Contents

第 1 章 集合

集合是数学中最基本的概念,它已深入到各种科学和技术领域中,特别是应用于数学的各个分支中,本章的内容是在高中数学课所介绍的基础上略有提高,引入了幂集、积集概念以及计算机科学中常用的集合的归纳定义.

1.1 集合的基本概念

1.1.1 集合

集合是一些对象的总体.总体中的对象称之为集合的元素或成员.给定任意一个对象x以及集合S,如果x是集合S的一个元素,我们将写成$x \in S$.如果x不是集合S的一个元素则写成$x \notin S$.

习惯上称之为集合的事物,通常在数学上是可以接受的.例如:

1° “小于4的非负整数集合”是由四个元素组成的集合.这四个元素分别是$0, 1, 2, 3$;

2° “全体活着的中国人”是个集合.集合中元素的个数很多,但是有限的.由于生死的变化,要列出这个集合的成员是困难的.这种困难是实践上的,不是理论上的;

3° “大于等于3的整数集合”是个有无限多个元素的集合.要判断一个整数是否是它的元素很容易;

4° “在具有无限存贮量的计算机上,运行足够长的时间之后能停止运行的所有Algol 60程序组成了一个无限集合”.但计算理论已经证明,判断任意程序是否是这个集合的元素的算法是不存在的.从而这个集合是不可判定的;

5° “全体大于0,小于1的整数集合”.在这个集合中没有任何元素,我们称它为空集,并记为$\varnothing$.

集合是以它的元素来表征的.一个有有限多个元素的集合可以用列出它的全部元素的方法来说明.这些元素用大括号括起来,并且元素之间用逗号分开.一般集合用大写字母表示,集合元素用小写字母表示.当集合A中有有限多个元素时,用$|A|$表示集合中的元素个数.特别对于空集$\varnothing$, $|\varnothing| = 0$.例如:

1° $A = \{a, b, c\}$, a, b, c是集合A的元素, $|A| = 3$;

2° $B=\{0,2,4,6,8\}$,B是小于10的非负偶数集合.$|B|=5$.

集合,特别是有无限多个元素的集合,通常用指出集合中元素性质的方法来说明.例如,记$\mathbf{Z}$是全体整数集合.

1° 全体偶数集合为$\{x \mid \exists y \in \mathbf{Z}, x=2y\}$;

2° 大于10的整数集合$\{x \mid x \in \mathbf{Z}$且$x>10\}$;

3° 有理数集合$\mathbf{Q}=\{x/y \mid x,y \in \mathbf{Z}$且$y \neq 0\}$.

1.1.2 集合的相等

同一个集合可以有不同的表示法.例如,$A=\{-1,1\}$,$B=\{\, x \mid x \in \mathbf{Z}, x^2=1\,\}$,$C=\{\, x \mid x \in \mathbf{R}, |x|=1\,\}$,其中$\mathbf{R}$表示全体实数集合.这就产生了一个问题,即如何判断两个集合是同一个集合.

定义 1.1. 给定两个集合A和B,如果集合A中的每个元素都是集合B中的元素,反过来集合B中的每个元素也都是集合A中的元素,那么称集合A和集合B**相等**,并记为$A=B$.

用这个定义可直接验证上面的集合A,B,C是相等的集合,$A=B=C$.

定理 1.1. *A,B,C是任意集合,集合间的相等关系满足:*

1° **自反性** $A=A$;

2° **对称性** 若$A=B$,则$B=A$;

3° **传递性** 若$A=B,B=C$,则$A=C$.

证明 在定义1.1中,将B改成A以后显然成立,它说明$A=A$.又在定义1.1 中, 先说后一句话,再说前一句话,也就是说集合B的每个元素都是集合A中的元素,反过来集合A的每个元素也都是集合B中的元素,其意思与原来完全相同,所以当$A=B$时,必有$B=A$.

下面证明传递性.已知$A=B$,对于任何$x \in A$,必有$x \in B$.又由$B=C$,从$x \in B$推出$x \in C$.反过来,由$A=B,B=C$及相等关系的对称性推出$B=A,C=B$.对于任何$x \in C$,由于$C=B$,必有$x \in B$.又由$B=A$,从$x \in B$推出$x \in A$.对照定义1.1知$A=C$.

1.1.3 集合的包含

集合的相等与包含是集合间的两种最基本的关系.现在定义两个集合的包含关系.

定义 1.2. A和B是两个集合.如果集合A中的每个元素都是集合B中的元素,我们称集合B包含集合A,而集合A叫做集合B的一个**子集**,表示成$B \supseteq A$或$A \subseteq B$.

如果集合B包含集合A,并且至少一个元素属于集合B而不属于集合A,我们称集合B真包含集合A,而集合A叫做集合B的一个**真子集**.

例如,偶数集合是整数集合的真子集.集合$\{1,2,3,4\}$是集合$\{x \mid x \in \mathbf{Z}$且$0 < x < 5\}$的子集,但不是真子集.

定理 1.2. A,B,C是任意集合,集合间的包含关系满足:

1° **自反性** $A \subseteq A$;

2° **反对称性** 若$A \subseteq B$且$B \subseteq A$,则$A = B$;

3° **传递性** 若$A \subseteq B$且$B \subseteq C$,则$A \subseteq C$.

证明 1°,3°的证明留作习题.这里只证2°.

若$A \subseteq B$且$B \subseteq A$,由集合包含的定义知集合A中的每个元素都是集合B中的元素,并且集合B中的每个元素都是集合A中的元素.这正是集合A和集合B相等的定义,从而得出$A = B$.

定理 1.3. 对于任何集合$A, \varnothing \subseteq A$.

证明 用反证法.假设空集$\varnothing$不是某个集合A的子集,那么至少有一个元素$x, x \in \varnothing$且$x \notin A$.而$\varnothing$是空集,它没有任何元素,即对任何x必有$x \notin \varnothing$.产生矛盾.故不可能.由此得出$\varnothing$是任何集合A的子集.

由定理1.3知,空集$\varnothing$是唯一的.这是因为假若$\varnothing_1$和$\varnothing_2$都是空集.因为$\varnothing_1$是空集,得出$\varnothing_1 \subseteq \varnothing_2$.因为$\varnothing_2$是空集,得$\varnothing_2 \subseteq \varnothing_1$.由集合包含关系的反对称性知$\varnothing_1 = \varnothing_2$.

在研究一个特定问题时,假设有一个足够大的集合使一切集合都包含在它之中.这个足够大的集合称之为万有集合,并记为U.对于任何集合A均有$A \subseteq U$.

1.1.4 幂集

$A, B, \cdots$是集合,把它们放在一起构成一个新的集合$\{A, B, \cdots\}$.这种集合以集合作为元素称为集族.集族通常用花写字母$\mathscr{A}, \mathscr{B}, \cdots$表示.

一个集合的全部子集构成的集族叫做该集合的幂集.若$A = \{a, b, c\}$, A的幕集$\mathscr{P}(A)$是有8个元素的集族:

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

定理 1.4. A是有限集合,$|\mathscr{P}(A)| = 2^{|A|}$.

证明 A是有限集合,$|A| = n$.A的i元子集的个数就是从n个元素中选取i个不同元素的方法$C_n^i \left(= \frac{n!}{i!(n-i)!}\right)$,这里$i$可以取$0, 1, \cdots, n$这$n+1$个值.故有

$$|\mathscr{P}(A)| = C_n^0 + C_n^1 + \cdots + C_n^n$$

在二项式定理

$$(x+y)^n = C_n^0 x^n y^0 + C_n^1 x^{n-1} y + \cdots + C_n^n x^0 y^n$$

中,令$x = y = 1$,于是有$2^n = C_n^0 + C_n^1 + \cdots + C_n^n$.从而$|\mathscr{P}(A)| = 2^n = 2^{|A|}$.

1.1.5 积集

定义 1.3. 对于正整数n,有序n元组$(a_1, a_2, \cdots, a_n)$是a_i为第i个分量的n个对象的**序列**.

两个有序n元组是相等的,当且仅当它们的每个分量都是相等的.

定义 1.4. n个集合$A_1, A_2, \cdots, A_n$的**积集**$A_1 \times A_2 \times \cdots \times A_n$是由全体有序$n$元组$(a_1, a_2, \cdots, a_n)$构成的集合,其中$a_i \in A_i, 1 \leqslant i \leqslant n$.

特别地,若$A_1 = A_2 = \cdots = A_n = A$时,记$A_1 \times A_2 \times \cdots \times A_n$为$A^n$.

例如,$A = \{1, 2\}, B = \{m, n\}, C = \{0\}, D = \varnothing$,那么

$A \times B = \{(1, m), (1, n), (2, m), (2, n)\}$,

$A \times C = \{(1, 0), (2, 0)\}, C \times A = \{(0, 1), (0, 2)\}, A \times D = \varnothing$. 注意,这里$A \times C \neq C \times A$.

定理 1.5. A, B是两个有限集合,$|A \times B| = |A| \cdot |B|$.

证明 从集合A中任取一个元素a作为第一分量,从集合B中任取一个元素b作为第二分量构成的有序2元组(a, b)是$A \times B$的一个元素.a与b的不同取法构成不同的有序2元组.从集合A中选取一个元素有$|A|$种方法,从集合B中选取一个元素有$|B|$种方法.它们可以构成$|A| \cdot |B|$个不同的2元组.于是$|A \times B| = |A| \cdot |B|$.

同理可以证明$|A_1 \times A_2 \times \cdots \times A_n| = |A_1| \cdot |A_2| \cdot \cdots \cdot |A_n|$.

1.2 集合的运算

我们在前一节谈到集合间的一些联系,如包含、子集等,各种不同集合的进一步联系是通过集合上的各种运算显示出来的.

定义 1.5. 集合A与B的**并,交,差**集$A \cup B, A \cap B, A - B$分别为

$$A \cup B = \{x \mid x \in A \text{或} x \in B\},$$
$$A \cap B = \{x \mid x \in A \text{且} x \in B\},$$
$$A - B = \{x \mid x \in A \text{且} x \notin B\}.$$

由定义看出$A \cup B$是由或是在集合A中,或是在集合B中的元素组成的.$A \cap B$是由集合A和集合B的公共元素组成的.$A - B$是由在集合A中但不在集合B中的元素组成的.若取A为万有集合$U, U - B$称为集合B的补集,并记为$\bar{B}$.不难看出

$$\bar{B} = \{x \mid x \in U \text{ 且} x \notin B\} = \{x \mid x \notin B\}.$$

例如,$A = \{0, 1, 2\}, B = \{1, 2, 3\}, U = \{x \mid x \in \mathbf{Z} \text{ 且} x \geqslant 0\}$.

$$A \cup B = \{0, 1, 2, 3\},$$
$$A \cap B = \{1, 2\},$$
$$A - B = \{0\}, \quad B - A = \{3\},$$
$$\bar{A} = U - A = \{x \mid x \in \mathbf{Z} \text{且} x \geqslant 3\}.$$

定理 1.6. 对于任意集合$A, A \cup \bar{A} = U, A \cap \bar{A} = \varnothing$.

证明 由并与交运算的定义

$$A \cup \bar{A} = \{x \mid x \in A或x \in \bar{A}\} = \{x \mid x \in A或x \notin A\} = U.$$
$$A \cap \bar{A} = \{x \mid x \in A且x \in \bar{A}\} = \{x \mid x \in A且x \notin A\} = \varnothing.$$

例 1.1. 证明$\bar{A} \subseteq \bar{B}$当且仅当$B \subseteq A$.

证明 用反证法证明必要性.假设$B \subseteq A$不成立,那么至少存在一个元素$x_0 \in B$且$x_0 \notin A$,从而$x_0 \in \bar{A}$.另一方面$x_0 \in B$, 故$x_0 \notin \bar{B}$.这就是说,至少存在一个元素x_0,使$x_0 \in \bar{A}$且$x_0 \notin \bar{B}$,与$\bar{A} \subseteq \bar{B}$相矛盾,故不可.于是仅当$B \subseteq A$时有$\bar{A} \subseteq \bar{B}$.

可用类似的方法证明充分性.

例 1.2. 证明$\overline{A \cap B} = \bar{A} \cup \bar{B}$.

证明 证明的思路是先证明$\overline{A \cap B} \subseteq \bar{A} \cup \bar{B}$,再证明$\bar{A} \cup \bar{B} \subseteq \overline{A \cap B}$,利用集合间包含关系的反对称性得到$\overline{A \cap B} = \bar{A} \cup \bar{B}$.

下面我们先证$\overline{A \cap B} \subseteq \bar{A} \cup \bar{B}$.

任取$x \in \overline{A \cap B}$,由补运算的定义知$x \notin A \cap B$,即$x \in A$与$x \in B$不能同时成立.由此得出$x \notin A$或$x \notin B$.再由集合并运算的定义知$x \in \bar{A} \cup \bar{B}$,这里$x$是$\overline{A \cap B}$的任意元素,故$\overline{A \cap B} \subseteq \bar{A} \cup \bar{B}$.

再证$\bar{A} \cup \bar{B} \subseteq \overline{A \cap B}$.

任取$x \in \bar{A} \cup \bar{B}$,由并运算的定义知$x \in \bar{A}$或$x \in \bar{B}$.因$A \cap B \subseteq A$,从上例知$\bar{A} \subseteq \overline{A \cap B}$.当$x \in \bar{A}$时,必有$x \in \overline{A \cap B}$.同样因$A \cap B \subseteq B$,从上例知$\bar{B} \subseteq \overline{A \cap B}$. 当$x \in \bar{B}$时,必有$x \in \overline{|A \cap B|}$.综上分析知$\bar{A} \cup \bar{B}$的每个元素都是$\overline{A \cap B}$的元素, 即$\bar{A} \cup \bar{B} \subseteq \overline{A \cap B}$.

定理 1.7. 对任意集合A, B, C下面等式成立:

1° $A \cup B = B \cup A, A \cap B = B \cap A;$

2° $A \cup (B \cup C) = (A \cup B) \cup C, A \cap (B \cap C) = (A \cap B) \cap C;$

3° $A \cup (B \cap C) = (A \cup B) \cap (A \cup C),$
$A \cap (B \cup C) = (A \cap B) \cup (A \cap C);$

4° $A \cup \varnothing = A, A \cap U = A;$

5° $A \cup \bar{A} = U, A \cap \bar{A} = \varnothing.$

证明 5°已在定理1.6中证明.其余的均可由集合并、交运算的定义直接证明.

定理 1.8. 下面三个关于集合A和B的命题是相互等价的*:*

1° $A \subseteq B$*;*

2° $A \cup B = B$*;*

3° $A \cap B = A$.

证明 我们的证明方法是通过证明1° $\Longrightarrow$ 2° $\Longrightarrow$ 3° $\Longrightarrow$ 1°来说明它们是等价的.

首先证明1° $\Longrightarrow$ 2°.

已知$A \subseteq B$, A的每个元素都是B中的元素,从集合并运算的定义知

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

再证明2° $\Longrightarrow$ 3°.

