[b]$，则由 $a\in[a]$ 知 $a\in[b]$，故 aRb.

（3）充分性．假设 $a\not R b$，要证 $[a]\cap[b]=\varnothing$.　若 $[a]\cap[b]\neq\varnothing$，则可取 $x\in[a]\cap[b]$，于是　xRa，xRb，由 xRa 及 R 的对称性知，aRx．从而由传递性知 aRb，矛盾．故必有 $[a]\cap[b]=\varnothing$.

必要性．假设 $[a]\cap[b]=\varnothing$，则　$a\notin[b]$，$a\not R b$.　▌

在我们讨论问题时，经常需要将讨论对象进行分类，即将一个集合分成一些适当的子集，对此，引入以下定义．

定义 2　设 A 是一个集合，$C=\{C_i \mid i\in J\}$ 是一个集合族，$C_i\neq\varnothing$　$(i\in J)$.

如果 $\bigcup\limits_{i\in J}C_i=A$，则称 C 是 A 的一个覆盖，若还有 $C_i\cap C_j=\varnothing$　$(i\neq j)$，则称 C 是 A 的一个划分，C_i 称为划分块.

例 6　设 $\mathbf{Z}$ 是整数集合，E 是偶数集合，O 是奇数集合．则 $\{E,O\}$ 是 $\mathbf{Z}$ 的一个划分.

例 7　设 A 是任意非空集，

$C_1=\{A\}$

$C_2=\{\{a\}\mid a\in A\}$

则 C_1，C_2 均为 A 的划分，其中，在 C_1 中整个集合 A 是一个划分块，而在 C_2 中 A 的每个元素 a 对应一个划分块$\{a\}$.

集合 A 的划分与集合 A 上的等价关系有着密切的联系．事实上，由划分的定义和等价类的性质，可立即得到：

定理 2　设 R 是集合 A 的等价关系，则 $A/R=\{[a]\mid a\in A\}$ 是 A 的一个划分.

证明　由于 $a\in[a]$，故 $[a]\neq\varnothing$且 $\bigcup\limits_{a\in A}[a]=A$．再证 A/R 是一个分离族.

$\forall\,[a],[b]\in A/R$，设 $[a]\neq[b]$，则 $a\not R\,b$，故 $[a]\cap[b]=\varnothing$，因此，A/R 是 A 的一个划分.

反之，我们有

定理 3　设 A 是一个集合，$C=\{C_i\mid i\in J\}$ 是 A 的一个划分，则由 C 可决定一个等价关系 R，使 $A/R=C$.

证明　令 R 是 A 上的关系，令 $R=\bigcup\limits_{i\in J}C_i\times C_i$，则易验证 R 是一个等价关系，　且 $A/R=C$. ▌

定理 4　设 R_1，R_2 为 A 上的等价关系，则 $R_1=R_2\ \Leftrightarrow\ A/R_1=A/R_2$.

证明　若 $R_1=R_2$，显然 $A/R_1=A/R_2$．下证若 $A/R_1=A/R_2$，则必有 $R_1=R_2$．事实上，设 $x_1R_1\,x_2$，则$[x_1]_{R_1}=[x_2]_{R_1}$，由于 $A/R_1=A/R_2$，故$[x_1]_{R_1}=[x_2]_{R_1}\in A/R_2$．不妨设 $[x_1]_{R_1}=[x_2]_{R_1}=[c]_{R_2}$　其中　$c\in A$. 于是 $x_1,x_2\in[c]_{R_2}$，从而 $x_1R_2\,x_2$，即知 $R_1\subseteq R_2$.

同理可知 $R_2\subseteq R_1$，于是 $R_1=R_2$. ▌

由上面诸定理知，集合 A 上的等价关系，在某种意义上与集合 A 的划分是等同的，给定等价关系，可相应唯一确定 A 的划分，反之亦然.

例 8　设 $A=\{a,\ b,\ c,\ d\}$，$C=\{\{a,\ b\},\{c\},\{d\}\}$，求 C 决定的等价关系.

解　设 C 决定的等价关系为 R，则

$$\begin{aligned}R&=\{a,\ b\}\times\{a,\ b\}\cup\{c\}\times\{c\}\cup\{d\}\times\{d\}\\&=\{\langle a,\ a\rangle,\langle a,\ b\rangle,\langle b,\ a\rangle,\langle b,\ b\rangle,\langle c,\ c\rangle,\langle d,\ d\rangle\}.\end{aligned}$$

例 9　设 $\mathbf{Z}$ 是整数集合，E，O 分别为偶数集与奇数集，则 $C=\{E,\ O\}$ 是 $\mathbf{Z}$ 的划分，现讨论 C 决定的等价关系.

设 C 决定的等价关系为 R，则 $R=E\times E\cup O\times O$,

故　　$iRj\ \Leftrightarrow\langle i,\ j\rangle\in E\times E$ 或 $\langle i,\ j\rangle\in O\times O$

$\Leftrightarrow$　i，j 同奇偶

$\Leftrightarrow$　$i\equiv j \bmod 2$

即 R 恰为模 2 同余关系.

习题五

1. 设 R_1，R_2 为 A 上的等价关系，证明

（1） $R_1 \cap R_2$ 为集合 A 上的等价关系.

（2） $R_1 \cup R_2$ 是 A 上的自反关系和对称关系，举例说明 $R_1 \cup R_2$ 未必是等价关系.

2. 设 R 是 A 上的传递和自反关系， T 是 A 上的二元关系， 满足

$\langle a, b\rangle \in T$ 当且仅当 $\langle a, b\rangle, \langle b, a\rangle \in R$，

证明 T 是一个等价关系.

3. 设 $\mathbf{N}^+$是正整数集，又设 R 是定义在 $\mathbf{N}^+ \times \mathbf{N}^+$上的二元关系：

$\langle a, b\rangle \, R \, \langle c, d\rangle$ 当且仅当 $a / c = b / d$.

证明 R 是 $\mathbf{N}^+ \times \mathbf{N}^+$上的一个等价关系.

4. 设 R 是 A 上的一个自反关系，证明 R 是一个等价关系 当且仅当

$\langle a, b\rangle \in R, \langle a, c\rangle \in R \Rightarrow \langle b, c\rangle \in R$.

5. 设 R_m 为 $\mathbf{Z}$ 上的模 m 同余关系，试写出 $\mathbf{Z} / R_3$，$\mathbf{Z} / R_5$，$\mathbf{Z} / R_6$.

6. （1）设 $A = \{1, 2, 3\}$，A 上关系 R_1，R_2 的关系矩阵如下：

$$M_{R_1} = \begin{bmatrix} 1 & 1 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \qquad M_{R_2} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 1 & 1 \end{bmatrix}$$

问 R_1，R_2 是否等价关系？$R_1 \circ R_2$ 是否等价关系？

（2）设 $B = \{1, 2, 3, 4\}$，举例说明当 S_1，S_2 是 B 上的等价关系时，$S_1 \circ S_2$ 不一定是 B 上的等价关系.

7. 设 $A = \{1, 2, 3\}$，A 上共有多少个等价关系？

8. 设 $A = \{1, 2, 3, 4, 5, 6\}$，C 是 A 上的一个划分：

$C = \{\{1, 2\}, \{3, 4, 5\}, \{6\}\}$

求出 A 上的等价关系 R，使 R 产生的划分恰为 C，画出 R 的关系图.

9. 设 A 是由 6 个彩球构成的集合，其中 a_1，a_3，a_5 是红球，a_2，a_6 是白球，a_4 是黑球.

令 R 是 A 上的关系：$xRy \Leftrightarrow x$ 与 y 颜色相同.

问 R 是否等价关系？若是，求出 $[a_i]_R$，$i = 1, 2, \cdots, 6$，并求 A / R.

§ 6 偏序关系与偏序集

本节再给出一类重要的关系.

定义 1 设 R 是 A 上的关系，如果 R 是自反的、反对称的、传递的，则称 R 是 A 上的偏序关系，简称偏序.

偏序关系习惯上用“≤”表示，偏序关系“≤”的逆“$\leqslant^{-1}$”则用“≥”表示．例如，实数的小于等于关系“≤”，集合的包含关系“⊆”等都是偏序关系．

例 1　设 $A=\{a, b, c, d\}$，$R=\{\langle a, a\rangle, \langle b, b\rangle, \langle c, c\rangle, \langle d, d\rangle, \langle a, b\rangle, \langle a, c\rangle\}$，则 R 是 A 上的偏序关系．

例 2　设 **N** 为自然数集合，则 **N** 上的整除关系“|”为偏序关系．

$\forall m \in N$，$m=1 \cdot m$，故 $m \mid m$．整除关系是自反的．又，$\forall m, n \in \mathbf{N}$，若 $m \mid n$，$n \mid m$，则存在 $q_1, q_2 \in \mathbf{Z}$，使

$$n=q_1 m, \quad m=q_2 n$$

显然，$q_1, q_2 \in \mathbf{N}$．若 $m=0$，则 $n=0$，于是 $m=n$，若 $m \neq 0$，则 $n \neq 0$．这时由

$$m=q_2 n=q_2 q_1 m$$

知　$q_1 q_2=1$，故　$q_1=1$，$q_2=1$　因此　$m=n$，从而整除关系是反对称的．

最后，$\forall m, n, l \in \mathbf{N}$，设 $m \mid n$，$n \mid l$ 则存在 q_1, q_2，使

$$n=q_1 m \qquad l=q_2 n$$

故　$l=q_1 q_2 m$，　即有 $m \mid l$．整除关系是传递的．

综上，整除关系是偏序关系．

设 P 为一集合，如果在 P 上定义了一个偏序关系≤，则称 P 在偏序关系≤下构成一偏序集，记为 $\langle P, \leqslant\rangle$．在不引起混乱的情况下，也简记为 P．

对偏序集 $\langle P, \leqslant\rangle$，如果 $a, b \in P$ 满足 $a \leqslant b$，则说在偏序集 P 中（或在偏序关系≤下）a “小于等于” b，这时也说，b “大于等于” a．注意，这里的“小于等于”或“大于等于”，并不意味着通常意义下的大小关系，而是一个从大小关系中抽象出来的概念．

例 3　设 $P=\{1, 2, 3, 4\}$，R 为通常实数的“大于等于”关系．

则 $3 R 2$，$4 R 3$．因此可说，在 R 下 3 “小于等于” 2，4 “小于等于” 3．

在偏序集 $\langle P, \leqslant\rangle$ 中，若 $a \leqslant b$，且 $a \neq b$，则记为 $a<b$，并说 a 小于 b．

定义 2　设 $\langle P, \leqslant\rangle$ 是一个偏序集，若 $a, b \in P$ 满足 $a<b$，且不存在 c 使 $a<c<b$，则称 b 盖住 a, 或称 b 是 a 的直接前辈，a 是 b 的直接后辈.

例如，设 **N** 是自然数集，≤是通常自然数的“小于等于”关系, 则在偏序集 $\langle \mathbf{N}, \leqslant\rangle$ 中，1 盖住 0，2 盖住 1，…，i 盖住 $i-1$，….

根据偏序关系≤的特点，可以对其关系图进行简化．简化过程如下：

（1）　由于≤是自反的，故在≤的关系图中，每个顶点上均有一个自环，故可将其省略．

（2）　由于≤是传递的，若 $a \leqslant b$，$b \leqslant c$，则必有 $a \leqslant c$．即若 a 到 b 有一条弧，b 到 c 有一条弧，即知 a 到 c 必有一条弧，故可省略 a 到 c 的弧，也就是说，当且仅当 c 盖住 a 时，画一条从 a 到 c 的弧．

（3）　由于≤是反对称的，≤的关系图中无首尾相接构成封闭路径的一串弧，故总可使弧线的箭头向上，从而省略箭头．

利用以上简化过程，我们得到 P 上偏序关系≤的关系图的画法：

（1） 用圆点表示集合 P 的元素.

（2） 如果 c 盖住 a，则 c 画在 a 上方，且在 a，c 之间连一条线.

这样得到的图，称为〈P，≤〉的 Hasse 图.

例 4　设 S_n 表示 n 的所有正因子构成的集合.“|”表示 S_n 上的整除关系，画出〈S_{75}，|〉，〈S_{30}，|〉的 Hasse 图.

〈S_{75}，|〉，〈S_{30}，|〉的 Hasse 图如图 6.1（a），（b）所示.

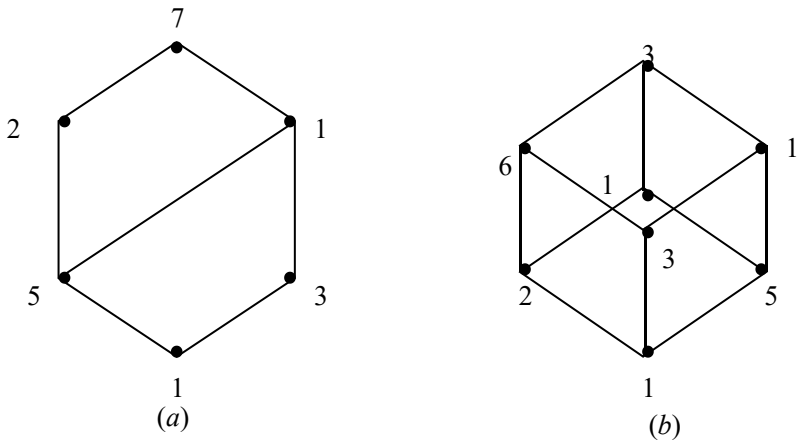


图 6.1

例 5　设 $A=\{a\}$，$B=\{a, b\}$，$C=\{a, b, c\}$，画出〈P（A），⊆〉，〈P（B），⊆〉，〈P（C），⊆〉的 Hasse 图.

〈P（A），⊆〉，〈P（B），⊆〉，〈P（C），⊆〉的 Hasse 图如图 6.2 所示.

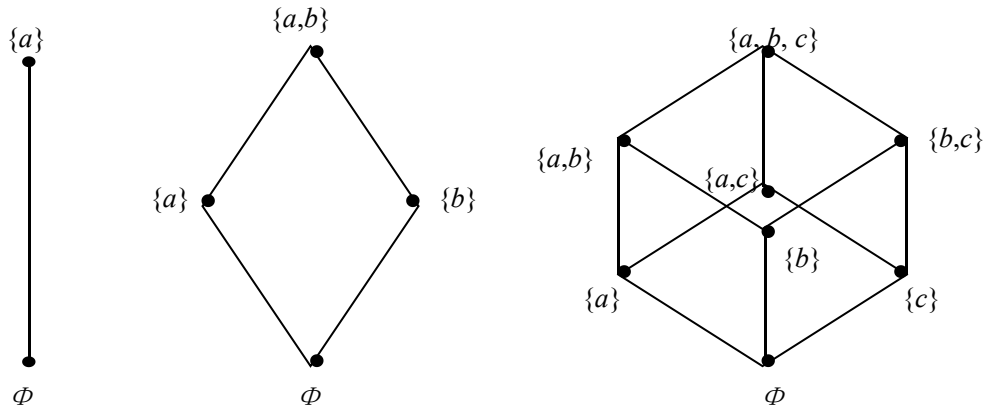


图 6.2

设〈P，$\leqslant$〉是一个偏序集，$\forall x$，$y\in P$，若 $x\leqslant y$ 或 $y\leqslant x$，称 x，y 是可比较的，否则称 x，y 不可比较．例 4 的〈S_{75}，|〉中，3 和 5 是不可比较的，同样，在〈P（C），$\subseteq$〉中，{a，b}，{b，c} 也是不可比较的．

定义 3　设$\leqslant$是 P 上的偏序，如果对任意 x，$y\in P$，总有 $x\leqslant y$ 或者 y $\leqslant x$，即任何两元素都可比较，那么，称$\leqslant$为全序关系，简称全序．当$\leqslant$是全序时，集合〈P，$\leqslant$〉称为全序集．

例 4 、例 5 中的〈S_{75}，|〉，〈S_{30}，|〉，〈P（B），$\subseteq$〉，〈P（C），$\subseteq$〉，均不是全序集．〈P（A），$\subseteq$〉是全序集，对通常整数的“小于等于”关系$\leqslant$，〈**N**，$\leqslant$〉是全序集．

定义 4　设〈A，$\leqslant$〉是偏序集．若 $B\subseteq A$ 且〈B，$\leqslant$〉是全序集，则称 B 为链．

定义 5　设〈P，$\leqslant$〉是一个偏序集，$a\in P$．如果对任意 $x\in P$，均有 $a\leqslant x$，则称 a 是〈P，$\leqslant$〉的最小元；如果对任意 $x\in P$ 均有 $x\leqslant a$，则称 a 是〈P，$\leqslant$〉的最大元．

例 6　对任意集合 A，〈P（A），$\subseteq$〉的最大元为 A，最小元为$\varnothing$．

例 7　设〈**N**，$\leqslant$〉为自然数集在通常整数的“小于等于”关系$\leqslant$下构成的偏序集，则 **N** 中不存在最大元，0 是**N**的最小元．

例 8　设 A＝｛2, 3, 6, 12, 24, 36｝，则〈A，|〉的 Hasse 图如图 6.3 所示．

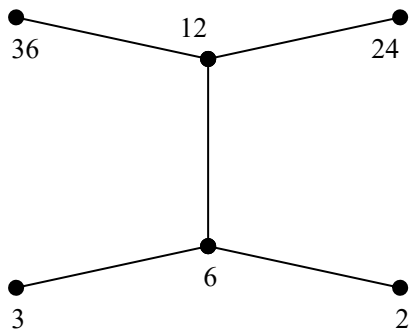


图 6.3

〈A，|〉中，不存在最大元和最小元．

在例 8 的偏序集 A 中，36 和 24 虽不是最大元，但却没有元素“大于”36，也没有元素“大于”24．同样，A 中 2 和 3 虽不是最小元，但却没有元素“小于”2，也没有元素“小于”3．

定义 6　设〈P，$\leqslant$〉是一个偏序集，$a\in P$．如果不存在元素 $x\in P$，使 $a<x$，则称 a 是〈P，$\leqslant$〉的极大元；如果不存在元素 $x\in P$，使 $x<a$，则称 a 为〈P，$\leqslant$〉的极小元．

例 8 中的 36，24 为极大元，2，3 为极小元，一般地，偏序集〈P，$\leqslant$〉中的极大（小）元，可以存在，也可以不存在．若存在则可以唯一，也可以不唯一．但对最大（小）元，有:

定理 1　设〈P，$\leqslant$〉是一个偏序集，若 P 中最大（小）元存在，则必唯一．

证明　只讨论最大元，最小元的情况完全类似．

设 P 中有两个最大元 a_1，a_2，则由 a_1 是最大元，有 $a_2\leqslant a_1$，同样，由于 a_2 是最大元，

有 $a_1 \leqslant a_2$，从而由≤的反对称性可知，$a_1 = a_2$，即 P 中最大元如果存在，则必唯一．▌

定理 2　偏序集〈P，≤〉中的最大（小）元，必是唯一极大（小）元．

证明　只讨论最大元的情况，最小元情况完全类似．

设 a 是 P 中最大元，往证 a 必为极大元．即证不存在 $x \in P$，使 $a < x$．

倘若有 $x \in P$，使 $a < x$，则

$$a \leqslant x \quad \text{且} \quad a \neq x$$

但由于 a 为最大元，故必有 $x \leqslant a$，因此，由≤的反对称性知，$a = x$，矛盾．故 a 必为极大元．

若另有极大元 c，$c \neq a$，则由于 a 是最大元，故有 $c \leqslant a$，因此 $c < a$，与 c 是极大元矛盾．故 a 是唯一极大元．▌

一般来说，极大（小）元未必是最大（小）元，既使极大（小）元唯一，也不一定能成为最大（小）元．

例 9　设 $\mathbf{Z}$ 是整数集合，令 $A = \mathbf{Z} \cup \{a\}$，$R$ 是图 6.4 表示的偏序关系．

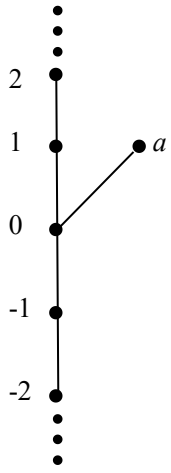


图 6.4

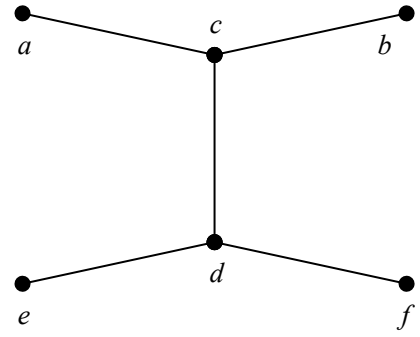


图 6.5

则 a 是唯一极大元，但却不是最大元．

定理 3　设〈P，≤〉是有限偏序集，若 P 中存在唯一极大（小）元 a，则 a 必为最大（小）元．

证明　设 a 为 P 中唯一极大元，往证 a 是最大元．

任取 $x \in P$，若 $x = a$，则 $x \leqslant a$，若 $x \neq a$，则 x 不是极大元．故必有 $x_1 \in P$，使 $x < x_1$，若 $x_1 = a$，则 $x < a$，否则，x_1 不是极大元，又可找到 x_2，使 $x_1 < x_2$，这时，$x < x_1 < x_2$，若 $x_2 = a$，则 $x < a$，否则…一直进行下去．

由于 P 是有限集，故上述过程必会在有限步终止．即存在 x_k，使

$$x < x_1 < x_2 < \cdots < x_k \text{ 且 } x_k = a$$

于是 $x<a$，总之，对任意 $x\in P$，我们证明了 $x\leqslant a$．即证明了 a 是最大元．

极小元情况的证明完全类似，略．▌

最大元、最小元的概念，可以推广到偏序集〈P，$\leqslant$〉的子集 A，更进一步地，引入下述定义．

定义 7　设〈P，$\leqslant$〉是偏序集，$A\subseteq P$，$a\in P$，如果$\forall x\in A$，都有 $x\leqslant a$，称 a 为 A 的上界．如果$\forall x\in A$，都有 $a\leqslant x$，称 a 为 A 的下界．

例 10　设〈P，$\leqslant$〉是图 6.5 所示的偏序集．则｛a，b｝无上界，c，d，e，f均为其下界．｛c，d，f｝具有上界 c，a，b，下界f.

定义 8　设〈P，$\leqslant$〉是偏序集，$A\subseteq P$，若 a 是 A 的上界，且对 A 的任意上界 b，有 $a\leqslant b$，则称 a 为 A 的最小上界（上确界），若 a 是 A 的下界，且对 A 的任意下界 b，有 $b\leqslant a$，则称 a 为 A 的最大下界（下确界）．A 的最小上界和 A 的最大下界分别用 sup$A$ 和 inf$A$ 表示．

在例 10 中，sup｛a，b｝不存在，inf｛a，b｝$=c$，sup｛c，d，f｝$=c$，inf｛c，d，f｝$=f$.

例 11　设〈P，$\leqslant$〉是图 6.6 所示的偏序集．则

sup｛2，3｝＝1　　inf｛2，3｝＝5

sup｛4，6，7｝＝4　　inf｛4，6，7｝＝8

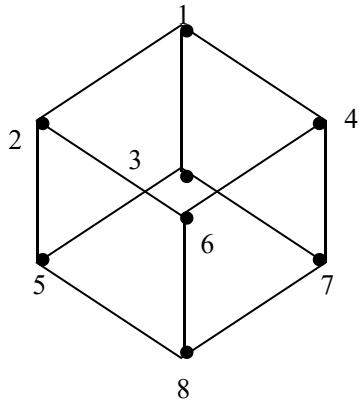


图 6.6

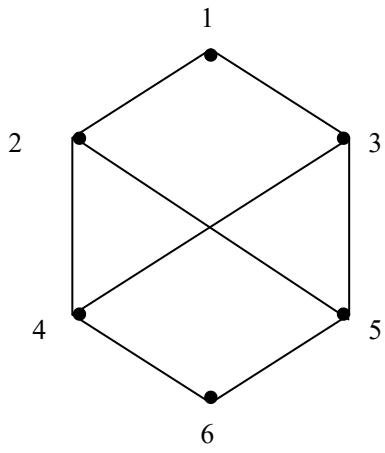


图 6.7

例 12　设〈P，$\leqslant$〉是图 6.7 所示的偏序集，则

｛4，5｝具有上界 1，2，3．但 sup｛4，5｝不存在，inf｛4，5｝＝6．

｛2，3｝具有下界 4，5，6，但 inf｛2，3｝不存在．sup｛2，3｝＝1．

由上面例子可见，偏序集 P 的子集 A 的上界、下界未必存在，若上、下界存在也不一定唯一．自然，A 的最小上界和最大下界未必存在，但若 A 的最小上界和最大下界存在，则必唯一．

定理 4　设 A 是偏序集〈P，≤〉的子集，若 A 的最小上界（最大下界）存在，则必唯一.

证明留作习题. ▌

习题六

1. 设≤是 P 上的偏序关系，≥为≤的逆，证明≥必为 P 上的偏序关系.
2. 设〈P，≤〉是有限偏序集，若 P 中存在唯一极小元 a，则 a 必为最小元.
3. 设〈P，≤〉是一偏序集，$A\subseteq P$，试给出 A 中最大（小）元的定义.
4. 设 A 是偏序集〈P，≤〉的子集，证明若 A 的最大下界（最小上界）存在，则必唯一.
5. 对下列集合在整除关系下构成的偏序集，画出 Hasse 图，并指出哪些是全序集，写出最大元，最小元，极大元，极小元.
   （1）{1，2，3，4，6，8，12，14}
   （2）{1，2，3，…，12}
   （3）{2，4，8，16}
   （4）{1，3，5，9，15，45}
6. 证明　在偏序集〈A，≤〉中任意两个极大元（极小元）都是不可比较的.
7. 证明　有限偏序集〈A，≤〉中至少有一个极大元和一个极小元.
8. 设〈A，R_1〉和〈B，R_2〉是两个偏序集，在 $A\times B$ 上定义一个二元关系 R：对 a_1，$a_2\in A$，b_1，$b_2\in B$，〈a_1，b_1〉R〈a_2，b_2〉当且仅当 $a_1R_1\,a_2$ 且 $b_1R_2\,b_2$，证明 R 是一个偏序关系.
9. 设 $A=\{a，b，c，d\}$，画出〈P（A），$\subseteq$〉的 Hasse 图.
10. 设 S_n 是 n 的所有正因子构成的集合，“|”为 S_n 上的整除关系，画出以下偏序集的 Hasse 图：〈S_8，|〉，〈S_{12}，|〉，〈S_{105}，|〉，〈S_{210}，|〉.

§7　函数

设 R 是集合 A 到 B 的关系，根据定义，对于 $x\in A$，允许没有 $y\in B$ 使〈x，y〉$\in R$，也允许有多个不同的 $y\in B$ 使〈x，y〉$\in R$.

如果我们限定对于每一 $x\in A$，存在唯一的 $y\in B$ 使〈x，y〉$\in R$，则 R 就称作函数.

定义 1　设 f 是集合 A 到 B 的关系，如果对于任意 $x\in A$，存在唯一的 $y\in B$ 使〈x，y〉$\in f$，则称 f 为 A 到 B 的函数，记为 f：$A\to B$.

A 到 A 的函数，也称为 A 上的函数.

符号“f：$A\to B$”可以读做“f 是 A 到 B 的函数”或“A 到 B 的函数 f……”等等，视上、下文而定.

设 f 是 A 到 B 的函数，〈x，y〉$\in f$ 可记为 $y=f(x)$ 或 f：$x\mid\to y$，y 称为 f 在 x 点的

值，也称 y 为 x 在 f 下的象．相应地，称 x 为 y 在 f 下的原象．

例 1　设 $A=\{a, b, c, d\}$，$B=\{1, 2, 3, 4\}$，在如下的关系图（图 7.1）所示的关系中，f_1，f_2 是函数，f_3，f_4 不是函数．

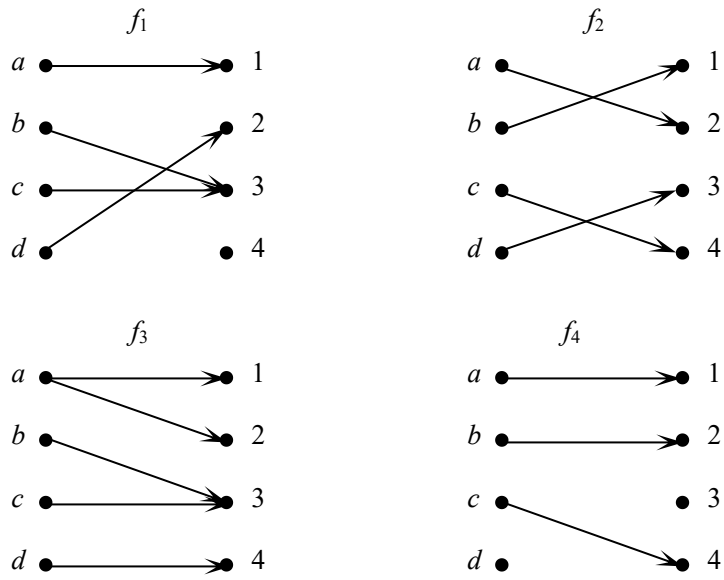


图 7．1

例 2　设 $\mathbf{R}$ 是实数集合，$\mathbf{R}_+$是非负实数集合．令

$$f_1=\{\langle x, x^2\rangle \mid x\in\mathbf{R}\}$$

$$f_2=\{\langle x^2, x\rangle \mid x\in\mathbf{R}\}$$

则 f_1 是 $\mathbf{R}$ 到 $\mathbf{R}_+$的函数，f_2 不是 $\mathbf{R}_+$到 $\mathbf{R}$ 的函数．

在其它学科（比如微积分）中，我们已多次接触到函数的概念．但在那里，函数被定义为一种对应规律或对应法则．这种定义实际上与我们上面给出的函数定义是等价的．现在就来说明这一点．

设 A，B 是两个集合，“f 是 A 到 B 的函数”意味着对任意 $x\in A$，存在唯一一个 $y\in B$，使 $\langle x, y\rangle \in f$. 或者说，对任意 $x\in A$, 在 f 决定的法则“$\langle x, y\rangle \in f$ ”之下有唯一的 y 与 x 相对应. 因而，这里的函数 f 决定了（也就直接可以看成）一个所谓的“对应法则”. 显然，在这种解释下，现在的函数概念与以前（比如，微积分中）所定义的函数是一致的，而且，现在的定义更加明确了法则的含义．鉴于此，我们下面可对函数作两种理解：一是按照定义 1 将函数理解为一种特殊的关系，二是按照以前的习惯将函数理解为一种对应法则，视其方便而定．以此为依据，我们将把映射，对应，变换等作为函数的同义语使用．

以后将经常使用以下两种形式来定义函数：

（i） 令 f：$A\to B$

$$f:\ a\mid\to b \qquad \forall a\in A$$

其意义为：f 是一个 A 到 B 的函数，该函数在点 $a\in A$ 的值为 b.

（ii） 令

$$f:\ a\mid\to b \qquad \forall a\in A$$

其意义为 f 是一个对应法则，在此法则下 a 对应 b.

当用以上形式定义函数时，“f：$a\mid\to b$”也可写成“$f(a)=b$”.

例 3 设 A 为一集合，令 I_A：$A\to A$

$$I_A:\ a\mid\to a \qquad \forall a\in A$$

I_A 称为 A 上的恒等函数，它就是 A 上的恒等关系.

例 4 设 A，B 是两个集合．令

$$P_1:\langle a,\ b\rangle\mid\to a \qquad \forall\langle a,\ b\rangle\in A\times B$$

$$P_2:\langle a,\ b\rangle\mid\to b \qquad \forall\langle a,\ b\rangle\in A\times B$$

P_1，P_2 分别称为从 $A\times B$ 到 A，B 的投影函数.

例 5 设 U 是全集，A 是 U 的子集．令 φ_A：$U\to\{0,\ 1\}$

$$\varphi_A(x)=\begin{cases}1 & x\in A\\ 0 & x\notin A\end{cases}$$

函数 $\varphi_A(x)$ 称为集合 A 的特征函数.

例 6 设 R 是集合 A 上的等价关系，令

$$\varphi:\ a\mid\to[a]_R \qquad \forall a\in A$$

则 φ 是 A 到 A/R 的函数，称为 A 到 A/R 的自然映射.

我们已经知道，对于 A 到 B 的函数 f，如果 $a\in A$，$b\in B$ 满足 $b=f(a)$，便称 b 是 a 在 f 下的象，而 a 则称为 b 在 f 下的原象，进一步地，如果 $A_1\subseteq A$，A_1 中所有点的象构成的集合称为 A_1 在 f 下的象，记为 $f(A_1)$，即

$$f(A_1)=\{f(x)\mid x\in A_1\}$$

如果 $B_1\subseteq B$，B_1 中元素的所有原象构成的集合称为 B_1 的完全原象，简称原象，记为 $f^{-1}(B_1)$，即

$$f^{-1}(B_1)=\{x\mid x\in A,\ f(x)\in B_1\}$$

$f^{-1}(\{b\})$可简记为 $f^{-1}(b)$.

显然，若 f：$A\to B$，则 $f(A)$ 即为 f 的值域.

例 7 设 $\mathbf{R}$ 是实数集，令 f：$\mathbf{R}\to\mathbf{R}$

$$f(x)=x^2 \qquad \forall x\in R$$

则 $f([0,1])=[0,1]$

$f([0,2])=[0,4]$

$f^{-1}([0,1])=[-1,1]$

$f^{-1}([0,4])=[-2,2]$

$f^{-1}([-1,4])=[-2,2]$

$f^{-1}([-2,-1])=\varnothing$

$f^{-1}(1)=\{-1,1\}$

例 8 设 f 是 $\mathbf{Z}$ 到 $\mathbf{Z}_m$ 的自然映射，即

$$f(i)=[i]=\{km+i \mid k\in\mathbf{Z}\}$$

则 $f(\{0,1\})=\{[0],[1]\}$

$f(\{0,n,n+1\})=\{[0],[1]\}$

$f^{-1}(\{[0],[1]\})=\{km+i \mid k\in\mathbf{Z},\ i\in\{0,1\}\}$

$f^{-1}([0])=\{km \mid k\in\mathbf{Z}\}$

设 f 是 A 到 B 的函数，$A_1\subseteq A$，$\forall x\in A_1$，自然存在唯一的 $y\in B$ 使 $\langle x,y\rangle\in f$. 因此，由 A 到 B 的函数 f 诱导出一个 A_1 到 B 的函数：

$$g=\{\langle x,y\rangle \mid x\in A_1,\langle x,y\rangle\in f\}$$

定义 2 设 A，B 为两个集合，$A_1\subseteq A$，f：$A\to B$，g：$A_1\to B$，且

$$g(x)=f(x) \quad \forall x\in A_1 \quad 即 \quad g=\{\langle x,y\rangle \mid x\in A_1,\ y=f(x)\}$$

称 g 为 f 在 A_1 上的限制，并将 g 记为 $f|_{A_1}$，也称 f 为 g 在 A 上的扩张.

在不引起混乱的情况下，f 在 A_1 上的限制有时仍用 f 表示.

定义 3 设 f：$A\to B$，如果$\forall x$，$y\in A$，当 $x\neq y$ 时，必有 $f(x)\neq f(y)$，则称 f 为 A 到 B 的单射（内射）.

显然，f：$A\to B$ 是单射的充要条件为

$$f(x)=f(y)\Rightarrow x=y$$

定义 4 设 f：$A\to B$，若 ran$f=B$，则称 f 为 A 到 B 的满射.

显然，f：$A\to B$ 是满射的充要条件是 $\forall y\in B$，$\exists x\in A$，使 $f(x)=y$

定义 5 设 f：$A\to B$，若 f 既为单射，又为满射，则称 f 为 A 到 B 的一一映射（双射）.

例 11 令 f：$\mathbf{R}\to\mathbf{R}$

$$f:\ a\mapsto a^2 \qquad \forall\ a\in\mathbf{R}$$

则 f 既不是单射，也不是满射.

例 12 令 f：$\mathbf{R}^+\to\mathbf{R}$

$$f:\ a\mapsto a^2 \qquad \forall\ a\in\mathbf{R}^+$$

则 f 是单射，但不是满射.

例 13 令 f：$\mathbf{R}^+\to\mathbf{R}^+$

$$f:\ a \mid\!\rightarrow a^2 \qquad \forall\ a\in \mathbf{R}^+$$

则 f 是一一映射.

最后考虑有限集 A 到有限集 B 的函数共有多少个. 我们已经知道，若 $|A|=m$，$|B|=n$，则 A 到 B 的关系，即 $A\times B$ 的子集共有 2^{mn} 个. 那么，其中有多少是函数呢？根据函数的定义，要使一个关系 f 构成函数，就是要求 $\forall a\in A$，存在唯一的 $b\in B$，使

$$\langle a,\ b\rangle \in f$$

因此，若设

$$A=\{a_1,\ a_2,\ \cdots,\ a_m\} \qquad B=\{b_1,\ b_2,\ \cdots,\ b_n\}$$

则 A 到 B 的函数即为如下形式的有序对集合.

$$f=\{\langle a_1,\ b_{i_1}\rangle,\langle a_2,\ b_{i_2}\rangle,\ \cdots,\langle a_m,\ b_{i_m}\rangle\}$$

其中，b_{i_1}，b_{i_2}，$\cdots$，b_{i_m} 均可在 B 中任意选取，故均有 n 种取法，因此，选取一组

（b_{i_1}，b_{i_2}，$\cdots$，b_{i_m}）共有 $n\cdot n\cdots n=n^m$ 种取法，即形如

$$f=\{\langle a_1,\ b_{i_1}\rangle,\langle a_2,\ b_{i_2}\rangle,\ \cdots,\langle a_m,\ b_{i_m}\rangle\}$$

的有序对集合共有 n^m 个，亦即 A 到 B 的函数共有 n^m 个，或说有 $|B|^{|A|}$ 个. 鉴于此，以后用 B^A 表示所有 A 到 B 的函数构成的集合（A，B 可以是无限集）.

习题七

1. 设 **Z** 是整数集，对给定正整数 m，在 **Z** 上定义一个二元关系：

   $f=\{<a,\ r>\mid a,\ r\in\mathbf{Z},\ \text{且}\ 0\le r<m,\ a\equiv r \bmod m\}$

   试问 f 是不是 **Z** 到 **Z** 的函数？若是，试问是不是满射，是不是单射？
2. 设 $A=\{a,\ b,\ c\}$，$B=\{1,\ 0\}$ 构造从 A 到 B 的一切可能的函数，问其中哪些是满射，哪些是单射？哪些是双射？
3. 下列二元关系中哪一个能构成函数？

   (1) $\{<x_1,\ x_2>\mid x_1, x_2\in\mathbf{N}\ \text{且}\ x_1+x_2<10\}$

   (2) $\{<y_1,\ y_2>\mid y_1, y_2\in\mathbf{R}\ \text{且}\ y_2=y_1^3\}$

   (3) $\{<y_1,\ y_2>\mid y_1, y_2\in\mathbf{R}\ \text{且}\ y_2^4=y_1\}$

   (4) $\{<x_1,\ x_2>\mid x_1, x_2\in\mathbf{N}\ \text{且}\ x_2=$ 小于 x_1 的质数个数$\}$
4. 设 **N** 是自然数集，确定下列函数中哪些是双射？哪些是满射？哪些是单射？

   (1) $f:\ \mathbf{N}\rightarrow\mathbf{N}$，$f(n)=n^2+2$

   (2) $f:\ \mathbf{N}\rightarrow\mathbf{N}$，$f(n)=n \bmod 3$

(3) f：$\mathbf{N}\to\mathbf{N}$，$f(n)=\begin{cases}1, & n\text{是奇数}\\ 0, & n\text{是偶数}\end{cases}$

(4) f：$\mathbf{N}\to\{0,1\}$，$f(n)=\begin{cases}0, & n\text{是奇数}\\ 1, & n\text{是偶数}\end{cases}$

5. 设 $\mathbf{N}$ 是自然数集，f 和 g 都是从 $\mathbf{N}\times\mathbf{N}$ 到 $\mathbf{N}$ 的函数，且 $f(<x, y>)=x+y$，$g(<x, y>)=xy$，证明 f 和 g 是满射，但不是单射.

6. 设 $f(x)=x$，$x\geq 0$. 下面哪个函数是 f 的扩张？
   (1) $g(x)=|x|$，$x\in\mathbf{R}$
   (2) $h(x)=I_R(x)$，这里 I_R 是 $\mathbf{R}$ 上的恒等函数。
   (3) $k(x)=x$，$-1\leq x\leq 1$

7. 设 A，B 是两个集合，$A_1\subseteq A$，f：$A\to B$，证明 $f|_{A_1}=f\cap(A_1\times B)$.

8. 设 A，B 为两个有限集.
   (1) 若 $|A|=|B|$，则 A 到 B 的单射、满射、双射各有多少？
   (2) 若 $|A|<|B|$，则 A 到 B 的单射、满射、双射有多少？

9. 设 A，B 为两个有限集，证明
   (1) A，B 之间存在单射 $\Leftrightarrow |A|\leq|B|$.
   (2) A，B 之间存在满射 $\Leftrightarrow |A|\geq|B|$.
   (3) A，B 之间存在双射 $\Leftrightarrow |A|=|B|$.

10. 设 A，B 为两个有限集，$|A|=|B|$，证明若 f：$A\to B$ 是单射，则必是满射，反之亦然.

11. 设 A，B 为两个集合，证明
   (1) $\varphi_A=\varphi_B\Leftrightarrow A=B$
   (2) $\varphi_A(x)\leqslant\varphi_B(x)\Leftrightarrow A\subseteq B$
   (3) $\varphi_{A\cap B}(x)=\varphi_A(x)\,\varphi_B(x)$
   (4) $\varphi_{A\cup B}(x)=\varphi_A(x)+\varphi_B(x)-\varphi_A(x)\,\varphi_B(x)$

§ 8　复合函数与逆函数

本节所讨论的函数复合，在记法上与关系的复合有所不同. 为了清楚起见，本节将暂时用符号“$\Diamond$”表示关系的复合，即对于 A 到 B 的关系 R 和 B 到 C 的关系 S，

$$R\Diamond S=\{<a, c>\mid a\in A, c\in C, \exists b\in B \text{ 使 } <a, b>\in R, <b, c>\in S\}.$$

我们知道，函数是一种特殊类型的关系. 因此，对于给定的函数 f：$A\to B$，g：$B\to C$，我们可以求 f，g 的复合关系 $f\Diamond g$，由定义

$$f \lozenge g = \{<a，c> \mid a\in A, c\in C，\exists b\in B，b = f(a)，c = g(b)\}$$

但由于函数的特殊记法，引入下述(左)复合概念更为方便.

定义 1 设 f：$A\to B$，g：$B\to C$，集合

$$\{<a，c> \mid a\in A, c\in C，\exists b\in B，b = f(a)，c = g(b)\}$$

称为函数 g 对 f 的(左)复合，记为 $g\circ f$.

由定义立即可见，定义 1 中的 $g\circ f$，恰为 $f\lozenge g$，即有 $g\circ f = f\lozenge g$. 与“左复合”的提法相应地，我们将 $R\lozenge S$ 说成是 R 与 S 的右复合.

首先我们需要考虑的是对于 f：$A\to B$，g：$B\to C$，$g\circ f$ 是否仍然是函数？

定理 1 设 f：$A\to B$，g：$B\to C$，则 $g\circ f$：$A\to C$，且 $(g\circ f)(a) = g(f(a))$.

证明：$\forall a\in A$，由于 f 是函数，故 $\exists b\in B$，使 $b = f(a)$，又因 g 是函数，对于该 $b\in B$ 存在 $c\in C$ 使 $c = g(b)$，从而〈a，c〉$\in g\circ f$，其中，$c = g(b) = g(f(a))$.

下证满足〈a，c〉$\in g\circ f$ 的 c 是唯一的.

设有〈a，c_1〉$\in g\circ f$，〈a，c_2〉$\in g\circ f$，则 $\exists b_1$，$b_2\in B$，使 $b_1 = f(a)$，$c_1 = g(b_1)$，$b_2 = f(a)$，$c_2 = g(b_2)$. 由于 f 是函数，故 $b_1 = b_2$，从而，$c_1 = c_2$.

因此我们证明了对任意 $a\in A$，存在唯一的 $c = g(f(a))$ 使〈a，c〉$\in g\circ f$，即 $g\circ f$ 是 A 到 C 的函数，且 $(g\circ f)(a) = g(f(a))$. ▌

该定理中给出的公式

$$(g\circ f)(a) = g(f(a))$$

是一个非常重要的公式，它使我们可以通过逐次求函数 f，g 的函数值来求出 $(g\circ f)$ 的函数值，在一些其它学科中，该公式就作为 $g\circ f$ 的定义.

例 1 设 $A = \{a，b，c，d\}$，$B = \{1，2，3\}$，$C = \{1，2，3，4\}$

$f = \{\langle a，1\rangle，\langle b，1\rangle，\langle c，2\rangle，\langle d，3\rangle\}$

$g = \{\langle 1，3\rangle，\langle 2，4\rangle，\langle 3，1\rangle\}$

则 $g\circ f = \{\langle a，3\rangle，\langle b，3\rangle，\langle c，4\rangle，\langle d，1\rangle\}$

例 2 设 $\mathbf{R}$ 是实数集

$$f(x) = 2x + 1 \qquad x\in\mathbf{R}$$

$$g(x) = x^2 \qquad x\in\mathbf{R}$$

则 $(g\circ f)(x) = g(f(x)) = g(2x + 1) = 4x^2 + 4x + 1$

$(f\circ g)(x) = f(g(x)) = f(x^2) = 2x^2 + 1$

例 3 设 I_A 是集合 A 上的恒等映射，f 是 A 上的任意函数，

则 $(I_A\circ f)(x) = I_A(f(x)) = f(x)$

$(f\circ I_A)(x) = f(I_A(x)) = f(x)$

即 $I_A\circ f = f\circ I_A = f$

定理 2 设 f：$A\to B$，g：$B\to C$，h：$C\to D$，则 $(h\circ g)\circ f = h\circ(g\circ f)$.

证明 由关系的(右)复合满足结合律知：

$$(h\circ g)\circ f = f\lozenge(h\circ g) = f\lozenge(g\lozenge h) = (f\lozenge g)\lozenge h = h\circ(g\circ f).$$ ▌

定理 3 设 f：$A\to B$，g：$B\to C$ 则

(1) 若 f，g 是满射，则 $g\circ f$ 是满射.

(2) 若 f，g 是单射，则 $g\circ f$ 是单射.

(3) 若 f，g 是双射，则 $g\circ f$ 是双射.

证明 (1)$\forall c\in C$，由于 g 为满射，故存在 $b\in B$ 使 $c=g(b)$，又对于 $b\in B$，由 f 为满射，故存在 $a\in A$ 使 $b=f(a)$，从而 $c=g(b)=g(f(a))=(g\circ f)(a)$，因此 $g\circ f$ 是满射.

(2) $\forall a_1$，$a_2\in A$，设 $a_1\neq a_2$，则因为 f 为单射，故 $f(a_1)\neq f(a_2)$，又因为 g 是单射，故 $g(f(a_1))\neq g(f(a_2))$. 即 $(g\circ f)(a_1)\neq(g\circ f)(a_2)$，因此，$g\circ f$ 是单射.

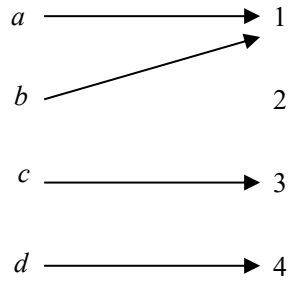
(3) 由(1)，$g\circ f$ 为满射，由(2)，$g\circ f$ 为单射，故 $g\circ f$ 为双射. ▌

下面再来讨论函数的逆. 设 f：$A\to B$，f 作为一种特殊的关系，其逆 f^{-1} 永远存在. 且由定义，f^{-1} 是一个 B 到 A 的关系，满足：

$$\langle y，x\rangle\in f^{-1}\Leftrightarrow\langle x，y\rangle\in f$$

但是，f^{-1} 是否一定是一个 B 到 A 的函数呢？回答是否定的，看下面的例子.

例 4 设 $A=\{a，b，c，d\}$，$B=\{1，2，3，4\}$，f：$A\to B$ 由下列关系图(图 8 .1)定义. 则 $f^{-1}=\{\langle 1，a\rangle，\langle 1，b\rangle，\langle 3，c\rangle，\langle 4，d\rangle\}$，显然 f^{-1} 不是函数.



定义 2 设 f：$A\to B$，如果 f^{-1} 为 B 到 A 的函数，则称 f 为可逆的，且称 f^{-1} 为 f 的逆函数(反函数).

定理 4 设 f：$A\to B$，则 f 可逆 $\Leftrightarrow f$ 为双射

证明 f 可逆 $\Leftrightarrow f^{-1}$：$B\to A\Leftrightarrow\forall b\in B$，存在唯一 $a\in A$ 使 $\langle b，a\rangle\in f^{-1}\Leftrightarrow\forall b\in B$，存在唯一 $a\in A$ 使 $\langle a，b\rangle\in f\Leftrightarrow f$ 是双射. ▌

定理 5 设 f：$A\to B$ 可逆，则 f^{-1}：$B\to A$ 必可逆.

证明 由关系逆的性质知 $(f^{-1})^{-1}=f$，故 $(f^{-1})^{-1}$ 为 A 到 B 的函数，即 f^{-1} 可逆. ▌

推论 若 f：$A\to B$ 为双射，则 f^{-1}：$B\to A$ 也必为双射.

最后考虑两个与函数逆及函数复合都有关系的结论.

定理 6 设 f：$A\to B$ 可逆，则 $f^{-1}\circ f=I_A$，　$f\circ f^{-1}=I_B$.

证明留做习题.

定理 7 设 f：$A\to B$，g：$B\to C$ 均可逆，则 $(g\circ f)$ 可逆，且 $(g\circ f)^{-1}=f^{-1}\circ g^{-1}$.

证明 因 f，g 均可逆，故均为双射，因此 $g\circ f$ 是双射，即 $g\circ f$ 可逆.

$$(g\circ f)^{-1}=(f\lozenge g)^{-1}=g^{-1}\lozenge f^{-1}=f^{-1}\circ g^{-1}.$$

习题八

1. 设 f：$\mathbf{R}\to\mathbf{R}$，g：$\mathbf{R}\to\mathbf{R}$，分别定义如下：

$$f(x)=\begin{cases}x^2, & x\geq 0\\ -1, & x<0\end{cases}\qquad g(x)=\begin{cases}1-x, & x\leq 1\\ 0, & x>1\end{cases}$$

求 $g\circ f$.

2. 设 f：$A\to B$，g：$B\to C$，证明

(1) 若 $g\circ f$ 是满射，则 g 是满射.

(2) 若 $g\circ f$ 是单射，则 f 是单射.

(2) 若 $g\circ f$ 是双射，则 g 是满射，f 是单射.

3. 设 f：$\mathbf{R}\to\mathbf{R}$，$f(x)=\sin x$，f 是否可逆？为什么？

4. 设 A 是任意集合，B 是 A 到 {0，1} 的一切函数所组成的集合，证明：存在 $P(A)$ 到 B 的双射.

5. 设 f：$A\to A$ 是可逆函数，证明 $f\circ f^{-1}=f^{-1}\circ f=I_A$.

第三章　无 限 集

§ 1　集合的势

我们在集合论中讨论问题时，集合所含元素的多少是集合的一个重要特征，对于有限集，我们可以用“元素个数”来刻划集合元素的多少，但对于无限集，“元素个数”变得没有意义，我们只能说无限集具有无穷多个元素，但这是远远不够的. 为了引出一般地刻划集合元素多少的方法，先看下面的例子.

设有一大群羊和一大捆绳子，如果我们不数出羊和绳子的“个数”，要比较羊和绳子是否一样多应如何进行呢？我们可以试图在每只羊上栓一条绳子，如果羊和绳子通过这种方式恰好能两两配对，则羊和绳子一样多，否则不一样多.

一般地，在直观上容易明白，对于两个有限集 A 和 B，当且仅当可以将 A 与 B 的元素两两配对(即建立双射)时，A 与 B 具有同样多的元素. 推而广之，引入下述定义.

定义 1　设 A, B 为任意两个集合，如果存在 A 到 B 的双射，则称 A 与 B 等势 (对等)，记为 $A \sim B$.

我们规定 $\varnothing \sim \varnothing$. 可以证明：两个有限集是等势的，当且仅当它们具有同样多的元素.

例 1　设 $\mathbf{N} = \{0, 1, 2, \cdots, n, \cdots\}$，$E = \{0, 2, 4, \cdots, 2n, \cdots\}$，令 f 是如下映射

$$\begin{array}{ccccccc} 0, & 1, & 2, & \cdots, & n, & \cdots \\ \downarrow & \downarrow & \downarrow & & \downarrow & \\ 0, & 2, & 4, & \cdots, & 2n, & \cdots \end{array}$$

即　$f\colon i \mapsto 2i \qquad \forall i \in \mathbf{N}$.

则　f 是 $\mathbf{N}$ 到 E 的双射，故 $\mathbf{N} \sim E$.

例 2　设 $\mathbf{N} = \{0, 1, 2, \cdots, n, \cdots\}$，$\mathbf{Z} = \{\cdots, -2, -1, 0, 1, 2, \cdots\}$，令 f 是如下映射

$$\begin{array}{ccccccc} 0, & 1, & 2, & 3, & 4, & \cdots \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \\ 0, & 1, & -1, & 2, & -2, & \cdots \end{array}$$

即

$$f(i)=\begin{cases}-\dfrac{i}{2}, & i\text{为偶数}\\ \dfrac{i+1}{2}, & i\text{为奇数}\end{cases}$$

则 f 是 **N** 到 **Z** 的双射，故 **N** ～ **Z**.

例 3 实数区间 $(0, 1)$ ～ (a, b)，其中，$a < b$.

证明 令 f：$x \mid\!\rightarrow (b-a)x+a$ $\quad\forall x\in(0, 1)$

则 f 是 $(0, 1)$ 到 (a, b) 的双射，故 $(0, 1)$ ～ (a, b).

例 4 $(0, 1)$ ～ $(0, \infty)$，$(0, 1)$ ～ $(-\infty, 0)$

证明 令 f：$(0, 1)\rightarrow(0, \infty)$

$$f\text{：}\ x \mid\!\rightarrow \frac{x}{1-x} \qquad \forall x\in(0, 1)$$

下证 f 为双射. $\forall x_1, x_2\in(0,1)$，如果 $f(x_1)=f(x_2)$，即 $\dfrac{x_1}{1-x_1}=\dfrac{x_2}{1-x_2}$，则 $x_1(1-x_2)=x_2(1-x_1)$

即有 $x_1 - x_1x_2 = x_2 - x_2x_1$，故 $x_1 = x_2$. 因此，f 是单射.

$$\forall y\in(0, \infty),\ f(x)=\mathrm{y}\Leftrightarrow\frac{x}{1-x}=\mathrm{y}\Leftrightarrow x=(1-x)y\Leftrightarrow x=\frac{y}{1+y}.$$

故取 $x=\dfrac{y}{1+y}$，则 $x\in(0, 1)$ 且 $f(x)=y$. 因此，f 是满射. 于是 f 是双射.

同理，$(0, 1)$ ～ $(-\infty, 0)$.

例 5 $(0, 1)$ ～ **R**，其中 **R** 为实数集.

证明 令 $f(x)=\mathrm{tg}\ \pi(x-\frac{1}{2})$ $\quad\forall x\in(0, 1)$.

则 f 是 $(0, 1)$ 到 **R** 的双射，故 $(0, 1)$ ～ **R**.

上面例题揭示了一个极其重要的事实：无限集有可能与其真子集等势，后面我们还将证明，一个无限集必定与其某个真子集等势，这点对有限集是无法办到的.

定理 1 设 A，B，C 为任意集合，则

(1) $A\sim A$.

(2) 若 $A\sim B$，则 $B\sim A$.

(3) 若 $A\sim B$，$B\sim C$ 则 $A\sim C$

即等势关系是一个等价关系.

证明留作习题. ▌

定理 2 设 $\mathbf{N}^+$ 为正整数集，$A=\{A_i \mid i\in\mathbf{N}^+\}$，$B=\{B_i \mid i\in\mathbf{N}^+\}$ 为两个集合族，且满

足 $A_i \cap A_j = \varnothing$，$B_i \cap B_j = \varnothing$ $(i \neq j)$. $A_i \sim B_i$，$(i = 1, 2, \cdots)$ 则

$$\bigcup_{i=1}^{\infty} A_i \sim \bigcup_{i=1}^{\infty} B_i \text{，} \bigcup_{i=1}^{m} A_i \sim \bigcup_{i=1}^{m} B_i \qquad (m = 1, 2, \cdots)$$

证明 由于 $A_i \sim B_i$，故存在双射 $f_i: A_i \to B_i$，作映射 $f: \bigcup_{i=1}^{\infty} A_i \to \bigcup_{i=1}^{\infty} B_i$，对任意 $x \in \bigcup_{i=1}^{\infty} A_i$，

当 $x \in A_i$ 时，令 $f(x) = f_i(x)$. 则易验证，f 是双射，因此 $\bigcup_{i=1}^{\infty} A_i \sim \bigcup_{i=1}^{\infty} B_i$.

同理可构造 $\bigcup_{i=1}^{m} A_i$ 到 $\bigcup_{i=1}^{m} B_i$ 的双射，从而知 $\bigcup_{i=1}^{m} A_i \sim \bigcup_{i=1}^{m} B_i$.

定理 3 无限集必与它的一个真子集等势.

证明 设 A 为一个无限集，则 $A \neq \varnothing$，故可取 $a_1 \in A$，因 A 为无限集，故 $A - \{a_1\} \neq \varnothing$，从而又可取 $a_2 \in A - \{a_1\}$， 同样，$A - \{a_1, a_2\} \neq \varnothing$，又可取 $a_3 \in A - \{a_1, a_2\}$，…，一直进行下去，我们便可得到一列彼此相异的元素

$$a_1, a_2, a_3, \cdots$$

记 $A_0 = A - \{a_1, a_2, a_3, \cdots\}$，则 $A = A_0 \cup \{a_1, a_2, a_3, \cdots\}$. 令 $B = A - \{a_1\} = A_0 \cup \{a_2, a_3, a_4, \cdots\}$，则 $B \subset A$. 作函数 $f: A \to B$，使

$$f(a_i) = a_{i+1} \qquad i = 1, 2, \cdots$$
$$f(x) = x \qquad x \in A_0$$

则 f 是 A 到 B 的双射，故 $A \sim B$. 这样我们就证明了 A 与其真子集 B 等势. ▌

能与真子集等势，是无限集与有限集的根本区别，故可用此性质来定义无限集.

在定义 1 中，我们建立了等势的概念，但并未明确定义集合的“势”，在此我们不打算讨论“势”的形式定义，只给出一种直观概念.

两个集合等势，意味着这两个集合的元素可以两两配对，因此，可将等势理解为“具有同样多的元素”，按照这种理解，我们可以将互相等势的集合放在一起，并给出一个专门的标志，来表示这些集合所具有的元素数量. 当然，这里引入的标志不一定是通常意义下的整数.

由定理 1 知，等势关系是一个等价关系，因此可以根据这个关系将所有集合划分成一些等价类，每个等价类由互相等势的所有集合构成，所以，将互相等势的所有集合放在一起，给出一个专门的标志，也就相当于对于每个等价类给出一个标志，由于每个集合恰好处于一个等价类中，因此，按照这种方法能够保证每个集合具有一个唯一的标志，这个标志就称为集合的势.

综上所述，集合的势是集合元素数量的一个标志，是有限集元素个数的推广，等势

的集合具有相同的势，不等势的集合具有不同的势. 对任意集合 A，A 的势用 $|A|$ 或 $\overline{\overline{A}}$ 表示. 我们规定，与 {1，2，…，n} 等势的集合(即具有 n 个元素的集合)的势为 n，空集 $\varnothing$ 的势为 0，与 $\mathbf{N}$ 等势的集合的势为 $\aleph_0$，与(0，1)等势的集合的势为 $\aleph$，…

集合 A 与集合 B 具有相同的势又可以说成 A 的势等于 B 的势，记为 $|A|=|B|$ 或 $\overline{\overline{A}}=\overline{\overline{B}}$，于是 $|A|=|B| \Leftrightarrow A\sim B$. A 的势为 α 记为 $|A|=\alpha$，于是 $|\mathbf{N}|=\aleph_0$.

设 A，B 是两个集合，$A\sim B$ 意味着 A 与 B 有同样多的元素，$A\not\sim B$ 且 A 与 B 的某子集等势，则自然意味着 A 的元素少于 B 的元素，或说 A 的势小于 B 的势.

定义 2 设 A，B 是两个集合，若 $A\not\sim B$ 且 A 与 B 的某子集等势，则称 A 的势小于 B 的势，记为 $|A|<|B|$. 象通常一样，下面将用 $|A|\leqslant|B|$ 表示“ $|A|$ 小于或等于 $|B|$ ”.

定理 4 $|A|\leqslant|B| \Leftrightarrow$ 存在 A 到 B 的单射.

证明 若 $|A|\leqslant|B|$，则 A 与 B 的某子集等势，设 $A\sim B_1\subseteq B$，则必存在双射 f：$A\to B_1$，显然，f 必为 A 到 B 的单射.

反之，若 f：$A\to B$ 是单射，则 f 是 A 到 $f(A)\subseteq B$ 的双射，故 $A\sim f(A)\subseteq B$，即有 $|A|\leqslant|B|$. ▌

例 6 $|\mathbf{N}|<|(0,1)|$，即 $\aleph_0<\aleph$.

证明 令 f：$\mathbf{N}\to(0,1)$，定义如下

$$f:\ n\mapsto\frac{1}{n+2} \qquad \forall n\in\mathbf{N}$$

则 f 是 $\mathbf{N}$ 到 (0，1) 的单射，故 $|\mathbf{N}|\leqslant|(0,1)|$，下证 $|\mathbf{N}|\neq|(0,1)|$.

用反证法，设 $\mathbf{N}\sim(0,1)$，则存在双射 g：$\mathbf{N}\to(0,1)$，于是 $(0,1)=g(\mathbf{N})=\{g(0),g(1),\cdots\}$. 现将 (0，1) 中的实数均表示成如下无限小数形式：

$$g(0)=0.a_{00}a_{01}a_{02}\cdots$$
$$g(1)=0.a_{10}a_{11}a_{12}\cdots$$
$$g(2)=0.a_{20}a_{21}a_{22}\cdots$$
$$\cdots$$

(注：(0，1)中任一实数均可唯一表示成无限小数形式，对有限小数，比如 0.3，可以表示成以“9”为循环节的无限循环小数，$0.3=0.2999\cdots$). 构造实数 $\tilde{a}$，使 $\tilde{a}=0.\tilde{a}_{00}\tilde{a}_{11}\tilde{a}_{22}\cdots=$ 其中 $\tilde{a}_{ii}\neq0$，$\tilde{a}_{ii}\neq9$，$\tilde{a}_{ii}\neq a_{ii}$ $i=0$，1，2，… 则 $\tilde{a}\in(0,1)$. 另一方面，由于对任何 $i\in\mathbf{N}$，$\tilde{a}_{ii}\neq a_{ii}$，所以 $\tilde{a}$ 不同于任何 $g(i)$，故 $\tilde{a}\notin g(\mathbf{N})$，即 $\tilde{a}\notin(0,1)$，矛盾，可见 $\mathbf{N}\not\sim(0,1)$，从而 $|\mathbf{N}|<|(0,1)|$.

由上面例题我们知道 $\aleph_0<\aleph$，于是可提出问题：在 $\aleph_0$ 与 $\aleph$ 之间是否存在其他的势呢？Contor 猜想：$\aleph_0$ 与 $\aleph$ 之间不存在其他势，这就是著名的连续统假设，这是数学中的

一个基本问题，也是集合论中最难的问题之一，这个问题至今没有得到解决.

集合势的“≤”关系，满足通常实数小于等于关系的某些性质，例如

定理 5　设 A，B，C 为任意集合，则

1) $|A|\leqslant|A|$

2) $|A|\leqslant|B|$，$|B|\leqslant|C|\Rightarrow|A|\leqslant|C|$

3) $|A|\leqslant|B|$，$|B|\leqslant|A|\Rightarrow|A|=|B|$

证明

(1) 因为 $|A|=|A|$，因此 $|A|\leqslant|A|$.

(2) 若 $|A|\leqslant|B|$，$|B|\leqslant|C|$，则存在单射 f：$A\to B$，g：$B\to C$，于是 $g\circ f$ 是 A 到 C 的单射，所以 $|A|\leqslant|C|$.

(3) 该结论称为 Bernstein 定理，证明较为复杂，在此不再讨论. ▌

由上面定理可知，集合势的“≤”关系为一个偏序关系.

定理 6 (三歧定理) 对任意集合 A 与 B，以下三式

$$|A|<|B|,\quad |B|<|A|,\quad |A|=|B|$$

中恰有一个成立.

证明　略. ▌

例 7　利用 Bernstein 定理证明 $[0,1]\sim(0,1)$.

证明　令 f：$(0,1)\to[0,1]$

$$f(x)=x\qquad \forall x\in(0,1)$$

则 f 是$(0,1)$到 $[0,1]$ 的单射，故 $|(0,1)|\leqslant|[0,1]|$,

再令　g：$[0,1]\to(0,1)$

$$g(x)=1/4+1/2x\qquad \forall x\in[0,1]$$

则 f 是 $[0,1]$ 到 $(0,1)$ 的单射，故 $|[0,1]|\leqslant|(0,1)|$. 因此，由 Berbstein 定理可知 $|[0,1]|=|(0,1)|$.

现在我们已经能够说出一些集合的势，比如有限集的势、自然数集 **N** 的势、区间 $(0,1)$ 的势等. 除此之外是否还存在别的势呢？特别地，是否存在一个最大的势呢？Contor 定理回答了这些问题.

定理 7 (Contor) 对任意集合 A，必有　$|A|<|2^A|$

证明　令

$$f:\ a\mapsto\{a\}\qquad \forall a\in A$$

则 f 是 A 到 2^A 的单射，故知 $|A|\leqslant|2^A|$. 下证 $A\not\sim 2^A$. 用反证法，设 $A\sim 2^A$，则存在双射 g：$A\to 2^A$.　$\forall a\in A$，若 $a\in g(a)$ 则称 a 为内元，若 $a\notin g(a)$, 则称 a 为外元. 由于对 A 中任何元素 a，$a\in g(a)$与 $a\notin g(a)$ 恰有一个成立，因此 A 的任何元素或为内元或为外元，两者必居其一. 设 B 为 A 中所有外元构成的集合， 由于 g 为双射，故必存在 $b\in A$ 使 $g(b)=B$，现考察 b 是内元还是外元. 若 b 是内元，则 $b\in g(b)=B$，由 B 的定义，b 是外元，矛盾. 若 b 为外元，则 $b\notin g(b)=B$，由 B 的定义，b 是内元，矛盾. 因此，$A\not\sim 2^A$. 于是 $|A|<|2^A|$ 得证. ▌

习题一

1. 证明定理 2，即证明等势关系是等价关系.
2. 证明：若 $|A|<|B|$，$|B|<|C|$ 则 $|A|<|C|$.
3. 设 $|A|=a$，$|B|=b$，且 $A\cap B=\varnothing$，则 $A\cup B$ 的势称为 a，b 的和，记为 $a+b$. 证明：若 a，b，d 均为集合的势，则
   (1) 当 $a\leqslant b$ 时 必有 $a+d\leqslant b+d$.
   (2) 用反例说明，$a<b$ 推不出 $a+d<b+d$.
4. 仿照习题 3 定义集合势的积，并证明势的积也具有习题 3 指出的类似性质.

§2 可数集

定义 1 与自然数集 **N** 等势的（或说势为$\aleph_0$的）集合称为可数集(可列集).

例如，自然数集 **N** 是可数集，整数集 **Z**、偶数集 E 也都是可数集，区间 (0，1) 不是可数集. 一个集合 A，如果是可数集，也说 A 具有可数(可列)个元素.

引理 1 对任意集合 A， 当且仅当 A 的元素可不重复的排成如下一个无穷序列

$$a_0，a_1，a_2，\cdots a_n，\cdots$$

证明 设 A 是可数集, 即 $A\sim\mathbf{N}$，则存在双射 f：$\mathbf{N}\to A$，令 $a_i=f(i)$，则 $A=f(\mathbf{N})$的元素可（不重复的）排成如下一列

$$a_0，a_1，a_2，\cdots$$

反之，若 A 的元素可不重复的排成上述序列，令 $f(i)=a_i$，则 f：$\mathbf{N}\to A$ 是一个双射，故 $\mathbf{N}\sim A$，即 A 是可数集.

引理 2 可数集的无穷子集必是可数集.

证明 设 A 是一可数集，则 A 的元素可排成如下一列

$$a_0，a_1，a_2，\cdots$$

设 B 是 A 的任一无穷子集，则 B 的元素构成上述序列的一个子列，从而按其在上面序列中的顺序也排成了如下一列

$$a_{i_0},a_{i_1},a_{i_2},\cdots$$

故 B 为可数集. ▌

定理 1 任何无限集必有可数子集.

证明 设 A 是无限集，按上节定理 3 的方法，可从 A 中取出一列彼此相异的元素

$$a_0，a_1，a_2，\cdots$$

这些元素构成 A 的一个可数子集. ▌

定理 2 在可数集中加入(或删除)有限个元素，仍为可数集.

证明留作习题. ▌

定理 3 设 A_1，A_2 为可数集，则 $A_1 \cup A_2$ 是可数集.

证明 分两种情况讨论.

(Ⅰ) $A_1 \cap A_2 = \varnothing$.

因为 A_1，A_2 是可数集，根据引理 1 可设

$$A_1 = \{a_1, a_2, \cdots, a_n, \cdots\}$$

$$A_2 = \{b_1, b_2, \cdots, b_n, \cdots\}$$

其中, a_1，a_2，…，a_n，…互不相同，b_1，b_2，…，b_n，…互不相同. 则

$$A_1 \cup A_2 = \{a_1, b_1, a_2, b_2, \cdots, a_n, b_n, \cdots\}$$

从而易知 $A_1 \cup A_2$ 是可数集.

(Ⅱ) $A_1 \cap A_2 \neq \varnothing$.

令 $A_2' = A_2 - A_1$，则 $A_1 \cup A_2 = A_1 \cup A_2'$ 且 $A_1 \cap A_2' = \varnothing$. 由于 A_2 是可数集，必为可数集或有限集，故由情况(Ⅰ)及定理 2 知 $A_1 \cup A_2'$ 即 $A_1 \cup A_2$ 为可数集. ▌

推论 设 A_1，A_2，…，A_n 为 n 个可数集，则 $A_1 \cup A_2 \cup \cdots \cup A_n$ 必为可数集.

证明 利用定理 3 及归纳法，即可证得. ▌

定理 4 设 A_1，A_2，…，A_n，…为一列可数集，则 $\bigcup_{i=1}^{\infty} A_i$ 是可数集.

证明 分两种情况：

(Ⅰ) $A_i \cap A_j = \varnothing\ (i \neq j)$，设

$$A_1 = \{a_{11}, a_{12}, a_{13}, \cdots\}$$

$$A_2 = \{a_{21}, a_{22}, a_{23}, \cdots\}$$

$$A_3 = \{a_{31}, a_{32}, a_{33}, \cdots\}$$

$$\cdots$$

则可将 $\bigcup_{i=1}^{\infty} A_i$ 的元素排成下列无穷方阵

$$\begin{array}{cccc}
a_{11} \rightarrow a_{12} & a_{13} \rightarrow a_{14} & \cdots \\
\downarrow \nearrow & \downarrow \nearrow & \\
a_{21} & a_{22} & a_{23} & a_{24} \cdots \\
\downarrow \nearrow & \downarrow & & \\
a_{31} & a_{32} & a_{33} & a_{34} \cdots \\
\downarrow \nearrow & & & \\
a_{41} & a_{42} & a_{43} & a_{44} \cdots \\
\cdots & \cdots & \cdots & \cdots
\end{array}$$

按图中箭头方向可将$\bigcup_{i=1}^{\infty}A_i$的元素不重复的排成一个无穷序列，故$\bigcup_{i=1}^{\infty}A_i$为可数集.

(Ⅱ) $\exists i, j\in\mathbf{N}^+$，$i\neq$ j，$A_i\cap A_{\text{j}}\neq\varnothing$.

按情况(Ⅰ)中方法将$\bigcup_{i=1}^{\infty}A_i$的元素排成一列，在排列过程中，若要排的元素与前面某元素相同，则不排这个元素，这样便可把$\bigcup_{i=1}^{\infty}A_i$的所有元素无重复的排成一个无穷序列，于是$\bigcup_{i=1}^{\infty}A_i$是可数集. ▌

推论 设 A，B 为可数集，则 $A\times B$ 必为可数集.

证明 设 $A=\{a_1, a_2, a_3, \cdots\}$，$B=\{b_1, b_2, b_3, \cdots\}$，令

$$A_1=\{\langle a_1, b_i\rangle \mid i\in\mathbf{N}^+\}=\{a_1\}\times B$$
$$A_2=\{\langle a_2, b_i\rangle \mid i\in\mathbf{N}^+\}=\{a_2\}\times B$$
$$\cdots$$

则 A_i ($i=1, 2, \cdots$) 均为可数集，所以 $A\times B=\bigcup_{i=1}^{\infty}A_i$ 为可数集. ▌

定理 5 设 A 为无限集，B 为可数集或有限集，则 $A\sim A\cup B$.

证明 不妨设 $A\cap B=\varnothing$，设 B 为可数集，令

$$B=\{b_0, b_1, b_2, \cdots\}$$

由于 A 为无限集，故可从中取出可数子集 A_1，令

$$A_1=\{a_0, a_1, a_2, \cdots\}$$
$$A_0=A-A_1.$$

则 $A=A_0\cup A_1$，$A\cup B=A_0\cup(A_1\cup B)$.

由于 $A_0\sim A_0$，$A_1\sim(A_1\cup B)$，且 $A_0\cap A_1=\varnothing$，$A_0\cap(A_1\cup B)=\varnothing$，故由上节定理 2 知 $A_0\cup A_1\sim A_0\cup(A_1\cup B)$，即 $A\sim A\cup B$.

B 为有限集的情况留作习题. ▌

例 1. 设 $\mathbf{N}$ 为自然数集，则 $\mathbf{N}\times\mathbf{N}$ 可数.

例 2. 有理数集 $\mathbf{Q}$ 可数.

证明 先证正有理数集 $\mathbf{Q}^+$可数，这里给出两种证法.

［证法一］令 $\boldsymbol{Q}'=\{\langle p, q\rangle \mid p, q\in\mathbf{N}^+, q\neq 0, (p, q)=1\}$

即 $\boldsymbol{Q}'$ 由 $\mathbf{N}\times\mathbf{N}$ 中的互素正整数对构成，显然，$\boldsymbol{Q}'$ 是 $\mathbf{N}\times\mathbf{N}$ 的无穷子集，故必是可数集，作函数 f: $\boldsymbol{Q}'\to\mathbf{Q}^+$

$$f:\langle p,\ q\rangle \mid\!\rightarrow pq \qquad \forall\ \langle p,\ q\rangle \in \boldsymbol{Q}'$$

则 f 是双射，故 $\boldsymbol{Q}' \sim \mathbf{Q}^+$. 从而 $\mathbf{Q}^+$ 是可数集.

［证法二］令 $Q_i = \{\frac{1}{i},\ \frac{2}{i},\ \frac{3}{i},\ \cdots\}$，$i = 1$，2，3…

则 Q_i 是可数集，且 $\mathbf{Q}^+ = \bigcup_{i=1}^{\infty} Q_i$，故知 $\mathbf{Q}^+$ 是可数集. ▌

显然，正有理数集 $\mathbf{Q}^+$ 与负有理数集 $\mathbf{Q}^-$ 是等势的，因此 $\mathbf{Q}^-$ 也是可数集. 于是 $\mathbf{Q} = \mathbf{Q}^+ \cup \{0\} \cup \mathbf{Q}^-$ 是可数集.

例 3．设 $A = \{a,\ b\}$，A^+ 是由 A 中字符 a，b 组成的有限长字符串构成的集合，则 A^+ 是可数集.

证明　令 f：$A^+ \rightarrow \mathbf{Q}$

$$f(a) = \begin{cases} 0.1, & a\text{是空串} \\ 0.\delta_1\delta_2\cdots\delta_n 1, & a = {}'a_1a_2\cdots a_n{}' \end{cases}$$

其中　$\delta_i = \begin{cases} 0, & a_i = a \\ 1, & a_i = b \end{cases}$

则 f 是 A^+ 到 $\mathbf{Q}$ 的单射，故 $A^+ \sim f(A^+) \subseteq \mathbf{Q}$.

显然，$f(A^+)$ 是 $\mathbf{Q}$ 的无限子集，因此是可数集，进而 A^+ 是可数集. ▌

习题二

1. 设 A 为无限集，B 为有限集，证明 $A \sim A \cup B$.
2. 证明定理 2.
3. 证明无理数集不是可数集.
4. 证明 $\mathbf{N}$ 的所有有限子集构成的集合是可数集.
5. 证明由实数轴上互不相交的有限开区间所成的集合是一个可数集.
6. 对任意有限非空字母表Σ，证明Σ上所有有限长字符串构成的集合是可数集.
7. 证明二进制有限小数所成的集合是可数集.
8. 构造双射 f：［0，1］→(0，1).
9. 构造双射 f：［0，1］→(－∞，∞).

**§3　连续势集

定义 1　与实数区间 (0，1) 等势的（或说势为ℵ的）集合称为连续势集. ℵ称为连续

势.

例如，(0，1)，[0，1]，(*a*，*b*)，(0，∞)，(-∞，0)，**R** 等都是连续势集，**N**，**Q** 等都不是连续势集.

定理 1　设 A 为连续势集，B 至多为连续势集，则 $A\cup B$ 为连续势集.

证明　不妨设 $A\cap B=\varnothing$，因为 A 是连续势集，故 $A\sim(0，1)$，又因为 B 至多是连续势集，故 $B\sim C\subseteq(1，2)$. 由于 $A\cap B=\varnothing$，$(0，1)\cap C=\varnothing$，故由 §1 定理 2 知 $A\cup B\sim(0，1)\cup C\subseteq\mathbf{R}$，故

$$|A\cup B|\leqslant|\mathbf{R}|，\text{又}$$

$$|\mathbf{R}|=|(0，1)|\leqslant|(A\cup B)|，$$

因此，根据 Bernstein 定理有 $|A\cup B|=|\mathbf{R}|=\aleph$. ▌

推论　设 A 为连续势集，B_1，B_2，…，B_n 至多为连续势集，则 $A\cup B_1\cup\cdots\cup B_n$ 为连续势集.

定理 2　设 A 是一个连续势集，$B_i(i=1，2，3，\cdots)$至多是连续势集，则 $A\cup B_1\cup B_2\cup\cdots\cdots$是连续势集.

证明留作习题. ▌

定理 3　(0，1)×(0，1)为连续势集

证明　按如下方式构造函数 f：(0，1)×(0，1)→(0，1)：

$\forall\langle a，b\rangle\in(0，1)\times(0，1)$，　a，b 均可唯一表为一个无穷小数，设

$$a=0.a_1a_2a_3\cdots$$

$$b=0.b_1b_2b_3\cdots$$

令　　$f：\langle a，b\rangle\mid\!\rightarrow 0.a_1b_1a_2b_2\cdots$

则 f 为(0，1)×(0，1)到(0，1)的单射，故

$$|(0，1)\times(0，1)|\leqslant|(0，1)|$$

又取 $A=\{\langle 0.5，a\rangle\mid a\in(0，1)\}$，则

$$A\subseteq(0，1)\times(0，1)\text{ 且 }A\sim(0，1).$$

故 $|(0，1)|\leqslant|(0，1)\times(0，1)|$. 从而 $|(0，1)\times(0，1)|=|(0，1)|=\aleph$. ▌

推论 1　设 A，B 为连续势集，则 $A\times B$ 为连续势集.

推论 2　设 A 为连续势集，则 $A^n=A\times A\times\cdots\times A$ 为连续势集.

定理 4　由 a，b 两个符号重复排列所成的无穷序列的全体构成的集合：

$$D=\{(a_1，a_2，a_3，\cdots)\mid a_i\in\{a，b\}，i=1，2，\cdots\}$$

具有连续势.

证明　将 D 表为两个分离子集 A 与 B 的并：若 $(a_1，a_2，\cdots)\in D$ 从某项开始以后全为 a，则把它作为 A 的元素，否则把它作为 B 的元素. 则 A 是可数集(留作习题). 下证 B 是连续势集.