已知$A \cup B = B$,等式两边同时与A求交仍然相等.然后再定理1.7中的诸性质

$$\begin{aligned}
A \cap B &= A \cap (A \cup B) \\
&= (A \cup \varnothing) \cap (A \cup B) && 4° \\
&= A \cup (\varnothing \cap B) && 3° \\
&= A \cup ((\varnothing \cap B) \cap \varnothing) && 4° \\
&= A \cup ((B \cap \varnothing) \cup (B \cap \bar{B})) && 1°, 5° \\
&= A \cup (B \cap (\varnothing \cup \bar{B})) && 3° \\
&= A \cup (B \cap \bar{B}) && 1°, 4° \\
&= A \cup \varnothing && 5° \\
&= A. && 4°
\end{aligned}$$

最后证明3° $\Longrightarrow$ 1°.

已知$A \cap B = A$,任取$x \in A \cap B$,由集合交运算的定义知$x \in A$且$x \in B$,特别注意到$x \in B$,由x的任意性,得到$A \cap B \subseteq B$.将$A \cap B = A$代入即是所求的结果$A \subseteq B$.

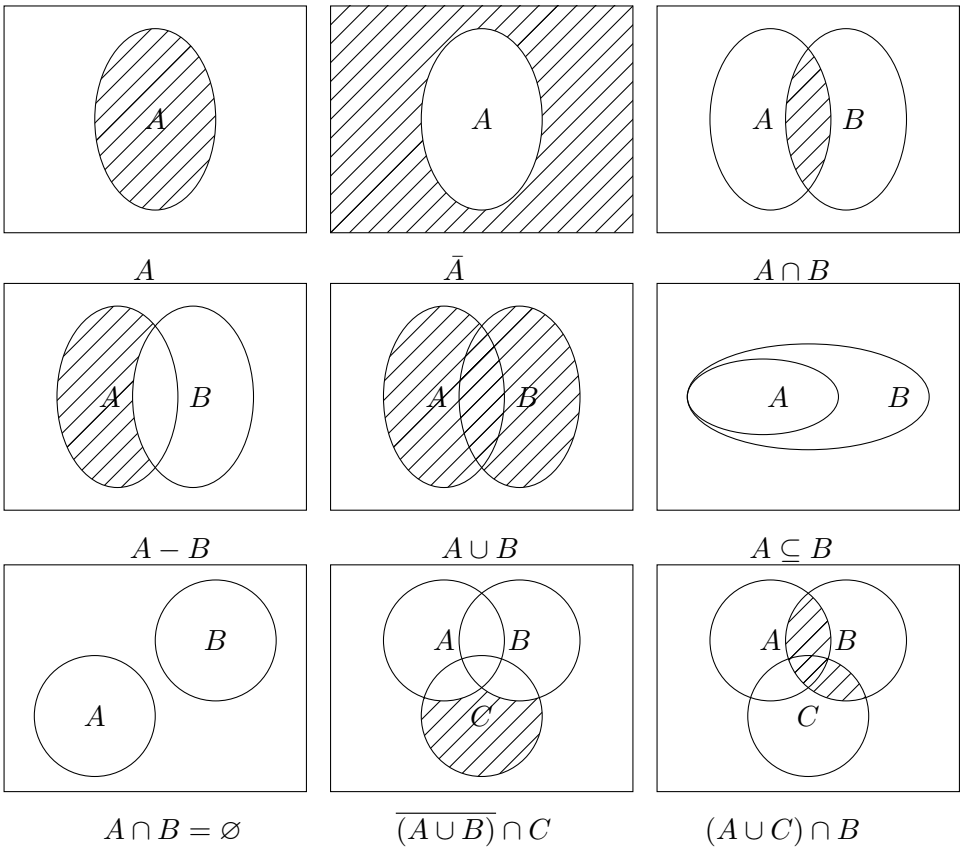


图 1.1: Venn图

对集合的运算可以用Venn图直观地表示.在图1.1中用矩形表示万有集合U,圆表示集合A, B, C.

1.3 集合的归纳定义

前面谈到有限集合可以用列出集合元素的方法,也可用刻画集合元素性质的方法来表述.但是用集合元素来定义集合,特别是无限集合,不总是很方便的.例如pascal程序集合、自然数集合等.对这样的集合通常自然地采用归纳定义.

集合的归纳定义是由基础语句,归纳语句和终结语句三个部分组成的.

先看个例子.非负偶整数集合E可以定义为

$$E = \{x \mid x \in \mathbf{Z}, x \geqslant 0 \text{ 且}\exists y \in \mathbf{Z}, \text{使} x = 2y\}.$$

它也可以归纳定义如下:

1° (基础语句)$0 \in E$;

2° (归纳语句)如果$n \in E$,则$n+2 \in E$;

3° (终结语句)除了有限多次使用$1^\circ, 2^\circ$产生的整数之外再也没有其他元素属于E.

在这个例子中,我们可以看出: 基础语句为该集合提供了基本建筑块.这些基本块应该尽可能地少.归纳语句指出如何从集合已有元素构造出其他元素.构造方法要简单可行.终结语句表述构造方法的完备性,即除掉基础语句给出的元素外,集合的每个元素都能用归纳语句提供的方法构造出来,并且该集合的全体元素就是有限次使用基础语句和归纳语句所得到的全部元素.

在计算机科学中符号行起着重要作用,在行文编辑程序、处理代数公式程序以及定理证明程序中,对符号行的运算是核心.字母表是由有限多个符号组成的集合,记为Σ.从Σ中选取有限个符号排成一行称为字母表Σ上的一个行.令$\Sigma = \{a_1, a_2, \cdots, a_n\}$,$x = a_{i_1}a_{i_2}\cdots a_{i_k}$.其中$a_{i_1}, a_{i_2}, \cdots, a_{i_k} \in \Sigma$,那么称$x$是$\Sigma$上长为$k$的行.特别地,称长为0的行为空行,记作$\lambda$.现有$\Sigma$上的两个行$x = a_{i_1}a_{i_2}\cdots a_{i_k}$,$y = b_{j_1}b_{j_2}\cdots b_{j_l}$,其中$a_{i_1}, a_{i_2}, \cdots, a_{i_k}, b_{j_1}, b_{j_2}, \cdots, b_{j_l} \in \Sigma$.行$x$与行$y$的连接是行$xy$:

$$xy = a_{i_1}a_{i_2}\cdots a_{i_k}b_{j_1}b_{j_2}\cdots b_{j_l},$$

它是Σ上长为$k+l$的行.一般地,行的连接运算不满足交换律.

特别地,$x\lambda = \lambda x = x$,即任何行与空行相连接,则保持不变.

下面归纳定义两个常用的集合Σ^+和Σ^*.

定义 1.6. 字母表Σ上所有非空行的集合Σ^+定义如下*:*

1° (基础语句)如果$a \in \Sigma$,则$a \in \Sigma^+$*;*

2° (归纳语句)如果$x \in \Sigma^+$且$a \in \Sigma$,则a与行x的连接$ax \in \Sigma^+$*;*

3° (终结语句)集合Σ^+只包含有限次使用$1^\circ, 2^\circ$所得到的那些行.

集合Σ^+包括长为$1, 2, \cdots$的行,它是一个无限集合.特别要指出的是,在Σ^+中的每一个元素都是由有限多个符号组成的行.

例如$\Sigma=\{a,b\}$,那么

$$\Sigma^{+}=\{a,b,aa,ab,ba,bb,aaa,aab,\cdots\}.$$

定义 1.7. Σ是字母表,Σ上所有行的集合Σ^{*}定义如下:

1° (基础语句)空行$\lambda\in\Sigma^{*}$;

2° (归纳语句)如果$x\in\Sigma^{*}$且$a\in\Sigma$,则a与行x的连接$ax\in\Sigma^{*}$;

3° (终结语句)除了有限次使用$1^{\circ},2^{\circ}$构造的行以外,Σ^{*}再没有其他元素.

例如$\Sigma=\{a,b\}$,那么

$$\Sigma^{*}=\{\lambda,a,b,aa,ab,ba,bb,aaa,aab,\cdots\}=\{\lambda\}\cup\Sigma^{+}.$$

例 1.3. 用归纳方法定义仅由整数,一元运算符$+,-$,二元运算符$+,-,*,/$及括号组成的算术表达式集合.

1° (基础语句)令$\mathbf{D}=\{0,1,2,\cdots,9\}$,若$x\in\mathbf{D}^{+}$,则$x$是算术表达式;

2° (归纳语句) 如果x和y是算术表达式,则$(-x),(+x),(x+y),(x-y),(x*y),(x/y)$是算术表达式;

3° (终结语句)一个符号行是算术表达式,当且仅当它是有限次使用$1^{\circ},2^{\circ}$ 得到的.

不难验证$341,0000,(3+7),(3*(-61)),((+1)-((+6)/7))$都是上面定义的集合中的元素.

习题

1.下面的集合A和集合B是否是相等的?

(1) $A=\{1,2,3\},B=\{x\mid x\in\mathbf{Z}\}$;

(2) $A=\{1,2,4\},B=\{1,2,2,4\}$;

(3) $A=\{a,b,ab\},B=\{b,ab,a,b,a\}$.

2.已知$A\subseteq B,B\subset C$,证明$A\subset C$.

3.下面的等式是否成立?

(1) $\{0\}=\varnothing$;

(2) $\varnothing=0$;

(3) $\{\varnothing\}=\varnothing$;

(4) $\varnothing = \{x \mid x \neq x\}$;

(5) $\varnothing = \{B \mid B \subseteq A$且$|B| = 0\}$;

(6) $\mathscr{P}(\varnothing) = \varnothing$.

4.下面的命题是否成立?

(1) 如果$A \neq B, B \neq C$,则$A \neq C$;

(2) 如果$a \notin A, A \supseteq B$,则$a \notin B$;

(3) $|\mathscr{P}(A)| > 1$推出$A \neq \varnothing$.

5.证明下列不等式:

(1) $A \cap (\bar{A} \cup B) = A \cap B$;

(2) $A \cup (A \cap B) = A$;

(3) $A_1, A_2, \cdots, A_n$为集合,证明

$$\overline{\bigcap_i A_i} = \bigcup_i \overline{A_i}, \quad \overline{\bigcup_i A_i} = \bigcap_i \overline{A_i}.$$

6.证明下列命题:

(1) $B \subseteq C \Rightarrow (A \cap B) \subseteq (A \cap C)$;

(2) $A \subseteq C, B \subseteq C \Rightarrow (A \cup B) \subseteq C$;

(3) A和B是有限集合,那么$|A \cup B| \leqslant |A| + |B|$,并且仅当$A \cap B = \varnothing$时等式成立.

7.用归纳法定义如下集合:

(1) 十进制无符号整数,它应该包括$4, 167, 0012$等;

(2) 带有限小数部分的无符号实数,它应该包括$6.1, 712., 61.200$等;

(3) 不以0打头的二进制偶整数,它应该包括$0, 110, 1010$等.

第 2 章 数论初步

数论是一个古老的数学分支.在本章中我们主要介绍初等数论中的基本知识,它包括整除性、同余式、原根与指数等内容,为第5章以后学习群、环、域的知识提供一个现实模型,也为今后学习保密通讯、密码体制作必要的准备.

2.1 整除性

在现实世界的数量关系中,人们首先认识到$1,2,3,\cdots$这些正整数,在正整数之间可以做加法运算.为了能做减法运算又扩充到负整数和零.全体正整数构成了自然数集合$\mathbf{N}$.全体正负整数和零构成了整数集合$\mathbf{Z}$.整数集合和自然数集合是初等数论研究的对象.

在整数集合$\mathbf{Z}$中可以进行加、减、乘运算,并且满足一些规律(例如,加法的交换律和结合律,乘法对加法的分配律等).一般不能做除法运算,所以,研究整数间能否相除是揭示整数特性的一个重要手段.

2.1.1 整除关系及其性质

定义 2.1. a,b是整数,a**整除**b当且仅当存在整数d,使得$ad = b$,并记为$a \mid b$,也称a 是b的一个**因子**.

整除性反映了两个整数之间的一种关系,如$-3 \mid 6, 3 \mid -6, 4 \nmid 6$.

定理 2.1. 设$a,b,c,x,y \in \mathbf{Z}$.整除关系具有如下一些性质:

1° 对任何a均有$a \mid a$;

2° 若$a \mid b$且$b \mid a$,则$a = \pm b$;

3° 若$a \mid b$且$b \mid c$,则$a \mid c$;

4° 若$a \mid b$,则$a \mid (bc)$;

5° 若$a \mid b$且$a \mid c$,则$a \mid (bx + cy)$;

6° 若$a,b > 0$且$a \mid b$,则$a \leqslant b$;

证明 $1^\circ, 3^\circ, 4^\circ, 5^\circ$利用整除定义可以证明.这里只证明$2^\circ$和$6^\circ$.

证明2° 由$a \mid b$和$b \mid a$,知存在$x, y \in \mathbf{Z}$,使得$ax = b, by = a$.将它们的左边、右边分别相乘得到$abxy = ab$,推出$xy = 1$.从而只能有两种情况$x = y = 1$或$x = y = -1$,即$a = b$或$a = -b$.

证明6° $a, b > 0$且$a \mid b$,必有$x \in \mathbf{N}$使$ax = b$.这里$x \geqslant 1$, 得出$a \leqslant b$.

更一般地,若$a, b \in \mathbf{Z}$,且$a, b \neq 0, a \mid b$,那么$|a| \mid |b|$.由6°推出$|a| \leqslant |b|$,即$-|b| \leqslant a \leq |b|$.这表明非零的整数$b$只有有限多个因子.由于任何$x \in \mathbf{Z}, x \cdot 0 = 0$,从而0有无限多个因子.

2.1.2 最大公因子

有了整除的概念就可以定义两个整数的最大公因子.

定义 2.2. a, b是两个不同时为零的整数,a, b的**最大公因子**$d = (a, b)$满足:

1° $d \mid a, d \mid b$,即d是a与b的公共因子;

2° 若$c \mid a, c \mid b$,则$c \leqslant d$,即d是a与b的所有公共因子中最大的一个.

类似地可以定义$(a_1, a_2, \cdots, a_n)$.

除了1以外的整数至少有两个因子:1和自身.两个整数至少有一个公因子1.前面已经分析过,每个非零整数只有有限多个因子.从而当a, b不全为零时,它们的公因子也只有有限多个.d则是最大的那个公因子.显然$d = (a, b) \geqslant 1$.例如,$(-3, -6) = 3, (-3, 6) = 3, (2, 3) = 1$.如果两个整数的最大公因子为1,则称这两个整数是互素的.

为了考察是否存在整数x, y,使得a与b的最大公因子$d = ax + by$.也就是a, b的最大公因子d是否能用a与b线性表示出来.为此,我们先扩大范围研究集合

$$S = \{ax + by \mid x, y \in \mathbf{Z}\}.$$

该集合有如下性质:

1° 若$m, n \in S$,则$m \pm n \in S$;

2° 若$n \in S, c \in \mathbf{Z}$,则$cn \in S$;

3° 记S中最小正整数为d,那么S中每个数都是d的倍数.反过来,d的每个倍数也必属于S.