令　　$g(a_1，a_2，\cdots)=0.\delta_1\delta_2\cdots$　　$\forall(a_1，a_2，\cdots)\in B$

其中 $\delta_i=\begin{cases}0, & a_i=a\\ 1, & a_i=b\end{cases}$

则 g 为 B 到二进制无穷小数全体的双射，因为二进制无穷小数与 (0，1)中的实数一一对应，所以，二进制无穷小数全体所成集合为连续势集，从而 B 是连续势集，于是，$D=A\cup B$ 是连续势集. ▌

定理 5 $|2^{\mathbf{N}}|=\aleph$.

证明 设 D 为 0，1 两个符号重复排列所成的无穷序列的全体，则由定理 4，$|D|=\aleph$. 令 f：$2^{\mathbf{N}}\to D$ 定义如下

$$\forall A\subseteq\mathbf{N},\ f(A)=(a_0,\ a_1,\ a_2,\ \cdots,\ )$$

其中 $a_i=\begin{cases}0, & i\notin A\\ 1, & i\in A\end{cases}$

则 f 是 $2^{\mathbf{N}}$ 到 D 的双射，故 $|2^{\mathbf{N}}|=|D|=\aleph$.

习题三

1. 证明定理 4 中的集合 A 是可数集.
2. 证明推论 1.
3. 证明$\aleph\cdot\aleph_0=\aleph$, 即 $|\mathbf{N}\times(0,\ 1)|=\aleph$.

*§4 关于集合论的讨论

由于集合论中的基本概念——集合，是建立在直观描述的基础上的，并未对其做清楚、严格的定义，因此，集合论从产生之日起就受到一部分数学家的激烈反对，同时，从上一世纪末开始，形形色色的关于集合论的悖论不断出现.

所谓悖论，是指这样一个论断 P，从 P 为真可导出 P 为假，从 P 为假又可导出 P 为真. 例如，假设有人断言“我在说谎”，那么，这句话就是一个悖论. 因为，如果这句话是真的，即他在说谎，从而他所说的“我在说谎”这句话就是假的，反之，如果这句话是假的，即他没在说谎，于是他所说的“我在说谎”这句话就是真的. 总之，

“我在说谎”为真 $\Leftrightarrow$“我在说谎”为假.

因此，这是一个悖论.

现在，我们来介绍集合论中两个著名的悖论.

(1) Cantor 悖论. 设 C 为所有集合构成的集合，则由 Cantor 定理知 $|C|<|2^C|$. 另一方面，由于 C 是所有集合构成的集合，故必有 $2^C\subseteq C$，因此，$|2^C|\leqslant|C|$. 于是导致矛盾. 这个矛盾称为 Cantor 悖论.

(2) Russell 悖论. 设 A 是一个集合，由集合的概念知 $A\in A$ 与 $A\notin A$ 中恰有一个成立，据此可将集合分成两类：满足 $A\in A$ 的集合 A 归于第一类，满足 $A\notin A$ 的集合 A 归于第二类，令 S 是第二类集合的全体构成的集合，即

$$S=\{A\mid A\notin A\}$$

考察 S 应属于哪一类，若 $S\in S$，则由 S 的定义知 $S\notin S$. 反之，若 $S\notin S$，则由 S 的定义知 $S\in S$. 从而产生一个悖论，这个悖论称为 Russell 悖论.

Russell 悖论从集合的基本概念入手，完全击中了“通俗集合论”的要害，可以说，不对集合这个概念作出严格的限制，就无法避免 Russell 悖论.

Russell 悖论有一个有趣的通俗化形式，利用这个通俗化形式，可以帮助我们更好地理解 Russell 悖论.

(3)理发师悖论. 一个乡村理发师宣称，他给本村所有不给自己理发的人理发，但不给本村所有自己理发的人理发. 那么，我们问，理发师本人的头发由谁来理？为了叙述更加清楚，我们不妨把不给自己理发的人归为 P 类，自己理发的人归为 Q 类，则理发师的论断可以说成：他给本村所有 P 类中的人理发，但不给本村所有 Q 类中的人理发. 如果理发师自己理发，则他属于 Q 类，那么，根据论断的第二部分，他不该给自己理发. 反之，若他不给自己理发，则他属于 P 类，按其论断的第一部分，他该给自己理发. 因此不论理发师是不是自己理发，都会导致相反的结论. 这是一个悖论.

现在来考察理发师悖论与 Russell 悖论的关系. 若用 xRy 表示 x 给 y 理发， a 表示理发师，则理发师的论断可表示为

$$aRy\Leftrightarrow y\not R y \tag{1}$$

若取 $y=a$，则导致矛盾.

Russell 悖论可表示为 $A\in S\Leftrightarrow A\notin A$

取 $A=S$，则导致矛盾.

由此可见，Russell 悖论与理发师悖论具有完全相同的形式，事实上，如果我们把(1)式看成一个一般形式，则这两个悖论，可以看成是在(1)式中对 a 与 R 作不同解释得到的特例，对 a 与 R 作出其它各种不同解释还可得到其它一些有趣的悖论，在此不再一一介绍.

追究以上各悖论发生的原因，我们发现这些悖论均源于“自我相关性”，例如，我们讨论 Russell 悖论时，把 S 的定义条件用于 S 自身，便发生了矛盾，同样，在讨论理发师悖论时，也是当把理发师的论断用于其自身时产生了矛盾.

为了避免理发师悖论，只要保证理发师的论断不描述自身即可，比如，我们让理发师搬到外地或不把理发师当“人”；同样，为了避免 Russell 悖论，我们应该保证不用 S 的定义条件考察 S 自身，比如，我们可以不把 S 当作一个集合.

不把 S 等诸如此类的事物全体当做一个集合，这就要求我们对于“集合”概念做出某些严格的限制，使其不能太漫无边际，并且还要讨论，对集合可以做哪些操作，不能做哪些操作等. 为了填补 Cantor 在理论上的不足，从而维护 Cantor 理论，在 190 8 年，E. Zermelo 首先为集合论设立了一套比较完整的公理，这些公理主要是明确了对已知集合做

哪些事情是合法的，以后经过 A. Fraenkel 等人的补充和完善，形成了现在所谓的 ZF 公理系统. 较晚一些，还有所谓的 GB 公理系统，是由 von Neumann，P. Bernays，K. Godel 等人建立的. 在这样的公理系统中，已知的悖论被排除了，但根据 Godel 不完全性定理，这些系统均不能在本系统中证明其无矛盾性.

第二篇 代数结构

在一个集合上定义一个或多个运算，就形成了一个代数运算系统，或称代数系统. 代数结构就是研究代数系统的一般性质及各种特殊代数系统的学科. 其理论和方法不仅对其它数学学科产生着深远的影响，在计算机科学领域也有着广泛的应用.

本篇首先介绍了一般代数系统的基本理论，主要包括同态、同构、同余关系、商代数等基本概念以及一些相关的基本理论. 这些内容有着较大的普遍性，也为以后的讨论提供了基础. 然后逐步介绍群、环、域、格与布尔代数等一些特殊代数系统. 群是较为简单的一类代数系统，也是本篇的重点，通过这部分内容的学习，可使读者初步掌握研究代数结构的基本方法，并为以后的学习打好基础. 对环和域我们着重介绍一些基本的概念和性质，这些内容与群论中的某些理论有着极大的类似性. 格与布尔代数与计算机科学有着密切关系，在本篇中介绍了其初步理论，特别对有限布尔代数的结构作了详细讨论.

第四章　代数系统

§1　运　算

对运算的概念我们早有认识. 比如，两实数 x，y 做加法运算得到一实数 $x+y$；两集合 A，B 做并运算得到一集合 $A\cup B$；一集合 A 做补运算得到一集合 $\sim A$ 等. 从这些例子可以看出，运算实际上是由一组事物唯一确定一个事物的一种法则. 现在我们在广泛的意义下给出运算的定义.

定义 1　设 A 是一个集合，$A\times A$ 到 A 的映射称为 A 上的二元运算. 一般地，A^n 到 A 的映射称为 A 上的 n 元运算.

设 f 是 A 上的 n 元运算，对任意的 x_1，x_2，…，$x_n\in A$，$f(\langle x_1, x_2, \cdots, x_n\rangle)$ 称作 x_1，x_2，…，x_n 在 f 下的运算结果，并简记为 $f(x_1, x_2, \cdots, x_n)$.

例 1　数的加法是实数集 $\mathbf{R}$ 上的二元运算. 因为对任意 $\langle a, b\rangle\in\mathbf{R}\times\mathbf{R}$，通过加法可唯一确定一个实数 $c=a+b$，故加法是 $\mathbf{R}\times\mathbf{R}$ 到 $\mathbf{R}$ 的映射；即是 $\mathbf{R}$ 上的二元运算. 同样，数的乘法、减法都是实数集 $\mathbf{R}$ 上的二元运算.

例 2　数的除法不是实数集 $\mathbf{R}$ 上的二元运算. 因为 0 不能做除数，某些实数对 $\langle a, b\rangle$ 不能通过除法唯一确定一个与之相应的实数（比如，$2/0$ 无意义），即除法不是一个 $\mathbf{R}\times\mathbf{R}$ 到 $\mathbf{R}$ 的映射，即不是 $\mathbf{R}$ 上的二元运算.

但是，任何非 0 实数 a，b，通过除法可唯一确定一个非 0 实数 a/b，故除法是非 0 实数集上的二元运算.

例 3　设 S 是一个集合，集合的并、交是 $P(S)$ 上的二元运算.

因为对任意 $\langle A, B\rangle\in P(S)\times P(S)$，通过集合的并（交）可唯一确定 $P(S)$ 的一个元素 $A\cup B$（或 $A\cap B$），故集合的并（交）是 $P(S)$ 上的二元运算.

例 4　设 $\mathbf{R}$ 是实数集，令 f：$\langle a, b\rangle\mapsto a+b-ab$　　$\forall a, b\in\mathbf{R}$

则 f 是 $\mathbf{R}$ 上的二元运算.

例 5　设 $\mathbf{R}$ 是实数集，令

g：$\langle a, b\rangle\mapsto\min\{a, b\}$

$$h:\langle a,\ b\rangle \mapsto \max\{a,\ b\} \qquad \forall\, a,\ b\in \mathbf{R}$$

则 g，h 均为 $\mathbf{R}$ 上的二元运算.

今后我们将主要讨论二元运算，因此，我们约定，除非特别指明，我们所说的“运算”均是指“二元运算”.

为了符合通常的习惯及表达的简明，我们总是用一些称作运算符的特殊符号，比如：$\lozenge$，$*$，$\bullet$，$\circ$，$+$ $\times$ 等表示二元运算，且将 a，b 在某运算“$*$”下的运算结果 $*(a,\ b)$ 记为 $a*b$. 在不引起混乱的情况下，也可省略运算符，把 $a*b$ 写成 ab.

例如，实数 a，b 作加法运算的结果，记做 $a+b$；实数 a，b 作乘法运算的结果，记作 $a\bullet b$ 或 ab；集合 A，B 作并、交运算的结果记作 $A\cup B$，$A\cap B$. 如果用 $*$ 表示例 4 的运算 f，则

$$a*b=a+b-ab$$

如果用 $\circ$、$\oplus$ 表示例 5 引进的运算 g，h，则

$$a\circ b=\min\{a,\ b\}$$

$$a\oplus b=\max\{a,\ b\}$$

例 6　设 n 为正整数，$\mathbf{Z}_n$ 为所有模 n 剩余类构成的集合：

$$\mathbf{Z}_n=\{[0],[1],\cdots,[n-1]\}$$

定义运算 $+_n$ 与 $\times_n$ 如下:

$$\forall\,[i],[j]\in \mathbf{Z}_n,\ \text{规定}$$

$$[i]+_n[j]=[i+j]$$

$$[i]\times_n[j]=[i\bullet j]$$

这里，“$+$”与“$\bullet$”分别为通常整数的加法和乘法. 我们已经知道，$\mathbf{Z}_n$ 中的元素 $[i]$ 的表示方法不是唯一的. 例如

$$[0]=[n],[1]=[n+1],\cdots$$

事实上，$\forall\, i'\in[i],[i']=[i]$，因此，为了说明如上定义的 $+_n$，$\times_n$ 确为二元运算，必须要说明 $[i]+_n[j]$ 与 $[i]\times_n[j]$ 由剩余类 $[i]$，$[j]$ 唯一确定，而与代表元 i，j 的选取无关. 为此，设

$$[i']=[i],[j']=[j]$$

则　$i'\equiv i \bmod n$,　$j'\equiv j \bmod n$,　即　$n\mid i'-i$,　$n\mid j'-j$.

由　$(i'+j')-(i+j)=(i'-i)+(j'-j)$　知　$n\mid(i'+j')-(i+j)$

即　$(i'+j')\equiv(i+j) \bmod n$, 从而　$[i'+j']=[i+j]$.

也就是说，当另外选取 $[i]$ 和 $[j]$ 的代表元时运算结果不变，因此，$[i+j]$ 由 $[i]$，$[j]$ 唯一确定，从而 $+_n$ 确为二元运算，同理可证，$\times_n$ 也为二元运算.

设 f 是 A 上的一个 n 元运算，有时，我们需要考虑 A 的子集在这个运算下的性质，为此，引入下述定义.

定义 2　设 f 是 A 上的 n 元运算，$S \subseteq A$，如果对 x_1，x_2，…，$x_n \in S$，恒有 $f(x_1, x_2, \cdots, x_n) \in S$，则称 S 对运算 f 是封闭的.

自然数集对实数集上的加法运算、乘法运算都是封闭的，但对实数集上的减法运算不是封闭的. 设 A 是 S 的子集，则 $P(A)$ 对 $P(S)$ 上的并运算、交运算都是封闭的. 设 g，h 是例 5 定义的实数集 $\mathbf{R}$ 上的二元运算，则 $\mathbf{R}$ 的任何子集对 g，h 都是封闭的.

很明显，要确定一个二元运算，就是要确定任意两个元素的运算结果，当 A 是有限集时，A 上的运算可用一个表来表示：设 $A=\{a_1, a_2, \cdots, a_n\}$，“$\circ$” 是 A 上的运算，则表 1.1 称为运算“$\circ$”的运算表:

$\circ$	a_1	a_2	…	a_j	…	a_n
a_1	a_{11}	a_{12}		a_{1j}		a_{1n}
a_2	a_{21}	a_{22}		a_{2j}		a_{2n}
⋮		⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯				
a_i	a_{i1}	a_{i2}		a_{ij}		a_{in}
⋮		⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯				
a_n	a_{n1}	a_{n2}		a_{nj}		a_{nn}

表 1.1

其中，a_{ij} 是 a_i 与 a_j 的运算结果：$a_{ij} = a_i \circ a_j$　（当把运算 “$\circ$” 叫做加法或乘法时，此表便叫做加法表或乘法表）.

对有限集上的任意运算，都可构造出其运算表. 反之，给出了有限集上的一个运算的运算表，这个运算也就随之唯一确定. 因此，可以通过构造运算表来定义运算. 用运算表表示运算的好处是运算结果一目了然，并能显示出运算的许多性质.

例 7　设 $\mathbf{Z}_3=\{[0], [1], [2]\}$，$+_3$、$\times_3$ 的运算表分别为：

$+_3$	[0]	[1]	[2]
[0]	[0]	[1]	[2]
[1]	[1]	[2]	[0]
[2]	[2]	[0]	[1]

$\times_3$	[0]	[1]	[2]
[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]
[2]	[0]	[2]	[1]

例 8　设 $A=\{0, 1\}$，则 A 到 A 的映射构成的集合 A^A 中有四个元素 f_0，f_1，f_2，f_3，如下图所示：

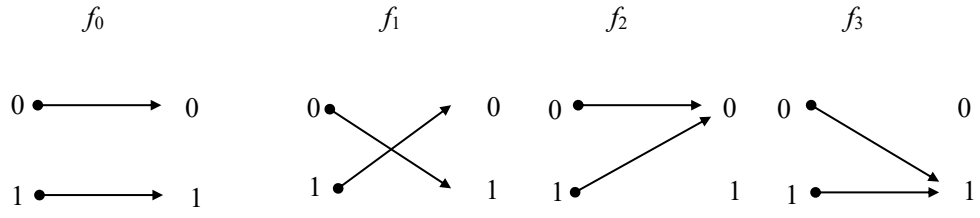


表 1.2 是 A^A 中的函数复合的运算表

$\circ$	f_0	f_1	f_2	f_3
f_0	f_0	f_1	f_2	f_3
f_1	f_1	f_0	f_3	f_2
f_2	f_2	f_2	f_2	f_2
f_3	f_3	f_3	f_3	f_3

表 1.2

下面是一些常用的表示运算性质的术语：

定义 3　设 X 为集合，$*$ ，$\circ$ 为 X 上的运算.

（1） 如果对任意 x，y，$z\in X$，有

$$(x * y) * z = x * (y * z)$$

则称 $*$ 满足结合律（可结合的）；

（2） 如果对任意 x，$y\in X$，有

$$x * y = y * x$$

则称 $*$ 满足交换律（可交换的）；

（3） 如果对任意 x，y，$z\in X$，有

$$x * (y \circ z) = (x * y) \circ (x * z)$$

则称 $*$ 对 $\circ$ 满足左分配律（左可分配）；

如果对任意 x，y，$z\in X$，有

$$(y \circ z) * x = (y * x) \circ (z * x)$$

则称 $*$ 对 $\circ$ 满足右分配律（右可分配）；

若 $*$ 对 $\circ$ 既满足左分配律，又满足右分配律，称 $*$ 对 $\circ$ 满足分配律（可分配）.

（4） 如果对任意 x，y，$z\in X$，

当 $x * y = x * z$ 时，必有 $y = x$，

则称 $*$ 满足左消去律；如果对任意 x，y，$z\in X$，

当 $y * x = z * x$ 时，必有 $y = z$，

则称 $*$ 满足右消去律；若 $*$ 既满足左消去律，又满足右消去律，称其满足消去律.

例 9　设 $A=\{1, 2, 3, 4, 5\}$，$*$ 是 A 上的运算，由如下运算表定义：

$*$	1	2	3	4	5
1	1	2	4	3	2
2	2	3	5	1	4
3	4	5	1	2	3
4	3	1	2	4	5

$$5 \mid 2 \quad 4 \quad 3 \quad 5 \quad 3$$

则 $*$ 是可交换的.

例 10 整数集上的加法、乘法均满足结合律、交换律，减法既不满足交换律，也不满足结合律；乘法对加法、减法均满足分配律；加法、减法满足消去律.

例 11 设 A 是一集合，$P(A)$ 上的并、交运算均满足结合律、交换律，并且互相可分配. 并与交运算均不满足消去律.

习题一

1. 在实数集 $\mathbf{R}$ 上定义运算 $*$ 如下：

$$a * b = |a| \cdot b \qquad \forall a, b \in \mathbf{R}$$

又设“$+$”为通常实数加法，问$+$，$*$ 具有哪些运算性质？

2. 用运算表在 $A=\{1, 2, 3, 4\}$ 上定义运算 “$*$”，使 “$*$” 为可交换的，一般地，当一个有限集上的运算满足交换律时，其运算表有何特点？
3. 写出 $\mathbf{Z}_5$ 的乘法运算与加法运算表.
4. 用“$-$”表示通常的实数减法，“$-$”是否满足交换律？结合律？证明之.

§ 2 代数系统

定义 1 设 A 是一个非空集合，$f_1, f_2, \cdots, f_n$ 是 A 上的运算（其元数可以不同），我们说 A 在运算 $f_1, f_2, \cdots, f_n$ 下构成一个代数系统，该代数系统记为 $\langle A, f_1, f_2, \cdots, f_n\rangle$. 在不引起混乱的情况下，也可将其简记为 A.

例 1 自然数集 $\mathbf{N}$ 在通常数的加法运算下构成代数系统 $\langle \mathbf{N}, + \rangle$，在通常数的乘法运算下构成代数系统 $\langle \mathbf{N}, \cdot \rangle$，而在这两个运算下又构成代数系统 $\langle \mathbf{N}, +, \cdot \rangle$. 同样，整数集 $\mathbf{Z}$，有理数集 $\mathbf{Q}$，实数集 $\mathbf{R}$，在通常数的加法与乘法运算下构成代数系统 $\langle \mathbf{Z}, + \rangle$，$\langle \mathbf{Z}, \cdot \rangle$，$\langle \mathbf{Z}, +, \cdot \rangle$，$\langle \mathbf{Q}, + \rangle$，$\langle \mathbf{Q}, \cdot \rangle$，$\langle \mathbf{Q}, +, \cdot \rangle$，$\langle \mathbf{R}, + \rangle$，$\langle \mathbf{R}, \cdot \rangle$，$\langle \mathbf{R}, +, \cdot \rangle$.

例 2 设 A 是一个集合，$P(A)$ 在集合的并和交运算下可构成代数系统 $\langle P(A), \cup \rangle$，$\langle P(A), \cap \rangle$，$\langle P(A), \cup, \cap \rangle$.

例 3 模 n 剩余类集 $\mathbf{Z}_n$ 在运算 $+_n$ 和 $\times_n$ 下可构成代数系统 $\langle \mathbf{Z}_n, +_n \rangle$，$\langle \mathbf{Z}_n, \times_n \rangle$，$\langle \mathbf{Z}_n, +_n, \times_n \rangle$，其中 $+_n$，$\times_n$ 定义如下:

$$[i] +_n [j] = [i+j],$$

$$[i] \times_n [j] = [ij] \qquad \forall\, [i], [j] \in \mathbf{Z}_n$$

今后我们经常要用到以上例题中的各代数系统，这些符号将作为标准符号使用，不再特别说明.

例 4　设 A 是一个集合，在 A 上规定运算 $*$ 如下：

$$\forall\ x, y\in A,\ x * y = x$$

则得到一个代数系统〈A，$*$ 〉.

定义 2　设〈A，$*$ 〉是代数系统，$S\subseteq A$，如果 S 对 $*$ 封闭，则称〈S，$*$ 〉为〈A，$*$ 〉的子代数.

由该定义知，任一代数系统均为自身的子代数，在〈**N**，+〉，〈**Z**，+〉，〈**Q**，+〉，〈**R**，+〉中，前者均为后者的子代数.〈 **Z**，• 〉不是〈**Q**，+〉的子代数.

今后我们将限于讨论只有一个或两个二元运算的代数系统，在此再强调一遍，如无特别说明，我们涉及到的运算都为二元运算.

定义 3　设〈A，∘ 〉是一个代数系统，$e_l\in A$，如果 $\forall x\in A$，有 $e_l x = x$，则称 e_l 为 A 的左单位元（左恒等元）；同样，设 $e_r\in A$，如果 $\forall x\in A$，有 $xe_r=x$，称 e_r 为 A 的右单位元（右恒等元）；A 中的一个元素如果既是左单位元，又是右单位元，则称之为单位元（恒等元）.

在〈**N**，+〉中 0 是单位元，在〈 **N**，• 〉中 1 是单位元，同样，在〈**Z**，+〉，〈**Q**，+〉，〈**R**，+〉中 0 是单位元，在〈 **Z**，• 〉，〈 **Q**，• 〉，〈 **R**，• 〉中 1 是单位元. 在〈$P(A)$，∪〉中 ∅ 是单位元，在〈$P(A)$，∩ 〉中 A 是单位元. 在〈$\mathbf{Z}_n$，$+_n$〉中［0］是单位元，在〈$\mathbf{Z}_n$，$\times_n$〉中［1］是单位元.

在例 4 的〈A，$*$ 〉中，任何元素均为右单位元，但无左单位元.

定理 1　设代数系统〈A，∘ 〉中既有左单位元 e_l，又有右单位元 e_r，则 $e_l=e_r$.

证明　因 e_l 为左单位元，故 $e_l e_r=e_r$，又因 e_r 为右单位元，故 $e_l e_r=e_l$，所以 $e_l=e_r$. ▌

推论　设〈A，∘〉是一个代数系统，〈A，∘〉中的单位元如果存在，则必定唯一.

证明　设 e_1，e_2 是〈A，∘〉中的单位元，则 e_1，e_2 必分别为左、右单位元，故由定理 1，$e_1=e_2$，因此〈A，∘〉中的单位元如果存在则必定唯一. ▌

定义 4　设〈A,$*$〉是一个代数系统，e 是〈A，$*$〉的单位元. 对于 $a\in A$，如果存在 $b\in A$，使得 $ba = e$，则称 a 为左可逆的，且称 b 为 a 的左逆元；如果存在 $c\in A$，使得 $ac = e$，则称 a 是右可逆的，且称 c 为 a 的右逆元；如果存在 $a'\in A$，使得 $a'a=aa' = e$，则称 a 是可逆的，且称 a' 为 a 的逆元.

〈**N**，+〉中 0 可逆，其逆元为 0，其它元素均不可逆.

〈**Z**，+〉，〈**Q**，+〉，〈**R**，+〉中，对任何元素 x，$-x$ 为 x 的逆元.

〈**N**，•〉中 1 可逆，其逆元为 1，其它元素均不可逆.

〈**Z**，•〉中， 1 和 -1 可逆， 1 的逆元为 1，-1 的逆元为 -1，其它元素无逆元.

〈**Q**，•〉，〈**R**，•〉中 0 不可逆，当 $x\neq 0$ 时，x 的逆元为 $\frac{1}{x}$.

〈$P(A)$，∪〉中 ∅ 为 ∅ 的逆元，其它元素无逆元，

〈$P(A)$，∩〉中 A 为 A 的逆元，其它元素无逆元.

〈$\mathbf{Z}_n$，$+_n$〉中［$n-i$］为［i］的逆元.

〈$\mathbf{Z}_n$，$\times_n$〉中的逆元情况较复杂，留在以后讨论.

例 4 的〈A，$*$〉中无单位元，所以不能讨论逆元.

例 5　设 $A=\{1, 2, 3, 4, 5\}$，A 中运算 $*$ 的运算表如表 2．1．

$*$	1	2	3	4	5
1	1	2	3	4	5
2	2	3	1	4	4
3	3	3	3	2	1
4	4	5	1	3	2
5	5	4	3	2	2

表 2．1

1 为单位元，2 和 4 均为 3 的左逆元，5 为 3 的右逆元，但 3 不存在逆元.

定理 2　设〈A，$*$ 〉是一代数系统，e 是其单位元，运算 $*$ 满足结合律，如果 $a\in A$ 的左逆元 b 及右逆元 c 均存在，则 $b = c$.

证明　由定义 $b = be = b(ac) = (ba)c = ec = c$.　▌

推论　设〈A，$*$〉是一个代数系统，e 是其单位元，运算 $*$ 满足结合律．如果 $a\in A$ 的逆元存在，则必定唯一.

证明与定理 1 的推论完全类似，读者自己完成.

定义 5　设〈A，$*$〉是一个代数系统，如果 $a\in A$ 满足 $a*a = a$，称 a 为 A 的幂等元.

任意代数系统的单位元如果存在则必为幂等元.〈$P(A)$，$\cup$〉，〈$P(A)$，$\cap$〉中任何元素均为幂等元.

例 6　指出代数系统〈$\mathbf{Z}_n$，$+_n$，$\times_n$〉所具有的性质.

（1） 关于$+_n$的性质：

结合律

$$([i]+_n[j])+_n[k]=[i]+_n([j]+_n[k]) \qquad \forall [i],[j],[k]\in\mathbf{Z}_n$$

交换律

$$[i]+_n[j]=[j]+_n[i] \qquad \forall [i],[j]\in\mathbf{Z}_n$$

单位元

$$[i]+_n[0]=[0]+_n[i]=[i] \qquad \forall [i]\in\mathbf{Z}_n$$

逆元

$$[i]+_n[n-i]=[n-i]+_n[i]=[0] \qquad \forall [i]\in\mathbf{Z}_n$$

（2） 关于$\times_n$的性质.

结合律

$([i]\times_n[j])\times_n[k]=[i]\times_n([j]\times_n[k])$　　$\forall\,[i],[j],[k]\in\mathbf{Z}_n$

交换律

$[i]\times_n[j]=[j]\times_n[i]$　　$\forall\,[i],[j]\in\mathbf{Z}_n$

单位元

$[i]\times_n[1]=[1]\times_n[i]=[i]$　　$\forall\,[i]\in\mathbf{Z}_n$

（3）$+_n$与$\times_n$的联合性质

$\times_n$对$+_n$的分配律

$$[i]\times_n([j]+_n[k])=([i]\times_n[j])+_n([i]\times_n[k])$$

$$([j]+_n[k])\times_n[i]=([j]\times_n[i])+_n[k]\times_n[i])$$

$\forall\,[i],[j],[k]\in\mathbf{Z}_n$

习题二

1. 在$A=\{1,2,3,4\}$上定义运算$*$，使$\langle A,*\rangle$有单位元.
2. $\langle\mathbf{Q},+,\cdot\rangle$有何性质？这些性质中哪些在，$\langle\mathbf{Z},+,\cdot\rangle$，$\langle\mathbf{N},+,\cdot\rangle$中不成立？
3. 设A为一非空集合，且$|A|\geqslant 2$，$E(A)$为A上的所有函数构成的集合，$\circ$为函数的复合运算，问$\langle E(A),\circ\rangle$中是否有单位元？找出$E(A)$的三个子代数.
4. 设$\langle A,*\rangle$为一代数系统，e_1，e_2为A中两个不同左单位元，证明$\langle A,*\rangle$中无右单位元.

§3　同态与同构

设A，B为两个集合，我们已经讨论过A到B的映射. 当A，B分别带有某些运算而形成代数系统时，我们自然要将映射与运算联系起来讨论. 在此，以具有一个二元运算的代数系统为例，讨论同态与同构的概念.

定义1　设$\langle A,*\rangle$，$\langle B,\circ\rangle$为两个代数系统，$f\colon A\to B$，如果f保持运算，即：$\forall x,y\in A$有

$$f(x*y)=f(x)\circ f(y)$$

称f为$\langle A,*\rangle$到$\langle B,\circ\rangle$的同态映射，简称同态.

例1　设$\langle A,*\rangle$，$\langle B,\circ\rangle$是两个代数系统，$e\in B$是B的单位元. 令

$$f\colon a\mapsto e\qquad\forall\,a\in A$$

则$\forall\,x,y\in A$，$f(x*y)=e$，$f(x)\circ f(y)=e\circ e=e$，即有$f(x*y)=f(x)\circ f(y)$，因此$f$是$A$到$B$的同态，称$f$为零同态.

例2　令$f\colon\mathbf{Z}\to\mathbf{Z}$　　定义如下

$$f:\ a\mapsto 8a \qquad \forall a\in\mathbf{Z}$$

则f是〈$\mathbf{Z}$，＋〉到〈$\mathbf{Z}$，＋〉的同态，但不是〈$\mathbf{Z}$，•〉到〈$\mathbf{Z}$，•〉的同态.

定义 2　设〈A，＊　〉，〈B，◦　〉为两个代数系统，f：$A\to B$ 为A到B的同态，如果f是单射，称f为单同态；如果f为满射，称f为满同态，这时称B是A在f下的同态象，记为f：$A\sim B$ 或 $A\overset{f}{\sim}B$；如果f是双射，称f为同构映射（简称同构），这时称A与B在f映射下同构．记为 f：$A\cong B$ 或 $A\overset{f}{\cong}B$.

我们说代数系统〈B，◦〉是〈A，＊〉的同态象，并记为$A\sim B$ 是指存在同态映射f，使 f：$A\sim B$．同样，我们说两个代数系统〈A，＊　〉，〈B，◦　〉是同构的，并记为$A\cong B$是指存在同构映射f，使 f：$A\cong B$.

例 3　对于〈$\mathbf{Z}$，＋〉与〈$\mathbf{Z}_n$，$+_n$〉，令

$$f:\ i\mapsto [i]$$

则f 是满射，且 $\forall\, i,\ j\in\mathbf{Z}$

$$f(i+j)=[i+j]=[i]+_n[j]=f(i)+_n f(j)$$

故有　　f：〈$\mathbf{Z}$，＋〉～〈$\mathbf{Z}_n$，$+_n$〉

同样讨论可知〈$\mathbf{Z}$，•〉～〈$\mathbf{Z}_n$，$\times_n$〉.

例 4　用 $\mathbf{R}^+$表示正实数集，考虑〈$\mathbf{R}$，＋〉与〈$\mathbf{R}^+$，•〉，令f：$x\mapsto e^x$　$\forall x\in\mathbf{R}$, 其中，e为自然对数的底，则f是双射，并且　$\forall x,\ y\in\mathbf{R}$

$$f(x+y)=e^{x+y}=e^x\cdot e^y=f(x)\cdot f(y)$$

故　　f：〈$\mathbf{R}$，＋〉≅〈$\mathbf{R}^+$，•〉

定理 1　设f是〈A，＊　〉到〈B，•〉的同态，g是〈B，•〉到〈C，△〉的同态，则$g\circ f$是〈A，＊　〉到〈C，△〉的同态. 且当f，g均为单同态、满同态、同构时，$g\circ f$也必是单同态、满同态、同构.

证明　因为 f：$A\to B$，g：$B\to C$，故知　$g\circ f$：$A\to C$．下面证明$g\circ f$保持运算.

$\forall\, x,\ y\in A$

$$\begin{aligned}(g\circ f)(x*y)&=g(f(x*y))\\&=g(f(x)\cdot f(y))\\&=g(f(x))\triangle g(f(y))\\&=(g\circ f)(x)\triangle(g\circ f)(y)\end{aligned}$$

因而,$g\circ f$是A到C的同态．因为当f，g均为单射、满射、双射时$g\circ f$ 也必为单射、满射、双射，故知当f，g均为单同态、满同态、同构时$g\circ f$也必为单同态、满同态、同构．从而定理得证.　▌

定理 2　设 φ：〈A，＊　〉≅〈B，◦　〉，则

$$\varphi^{-1}:\ \langle B,\circ\ \rangle\cong\langle A,*\ \rangle$$

证明　由函数的性质可知，φ^{-1}是B到A的双射．又，$\forall\, x,\ y\in B$ 记 $\varphi^{-1}(x)=x_1$，$\varphi^{-1}(y)=y_1$，则 $x=\varphi(x_1)$，$y=\varphi(y_1)$，故

$$\varphi^{-1}(x\circ y)=\varphi^{-1}(\varphi(x_1)\circ\varphi(y_1))=\varphi^{-1}(\varphi(x_1*y_1))$$
$$=x_1*y_1=\varphi^{-1}(x)*\varphi^{-1}(y)$$

即φ^{-1}保持运算，故φ^{-1}：〈B，$\circ$〉≅〈A，$*$ 〉. ▌

定理 3 （满同态保持结合律）

设 φ：〈A，$*$ 〉～〈B，$\circ$〉，$*$ 满足结合律，则 $\circ$ 也必满足结合律.

证明 $\forall x, y, z\in B$，由于 φ 是 A 到 B 的满同态，故必存在 x_1，y_1，$z_1\in A$，使 $\varphi(x_1)=x$，$\varphi(y_1)=y$，$\varphi(z_1)=z$，于是

$$\begin{aligned}(x\circ y)\circ z&=(\varphi(x_1)\circ\varphi(y_1))\circ\varphi(z_1)\\&=\varphi(x_1*y_1)\circ\varphi(z_1)\\&=\varphi((x_1*y_1)*z_1)\\&=\varphi(x_1*(y_1*z_1))\\&=\varphi(x_1)\circ\varphi(y_1*z_1)\\&=\varphi(x_1)\circ(\varphi(y_1)\circ\varphi(z_1))\\&=x\circ(y\circ z)\end{aligned}$$ ▌

定理 4 （满同态保持交换律） 设〈A，$*$ 〉～〈B，$\circ$〉，$*$ 满足交换律，则 $\circ$ 必满足交换律.

读者自证. ▌

定理 5 （满同态保持单位元） 设 φ：〈A，$*$ 〉～〈B，$\circ$〉，$e\in A$ 是 A 的单位元，则$\varphi(e)$是 B 的单位元.

证明 $\forall b\in B$，由于 φ 是满同态，必存在 $a\in A$ 使 $\varphi(a)=b$，因此，

$$\begin{aligned}b\circ\varphi(e)&=\varphi(a)\circ\varphi(e)\\&=\varphi(a*e)\\&=\varphi(a)\\&=b\end{aligned}$$

同理 $\varphi(e)\circ b=b$.

因此 $\varphi(e)$是 B 的单位元. ▌

定理 6 （满同态保持逆元） 设 φ：〈A，$*$ 〉～〈B，$\circ$ 〉，e_A，e_B分别为 A，B 的单位元，a，$a'\in A$ 且 a' 是 a 的逆元，则 $\varphi(a')$是$\varphi(a)$的逆元.

证明 $\varphi(a')\circ\varphi(a)=\varphi(a'*a)=\varphi(e_A)=e_B$

同理 $\varphi(a)\circ\varphi(a')=e_B$.

故 $\varphi(a')$是 $\varphi(a)$的逆元. ▌

定理 7 （同态保持幂等元） 设 φ 是〈A，$*$ 〉到〈B，$\circ$ 〉的同态，若 $a\in A$ 是幂等元，则$\varphi(a)\in B$ 也是幂等元.

读者自证

由以上诸定理可见，若〈A，$*$ 〉～〈B，$\circ$ 〉，则 A中的性质都可推到 B 中，特别地，若〈A，$*$ 〉≅〈B，$\circ$ 〉，则〈B，$\circ$ 〉≅〈A，$*$ 〉，因而 A，B 的性质可以互推，即 A，B 应具有完全相同的性质，这时，从代数的观点来看，A，B 的差别仅在于所用符

号不同，本质是等同的．因此，同构的代数系统有时不加区别．

定义 3　设〈A，＊ 〉为一个代数系统，〈A，＊ 〉到自身的同态称为 A 的自同态，〈A，＊ 〉到自身的同构称为A的自同构．

例 5　设〈A，＊ 〉是一个代数系统，A 上的恒等映射 I_A 是 A 的自同构．若 A 中存在单位元 e，令 f：$a \mapsto e$，　$\forall a \in A$，则 f 是 A 的自同态．

习题三

1．设〈A，＋，•〉和〈B，⊕，⊙〉为两个代数系统，写出 A 到 B 的同态的定义．
2．证明：〈$\mathbf{Z}$，•〉～〈{－1，0，1}，• 〉．
3．证明：〈$\mathbf{N}$，＋〉～〈{0，1}，∨〉．
4．找出〈$\mathbf{Z}_3$，$+_3$〉的所有自同构．
5．证明〈 $\mathbf{R}$，• 〉与〈 $\mathbf{Z}$，• 〉不同构．
6．证明〈$\mathbf{R}$，＋〉与〈 $\mathbf{R}$，• 〉不同构．
7．证明定理 4、定理 7．

*§ 4　同余关系与商代数

（一） 同余关系与商代数

上节我们将集合之间的映射与运算联系起来定义了同态，本节将集合上的等价关系与运算联系起来，引入下述定义．

定义 1　设〈A，＊ 〉是一个代数系统，E 是 A 上的等价关系，如果 $\forall x_1$，x_2，$y_1, y_2 \in A$，当 $x_1 E y_1$，$x_2 E y_2$ 时，必有 $x_1 * x_2 \quad E \quad y_1 * y_2$，则称 E 为 A 上的同余关系．

例 1　设〈A，＊ 〉是一个代数系统，其中运算定义如下：

$$x * y = x \qquad \forall x, y \in A$$

E 是 A 上的任一等价关系，则 E 必为 A 上的同余关系．

事实上，假设 x_1，x_2，y_1，$y_2 \in A$，且 $x_1 E y_1$，$x_2 E y_2$，则由 $x_1 * x_2 = x_1$，$y_1 * y_2 = y_1$ 知：$x_1 * x_2 \ E \ y_1 * y_2$．

例 2　整数集 $\mathbf{Z}$ 上的模 m 同余关系是〈$\mathbf{Z}$，＋〉及〈 $\mathbf{Z}$，• 〉上的同余关系．

证明　$\forall i_1$，i_2，j_1，$j_2 \in \mathbf{Z}$，设 $i_1 \equiv i_2 \bmod m$，　$j_1 \equiv j_2 \bmod m$，则

$$m \mid i_1 - i_2, \quad m \mid j_1 - j_2.$$

由于　$(i_1 + j_1) - (i_2 + j_2) = (i_1 - i_2) + (j_1 - j_2)$

故　　$m \mid (i_1 + j_1) - (i_2 + j_2)$

即　　$i_1 + j_1 \equiv i_2 + j_2 \bmod m$

因此，模 m 同余关系是〈$\mathbf{Z}$，＋〉上的同余关系．

又　$i_1 j_1 - i_2 j_2 = i_1 j_1 - i_1 j_2 + i_1 j_2 - i_2 j_2$

$$= i_1(j_1-j_2)+(i_1-i_2)j_2$$

故　　$m \mid i_1j_1-i_2j_2$　即　$i_1j_1 \equiv i_2j_2 \mod m$

因此，模 m 同余关系也为〈 $\mathbf{Z}$，• 〉上的同余关系.

设 E 为〈A，＊ 〉上的同余关系，我们可以在商集

$$A/E=\{[x]_E \mid x\in A\}$$

上合理地引入一个运算：

令 ∘ 是 A/E 上的运算，由下式定义：

$$[x]\circ[y]=[x*y] \qquad \forall [x],[y]\in A/E$$

由于 ∘ 是通过等价类的代表元定义的，为了说明它确为 A/E 上的运算，需要证明运算结果 $[x]\circ[y]$ 由 $[x]$，$[y]$ 唯一确定，而与其代表元的选取无关. 为此，在 $[x]$，$[y]$ 中另取代表元 x'，y' ，则 $[x]=[x']$，$[y]=[y']$，$x\,E\,x'$，$y\,E\,y'$，因为 E 为同余关系，则 $x*y\,E\,x'*y'$，故有 $[x*y]=[x'*y']$，即 $[x]\circ[y]=[x']\circ[y']$，或说 $[x]\circ[y]$ 与代表元选取无关，∘ 的定义是合理的.

在 A/E 上按如上方式引入运算 ∘ 而得到的代数系统〈A/E，∘〉，称为 A 对 E 的商代数.

例 3　用 R_m 表示 $\mathbf{Z}$ 上的模 m 同余关系，则由例 2 知 R_m 为〈$\mathbf{Z}$，＋〉，〈 $\mathbf{Z}$，• 〉上的同余关系.〈$\mathbf{Z}$，＋〉对 R_m 的商代数为

$$\langle \mathbf{Z}/R_m,\circ\ \rangle$$

其中，$\mathbf{Z}/R_m = \mathbf{Z}_m = \{[0],[1],\cdots,[m-1]\}$，运算由下式定义：

$$[i]\circ[j]=[i+j]=[i]+_m[j]$$

即〈$\mathbf{Z}$，＋〉对 R_m 的商代数即为〈$\mathbf{Z}_m$，$+_m$〉.

同样，〈$\mathbf{Z}$，•〉对 R_m 的商代数即为〈$\mathbf{Z}_m$，$\times_m$〉.

定理 1　设 E 为〈A，＊ 〉上的同余关系，〈A/E，∘ 〉为 A 对 E 的商代数，令 φ：$A\to A/E$，定义如下：

$$\varphi(x)=[x] \qquad \forall x\in A$$

则　φ：〈A，＊ 〉～〈A/E，∘ 〉.

证明　显然 φ 为满射，又　$\forall\, x, y\in A$

$$\varphi(x*y)=[x*y]=[x]\circ[y]=\varphi(x)\circ\varphi(y)$$

因此，φ：〈A，＊ 〉～〈A/E，∘ 〉.

这里的 φ 称为〈A，＊ 〉到〈A/E，∘ 〉的自然同态.

（二） 同态基本定理

由以上讨论可知，对任何代数系统〈A，＊ 〉，由 A 上的同余关系 E 可确定一个同态——A 到 A/E 的自然同态，反之，我们有

定理 2　设 f 是〈A，＊ 〉到〈B，∘ 〉的同态，由 f 在 A 上按下式定义关系 E_f

$$x\,E_f\,y \Leftrightarrow f(x)=f(y) \qquad \forall\, x, y\in A$$

则 E_f 为〈A，＊ 〉上的同余关系.

证明 先证 E_f 为等价关系， $\forall x\in A$，$f(x)=f(x)$，故 xE_fx，即 E_f 是自反的．又 $\forall x, y\in A$，若 xE_fy，则 $f(x)=f(y)$，因此 $f(y)=f(x)$，即 yE_fx，E_f 为对称的，再取 x，y，$z\in A$，设 xE_fy，yE_fz，则 $f(x)=f(y)$，$f(y)=f(z)$，故 $f(x)=f(z)$ 即 xE_fz，E_f 是传递的，总之 E_f 是 A 上的等价关系．现设 x_1，x_2，y_1，$y_2\in A$ 且 $x_1E_fy_1$，$x_2E_fy_2$，则 $f(x_1)=f(y_1)$，$f(x_2)=f(y_2)$，因此 $f(x_1)\circ f(x_2)=f(y_1)\circ f(y_2)$，因为 f 为同态，$f(x_1)\circ f(x_2)=f(x*x_2)$，$f(y_1)\circ f(y_2)=f(y_1*y_2)$，所以 $f(x_1*x_2)=f(y_1*y_2)$，即 $x_1*x_2\ E_f\ y_1*y_2$，因此，E_f 为 A 上的同余关系． ▌

该定理中的 E_f 称为由同态 f 确定的同余关系．

定理 3 设 f：〈A，$*$ 〉～〈B，△〉，E_f 为由 f 确定的同余关系，〈A/E_f，$\circ$ 〉为 A 对 E_f 的商代数，则〈A/E_f，$\circ$ 〉≅〈B，△〉．

证明 建立 A/E_f 到 B 的映射 φ：$[x]\mapsto f(x)$，由于 f 是满同态，易证 φ 为满射，事实上，$\forall y\in B$，$\exists x\in A$ 使得 $f(x)=y$，于是 $\varphi([x])=f(x)=y$，因此 φ 为满射．又设 $[x_1]$，$[x_2]\in A/E_f$，且 $[x_1]\neq[x_2]$，则〈x_1，x_2〉$\notin E_f$，即 $f(x_1)\neq f(x_2)$，也就是说，$\varphi([x_1])\neq\varphi([x_2])$，因此 φ 为单射，综上所述，φ 为双射．下证 φ 保持运算．

$\forall\ [x_1]$，$[x_2]\in A/E_f$

则 $\varphi([x_1]\circ[x_2])=\varphi([x_1*x_2])$

$=f(x_1*x_2)$

$=f(x_1)\triangle f(x_2)$

$=\varphi([x_1])\triangle\varphi([x_2])$

从而我们证明了 φ：$A/E_f\cong B$． ▌

该定理可由图 4.1 表示．

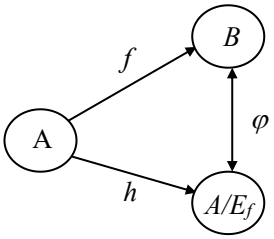


图 4.1

定理 1 与定理 3 合称为同态基本定理．他们表明了，从同构观点来看，商代数与同态象是等同的，即商代数必为同态象，同态象（在同构意义下）必为商代数．

习 题 四

1．设 E_1，E_2 均为〈A，$*$ 〉上同余关系，证明：$E_1\cap E_2$ 必为 A 上的同余关系．

2．若 E_1，E_2 是〈A，$*$ 〉上同余关系，证明：$E_1\circ E_2$ 不一定是同余关系．

§5 直 积

定义 1 设〈A，$*$ 〉，〈B，$\circ$ 〉为两个代数系统，〈$A\times B$，△〉称为 A 与 B 的直积，其中，$A\times B$ 是 A，B 的笛卡尔积，△ 定义如下：

$\langle x, y\rangle \triangle \langle u, v\rangle = \langle x * u, y \circ v \rangle \qquad \forall \langle x, y\rangle, \langle u, v\rangle \in A\times B$

由定义立即可以看出，A 与 B 的直积 $A\times B$ 能够保持 A，B 的某些性质：

如果 $*$ ，$\circ$ 均满足结合律（交换律），则 $\triangle$ 也必满足结合律（交换律）；如果 A，B 中分别有单位元 e_A，e_B，则 $\langle e_A, e_B\rangle$ 是 $A\times B$ 的单位元；如果 $x\in A$，$y\in B$ 分别有逆元 x'，y' ，则 $\langle x', y'\rangle$ 是 $\langle x, y\rangle$ 的逆元.

定理 1　设 $\langle A, * \rangle$，$\langle B, \circ \rangle$ 为两个代数系统，且分别有单位元 e_A，e_B，则在 A，B 的直积 $\langle A\times B, \triangle\rangle$ 中存在子代数 S，T 使

$$S\cong A, \qquad T\cong B$$

证明　令 $S = A\times \{e_B\} = \{\langle x, e_B\rangle \mid x\in A\}$　则　$S \subseteq A\times B$，　$\forall \langle x, e_B\rangle$，$\langle y, e_B\rangle \in S$,

$$\begin{aligned}\langle x, e_B\rangle \triangle \langle y, e_B\rangle &= \langle x * y, e_B \circ e_B\rangle\\ &= \langle x * y, e_B\rangle \in S\end{aligned}$$

因此 $\langle S, \triangle\rangle$ 构成 $A\times B$ 的子代数，考虑映射 f：$A\to S$

$$f: a\mapsto \langle a, e_B\rangle \qquad \forall a\in A$$

显然，f 为双射，又　$\forall x, y\in A$

$$\begin{aligned}f(x * y) &= \langle x * y, e_B\rangle = \langle x, e_B\rangle \triangle \langle y, e_B\rangle\\ &= f(x) \triangle f(y)\end{aligned}$$

则 f 保持运算，因此 f：$A \cong S$. 同理可证，若令 $T = \{e_A\}\times B$ 则 $B \cong T$. ▌

习 题 五

1．设 $\langle A, * \rangle$，$\langle B, \circ \rangle$ 为两个代数系统，$\langle A\times B, \triangle\rangle$，$\langle B\times A, \triangledown \rangle$ 分别为 A 与 B，B 与 A 的直积，证明 $A\times B \cong B\times A$.

2．写出 $\langle \mathbf{Z}_3, +_3\rangle$ 与 $\langle \mathbf{Z}_2, \times_2\rangle$ 的直积的运算表.

第五章　群

§1　半　群

定义 1　设〈S，$\circ$〉为一代数系统，若其中运算“$\circ$”满足结合律，即 $\forall x, y, z \in S$，有 $(x \circ y) \circ z = x \circ (y \circ z)$，则称〈$S$，$\circ$〉为半群.

例 1　〈$\mathbf{N}$，$+$〉，〈$\mathbf{N}$，$\cdot$〉，〈$\mathbf{Z}$，$+$〉，〈$\mathbf{Z}$，$\cdot$〉都是半群.

例 2　对任意集合 A，〈$P(A)$，$\cup$〉，〈$P(A)$，$\cap$〉均为半群.

例 3　由集合 A 到 A 的全体映射构成的集合 A^A，在映射的复合运算下构成半群〈A^A，$\circ$〉.

例 4　在自然数集合 $\mathbf{N}$ 上定义运算“$\circ$”：

$$a \circ b = a + b + ab \qquad \forall a, b \in \mathbf{N}$$

显然，$\forall a, b \in \mathbf{N}$，$a \circ b \in \mathbf{N}$ 是唯一确定的，即 $\circ$ 确为 $\mathbf{N}$ 上的运算. 下面我们验证其结合性.

$$\begin{aligned}(a \circ b) \circ c &= (a+b+ab) \circ c \\ &= (a+b+ab) + c + (a+b+ab)c \\ &= a+b+c+ab+ac+bc+abc\end{aligned}$$

$$\begin{aligned}a \circ (b \circ c) &= a \circ (b+c+bc) \\ &= a + (b+c+bc) + a(b+c+bc) \\ &= a+b+c+bc+ab+ac+abc \\ &= a+b+c+ab+ac+bc+abc\end{aligned}$$

故有 $(a \circ b) \circ c = a \circ (b \circ c)$，即〈$\mathbf{N}$，$\circ$〉为一半群.

在半群〈S，$\circ$〉中，任取三个元素 a，b，c，若保持次序不变，则只有两种计算方法.

$$(a \circ b) \circ c, \qquad a \circ (b \circ c)$$

结合律表示这两种计算方法计算结果相同，因而可省略括号记为 $a \circ b \circ c$. 一般地，在 S 中取 n 个元素 a_1，a_2，a_3，…，a_n，可以用数学归纳法证明，若元素次序不变，以任一种结合方式进行计算，计算结果都相同. 这样，在半群中，$a_1 \circ a_2 \circ \cdots \circ a_n$ 这个符号是有意义的.

半群〈S，$\circ$〉的运算 $\circ$ 通常叫做“乘法”，并且在书写 $a \circ b$ 时，常省略运算符号，简记为 ab.

定义 2　设〈S，$\circ$〉为一半群，$a \in S$，n 为正整数，符号 a^n 表示 n 个 a 的计算结果，即

$$a^n=\overbrace{a\circ a\circ\cdots\circ a}^{n}$$

由该定义立即可知，在半群〈S，$\circ$〉中指数律成立，即对任意正整数 m，n 和 S 中的元素 a，有

$$a^m a^n=a^{m+n}.$$

$$(a^m)^n = a^{mn}.$$

例 5　在半群〈$\mathbf{Z}$，+〉中，

$$1^n = \overbrace{1+1+\cdots+1}^{n} = n.$$

$$2^n = \overbrace{2+2+2\cdots+2}^{n} = 2n.$$

在半群〈$\mathbf{Z}$，·〉中，

$$1^n =\overbrace{1+1+1+\cdots+1}^{n}=1$$

$$2^n =\overbrace{2+2+2+\cdots+2}^{n}$$（即为通常的 2^n）.

如果半群〈S，$\circ$〉中的乘法满足交换律，则称〈S，$\circ$〉为可交换半群，用数学归纳法可以证明．在可交换半群〈S，$\circ$〉中，任取 n 个元素 a_1，a_2，…，a_n，乘积 $a_1a_2\cdots a_n$ 中各项任意交换次序，所得运算结果相同．这样，在可交换半群中又有另一指数律：

$$(ab)^n = a^n b^n.$$

前面已经指出，半群〈S，$\circ$〉中的运算一般叫做“乘法”，并且在书写时采用乘法记号，但对于可交换半群，根据习惯，其运算有时采用加法记号“+”表示，这时我们有一套相应的特殊记号，比如将 a^n 记为 na，即

$$na=\overbrace{a+a+a+\cdots+a}^{n}$$

指数律在这种加法记号下变为如下形式：

$$ma+na=(m+n)a.$$

$$m(na)=(mn)a.$$

$$n(a+b)=na+nb.$$

定义 3　设〈S，$\circ$〉为一半群，若〈S，$\circ$〉中有单位元，即存在 $e\in S$，使得 $\forall x\in S$，$xe=ex=x$，则称〈S，$\circ$〉为幺半群（有 1 半群、独异点）.

例如，〈$\mathbf{N}$，+〉，〈$\mathbf{Z}$，+〉，〈$\mathbf{N}$，·〉，〈$\mathbf{Z}$，·〉等均为幺半群．但偶数集合 E 在乘法下形成的半群〈E，·〉不是幺半群.

在一个幺半群中，单位元一般用 e 表示，但当使用加法记号时，单位元常用 0 表示，并称其为零元．使用这些记号及术语时，通常不再说明.

设〈S，$*$〉为幺半群，如果 $a\in S$ 的逆元存在，则由于 $\circ$ 满足结合律，其逆元必是唯一的．以后，在幺半群〈S，$*$〉中将始终用 a^{-1} 表示 a 的唯一逆元，即 $a^{-1}\in S$，且 $a^{-1}*a=a*a^{-1}=e$，当采用加法记号时，a^{-1} 常记作 $-a$，且称为 a 的负元．

定理 1　设〈S，$*$〉是幺半群，如果 a，$b\in S$ 的逆元 a^{-1}，b^{-1} 存在，则

（1）　$(a^{-1})^{-1}=a$.

（2）　$(ab)^{-1}=b^{-1}a^{-1}$.

证明　由逆元 a^{-1} 的定义，得

$$a^{-1}a=aa^{-1}=e,$$

由此及逆元定义可知 a 为 a^{-1} 的逆元，即

$$(a^{-1})^{-1}=a.$$

又　　$(ab)(b^{-1}a^{-1})=a(bb^{-1})a^{-1}=aa^{-1}=e.$

同理　　$(b^{-1}a^{-1})(ab)=b^{-1}b=e$

故由逆元定义，　　$(ab)^{-1}=b^{-1}a^{-1}$.

定义 4　设〈S，$\circ$〉为一半群，若 $T\subseteq S$ 在 S 的运算 $\circ$ 下也构成半群，则称〈T，$\circ$〉为〈S，$\circ$〉的子半群．

显然，对于半群〈S，$\circ$〉，只要 $T\subseteq S$ 对运算 $\circ$ 封闭，则〈T，$\circ$〉即为〈S，$\circ$〉的子半群．事实上，若 T 对 $\circ$ 封闭，即对任意 a，$b\in T$，$a\circ b$（存在唯一）属于 T，因而可将 $\circ$ 视为 T 上的运算，从而得到代数系统〈T，$\circ$〉，由于 $\circ$ 在 S 上是可结合的，在 $T\subseteq S$ 上自然也是可结合的．所以〈T，$\circ$〉必为半群，从而是〈S，$\circ$〉的子半群．

例如，在〈$\mathbf{N}$，$\cdot$〉，〈$\mathbf{Z}$，$\cdot$〉，〈$\mathbf{Q}$，$\cdot$〉中，前者均为后者的子半群．

例 7　令 $T=\{km\mid k\in\mathbf{N}\}$，则 T 是〈$\mathbf{N}$，$\cdot$〉的子半群．

例 8　设〈S，$*$〉是一半群，$a\in S$，$T=\{a^i\mid i\in\mathbf{Z}^+\}$，则 T 是 S 的子半群．

因为，$\forall\, a^i$，$a^j\in T$，　$a^i*a^j=a^{i+j}\in T$，　即 T 对运算 $*$ 是封闭的，从而必构成半群，因此是 S 的子半群．

若〈S，$*$〉有单位元 e，〈S，$*$〉的子半群未必有单位元，即使有的话，也未必等于 S，请看下面的例子．

例 9　（1）偶数集 E 在乘法运算下构成的半群〈E，$\cdot$〉是〈$\mathbf{Z}$，$\cdot$〉的子半群，但 $\mathbf{Z}$ 中有单位元而 E 中无单位元．

（2）设 A 为非空集合，$B\subset A$，则〈$P(B)$，$\cap$〉为〈$P(A)$，$\cap$〉的子半群，但 $P(A)$ 中有单位元 A，$P(B)$ 中有单位元 B．

定义 5　设 S 是幺半群，若 T 是 S 的子半群，且 S 的单位元 $e\in T$，则称 T 是 S 的子幺半群．

例 10　设〈S，$*$〉是幺半群，$a\in S$，$T=\{a^i\mid i\in\mathbf{N}\}$，则 T 是 S 的子幺半群，这里，规定 $a^0=e$．

同例 7 类似，可知 T 是 S 的子半群，因为单位元 $e=a^0\in T$，故 T 是子幺半群．

例 11　设〈S，$*$〉是可交换幺半群，$T=\{a\mid a\in S,\ a*a=a\}$，则 T 是 S 的子幺半群．

$\forall x, y\in T$，$x*x=x$，$y*y=y$ 故

$$(x*y)*(x*y)=x*(y*x)*y$$
$$=x*(x*y)*y$$
$$=(x*x)*(y*y)=x*y$$

因此，$x*y\in T$，即 T 对 $*$ 是封闭的，必构成半群，从而是 S 的子半群．又，S 的单位元 e 满足 $e*e=e$，故 $e\in T$，所以，T 是 S 的子幺半群．

习 题 一

1．设 $S=\{a, b\}$，证明〈S^S，∘ 〉不是可交换半群．

2．设 M 为〈A，∘ 〉的所有自同态构成的集合，证明〈M，∘ 〉是幺半群．

3．设〈S，∘ 〉是一个半群，且消去律成立，证明：S 是可交换半群的充分必要条件是

$$\forall a, b\in S, \text{有}(ab)^2=a^2b^2.$$

§2 群的概念及基本性质

在半群、幺半群概念的基础上，我们引进一类特别重要的代数系统——群．

定义1 设〈G，$*$ 〉为幺半群，如果 $\forall a\in G$，a 的逆元 a^{-1} 均存在，则称〈G，$*$〉为群．换言之，一个代数系统〈G，$*$ 〉，如果满足下列条件：

（1） 结合律成立 $(ab)c=a(bc)$ $\forall a, b, c\in G$

（2） G 中具有单位元 e， $ea=ae=a$ $\forall a\in G$

（3） $\forall a\in G$，存在 $a^{-1}\in G$ 使 $a^{-1}a=aa^{-1}=e$.

称〈G，$*$ 〉为群．

当群 G 中只含有有限个元素时，称其为有限群，否则称其为无限群．有限群 G 的元素个数称为群 G 的阶，并规定无限群 G 的阶为∞．同集合的情况一样，群 G 的阶也记为 $|G|$．

一个群 G，如果其运算是可交换的，则称之为交换群或 Abel 群．

例1 $\{1, -1\}$ 对整数的乘法作成有限交换群〈$\{1, -1\}$，$\cdot$〉．

例2 〈$\mathbf{Z}$，$+$〉，〈$\mathbf{Q}$，$+$〉，〈$\mathbf{R}$，$+$〉均为无限交换群，〈$\mathbf{Q}^+$，$\cdot$〉，〈$\mathbf{R}^+$，$\cdot$〉也为无限交换群，但〈$\mathbf{Q}$，$\cdot$〉，〈$\mathbf{R}$，$\cdot$〉不是群（为何？）．

例3 〈$\mathbf{Z}_n$，$+_n$〉为有限交换群，其中零元为 $[0]$，$[i]$ 的负元为 $[-i]=[n-i]$．

定理1 设〈G，$*$ 〉为群，则

（1）G 中消去律成立．

（2）单位元 e 是 G 中唯一幂等元．

证明 （1） $\forall a, b, c\in G$，设 $ab=ab$,

则　　$a^{-1}(ab) = a^{-1}(ac)$

于是　　$(a^{-1}a)b = (a^{-1}a)c$

即　　$b = c.$

同理，若 $ba = ca$，则 $b = c$．因此 G 中消去律成立．

(2) 显然 e 是幂等元，又若 $a \in G$ 是幂等元，则 $aa = a$，因此 $a^{-1}aa = a^{-1}a$，故得 $a = e$，因此 e 是 G 中唯一幂等元． ▌

定理 2　设〈G，$*$ 〉，〈H，$\circ$ 〉是群，f 是 G 到 H 的同态．若 e 为 G 的单位元，则 $f(e)$ 为 H 的单位元，且 $\forall a \in G$，　有 $f(a)^{-1} = f(a^{-1})$．

证明　$f(e) \circ f(e) = f(e * e) = f(e)$．故　$f(e)$ 是 H 的幂等元，从而是单位元．又，$\forall a \in G$

$$f(a) \circ f(a^{-1}) = f(a * a^{-1}) = f(e),$$

$$f(a^{-1}) \circ f(a) = f(a^{-1} * a) = f(e).$$

故　$f(a^{-1})$ 为 $f(a)$ 的逆元，即 $f(a)^{-1} = f(a^{-1})$． ▌

定理 3　设〈G，$*$〉是群，〈H，$\circ$〉是任意代数系统，若存在 G 到 H 的满同态，则〈H，$\circ$〉必为群．

证明　设 f：$G \sim H$，则由满同态的性质知，H 中运算 $\circ$ 满足结合律，且 G 的单位元 e 的象 $f(e)$ 是 H 的单位元，又因为 f 为满射，即 $\forall y \in H$，$\exists x \in G$ 使 $y = f(x)$，由于 x 可逆，故 y 可逆，且

$$y^{-1} = f(x)^{-1} = f(x^{-1})$$

所以，〈H，$\circ$ 〉是群． ▌

现在给出几个关于半群构成群的定理．

定理 4　设〈G，$*$ 〉是一个半群，且

（1）G 中有一左单位元 e，使 $ea = a$　　$\forall a \in G.$

（2）G 中任一元素 a，均有一“左逆元” a^{-1}，使 $a^{-1}a = e.$

则 G 为群．

证明　　$\forall a \in G$，有 $a^{-1} \in G$ 使 $a^{-1}a = e$，又对 $a^{-1} \in G$，应有 $(a^{-1})^{-1} \in G$ 使 $(a^{-1})^{-1}a^{-1} = e$，因此，

$$\begin{aligned} aa^{-1} &= e(aa^{-1}) \\ &= ((a^{-1})^{-1}a^{-1})(aa^{-1}) \\ &= (a^{-1})^{-1}(a^{-1}a)a^{-1} \\ &= (a^{-1})^{-1}ea^{-1} \\ &= (a^{-1})^{-1}a^{-1} \\ &= e \end{aligned}$$

下面证明 e 是单位元，即证 e 也是右单位元．

$\forall a \in G$，　　$ae = a(a^{-1}a) = (aa^{-1})a = ea = a.$

故 e 确为右单位元．

综上，G 有单位元 e，且对 G 中任一元素 a，存在元素 $a^{-1}\in G$ 使

$$a^{-1}a=aa^{-1}=e.$$

故知G为群. ▌

定理 5　设〈G，＊ 〉是一个半群，如果 $\forall a, b\in G$，方程

$$ax=b,\qquad ya=b$$

在 G 中总有解，则 G 是一个群.

证明　先证 G 有左单位元，为此，任取 $b\in G$ 令 $yb=b$ 的一个解为 e，则 $eb=b$.

下证 e 即为左单位元.

$\forall a\in G$，　设 $bx=a$ 的解为 c，　即　$bc=a$

则　$ea=e(bc)=(eb)c=bc=a.$

从而知 e 为左单位元.

再者，任取 $a\in G$，$ya=e$ 有解，设 a' 为一解，则 $a'a=e$，即 a' 是 a 的左逆元，这就是说，$\forall a\in G$，a 均有左逆元，由定理 4 可知，G 是群. ▌

定理 6　有限半群，如果消去律成立则必为群.

证明　设 G 为有限半群，且其中消去律成立，不妨设 G 中有 n 个元素：$G=\{a_1, a_2, \cdots, a_n\}$，其中，$a_i\neq a_j$（$i\neq j$）. 要证 G 为群，只要证明 $\forall a, b\in G$，$ax=b$，$ya=b$ 均有解即可.

$\forall a, b\in G$ 令 $aG=\{aa_1, aa_2, \cdots, aa_n\}$，则 $aG\subseteq G$，由消去律易知：

当 $i\neq j$ 时，　$aa_i\neq aa_j$

因此，G 的子集 aG 中也含有 n 个元素，故必有 $aG=G$，从而知 $b\in aG$　即

$\exists k\in\{1, 2, \cdots, n\}$，使得 $aa_k=b$，或者说 $ax=b$ 有解.

同理可证 $ya=b$ 也必有解.

综上可得，G 为群. ▌

对于低阶群，我们可以通过讨论其运算表来认识其结构.

定理 7　设〈G，＊ 〉是一个有限群，则其运算表中每一行（列）都是 G 中元素的一个全排列.

证明　设 G 中所有不同元素为 $a_1, a_2, \cdots, a_n$，即设 $G=\{a_1, a_2, \cdots, a_n\}$，其中，$a_i\neq a_j$（$i\neq j$），则其运算表中第 i 行为

$$a_ia_1,\ a_ia_2,\ \cdots,\ a_ia_n$$

为了证明这是 G 中元素的一个全排列，只需证明其中任意两项必不相同. 事实上，若

$$a_ia_j=a_ia_k,\ j\neq k,$$

则由消去律得 $a_j=a_k$，矛盾.

因此，a_ia_1，a_ia_2，$\cdots$，a_ia_n 必为 G 中 n 个元素的一个全排列. ▌

由此定理可以得出所有 1 － 4 阶群的运算表形式. 以 3 阶群为例进行讨论.

设 $G=\{e, a, b\}$ 是一个三阶群，e 是其单位元，则其运算表形式为：

$*$	e	a	b
e	e	a	b
a	a	①	②
b	b		

现在剩下四个空位需要决定，注意到每一行（列）均应为 G 中元素的一个排列，①位置只有两种选择 e 或 b，若选 e 则②位置只能选 b，但这样第三列中出现两个 b，产生矛盾，故①位置只能选 b．①位置元素选定后，②位置及其它位置的元素也随之确定．即有

$*$	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

表 2.1

以上我们说明了，若 $G=\{e, a, b\}$ 是三阶群，则其运算表必为表 2.1．反之，我们证明若〈G，$*$ 〉的运算表为表 2.1，则〈G，$*$ 〉必为三阶群．事实上，从表中立即可见，$*$ 是 G 上的运算，且有单位元 e，每个元素的逆元也均存在（$a^{-1}=b$，$b^{-1}=a$，$e^{-1}=e$）．现在只需验证运算的结合律成立，即验证

$$(x*y)*z = x*(y*z) \qquad \forall x, y, z\in G \qquad (1)$$

因 x，y，z 均有三种选择，故需 $3^3=27$ 次验证，但由于 e 是单位元，即 $\forall x\in G$，$ex = xe = x$，故若 x，y，z 取到 e，则（1）式必然成立，因此，只需验证 x，y，z 取 a 或 b 的情形，这样也需 $2^3=8$ 次验证．我们在此只以验证 $(b*b)*b = b*(b*b)$ 为例，其余不再验证．

$$(b*b)*b = a*b = e$$

$$b*(b*b) = b*a = e$$

故 $$(b*b)*b = b*(b*b)$$

通过以上讨论可知：

〈G，$*$ 〉是一个三阶群 $\Leftrightarrow$〈G ，$*$ 〉的运算表具有表 2.1 的形式．

所有 1 － 4 阶群的运算表形式列举如下：

*	e
e	e

一阶群
（a）

*	e	a
e	e	a
a	a	e

二阶群
（b）

*	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

三阶群
（c）

*	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

四阶群－1
（d）

*	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	a	e
c	c	b	e	a

四阶群－2
（e）

表 2．2

1 － 3 阶群的运算表具有唯一确定的形式，而 4 阶群的运算表有两种形式，由其中第一种形式的运算表定义的四阶群〈G，＊ 〉，称为 Klein 四元群．

例 4　设〈G，＊ 〉是二阶群，则直积〈$G\times G$，∘ 〉是 Klein 四元群．

证明　设 $G=\{e, a\}$，则 $G\times G$ 的运算表为

∘	<e,e>	<e,a>	<a,e>	<a,a>
<e,e>	<e,e>	<e,a>	<a,e>	<a,a>
<e,a>	<e,a>	<e,e>	<a,a>	<a,e>
<a,e>	<a,e>	<a,a>	<e,e>	<e,a>
<a,a>	<a,a>	<a,e>	<e,a>	<e,e>

故〈$G\times G$，∘ 〉为 Klein 四元群．

我们可以一般地说明，两个有限群（或代数系统），如果其运算表结构相同，则必定同构．因此可说，从同构观点来看，1 － 3 阶群都是存在唯一的，而四阶群有两个．

习　题　二

1．若 $A\subseteq \mathbf{R}$ 且〈A，•〉是群，则称 A 为实数乘法群，证明〈{ 0 }，•〉，〈{ 1 }，•〉，〈{1，-1}，•〉是所有有限实数乘法群．

2．设〈S，＊ 〉是幺半群，令 $S_1=\{a \mid a\in S,\ a^{-1}\in S$ 存在$\}$，证明〈S_1，＊ 〉是群．

3．举例说明无穷半群既使消去律成立也未必构成群．

4．设〈S，$*$ 〉是半群，a_1，$a_2 \in S$ 是 S 的两个不同幂等元．证明〈S，$*$ 〉必不能构成群．

5．设〈G，$*$ 〉为群，若 $\forall a \in G$，$a = a^{-1}$ 证明〈G，$*$ 〉为 Abel 群．

6．设〈G，$*$ 〉为群，$a \in G$，令

$$f: x \mapsto a\,x\,a^{-1}, \quad \forall x \in G,$$

证明 f 是 G 的自同构．

§ 3　子群与元素的周期

定义 1　设〈G，$*$ 〉是一个群，$H \subseteq G$，如果 H 在 G 的运算下也构成群，则称〈H，$*$ 〉为〈G，$*$ 〉的子群．

例 1　任何群 G 都有两个明显的子群，一个是 $\{e\}$，另一个是 G 本身．这两个子群称为 G 的平凡子群，其它子群称为真子群．

例 2　〈$\mathbf{Z}$，＋〉，〈$\mathbf{Q}$，＋〉，〈$\mathbf{R}$，＋〉中，前者均为后者的子群．

例 3　记 $\mathbf{R}^* = \mathbf{R} - \{0\}$，则〈$\mathbf{R}^*$，$\cdot$〉是群，〈$\{1, -1\}$，$\cdot$〉，〈$\mathbf{R}^+$，$\cdot$〉均为 $\mathbf{R}^*$ 的子群，但不是〈$\mathbf{R}$，＋〉的子群．

例 4　设〈G，$*$ 〉，〈H，$\circ$ 〉为两个群，f 是 G 到 H 的同态，A 是 G 的子群，则 $f(A)$ 是 H 的子群．

证明　$\forall y_1, y_2 \in f(A)$，$\exists x_1, x_2 \in A$ 使 $f(x_1) = y_1$，$f(x_2) = y_2$

故　　$y_1 \circ y_2 = f(x_1) \circ f(x_2) = f(x_1 * x_2) \in f(A)$．

因此，$f(A)$ 对 $\circ$ 是封闭的，故构成代数系统〈$f(A)$，$\circ$〉．由于

$$f|_A: A \sim f(A)$$

由上节定理 3，〈$f(A)$，$\circ$〉是群，从而 $f(A)$ 是 H 的子群．

定理 1　设 H 是群 G 的子群，则

（1） H 的单位元 e' 就是 G 的单位元 e．

（2） 对 $a \in H$，a 在 H 中的逆元 a' 就是 a 在 G 中的逆元 a^{-1}．

证明　（1）因为 e' 是 H 的单位元，则

$$e'e' = e'$$

故 e' 为 G 的幂等元，但 G 的单位元 e 是唯一的幂等元，故 $e' = e$．

（2）$\forall a \in H$，因为 a' 为 a 在 H 中的逆元，且 H 的单位元 e' 就是 G 的单位元 e，故

$$a'a = a\,a' = e' = e.$$

因而，a' 为 a 在 G 中的逆元．　▌

下面我们来讨论群 G 的子集作成子群的条件．

定理 2　设 H 是群〈G，$*$ 〉的非空子集，则 H 作成 G 的子群 当且仅当

（1） $\forall a, b\in H$ 有 $a * b\in H$.

（2） $\forall a\in H$ ，a 在 G 中的逆元 $a^{-1}\in H$.

证明　设 H 是 G 的子群，则由定义知（1）必成立．又由定理 1 知，a 在 H 中的逆元 a' 即为 a^{-1}，故 $a^{-1}\in H$.

反之，设（1）、（2）成立，则由（1）知 H 必为半群．因 H 为非空的，故可取 $a\in H$，由（2），$a^{-1}\in H$，由（1），$a * a^{-1} = e\in H$，显然，e 是 H 的单位元．又，$\forall a\in H$，$a^{-1}\in H$ 必是 a 在 H 中的逆元．故 H 是子群．　▌

推论　设〈G，$*$〉为群，S 是 G 的非空子集，则

$$S \text{ 是 } G \text{ 的子群} \Leftrightarrow \forall a, b\in S \quad a * b^{-1}\in S.$$

证明　必要性显然成立，只证充分性．

首先，由假设，$S\neq\varnothing$，故可取 $a\in S$，于是，$e = a * a^{-1}\in S$. 从而，对任意 $a\in S$，$a^{-1} = e * a^{-1}\in S$. 现设 $a, b\in S$，由以上所证，$b^{-1}\in S$，因此

$$a * b = a * (b^{-1})^{-1}\in S,$$

从而 S 是 G 的子群．　▌

例 5　设 G 是群，$C = \{a \mid a\in G, \forall x\in G: ax = xa\}$，则 C 为 G 的子群．

证明　由于 $\forall x\in G$，$ex = xe$，故 $e\in C$，即 C 非空．设 a，$b\in C$，则 $\forall x\in G$，

$$(ab)x = a(bx) = a(xb) = (ax)b = (xa)b = x(ab).$$

即 $ab\in C$. 又设 $a\in C$，则 $\forall x\in G$，$ax = xa$，两边左乘 a^{-1}，得 $x = a^{-1}xa$，两边再右乘 a^{-1}，得 $xa^{-1} = a^{-1}x$. 从而得知 $a^{-1}\in C$．综上所述，C 是群的子群，这个子群叫做群 G 的中心．

在 § 1 中，对于半群〈S，$*$ 〉中的元素 a 定义了正整数方幂 $a^n = a * a * \cdots * a$（共 n 个），现在对该定义作进一步扩充．

如果〈S，$*$ 〉是幺半群，e 是 S 的单位元，$a\in S$，令

$$a^0 = e$$

如果〈S，$*$〉是群，$a\in S$，n 为正整数，令

$$a^{-n} = (a^{-1})^n.$$

读者不妨自己写出当采用加法记号时，以上规定的表现形式．

这样一来，假设〈G，$*$ 〉是群，$a\in G$，则对任何 $m\in\mathbf{Z}$，a^m 有意义，且可验证指数律仍然成立．即

$$\begin{aligned} a^m \cdot a^n &= a^{m+n}, \\ (a^m)^n &= a^{mn}, \end{aligned} \qquad m, n\in\mathbf{Z}$$

例 6　设 G 是群，$a\in G$，令 $(a) = \{a^i \mid i\in\mathbf{Z}\}$，则 (a) 构成 G 的子群，称之为由 a 生成的循环子群．

证明　显然 (a) 非空，又 $\forall a^i, a^j\in(a)$，$a^i a^j = a^{i+j}\in(a)$；又，$\forall a^i\in(a)$ 由指数律

$$(a^i)^{-1} = a^{-i}\in(a)$$

故知（a）为 G 的子群.

例 7　对〈$\mathbf{Z}$，＋〉

（2）＝｛2i|$i\in\mathbf{Z}$｝

（1）＝｛i|$i\in\mathbf{Z}$｝＝$\mathbf{Z}$

对于〈R^+，·〉

（2）＝｛2^i|$i\in\mathbf{Z}$｝

（1）＝｛1｝

例 8　考虑〈$\mathbf{Z}_6$，$+_6$〉则

（[2]）＝｛[0]，[2]，[4]｝

（[5]）＝｛[0]，[5]，[4]，[3]，[2]，[1]｝

＝$\mathbf{Z}_6$

（[3]）＝｛[0]，[3]｝

设〈G，∗〉是群，$a\in G$，则由 a 生成的循环子群（a）既可以是有限群，也可以是无限群. 元素的周期（或称阶）是一个与此相关的重要概念.

定义 2　设 G 是群，$a\in G$，若存在正整数 n，使 $a^n=e$，则将满足该条件的最小正整数 n 称为 a 的周期（阶），若这样的 n 不存在，称 a 的周期为∞.

由定义可见，a 的周期为 n，意味着 $a^n=e$ 且 当 $0<m<n$ 时 $a^m\neq e$.

以后，我们将用|a|表示 a 的周期（阶）. 并将周期（阶）为 n 的元素称为 n 阶元素.

例 9　在〈$\mathbf{Z}$，＋〉中，0 的周期为 1，$\forall i\in\mathbf{Z}$，$i\neq 0$，i 的周期为 ∞；在〈$\mathbf{Z}_6$，$+_6$〉中，[2] 的周期为 3，[5] 的周期为 6，[3] 的周期为 2.

元素的周期是群论中非常重要的概念，下面是元素周期的两条基本性质.

定理 3　设 G 是一个群，$a\in G$，

（1）a 的周期等于 a 生成的循环子群（a）的阶，即

$$|a|=|(a)|$$

（2）若 a 的周期为 $n<\infty$，则

$$a^m=e \Leftrightarrow n|m.$$

证明　（1）分两种情况

（Ⅰ）a 的周期为有限数 n，往证（a）＝｛a^0，a^1，…，a^{n-1}｝且 a^0，a^1，…，a^{n-1} 互不相同.

∀　$a^i\in(a)$，由带余式除法，可令

$$i=kn+r \quad k,r\in\mathbf{Z},\ 0\leqslant r<n$$

则　$a^i=a^{kn+r}=a^{kn}a^r=a^r$

故　$a^i\in\{a^0,a^1,\cdots,a^{n-1}\}$

因此　$(a)\subseteq\{a^0,a^1,\cdots,a^{n-1}\}$

又显然　$\{a^0,a^1,\cdots,a^{n-1}\}\subseteq(a)$，

所以　（a）＝｛a^0，a^1，…，a^{n-1}｝.

下面说明 a^0，a^1，…，a^{n-1} 互不相同，因若

$$a^i = a^j \qquad 0 \leqslant i, j < n, i \neq j$$

不妨设 $i>j$，则 $a^{i-j} = e$，$0 < i-j < n$，与 a 的周期为 n 矛盾．所以 a^0，a^1，…，a^{n-1} 互不相同，从而 $|(a)| = n$，即有 $|a| = |(a)|$．

（Ⅱ）a 的周期为∞，这时

$$a^1, a^2, \cdots, a^i \cdots$$

互不相同，故 $|(a)| = \infty$，因此也有 $|a| = |(a)|$．

总之，在任何情况下，$|a| = |(a)|$ 总成立．

（2）设 $a^m = e$，由带余式除法，令

$$m = kn + r \qquad 0 \leqslant r < n$$

则 $$a^m = a^{kn+r} = a^{kn} a^r = a^r$$

因此 $$a^r = e, \quad 0 \leqslant r < n$$

由于 a 的周期为 n，故必有 $r = 0$，即 $n|m$．

反之，若 $n|m$，显然 $a^m = e$． ▌

由以上（1）的证明，立即可得到如下重要推论：

推论 设 G 为群，$a \in G$，若 a 的周期为 n（或等价地说 (a) 的阶为 n），则

$$(a) = \{a^0, a^1, \cdots, a^{n-1}\}$$

例 10 设 a，b 是群 G 的元素．$|a| = 2$，$|b| = 3$，且 $ab = ba$，则

$$|ab| = 6.$$

证明 因 $(ab)^6 = a^6 b^6 = b$，故 ab 必有有限周期，设 $|ab| = n$，则 $n|6$，故 n 只有四种可能，$n = 1$，2，3 或 6．若 $n = 1$，则 $ab = e$，$b = a^{-1}$，$b^2 = (a^{-1})^2 = (a^2)^{-1} = e$，矛盾，故 $n \neq 1$．又 $(ab)^2 = a^2b^2 = b^2 \neq e$，故 $n \neq 2$．$(ab)^3 = a^3b^3 = a \neq e$，故 $n \neq 3$．因此，$n = 6$．

习 题 三

1．设 G 是有限群，证明 $\forall a \in G$，a 的周期必为有限数．

2．设 G 为群，证明 G 的子群的交必为子群．子群的并如何？

3．设 G 是群，$a \in G$，$|a| = 2$，证明 $a^{-1} = a$．

4．设 G 是群，证明 $\forall a \in G$，$|a| = |a^{-1}|$．

5．证明有限群中周期大于 2 的元素必有偶数个．

6．设 G 是群，a，$b \in G$，证明 $|ab| = |ba|$．

7．求出 $\langle \mathbf{Z}_6, +_6 \rangle$ 中各元素的周期．

8．设 G_1，G_2 为两个群，f：$G_1 \cong G_2$，证明 $|a| = |f(a)|$，$a \in G_1$．

§ 4　循环群

本节我们讨论结构最简单，又是非常重要的一类群.

定义 1　设 G 是一个群，如果存在 $a\in G$，使 $G=(a)=\{a^i \mid i\in\mathbf{Z}\}$，称 G 为由 a 生成的循环群，a 称为其生成元.

由定义可见，G 是由 a 生成的循环群，意味着 G 的任何元素 x，均可表示成 a 的方幂形式，即

$$G \text{ 是由 } a \text{ 生成的循环群} \Leftrightarrow \forall x\in G,\ \exists i\in\mathbf{Z} \text{ 使 } x=a^i.$$

例 1　$\langle\mathbf{Z},+\rangle$ 是循环群. 事实上，$\forall i\in\mathbf{Z}$，$i=\overbrace{1+1+\cdots+1}^{i\text{个}}=i1$，即 $\mathbf{Z}=(1)$，$\mathbf{Z}$ 是由 1 生成的循环群. 另外，易知 -1 也为 $\mathbf{Z}$ 的生成元.

例 2　$\langle\mathbf{Q},+\rangle$ 不是循环群. 事实上，0 显然不是 $\mathbf{Q}$ 的生成元，而对 $\mathbf{Q}$ 中任何非零元素 a，$\frac{1}{2}a$ 不能表成 na（$n\in\mathbf{Z}$）的形式，即

$$\frac{1}{2}a\notin(a)$$

总之，不存在 $a\in\mathbf{Q}$，使得 $\mathbf{Q}=(a)$.

例 3　$\langle\mathbf{Z}_n,+_n\rangle$ 是循环群.

因为 $\forall\,[i]\in\mathbf{Z}_n$，$[i]=\overbrace{[1]+_n[1]+_n\cdots+_n[1]}^{i\text{个}}=i[1]$，所以

$$\mathbf{Z}_n=([1])$$

例 4　设 $\langle G,\circ\rangle$ 是由下面的运算表定义的四阶群

$\circ$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	a	e
c	c	b	e	a

则 G 是循环群.

事实上，由运算表知 $b^1=b$，$b^2=a$，$b^3=c$，$b^4=e$，故 $G=(b)$.

定理 1　设 $\langle G,*\rangle$ 是一个循环群，若 G 是无限群，则 $\langle G,*\rangle\cong\langle\mathbf{Z},+\rangle$，若 G 是 n 阶群，则 $\langle G,*\rangle\cong\langle\mathbf{Z}_n,+_n\rangle$.

证明　（1）设 G 是无限循环群，不妨设 a 为其生成元，则

$$G=(a)=\{\cdots,\ a^{-2},\ a^{-1},\ a^0,\ a^1,\ a^2,\ \cdots\}$$

令 f：$\mathbf{Z}\to G$，定义如下：

$$f:\ i\mapsto a^i \qquad \forall i\in\mathbf{Z}$$

则显然 f 为满射. 下证 f 为单射，$\forall i,j\in\mathbf{Z}$ 若 $f(i)=f(j)$，即 $a^i=a^j$，要证 $i=j$. 若

$i \neq j$，不妨设 $i>j$，则

$$a^{i-j}= e \qquad i-j> 0$$

因此 a 必有有限周期，从而 $G=(a)$ 为有限群，矛盾．所以，$i=j$，从而 f 为单射．总之 f 是双射．又 $\forall i, j\in \mathbf{Z}$

$$f(i+j) =a^{i+j}=a^{i} * a^{j} = f(i) * f(j)$$

即 f 保持运算，从而 f：$\mathbf{Z}\cong G$.

（2）设 G 为 n 阶循环群，a 为其生成元，则由上节定理 3 及推论知，a 的周期为 n，且

$$G= \{a^{0}, a^{1}, a^{2}, \cdots, a^{n-1}\}$$

其中 $a^{0}, a^{1}, \cdots, a^{n-1}$ 互不相同，令

$$f: [i] \mapsto a^{i} \qquad \forall [i] \in \mathbf{Z}_{n}$$

则显然 f 是 $\mathbf{Z}_n$ 到 G 的映射，且为满射，又设

$$f([i]) =f([j])$$

即 $a^{i}=a^{j}$，则 $a^{i-j} = e$，由周期的性质（上节定理 3 （2））可知，$n \mid i-j$ 即 $i \equiv j \mod n$. 因此 $[i] = [j]$．从而知 f 是单射．总之 f 是双射．下证 f 是同态．$\forall [i], [j] \in \mathbf{Z}_n$，

$$f([i] +_{n} [j]) = f([i+j]) =a^{i+j} = a^{i} * a^{j}$$
$$=f([i]) * f([j])$$

因此 f：$\mathbf{Z}_n\cong G$. ▌

以上定理表明，对于循环群的结构我们已经完全掌握，可以说〈$\mathbf{Z}$，+〉与〈$\mathbf{Z}_n$，$+_n$〉代表了所有循环群．

定理 2　循环群的子群必为循环群．

证明　设 G 是由 a 生成的循环群，H 是其子群，若 $H = \{a^{0}\} = \{e\}$，则 H 是由 e 生成的循环群，若 $H \neq \{e\}$，则必有 $n\neq 0$ 使 $a^{n} \in H$，由于 H 为子群，故 $a^{-n} \in H$．n 与 $-n$ 中必有一个为正整数，因此 H 中必有 a 的正整数幂．令

$$i_0 = \min \{i \mid a^{i} \in H, \quad i> 0\}$$

即 i_0 是 H 中 a 的最小正指数．往证 $H = (a^{i_0})$，$\forall a^{i} \in H$，根据带余式除法可令

$$i=ki_0+r, \quad 0 \leqslant r<i_0$$

则

$$a^{i} = a^{ki_0+r} = a^{ki_0} a^{r}$$

$$a^{r}= a^{-ki_0} a^{i}$$

由此易知 $a^{r}\in H$，由于 $0 \leqslant r<i_0$ 并注意到 i_0 的定义，可知必有 $r= 0$.

即

$$i=ki_0, \qquad a^{i} = (a^{i_0})^{k}.$$

从而　　$H=(a^{i_0})$. ▌

定理 3　设〈G，$*$　〉是 n 阶循环群，m 是正整数且 $m|n$，则 G 中存在唯一一个 m 阶子群.

证明　由于 $m|n$，可设 $n = dm$，则

$$(a^d)^m=a^{dm} = a^n =e.$$

又,$\forall h\in\mathbf{Z}$，若 $0<h<m$，则 $0<dh<n$，故由周期的定义,

$$(a^d)^h = a^{dh} \neq e.$$

从而 a^d 的周期为 m，因此，a^d 生成的循环子群 $A=(a^d)$ 是 G 的 m 阶子群. 下面再证 G 中 m 阶子群是唯一的. 在 G 中任取一 m 阶子群 H，由定理 2 知，H 是循环群，设 H 的生成元为 a^i，即 $H = (a^i)$，则 a^i 的周期为 m，因此

$$a^{im}=(a^i)^m = e.$$

所以　　$n|im$

即　　$md|\ im$

由此可见 $d|i$，不妨设 $i=kd$，则

$$a^i = a^{kd} = (a^d)^k$$

因此，$a^i\in A$. 从而，对任何 $j\in\mathbf{Z}$，$(a^i)^j\in A$，因而 $H\subseteq A$，又 H 与 $A=(a^d)$ 均有 m 个元素，所以有 $H = (a^d)$，这样就证明了 G 中有唯一的 m 阶子群. ▌

习 题 四

1．证明循环群必为 Abel 群.

2．找出〈$\mathbf{Z}_5$，$+_5$〉的所有生成元，并求出〈$\mathbf{Z}_5$，$+_5$〉所有子群.

3．设 G 是无限循环群，H 是任意循环群，证明：存在 f，使　f：$G\sim H$.

4．证明：无限循环群的子群除｛e｝外均为无限群.

§ 5　置换群

本节首先讨论一种特殊的群——置换群，进而引入置换群与一般有限群的关系，从而说明置换群可视为有限群的代表.

定义 1　有限集 S 到自身的双射称为 S 上的置换，当 $|S|=n$ 时，S 上的置换也称为 n 次置换.

例 1　令

$$f_1:\ 1\mapsto 2,\ 2\mapsto 3,\ 3\mapsto 4,\ 4\mapsto 1$$

$$f_2:\ 1\mapsto 2,\ 2\mapsto 1,\ 3\mapsto 2,\ 4\mapsto 1$$

$$f_3:\ 1\mapsto 3,\ 3\mapsto 1,\ 2\mapsto 2$$

则f_1是｛1，2，3，4｝上的置换（4次置换），f_2不是置换，f_3是｛1，2，3｝上的置换（3次置换）.

设$S=\{a_1, a_2, \cdots, a_n\}$是一个具有$n$个元素的集合，为了符号的简捷，不妨设$S=\{1, 2, \cdots, n\}$. 要确定$S$上的一个置换$\sigma$，只要指出$S$中任一元素$i$在$\sigma$下的象即可，因此，$\sigma$可以表示成如下形式

$$\sigma=\begin{pmatrix}1 & 2 & \cdots\cdots & n\\ \sigma(1) & \sigma(2) & \cdots\cdots & \sigma(n)\end{pmatrix}$$

值得注意的是，S上的置换表示的是S中元素的某种对应法则，故在以上记法中，元素的顺序是无关紧要的，对1，2，…，n的任一排列i_1，i_2，…，i_n，　σ也可记作

$$\sigma=\begin{pmatrix}i_1 & i_2 & \cdots\cdots & i_n\\ \sigma(i_1) & \sigma(i_2) & \cdots\cdots & \sigma(i_n)\end{pmatrix}$$

例如，设σ是S=｛1，2，3｝上的置换，定义如下

σ：$1\mapsto 2$，$2\mapsto 3$，$3\mapsto 1$

则
$$\sigma=\begin{pmatrix}1 & 2 & 3\\ 2 & 3 & 1\end{pmatrix}=\begin{pmatrix}3 & 2 & 1\\ 1 & 3 & 2\end{pmatrix}$$

利用以上记法，可方便地进行置换的复合和求逆运算（置换的复合也称为置换的乘法. 两置换σ，τ进行复合的结果$\sigma\circ\tau$也称为σ与τ的乘积，简记为$\sigma\tau$）.

设

$$\tau=\begin{pmatrix}1 & 2 & \cdots\cdots & n\\ i_1 & i_2 & \cdots\cdots & i_n\end{pmatrix}\qquad \sigma=\begin{pmatrix}i_1 & i_2 & \cdots\cdots & i_n\\ j_1 & j_2 & \cdots\cdots & j_n\end{pmatrix}$$

则$\sigma\tau(1)=\sigma(\tau(1))=\sigma(i_1)=j_1$，$\sigma\tau(2)=\sigma(\tau(2))=\sigma(i_2)=j_2$，…

即

$$\sigma\tau=\begin{pmatrix}i_1 & i_2 & \cdots\cdots & i_n\\ j_1 & j_2 & \cdots\cdots & j_n\end{pmatrix}\begin{pmatrix}1 & 2 & \cdots\cdots & n\\ i_1 & i_2 & \cdots\cdots & i_n\end{pmatrix}=\begin{pmatrix}1 & 2 & \cdots\cdots & n\\ j_1 & j_2 & \cdots\cdots & j_n\end{pmatrix}$$

且易知
$$\tau^{-1}=\begin{pmatrix}i_1 & i_2 & \cdots\cdots & i_n\\ 1 & 2 & \cdots\cdots & n\end{pmatrix}.$$

例2　设

$$\varphi_1=\begin{pmatrix}1 & 2 & 3\\ 3 & 2 & 1\end{pmatrix},\qquad \varphi_2=\begin{pmatrix}1 & 2 & 3\\ 2 & 3 & 1\end{pmatrix}$$

则

$$\varphi_1\varphi_2=\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}$$

$$=\begin{pmatrix}2&3&1\\2&1&3\end{pmatrix}\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}$$

$$=\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}$$

$$\varphi_1^{-1}=\begin{pmatrix}3&2&1\\1&2&3\end{pmatrix}=\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}$$

$$\varphi_2^{-1}=\begin{pmatrix}2&3&1\\1&2&3\end{pmatrix}=\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}$$

定义 2　S 上如下形状的置换

$$\sigma=\begin{pmatrix}i_1&i_2&\cdots&i_{d-1}&i_d&i_{d+1}&\cdots&i_n\\i_2&i_3&\cdots&i_d&i_1&i_{d+1}&\cdots&i_n\end{pmatrix}$$

称为循环置换，记为（i_1，i_2，…，i_d），d 为循环长度．当 $d=2$ 时称为对换．

单位置换即恒等映射也视为循环置换，并记为（1）或（n）．

由以上定义可知，循环置换（i_1，i_2，…，i_d）是把 i_1 变为 i_2，i_2 变为 i_3，…，i_d 又变为 i_1，其余元素保持不变的置换．例如

$$\begin{pmatrix}1&2&3&4\\2&4&3&1\end{pmatrix}=（1\quad 2\quad 4）$$

$$\begin{pmatrix}1&2&3&4\\1&3&2&4\end{pmatrix}=（2\quad 3）$$

$$\begin{pmatrix}1&2&3&4\\1&2&3&4\end{pmatrix}=（1）$$

采用这种记法，必须指明置换的次数，即 S 中的元素数．

下面我们来讨论置换群．

当 S 是具有 n 个元素的有限集时，S 中的 n 个元素总可以用 1，2，…，n，这 n 个

数字（作为抽象符号）表示，故在以后的讨论中，可不失一般性地假设 $S=\{1, 2, \cdots, n\}$ 而不必特别指明 S. 同时，所有 n 次置换（即 $S=\{1, 2, \cdots, n\}$ 上的所有置换）构成的集合将用符号 S_n 表示.

定理 1　S_n 在置换乘法（即复合）运算下构成群.

证明　我们已经知道，$\forall f, g \in S_n$，$g \circ f \in S_n$，即 S_n 对运算 $\circ$ 是封闭的，而 $\circ$ 满足结合律，故知 $\langle S_n, \circ \rangle$ 是一个半群，显然，恒等映射 $I_s \in S_n$，且是 $\langle S_n, \circ \rangle$ 中单位元，又，对任意 $f \in S_n$，f 的逆函数 $f^{-1} \in S_n$ 且 $f^{-1} \circ f = f \circ f^{-1} = I_s$. 即 f^{-1} 为 f 在 $\langle S_n, \circ \rangle$ 中的逆元，从而 $\langle S_n, \circ \rangle$ 是群. ▌

定理 2　$|S_n| = n!$

证明　任取一个 n 次置换 φ，则

$$\varphi(1), \varphi(2), \cdots, \varphi(n)$$

必是 1，2，…，n 的一个全排列，且置换 φ 不同，对应的全排列也不同. 反之，任取 1，2，…，n 的一个全排列 $i_1, i_2, \cdots, i_n$，令

$$\varphi=\begin{pmatrix} 1 & 2 & \cdots\cdots & n \\ i_1 & i_2 & \cdots\cdots & i_n \end{pmatrix}$$

则 φ 是与之对应的置换，因此，n 次置换与 n 个元素的全排列一一对应，而 n 个元素的全排列共有 $n!$ 个，故知 $|S_n| = n!$. ▌

定义 3　S_n 称为 n 次对称群，其子群称为 n 次置换群.

例 3　写出 $\langle S_3, \circ \rangle$ 的元素与运算表.

S_3 的所有元素为

$$\sigma_0=\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \quad \sigma_1=\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \quad \sigma_2=\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

$$\sigma_3=\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \quad \sigma_4=\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \quad \sigma_5=\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

S_3 的运算表为

$\circ$	σ_0	σ_1	σ_2	σ_3	σ_4	σ_5
σ_0	σ_0	σ_1	σ_2	σ_3	σ_4	σ_5
σ_1	σ_1	σ_0	σ_5	σ_4	σ_3	σ_2
σ_2	σ_2	σ_4	σ_0	σ_5	σ_1	σ_3
σ_3	σ_3	σ_5	σ_4	σ_0	σ_2	σ_1
σ_4	σ_4	σ_2	σ_3	σ_1	σ_5	σ_0
σ_5	σ_5	σ_3	σ_1	σ_2	σ_0	σ_4

从上表可见 $\langle S_3, \circ \rangle$，不是 Abel 群，其中，$\sigma_0$（单位元）周期为 1；$\sigma_1$，$\sigma_2$，$\sigma_3$ 周期为 2；　σ_4，σ_5 周期为 3，且

$(\sigma_0)=\{\sigma_0\}$，　$(\sigma_1)=\{\sigma_0,\ \sigma_1\}$，　$(\sigma_2)=\{\sigma_0,\ \sigma_2\}$

$(\sigma_3)=\{\sigma_0,\ \sigma_3\}$，　$(\sigma_4)=(\sigma_5)=\{\sigma_0,\ \sigma_4,\ \sigma_5\}$

以上循环子群皆为 3 次置换群.

例 4　设 $S=\{a,\ b,\ c,\ d\}$

$$\varphi_1=\begin{pmatrix} a & b & c & d \\ a & c & b & d \end{pmatrix} \qquad \varphi_2=\begin{pmatrix} a & b & c & d \\ a & b & c & d \end{pmatrix}$$

则 $\{\varphi_1,\ \varphi_2\}\subseteq S_4$，且 $\langle\{\varphi_1,\ \varphi_2\},\circ\ \rangle$ 构成群，因此 $\langle\{\varphi_1,\ \varphi_2\},\circ\ \rangle$ 是一个 S 上的 2 阶置换群.

定理 3（Cayley 定理）　任意 n 阶群必同构于一个 n 次置换群.

证明　设 G 为一个 n 阶群，G_n 是 G 上的所有置换构成的 n 次对称群，$a\in G$，令 f_a：$G\to G$ 由下式定义：

$$f_a(x)=ax \qquad x\in G$$

则不难验证 f_a 是一个 G 上的置换（读者自证），记

$$F_G=\{f_a\mid a\in G\},$$

则 $F_G\subseteq G_n$. 下证 F_G 是 G_n 的子群. $\forall f_a,\ f_b\in F_G$

$$(f_af_b)(x)=f_a(f_b(x))=abx=f_{ab}(x)$$

即有　　$f_af_b=f_{ab}\in F_G$,

又对任意 $f_a\in F_G$,

$$f_af_{a^{-1}}(x)=f_a(f_{a^{-1}}(x))=f_a(a^{-1}x)=a(a^{-1}x)=x$$

即　$f_af_{a^{-1}}=I_G$，同理 $f_{a^{-1}}f_a=I_G$，注意到 I_G 是 G_n 的单位元，

便知　　$f_a^{-1}=f_{a^{-1}}\in F_G$,

因此，F_G 是 G_n 的子群, 从而是 n 次置换群. 下证 $G\cong F_G$.

令　　h：$G\to F_G$

$$h(a)=f_a \qquad \forall\, a\in G$$

显然 h 为满射，又若 $a\neq b$，则 $f_a(e)\neq f_b(e)$，故 $f_a\neq f_b$，因此 h 也是单射. 从而，h 是双射. 又，

$$h(a\,b)=f_{ab}=f_af_b=h(a)\,h(b)$$

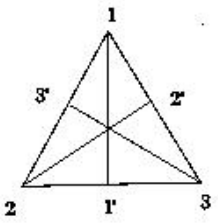
即 h 保持运算，故知　h：$G\cong F_G$，定理得证. ▌

若设 $G=\{a_1,\ a_2,\ \cdots,\ a_n\}$，定理中的 f_a 实际上就是置换

$$\begin{pmatrix} a_1 & , a_2 & , & \cdots & a_n \\ aa_1, & aa_2, & & \cdots & aa_n \end{pmatrix}$$

最后，我们看一个置换群的例子，取定一正三角形，其三个角分别标以 1 、 2 、 3 ，

能使三角形与原来位置重合的刚体变换称为三角形的对称变换，三角形的对称变换有 6 个（如图 5.1）：绕中心旋转 120°，240°，360°；分别绕轴 1－1'，2－2'，3－3' 旋转 180°．所谓绕中心旋转 120° 即将∠1 变为∠2，∠2 变为∠3，∠3 变为∠1，它可用置换 $\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}$ 表示，同样，其它 5 个对称变换也可用置换表示．所有这些变换构成的集合 D_3 恰为 S_3，我们已经知道它在置换复合运算下构成一个群．同样，正四边形的对称变换也可用 4 次置换表示，所有这些变换构成的集合 D_4，在置换复合运算下也构成群，但 $D_4 \neq S_4$．请读者自己验证．



习 题 五

1. 设 φ_1，φ_2，$\varphi_3 \in S_4$

φ_1＝（1，2），φ_2＝（1，3）（2，4），φ_3＝（1，2，3）

求 $\varphi_1\varphi_2$，$\varphi_2\varphi_1$，$(\varphi_2)^{-1}\varphi_3$，并解方程 $\varphi_3 x = \varphi_1$．

2．求出正四边形的所有对称变换构成的集合 D_4，并证明〈D_4，∘〉为群．

3．设〈G，＊〉是 4 阶群，写出与 G 同构的 4 次置换群．

*§ 6 陪 集

首先把整数集 **Z** 上的模 m 同余关系推广到一般群．由定义，∀ a，b∈**Z**，

$a \equiv b \bmod m \Leftrightarrow m \mid a-b \Leftrightarrow a-b \in \{k\,m \mid k \in \mathbf{Z}\} \Leftrightarrow a+(-b) \in (m)$

其中，(m) 表示群〈**Z**，＋〉中 m 生成的循环子群．更一般地（并且改写成乘法记号）我们有

定义 1　设 G 是一个群，H 是其子群，利用 H 在 G 上按如下方式定义关系 R_H，$\overline{R}_H$

$$a\,R_H\,b \Leftrightarrow b^{-1}a \in H$$

$$a\,\overline{R}_H\,b \Leftrightarrow a\,b^{-1} \in H$$

称 R_H 为模 H 左同余关系，$\overline{R}_H$ 为模 H 右同余关系，并将 $a\,R_H\,b$ 记为 $a \equiv b \bmod H$，

$a\,\overline{R}_H\,b$ 记为 $a \equiv_r b \bmod H$.

显然，群〈**Z**，＋〉中的模（m）左（右）同余关系，即为通常整数集 **Z** 上的模 m 同余关系.

模 H 右同余关系与模 H 左同余关系具有类似的性质，下面将以左同余关系为例讨论. 在不引起混乱的情况下，有时将 $a \equiv b \mod H$ 简写成 $a \equiv b$.

定理 1　设 H 是群〈G，＊ 〉的子群，则 G 中的模 H 左同余关系 R_H 是等价关系.

证明　$\forall a \in G$，$a^{-1} * a = e \in H$，故 $a \equiv a \bmod H$. 因此，R_H 是自反的. 又 $\forall a, b \in G$，若 $a \equiv b \mod H$ 则 $b^{-1} * a \in H$，由于 H 是子群

$$(b^{-1} * a)^{-1} = a^{-1} * b \in H$$

即 $b \equiv a \mod H$. 因此 R_H 是对称的. 最后，$\forall a, b, c \in G$，

若　$a \equiv b \bmod H$　　$b \equiv c \bmod H$

则　　$b^{-1} * a \in H$　　$c^{-1} * b \in H$

因此　　$c^{-1} * a = c^{-1} * (b * b^{-1}) * a$

$$= (c^{-1} * b) * (b^{-1} * a) \in H$$

故　$a \equiv c \mod H$，　即 R_H 是传递的.

综上，模 H 左同余关系 R_H 是等价关系. ▌

再来考虑 G 中模 H 左同余关系所产生的等价类，和从前一样，$a \in G$ 所在的等价类用［a］表示，则

$$[a] = \{x \mid x \equiv a \mod H\} = \{x \mid a^{-1}x \in H\}$$
$$= \{x \mid a^{-1}x = h, h \in H\} = \{x \mid x = ah, h \in H\}$$
$$= \{ah \mid h \in H\}$$

于是有：

定理 2　设 H 是 G 的子群，则 $a \in G$ 所在的模 H 左同余关系等价类

$$[a] = \{ah \mid h \in H\}.$$

由于 R_H 等价类［a］中元素的形式，以后将用 aH 表示［a］，即

$$aH = [a] = \{ah \mid h \in H\},$$

并称其为 H 在 G 内由 a 决定的左陪集，a 称为 aH 的代表元.

若用加法记号，则左陪集 aH 可记为 $a+H$，即

$$a+H = \{a+h \mid h \in H\}$$

由左陪集的形式及等价类的性质，立即知道

定理 3　设 H 是群 G 的子群，则

（1）$eH = H$

（2）$aH = bH \Leftrightarrow b^{-1}a \in H \quad \forall a, b \in G$

（3）$aH = H \Leftrightarrow a \in H \quad \forall a \in G$

证明留作习题.

例 1　对 3 次置换群 S_3，仍采用上节例 3 的记号，则 $H_1 = \{\sigma_0, \sigma_1\}$，$H_2 = \{\sigma_0, \sigma_4, \sigma_5\}$ 是 S_3 的子群，且由上节例 3 给出的运算表易知.

$$\sigma_0 H_1 = \sigma_1 H_1 = \{\sigma_0, \sigma_1\}$$

$$\sigma_2H_1=\sigma_4H_1=\{\sigma_2,\ \sigma_4\}$$
$$\sigma_3H_1=\sigma_5H_1=\{\sigma_3,\ \sigma_5\}$$
$$\sigma_0H_2=\sigma_4H_2=\sigma_5H_2=\{\sigma_0,\ \sigma_4,\ \sigma_5\}$$
$$\sigma_1H_2=\sigma_2H_2=\sigma_3H_2=\{\sigma_1,\ \sigma_2,\ \sigma_3\}$$

例 2　$H=\{[0],[2]\}$ 是 $\langle \mathbf{Z}_4,+_4\rangle$ 的子群，H 的各左陪集为

$$[0]+H=[2]+H=\{[0],[2]\}$$
$$[1]+H=[3]+H=\{[1],[3]\}$$

注意，这里用的是加法记号.

同样地，群 G 中的模 H 右同余关系 $\overline{R}_H$ 是等价关系，在关系 $\overline{R}_H$ 下 $a\in G$ 所在的等价类

$$[a]=\{ha\mid h\in H\}$$

称为 H 在 G 内由 a 决定的右陪集，右陪集具有与左陪集相同的性质，但一般来说 $aH\neq Ha$.

例 3　对例 1 的 H_1，有以下右陪集

$$H_1\sigma_0=H_1\sigma_1=\{\sigma_0,\ \sigma_1\}$$
$$H_1\sigma_2=H_1\sigma_5=\{\sigma_2,\ \sigma_5\}$$
$$H_1\sigma_3=H_1\sigma_4=\{\sigma_3,\ \sigma_4\}$$

我们看到，$H_1\sigma_2\neq\sigma_2H_1$，$H_1\sigma_3\neq\sigma_3H_1$ 等.

定义 2　设 H 是群 G 的子群，H 的所有左陪集构成的集合，即集合族

$$S_L=\{aH\mid a\in G\}$$

称为 G 对 H 的左商集，H 的所有右陪集构成的集合，即集合族

$$S_R=\{Ha\mid a\in G\}$$

称为 G 对 H 的右商集.

由该定义立即可知，S_L 实际上是 G 中模 H 左同余关系 R_H 产生的等价类集合——G 对 R_H 的商集 G/R_H. S_R 则是 G 中模 H 右同余关系 $\overline{R}_H$ 产生的等价类集合——G 对 $\overline{R}_H$ 的商集 $G/\overline{R}_H$.

在例 1 中，S_3 对 H_1 的左商集为 $\{\{\sigma_0,\ \sigma_1\},\{\sigma_2,\ \sigma_4\},\{\sigma_3,\ \sigma_5\}\}$，右商集为 $\{\{\sigma_0,\ \sigma_1\},\{\sigma_2,\ \sigma_5\},\{\sigma_3,\ \sigma_4\}\}$，$S_3$ 对 H_2 的左、右商集均为 $\{\{\sigma_0,\ \sigma_4,\ \sigma_5\},\{\sigma_1,\ \sigma_2,\ \sigma_3\}\}$，在例 2 中，$\mathbf{Z}_4$ 对 H 的左、右商集均为 $\{\{[0],[2]\},\{[1],[3]\}\}$

在下面我们将较随意地使用“元素个数”这个词，而不限于有限集，因为这样虽不严格，但对我们关注的问题已经足够了（我们关注的往往是有限的情况）.

定理 4　对任意群 G 及其子群 H，H 的左、右陪集数必相等，即可在 G 对 H 的左商集 S_L 与右商集 S_R 之间建立双射.

证明　令 φ：$S_L\to S_R$，定义如下

$$\varphi:\ aH\mapsto Ha^{-1}\qquad \forall a\in G$$

首先需要证明 φ 的定义是合理的，即 $\forall\, aH\in S_L$，$\varphi(aH)$ 唯一确定而与代表元 a 的选取无关．事实上，设 $aH=bH$，则 $b^{-1}a\in H$，由于 H 是子群，故 $(b^{-1}a)^{-1}\in H$, 即 $a^{-1}(b^{-1})^{-1}\in H$. 因而 a^{-1}，b^{-1}满足模 H 右同余关系，从而 $Ha^{-1}=Hb^{-1}$．于是 $\varphi(aH)=\varphi(bH)$，即 $\varphi(aH)$ 由左陪集 aH 唯一确定，而与代表元选取无关，φ 的定义合理．

现证明 φ 是双射，先证满射，

$\forall\, Ha\in S_R$，$\varphi(a^{-1}H)=Ha$，故φ为满射，往证φ是单射．

$\forall\, aH,\ bH\in S_L$，若 $aH\neq bH$，则 $b^{-1}a\notin H$，从而由于 H 是子群，$(b^{-1}a)^{-1}\notin H$，即

$$(a^{-1})(b^{-1})^{-1}\notin H$$

或说 a^{-1} 与 b^{-1} 不满足模 H 右同余关系，因此，$Ha^{-1}\neq Hb^{-1}$，即

$$\varphi(aH)\neq\varphi(bH)$$

φ 是单射，综上，φ 为双射． ▌

定理 3 说明了，群 G 的子群 H 的左陪集数与右陪集数是相等的．因此，可引入如下定义．

定义 3　设 H 是群 G 的子群，H 的左（右）陪集数称为 H 在 G 内的指数，记为 $[G:H]$.

$[G:H]$ 可以是有限数也可以是无穷，而我们感兴趣的是有限的情况．

例 1 中 $[S_3:H_1]=3$，$[S_3:H_2]=2$；例 2 中 $[\mathbf{Z}_4:H]=2$．

不仅象我们已看到的，子群 H 的左陪集与右陪集一样多，而且进一步还可以证明每个左（右）陪集的元素也都一样多．

定理 5　对 G 的任意子群 H，H 的任意左（或右）陪集 aH(或 Ha) 必与 H 具有相同的元素个数，即 $|aH|=|Ha|=|H|$.

证明　对于 $a\in G$, 为证 $|aH|=|H|$，

令 $\varphi:\ H\to aH$，

$$\varphi:\ h\mapsto ah\qquad \forall\, h\in H$$

则显然φ是满射，又若 h_1，$h_2\in H$，$h_1\neq h_2$，则 $a\,h_1\neq a\,h_2$（因为, 否则由消去律可得 $h_1=h_2$），即

$$\varphi(h_1)\neq\varphi(h_2)$$

因而 φ 为单射，从而 φ 为双射．于是$|aH|=|H|$，同理可证$|Ha|=|H|$． ▌

这个定理所指出的结果，我们在前面的各例题中都可明显看到．

将这个定理用于有限群，立即可得到如下重要定理．

定理 6（拉格朗日定理）　设 G 是有限群，H 是其子群，则 H 的阶必整除 G 的阶，且

$$|G|=[G:H]\,|H|$$

证明　H 共有$[G:H]$个左陪集，由等价类的性质，这些左陪集产生 G 的一个划分．而由上定理知，H 的每个左陪集都有$|H|$个元素．因此

$$|G| = [G:H]\ |H|$$

由于 $[G:H]$ 必为整数，故 $|H|$ 整除 $|G|$. ▌

这个定理揭示了有限群与其子群阶数之间的关系，是一个非常重要的结论.

推论 1　素数阶群必为循环群.

证明　设 G 是 p 阶群，p 是素数，则 $p>1$，因此可取 $a\in G$，$a\neq e$，设（a）的阶为 m，则 $m>1$，且由拉格朗日定理，$m|p$，由于 p 为素数，故 $m=p$，即（a）是 p 阶循环子群，从而知 G 的 p 个元素均含于（a）中，故 G =（a）.

推论 2　若 G 为有限群，则 $\forall a\in G$，$|a|$ 整除 $|G|$.

证明　$\forall\, a\in G$，由于 G 为有限群，由由拉格朗日定理 $|(a)|\,|\,|G|$. 又，$|(a)|=|a|$，故 $|a|\,|\,|G|$.

推论 3　若 G 为有限群，则 $\forall\, a\in G$，$a^{|G|}=e$.

证明　$\forall\, a\in G$，$|a|$ 整除 $|G|$，故 $a^{|G|}=e$.

以上定理及推论对有限群的研究有着重要的作用，通过以下例题可对此有所了解.

例 5　前面我们已经讨论过 1 － 4 阶群，现在用拉格朗日定理及其推论重新考查，一阶群不必再讨论，2 、3 阶群必为循环群. 设〈G，＊ 〉为四阶群，若 G 中有一周期为 4 的元素 a，则 G =（a）是循环群，否则 G 中元素的周期只可能是 1 或 2 ，即除单位元 e 处，其余元素周期均为 2 ，这时为 Klein 四元群.

例 6　6 阶群中必有 3 阶子群.

证明　设 G 是一个 6 阶群，则 G 中元素的周期只可能是 1 ， 2 ， 3 或 6 ，下面用反证法证明 G 中必有 3 阶子群.

若 G 中无 3 阶子群，则 G 中必无周期为 3 的元素，从而也无周期为 6 的元素（因为若 a 的周期为 6 ，则 a^2 的周期为 3 ），所以，G 中元素的周期只能是 1 或 2 ，因此，$\forall\, a\in G$，必有 $a^2=e$，即 $a=a^{-1}$ ，由习题二题 5 知，G 为 Abel 群. 取 a，$b\in G$，满足 $a\neq e$，$b\neq e$，$a\neq b$，令 $H=\{e, a, b, ab\}$，可以验证，e，a，b，ab 互不相同，作出这些元素的运算表如下：

	e	a	b	ab
e	e	a	b	ab
a	a	e	ab	b
b	b	ab	e	a
ab	ab	b	a	e

由此可见，H 是一个 Klein 四元群，从而是 G 的子群，由拉格朗日定理，4 | 6 ，矛盾. 故 G 中必有 3 阶子群.

习 题 六

1 . 证明定理 3 .

2 . 证明 1 － 5 阶群必为 Abel 群，求出一非交换的 6 阶群.

3．设 S_3 为 3 次对称群，$H=\{\sigma_0,\ \sigma_2\}$，求 H 的所有左、右陪集及 G 对 H 的左、右商集.

4．设〈**Q**，＋〉为有理数加法群，整数加法群〈**Z**，＋〉是其子群．问 $6+\mathbf{Z}$ 意义为何，并求之.

5．设 G 是 pq 阶 Abel 群，p，q 为不同素数．a，$b\in G$ 且 $|a|=p$，$|b|=q$，证明：G 为循环群.

6．设 H 是群 G 的子群，证明 H 的所有左陪集中恰有一个是 G 的子群.

7．设 H，K 是群 G 的子群，$|H|=m$，$|K|=n$，且（m，n）＝1，证明 $H\cap K=\{e\}$.

8．设 p 为素数，m 为正整数，证明 p^m 阶群中必有 p 阶子群.

*§ 7　正规子群

（一） 正规子群的定义及等价条件

为了引出商群的概念，我们首先来定义正规子群.

定义 1　设 G 是一个群，H 是其子群，如果 $\forall a\in G$，有

$$aH = Ha$$

则称 H 为 G 的正规子群.

由此定义易知，Abel 群的任何子群必为正规子群．事实上，设 H 是 Abel 群 G 的子群，则

$$aH=\{ah\mid h\in H\} = \{ha\mid h\in H\} =Ha \qquad \forall a\in G$$

例 1　设 S_3 是 3 次对称群，令 $H_1=\{\sigma_0,\ \sigma_2\}$，$H_2=\{\sigma_0,\ \sigma_4,\ \sigma_5\}$，则 H_1，H_2 均为 S_3 的子群．考查其是否为正规子群．由于

$$\sigma_2H_1=\{\sigma_2,\ \sigma_4\},\ H_1\sigma_2=\{\sigma_2,\ \sigma_5\},$$

$$\sigma_2H_1 \neq H_1\sigma_2$$

故 H_1 不是 S_3 的正规子群．由于

$$\sigma_0H_2=\sigma_4H_2=\sigma_5H_2=\{\sigma_0,\ \sigma_4,\ \sigma_5\}$$

$$H_2\sigma_0=H_2\sigma_4=H_2\sigma_5=\{\sigma_0,\ \sigma_4,\ \sigma_5\}$$

$$\sigma_1H_2=\sigma_2H_2=\sigma_3H_2=\{\sigma_1,\ \sigma_2,\ \sigma_3\}$$

$$H_2\sigma_1=H_2\sigma_2=H_2\sigma_3=\{\sigma_1,\ \sigma_2,\ \sigma_3\}$$

因此可见，$\forall\, a\in S_3$，$aH_2=H_2a$，即 H_2 是 S_3 的正规子群.

例 2　由于〈$\mathbf{Z}_n$，$+_n$〉是 Abel 群，故其任何子群必为正规子群.

例 3　设 H 是 G 的子群，且 $[G:H]=2$，则 H 是 G 的正规子群.

证明　由于 $[G:H]=2$，故 H 在 G 中共有 2 个左陪集及 2 个右陪集.

$\forall\, a\in G$，若 $a\in H$，则

$$aH=H=Ha$$

若 $a\notin H$，则 H，aH 是两个不同的左陪集，即为 H 的所有左陪集，因此 $\{H,\ aH\}$ 是 G

的一个划分，因此 $aH=G-H$. 同理 $Ha=G-H$，所以 $aH=Ha$. 即对任何 $a\in G$，$aH=Ha$，从而 H 是正规子群.

定理 1　设 G 是一个群，H 是 G 的子群，则以下各条等价.

（1）　$aH=Ha$　　$\forall a\in G$

（2）　$\forall a\in G$，$h\in H$，必存在 $h'\in H$，使 $ha=ah'$

（3）　$a^{-1}ha\in H$　　$\forall a\in G$，$h\in H$

证明　（1）$\Rightarrow$（2）

$\forall a\in G$，$h\in H$，$ha\in Ha$，因为 $Ha=aH$，所以 $ha\in aH$，故存在 $h'\in H$ 使 $ha=ah'$.

（2）$\Rightarrow$（3）

$\forall a\in G$，$h\in H$，由（2），必存在 $h'\in H$ 使 $ha=ah'$，故 $a^{-1}ha=h'\in H$.

（3）$\Rightarrow$（1）

设 a 是 G 中任一元素，如果 $x\in Ha$，则 $\exists h\in H$，使得 $x=ha$，因而

$$x=ha=(aa^{-1})ha=a(a^{-1}ha).$$

由题设，$a^{-1}ha\in H$，故 $x=a(a^{-1}ha)\in aH$. 因此 $Ha\subseteq aH$.

反之，设 $x\in aH$，则 $\exists h\in H$，使得 $x=ah$，因而

$$x=ah=aha^{-1}a=(aha^{-1})a=((a^{-1})^{-1}ha^{-1})a.$$

由题设，$(a^{-1})^{-1}ha^{-1}\in H$，故 $x=((a^{-1})^{-1}ha^{-1})a\in Ha$. 因此 $aH\subseteq Ha$.

总之，有 $aH=Ha$. ▌

对于 G 的正规子群 H，我们不必区分左、右陪集 aH 与 Ha 而称为陪集，从而也不必区分 G 对 H 的左、右商集 S_L 与 S_R 而称为商集，并记为 G/H，即

$$G/H=\{aH\mid a\in G\}=\{Ha\mid a\in G\}$$

进一步地，由于 $G/R_H=G/\overline{R}_H=G/H$，故由第二章 § 5 定理 4 知：$R_H=\overline{R}_H$，因而也不必区分模 H 左、右同余关系 R_H 与 $\overline{R}_H$ 而称为模 H 同余关系.

例 4　$\langle\mathbf{Z},+\rangle$ 是 Abel 群，$(m)=\{km\mid k\in\mathbf{Z}\}$ 是 $\mathbf{Z}$ 的正规子群. $i\in\mathbf{Z}$ 所在的陪集为 $i+(m)$，故

$$\mathbf{Z}/(m)=\{i+(m)\mid i\in\mathbf{Z}\}$$

由于 $i+(m)=\{km+i\mid k\in\mathbf{Z}\}=[i]_m$

故　$\mathbf{Z}/(m)=\{[i]\mid i\in\mathbf{Z}\}=\mathbf{Z}_m$

例 5　设 S_3 为 3 次对称群，

$$H=\{\sigma_0,\ \sigma_4,\ \sigma_5\}=\{(1),(1,2,3),(1,3,2)\}$$

则 $S_3/H=\{H,\ \sigma_2H\}$

$$=\{\{(1),(1,2,3),(1,3,2)\},\{(1,2),(1,3),(2,3)\}\}.$$

例 6　令 $\mathbf{Q}^*=\mathbf{Q}-\{0\}$，$H=\{-1,\ 1\}$ 是 $\langle\mathbf{Q}^*,\cdot\rangle$ 的正规子群.

$$\mathbf{Q}^*/H=\{aH\mid a\in\mathbf{Q}\}=\{\{-a,a\}\mid a\in\mathbf{Q}\}.$$

（二） 商群

设〈G，$*$ 〉为群，H 是其正规子群，现利用 G 中的运算在商集 G/H 上定义运算“$\circ$”如下：

$$aH\circ bH = (ab)H$$

这里，用代表元定义陪集的运算，须验证运算结果与代表元的选取无关，而由陪集 aH 与 bH 唯一确定.

分别任取 aH 与 bH 的代表元 a_1，b_1，即设 $aH=a_1H$，$bH=b_1H$，须证 $(ab)H=(a_1b_1)H$. 由于 $aH=a_1H$，$bH=b_1H$，故 $a_1\equiv a \mod H$，$b_1\equiv b \mod H$. 即 $a^{-1}a_1\in H$，$b^{-1}b_1\in H$. 令 $a^{-1}a_1=h_1$，$b^{-1}b_1=h_2$，则

$$\begin{aligned}(ab)^{-1}(a_1b_1) &= b^{-1}a^{-1}a_1b_1=b^{-1}h_1b_1\\ &= b^{-1}h_1b\,b^{-1}b_1=b^{-1}h_1b\,h_2\end{aligned}$$

因为 H 为正规子群，故 $b^{-1}h_1b\in H$，又 $h_2\in H$. 于是（$b^{-1}h_1b$）$h_2\in H$，即$(ab)^{-1}(a_1b_1)\in H$，因而有 $a_1b_1\equiv ab \mod H$ 即有（a_1b_1）H=（ab）H，因此，运算结果与代表元选取无关，以上定义的运算是合理的.

容易验证，〈G/H，$\circ$ 〉是一个群，且 $eH=H$ 是其单位元，$aH\in G/H$ 的逆元为 $a^{-1}H$. 〈G/H，$\circ$ 〉称为 G 对 H 的商群.

令 $$g_H:\ a\mapsto aH \qquad \forall a\in G$$

则 g_H 是〈G，$*$ 〉到〈G/H，$\circ$〉的满同态，称为 G 到 G/H 的自然同态.

例 7 〈$\mathbf{Z}$，$+$〉是整数加法群，（m）=$\{km\mid k\in\mathbf{Z}\}$ 是其正规子群，易见，$\mathbf{Z}$ 对（m）的商群为〈$\mathbf{Z}_m$，$+_m$〉.

例 8 例 6 中的〈$\mathbf{Q}^*$，$\cdot$ 〉对其正规子群 H=｛-1，1｝的商群为〈Q^*/H，$\circ$ 〉，其中运算“$\circ$”定义如下：

$\{-a,a\}\circ\{-b,b\}=\{-ab,ab\}$.

例 9 H=｛（1），（1，2，3），（1，3，2）｝=｛σ_0，σ_4，σ_5｝为三次对称群 S_3 的正规子群，商群 S_3/H=｛H，（1，2）H｝中的运算由下表给出

$\circ$	H	（1，2）H
H	H	（1，2）H
（1，2）H	（1，2）H	H

（三） 子集乘积

设〈G，$*$ 〉是一个群，A，B 是 G 的子集，集合

$$\{ab\mid a\in A,\ b\in B\}$$

叫做 A，B 的乘积，记为 $A*B$ 或 AB. 这样定义的子集的乘积，有如下两条基本性质：

1）子集的乘积满足结合律，即（AB）C = A（BC）.

事实上，$\forall x\in$（AB）C，$\exists a\in A$，$b\in B$，$c\in C$，使得 $x=(ab)c$ = $a(bc)$，故 $x\in A$（BC），于是，（AB）$C\subseteq A$（BC），同理 A（BC）$\subseteq$（AB）C，因此（AB）$C=A$（BC）.

2）在子集乘法下，任何子群皆为幂等元.

设 H 是 G 的子群，则 $e\in H$，故对任意 $h\in H$，$h=eh\in HH$，反之，$\forall\, a\in HH$，$\exists\, h_1$，$h_2\in H$，使得 $a=h_1h_2$，故知 $a\in H$，总之，有 $HH=H$.

我们已经知道，对群 G 中的子群 H，$a\in G$ 所在的左陪集 $aH=\{ah|h\in H\}$，根据子集乘积的定义，$aH=\{a\}H$. 同样，a 所在的右陪集 $Ha=H\{a\}$. 因此，以后我们可把左（右）陪集符号 aH（或 Ha）视为 $\{a\}H$（或 $H\{a\}$）的简写. 更一般地，对于群 G 的任意子集 S（不要求是子群），我们将把 $\{a\}$ 与 S 的乘积 $\{a\}S$ 和 $S\{a\}$ 分别简记为 aS 和 Sa.

例 10 设 S_3 为三次对称群，子集：

$$H_1=\{\sigma_0,\ \sigma_1\}=\{(1),(1,2)\}$$
$$H_2=\{\sigma_1,\ \sigma_2\}=\{(1,2),(1,3)\}$$
$$H_3=\{\sigma_0,\ \sigma_4,\ \sigma_5\}=\{(1),(1,2,3),(1,3,2)\}$$

则

$$\sigma_1H_3=\{\sigma_1\sigma_0,\ \sigma_1\sigma_4,\ \sigma_1\sigma_5\}=\{\sigma_1,\ \sigma_3,\ \sigma_2\}$$
$$=\{(1,2),(2,3),(1,3)\}$$
$$\sigma_1H_2=\{\sigma_1\sigma_1,\ \sigma_1\sigma_2\}=\{\sigma_0,\ \sigma_5\}=\{(1),(1,3,2)\}$$
$$H_1H_3=\{(1),(1,2,3),(1,3,2),(1,2),(2,3),(1,3)\}.$$

例 11 $(8)=\{8i|i\in\mathbf{Z}\}$ 是 $\langle\mathbf{Z},+\rangle$ 的循环子群，

令 $A=3+(8)$，$B=6+(8)$，则

$$A+B=\{3+8i+6+8j\,|\,i,\ j\in\mathbf{Z}\}=\{1+8k|k\in\mathbf{Z}\}=1+(8).$$

例 12 若 H 是 G 的正规子群，则对任意 $a\in G$，有 $a^{-1}Ha=H$.

证明 因为 H 是正规子群，故对任意 $a\in G$，有 $Ha=aH$，即 $H\{a\}=\{a\}H$，因而

$$a^{-1}Ha=\{a^{-1}\}(H\{a\})=\{a^{-1}\}(\{a\}H)=(\{a^{-1}\}\{a\})H=\{e\}H=H.$$

只要记住 aH，Ha 是 $\{a\}H$，$H\{a\}$ 的简写，以上证明过程可简化如下：

$$a^{-1}Ha=a^{-1}(Ha)=a^{-1}(aH)=(a^{-1}a)H=eH=H.$$

设 H 是群 G 的子群，考察 H 的两个陪集 aH，bH 作为 G 的两个子集的乘积 $aH\cdot bH$，一般来说，$aH\cdot bH$ 未必还是陪集，但若 H 是正规子群，则有：

定理 2 设 H 是群 G 的正规子群，则

$$aH\cdot bH=(ab)H\qquad\forall a,\ b\in G$$

证明 $\forall\, a$，$b\in G$，注意 $xH=\{x\}H$，$Hx=H\{x\}$ 及子集乘法的结合律，有

$$aH\cdot bH=a(Hb)H=a(bH)H$$
$$=(ab)(HH)=(ab)H.$$ ▌

由该定理可知，当 H 是 G 的正规子群时，G 中子集的乘法是 G 对 H 的商集 G/H 上的运算，且恰为我们前面定义的商群中的运算.

习 题 七

1．证明　两个正规子群的交是正规子群.

2．证明　群 G 的 2 阶正规子群必含在 G 的中心里（中心定义见第五章 § 3 例 5 ）.

3．设 G 为群，A，B 均为 G 的子集，证明：若 A，B 均为 G 的子群，且 B 为正规子群，则 AB 为 G 的子群.

4．设 A，B 是群 G 的正规子群，证明 AB 为正规子群.

5．设 H 是含于 G 的中心的子群，证明：H 是正规子群，又若 G/H 是循环群，则 G 必为 Abel 群.

6．写出 3 次对称群的所有非平凡正规子群.

*7．设 H 是群 G 的正规子群，证明模 H 同余关系 R_H 是 G 上的同余关系.

*§ 8　群同态基本定理

定义 1　设 φ 是群 G 到群 H 的同态，H 的单位元 e' 的所有原象构成的集合

$$N = \{x \mid x \in G，\ \varphi(x) = e\ \}$$

称为同态 φ 的核，记为 $\mathrm{Ker}\varphi$

定理 1　设 φ 是群 G 到群 H 的同态，则 $\mathrm{Ker}\varphi$ 为 G 的正规子群.

证明　用 e，e' 分别表示 G，H 的单位元，则由同态的性质知，$\varphi(e) = e'$，即知 $\mathrm{Ker}\varphi$ 非空.

$\forall\ a，b \in \mathrm{Ker}\varphi$，有 $\varphi(ab) = \varphi(a)\varphi(b) = e'e' = e'$，故 $ab \in \mathrm{Ker}\varphi$.

又，$\forall\ a \in \mathrm{Ker}\varphi$，$\varphi(a^{-1}) = \varphi(a)^{-1} = (e')^{-1} = e'$，故 $a^{-1} \in \mathrm{Ker}\varphi$.

因此，$\mathrm{Ker}\varphi$ 为子群. 现证其为正规子群. $\forall\ a \in G$，$n \in \mathrm{Ker}\varphi$，

$$\begin{aligned} f(a^{-1}na) &= f(a^{-1})f(n)f(a) \\ &= f(a^{-1})\,e'f(a) \\ &= f(a^{-1})f(a) \\ &= f(a^{-1}a) \\ &= e' \end{aligned}$$

即 $a^{-1}na \in \mathrm{Ker}\varphi$，从而知 $\mathrm{Ker}\varphi$ 为正规子群. ▌

定理 2　设 G 为群，N 为 G 的任一正规子群，

$$g_N：\ a \mapsto aN \qquad \forall a \in G$$

为 G 到 G/N 的自然同态，则 $\mathrm{Ker}\, g_N = N$.

证明　由于 $eN = N$ 为 G/N 的单位元，故

$$a \in \mathrm{Ker}\, g_N \ \Leftrightarrow\ g_N(a) = N \ \Leftrightarrow\ aN = N \ \Leftrightarrow\ a \in N$$

故知　　$\mathrm{Ker}\, g_N = N$. ▌

定理 3（群同态基本定理） 设 G 是一个群，则 G 的任一商群都是 G 的同态象，反之，若 G' 是 G 的同态象，f：$G\sim G'$，则

$$G' \cong G/\mathrm{Ker}\, f.$$

证明 我们已知道，对 G 的任一正规子群 H，可按如下方式构造 G 到 G/H 的自然同态.

$$g_H\text{：}\ a\mapsto aH \qquad \forall a\in G$$

且 g_H 是 G 到 G/H 的满同态，即 g_H：$G\sim G/H$. 这就证明了任一商群必是同态象.

反之，设 f：$G\sim G'$，为方便起见，记 $K=\mathrm{Ker}\, f$,

令 φ：$G/K\to G'$

$$\varphi\text{：}\ aK\mapsto f(a) \qquad \forall aK\in G/K$$

则由于 f 是满同态，易证 φ 为满射. 事实上，$\forall y\in G'$，$\exists\, a\in G$ 使 $f(a)=y$. 于是

$$\varphi(aK)=f(a)=y$$

因此 φ 为满射.

又设 aK，$bK\in G/K$ 且 $aK\neq bK$ 则 $a\not\equiv b \bmod K$. 即 $b^{-1}a\notin K$，或说 $f(b^{-1}a)\neq e'$，从而 $f(b)^{-1}f(a)\neq e'$，故 $f(a)\neq f(b)$，即 $\varphi(aK)\neq\varphi(bK)$， φ为单射.

综上，φ 为双射.

下证 φ 保持运算. $\forall\, aK$，$bK\in G/K$

$\varphi(aK\cdot bK)=\varphi(abK)=f(ab)=f(a)f(b)=\varphi(aK)\varphi(bK)$.

所以，φ：$G/K\cong G'$，从而 $G'\cong G/K$. ▌

例 1 设 G，G' 分别是 m，n 阶群，证明：如果 $G\sim G'$，则 $n\mid m$.

证明 不妨令 f：$G\sim G'$，由同态基本定理知

$$G'\cong G/\mathrm{Ker}\, f$$

故 $|G'|=|G/\mathrm{Ker}f|$，因而由拉格朗日定理，得

$$\begin{aligned}|G| &= [G:\mathrm{Ker}\, f]\cdot|\mathrm{Ker}\, f|=|G/\mathrm{Ker}f|\cdot|\mathrm{Ker}f|\\ &=|G'|\cdot|\mathrm{Ker}f|.\end{aligned}$$

即 $m=n|\mathrm{Ker}\, f|$， 所以 $n\mid m$.

例 2 设 f：$G\sim G'$，H' 是 G' 的正规子群，

$$H=f^{-1}(H')=\{x\mid x\in G,\ f(x)\in H'\},$$

则 $G/H\cong G'/H'$.

证明 设 φ 是 G' 到 G'/H' 的自然同态，由题设及自然同态的性质知，

$$f\text{：}\ G\sim G',\quad \varphi\text{：}\ G'\sim G'/H'.$$

故 $\varphi\circ f$：$G\sim G'/H'$. 由同态基本定理可知，$G'/H'\cong G/\mathrm{Ker}(\varphi\circ f)$. 故只需证明 $\mathrm{Ker}(\varphi\circ f)=H$ 即可.

由于 G'/H' 的单位元为 H'，故

$$\begin{aligned}a\in\mathrm{Ker}(\varphi\circ f) &\Leftrightarrow(\varphi\circ f)(a)=H' \Leftrightarrow\varphi(f(a))=H' \Leftrightarrow f(a)H'=H'\\ &\Leftrightarrow f(a)\in H' \Leftrightarrow a\in H.\end{aligned}$$

因而，$\mathrm{Ker}(\varphi\circ f)=H$. 于是，有 $G/H\cong G'/H'$.

习 题 八

1．利用群同态基本定理证明 n 阶循环群必同构于〈$\mathbf{Z}_n$，$+_n$〉.

2．设 $\varphi: G\sim G'$，φ 的核为 $N=\varphi^{-1}(e')$；$a, b\in G$. 证明 G 中任意两个元素在 G' 中有相同的象 当且仅当 a，b 在 N 的同一陪集中.

3．根据同构的观点，决定〈$\mathbf{Z}_{12}$，$+_{12}$〉，〈S_3，$\circ$〉的所有同态象.

第六章　环 与 域

§ 1　定义及基本性质

到目前为止，我们讨论的代数系统仅限于一个集合上有一个二元运算的最简单情形，从本节开始，我们介绍一个集合上带有两个二元运算的代数系统.

定义 1　设〈R，＋，• 〉是一个代数系统，其中，＋，• 均为二元运算，如果

（1）〈R，＋〉是一个 Abel 群.

（2）〈R，• 〉是一个半群.

（3）• 对 ＋ 满足分配律，即

$$a\cdot(b+c)=(a\cdot b)+(a\cdot c)$$

$$(b+c)\cdot a=(b\cdot a)+(a\cdot c)\qquad \forall a,b,c\in R$$

称〈R，＋，• 〉为一个环，其中的运算 ＋ 称作加法，• 称为乘法.

在不引起混乱的情况下，环〈R，＋，• 〉也简单地记成 R，$a\cdot b$ 记成 ab，且为方便起见，规定“• ”的优先级高于“＋”. 例如，$ab+c$ 的意思是（ab）＋c 而非 a（$b+c$）.

例 1　〈$\mathbf{Z}$，＋，• 〉是一个环，称作整数环. 同样，〈$2\mathbf{Z}$，＋，• 〉，〈$\mathbf{Q}$，＋，• 〉，〈$\mathbf{R}$，＋，• 〉也为环.

例 2　设 i 是虚数单位，即 $i^2=-1$，令

$$\mathbf{Z}(i)=\{a+bi\mid a,\ b\in\mathbf{Z}\}$$

则 $\mathbf{Z}(i)$ 关于数的加法＋、乘法• 构成环，通常称作高斯环.

例 3　n 阶整数矩阵所成集合，$(\mathbf{Z})_n$ 关于矩阵的加法与乘法作成一个环. 同样，n 阶有理数矩阵集合$(\mathbf{Q})_n$，n 阶实数矩阵集合 $(\mathbf{R})_n$，在矩阵加法与乘法运算下也均构成环.

例 4　x 的一切整（有理、实）系数多项式所成集合 $\mathbf{Z}[x]$（$\mathbf{Q}[x]$，$\mathbf{R}[x]$）在多项式加法与乘法运算下构成环.

例 5　〈$\mathbf{Z}_m$，$+_m$，$\times_m$〉构成环，称为模 m 剩余环.

例 6　设〈A，＋〉是一个 Abel 群，0 为其零元，规定乘法 • 如下：

$$a\cdot b=0\qquad \forall a,b\in A$$

则〈A，＋，• 〉是一个环.

由以上例子看出，环的类型可以是多种多样的. 因而，所讨论的对象也象群、半群一样是相当广泛的. 下面从定义出发给出环的一些初步性质.

设 R 是一个环[①]，在 Abel 群〈R，＋〉中，我们采用了加法记号，因此，〈R，＋〉的单位元用 0 表示，称为零元，$a\in R$ 在〈R，＋〉中的逆元用$-a$ 表示，称为 a 的负元，且记 $ma = a+a+\cdots+a$（共 m 个）.

（1） 加法结合律

$(a+b)+c=a+(b+c)$ $\quad\forall a,b,c\in R$

（2） 零元：存在 $0\in R$，使

$a+0=0+a=a$ $\quad\forall a\in R$

（3） 负元：$\forall a\in R$，有$-a\in R$，使

$a+(-a)=(-a)+a=0$

（4） 加法交换律：

$a+b=b+a$ $\quad\forall a,b\in R$

（5） 加法消去律

$a+b=a+c \Rightarrow b=c$ $\quad\forall a,b,c\in R$

（6） 指数律－1

$n(a+b)=na+nb$ $\quad\forall n\in\mathbf{Z},a,b\in R$

（7） 指数律－2

$(m+n)a=ma+na$ $\quad\forall m,n\in\mathbf{Z},a\in R$

（8） 指数律－3

$(mn)a=m(na)$ $\quad\forall m,n\in\mathbf{Z},a\in R$

以上性质仅涉及加法运算，但环 R 中还有另一个二元运算——乘法，这两个运算被分配律联系起来，因此，需要考虑由于这种联系而产生出的性质.

（9） $0a=a0=0$ $\quad\forall a\in R$

（10） $a(-b)=b(-a)=-(ab)$ $\quad\forall a,b\in R$

（11） $(-a)(-b)=ab$ $\quad\forall a,b\in R$

证明 $\forall a\in R$ 由于 $0+0=0$ 所以 $a(0+0)=a0$，由分配律得

$$a0+a0=a0+0$$

现利用消去律，即有 $a0=0$，同理 $0a=0$，（9）式得证.

$\forall a,b\in R$ $\quad a(-b)+ab=a((-b)+b)=a0=0$.

故 $\quad a(-b)=-(ab)$.

同理 $\quad(-a)b=-(ab)$.

又 $\quad(-a)(-b)=-(a(-b))=-(-(ab))=ab$.

即（10），（11）式得证. ▌

在一个环 R 中，$a+(-b)$ 可简记为 $a-b$，并把符号“－”称作“减法”. 利用以上运算律可以证明，环 R 中乘法对减法的分配律成立.

（12） $a(b-c)=ab-ac$.

[①]按照习惯，今后经常使用白、斜体 R 作为环的记号，要注意与实数集符号——粗黑体正体 $\mathbf{R}$——区别.

$(b-c)a = ba - ca.$

证明留给读者.

利用环 R 中的分配律，还可证明环 R 中广义分配律成立.

（13） $a(b_1+b_2+\cdots+b_n) = ab_1+ab_2+\cdots+ab_n$

$(b_1+b_2+\cdots+b_n)a = b_1a+b_2a+\cdots+b_na \quad \forall a, b_1, b_2, \cdots, b_n \in R$

（14） $(\sum_{i=1}^{n}a_i)(\sum_{j=1}^{m}b_j)=\sum_{i=1}^{n}\sum_{j=1}^{m}(a_ib_j) \quad \forall a_i, b_j \in R \quad i=1,2,\cdots,n \quad j=1,2,\cdots,m$

（15） $(na)b = a(nb) = n(ab) \quad a, b \in R, n \in \mathbf{Z}.$

性质（13）可用归纳法证明，性质（14）、（15）均易从性质（13）推出.

在环〈R，+，·〉中，若〈R，·〉为幺半群，则称〈R，·〉的单位元为环 R 的单位元，通常用 1 表示，这时称 R 为有单位元的环或有 1 的环.

设 R 为有 1 的环，$a \in R$，如果 a 在〈R，·〉中的逆元存在，则称 a 为 R 中的可逆元.并把 a 在半群〈R，·〉中的逆元，就称为 a 在环 R 中的逆元，用 a^{-1} 表示.

显然，有 1 的环 R 中所有可逆元在乘法运算下构成一个群，该群记为 R^*，并称为环 R 的乘法群.

环 R 可以只含一个元素，这时 $R = \{0\}$，0 既是 R 的零元，也是 R 的单位元. 这种环通常称为零环. 但当有单位元的环 R 中含有多于一个元素时，有如下结论.

定理 1　设 R 为有单位元的环，且不只含一个元素，则 $1 \neq 0$.

证明　若 $1 = 0$，则 $\forall a \in R$

$a = a \cdot 1 = a \cdot 0 = 0.$

故 R 只含一个元素 0，矛盾. ▌

零环对我们来说意义不大，以后除非特别说明，当提到有单位元的环时，总指非零环. 因此 $1 \neq 0$ 总成立.

当环 R 的乘法运算满足交换律，即〈R，·〉为（可）交换半群时，称 R 为（可）交换环.

读者自行考察例 1 － 5 中的诸环是否是有 1 的环. 是否是交换环.

习 题 一

1．在环 R 中 $(a+b)^3 = ?$

2．证明 $\mathbf{Z}(\sqrt{5}) = \{a+b\sqrt{5} \mid a, b \in \mathbf{Z}\}$ 关于通常数的加法与乘法作成一个环.

3．设 $\mathbf{R}$ 是实数集，+、·分别是通常数的加法与乘法，在 $\mathbf{R}$ 上定义运算 $*$ 如下：

$a * b = |a| \cdot b$

问〈$\mathbf{R}$，+，$*$〉是否为环.

4．证明多于一个元素的有限实数集关于数的加法与乘法不构成环.

5．设 R 为有 1 的环，$a\in R$，证明：若 a 可逆则 $-a$ 必可逆，且

$$(-a)^{-1}=-a^{-1}.$$

6．证明性质（1 2）、（1 3）.

7．设 R 为有单位元的环，在 R 上定义新运算 $\oplus$、$\otimes$ 如下：

$$a\oplus b=a+b-1$$

$$a\otimes b=a+b-ab$$

证明〈R, $\oplus$, $\otimes$〉也构成有单位元的环.

§2 整环 除环 域

在剩余环〈$\mathbf{Z}_6$，$+_6$，$\times_6$〉中我们看到，[2] ≠ [0]，[3] ≠ [0]，但 [2] $\times_6$ [3] = [0]，其中 [0] 为 $\mathbf{Z}_6$ 的零元．这种现象使我们一般地引入如下定义：

定义 1 设〈R，+，·〉为一个环，$a\in R$ 且 $a\neq 0$，若 R 中存在非零元素 b，使 $ab=0$（$ba=0$），则称 a 为 R 的左（右）零因子．R 的左、右零因子统称为零因子.

由以上定义可以看出，零因子总是成对出现的. 当 $a\neq 0, b\neq 0$ 但 $ab=0$ 时，a, b 是一对零因子.

例 1 对于剩余环〈$\mathbf{Z}_n$，$+_n$，$\times_n$〉，若 n 不是素数，则 $\mathbf{Z}_n$ 中必存在零因子.

首先注意，$\mathbf{Z}_n$ 中的零元为 [0]. 因为 n 不是素数，故存在整数 n_1，n_2，使

$$n=n_1n_2 \qquad 1<n_1\leqslant n_2<n$$

因此 $[n_1]\neq[0]$，$[n_2]\neq[0]$，但 $[n_1]\times_n[n_2]=[0]$．即 $[n_1]$，$[n_2]$ 是 $\mathbf{Z}_n$ 的一对零因子.

例 2 用 $(\mathbf{R})_2$ 表示 2 阶实数矩阵集合，+，· 表示矩阵的加法与乘法，则

〈 $(\mathbf{R})_2$，+，· 〉是一个环，其零元为 $\begin{pmatrix}0&0\\0&0\end{pmatrix}$， 由于

$$\begin{pmatrix}1&0\\0&0\end{pmatrix}\begin{pmatrix}0&0\\0&1\end{pmatrix}=\begin{pmatrix}0&0\\0&0\end{pmatrix},$$

故 $\begin{pmatrix}1&0\\0&0\end{pmatrix}$ 与 $\begin{pmatrix}0&0\\0&1\end{pmatrix}$ 为一对零因子.

定理 1 若 R 为无零因子的环，则 R 中乘法消去律成立．即

$$ab = ac \Rightarrow b = c$$
$$ba = ca \Rightarrow b = c \qquad \forall a,b,c \in R, a \neq 0$$

反之亦然.

证明 设 R 中无零因子，$\forall a,b,c \in R, a \neq 0$，如果 $ab=ac$，则

$ab-ac=0$，　$a(b-c)=0$.

由于 $a \neq 0$，R 中无零因子，故 $b-c=0$，即 $b=c$.

同理可得　　$ba=ac \Rightarrow b=c$　　$\forall a,b,c \in R, a \neq 0$

反之，设环 R 中乘法消去律成立，若 R 中有零因子 a，b，使得 $ab=0=a0$，由消去律得 $b=0$，矛盾. 故 R 中必无零因子. ▌

定义 2　有单位元、无零因子的交换环称为整环.

例 3　整数环〈$\mathbf{Z}$，+，·〉是一个整环，高斯环〈$\mathbf{Z}[i]$，+，·〉是一个整环.

例 4　若 p 是一个素数，则〈$\mathbf{Z}_p$，$+_p$，$\times_p$〉是一个整环.

首先易见，〈$\mathbf{Z}_p$，$+_p$，$\times_p$〉是一个有单位元的交换环，其单位元为 [1]. 下证 $\mathbf{Z}_p$ 中无零因子.

若有零因子 $[i]$，$[j] \in \mathbf{Z}_p$，使得 $[i]$，$[j] \neq [0]$，$[i] \times_p [j] = [0]$，则 $[ij] = [0]$，因而 $p \mid ij$. 由于 p 是素数，故 $p \mid i$ 或 $p \mid j$. 即 $[i]=[0]$ 或 $[j]=[0]$ 矛盾. 因此，$\mathbf{Z}_p$ 中无零因子，从而 $\mathbf{Z}_p$ 是整环.

由例 1 及例 4 可见，〈$\mathbf{Z}_n$，$+_n$，$\times_n$〉是整环 $\Leftrightarrow$ n 为素数.

定义 3　设 R 是一个有 1 的环，$\hat{R} = R - \{0\} \neq \varnothing$，如果〈$\hat{R}$，·〉是一个群，则称 R 为除环，可交换的除环称为域.

由定义 3 易见

（1）有单位元的环 R 是除环 $\Leftrightarrow R$ 中非零元均可逆 $\Leftrightarrow R$ 的乘法群 $R^* = R - \{0\}$.

（2）有单位元的环 R 是域 $\Leftrightarrow R$ 是交换环且 R 中非零元素均可逆.

读者自证.

例 5　〈$\mathbf{Q}$，+，·〉，〈$\mathbf{R}$，+，·〉均是域，分别称为有理数域和实数域.

例 6　令 $\mathbf{Q}[\sqrt{2}] = \{a + b\sqrt{2} \mid a,b \in \mathbf{Q}\}$；+，·为通常数的加法和乘法，则

〈$\mathbf{Q}[\sqrt{2}]$ +，· 〉是域.

由于一个环 R 是否构成除环，取决于〈$\hat{R}$，·〉是否构成一个群. 因此，将半群构成群的定理用到环，即可相应得出一些环构成除环的定理. 比如，我们已经知道，有限半群如果消去律成立，则必构成群，对应地，有

定理 2　设 R 是一个无零因子的有限环，且 $|R| \geqslant 2$，则 R 必为除环.

证明 根据除环的定义，我们需要证明〈$\hat{R}$，•〉为群. 由于 | R | ≥ 2，故 $\hat{R}$ 非空，又，R 中不含零因子，故 $\hat{R}$ 对 • 封闭，从而〈$\hat{R}$，•〉必构成半群，且由定理 1 知，在该半群中消去律成立，从而〈$\hat{R}$，•〉是一个满足消去律的有限半群，故必为群. 从而 R 是除环. ▌

推论 有限整环必为域.

由于 $\mathbf{Z}_p$ 是一个有限整环，利用上推论立即可知 $\mathbf{Z}_p$ 为域（这个域称为素域）.

推论 若 p 为素数，则〈$\mathbf{Z}_p$，$+_p$，$\times_p$〉为域.

设 F 是一个域，$\forall a,b\in F$，若 $b\neq 0$，则与通常数的情形类似，我们也将 b^{-1} 写成 $\frac{1}{b}$，$b^{-1}a$（或 ab^{-1}）写成 $\frac{a}{b}$，在这种记号下，有以下性质成立.

（1） 设 $b\neq 0$，$d\neq 0$，则 $ad = bc \Leftrightarrow \frac{a}{b}=\frac{c}{d}$.

（2） 设 $b\neq 0$，$d\neq 0$，则 $\frac{a}{b}\pm\frac{c}{d}=\frac{ad\pm bc}{bd}$.

（3） 设 $b\neq 0$，$d\neq 0$，则 $\frac{a}{b}\cdot\frac{c}{d}=\frac{ac}{bd}$.

（4） 设 $b\neq 0$，$c\neq 0$，$d\neq 0$，则 $\frac{a}{b}/\frac{c}{d}=\frac{ad}{bc}$.

证明

（1） 设 $ad=bc$，两边同乘 $b^{-1}d^{-1}$ 则有 $b^{-1}a= cd^{-1}$，即 $\frac{a}{b}=\frac{c}{d}$.

反之，设 $\frac{a}{b}=\frac{c}{d}$，即 $b^{-1}a= cd^{-1}$，两边同乘 bd， 则有 $ad=bc$.

（2）
$$\begin{aligned}\frac{a}{b}\pm\frac{c}{d} &= b^{-1}a \pm d^{-1}c\\ &=(b^{-1}a)(dd^{-1}) \pm (d^{-1}c)(bb^{-1})\\ &= ad(bd)^{-1} \pm bc(bd)^{-1}\\ &=(ad\pm bc)(bd)^{-1}\\ &=\frac{ad\pm bc}{bd}.\end{aligned}$$

式（3）、（4）类似可证. ▌

习 题 二

1．设 R 为有单位元的环，证明 R 中可逆元一定不是零因子．

2．设 R 是一个环，证明：若 R 中有左零因子，则必有右零因子，反之亦然．

3．证明例 6．

4．设 R 为有 1 的有限环，证明 R 中的非零元或为可逆元，或为零因子．

5．设 S 表示环 R 中一切不是零因子的元素构成的集合，证明〈S，• 〉是〈R，• 〉的子半群．

*§ 3　理想与商环

研究任何代数系统，子代数都起着重要作用．本节我们引进子环的概念，并讨论一类非常重要的子环——理想．

定义 1　设〈R，+，• 〉是一个环，　$S\subseteq R$，如果 S 关于 R 的+，• 作成一个环，则称 S 为 R 的子环，R 为 S 的扩环．

显然，S 是 R 的子环，当且仅当

（1）〈S，+〉是〈R，+〉的子群．

（2）〈S，• 〉是〈R，• 〉的子半群．

据此易证

定理 1　$S\subseteq R$ 是环 R 的子环当且仅当下面三条成立

（1）　$S\neq\varnothing$

（2）　$\forall a,b\in S$，$a-b\in S$

（3）　$\forall a,b\in S$，$ab\in S$

对任意环 R，R 本身及｛0｝必为 R 的子环，称为 R 的平凡子环．

例 1　偶数环 $2\mathbf{Z}$ 是整数环 $\mathbf{Z}$ 的子环．

例 2　在整数环 $\mathbf{Z}$、有理数域 $\mathbf{Q}$ 和实数域 $\mathbf{R}$ 中，前者为后者的子环．

例 3　实数域 $\mathbf{R}$ 是实数域上的多项式环 $\mathbf{R}[x]$ 的子环．

要注意，子环未必能保持其扩环的所有性质．例如，当环 R 有单位元时，其子环 S 未必有单位元，这点在例 1 中已经看到，再看下面的例子．

例 4　剩余环〈$\mathbf{Z}_6$，$+_6$，$\times_6$〉是有 1 的交换环，单位元为［1］．令

$$S_1=\{[0],[3]\}\qquad S_2=\{[0],[2],[4]\}$$

则 S_1，S_2 都是 $\mathbf{Z}_6$ 的子环．且易知 S_1，S_2 均为有单位元的环，S_1，S_2 的单位元分别为［3］，［4］．这样，环 $\mathbf{Z}_6$ 与其子环 S_1，S_2 均为有单位元的交换环，但其单位元互不相同．

在群的理论中，正规子群起着重要作用．同样，在环的理论中我们也引进一种特殊

子环——理想，它在环论中的作用类似于正规子群在群论中的作用.

定义 2　设 R 是一个环，$S \subseteq R$，如果

（1）　$S \neq \varnothing$

（2）　$\forall a,b \in S \qquad a-b \in S$

（3）　$\forall x \in R,\ a \in S,\ \ ax,\ xa \in S$

则称 S 为 R 的理想子环，简称理想.

由该定义及子环的充要条件（定理 1）知，理想一定是子环. 对任意环 R，其平凡子环 R 和 {0} 一定是理想，称为 R 的平凡理想，除此之外，若还存在其它理想，则称为 R 的真理想.

例 5　在整数环 $\mathbf{Z}$ 中取非负整数 m，令

$$(m) = \{im \mid i \in \mathbf{Z}\}$$

则 (m) 是 $\mathbf{Z}$ 的理想. 当 $m = 0$，1 时，(m) 分别是平凡理想 {0}，$\mathbf{Z}$，当 $m > 1$ 时，(m) 是真理想.

例 6　设 F 是一个域，形如　$a_n x^n + a_{n-1}x^{n-1} + \cdots\cdots + a_0$（其中，$a_n$，$a_{n-1}$，…，$a_0 \in F$，$n \in \mathbf{N}$）的式子，称为 F 上 x 的多项式. a_0，a_1，…，a_n 称为多项式的系数，在一个多项式中，可任意添加系数为 0 的项. F 上 x 的多项式可用 $f(x)$，$g(x)$ 等符号表示，并可将多项式

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots\cdots + a_0$$

简记为

$$f(x) = \sum_{i=0}^{n} a_i x^i$$

设 $f(x) = \sum_{i=0}^{n} a_i x^i$ 是一个多项式，若 $a_n \neq 0$，则称 $a_n x^n$ 为 $f(x)$ 的首项，a_n 为首项系数，n 为 $f(x)$ 的次数，用 $\deg f(x)$ 表示，若 $f(x) = 0$，则约定 $\deg f(x) = -\infty$.

两个多项式 $f(x) = \sum_{i=0}^{n} a_i x^i$，$g(x) = \sum_{i=0}^{n} b_i x^i$ 相等，是指 $a_i = b_i$（$i = 0, 1, \cdots, n$）

与实数域上的多项式一样，可以定义多项式的加法与乘法：

$$\left(\sum_{i=0}^{n} a_i x^i\right) + \left(\sum_{i=0}^{n} b_i x^i\right) = \sum_{i=0}^{n} (a_i + b_i) x^i$$

$$\left(\sum_{i=0}^{n} a_i x^i\right)\left(\sum_{i=0}^{n} b_i x^i\right) = \sum_{i=0}^{n}\sum_{j=0}^{n} a_i b_j x^{i+j}$$

容易看到

$$\deg(f(x)+g(x)) \leqslant \max(\deg f(x), \deg g(x))$$

$$\deg(f(x)g(x)) = \deg f(x)+\deg g(x)$$

令 $F[x]$ 为 F 上所有 x 的多项式构成的集合，则 $\langle F[x], +, \cdot \rangle$ 是一个整环，称为域 F 上的多项式环，其单位元为 F 的单位元 1．

令 $F_0[x]$ 为 $F[x]$ 中所有常数项为 0 的多项式构成的集合，则 $F_0[x]$ 是 $F[x]$ 的理想．

例 7 设 R 是一个有 1 的交换环，令 $(a)=aR=\{ar \mid r \in R\}$，则 (a) 是 R 的理想．称为 a 生成的主理想[①].

上面例 5 中的 (m)，正是由 m 生成的主理想，$(m)=m\mathbf{Z}$，而例 6 中的 $F_0[x]$ 是由 x 生成的主理想，$F_0[x]=xF[x]$.