上面的性质1°和2°是显然的.现证明性质3°.因为a,b不全为零,$\pm a,\pm b$显然属于集合S.也就是说,集合S中有正元素,所以S中一定存在着一个最小的正整数d.任取$c\in S$,有$c=qd+r$,其中q和r分别为c除以d得到的商和非负余数,$0\leqslant r<d$.因为$d\in S$,由性质2°知$q\cdot d\in S$.又因$c\in S$,由性质1°知$r=c-q\cdot d\in S$.由于d是S中最小的正整数,从而必有$r=0$,即$c=q\cdot d$,故

$$S=\{ax+by\mid x,y\in\mathbf{Z}\}=\{k\cdot d\mid k\in\mathbf{Z}\}.$$

下面证明S的最小正整数d就是a与b的最大公因子.由于$d\in S$,存在$x_0,y_0\in\mathbf{Z}$,使得$d=ax_0+by_0$.因为$(a,b)\mid a,\ (a,b)\mid b$,于是$(a,b)\mid d$.由整除的性质6°,知$(a,b)\leqslant d$.另一方面,因为$a\in S,b\in S$,那么存在$k_1,k_2\in\mathbf{Z}$,使得$a=k_1d,b=k_2d$,从而$d$是$a$与$b$的公因子.而$(a,b)$是$a$与$b$的最大公因子,所以$d\leq(a,b)$. 综上知$d=(a,b)$.

从上面的讨论看出,若a,b是不全为零的整数,那么一定存在整数x,y使$ax+by=(a,b)$.另外,整数n可以表示成$ax+by$形式的充要条件是$(a,b)\mid n$.显然,当a与b互素时,任何整数n都可以表示成$ax+by$的形式,由此得到:

定理 2.2. 设a,b是不为零的整数,那么

1° (a,b)是集合$S=\{ax+by\mid x,y\in\mathbf{Z}\}$中最小的正整数;

2° 整数n可以表示成$ax+by$形式的充要条件是$(a,b)\mid n$.

利用定理2.2可以得到关于最大公因子的一些有用的性质.

推论 2.1. 若m为正整数,则$(ma,mb)=m\,(a,b)$.

证明

$$\begin{aligned}(ma,mb)&=\text{形如 }max+mby\text{ 的最小正整数}\\&=m\cdot\text{形如 }ax+by\text{ 的最小正整数}\\&=m\cdot(a,b)\,.\end{aligned}$$

特别有:

1° 若$(a,b)=d$,则$d=(a,b)=d\left(\frac{a}{d},\frac{b}{d}\right)$.两边除以$d$,得到$\left(\frac{a}{d},\frac{b}{d}\right)=1$.

2° 若m是a与b的公因子,$a=ma_1,b=mb_1$. $(a,b)=m\,(a_1,b_1)$,所以$m\mid(a,b)$,即a与b的公因子是最大公因子的因子.

推论 2.2. 若$(a,m)=(b,m)=1$,则$(ab,m)=1$.

证明 由$(a,m)=(b,m)=1$知存在$x_0,y_0,x_1,y_1\in\mathbf{Z}$,使得$ax_0+my_0=1$,$bx_1+my_1=1$.将这两个式子左右两边分别相乘,得到

$$abx_0x_1+m\left(ax_0y_1+bx_1y_0+my_0y_1\right)=1.$$

从而$(ab,m)=1$.

推论 2.3. a,b是不全为零的整数,对任意整数x有$(a,b)=(a,b+ax)$.

证明 令$g=(a,b)$, $h=(a,b+ax)$.由$g\mid a,g\mid b$知$g\mid(b+ax)$,即g是a与$b+ax$的公因子.从推论2.1中的2°知$g\mid h$.另一方面$h\mid a,h\mid(b+ax)$,推出$h\mid b$.从而h是a与b的公因子.同理$h\mid g$.由定理2.1中2°和$h,g>0$,得出$h=g$,即$(a,b)=(a,b+ax)$.

推论 2.4. 若$c\mid ab$且$(c,b)=1$,则$c\mid a$.

证明 由$c\mid ab,c\mid ac$,根据推论2.1中的2°知$c\mid(ab,ac)$.而从推论2.1知$(ab,ac)=a(b,c)=a\cdot1=a$.于是$c\mid a$.

上面的证明(a,b)可以表示成$ax+by$形式的过程中,没有给出一种可行的方法求出x和y.我们利用推论2.3,可以得到求解$ax+by=(a,b)$的欧几里得算法.由于$(a,b)=(|a|,|b|)$,我们这里不妨假设$a\geqslant b>0$.

定理 2.3. a,b为正整数,有下列关系式:

$$\begin{aligned}
a&=bq_0+r_0,0<r_0<b,\\
b&=r_0q_1+r_1,0<r_1<r_0,\\
r_0&=r_1q_2+r_2,0<r_2<r_1,\\
&\cdots\cdots\cdots\\
r_i&=r_{i+1}q_{i+2}+r_{i+2},0<r_{i+2}<r_{i+1},\\
r_{i+1}&=r_{i+2}q_{i+3},
\end{aligned}$$

则$(a,b)=r_{i+2}$.

证明 在上述辗转相除的一系列关系式中,$b > r_0 > r_1 > \cdots r_{i+1} > r_{i+2} \geqslant 0$是一个非负的递减序列.因此经过数次相除以后所得到的余数必为0.我们这里假设$r_{i+3} = 0$.根据推论2.3有

$$\begin{aligned}(a,b) &= (b,r_0) = (r_0,r_1) = \cdots = (r_i,r_{i+1})\\ &= (r_{i+1},r_{i+2}) = r_{i+2}.\end{aligned}$$

由上述辗转相除算法,不仅可以得到(a,b),利用这些关系式反推回去,就可以得到$(a,b) = ax + by$中的x,y的值.

例 2.1. 计算$(963,657)$.

解 按定理2.3提供的辗转相除算法得到关系式:

$$\begin{aligned}963 &= 657\cdot 1 + 306,\\ 657 &= 306\cdot 2 + 45,\\ 306 &= 45\cdot 6 + 36,\\ 45 &= 36\cdot 1 + 9,\\ 36 &= 9\cdot 4,\end{aligned}$$

于是$(963,657) = 9$.

又有

$$\begin{aligned}9 &= 45 - 36\cdot 1 = 45 - (306 - 45\cdot 6) = 45\cdot 7 - 306\\ &= (657 - 306\cdot 2)\cdot 7 - 306 = 657\cdot 7 - 306\cdot 15\\ &= 657\cdot 7 - (963 - 657\cdot 1)\cdot 15 = 657\cdot 22 - 963\cdot 15,\end{aligned}$$

方程$963x + 657y = 9$的解为$x = -15, y = 22$.

2.1.3 最小公倍数

定义 2.3. a,b为整数,a与b的**最小公倍数**$c = [a,b]$满足:

1° $a \mid c, b \mid c$,且$c > 0$;

2° 若$a \mid e, b \mid e$,则$c \leqslant |e|$.

类似可以定义$[a_1, a_2, \cdots, a_n]$.

任何两个整数a, b存在着正公倍数,如$|ab|$.我们知道,若u是a与b的公倍数,则对于任何正整数x,ux也是a与b的公倍数.所以a与b不存在最大公倍数.显然a与b有最小正公倍数c.我们称c为a与b的最小公倍数.

对于两个非零整数的最小公倍数也有类似于最大公因子的结论.

定理 2.4. a, b为非零整数,a与b的每个公倍数均是最小公倍数的倍数.

证明 考虑集合$S' = \{a$与b的所有公倍数$\}$.该集合有如下性质:

1° 若$m, n \in S'$,则$m \pm n \in S'$;

2° 若$n \in S', c \in \mathbf{Z}$,则$cn \in S'$;

3° S'中有最小正整数u,那么S'中每个元素均是u的倍数.反过来u的任意倍数必属于S'.显然u就是a与b的最小公倍数.

$1^\circ, 2^\circ$是显然的.因S'是由a与b的所有公倍数组成的,$\pm ab \in S'$,即S' 中有正数,从而S'中存在最小正整数u.任取$v \in S', v = qu + r, 0 \leqslant r < u$. 由于$v, u \in S', q \in \mathbf{Z}$,所以$r = v - qu \in S'$.$u$是$S'$中的最小正整数,因此必有$r = 0$,即$v = qu$.由$a$与$b$的最小公倍数的定义知$u = [a, b]$.$S' = \{ku | k \in \mathbf{Z}\}$.这说明非零整数$a, b$的每个公倍数都是最小公倍数的倍数.

利用定理2.4可以得到关于最小公倍数的一些有用的性质.

推论 2.5. m为正整数,则$[ma, mb] = m[a, b]$.

证明 由$a \mid [a, b], b \mid [a, b]$,知$ma \mid m[a, b], mb \mid m[a, b]$,即$m[a, b]$是$ma$与$mb$ 的公倍数,从而$[ma, mb] \mid m[a, b]$.另一方面,若l是ma与mb的公倍数,必有$m \mid l$.不妨令$l = l'm$,那么l'是a与b的公倍数,从而$[a, b] \mid l'$.由此推出$m[a, b] \mid l$,现取$l = [ma, mb]$,得到$m[a, b] \mid [ma, mb]$.由定理2.1中2°以及$m[a, b] > 0$, $[ma, mb] > 0$,最后得出

$$[ma, mb] = m[a, b].$$

推论 2.6. 若a, b为正整数,则$[a, b](a, b) = ab$.

证明 首先讨论$(a, b) = 1$的情况,$[a, b]$是a与b的最小公倍数,存在m_1使得$[a, b] = m_1 a$.由$b \mid [a, b]$,知$b \mid m_1 a$.而$(a, b) = 1$,由推论2.4得出$b \mid m_1$.m_1应该是满足此关系的最小正整数,所以$m_1 = b$,即$[a, b] = ab$.

当$(a,b)=d$时,由推论2.1中的1°知$\left(\frac{a}{d},\frac{b}{d}\right)=1$.从上面的结论,有$\left[\frac{a}{d},\frac{b}{d}\right]=\frac{1}{d^2}ab$.根据推论2.1和推论2.5,

$$(a,b)\,[a,b]=d^2\left(\frac{a}{d},\frac{b}{d}\right)\left[\frac{a}{d},\frac{b}{d}\right]=d^2\cdot 1\cdot\frac{1}{d^2}\cdot ab=ab.$$

这正是所要的结论.

2.1.4 素因子分解唯一性定理

a是b的因子当且仅当$a\mid b$.如果正整数b只有1和b为其因子,则称b为素数.例如$2,3,5,7,11,13,17,19,\cdots$,每个大于1的整数都可以被一个素数整除,从而得到该整数的素因子分解式.例如$60=2^2\cdot 3\cdot 5$.如果不考虑因子出现的次序,那么这种分解形式是唯一的.我们只叙述素因子分解唯一性定理,而不加以证明.

定理 2.5. (素因子分解唯一性定理)

任意正整数都能用一种方式且只有一种方式写成素数的乘积.

我们可以用加法作为构造自然数的手段,任何正整数$n=\underbrace{1+1+\cdots+1}_{n}$,其基本元素就是1.当用乘法作为构造自然数的手段时,其基本元素是全体素数.这个结论是素因子分解唯一性定理告诉我们的.

那么有多少个素数呢?结论是:存在着无限多个素数.可用反证法证明这一结论.假若只有有限多个素数$p_1,p_2,\cdots,p_k$.令$n=p_1p_2\cdots p_k+1$.n是自然数,存在一个素数p_i使$p_i\mid n$,推出$p_i\mid 1$.产生矛盾,故不可.所以有无限多个素数.

一般来说,对给定的整数进行素因子分解是很困难的.首先遇到的问题是没有一种“可行性算法”来确定所给的整数是否是素数.奥地利天文学家用厄氏筛法花了20年时间得到了10^8 以内的素数.20 世纪60年代美国宣布他们的计算机内存放着前5×10^8个素数.1985年9月美国在CRAY X-MP超级计算机上计算的最大素数为$2^{216091}-1>10^{65050}$.这是目前人们知道的最大素数.

2.2 线性不定方程

限制在某类数中(如正整数、有理数等)求解的方程叫丢番图方程,最简单的丢番图方程就是线性不定方程

$$a_1x_1 + a_2x_2 + \cdots + a_nx_n = n.$$

求其整数解.

早在1400多年前,隋朝《张丘健算径》一书中最后一问是世界著名的百鸡问题.问题是:鸡翁一,值钱五,鸡母一,值钱三,鸡仔三,值钱一,百钱买百鸡,问鸡翁、鸡母、鸡仔各几何?设鸡翁x只,鸡母y 只,鸡仔$3z$只.由题意列出方程

$$\begin{cases} 5x + 3y + z = 100 \\ x + y + 3z = 100. \end{cases}$$

消去z,得到$7x + 4y = 100$.这时多元线性不定方程化为二元线性不定方程.

以下我们只讨论二元线性不定方程.

定理 2.6. a,b,n为整数.$ax+by = n$有解当且仅当$(a, b) \mid n$.如果x_0,y_0是$ax+by = n$的一组解,则通解为

$$x = x_0 + \tfrac{b}{(a,b)}t, \quad y = y_0 - \tfrac{a}{(a,b)}t,$$

其中t为整数.

证明 由上节定理2.2对集合$S = \{ax + by \mid x, y \in \mathbf{Z}\}$的讨论知$ax + by = n$有解当且仅当$(a, b) \mid n$.

如果x_0,y_0是$ax + by = n$的一组解,即$ax_0 + by_0 = n$.由于

$$a\left(x_0 + \tfrac{b}{(a,b)}t\right) + b\left(y_0 - \tfrac{a}{(a,b)}t\right) = n.$$

所以$x = x_0 + \frac{b}{(a,b)}t$,$y = y_0 - \frac{a}{(a,b)}t$是$ax + by = n$的解.反过来,若$x$,$y$是方程$ax + by = n$的解,则

$$a(x - x_0) + b(y - y_0) = 0.$$

由此得出$b \mid a\,(x - x_0)$,即$\frac{b}{(a,b)} \mid \frac{a}{(a,b)}\,(x - x_0)$.而$\left(\frac{a}{(a,b)}, \frac{b}{(a,b)}\right) = 1$,于是$\frac{b}{(a,b)} \mid (x - x_0)$,即$x = x_0 + \frac{b}{(a,b)}t$,其中$t$为一个整数,将$x$的表达式代入$a\,(x - x_0) + b\,(y - y_0) = 0$,解出$y = y_0 - \frac{a}{(a,b)}t$.由此可知该方程的通解为

$$x = x_0 + \tfrac{b}{(a,b)}t, \quad y = y_0 - \tfrac{a}{(a,b)}t.$$

例 2.2. 前面的百鸡问题$7x+4y=100$.因$(7,4)=1$,所以方程有解,$x_0=0,y_0=25$是一组特解.通解为$x=4t,y=25-7t$.为保证x,y为非负整数,t只能取值$0,1,2,3$.故该方程的解共有四组.它们是

$$\begin{cases} x=0 \\ y=25 \\ 3z=75, \end{cases} \quad \begin{cases} x=4 \\ y=18 \\ 3z=78, \end{cases} \quad \begin{cases} x=8 \\ y=11 \\ 3z=81, \end{cases} \quad \begin{cases} x=12 \\ y=4 \\ 3z=84. \end{cases}$$

2.3 同余式与线性同余方程

2.3.1 同余式及其性质

在2.1节中我们讲到整除性.整数a除以整数b,如果余数为0,称$b \mid a$.当$b \nmid a$时,余数有各种可能性.为了区分它们,我们引入同余的概念.

定义 2.4. 设$a,b,m \in \mathbf{Z}, m \neq 0$,$a$与$b$**模**$m$**同余**当且仅当$m \mid (a-b)$,并记为$a \equiv b \pmod{m}$.

显然$a \equiv b \pmod{m}$与$a \equiv b \pmod{-m}$等价.所以,以后假设$m>0$.

同余式有许多与通常等式相类似的性质.我们列举如下(设$a,b,c,x,y \in \mathbf{Z}$):

1° $a \equiv a \pmod{m}$;

2° 若$a \equiv b \pmod{m}$,则$b \equiv a \pmod{m}$;

3° 若$a \equiv b \pmod{m}$,$b \equiv c \pmod{m}$,则$a \equiv c \pmod{m}$;

4° 若$a \equiv b \pmod{m}$,$c \equiv d \pmod{m}$,则

$$a+c \equiv b+d \pmod{m}, \quad ac \equiv bd \pmod{m};$$

5° 若$a \equiv b \pmod{m}$且$d \mid m$,则$a \equiv b \pmod{d}$;

6° 若$a \equiv b \pmod{m}$,则$ax \equiv bx \pmod{m}$;

7° $ax \equiv ay \pmod{am}$当且仅当$x \equiv y \pmod{m}$;

8° 若$ax \equiv ay \pmod{m}$且$(a,m)=1$,则$x \equiv y \pmod{m}$;

9° $x \equiv y \pmod{m_i}, 1 \leqslant i \leqslant r$当且仅当$x \equiv y \pmod{[m_1, m_2, \ldots, m_r]}$.

以上诸性质都可以由同余定义直接得到.证明从略.

2.3.2 线性同余方程

a, b为整数,我们要求线性同余方程$ax \equiv b \pmod{m}$的解.先看一个特殊情况.

定理 2.7. 设$(a, m) = 1$.对于每个整数b,同余方程$ax \equiv b \pmod{m}$有模m唯一解.

证明 因为$(a, m) = 1$,对于每个整数b都存在着$x, y \in \mathbf{Z}$,使得$ax + my = b$,即$ax \equiv b \pmod{m}$,x就是该同余方程的解.

下面证明解是模m唯一的.若x_1, x_2都是$ax \equiv b \pmod{m}$的解,即$ax_1 \equiv ax_2 \equiv b \pmod{m}$.由于$(a, m) = 1$,得到$x_1 \equiv x_2 \pmod{m}$.这说明方程的任意两个解是模$m$同余的,即解模$m$唯一.

定理 2.8. 同余方程$ax \equiv b \pmod{m}$有解当且仅当$(a, m) \mid b$.当条件满足时,该同余方程有(a, m)个模m不同余的解:

$$x = x_0 + \frac{m}{(a, m)} t \pmod{m}, \quad 0 \leqslant t \leqslant (a, m) - 1.$$

其中x_0是同余方程

$$\frac{a}{(a, m)} x \equiv \frac{b}{(a, m)} \left(\mathrm{mod}\ \frac{m}{(a, m)} \right)$$

的解.

证明 设x_0是同余方程$ax \equiv b \pmod{m}$的解.即$m \mid (ax_0 - b)$.由于$(a, m) \mid m$,显然有$(a, m) \mid (ax_0 - b)$.又由$(a, m) \mid a$,推出$(a, m) \mid b$.反过来,当$(a, m) \mid b$时,存在$x_1, y_1 \in \mathbf{Z}$, 使$ax_1 + my_1 = b$,即$ax_1 \equiv b \pmod{m}$.这表明x_1就是同余方程$ax \equiv b \pmod{m}$的一个解.

当满足同余方程有解的条件$(a,m)\mid b$时,$ax\equiv b\,(\mathrm{mod}\ m)$可以化成等价的同余方程

$$\frac{a}{(a,m)}x\equiv\frac{b}{(a,m)}\left(\mathrm{mod}\ \frac{m}{(a,m)}\right).$$

由于$\left(\frac{a}{(a,m)},\frac{m}{(a,m)}\right)=1$,该方程有模$\frac{m}{(a,m)}$唯一解$x\equiv x_0\left(\mathrm{mod}\ \frac{m}{(a,m)}\right)$.这里不妨取$0\leqslant x_0<\frac{m}{(a,m)}$.这个$x_0$也是$ax\equiv b\,(\mathrm{mod}\ m)$的一个解.下面证明$x_0+i\frac{m}{(a,m)},0\leqslant i\leqslant(a,m)-1$也是$ax\equiv b\,(\mathrm{mod}\ m)$的解.把它们代入方程

$$a\left(x_0+i\frac{m}{(a,m)}\right)=ax_0+\frac{a}{(a,m)}im\equiv b\,(\mathrm{mod}\ m).$$

而

$$0\leqslant x_0+i\frac{m}{(a,m)}<\frac{m}{(a,m)}+((a,m)-1)\frac{m}{(a,m)}=m,$$

所以$x_0+i\frac{m}{(a,m)},0\leqslant i\leqslant(a,m)-1$是$(a,m)$个模$m$不同余的解.反过来,假设$y$是$ax\equiv b\,(\mathrm{mod}\ m)$的一个解.必有$ax_0\equiv ay\equiv b\,(\mathrm{mod}\ m)$,推出$x_0\equiv y\left(\mathrm{mod}\ \frac{m}{(a,m)}\right)$,即$y=x_0+k\frac{m}{(a,m)}$.令$i$表示$k$除以$(a,m)$的非负余数,那么$y\equiv x_0+i\frac{m}{(a,m)}\,(\mathrm{mod}\ m)$.这说明$ax\equiv b\,(\mathrm{mod}\ m)$除上述$(a,m)$个解之外没有其他形式的解.

例 2.3. 解同余方程$14x\equiv 27\,(\mathrm{mod}\ 31)$.

解 因$(14,31)=1,14x\equiv 27\,(\mathrm{mod}\ 31)$.有模31唯一解,

$$14x\equiv 27\equiv 58\,(\mathrm{mod}\ 31).$$

因$(2,31)=1$,利用同余式性质8°得到

$$7x\equiv 29\,(\mathrm{mod}\ 31).$$

又由$7x\equiv 29\equiv 91\,(\mathrm{mod}\ 31)$,且$(7,31)=1$,解出$x\equiv 13\,(\mathrm{mod}\ 31)$.

例 2.4. 解同余方程$6x\equiv 30\,(\mathrm{mod}\ 33)$.

解 $(6,33)=3$且$3\mid 30$,由定理2.8知该同余方程有3个模33不同余的解.

与$6x\equiv 30\,(\mathrm{mod}\ 33)$等价的同余方程$2x\equiv 10\,(\mathrm{mod}\ 11)$中$(2,11)=1,x\equiv 5\,(\mathrm{mod}\ 11)$是它的模11唯一解.$x\equiv 5+11t\,(\mathrm{mod}\ 33),0\leqslant t\leqslant 2$是同余方程$6x\equiv 30\,(\mathrm{mod}\ 33)$的三个模33不同余的解,即该同余方程的解为

$$x\equiv 5,16,27\,(\mathrm{mod}\ 33).$$

2.3.3 线性同余方程组

我国古代数学著作《孙子算经》中“物有不知其数”一问:“今有物不知其数.三三数之余二,五五数之余三,七七数之余二,问物几何?”用数学语言来描述就是(设其数为x)

$$\begin{cases} x \equiv 2\,(\mathrm{mod}\ 3) \\ x \equiv 3\,(\mathrm{mod}\ 5) \\ x \equiv 2\,(\mathrm{mod}\ 7)\,. \end{cases}$$

这一问题的古代算法在程大位的《算法统宗》中总结成:

“三人同行七十稀,
五树梅花廿一枝,
七子团圆月正半,
除百零五便得知.”

意思是以$70, 21, 15$分别乘该数除以$3, 5, 7$所得的余数$2, 3, 2$,将结果相加再模105. 即

$$x \equiv 70 \cdot 2 + 21 \cdot 3 + 15 \cdot 2 = 233 \equiv 23(\mathrm{mod}\ 105).$$

国外数论文献中把这个算法称之为中国剩余定理.在下面定理中将给出证明.

定理 2.9. 设自然数$m_1, m_2, \cdots, m_r$,两两互素,对任意整数$a_1, a_2, \cdots, a_r$,线性同余方程组$x \equiv a_i(\mathrm{mod}\ m_i)$,$1 \leqslant i \leqslant r$均有解,并且解是模$m_1 m_2 \cdots m_r$唯一的.

证明 令$M = m_1 m_2 \cdots m_r, M_i = \frac{M}{m_i}, (M_i, m_i) = 1, 1 \leqslant i \leqslant r$.对每个$i, M_i b_i \equiv 1(\mathrm{mod}\ m_i)$有解并且当$j \neq i$时,$M_i b_i \equiv 0(\mathrm{mod}\ m_i)$.现令$y = \sum_{j=1}^{r} M_j b_j a_j$,显然

$$y = M_i b_i a_i \equiv a_i(\mathrm{mod}\ m_i), 1 \leqslant i \leqslant r,$$

从而y是同余方程组的解.同时与y模$m_1 m_2 \cdots m_r$同余的数也是该同余方程组的解.

令y_1, y_2都是同余方程组的解,那么$y_1 - y_2 \equiv 0(\mathrm{mod}\ m_i), 1 \leqslant i \leqslant r$.也就是说$y_1 - y_2$是$m_1, m_2, \cdots, m_r$的公倍数,从而$[m_1, m_2, \cdots, m_r] \mid (y_1 - y_2)$.而$m_1, m_2, \cdots, m_r$ 两两互素,$[m_1, m_2, \cdots, m_r] = m_1 m_2 \cdots m_r$. 最后得出

$$y_1 \equiv y_2(\mathrm{mod}\ m_1 m_2 \cdots m_r).$$

该定理的证明是构造性的,它已指明解线性同余方程组的具体步骤.

例 2.5. 解同余方程组

$$\begin{cases} x \equiv 2(\mathrm{mod}\ 3) \\ x \equiv 3(\mathrm{mod}\ 5) \\ x \equiv 2(\mathrm{mod}\ 7). \end{cases}$$

解 本题中$M = 3 \cdot 5 \cdot 7 = 105, M_1 = 35, M_2 = 21, M_3 = 15$.由$35b_1 \equiv 1(\mathrm{mod}\ 3), 21b_2 \equiv 1(\mathrm{mod}\ 5), 15b_3 \equiv 1(\mathrm{mod}\ 7)$分别解出$b_1 = 2, b_2 = 1, b_3 = 1$.从而

$$\begin{aligned} y &= 35 \cdot 2 \cdot 2 + 21 \cdot 1 \cdot 3 + 15 \cdot 1 \cdot 2 \\ &= 70 \cdot 2 + 21 \cdot 3 + 15 \cdot 2 = 233. \end{aligned}$$

$y \equiv 23(\mathrm{mod}\ 105)$是该同余方程组的解.

定理 2.10. 线性同余方程组$x \equiv a_i(\mathrm{mod}\ m_i), i = 1, 2$,有解的充要条件是$(m_1, m_2) \mid (a_1 - a_2)$.在条件满足时,该方程的解模$[m_1, m_2]$唯一.

证明 该方程有解就是存在着整数s, t,使$x = m_1 t + a_1$且$x = m_2 s + a_2$,即$m_1 t - m_2 s = a_2 - a_1$.从定理2.6知该方程有解当且仅当$(m_1, m_2) \mid (a_2 - a_1)$.所以线性同余方程组有解的充要条件是$(m_1, m_2) \mid (a_1 - a_2)$.

若当条件满足时,x_1和x_2都是该方程组的解,则

$$\begin{cases} x_1 - x_2 \equiv 0(\mathrm{mod}\ m_1) \\ x_1 - x_2 \equiv 0(\mathrm{mod}\ m_2). \end{cases}$$

$x_1 - x_2$是m_1, m_2的公倍数.于是$[m_1, m_2] \mid (x_1 - x_2)$,即$x_1 \equiv x_2(\ \mathrm{mod}\ [m_1, m_2])$.它说明该方程的解模$[m_1, m_2]$唯一.

例 2.6. 求解同余方程组

$$\begin{cases} x \equiv 2(\mathrm{mod}\ 4) \\ x \equiv 0(\mathrm{mod}\ 6). \end{cases}$$

解 因$(4,6) \mid (2-0)$,该方程组有解并且解模12唯一.下面就求它的解.由$x \equiv 2(\mathrm{mod}\ 4)$,知$x = 2 + 4k_1$,将其代入$x \equiv 0(\mathrm{mod}\ 6)$, 得到$4k_1 \equiv 4(\mathrm{mod}\ 6)$,化简后为$k_1 \equiv 1(\mathrm{mod}\ 3)$.于是$k_1 = 1 + 3k_2$.再代入$x = 2 + 4k_1$, 得到$x = 6 + 12k_2$.从而解为

$$x \equiv 6(\mathrm{mod}\ 12).$$

2.4 欧拉定理及欧拉函数

2.4.1 完系与缩系

对于给定的整数m,每个整数都与且仅与集合$\{0, 1, \cdots, m-1\}$中一个数模m同余.一般地,

定义 2.5. 整数集合$\{x_1, x_2, \cdots, x_m\}$,如果每个整数都与且仅与该集合中一个$x_i$模$m$同余,则称$\{x_1, x_2, \cdots, x_m\}$为模$m$的**完系**.

显然$\{0, 1, 2, 3, 4\}$是模5 的完系,$\{10, 21, 27, 38, -1\}$也是模5 的完系.不难看出, 模m的完系有两个特征, 首先它是由m个元素组成的,其次这些元素相互不模m同余.

我们把模m的同余类表示成$A_i = \{x | x \in \mathbf{Z}, x \equiv i(\mathrm{mod}\ m)\}, 0 \leqslant i \leqslant m-1$.每个整数都与$\{0, 1, \cdots, m-1\}$中一个数同余,所以每个整数只属于$A_0, A_1, \cdots, A_{m-1}$ 中的一个.若$x \in A_i$且$(x, m) = 1$,那么A_i中的任意元素y都必有$(y, m) = 1$,这是因为$x, y \in A_i, x \equiv y(\mathrm{mod}\ m)$,即$x = y + km$, 如果$(y, m) = d$,则必有$d \mid x$.再由$d \mid m$知$d \mid (x, m)$.而$(x, m) = 1$,从而$(y, m) = d = 1$.