定义 3 设 R 是一个整环，如果 R 的每个理想都是主理想，则称 R 为主理想整环．

例 8 $\langle \mathbf{Z}, +, \cdot \rangle$ 是主理想整环．

首先，$\langle \mathbf{Z}, +, \cdot \rangle$ 是整环，设 A 是 $\mathbf{Z}$ 的任一理想，若 $A=\{0\}$，则 A 是主理想，否则，令 m 是 A 中的最小正整数，即

$$m=\min\{x \mid x \in A, x>0\}$$

$\forall i \in A$，用 m 对 i 做带余数除法得，

$$i=km+r \qquad k \in \mathbf{Z}, \quad 0 \leqslant r < m.$$

则 $r=i-km \in A$. 由 m 在 A 中的最小性，$r=0$，即 $i=km \in (m)$．故 $A \subseteq (m)$．又显然 $(m) \subseteq A$，所以有 $A=(m)$．A 是主理想．

例 9 $\langle F[x], +, \cdot \rangle$ 是主理想整环．

象实数域上的多项式一样，在 $F[x]$ 中有带余式除法，即如果 $f(x), g(x) \in F[x]$，$g(x) \neq 0$，则存在 $q(x), r(x) \in F[x]$ 使

$$f(x)=q(x)g(x)+r(x) \quad \deg(r(x)) < \deg(g(x))$$

与例 8 类似可以证明，对 $F[x]$ 的任一理想 A，若令 $f(x)$ 是 A 中次数最小的多项式，则 $A=(f(x))$．一般地，我们引入下述定义．

我们说过，理想在环论中所起的作用，类似于正规子群在群论中所起的作用．下面就来讨论这种类似性．为了更加明确起见，我们首先来熟悉一下将采用的记号：设 $\langle R, +, \cdot \rangle$ 是一个环，N 是 R 的一个理想，则 $\langle N, + \rangle$ 是 $\langle R, + \rangle$ 的子群，由于 $\langle R, + \rangle$ 是 Abel 群，故 $\langle N, + \rangle$ 必是正规子群．因为在 $\langle R, + \rangle$ 中使用的是加法记号，故 $\langle R, + \rangle$ 中的模 N 同余关系的定义应为

$$a \equiv b \bmod N \quad \Leftrightarrow \quad a-b \in N \qquad \forall a, b \in R$$

这个关系将被称作环 R 上的模 N 同余关系，而 a 所在的陪集则记为 $a+N$.

即

$$a+N=\{a+n \mid n \in N\}$$

---

① 由 a 生成的主理想与由 a 生成的循环子群使用了同样的符号：(a)，请注意根据上下文区别.

以后我们将称 $a+N$ 为 a 所在的模 N 剩余类．为符号简捷，常用 $[a]_N$ 或 $[a]$ 表示 $a+N$．$\langle R, +\rangle$ 对 N 的商群 $\langle R/N, +\rangle$ 是 $\langle R, +\rangle$ 对 N 的商集：

$$R/N=\{a+N \mid a\in R\}=\{[a] \mid a\in R\}$$

在以下加法运算下构成的群:

$$[a]+[b]=[a+b] \qquad \forall a, b\in R$$

显然，$\langle R/N, +\rangle$ 为一个 Abel 群，为使 R/N 构成环，我们现在需要在 R/N 上引入一个乘法运算．自然，该乘法运算应通过 R 中的乘法运算来定义，即

$$[a]\cdot[b]=[ab] \qquad \forall a, b\in R$$

与商群的情况类似，这里也是用代表元定义剩余类的运算，故须验证运算结果与代表元的选取无关，而由剩余类 $[a]$，$[b]$ 唯一确定．设 $a'\in[a]$，$b'\in[b]$，则 $[a]$，$[b]$ 可分别选 a'，b' 为代表元：$[a]=[a']$，$[b]=[b']$，下证 $[ab]=[a'b']$．

由 $a'\in[a]$，$b'\in[b]$ 知

$$a' \equiv a \mod N \qquad b' \equiv b \mod N,$$

即 $a'-a\in N$，$b'-b\in N$，令 $a'-a=n_1$，$b'-b=n_2$，则 $n_1, n_2\in N$ 且 $a'=a+n_1$，$b'=b+n_2$，于是

$$a'b'=(a+n_1)(b+n_2)=ab+n_1b+an_2+n_1n_2$$

因为 N 为理想，故 $n_1b+an_2+n_1n_2\in N$，所以 $a'b'-ab\in N$．即 $a'b'\equiv ab \mod N$，亦即 $[a'b']=[ab]$，从而知运算结果与代表元选取无关，运算的定义是合理的．

容易验证，以上定义的运算满足结合律，为证 $\langle R/N, +, \cdot\rangle$ 是环，需证 $\cdot$ 对 $+$ 满足分配律．

$\forall [a], [b], [c]\in R/N$

$$\begin{aligned}[a]\cdot([b]+[c]) &= [a]\cdot[b+c]\\ &= [a(b+c)]=[ab+ac]\\ &= [ab]+[ac]=[a][b]+[a][c]\end{aligned}$$

同理 $([b]+[c])[a]=[b][a]+[c][a]$，从而知 $\langle R/N, +, \cdot\rangle$ 是一个环，称之为 R 对 N 的商环或 R 中模 N 剩余类环，显然，R/N 的零元为 $0+N=N$.

例 10 取整数环 $\langle \mathbf{Z}, +, \cdot\rangle$ 的主理想 $(m)=m\mathbf{Z}$（$m>0$）．则 $\mathbf{Z}$ 对 (m) 的商环为 $\langle \mathbf{Z}_m, +_m, \times_m\rangle$.

例 11 设 $\mathbf{R}[x]$ 为实数域 $\mathbf{R}$ 上的多项式环，$N=(x)=\{x\,r(x) \mid r(x)\in\mathbf{R}[x]\}$ 是 $\mathbf{R}[x]$ 中由 x 生成的主理想．则 $\forall f(x)\in\mathbf{R}[x]$，若 $f(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots\cdots+a_0$，则 $f(x)\equiv a_0 \mod N$. 因此 $[f(x)]_N=[a_0]_N$ 故

$$\begin{aligned}\mathbf{R}[x]/(x) &= \mathbf{R}[x]/N=\{[f(x)]_N \mid f(x)\in\mathbf{R}[x]\}\\ &= \{[a]_N \mid a\in\mathbf{R}\}.\end{aligned}$$

且其中的加法与乘法分别为

$$[a]+[b]=[a+b]$$

$$[a]\cdot[b]=[ab]$$

从中可以看出，$\mathbf{R}[x]/(x)$ 上的加法与乘法运算实际上是按实数加法、乘法来定义的，

故其性质与〈**R**，＋，• 〉没有什么区别.

习 题 三

1．令 $\mathbf{Q}_p=\{\frac{a}{b}\mid a, b\in\mathbf{Z}, p\nmid b\}$，证明 $\mathbf{Q}_p$ 为有理数域 **Q** 的子环．这里，p 是一个素数.

2．找出 $\mathbf{Z}_6$ 的所有理想.

3．设 N_1 ，N_2 是环 R 的两个理想．证明 $N_1\cap N_2$ 必为 R 的理想.

4．设 N_1 ，N_2 是环 R 的两个理想，证明 $N_1N_2\subseteq N_1\cap N_2$.

5．设 p，q 是两个素数，$(p)\cap(q)$ 是 **Z** 的一个怎样的理想？$(p)\cdot(q)$ 是 **Z** 的一个怎样的理想？

6．一个没有零因子的环 R，其剩余类环是否一定没有零因子？

7．设 F 是一个域，找出 F 的所有理想.

8．完成例 9，即证明域 F 上的多项式环〈$F[x]$，＋，• 〉是一个主理想环.

9．设 R 是一个环，N 是 R 的理想，令 $\oplus$、$\otimes$ 为 R 中子集的加法及乘法，定义如下：

$$A\oplus B=\{a+b\mid a\in A, b\in B\}$$

$$A\otimes B=\{ab\mid a\in A, b\in B\}$$

商环 R/N 中的加法与乘法仍用＋、• 表示，证明：

$\forall\ [a], [b]\in R/N$

$$[a]+[b]=[a]\oplus[b].$$

但未必有

$$[A]\otimes[b]=[A]\cdot[b]$$

10．证明 实数域上的二元多项式环 $R[x, y]$ 不是主理想环.

§4 域的特征 素域

定义 1 设 F 是一个域，$S\subseteq F$，若 S 在 F 的加法与乘法运算下也构成域，则称 S 为 F 的子域，F 为 S 的扩域（或扩张）.

显然，若 S 是 F 的子域，则〈S，＋〉是〈F，＋〉的子群，故 $0\in S$，〈S^*，• 〉是〈F^*，•〉的子群（其中，$S^*=S-\{0\}$，$F^*=F-\{0\}$），故 $1\in S$.

因此，F 的任意子域必含 F 的 0 ， 1 .

为了给出域论中的一个重要概念——域的特征，我们首先证明如下定理.

定理 1 设〈F，＋，• 〉是一个域，则：

（1） 在加法群〈F，＋〉中，每个非零元都具有同样的周期（阶）.

（2） 如果〈F，＋〉中非零元素的周期为有限数 p，则 p 必为素数.

证明

（1）$\forall a\in F$，设 $a\neq 0$，用 e 表示 F 的单位元，则：

$$na = a+a+\cdots+a = ea+ea+\cdots+ea = (e+e+\cdots+e)a$$
$$= (ne)a$$

由于 $a\neq 0$，且域中无零因子，故

$$na=0 \Leftrightarrow (ne)a=0 \Leftrightarrow ne=0$$

由此可见，a 的加法周期与单位元 e 相同，从而知 F 中任何非零元素的加法周期均相同，以后经常用单位元的周期代表这个共同值.

（2）设 F 中非零元素的周期为有限数 p，则 $p>1$．如果 p 不是素数，则必有 p_1，$p_2\in\mathbf{N}$ 使 $p=p_1p_2$，$1<p_1\leqslant p_2<p$．于是

$$pe=(p_1p_2)e = p_1(p_2e)=(p_1e)(p_2e)$$

故由 $pe=0$ 知 $(p_1e)(p_2e)=0$，由于域 F 中无零因子，因此 $p_1e=0$ 或 $p_2e=0$，与 e 的周期为 p 矛盾．故 p 必为素数． ▌

定义 2　设〈F，+，·〉是一个域，若〈F，+〉中非零元的周期为有限数 p，则称域 F 的特征为 p．若〈F，+〉中非零元的周期为∞，则称域 F 的特征为 0．

由定理 1 可知，域 F 的特征或者为素数或者为 0．

例 1　设 p 是一个素数，则模 p 剩余类环 $\mathbf{Z}_p$ 是一个域，$\mathbf{Z}_p$ 的特征为 p.

证明　容易看出 $\mathbf{Z}_p$ 中单位元［1］的加法周期为 p，故知 $\mathbf{Z}_p$ 的特征为 p.

例 2　有理数域 $\mathbf{Q}$ 的特征为 0．

证明　因为对任意正整数 n，$n1=n\neq 0$．故 1 的加法周期为∞，故 $\mathbf{Q}$ 的特征为 0．

定理 2　设 S 是 F 的子域，则 S 与 F 具有相同的特征.

只需注意 S 与 F 的运算是相同的，且具有相同的 0，1，则定理易明.

定理 3　n 元有限域的特征数必为素数 p，且 $p\mid n$.

证明　若 F 是 n 元有限域，则〈F，+〉是 n 阶群，故 $1\in F$ 在〈F，+〉中的周期必为有限数 p，且 $p\mid n$．由定义，F 的特征为 p. 且由定理 1 知 p 为素数． ▌

特征不同的域，结构不同. 为了以特征为线索研究域的结构，现引入环（当然包括域）同态的概念.

定义 3　设〈R，+，·〉，〈S，⊕，⊗〉是两个环，$f: R\to S$，如果 f 保持运算，即满足：

$$f(a+b)=f(a)\oplus f(b)$$
$$f(a\cdot b)=f(a)\otimes f(b) \qquad \forall a,b\in R$$

则称 f 是环 R 到环 S 的同态.

与前面完全类似，可以定义单同态、满同态、同构等，还可证明满同态保持环、保持域等类似结论，不再一一赘述，但特别指出，若 $R\cong S$，则当 R 是域时 S 必是域.

定理 4　若域 F 的特征为素数 p，则 F 中必存在与 $\mathbf{Z}_p$ 同构的子域 $\mathbf{Z}'_p$.

证明　设 e 是 F 的单位元，令

$$\mathbf{Z}'_p = \{ie \mid i\in\mathbf{Z}\}$$

因为 e 的加法周期为 p，故

$$\mathbf{Z}'_p = \{0, e, 2e, \cdots, (p-1)e\}$$

作 $\mathbf{Z}_p$ 到 $\mathbf{Z}'_p$ 的映射 φ:

$$\varphi: [i] \mapsto ie \qquad \forall [i] \in \mathbf{Z}_p$$

显然 φ 是 $\mathbf{Z}_p$ 到 $\mathbf{Z}'_p$ 的双射，下证 φ 保持运算. $\forall [i], [j] \in \mathbf{Z}_p$ 有

$$\varphi([i] +_p [j]) = \varphi([i+j]) = (i+j)e$$
$$= (ie) + (je) = \varphi([i]) + \varphi([j])$$
$$\varphi([i] \times_p [j]) = \varphi([ij]) = (ij)e$$
$$= (ie) \cdot (je) = \varphi([i]) \cdot \varphi([j])$$

由此便知 φ 是 $\mathbf{Z}_p$ 到 $\mathbf{Z}'_p$ 的同构，即 $\varphi: \mathbf{Z}_p \cong \mathbf{Z}'_p$.

由于 $\mathbf{Z}_p$ 是域，与之同构的 $\mathbf{Z}'_p$ 必为域，从而是 F 的子域. 这样就证明了 F 中存在与 $\mathbf{Z}_p$ 同构的子域. ▌

设 F 是一个特征为素数 p 的域，由于 F 的任何子域 S，必包含单位元 e，从而包含 e 的所有整数倍 ie，故 $\mathbf{Z}'_p \subseteq S$. 因此 $\mathbf{Z}'_p$ 是 F 的最小子域. 所以，从同构观点来看，特征为素数 p 的域 F 含有 $\mathbf{Z}_p$ 为其最小子域.

若域 F 的特征为 0，则 $\mathbf{Z}'_0 = \{ie \mid i \in \mathbf{Z}\}$ 与整数环 $\mathbf{Z}$ 同构，不能构成 F 的子域，但我们有下述定理.

定理 5 若域 F 的特征为 0，则 F 中含有与有理数域 $\mathbf{Q}$ 同构的子域.

证明 用 e 表示 F 的单位元，令

$\mathbf{Q}' = \left\{\dfrac{me}{ne} \mid m, n \in \mathbf{Z}, n \neq 0\right\}$，作有理数域 $\mathbf{Q}$ 到 $\mathbf{Q}'$ 的映射 φ:

$$\varphi: \frac{m}{n} \mapsto \frac{me}{ne} \qquad \forall m, n \in \mathbf{Z}, n \neq 0.$$

首先需要说明以上定义是合理的，即有理数 q 的象由 q 唯一确定，而与其表示方法无关.

设 $\dfrac{m}{n} = \dfrac{m'}{n'}$，则 $mn' = nm'$，故 $(mn')e = (nm')e$. 由于

$$(mn')e = m(n'e) = (me)(n'e),$$
$$(nm')e = n(m'e) = (ne)(m'e),$$

故 $(me)(n'e) = (ne)(m'e)$. 两边同乘 $(n'e)^{-1}(ne)^{-1}$，有 $\dfrac{me}{ne} = \dfrac{m'e}{n'e}$ 或说 $\varphi\left(\dfrac{m}{n}\right) = \varphi\left(\dfrac{m'}{n'}\right)$，即同一个有理数的不同表达形式在 φ 映射下得到的象是相同的，因此 φ 确为一个合理的 $\mathbf{Q}$ 到 $\mathbf{Q}'$ 的映射.

不难看出 φ 是满射，且容易验证 φ 是单射、保持运算，因而 $\varphi: \mathbf{Q} \cong \mathbf{Q}'$.
由于 $\mathbf{Q}$ 是域，知 $\mathbf{Q}'$ 是域，从而是 F 的子域，这样就证明了 F 中存在与 $\mathbf{Q}$ 同构的子域. ▌

设 F 是一特征为 0 的域，则对 F 的任何子域 S，S 必包含 F 的单位元 e，从而包含 e 的所有整数倍 me，由域的定义，$(me)^{-1}$ 及形如$(me)(ne)^{-1}$的元素均应包含在 S 中，故 $\mathbf{Q}'\subseteq S$. 因此 $\mathbf{Q}'$ 是 F 的最小子域. 所以，从同构观点来看，特征为 0 的域 F 包含有理数域 $\mathbf{Q}$ 为其最小子域.

如果将 F 中的单位元记为 1，则 F 中的元素 me，$\dfrac{me}{ne}$ 可记作 m，$\dfrac{m}{n}$. 特别地，对于素域 $\mathbf{Z}_p$，其中的元素 $[i]=i$ [1] 常记为 i，在这种记号下，$\mathbf{Z}_p=\{0,1,\cdots,p-1\}$.

习 题 四

1. 证明在特征为 p 的有限域 F 中，映射 φ：$a\mid\rightarrow a^p$，$a\in F$，是 F 的一个自同构.
2. 完成定理 5 的证明.

第七章　格与布尔代数

§1　格——偏序集

我们已经学习了偏序关系、偏序集及一些相关的概念，由此我们已经知道,对于一个偏序集〈P，$\leqslant$〉，其子集 A 未必有最小上界和最大下界．例如，图 1.1 所示的偏序集中 $\{c, d\}$ 有两个上界 a 和 b，但无最小上界，$\{g, f\}$ 无下界，自然无最大下界．

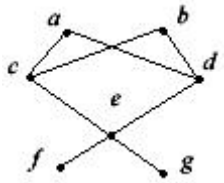


图 1．1

如果在一个偏序集中任意两元素构成的子集均有最大下界和最小上界，这种偏序集就称为格．

定义 1　设〈L,$\leqslant$〉是一个偏序集，如果 $\forall x, y \in L$, $\{x, y\}$ 必有最小上界和最大下界，则称〈L,$\leqslant$〉为格．

为方便起见，对于偏序集 P 中两元素 x, y，我们将把 $\{x, y\}$ 的最小上界说成是 x, y 的最小上界，$\{x, y\}$ 的最大下界说成是 x, y 的最大下界．

例 1　下图所示的偏序集均为格.

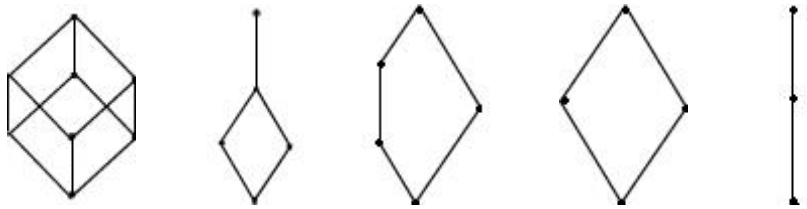


图 1.2

例 2　下图所示的偏序集均不是格.


图 1.3

例 3　设 S 是集合, 则〈P（S），$\subseteq$〉是一个格，且对任意 A，$B \in P$（S），$A \cup B$ 是 $\{A, B\}$ 的最小上界，$A \cap B$ 是 $\{A, B\}$ 的最大下界．

例 4　设 **N** 是自然数集合，$\leqslant$ 为通常自然数的小于等于关系，则〈**N**，$\leqslant$〉是一个

格，且对任意 $i, j \in \mathbf{N}$，$\min\{i, j\}$ 为 i, j 的最大下界，$\max\{i, j\}$ 为 i, j 的最小上界.

一般地，在格 $\langle L, \leqslant \rangle$ 中，a, b 的最小上界用 $a \oplus b$ 表示，a, b 的最大下界用 $a * b$ 表示. 于是，$\forall\, a, b \in L$，由最小上界、最大下界的唯一性，$a \oplus b$，$a * b$ 都在 L 上唯一确定，从而可将 $\oplus, *$ 视为 L 上的两个运算，通常分别称为 $\langle L, \leqslant \rangle$ 上的并运算与交运算.

下面研究格中并、交两个运算的性质.

定理 1　设 $\langle L, \leqslant \rangle$ 是一个格，$\langle L, \leqslant \rangle$ 上的并运算 $\oplus$ 与交运算 $*$ 满足如下性质：

L_1　$a * a = a$　　$a \oplus a = a$　　（幂等律）

L_2　$a * b = b * a$　　$a \oplus b = b \oplus a$　　（交换律）

L_3　$(a * b) * c = a * (b * c)$

　　$(a \oplus b) \oplus c = a \oplus (b \oplus c)$　　（结合律）

L_4　$a * (a \oplus b) = a$

　　$a \oplus (a * b) = a$　　（吸收集）

证明

(1)　由于 $a \leqslant a$，故 a 是 $\{a\} = \{a, a\}$ 的下界，又设 c 是 $\{a, a\}$ 的任一下界，则 $c \leqslant a$，故 a 是 $\{a, a\}$ 的最大下界，即 $a * a = a$，同理可证 $a \oplus a = a$，即 L_1 成立.

(2)　由于 $\{a, b\} = \{b, a\}$，故 $a * b = b * a$，同理 $a \oplus b = b \oplus a$. 即 L_2 成立.

(3)　根据 $*$ 的定义

$$(a * b) * c \leqslant a * b \leqslant a$$
$$(a * b) * c \leqslant a * b \leqslant b$$
$$(a * b) * c \leqslant c$$

因此，$(a * b) * c$ 是 b, c 的下界，从而小于等于其最大下界，即

$$(a * b) * c \leqslant b * c$$

因此又知 $(a * b) * c$ 是 $a, b * c$ 的下界，从而

$$(a * b) * c \leqslant a * (b * c)$$

同理　　$a * (b * c) \leqslant (a * b) * c$

所以　　$a * (b * c) = (a * b) * c$

同理可证　　$(a \oplus b) \oplus c = a \oplus (b \oplus c)$，即 L_3 成立.

(4)　由于 a 是 $\{a, a \oplus b\}$ 的下界，故 $a \leqslant a * (a \oplus b)$，再由 $*$ 的定义，$a * (a \oplus b) \leqslant a$，从而 $a * (a \oplus b) = a$. 同理可证 $a \oplus (a * b) = a$，即 L_4 成立. ▌

上面我们所给出的运算性质都是成对出现的，而我们在证明这些性质时，只证明了每对性质中的一条，同样步骤，只不过将符号 $\leqslant$ 换为 $\geqslant$（这里，$\geqslant$ 表示 $\leqslant$ 的逆 $\leqslant^{-1}$，下同），$*$ 换为 $\oplus$，$\oplus$ 换为 $*$，即可得另一条性质的证明，这种“对偶性”是以下一般原理的体现.

对偶原理　设 Q 是一个对任意格都成立的命题，则将 Q 中的 $\leqslant$ 换为 $\geqslant$（或 $\geqslant$ 换

为 $\leqslant$），$*$ 换为 $\oplus$，$\oplus$ 换为 $*$ 得到的“对偶命题”Q^*亦必成立.

对此原理，我们做如下直观说明：

首先注意，如果 $\leqslant$ 是集合 P 上的偏序，则 $\leqslant$ 的逆 $\leqslant^{-1}$ 也为 P 上的偏序. 因此，给定偏序集〈P，$\leqslant$〉，便又可对应地得到偏序集〈P，$\leqslant^{-1}$〉. 在这两个偏序集中，“大小关系”是颠倒的：

$$a \leqslant b \quad \Leftrightarrow \quad b \leqslant^{-1} a$$

即 a 在〈P，$\leqslant$〉中小于等于 b $\Leftrightarrow$ b 在〈P，$\leqslant^{-1}$〉中小于等于 a

因而，P 的任意子集 A 在〈P，$\leqslant$〉中的最小上界和最大下界恰分别为 A 在〈P，$\leqslant^{-1}$〉中的最大下界和最小上界，我们把〈P，$\leqslant^{-1}$〉称作〈P，$\leqslant$〉的对偶.

由上所述可知，如果〈P，$\leqslant$〉是格，则其对偶〈P，$\leqslant^{-1}$〉也必是格，且〈P，$\leqslant$〉中的并、交运算恰为〈P，$\leqslant^{-1}$〉中的交、并运算.

现设 Q 为对任意格都成立的命题，〈L，$\leqslant$〉为任意一个格，则 Q 对〈L，$\leqslant$〉成立，Q 一般与 $\leqslant$，$\oplus$，$*$ 有关，因此，不妨记 $Q=Q(\leqslant, \oplus, *, \cdots)$. 由于〈$L$，$\leqslant^{-1}$〉为格，而 Q 对任意格均成立，故 Q 必对〈L，$\leqslant^{-1}$〉成立，即 $Q(\leqslant^{-1}, \oplus_1, *_1, \cdots)$ 成立，其中$\oplus_1$，$*_1$分别为〈L，$\leqslant^{-1}$〉中的并、交运算，由于〈L，$\leqslant^{-1}$〉中并运算$\oplus_1$恰为〈L，$\leqslant$〉中的交运算 $*$，〈L，$\leqslant^{-1}$〉中的交运算 $*_1$ 恰为〈L，$\leqslant$〉中的并运算$\oplus$，所以 $Q(\leqslant^{-1}, \oplus_1, *_1, \cdots) = Q(\geqslant, *, \oplus, \cdots) = Q^*$，即〈$L$，$\leqslant$〉中的命题 Q^* 即为〈L，$\leqslant^{-1}$〉中的命题 Q，因此 Q^* 成立，由〈L，$\leqslant$〉的任意性，Q^* 对任意格都成立.

这样，在格中只要证明一个一般性命题，利用对偶原理马上可以写出其对偶命题，上面运算性质 L_1-L_4 中，每条性质都包含互为对偶的两式，例如，在 L_4 中将第一式 $a*(a\oplus b) = a$ 中的 $*$，$\oplus$ 互换正好得第二式 $a\oplus(a*b) = a$.

在应用对偶原理时必须注意，Q 是对任意格都成立的命题，其对偶命题 Q^* 才必定成立，而只对某些特殊格成立的命题，其对偶命题未必为真，例如，设〈$\mathbf{N}$，$\leqslant$〉是自然数集 $\mathbf{N}$ 在通常小于等于关系 $\leqslant$ 下构成的格，则“$\forall x\in\mathbf{N}, \exists y\in\mathbf{N}$ 使 $x<y$”在〈$\mathbf{N}$，$\leqslant$〉中成立，但其对偶命题“$\forall x\in\mathbf{N}, \exists y\in\mathbf{N}$ 使 $x>y$”不成立.

习 题 一

1. 图 1.4 所示的偏序集，哪几个不是格？为什么？

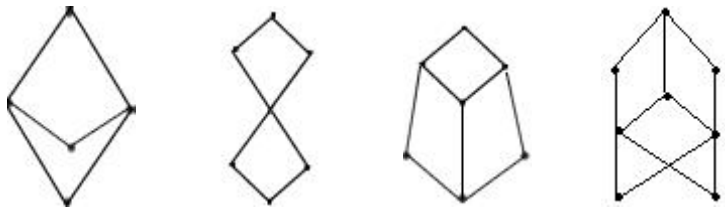


图 1.4

2. 由下列集合 L 构成的偏序集〈L，$\leqslant$〉中，哪几个是格？其中，$\leqslant$ 表示 L 上的整除关系，

a） $L=\{1, 2, 3, 4, 6, 12\}$

b） $L=\{1, 2, 3, 4, 6, 8, 12, 14\}$

c） $L=\{1, 2, 3, \cdots, 12\}$

3. 设 a，b 是格〈L，$\leqslant$〉中的两个元素，证明：

$$a*b<b, \quad a*b<a \text{ 当且仅当 } a \text{ 与 } b \text{ 不可比较.}$$

4. 设〈L，$\leqslant$〉是一个格，证明〈L，$\geqslant$〉也是格，其中 $\geqslant$ 为 $\leqslant$ 的逆.

§ 2 格——代数系统

在上节我们看到，在任意格〈L，$\leqslant$〉中自然存在两个运算 $\oplus$ 和 $*$，从而派生出一个代数系统〈L，$\oplus$，$*$〉，其中，$\oplus$ 与 $*$ 满足 L_1-L_4。反之，若给定一个代数系统〈L，$\oplus$，$*$〉，其中，运算 $\oplus$ 与 $*$ 满足 L_1-L_4，是否一定能找到一个与该代数系统对应的格呢？本节将讨论这个问题.

定理 1 设〈L，$\leqslant$〉是一个格，则对任意 a，$b\in L$

$$a\leqslant b \Leftrightarrow a*b=a \Leftrightarrow a\oplus b=b$$

证明 先证 $a\leqslant b \Leftrightarrow a*b=a$

设 $a\leqslant b$，则 a 是 $\{a, b\}$ 的下界，故 $a\leqslant a*b$，又 $a*b\leqslant a$，从而 $a*b=a$，反之，设 $a*b=a$，则由 $a*b\leqslant b$ 即知 $a\leqslant b$.

同理可证 $a\leqslant b\Leftrightarrow a\oplus b=b$ ▌

这个定理直接揭示了一个格〈L，$\leqslant$〉中偏序 $\leqslant$ 与运算 $\oplus$，$*$ 之间的关系，它告诉我们，给定代数系统〈L，$\oplus$，$*$〉，（其中，运算 $\oplus$，$*$ 满足 L_1-L_4），要想得到一个与之对应的格〈L，$\leqslant$〉，使得〈L，$\leqslant$〉中的并、交运算恰为给定运算 $\oplus$ 与 $*$，引入的偏序 $\leqslant$ 必须满足

$$a\leqslant b \Leftrightarrow a*b=a \Leftrightarrow a\oplus b=b \qquad (1)$$

为了得到一个满足该条件的偏序 $\leqslant$，我们自然考虑就用该式规定偏序$\leqslant$，为了保证这种规定的合理性，首先要求给定的运算 $\oplus$ 与 $*$ 满足

$$a*b=a \Leftrightarrow a\oplus b=b \qquad (2)$$

这可由下面引理保证

引理 设〈L，$\oplus$，$*$〉是一个代数系统，$\oplus$，$*$ 满足 L_1-L_4，则（2）式成立.

证明 设 $a*b=a$，则

$$a\oplus b=(a*b)\oplus b=b\oplus(b*a)=b$$

反之，设 $a\oplus b=b$ 则

$$a*b=a*(a\oplus b)=a$$

于是　　$a*b=a \Leftrightarrow a\oplus b=b$　　▌

这样一来，（1）式相当于　　$a\leqslant b \Leftrightarrow a*b=a$

显然，用此式规定关系 $\leqslant$ 是可行的，但这样规定的关系 $\leqslant$ 是否一定是要求的偏序关系呢？

定理 2　设〈L，$\oplus$，$*$〉是一个代数系统，其中的运算 $\oplus$ 与 $*$ 满足 L_1-L_4，令 $\leqslant$ 是 L 上的关系，定义如下：

$$a \leqslant b \Leftrightarrow a*b=a$$

则 $\leqslant$ 是一个偏序关系，且 $\forall a, b\in L$，$a*b$，$a\oplus b$ 分别为 a，b 在〈L，$\leqslant$〉中的最大下界与最小上界，即

$$a*b=\inf\{a, b\}\qquad a\oplus b=\sup\{a, b\}$$

从而〈L，$\leqslant$〉是一个格，其中的并、交运算恰为给定的 $\oplus$ 与 $*$.

证明

（1）　先证 $\leqslant$ 为偏序关系，$\forall a\in L$，因为 $a*a=a$，故 $a\leqslant a$，即$\leqslant$满足自反性．又 $\forall a, b\in L$，设 $a\leqslant b$，$b\leqslant a$，则 $a*b=a$，$b*a=b$，因为 $a*b=b*a$，故 $a=b$，即 $\leqslant$ 满足反对称性，最后，$\forall a, b, c\in L$，设 $a\leqslant b$，$b\leqslant c$，则 $a*b=a$，$b*c=b$，故 $a*c=(a*b)*c=a*(b*c)=a*b=a$，即 $a\leqslant c$，$\leqslant$满足传递性，总之，$\leqslant$是偏序关系．

（2）　再证〈L，$\leqslant$〉为要求的格．

$\forall a, b\in L$，$(a*b)*a=a*(a*b)=(a*a)*b=a*b$，故 $a*b\leqslant a$，同理 $a*b\leqslant b$，因此 $a*b$ 是 $\{a, b\}$ 的下界，又设 c 是 $\{a, b\}$ 的任一下界，即 $c\leqslant a$，$c\leqslant b$，则 $a*c=c$，$b*c=c$，于是 $(a*b)*c=a*(b*c)=a*c=c$，即 $c\leqslant a*b$，所以 $a*b$ 是 $\{a, b\}$ 的最大下界，即 $a*b=\inf\{a, b\}$，同理可证 $a\oplus b=\sup\{a, b\}$，这就证明了〈L，$\leqslant$〉是格且其中的并、交运算分别为 $\oplus$，$*$.　　▌

通过前面的讨论，我们已经知道，一个格〈L，$\leqslant$〉与一个满足运算性质 L_1—L_4 的代数系统〈L，$\oplus$，$*$〉是等同的，给定其中之一则可相应得到另一个，因此，我们可以引入如下格的等价定义．

定义 1　设〈L，$\oplus$，$*$〉是一个代数系统，如果 $\oplus$，$*$ 满足 L_1-L_4，则称〈L，$\oplus$，$*$〉为格．

以后，对于给定的格，我们即可以把它看成是偏序格（由上节定义 1 定义的格），也可把它看成代数格（由本节定义 1 定义的格），且认为，给出格的一种形式也就给出了另一个形式．

例 1　设 **N** 是自然数集合，对任意 a，$b\in\mathbf{N}$，规定 $a*b=(a, b)$（即 a，b 的最大公因数），$b=[a, b]$（即 a，b 的最小公倍数），由于任意两自然数 a，b 都有唯一确定的最大公因数与最小公倍数，故 $*$，$\oplus$ 是 **N** 上的两个运算．

$a*a=(a, a)=a$，　$a\oplus a=[a, a]=a$，L_1成立

$a*b=(a, b)=(b, a)=b*a$，　$a\oplus b=[a, b]=[b, a]=b\oplus a$，$L_2$成立．

$(a*b)*c=((a, b), c)=(a, b, c)=(a, (b, c))=a*(b*c)$.

$(a\oplus b)\oplus c=[[a,b],c]=[a,b,c]=[a,[b,c]]=a\oplus(b\oplus c)$，$L_3$成立.

因为$a\mid[a,b]$，故$a*(a\oplus b)=(a,[a,b]))=a$，因为$(a,b)\mid a$，故$a\oplus(a*b)=[a,(a,b)]=a$，　　L_4成立.

总之，〈**N**，$\oplus$，$*$〉是一个格，其中的偏序 $\leqslant$ 应由下式规定

$$a\leqslant b \Leftrightarrow a*b=a$$

由于$a*b=a \Leftrightarrow a\mid b$，故$a\leqslant b \Leftrightarrow a\mid b$，即 $\leqslant$ 为整数的整除关系.

例 2　设S是一个集合，$\cup$，$\cap$为集合的并、交运算，则〈$P(S)$，$\cup$，$\cap$〉是格，且其中的偏序为集合的包含关系.

以上我们讨论了格的两种等价定义，为了以后使用方便，我们再把几个常用的事实写成以下定理形式.

定理 3　设〈L，$\leqslant$〉是格，a，$b\in L$，则

（1）$a*b\leqslant a$　　$a*b\leqslant b$

（2）$a\leqslant a\oplus b$　　$b\leqslant a\oplus b$

定理 4　设〈L，$\leqslant$〉是格，a，b，$c\in L$.

（1）若　$c\leqslant a$，$c\leqslant b$ 则 $c\leqslant a*b$

（2）若　$a\leqslant c$，$b\leqslant c$ 则 $a\oplus b\leqslant c$

以上两定理由并、交运算的定义立即可得到

定理 5　设〈L，$\leqslant$〉是一个格，a_1，a_2，b_1，$b_2\in L$，如果

$$a_1\leqslant b_1,\ a_2\leqslant b_2,$$

则

$$a_1*a_2\leqslant b_1*b_2$$

$$a_1\oplus a_2\leqslant b_1\oplus b_2$$

证明

因为　$a_1*a_2\leqslant a_1\leqslant b_1$

　　$a_1*a_2\leqslant a_2\leqslant b_2$

故　$(a_1*a_2)\leqslant b_1*b_2$

又　$a_1\leqslant b_1\leqslant b_1\oplus b_2$

　　$a_2\leqslant b_2\leqslant b_1\oplus b_2$

故　$a_1\oplus a_2\leqslant(b_1\oplus b_2)$　　▌

推论　设〈L，$\leqslant$〉是一个格，a，b，$c\in L$，

若$a\leqslant b$，　则　　$a*c\leqslant b*c$

　　$a\oplus c\leqslant b\oplus c$

定理 6　设L是一个格，a，b，$c\in L$，则

$$a*(b\oplus c)\geqslant(a*b)\oplus(a*c)$$

$$a\oplus(b*c)\leqslant(a\oplus b)*(a\oplus c)$$

证明

因为　$b\leqslant b\oplus c$

故　　$a*b \leqslant a*(b\oplus c)$

又　　$c \leqslant b\oplus c$

故　　$a*c \leqslant a*(b\oplus c)$

所以　　$(a*b)\oplus(a*c) \leqslant a*(b\oplus c)$

即　　$a*(b\oplus c) \geqslant (a*b)\oplus(a*c)$

由此，利用对偶原理又可得

$$a\oplus(b*c) \leqslant (a\oplus b)*(a\oplus c)$$

习 题 二

1. 设〈L，$\oplus$，$*$〉是一个代数系统，证明　如果 $\oplus$，$*$ 满足吸收律，则 $\oplus$，$*$ 必满足幂等律.
2. 设〈L，$\oplus$，$*$〉是一个代数系统, 其中 $\oplus$，$*$ 都是二元运算且满足幂等律，试举例说明吸收律未必成立.
3. 设 A 是实数集 **R** 的一个子集，令

$$a\oplus b=\max\{a，b\}\quad a*b=\min\{a，b\}$$

证明〈A，$\oplus$，$*$　〉是格，该格中的偏序为何？又若令

$$a\oplus b=\min\{a，b\}$$

$$a*b=\max\{a，b\}$$

〈A，$\oplus$，$*$〉是否还是格？若是，其中的偏序又为何？

§ 3　子格与格同态

既然格是一个代数系统，前面有关代数系统的一些概念便可应用到格上.

定义 1　设〈L，$\oplus$，$*$〉是一个格，S 是 L 的非空子集，如果 S 关于$\oplus$，$*$ 封闭，则说 S 是 L 的子格.

例 1　对于上节例 1 的〈**N**，$\oplus$，$*$〉，令 S 为 **N** 中所有偶数构成的集合，则 S 是 **N** 的非空子集. 因为偶数的最小公倍数与最大公因数均为偶数，即$\forall\, a$，$b\in S$，$a\oplus b\in S$，$a*b\in S$，所以 S 为 **N** 的子格.

例 2　设〈L，$\leqslant$〉是一个格，$a\in L$，令 $T=\{x\mid x\in L，x\leqslant a\}$

则 T 是 L 的子格.

事实上，$\forall x$，$y\in T$，$x\leqslant a$，$y\leqslant a$，故 $x*y\leqslant a$，$x\oplus y\leqslant a$，即 $x*y\in T$，$x\oplus y\in T$，因此 T 是 L 的子格.

同样，在格〈L，$\leqslant$〉中，$\forall\, a$，$b\in L$，$a\leqslant b$，令

$$I[a，b]=\{x\mid x\in L，a\leqslant x\leqslant b\}$$

则 $I[a, b]$ 是 L 的子格，通常称这个子格为 L 的一个闭区间.

例 3　设偏序集 $\langle L, \leqslant\rangle$ 由图 3.1（a）给出，$S=\{1, a, c, 0\}$，则 S 在 L 中的偏序 $\leqslant$ 下构成一个偏序集 $\langle S, \leqslant\rangle$，其 Hasse 图如图 3.1（b）所示.

显然，$\langle S, \leqslant\rangle$ 本身是一个格，但它不是 $\langle L, \leqslant\rangle$ 的子格.

定义 2　设 $\langle L, \oplus, *\rangle$，$\langle L', \cup, \cap\rangle$ 是两个格，$f: L \to L'$，如果 $\forall a, b \in L$，有

$$f(a \oplus b) = f(a) \cup f(b)$$
$$f(a * b) = f(a) \cap f(b)$$

则称 f 是格 L 到 L' 的同态.

与前面类似地可定义单同态，满同态，同构. f 是 L 到 L' 的满同态记为 $f: L \sim L'$，f 是 L 到 L' 的同构记为 $f: L \cong L'$.

为了书写简捷，经常用 L 表示格 $\langle L, \leqslant\rangle$ 或 $\langle L, \oplus, *\rangle$，在提到不同格时，这些格中的并、交运算往往用同样符号 $\oplus$，$*$ 表示，而其中的偏序也用同一符号 $\leqslant$ 表示.

（a）　　（b）

图 3.1

定理 1　设 f 是格 L 到 L' 的同态，则 f 是偏序集 L 到 L' 的保序映射，即 $\forall x, y \in L$，当 $x \leqslant y$ 时，$f(x) \leqslant f(y)$

证明　设 $x \leqslant y$，则 $x * y = x$，故

$$f(x) * f(y) = f(x * y) = f(x)$$

即知 $f(x) \leqslant f(y)$. ▌

注意，以上定理的逆命题不成立，即是说，格 L 到 L' 的保序映射未必是 L 到 L' 的同态，看下面例子.

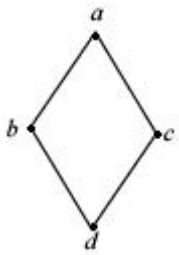
例 4　设 $\langle L, \leqslant\rangle$，$\langle L', \leqslant\rangle$ 分别是由图 3.2（a），图 3.2（b）给出的两个格，令

$$f: a \mapsto 3,\ b \mapsto 2,\ c \mapsto 2,\ d \mapsto 1$$

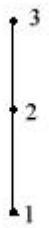
则 f 是 L 到 L' 的保序映射，但是

$$f(b * c) = f(d) = 1$$
$$f(b) * f(c) = 2 * 2 = 2$$
$$f(b * c) \neq f(b) * f(c)$$

因此，f 不是 L 到 L' 的同态.



(*a*)



（*b*）

图 3.2

***定理** 2　设 f 是格 L 到 L' 的双射，则 f 是 L 到 L' 的同构，当且仅当

$$\forall\ a, b\in L,\quad a\leqslant b \Leftrightarrow f(a)\leqslant f(b)$$

证明　（1）设 f 是 L 到 L' 的同构.

对任意 a，$b\in L$，若 $a\leqslant b$，由定理 1 知 $f(a)\leqslant f(b)$，反之，若 $f(a)\leqslant f(b)$，则 $f(a)*f(b)=f(a)$，另一方面，根据同态的定义，$f(a)*f(b)=f(a*b)$，所以 $f(a*b)=f(a)$，因为 f 是双射，故知 $a*b=a$，即 $a\leqslant b$.

这样就证明了 $a\leqslant b\Leftrightarrow f(a)\leqslant f(b)$

（2）设对任意 a，$b\in L$，$a\leqslant b \Leftrightarrow f(a)\leqslant f(b)$

取 x，$y\in L$，则 $x*y\leqslant x$，$x*y\leqslant y$，故 $f(x*y)\leqslant f(x)$，$f(x*y)\leqslant f(y)$，因此，$f(x*y)\leqslant f(x)*f(y)$。又因为 f 是双射，故必存在 $z\in L$，使 $f(x)*f(y)=f(z)$，此时必有，$f(z)\leqslant f(x)$，$f(z)\leqslant f(y)$，从而 $z\leqslant x$，$z\leqslant y$，于是 $z\leqslant x*y$，$f(z)\leqslant f(x*y)$，即 $f(x)*f(y)\leqslant f(x*y)$.

总之，$f(x*y)=f(x)*f(y)$，类似可证 $f(x\oplus y)=f(x)\oplus f(y)$，所以，$f$ 是 L 到 L' 的同构. ▌

习 题 三

1. 设 L 是格，a，$b\in L$ 且 $a<b$，若 $A=\{x\mid x\in L, a<x<b\}$ 非空，问 A 是否必为 L 的子格？
2. 设〈**N**，≤〉是自然数集 **N** 在通常小于等于关系下构成的格，D 是奇数集合，〈D，≤〉是否是 **N** 的子格？
3. 设 L_1，L_2 是两个格，f：$L_1\cong L_2$，证明 f^{-1}：$L_2\cong L_1$.

§4　完全格　有界格　补格

在格的定义中，要求任意子集 $\{a, b\}$ 的最小上界与最大下界存在，利用数学归纳法容易证明，格的任意有限子集，其最小上界与最大下界都必然存在。但无限子集的最

小上界与最大下界却未必存在，例如，整数集 $\mathbf{Z}$ 在通常数的小于等于关系≤下是一个格，其子集 $E=\{\cdots,-4,-2,0,2,\cdots\}$ 既无最小上界也无最大下界．一个格，如果其任意子集（有限的或无限的）均存在最小上界和最大下界，我们就把它称做完全格．

定义 1　设〈L，≤〉是一个格，如果 L 的任意子集均有最小上界和最大下界，则称其为完全格．

显然，有限格必为完全格．

例 1　实数闭区间［0，1］在通常的小于等于关系 ≤ 下是完全格，实数开区间（0，1）则不然．

例 2　集合 A 的幂集格〈$P(A)$，$\subseteq$〉是完全格．

事实上，对 $P(A)$ 的任意子集 S，S 中所有元素的交即为 S 的最大下界，S 中所有元素的并即为 S 的最小上界．

定义 2　设〈L，≤〉是一个格，如果 L 中存在最大元与最小元，则称 L 是有界格．

在偏序集中，最大元也称为全上界或单位元，用 1 表示；最小元也称为全下界或零元，用 0 表示，对应地，有界格也称为有单位元和零元的格．

显然，完全格必为有界格．

例 3　设 A 是集合，A 的幂集格〈$P(A)$，$\subseteq$〉是有界格，其单位元为 A，零元为∅.

例 4　实数开区间（0，1）在通常小于等于关系≤下构成的格不是有界格．

定理 1　设 L 是一个有界格，则对任意 $x\in L$，有

$$x\oplus 0=x,\qquad x*0=0$$

$$x\oplus 1=1,\qquad x*1=x$$

证明　对任意 $x\in L$，因为 0 是最小元，故有 $0\leqslant x$，所以 $x\oplus 0=x$，$x*0=0$．同理可证 $x\oplus 1=1$，$x*1=x$. ∎

定义 3　设 L 是一个有界格，$a\in L$，如果存在 $b\in L$ 使

$$a\oplus b=1\qquad a*b=0$$

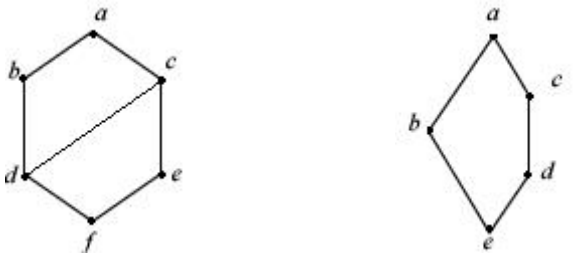
则称 b 是 a 的补元．

由定义可知，当 b 是 a 的补元时，a 也是 b 的补元，因此，这时可以说 a，b 是互补的．

例 5　设 A 是一个集合，〈$P(A)$，$\subseteq$〉是 A 的幂集格，则对 $P(A)$ 中任意元素 S，由于 $(A-S)\cup S=A$，$(A-S)\cap S=\varnothing$，　故知 $A-S$ 是 S 的补元．

例 6　（1）设 $L=\{a,b,c,d,e\}$，≤ 是 L 中由图 4.1（a）确定的偏序，则〈L，≤〉是一个有界格，其中，a，f 互补，b，e 互补，d，c 无补元．

（2）设 $L_1=\{a,b,c,d,e\}$，$\leqslant_1$ 是 L_1 中由图 4.1（b）确定的偏序，则〈L_1，$\leqslant_1$〉是有界格，其中 a，e 互补，c，d 均是 b 的补元．



(*a*)　　（*b*）

图 4.1

通过上面例子我们看到，在有界格中，一个元素可以有一个或多个补元，也可以没有补元，但是，对 1 和 0 我们有

定理 2　设 L 是有界格，则单位元 1 是零元 0 的唯一补元，反之亦然.

证明　由于 $1*0=0$，$1\oplus 0=1$，故 0 是 1 的补元，又设 a 是 1 的任一补元，则由补元的定义，$1*a=0$，而由 1 的性质，$1*a=a$，所以 $a=0$，于是，0 是 1 的唯一补元，同理 1 是 0 的唯一补元. ▌

定义 4　设 L 是一个有界格，如果 L 中每个元素都有补元，则称其为补格或有补格.

例如，集合 A 的幂集格 $P(A)$ 是补格，例 6 的（2）中定义的格 L_1 是补格，例 6 的（1）中定义的格 L 不是补格.

例 7　图 4.2 的各 Hasse 图中，（*a*），（*b*），（*c*）定义的格是补格，（*d*），（*e*）定义的格不是补格.

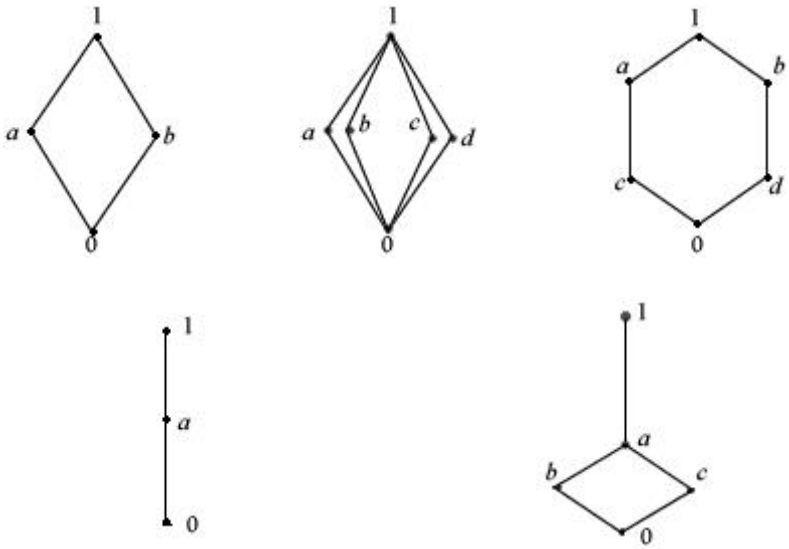


图 4.2

习 题 四

1．举例说明有界格未必是完全格.

2．根据图 4.3 所示有界格回答以下问题（1）a 和 f 的补元分别是哪些元素？（2）该格是否为补格？

3．证明具有两个或更多个元素的格中不存在以自身为补元的元素.

4．设〈L，$\leqslant$〉是有界格，x，$y\in L$，证明

（1）$x\oplus y=0 \Leftrightarrow x=0$，$y=0$

（2）$x*y=1 \Leftrightarrow x=1$，$y=1$

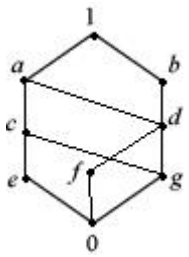


图 4.3

§ 5　分配格与模格

我们知道，格是具有两个二元运算并和交的代数系统，这两个运算由吸收集 L_4 联系起来。那么，我们通常所熟悉的联系两个运算的算律——分配律是否成立呢？

集合 A 的幂集格 $P(A)$ 中的并、交运算确实满足分配律，即 A_1，A_2，$A_3\in P(A)$，有

$$A_1\cap(A_2\cup A_3)=(A_1\cap A_2)\cup(A_1\cap A_3)$$

$$A_1\cup(A_2\cap A_3)=(A_1\cup A_2)\cap(A_1\cup A_3)$$

但并非每一格都具有该性质，例如，在图 5.1 所示的格中

$$b*(c\oplus d)=b*1=b$$

$$(b*c)\oplus(b*d)=0\oplus d=d$$

因此，$b*(c\oplus d)\neq(b*c)\oplus(b*d)$，即分配律不成立.

图 5.1

定义 1　设 L 是一个格，如果 L 中的并、交运算互相可分配，即对任意 a，b，$c\in L$

$a*(b\oplus c)=(a*b)\oplus(a*c)$

$a\oplus(b*c)=(a\oplus b)*(a\oplus c)$

则称 L 是分配格.

其实，以上定义中的两个分配律是等价的，只要一个成立，另一个也必然成立.

定理 1　设 L 是一个格，如果 L 中的交对并可分配，则并对交必可分配．反之亦然.

证明　设 L 中交对并可分配，即 $\forall a$，b，$c\in L$

$$a*(b\oplus c)=(a*b)\oplus(a*c)$$

则　$(a\oplus b)*(a\oplus c)$

$=((a\oplus b)*a)\oplus((a\oplus b)*c)$

$= a \oplus ((a \oplus b) * c)$

$= a \oplus ((a * c) \oplus (b * c))$

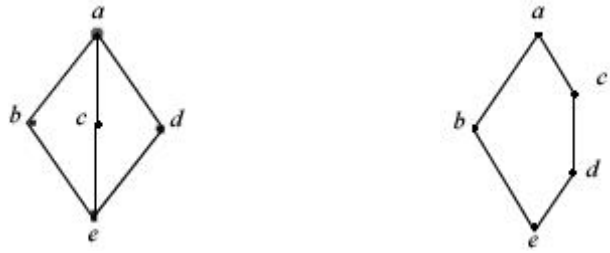
$= (a \oplus (a * c)) \oplus (b * c)$

$= a \oplus (b * c)$

即并对交可分配，同理可证并对交可分配时，交对并必可分配. ▌

例 1　集合 A 的幂集格 $P(A)$ 是分配格.

例 2　图 5.2 所示的两个格都不是分配格.



(a)　　(b)

图 5.2

这是因为，在图 5.2（a）所示格中

$$b * (c \oplus d) = b * a = b$$

$$(b * c) \oplus (b * d) = e \oplus e = e$$

所以

$$b * (c \oplus d) \neq (b * c) \oplus (b * d)$$

在图 5.2（b）所示格中

$$c * (b \oplus d) = c * a = c$$

$$(c * b) \oplus (c * d) = e \oplus d = d$$

$$c * (b \oplus d) \neq (c * b) \oplus (c * d)$$

例 2 所给出的两个五元素格是很重要的，因为可以证明，一个格是分配格的充要条件是在该格中没有与这两个五元素格之一同构的子格.

例 3　图 5.3 所示格不是分配格，因为，〈{a，b，d，g，c,}，≤〉是该格的一个子格，而这个子格与图 5.2（b）所示格同构.

由于对任意格 L 总有

$$a * (b \oplus c) \geqslant (a * b) \oplus (a * c)$$

$$a \oplus (b * c) \leqslant (a \oplus b) * (a \oplus c)$$

因此，要证明分配律，只要证明

$$a * (b \oplus c) \leqslant (a * b) \oplus (a * c)$$

$$a \oplus (b * c) \geqslant (a \oplus b) * (a \oplus c)$$

再注意两个分配律的等价性，只需证明这两式之一成立即可.

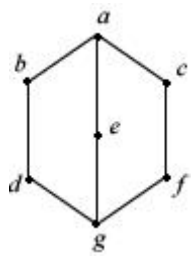


图 5．3

定理 2　设〈L，$\oplus$，$*$〉是一个分配格，a，b，$c \in L$，

如果　$a*b=a*c$　$a\oplus b=a\oplus c$　则　$b=c$

证明　$b=b*(b\oplus a)$

$=b*(a\oplus b)$

$=b*(a\oplus c)$

$=(b*a)\oplus(b*c)$

$=(a*c)\oplus(b*c)$

$=(a\oplus b)*c$

$=(a\oplus c)*c$

$=c$ ▌

推论　设〈L，$\oplus$，$*$〉是一个分配格，则$\forall a\in L$，A 的补元若存在则是唯一的.

证明　设 a_1，a_2都是 a 的补元，则由补元的定义，有

$$a*a_1=0=a*a_2$$

$$a\oplus a_1=1=a\oplus a_2$$

因此，$a_1=a_2$，即 a 的补元如果存在，则是唯一的. ▌

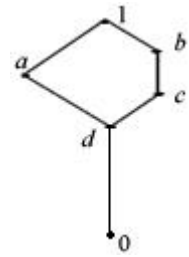


图 5.4

由以上定理及推论，有时可方便地断定某格不是分配格，例如，在图 5.4 所示格中

$$a*b=a*c=d$$

$$a\oplus b=a\oplus c=1$$

但 $b\neq c$，故图 5.4 所示不是分配格。又如，在图 5.2（a）所示格中，b 有两个相异补元 c，d，由此也可以知该格不是分配格.

定义 2　设〈L，$\oplus$，$*$〉是一个格，如果对于任意 a，b，$c\in L$，当 $a\geqslant b$ 时必有

L_5　$a*(b\oplus c)=b\oplus(a*c)$　（模律）

则称 L 为模格（或 Dedekind 格）.

定理 3　分配格必是模格.

证明　设〈L，$\oplus$，$*$ 〉是一分配格，$\forall a$，b，$c\in L$，若 $a\geqslant b$，则 $a*b=b$，从而

$$a*(b\oplus c)=(a*b)\oplus(a*c)=b\oplus(a*c)$$

所以 L 是模格. ▌

定理 4　设〈L，$\oplus$，$*$〉是一个格，则 L 是模格当且仅当对任意 a，b，$c\in L$

由　$a\geqslant b$，$a*c=b*c$，$a\oplus c=b\oplus c$，可推出 $a=b$.

证明　先证条件是必要的.

设〈L，$\oplus$，$*$〉是模格，$\forall a$，b，$c\in L$，

若　$a\geqslant b$，$a*c=b*c$，$a\oplus c=b\oplus c$

则　$a=a*(a\oplus c)=a*(b\oplus c)$

$=b\oplus(a*c)=b\oplus(b*c)$

$=b$

再证条件是充分的.

设 $a\geqslant b$，则

$$b\oplus(a*c)\leqslant a\oplus(a*c)=a$$

因此　　$(b\oplus(a*c))*c\leqslant a*c$

又　　$(b\oplus(a*c))*c\geqslant(a*c)*c=a*c$

故　　$(b\oplus(a*c))*c=a*c$

另一方面

$$(a*(b\oplus c))*c=a*((b\oplus c)*c)=a*c$$

所以

$$(a*(b\oplus c))*c=(b\oplus(a*c))*c \qquad (1)$$

同理　$(a*(b\oplus c))\oplus c=(b\oplus(a*c))\oplus c \qquad (2)$

又因为　$a\geqslant b$，$a\geqslant a*c$

故　　$a\geqslant b\oplus(a*c)$

又　　$b\oplus c\geqslant b\oplus(a*c)$

所以　　$a*(b\oplus c)\geqslant b\oplus(a*c)$

注意（1），（2）及定理条件便知

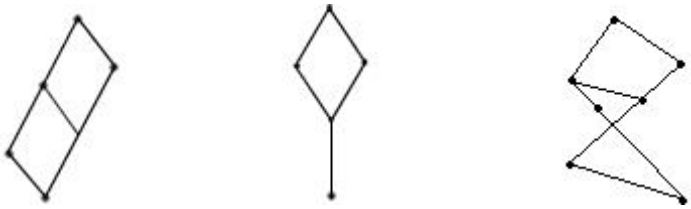
$$a*(b\oplus c)=b\oplus(a*c)$$

即 L 是模格. ▌

习 题 五

1．试找出两个含有 6 个元素的格，其中一个是分配格，另一个不是分配格.

2．在图 5.5 所给出的格中，哪几个是分配格？



(*a*)　　(*b*)　　(*c*)

图 5.5

3．证明〈$\mathbf{Z}$，$\oplus$，$*$〉是分配格，其中

$$a\oplus b=\max\{a，b\}，\quad a*b=\min\{a，b\}$$

4．证明　在分配格中必有

$$a*(b_1\oplus b_2\oplus\cdots\oplus b_n)=(a*b_1)\oplus(a*b_2)\oplus\cdots\oplus(a*b_n)$$

$$a\oplus(b_1*b_2*\cdots*b_n)=(a\oplus b_1)*(a\oplus b_2)*\cdots*(a\oplus b_n)$$

5．设〈L，$\leqslant$〉是模格，$x,y,a\in L$，且 x,y 分别盖住 a，证明 $x\oplus y$ 盖住 x 和 y.

6．设 S 是分配格，$a\in S$，　f：$x\mapsto x\oplus a$　　g：$x\mapsto x*a$

证明　f，g 是 S 的两个自同态，求出 $f(S)$，$g(S)$.

§ 6　布尔代数

本节我们以上面各节的内容为基础，定义一类特殊的格——布尔代数.

定义 1　一个格，如果既是补格又是分配格则称其为布尔代数.

例 1　设 S 是一个集合，则〈$P(S)$，∪，∩〉是一个布尔代数，称为 S 的幂集代数.

例 2　设〈P，≤〉是一个全序集，且 $|P|\geqslant 3$，则〈P，≤〉不是布尔代数.

事实上，若 P 无最大元 1 或无最小元 0，则 P 不是有界格，因此不是补格，这时 P 不是布尔代数，若 P 中有最大元 1 和最小元 0，由于 $|P|\geqslant 3$，故可取 $a\in P$，$a\neq 0$，$a\neq 1$，则 a 无补元. 因若 a 有补元 b，则由于 P 是全序集，故必有 $a\leqslant b$ 或 $b\leqslant a$. 如果 $a\leqslant b$，则 $a*b=a\neq 0$，与 b 是 a 的补元矛盾，如果 $b\leqslant a$，则 $a\oplus b=a\neq 1$ 也与 b 是 a 的补元矛盾，所以，a 无补元.

因为布尔代数是一个补格，故其每个元素均有补元，又因布尔代数是分配格，故每个元素的补元必定是唯一的，以后用 a' 表示 a 的（唯一）补元.

设〈B，⊕，$*$〉是一个布尔代数，则 $\forall a\in B$，a' 是唯一确定的，故可把 “ $'$ ” 看做是 B 上的一元运算，称为补运算，该一元运算满足如下性质.

定理 1　设〈B，⊕，$*$〉是一个布尔代数，则 $\forall a$，$b\in B$，有

$$(a')' = a \qquad \text{（反身性）}$$

$$(a*b)' = a'\oplus b'$$

$$(a\oplus b)' = a'*b' \qquad \text{（De Morgan 律）}$$

证明　由 a' 的定义，$a*a' = 0$，　$a\oplus a' = 1$，于是 a 是 a' 的补元，即 $(a')' = a$，反身性成立.

现在证明　$(a*b)' = a'\oplus b'$

因为　$(a*b)*(a'\oplus b')$

$$= ((a*b)*a')\oplus((a*b)*b')$$

$$= ((a*a')*b)\oplus(a*(b*b'))$$

$$= 0$$

$(a*b)\oplus(a'\oplus b')$

$$= (a\oplus(a'\oplus b'))*(b\oplus(a'\oplus b'))$$

$$= 1$$

所以，$a'\oplus b'$ 是 $(a*b)$ 的补元，即 $(a*b)' = a'\oplus b'$

同理可证　$(a\oplus b)' = a'*b'$.　▌

在讨论两个或多个布尔代数时，有时需要在记号上区别这些布尔代数中的运算与最大元，最小元. 为此，可以在给定布尔代数时，同时写出所用的运算符号与最大元、最小元符号. 例如，如果布尔代数 B 中的并、交、补运算及最小元、最大元分别用 $\{\oplus, *, ', 0, 1\}$ 表示，则这个布尔代数可以记成〈B，⊕，$*$，$'$，0，1〉或〈B，⊕，$*$，$'$〉.

习 题 六

1．证明在布尔代数中有

$$(a \oplus b \oplus c)' = a' * b' * c'$$

$$(a * b * c)' = a' \oplus b' \oplus c'$$

2．设 B 是一个布尔代数，a，$b \in B$，若 $a \leqslant b'$ 不成立，证明有非零元 x 使 $x \leqslant a$，$x \leqslant b$.

*§ 7　子布尔代数与布尔同态

设 $\langle B, \oplus, * \rangle$ 是一个布尔代数，$B_1 \subseteq B$，如果 B_1 对 $\{\oplus, *\}$ 封闭，则 $\langle B_1, \oplus, * \rangle$ 是 $\langle B, \oplus, * \rangle$ 的子格，这里不要求 B_1 对补运算封闭.

定义 1　设 $\langle B, \oplus, *, ' \rangle$ 是布尔代数，$B_1 \subseteq B$ 且 $B_1 \neq \varnothing$，如果 B_1 对运算 $\{\oplus, *, '\}$ 都是封闭的，即 $\forall a, b \in B_1$

$$a \oplus b \in B_1 \qquad a * b \in B_1 \qquad a' \in B_1$$

则称 $\langle B_1, \oplus, *, ' \rangle$ 是 $\langle B, \oplus, *, ' \rangle$ 的子布尔代数.

例 1　设 $S = \{a, b, c, d\}$，则 $\langle P(S), \cup, \cap, \sim \rangle$ 是一个布尔代数，令

$$A = \{\varnothing, \{d\}, \{a, b, c\}, \{a, b, c, d\}\}$$

则 $\langle A, \cup, \cap, \sim \rangle$ 是 $P(S)$ 的子布尔代数.

例 2　设 B 是一个布尔代数，$a \in B$，$B_1 = \{1, 0, a, a'\}$，则 B_1 是 B 的子布尔代数.

定理 1　设 $\langle B, \oplus, *, ', 0, 1 \rangle$ 是一个布尔代数，B_1 是 B 的子布尔代数，则 $0 \in B_1$，$1 \in B_1$.

证明　因为 $B_1 \neq \varnothing$，可取 $a \in B_1$，于是 $a' \in B_1$，所以 $0 = a * a' \in B_1$，$1 = a \oplus a' \in B_1$. ▌

例 3　设 S 是非空集合，$S_1 \subset S$，则 $P(S_1)$ 是 $P(S)$ 的子格，但不是子布尔代数，这是因为 $P(S)$ 的最大元 $S \notin P(S_1)$.

例 4　设 B 是由图 7.1 确定的布尔代数.

令 $B_1 = \{a, b, c, e\}$，则 B_1 不是 B 的子布尔代数，尽管 B_1 本身是一个布尔代数，B_1 的 Hasse 图如图 7.2.

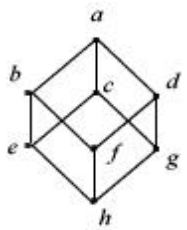


图 7.1

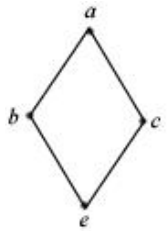


图 7.2

例 3、例 4 说明，可能会出现这样的情况，布尔代数 B 的子集 B_1 本身是一个布尔代数，但它却不是 B 的子布尔代数.

定理 2 设 B 是一个布尔代数，B_1 是 B 的非空子集，则 B_1 构成 B 的子布尔代数当且仅当 B_1 对运算 $\{*,'\}$（或 $\{\oplus,'\}$）封闭.

证明 设 B_1 是 B 的子布尔代数，由定义，它必对运算 $\{*、'\}$ 封闭. 反之，设 B_1 对 $\{*，'\}$ 封闭，则 $\forall a，b\in B_1$

$$a\oplus b=(a'*b')'\in B_1$$

即 B_1 对 $\oplus$ 也封闭，从而构成子布尔代数.

同理可证，B_1 构成子布尔代数当且仅当 B_1 对 $\{\oplus，'\}$封闭. ▌

以上通过要求子格对补运算封闭定义了子布尔代数，下面通过要求格同态保持补运算来定义布尔同态.

定义 2 设 $\langle A，\oplus，*，'\rangle$，$\langle B，\cup，\cap，\sim\rangle$ 是两个布尔代数，f：$A\to B$，如果 f 保持 $\{\oplus，*，'\}$ 运算，即 $\forall a，b\in A$，

$$f(a\oplus b)=f(a)\cup f(b)$$
$$f(a*b)=f(a)\cap f(b)$$
$$f(a')=\sim f(a)$$

则称 f 是 A 到 B 的布尔同态.

定理 3 设 f 是 $\langle A，\oplus，*，'，0，1\rangle$ 到 $\langle B，\cup，\cap，\sim，\alpha，\beta\rangle$ 的布尔同态，则

$$f(0)=\alpha \qquad f(1)=\beta$$

证明 取 $a\in A$，则

$$\begin{aligned} f(0)&=f(a*a')=f(a)\cap f(a')\\ &=f(a)\cap\sim f(a)\\ &=\alpha \end{aligned}$$

$$\begin{aligned} f(1)&=f(a\oplus a')=f(a)\cup f(a')\\ &=f(a)\cup\sim f(a)\\ &=\beta \end{aligned}$$

定理 4 设 $\langle A，\oplus，*，'\rangle$，$\langle B，\cup，\cap，\sim\rangle$ 是两个布尔代数，则 f：$A\to B$ 是 A 到 B 的布尔同态，当且仅当 f 保持运算 $\{*，'\}$（或 $\{\oplus，'\}$）.

证明 设 f：$A\to B$ 是布尔同态，则由定义，f 保持 $\{*，'\}$，反之，设 f 保持 $\{*，'\}$，则 $\forall a，b\in A$

$$\begin{aligned} f(a\oplus b)&=f((a'*b')')\\ &=\sim f(a'*b')\\ &=\sim[(\sim f(a))\cap(\sim f(b))]\\ &=f(a)\cup f(b) \end{aligned}$$

即f 也保持 $\oplus$，因此f 是布尔同态.

同理可证，f是布尔同态当且仅当f 保持$\{\oplus, '\}$. ▌

定义 3　设〈A，$\oplus$，$*$，$'$〉，〈B，$\cup$，$\cap$，$\sim$〉是两个布尔代数，如果f：$A\to B$ 是布尔同态且为双射，则称f为A 到B 的布尔同构，记为 f：$A\cong B$.

我们说两个布尔代数A，B 是同构的，并记为$A\cong B$，是指存在A 到B 的布尔同构，即存在 f：$A\to B$ 使f：$A\cong B$.

定理 5　布尔代数之间的布尔同构关系是等价关系，即对任何布尔代数A，B，C.

（1） $A\cong A$

（2） 若$A\cong B$则$B\cong A$

（3） 若$A\cong B$，$B\cong C$　则$A\cong C$

证明留给读者自己完成.

例 8　设A，B 是两个有限集，且$|A|=|B|$，则$P(A)\cong P(B)$.

证明　设$|A|=|B|=n$，并设

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

$$B=\{b_1, b_2, \cdots, b_n\}$$

令

$$f(S)=\begin{cases}\phi & S=\phi\\ \{b_{i_1}, b_{i_2}, \cdots, b_{i_k}\} & S=\{a_{i_1}, a_{i_2}, \cdots, a_{i_k}\}\end{cases}$$

则f是$P(A)$到$P(B)$的双射，且$\forall A_1, A_2\in P(A)$，若$A_1=\varnothing$　或$A_2=\varnothing$　则显然$f(A_1\cup A_2)=f(A_1)\cup f(A_2)$

若　$A_1\neq\varnothing$　，$A_2\neq\varnothing$　，不妨设

$$A_1=\{a_{i_1}, a_{i_2}, \cdots, a_{i_k}\},\quad A_2=\{a_{j_1}, a_{j_2}, \cdots, a_{j_k}\}$$

则

$$f(A_1\cup A_2)=f(\{a_{i_1}, a_{i_2}, \cdots, a_{i_k}, a_{j_1}, a_{j_2}, \cdots, a_{j_k}\})$$

$$=\{b_{i_1}, b_{i_2}, \cdots, b_{i_k}, b_{j_1}, b_{j_2}, \cdots, b_{j_k}\}$$

$$=\{b_{i_1}, b_{i_2}, \cdots, b_{i_k}\}\cup\{b_{j_1}, b_{j_2}, \cdots, b_{j_k}\}$$

$$=f(A_1)\cup f(A_2)$$

又，$\forall A_1\in P(A)$，若$A_1=\varnothing$，则

$$f(\sim A_1)=f(A)=B=\sim f(A_1)$$

若$A_1\neq\varnothing$，设$A_1=\{a_{i_1}, a_{i_2}, \cdots, a_{i_k}\}$，则

$$f(\sim A_1)=f(\{a_i|\ i\in\{1, 2, \cdots, n\},\ i\notin\{i_1, i_2, \cdots, i_k\}\})$$

$$=\{b_i|i\in\{1, 2, \cdots, n\}, i\notin\{i_1, i_2, \cdots i_k\}\}$$

$$=\sim\{b_{i_1},b_{i_2},\cdots,b_{i_k}\}$$

$$=\sim f(A_1)$$

因此，f 保持∪与～，故是布尔同态，从而是布尔同构. ▌

习 题 七

1．证明定理 5．

2．设 B_1，B_2是两个布尔代数，f是 B_1到 B_2的布尔同态，证明$f(B_1)$是 B_2的子布尔代数.

*§ 8　有限布尔代数的结构

设 S 是一个非空集合，在布尔代数 $P(S)$ 中，形如 $\{a\}$ 的单元素集合是 $P(S)$ 中的极小非 0 元素，它们可以看成是 $P(S)$ 的基本元素，$P(S)$ 中的任何非零元素均可由这类元素求并得到，例如，设 $\{a, b, c\} \in P(S)$，则 $\{a\}, \{b\}, \{c\} \in P(S)$ 且 $\{a, b, c\} = \{a\} \cup \{b\} \cup \{c\}$. 一般地，引入下述定义.

定义 1　设 B 是一个布尔代数，$a \in B$，如果 a 盖住 0（或说 a 是 0 的直接前辈），即 $a \neq 0$ 且不存在 b 使 $0 < b < a$，则称 a 是 B 的原子.

例如，在图 8.1（a）所示的布尔代数中，d，e，f是原子；在图 8.1（b）所示布尔代数中，a，b 是原子；在 S 的幂集代数 $P(S)$ 中，$a \in S$ 构成的单元素集合 $\{a\}$ 是原子.

(a)　　（b）

图 8.1

先来研究原子的性质.

定理 1　设 B 是一布尔代数，$a \in B$ 是原子，则 $\forall x \in B$，$a * x = a$ 或 $a * x = 0$.

证明　因为 $0 \leqslant a * x \leqslant a$，若 $a * x \neq 0$ 且 $a * x \neq a$，则 $0 < a * x < a$ 与 a 是原子矛盾，故 $a * x = a$ 或 $a * x = 0$. ▌

定理 2　设 B 是一个布尔代数，a，$b \in B$ 是两个原子，如果 $a \neq b$，则 $a * b = 0$.

证明　若 $a * b \neq 0$，因为 a 是原子，则 $a * b = a$，又因为 b 是原子，则 $a * b = b$，

故 $a=b$，矛盾，因而 $a*b=0$. ▌

定理 3　设 B 是一个布尔代数，$a\in B$ 是原子，则对任意 $b\in B$，

$$a\leqslant b \qquad a\leqslant b'$$

中恰有一个成立.

证明　因为 a 是原子，故 $a*b=0$ 或 $a*b=a$，若 $a*b=a$，则 $a\leqslant b$，若 $a*b=0$，则

$$a*b'=(a*b')\oplus 0=(a*b')\oplus(a*b)=a*(b'\oplus b)=a$$

即 $a\leqslant b'$. 所以，无论何种情况，$a\leqslant b$ 与 $a\leqslant b'$ 必有一个成立，若它们同时成立，则

$$a\leqslant b*b'=0$$

矛盾，因此，$a\leqslant b$ 与 $a\leqslant b'$ 恰有一个成立. ▌

定理 4　设 B 是一个有限布尔代数，则对任何非零元素 $x\in B$，必存在原子 $a\in B$ 使 $a\leqslant x$.

证明　若 x 是原子，取 $a=x$ 即可，若 x 不是原子，则必有 $x_1\in B$ 使

$$0<x_1<x$$

若 x_1 是原子，取 $a=x_1$ 即可，若 x_1 不是原子，则必有 $x_2\in B$ 使

$$0<x_2<x_1<x$$

……一直进行下去. 由于 B 是有限布尔代数，上述过程一定在某步终止，即存在 $i\in\mathbf{N}$ 使

$$0<x_i<x_{i-1}<\cdots<x_1<x$$

且 x_i 是原子，取 $a=x_i$，则 a 是原子且 $a\leqslant x$. 定理得证. ▌

基于原子的以上性质，下面通过对有限布尔代数建立一系列定理来揭示其结构.

引理　设 B 是一个布尔代数，a，$b\in B$，则

$$a\leqslant b \Leftrightarrow a*b'=0 \Leftrightarrow a'\oplus b=1$$

证明　由 Morgan 律易见 $a*b'=0\Leftrightarrow a'\oplus b=1$. 下面只需证明

$$a\leqslant b \Leftrightarrow a*b'=0$$

若 $a\leqslant b$，则 $a=a*b$，故 $a*b'=a*b*b'=0$.

反之，若 $a*b'=0$，则

$$a*b=(a*b)\oplus(a*b')=a*(b\oplus b')=a,$$

从而 $a\leqslant b$. 所以 $a\leqslant b \Leftrightarrow a*b'=0$. ▌

定理 5　设 B 是有限布尔代数，$b\in B$ 且 $b\neq 0$，若 a_1，a_2，…，a_n 是 B 中所有小于等于 b 的原子，则 $b=a_1\oplus a_2\oplus\cdots\oplus a_n$.

证明　记 $a=a_1\oplus a_2\oplus\cdots\oplus a_n$，由于 $a_i\leqslant b$（$i=1$，2，…，n）易知

$$a=a_1\oplus a_2\oplus\cdots\oplus a_n\leqslant b,$$

下证 $b\leqslant a$. 根据引理，只需证明 $b*a'=0$. 用反证法，若 $b*a'\neq 0$，则必有原子 c 使 $c\leqslant b*a'$

由于 $b*a'\leqslant b$，$b*a'\leqslant a'$

故由传递性知

$$c\leqslant b,\qquad c\leqslant a'$$

由于 $a_1, a_2 \cdots, a_n$ 是所有小于等于 b 的原子，且原子 c 满足 $c \leqslant b$，因此，c 必定是 $a_1, a_2, \cdots, a_n$ 中的一个，即存在 $i \in \{1, 2 \cdots, n\}$ 使 $c = a_i$，从而 $c \leqslant a_1 \oplus a_2 \oplus \cdots \oplus a_n = a$，而我们已知 $c \leqslant a'$，故 $c \leqslant a * a' = 0$，矛盾，所以 $b * a' = 0$，即 $b \leqslant a$.

总之，我们证明了 $a \leqslant b$ 且 $b \leqslant a$，因此 $b = a = a_1 \oplus a_2 \oplus \cdots \oplus a_n$ ▌

对于布尔代数 B 中的元素 b，如果存在原子 a_1，a_2，…，a_n 使

$$b = a_1 \oplus a_2 \oplus \cdots \oplus a_n$$

我们把 $a_1 \oplus a_2 \oplus \cdots \oplus a_n$ 称作 b 的原子表达式.

定理 6　设 B 是有限布尔代数，b 是 B 中的非零元素，a_1，a_2，…，a_n 是 B 中所有小于等于 b 的原子，若不考虑原子的顺序，则

$$b = a_1 \oplus a_2 \oplus \cdots \oplus a_n$$

是 b 的唯一原子表达式.

证明　任取 b 的一个原子表达式

$$b = b_1 \oplus b_2 \oplus \cdots \oplus b_k$$

我们证明该表达式与 $a_1 \oplus a_2 \oplus \cdots \oplus a_n$ 是相同的，即证

$$\{b_1, b_2, \cdots, b_k\} = \{a_1, a_2, \cdots, a_n\}$$

令 $A_1 = \{a_1, a_2, \cdots, a_n\}$，$B_1 = \{b_1, b_2, \cdots, b_k\}$，$\forall a_i \in A_1$，若 $a_i \notin B_1$，则

$$a_i * b = a_i * (b_1 \oplus b_2 \oplus \cdots \oplus b_k) = 0, \text{ 但 } a_i * b = a_i * (a_1 \oplus a_2 \oplus \cdots \oplus a_n) = a_i$$

矛盾，故必有 $a_i \in B_1$，因此 $A_1 \subseteq B_1$，同理 $B_1 \subseteq A_1$，从而 $A_1 = B_1$，得证. ▌

有了以上准备以后，我们来讨论有限布尔代数的结构.

设 B 是一个有限布尔代数，M 是 B 中所有原子构成的集合，根据定理 6，B 中任何非零元素 b 总可唯一表成一个原子表达式

$$b = a_1 \oplus a_2 \oplus \cdots \oplus a_n$$

其中，a_1，a_2，…，a_n 是所有小于等于 b 的原子. 通过这种方式，由 b 唯一确定了 M 的一个非空子集 $\{a_1, a_2, \cdots, a_n\}$，我们便建立起了 B 的非零元与 M 的非空子集之间的一个对应关系. 若补充规定 B 的零元对应 M 的子集 $\varnothing$，则我们得到一个 B 与 $P(M)$ 之间的一一映射(双射). 进一步地，我们将证明这个一一映射是 B 到 $P(M)$ 的布尔同构.