若$x \in A_i$且$(x, m) = 1$,则称A_i是与m互素的同余类,与m互素的同余类个数记为$\phi(m)$,称为**欧拉函数**.

定义 2.6. 在每个与m互素的同余类中取一个元素作为代表放在一起构成的集合$\{r_1, r_2, \cdots, r_{\phi(m)}\}$叫做模$m$的**缩系**.

例 2.7. $\{0,1,2,3,4,5\}$是模6的完系,六个同余类$A_i = \{6k+i | k \in Z\}, 0 \leqslant i \leqslant 5$中$A_1, A_5$是与6互素的同余类,故$\phi(6) = 2$.$\{1,5\}, \{7,-1\}$都是模6 的缩系.

实际上,把$\{1,2,\cdots,m-1\}$中与m互素的数放在一起恰好是模m的一个缩系.$\phi(m)$就是不超过m且与m互素的正整数个数.不难验证$\phi(2)=1, \phi(3)=\phi(4)=\phi(6)=2, \phi(5)=\phi(8)=4, \phi(7)=6$.我们规定$\phi(1)=1$.显然对于素数$p$, $\phi(p)=p-1$.

引理 2.1. 已知$(a,m)=1$.若$\{x_1, x_2, \cdots, x_m\}$是模$m$的完系,则$\{ax_1, ax_2, \cdots, ax_m\}$也是模$m$的完系,若$\{r_1, r_2, \cdots, r_{\phi(m)}\}$是模$m$的缩系,则$\{ar_1, ar_2, \cdots, ar_{\phi(m)}\}$也是模$m$的缩系.

证明 $\{x_1, x_2, \cdots, x_m\}$是模$m$的完系,由其定义知$i \neq j, x_i \not\equiv x_j (\mathrm{mod}\ m)$. 如果$ax_i \equiv ax_j (\mathrm{mod}\ m)$,由于$(a,m)=1$,推出必有$x_i \equiv x_j (\mathrm{mod}\ m)$.这与$\{x_1, x_2, \cdots, x_m\}$ 是模m的完系矛盾. 由此得出$ax_1, ax_2, \cdots, ax_m$是两两模m 互不同余的m个元素, 它们正好构成一个模m的完系.

$\{r_1, r_2, \cdots, r_{\phi(m)}\}$是模$m$的缩系,由其定义知$(r_i, m)=1, 1 \leqslant i \leqslant \phi(m)$,并且$i \neq j, r_i \not\equiv r_j (\mathrm{mod}\ m)$.从$(r_i, m)=1$和$(a,m)=1$,根据推论2.2 知$(ar_i, m)=1$.前面已经证明过$i \neq j, ar_i \not\equiv ar_j (\mathrm{mod}\ m)$.$ar_1, ar_2, \cdots, ar_{\phi(m)}$恰是$\phi(m)$个与$m$互素且两两模$m$ 不同余的元素.它们恰好构成模m的一个缩系.

2.4.2 欧拉定理与费马定理

定理 2.11. (欧拉定理)
如果$(a,m)=1$,则$a^{\phi(m)} \equiv 1 (\mathrm{mod}\ m)$.

证明 取一个模m的缩系$\{r_1, r_2, \cdots, r_{\phi(m)}\}$.当$(a,m)=1$时,$\{ar_1, ar_2, \cdots, ar_{\phi(m)}\}$也是模$m$的缩系.任选一个$r_i$,必存在一个$r_j$使$r_i \equiv ar_j (\mathrm{mod}\ m)$,并且不同的下标$i$对应不同的下标$j$.由此得出

$$\begin{aligned} r_1 r_2 \cdots r_{\phi(m)} &\equiv ar_{j_1} \cdot ar_{j_2} \cdots ar_{j_{\phi(m)}} \\ &= a^{\phi(m)} \cdot r_1 r_2 \cdots r_{\phi(m)} (\mathrm{mod}\ m). \end{aligned}$$

由于$(r_i, m) = 1, 1 \leqslant i \leqslant \phi(m)$,根据推论2.2知

$$(r_1 r_2 \cdots r_{\phi(m)}, m) = 1,$$

从前式立即推出

$$a^{\phi(m)} \equiv 1 (\mathrm{mod}\ m).$$

在定理2.11中取m为素数p,$(a, p) = 1$就是$p \nmid a$,$\phi(p) = p - 1$, 从而得到费马定理: p为素数且$p \nmid a$,则

$$a^{p-1} \equiv 1 (\mathrm{mod}\ p).$$

若$p|a$,$a \equiv 0 (\mathrm{mod}\ p)$,则显然成立$a^p \equiv a (\mathrm{mod}\ p)$.而当$p \nmid a$时,从费马定理知$a^{p-1} \equiv 1 (\mathrm{mod}\ p)$.再由同余式性质6°,仍成立$a^p \equiv a (\mathrm{mod}\ p)$.所以,对于任何$a$都有$a^p \equiv a (\mathrm{mod}\ p)$,其中$p$是素数.

2.4.3 计算欧拉函数

引理 2.2. p为素数,对一切正整数n,$\phi(p^n) = p^{n-1}(p - 1)$.

证明 小于等于p^n的数共有p^n个, 其中与p^n有公因子p的数是$p, 2p, \cdots, p^{n-1}p$,一共有p^{n-1}个.那么与p^n无公因子p的, 即与p^n互素的数共有$p^n - p^{n-1} = p^{n-1}(p - 1)$个.

定理 2.12. 当$(m, n) = 1$时,$\phi(mn) = \phi(m) \cdot \phi(n)$.

证明 $\phi(mn)$是小于等于mn且与mn互素的正整数个数,下面把所有小于等于mn的正整数列成一个方阵

$$\begin{array}{cccccc}
1 & m+1 & 2m+1 & \cdots & (n-1)m+1 \\
2 & m+2 & 2m+2 & \cdots & (n-1)m+2 \\
3 & m+3 & 2m+3 & \cdots & (n-1)m+3 \\
\vdots & \vdots & \vdots & & \vdots \\
m & m+m & 2m+m & \cdots & (n-1)m+m
\end{array}$$

若$(m, r) = d > 1$,那么r所在行的全部元素$r, m+r, 2m+r, \cdots, (n-1)m+r$均与$mn$有公因子$d$,由此可知,与$mn$互素的数只能在$(m, r) = 1$的$\phi(m)$行中寻

找,而当$(m,r)=1$时,$\{r,m+r,2m+r,\cdots,(n-1)m+r\}$是$n$元集合,并且两两模$n$不同余.它是模$n$的完系.在一个模$n$的完系中有$\phi(n)$个数与$n$互素.而该完系中每个数均与$m$互素,从而它里面有$\phi(n)$个数与$mn$互素.

从上分析得到$\phi(mn)=\phi(m)\cdot\phi(n)$.

若$(m,n)=1$,满足$f(mn)=f(m)f(n)$的函数f成为**积性函数**.欧拉函数ϕ是积性函数.从定理2.12不难看出.若n的素因子分解式为$n=p_1^{l_1}p_2^{l_2}\cdots p_k^{l_k}$,则

$$\phi(n)=p_1^{l_1-1}(p_1-1)\cdots p_k^{l_k-1}(p_k-1)=n(1-\frac{1}{p_1})\cdots(1-\frac{1}{p_k}).$$

例 2.8. 求2^{340}除以341的余数.

解 $341=11\cdot31$.由欧拉定理$2^{10}\equiv1(\mathrm{mod}\ 11),2^{30}\equiv1(\mathrm{mod}\ 31)$.

$$2^{340}=(2^{10})^{34}\equiv1(\mathrm{mod}\ 11),$$
$$2^{340}=(2^{30})^{11}\cdot2^{10}\equiv2^{10}=(2^5)^2\equiv1(\mathrm{mod}\ 31),$$

即2^{340}是下面线性同余方程组的解:

$$\begin{cases}x\equiv1(\mathrm{mod}\ 11)\\x\equiv1(\mathrm{mod}\ 31).\end{cases}$$

解得$x\equiv1(\mathrm{mod}\ 341)$,即$2^{340}\equiv1(\mathrm{mod}\ 341)$.

本例说明费马定理的逆定理不成立,$2^{340}\equiv1(\mathrm{mod}\ 341)$,但是341不是素数.

例 2.9. 解同余方程$9x\equiv7(\mathrm{mod}\ 13)$.

解 13是素数.由费马定理知$3^{12}\equiv1(\mathrm{mod}\ 13)$.

$$x\equiv3^{12}\cdot x\equiv3^{10}\cdot9x\equiv3^{10}\cdot7\equiv(13-4)^5\cdot7\equiv(-4)^5\cdot7$$
$$\equiv(13+3)^2(-28)\equiv9\cdot(-2)\equiv8(\mathrm{mod}\ 13)$$

$x\equiv8(\mathrm{mod}\ 13)$是该方程的解.

2.4.4 威尔逊定理

威尔逊定理给出了判定素数的充要条件.为此先给出两个引理.

引理 2.3. $x^2 \equiv 1(\mathrm{mod}\ p)$恰好有两个解$x \equiv 1, p-1(\mathrm{mod}\ p)$.

证明 $x^2 \equiv 1(\mathrm{mod}\ p)$是二次同余方程.设$r$是其解,$r^2 - 1 \equiv 0(\mathrm{mod}\ p)$,即$p \mid (r+1)(r-1)$.这里有两种可能：若$p \mid (r+1)$,则$r \equiv p-1(\mathrm{mod}\ p)$;若$p \mid (r-1)$,则$r \equiv 1(\mathrm{mod}\ p)$.

引理 2.4. p为奇素数,a'表示线性同余方程$ax \equiv 1(\mathrm{mod}\ p)$的解,这里$a$可以取值$1, 2, \cdots, p-1$.当$a \not\equiv b(\mathrm{mod}\ p)$时,$a' \not\equiv b'(\mathrm{mod}\ p)$.若$a' \equiv a(\mathrm{mod}\ p)$, 则$a = 1$或$p-1$.

证明 由于a取值$\{1, 2, \cdots, p-1\}, (a, p) = 1$.方程$ax \equiv 1(\mathrm{mod}\ p)$恰好有一个解$a'$.假若$a' \equiv b'(\mathrm{mod}\ p)$,在同余式两边同乘$ab$,$aa'b \equiv ab'b(\mathrm{mod}\ p)$.因$aa' \equiv 1(\mathrm{mod}\ p), bb' \equiv 1(\mathrm{mod}\ p)$,推出$a \equiv b(\mathrm{mod}\ p)$.从而当$a \not\equiv b(\mathrm{mod}\ p)$ 时,必有$a' \not\equiv b'(\mathrm{mod}\ p)$.又若$a' \equiv a(\mathrm{mod}\ p)$,同余式两边同乘$a$,有$a^2 \equiv 1(\mathrm{mod}\ p)$.从引理2.3 知$a \equiv 1(\mathrm{mod}\ p)$或$a \equiv p-1(\mathrm{mod}\ p)$.

定理 2.13. (**威尔逊定理**) p为素数当且仅当$(p-1)! \equiv -1(\mathrm{mod}\ p)$.

证明 p是素数.当$p = 2$时,显然$(2-1)! \equiv -1(\mathrm{mod}\ 2)$.当$p > 2$时.由引理2.4知$a$取值于集合$\{2, 3, \cdots, p-2\}$时,存在$a' \neq a$且$aa' \equiv 1(\mathrm{mod}\ p)$.当$a$取值不同时相应的$a'$也是不同的,从而$2, 3, \cdots, p-2$这$p-3$个数可以把$a$ 与a'组成一对,即

$$2 \cdot 3 \cdots (p-2) \equiv 1(\mathrm{mod}\ p);$$
$$(p-1)! = (p-1) \cdot 2 \cdot 3 \cdots (p-2) \equiv p-1 \equiv -1(\mathrm{mod}\ p)$$

反过来,已知$(n-1)! \equiv -1(\mathrm{mod}\ n)$.令$a$是$n$的因子且$a \neq n$.由$n \mid ((n-1)! + 1)$,得到$a \mid ((n-1)! + 1)$.显然$a \mid (n-1)!$,于是$a \mid 1$.由此推出$a = 1$. 这说明$n$除了自身之外只有因子$1, n$是素数.

2.5 整数的因子及完全数

n为正整数,$d(n)$表示n的正因子数,$\sigma(n)$表示n的正因子之和.显然

$$d(n)=\sum_{d|n}1,\sigma(n)=\sum_{d|n}d.$$

若$n=p_1^{l_1}p_2^{l_2}\cdots p_k^{l_k}$,那么$p_1^{f_1}p_2^{f_2}\cdots p_k^{f_k}(0\leqslant f_i\leqslant l_i,1\leqslant i\leqslant k)$是$n$的正因子.每个$f_i$ 有l_i+1种不同的取值,从而n有$(l_1+1)(l_2+1)\cdots(l_k+1)$个正因子,即

$$\begin{aligned}
d(n)=&\left(l_1+1\right)\left(l_2+1\right)\cdots\left(l_k+1\right),\\
\sigma(n)=&\sum_{\substack{0\leqslant f_i\leqslant l_i\\1\leqslant i\leqslant k}}p_1^{f_1}p_2^{f_2}\cdots p_k^{f_k}\\
=&\sum_{\substack{0\leqslant f_i\leqslant l_i\\1\leqslant i\leqslant k-1}}p_1^{f_1}p_2^{f_2}\cdots p_{k-1}^{f_{k-1}}\left(\sum_{f_k=0}^{l_k}p_k^{f_k}\right)\\
=&\sum_{\substack{0\leqslant f_i\leqslant l_i\\1\leqslant i\leqslant k-1}}p_1^{f_1}p_2^{f_2}\cdots p_{k-1}^{f_{k-1}}\left(\frac{p_k^{l_k+1}-1}{p_k-1}\right)\\
&\cdots\cdots\cdots\cdots\\
=&\frac{p_1^{l_1+1}-1}{p_1-1}\cdot\frac{p_2^{l_2+1}-1}{p_2-1}\cdot\cdots\cdots\frac{p_k^{l_k+1}-1}{p_k-1}.
\end{aligned}$$

不难看出,当$(m,n)=1$时,$\sigma(mn)=\sigma(m)\cdot\sigma(n)$,$d(mn)=d(m)\cdot d(n)$,即$d$和$\sigma$均是积性函数.

定义 2.7. 正整数n为**完全数**当且仅当n等于除自身之外的正因子之和,即$\sigma(n)=2n$.

例如$6=1+2+3$,$28=1+2+4+7+14$,6与28是完全数.对于完全数已经得到了很好的结果.

定理 2.14. p为素数.如果2^p-1也是素数,则$2^{p-1}(2^p-1)$是完全数.