定理 7 (Stone)　设 $\langle B, \oplus, *, ', 0, 1 \rangle$ 是一个有限布尔代数，M 是 B 的原子集合，则 $\langle B, \oplus, *, ', 0, 1 \rangle \cong \langle P(M), \cup, \cap, \sim, \varnothing, M \rangle$.

证明　令 $f: B \to P(M)$

$$f(x) = \{a \mid a \in M, a \leqslant x\} = \begin{cases} \phi & x = 0 \\ \{a_1, a_2, \cdots, a_k\} & x = a_1 \oplus a_2 \oplus \cdots \oplus a_k \end{cases}$$

其中，a_1，a_2，…，a_k 是原子.

易证 f 是一一映射，下面证明 f 是同态.

$\forall\ b, c \in B$，若 $b = 0$ 或 $c = 0$，则显然 $f(b \oplus c) = f(b) \cup f(c)$，下设 $b \neq 0$，$c \neq 0$，于是可令

$$b=b_1\oplus b_2\oplus\cdots\oplus b_k$$
$$c=c_1\oplus c_2\oplus\cdots\oplus c_m$$

其中 b_i，$c_j\in M$，$i=1$，2，…，k；$j=1$，2，…，m.

因此，　$b\oplus c=b_1\oplus b_2\oplus\cdots\oplus b_k\oplus c_1\oplus c_2\oplus\cdots\oplus c_m$

所以，　$f(b\oplus c)=\{b_1,\ b_2,\ \cdots,\ b_k,\ c_1,\ c_2,\ \cdots,\ c_m\}$

$$=\{b_1,\ b_2,\ \cdots,\ b_k\}\cup\{c_1,\ c_2,\ \cdots,\ c_m\}$$
$$=f(b)\cup f(c)$$

下面再证 $f(b')=\sim f(b)$

$$a\in f(b')\Leftrightarrow\ a\in M,\ a\leq b'$$
$$\Leftrightarrow\ a\in M,\ a\not\leq b$$
$$\Leftrightarrow\ a\in M,\ a\notin f(b)$$
$$\Leftrightarrow\ a\in\sim f(b)$$

故　$f(b')=\sim f(b)$.

总之，f 既是一一映射又能保持运算$\{\oplus,'\}$，故是 B 到 $P(M)$的布尔同构，因此有 $B\cong P(M)$. ▌

推论 1　有限布尔代数的元素个数必为 2^n，其中 n 是 B 的原子个数.

推论 2　元素个数相等的有限布尔代数必定同构.

读者自证.

习 题 八

1. 证明定理 7 中定义的映射 f 满足 $f(a*b)=f(a)\cap f(b)$.
2. 设 S_{210} 是 210 的所有正因子构成的集合，D 是 S_{210} 上的整除关系，画出〈S_{210}，D〉的 Hasse 图.

§ 9　布尔表达式

本节将研究定义在布尔代数 B（严格地说是 B^n）上的一类特殊的函数——布尔函数，为此，先定义布尔表达式.

定义 1　设 B 是一个布尔代数，x_1，x_2，…，x_n 是 B 上的变量，B 上由 x_1，x_2，…，x_n 生成的布尔表达式归纳定义如下：

（1）　B 中的元素是 B 上由 x_1，x_2，…，x_n 生成的布尔表达式.

（2）　B 上的任一变量 x_i（$i=1$，2，…，n）是 B 上由 x_1，x_2，…，x_n 生成的布尔表达式.

（3）如果 α，β 是 B 上由 x_1，x_2，…，x_n 生成的布尔表达式. 则 $\alpha\oplus\beta$，$\alpha*\beta$，α'（必要时加括号）是 B 上由 x_1，x_2，…，x_n 生成的布尔表达式.

（4）只有通过有限次使用（1），（2），（3）得到的符号串是 B 上由 x_1，$x_2\cdots,x_n$ 生成的布尔表达式.

例 1　设 $A=\{a,\ b\}$，x_1，x_2，x_3 是 $P(A)$ 上的变量，则符号串 $\varnothing$，$\{a\}$，x_1，$x_1\cup\{a\}$，$x_1\cap x_2$，$\sim(x_2\cup x_3)\cap\{b\}$ 均是 $P(A)$ 上由 x_1，x_2，x_3 生成的布尔表达式. B 上由 x_1，x_2，…，x_n 生成的布尔表达式可记为 $f(x_1,\ x_2,\ \cdots,\ x_n)$，由定义可见，布尔表达式只是一个形式符号串，但是，如果其中变量 x_1，x_2，…，x_n 取定为 B 上的一组值 a_1，a_2，…，a_n，从表达式 $f(a_1,\ a_2,\ \cdots,\ a_n)$ 可计算出一个值，这个值是 B 中的元素，换言之，给定一个有序 n 元组 $\langle a_1,\ a_2,\ \cdots,\ a_n\rangle\in B^n$，通过布尔表达式 $f(x_1,\ x_2,\ \cdots,\ x_n)$ 可唯一确定 B 中的一个元素 $f(a_1,\ a_2,\ \cdots,\ a_n)$，因此，$f(x_1,\ x_2,\ \cdots,\ x_n)$ 可视为 B^n 到 B 的映射，这时，称 $f(x_1,\ x_2,\ \cdots,\ x_n)$ 为布尔函数.

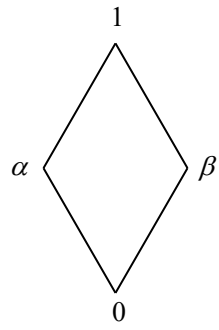


图 9.1

例 2　设 $B=\{0,\ \alpha,\ \beta,\ 1\}$ 是由图 9.1 确定的布尔代数，$f(x,\ y)$ 是 B 上的布尔函数.

$f(x,\ y)=(\beta*x'*y)\oplus(\beta*x*(x\oplus y)'\ )\oplus(\alpha*(x'*y))$

于是，

$$f(0,\ 0)=(\beta*1*0)\oplus(\beta*0*(0\oplus 0)'\ )\oplus(\alpha*(1*0))$$
$$=0$$
$$f(1,\ 0)=(\beta*0*0)\oplus(\beta*1*(1\oplus 0)'\ )\oplus(\alpha*(0*0))$$
$$=0$$
$$f(\alpha,\ \beta)=(\beta*\beta*\beta)\ \oplus\ (\beta*\alpha*(\alpha\oplus\beta)'\ )\ \oplus\ (\beta*(\beta*\beta))$$
$$=\beta$$

为了更深入地研究布尔函数，我们希望把布尔函数化成一种标准形式，为此，先引进如下概念.

定义 2　设 B 是一个布尔代数，x_1，x_2，…，x_n 是 B 上的变量，形如 $\tilde{x}_1*\tilde{x}_2*\cdots*\tilde{x}_n$ 的布尔表达式称为 x_1，x_2，…，x_n 生成的极小项，其中，$\tilde{x}_i=x_i$ 或 x_i'.

例如，$x_1*x_2'*x_3'$ 是由 x_1，x_2，x_3 生成的极小项，但不是 x_1，x_2 生成的极小项，也不是 x_1，x_2，x_3，x_4 生成的极小项，$x_1*x_3'*x_2$ 是由 x_1，x_3，x_2 生成的极小项，但不是 x_1，x_2，x_3 生成的极小项.

为了表示的方便，我们下面给出极小项的一种编码方式.

设 x_1，x_2，…，x_n 是布尔代数 B 上的变量，对极小项 $\tilde{x}_1*\tilde{x}_2*\cdots*\tilde{x}_n$，　令

$$\delta_i=\begin{cases}0 & \tilde{x}_i=x_i' \\ 1 & \tilde{x}_i=x_i\end{cases}\qquad i=1,2,\cdots,n$$

则相应得到一个 n 位二进制数 $\delta_1\delta_2\cdots\delta_n$. 按照这种方式，我们就在 x_1，x_2，…，x_n 生成的极小项与 n 位二进制数之间建立了一个一一对应关系，例如，极小项 $x_1'*x_2'*x_3$ 对应二进制数 0 0 1，极小项 $x_1*x_2*x_3'$ 对应二进制数 1 1 0．另一方面，二进制数 1 0 1 对应极小项 $x_1*x_2'*x_3$，二进制数 0 0 0 对应极小项 $x_1'*x_2'*x_3'$.

对于极小项 $\tilde{x}_1*\tilde{x}_2*\cdots*\tilde{x}_n$，如果它对应的二进制数为 $\delta_1\delta_2\cdots\delta_n$，则将其用

$m_{\delta_1\delta_2\cdots\delta_n}$ 表示，为了书写方便，常将 $m_{\delta_1\delta_2\cdots\delta_n}$ 写成 m_i，这里，i 是 $\delta_1\delta_2\cdots\delta_n$ 的十进制形式．例如，设 x_1，x_2，x_3，x_4 是布尔代数 B 上的变量，由这四个变量生成的极小项

$$m_8=m_{1000}=x_1*x_2'*x_3'*x_4'$$
$$m_3=m_{0011}=x_1'*x_2'*x_3*x_4$$
$$m_0=m_{0000}=x_1'*x_2'*x_3'*x_4'$$

定理 1　设 x_1，x_2，…，x_n 是布尔代数 B 上的 n 个变量，由 x_1，x_2，…，x_n 生成的极小项具有如下性质

（1）　极小项共有 2^n 个

（2）　$m_i*m_j=\begin{cases}m_i & i=j\\ 0 & i\neq j\end{cases}$

（3）　$\bigoplus_{i=0}^{2^n-1} m_i=1$

证明

（1）　由极小项与 n 位二进制数的一一对应关系，即知极小项共有 2^n 个.

（2）　设　$m_i=m_{\delta_1\delta_2\cdots\delta_n}=\tilde{x}_1*\tilde{x}_2*\cdots*\tilde{x}_n$

$$m_j=m_{\lambda_1\lambda_2\cdots\lambda_n}=\hat{x}_1*\hat{x}_2*\cdots*\hat{x}_n$$

若 $i=j$，则由幂等律知 $m_i*m_j=m_i*m_i=m_i$，若 $i\neq j$，则 i 与 j 的二进制表示必不相同，不妨设 $\delta_k\neq\lambda_k$，于是 $\tilde{x}_k=(\hat{x}_k)'$，故 $\tilde{x}_k*\hat{x}_k=0$，所以

$$m_i*m_j=\tilde{x}_1*\tilde{x}_2*\cdots*\tilde{x}_n*\hat{x}_1*\hat{x}_2*\cdots*\hat{x}_n=\tilde{x}_k*\hat{x}_k*\cdots=0$$

（3）　用归纳法，当 $n=1$ 时，

$$\bigoplus_{i=0}^{2^n-1} m_i=m_0\oplus m_1=x_1'\oplus x_1=1$$

设当 $n=k$ 时（3）成立，下证 $n=k+1$ 时（3）也成立.

因在极小项 $m_i=m_{\delta_1\delta_2\cdots\delta_{k+1}}=\tilde{x}_1*\tilde{x}_2*\cdots*\tilde{x}_{k+1}$ 中去掉 $\tilde{x}_{k+1}$ 就得到一个由 x_1，x_2，…，x_k 生成的极小项 $\overline{m}_i=\overline{m}_{\delta_1\delta_2\cdots\delta_k}=\tilde{x}_1*\tilde{x}_2*\cdots*\tilde{x}_k$（为了区别于 x_1，x_2，…，x_{k+1} 生成的极小项，x_1，x_2，…，x_k 生成的极小项用 $\overline{m}_i=\overline{m}_{\delta_1\delta_2\cdots\delta_k}$ 表示），故

$$\begin{aligned}\bigoplus_{i=0}^{2^{k+1}-1} m_i &= (m_{00\cdots00}\oplus m_{00\cdots10}\oplus\cdots\oplus m_{11\cdots10})\oplus(m_{00\cdots01}\oplus m_{00\cdots11}\oplus\cdots\oplus m_{11\cdots11})\\ &= [(\overline{m}_{00\cdots0}\oplus\overline{m}_{00\cdots1}\oplus\cdots\oplus\overline{m}_{11\cdots1})*x'_{k+1}]\\ &\quad\oplus[(\overline{m}_{00\cdots0}\oplus\overline{m}_{00\cdots1}\oplus\cdots\oplus\overline{m}_{11\cdots1})*x_{k+1}]\\ &= [(\bigoplus_{i=0}^{2^k-1}\overline{m}_i)*x'_{k+1}]\oplus[(\bigoplus_{i=0}^{2^k-1}\overline{m}_i)*x_{k+1}]\\ &= (1*x'_{k+1})\oplus(1*x_{k+1})\\ &= 1\end{aligned}$$

即当 $n=k+1$ 时（3）成立，由归纳法，（3）对任何正整数 n 均成立. ▌

利用极小项，我们可以给出布尔表达式的一种标准形式——积和范式.

定义 3　设 B 是布尔代数，$\alpha_i\in B$（$i=0$，1，…，2^n-1），x_1，x_2，…，x_n 是 B 上的变量，形如

$$\bigoplus_{i=0}^{2^n-1}(\alpha_i * m_i)$$

的布尔表达式称为由 x_1，x_2，…，x_n 生成的积和范式（极小项范式），α_i（$i=0,1,\cdots,2^n-1$）称为积和范式的系数.

定理 2　设 α，β 是两个积和范式，则

$$\alpha\oplus\beta,\qquad \alpha*\beta,\qquad \alpha'$$

均可化为积和范式（在函数相等意义下）.

证明　设　$\alpha=\bigoplus_{i=0}^{2^n-1}(\alpha_i * m_i)$

$$\beta=\bigoplus_{i=0}^{2^n-1}(\beta_i * m_i)$$

则　$\alpha\oplus\beta=\bigoplus_{i=0}^{2^n-1}[(\alpha_i * m_i)\oplus(\beta_i * m_i)]$

$$=\bigoplus_{i=0}^{2^n-1}[(\alpha_i\oplus\beta_i)*m_i]$$

$$\alpha * \beta = [\bigoplus_{i=0}^{2^n-1} (\alpha_i * m_i)] * [\bigoplus_{j=0}^{2^n-1} (\beta_j * m_j)]$$

$$= \bigoplus_{i,j=0}^{2^n-1} (\alpha_i * \beta_j * m_i * m_j)$$

$$= \bigoplus_{i=0}^{2^n-1} (\alpha_i * \beta_i * m_i)$$

即 $\alpha \oplus \beta$，$\alpha * \beta$ 均可化为积和范式.

又，
$$[\bigoplus_{i=0}^{2^n-1} (\alpha_i * m_i)] \oplus [\bigoplus_{i=0}^{2^n-1} (\alpha_i' * m_i)]$$
$$= \bigoplus_{i=0}^{2^n-1} (\alpha_i \oplus \alpha_i') * m_i$$
$$= 1$$
$$[\bigoplus_{i=0}^{2^n-1} (\alpha_i * m_i)] * [\bigoplus_{i=0}^{2^n-1} (\alpha_i' * m_i)]$$
$$= \bigoplus_{i=0}^{2^n-1} (\alpha_i * \alpha_i' * m_i)$$
$$= 0$$

故知 $[\bigoplus_{i=0}^{2^n-1} (\alpha_i * m_i)]' = \bigoplus_{i=0}^{2^n-1} (\alpha_i' * m_i))$. 即 α' 可化为积和范式. ▌

定理 3　布尔代数 B 上任一布尔表达式 $f(x_1, x_2, \cdots, x_n)$ 均可化为积和范式，且

$$f(x_1, x_2, \cdots, x_n) = \bigoplus_{i=0}^{2^n-1} f(i_1, i_2, \cdots, i_n) * m_i$$

其中，$(i_1\ i_2 \cdots i_n)$ 是 i 的二进制形式.

证明　根据布尔表达式的归纳定义，用所谓“结构归纳法”进行证明.

（1）若 $f(x_1, x_2, \cdots, x_n)$ 是 B 的元素，设

$$f(x_1, x_2, \cdots, x_n) = a$$

则
$$f(x_1, x_2, \cdots, x_n) = a * 1$$
$$= a * \bigoplus_{i=0}^{2^n-1} m_i$$
$$= \bigoplus_{i=0}^{2^n-1} (a * m_i)$$
$$= \bigoplus_{i=0}^{2^n-1} f(i_1, i_2, \cdots, i_n) * m_i.$$

（2）若 $f(x_1, x_2, \cdots, x_n)$ 是 B 上的变量 $x_1, x_2, \cdots, x_n$ 之一，设

$$f(x_1, x_2, \cdots, x_n) = x_k$$

则　　$f(x_1, x_2, \cdots, x_n)$

$$=x_k * 1$$

$$=x_k * \bigoplus_{i=0}^{2^n-1} m_i$$

$$= \bigoplus_{i=0}^{2^n-1} (x_k * m_i)$$

$$= \bigoplus_{i=0}^{2^n-1} (x_k * m_{i_1 i_2 \ldots i_n})$$

其中，$(i_1\ i_2 \cdots\ i_n)$是 i 的二进制形式，由于 x_k 是变量而不是 B 中的元素，上式还不是一个积和范式，还需进一步变换，令

$$m_{i_1 i_2 \ldots i_n} = \tilde{x}_1 * \tilde{x}_2 * \cdots * \tilde{x}_n$$

则　$x_k * m_{i_1 i_2 \ldots i_n} = x_k * \tilde{x}_1 * \tilde{x}_2 * \cdots * \tilde{x}_k * \cdots * \tilde{x}_n$

$$= \begin{cases} 0 & i_k = 0 \quad (\text{即} \tilde{x}_k = x_k') \\ m_i & i_k = 1 \quad (\text{即} \tilde{x}_k = x_k) \end{cases}$$

$$= i_k * m_i$$

于是　　$f(x_1, x_2, \cdots, x_n) = \bigoplus_{i=0}^{2^n-1} (x_k * m_{i_1 i_2 \ldots i_n})$

$$= \bigoplus_{i=0}^{2^n-1} (i_k * m_i)$$

$$= \bigoplus_{i=0}^{2^n-1} f(i_1, i_2, \cdots, i_k) * m_i .$$

（3）若 $h(x_1, x_2, \cdots, x_n)$，$g(x_1, x_2, \cdots, x_n)$ 可化为定理中的积和范式，由定理 1 易证

$h(x_1, x_2, \cdots, x_n) \oplus g(x_1, x_2, \cdots, x_n)$，　$h(x_1, x_2, \cdots, x_n) * g(x_1, x_2, \cdots, x_n)$，$h(x_1, x_2, \cdots, x_n)'$ 均可化为定理中的积和范式．这样一来，根据布尔表达式的定义，任何布尔表达式均可化为积和范式．▌

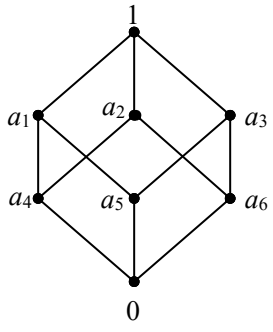


图 9.2

例 3　设 B 是由图 9.2 决定的布尔代数，$f(x, y)$，$g(x, y)$ 是由 x，y 生成的布尔函数

$f(x, y) = (x * a_1)' \oplus ((y \oplus a_3)' * a_4)'$

$g(x, y) = (x * a_1) * (x' \oplus a_4) * a_1$

求 $f(x, y)$ 与 $g(x, y)$ 的积和范式．

因为

$f(0, 0) = (0 * a_1)' \oplus ((0 \oplus a_3)' * a_4)' = 1$

$f(0,\ 1)=(0*a_1)'\oplus((1\oplus a_3)'*a_4)'=1$

$f(1,\ 0)=(1*a_1)'\oplus((0\oplus a_3)'*a_4)'=a_3$

$f(1,\ 1)=(1*a_1)'\oplus((1\oplus a_3)'*a_4)'=1$

故

$$\begin{aligned}f(x,y)&=(f(0,\ 0)*m_0)\oplus(f(0,\ 1)*m_1)\\&\quad\oplus(f(1,\ 0)*m_2)\oplus(f(1,\ 1)*m_3)\\&=m_0\oplus m_1\oplus(a_3*m_2)\oplus m_3\end{aligned}$$

因为

$g(0,\ 0)=(0*a_1)*(1\oplus a_4)*a_1=0$

$g(0,\ 1)=(0*a_1)*(1\oplus a_4)*a_1=0$

$g(1,\ 0)=(1*a_1)*(0\oplus a_4)*a_1=a_4$

$g(1,\ 1)=(1*a_1)*(0\oplus a_4)*a_1=a_4$

故

$$\begin{aligned}g(x,y)&=(g(0,\ 0)*m_0)\oplus(g(0,\ 1)*m_1)\\&\quad\oplus(g(1,\ 0)*m_2)\oplus(g(1,\ 1)*m_3)\\&=(a_4*m_2)\oplus(a_4*m_3)\end{aligned}$$

例 4　设 B 是由图 9.2 决定的布尔代数，$f(x,y)$ 是 B 上的布尔函数，满足

$f(0,\ 0)=a_1$，　$f(0,\ 1)=0$，　$f(1,\ 0)=a_3$，　$f(1,\ 1)=1$

求 $f(a_1,\ a_2)$，$f(1,\ a_3)$ 的值.

因为 $f(x,y)$ 是布尔函数，所以

$$\begin{aligned}f(x,y)&=(f(0,\ 0)*m_0)\oplus(f(0,\ 1)*m_1)\oplus(f(1,\ 0)*m_2)\\&\quad\oplus(f(1,\ 1)*m_3)\\&=(a_1*m_0)\oplus(a_3*m_2)\oplus m_3\\&=(a_1*x'*y')\oplus(a_3*x*y')\oplus(x*y)\end{aligned}$$

因此
$$\begin{aligned}f(a_1,\ a_2)&=(a_1*a_1'*a_2')\oplus(a_3*a_1*a_2')\oplus(a_1*a_2)\\&=a_1\end{aligned}$$

$$\begin{aligned}f(1,\ a_3)&=(a_1*1'*a_3')\oplus(a_3*1*a_3')\oplus(1*a_3)\\&=a_3\end{aligned}$$

例 5　设 B 是图 9.2 决定的布尔代数，f 是 $B\times B$ 到 B 的函数，满足

$f(0,\ 0)=1$，　$f(0,\ 1)=0$，　$f(1,\ 0)=a_1$，

$f(1,\ 1)=0$，　$f(a_1,\ a_2)=a_4$

问　f 是否是 B 上的布尔函数?

若 f 是 B 上的布尔函数，则

$$\begin{aligned}f(x,y)&=(f(0,\ 0)*m_0)\oplus(f(0,\ 1)*m_1)\\&\quad\oplus(f(1,\ 0)*m_2)\oplus(f(1,\ 1)*m_3)\\&=m_0\oplus(a_1*m_2)\\&=(x'*y')\oplus(a_1*x*y')\end{aligned}$$

因此　$f(a_1, a_2) = (a_1' * a_2') \oplus (a_1 * a_1 * a_2') = 0 \oplus a_5 = a_5$

但是，由题设，$f(a_1, a_2) = a_4$. 矛盾，故f不是布尔函数.

定理 3 表明，一个布尔函数$f(x_1, x_2, \cdots, x_n)$可由其在〈0，0，…，0〉，〈0，0，…，1〉，…，〈1，1，…，1〉这 2^n个点处的值完全确定，就象一条直线可由直线上两点决定一样——尽管一条直线上有无穷多个点.

对有限布尔代数 B，我们已经知道，B^n到 B 的函数共$|B|^{|B|^n}$个，那么，其中有多少个是布尔函数呢？

由上所述，B 上的一个布尔函数$f(x_1, x_2, \cdots, x_n)$总可以表示成一个积和范式：

$f(x_1, x_2, \cdots, x_n) = \bigoplus_{i=0}^{2^n-1} (\alpha_i * m_i)$，因而易知，$B$ 上的 n 元布尔函数$f(x_1, x_2, \cdots, x_n)$与 B 上的 2^n元有序组〈$\alpha_0, \alpha_1, \cdots, \alpha_{2^n-1}$〉一一对应，由于其中每个$\alpha_i$均有$|B|$种选择，故 2^n元组〈$\alpha_0, \alpha_1, \cdots, \alpha_{2^n-1}$〉共有$|B|^{2^n}$个，从而 B 上的 n 元布尔函数共有$|B|^{2^n}$个.

与上面的讨论完全类似地，我们还可引进布尔函数的另一标准形式——和积范式.

定义 4　设 B 是一个布尔代数，$x_1, x_2, \cdots, x_n$是 B 上的变量，形如 $\tilde{x}_1 \oplus \tilde{x}_2 \oplus \cdots \oplus \tilde{x}_n$的布尔表达式称为 $x_1, x_2, \cdots, x_n$生成的极大项，其中，$\tilde{x}_i = x_i$ 或 x_i'.

极大项$\tilde{x}_1 \oplus \tilde{x}_2 \oplus \cdots \oplus \tilde{x}_n$用$\tilde{m}_{\delta_1\delta_2\cdots\delta_n}$表示，其中

$$\delta_i = \begin{cases} 1 & \tilde{x}_i = x_i' \\ 0 & \tilde{x}_i = x_i \end{cases} \qquad i = 1, 2, \cdots, n$$

$\tilde{m}_{\delta_1\delta_2\cdots\delta_n}$也可写成$\tilde{m}_i$，其中，$i$ 是($\delta_1\ \delta_2 \cdots\ \delta_n$)的十进制形式.

定义 5　设 B 是布尔代数，$x_1, x_2, \cdots, x_n$是 B 上的变量，形如

$$\mathop{*}_{i=0}^{2^n-1} (\alpha_i \oplus m_i)$$

的布尔表达式称为由 $x_1, x_2, \cdots, x_n$生成的和积范式，其中，$\alpha_i \in B (i = 0, 1, \cdots, 2^n - 1)$.

同积和范式的讨论完全类似，可以证明，任何布尔函数$f(x_1, x_2, \cdots, x_n)$均可化为和积范式，且

$$f(x_1, x_2, \cdots, x_n) = \mathop{*}_{i=0}^{2^n-1} (f(i_1, i_2, \cdots, i_n) \oplus \tilde{m}_i).$$

其中，($i_1\ i_2 \cdots\ i_n$) 是 i 的二进制形式.

习 题 九

1．设 B 是由图 9.3 确定的布尔代数，$f(x, y, z)$ 是 B 上的布尔函数，

$$f(x, y, z) = (\alpha * x * y)' \oplus (x' * y' * \beta) \oplus ((z' * \beta)' \oplus (x * z))'$$

求 $f(x, y, z)$ 的积和范式 和 和积范式.

2．设 B 是由图 9.3 确定的布尔代数， f 是 $B \times B$ 到 B 的函数， 满足 $f(0, 0) = \alpha$, $f(0, 1) = 0$， $f(1, 0) = \beta$， $f(1, 1) = 1$ 试决定 $f(\alpha, 1)$ 使 f 不是布尔函数，这种决定共有多少种方式?

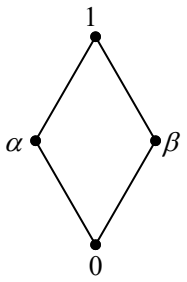


图 9.3

3．设 B 是图 9.3 确定的布尔代数，B 上满足 $f(0, 0) = 0$ 的布尔函数 $f(x, y)$ 共有多少个?

4．证明 当布尔代数 B 的元素多于 2 个时，必存在 B^n 到 B 的函数不是布尔函数.

5．设 B 是由图 9.3 决定的布尔代数，B 上由 x 生成的布尔函数有多少个? 试将它们全部写出来，B 到 B 的函数中，有几个不是布尔函数?

6．证明 对任何布尔函数 $f(x, y)$ 有

$$\begin{aligned} f(x, y) &= (x * f(1, y)) \oplus (x' * f(0, y)) \\ &= (x \oplus f(0, y)) * (x' \oplus f(1, y)). \end{aligned}$$

第三篇　图论与组合初步

图论起源于1736年Euler的一篇文章,这篇文章解决了Königsberg七桥问题，标志着图论的诞生，但在以后的200年中，图论发展比较缓慢，1936年Köning发表了第一本图论书籍——《有限图与无限图理论》,这部著作总结了图论二百年的重要成果，是图论发展的重要里程碑，此后，图论得到了重大发展.

近三十年来，由于计算机的广泛应用，图论在科学界异军突起，占有越来越重要的地位，图论在计算机科学、运筹学、电网络分析、化学、物理以及社会科学等方面取得了丰硕成果，比如在计算机科学领域，图论在算法、语言、数据库、网络理论、开关理论、操作系统、人工智能等方面都有重大贡献.

本篇将仅限于介绍图论的基本概念、基本理论及一些重要算法，旨在为今后研究计算机科学与工程打下基础,学习本篇内容仅要求读者具有线性代数及集合论的基础知识，但由于图论自身的特点，还要求读者具有良好的数学机敏性.

组合论是算法分析的基础，本篇在主要讨论图论的同时，简要介绍组合论中的一些初步概念与基本技巧.

第八章　基本概念

§1　图

1736 年 Euler 研究了所谓 Königsberg 七桥问题.

在 Königsberg 城有一条河(Pregel 河)，河中有两个岛屿，从而，这条河就把陆地分成了 A、B、C、 D四部分，这四部分陆地由七桥座连接(见图 1.1(a)).

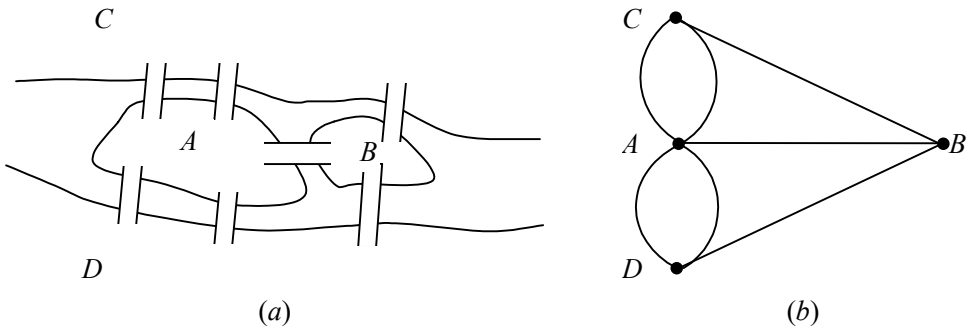


图 1.1

Königsberg 七桥问题就是说，能否从某点出发通过每桥恰好一次回到原地？

从问题的提法可见，各部分陆地的大小是无关仅要的，因此，我们不妨把每块陆地都视为一个点，于是就得到图 1.1(b). 从该图中可清楚地看到，与每点相连的桥都是奇数座，从任何一点出发，若想通过与该点相连的每桥恰好一次，都必须先“出”后“进”…最后必定是“出”，不可能最终回到出发点，因此，Königsberg 七桥问题的答案是否定的，Euler 解决这个问题的抽象与论证方法，导致了图论的诞生.

事实上，在科技领域或日常生活中，有许多问题都可以用由点和连接这些点的线构成的图形来表示，而在这些图形中，点的位置及线的形状是无关紧要的，重要的是图中有哪些点，哪些点之间有连线等，将这种图形进行数学抽象，就得到数学上图的概念.

定义 1　设 V 是一个非空集合，E 是一个 V 中元素的无序对构成的多重集，有序对 $G=\langle V, E\rangle$ 称为一个图，其中，V 称为顶点集，其元素称为顶点或点，E 称为边集，其元素称为边.

以上定义的图也称为无向图.

我们约定，由元素 u，v 构成的无序对用 uv 或（u，v）表示，也可用一个字母(通常是带或不带下标的 e)表示.

例 1　设 $V=\{v_1, v_2, v_3, v_4\}$，$E=\{v_1v_3, v_2v_4, v_4v_4, v_3v_4\}$　则 $G=\langle V, E\rangle$ 是一个图.

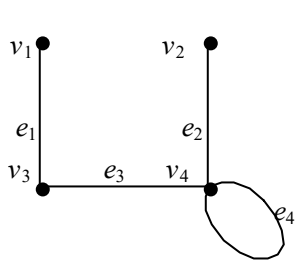
对任一图 G，总是用 $V(G)$表示 G 的顶点集，$E(G)$表示 G 的边集，一般不再特别说明.

为直观起见，一个图 G 可用一个图形表示：$V(G)$的元素用不重合的几何点表示，位置任意，当 $uv\in E(G)$且其重复度为 k 时，在 u，v 之间画 k 条连线表示这些边，其形状、长短不加考虑，这样得到的图形叫做图 G 的图示，图 1.2(a)即为例 1 中图的图示.

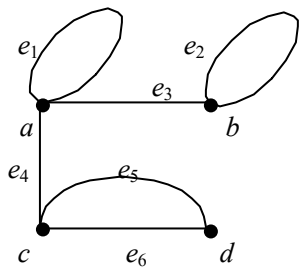
一个图与其图示从概念上来说并不是一回事，但二者是等同的，给定其中之一，另一个也就随之唯一确定，因此，我们将对图与其图示不加区别.

定义 2　设 G 是一个图，u，$v\in V(G)$，$e=uv\in E(G)$，称 u，v 为边 e 的端点，e 为连接 u，v 的边，并称顶点 u，v 与边 e 彼此关联.

例如，图 1.2(a)中，v_1，v_3 是 e_1 的端点，v_2，v_4 是 e_2 的端点，v_4 是 e_2，e_3，e_4 的端点；与 v_4 相关联的边是 e_2，e_3，e_4，与 v_3 相关联的边是 e_1，e_3，与 v_1，v_3 相关联的边是 e_1.



(a)



(b)

图 1.2

以上定义与图的图示有着显而易见的联系，事实上，图论中的大多数定义和概念都是根据图的这种表示形式提出的.

定义 3　在任意图中，同一条边关联的两点，称为相邻点，同一个点关联的诸边称为相邻边.

例如，图 1.2(a)中，v_1，v_3 是相邻的，v_1，v_4 不相邻，e_2，e_3，e_4 是相邻的，e_1，e_2 不相邻.

定义 4　设 G 是一个图，若 $e\in E(G)$的两端点重合为一点，即 $e=uu$，则称 e 为自环. 若 $uv\in E(G)$的重复度>1，则称 uv 是多重边.

例如，图 1.2(a)中 e_4 是自环，图 1.2(b)中 e_1，e_2 是自环，cd 是多重边.

这里，对相应于 cd 的每一条连线给予了不同的命名，这是允许的，也是自然的.

诸如图 1.2(b)中 e_5，e_6 这样的边，称为平行边.

定义 5　设 G 是一个图，$v\in V(G)$，与 v 相关联的边数(自环计算两次)称为 v 的度数，记为 $d_G(v)$或简记为 $d(v)$. 度数为 0 的点称为孤立点，度数为 1 的点称为悬挂点，度数为

奇数的点称为奇顶点，度数为偶数的点称为偶顶点.

图 G 中顶点的最小度数记为 $\delta(G)$，最大度数记为$\triangle(G)$，即

$$\delta(G)=\min\{d(v)\mid v\in V(G)\}$$

$$\triangle(G)=\max\{d(v)\mid v\in V(G)\}$$

$\delta(G)$与$\triangle(G)$也简记为 δ，$\triangle$.

例如，在图 1.2(*b*)中，$d(a)=4$，$d(b)=3$，$d(c)=3$，$d(d)=2$，$\delta=2$，$\triangle=4$.

定义 6　设 G 是图，若 $V(G)$，$E(G)$均是有限集，则称 G 为有限图.

本篇中所说的图均指有限图，并用 $\upsilon(G)$或 υ表示图 G 的点数，$\varepsilon(G)$或 ε表示图 G 的边数.

定理 1（握手引理）　对任一图 G，有 $\sum_{v\in V(G)}d(v)=2\varepsilon$.

证明　由于在计算度数时 G 中每条边均提供 2 度，故总度数必为边数的两倍，即

$$\sum_{v\in V(G)}d(v)=2\varepsilon.$$ ▌

推论　任意图中奇顶点的个数必为偶数.

证明　设 V_1，V_2 分别是图 G 的奇顶点、偶顶点构成的集合，则

$$\sum_{v\in V(G)}d(v)=\sum_{v\in V_1(G)}d(v)+\sum_{v\in V_2(G)}d(v)=2\varepsilon,$$

由于 V_2 中每一点的度数是偶数，故 $\sum_{v\in V_2(G)}d(v)$ 必是偶数，从而

$$\sum_{v\in V_1(G)}d(v)=2\varepsilon-\sum_{v\in V_2(G)}d(v)$$

是偶数，由于 $\sum_{v\in V_1(G)}d(v)$ 中每一项均是奇数，故该和式的项数必为偶数，即 G 中奇顶点数是偶数. ▌

例 2　在一次围棋比赛中，下过奇数盘棋的人数是偶数.

以参加比赛的人为顶点，若两人下过 n 盘棋则在相应的两顶点之间连 n 条边，这样便构成一个图，每人在比赛中下过的棋的盘数即为相应顶点的度数，由推论，该图中奇顶点数为偶数，即下过奇数盘棋的人数为偶数.

定义 7　设 G 是一个图

（1）　如果 $\upsilon=1$，$\varepsilon=0$，称 G 是平凡图.

（2）　如果 $\varepsilon=0$，称 G 是零图.

（3）　不含多重边和自环的图称为简单图.

（4）　含有多重边的图称为多重图.

定义 8　设 G 是一个简单图，如果 G 中任意两顶点之间均有边相连，则称 G 为完全图，具有 n 个顶点的完全图记为 K_n.

定义 9　设 G 是一个图，如果存在 $V(G)$的子集 V_1，V_2 使得　$V_1\cup V_2=V(G)$，

$V_1 \cap V_2 = \varnothing$，且 V_1 中任意两点不相邻，V_2 中任意两点也不相邻，则称 G 为二分图，并称 $\{V_1, V_2\}$ 为 G 的一个二划分，进一步地，若 V_1 中每一点皆与 V_2 中所有点相邻，则称 G 为完全二分图，且当 $|V_1|=m$，$|V_2|=n$ 时，将其记为 $K_{m,n}$.

例如，图 1.3(a)是零图，图 1.3(b)是简单图，图 1.3(c)是多重图，图 1.3(d)是完全图 K_5，图 1.3(e)是二分图，图 1.3(f)是完全二分图 $K_{3,2}$.

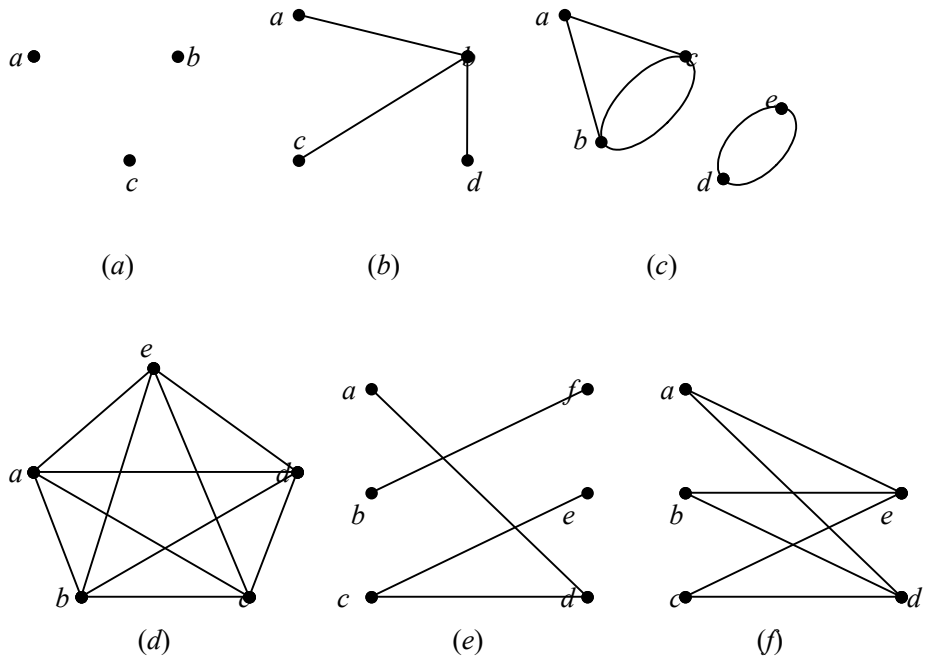


图 1.3

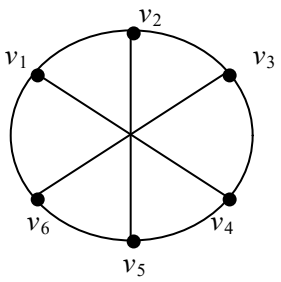


图 1.4

定义 10　设 G 是一个图，k 是一个常数，若 G 中每个顶点的度数均为 k，则称 G 为 k 次正则图.

图 1.4 是一个三次正则图.

类似于子集，我们也可以讨论子图的概念.

定义 11　设 G，H是两个图，如果 $V(H)\subseteq V(G)$，$E(H)\subseteq E(G)$，则称 H是 G 的子图，记为 $H\subseteq G$．若 $H\subseteq G$ 且 $H\neq G$ 称 H是 G 的真子图，记为 $H\subset G$．若 $H\subseteq G$ 且 $V(H)=V(G)$，称 H是 G 的生成子图．

例如，图 1.5(b)是图 1.5(a)的生成子图，图 1.5(c)是图 1.5(a)的子图，图 1.5(d)不是图 1.5(a)的子图．

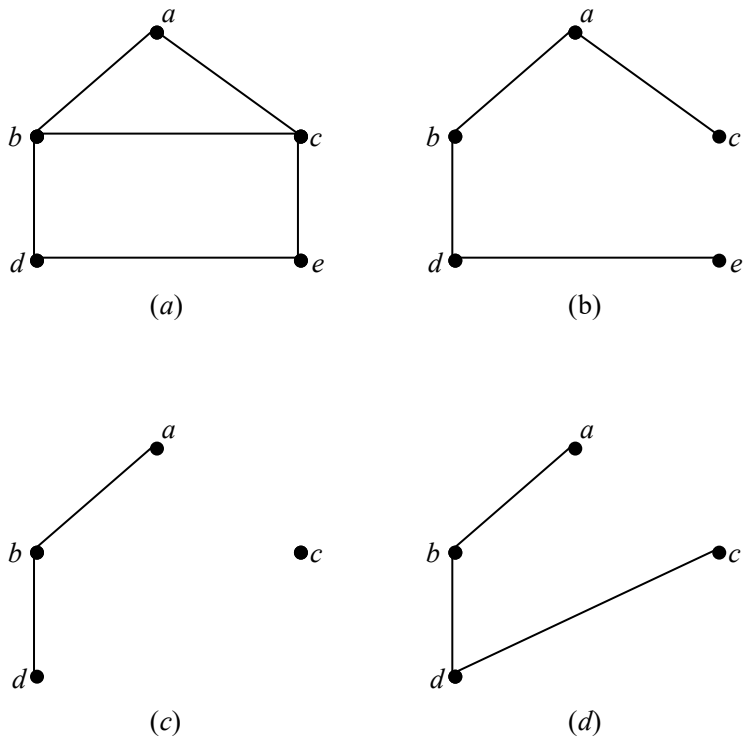


图 1.5

定义 12　设 G 是一个图，$E_1\subseteq E(G)$，以 E_1 为边集，E_1 中边的端点全体为顶点集构成的子图，称为由 E_1 导出的 G 的子图(边导出子图)，记为 $G(E_1)$．又设 $V_1\subseteq V(G)$，以 V_1 为顶点集，端点均在 V_1 中的边的全体为边集，构成的子图，称为由 V_1 导出的 G 的子图(点导出子图)，记为 $G(V_1)$．

例如，设 G 是由图 1.6(a)给出的图，则图 1.6(b)是 G 的边 ab，bc，ce 导出的子图，图 1.6(c)是 G 中点 a，b，c，d 导出的子图．

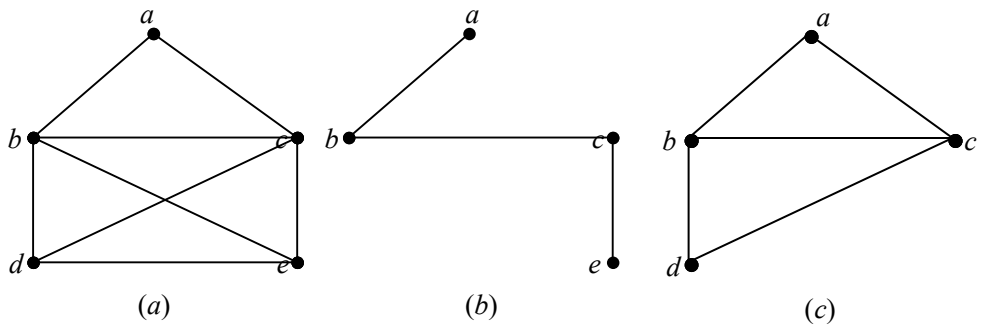


图 1.6

定义 13　设 G 是具有 n 个顶点的简单图，从这 n 个顶点构成的完全图 K_n 中删去 G 的所有边，但保留顶点集 $V(G)$所得到的图称为 G 的补图，简称 G 的补，记为$\sim G$.

例如，图 1.7(b)是图 1.7(a)的补.

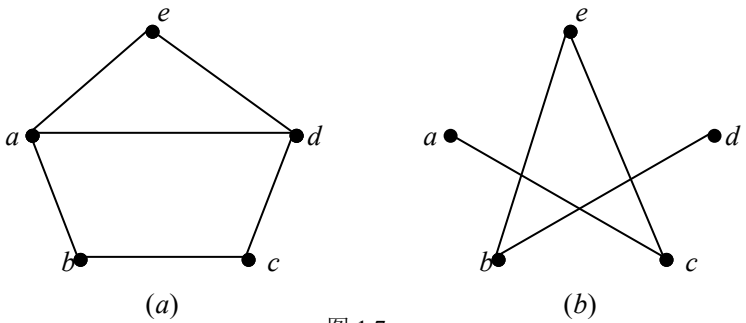


图 1.7

显然，简单图 G 的补图$\sim G$ 是一个以 $V(G)$为顶点集的简单图，$\sim G$ 中两个顶点相邻当且仅当这两个顶点在 G 中不相邻，特别地，完全图的补图是零图，正则图的补图是正则图，且显然　　$\sim(\sim G)=G$.

我们已经知道，在一个图中，顶点的位置，边的长度及形状是不加考虑的，例如图 1.8(a)与图 1.8(b)粗看起来似乎不相同，但实际上是同一个图.

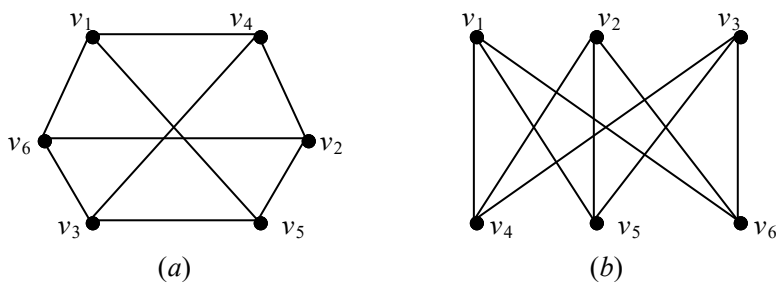


图 1.8

这样，一个图可以画出许多种形状，它们都表示同样的内容，事实上，一个图的实质性内容是边与点的关联关系，不仅图示的形状，就连顶点的标名也是无关紧要的，如图 1.9 中的两个图，除了标名不同外，其结构完全相同，只需将 a 改为 v_1，b 改为 v_2，c 改为 v_3，d 改为 v_4，图 1.9(b)与图 1.9(a)便是同一图，因此，这两个图必定具有完全相同的性质，这时，我们称这两个图是同构的.

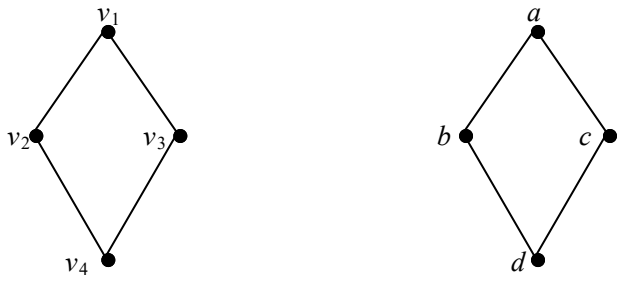


图 1.9

定义 14　设 G，H 是两个图，若存在双射（一一映射）

$$\theta: V(G)\to V(H)$$

$$\psi: E(G)\to E(H)$$

使得当且仅当 $e=uv$ 时，$\psi(e)=\theta(u)\theta(v)$，则称 G，H 是同构的，记为 $G\cong H$，而有序对 $<\theta, \psi>$ 称为 G 与 H 之间的一个同构映射或同构.

为表明两个图是同构的，就必须指出它们之间的一个同构映射，下面规定的一对映射$<\theta, \psi>$便是图 1.9(a)与图 1.9(b)之间的一个同构映射：

$$\theta:\ v_1\mapsto a,\ \ v_2\mapsto b,\ \ v_3\mapsto c,\ \ v_4\mapsto d$$

$$\psi:\ v_1v_2\mapsto ab,\ \ v_2v_3\mapsto bc,\ \ v_3v_4\mapsto cd,\ \ v_4v_1\mapsto da\ .$$

例 3　证明图 1.10(a)与图 1.10(b)同构.

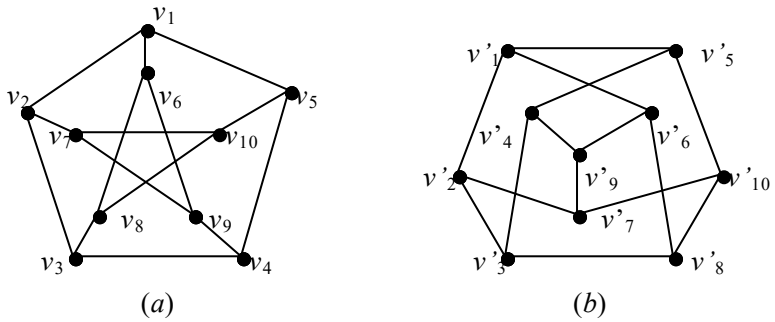


图 1.10

证明　为了方便，将图 1.10(*a*)称为图 G，图 1.10(*b*)称为图 G'，为证明这两个图同构，先把图 G' 画成与图 G 类似的形状(见图 1.11)．易见，以下映射对$<\theta, \psi>$构成 G 到 G' 的同构

$$\theta:\quad v_i \mapsto v_i',\qquad i=1,2,\cdots,10,$$

$$\psi:\quad v_iv_j \mapsto v_i'v_j',\quad v_iv_j \in E(G),$$

因此，图 G 与 G' 是同构的．

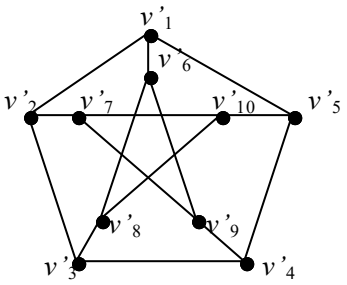


图 1.11

可以证明，图的同构关系是一个等价关系，因此可以根据该关系将所有图划分成一些等价类，同一等价类中的图只是点与边的标名不同，其结构是完全相同的．

顶点标以名称的图称为标志图．例如，前面所给出的图都是标志图，给一个图的顶点和边赋以标记的目的，主要是为了便于称呼它们，而我们感兴趣的则主要是图的结构性质，所以在画图时，有时略去那些标记，一个无标记的图可以认为是互相同构的一类图的代表．本篇中常用字母 G 表示图，并且当被研究的图只有一个时，我们总是用 G 来表示这个图，这时，在一些通用的符号中，可略去字母 G，例如，分别用 V，E，υ，ε 代替 $V(G)$，$E(G)$，$\upsilon(G)$，$\varepsilon(G)$等．

习 题 一

1．证明　在一次晚会上，握过奇次手的人数是偶数．

2．证明　空间中不可能有这样的多面体存在，它有奇数个面，而每个面又有奇数条边．

3．举一实例，它可由二分图描述，写出该二分图的一个二划分．

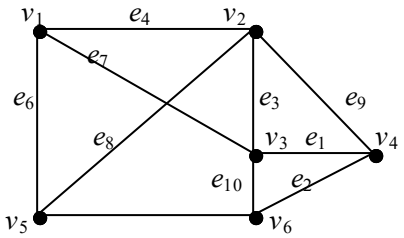
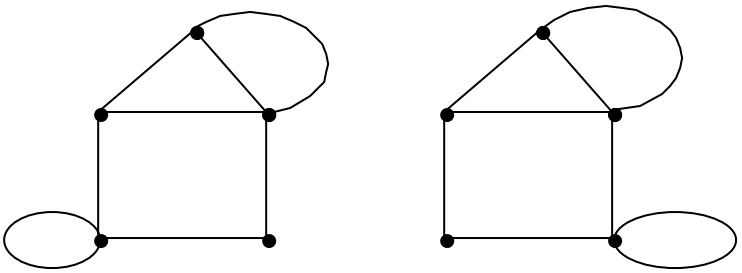


图 1.12

4．证明　简单图必满足 $\varepsilon \leqslant C_\nu^2$．

5．设图 G 由图 1.12 给出，求 $G(\{v_1, v_2, v_3\})$，$G(\{e_1, e_2, e_3\})$．

6．证明　图 1.13(*a*)与图 1.13(*b*)不同构．



(*a*)　　(b)

图 1.13

7．证明　若 $G\cong H$，则 $\upsilon(G)=\upsilon(H)$，$\varepsilon(G)=\varepsilon(H)$．举例说明，反之不然．

8．证明　在两个或更多个人组成的人群中，总存在这样两人，他们在该人群中的朋友数相同．

9．写出具有四个顶点的所有非同构简单图．

§ 2　路与连通

设 G 是一个图，u，v，$w\in V(G)$，当 u，v 之间有边 e_1 连接，v，w 之间有边 e_2 连接时，u，w 之间未必有边连接，但我们可以从 u 沿着边 e_1，e_2 到达 w，这时我们可称 u，w 之间有一条“路”．一般地，有

定义 1　图 G 的一个非空点、边交替序列

$$W=v_0e_1v_1\,e_2\,v_2\cdots e_k\,v_k$$

称为一条从 v_0 到 v_k 的路径或(v_0，v_k)-路径，其中，v_{i-1}，v_i 是 e_i 的端点($1\leqslant i\leqslant k$)．称 v_0 为 W 的起点，v_k 为 W 的终点，v_i($1\leqslant i\leqslant k-1$)为 W 的内点，k 为 W 的路长．

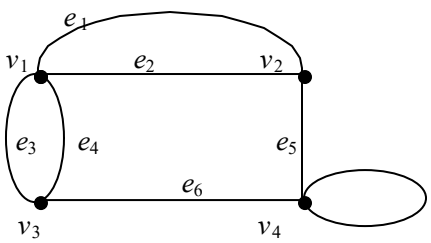


图 2.1

例如，在图 2.1 中，$v_1e_1v_2e_5v_4e_7v_4e_5v_2e_2v_1e_4v_3$ 是一条从 v_1 到 v_3 的路径，路长为 6．

若 $W=v_0e_1v_1e_2v_2\cdots e_kv_k$ 是一条(v_0，v_k)-路径，W 逆转后得到的点、边交替序列

$$v_ke_k\cdots v_2e_2v_1e_1v_0$$

必为一条(v_k，v_0)-路径，这条路径可记为 W^{-1}．路径 W 的部分相连项构成的子序列

$$v_i e_i v_{i+1} \cdots e_j v_j, \quad 0 \leqslant i \leqslant j \leqslant k$$

也必构成一条路径，这条路径称为 W 的节．又若

$$W' = v_k e_{k+1} v_{k+1} \cdots e_l v_l$$

也为一条路径，将 W 与 W' 衔接在一起便得一条新路径，该路径可记为 WW'．

为书写方便，常常只用顶点序列 $v_0v_1v_2\cdots v_k$ 或边序列 $e_1e_2\cdots e_k$ 表示路径 $v_0e_1v_1e_2v_2\cdots e_kv_k$．但要注意，由于一条路径未必能由其顶点序列唯一确定，用顶点序列表示路径有时会产生歧义．用顶点序列表示路径只用在不会产生歧义（比如简单图中）或具有相同顶点序列的路径不需要严格区分时．

定义 2　设 $v_0e_1v_1e_2v_2\cdots e_kv_k$ 为图 G 中的一条路径，若边 e_1，e_2，…，e_k 互不相同，则称该路径为迹；若点 v_0，v_1，…，v_k 互不相同，则称该路径为路．

定义 3　设 $v_0e_1v_1e_2v_2\cdots e_kv_k$ 是图 G 中的一条路径且 $k \geqslant 1$，如果 $v_0 = v_k$，则称该路径为闭路径，否则称为开路径．特别地，若 $v_0e_1v_1e_2v_2\cdots e_kv_k$ 是一条迹，$k \geqslant 1$，当 $v_0 = v_k$ 时称为闭迹，否则称为开迹．闭迹也称为回路．

定义 4　设 $v_0e_1v_1e_2v_2\cdots e_kv_0$ 是一条闭迹，如果 v_0，v_1，…，v_{k-1} 互不相同，则称该闭迹为圈或 k 圈，且当 k 为偶数时称为偶圈，k 为奇数时称为奇圈．

例如，在图 2.2 中，$v_2e_6v_5e_7v_2e_8v_4e_4v_5e_7v_2$ 是一条闭路径，$v_1e_1v_2e_2v_3$ 是一条开路径，$v_1e_1v_2e_6v_5e_7v_2e_8v_4e_4v_5e_5v_1$ 是一条回路，$v_3e_3v_4e_8v_2e_2v_3$ 是一个圈．

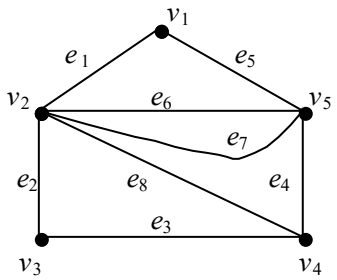


图 2.2

显然，一条路必是一条迹，自环和两条平行边都自成一圈．

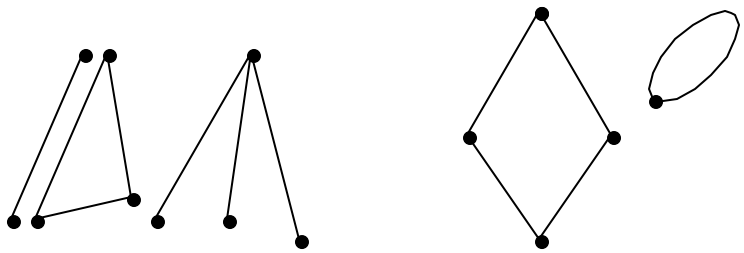
定理 1　若图 G 中每个顶点度数至少为 2，则 G 中必含有圈．

读者自证．

将边的概念推广，得到了路的概念，同样，将相邻的概念推广，则得到连通的概念．

定义 5　设 G 是一个图，u，$v \in V(G)$，如果存在从 u 到 v 的路，则称 u，v 是相连的或连通的，若 G 中任意两点都连通，则称图 G 是连通的．

容易证明，图 G 中顶点之间的连通关系是一个等价关系，根据该关系可将 $V(G)$划分成一些等价类 V_1，V_2，…，V_n，每个 V_i 导出的子图 $G(V_i)$称为 G 的一个连通分支，例如，图 2.3(a)有 3 个连通分支，图 2.3(b)有 2 个连通分支．



(*a*)　　(*b*)

图 2.3

G 的连通分支数通常用 $\omega(G)$表示，显然

$$G \text{ 是连通的} \Leftrightarrow \omega(G)=1.$$

定义 6　设 G 是一个图，u，$v\in V(G)$，若 u，v 是连通的，则称最短(u, v)-路的长为 u，v 的距离，记为 $d(u, v)$.

为方便起见，当 u，v 不连通时，可以认为 u，v 的距离是∞．例如，在图 2.4 中，$d(v_1, v_3)=1$，$d(v_1, v_4)=2$，$d(v_1, v_5)=2$，$d(v_1, v_6)=\infty$.

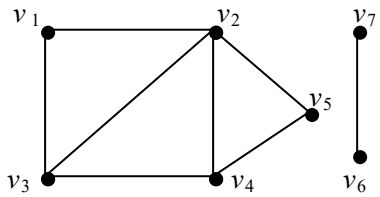


图 2.4

定理 2　一个图 G 是二分图 $\Leftrightarrow G$ 中不含奇圈.

证明　必要性　设 G 是一个二分图，不妨设$\{X, Y\}$是 G 的一个二划分，令 $C=v_0v_1\cdots v_kv_0$ 是一个圈($(k+1)$圈)，不失一般性，假定 $v_0\in X$，由于 v_1 与 v_0 相邻，根据二分图的定义，$v_1\in Y$，同理，$v_2\in X$，$v_3\in Y$，…，一般地，$v_{2i}\in X$，$v_{2i+1}\in Y$．又因为 $v_0\in X$，所以 $v_k\in Y$，即 k 是奇数，因此 C 为偶圈，从而知，G 中任何圈均为偶圈.

充分性　假设 G 中无奇圈，不妨设 G 是连通图(否则讨论其连通分支)，任取一固定点 $u\in V(G)$，令

$$X=\{x \mid x\in V(G),\ d(u, x)\text{是偶数}\},$$

$$Y=\{x \mid x\in V(G),\ d(u, x)\text{是奇数}\},$$

则 $V(G)$被划分成了两个集合 X，Y，现证明 $\{X, Y\}$ 是 G 的一个二划分．假设 v 和 w 是 X 中两点，P 是最短的(u, v)-路，Q是最短的(u, w)-路，则 P，Q的长都是偶数，以 u_1 记 P和 Q的最后一个公共顶点，因 P和 Q是最短路，P和 Q二者的(u, u_1)-节也是最短 (u, u_1)-路，故长度相同，现因 P和 Q的长都是偶数，所以 P的(u_1, v)-节 P_1和 Q的 (u_1, w)-节 Q_1必有相同奇偶性，因此推出(v, w)-路 $P_1^{-1}Q_1$长为偶数，若 u 和 w 相邻，则

$P_1^{-1}Q_1wv$ 就是一个奇圈，与假设矛盾，故 X 中任意两点均不相邻，类似地，Y 中任意两个顶点也不相邻. ▌

定理 3　设 G 是具有 n 个顶点的简单图，若 G 有 ε 条边，ω 个连通分支，则

$$n-\omega \leqslant \varepsilon \leqslant \frac{1}{2}(n-\omega)(n-\omega-1)$$

证明　为证明 $\varepsilon \geqslant n-\omega$，我们对 G 的边数 ε 施行归纳法. 当 $\varepsilon=0$ 时，G 是零图，这时 $\varepsilon=0$，$\omega=n$，结论成立. 假设当 $\varepsilon=k$ 时结论成立，现考察 $\varepsilon=k+1$ 的情况，从 G 中删去一边，得到图 G'，可能有如下两种情况：

(1)　没有因为删去一边而增加连通分支，这时 G' 有 n 个顶点，ω 个连通分支，k 条边，由归纳假设可知 $n-\omega \leqslant k$，自然有 $n-\omega \leqslant k+1$；

(2)　因为删去一边而增加了一个连通分支，这时 G' 有 n 个顶点，$\omega+1$ 个连通分支，k 条边，由归纳假设可知 $n-(\omega+1) \leqslant k$. 即 $n-\omega \leqslant k+1$，

总之，必有 $n-\omega \leqslant k+1$. 从而知对任何 $\varepsilon \geqslant 0$，$n-\omega \leqslant \varepsilon$ 成立.

下面证明 $\varepsilon \leqslant \frac{1}{2}(n-\omega)(n-\omega-1)$. 假设 G 的 ω 个连通分支分别具有 n_1，n_2，…，n_ω 个顶点，则 $n_1+n_2+\cdots+n_\omega=n$. 因为 G 是简单图，故 G 的第 i 个连通分支的边数 ε_i 满足

$$\varepsilon_i \leqslant C_{n_i}^2,$$

从而

$$\varepsilon \leqslant C_{n_1}^2 + C_{n_2}^2 + \cdots + C_{n_\omega}^2 .$$

由基本组合公式　$C_s^2 + C_t^2 \leq C_{s+t-1}^2$（$s$，$t$ 为正整数），　有

$$\begin{aligned}
\varepsilon &\leq C_{n_1}^2 + C_{n_2}^2 + \cdots + C_{n_\omega}^2 \\
&\leq C_{n_1+n_2-1}^2 + C_{n_3}^2 + \cdots + C_{n_\omega}^2 \\
&\leq C_{n_1+n_2+n_3-1}^2 + C_{n_4}^2 + \cdots + C_{n_\omega}^2 \\
&\leq \cdots \\
&\leq C_{n_1+n_2+\cdots+n_\omega-(\omega-1)}^2 \\
&= C_{n-\omega+1}^2 \\
&= \frac{1}{2}(n-\omega)(n-\omega+1)
\end{aligned}$$

总之，我们有　$n-\omega \leqslant \varepsilon \leqslant \frac{1}{2}(n-\omega)(n-\omega-1)$ ▌

由于 $C_{n-\omega+1}^2 = \frac{1}{2}(n-\omega)(n-\omega+1)$ 恰好为 $n-\omega+1$ 个顶点组成的完全图 $K_{n-\omega+1}$ 的边数，因此，由上定理可见，当 G 有 n 个顶点 ω 个分支时，G 的边数在以下情况下达到最大：

G 的某一个连通分支是 $n-\omega+1$ 个顶点的完全图，其余 $\omega-1$ 个连通分支均是弧立点.

上定理还告诉我们，当 $\omega=1$ 时，$\varepsilon \geqslant n-1$. 即 n 个顶点的连通图至少有 $n-1$ 条边，因此可把具有 n 个顶点，$n-1$ 条边的连通图称为最小连通图.

习 题 二

1. $2n$ 个电话交换台，每个台至少与 n 个台有直通线路，证明其中任意两台之间可以通话.
2. 图中只有两个奇顶点，则它们必连通.
3. 证明　每顶点皆 2 度的连通图是圈.
4. 证明　在简单图中，必存在长为 δ 的路.
5. 证明　G 是连通图，当且仅当对于 $V(G)$的任意划分 $\{V_1,V_2\}$，总存在边 e 使得 e 的一个端点在 V_1 中，另一端点在 V_2 中.
6. 证明　若 G 是简单图，且 $\varepsilon > C_{\upsilon-1}^2$，则 G 连通. 找出一个边数为 $C_{\upsilon-1}^2$ 的不连通简单图 ($\upsilon>1$).
7. 证明　若 G 不连通，则 $\sim G$ 连通.
8. 证明　若 $e\in E(G)$，则
$$\omega(G)\leqslant \omega(G-e)\leqslant \omega(G)+1,$$
其中，$G-e$ 表示从 G 中去掉边 e 得到的图.
9. 证明　连通图中，任意两条最长路必有公共顶点.
10. 证明　若 e 在 G 的某回路中，则 e 在 G 的某圈中.

§3　最 短 路

在实际问题当中，图的边往往与某种数量相联系，例如，在铁路交通图中，根据所讨论的问题，每条边上可以标上其代表的铁路的长度，或标上修建该铁路所需的费用等，一般地，引入如下定义.

定义 1　设 G 是一个图，若对 G 中每条边 e 都规定一个非负实数 $w(e)$，则称 G 为赋权图（或权图），$w(e)$ 称为边 e 的权. G 的边与非负实数的这种对应关系(用 w 表示)称为权函数.

例如，设 G 是铁路交通图，对 G 中每条边 e 规定 $w(e)$为 e 所代表的铁路的长度，则得到一权图，若规定 $w(e)$为修建 e 所代表的铁路所需费用，则又得到另一权图. 再如，设 G 是秘密通讯图，对边 e 规定 $w(e)$为泄秘可能性则得到一权图，又若规定 $w(e)$为维护 e 所需费用，则又得到另一权图.

按照通常惯例，当 u，v 不相邻时，规定 $w(uv)=\infty$.

定义 2　设 G 是一个权图，H是 G 的子图，H中各边的权之和称为子图 H的权，记为 $w(H)$，即

$$w(H)=\sum_{e\in E(H)}w(e).$$

由于权图中的权常常代表某种耗费，许多最优化问题都是要在一个权图中找出某类具有最小权的子图，其中之一就是最短路问题.

定义 3　设 G 是一个权图，路 P 的权 $w(P)$称为 P 的长度，两点 u，v 之间最短路的长度称为 u，v 之间的距离，记为 d (u，v)，即

$$d(u,v)=\begin{cases}0, & u=v\\ \min\{w(P)\mid P\text{是}(u,v)\text{-路}\}, & u,v\text{连通}\\ \infty, & u,v\text{不连通}\end{cases}$$

可以看出，如果权图 G 中每边的权均为 1，则这里定义的路的长度及两点间的距离与 § 2 中定义的通常图的路长及两点间的距离是一致的.

定义 4　设 G 是一个权图，$u_0\in V(G)$，$S\subseteq V(G)$，u_0 到 S 内各点的所有路中长度最小者，称为 u_0 到 S 的最短路，其长度称为 u_0 到 S 的距离，记为 $d(u_0, S)$.

现在我们就来讨论在权图 G 中寻找最短路的问题，为此，先做几点假设.

1)　显然，只要讨论简单图的问题就够了，所以下面假设 G 是简单图.

2)　因为当 $w(uv)=0$ 时，我们认为 u，v 重合，所以我们不妨假定所有边的权均为正数.

下面介绍的算法是 Dijkstra 在 1959 年提出的，这个算法可以求出 G 中一点 u_0 到其余各点的最短路及距离，它至今是解最短路问题的最好算法之一.

Dijkstra 算法基于如下基本原理.

假设 S 是 V 的真子集，$u_0\in S$，令 $\bar{S}=V-S$，若 $P=u_0\cdots\bar{u}\bar{v}$ 是从 u_0 到 $\bar{S}$的最短路，则显然 $\bar{u}\in S$，$\bar{v}\in\bar{S}$，且 P 的(u_0，$\bar{u}$)节必然是最短(u_0，$\bar{u}$)路，所以

$$\begin{aligned} d(u_0,\bar{S}) &= w(P)=d(u_0,\bar{v})\\ &= d(u_0,\bar{u})+w(\bar{u}\bar{v})\\ &= \min_{u\in S,v\in\bar{S}}\{d(u_0,u)+w(uv)\}\end{aligned}\tag{1}$$

利用该公式，便可按如下过程求最短路.

首先，确定距 u_0 最近的一个顶点．令 $S_0=\{u_0\}$，由于距 u_0 最近的顶点必为 u_0 的邻点，故只需求出 u_1 使

$$w(u_0u_1)=\min\{w(u_0v)\mid v\in\bar{S}_0\},$$

即 u_0u_1 是与 u_0 关联的最短边，显然，u_0u_1 便是最短$(u_0，u_1)$-路．又令 $S_1=\{u_0，u_1\}$，且用 P_1 表示路 u_0u_1，……，一般地，若 $S_k=\{u_0，u_1，\cdots，u_k\}$ 以及相应的最短路 P_1，P_2，…，P_k 已经确定，则可用(1)式来计算 $d(u_0,\overline{S}_k)$，并选取顶点 $u_{k+1}\in\overline{S}_k$ 使 $d(u_0，u_{k+1})=d(u_0,\overline{S}_k)$．这时，$d(u_0，u_{k+1})=d(u_0，u_j)+w(u_ju_{k+1})$对某个 $j\leqslant k$ 成立．将边 u_ju_{k+1} 连接到路 P_j 上，即得最短$(u_0，u_{k+1})$-路 P_{k+1}，再令 $S_{k+1}=\{u_0，u_1，\cdots，u_k，u_{k+1}\}$，……，这样一直下去，直到 $\overline{S}_k=\varnothing$，即可求出 u_0 到 G 中任意一点的最短路．

为了说明上述过程，考察图 3.1，u_0 到任一点的最短路用粗黑线表示（带圈的数字①、②、③…表示该过程中边加入最短路的顺序）．

在上述过程中，若每一步都通过搜索来计算(1)式的最小值，则必定会有大量的重复比较，为避免重复并保留从每一步到下一步的计算信息，采用如下的标号方法：在整个算法中，每个顶点 v 给以标号 $l(v)$，它是 $d(u_0，v)$的一个上界，开始时，$l(u_0)=0$，$l(v)=\infty(v\neq u_0)$，在算法进行时，这些标号不断修改，当求出 S_i 时，

$$l(u)=d(u_0，u)，\ u\in S_i,$$

并且

$$l(v)=\min_{u\in S_{i-1}}\{d(u_0,u)+w(uv)\}，\ v\in\overline{S}_i.$$

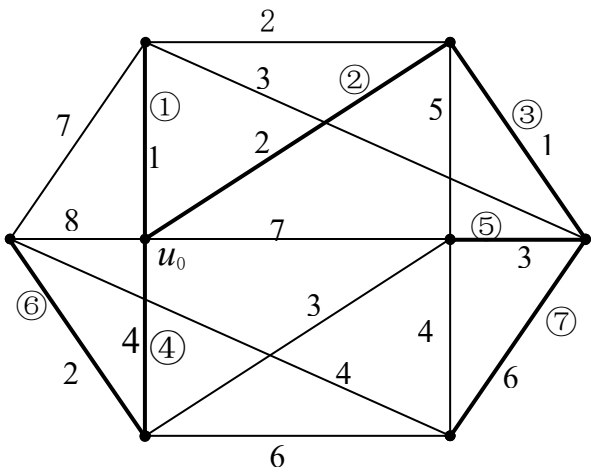


图 3.1

Dijkstra 算法

1．令 $l(u_0)=0$，$l(v)=\infty(v\neq u_0)$，$S_0=\{u_0\}$，　$i=0$．

2．对每个 $v\in\overline{S}_i$，用 $\min\{l(v)，l(u_i)+w(u_iv)\}$ 代替 $l(v)$，计算 $\min\{l(v)|\ v\in\overline{S}_i\}$，并把达到这个最小值的一个顶点记为 u_{i+1}．令 $S_{i+1}=S_i\cup\{u_{i+1}\}$．

3．若 $i=v-1$，则停止，若 $i<v-1$，$i\leftarrow i+1$，转入 2．

当算法结束时，$d(u_0，v)$由标号 $l(v)$的终值给出．

如上所述，Dijkstra 算法仅确定了从 u_0 到所有其他顶点的距离，而并未给出实际最短路，然而，只要附加某些指令，不难获得这些最短路．

以上算法的计算量为 $O(v^2)$，因此是一个有效算法．

习 题 三

1．某公司在六个城市 C_1，C_2，…，C_6 中都有分公司，从 C_i 到 C_j 的直接航程票价由下述矩阵的$(i，j)$元素给出(∞表示无直接航线)

$$\begin{bmatrix} 0 & 50 & \infty & 40 & 25 & 10 \\ 50 & 0 & 15 & 20 & \infty & 25 \\ \infty & 15 & 0 & 10 & 20 & \infty \\ 40 & 20 & 10 & 0 & 10 & 25 \\ 25 & \infty & 20 & 10 & 0 & 55 \\ 10 & 23 & \infty & 25 & 55 & 0 \end{bmatrix}$$

该公司想算出一张任意两城市之间的最廉航价路线表，试作出这样的表来．

2．一只狼，一头山羊和一筐卷心菜在河的同侧，一个摆渡人要将它们运过河去，但由于船小，他一次只能载三者之一过河，显然，不管是狼和山羊，还是山羊和卷心菜，都不能在无人监视的情况下留在一起，问摆渡人应怎样把它们运过河去？

3．两人有一只容积为 8 加仑的酒壶盛满了酒，还有两只容积分别为 5 和 3 加仑的空壶，问平分酒的最简单方法应当怎样？

4．为了使 Dijkstra 算法不仅能确定距离，而且能确定最短路，必须附加哪些指令？

§4　有向图

前面我们讨论的图，其边是没有方向性的，即每条边对应一个无序点对 uv，但有时我们需要这些边有一个指定的方向．例如，用点表示企业，连线表示债务关系，就得到一个企业之间的债务图，但为了从该图中看出债务方与债权方，必须给这些连线标以方向，比如，当 a 方欠 b 方债时，规定连线的方向由 a 到 b．对这种“有方向的图”加以抽象，便得到如下有向图的概念．

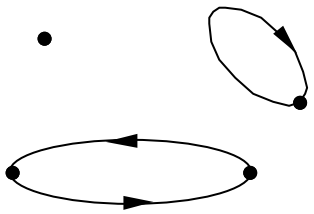


图 4.1

定义 1　设 V 是一个非空集合，A 是一个由 V 中元素的有序对构成的多重集，有序对 $D=\langle V, A\rangle$ 称为一个有向图，其中，V 称为顶点集，其元素称为顶点或点；A 称为弧集，其元素称为弧．

由该定义可见，有向图与无向图的区别仅仅在于有向图的弧集是有序顶点对的多重集，而无向图的边集是无序顶点对的多重集，无向图中的一切概念均可平移到有向图．

对有向图 D，总是用 $V(D)$表示其顶点集，$A(D)$表示其弧集．

同无向图一样，有向图也可用一个图形表示：$V(D)$的元素用不重合的几何点表示，位置任意，当 $a=\langle u, v\rangle \in A(D)$且其重复度为 k 时，画 k 条自 u 到 v 的带箭头的弧线表示 a，其形状、长短不加考虑，这样得到的图形叫做有向图的图示．

以后也将不区别有向图及其图示．

例 1　令

$$V=\{v_1, v_2, v_3, v_4\},$$

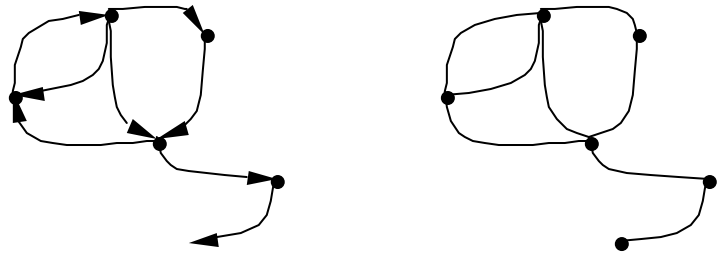
$$A=\{\langle v_1, v_2\rangle, \langle v_2, v_1\rangle, \langle v_3, v_3\rangle\},$$

则 $\langle V, A\rangle$ 是一个有向图，其图示见图 4.1．

设 D 是一个有向图，若 $a=\langle u, v\rangle \in A(D)$，则称 a 从 u 连接到 v，且称 u，v 与 a 彼此相关联；称 u 是 a 的尾或起点，v 是 a 的头或终点，且将 u，v 统称为 a 的端点．

设 D，D' 是两个有向图，如果 $V(D')\subseteq V(D)$，$A(D')\subseteq A(D)$，称有向图 D' 是 D 的子有向图．关于子有向图的术语及记号与子(无向)图所使用的类似，比如真子有向图，支撑子有向图，导出子有向图等等．

对于每个有向图 D，忽略其弧的方向，即将其每条弧均视为一条无方向的边，这样得到的(无向)图 G 称为 D 的底图，反之，给定任意图 G，对于它的每条边，给其端点指定一个顺序，从而确定一条弧，由此得到一个有向图，这样的有向图称为 G 的一个定向图，图 4.2 给出了一个有向图及其底图．



(*a*)　　(*b*)

图 4.2

利用底图，可将图中所有概念完全平移到有向图中，比如，当有向图 D 的底图 G 连通时，我们说 D 连通，当底图 G 中有圈时，我们说 D 中有圈等等.

由于有向图中具有了方向的概念，围绕着这个概念，可产生一些与此有关的术语.

D 中顶点 v 的入度 $d_D^-(v)$ 是指以 v 为头的弧的数目，v 的出度 $d_D^+(v)$ 是指以 v 为尾的弧的数目，v 的度 $d_D(v)$则是入度与出度之和，我们用 $\delta^-(D)$，$\triangle^-(D)$，$\delta^+(D)$，$\triangle^+(D)$ 分别表示 D 中顶点的最小和最大入度、最小和最大出度，并同以前一样，用 $\delta(D)$，$\triangle(D)$ 分别表示 D 中顶点的最小度和最大度，并用 $\upsilon(D)$，$\varepsilon(D)$表示 D 中顶点数及弧数.

以后，我们总是用 D 表示有向图，而用 G 表示它的底图，并常从有关记号中省去字母 D，例如，$\triangle(D)$写成$\triangle$，$d_D^+(v)$写成 $d^+(v)$等等.

定理 1　设 D 是有向图，则 D 中顶点的入度之和与出度之和均为 ε，即

$$\sum_{v\in V} d^-(v) = \sum_{v\in V} d^+(v) = \varepsilon .$$

读者自证.

有向图 D 的有向路径是指一个非空有限点、弧交替序列

$$W = v_0a_1v_1a_2v_2\cdots a_kv_k$$

使得对于 $i=1$，2，…，k，弧 a_i 的头为 v_i，尾为 v_{i-1}，和无向图的路径一样，有向路径 $v_0a_1v_1a_2v_2\cdots a_kv_k$ 也常用它的顶点序列 $v_0v_1\cdots v_k$ 或弧序列 $a_1a_2\cdots a_k$ 表示.

一条有向路径 $v_0a_1v_1a_2v_2\cdots a_kv_k$，若其中的弧 a_1，a_2，…，a_k 互不相同，则称其为有向迹，有向路、有向回路、有向圈等也可类似定义.

如果 D 中存在有向(u, v)-路，则称 v 是从 u 可达的，如果 u，v 是互相可达的，则称 u，v 是双向连通的，若对 D 中任何两顶点，至少有一顶点可从另一顶点可达，则称 D 是单向连通图，若 D 中任何两顶点都是双向连通的，则称 D 是双向连通图或强连通图.

双向连通关系是 D 的顶点集 V 上的一个等价关系，根据该关系可以将 V 划分成一些等价类 V_1，V_2，…，V_m，它们导出的子图 $D(V_1)$，$D(V_2)$，…，$D(V_m)$称为 D 的双向分支或强连通分支，显然，D强连通 $\Leftrightarrow$ D恰有一个强连通分支.

若有向图 D 中每两个顶点之间恰有一条弧，则称 D 为竞赛图，显然，D 是竞赛图当

且仅当 D 是完全图的定向图，具有四个顶点的竞赛图如图 4.3 所示，其中每个竞赛图都可以看成是四名运动员在循环赛中的比赛结果. 例如，图 4.3 中第一个竞赛图表示一个运动员在所有三次比赛中都获胜，而另外三个运动员每人各胜一次.

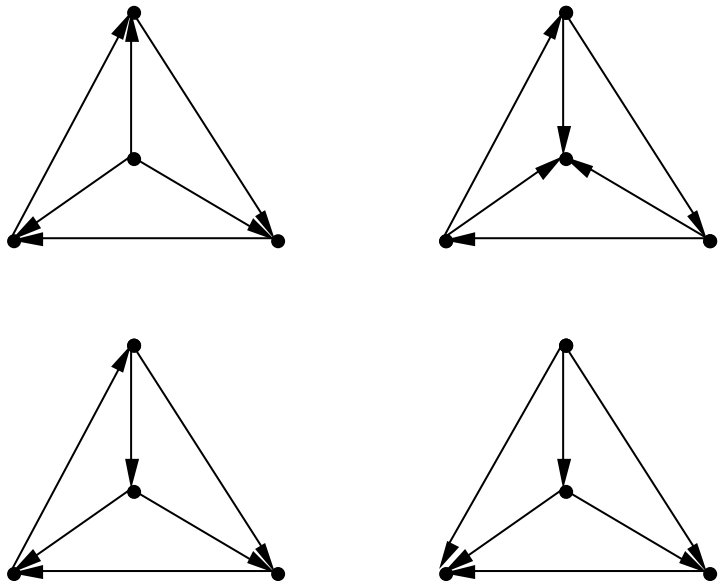


图 4.3

习 题 四

1．一个简单图 G 具有多少个定向图?

2．证明定理 1.

3．设 D 是没有有向圈的有向图，

(a) 证明 $\delta^{-}=0$;

(b) 证明 存在 V 的一个有序顶点列 v_1，v_2，…，v_v，使得对于 $1\leqslant i\leqslant v$，D 的每条以 v_i 为头的弧在 $\{v_1, v_2, \cdots, v_{i-1}\}$ 中都有它的尾.

4．设 D_1，D_2，…，D_m 是 D 的双向连通分支，D 的凝图 $\hat{D}$ 是指一个有 m 个顶点 w_1，w_2，…，w_m 的有向图，$\hat{D}$ 中存在一条以 w_i 为尾 w_j 为头的弧当且仅当 D 中存在一条尾在 D_i 中而头在 D_j 中的弧，证明 D 的凝图 $\hat{D}$ 不包含有向圈.

§ 5　图的矩阵表示

定义 1　设 G 是一个无自环的图，$v\times\varepsilon$ 矩阵 $A(G)=(a_{ij})$ 称为 G 的关联矩阵，其中

$$a_{ij}=\begin{cases}1, & v_i\text{关联于}e_j,\\ 0, & \text{否则。}\end{cases}$$

例 1　图 5 .1 的关联矩阵为

$$A(G)=\begin{array}{c} \\ v_1\\ v_2\\ v_3\\ v_4\\ v_5\end{array}\begin{array}{c}\begin{array}{cccccccc}a & b & c & d & e & f & g & h\end{array}\\ \begin{bmatrix}0&0&0&0&1&1&1&0\\0&0&0&1&1&0&0&1\\0&0&1&1&0&1&0&0\\1&1&1&0&0&0&1&1\\1&1&0&0&0&0&0&0\end{bmatrix}\end{array}$$

图 G 的关联矩阵有下列性质：

（ 1 ）G 中每一边关联两个顶点，所以 $A(G)$中每一列恰好有两个 1；

（ 2 ）每一行中 1 的个数是对应顶点的度数；

（ 3 ）平行边对应的列全同；

（ 4 ）若 G 有两个分支 G_1，G_2，则适当调整顶点及边的顺序，可使关联矩阵呈块对角形

$$A(G)=\begin{bmatrix}A(G_1) & 0\\ 0 & A(G_2)\end{bmatrix}.$$

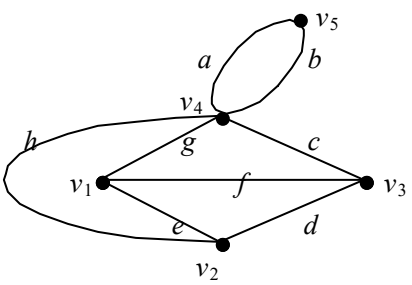


图 5 .1

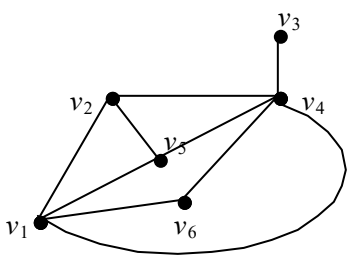


图 5 .2

定义 2　设 G 是无平行边的图，$v\times v$ 矩阵 $X(G)=(x_{ij})$ 称为图 G 的邻接矩阵，其中

$$x_{ij}=\begin{cases}1, & v_i\text{与}v_j\text{相邻},\\ 0, & \text{否则}。\end{cases}$$

显然，$X(G)$是对称矩阵.

例 2　图 5.2 的邻接矩阵为

$$X(G)=\begin{array}{c} \\ v_1\\ v_2\\ v_3\\ v_4\\ v_5\\ v_6\end{array}\begin{array}{c}\begin{array}{cccccc}a & b & c & d & e & f\end{array}\\ \begin{bmatrix}0&1&0&1&1&1\\1&0&0&1&1&0\\0&0&0&1&0&0\\1&1&1&0&1&1\\1&1&0&1&0&0\\1&0&0&1&0&0\end{bmatrix}\end{array}$$

令 $X^2=(x_{ij}^{(2)})$，则容易证明 $x_{ij}^{(2)}(i\neq j)$等于顶点 v_i 和 v_j 之间长度为 2 的路径数目，一般地，用归纳法可证对于正整数 k，X^k有如下特性

定理 1　设 G 是一个简单图，X是 G 的邻接矩阵，令 $X^k=(x_{ij}^{(k)})$. 则 $x_{ij}^{(k)}$ 等于顶点 v_i，v_j之间长度为 k 的路径数目.

证明留作习题.

类似地，对于有向图我们也可以定义其关联矩阵、邻接矩阵.

定义 3　设 D 是一个无自环的有向图，$v\times\varepsilon$ 矩阵 $A(D)=(a_{ij})$ 称为 D的关联矩阵，其中

$$a_{ij}=\begin{cases}0, & v_i\text{与}a_j\text{不关联},\\ -1, & v_i\text{是}a_j\text{的头},\\ 1, & v_i\text{是}a_j\text{的尾}。\end{cases}$$

D的关联矩阵有如下性质：

(1) D 中每一弧关联两个顶点，其中之一为头，另一为尾，所以，$A(D)$中每一列必有一个 1 和一个－1；

(2) 每一行中 1 的个数是对应顶点的出度数，－1 的个数是对应顶点的入度数，非零元的个数是对应顶点的度数；

(3) 平行弧对应的列全同.

定义 4　设 D 是一个无平行弧的有向图，$v\times v$矩阵 $X(D)=(x_{ij})$ 称为 D 的邻接矩

阵．其中

$$x_{ij}=\begin{cases}1, & \text{从}v_i\text{到}v_j\text{有弧},\\ 0, & \text{否则}。\end{cases}$$

类似于定理 1，有

定理 2　设 X 是简单有向图 D 的邻接矩阵，令 $X^k=(x_{ij}^{(k)})$，则 $x_{ij}^{(k)}$ 等于从 v_i 到 v_j 长度为 k 的有向路径的数目．

习 题 五

1．写出下列两图的关联矩阵、邻接矩阵．

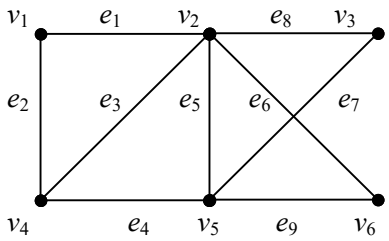


图 5.3

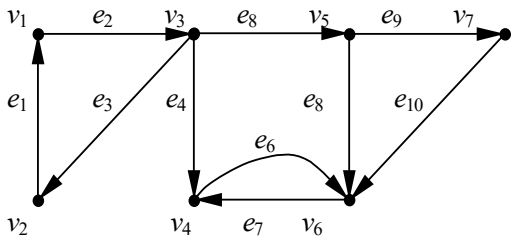


图 5.4

2．证明定理 1.

3．设 A 是图 G 的关联矩阵，X 是它的邻接矩阵．

(1) 证明 A 的每一列之和均为 2．

(2) X 的每一列之和是多少？

4．设 G 是二分图，证明把 G 的顶点适当排列后，可使 G 的邻接矩阵有形如 $\begin{bmatrix}0 & X_{12}\\ X_{21} & 0\end{bmatrix}$，其中 X_{21} 是 X_{12} 的转置．

第九章　Euler 图与 Hamilton 图

§1　Euler 图

前面我们已经介绍过 Königsberg 七桥问题，做为图论方法解决的第一个问题，它引出了 Euler 图及一些有关的概念，如前所述 Königsberg 七桥问题，就是讨论图 1.1 中是否存在一条遍游各边恰好一次的闭路径.

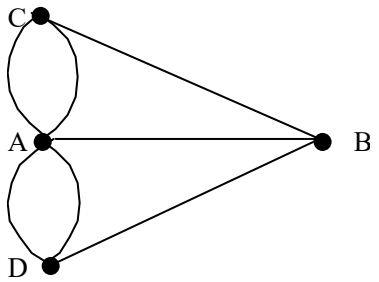


图 1.1

定义 1　设 G 是一个图，G 中包含所有边的迹(即每条边恰好出现一次的路径)称为 Euler 迹，闭的 Euler 迹称为 Euler 闭迹或 Euler 回路，具有 Euler 回路的图称为 Euler 图，开的 Euler 迹称为 Euler 开迹，具有 Euler 开迹的图称为半 Euler 图.

从以上定义可见 Euler 图就是能从一点出发，经过每边恰好一次，再回到出发点的那种图，而半 Euler 图则是能从一点出发，不重复地遍历诸边不回到出发点的那种图，Euler 回路或 Euler 开迹实际上是一条一笔画路线.

定理 1　设 G 是连通图，则 G 是 Euler 图当且仅当 G 的所有顶点均是偶顶点.

证明　显然，在讨论一个图是否构成 Euler 图时，自环不起作用，因此不妨设 G 中无自环.

必要性　设 G 是 Euler 图，

$$W=v_0e_1v_1e_2v_2\cdots e_kv_0$$

是一条 Euler 回路，由于 G 是连通图，故必无弧立点，即 G 的每点必与某边关联，又 W 中出现 G 的所有边，所以，W 中必出现 G 的所有点，任取 $v\in V$，如果 $v\neq v_0$，即 v 只出现在 W 的内部，则 v 每出现一次就有两条与它关联的边出现，故若 v 在 W 中共出现 m 次，则 W 中出现 $2m$ 条与 v 关联的边. 因为 G 中每边在 W 中恰好出现一次，且已经假设 G 中无自环，W 中不可能连续出现两个相同顶点，因而这 $2m$ 条边无重复计算，他们就是 G 中与 v 关联的所有边，即 $d(v)=2m$，即知 $d(v)$必为偶数. 类似地，如果 $v=v_0$，由于 W 开始于 v 且止于 v，故也有 $d(v)$是偶数，总之，G 中任意点均为偶顶点.

充分性，设 G 中每点均为偶顶点，则可按如下步骤构造一条 Euler 回路：

(1) 从任一顶点 v_0开始，取关联于 v_0的边 e_1到 v_1，因为 $d(v_1)$为偶数，故当 $v_1\neq v_0$时可取关联于 v_1 的边 $e_2(e_2\neq e_1)$到 v_2，…，一直下去(在此过程中，每边只取一次)，直到回到顶点 v_0，得到一条闭迹 $h_1=v_0e_1v_1e_2v_2\cdots v_ie_{i+1}\cdots v_0$ ；

(2) 若 $h_1=G$，则 G 为 Euler 图，否则，令 $h'_1=G(E(G)\text{-}E(h_1))$，即 h'_1 是从 G 中删除 h_1 中的边以及在此之后出现的弧立点得到的图，显然，h'_1 不是零图且其顶点均为偶顶点，因为 G 是连通的，h'_1 与 h_1 必有一个公共顶点 v_i，在 h'_1 中从 v_i 出发重复步骤(1)得到一条闭迹 $h_2=v_i e'_1 u_1 e'_2\cdots v_i$；

(3) 若 $h_1\cup h_2=G$，则 $v_0e_1\cdots v_i e'_1u_1e'_2\cdots v_i e_{i+1}\cdots v_0$ 是 G 中一条 Euler 回路，故 G 是 Euler 图，否则，重复步骤(2)，直到构造一条包含 G 中所有边的闭迹为止，此闭迹即为 Euler 回路，从而知 G 是 Euler 图. ▌

定理 2 设 G 是连通图，则 G 是半 Euler 图当且仅当 G 中恰有两个奇顶点.

证明 若 G 是半欧拉图，不妨设 $W=v_0e_1v_1\,e_2\,v_2\cdots e_kv_k$ 是一条 Euler 开迹，则 $v_0\neq v_k$，在 G 的顶点 v_0 与 v_k 之间附加一边 e 得到图 G'，则 $v_0e_1v_1\,e_2\,v_2\cdots e_kv_kev_0$ 是 G' 中的一条 Euler 回路，因此，G' 是 Euler 图，由定理 1，Euler 中每点均为偶顶点，对任意 $v\in V(G)$，若 $v\neq v_0$，$v\neq v_k$，则 $d_G(v)=d_{G'}(v)$，故 v 在 G 中是偶顶点，又 $d_G(v_0)=d_{G'}(v_0)-1$，$d_G(v_k)=d_{G'}(v_k)-1$，故 v_0，v_k 是 G 中的奇顶点，所以，G 中恰有两个奇顶点.

反之，若 G 中恰有两个奇顶点，设为 u，v，在 u，v 之间附加一边 e'，则得到一个顶点均为偶顶点的图 G'，由定理 1，G' 是 Euler 图，故在 G' 中必存在 Euler 回路 W'.因为 e' 必出现在 W' 中，不妨设 $W'=v_0e_1v_1\cdots ue'v\cdots e_kv_0$，则 $W=v\cdots e_kv_0e_1v_1\cdots u$ 即是 G 中的一条 Euler 开迹，从而 G 是半欧拉图. ▌

当然，该定理也可用完全类似于定理 1 的方法直接证明，请读者自己完成.

对于有向图，我们也可以类似地定义 Euler 有向图和半 Euler 有向图，并得到类似的充要条件.

定义 2 设 D 是一个有向图，D 中包含所有弧的有向迹，称为 Euler 有向迹，闭的 Euler有向迹称为Euler有向闭迹或Euler有向回路，具有Euler有向回路的有向图称为Euler有向图，开的 Euler 有向迹称为 Euler 有向开迹，具有 Euler 有向开迹的有向图称为半 Euler 有向图.

显然，一个 Euler 有向图，如果没有弧立点，则必是强连通的.

为了将有关 Euler 图(或半 Euler 图)的定理平移到 Euler 有向图上(或半 Euler 有向图上)，引入下述定义.

定义 3 设 D 是有向图，$v\in V(G)$，若 $d^-(v)=d^+(v)$，称 v 是平衡的. 若 D 中每个顶点都是平衡的，则称 D 是平衡的. 如果存在 $k\in\mathbf{N}$，使得 D 中每点的入度、出度均为 k，则称 D 是一致平衡的.

完全类似于定理 1 与定理 2，我们有

定理 4 设 D 是单连通有向图，则 G 是 Euler 有向图当且仅当 G 是平衡的.

定理 5 设 D 是单连通有向图，则 G 是半 Euler 有向图当且仅当 G 中恰有两个奇顶

点 u, v，满足 $d^-(u)=d^+(u)+1$， $d^+(v)=d^-(v)+1$，而其它顶点都是平衡的.

习 题 一

1．下列图形中哪些能一笔画成？

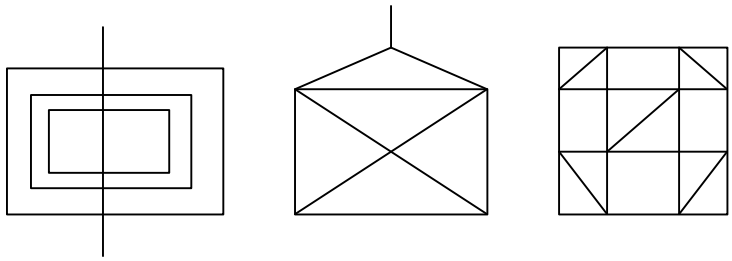


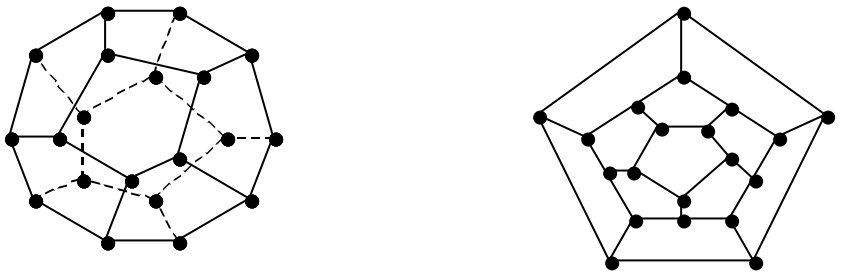
图 1.1

2．如果可能，画出一个点数为偶数而边数为奇数的 Euler 图，否则说明为什么不存在这样的图.

3．在棋盘上跳动一个马，使完成每一个可能的跳动恰好一次，问这是否可能？

§ 2 Hamilton 图

Hamilton 在 1859 年发明了一种“环游世界”游戏，即在如图 2.1(a)所示的 12 面体上，从一个顶点出发，沿棱行走，要求经过每个顶点恰好一次后返回出发点，这相当于在图 2.1(b)中找出一条包含图中所有顶点的圈.



(a) (b)

图 2.1

定义 1 设 G 是一个图，G 中包含所有顶点的圈称为 Hamilton 圈，含有 Hamilton 圈的图称为 Hamilton 图，G 中含有所有顶点的路称为 Hamilton 路，含有 Hamilton 路的图称为半 Hamilton 图.

初看起来，Hamilton 圈(路)与 Euler 回路(开迹)提法上有点类似，Euler 回路(开迹)遍

游所有边，而 Hamilton 圈(路)遍游所有点. 但这两个判定问题的难度却大不相同，Hamilton 图的判定问题是所谓的 NP 完全问题，有效的 Hamilton 图的判定算法至今尚未找到——似乎不可能找到. 下面我们给出判断 Hamilton 图的几个常用(充分或必要)条件，为此，先介绍几个记号.

假设 G 是一个图，$S\subseteq V$，我们将用 $G-S$ 表示从 G 中去掉 S 中的点以及与其关联的边得到的子图，$G-\{v\}$ 也记为 $G-v$；又对边集 E 的子集 T，用 $G-T$ 表示从 G 中去掉 T 中的边后得到的图. $G-\{e\}$也记为 $G-e$；类似地，在 G 中加入边集 T 后得到的图记为 $G+T$，$G+\{e\}$也记为 $G+e$.

定理 1　设 G 是 Hamilton 图，则对于顶点集 V 的任一非空真子集 S，均有

$$\omega(G-S)\leqslant|S|.$$

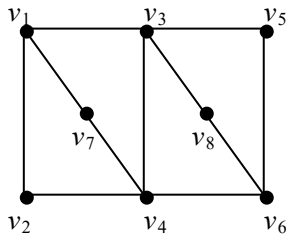
证明　设 C 是图 G 的一个 Hamilton 圈，则对 V 的任一非空真子集 S，必有

$$\omega(C-S)\leqslant|S|,$$

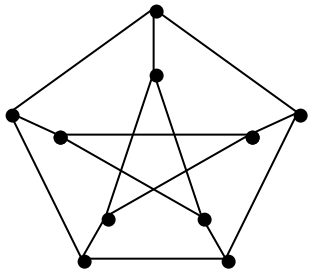
由于 G 是由 C 中再加入一些边构成的，故 $G-S$ 也必是由 $C-S$ 加入一些边构成，因而

$$\omega(G-S)\leqslant \omega(C-S)\leqslant|S|. \qquad \blacksquare$$

例 1　在图 2.2(a)所示的图中，取 $S=\{v_1, v_4\}$，则 $G-S$ 有 3 个连通分支，故该图不是 Hamilton 图.



(a)



(b)

图 2.2

以上定理给出了 Hamilton 图的必要条件，利用该定理有时可方便地判定某图不是 Hamilton 图，但该方法并不总是有效的，例如，图 2.2(b)中的图(Peterson 图)不是 Hamilton 图，但无法用定理 1 判定.

下面再来给出一个 Hamilton 图的充分条件. 若图中的顶点不少于 3 个，则 Hamilton 圈决不会在两点之间走两次，也不会经过自环，故平行边与自环对 Hamilton 图的构成是无关紧要的，因此，只需讨论简单图即可.

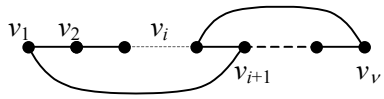
定理 2　设 G 是简单图，且 $\upsilon\geqslant 3$，$\delta\geqslant \upsilon/2$，则 G 是 Hamilton 图.

证明　用反证法　假设 G 不是 Hamilton 图，由于在 G 的任意两个不相邻顶点间加入一边，得到的图仍满足定理条件，且完全图必为 Hamilton 图，因此，通过加边，总可以使 G 变成一个满足定理条件的极大非 Hamilton 图(所谓极大非 Hamilton 图，是指这样的图，它不是 Hamilton 图，但在该图的任意两不相邻顶点间加入一边，必定成为 Hamilton

图). 因而不妨设 G 是极大非 Hamilton 图，因为 G 不可能是完全图，故可从中取两个不相邻顶点 u，v，由于 G 是极大非 Hamilton 图，故 $G+uv$ 必是 Hamilton 图，且 $G+uv$ 的每个 Hamilton 圈必然包含边 uv，于是，在 G 中存在起点为 $u=v_1$，终点为 $v=v_\upsilon$ 的 Hamilton 路 $v_1v_2\cdots v_\upsilon$，令

$S=\{v_i \mid v_1v_{i+1}\in E(G)\}$，$T=\{v_i \mid v_i v_\upsilon\in E(G)\}$，

由于 $v_\upsilon\notin S\cup T$，故 $|S\cup T|<\upsilon$. 又，若 $S\cap T\neq\varnothing$，则可取 $v_i\in S\cap T$，则 G 包含 Hamilton 圈 $v_1v_2\cdots v_iv_\upsilon\cdots v_{i+1}v_1$(如下图)，



矛盾，故 $S\cap T=\varnothing$，所以，

$$d(u)+d(v)=|S|+|T|=|S\cup T|<\upsilon, \tag{1}$$

这与 $\delta\geqslant\upsilon/2$ 矛盾，从而 G 必为 Hamilton 图. ▌

1974 年，Bondy 和 Chvatal 对该证明稍加修改，便得到一个更有力的定理.

引理 设 G 是简单图，u 和 v 是 G 中不相邻的顶点，且满足

$$d(u)+d(v)\geqslant\upsilon \tag{2}$$

则 G 是 Hamilton 图当且仅当 $G+uv$ 是 Hamilton 图.

证明 若 G 是 Hamilton 图，则显然 $G+uv$ 也是 Hamilton 图. 反之，若 $G+uv$ 是 Hamilton 图，与定理 2 完全类似可以证明，若 G 不是 Hamilton 图则(1)式成立，与(2)式矛盾，因而知 G 必是 Hamilton 图. ▌

这样，为判断 G 是否是 Hamilton 图，可对图 G 中满足 $d(u)+d(v)\geqslant\upsilon$ 的不相邻顶点对进行连接，且这种连接可反复进行，由此引出图 G 的闭包的概念.

设 G 是一个图，反复连接满足 $d(u)+d(v)\geqslant\upsilon$ 的不相邻顶点 u，v，直到没有这样的顶点对为止，这样得到的图称作图 G 的闭包，记为 $C(G)$.

可以证明，对任何图 G，$C(G)$是存在唯一的，图 2.3 表明了一个求闭包的过程.

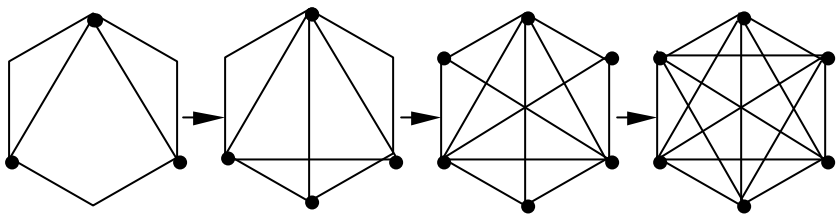


图 2.3

定理 3　简单图 G 是 Hamilton 图当且仅当 $C(G)$是 Hamilton 图.

证明 假设 $C(G)$由 G 依次加入边 e_1，e_2，…，e_n 构成，则由于在求闭包 $C(G)$的过程

中，每次连接的点 u，v 都满足 $d(u)+d(v)\geqslant v$，故由引理知

G 是 Hamilton 图 $\Leftrightarrow G+e_1$ 是 Hamilton 图

$\Leftrightarrow G+\{e_1, e_2\}$ 是 Hamilton 图

$\Leftrightarrow \cdots\cdots$

$\Leftrightarrow G+\{e_1, e_2, \cdots, e_n\}$ 是 Hamilton 图，

即 G 是 Hamilton 图 $\Leftrightarrow C(G)$是 Hamilton 图.

推论 1　若 $C(G)$是完全图，则 G 是 Hamilton 图.

推论 2　若 G 中任意不相邻顶点 u，v 均满足 $d(u)+d(v)\geqslant v$，则 G 是 Hamilton 图.

对于有向图，我们也可类似定义 Hamilton 有向图和半 Hamilton 有向图.

定义 2　设 D 是有向图，D 中包含所有顶点的有向圈称为 Hamilton 有向圈，含有 Hamilton 有向圈的有向图称为 Hamilton 有向图，D 中包含所有顶点的有向路，称为 Hamilton 有向路，含有 Hamilton 有向路的有向图称为半 Hamilton 有向图.

由定义 2 可见，Hamilton 有向图必定是强连通的.

下面的两个定理，指出了竞赛图与 Hamilton 图的关系.

定理 4　竞赛图必是半 Hamilton 有向图.

定理 5　强连通的竞赛图必是 Hamilton 有向图.

证明　略.

最后，我们介绍一个图论中的著名问题——货郎担问题.

设有 n 个城镇，其中每两个城镇之间的直接距离是已知的，一个货郎自一城镇出发巡回售货，问这个货郎应该如何选择路线，使每个城镇恰好经过一次，并且总的行程最短. 显然，这个问题也就是要在一个带权完全图中，找一个权最小的 Hamilton 圈.

在 n 个顶点的带权完全图中，所有可供选择的不同 Hamilton 圈共有$(n\text{-}1)!/2$ 个，在这么多的 Hamilton 圈中求一个权最小者，其计算量是相当大的，解决这个问题的有效算法至今尚未找到，下面我们给出一个较好的近似算法：最近邻居法.

设 G 是具有 n 个顶点的带权完全图，w 是其权函数，求最小权 Hamilton 圈的最近邻居法步骤如下：

(1) 任选一点 v_0 作起始点，找一个与 v_0 最近的相邻点 x，得到一条路 v_0x；

(2) 设已得到路 $W=v_0v_1\cdots x$，x 是新加到这条路 W 中的点，从不在路中的所有点中，选一个与 x 最近的相邻点 y，将它加到 W 中，构成一条新的路：$v_0v_1\cdots xy$，重复该步骤，直到 G 中所有顶点都在所形成的路中；

(3) 连接 v_0 和最后加到路中的顶点，构成一圈，它就是求出的 Hamilton 圈.

例 2　图 2.6 表明了对图 2 . 4 用最近邻居法求 Hamilton 圈的过程. 该方法求出的 Hamilton 圈的权为 40，而真正解的权为 37，见图 2.5.

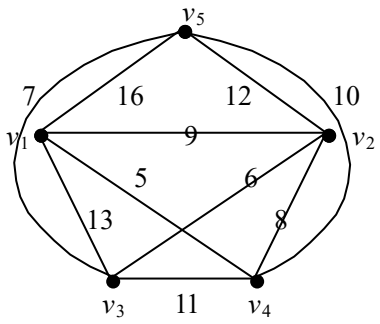


图 2.4

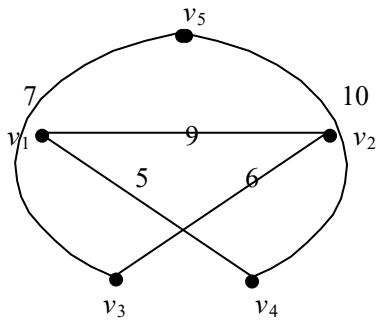


图 2.5

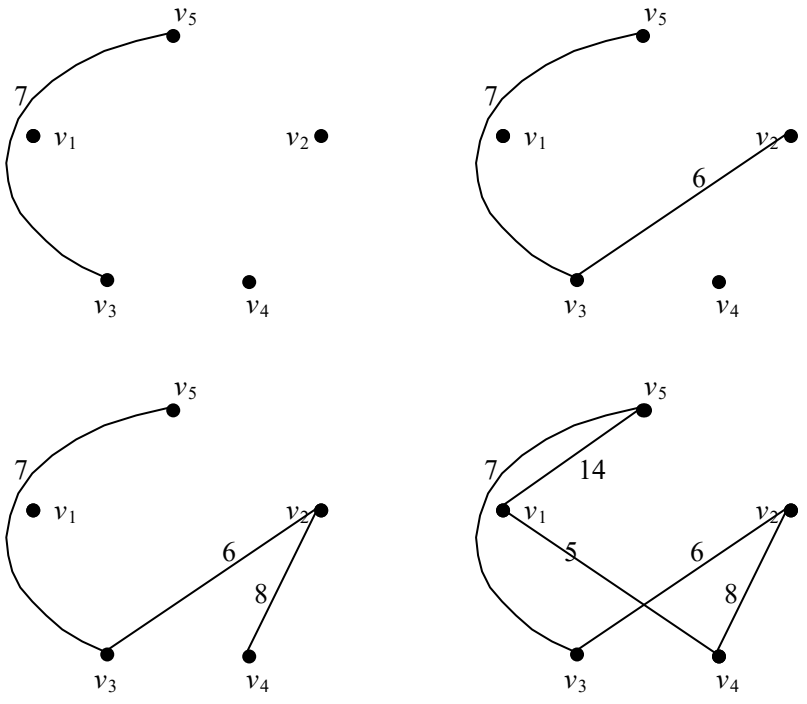


图 2.6

习 题 二

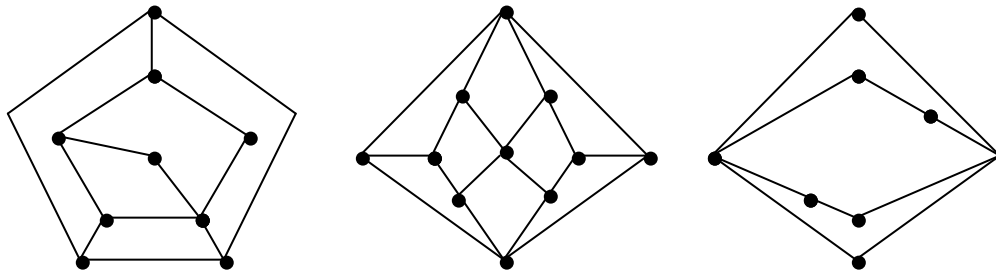
1．找一个图使它既是 Euler 图又是 Hamilton 图.

找一个图使它是 Euler 图，但不是 Hamilton 图.

找一个图是 Hamilton 图，但不是 Euler 图.

找一个图既不是 Euler 图，也不是 Hamilton 图.

2．判别图 2.7 中的图是否是 Hamilton 图或半 Hamilton 图．



(*a*)　　(*b*)　　(*c*)

图 2.7

3．证明　若 G 是一个具有奇数个顶点的二分图，则 G 中没有 Hamilton 圈，试说明图 2.8 中无 Hamilton 圈．

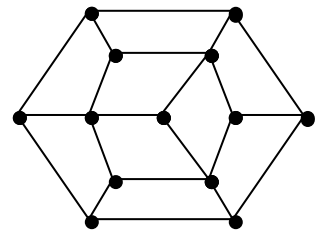


图 2.8

4．若一个图中对每一条边能给它定一个方向，使得所得到的有向图强连通，则称这个图是可定向的．

（1）　证明任意一个 Euler 图是可定向的．

（2）　证明任意一个 Hamilton 图是可定向的．

第十章　树

§1　树

定义 1　连通无回路的图称为树，树中度为 1 的点称为树叶，度大于 1 的点称为分枝点或内点，每个连通分支均为树的图称为森林.

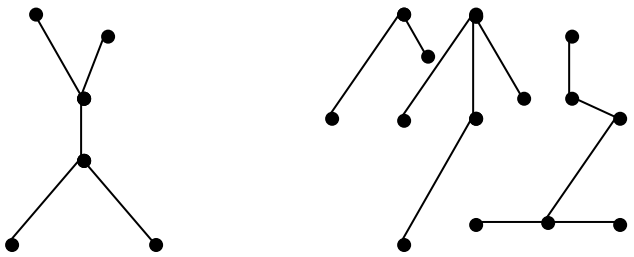


图 1.1

图 1.1(*a*)是一棵树，图 1.1(*b*)是一个森林.

下面我们给出几个有关树的等价条件.

定理 1　设图 T 是有 n 个顶点、 ε 条边的非平凡图，则下列各条等价.

(1)　T 是树.

(2)　T 中无回路，且 $\varepsilon = n-1$.

(3)　T 连通，且 $\varepsilon = n-1$.

(4)　T 中无回路，且在 T 的任意两个不相邻点之间添加一边恰得一条回路.

(5)　T 连通，删去任一边则不连通.

(6)　T 的任意两个不同顶点之间恰有一条路.

证明　(1) $\Rightarrow$ (2)

只需证明 $\varepsilon = n-1$. 对顶点数 n 采用归纳法，$n=2$ 时显然成立，假设 $n=k$ 时结论成立，考虑 $n=k+1$ 的情况. 由于 T 是连通的且不是平凡图，故其每个顶点的度至少为 1，又 T 中无回路，由第八章 §2 定理 1 知，T 中存在度小于 2 的顶点，从而 T 中必有度为 1 的顶点 u，从 T 中删去 u 及其关联边 e，便得到一个只有 k 个顶点的树，由归纳假设知，它有 $k-1$ 条边，于是，T 中有 k 条边，即结论对 $n=k+1$ 也成立，从而对任何 n 都成立.

(2) $\Rightarrow$ (3)

用反证法，若图 T 不连通，不妨设 T 有 ω 个连通分支($\omega>1$)：T_1，T_2，…，T_ω，其

顶点数分别为 n_1，n_1，…，n_ω，则 $\sum_{i=1}^{\omega} n_i = n$．由于每个连通分支都是连通无回路的，因而是树，从而 $\varepsilon_i = n_i - 1$，所以 T 中的边数为

$$\varepsilon = \sum_{i=1}^{\omega} \varepsilon_i = n - \omega < n - 1,$$

矛盾，故 T 必定连通．

(3) ⇒ (4)

首先证明 T 是无回路的，对顶点数 n 采用归纳法，$n=2$ 时，$\varepsilon = 1$ 且 T 连通，显然是无回路的．假设 $n=k$ 时结论成立，考虑 $n=k+1$ 的情况，由于 T 是连通的，且不是平凡图，所以，每个顶点度数至少为 1，利用总度数与边数的关系我们还可证明必存在 $u \in V$ 使 $d(u)=1$，事实上，如果每个顶点的度数均≥2，则

$$2\varepsilon = \sum_{v \in V} d(v) \geq 2(k+1),$$

即 T 中至少有 $k+1$ 条边，这与假设矛盾，从而证明了必有一点 $u \in V$，使 $d(u)=1$．现删去 u 及其关联边，得到一个连通且具有 k 个顶点、$k-1$ 条边的图 T'，由归纳假设，T' 中无回路，将 u 及其关联边加入 T' 得到的图(即 T)也必无回路，归纳法完成．若在 T 的两个不相邻顶点 u，v 之间增加一边 uv，由于 T 是连通的，必定存在一条(u，v)路，该路与 uv 一起便构成一回路，下证该回路是唯一的，事实上，如果不唯一，删去 uv 后，T 中仍有回路，矛盾．

(4) ⇒ (5)

若 T 不连通，则必有顶点 u，v 不连通，在 T 中加入边 uv，则不会产生回路，与假设矛盾，又由于 T 中无回路，易知删去一边后必不连通．

(5) ⇒ (6)

由于 T 是连通的，任意两点 u，v 之间必有路，如果有多于一条的路，则图中必有回路，删去该回路上一边，所得图仍然连通，矛盾，故 u，v 间恰有一条路．

(6) ⇒ (1)

由于任意两顶点间均有一条路，故必是连通的，若有回路，则该回路上任意两点间均至少有两条路，矛盾，故无回路，即 T 是树．▌

定理 2　任意一棵非平凡树 T 中，至少有两片树叶．

证明　设 T 有 n 个顶点，则 T 的边数 $\varepsilon(T) = n-1$，从而由总度数与边数的关系知

$$\sum_{v \in V} d(v) = 2(n-1), \tag{1}$$

因为 T 是连通非平凡图，T 中任意一点 v 均满足 $d(v) \geq 1$，若 T 中度为 1 的点即树叶不超过 1 个，则

$$\sum_{v \in V} d(v) \geq 2(n-1) + 1,$$

与(1)式矛盾，从而 T 中至少有两片树叶．▌

习 题 一

1．画出具有 6 个顶点的所有树．

2．证明　非平凡树中最长路的起点和终点均为树叶．

3．证明　一棵树恰有 2 片树叶，则此树为路．

4．(1) 证明　对于 n 个顶点的树，其顶点度数之和为 $2n-2$．

(2) 对于 $n\geqslant 2$，设 d_1，d_2，…，d_n 是 n 个正整数，且 $\sum_{i=1}^{n} d_i = 2n-2$，证明，存在顶点度数为 d_1，d_2，…，d_n 的一棵树．

5．$\triangle \geqslant k$ 的树至少有 k 个树叶．

§ 2　生成树

在前面我们已经介绍过生成子图的概念，特别地，我们再引入下述定义．

定义 1　若图 G 的生成子图 T 是树，则称 T 为 G 的生成树．

定理 1　G 是连通图当且仅当 G 有生成树．

证明　充分性　若 G 有生成树 T，则由于 T 是连通的，易知 G 必是连通的．

必要性　设 G 是连通图，若 G 中无回路，则 G 本身就是一棵树，从而有生成树．若 G 中有回路，从回路中去掉一边，得到的图 G_1 仍然连通，若 G_1 中无回路，则 G_1 是 G 的生成树，若 G_1 中有回路，从回路中删去一边，…，一直下去，最后必得到一个图 G_k，G_k 是连通的且无回路，从而 G_k 是 G 的生成树．▌

显然，一个图 G 可能有多棵生成树，特别地，在赋权图当中，生成树的权一般也是不相同的，由于赋权图中的权往往代表着某种花费，寻找权最小的生成树，便有一定的实际意义．

权图 G 中带权最小的生成树称为最小生成树或最优树，看下面例子．

我们设想要建筑一个连接若干城市的铁路网，已知建造直接连接城市 u 与 v 的铁路费用为 C_{uv}，试设计一个铁路网，要求建造费用最小．

将每个城市作为顶点，在顶点 u，v 之间连接一条权为 C_{uv} 的边，则得到一个权图 G，显然，我们建造的铁路网应该是连通的，且必定没有回路，因而，我们面临的问题便是求 G 的最小生成树．

下面介绍最小生成树的 Kruskal 算法，先来介绍一下其直观思想．

设有赋权图 G，既然我们要寻找 G 的最小生成树，我们所取边的权当然是越小越好，

采用贪心策略，我们首先找到 G 的权最小的边，并取出来．然后，在剩下的边中再找出权最小且与已选出的边不构成回路的，再把它取出来，…，一直下去，直到选不出边．在上述过程中，我们得到的图是无回路的．进一步地，我们可证明我们最终得到的是一棵最小生成树．

将以上直观思想叙述成算法，即是 Kruskal 算法．

设 G 是简单连通权图，w 是其权函数．

(1) 选取 G 的一边 e_1，使 $w(e_1)=\min\{w(e)|e\in E\}$，令 $E_1=\{e_1\}$，

(2) 若已选出 $E_i=\{e_1, \cdots, e_i\}$，那么，从 $E-E_i$ 中选取一边 e_{i+1}，使

(Ⅰ) $E\cup\{e_{i+1}\}$ 的导出子图中不含回路；

(Ⅱ) $w(e_{i+1})=\min\{w(e)|\ e\in E-E_i, E_i\cup\{e\}$的导出子图无回路$\}$

(3) 若 e_{i+1} 存在，令 $E_{i+1}=E_i\cup\{e_{i+1}\}$，$i+1\to i$，转(2)，若 e_{i+1} 不存在，则输出 $E_i=\{e_1, \cdots, e_i\}$，算法停止．

可以证明，如上算法所得到的边集的导出子图 T^*(就称其为算法得到的子图)，即为 G 的最小生成树．

定理 2　Kruskal 算法得到的图 T^*是 G 的最小生成树．

证明　由算法可知，T^*必包含了 G 的所有顶点且是连通、无回路的，从而可知 T^*是生成树．因而，若设 G 有 n 个顶点，则 T^*中也必有 n 个顶点，从而 T^*中必有 $n-1$ 条边，于是，T^*是边集 $E_{n-1}=\{e_1, e_2, \cdots, e_{n-1}\}$ 的导出子图，这里，$e_1, e_2, \cdots, e_{n-1}$依次是算法产生的边．

下面用反证法证明 T^*是最小生成树．若不然，取所有最小生成树中与 T^*具有最多公共边者为 T_1，则边集 $E(T^*)\neq E(T_1)$，设 e_k是 T^*中第一条不在 T_1中的边，即 $e_1, e_2, \cdots, e_{k-1}\in E(T_1)$，$e_k\notin E(T_1)$．由树的性质，$T_1+e_k$必有回路 C．由于 T^*中无回路，C 中的边必有不在 T^*中者，设回路中的边 $e'_k\notin E(T^*)$，显然 $T_2=(T_1+e_k)-e'_k$也是一棵生成树，且

$$w(T_2)=w(T_1)+w(e_k)-w(e'_k)$$

因为 $e_1, e_2, \cdots, e_{k-1}, e'_k\in E(T_1)$，故这 k 条边不构成回路，由 Kruskal 算法中 e_k的取法知 $w(e'_k)\geqslant w(e_k)$．所以，$w(T_2)\leqslant w(T_1)$，因此 T_2也是一棵最小生成树，且与 T^*的公共边多于 T_1，与 T_1的定义矛盾．这样就证明了 T^*必为最小生成树．▌

习 题 二

1．Kruskal 算法能否用来：

(a) 在连通赋权图中求最大权生成树？

(b) 在不连通图中求最小权生成林？

如果能，怎么求？写出算法．

2．求出图 2.1 的最小生成树．

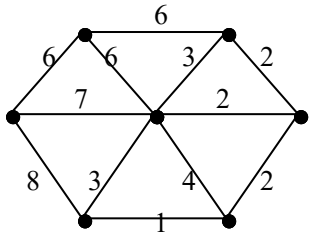


图 2.1

§ 3　有向树

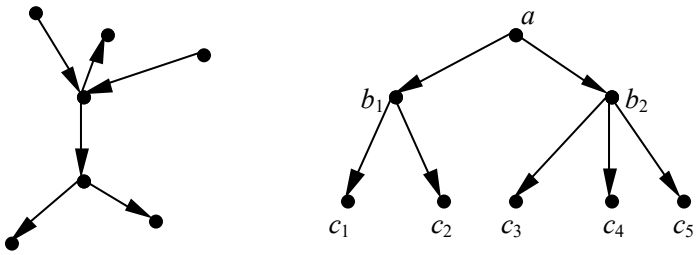
上面两节，我们以无向图的概念为基础讨论了树的定义及性质，在本节，我们把问题的讨论转移到有向图上面来.

定义 1　设 D 是一个有向图，如果在不考虑弧的方向时 D 是一棵树(即 D 的底图是一棵树)则称 D 为一棵有向树.

因为在有向树的定义中没有考虑弧的方向，这对某些与“方向”有关的问题是不够的，因此我们再考虑有向树的一种特殊情况.

定义 2　若一棵有向树中恰有一个顶点的入度为 0，其余所有顶点的入度均为 1，则称该有向树为有根树(或树形图)，入度为 0 的顶点称为根.

例 1　图 3.1(a)是一棵有向树，图 3.1(b)是一棵有根树，其中，a 是根.



(a)　　(b)

图 3.1

定理 1　设 T 是一棵有根树，r 是 T 的根，则 r 到其余每个顶点恰有一条有向路.

证明　设 v 是 T 中任意一点，且 $v\neq r$，由于 T 是有向树，故在 T 的底图上必有一条(r, v)-路，不妨设为

$$W=re_1v_1e_2\cdots e_kv \tag{1}$$

由于 r 的入度为 0，弧 e_1 的方向必是从 r 到 v_1，又 v_1 的入度为 1，e_2 的方向必定从 v_1 到 v_2，…，一直下去，e_k 的方向必定从 v_{k-1} 到 v，因而，W 是一条 r 到 v 的有向路. 由于 T

的底图是树，W 必是唯一(r, v)-路，从而必定是唯一的(r, v)-有向路. ▌

根据上面定理我们知道，一棵有根树 T，可用下述方法画出. 首先画出 T 的根 r，在 r 的下面画出 r 的所有邻点，并从 r 到其邻点连一条有向弧，然后，对 r 的每个邻点 v，在 v 的下方画出其除 r 之外的所有邻点 v_1，v_2，…，v_p，并从 v 到 $v_i(i=1, 2, \cdots, p)$连一条有向弧，……，一直进行下去，由定理 1 可知，最后必可画出整个 T，如图 3.2.

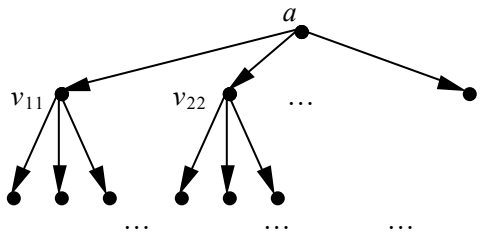


图 3.2

按照以上画法，弧线的方向总是向下的，因此，我们可以省略其箭头. 由于有根树总可以画成图 3.2 的形式，因此可以直观地说，有根树实际上描述了一个离散结构的层次关系，而层次结构在计算机领域是一种非常重要的结构，从而可知，有根树在计算机领域有着非常广泛的应用.

有根树中，还有一些专门术语，我们列举几个如下：

定义 3　设 u 是有根树的分枝点，若从 u 到 s 有一条弧〈u，s〉，则称 s 为 u 的儿子，u 为 s 的父亲；同一父亲的儿子称为兄弟；若从 u 到 v 有一条有向路，则称 v 是 u 的子孙，u 是 v 的祖先；从根到某一顶点的路长称为该顶点的路长或层数，从根到树叶的最大层数，称为有根树的高.

例 2　在图 3.3(a)中，r 是树根，a_1，a_2 是 r 的儿子(r 是 a_1，a_2 的父亲)，b_1，b_2，b_3 是 a_1 的儿子(a_1 是 b_1，b_2，b_3 的父亲)，b_1，b_2，b_3 也是 a_1，r 的子孙(a_1，r 是 b_1，b_2，b_3 的祖先)；a_1 与 a_2 是兄弟，b_1，b_2，b_3 也是兄弟；a_1，a_2 的层数为 1，而 b_1，b_2，b_3 的层数为 2；该有根树的树高为 2.

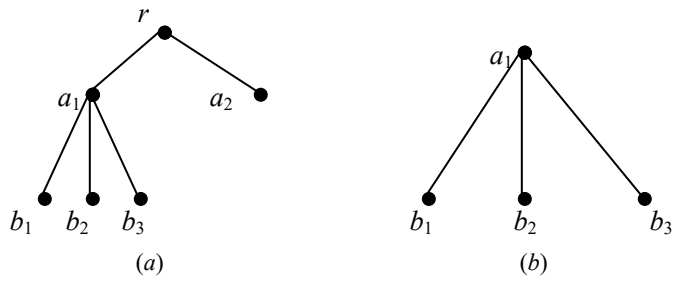


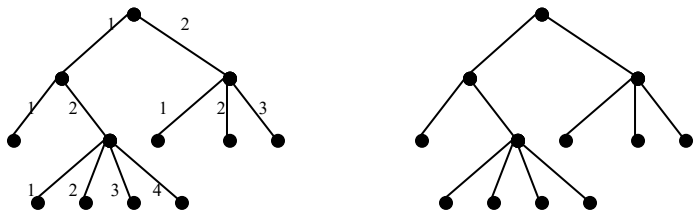
图 3.3

定义 4　设 u 是有根树 T 的一个顶点，V_u 是 u 及其子孙构成的顶点集，V_u 的导出子图称为 T 的以 u 为根的子树. 例如，图 3.3(b)是图 3.3(a)的以 a_1 为根的子树.

在上面的讨论中，我们没有考虑同一分枝点发出的弧的次序，但在许多实际问题中，需要考虑这种次序，为此，引入下述定义.

定义 5　在有根树中，将每个分枝点发出的弧从左到右依次标以正整数 1，2，3，…，则该有根树称为有序树.

例如，图 3.4(a)是一棵有序树. 既然我们已规定标号总是从左到右依次给出，因此，在画有序树时可以将这些标号省略，于是，有序树图 3.4(a)可以简化成图 3.4(b)的形式.



(a)　　(b)

图 3.4

定义 6　在有序树中，如果每个顶点 v 都满足 $d^+(v)\leqslant m$，则称该有序树为 m 叉树，如果每个顶点 v 都满足 $d^+(v)=m$，称该有序树为正则 m 叉树.

一类重要的 m 叉树是二叉树和正则二叉树，对于二叉树，一个分枝点的两个(或一个)儿子按其位置分别称为左儿子、右儿子，以左、右儿子为根的子树分别称为左子树、右子树.

例 3　算术表达式 $a-b+(c/d+e/f)$可以用图 3.5 中的二叉树表示.

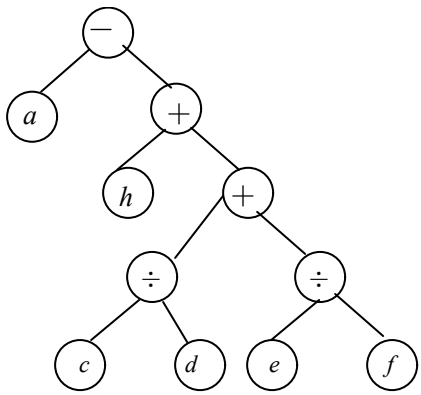


图 3.5

所有运算对象都是树叶，所有运算符都是分枝点，如果将弧线次序改变，得到的二叉树将对应另一个(不一定相等的)算术表达式.

定理 2　在正则 m 叉树中，分枝点数 i 与树叶数 l 满足

$$(m-1)i=l-1.$$

证明　因为每个分枝点都有 m 个儿子，且每个儿子都是互不相同的，所以，分枝点儿子的总数为 mi．又，正则 m 叉树中除树根之外都是儿子，故顶点总数应为 $mi+1$，即 $i+l=mi+1$，从而 $(m-1)i=l-1$．▌

定理 3　设 T 是正则 m 叉树，I 表示分枝点的路长总和，L 表示树叶的路长总和，则

$$L=(m-1)I+mi$$

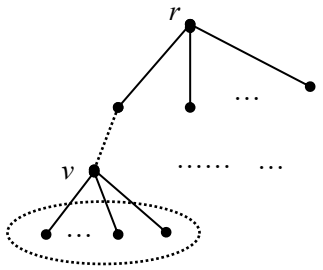
其中，i 是分枝点数．

证明　对分枝点数 i 运用归纳法．当 $i=1$ 时，$I=0$，$L=m$，所以 $L=(m-1)I+mi$．假设 $i=k-1$ 时结论成立，现令 $i=k$，删去具有同一个父亲 v 的 m 个树叶，得到一棵正则 m 叉树 T'，由于 v 在 T'中是树叶，故 T'中有 $k-1$ 个分枝点，这些分枝点的总路长为

$$I'=I-l,$$

其中，l 是 v 的路长．删去 v 的 m 个儿子使树叶总路长减少 $m(l+1)$，又因 v 变成树叶，使树叶总路长增加 l，从而 T'中树叶总路长为

$$L'=L-m(l+1)+l,$$



由归纳假设

$$L'=(m-1)I'+m(k-1),$$

因此　　$L-m(l+1)+l=(m-1)(I-l)+m(k-1)$，

即　　$L=(m-1)I+mk$，

从而，$i=k$ 时结论也成立，归纳法完成．

习　题　三

1．写出下列表达式的二叉树表示

$$\left(\frac{(a+b)\cdot c}{d}+b(d+f)\right)^{-1}\quad .$$

2．对非平凡正则 m 叉数的分枝点数 i 施行归纳法，以证明定理 2．

3．对有 n 个顶点的正则二叉树，给出树高的上、下界(用 n 表示)．

第十一章　平面图　图的着色

§1　平面图

1. 平面图的定义　定义 1　如果一个图能画在平面上，使得它的边在端点之外不相交，则称这个图为平面图。平面图 G 的这样一种画法 $\widetilde{G}$，称为 G 的一个平面嵌入。平面图 G 的平面嵌入 $\widetilde{G}$ 称为平图。

2. 面的定义　定义 3　设 G 是一个平图，则 G 把平面划分成若干个连通区域，每个连通区域的闭包称为 G 的一个*面*，其中恰有一个无界的面，称为*外部面*。围成面的边数，称为面的度，记为 $d(F)$，其中 F 表示一个面。

3. Euler 公式　定理 1　若 G 是连通平图，则

$$v-\varepsilon+f=2$$

其中，f 是 G 的面数，这个公式称为 Euler 公式。

证明　对 G 的边数 ε 用归纳法：

1）基本情况：当 $\varepsilon=1$ 时，Euler 公式显然成立。

2）归纳假设：设当 $\varepsilon=m-1$ 时 Euler 公式成立。

3）归纳结论：设 G 的边数 $\varepsilon=m$，若 G 中有一个度为 1 的顶点，删去该顶点及其关联边得到一连通平图 G_1，G_1 中有 $m-1$ 条边，$v-1$ 个顶点，f 个面，于是由归纳假设知 $v-1-(m-1)+f=2$，即有 $v-m+f=2$。

若 G 中无度为 1 的顶点，则 G 中必定有圈，从该圈中删去一边，得到一连通平图 G_2，G_2 中有 $m-1$ 条边，v 个顶点，$f-1$ 个面，由归纳假设知

$$v-(m-1)+f-1=2，\text{即 } v-m+f=2。$$

因此，当 $\varepsilon=m$ 时 Euler 公式对成立，归纳法完成。

推论 1　给定平面连通图 G，则 G 的所有平面嵌入有相同的面数.

证明　设 G_1，G_2 是 G 的两个平面嵌入，则

$$v(G_1)=v(G_2)，\quad \varepsilon(G_1)=\varepsilon(G_2)，$$

因此，若设 G_1，G_2 的面数分别为 f_1，f_2，则由 Euler 公式，得

$$f_1=2+\varepsilon(G_1)-v(G_1)=2+\varepsilon(G_2)-v(G_2)=f_2。$$

由于该推论，以后我们说平面图的面数也是有意义的.

推论 2　若 G 是平面简单图，$v\geqslant 3$，则 $\varepsilon\leqslant 3v-6$.

证明　显然只要对连通图讨论就够了，设 $\widetilde{G}$ 是 G 的一个平面嵌入，不妨设 $\widetilde{G}$ 有 f 个面 F_1，F_2，…，F_f。

1）当 $v=3$ 时公式显然成立

2）下设 $v>3$。由于 G 是平面简单图，$\widetilde{G}$ 的每个面至少由三条边围成，即 $d(F_i)\geqslant 3$，

$(i=1, 2, \cdots, f)$，因此 $\sum_{i=1}^{f} d(F_i) \geq 3f$ 。

另一方面，由于每条边至多是两个面的公共边，也就是说，在计算 $\sum_{i=1}^{f} d(F_i)$ 时每条边至多被计算两次，因此 $2\varepsilon \geq \sum_{i=1}^{f} d(F_i)$ ，

从而，$2\varepsilon \geq 3f$，所以 $f \leq 2\varepsilon/3$。利用欧拉公式，有

$$v - \varepsilon + 2\varepsilon/3 \geq 2 \text{，因此}$$

$$\varepsilon \leq 3v - 6。$$

推论 3　若平图 G 的每个面由至少四条边围成，则

$$\varepsilon \leq 2v - 4.$$

推论 4　K_5 与 $K_{3,3}$ 是非平面图.

证明　对于 K_5：$v=5$，$\varepsilon=10$，若 K_5 是平面图，则由推论 2 知 $3 \cdot 5 - 6 \geq 10$ 矛盾，故 K_5 是非平面图。

对于 $K_{3,3}$：由于它是二分图，必不含奇圈，因此，如果 $K_{3,3}$ 是平面图，则其每个面至少由四边围成，从而

$$\varepsilon \leq 2v - 4,$$

由于 $\varepsilon = 9$，$v = 6$，故 $9 \leq 2 \cdot 6 - 4$，矛盾，所以 $K_{3,3}$ 必非平面图。

定理 2　在平面简单图 G 中，至少存在一个顶点 v_0，$d(v_0) \leq 5$.

证明　用反证法　假设一个平面简单图的所有顶点度数均大于 5，则

$$6v \leq \sum_{v \in V} d(v) = 2\varepsilon \leq 6v - 12,$$

矛盾，因此，平面简单图中至少有一个顶点 v_0，使 $d(v_0) \leq 5$。

习　题　一

1. (1) 证明　对于 K_5 的任意边 e，$K_5 - e$ 是平面图.
   (2) 证明　对于 $K_{3,3}$ 的任意边 e，$K_{3,3} - e$ 是平面图.
2. 若 G 是一个平面图，证明 $v - \varepsilon + f = \omega(G) + 1$.
3. 在一个连通平图中，若每个面至少由 $k(\geq 3)$ 条边围成，证明 $\varepsilon \leq k(v-2)/(k-2)$.
4. 证明下图不是平面图.

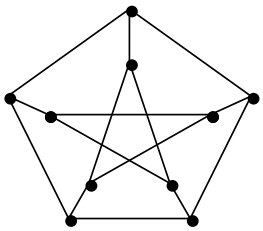


图 1.3

§ 2　对偶图

设 G 是一个平图（平面图的平面嵌入），现根据其面的相邻关系作一图 G^*如下：

(1) 对应 G 的面 F_1，F_2，…，F_f作顶点 F_1^*，F_2^*，…，F_f^*;

(2) 当且仅当 $e\in E(G)$是 G 的两个面 F_i，F_j的公共边时，在 F_i^* 与 F_j^* 之间连一边 e^*；

(3) 当且仅当 $e\in E(G)$仅是一个面 F_i的边界时，在 F_i^* 上作一自环 e^*.

图 G^* 称为 G 的对偶图.

注意，当 G 中两个面由多条边分隔时，G^* 中与之对应的顶点由多条平行边连接.

例如，图 2.1 给出一个平图及其对偶.

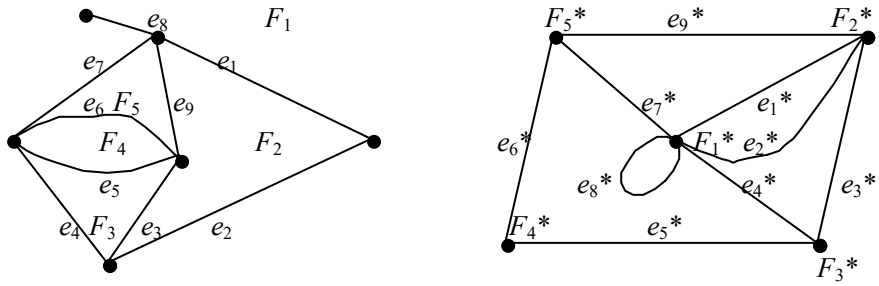


图 G　　图 G^*

图 2.1

对于任意平图 G，我们可以用如下自然的方式作出 G^* 的一个平面嵌入：

在 G 的每个面 F 中放置一个顶点，如果 G 中两个面 F_i，F_j有公共边 e，则在 F_i，F_j 中放置的顶点 F_i^* 与 F_j^* 之间画出边 e^*，使它穿过 G 的边 e 恰好一次，且不穿过其它边，这一过程如图 2.2 所示．直观上很清楚，用这种方式总可以作出平图 G 的对偶图．因此对偶图 G^*必是平面图.

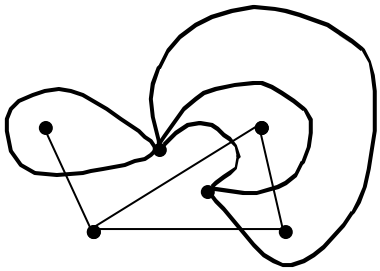
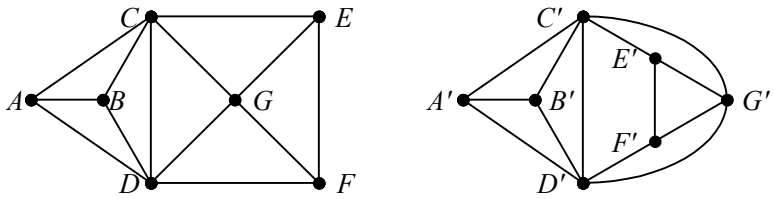


图 2.2

尽管平图的对偶图是一个抽象图，但把它看作是一个平图(比如是按上述方法作出的平图)有时是方便的，例如，这时可考察 G^*的对偶图 G^{**}. 根据这一观点可以证明，当 G 连通时，

$$G^{**} \cong G.$$

值得注意的是，同构的平图可以有不同的对偶图，例如，图 2.3 中两个图是同构的，但他们的对偶图却不同构——图 2.3(a)中有一个由 5 条边围成的面(无界面)，而图 2.3(b)却没有这样的面，因此，G_1^*，G_2^* 不同构.



(a) 图 G_1　　(b) 图 G_2

图 2.3

所以，对偶图的概念仅对平图有意义，一般不能扩展到平面图.

定理 1　设 G 是一个平图，G^*是 G 的对偶图(平图)，则

$$\upsilon^* = f, \varepsilon^* = \varepsilon, f^* = \upsilon .$$

证明　前面两个等式可直接由定义得知，第三个等式则由欧拉公式推出：

$$\left.\begin{aligned} \upsilon - \varepsilon + f &= 2 \\ \upsilon^* - \varepsilon^* + f^* &= 2 \end{aligned}\right\} \Rightarrow f^* = 2 - \upsilon^* + \varepsilon^* = 2 - f + \varepsilon = \upsilon .$$

习　题　二

1. 举例说明同一个平面图的平面嵌入可以有不同的对偶图.
2. 若一个平图和它的对偶图同构，这个平图称为自对偶的.

(1) 证明　若 G 是自对偶的，则$\varepsilon = 2\upsilon - 2$.

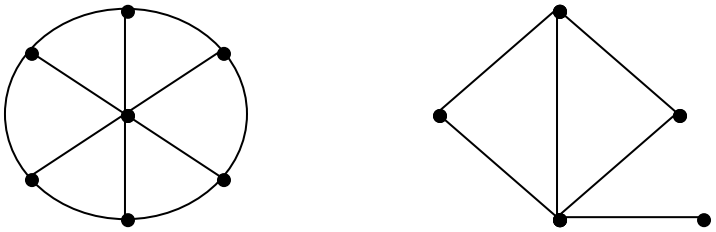
(2) 对于每个 $n\leqslant 4$，找出有 n 个顶点的自对偶平图.

§ 3　顶点着色

在这一节中，我们讨论图的顶点着色概念，然后在下一节介绍地图四色问题并证明平面图的五色定理.

定义 1　设 G 是一个图，对 G 的每个顶点着色，使得没有两个相邻的顶点着上相同的颜色，这种着色称为图的正常着色. 若图 G 的顶点可用 k 种颜色正常着色，称 G 为 k-可着色的. 使 G 是 k-可着色的数 k 的最小值称为 G 的色数，记为$\chi(G)$，如果 $\chi(G)=k$，则称 G 是 k 色的.

图 3.1(a)、图 3.1(b)的色数都是 3 .



(a)　　(b)

图 3.1

在着色问题中，若 G 是非连通图，我们只需对其每个连通分支分别考虑即可，因此不妨设 G 是连通图.

由于一个顶点不能着上不同颜色，因此我们只能考虑没有自环的图，又对于着色问题，两点之间有一条边或几条平行边是等效的，故不妨设所讨论的图无平行边.

总之，在着色问题中，只需要讨论简单连通图.

定理 1

(1) 对于完全图 K_n，有$\chi(K_n)=n$，$\chi(\sim K_n)=1$.

(2) 对于 n 个顶点构成的圈 C_n，当 n 是偶数时，$\chi(C_n)=2$，当 n 是奇数时，$\chi(C_n)=3$.

(3) 对于非平凡树 T，有$\chi(T)=2$.

(4) G 是二分图，当且仅当$\chi(G)=2$.

证明由读者自己完成.

定理 2　对于任意简单图 G，有

$$\chi(G)\leqslant 1+\triangle(G).$$

证明　需要证明 G 是 $1+\triangle(G)$-可着色的. 对 G 的顶点数施行归纳法，当 $\upsilon=1$ 时，

$\triangle(G)=0$，显然 G 是 1-可着色的，即 G 是 $1+\triangle(G)$可着色的．假设 $v=n-1$ 时成立，现设 $v=n$．删去 G 中一点 v 及其关联边，得到一个具有 $n-1$ 个顶点的图 G'，它的最大顶点度数至多是$\triangle(G)$，根据归纳假设，该图是 $1+\triangle(G)$可着色的，再将 v 及其关联边加回该图得到图 G，顶点 v 的度数至多是$\triangle(G)$，v 的相邻点最多着上$\triangle(G)$种颜色，因此可将 v 着上第 $1+\triangle(G)$种颜色，所以，G 是 $1+\triangle(G)$可着色的．从而知$\chi(G)\leqslant 1+\triangle(G)$． ▌

更进一步地，我们有

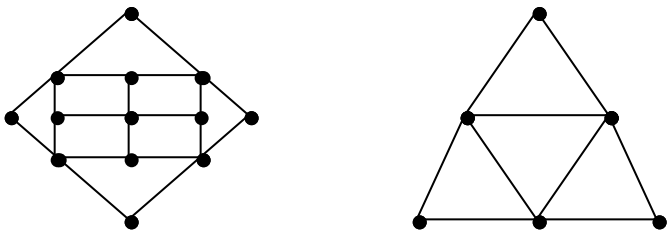
定理 3　若简单连通图 G 不是完全图且不是奇圈，则

$$\chi(G)\leqslant\triangle(G).$$

证明从略．

习　题　三

1．求图 3.2 中两个图的色数χ ．



(*a*)　　(b)

图 3.2

2．证明　图 G 是 2-可着色的，当且仅当 G 中无奇圈．

3．一个图 G 称为临界的，如果对 G 的每个真子图 H，有$\chi(H)<\chi(G)$，k 色的临界图称为 k-临界图．证明若 G 是 k-临界图，则 $\delta\geqslant k-1$．

4．证明　每个 k 色图至少有 k 个度不小于 $k-1$ 的顶点．

§4　面着色

1852 年，英国青年 Guthrie 在画地图时发现，如果相邻两国着上不同的颜色，那么，画任何一张地图只需要四种颜色就够了，这就是地图的四色问题，直到 1976 年 6 月，美国伊利诺斯大学两位教授阿培尔和哈根使用计算机，化了 1200 多个小时证明了四色问题，然而，这个问题至今未找到通常的数学证明．

定义 1　设 e 是图 G 的一条边，如果

$$\omega(G-e)>\omega(G),$$

则称 e 是 G 的割边.

例如，在图 4.1 中，e_1，e_2，e_3 是三条割边，其余边不是割边.

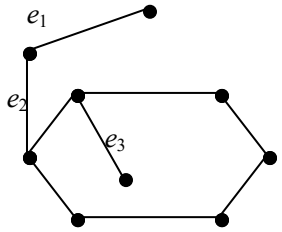


图 4.1

在平图中，割边的两侧是同一个面，或说割边即仅为一个面边界的边.

定义 2　一个没有割边的连通平图，称为地图.

地图可以有自环和平行边，地图中每一条边是两个面的公共边.

地图中的两个面称为相邻的，如果这两个面至少有一条公共边.

定义 3　设 G 是一个地图，对 G 的每个面着色，使得没有两个相邻的面着上相同的颜色，这种着色称为地图的正常面着色，地图 G 可用 k 种颜色正常面着色，称 G 是 k-面可着色的. 使得 G 是 k-面可着色的数 k 的最小值称为 G 的面色数，记为$\chi^*(G)$. 若$\chi^*(G)=k$，则称 G 是 k-面色的.

图 4.2(a)，(b)的面色数为 3，(c)，(d)的面色数为 4.

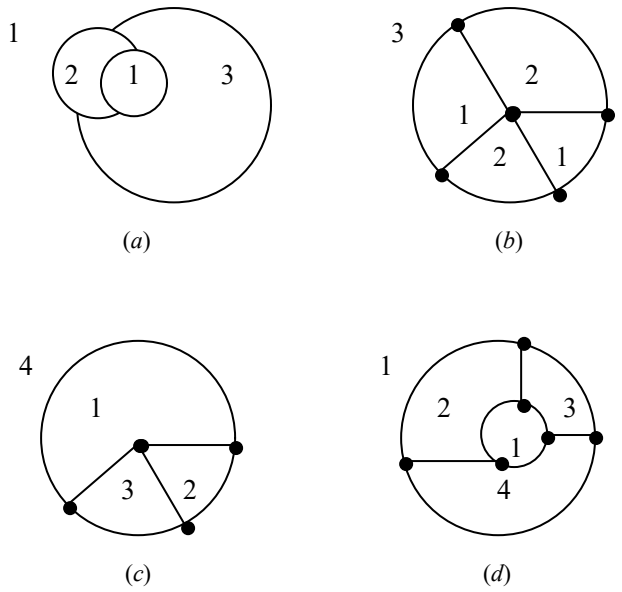


图 4.2

利用现在的术语，地图的四色问题可以叙述为：任何地图是 4 -面可着色的.

由上面的定义可以直接推出，对于任何具有对偶图 G^*的地图 G，必有

$$\chi^*(G)=\chi(G^*).$$

这样，地图的 k-面可着色问题便可化为平面图的 k-(顶点)可着色问题.

定理 1* (五色定理) 任何无自环的平面图 G 是 5-可着色的.

证明 不妨设 G 是平面简单图，下面对 G 的顶点数 υ 施行归纳法，当 $\upsilon\leqslant 5$ 时，结论显然成立. 假设当 $\upsilon=n-1$ 时结论成立. 今考虑 $\upsilon=n$ 的情况，由于 G 是平面图，在 G 中必有顶点 v_0 使 $d(v_0)\leqslant 5$，由归纳假设，$G-v_0$ 是 5 -可着色的，在给定 $G-v_0$ 的一种着色方案之后，将 v_0 及其关联边加回到图中得到 G，分两种情况：

(1) 如果 $d(v_0)<5$，则 v_0 的相邻点已着上的颜色小于等于 4 种，所以，v_0 可以着另一颜色，因此 G 是 5 可着色的.

(2) 如果 $d(v_0)=5$，则将 v_0 的相邻点依次记为 v_1，v_2，…，v_5，不妨设这五个顶点已着上五种颜色，并设 v_i 点着第 i 色，如图 4.3(a)所示.

设 H_{13} 为 $G-v_0$ 中着 1 号色和 3 号色的顶点集导出的子图，如果 v_1 和 v_3 属于 H_{13} 的不同分支，将 v_1 所在分支中着色 1 的顶点和着色 3 的顶点颜色对换，这时 v_1 着色 3，这样并不影响 $G-v_0$ 的正常着色，然后在 v_0 着色 1，因此 G 是 5 可着色的.

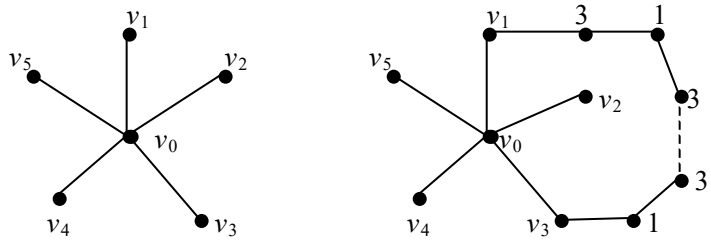


图 4.3

如果 v_1 和 v_3 属于 H_{13} 的同一连通分支，则在 H_{13} 中存在一条 (v_1, v_3)-路，这条路的顶点交替着色 1、色 3，这条路与路 $v_3v_0v_1$ 一起构成一圈，如图 4.3(b)所示，它或者把 v_2 围在里面，或者把 v_4 和 v_5 一同围在里面. 由于 G 是平面图，在任何一种情况下，都不存在连接 v_2 和 v_4 并且顶点着色 2 或 4 的一条路，现在设 H_{24} 为 $G-v_0$ 的另一个子图，它是由着色 2 和 4 的顶点集导出的子图，则 v_2 和 v_4 属于 H_{24} 的不同连通分支中，于是在 v_2 所在分支中，可将着色 2 的顶点和着色 4 的顶点颜色对换，这时 v_2 着色 4，这样作出了 $G-v_0$ 的另一种正常着色，然后在 v_0 着色 2，同样可得 G 是 5 可着色的. ▌

推论 任何地图是 5 可面着色的.

习 题 四

1. 设 G 为图 4.4 表示的地图，求$\chi^*(G)$.

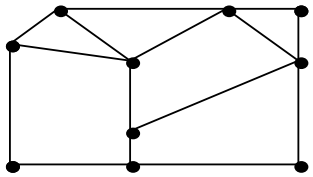


图 4.4

2. 设 G 是一地图，证明：$\chi^*(G)=\chi(G^*)$.

3. 证明地图 G 是 2 面可着色的，当且仅当它是一个欧拉图.

*第十二章　网络　匹配　独立集

§1　网络模型

设 $N=<V, U>$为一个加权的有向图，权值为非负整数，若存在 X，$Y\subseteq V$，满足 $X\cap Y=\varnothing$，X 中所有顶点的入度均为 0，Y 中所有顶点的出度均为 0，则称有向图 N 为网络，并将 X 中的点称为源点，将 Y 中的点称为聚点（汇点），N 中其他顶点称为中间点，N 上的权函数 c 也称为容量函数. 一条弧 $a=<i,j>$的权值称为 a 的容量，记为 $c(a)$ 或 $c(<i,j>)$ 或 $c(i,j)$.

我们主要讨论 $|X|=|Y|=1$ 的情况，即假设网络中恰有一个源点 x 和一个聚点 y，并总是将中间点集合记为 I.

设 $N=<V, U>$为恰含有一个源点和一个聚点的网络，f 为 N 的弧集 U 上的实数值函数，V_1，$V_2\subseteq V$，用 $<V_1$，$V_2>$表示起点在 V_1 中，终点在 V_2 中的弧的集合，记

$$f(V_1,V_2)=\sum_{a\in<V_1,V_2>}f(a),$$

当 $V_1=\{i\}$ 时可以将 $f(V_1, V_2)$ 简记为 $f(i, V_2)$.

定义 1　设 f 为网络 $N=<V, U>$的弧集 U 上的实数值函数，如果函数 f 满足

(1) 容量约束：$0\leqslant f(i,j)\leqslant c(i,j)$，$\forall$ $<i, j>\in U$，

(2) 守恒条件：$f(i, V)=f(V, i)$，$\forall\, i\in I$，

则称函数 f 为网络 N 的一个容许流，简称为流；当 N 的源点为 x，聚点为 y 时，称 $f(x, V)$ 为流的值，简记为 $f_{x,y}$.

由定义 2 可以证明

$$f(i,V)-f(V,i)=\begin{cases}f_{x,y}, & i=x,\\ 0, & i\neq x,y,\\ -f_{x,y}, & i=y.\end{cases}$$

定义 2　设函数 f 为网络 $N=<V, U>$的一个流，$a\in U$，如果 $f(a)=0$，则称弧 a 是 f-零的；如果 $f(a)>0$，则称弧 a 是 f–正的；如果 $f(a)<c(a)$，则称弧 a 是 f–不饱和的；如果 $f(a)=c(a)$，则称弧 a 是 f–饱和的.

§2　网络最大流

定义 1　设 f 为网络 $N=<V, U>$ 的一个流，如果

$$f(i,j)=0,\ \forall <i,j>\in U,$$

则称 f 为零流；如果不存在网络 N 的流 f' 使得 f' 的流值大于 f 的流值，则称 f 为网络 N 的最大流，最大流的值记为 $f_{\max}$.

定义 2　设 $N=<V, U>$ 是只有一个源点 x 和一个聚点 y 的网络，V_1 是 V 的一个子集，$x\in V_1$，$y\notin V_1$，N 中弧的集合 $<V_1, V\text{-}V_1>$ 称为 N 的一个割，记为 $K=<V_1, V\text{-}V_1>$；K 中所有弧的容量和称为割 K 的容量，记为 $c(K)$.

例 1　在图 2.1 所示网络 N 中（注：图中每条弧上标明的数对，前一个数为弧的容量，后一个数为一个流的函数值，下同），取 $V_1=\{x, v_1, v_2\}$，则 $V\text{-}V_1=\{y, v_3, v_4\}$，于是

$$K=<V_1, V\text{-}V_1>=\{v_1v_3,\ v_2v_4\},$$

K 的容量为 $c(K)=18$.

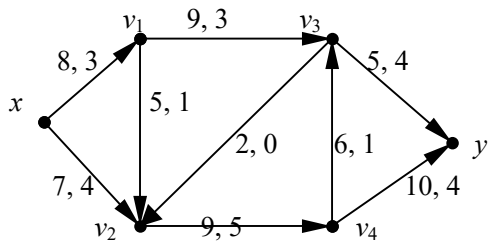


图 2.1

由割的定义知，网络 N 的一个割是分离源点 x 和聚点 y 的弧的集合，若 K 是网络 N 的割，显然 $N-K$ 中不再有 x 到 y 的有向路.

定理 1　设 f 为网络 N 的一个流，流值为 $f_{x,y}$，$K=<V_1, V\text{-}V_1>$ 为 N 的一个割，则

$$f_{x,y}=f(V_1, V\text{-}V_1)-f(V\text{-}V_1, V_1).$$

证明　因为 $f(x, V)=f_{x,y}$，$f(V, x)=0$，$f(v, V)-f(V, v)=0$，$\forall v\in I$，所以

$$f(V_1, V)-f(V, V_1)=f_{x,y},$$

再由

$$f(V_1, V)=f(V_1, V_1\cup(V\text{-}V_1))=f(V_1, V_1)+f(V_1, V\text{-}V_1),$$

$$f(V, V_1)=f(V_1\cup(V\text{-}V_1), V_1)=f(V_1, V_1)+f(V_1\text{-}V_1, V),$$

即可得证. ▌

推论 1　设 $<V_1, V\text{-}V_1>$ 是网络 N 的任一割，则 $f_{x,y}\leqslant c(V_1, V\text{-}V_1)$.