证明 p与2^p-1都是素数,由$2^{p-1}<2^p-1$知,$(2^{p-1},2^p-1)=1$.σ是积性函数且

$$\sigma\left(2^{p-1}\right)=\frac{2^p-1}{2-1}=2^p-1,\quad \sigma\left(2^p-1\right)=\left(2^p-1\right)+1=2^p,$$
$$\sigma(n)=\sigma\left(2^{p-1}\left(2^p-1\right)\right)=\sigma\left(2^{p-1}\right)\sigma\left(2^p-1\right)$$
$$=\left(2^p-1\right)\cdot 2^p=2n.$$

它说明$2^{p-1}(2^p-1)$是完全数.

定理 2.15. n是一个偶完全数,必有$n=2^{p-1}\cdot(2^p-1)$,其中p和2^p-1均为素数.

证明 n为偶完全数,可以表示成$n=2^k\cdot m$,其中$2\nmid m$,$k\geqslant 1$.根据完全数的定义$\sigma(n)=2n$,即

$$2^{k+1}\cdot m=\sigma\left(2^k\cdot m\right)=\sigma\left(2^k\right)\sigma(m)=\left(2^{k+1}-1\right)\cdot(m+l).$$

解出$m=(2^{k+1}-1)\cdot l$,这里l是m的小于m的因子之和并且l本身也是m的因子.所以只能$l=1$.从而$m=2^{k+1}-1,\sigma(m)=m+1$.这说明$m$是素数.假设$k+1$不是素数,$k+1=c\cdot d, m=2^{k+1}-1=2^{c\cdot d}-1=\left(2^c-1\right)\left(2^{c(d-1)}+2^{c(d-2)}+\cdots+1\right)$,这与$m$是素数矛盾,故不可能.所以,$k+1$为素数$p$. 综上分析知$n=2^{p-1}\left(2^p-1\right)$,其中$p$和$2^p-1$均为素数.

形如2^p-1的素数叫作Mersenne数,截至1985年找到的最大Mersenne数为$2^{216091}-1$.目前仅发现51个梅森素数,最大的是$2^{82589933}-1$,有24862048位。

2.6 原根与指数

本节我们要解同余方程$x^n\equiv c(\mathrm{mod}\ m)$.当$(c,m)=1$时,$x_0$是$x^n\equiv c(\mathrm{mod}\ m)$的一个特解,而$y$是$x^n\equiv 1(\mathrm{mod}\ m)$的解,则$x\equiv yx_0(\mathrm{mod}\ m)$是$x^n\equiv c(\mathrm{mod}\ m)$的解.反过来$x^n\equiv c(\mathrm{mod}\ m)$的每个解都可以写成$yx_0$形式,其中$y$是$x^n\equiv 1(\mathrm{mod}\ m)$的解.所以,解同余方程$x^n\equiv c(\mathrm{mod}\ m)$,只要找到一个特解$x_0$,并用$x_0$乘以$x^n\equiv 1(\mathrm{mod}\ m)$的全部解就得到了$x^n\equiv c(\mathrm{mod}\ m)$的全部解.

下面我们就来研究$x^n\equiv 1(\mathrm{mod}\ m)$的解.为此引进阶、原根及指数的概念.

2.6.1 a模m的阶

当$(a,m)=1$时,考虑集合

$$A=\{n \mid n\in \mathbf{Z}且a^n\equiv 1(\mathrm{mod}\ m)\},$$

由欧拉定理知$\phi(m)\in A$且$\phi(m)>0$.那么集合A中一定存在最小正整数l.集合A显然有如下性质:

1° 若$n_1,n_2\in A$,则$n_1\pm n_2\in A$;

2° 若$n\in A,c\in \mathbf{Z}$则$cn\in A$;

3° 集合A是由l的整数倍数组成的,并且只由这些整数倍数组成,即$A=\{k\cdot l \mid k\in \mathbf{Z}\}$.

我们称l为a模m的阶.由集合A的性质知,当$(a,m)=1$时,a模m的阶为l,那么对每个满足$a^n\equiv 1(\mathrm{mod}\ m)$的整数$n$均有$l\mid n$.特别地,$l\mid \phi(m)$.不难看出$a^{n_1}\equiv a^{n_2}(\mathrm{mod}\ m)$当且仅当$n_1\equiv n_2(\mathrm{mod}\ l)$.

推论 2.7. 若$(a,m)=1$,l为a模m的阶,则a^k模m的阶为$\frac{l}{(l,k)}$.

证明 首先看满足$\left(a^k\right)^j\equiv 1(\mathrm{mod}\ m)$的$j$应具有什么性质.从集合$A$的性质知$l\mid k\cdot j$,即

$$\frac{l}{(l,k)}\mid \frac{k}{(l,k)}\cdot j,$$

由于$\left(\frac{l}{(l,k)},\frac{k}{(l,k)}\right)=1$,得到$\frac{l}{(l,k)}\mid j$,$a^k$的阶应是满足该性质最小的正整数,故$a^k$的阶为$\frac{l}{(l,k)}$.

2.6.2 原根

定义 2.8. 若$(g,m)=1$且g模m的阶为$\phi(m)$,则称g为模m的**原根**.

例如,2是模5的原根,$\phi(5)=4,2^4\equiv 1(\mathrm{mod}\ 5)$.3是模7的原根,$\phi(7)=6$,$3^6\equiv 1(\mathrm{mod}\ 7)$.但并不是所有$m$都有原根.例如$m=8,\phi(8)=\phi\left(2^3\right)=4$.$\{1,3,5,7\}$ 是模8的缩系,而1模8的阶为1;3,5,7模8的阶为2.任何与8互素的数均与且仅与$\{1,3,5,7\}$中的一个元素模8 同余,故其模8的阶与该元素相同.由此可知正整数8无原根.

取$0 \leqslant i, j \leqslant \phi(m)-1, i \neq j$,显然$g^i \not\equiv g^j (\bmod\ m)$,$\left\{g^0, g^1, \cdots, g^{\phi(m)-1}\right\}$构成模$m$的缩系.也就是说,$g$是模$m$的原根,每个与$m$互素的$a$均与且仅与某个$g^i$模$m$同余,其中$0 \leqslant i \leqslant \phi(m)-1$.模$m$的原根都在$\left\{g^0, g^1, \cdots, g^{\phi(m)-1}\right\}$中.若$(l, \phi(m)) = 1$,则$g^l$也是模$m$的原根.

下面接下去讨论哪些数有原根,其结论是所有的素数p都有原根,原根个数为$\phi(p-1)$.为此先给出两个引理.

引理 2.5. 若$f(x)$是n次整系数多项式,$f(x) \equiv 0(\bmod\ p)$至多有n个解.

证明 $f(x)$是n次整系数多项式,$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0$,其中$a_n \not\equiv 0(\bmod\ p)$.对$f(x)$的次数$n$进行归纳证明.

当$n = 1$时,$a_1 x + a_0 \equiv 0(\bmod\ p)$且$a_1 \not\equiv 0(\bmod\ p)$,由定理2.7 知该线性同余方程有唯一解.命题成立.

假设$n = k$时,$a_k x^k + a_{k-1}x^{k-1} + \cdots + a_0 \equiv 0(\bmod\ p)$至多有$k$个解.现$n = k+1$.如果$f(x) \equiv 0(\bmod\ p)$无解,显然命题成立.如果$f(x) \equiv 0(\bmod\ p)$至少有一个解$r$,即$f(r) \equiv 0(\bmod\ p)$.

$$\begin{aligned} f(x) &\equiv f(x) - f(r) \\ &= a_{k+1}\left(x^{k+1} - r^{k+1}\right) + a_k\left(x^k - r^k\right) + \cdots + a_1(x-r) \\ &= (x-r)g(x)(\bmod\ p), \end{aligned}$$

其中$a_{k+1} \not\equiv 0(\bmod\ p)$,$g(x)$是$k$次整系数多项式.$f(x) \equiv (x-r)g(x) \equiv 0(\bmod\ p)$的任意解$s$使$(s-r)g(s) = 0(\bmod\ p)$,即$s \equiv r(\bmod\ p)$或$g(s) = 0(\bmod\ p)$,也就是说$s$或是$r$或是$g(s) \equiv 0(\bmod\ p)$的解.由归纳假设知后者至多有$k$个解,所以$f(x)$至多有$k+1$个解.命题对$n = k+1$也成立.

引理 2.6. 若$n \geqslant 1$,则$\sum_{d|n}\phi(d) = n$.

证明 由$d \mid n$知$\frac{n}{d} \mid n$.故$\sum_{d|n}\phi(d) = \sum_{d|n}\phi\left(\frac{n}{d}\right)$.
考虑集合C_d,其中d是n的因子.

$$\begin{aligned} C_d &= \{m \mid 1 \leqslant m \leqslant n \text{ 且} (m, n) = d\} \\ &= \left\{m \mid 1 \leqslant m \leqslant n \text{ 且} \left(\frac{m}{d}, \frac{n}{d}\right) = 1\right\}, \end{aligned}$$

显然$|C_d| = \phi\left(\frac{n}{d}\right)$.$\{1, 2, \cdots, n\}$中每个元素均在且仅在一个$C_d$中,从而

$$n = \sum_{d|n} |C_d| = \sum_{d|n} \phi\left(\frac{n}{d}\right) = \sum_{d|n} \phi(d).$$

例如$n = 6, n$的因子分别为$1, 2, 3, 6$.集合$C_1 = \{1, 5\}, C_2 = \{2, 4\}, C_3 = \{3\}, C_6 = \{6\}$.

定理 2.16. *p为素数,$l \mid (p-1)$.那么模p阶为l的数恰好有$\phi(l)$个.*

证明 对于每个$l \mid (p-1)$,令模p阶为l的元素个数为$\psi(l)$.如果对某个l不存在模p阶为l的元素,那么$\psi(l) = 0$.如果存在a,a与p互素且a模p阶为l,即$a^l \equiv 1(\mathrm{mod}\ p)$.在集合$\left\{a^0, a^1, \cdots, a^{l-1}\right\}$中,由于各个元素的指数模$l$不同余,所以这些元素均模$p$不同余.而对于$0 \leqslant i \leqslant l-1$,

$$\left(a^i\right)^l = \left(a^l\right)^i \equiv 1(\mathrm{mod}\ p),$$

$a^0, a^1, \cdots, a^{l-1}$均是$x^l \equiv 1(\mathrm{mod}\ p)$的解.根据引理2.5,该同余方程至多有$l$个解.这说明$a^0, a^1, \cdots, a^{l-1}$是它的全部解,从推论2.7知$a^k$ 模p阶为l当且仅当$(k, l) = 1$.$\{0, 1, \cdots, l-1\}$中有$\phi(l)$个与l互素的数,所以$\left\{a^0, a^1, \cdots, a^{l-1}\right\}$中有$\phi(l)$个模$p$阶为$l$的数,即$\psi(l) = \phi(l)$.综上知,对任何$l \mid (p-1)$均成立$\psi(l) \leqslant \phi(l)$.

另一方面,根据费马定理$(a, p) = 1, a^{p-1} \equiv 1(\mathrm{mod}\ p)$.若$a$模$p$的阶为$t$,则必有$t \mid (p-1)$.满足该条件的$a$至少有$p-1$个.由前面假设$\psi(l)$是模$p$阶为$l$ 的元素个数.再由引理2.6得到

$$\sum_{l|(p-1)} \psi(l) \geqslant p-1 = \sum_{l|(p-1)} \phi(l).$$

并推出$\psi(l) \geqslant \phi(l)$.

最后得到$\psi(l) = \phi(l)$,即模p阶为l的数恰好有$\phi(l)$个.

特别取$l = \phi(p)$,模p阶为$\phi(p)$的元素个数为$\phi(\phi(p)) = \phi(p-1)$.这说明有$\phi(p-1)$个模$p$的原根.例如37是素数,它的原根数为

$$\begin{aligned}\phi(\phi(37)) = \phi(36) &= \phi\left(2^2\right)\phi\left(3^2\right) \\ &= 2^1 \cdot (2-1) \cdot 3^1(3-1) = 12.\end{aligned}$$

通过简单计算知1是2的原根,3是4的原根,可以证明:m有原根当且仅当$m = 2$, 4, $p^k, 2 \cdot p^k$,其中p是奇素数,k为正整数.再次说明8没有原根.

2.6.3 指数

设g为模p的原根,$\{g^0, g^1, \cdots, g^{p-2}\}$为模$p$的缩系.对每个整数$n$,若$(n,p)=1$,则存在$m, 0 \leqslant m \leqslant p-2$,使得$n \equiv g^m (\mathrm{mod}\ p)$成立.我们称$m$为$n$(对于原根$g$)的模$p$指数,并记为$\mathrm{ind}_g\, n$.

若有l使$n \equiv g^l (\mathrm{mod}\ p)$,而$n \equiv g^{\mathrm{ind}\ _g n} (\mathrm{mod}\ p)$,所以$l \equiv \mathrm{ind}_g\, n (\mathrm{mod}\ p-1)$.

模p指数有如下性质:

1° $p \nmid ab, \mathrm{ind}_g\, ab \equiv \mathrm{ind}_g\, a + \mathrm{ind}_g\, b (\mathrm{mod}\ p-1)$;

2° $p \nmid a, \mathrm{ind}_g\, a^l \equiv l \cdot ind_g a\, (\mathrm{mod}\ p-1)$.

这些性质从指数的定义很容易证出.不难看出模p指数与对数函数有相类似的性质.

定理 2.17. 若$(n,p)=1, g$为模p的原根,则同余方程$x^k \equiv n\, (\mathrm{mod}\ p)$有解当且仅当$(k, p-1) \mid \mathrm{ind}_g\, n$.当条件满足时,该方程有$(k, p-1)$个解.

证明 令$y = \mathrm{ind}_g\, x, x \equiv g^y\, (\mathrm{mod}\ p)$ 代入$x^k \equiv n\, (\mathrm{mod}\ p)$得到$g^{yk} \equiv g^{\mathrm{ind}_g\, n}\, (\mathrm{mod}\ p)$,即$yk \equiv \mathrm{ind}_g\, n\, (\mathrm{mod}\ p-1)$. 该方程有解$y$当且仅当$(k, p-1) \mid ind_g n$,并且条件满足时有$(k, p-1)$个解.它们是

$$y \equiv y_1, y_2, \cdots, y_{(k,p-1)}\, (\mathrm{mod}\ p-1).$$

那么$x \equiv g^{y_1}, g^{y_2}, \cdots, g^{y_{(k,p-1)}}\, (\mathrm{mod}\ p)$是$x^k \equiv n\, (\mathrm{mod}\ p)$的解.

例 2.10. 解同余方程$x^8 \equiv 3\, (\mathrm{mod}\ 11)$.

解 查原根指数表知11的最小原根是2, 3对于原根2的模11指数是8,令$y = \mathrm{ind}_2\, x$,先解$8 \cdot y = \mathrm{ind}_2\, 3 = 8\, (\mathrm{mod}\ 10)$.因$(8, 10) = 2$,该线性同余方程有2个模10不同余的解,它们是

$$y \equiv 1, 6\, (\mathrm{mod}\ 10),$$

由此得到$x \equiv 2^1, 2^6 \equiv 2, 9\, (\mathrm{mod}\ 11)$,它们是$x^8 \equiv 3\, (\mathrm{mod}\ 11)$的解.