证明　因为 $0\leqslant f(i,j)\leqslant c(i,j)$，所以

$$f_{x,y}=f(V_1, V\text{-}V_1)-f(V\text{-}V_1, V_1)\leqslant f(V_1, V\text{-}V_1)$$

$$=\sum_{<i,j>\in<V_1, V-V_1>} f(i,j)\leqslant \sum_{<i,j>\in<V_1, V-V_1>} c(i,j)=c(V_1, V\text{-}V_1).$$ ▌

定义 2　设 K 为网络 N 的一个割，如果不存在 N 的割 K' 使得 $c(K') \leqslant c(K)$，则称 K 为网络 N 的最小割．最小割的容量记为 $c_{\min}$．

推论 2　对任何网络 N，有 $f_{\max} \leqslant c_{\min}$．

为了便于阅读，重述有向图中路的定义．

定义 3　设 $v_0a_1v_1a_2v_2\cdots a_kv_k$ 为网络 N 中的一个点、弧交替序列，如果对 $i \in \{1, 2, \cdots, k\}$，$a_i = < v_{i-1}, v_i >$ 或 $a_i = < v_i, v_{i-1} >$ 且 v_0，v_1，v_2，…，v_k 互不相同，则称该序列为网络 N 中的 v_0 到 v_k 的路．

注意：这里定义的路并不是有向路．

路 $v_0a_1v_1a_2v_2\cdots a_kv_k$ 可用弧序列 $a_1a_2\cdots a_k$ 表示，在没有歧义时也可以用点序列 $v_0v_1v_2\cdots v_k$ 表示．

定义 4　设 $v_0a_1v_1a_2v_2\cdots a_kv_k$ 为网络 $N = <V, U>$ 中的路，$i \in \{1, 2, \cdots, k\}$，若 $a_i = < v_{i-1}, v_i >$，则称 a_i 为前向弧，若 $a_i = < v_i, v_{i-1} >$，则称 a_i 为反向弧．

定义 4　设 P 是网络 N 的一条路，如果 P 的每一条前向弧是 f–不饱和的，而 P 的每一条反向弧是 f–正的，则称 P 是 f–不饱和路，否则称 P 是 f–饱和路；从源点到聚点的 f–不饱和路称为 f–可增广路，从源点到聚点的 f–饱和路称为 f–不可增广路．

例如，图 2.1 中，$xv_1v_3v_4y$ 是 f–可增广路，$xv_1v_2v_3y$ 是 f–不可增广路．

可增广路上的流值总是可以增大的．

定理 2　在任何网络 N 中，最大流的值等于最小割的值，即

$$f_{\max} = c_{\min}.$$

证明　假设 f 为网络 N 中的一个最大流，按如下方法构造集合 V_1：

1）源点 $x \in V_1$；

2）若 $i \in V_1$，且 $f(i, j) < c(i, j)$ 或 $f(j, i) > 0$，则 $j \in V_1$，

则聚点 $y \notin V_1$．如若不然，$y \in V_1$，则存在 x 到 y 的路 $xv_1v_2\cdots v_ky$，此路中的前向弧 $< i, j >$ 满足 $f(i, j) < c(i, j)$，反向弧 $< j, i >$ 满足 $f(j, i) > 0$，则此路为 f–可增广路，此与 f 为最大流函数矛盾．故 $< V_1, V\text{-}V_1 >$ 是分离 x 和 y 的一个割，且由 V_1 的定义，若 $< i, j > \in < V_1, V\text{-}V_1 >$，则 $f(i, j) = c(i, j)$，若 $< j, i > \in < V\text{-}V_1, V_1 >$，则 $f(j, i) = 0$，所以 $f_{x,y} = f(V_1, V\text{-}V_1) - f(V\text{-}V_1, V_1) = c(V_1, V\text{-}V_1)$，再由推论 2 得证．▌

习　题　二

1．　证明：对网络 $N = <V, U>$ 中任一流 f 和 $X \subseteq V$，均有

$$\sum_{v \in X} [f(v, V) - f(V, v)] = f(X, V - X) - f(V - X, X).$$

2．　证明若网络 N 中不存在有向 $< x, y >$ 路，则最大流的值和最小割的容量均等于零．

§3　图与二分图的匹配

定义 1　设图 $G=\langle V, E\rangle$，$M\subseteq E$，如果 M 中任意两条边在 G 中均不相邻，则称 M 是 G 的一个匹配．M 中一条边的两个端点称为在 M 下是配对的．

定义 2　若匹配 M 的一条边与顶点 v 关联，则称 M 饱和 v，或称 v 是 M-饱和的，否则称 v 是 M-不饱和的．

定义 3　如果 M 是 G 的一个匹配，对 G 的任意匹配 M'，有 $|M|\geq|M'|$，则称 M 是 G 的最大匹配．

例 1　图 3.1 中，$\{v_1v_2, v_5v_4, v_7v_8\}$和$\{v_1v_2, v_3v_4, v_6v_6, v_7v_8\}$均是匹配，其中$\{v_1v_2, v_3v_4, v_6v_6, v_7v_8\}$是一个最大匹配．

定义 4　设 M 是 G 的一个匹配，边在 $E(G)$- M 和 M 中交错出现的路称为 M-交错路，起点和终点都是 M-不饱和点的 M-交错路称为 M-增广路．

例 2　图 3.2 中 $v_3v_2v_7v_6v_1$ 是一条 M-交错路，$v_4v_5v_{10}v_9v_3v_8$ 是一条 M-增广路．

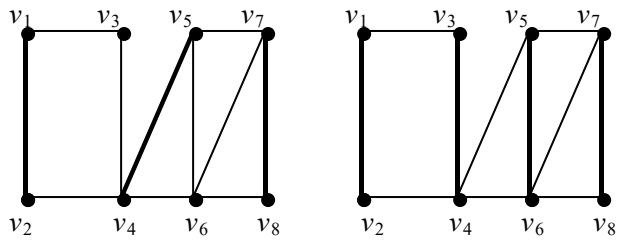


图 3.1

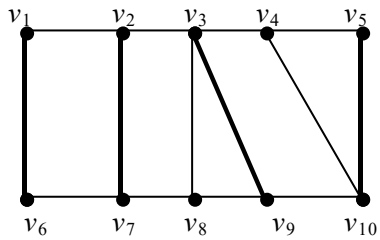


图 3.2

定理 1　图 G 的一个匹配 M 是最大匹配的充要条件是 G 不包含 M-增广路．

证明　设 M 是 G 的一个最大匹配，若 G 包含一条 M-增广路 $v_0v_1v_2\cdots v_{2m+1}$，设

$$M'=(M-\{v_1v_2, v_3v_4, \ldots, v_{2m-1}v_{2m}\})\cup\{v_0v_1, v_2v_3, \ldots, v_{2m}v_{2m+1}\},$$

显然，$M'\subseteq E$，且 M' 是 G 的一个匹配．因 $|M'|=|M|+1$，与 M 是最大匹配矛盾．因而，G 不包含 M-增广路．

反之，设 G 不包含 M-增广路，若 M 不是最大匹配，令 M' 是 G 的一个最大匹配，设 H 是由 $M' \oplus M$ 导出的 G 的子图，则 H 的每个顶点在 H 中的度只能是 1 或 2，因此 H 中的每一个分支或是一个边在 M 和 M' 中交错的偶圈，或是边在 M 和 M' 中交错的路．由 $|M'|>|M|$，H 包含的 M' 的边多于 M 的边，因此必有 H 中的一条路 P 开始于 M' 的边且终止于 M' 的边，故在 H 中被 M' 所饱和的 P 的起点和终点在图 G 中就是 M-不饱和的，于是 P 是 G 的一条 M-增广路，矛盾．因而，M 是最大匹配． ▌

定义 5 设 V_0 是图 G 的任一顶点子集，G 中与 V_0 的顶点相邻的所有顶点构成的集合称为 V_0 的邻集，记为 $N_G(V_0)$．

定理 2 设 G 是一个二分图，$\{V_1, V_2\}$ 是 G 的一个二划分，G 含有饱和 V_1 所有顶点的匹配的充要条件为

$$|N_G(V_0)| \geqslant |V_0|, \quad \forall V_0 \subseteq V_1.$$

证明 设 G 含有匹配 M，它饱和 V_1 的每个顶点，并设 $V_0 \subseteq V_1$．由于 V_0 的顶点在 M 下和 $N_G(V_0)$ 中相异顶点配对，故 $|N_G(V_0)| \geqslant |V_0|$．

反之，$|N_G(V_0)| \geqslant |V_0|$，$\forall V_0 \subseteq V_1$．假设 G 不含饱和 V_1 所有顶点的匹配．设 M^* 是 G 的一个最大匹配，根据假设，M^* 不饱和 V_1 的所有顶点．设 u 是 V_1 的一个 M^* 不饱和顶点，并设 Q 表示通过 M^* 交错路与 u 连接的所有顶点的集合．由于 M^* 是最大匹配，由定理 1 知 u 为 Q 中唯一 M^* 不饱和点．

设 $V_0 = Q \cap V_1$，$V'_0 = Q \cap V_2$，显然，$V_0 - u$ 中的顶点在 M^* 下与 V'_0 中的顶点配对，因此 $|V'_0| = |V_0| - 1$，又 $N_G(V_0) = V'_0$，所以，

$$|N_G(V_0)| = |V_0| - 1 < |V_0|,$$

矛盾． ▌

定义 6 设 G 含有匹配 M，如果 G 的每一个顶点都是 M-饱和的，则称 M 是图 G 的一个完美匹配．

定理 3 设 G 是一个 k-正则二分图，则 G 有完美匹配．

证明 设 $\{V_1, V_2\}$ 是 G 的一个二划分，则 $k|V_1| = |E| = k|V_2|$，$|V_1| = |V_2|$．设 $V_0 \subseteq V_1$．，用 E_1 和 E_2 分别表示与 V_0 和 $N_G(V_0)$ 中顶点关联的边的集合，则 $E_1 \subseteq E_2$，故 $k|N_G(V_0)| = |E_2| \geqslant |E_1| = k|V_0|$，所以 $|N_G(V_0)| \geqslant |V_0|$，由定理 2 及 $|V_1| = |V_2|$ 得证． ▌

我们用 $O(G)$ 表示图 G 含有奇数个顶点的连通分支的个数，则有

定理 4 图 G 有完美匹配的充要条件为

$$O(G - V_0) \leqslant |V_0|, \quad \forall V_0 \subset V(G).$$

证明略．

习　题　三

1．证明树至多只有一个完美匹配．

2．证明树 T 有完美匹配的充要条件为 $O(T - v) = 1$，$\forall v \in V(T)$．

§4 独立集与覆盖

定义 1 设图 $G=\langle V, E\rangle$，$S\subseteq V$，如果 S 中的任意两个顶点在 G 中均不相邻，则称 S 为 G 的一个独立集.

独立集 S 称为最大的，如果不存在 S' 使 $|S'|>|S|$. 最大独立集中顶点的个数称为图 G 的独立数，记为 $\alpha(G)$.

例 1 图 1.1 中，$\{v_2, v_4\}$，$\{v_2, v_6\}$，$\{v_2, v_4, v_6\}$均为独立集，$\{v_2, v_4, v_6\}$是最大独立集，$\alpha(G)=3$.

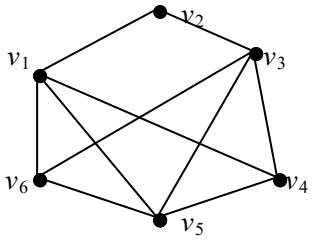


图 1.1

定义 2 设图 $G=<V, E>$，$K\subseteq V$，如果 G 中的任意边都至少有一个顶点在 K 中，则称 K 是 G 的一个覆盖.

称覆盖 K 为最小覆盖，如果不存在覆盖 K' 使 $|K'|<|K|$. 图 G 的最小覆盖中元素的个数记为 $\beta(G)$.

例 2 图 1.2 中$\{v_1, v_2, v_4, v_5\}$和$\{v_2, v_3, v_4\}$均为覆盖，$\{v_2, v_3, v_4\}$是最小覆盖，$\beta(G)=3$.

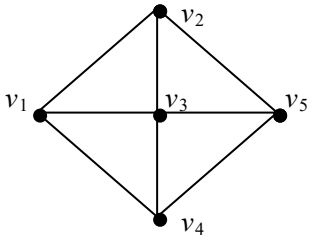


图 1.2

定理 1 设图 $G=<V, E>$，$S\subseteq V$，则 S 是 G 的独立集当且仅当 $V-S$ 是 G 的一个覆盖.

证明 S 是 G 的独立集当且仅当没有 G 中边的两个端点同时属于 S，当且仅当 G 中任意边的两个端点至少有一个属于 $V-S$. ▌

推论 图 G 有 υ 个顶点，则 $\alpha(G)+\beta(G)=\upsilon$.

证明　设 S 是 G 的最大独立集，K 为 G 的最小覆盖，则 $V-S$ 是 G 的一个覆盖，故 $\upsilon-\alpha(G)=|V-S|\geqslant\beta(G)$；又 $V-K$ 是 G 的独立集，故 $\upsilon-\beta(G)=|V-K|\leqslant\alpha(G)$，因而 $\upsilon-\alpha(G)\leqslant\beta(G)$，故得 $\upsilon-\alpha(G)=\beta(G)$. ▌

习　题　四

1．设 M 是图 G 的一个匹配，K 是 G 的一个覆盖，证明

1)　$|M|\leqslant|K|$；

2)　若 $|M|=|K|$，则 M 是最大匹配，K 是最小覆盖.

**第十三章　组合分析的基本原理

§1　计数基本法则

加法法则　设事件 A 有 m 种发生方式，事件 B 有 n 种发生方式，则事件 A 发生或事件 B 发生共有 $m+n$ 种不同方式.

例 1　一个班有 30 个男生和 20 个女生，要选一名学生为班长，则可能的选取结果有 50 种.

例 2　不大于 10 的正偶数有 5 个，不大于 10 的正奇数有 5 个，则不大于 10 的正整数有 10 个.

注意　事件 A 的发生与事件 B 的发生不能相关，例如整数 1,2，…，10 中能被 2 整除的有 5 个，能被 3 整除的有 3 个，能被 2 整除或能被 3 整除的不是 5＋3＝8 个，而是 7 个.

例 3　若 $|A|=m$, $|B|=n$, $|A\cap B|=\varnothing$, 则 $|A\cup B|=m+n$.

加法法则推广　设有 k 个互不相关的事件 A_1，A_2，…，A_k，若 A_i 发生的方式有 n_i 种，则有事件发生共有 $n_1+n_2+\cdots+n_k$ 种可能.

例 4　由 A 城市到 B 城市有两条公路，一条铁路，一个航班，则从 A 城市到 B 城市可以有 4 种走法.

乘法法则　设事件 A 有 m 种发生方式，事件 B 有 n 种发生方式，则事件 A 与事件 B 均发生共有 mn 种不同方式.

例 5　一个班有 30 个男生和 20 个女生，要选一名男生班长，一名女生班长，则可能的选取结果有 600 种.

例 6　若 $|A|=m$, $|B|=n$, 则 $|A\times B|=mn$.

例 7　从 A 到 B 有三条道路，从 B 到 C 有两条道路，则从 A 经 B 到 C 有 6 条道路.(见图 1.1)

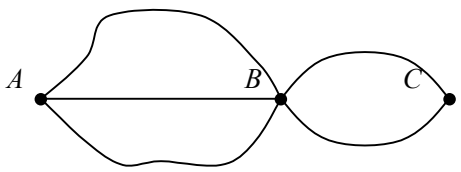


图 1.1

乘法法则推广　设有 k 个互不相关的事件 A_1，A_2，…，A_k，若 A_i 发生的方式有 n_i 种，则所有事件均发生共有 $n_1n_2\cdots n_k$ 种方式.

例 8　由 1，2，3，4 四个数字组成的四位数共有 $4\times4\times4\times4=256$ 个.

例 9　求比 10000 小的正整数中含有数字 1 的数的个数.

解　比 10000 小的正整数共有 9999 个，考虑其中不含有数字 1 的正整数. 由数字 0, 2, 3, 4, 5, 6, 7, 8, 9 构成的四位数共有 $9\times9\times9\times9$ 个，其中 0000 不是正整数，故比 10000 小的不含有数字 1 的正整数有 $9\times9\times9\times9-1=6560$ 个，所以所求的结果为 9999－6560＝3439.

§2　排列与组合

定义 1　从集合 $S=\{1,2,3,4,\cdots,n\}$ 中取出 r 个不同的元素 $p_1, p_2, \cdots, p_r$ 排成一行，称为一个 n 取 r 的不重排列，简称为 r 排列或排列，记为 $P=p_1p_2\cdots p_r$. 当 $r = n$ 时，称 P 为一个全排列.

我们称两个排列 $P=p_1p_2\cdots p_r$ 与 $Q=q_1q_2\cdots q_t$ 相等，当且仅当 $r = t$ 且 $p_i = q_i$，$1\le i\le t$.

S 中所有不同 r 排列的个数称为 n 取 r 的排列数，记为 $P(n, r)$.

例 1　从 $S=\{1, 2, 3, 4\}$ 中取 2 个元素的排列共有 12 个，它们是

12，13，14，21，23，24，31，32，34，41，42，43，

故 $P(4, 2)=12$.

定义 2　从集合 $S=\{1, 2, 3, 4, \cdots, n\}$ 中取 r 个元素 c_1，c_2，…，c_r 组成一个整体，称为 n 取 r 的一个组合，简称为 r 组合或组合，记为 $\{c_1, c_2, \cdots, c_r\}$ 或简记为 $c_1c_2\cdots c_r$ (注意这里 r 个元素没有顺序上的区别). S 的所有不同 r 组合的个数称为 n 取 r 的组合数，记为 $C(n, r)$或$\binom{n}{r}$.

例 2　$S=\{1, 2, 3, 4\}$ 中取两个元素的组合共有 6 个，它们是

12,　13,　14,　23,　24,　34,

故 $C(4, 2)=6$.

例 3　将红白蓝三个球放入编号为 1 到 10 的 10 个盒子里，每个盒子最多放一个球，则可能的放法为$10\times9\times8=720$ 种.

证明　将红球放入一个盒子，有 10 种可能，红球放入任何一个盒子后，考虑白球可能的放法，由于每个盒子最多放一个球，故白球只能放入其余 9 个盒子之一，有 9 种放法，最后，蓝球只能放入其余八个空盒子之一，有 8 种放法，由乘法法则知所有可能的放法为 $10\times9\times8=720$ 种.

一般的，考虑 n 取 r 的排列数，我们有

定理 1　$P(n,r) = n(n-1)\cdots(n-r+1)$.

推论 1　$P(n,n) = n!$.

定理 2　$C(n,r)=\dfrac{n!}{r!(n-r)!}$.

证明　考虑 $P(n, r)$的计算．n 取 r 的排列，相当于先做 n 取 r 的组合，再做 r 个元素的全排列，所以 $P(n, r) = C(n, r)\, r!$，故 $C(n, r) = P(n, r)/r!$，将 $P(n, r)$的计算表达式代入即得定理结论．

§3　组合的生成

我们已经知道 n 取 r 的组合数 $C(n, r)$的计算方法，这里讨论一下如何具体给出所有 $C(n, r)$个不同的组合．我们希望能够给出一个算法，可以规律性地依次给出全部组合．

以从 1, 2, 3, 4, 5, 6 中取 3 个为例，从中找出规律来．将取法按顺序排列为

123，124，125，126，134，135，136，145，146，156，

234，235，236，245，246，256，345，346，356，456，

可以看出，将每一个取法对应为一个 3 位数，按从小到大的顺序写出所有 3 位数时，总是先试着将已经列出的 3 位数的最后一位加 1，如果最后一位无法再加时，就将倒数第二位加 1，并将最后一位取为最小(当然仍然大于倒数第二位)；如果倒数第二位也无法再增加，则将倒数第三位加 1，等等．由此，我们给出一般情况下的组合生成算法：

(1) 设 $S=\{1, 2, 3, 4, \cdots, n\}$，$c_1c_2\cdots c_r$ 为一个 r 组合，不妨设 $c_1<c_2<\cdots<c_r$，则 $c_r \leqslant n$，$c_{r-1}\leqslant n-1, \cdots, c_1\leqslant n-r+1$，即 $c_i\leqslant n-r+i$，$i\in\{1, 2, \cdots, r\}$；

(2) 取 $c_1c_2\cdots c_r = 123\cdots r$，输出 $c_1c_2\cdots c_r$；

(3) 找满足 $c_i<n-r+i$ 的最大 i，若找不到，则结束，否则，令

$c_i:=c_i+1$，并且 $c_j:=c_{j-1}+1$，$j = i+1,\ldots,r$；输出 $c_1c_2\cdots c_r$；

(4) 转到(3).

§4　可重复的排列组合

定理 1　从 n 个不同元素中取 r 个进行排列，若允许重复选取，则不同排列的个数为 n^r.

例 1　从{1,2,3}中可重复地选取 2 个做排列，结果如下：

11, 12, 13, 21, 22, 23, 31, 32, 33.

定理 2　设有 k 类元素，第 i 类有 n_i 个，$n_1+n_2+\cdots+n_k=n$，对这 n 个元素进行全排列，则不同排列的个数为 $n!/(n_1!n_2!\cdots n_k!)$.

证明　最后的排列中有 n 个位置，排列结果相当于先从 n 个位置中选取 n_1 个位置放置第一类元素，再从剩余的 n-n_1 个位置中选取个放置第二类元素，同理依次放置第三、第四、… 、第 k 类元素，故不同排列个数为

$$C(n, n_1)\bullet\bullet\bullet\bullet C(n-n_1, n_2)\bullet\ C(n-n_1-n_2,\ \ n_2)\bullet\bullet\bullet\ \cdots\ \bullet C(n_k,\ \ n_k)$$

$$= \frac{n!}{n_1!(n-n_1)!}\times\frac{(n-n_1)!}{n_2!(n-n_1-n_2)!}\times\cdots\times\frac{n_k!}{n_k!(n_k-n_k)!}$$

$$= n!/(n_1!n_2!\cdots n_k!).$$

例 2　2 个 1 和 2 个 2 可以排列成的四位数共有 4! / (2!2!)　=　6 个：

1122，1212，1221，2121，2112，2211.

例 3　简单格路问题　从(0, 0)沿 x 轴和 y 轴的正方向走到(m, n)，问有多少不同的走法．(图 4.1)

解　将走法对应成一个有重复元素的排列：在一个走法中，每向 x 轴正方向走一步，就在排列中追加一个字母 x，每向 y 轴正方向走一步，就在排列中追加一个字母 y，则一个走法对应一个含 m 个 x 和 n 个 y 的序列，因为 m 个 x 和 n 个 y 排成的序列共有

$$(m+n)!/(m!n!) = C(m+n, m)$$

个，所以要求的不同走法有 $C(m+n, m)$个．

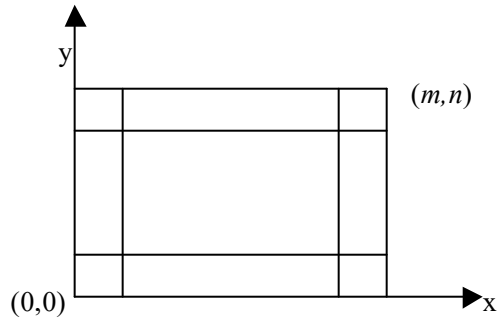


图 4.1

定理 3　在 n 个不同元素中取 r 个进行组合，若允许重复选取，则所有组合的个数为 $C(n+r-1, r)$.

证明　只须证明定理所述的所有组合与不允许重复的 $n+r$-1 取 r 组合是一一对应的．设 n 个不同元素为 1, 2, …, n，可重复地选取 r 个为 $a_1a_2\cdots a_r$，不妨设 $a_1\leqslant a_2\leqslant\cdots\leqslant a_r$，令

$$c_1=a_1,\ c_2=a_2+1,\ \cdots,\ c_r=a_r+r-1,$$

则

$$1\ \leqslant\ c_1<c_2<\cdots<c_r\ \leqslant\ n+r-1,$$

故 $c_1c_2\cdots c_r$ 是 1, 2, …,　$n+r-1$ 的一个无重复元素的 r 组合；

反之设 $c_1c_2\cdots c_r$ 是 1, 2, …, $n+r-1$ 的一个无重复元素的 r 组合，不妨设

$$1 \leqslant c_1 < c_2 < \cdots < c_r \leqslant n+r-1,$$

令

$$a_1=c_1,\ a_2=c_2-1,\ \cdots,\ a_r=c_r-r+1,$$

则 $1\leqslant a_1\leqslant a_2\leqslant\cdots\leqslant a_r\leqslant n$，所以 $a_1a_2\cdots a_r$ 是 n 个不同元素可重复 r 组合.

定理 4 r 个无区别的球放进 n 个有区别的盒子，不限制每个盒子里的球数，则共有 $C(n+r-1,\ r)$种放法.

证明 每放一个球，都相当于从 n 个盒子中选一个，所以放法数相当于允许重复的 n 取 r 的组合数.

§5 组合恒等式

定理 1 $C(n,\ r)=C(n,\ n-r)$.

证明 显然从 n 个里面取出 r 个和剩下 $n-r$ 个是一回事.

定理 2 $C(n,\ r)=C(n-1,\ r)+C(n-1,\ r-1)$.

证明 对从 n 个里面取出 r 个的所有组合进行分类，不含特定元素 a 的为一类， 含有 a 的为另一类. 不含 a 的组合相当于从 $n-1$ 个元素中取出 r 个进行组合，这一类组合有 $C(n-1,\ r)$个，含有 a 的组合相当于从 $n-1$ 个元素中取出 $r-1$ 个进行组合，组合数为 $C(n-1,\ r-1)$，由加法法则即得 $C(n,\ r)=C(n-1,\ r)+C(n-1,\ r-1)$.

推论 1 $C(n,\ r)=C(n-1,\ r)+C(n-2,\ r-1)+\cdots+C(n-r-1,\ 0)$.

证明

$$\begin{aligned}C(n,\ r)&=C(n-1,\ r)+C(n-1,\ r-1)\\&=C(n-1,\ r)+C(n-2,\ r-1)+C(n-2,\ r-2)\\&=\cdots\\&=C(n-1,\ r)+\cdots+C(n-r,\ 1)+C(n-r,\ 0)\\&=C(n-1,\ r)+\cdots+C(n-r,\ 1)+C(n-r-1,\ 0).\end{aligned}$$

定理 3 $C(n,\ 0)+C(n,\ 1)+\cdots+C(n,\ n)=2^n$.

证明 由二项式定理知

$$(x+y)^n=C(n,\ 0)\,x^n+C(n,\ 1)\,x^{n-1}y+\cdots+C(n,\ n)\,y^n,$$

令 $x=y=1$ 得证.

定理 4 $C(n,\ 0)-C(n,\ 1)+C(n,\ 2)-\cdots+(-1)^nC(n,\ n)=0$.

证明 即要证明从 n 个元素中取出奇数个元素的取法和取出偶数个元素的取法数目相同，这只要构造奇数个元素的组合和偶数个元素的组合之间的双射即可. 在 n 个元素中取一个特定元素 a，对任意的一个若干元素的组合，若其不含有 a，则加进 a，否则就去掉 a，也就是构造函数

$$f:\ A_1\to A_2,\ \forall c\in A_1,\ f(c)=\begin{cases}c-a, & a\in c,\\ c+a, & a\notin c.\end{cases}$$

其中 A_1 为含有奇数个元素的组合构成的集合，A_2 为含有偶数个元素的组合构成的集合，显然是 f 双射，故 $|A_1| = |A_2|$.

定理 5 $C(m+n, r)=C(m, 0)C(n, r)+C(m, 1)C(n, r-1)$
$$+\cdots+C(m, r)C(n, 0).$$

证明 等式左边为 $m+n$ 个元素的 r 组合的个数，我们可以用另一种方法来计算这一数字：将 $m+n$ 个元素分为两组，第一组 m 个，第二组 n 个，将所有的 r 组合分为 $r+1$ 类，第一类为 r 个元素全在第二组全部组合，共有 $C(m, 0)C(n, r)$个；第二类组合为有一个元素在第一组、其余 $r-1$ 个元素在第二组的组合，共有 $C(m, 1)C(n, r-1)$ 个；一般的，第 i 类为有 $i-1$ 个元素在第一组、其余 $r-i+1$ 个元素在第二组的组合，共有
$$C(m, i-1)C(n, r-i+1)\text{个},\ 1\leqslant i\leqslant r+1,$$
由加法法则得不同组合个数为
$$C(m, 0)C(n, r)+C(m, 1)C(n, r-1)+\cdots+C(m, r)C(n, 0).$$

§6 容斥原理

例 1 求 1 到 10 中能被 2 或 3 整除的数的个数.

解 1 到 10 中 2 的倍数有 2, 4, 6, 8, 10 共 5 个，3 的倍数有 3, 6, 9 共 3 个，能被 2 或 3 整除的数有 2, 3, 4, 6, 8, 9, 10 共 7 个，其中 6 既能被 2 整除又能被 3 整除.

定理 1 对集合 A_1，A_2，有 $|A_1\cup A_2| = |A_1|+|A_2|-|A_1\cap A_2|$.

定理 2 对集合 A_1，A_2，A_3，有
$$|A_1\cup A_2\cup A_3| = |A_1|+|A_2|+|A_3|-|A_1\cap A_2|-|A_1\cap A_3|-|A_3\cap A_2|+|A_1\cap A_2\cap A_3|.$$

定理 3 对有限集合 A_1，A_2，…，A_n，记 C_k 为 $\{1, 2, \cdots, n\}$ 的 k 元子集的集合，即
$$C_k=\{I\mid I\subseteq\{1, 2, \cdots, n\},\ |I| = k\},$$
则
$$\Big|\bigcup_{i=1}^{n}A_i\Big|=\sum_{k=1}^{n}(-1)^{k-1}\sum_{I\in C_k}\Big|\bigcap_{i\in I}A_i\Big|.$$

证明略.

例 2 求 a，b，c，d，e，f 六个字母的全排列中不出现 *ace* 和 *df* 字节的排列的个数.

解 设 A_1 为 *ace* 作为一个整体出现的排列的集合，A_2 为 *df* 作为一个整体出现的排列的集合，则 $A_1\cap A_2$ 为同时出现 *ace* 和 *df* 的排列的集合，$\sim A_1\cap\sim A_2$ 为既不出现 *ace* 也不出现 *df* 的排列的集合，$|A_1| = 4!$，$|A_2| = 5!$，$|A_1\cap A_2| = 3!$，则所求的排列数为
$$|\sim A_1\cap\sim A_2| = |\sim(A_1\cup A_2)| = 6!-|(A_1\cup A_2)| = 6!-4!-5!+3! = 582.$$

§7 鸽巢原理

鸽巢原理 $n+1$ 只鸽子进入 n 个鸽巢，则至少有一个鸽巢有不少于两只鸽子.

例 1 任取 11 个整数，必定存在两个，其差为 10 的倍数.

例 2 从 1 到 $2n$ 的正整数中任取 $n+1$ 个，其中必有两个，一个是另一个的倍数.

证明 对取出的 $n+1$ 个数重复作如下处理：奇数不变，偶数除以 2，直到转化为 $n+1$ 个奇数为止；因为 $2n$ 个数中只有 n 个奇数，所以最后得到的 $n+1$ 个奇数至少有两个相等，由于我们的处理只是去掉了一些因子 2，所以处理后相等的两个数在被处理前一个是另一个的倍数.

例 3 设 a_1，a_2，…，a_{100}，是由 1 和 2 组成的序列，已知从其中任意一个数开始的顺序 10 个数的和不超过 16，求证存在顺序的一组数，其和恰好为 39.

证明 作序列 $s_1 = a_1$，$s_2 = a_1+a_2$，…，$s_{100} = a_1+a_2+\cdots+a_{100}$，由于 a_i 等于 1 或 2，所以 $s_1<s_2<\cdots<s_{100}$，而且 $s_{100}\leqslant 160$；再构造

$$s_1+39 < s_2+39 < \cdots < s_{100}+39 \leqslant 199,$$

则共有 200 个不超过 199 的正整数，显然存在相等者，由上面的不等式即知必然存在 k, h，使得 $s_k = s_h+39$，所以 $s_k - s_h = 39$，证完.

推广的鸽巢原理 设有正整数 $m_1, m_2, \cdots, m_n$，若 n 个鸽巢里共有 $m_1+m_2+\cdots+m_n-n+1$ 只鸽子，则存在 $i\in\{1, 2, \cdots, n\}$，使得第 i 个鸽巢里有不少于 m_i 只鸽子.

当 $m_1 = m_2 = \cdots = m_n = 2$ 时，此即为前述的鸽巢原理.

证明 如若不然，则所有鸽巢里的鸽子数不多于

$$(m_1-1) + (m_2-1) + \cdots + (m_n-1) = m_1 + m_2 + \cdots + m_n - n,$$

这与已知鸽子数矛盾.

推论 1 m 只鸽子，n 个鸽巢，则存在一个鸽巢里有不少于$[(m-1)/n]$只鸽子.

推论 2 若 n 个盒子里共有 $n(m-1)+1$ 个球，则至少有一个盒子里有不少于 m 个球.

推论 3 设有正整数 m_1，m_2，…，m_n，且$(m_1+m_2+\cdots+m_n)/n>r-1$，则这 n 个数中必有一个不小于 r.

例 3 (Ramsey 问题)六个人中必定存在三个人相互认识，或者存在三上人相互不认识.

证明 设六个人为 A，B，C，D，E，对 A 以外的 5 个人按是否与 A 认识分为两类：与 A 认识的人归入集合 F，与 A 不认识的人归入集合 S，则 F 和 S 至少有一个元素个数不少于 3. 若 F 中有不少于 3 人，不妨设 B，C，$D\in F$，若 B，C，D 相互不认识，则六人中有三人相互不认识，若 B，C，D 三人中有两人相互认识，则这两人与 A 就成为六人中相互认识的三个人；若 S 中有不少于 3 人，不妨设 B，C，$D\in S$，若 B，C，D 相互认识，则六人中有三人相互认识，若 B，C，D 三人中有两人相互不认识，则这两人与 A 就成为六人中相互不认识的三个人.

习　题

1. 10！的末尾有多少个零？1000！的末尾有多少个零？
2. 证明组合等式 $nC(n\text{-}1，r) = (r+1)C(n，r+1)$.
3. 有 n 个不同的整数，从中取出两组来，要求第一组数里的最小数大于第二组的最大数．问有多少种方案？
4. 六个引擎分列两排，要求引擎的点火的次序两排交错开来，试求从一特定引擎开始点火有多少种方案.
5. 试求从 1 到 1000000 的整数中，0 出现了多少次？
6. n 个男士和 n 个女士排成男女相间的队伍，试问有多少种不同的方案？若围成一圆桌坐下，又有多少种不同的方案？
7. n 个完全一样的球，放到 r 个有标志的盒子里, $n\geqslant r$, 要求无一空盒，试证所有放法数为 $C(n-1，r-1)$.
8. 求从 1 到 500 的整数中被 3 和 5 整除但不被 7 整除的数的个数.
9. 用 $abcd$ 四个字母排列成长度为 n 的符号串，要求 abc 均必须出现，求可能的排列的个数.
10. 对六个顶点的完全图的边用红蓝二色着色，证明结果中必有一个同色三角形.
11. 证明 10 个人中或者有三个人相互认识，或者有四个人相互不认识.
12. n 个球放入 m 个盒子，$n<m(m\text{-}1)/2$，求证必有两个盒子有相同的球数.
13. 一位棋师用 11 周时间备战一场比赛，他决定每天下一到两盘棋，但每周下棋总共不超过 12 盘，证明必存在连续若干天，这些天里该棋师共下了 21 盘棋.

**第十四章　母函数与递推关系

§1　母函数

算法分析中经常要求解递推关系，母函数是求解递推关系的一个强有力的工具.

定义 1　若已知序列$\{a_n\}=\{a_0, a_1, a_2, \cdots\}$，则称函数

$$A(x)=a_0+a_1x+a_2x^2+\cdots$$

为序列$\{a_n\}$的母函数.

显然，序列与其母函数是一一对应的.

这里我们并不需要保证序列$\{a_n\}$是无限序列. 事实上，如果序列$\{a_n\}$只有有限项，则可以在序列后加 0 使其成为一个无限序列.

注意，母函数是形式上的一个推导工具，我们并没有保证序列$\{a_n\}$的母函数$A(x)=a_0+a_1x+a_2x^2+\cdots$总是一个收敛的函数，比如序列

$$\{a_n\}=\{1, 1, 1, \cdots\}$$

的母函数$A(x)=1+x+x^2+\cdots$在$x=-1$点就没有函数值，甚至我们可能给出没有收敛点的母函数，但从后面的讨论中可以看出，这并不影响我们对母函数的使用.

例 1　序列$C(n, 0), C(n, 1), \cdots, C(n, n)$的母函数为

$$C(x)=C(n, 0)+C(n, 1)x+\cdots+C(n, n)x^n=(1+x)^n.$$

例 2　对例 1 中$C(x)$的求导，得

$$C'(x)=C(n, 1)+2C(n, 2)x+\cdots+nC(n, n)x^{n-1}=n(1+x)^{n-1},$$

从而知序列

$$C(n, 1), 2C(n, 2), \cdots, nC(n, n)$$

的母函数为$n(1+x)^{n-1}$.

例 3　求证组合等式

$$C(m+n, m)=C(n, 0)C(m, 0)+C(n, 1)C(m, 1)+\cdots+C(n, m)C(m, m).$$

证明　将例 1 结论应用到等式

$$(1+x^{-1})^m(1+x)^n=x^{-m}(1+x)^{m+n}$$

两边，得

$$[C(m, 0)+C(m, 1)x^{-1}+\cdots+C(m, m)x^{-n}]\cdot[C(n, 0)+C(n, 1)x+\cdots+C(n, n)x^n]$$
$$=x^{-m}[C(m+n, 0)+C(m+n, 1)x+\cdots+C(m+n, n)x^{m+n}],$$

比较等号两边的常数项得证.

以下设序列$\{a_n\}$的母函数为$A(x)$，序列$\{b_n\}$的母函数为$B(x)$.

性质 1 若 $b_k=\begin{cases}0, & k<l,\\ a_{k-l}, & k\geq l,\end{cases}$ 则 $B(x)=x^lA(x)$.

性质 2 若 $b_k=a_k+l$，则

$$B(x)=x^{-l}\left[A(x)-\sum_{k=0}^{l-1}a_kx^k\right].$$

性质 3 若 $b_k=\sum_{i=0}^{k}a_i$ ，则 $B(x)=A(x)/(1-x)$.

证明 $B(x)=b_0+b_1x+b_2x^2+\cdots$

$=a_0+(a_0+a_1)x+(a_0+a_1+a_2)x^2+\cdots$

$=(a_0+a_0x+a_0x^2+\cdots)+(a_1x+a_1x^2+\cdots)+\cdots$

$=a_0/(1-x)+a_1x/(1-x)+\cdots$

$=(a_0+a_1x+a_2x^2+\cdots)/(1-x)$

$=A(x)/(1-x)$.

例 4 设 $A(x)=1+x+x^2+\cdots=(1-x)^{-1}$，则

$B(x)=1+2x+3x^2+\cdots=A(x)/(1-x)=(1-x)^{-2}$.

性质 4 若 $\sum_{i=0}^{\infty}a_i$ 收敛，$b_k=\sum_{i=k}^{\infty}a_i$ ，则 $B(x)=[A(1)-xA(x)](1-x)^{-1}$.

证明 易见 $b_0=A(1)$，$b_1=A(1)-a_0$，$b_2=A(1)-a_0-a_1$，…，所以

$B(x)=A(1)+(A(1)-a_0)x+[A(1)-a_0-a_1]x^2+\cdots$

$=A(1)(1+x+x^2+\cdots)-a_0x(1+x+x^2+\cdots)-a_1x^2(1+x+x^2+\cdots)-\cdots$

$=[A(1)-a_0x-a_1x^2-\cdots](1+x+x^2+\cdots)$

$=[A(1)-xA(x)](1-x)^{-1}$.

性质 5 若 $b_k=ka_k$，则 $B(x)=xA'(x)$.

性质 6 若 $b_k=\dfrac{1}{1+k}a_k$ ，则 $B(x)=\frac{1}{x}\int_0^xA(x)dx$.

§2 递推关系

例 1 已知序列$\{a_n\}$满足 $a_{n+1}=2a_n+1$，$a_0=0$,求该序列的通项.

解 设序列$\{a_n\}$的母函数为

$$A(x)=a_1x+a_2x^2+\cdots,$$

则

$$2xA(x) = \quad 2a_1x^2+2a_2x^3+\cdots,$$

注意到 $a_{n+1}-2a_n = 1, n\geqslant 1$, 及 $a_1 = 1$, 得

$$A(x)-2xA(x) = \quad a_1x+ (a_2-2a_1)x^2+ (a_3-2a_2)x^3+\cdots$$

$$= \quad x+ x^2+x^3+\cdots \quad = \quad \frac{x}{1-x},$$

故

$$A(x) \quad = \quad \frac{x}{(1-2x)(1-x)} = \frac{1}{1-2x} - \frac{1}{1-x}$$

$$= (1+2x+ (2x)^2+ (2x)^3+\cdots)-(1+ x+ x^2+x^3+\cdots)$$

$$= (2-1)x+ (2^2-1)x^2+ (2^3-1)x^3+\cdots,$$

得序列 $\{a_n\}$ 的通项 $a_n = 2^n-1$.

例 2 求含有偶数个 5 的 n 位十进制数的个数.

解 设 a_n 为含有偶数个 5 的 n 位十进制数的个数，b_n 为含有奇数个 5 的 n 位十进制数的个数，考虑 a_n 和 b_n 的递推关系式.

设 $p_1p_2\cdots p_n$ 为含有偶数个 5 的 n 位十进制数，若前 n-1 位中含有偶数个 5，则最后一位 p_n 只能是 0,1,2,3,4,6,7,8,9 中的一个，若前 n-1 位中含有奇数个 5，则最后一位 p_n 只能取 5，所以我们将含有偶数个 5 的 n 位十进制数分成两类，一类为前 n-1 位中含有偶数个 5 的，共有 $9a_{n-1}$ 个，一类为前 n-1 位中含有奇数个 5 的，共有 b_{n-1} 个，所以

$$a_n = 9a_{n-1}+ b_{n-1},$$

类似的分析可得 $b_n = 9b_{n-1}+ a_{n-1}$，再由初值 $a_1 = 8$，$b_1 = 1$，即得到 a_n 和 b_n 的完整递推关系. (这里认为含有偶数个 5 的 1 位十进制数只能为 1,2,3,4,6,7,8,9，不能取 0，建议读者仔细考虑原因)

由递推式的形式，构造下面三个等式，

$$\begin{aligned} A(x) &= a_1 + a_2x + a_3x^2 + \cdots, \\ -9xA(x) &= -9a_1x - 9a_2x^2 - \cdots, \\ -xB(x) &= -b_1x - b_2x^2 - \cdots, \end{aligned}$$

两边相加，得$(1-9x)A(x) -xB(x) = 8$，同理得$(1-9x)B(x) -xA(x) = 1$，联立解得

$$\begin{aligned} A(x) &= \frac{-71x+8}{(1-8x)(1-10x)} = \frac{1}{2}\left(\frac{7}{1-8x} + \frac{9}{1-10x}\right) \\ &= \frac{7}{2}(1+8x+(8x)^2+\cdots) + \frac{9}{2}(1+10x+(10x)^2+\cdots) \\ &= \left(\frac{7}{2}+\frac{9}{2}\right) + \left(\frac{7}{2}\cdot 8 + \frac{9}{2}\cdot 10\right)x + \left(\frac{7}{2}\cdot 8^2 + \frac{9}{2}\cdot 10^2\right)x^2 + \cdots, \end{aligned}$$

所以

$$a_n = \frac{7}{2} \cdot 8^{n-1} + \frac{9}{2} \cdot 10^{n-1}.$$

习　题

1．已知序列$\{a_n\}$的递推关系$a_{n+1}=2a_n+1$及初值$a_1 = 1$，试用母函数方法求解该序列的通项.

2．在所有 位二进制数中，没有相邻两位同时为 0 的有多少个？

3．从n个不同元素中允许重复地取出k个做排列，若不允许有相邻三位相同，则可能的排列有多少个？

第四篇　数理逻辑

数理逻辑是研究推理的科学，它采用的是数学符号化的方法，因此也称为符号逻辑.

从广义上讲，数理逻辑包括四论、两演算——即集合论、模型论、递归论、证明论和命题演算、谓词演算. 但现在提到数理逻辑，一般是指命题演算与谓词演算，本篇也只研究这两个演算.

数理逻辑的创始人是 Leibniz，为了实现把推理变为演算的想法，他把数学引入了形式逻辑. 1847 年，英国数学家 Boole 实现了命题演算，1897 年，德国数学家 Frege 建立了第一个谓词演算系统. 以后，英国逻辑学家 Witehead 和 Russel 集当时数理逻辑之大成，发表了《数学原理》一书，从而使数理逻辑成为一门专门的学科.

本世纪 30 年代以后，数理逻辑进入了一个新的时期，逻辑学不仅与数学相互渗透与结合，而且与其他科学技术，比如计算机科学，产生了密切联系，1931 年 Godel 不完全性定理的提出，以及递归函数可计算性的引入，促使了 1936 年 Turling 机的产生，十年后，第一台电子计算机问世.

数理逻辑与计算机科学、控制论、人工智能的相互渗透推动了数理逻辑的发展，模糊逻辑、概率逻辑、归纳逻辑、时态逻辑等是目前人们非常感兴趣的研究领域.

本篇我们只从语义出发，对数理逻辑中的命题演算与谓词演算等作一简单的、直观的、非形式化的介绍，将不涉及任何公理系统，对数理逻辑公理系统感兴趣的读者可参阅胡世华、陆钟万著《数理逻辑基础》和陆钟万著《面向计算机科学的数理逻辑》.

第十五章　命题逻辑

§1　命 题

数理逻辑是研究推理规律的科学，而推理过程中必然会用到某些具有真、假意义的句子或论断，比如推理中使用的前提和结论等．我们把这种具有真假意义的句子称作命题．

例如，下列语句均为命题.

（1）　3＞2．

（2）　雪是白色的.

（3）　雪是黑色的.

（4）　任何大于等于 6 的偶数，必可表为两个奇素数之和.

（5）　1＋1＝10.

（6）　那个人是本科生.

其中,(1)是正确的即真的，(2)也是真的，(3)是不正确的即假的，(4)是著名的“哥德巴赫猜想”，目前虽不能判断其真假，但其本身是具有真假意义的，(5)所表达的内容是具有真假意义的，其真假依赖于使用的数制，比如二进制或十进制.(6)中的那个人是具体有所指的，因此(6)具有真假意义.

既然命题是具有真假意义的句子，因此它必然陈述了某个事实, 是一个陈述句. 象感叹句、祈使句、疑问句等表达某种感情、感叹、请求、命令、疑问等的句子，它本身无所谓真假，不能构成命题.

例如，下列语句不是命题.

（1）　请关好门!

（2）　好大的雪啊!

（3）　他明天会来吗?

（4）　本语句为假.

其中，(1)是祈使句，(2)是感叹句，(3)是疑问句，因此都不是命题；(4)虽然是陈述句，但假设其为真，可推出其为假；假设其为假，又可推出其为真，因而无法讨论其真假，也不是命题．这是一种很特殊的语句，逻辑上称为悖论.

一个命题或者是真的,或者是假的,二者必居其一且不可兼得. 如果一个命题是真的，则说这个命题的真值(或值)为“真”，否则，说这个命题的真值(或值)为“假”. 通常，“真”用 1 或 **T** 表示，“假”用 0 或 **F** 表示． 1 、 0 (或 **T**、**F**)也用来表示一个抽象的真、假命

题.

为了对命题作逻辑演算，需要将命题符号化. 我们规定，用大写字母 P，Q，R 等表示命题. 例如可用 P 表示“北京是中国的首都”，Q 表示“雪是黑色的”等等. 我们也同样用字母 P，Q，R…等一个抽象的“命题位置”，需要时可将这种“命题位置符号”代换为具体命题(同一个符号代换为同一个命题)，这时我们把这些字母称作命题变元或命题符号. 相对于命题变元，一个具体的命题也称为命题常元. 按较为通俗的观点，“命题变元”是可在命题集合中任意变化的量. 命题变元(命题符号)无确定的真值，故不是命题. 事实上，命题(常元)与命题变元的关系正如数学中常量与变量的关系一样，例如，5 是一个常量，是一个确定的数字，而 x 是一个变量，赋给它什么值它就具有什么值，即 x 的值是不定的. 初等数学的运算规则对常量与变量的处理原则是相同的，同样地，在命题逻辑的演算中，命题与命题变元的处理原则也是相同的，因此，除了在概念上要区分命题与命题变元之外，在逻辑演算中就不再区分它们了.

一个命题，如果不能再分解为更简单的命题，则称之为简单命题或原子命题，否则，如果它可以分解成更简单的命题及一些“逻辑联结词”，则称之为复合命题. 例如“地球是圆的”是简单命题，“地球不是圆的”可分解成“地球是圆的”与否定词“不”，故是复合命题，“雪是白的且是凉的”可分解为“雪是白的”，“雪是凉的”两个更简单的命题与联结词“且”，故也是复合命题. 显然，复合命题的真值由组成该复合命题的简单命题的真值及使用的联结词决定.

习 题 一

1．判断下列语句是否是命题：

(1) 1 2 是素数.

(2) $x+y=2$.

(3) 如果 $f(x)$是连续的，则 $f(x)$是可导的.

(4) 结果对吗？

(5) 我在说假话.

(6) 这盆茉莉花真香！

(7) 存在外星人.

§ 2 联 结 词

如果仅限于简单命题的讨论，除分别讨论其真值外，再没有什么可研究的了. 而命题逻辑所讨论的是多个命题联结而成的复合命题之间的真值关系的规律性. 下面引入几个最基本、最常用的将简单命题联结为复合命题的联结词. 它们在数理逻辑中是非常重要的，其作用相当于实数集合上的＋，－，×，÷等运算.

1．**否定**

定义 1　设 P 是一个命题，“P 的否定”是一个命题，记为 $\neg P$，规定 $\neg P$ 为 1 当且仅当 P 为 0，$\neg P$ 读作“非 P”.

P 与 $\neg P$ 的真值关系可用下表表示.

P	$\neg P$
0	1
1	0

例如，若 P 表示“地球是圆的”，则 $\neg P$ 表示“地球不是圆的”，若 Q 表示“今天星期二”，则 $\neg Q$ 表示“今天不是星期二”.

2．**析取**

定义 2　设 P，Q 为两个命题，“P，Q 的析取”是一个命题，记为 $P\vee Q$，规定：$P\vee Q$ 为 1 当且仅当 P，Q 中至少有一个为 1．$P\vee Q$ 读作“P 或 Q”.

$P\vee Q$ 与 P，Q 的真值关系可用下表表示.

P	Q	$P\vee Q$
0	0	0
0	1	1
1	0	1
1	1	1

例如，若 P 表示“今天下雨”，Q 表示“今天刮风”，则 $P\vee Q$ 表示“今天下雨或者刮风”.

3．**合取**

定义 3　设 P，Q 为两个命题，“P，Q 的合取”是一个命题，记为 $P\wedge Q$，规定：$P\wedge Q$ 为 1 当且仅当 P，Q 均为 1，$P\wedge Q$ 读作“P 且 Q”.

$P\wedge Q$ 与 P，Q 的真值关系可用下表表示

P	Q	$P\wedge Q$
0	0	0
0	1	0
1	0	0
1	1	1

例如，若 P 表示“$f(x)$是连续函数”，Q 表示“$f(x)$是非负函数”，则 $P\wedge Q$ 表示“$f(x)$是连续的非负函数”.

4．**蕴涵**

定义 4　设 P，Q 是两个命题，“P 蕴涵 Q”是一个命题，记为 $P\to Q$，规定：$P\to Q$ 为 0 当且仅当 P 为 1，Q 为 0．$P\to Q$ 读作“如果 P 则 Q”.

$P\to Q$ 与 P，Q 的真值关系可用下表表示

P	Q	$P\to Q$
0	0	1
0	1	1
1	0	0
1	1	1

例如，若 P 表示“$f(x)$可导”，Q 表示“$f(x)$连续”，则 $P\to Q$ 表示“如果 $f(x)$可导，则 $f(x)$连续”.

当 P 为真命题时，为了使 $P\to Q$ 为真，必须 Q 为真，因此，$P\to Q$ 的直观含义为“如果 P 为真则 Q 为真”．但是，联结词“→”与自然语言中的“如果…则…”意义不尽相同．首先，当在自然语言中说“如果 P 则 Q”的时候，P，Q 一般是有联系的两个命题，例如，“如果明天下雨，则我们不去看电影”．而在逻辑上讨论“$P\to Q$”时，允许 P，Q 是毫无关系的命题，例如，若 P 表示“$2+3=5$”，Q 表示“雪是白的”，$P\to Q$ 便是一个真命题；其次，在自然语言中说“如果 P 则 Q”的时候，我们往往只注意 P 为真的情况，而在逻辑上规定，当 P 为假时“$P\to Q$”总为真．这点对初学者有点不习惯，但并没有与自然语言产生不一致，例如，“如果我拿到奖学金，我就去买一套克努克的《程序设计技巧》”，当“我”拿到奖学金而不去买这套书时，“我”就讲了假话，但是，如果“我”没拿到奖学金，则不论“我”是否去买这套书，都不能说“我”讲的是假话．因此，在这种情况下，只能认为“我”说的是真话．再如，“如果老王今天来，则太阳会从西边出来”．说话人当然知道太阳不会从西边出来，他说这句话的目的只是在于说明老王今天不会来，由于他确信老王今天不会来，即“老王今天来”是假的，因而，以此为前提说出任何荒唐结论都不能认为是错的，而只能认为是正确的．所以他才敢断言“如果老王今天来，则太阳会从西边出来”．第三，自然语言中说“如果 P 则 Q”，有时同时具有“如果 P 不成立，则 Q 不成立”的意思．例如，我们说“如果主任来了，我们就开始讨论”，它也具有主任没来，我们不开始讨论的意思．但在逻辑上，当 P 为假时，$P\to Q$ 总为真．这时，$P\to Q$ 不能给出关于 Q 真值的任何信息，更不具有 Q 为假的含义．

5．**等价**

定义 5　设 P，Q 为两个命题，“P 等价于 Q”是一个命题，记为 $P\leftrightarrow Q$，规定 $P\leftrightarrow Q$ 为 1 当且仅当 P，Q 的真值相同．$P\leftrightarrow Q$ 读作“P 当且仅当 Q”.

$P\leftrightarrow Q$ 与 P，Q 的真值关系可用下表表示

P	Q	$P\leftrightarrow Q$
0	0	1
0	1	0
1	0	0
1	1	1

例如，若 P 表示 $a^2+b^2=a^2$，Q 表示 $b=0$，则“$P\leftrightarrow Q$”表示“$a^2+b^2=a^2$ 当且仅当 $b=0$”.

在以上五个逻辑联结词中，$\vee$，$\wedge$，$\rightarrow$，$\leftrightarrow$ 均联结两个命题，因此称为二元联结词，$\neg$ 只作用于一个命题，因此称为一元联结词. 这五个联结词中，最不易接受的是“$\rightarrow$”，但在表示因果关系时，它是最有用的.

注意，上面介绍的逻辑联结词，是从自然语言中提炼出来的，但它们并不能完全对应于自然语言中某个联结词. 又由于自然语言本身并不严谨，常有二义性，因此，将自然语言中的语句用逻辑符号表达时，要特别注意正确理解所给语句的含义，而不能只凭字面形式生搬硬套.

例 1　张三和李四都会修电视机.

若用 P 表示“张三会修电视机”，Q 表示“李四会修电视机”，则上述命题可表示为 $P\wedge Q$.

例 2　张三与李四是表兄弟

这里虽然用了一个联结词“与”，但这是一个不能再进行分解的简单命题，因此只能用一个字母比如 P 表示.

例 3　除非你努力，否则将失败.

这句话的意思应是如果你不努力，就会失败. 因此，若用 P 表示“你努力”，Q 表示“你失败”，则上述命题可表为$(\neg P)\rightarrow Q$.

习 题 二

1．找出下列复合命题中的简单命题及联结词，并用符号表达这些复合命题.

(1)　这台机器很好，但很贵.

(2)　这座楼房既高又漂亮.

(3)　王平与刘利都是三好学生.

(4) 如果你不去，我也不去.

(5) 要是明天下雨，我就不来了.

(6) 只有同他一起干，我们才能成功.

2. 设命题 P：“这本书很有趣”；Q：“这些习题很难”；R：“这门课程使人喜欢”。将下列命题符号化：

（1） 这本书很有趣，并且这些习题很难。

（2） 这本书无趣，习题也不难，那么，这门课程不会使人喜欢。

（3） 这本书无趣，习题也不难，而且这门课程也不会使人喜欢。

（4） 这本书很有趣意味着这些习题很难，反之亦然。

（5） 或者这本书很有趣，或者这些习题很难，且两者恰具其一。

§ 3 合式公式

我们已经知道，命题可用逻辑联结词联结起来构成更复杂的命题. 同样地，命题变元也可用逻辑联结词联结而构成一些有意义的“命题结构形式”，为了表达这个问题，先引入下述定义.

定义 1 合式公式(well formed formula 简记为 *wff*)的归纳定义如下

(1) 命题变元及命题常元 0 、 1 是合式公式.

(2) 如果 A，B 是合式公式，则$(\neg A)$，$(A\vee B)$，$(A\wedge B)$，$(A\to B)$，$(A\leftrightarrow B)$是合式公式.

(3) 任何合式公式均通过有限次使用(1)、(2)得到.

合式公式也简称公式. 例如，$((P\wedge Q)\to(\neg(Q\vee R)))$是公式. 事实上，因为 P，Q 是公式，故$(P\wedge Q)$是公式，又 Q，R 是公式，则 $(Q\vee R)$ 是公式，从而$(\neg(Q\vee R))$是公式，最后，由 $(P\wedge Q)$，$(\neg(Q\vee R))$是公式知$((P\wedge Q)\to(\neg(Q\vee R)))$是公式. 同样，$((P\wedge Q)\vee R)$，$((\neg(R\wedge Q))\to P)$，$(((\neg P)\vee Q)\wedge(\neg R))$均是公式，但$(\neg P\vee Q\to)$，$(P\vee Q\wedge)$，$(P\to Q\to R)\vee$，$\vee R$ 都不是公式.

在实际使用时，为了书写的方便，我们引入以下约定以减少括号数量.

(1) 最外层括号可以省略.

(2) 对逻辑联词规定优先级. 逻辑联结词按优先级从高到低的顺序依次排列为：

$$\neg \quad \wedge \quad \vee \quad \to \quad \leftrightarrow$$

这样，$((P\wedge Q)\to R)$ 简写为 $P\wedge Q\to R$，$((\neg P)\wedge Q)$ 简写为 $\neg P\wedge Q$，$((P\to Q)\leftrightarrow R)$ 简写为 $P\to Q\leftrightarrow R$ 等.

从以上定义可见，公式是符合某种规则的符号串，若将公式中出现的每个命题变元均指定一个真值 1 或 0 ，则可按照该公式的形成过程计算出公式的真值.

定义 2 设 G 是一个公式，对 G 中出现的每个命题变元指定一个真值 1 或 0 ，则得到该公式中命题变元的一个真值组合，称之为对公式 G 的一个指派(或解释). 公式 A 在

指派 I 下的真值可记为 A^I.

例 1　对于公式 $\neg(P\wedge Q)\rightarrow Q\vee\neg R$，指定 P 为 1，Q 为 1，R 为 1 即是对公式的一个指派，在该指派下，公式的真值为 1，指定 P 为 0，Q 为 0，R 为 1 是公式的另一个指派，在该指派下，公式的真值为 0.

设 A 是一个公式，其中包含 n 个命题变元，不妨设为 P_1，P_2，…，P_n，指定 P_1 为 δ_1，P_2 为 δ_2，…，P_n 为 δ_n (其中 $\delta_i=1$ 或 0) 可以说成是指定 $(P_1, P_2, \cdots, P_n)$ 为 $(\delta_1, \delta_2, \cdots, \delta_n)$，而对公式 A 的这个指派可用 $(\tilde{p}_1, \tilde{p}_2, \cdots \tilde{p}_n)$ 表示，

其中，$\tilde{p}_i=\begin{cases}P_i & \delta_i=1\\ \neg P_i & \delta_i=0\end{cases}$

例如，指定 (P, Q, R) 为 (0，1，0) 的指派按这种记号应记为 $(\neg P, Q, \neg R)$，而指定 (P, Q, R) 为 (1，0，1) 的指派应记为 $(P, \neg Q, R)$. 反之，指派 $(\neg P, \neg Q, R)$ 即指定 (P, Q, R) 为 (0，0，1)，指派 $(P, \neg Q, \neg R)$ 即指定 (P, Q, R) 为 (1, 0, 0). 一般地，容易看出，指派 $(\tilde{p}_1, \tilde{p}_2, \cdots \tilde{p}_n)$ 意味着指定 $\tilde{P}_i$ 为 1 ($i=1, 2, \cdots, n$).

求出一个公式 A 在所有指派下的真值并列成表，即得到公式 A 的“真值表”.

例 2　公式 $A=(P\rightarrow Q)\wedge R$ 的真值表为

P	Q	R	A
0	0	0	0
0	0	1	1
0	1	0	0
0	1	1	1
1	0	0	0
1	0	1	0
1	1	0	0
1	1	1	1

真值表是一个常用工具，经常用来处理一些规模较小的问题. 但由于公式 A 中每个命题变元有两个可能的真值，当 A 中含有 n 个命题变元时，A 共有 2^n 个指派，即 A 的真值表有 2^n 行. n 较大时，列真值表是不可行的.

定义 3　设 A 为一公式，如果在所有指派下 A 均为真，则称 A 为永真式，如果在所有指派下 A 均为假，则称 A 为永假式，如果至少有一个指派使 A 为真，则称 A 为可满足的.

永真式又称重言式，永假式又称矛盾式.

由以上定义可以看出，A 是可满足的当且仅当 A 不是永假式；A 是永真式当且仅当 $\neg A$

是永假式；A 是永真式则 A 是可满足的.

为判定一个公式是永真、永假或可满足，可以利用构造真值表的方法，由于公式的指派数总是有限的，故公式的以上判定问题是可解的.

例 3　(1)　$P\vee(\neg P)$是永真式

(2)　$P\wedge(\neg P)$**是**永假式.

(3)　$(P\to Q)\vee R$ 是可满足的.

以上结论可用真值表验证，在此从略.

定理 1 (代入原则)　设 A 是一个永真式，P_1，P_2，…，P_n 为其中出现的所有命题变元，A_1，A_2，…，A_n 是任意一组公式，若用 A_i ($1\leqslant i\leqslant n$) 代替 A 中的 P_i 得到公式 B，则 B 必为永真式.

证明　任取公式 B 的一个指派 I，在此指派下 A_1，A_2，…，A_n 都有一个确定的真值，不妨将 A_i 的真值为 δ_i，即 $A_i^I=\ \delta_i$, 根据 B 的形成过程，B 在指派 I 下的真值，即是公式 A 在指派 (P_1，P_2，…，P_n) 为 ($\delta_1, \delta_2,\cdots, \delta_n$) 时的真值. 由于 A 是永真式，这个指派下 A 的真值必为 1，即 B 在指派 I 下的真值为 1，从而知 B 是永真的. ▌

习 题 三

1．试确定下列公式在指派 (P，Q，$\neg R$，$\neg S$) 下的真值.

(1)　$(P\wedge(Q\wedge R))\vee\neg((P\vee Q)\wedge(R\vee S))$

(2)　$(\neg(P\wedge Q)\vee\neg R)\vee(((\neg P\wedge Q)\vee\neg R)\wedge S)$

(3)　$(\neg(P\wedge Q)\vee\neg R)\vee((Q\leftrightarrow\neg P)\to(R\vee\neg S))$

(4)　$(P\vee(Q\to(R\wedge\neg P)))\leftrightarrow(Q\vee\neg S)$

2．证明下列合式公式为永真式.

(1)　$(((P\vee Q)\to R)\leftrightarrow((P\to R)\vee(Q\to R)))$

(2)　$(P\to(Q\vee R))\leftrightarrow(\neg R\to(P\to Q))$

(3)　$(P\to Q)\to((R\to Q)\to((P\vee R)\to Q))$

(4)　$(P\to(Q\to R))\leftrightarrow(Q\to(P\to R))$

(5)　$(P\to(Q\to R))\to((P\to Q)\to(P\to R))$

§4　等 价 式

定义 1　设 A，B 是两个公式，如果在任意指派下，A，B 的真值总是相同的，则称 A，B 等价，记为 $A=B$.

注意：A，B 中出现的命题变元未必完全相同，在对 A，B 指派时，应指定 A, B 两个

公式中出现的所有命题变元的真值.

要注意, 公式的等价符号“＝”与逻辑联词符号“$\leftrightarrow$”的区别,“＝”是一个关系符, 表达两公式之间的一种关系. “$\leftrightarrow$”是逻辑联词，把两个公式联接成一个新的公式.

显然，两个公式是否等价，可以利用真值表来判断.

例 1　证明 $(P\wedge\neg P)\vee Q = Q$

求出 $(P\wedge\neg P)\vee Q$ 与 Q 的真值表如下

P	Q	$(P\wedge\neg P)\vee Q$	Q
0	0	0	0
0	1	1	1
1	0	0	0
1	1	1	1

可见，$(P\wedge\neg P)\vee Q = Q$.

公式的等价“＝”作为公式间的一种关系，具有如下性质：

定理 1　设 A，B，M 是公式，则

(1)　$A=A$

(2)　若 $A=B$，则 $B=A$

(3)　若 $A=B$，$B=M$，则 $A=M$

即是说公式的等价“＝”满足自反、对称、传递性，是一个等价关系.

读者自证.

“＝”与“$\leftrightarrow$”虽然在概念上不同，但他们之间有着密切联系.

定理 2　设 A，B 是公式，则 $A=B$ 当且仅当 $A\leftrightarrow B$ 是永真式.

证明　若 $A=B$，则对任何指派 I，A，B 的真值必定相同，从而 $A\leftrightarrow B$ 的真值为 1 .因此，$A\leftrightarrow B$ 是永真式.

反之，设 $A\leftrightarrow B$ 是永真式，则对任何指派 I，$A\leftrightarrow B$ 必为 1，由定义，A，B 的真值必定相同，因此，$A=B$. ▌

现在，我们列出一些常用的等价公式，读者不难利用真值表对他们进行验证.

1．双重否定律

$\neg\neg P=P$

2．结合律

$(P\vee Q)\vee R=P\vee(Q\vee R)$　　$(P\wedge Q)\wedge R=P\wedge(Q\wedge R)$

3．交换律

$P\vee Q=Q\vee P$　　$P\wedge Q=Q\wedge P$

4．分配律

$P\wedge(Q\vee R)=(P\wedge Q)\vee(P\wedge R)$　　$P\vee(Q\wedge R)=(P\vee Q)\wedge(P\vee R)$

5．幂等律

$P\vee P=P$　　$P\wedge P=P$

6．吸收律

$P\vee(P\wedge Q)=P$　　$P\wedge(P\vee Q)=P$

7．De Morgan 律

$\neg(P\vee Q)=\neg P\wedge\neg Q$　　$\neg(P\wedge Q)=\neg P\vee\neg Q$

8．单位律

$P\vee 0=P$　　$P\wedge 1=P$

9．零律

$P\vee 1=1$　　$P\wedge 0=0$

10．补律

$P\vee\neg P=1$　　$P\wedge\neg P=0$

11．$P\to Q=\neg P\vee Q$

12．$P\to Q=\neg Q\to\neg P$

13．$P\to(Q\to R)=P\wedge Q\to R$

14．$P\to(Q\to R)=Q\to(P\to R)$

15．$(P\to R)\wedge(Q\to R)=(P\vee Q)\to R$

16．$P\leftrightarrow Q=(P\to Q)\wedge(Q\to P)$

17．$P\leftrightarrow Q=(P\wedge Q)\vee(\neg P\wedge\neg Q)$

18．$P\leftrightarrow Q=(P\vee\neg Q)\wedge(\neg P\vee Q)$

定理 3　（等价式代入原则）设 A, B 是两个公式，$A=B$，P_1，P_2，…，P_n 为这两个公式中出现的所有命题变元，A_1，A_2，…，A_n 是任意一组公式，若用 $A_i\,(1\leqslant i\leqslant n)$ 代替 A，B 中的 P_i 分别得到公式 A', B'，则 $A'=B'$.

证明　由定理 2 立即可得. ▌

根据上述代入原则，用任意公式 A，B，W 代替上列诸等价式中的命题变元 P，Q，R 得到的等价式仍然成立.

于是，给出一个公式 A，我们就可以依据上面的基本等价式，在等价意义下对 A 进行推演，得到 A 的各种等价形式.

给出两个公式 A，B，判断 A 是否等价于 B，我们现在有三种办法，一是用真值表，二是在等价意义下看 A 是否能化为 B，三是判断 $A\leftrightarrow B$ 是否永真．若用第二、第三种方法，在等价转化过程中，我们可能会不自觉地将公式的某一部分用其等价的公式代换，例如，我们可能会写出如下推导步骤：

$$P\wedge(Q\vee R)\to P$$

$=(P\wedge Q)\vee(P\wedge R)\rightarrow P$

在这里，利用 $(P\wedge Q)\vee(P\wedge R)$ 代换了 $P\wedge(Q\vee R)$，这似乎是很自然的，现在我们把这个原则明确提出来.

定义 2　设 A_1 是公式 A 的一部分，且 A_1 本身是公式，则称 A_1 是 A 的子公式.

定理 4　设 A 是一个公式，A_1 是 A 的子公式. 如果公式 B_1 满足 $A_1=B_1$，则用 B_1 替换 A_1 在 A 中的一个或若干个出现后得到的公式 B 必满足 $A=B$.

证明　由 B 的形成过程可知，B 与 A 的不同仅在于一个或若干个地方出现不同子公式 B_1 或 A_1，其它完全相同. 对于任一指派 I，我们可以先求出子公式 A_1，B_1 的真值，进而完成 A 与 B 的求值. 由于 $A_1=B_1$，A_1 与 B_1 的真值必定相同，因此，在公式 A 与 B 中求出 A_1，B_1 的真值后，A 与 B 也变得完全相同，从而在指派 I 下 A 与 B 的真值必然相同. 所以 $A=B$. ▌

例 2　证明

$(\neg P\wedge(\neg Q\wedge R))\vee(Q\wedge R)\vee(P\wedge R)=R$

左端 $=(\neg P\wedge(\neg Q\wedge R))\vee((Q\vee P)\wedge R)$

$=(\neg P\wedge\neg Q)\vee(Q\vee P))\wedge R$

$=(\neg(P\vee Q)\vee(P\vee Q))\wedge R$

$=1\wedge R$

$=R$

例 3　证明

$((P\vee Q)\wedge\neg(\neg P\wedge(\neg Q\vee\neg R)))\vee(\neg P\wedge\neg Q)\vee(\neg P\wedge\neg R)=1$

左端 $=((P\vee Q)\wedge(P\vee(Q\wedge R)))\vee\neg((P\vee Q)\wedge(P\vee R))$

$=((P\vee Q)\wedge(P\vee Q)\wedge(P\vee R))\vee\neg((P\vee Q)\wedge(P\vee R))$

$=((P\vee Q)\wedge(P\vee R))\vee\neg((P\vee Q)\wedge(P\vee R))$

$=1$

习 题 四

1．证明下列等价式.

(1)　$(\neg P\wedge(\neg Q\wedge R))\vee(Q\wedge R)\vee(P\wedge R)\vee(P\wedge\neg R)\vee(\neg P\wedge\neg R)=1$

(2)　$P\rightarrow(Q\rightarrow P)=\neg P\rightarrow(P\rightarrow Q)$

(3)　$P\rightarrow(Q\vee R)=(P\rightarrow Q)\vee(P\rightarrow R)$

(4)　$(P\rightarrow Q)\wedge(R\rightarrow Q)=(P\vee R)\rightarrow Q$

2．证明等价式 6，13，14，17.

*§ 5　对偶式

观察上节给出的等价式，我们可以看到，五个逻辑联结词并非是互相独立的，某些联结词可以在等价意义下被其它联结词表示，例如，$P\rightarrow Q=\neg P\vee Q$， 即$\rightarrow$可由$\neg$与$\vee$表示; $P\wedge Q=\neg(\neg P\vee\neg Q)$, 即$\wedge$也可由$\neg$与$\vee$表示; 进一步地，容易说明, $\leftrightarrow$也可由$\neg$与$\vee$表示. 这样，五个联结词仅需使用$\neg$与$\vee$就可完全表示出来，一般地，设 C 是由某些联结词构成的集合，如果所有联结词可由 C 中的联结词等价地表示，则称 C 是完备的.

如上所述，{ $\neg$，$\vee$ } 是完备的，同样可知 { $\neg$，$\wedge$ } 也是完备的，显而易见 { $\neg$，$\vee$，$\wedge$ } 自然是完备的.

尽管 { $\neg$，$\vee$ }，{ $\neg$，$\wedge$ } 是完备的，且仅使用了两个逻辑联词，但在使用上不够方便，通常取 { $\neg$，$\vee$，$\wedge$ } 为完备集作为一种折衷：既在使用上足够方便，又不用过多的联结词. 基于此，本节将假设所有公式中仅出现$\neg$，$\vee$及$\wedge$三个联结词或更少.

另外，我们还可注意到，在上节所列的仅含$\neg$，$\vee$，$\wedge$的运算定律 (即等价式 1—10) 中，除双重否定律外，等价式都是成对出现的，且成对的两个等价式不同之处只是$\vee$和$\wedge$互换. 0 和 1 互换，我们把这样的规律称作对偶律.

定义 1　设 A 是一个公式，将 A 中出现的$\vee$，$\wedge$，1，0 分别换以$\wedge$，$\vee$，0，1 得到公式 A^*，称 A^*是 A 的对偶式.

显然，A 也是 A^*的对偶式，即 $(A^*)^*=A$，因此可称 A 与 A^* 是互相对偶的.

若 A 中出现的所有命题变元为 P_1，P_2，…，P_n，这时可记 $A=A(P_1，P_2，\cdots，P_n)$，我们将记 $A^-=A(\neg P_1，\neg P_2，\cdots，\neg P_n)$，在这种记号下显然有 $A^{--}=A$.

定理 1　对任何公式 A，有

$$\neg(A^*)=(\neg A)^*$$

$$\neg(A^-)=(\neg A)^-$$

读者自证

定理 2　对任何公式 A，均有　$\neg A=A^{*-}$

证明　施归纳法于 A 中出现的联结词个数 n，当 $n=0$ 时 A 中无联结词，则 $A=P$，或 $A=1$ 或 $A=0$，若 $A=P$，则$\neg A=\neg P$，而 $A^{*-}=\neg P$，所以$\neg A=A^{*-}$. 同样可证，当 $A=1$ 或 $A=0$ 时，$\neg A=A^{*-}$也成立. 因此 $n=0$ 时定理成立. 设 $n\leqslant k$ 时定理成立，下证 $n=k+1$ 时定理也成立. 因为 $n=k+1\geqslant 1$，A 中至少有一个联结词，可分三种情况：

$$A=\neg A_1，\quad A=A_1\wedge A_2，\quad A=A_1\vee A_2$$

其中，A_1，A_2中联结词个数$\leqslant k$，依归纳假设　$\neg A_1=A_1^{*-}$，$\neg A_2=A_2^{*-}$

（1）　当 $A=\neg A_1$时，

$$\neg A=\neg(\neg A_1)=\neg(A_1^{*-})=(\neg A_1^*)^-$$

$$=(\neg A_1)^{*-}=A^{*-}.$$

(2)　当 $A=A_1\wedge A_2$时，

$$\neg A=\neg(A_1\wedge A_2)=\neg A_1\vee\neg A_2$$

$$=A_1^{*-}\vee A_2^{*-}=(A_1^*\vee A_2^*)^-$$

$$=(A_1\wedge A_2)^{*-}$$

$$=A^{*-}$$

(3) 当 $A=A_1\vee A_2$ 时，

$$\begin{aligned}\neg A &= \neg(A_1\vee A_2)=\neg A_1\wedge\neg A_2\\ &=A_1{}^{*-}\wedge A_2{}^{*-}=(A1{}^{*}\wedge A2{}^{*})^{-}\\ &=(A1\vee A2)^{*-}\\ &=A^{*-}\end{aligned}$$

从而定理得证. ▌

定理 3　设 A，B 是公式，若 $A=B$，则 $A^*=B^*$.

证明　因为 $A=B$，所以 $A\leftrightarrow B$ 永真，从而 $\neg A\leftrightarrow\neg B$ 永真，由定理 2，$A^{*-}\leftrightarrow B^{*-}$ 永真. 对任意指派 $I=(b_1,b_2,\cdots,b_n)$，记 $\bar{I}=(\bar{b_1},\bar{b_2},\cdots,\bar{b_n})$ 为其反指派，其中，

$$\bar{b_i}=\begin{cases}0 & b_i=1\\ 1 & b_i=0\end{cases}$$

则 $A^*\leftrightarrow B^*$ 在 I 下的真值即为 $A^{*-}\leftrightarrow B^{*-}$ 在 $\bar{I}$ 下的真值，于是由 $A^{*-}\leftrightarrow B^{*-}$ 的永真性得知 $A^*\leftrightarrow B^*$ 永真，从而 $A^*=B^*$. ▌

这个定理解释了我们在上节定律 2—10 中观察到的对偶律，在这些定律中，将每个定律的某一式记作 $A=B$，另一式则恰为 $A^*=B^*$，由此可见，这些定律中的两个式子事实上是等价的.

习 题 五

1. 写出如下公式的对偶式.

(1) $\neg(P\vee Q)\wedge(R\vee 0)$

(2) $(P\vee R)\vee((\neg P\wedge Q)\wedge(Q\wedge\neg R)\wedge 0)$

(3) $(P\vee Q)\wedge(\neg 0\vee 1)$

2. 施归纳法于公式 A 中的联结词数量，以证明定理 1.

3. 证明：对任意公式 A，B.

(1) $A\rightarrow B$ 与 $B^*\rightarrow A^*$ 同永真，同可满足.

(2) $A\leftrightarrow B$ 与 $A^*\leftrightarrow B^*$ 同永真，同可满足.

§6　范　式

由公式的定义可见，形式不同的公式有无穷多个，而这些公式中大量都是相互等价的，那么，我们自然要问，能否规定一种标准形式，使得任一公式都可在等价意义下化成这种标准形式，这种命题公式形式的规范化，无疑会为我们的讨论带来方便. 例如，借助这种标准形式判断两个公式是否等价，或判断一个公式是否永真、永假、可满足等. 为

叙述方便，先来引入几个术语.

定义 1　命题变元及其否定统称为文字.

一些文字的合取称为基本合取式或短语，

一些文字的析取称为基本析取式或子句.

特别地，一个文字既是短语又是子句.

例如，P，$\neg P$，$\neg P\wedge Q$，$P\wedge\neg Q\wedge R$ 都是短语（基本合取式），P，$\neg P$，$\neg P\vee Q$，$P\vee Q\vee R$ 都是字句（基本析取式）.

定义 2　有限个短语的析取，即形如 $A_1\vee A_2\vee\cdots\vee A_n$ 的公式，其中 A_i($i=1$，2，…，n) 为短语，称为析取范式；有限个字句的合取，即形如 $B_1\wedge B_2\wedge\cdots\wedge B_n$ 的公式，其中 B_i($i=1$，2，…，n)为子句，称为合取范式.

特别地，短语既是析取范式又是合取范式，子句同样既是析取范式又是合取范式.

例如，P，$\neg P$，$P\wedge\neg Q\wedge R$，$P\vee\neg Q\vee R$，$(P\wedge\neg Q\wedge R)\vee(\neg P\wedge Q)\vee R$ 均是析取范式．P，$\neg P$，$P\wedge\neg Q\wedge R$，$P\vee\neg Q\vee R$，$(P\vee\neg Q\vee R)\wedge(\neg P\vee Q)\wedge R$ 均是合取范式.

定理 1　对于任意命题公式，都存在等价于它的析取范式和合取范式.

证明　对于任意公式 A，通过如下算法即可得出等价于它的范式.

（1）　使用基本等价式，将 A 中的逻辑联结词$\rightarrow$，$\leftrightarrow$去除.

（2）　使用 Morgan 律和双重否定律，将 A 中所有的否定词$\neg$ 都放在命题变元之前，形成文字.

（3）　反复使用分配律，即可得到等价的范式. ▌

例 1　$A=(P\wedge(Q\rightarrow R))\rightarrow S$

$=\neg(P\wedge(\neg Q\vee R))\vee S$

$=\neg P\vee\neg(\neg Q\vee R)\vee S$

$=\neg P\vee(Q\wedge\neg R)\vee S$　　(析取范式)

$=((\neg P\vee Q)\wedge(\neg P\vee\neg R))\vee S$

$=(\neg P\vee Q\vee S)\wedge(\neg P\vee\neg R\vee S)$　　(合取范式)

利用析取范式，可以判断一个公式是否永真或永假. 显然，A 永真当且仅当$\neg A$ 永假，故只需讨论永假的判定即可. 容易明白，一个公式 A 永假，当且仅当其析取范式中每个短语永假，而一个短语永假当且仅当该短语中同时含有某命题变元及其否定.

例 2　判断公式 $A=(P\rightarrow Q)\wedge(Q\rightarrow R)\wedge(R\rightarrow P)$是否永假.

$A=(P\rightarrow Q)\wedge(Q\rightarrow R)\wedge(R\rightarrow P)$

$=(\neg P\vee Q)\wedge(\neg Q\vee R)\wedge(\neg R\vee P)$

$=((\neg P\wedge\neg Q)\vee(\neg P\wedge R)\vee(Q\wedge\neg Q)\vee(Q\wedge R))\wedge(\neg R\vee P)$

$=(\neg P\wedge\neg Q\wedge\neg R)\vee\cdots$

故公式 A 不是永假的.

例 3　判断公式 $A=(P\rightarrow Q)\wedge P\wedge\neg Q$ 是否永假.

$A=(P\rightarrow Q)\wedge P\wedge\neg Q$

$=(\neg P\vee Q)\wedge P\wedge\neg Q$

$=(\neg P\wedge P\wedge\neg Q)\vee(Q\wedge P\wedge\neg Q)$

$=0$

A 是永假的.

同样，利用合取范式也可以判断一个公式是否永真、永假、可满足，请读者将前面的判断方法平移过来.

显然，给出一个公式 A，其范式并非是唯一的. 例如， 析取范式

$$(P\wedge Q)\vee(Q\wedge\neg R)$$

可等价地写成

$$(P\wedge Q\wedge R)\vee(P\wedge Q\wedge\neg R)\vee(Q\wedge\neg R)$$

或

$$(P\wedge Q\wedge R)\vee(Q\wedge\neg R),$$

这为利用范式判断公式是否等价带来不便，为进一步将公式标准化，下面引进主范式的概念.

定义 3　设 P_1，P_2，…，P_n 是 n 个命题变元，形如

$$\widetilde{P}_1\wedge\widetilde{P}_2\wedge\cdots\wedge\widetilde{P}_n$$

的公式，称为由 P_1，P_2，…，P_n 生成的极小项，其中 $\widetilde{P}_i=P_i$ 或 $\neg P_i$ ($i=1$，2，…，n).

例如，$P\wedge Q\wedge R$，$\neg P\wedge Q\wedge\neg R$ 是由 P，Q，R 生成的极小项，但不是 Q，P，R 生成的极小项；$P\wedge Q$，$\neg P\wedge Q$ 是由 P，Q 生成的极小项，但不是 P，Q，R 生成的极小项，也不是 P 生成的极小项.

两个命题变元 P_1，P_2 生成的极小项共有四个：

$\neg P_1\wedge\neg P_2$，$\neg P_1\wedge P_2$，$P_1\wedge\neg P_2$，$P_1\wedge P_2$

若将极小项中 P_i 对应二进制数 1，$\neg P_i$ 对应二进制数 0，则 $\neg P_1\wedge\neg P_2$ 对应 0 0，该极小项可记为 m_{00}；$\neg P_1\wedge P_2$ 对应 0 1，该极小项可记为 m_{01}；$P_1\wedge\neg P_2$ 对应 1 0，该极小项可记为 m_{10}；$P_1\wedge P_2$ 对应 1 1，该极小项可记为 m_{11}.

一般地，设 P_1，P_2，…，P_n 是 n 个命题变元，若将 P_i 对应 1，$\neg P_i$ 对应 0，则极小项 $\widetilde{P}_1\wedge\widetilde{P}_2\wedge\cdots\wedge\widetilde{P}_n$ 对应 n 位二进制数 $\delta_1\,\delta_2\cdots\delta_n$，其中

$$\delta_i=\begin{cases}1 & \widetilde{P}_i=P_i\\ 0 & \widetilde{P}_i=\neg P\end{cases}$$

该极小项可记为 $m_{\delta_1\delta_2\cdots\delta_n}$，为方便，通常将 $\delta_1\,\delta_2\cdots\delta_n$ 化为十进制形式书写，例如 m_{10} 写为 m_2，m_{1100} 写为 m_{12} 等.

易见，在极小项 $m_{\delta_1\delta_2\cdots\delta_n}=\widetilde{P}_1\wedge\widetilde{P}_2\wedge\cdots\wedge\widetilde{P}_n$ 的 2^n 个指派中，指定 (P_1，P_2，…，

P_n) 为 (δ_1， δ_2，…， δ_n) 作成的指派是唯一使 $m_{\delta_1\delta_2\cdots\delta_n}$ 为 1 的指派，该指派又可记为

($\widetilde{P}_1$， $\widetilde{P}_2$，…， $\widetilde{P}_n$).

例如，极小项 $m_{110}=P_1\wedge P_2\wedge\neg P_3$ 的唯一成真指派为指定 (P_1，P_2，P_3) 为 (1 ， 1 ， 0). 该指派即为 (P_1，P_2，$\neg P_3$). 极小项 $m_{010}=\neg P_1\wedge P_2\wedge\neg P_3$ 的唯一成真指派为指定 (P_1，P_2，P_3) 为 (0 ， 1 ， 0)，该指派即为 ($\neg P_1$，P_2，$\neg P_3$).

极小项具有如下性质：

（ 1 ） n 个命题变元生成的极小项共有 2^n 个.

（ 2 ） 对于每个极小项，存在唯一一个指派使该极小项为 1 .

（ 3 ） 极小项两两不等价，且 $m_i\wedge m_j=0\quad (i\neq j)$

（ 4 ） $\sum_{i=0}^{2^n-1} m_i=1$

定义 4　设公式 A 中出现的所有命题变元为 P_1，P_2，…，P_n，如果在 A 的析取范式 A' 中，每个短语均为关于 P_1，P_2，…，P_n 的极小项，则称 A' 为 A 的主析取范式.

定理 2　对任意公式 A，都存在唯一一个与之等价的主析取范式.

证明　设 A 中所有不同的命题变元为 P_1，P_2，…，P_n. 由定理 1 ，A 必可化为一个析取范式，不妨设 $A=A_1\vee A_2\vee\cdots\vee A_m$，其中，$A_i$($i$= 1 ， 2 ，…，$m$)是短语，如果某命题变元 P_j 在短语 A_i 中出现多于一次，则不外如下两种情况：

（ 1 ） P_j 与 $\neg P_j$ 同时出现，这时 A_i= 0 ，删除之.

（ 2 ） 文字 $\widetilde{P}_j$ 重复出现，这时利用 $\widetilde{P}_j\wedge\widetilde{P}_j=\widetilde{P}_j$ 进行合并.

因此，我们不妨设任一命题变元 P_j (j= 1 ， 2 ，…，n)在短语 A_i(i= 1 ， 2 ，…，m)中最多出现一次. 检查每个短语 A_i，若 A_i 中缺少命题变元 P_j，则以如下方式将 A_i 化为两个含有 P_j 的短语的析取.

$$A_i=A_i\wedge(P_j\vee\neg P_j)=(A_i\wedge P_j)\vee(A_i\wedge\neg P_j)$$

记　$A_{i_1}=A_i\wedge P_j$，　$A_{i_2}=A_i\wedge\neg P_j$　　则 $A=A_1\vee\cdots\vee A_{i_1}\vee A_{i_2}\vee\cdots\vee A_m$.

再次检查每个短语，……，一直下去，直到 A 的析取范式中每个短语都包含所有命题变元为止. 这时，调整诸短语中文字的次序可使其成为极小项，从而得到与 A 等价的主析取范式.

唯一性留给读者. ▌

为求一个公式 A 的主析取范式，可以利用定理 2 的证明所指出的方法，即：先把 A 化为析取范式，进而添加短语中缺少的命题变元，最终得到主析取范式.

例 4　求 $P\rightarrow Q$ 的主析取范式.

$P\rightarrow Q=\neg P\vee Q$

$=(\neg P\wedge(Q\vee\neg Q))\vee(Q\wedge(P\vee\neg P))$

$=(\neg P\wedge Q)\vee(\neg P\wedge\neg Q)\vee(Q\wedge P)\vee(Q\wedge\neg P)$

$=(\neg P\wedge Q)\vee(\neg P\wedge\neg Q)\vee(P\wedge Q)$

$=m_0\vee m_1\vee m_3$

求主析取范式还可利用真值表进行.

例 5　求 $P\leftrightarrow Q$ 的主析取范式.

$P\leftrightarrow Q$ 的真值表如下：

P	Q	$P\leftrightarrow Q$
0	0	1
0	1	0
1	0	0
1	1	1

由于在指派(0,0)下，即指定 $(P,\ Q)$ 为(0，0)时，$P\leftrightarrow Q$ 为1，故 $P\leftrightarrow Q$ 的主析取范式必含有极小项 m_0，又由于在指派(0，1)下，$P\leftrightarrow Q$ 为0，故 $P\leftrightarrow Q$ 的主析取范式中必不含极小项 m_1，类似讨论其它情况可得 $P\leftrightarrow Q$ 的主析取范式：$P\leftrightarrow Q=m_0\vee m_3$.

例 6　$A=(P\wedge Q)\vee(\neg P\wedge R)\vee(Q\wedge R)$

P	Q	R	A
0	0	0	0
0	0	1	1
0	1	0	0
0	1	1	1
1	0	0	0
1	0	1	0
1	1	0	1
1	1	1	1

于是，　$A=m_1\vee m_3\vee m_6\vee m_7$

例 7 甲说乙说谎，乙说丙说谎，丙说甲、乙都说谎。问谁说真话、谁说谎。

令　P：甲说真话；Q：乙说真话；R：丙说真话；

依题意：

$$P=\neg Q,\ Q=\neg R,\ R=\neg P\wedge\neg Q.$$

因而，

$$(P\leftrightarrow\neg Q)\ \wedge\ (Q\leftrightarrow\neg R)\ \wedge\ (R\leftrightarrow(\neg P\wedge\neg Q))=1\ .$$

而

$$\begin{aligned}&(P\leftrightarrow\neg Q)\ \wedge\ (Q\leftrightarrow\neg R)\ \wedge\ (R\leftrightarrow(\neg P\wedge\neg Q))\\&\quad=\ (P\rightarrow\neg Q)\wedge(\neg Q\rightarrow P)\ \wedge(Q\rightarrow\neg R)\ \wedge(\neg R\rightarrow Q)\ \wedge(R\rightarrow(\neg P\wedge\neg Q))\\&\qquad\wedge((\neg P\wedge\neg Q))\rightarrow R)\\&\quad=\ (\neg P\vee\neg Q)\ \wedge\ (Q\vee P)\ \wedge\ (\neg Q\vee\neg R)\ \wedge\ (R\vee Q)\\&\qquad\wedge\ (\neg R\vee(\neg P\wedge\neg Q))\ \wedge\ (\neg\ (\neg P\wedge\neg Q))\ \vee R)\\&\quad=\ \neg P\wedge Q\wedge\neg R.\end{aligned}$$

故 $\neg P\wedge Q\wedge\neg R=1$，即：乙说真话，甲和丙说谎.

注：该题也可用真值表做，读者自己完成.

与主析取范式完全类似，我们也可以讨论主合取范式.

定义 5　设 P_1，P_2，…，P_n 是 n 个命题变元，形如

$$\widetilde{P}_1\vee\widetilde{P}_2\vee\cdots\vee\widetilde{P}_n$$

的公式，称为 P_1，P_2，…，P_n 生成的极大项，其中 $\widetilde{P}_i=P_i$ 或 $\neg P_i$.

极大项 $\widetilde{P}_1\vee\widetilde{P}_2\vee\cdots\vee\widetilde{P}_n$ 可用 $\widetilde{m}_{\delta_1\delta_2\cdots\delta_n}$ 或 $\widetilde{m}_i$ 表示，

其中 $\delta_i=\begin{cases}0 & \widetilde{P}_i=P_i\\1 & \widetilde{P}_i=\neg P\end{cases}$

而 i 为 $\delta_1\ \delta_2\cdots\delta_n$ 的十进制表示.

极大项与极小项有着类似的性质，请读者列出.

定义 6　设公式 A 中出现的所有命题变元为 P_1，P_2，…，P_n，如果在 A 的合取范式 A' 中，每个子句均为关于 P_1，P_2，…，P_n 的极大项，则称 A' 为 A 的主合取范式.

定理 3　任意公式 A，都存在唯一一个与之等价的主合取范式.

读者自证.

习 题 六

1．试证公式 $((P\vee Q)\wedge\neg(\neg P\wedge(\neg Q\vee\neg R)))\vee(\neg P\wedge\neg Q)\vee(\neg P\wedge\neg R)$ 是永真公式.

2．试将下列公式化为析取范式和合取范式.

（1）　$P\wedge(P\rightarrow Q)$.

（2）　$\neg(P\vee Q)\leftrightarrow\neg P\wedge Q$.

3．试将下列公式化为主析取范式和主合取范式.

（1）　$P\rightarrow((P\rightarrow Q)\wedge\neg(\neg Q\vee\neg P))$.

（2）　$P\vee(\neg P\rightarrow(Q\vee(\neg Q\rightarrow R)))$.

4．判断下列公式是否永真式？永假式？可满足的？

（1） $(P\rightarrow(Q\wedge R))\wedge(\neg P\rightarrow(\neg Q\wedge\neg R))$.

（2） $P\rightarrow(P\wedge(Q\rightarrow P))$

5．证明定理 2 中的唯一性.

§ 7　推理理论

我们通常采用的推理形式，大多是从某些前提出发推出某些结论，本节就来研究这种形式的推理.

当前提的真蕴涵结论的真时，称前提和结论之间有可推导性关系，即前提与结论之间的推理是正确的. 称这种推理为演绎推理. 演绎逻辑研究怎样的前提和结论之间有可推导性关系.

归纳逻辑与演绎逻辑不同，从真的前提出发，使用归纳推理，得到的结论只能要求它自身是协调的，或者它与前提是协调的，但结论不一定是真的. 在归纳推理中，前提的真并不蕴涵结论的真.

本节乃至本篇研究的推理属于演绎推理.

定义 1　设 A，B 是两个公式，如果对任何指派 I，当 A 为 1 时 B 必为 1，则称 A 蕴涵 B，或称 B 是 A 的逻辑结果，记为 $A\Rightarrow B$. A 称为蕴涵式前件，B 称为蕴涵式后件.

注意：符号“$\Rightarrow$”与“$=$”一样，表示两个公式之间的某种关系，它是关系符而不是联结词，因此，$A\Rightarrow B$ 不是公式. 而“$\rightarrow$”是逻辑联结词，将公式 A, B 联结成一个新公式.

显然，$A\Rightarrow B$ 当且仅当 $A\rightarrow B$ 永真.

为证 $A\Rightarrow B$，可以列出 A，B 的真值表，看看对任何指派 I，当 A 为 1 时 B 是否一定为 1，也可按照定义采用解释性证明或通过推导证明 $A\rightarrow B$ 永真(称为永真式推导).

例 1　$\neg(P\rightarrow Q)\Rightarrow P$

列出真值表

P	Q	$\neg(p\rightarrow Q)$	P
0	0	0	0
0	1	0	0
1	0	1	1
1	1	0	1

即可看出 $\neg(P\rightarrow Q)\Rightarrow P$.

例 2　$A\wedge(A\rightarrow B)\Rightarrow B$.

先证　$P\wedge(P\rightarrow Q)\Rightarrow Q$，列出真值表

P	Q	$P\wedge(P\to Q)$	Q
0	0	0	0
0	1	0	1
1	0	0	0
1	1	1	1

从而看出 $P\wedge(P\to Q)\Rightarrow Q$，因而 $P\wedge(P\to Q)\to Q$ 是永真的，根据代入原则，$A\wedge(A\to B)\to B$ 永真，于是 $A\wedge(A\to B)\Rightarrow B$.

例 3　$(A\to B)\wedge(B\to C)\Rightarrow(A\to C)$

[证法一] 解释性证明.

对任意指派 I，若 $(A\to B)\wedge(B\to C)^I=1$，则 $(A\to B)^I=1$，$(B\to C)^I=1$，故当 $A^I=1$ 时，$B^I=1$，从而 $C^I=1$，即知在指派 I 下 $(A\to C)^I=1$，所以 $(A\to B)\wedge(B\to C)\Rightarrow(A\to C)$.

[证法二] 永真式（重言式）推导.

$$
\begin{aligned}
&(A\to B)\wedge(B\to C)\to(A\to C)\\
&\quad=\ (\neg A\vee B)\wedge(\neg B\vee C)\to(\neg A\vee C)\\
&\quad=\ \neg((\neg A\vee B)\wedge(\neg B\vee C))\vee(\neg A\vee C)\\
&\quad=\ ((A\wedge\neg B)\vee(B\wedge\neg C))\vee(\neg A\vee C)\\
&\quad=\ (A\wedge\neg B)\vee((B\wedge\neg C)\vee(\neg A\vee C))\\
&\quad=\ (A\wedge\neg B)\vee((B\vee\neg A\vee C)\wedge(\neg C\vee\neg A\vee C))\\
&\quad=\ (A\wedge\neg B)\vee(B\vee\neg A\vee C)\\
&\quad=\ (A\vee B\ \vee\neg A\vee C)\wedge(\neg B\vee B\ \vee\neg A\vee C)\\
&\quad=\ 1.
\end{aligned}
$$

故 $(A\to B)\wedge(B\to C)\Rightarrow(A\to C)$.

定理 1　公式的蕴涵是反对称关系，即

（1）　$A\Rightarrow A$

（2）　若 $A\Rightarrow B$，$B\Rightarrow A$ 则 $A=B$

（3）　若 $A\Rightarrow B$，$B\Rightarrow C$ 则 $A\Rightarrow C$.

证明 只证（3），其它读者自证.

[证法一] 解释性证明

对任意解释 I, 若 $A^I=1$, 则由 $A\Rightarrow B$ 知，$B^I=1$, 又由 $B\Rightarrow C$ 知，$C^I=1$, 从而 $A\Rightarrow C$.

[证法二] 永真式推导

因为 $A\Rightarrow B$ 且 $B\Rightarrow C$，所以 $A\to B=1, B\to C=1$.

$$
\begin{aligned}
A\to C\ &=\ \neg A\vee C\\
&=\ (\neg A\vee C)\vee(\neg B\wedge B)\\
&=\ (\neg A\vee C\vee\neg B)\wedge(\neg A\vee C\vee B)\\
&=\ (\neg A\vee(B\to C))\ \wedge((A\to B)\ \vee C)
\end{aligned}
$$

$= \quad 1.$

故 $\quad A \Rightarrow C.$ ▌

定义 2　设 $\Gamma = \{A_1, A_2, \cdots, A_n\}$ 是一个公式集合，B 是公式，如果

$$A_1 \wedge A_2 \wedge \cdots \wedge A_n \Rightarrow B$$

则称 B 是 Γ (或 $A_1, A_2, \cdots, A_n$) 的逻辑结果，记为

$$\Gamma \Rightarrow B \quad \text{或} \quad A_1, A_2, \cdots, A_n \Rightarrow B.$$

不难验证如下基本蕴涵式：

1．$P \wedge Q \Rightarrow P$

2．$P \wedge Q \Rightarrow Q$

3．$P \Rightarrow P \vee Q$

4．$Q \Rightarrow P \vee Q$

5．$\neg P \Rightarrow P \rightarrow Q$

6．$Q \Rightarrow P \rightarrow Q$

7．$\neg(P \rightarrow Q) \Rightarrow P$

8．$\neg(P \rightarrow Q) \Rightarrow \neg Q$

9．$P, Q \Rightarrow P \wedge Q$

10．$\neg P, P \vee Q \Rightarrow Q$

11．$P, P \rightarrow Q \Rightarrow Q$

12．$\neg Q, P \rightarrow Q \Rightarrow \neg P$

13．$P \rightarrow Q, Q \rightarrow R \Rightarrow P \rightarrow R$

14．$P \vee Q, P \rightarrow R, Q \rightarrow R \Rightarrow R$

15．$P \rightarrow Q \Rightarrow P \vee R \rightarrow Q \vee R$

16．$P \rightarrow Q \Rightarrow P \wedge R \rightarrow Q \wedge R$

定理 2（蕴涵式代入原则） 设 A, B 是两个公式，$A \Rightarrow B$，P_1，P_2，…，P_n 为这两个公式中出现的所有命题变元，A_1，A_2，…，A_n 是任意一组公式，若用 A_i ($1 \leqslant i \leqslant n$) 代替 A，B 中的 P_i 分别得到公式 A', B'，则 $A' \Rightarrow B'$.

读者自证

以上通过例题介绍了几种证明 $A \Rightarrow B$ 的方法，下面引入一种更为符合通常推理习惯的方法——演绎法

定义 3　设 Γ 是一个公式集合，从 Γ 推出公式 A 的一个演绎推理是一个有限公式序列：

$$A_1, A_2, \cdots, A_k$$

其中，A_i ($1 \leqslant i \leqslant k$) 满足如下条件之一：

（1）$A_i \in \Gamma$.

（2）A_i 是某些 A_j（$j<i$）的逻辑结果.

（3）A_i 是永真式.

且 A_k 就是 A.

当存在一个从公式集合 Γ 推出公式 A 的演绎推理时，称 Γ 可演绎出 A，记为 $\Gamma|==A$. Γ 中的公式称为前提，A 称为演绎结果或结论.

定理 3 设 Γ 是公式集合，A 是公式，则 $\Gamma|==A$ 当且仅当 $\Gamma \Rightarrow A$.

证明 必要性，设从 Γ 可演绎出 A，令 A_1，A_2，…，A_k 是一个从 Γ 推出 A 的演绎推理，往证，对任意 $i \in \{1, 2, \cdots, k\}$，$\Gamma \Rightarrow A_i$，对 i 施以归纳法，当 $i=1$ 时，由演绎推理序列的定义可知 $A_i = A_1$ 或为前提（即 $A_1 \in \Gamma$）或为永真式，无论何种情况均有 $\Gamma \Rightarrow A_i$ 成立. 设当 $i \leqslant n-1$ $(n \leqslant k)$ 时成立，考虑 $i=n$ 的情形. 若 $A_n \in \Gamma$ 或 A_n 永真，则显然 $\Gamma \Rightarrow A_n$，否则，A_n 是某些 A_j $(j<n)$ 的逻辑结果，不妨设

$$A_{j_1}, A_{j_2}, \cdots, A_{j_l} \Rightarrow A_n$$

其中 $1 \leqslant j_1, j_2, \cdots, j_l \leqslant n-1$. 由归纳假设知 $\Gamma \Rightarrow A_{j_m}$ $(m=1, 2, \cdots, l)$，故知

$$\Gamma \Rightarrow A_{j_1} \wedge \cdots \wedge A_{j_l}$$

再由 $\Rightarrow$ 的传递性，有 $\Gamma \Rightarrow A_n$. 归纳法完成.

充分性. 设 $\Gamma \Rightarrow A$，不妨设 $\Gamma = \{A_1, A_2, \cdots, A_m\}$，由演绎推理的定义知

$$A_1, A_2, \cdots, A_m, A$$

是一个从 Γ 推出 A 的演绎，于是便知，Γ $|==A$. ▌

定理 4 设 Γ 是一个公式集合，B，C 是两个公式，如果从 $\Gamma \cup \{B\}$ 可演绎出 C，则 $\Gamma \Rightarrow B \rightarrow C$.

证明 因为从 $\Gamma \cup \{B\}$ 可演绎出 C，则 $\Gamma \cup \{B\} \Rightarrow C$，不妨设

$$\Gamma = \{A_1, A_2, \cdots, A_m\}$$

则 $$A_1 \wedge A_2 \wedge \cdots \wedge A_m \wedge B \Rightarrow C,$$

故 $$A_1 \wedge A_2 \wedge \cdots \wedge A_m \wedge B \rightarrow C = 1$$

利用基本等价式 $P \wedge Q \rightarrow R = (P \rightarrow (Q \rightarrow R))$ 及 等价式代入原则知

$$(A_1 \wedge A_2 \wedge \cdots A_m \wedge B \rightarrow C) = (A_1 \wedge A_2 \wedge \cdots \wedge A_m \rightarrow (B \rightarrow C)),$$

所以 $$A_1 \wedge A_2 \wedge \cdots \wedge A_m \rightarrow (B \rightarrow C) = 1,$$

从而 $$A_1 \wedge A_2 \wedge \cdots \wedge A_m \Rightarrow B \rightarrow C$$

因而知 $\Gamma \Rightarrow B \rightarrow C$. ▌

至此，给出公式集合 $\Gamma = \{A_1, A_2, \cdots, A_m\}$ 和公式 B，证明 $\Gamma \Rightarrow B$ 可用三种方法：

（1） 真值表法：列出 $A_1 \wedge A_2 \wedge \cdots \wedge A_m$ 和 B 的真值表，判断是否有

$$A_1 \wedge A_2 \wedge \cdots \wedge A_m \Rightarrow B.$$

（2） 证明 $A_1 \wedge A_2 \wedge \cdots \wedge A_m \rightarrow B$ 永真.

（３） 演绎法：根据一些基本等价式和基本蕴涵式，从 Γ 出发演绎出 B.

根据演绎推理的定义及定理３，我们将构造演绎推理序列必须遵循的规则总结如下：

（１） 前提引入规则　在演绎过程中，可随便使用前提，该规则记为 **P**.

（２） 结论引用规则　在演绎过程中，可随便引入前边公式的逻辑结果．该规则记为 **C**.

（３） 永真式引用规则　在演绎过程中，可随便引入永真式，该规则记为 **T**.

（４） 分离规则　由公式 A，$A\rightarrow B$ 可引入 B．该规则记为 **MP**.

（５） 附加条件规则　为证 $\Gamma\Rightarrow B\rightarrow C$，可证 $\Gamma\cup\{B\}\Rightarrow C$，该规则记为 **CP**.

注： 分离规则是结论引用规则的特殊情况，由于其重要性而单独列出作为一条规则.

例 4　$\{P\vee Q,\ P\rightarrow R,\ Q\rightarrow S\}\Rightarrow S\vee R$.

由于 $S\vee R=\neg S\rightarrow R$，只需证 $\{P\vee Q,\ P\rightarrow R,\ Q\rightarrow R\}\Rightarrow\neg S\rightarrow R$

又根据 **CP** 规则，可将 $\neg S$ 作为附加前提去演绎 R，即只需证

$$\{P\vee Q,\ P\rightarrow R,\ Q\rightarrow S,\ \neg S\}\ |==R$$

(1)	$Q\rightarrow S$	**P**
(2)	$\neg S$	**P**
(3)	$\neg Q$	**C** (1)(2)
(4)	$P\vee Q$	**P**
(5)	P	**C** (3)(4)
(6)	$P\rightarrow R$	**P**
(7)	R	**MP**(5)(6)

例 5　前提：如果马会飞或狗不叫，则母鸡就会是飞鸟；如果母鸡是飞鸟，那么烤熟的鸭子还会跑；烤熟的鸭子不会跑. 结论：马不会飞、狗要叫.

令　P：马会飞，Q：狗要叫，R：母鸡是飞鸟，S：烤熟的鸭子还会跑.

要证：$\{P\vee\neg Q\rightarrow R,\ \ R\rightarrow S,\ \neg S\}\Rightarrow\neg P\wedge Q$.

(1)	$\neg S$	**P**
(2)	$R\rightarrow S$	**P**
(3)	$\neg R$	**C** (1)(2)
(4)	$P\vee\neg Q\rightarrow R$	**P**
(5)	$\neg(P\vee\neg Q)$	**C**(3)(4)
(6)	$\neg P\wedge Q$	**C**(5)

在进行演绎推理时，我们有时采用反证法的思想，其基础是下面的定义和定理.

定义 3 设 $A_1, A_2, \cdots, A_n$ 是 n 个公式，若 $A_1 \wedge A_2 \wedge \cdots \wedge A_n$ 为可满足式，则称公式 $A_1, A_2, \cdots, A_n$ 是相容的或一致的. 否则，称其是不相容的或不一致的.

定理 5 设 Γ 是一个公式集合，B 是一个公式，则 $\Gamma \Rightarrow B$ 当且仅当 $\Gamma \cup \{\neg B\}$ 中的公式不相容.

证明 设 $\Gamma = \{A_1, A_2, \cdots, A_n\}$，

则 $\Gamma \cup \{\neg B\}$ 中的公式不相容

当且仅当 $(A_1 \wedge A_2 \wedge \cdots \wedge A_n) \wedge \neg B = 0$

当且仅当 $\neg(A_1 \wedge A_2 \wedge \cdots \wedge A_n) \vee B = 1$

当且仅当 $(A_1 \wedge A_2 \wedge \cdots \wedge A_n) \rightarrow B = 1$

当且仅当 $(A_1 \wedge A_2 \wedge \cdots \wedge A_n) \Rightarrow B$ ▌

对公式不相容的判断有时用到下列形式.

定理 6 公式 $A_1, A_2, \cdots, A_n$ 是不相容的当且仅当存在命题公式 R，使得

$$A_1 \wedge A_2 \wedge \cdots \wedge A_n \Rightarrow R \wedge \neg R$$

证明 若 $A_1 \wedge A_2 \wedge \cdots \wedge A_n \Rightarrow R \wedge \neg R$，则意味着 $A_1 \wedge A_2 \wedge \cdots \wedge A_n \rightarrow R \wedge \neg R$ 是永真公式，而该蕴涵式的后件是一永假公式，因此前件 $A_1 \wedge A_2 \wedge \cdots \wedge A_n$ 也必为永假公式，故 $A_1, A_2, \cdots, A_n$ 是不相容的.

反之，若 $A_1, A_2, \cdots, A_n$ 是不相容的，则 $A_1 \wedge A_2 \wedge \cdots \wedge A_n$ 是一永假公式. 由蕴涵联结词的定义，$A_1 \wedge A_2 \wedge \cdots \wedge A_n \rightarrow R \wedge \neg R$ 为永真公式，因而

$$A_1 \wedge A_2 \wedge \cdots \wedge A_n \Rightarrow R \wedge \neg R.$$ ▌

例 6 $\{P \rightarrow (Q \rightarrow S),\ \neg R \vee P,\ Q\} \Rightarrow R \rightarrow S$

根据 **CP** 规则，只需证 $\{P \rightarrow (Q \rightarrow S),\ \neg R \vee P,\ Q,\ R\} \Rightarrow S$.

根据定理 5，只需证 $P \rightarrow (Q \rightarrow S),\ \neg R \vee P,\ Q,\ R,\ \neg S$ 不相容.

(1) $\neg R \vee P$	**P**
(2) R	**P**
(3) P	**C** (1)(2)
(4) $P \rightarrow (Q \rightarrow S)$	**P**
(5) $Q \rightarrow S$	**MP** (3)(4)
(6) $\neg S$	**P**
(7) $\neg Q$	**C** (6)(5)
(8) Q	**P**
(7) $\neg Q \wedge Q$	**C** (6)(5)

由定理 6 得证.

习 题 七

1．证明定理 1 中(2)式.

2．设 A_1，A_2，…，A_n 是公式，利用演绎推理序列的定义证明：从 $\{A_1, A_2, \cdots, A_n\}$ 可演绎出 A，当且仅当 $\{A_1, A_2, \cdots, A_n, \neg A\}$ 可演绎出 $R \wedge \neg R$.

3．证明

（1） $\{C \vee D, (C \vee D) \rightarrow \neg H, \neg H \rightarrow (A \wedge \neg B), (A \wedge \neg B) \rightarrow (R \vee S)\}$
$\Rightarrow R \vee S$.

（2） $\{P \vee Q, Q \rightarrow R, P \rightarrow M, \neg M\} \Rightarrow R \wedge (P \vee Q)$.

（3） $\{\neg P \vee Q, \neg Q \vee R, R \rightarrow S\} \Rightarrow P \rightarrow S$.

4．在去天堂和地狱的岔路口，站着天使和魔鬼，他们都化作人形，无法区别. 他们对所有的问题只回答对和错. 天使永远说真话，魔鬼永远说假话. 有两个命题：(1) 你是天使. (2) 左边的路通天堂. 用这两个命题组合成一个命题问他们中的一个，使得能够根据回答知道上天堂的路.

第十六章　谓词逻辑

§ 1　谓词与量词

上一章我们讨论了命题逻辑，在命题逻辑中，把简单命题作为基本单位，而不再对其内部结构进行分析，这样就丢失了简单命题之间的联系，例如，

所有人都会死，

苏格拉底是人，

所以，苏格拉底必会死.

这个推理称为苏格拉底论题，从直观上看，它应该是正确的，然而，在命题逻辑中却不能表示这样的推理. 因在命题逻辑中，与苏格拉底论题相应的推理形式为：

$$P \wedge Q \Rightarrow R$$

但是，这个推理形式是不正确的，从而不能由此断定苏格拉底论题是正确的. 出现这种情况的原因在于，苏格拉底论题的正确性依赖于各命题的结构及他们之间的联系，而这些信息在命题逻辑中已全部丢失. 苏格拉底论题中的三个命题, 只能看作是三个独立的命题，又如命题

$\sqrt{2}$ 是无理数.　$\sqrt{3}$ 是无理数.

在命题逻辑中，这两个命题只能当作独立的命题来看待，无法考虑其共性. 事实上，这两个命题有共同的谓语“是无理数”，它们描述了两个数 $\sqrt{2}$ 与 $\sqrt{3}$ 的一个共同特征.

从以上例子可见，由于命题逻辑把命题作为基本单位，而不考虑命题的结构，这种抽象过于粗糙，使得其表达能力受到了极大限制，因此有必要对命题作进一步的剖析，唯此才能增强其表达能力，适应更广泛的推理需要.

由于命题是一个具有真假意义的句子，对命题的结构进行分析，也就是对句子结构进行分析. 我们知道，一个陈述句一般由主语部分和谓语部分构成，例如，下列语句中，划_____线的为主语部分，划……线的为谓语部分：

苏格拉底 是人.

这本书 很有趣.

直线 l 通过 点 x，y.

一个命题的主语部分，通常由我们所讨论的对象担任，这些对象称为个体，可以用小写字母 a，b，c，…表示. 个体所在的范围称为论域或个体域，用 D 表示. 它相当于集

合论中的全集. 最大的论域包括所有事物——有形的、无形的、抽象的、具体的……，称为全总论域或全总个体域. 当论域没有明确指定时，我们常常是在使用全总论域.

命题中的谓语部分，描述个体的性质、行为、状态或个体之间的关系等，一般用大写字母 P，Q，R，…表示. 在数理逻辑中，命题的谓语部分一般称作谓词，例如

（1） 王平是学生.

（2） 刘利是学生.

若用 $P(\cdot)$ 表示“…是学生”，a 表示“王平”，b 表示“刘利”，则这两个命题可表示为 $P(a)$，$P(b)$. 当然，这两个命题也可直接表示为 P(王平)，P(刘利)，又如

（1） 李平与李刚是兄弟.

（2） 5 大于 3.

（3） 天津位于北京的东南方.

若用 $B(\cdot,\cdot)$ 表示“…与…是兄弟”，a_1 表示李平，a_2 表示李刚，则命题 (1) 可表示为 $B(a_1, a_2)$ 或直接写成 B(李平，李刚)；若用 $G(\cdot,\cdot)$表示“…大于…”，命题(2)可表示为 $G(5, 3)$；若用 $D(\cdot,\cdot,\cdot)$ 表示“…位于…的…”，a 表示“天津”，b 表示“北京”，c 表示“东南方”，则命题(3)可表示为 $D(a, b, c)$，或直接表示为 D(天津，北京，东南方).

由上面例子可以看到，当把一个命题中的个体去掉，只抽出其谓词时，在表达上是不够方便的. 为此，我们引入个体变元 x，y，z，…填补个体的位置，以求在表达上更清楚、准确. 例如，“…是学生”可以表达成“x 是学生”，用 $P(x)$表示，“…大于…”可以表达成“x 大于 y”，用 $G(x, y)$表示等等.

个体变元符号 x，y，z，…，有时也用来表示任一固定个体，就象微积分中，实数变量符号 x 常用来表示任一固定实数一样.

谓词中的个体变元标志着个体出现的位置，它们可以用论域中的任何个体代替，从而形成命题. 因此，也可以把个体变元说成是可以在论域中任意变化的量.

在谓词中引入个体变元后，谓词便具有命题的“形式”，例如“x 大于 y”，“x 是学生”等，但这里的 x，y 不是确定的个体，这些谓词不具有真假意义，也就不是命题. 但是，一旦用具体的个体去代换谓词中的个体变元，便得到一个命题.

上面我们从直观的角度介绍了谓词的概念. 在数学上，我们还需要对它进行抽象.

设 $P(x_1, x_2, \cdots, x_n)$是一个谓词，用论域 D 中的一组个体 a_1，a_2，…，a_n 代替 x_1，x_2，…，x_n，我们便得到一个命题 $P(a_1, a_2, \cdots, a_n)$，该命题的真值或为 1 或为 0，所以，可以把 P 看成是从 D^n 到 {0，1} 的一个映射.

定义 1　D^n 到 {0，1} 的函数称为 n 元谓词或 n 元命题函数.

例 1　设 D＝{1，2}，$P(x, y)$表示“x 大于 y”，则 $P(x, y)$定义了如下映射：

$P(1, 1)=0$，$P(1, 2)=0$，$P(2, 1)=1$，$P(2, 2)=0$.

例 2　设 $D=\mathbf{N}$，$P(x)$表示“x 是素数”，则 $P(x)$定义了如下映射：

$P(0)=0$，$P(1)=0$，$P(2)=1$，$P(3)=1$，$P(4)=0$，…，

由以上二例可以看出，定义 1 给出的谓词概念与直观上的谓词概念是一致的.

如同简单命题一样，可以定义简单谓词，又如同简单命题可以通过逻辑联词联结而成复合命题一样，简单谓词也可由逻辑联词联结而成复合谓词，命题逻辑中的五个联结词$\neg$，$\vee$，$\wedge$，$\rightarrow$，$\leftrightarrow$，均可平移到谓词逻辑，其意义保持不变.

上面我们讨论了谓词的概念，谓词概念的引入使我们可以讨论命题的结构及命题之间的联系. 但是，只有谓词概念还不足以表达我们通常感兴趣的推理过程，例如，“所有人都会死”或“有一个人不会死”该如何表达？为了解决这类问题，需要引入量词的概念.

定义 2　（1）表示“所有”、“任意”、“一切”的词称为全称量词，记为$\forall$，$\forall x$ 表示对论域中的所有个体，x 称为$\forall$的指导变元(全称性变元)，用来指代所讨论的个体. $\forall x\,P(x)$表示论域中的所有个体都有性质 P.　（2）表示“存在着”、“至少有一个”的词称为存在量词，记为$\exists$.　$\exists x$ 表示论域中存在个体，同全称量词一样，这里的 x 也称为$\exists$的指导变元(存在性变元)，用来指代所讨论的个体. 而$\exists xP(x)$表示论域中存在着个体具有性质 P.

例 3 设 $F(x)$：x 会飞，论域 D 为鸟集合.

$\forall x\,F(x)$ 表示所有的鸟都会飞.

例 4 设 $W(x)$：x 是白的，论域 D 为菊花集合.

$\exists x\,W(x)$ 表示有些菊花是白的.

包含有量词的命题的真值与论域的指定有关，使用量词必须确定论域. 比如，若 $P(x)$表示“x 是素数”，当论域 $D=\{2,3,5,7\}$时，$\forall x\,P(x)=1$；当论域 $D=\{1,2,3,4\}$时，$\forall x\,P(x)=0$. 论域的确定一般有两种方式：默认或明确指定. 默认的论域根据讨论的问题及上下文确定. 有时，论域中包含多种类型的元素，为了讨论论域中某部分个体的性质，就要引入刻划这部分个体性质的谓词，称其为特性谓词. 全称量词后的特性谓词一般应作为蕴涵联结词的前件，存在量词后的特性谓词则一般为合取式的一项. 比如，用 $M(x)$表示“x 是人”(特性谓词)，$D(x)$ 表示“x 会死”，则“所有人会死”应表为：$\forall x\,(M(x)\rightarrow F(x))$，“有些人会死”则应表为：$\exists x\,(M(x)\wedge D(x))$.

量词本身并不是一个独立的逻辑概念，当论域是有限集时，它可以用联结词替代. 设论域 $D=\{a_1,\ a_2,\ \cdots,\ a_n\}$，$P(x)$是一元谓词，则

$$\forall xP(x) \quad = \quad P(a_1)\wedge P(a_2)\wedge\cdots\wedge P(a_n)$$

$$\exists xP(x) \quad = \quad P(a_1)\ \vee P(a_2)\ \vee\cdots\vee P(a_n)$$

但当论域为无限时，则不能如上转化. 我们只能直观地说，这时全称量词“相当于”无限个合取联结词的作用，存在量词“相当于”无限个析取联结词的作用.

例 5 我为人人，人人为我.

令　论域 D 为人类集合，$S(x,\ y)$：x 为 y 服务，I 表示我. 则命题表示为

$$\forall x\,S(\mathrm{I},\ x)\wedge\forall x\,\mathrm{S}(x,\ \mathrm{I}).$$

例 6 勇敢者未必都是成功者.

令　论域 D 为人类集合，$B(x)$：x 是勇敢者，$S(x)$：x 是成功者. 命题可表示为：

$$\neg\forall x(B(x)\rightarrow S(x)) \quad 或 \quad \exists x(B(x)\wedge\neg S(x)).$$

为了容易建立概念，上面的讨论大多以一元谓词为例，现考虑 n 元谓词的情况. 如果 $P(x, y, \cdots, z)$是一个 n 元谓词，则 $\forall xP(x, y, \cdots, z)$，$\exists xP(x, y, \cdots, z)$ 均是以 $y, \cdots, z$ 为个体变元的 $n-1$ 元谓词，且对于任意取定的 $b, \cdots, c\in D$，

$\forall x\, P(x, b, \cdots, c)=1$　当且仅当　对于每一 $a\in D$，$P(a, b, \cdots, c)=1$

$\exists x\, P(x, b, \cdots, c)=1$　当且仅当　至少有一 $a\in D$，$P(a, b, \cdots, c)=1$

例 7　苏格拉底论题

令 $M(x)$表示“x 是人”，$D(x)$表示“x 会死”，s 表示苏格拉底，则苏格底论题表示为

$$\forall x\,(M(x)\rightarrow D(x))$$

$$M(s)$$

所以，$D(s)$

例 8　所有有理数都是实数.

有的实数是有理数.

有的实数不是有理数.

令 $Q(x)$表示“x 是有理数”，$R(x)$表示“x 是实数”，以上三命题可分别形式化为

$$\forall x(Q(x)\rightarrow R(x))$$

$$\exists x(R(x)\wedge Q(x))$$

$$\exists x(R(x)\wedge\neg Q(x))$$

例 9　至少有一偶数是素数.

至少有一偶数且至少有一素数.

令：　$P(x)$：x 是素数.

$E(x)$：x 是偶数.

以上两命题可分别形式化为

$$\exists x(E(x)\wedge P(x))$$

$$\exists xE(x)\wedge\exists xP(x)$$

例 10　通过两个不同点至多有一条直线.

令：　$T(x)$：x 是点.

$L(x)$：x 是直线.

$P(x, y, z)$：x 通过 y，z.

$E(x, y)$：$x=y$.

则有

$$\forall x\forall y(\,(T(x)\wedge T(y)\wedge\neg E(x, y)\,)\rightarrow\forall z_1\forall z_2(\quad(L(z_1)\wedge L(z_2)\wedge P(z_1, x, y)\wedge P(z_2, x, y)\,)\rightarrow E(z_1, z_2)\quad)\,).$$

习 题 一

1．令 $P(x)$：x 是素数，$E(x)$：x 是偶数；$O(x)$：x 是奇数；

$D(x，y)$：x 整除 y.

合理指定论域，并将下列各式译成汉语：

（1） $P(5)$

（2） $E(2)\wedge P(2)$

（3） $\forall x(D(2，x)\rightarrow E(x))$

（4） $\exists x(E(x)\wedge D(x，6))$

（5） $\forall x(\neg E(x)\rightarrow \neg D(2，x))$

（6） $\forall x(E(x)\rightarrow \forall y(D(x，y)\rightarrow E(y)))$

（7） $\forall x(P(x)\rightarrow \exists y(E(y)\wedge D(x，y)))$

2．将下列命题符号化.

(1) 对于每一个实数 x，存在一个更大的实数 y.

(2) 存在实数 x，y，z，使得 x 与 y 之和大于 x 与 z 之积.

(3) 若 $x<y$ 且 $z<0$，则 $xz>yz$.

3．用符号化的形式表达函数 f 在 A 点连续的定义.

§ 2 合式公式

同命题逻辑一样，谓词逻辑中也可引入合式公式的概念，为此，我们首先约定如下四种符号：

1. 常量符号（个体符号）：a，b，c，… (或 a_1，a_2，…； b_1，b_2，…).

2. 变量符号：x，y，z … (或 x_1，x_2，…； y_1，y_2，…).

3. 函数符号：f，g，h，… (或 f_1，f_2，…； g_1，g_2，…). 每个函数符号使用时都有确定的元数. 为了指明元数，n 元函数符号通常记为 $f(x_1, x_2, \cdots, x_n)$.

4. 谓词符号：P，Q，R，… (或 P_1，P_2，…， Q_1，Q_2，…)，每个谓词符号使用时都有确定的元数. 为了指明元数，n 元谓词符号通常记为 $P(x_1, x_2, \cdots, x_n)$.

定义 1 谓词逻辑中的项归纳定义为

（1） 常量符号是项.

（2） 变量符号是项.

（3） 若 t_1，t_2，…，t_n 是项，则 $f(t_1，t_2，\cdots，t_n)$ 是项.

（4） 所有项都是有限次使用(1)，(2)，(3)生成的.

例如 a，b，c，a_1，a_2，x，y，x_1，x_2，$f(a，x，x_1)$，$f(g(b，x，y)，h(x，y))$ 均为项.

定义 2　若 t_1，t_2，…，t_n 是项，则 $P(t_1, t_2, \cdots, t_n)$ 是原子公式.

例如，P，$P(a, b)$，$P(a, x)$，$P(f(a, b), g(x))$都是原子公式.

定义 3　谓词逻辑中的合式公式 (wff) 归纳定义如下：

（1）　原子公式是合式公式.

（2）　若 A，B 是合式公式，则$(\neg A)$，$(A \vee B)$，$(A \wedge B)$，$(A \rightarrow B)$，$(A \leftrightarrow B)$ 是合式公式.

（3）　若 A 是合式公式，则 $(\forall x A)$，$(\exists x A)$ 是合式公式.

（4）　所有合式公式，都是有限次使用(1)，(2)，(3)生成的.

合式公式也简称公式.

同命题公式一样，在不会引起混乱时公式中的括号可以省写，例如，$(\forall x A)$可写为$\forall x A$，$((A \wedge B) \rightarrow C)$可以写为 $A \wedge B \rightarrow C$ 等. 至此，项与公式均采用了归纳定义，正是由于这种定义方法，在谓词演算中有关定理、性质的证明大量地使用(广义的)数学归纳法.

定义 4　设 A 是公式，若 A_1 是 A 的一部分且本身是公式，则称 A_1 是 A 的子公式.

定义 5　设 A 是公式，$\forall x A_1$(或$\exists x A_1$) 是 A 的子公式，则 A 中相应于 A_1 的一段称为$\forall x$(或$\exists x$)的辖域.

定义 6　设 A 是一个公式，若个体变元 x 出现在某个量词$\forall x$ 或$\exists x$ 的辖域之内，称 x 的这次出现是约束的，否则称 x 的这次出现是自由的. 一个个体变元，如果至少有一次出现是约束的，则称其为约束变元; 如果至少有一次出现是自由的，则称其为自由变元.

例如，$\exists x(P(x, y) \rightarrow Q(x, z)) \vee R(x)$从左向右算起，$x$ 的第一，二次出现是约束的，第三次出现是自由的，变量 y，z 的出现是自由的，x 既是约束变元也是自由变元，y，z 是自由变元.

例 1　证明下式是 wff，且指出各个量词的辖域以及各变元的性质.

$$\forall x(P(x, y) \rightarrow \exists y Q(x, y, z)) \wedge R(f(x, z))$$

证明

(1)　x，y，z 是个体变元，是项.

(2)　$P(x, y)$是原子公式，是 wff.

(3)　$Q(x, y, z)$是原子公式，是 wff.

(4)　$f(x, z)$是项.

(5)　$R(f(x, z))$是原子公式，是 wff.

(6)　$\exists y\, Q(x, y, z)$是 wff.

(7)　$P(x, y) \rightarrow \exists y Q(x, y, z)$是 wff.

(8)　$\forall x\, x(P(x, y) \rightarrow \exists y Q(x, y, z)) \wedge R(f(x, z))$是 wff.

其中，$\exists y$ 的辖域是 $Q(x, y, z)$，$\forall x$ 的辖域是 $P(x, y) \rightarrow \exists y Q(x, y, z)$，$x$ 在谓词 P 及 Q 中的出现是约束出现，x 在谓词 R 中的出现是自由出现，y 在谓词 Q 中的出现是约束出现，在谓词 P 中的出现是自由出现，z 的所有出现都是自由出现.

由于一个合式公式中，个体变元可以同时是约束变元和自由变元，这就给讨论问题带来不便，我们希望一个变元在同一个 wff 中只以一种面目出现，为达到此目的，我们引

入下面的换名规则.

首先看一个简单例子

$\forall xP(x)\vee Q(x)$

由量词的定义知，$\forall xP(x)$ 与 $\forall yP(y)$ 是同一个命题，因此上式应与

$\forall yP(y)\vee Q(x)$

具有同样意义.

推而广之，任一公式均可用如下换名规则给其中的变元换名.

(1) 将某个个体变元在量词中作为指导变元的出现和它在该量词辖域中的所有出现都用同一个新个体变元去替换.

(2) 所用新个体变元在原式中不出现.

例如 $\forall x(P(x，y)\rightarrow\exists yQ(x，y，z))\wedge R(f(x，z))$经过换名可化为

$\forall v(P(v，y)\rightarrow\exists wQ(v，w，z))\wedge R(f(x，z))$

任一公式，经过换名以后，总可以使任意约束变元不是自由变元. 下面, 当需要是我们将总是假设，所遇到的公式已经具备此特性. 同命题公式一样，谓词公式本身只是某种形式的符号串，必须通过“解释”才具有真假意义. 但是，由于谓词公式的结构较命题公式复杂得多，其“解释”也相应复杂.

定义 7　谓词公式 A 的一个解释 I，由对论域 D 和常量符号、函数符号、谓词符号依下列规则进行的一组指定构成.

（1） 指定 D 为一非空集合.

（2） 对每个常量符号指定 D 中一个元素.

（3） 对每个函数符号，指定一个同元函数.

（4） 对每个谓词符号，指定一个同元谓词.

谓词公式 A，如果不含自由变元，经过解释后便成为一个命题.

例 2　给出三个公式：

(1) $\forall xP(x)$.

(2) $\forall x\exists yP(x，y)$.

(3) $\forall x(P(x)\rightarrow Q(f(x)，a))$.

试分别给出上述公式的一个解释.

（1） 令　论域 $D=\{1，2\}$；　$P(1)=1$，$P(2)=0$.

在这个解释下，　$\forall xP(x)$ 的真值为 0.

（2） 令　论域 $D=\{1，2\}$；

$P(1，1)=1$，$P(1，2)=0$，$P(2，1)=0$，$P(2，2)=1$.

在这个解释下，$\forall x\exists yP(x，y)$ 的真值为 1.

（3） 令　论域 $D=\{1，2\}$；

$f(1)=2$，$f(2)=1$；　$a=1$；　$P(1)=0$，$P(2)=1$；

$Q(1，1)=1$，$Q(1，2)=1$，$Q(2，1)=0$，$Q(2，2)=1$.

在这个解释下，$\forall x(P(x)\rightarrow Q(f(x)，a))$ 的真值为 1.

谓词公式 A，如果含有自由变元，则为使其成为命题，除对 A 进行解释外，还需要将其中的自由变元指定为论域中的元素，即需要对自由变元“赋值”.

定义 8　设 A 是一个谓词公式，I 是对 A 的一个解释，在 I 的基础上，指定 A 中的自由变元为 D 中元素，称为对公式 A 在解释 I 下的一个赋值.

谓词公式经过解释 I 和赋值 v 以后，便成为一个命题，记为 $A^{I,v}$.

例 3　给出以下公式的某个解释和赋值.

$\forall xP(f(a，x)+g(y)，z)$.

令　D 为非负实数集；　$a=1$；　$P(x，y)$：$x>y$；　$f(x，y)=x+y$；　$g(x)=x^2$.

在此解释下，所给公式为：　$\forall x(1+x+y^2>z)$.

做如下赋值：　　$y=6$，　　$z=1$.

则所给公式的真值为 1.

而若做如下赋值：

$y=5$，　　$z=4\ 6$

则所给公式的真值为 0.

定义 9　设 A 是一个公式，如果对任意解释 I 和赋值 v，A 的真值总为 1，则称 A 是有效的（或永真的），否则，称 A 是非有效的. 永假、可满足也可类似定义.

定理 1 (代入原则)　设 A 是一个永真命题公式，P_1，P_2，…，P_n 是其中出现的所有命题变元，A_1，A_2，…，A_n 是任意一组谓词公式，若分别用 A_1，A_2，…，A_n 代替 A 中的 P_1，P_2，…，P_n 得到公式 B，则 B 必是有效的.

我们已知道，对于一个命题公式，我们总可以判断其是否永真、永假、可满足. 比如可通过做真值表或化范式来判断. 但对谓词公式判断其是否有效，是难以做到的，谓词公式的解释和赋值依赖于论域 D，当 D 是无穷集合时，D 中的元素及 D 上的函数、谓词都有无限多个，不可能逐个列举，事实上，谓词公式的判定问题是不可解的.

习 题 二

1．设 I 是如下一个解释：

$D=\{a，b\}$；

$P(a，a)=1$，$P(a，b)=0$，$P(b，a)=0$，$P(b，b)=1$.

试确定下列公式在 I 下的真值.

（1）　$\forall x\exists yP(x，y)$.

（2）　$\forall x\ \forall yP(x，y)$.

（3）　$\exists x\forall y\ P(x，y)$.

（4）　$\exists y\neg P(a，y)$.

（5）　$\forall x\forall y(P(x，y)\rightarrow P(y，x))$.

（6）　$\forall x\ P(x，x)$.

2．设 $A=\ \exists xP(x)\rightarrow\forall xP(x)$

（1） 若解释 I 的论域 D 仅含一个元素，A 的真值为何？

（2） 设 $D=\{1, 2\}$，求出使 A 为假的一个解释.

3. 设 I 是如下一个解释：

$D=\{1, 2, 3, 4\}$; $a=3$, $b=2$; $f(x)=x^2 \bmod 4+1$; $P(x, y)$: $x>y$.

求出下列公式在 I 下的真值：

(1) $P(a, f(a))\wedge P(b, f(b))$.

(2) $\forall x\forall y(P(x, y)\rightarrow P(f(x), f(y)))$.

§3 等价与范式

定义 1 设 A，B 是两个公式，如果在 A，B 的每一个解释及赋值下，A，B 总有相同的真值，则称 A 与 B 等价，记为 $A=B$.

显然，$A=B$ 当且仅当 $A\leftrightarrow B$ 有效. 由此，等价式代入原则也类似成立.

定理 1 (等价式代入原则) 设 $A=A(P_1, P_2, \cdots, P_n)$，$B=B(P_1, P_2, \cdots, P_n)$ 是两个命题公式，P_1，P_2，…，P_n 是其中出现的所有命题变元，$A=B$; 则对任意一组谓词公式 A_1，A_2，…，A_n，若分别用 A_1，A_2，…，A_n 代替 A, B 中的 P_1，P_2，…，P_n 得到公式 A', B'，即 $A'=A(A_1, A_2, \cdots, A_n)$，$B'=B(A_1, A_2, \cdots, A_n)$，则 $A'=B'$.

谓词逻辑中的基本等价式，可分为如下几组.

1．从命题逻辑中移植来的等价式.

根据等价式代入原则，命题逻辑中的基本等价式在谓词逻辑中相应成立.

例如， 由 $\neg\neg P=P$.

可得 $\neg\neg A=A$.

由 $P\rightarrow Q=\neg P\vee Q$.

可得 $A\rightarrow B=\neg A\vee B$.

由 $(P\wedge Q)\vee R=(P\vee R)\wedge(Q\vee R)$.

可得 $(A\wedge B)\vee C=(A\vee C)\wedge(B\vee C)$.

等等, 其中 A, B, C 是任意谓词公式.

2．量词否定型等价式

$\neg\forall xA(x) = \exists x\neg A(x)$.

$\neg\exists xA(x) = \forall x\neg A(x)$.

从直观上看，$\neg\forall xA(x)$是说“并非所有 x 都使 $A(x)$为真”，而$\exists x\neg A(x)$是说“存在一个 x 使 $A(x)$为假”，这二者应该是相同的，同样可以作出第二个等价式的直观说明.

下面我们运用定义，给出解释性的证明.

任取一个解释 I 及赋值 v，设在此解释及赋值下，$\neg\forall xA(x)$为 1，即 $\neg\forall xA(x)^{I,v}=1$，

则 $\forall xA(x)^{I,v}=0$，即有一个 $a\in D$ 使 $A(a)^{I,v}=0$，于是 $\neg A(a)^{I,v}=1$，故 $\exists x\neg A(x)^{I,v}=1$.

反之，任取一个解释 I 和赋值 v，设在此解释和赋值下 $\exists x\neg A(x)$的真值为 1，即 $\exists x\neg A(x)^{I,v}=1$，则有 $a\in D$ 使 $\neg A(a)^{I,v}=1$，从而 $A(a)^{I,v}=0$，于是$\forall xA(x)^{I,v}=0$，即 $\neg\forall xA(x)^{I,v}=1$.

同理可证第二式. ▌

3. 量词分配等价式.

(1) $\forall x(A(x)\vee B)=\forall xA(x)\vee B.$

$\exists x(A(x)\vee B)=\exists xA(x)\vee B.$

$\forall x(A(x)\wedge B)=\forall xA(x)\wedge B.$

$\exists x(A(x)\wedge B)=\exists xA(x)\wedge B.$

其中，B 不含自由变元 x.

我们仅对第一个等式给出证明，其余三式同理可证.

设在解释 I 和赋值 v 下，$\forall x(A(x)\vee B)$的真值为 1，则对任一 $x\in D$，$A(x)\vee B$ 的真值为 1. 若 B 的真值为 1，则 $\forall xA(x)\vee B$ 的真值为 1；若 B 的真值为 0，则因 B 中不含自由变元 x, 故对任一 $x\in D$，$A(x)$的真值为 1，即有 $\forall xA(x)$ 的真值为 1，故 $\forall xA(x)\vee B$ 的真值为 1. 因而，若在解释 I 和赋值 v 下，$\forall x(A(x)\vee B)$的真值为 1，$\forall xA(x)\vee B$ 的真值必为 1.

反之，设在解释 I 和赋值 v 下，$\forall xA(x)\vee B$ 的真值为 1，若 B 的真值为 1，则 $\forall x(A(x)\vee B)$ 的真值为 1，若 B 的真值为 0，则 $\forall xA(x)$ 的真值为 1，从而对任一 $x\in D$，$A(x)$的真值为 1，于是对任一 $x\in D$，$A(x)\vee B$ 的真值为 1，故 $\forall x(A(x)\vee B)$的真值为 1. 因而，若在解释 I 和赋值 v 下，$\forall xA(x)\vee B$ 的真值为 1，$\forall x(A(x)\vee B)$的真值必为 1. ▌

（2） $\forall x(A(x)\wedge B(x))=\forall xA(x)\wedge\forall xB(x).$

$\exists x(A(x)\vee B(x))=\exists xA(x)\vee\exists xB(x).$

$\forall x\forall y(A(x)\vee B(y))=\forall xA(x)\vee\forall xB(x).$

$\exists x\exists y(A(x)\wedge B(y))=\exists xA(x)\wedge\exists xB(x).$

后两式需要限定 $A(x)$中无自由变元 y，$B(y)$中无自由变元 x.

前两式可用定义给出解释性证明，后两式可用换名规则及前面的结论证明，比如，证明第三式：

由于 $B(y)$ 中无自由变元 x，$A(x)$ 中无自由变元 y，故由第(1)组量词分配等价式，得

$$\begin{aligned}\forall x\forall y(A(x)\vee B(y)) &= \forall x(A(x)\vee\forall yB(y))\\ &= \forall xA(x)\vee\forall yB(y)\\ &=\forall xA(x)\vee\forall xB(x).\end{aligned}$$

从而得知第三式成立. ▌

以上述 3 组等价式为基础，下面来讨论谓词公式的范式.

定义 2　形如

$$Q_1x_1Q_2x_2\cdots Q_nx_nM$$

的公式称为前束范式，其中 Q_ix_i（$1\leqslant i\leqslant n$）是 $\forall x_i$ 或 $\exists x_i$，称为首标，M 中不含任何量词，称为母式．如果将 M 中的原子公式及其否定视为文字，当 M 是析取范式时，上述公式称为前束析取范式；当 M 是合取范式时，上述公式称为前束合取范式.

例如，$\exists x\exists y\forall z\neg(P(x，y)\rightarrow Q(x，z))$，$\forall x\exists y\forall z(P(x，y)\vee(\neg Q(z)\wedge R(y,z)))$，$\forall x\exists y\forall z(P(x，y)\wedge(\neg Q(z)\vee R(y,z)))$都是前束范式，且第二、三式分别是前束析取范式和前束合取范式.

定理 1　对任意谓词公式 A，都存在与其等价的前束范式.

证明　通过如下步骤，可将 A 化为前束范式.

（1）　使用等价式

$A\leftrightarrow B=(A\rightarrow B)\wedge(B\rightarrow A)$，　$A\rightarrow B=\neg A\vee B$

去除→与↔，

（2）　使用 Morgan 律和双重否定律及量词否定型等价式，将 ¬ 放在原子公式之前.

（3）　利用量词分配等价式，将所有量词提到公式前面(必要时换名).　▌

例 1　求公式　$A=\neg(\forall x\exists yP(a，x，y)\rightarrow\exists x(\neg\forall yQ(y，b)\rightarrow R(x)))$　的前束范式.

$$\begin{aligned}
A&=\neg(\forall x\exists yP(a，x，y)\rightarrow\exists x(\neg\forall yQ(y，b)\rightarrow R(x)))\\
&=\neg(\neg\forall x\exists yP(a，x，y)\vee\exists x(\neg\neg\forall yQ(y，b)\vee R(x)))　　（消去\rightarrow）\\
&=\forall x\exists yP(a，x，y)\wedge\neg\exists x(\forall yQ(y，b)\vee R(x))　　（\neg内移）\\
&=\forall x\exists yP(a，x，y)\wedge\forall x(\exists y\neg Q(y，b)\wedge\neg R(x))\\
&=\forall x(\exists yP(a，x，y)\wedge\exists y\neg Q(y，b)\wedge\neg R(x))　　（量词前移）\\
&=\forall x(\exists yP(A，x，y)\wedge\exists z\neg Q(z，b)\wedge\neg R(x))\\
&=\forall x\exists y\exists z(P(a，x，y)\wedge\neg Q(z，b)\wedge\neg R(x))
\end{aligned}$$

如果进一步要求前束范式中的存在量词都在全称量词之前，或是只保留全称量词而消去存在量词，便得到所谓 Skolem 范式，我们在此只介绍第二种类型的 Skolem 范式.

设 A 是一个公式，首先将其化为前束范式

$$Q_1x_1Q_2x_2\cdots Q_nx_nM$$

若 Q_r 是存在量词，并且它左边没有全称量词，则取异于出现在 M 中所有常量符号的新常量符号 c，并用 c 代替 M 中所有 x_r，删除首标中的 Q_rx_r．这里，c 称为 Skolem 常数.

若存在量词 Q_r 左边有全称量词，设 Q_{i_1}，Q_{i_2}，…，Q_{i_m} 是出现在 Q_rx_r 左边的所有全称量词，则取异于出现在 M 中所有函数符号的 m 元函数符号 $f(x_{i_1}，x_{i_2}，\cdots，x_{i_m})$，用其代替 M 中的 x_r，并删除首标的 Q_rx_r．这里，f 称为 Skolem 函数.

若将常量视为 0 元函数，以上两种情况是一致的，以后我们总是采取这样的观点.

对公式 A 做上述处理后，得到一个首标中没有存在量词的前束范式，这个前束范式就称为 A 的 Skolem 范式.

例 2　设 $A=\exists x\forall y\forall z\exists u\forall v\exists w P(x, y, z, u, v, w)$

用常量符号 a 代替 x，删除$\exists x$.

用 $f(y, z)$代替 u，删除 $\exists u$.

用 $g(y, z, v)$代替 w，删除$\exists w$.

得到 A 的 Skolem 范式:　$\forall y\forall z\forall v\, P(a, y, z, f(y, z), v, g(y, z, v))$.

显然，公式 A 的 Skolem 范式未必与 A 等价. 比如，考虑公式 $\exists x P(x)$, 其 Skolem 范式为 $P(a)$.

给定解释 I：

论域 $D=\{1, 2, 3, 4\}$;　$a=4$;　$P(x)$:　x 是素数.

则　　$\exists x P(x)^I=1$,　　$P(a)^I=0$.

故　　$\exists x P(x)\neq P(a)$.

定理 2　公式 A 永假当且仅当其 Skolem 范式永假.

证明　设公式 G 是公式 A 的 Skolem 范式，需要证明 A 永假当且仅当 G 永假. 由于任何谓词公式都有与其等价的前束范式，不妨设我们已经把 A 化成了前束范式. 并令

$$A=Q_1x_1Q_2x_2\cdots Q_nx_nM(x_1, x_2, \cdots, x_n)$$

设 Q_k 是 A 中从左往右数的第一个存在量词，即

$$A=\forall x_1\forall x_2\cdots\forall x_{k-1}\exists x_k\cdots Q_nx_nM(x_1, x_2, \cdots, x_n)$$

令　　$A'=\forall x_1\forall x_2\cdots\forall x_{k-1}Q_{k+1}x_{k+1}\cdots Q_nx_n\, M(x_1, x_2, \cdots, x_{k-1}, f(x_1, x_2, \cdots x_{k-1}), x_{k+1}, \cdots, x_n)$

其中，f 是 Skolem 函数.　即 A' 是对 A 化 Skolem 范式时，消去存在量词 Q_kx_k 所得到的公式. 我们先证明，A 是永假式 当且仅当 A' 是永假式.

如若不然，设 A 是永假式，而 A' 是可满足的，则存在解释 I 和赋值 v，使 A' 为真，则对论域 D 中任意的元素 $x_1^0, x_2^0\cdots, x_{k-1}^0$ ，

$$Q_{k+1}x_{k+1}\cdots Q_nx_n\, M(x_1^0, x_2^0\cdots, x_{k-1}^0, f(x_1^0, x_2^0\cdots, x_{k-1}^0), x_{k+1}, \cdots, x_n)^{I,v}=1.$$

因而，对论域 D 中任意的元素 $x_1^0, x_2^0\cdots, x_{k-1}^0$ ，取 $x_k^0=f(x_1^0, x_2^0\cdots, x_{k-1}^0)\in D$，有

$$Q_{k+1}x_{k+1}\cdots Q_nx_n\, M(x_1^0, x_2^0\cdots, x_{k-1}^0, x_k^0, x_{k+1}, \cdots, x_n)^{I,v}=1.$$

即　　$A^{I,v}=\forall x_1\forall x_2\cdots\forall x_{k-1}\exists x_k\cdots Q_nx_nM(x_1, x_2, \cdots, x_n)^{I,v}=1.$

这与 A 永假矛盾.

反之，如果 A' 永假，而 A 可满足，则存在解释 I 和赋值 v，使 A 为真，则对 D中任

意的元素 $x_1^0, x_2^0 \cdots, x_{k-1}^0$，存在 $x_k^0 \in D$，使得

$$Q_{k+1}x_{k+1}\cdots Q_n x_n\, M(x_1^0, x_2^0 \cdots, x_{k-1}^0,\ x_k^0, x_{k+1}, \cdots, x_n)^{I,v} = 1.$$

构造函数：$f^0: D^{k-1} \to D$, 对任意 $x_1^0, x_2^0 \cdots, x_{k-1}^0 \in D$, 任意取定一个满足上式的 x_k^0 作为 $f^0(x_1^0, x_2^0 \cdots, x_{k-1}^0)$. 在解释 I 的基础上，指定 A' 中的函数符号 f 为 f^0, 则得到 A' 的解释 I', 且在此解释下，对任意 $x_1^0, x_2^0 \cdots, x_{k-1}^0 \in D$

$$Q_{k+1}x_{k+1}\cdots Q_n x_n\, M(x_1^0, x_2^0 \cdots, x_{k-1}^0, f(x_1^0, x_2^0 \cdots, x_{k-1}^0), x_{k+1}, \cdots, x_n)^{I',v} = 1.$$

即

$$(A')^{I',v} = \forall x_1 \forall x_2 \cdots \forall x_{k-1} Q_{k+1}x_{k+1}\cdots Q_n x_n\, M(x_1, x_2, \cdots, x_{k-1}, f(x_1, x_2, \cdots x_{k-1}), x_{k+1}, \cdots, x_n)^{I',v} = 1.$$

这与 A' 永假矛盾.

现设公式 A 中含有 m 个存在量词($1 \leqslant m \leqslant n$)，并设 A_i 是对 A 化范式时消去第 i 个存在量词得到的公式，则 A_m 即是 G. 由上面的讨论知, A 永假, 当且仅当 A_1 永假 当且仅当 A_2 永假, …，当且仅当 $A_m = G$ 永假. 因此，证明了:

A 永假 当且仅当 G 永假. ▌

习 题 三

1．将下列公式化为前束范式.

（1） $\forall x(P(x) \to \exists y Q(x, y))$.

（2） $\exists x((\neg \exists y P(x, y)) \to (\exists z Q(z) \to R(x)))$.

（3） $\forall x \forall y(\exists z P(x, y, z) \wedge \exists u Q(x, u) \to \exists v Q(y, v))$.

2．求下列公式的 Skolem 范式.

（1） $\neg(\forall x P(x) \to \exists y \forall z Q(y, z))$

（2） $\forall x(\neg E(x, 0) \to \exists y(E(y, g(x)) \wedge \forall z(E(z, g(x)) \to E(y, z))))$.

（3） $\neg(\exists x P(x) \to \forall y P(y))$.

3．证明量词分配分配等价式中第(1)组第二、三式及第(2)组第一、四式.

§ 4 推理理论

定义 1 设 A，B 是两个公式，如果对任意解释 I 及赋值 v，当 A 的真值为 1 时必有

B 的真值为 1，则称 A 蕴涵 B，记为 $A \Rightarrow B$.

显然，$A \Rightarrow B$ 当且仅当 $A \rightarrow B$ 有效.

定理 1 (蕴涵式代入原则)　设 $A = A(P_1, P_2, \cdots, P_n)$，$B = B(P_1, P_2, \cdots, P_n)$ 是两个命题公式，$P_1, P_2, \cdots, P_n$ 是其中出现的所有命题变元，$A \Rightarrow B$;　则对任意一组谓词公式 $A_1, A_2, \cdots, A_n$，若分别用 $A_1, A_2, \cdots, A_n$ 代替 A, B 中的 $P_1, P_2, \cdots, P_n$ 得到公式 A',　B'，即 $A' = A(A_1, A_2, \cdots, A_n)$，$B' = B(A_1, A_2, \cdots, A_n)$，则 $A' \Rightarrow B'$.

利用定义可以证明如下基本推理公式.

1．$\forall x A(x) \vee \forall x B(x) \Rightarrow \forall x(A(x) \vee B(x))$

2．$\exists x(A(x) \wedge B(x)) \Rightarrow \exists x A(x) \wedge \exists x B(x)$

3．$\forall x(A(x) \rightarrow B(x)) \Rightarrow \forall x A(x) \rightarrow \forall x B(x)$

4．$\forall x(A(x) \rightarrow B(x)) \Rightarrow \exists x A(x) \rightarrow \exists x B(x)$

5．$\forall x(A(x) \leftrightarrow B(x)) \Rightarrow \forall x A(x) \leftrightarrow \forall x B(x)$

6．$\forall x(A(x) \leftrightarrow B(x)) \Rightarrow \exists x A(x) \leftrightarrow \exists x B(x)$

7．$\forall x(A(x) \leftrightarrow B(x)) \wedge \forall x(B(x) \rightarrow C(x)) \Rightarrow \forall x(A(x) \rightarrow C(x))$

8．$\forall x(A(x) \rightarrow B(x)) \wedge A(a) \Rightarrow B(a)$

9．$\forall x \forall y A(x, y) \Rightarrow \exists x \forall y A(x, y)$

10．$\exists x \forall y A(x, y) \Rightarrow \forall y \exists x A(x, y)$

为证明这些基本蕴涵式，可以采用解释性证明，现举几例.

公式 2：$\exists x(A(x) \wedge B(x)) \Rightarrow \exists x A(x) \wedge \exists x B(x)$

设在解释 I 和赋值 v 下，$\exists x(A(x) \wedge B(x))$的真值为 1，则有 $a \in D$ 使 $A(a) \wedge B(a)$的真值为 1，从而 $A(a)$的真值为 1，$B(a)$的真值为 1，因此，$\exists x A(x)$的真值为 1，$\exists x B(x)$的真值为 1，于是 $\exists x A(x) \wedge \exists x B(x)$的真值为 1.

公式 3：$\forall x(A(x) \rightarrow B(x)) \Rightarrow \forall x A(x) \rightarrow \forall x B(x)$

设在解释 I 和赋值 v 下，$\forall x(A(x) \rightarrow B(x))$的真值为 1，则对任一 $x \in D$，$A(x) \rightarrow B(x)$的真值为 1. 现在假设$\forall x A(x)$的真值为 1，则对任一 $x \in D$，$A(x)$的真值为 1，因而 $B(x)$的真值为 1，所以$\forall x B(x)$的真值为 1，于是$\forall x A(x) \rightarrow \forall x B(x)$的真值为 1.

公式 10：$\exists x \forall y A(x, y) \Rightarrow \forall y \exists x A(x, y)$

设在解释 I 和赋值 v 下，$\exists x \forall y A(x, y)$的真值为 1，则必有 $a \in D$ 使 $\forall y A(a, y)$的真值为 1，即对每一 $y \in D$，$A(a, y)$ 的真值为 1，从而对每一 $y \in D$，$\exists x A(x, y)$为 1，即 $\forall y \exists x A(x, y)$的真值为 1.

从以上蕴涵式的解释性证明中，我们看到，为证明一个蕴涵式，我们总是先通过解释量词的含义，把量词去掉，进行论证后，再把量词添上，一般地，我们指出如下推理规则.

1．全称量词消去律 (∀-)

$$\frac{\forall xA(x)}{\therefore A(x)} \qquad \frac{\forall xA(x)}{\therefore A(y)} \qquad \frac{\forall xA(x)}{\therefore A(c)}$$

条件：y 不在 $A(x)$中约束出现. c 为固定个体.

2．全称量词引入律 (∀+)

$$\frac{A(x)}{\therefore \forall xA(x)}$$

条件：在任意解释 I 和赋值 v 下，$A(x)^{I,v}$ 的真值与 x 无关.

3．存在量词消去律.

$$\frac{\exists xA(x)}{\therefore A(c)}$$

条件：$\exists xA(x)$中无自由变元，c 是一个固定个体.

4．存在量词引入律

$$\frac{A(c)}{\therefore \exists xA(x)}$$

条件：x 不在 $A(c)$中出现.

利用以上规则及基本蕴涵式、基本等价式，我们便可以象命题逻辑中的演绎法一样进行谓词逻辑的推理了，事实上，命题逻辑中的推理方法及术语均可移植到谓词逻辑中来，命题逻辑的推理可视为谓词逻辑推理的特殊情况.

例 1　前提：$\forall x(P(x)\rightarrow Q(x))$
$\forall x(Q(x)\rightarrow R(x))$
结论：$\forall x(P(x)\rightarrow R(x))$

证明

(1)	$\forall x(P(x)\rightarrow Q(x))$	**P**
(2)	$P(x)\rightarrow Q(x)$	∀- (1)
(3)	$\forall x(Q(x)\rightarrow R(x))$	**P**
(4)	$Q(x)\rightarrow R(x)$	∀- (3)
(5)	$P(x)\rightarrow R(x)$	**C**(2)(4)
(6)	$\forall x(P(x)\rightarrow R(x))$	∀+ (5)

例 2　所有人都会死.
苏格拉底是人.

所以，苏格拉底必会死.

令　$M(x)$：x 是人，

$D(x)$：x 会死.

s：苏格拉底

问题形式描述为：

$\forall x(M(x)\rightarrow D(x))\wedge M(s)\Rightarrow D(s)$

证明

(1)	$\forall x(M(x)\rightarrow D(x))$	**P**
(2)	$M(s)\rightarrow D(s)$	$\forall$- (1)
(3)	$M(s)$	**P**
(4)	$D(s)$	**MP**(2)(3)

例 3　前提　$\exists xP(x)\rightarrow\forall x((P(x)\vee Q(x))\rightarrow R(x))$，　$\exists xP(x)$.

结论　$\exists x\exists y(R(x)\wedge R(y))$

证明

(1)	$\exists xP(x)\rightarrow\forall x((P(x)\vee Q(x))\rightarrow R(x))$	**P**
(2)	$\exists xP(x)$	**P**
(3)	$\forall x((P(x)\vee Q(x))\rightarrow R(x))$	**MP**(1)(2)
(4)	P(c)	$\exists$- (2)
(5)	$P(c)\vee Q(c)\rightarrow R(c)$	$\forall$- (3)
(6)	$P(c)\vee Q(c)$	**C**(4)
(7)	$R(c)$	**MP**(6)(5)
(8)	$\exists xR(x)$	$\exists$+ (7)
(9)	$\exists yR(y)$	$\exists$+ (7)
(10)	$\exists xR(x)\wedge\exists yR(y)$	**C**(8)(9)
(11)	$\exists x\exists y(R(x)\wedge R(y))$	**C**(10)

例 4 证明　$\exists xA(x)\rightarrow\forall xB(x)\Rightarrow\forall x(A(x)\rightarrow B(x))$

证明　只需要证明 $\exists xA(x)\rightarrow\forall xB(x)$ ，　$\neg\forall x(A(x)\rightarrow B(x))$　不相容.

(1)	$\neg\forall x(A(x)\rightarrow B(x))$	**P**
(2)	$\exists x\neg(A(x)\rightarrow B(x))$	**C**(1)
(3)	$\neg(A(a)\rightarrow B(a))$	$\exists$- (2)
(4)	$\neg(\neg A(a)\vee B(a))$	**C**(3)
(5)	$A(a)\wedge\neg B(a)$	**C**(4)
(6)	$A(a)$	**C**(5)
(7)	$\neg B(a)$	**C**(5)
(8)	$\exists x$A(x)	**C**(7)

(9)	$\exists xA(x)\rightarrow \forall xB(x)$	**P**
(10)	$\forall xB(x)$	MP(8)(9)
(11)	$B(a)$	$\forall$- (10)
(12)	$B(a)\wedge\neg B(a)$	**C**(11)(7)

例 5 证明 $\forall x(P(x)\vee Q(x))\Rightarrow \forall xP(x)\vee\exists xQ(x)$

证明 因为 $\forall xP(x)\vee\exists xQ(x)=\neg\forall xP(x)\rightarrow\exists xQ(x)$

故只需证明 $\forall x(P(x)\vee Q(x))\Rightarrow\neg\forall xP(x)\rightarrow\exists xQ(x)$

由 CP 规则，只需证明 $\forall x(P(x)\vee Q(x))$，$\neg\forall xP(x)\Rightarrow\exists xQ(x)$

(1)	$\neg\forall x\mathrm{P}(x)$	**P**
(2)	$\exists x\neg P(x)$	**C**(1)
(3)	$\neg P(c)$	$\exists$- (2)
(4)	$\forall x(P(x)\vee Q(x))$	**P**
(5)	$P(c)\vee Q(c)$	$\forall$- (4)
(6)	$Q(c)$	**C**(3)(5)
(7)	$\exists xQ(x)$	$\exists$+ (6)

习 题 四

1. 证明下列各式.

(1) $\forall x(\neg A(x)\rightarrow B(x))$，$\forall x\neg B(x)\Rightarrow\exists xA(x)$

(2) $\exists xA(x)\rightarrow\forall xB(x)\Rightarrow\ \forall x(A(x)\rightarrow B(x))$

(3) $\forall x(A(x)\rightarrow B(x))$，$\forall x(C(x)\rightarrow\neg B(x))\ \Rightarrow\ \forall x(C(x)\rightarrow\neg A(x))$

(4) $\forall x(A(x)\vee B(x))$，$\forall x(B(x)\rightarrow\neg C(x))$，$\forall xC(x)\ \Rightarrow\ \forall xA(x)$

2．符号化并证明下列论断.

(1) 所有有理数是实数，某些有理数是整数，因此某些实数是整数.

(2) 任何人如果他喜欢步行，他就不喜欢乘车，每一个人或者喜欢乘车或者喜欢骑自行车，有的人不爱骑自行车，因而有的人不爱步行.

3．证明 $\forall x(P(x)\vee Q(x))$，$\neg\exists xQ(x)\Rightarrow\forall xP(x)$.