例 2.11. 解线性同余方程$5x \equiv 7\, (\mathrm{mod}\ 11)$.

解 由$5x \equiv 7\, (\mathrm{mod}\ 11)$,以及11的最小原根为2知

$$\operatorname{ind}_2 5 + \operatorname{ind}_2 x \equiv \operatorname{ind}_2 7 \pmod{10}.$$

从原根指数表知$\operatorname{ind}_2 5 = 4, \operatorname{ind}_2 7 = 7$,代入上式得到$\operatorname{ind}_2 x \equiv 3 \pmod{10}$,故$x \equiv 8 \pmod{11}$是原同余方程的解.

例 2.12. 解同余方程$x^8 \equiv 3 \pmod{143}$.

解 因$143 = 11 \cdot 13$.要解$x^8 \equiv 3 \pmod{143}$就是要解同余方程组

$$\begin{cases} x^8 \equiv 3 \pmod{11} \\ x^8 \equiv 3 \pmod{13}. \end{cases}$$

由例2.10知$x^8 \equiv 3 \pmod{11}$的解为$x \equiv 2, 9 \pmod{11}$.用例2.10中的方法解出$x^8 \equiv 3 \pmod{13}$的解为$x \equiv 4, 6, 7, 9 \pmod{13}$.

下面求解

$$\begin{cases} x \equiv a \pmod{11} \\ x \equiv b \pmod{13}, \end{cases}$$

其中$a = 2, 9; b = 4, 6, 7, 9$.求解方法在2.3.4小节中已详述过,这里只给出结果$x = 13 \cdot 6 \cdot a + 11 \cdot 6 \cdot b \pmod{143}$.代入$a, b$的值,得到

$$x = \pm 9, \pm 20, \pm 35, \pm 46 \pmod{143}.$$

目前对给定素数p如何求出模p的原根尚无一般的方法.另外,给定一个整数a,它是哪些素数的原根也没有一般的方法.在使用时可在一般的数论书中查到小素数的原根及相应的指数表.表2.1给出了50以内的素数的最小原根及相应的指数.该表中第一行列出50以内的全部素数p,第一列是正整数n.素数p相应列中数值为1的元素对应的n值则是该素数的最小原根g,该列的其他元素则是$\operatorname{ind}_g n$.

表 2.1: 素数$p(\leqslant 50)$的最小原根和指数表

$\mathrm{ind}_g n$ n \ p	3	5	7	11	13	17	19	23	29	31	37	41	43	47
1	0	0	0	0	0	0	0	0	0	0	0	0	0	0
2	1	1	2	1	1	14	1	2	1	24	1	26	27	18
3		3	1	8	4	1	13	16	5	1	26	15	1	20
4		2	4	2	2	12	2	4	2	18	2	12	12	36
5			5	4	9	5	16	1	22	20	23	22	25	1
6			3	9	5	15	14	18	6	25	27	1	28	38
7				7	11	11	6	19	12	28	32	39	35	32
8				3	3	10	3	6	3	12	3	38	39	8
9				6	8	2	8	10	10	2	16	30	2	40
10				5	10	3	17	3	23	14	24	8	10	19
11					7	7	12	9	25	23	30	3	30	7
12					6	13	15	20	7	19	28	27	13	10
13						4	5	14	18	11	11	31	32	11
14						9	7	21	13	22	33	25	20	4
15						6	11	17	27	21	13	37	26	21
16						8	4	8	4	6	4	24	24	26
17							10	7	21	7	7	33	38	16
18							9	12	11	26	17	16	29	12
19								15	9	4	35	9	19	45
20								5	24	8	25	34	37	37
21								13	17	29	22	14	36	6
22								11	26	17	31	29	15	25
23									20	27	15	36	16	5
24									8	13	29	13	40	28
25									16	10	10	4	8	2

表 2.2: 续表2.1

$\text{ind}_g n$ n \ p	3	5	7	11	13	17	19	23	29	31	37	41	43	47
26									19	5	12	17	17	29
27									15	3	6	5	3	14
28									14	16	34	11	5	22
29										9	21	7	41	35
30										15	14	23	11	39
31											9	28	34	3
32											5	10	9	44
33											20	18	31	27
34											8	19	23	34
35											19	21	18	33
36											18	2	14	30
37												32	7	42
38												35	4	17
39												6	33	31
40												20	22	9
41													6	15
42													21	24
43														13
44														43
45														41
46														23

习题

1. 证明:

(1) 若$a|b, a>0$,则$(a,b)=a$;

(2) $((a,b),b)=(a,b)$.

2. 证明:

(1) 对所有$n>0$成立$(n,n+1)=1$;

(2) 当$n>0$时,$(n,n+k)$可取什么值?

3. 求x和y使得:

(1) $314x+159y=1$;

(2) $3141x+1592y=1$.

4. 证明: 对于所有$n>0$,有$6 \mid \left(n^3-n\right)$.

5. 证明: 若对于某个m有$10 \mid (3^m+1)$,则对所有$n>0, 10 \mid \left(3^{m+4n}+1\right)$.

6. 求2345及3456两个数的素数分解式.

7. 证明: 当$n>0$时,$n(n+1)$不是一个平方数.

8. 令$n=5!+1$,证明$n+1, n+2, n+3, n+4$均为合数.

9. 求下列方程的所有整数解

(1) $x+y=2$;

(2) $2x+y=2$;

(3) $15x+16y=17$.

10. 求下列方程的负整数解:

(1) $6x-15y=51$;

(2) $6x+15y=51$.

11. 用30张票面值为5分、1角、2角5分的纸币,换5元钱.问有多少种不同的兑换方法?

12. 某人用0.99元买了苹果和桔子共12个,每只苹果比每只桔子贵3分钱,买的苹果数多于桔子数.问苹果和桔子各买多少个?

13. 若$k \equiv 1 \pmod 4$,则$6k+5$模4等于多少?

14. 证明: 每个大于3的素数模6或与1同余或与5同余.

15. 证明: 相继的两个立方数之差不能被3整除.

16. 证明: 若一个整数的各位数字之和能被3整除,那么该数也能被3整除.

17. 证明:

(1) $10^k \equiv (-1)^k \pmod{11}, k = 0, 1, 2, \cdots$;

(2) 推导出一个整数能被11整除的判别法.

18. 解下列线性同余方程:

(1) $2x \equiv 1 \pmod{17}$; (2)$3x \equiv 6 \pmod{18}$;

(3) $4x \equiv 6 \pmod{18}$; (4)$3x \equiv 1 \pmod{17}$.

19. 解下列同余方程组:

(1) $\begin{cases} x \equiv 1 \pmod{2} \\ x \equiv 1 \pmod{3} \end{cases}$ (2) $\begin{cases} x \equiv 31 \pmod{41} \\ x \equiv 59 \pmod{26} \end{cases}$

(3) $\begin{cases} x \equiv 1 \pmod{2} \\ x \equiv 1 \pmod{3} \\ x \equiv 6 \pmod{7} \end{cases}$ (3) $\begin{cases} 2x \equiv 1 \pmod{5} \\ 3x \equiv 2 \pmod{7} \\ 4x \equiv 1 \pmod{11} \end{cases}$

20. 试求同时满足如下两条要求的正整数x, y, z:

(1) 它们分别乘以3, 5, 7所得乘积模20的余数是公差为1的算术级数;

(2) 它们分别乘以3, 5, 7所得乘积除以20得到的商分别等于(1) 中的相应的余数.

21. 求满足$2 \mid n, 3 \mid (n+1), 4 \mid (n+2), 5 \mid (n+3), 6 \mid (n+4)$的最小整数$n(> 2)$.

22. 计算$\phi(42), \phi(420), \phi(4200)$.

23. 小于18且与18互素的正整数是哪些? 当$m = 18, a = 5$时,验证引理2.1.

24. p为素数,$(m, n) = p$,问$\phi(mn)$与$\phi(m)\phi(n)$之间有什么关系?

25. 证明:

(1) 如果$6 \mid n$,则$\phi(n) \leqslant \frac{n}{3}$;

(2) 如果$n-1$和$n+1$均为素数,$n > 4$,则$\phi(n) \leqslant \frac{n}{3}$.

26. (1) 验证$1+2 = \frac{2}{3}\phi(3), 1+3 = \frac{4}{2}\phi(4), 1+2+3+4 = \frac{5}{2}\phi(5), 1+5 = \frac{6}{2}\phi(6), 1+2+3+4+5+6 = \frac{7}{2}\phi(7), 1+3+5+7 = \frac{8}{2}\phi(8)$;

(2) 推想一个定理;

(3) 证明你的定理.

27. 314^{159}除以7的余数是多少?

28. 7^{355}的末位数是什么? 末两位数是什么?

29. p为素数.证明: 对非负整数$k, (k+1)^p - k^p \equiv 1 \pmod{p}$,并由此推出费马定理.

30. 假设p是一个奇素数.证明:

(1) $1^{p-1} + 2^{p-1} + \cdots + (p-1)^{p-1} \equiv -1 \pmod{p}$;

(2) $1^p + 2^p + \cdots + (p-1)^p \equiv 0 \pmod{p}$.

31. 计算$d(42), d(420), d(4200), \sigma(42), \sigma(420), \sigma(4200)$.

32. 求具有60个因子的数n $\left(n < 10^4\right)$.

33. 证明

$$\sum_{d|n} \frac{1}{d} = \frac{1}{n}\sigma(n).$$

34. 证明所有的偶完全数以6或8结尾.

35. 若n为偶完全数,$n > 6$,证明$n \equiv 1 \pmod{9}$.

36. 证明

$$\sum_{p \leqslant x} \sigma(p) = \sum_{p \leqslant x} \phi(p) + \sum_{p \leqslant x} d(p).$$

37. 求$2, 4, 7, 8, 11, 13, 14$模15的阶是多少?

38. (1) 算出关于原根2的最小指数$\pmod{29}$;

(2) 利用此表解$9x \equiv 2 \pmod{29}$;

(3) 利用此表解$x^9 \equiv 2 \pmod{29}$.

39. $457^{911} \equiv 1 \pmod{10021}$对不对? (这里$457, 911$都是素数,$10021 = 11 \cdot 911$.)

40. 求37的12个原根.

41. 证明: 若p, q为奇素数,$q \mid (a^p + 1)$,则有$q \mid (a+1)$或$q \mid (2kp+1)$,其中k为某个整数.

42.证明: 若a模p的阶为3,则$a+1$模p的阶为6.

第 3 章 映射

3.1 映射的基本知识

定义 3.1. 设A与B为任意两个集合，如果有一个确定的规律（或法则）f，使得任给$a \in A$，f将a 对应到B中唯一的一个元素$b \in B$，则称f为集合A到集合B的一个映射，记作$f : A \to B$或$A \xrightarrow{f} B$。

定义 3.2. 设f为集合A到集合B的一个映射，任给$a \in A$，如果f将a对应到$b \in B$，则称b为a在映射f作用下的像，记作$f(a) = b$；称a为b的原像。

从映射的定义可以看出，集合A中的每个元素在映射f的作用下都有像，而B中的元素则有可能没有原像。同时，集合A中不同元素的像可能相同，而B中不同元素的原像则一定不同。

如果A与B是数的集合，如复数集合、实数集合或整数集合等，那么从A到B的映射就是通常的函数。可见，映射的概念是函数概念的推广。如果A是多个集合的笛卡尔积，比如说$A = A_1 \times A_2 \times \cdots \times A_n$，而$f$是$A$到$B$的映射，设$(a_1, a_2, \cdots, a_n) \in A_1 \times A_2 \times \cdots \times A_n$在$f$作用下的像为$b \in B$，则记为$f(a_1, a_2, \cdots, a_n) = b$，这类的映射对应于我们常见的多元函数。

设f是A到B的一个映射，且$f(a) = b$，我们也可以记作$(a, b) \in f$，也就是说，将映射f 看作是所有原像与像构成的有序二元组的集合，即$f = \{(a, b)|a \in A$且$f(a) = b\}$。所以，映射f可以看作是$A \times B$的子集，即$f \subseteq A \times B$。因为任给$a \in A$，a的像唯一，所以若$(a, b) \in f$且$(a, c) \in f$，则一定有$b = c$。

定义 3.3. 设$f : A \to B$，集合A中所有元素在f作用下的像所构成的集合称为f的值域，记作R_f，即

$$R_f = \{f(a)|a \in A\}.$$

显然有$R_f = \{b|b \in B$，且存在$a \in A$，使得$f(a) = b\} \subseteq B$。

定义 3.4. 设$f : A \to B$，$g : A \to B$，如果对任意$a \in A$，都满足$f(a) = g(a)$，则称映射f与g相等，记作$f = g$。

例 3.1. 设有两个集合$A=\{a_1,a_2,a_3,a_4\}$、$B=\{b_1,b_2,b_3\}$。如果有一个规则f，f将a_1与a_2对应到b_2，而将a_3与a_4对应到b_1，则f为A到B的映射，其中$f(a_1)=f(a_2)=b_2$，$f(a_3)=f(a_4)=b_1$，$R_f=\{b_1,b_2\}$。

例 3.2. 设有两个集合$A=\{a_1,a_2,a_3\}$，$B=\{b_1,b_2,b_3\}$，

(1) 如果有一个规则f，f将a_1对应到b_1和b_2，a_2对应到b_2，a_3对应到b_3，则f不是映射，这是因为f将a_1对应到两个不同的元素b_1和b_2。

(2) 如果有一个规则g，g将a_1对应到b_2，a_2对应到b_1，但a_3没有对应的元素，则g不是映射，这是因为a_3在B中没有对应的元素。

(3) 如果有一个规则h，h将a_1对应到b_2，a_2对应到b_1，a_3对应到某个元素$c\notin B$，则h不是A到B映射，这是因为a_3对应的元素c不在B中。

有了定义3.4，我们可以判断两个映射是否相等。那么，给定两个有限集合A 与B，从A到B到底有多少个不相等的映射呢? 下面的定理给出了答案。

定理 3.1. 给定两个有限集合A与B，从A到B的映射共有$|B|^{|A|}$个.

证明: A、B是有限集合，假设$A=\{a_1,a_2,\cdots,a_n\}$，$B=\{b_1,b_2,\cdots,b_m\}$，也意味着$|A|=n$、$|B|=m$。设f是A到B的映射，则f与n维向量

$$(f(a_1),f(a_2),\cdots,f(a_n))$$

一一对应。而$f(a_1)$可以是B中元素$b_1,b_2,\cdots,b_m$的任意一个，有m种可能。同理，$f(a_2)$ 有m种可能，...，$f(a_n)$有m种可能。所以，A到B的映射共有$\overbrace{m\times m\times\cdots\times m}^{n个}=m^n=|B|^{|A|}$ 个。证毕。

例 3.3. 设$A=\{a_1,a_2\}$、$B=\{b_1,b_2,b_3\}$。则从A到B的映射共有$|B|^{|A|}=3^2=9$ 个。参见表*3.1*。

而从B到A的映射共有$|A|^{|B|}=2^3=8$ 个。参见表3.2。

表 3.1: 从A到B的9个映射

像 函数 / 原像	f_1	f_2	f_3	f_4	f_5	f_6	f_7	f_8	f_9
a_1	b_1	b_1	b_1	b_2	b_2	b_2	b_3	b_3	b_3
a_2	b_1	b_2	b_3	b_1	b_2	b_3	b_1	b_2	b_3

表 3.2: 从B到A的8个映射

像 函数 / 原像	g_1	g_2	g_3	g_4	g_5	g_6	g_7	g_8
b_1	a_1	a_2	a_1	a_1	a_2	a_2	a_1	a_2
b_2	a_1	a_1	a_2	a_1	a_2	a_1	a_2	a_2
b_3	a_1	a_1	a_1	a_2	a_1	a_2	a_2	a_2

3.2 特殊映射

本节介绍几种具有特殊性质的映射，它们在以后各章节中起到重要作用。

定义 3.5. 设$f : A \to A$。若对任意$a \in A$，均有$f(a) = a$，则称映射f为A上的恒等映射，记为$f = I_A$。

定义 3.6. 设$f : A \to B$，

(1) 如果$R_f = B$；即任给$b \in B$，存在$a \in A$，使得$f(a) = b$，则称f为满射。

(2) 任给$a_1, a_2 \in A$，若$a_1 \neq a_2$，则有$f(a_1) \neq f(a_2)$，则称f为单射。也即，设f是单射，则若$f(a_1) = f(a_2)$，一定有$a_1 = a_2$。

(3) 如果f既是单射，也是满射，则称f是一一映射或双射。

设f为集合A到集合B的映射，任取A的子集S，定义S的像集为

$$f(S) = \{f(x)|x \in S\}.$$

特别，当$S = \emptyset$时，$f(S) = \emptyset$；当$S = A$时，$f(A)$叫作映射f的像集，记作$Im(f)$. 若我们将集合B换成$Im(f)$，将f看作是从集合A到集合$Im(f)$的映射，则$f : A \to Im(f)$是满射。

定义 3.7. 设f为集合A到集合B的双射。因为f是满射，所以任给$b \in B$，存在$a \in A$，使得$f(a) = b$。据此我们定义一个从集合B中元素到集合A中元素的对应规则f^{-1}，使得任给$b \in B$，若$f(a) = b$，则f^{-1} 将b对应到a。

定理 3.2. 设f为集合A到集合B的双射，则如上定义的f^{-1}为集合B到集合A的双射。

证明: 首先证明f^{-1}为集合B到集合A的映射。任给$b \in B$，因为f是满射，所以存在$a \in A$，使得$f(a) = b$，而且又因为f是单射，仅有唯一

的$a \in A$，使得$f(a) = b$。所以，f^{-1}将B中任意一个元素对应到A中唯一的一个元素，因此f^{-1}是集合B到集合A的映射。

接下来证明f^{-1}是单射。用反证法。任给$b_1, b_2 \in B$，且$b_1 \neq b_2$，假设$f^{-1}(b_1) = f^{-1}(b_2) = a \in A$。由$f^{-1}$的定义知，有$f(a) = b_1$且$f(a) = b_2$. 而$b_1 \neq b_2$，意味着$f$将$a \in A$对应到$B$中两个不同的元素$b_1$和$b_2$，与$f$是映射矛盾。故$f^{-1}$是单射。

最后证明f^{-1}是满射。任给$a \in A$，因为f是映射，所以存在$b \in B$，使得$f(a) = b$，由f^{-1}的定义知，有$f^{-1}(b) = a$。所以f^{-1}是满射。

综上可知，f^{-1}为集合B到集合A的双射。证毕。

事实上，由映射的有序二元组集合的表示方式，我们可以将f表示成$f = \{(a, b)|a \in A \text{ 且} f(a) = b\}$。若$f$是双射，则$f^{-1} = \{(b, a)|(a, b) \in f\}$。

定理 3.3. 设A与B是有限集合，则存在从A到B的满射的充要条件是$|A| \geq |B|$。

证明： 设f是从A到B的满射，则集合B中每个元素在A中都有一个原像。由映射的定义知，B中不同的元素在A 中的原像一定不同，而且B中的一个元素在A中可能有多个原像。因此，集合A中的元素个数一定大于等于集合B中的元素个数，即$|A| \geq |B|$。

反之，假设A、B都是有限集合，且$|A| \geq |B|$。记$A = \{a_1, a_2, \cdots, a_m\}$，$B = \{b_1, b_2, \cdots, b_n\}$，则$m \geq n$。我们定义一个映射$f : A \to B$，

$$f(a_i) = \begin{cases} b_i & 1 \leq i < n \\ b_n & n \leq i \leq m. \end{cases}$$

则任给$b_i \in B(1 \leq i \leq n)$，都存在$a_i \in A(1 \leq i \leq n)$，使得$f(a_i) = b_i$，$f$是$A$到$B$的满射。所以，从集合$A$到集合$B$存在满射。证毕。

定理 3.4. 设A与B是有限集合，则从A到B存在双射的充要条件是$|A| = |B|$。

证明： 如果从A到B存在双射，设为f。一方面，因为f是满射，由定理3.3知，$|A| \geq |B|$。另一方面，因为f为双射，由定理3.2知，存在

从B到A的逆映射f^{-1}，而且f^{-1}为双射，是满射。由定理3.3知，$|B| \geq |A|$。因此，$|A| = |B|$。

如果$|A| = |B|$，设$|A| = |B| = n$，$A = \{a_1, a_2, \cdots, a_n\}$，$B = \{b_1, b_2, \cdots, b_n\}$。定义一个函数$f$，使得对于$1 \leq i \leq n$，$f(a_i) = b_i$，则易知$f$是双射。证毕。

定理 3.5. 设A与B是有限集合，且$|A| = |B| = n$，则从A到B有$n!$个不同的双射。

证明： 设$A = \{a_1, a_2, \cdots, a_n\}$，$B = \{b_1, b_2, \cdots, b_n\}$，$f$为$A$到$B$的双射。首先，$f(a_1)$可以是$B$ 中的任意一个元素，所以有n个选择；而后，由于f 是双射，$f(a_2) \neq f(a_1)$，在$f(a_1)$确定后，$f(a_2)$不能取与$f(a_1)$相同的元素，只能取$B - \{f(a_1)\}$中的某个元素，有$n-1$种选择；同理，在$f(a_1)$、$f(a_2)$ 确定后，$f(a_3)$有$n-2$种选择；...；最后，在$f(a_1)$、$f(a_2)$、...、$f(a_{n-1})$确定后，$f(a_n)$只有一种选择。因此，从A到B 的双射有$n \times (n-1) \times \cdots \times 1 = n!$个。

事实上，从A到B的双射与B的全排列一一对应。若f是A到B的双射，则$f(a_1)f(a_2)\cdots f(a_n)$是$B$中元素的一个全排列；反之，给定$B$的全排列$b_{j_1}b_{j_2}\cdots b_{j_n}$，我们定义映射$f : A \to B$，使得$f(a_i) = b_{j_i}(1 \leq i \leq n)$，则$f$是$A$到$B$的一一映射。所以，从$A$到$B$的双射个数等于$B$的全排列数，为$n!$。证毕。

例 3.4. 设A、B分别是整数集合与偶数集合，则B是A的真子集。定义映射$f : A \to B$，任给$n \in A$，$f(n) = 2n$，则易知，f是从A到B的双射。这个例子说明了，对于无限集合来说，可能存在到其真子集的双射。但是，由定理*3.4*知，对于有限集合来说，这是不可能的。

例 3.5. 设R为实数集合，定义映射$f : R \times R \to R$，$f((x, y)) = x \times y$，则f是满射，但f不是单射。例如，$f((2, 3)) = 2 \times 3 = 6$，也有$f((1, 6)) = 1 \times 6 = 6$。

例 3.6. 设$S = \{1, 2, 3\}$，$\mathscr{P}(S) = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}\}$为$S$的幂集，定义集合的并运算$\cup : \mathscr{P}(S) \times \mathscr{P}(S) \to \mathscr{P}(S)$。任给$A \subseteq S$、$B \subseteq S$，$\cup((A, B)) = A \cup B$，则任给$A \in \mathscr{P}(S)$，$(\emptyset, A) \in$

$\mathscr{P}(S)\times\mathscr{P}(S)$，$\cup((\emptyset,A))=\emptyset\cup A=A$，所以，$\cup$是$\mathscr{P}(S)\times\mathscr{P}(S)$到$\mathscr{P}(S)$的满射，但不是单射，例如，$\{1,2\}\cup\{2,3\}=\{1\}\cup\{1,2,3\}=\{1,2,3\}$。

同理，集合的交运算也具有与并运算相同的性质，而补运算则是$\mathscr{P}(S)$到$\mathscr{P}(S)$的双射。

例 3.7. 设$A=\{a_1,a_2,\cdots,a_n\}$，$B=\{0,1\}$，$\mathscr{P}(A)$为A的幂集，定义$f:\mathscr{P}(A)\to B^n=\overbrace{B\times B\times\cdots\times B}^{n}$，任给$C\in\mathscr{P}(A)$，即$C\subseteq A$，定义$f(C)=(b_1,b_2,\cdots,b_n)$，其中，对于$1\le i\le n$，

$$b_i=\begin{cases}0 & a_i\notin C,\\ 1 & a_i\in C.\end{cases}$$

则f是集合A的幂集$\mathscr{P}(A)$到集合B^n的一个映射，而且是双射。

任取B^n的一个元素$(b_1,b_2,\cdots,b_n)$，$b_i\in B$，$1\le i\le n$，构造集合$C=\{a_i|a_i\in A,b_i=1\}$，显然C是A的子集，即$C\in\mathscr{P}(A)$，并且

$$f(C)=(b_1,b_2,\cdots,b_n).$$

即C是$(b_1,b_2,\cdots,b_n)$的原像。所以，f是满射。

假设，A的子集C_1与C_2都是$(b_1,b_2,\cdots,b_n)$的原像。任给$a_i\in A$，若$a_i\in C_1$，则由$(b_1,b_2,\cdots,b_n)$的定义可知，$b_i=1$，进而可知，$a_i\in C_2$，所以$C_1\subseteq C_2$。同理，$C_2\subseteq C_1$。所以，$C_1=C_2$。即$(b_1,b_2,\cdots,b_n)$只有一个原像，所以f是单射。

综上可知，f是集合$\mathscr{P}(A)$到集合B^n的双射。

3.3 映射的复合

定义 3.8. 设f是集合A到集合B的映射，而g是集合B到集合C的映射。任给$a\in A$，设$f(a)=b\in B$，进一步有$g(b)=c\in C$。也就是，连续执行映射f与g，就将A中的元素对应到C 中的元素，构成了一个新的映射，叫作f与g的复合映射，记作$g\circ f$ （参见图*3.1*）。注意，这里将f 写在复合映射的右边，表示先执行映射f，然后在执行映射g。于是，对于$a\in A$，有

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

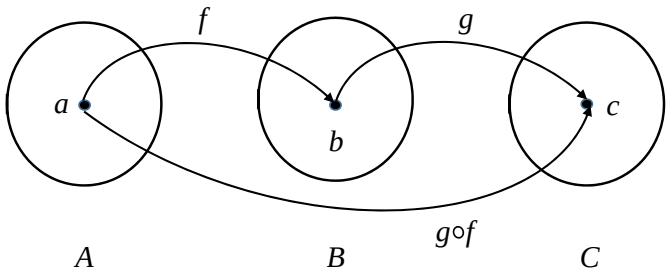


图 3.1: 复合映射的示意图

如果A、B、C都是数的集合，如复数集合、实数集合或整数集合等，那么f与g就是通常的函数，复合映射$g \circ f$就是复合函数。

下面讨论复合映射的性质。

定理 3.6. 设f是集合A到集合B的双射，因此存在逆映射$f^{-1} : B \to A$，那么$f^{-1} \circ f = I_A$，$f \circ f^{-1} = I_B$。

证明: 因为$f : A \to B$，任取$a \in A$，设$f(a) = b$，则$b \in B$。由于f是双射，所以有逆映射f^{-1}，$f^{-1}(b) = a$。从而有

$$f^{-1} \circ f(a) = f^{-1}(f(a)) = f^{-1}(b) = a.$$

所以，双射f与其逆映射f^{-1}的复合映射就是A上的恒等映射，即$f^{-1} \circ f = I_A$。同理可证，$f \circ f^{-1} = I_B$。证毕。

定理 3.7. 映射的复合运算满足结合律。

证明: 设$f : A \to B$、$g : B \to C$、$h : C \to D$，要证明

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

首先看到，$(h \circ g) \circ f$和$h \circ (g \circ f)$都是从集合A到集合D的映射。任取$a \in A$，设$f(a) = b$、$g(b) = c$、$h(c) = d$，其中$b \in B$、$c \in C$、$d \in D$。由复合映射的定义，可以得出

$$(h \circ g) \circ f(a) = (h \circ g)(f(a)) = (h \circ g)(b) = h(g(b)) = h(c) = d;$$

$$h \circ (g \circ f)(a) = h(g \circ f(a)) = h(g(f(a))) = h(g(b)) = h(c) = d.$$

因此，$(h \circ g) \circ f(a) = h \circ (g \circ f)(a)$。因为对任意$a \in A$，都满足$(h \circ g) \circ f(a) = h \circ (g \circ f)(a)$，所以$(h \circ g) \circ f = h \circ (g \circ f)$。证毕。

定理 3.8. 设$f : A \to B$、$g : B \to C$，

(1) 若f与g都是满射，则$g \circ f$也是满射。

(2) 若f与g都是单射，则$g \circ f$也是单射。

(3) 若f与g都是双射，则$g \circ f$也是双射，并且$g \circ f$的逆映射是$(g \circ f)^{-1} = f^{-1} \circ g^{-1}$。

证明： 因为$f : A \to B$、$g : B \to C$，所以复合映射是$g \circ f : A \to C$。

(1) 任取$c \in C$，因为$g : B \to C$是满射，所以存在$b \in B$，使得$g(b) = c$。又因为$f : A \to B$ 是满射，所以存在$a \in A$，使得$g(a) = b$。所以

$$g \circ f(a) = g(f(a)) = g(b) = c.$$

也就是说，对于映射$g \circ f$来说，a是c的原像，所以$g \circ f$是满射。

(2) 留作习题。

(3) 由(1)与(2)知，若f与g都是双射时，$g \circ f$也是双射。下面证明：$(g \circ f)^{-1} = f^{-1} \circ g^{-1}$。

首先，因为$f : A \to B$、$g : B \to C$，所以$g \circ f : A \to C$，$(g \circ f)^{-1} : C \to A$。而$f^{-1} : B \to A$、$g^{-1} : C \to B$，所以也有$f^{-1} \circ g^{-1} : C \to A$。任取集合$C$中元素$c$，因为$g$是满射，存在$b \in B$，使得$g(b) = c$，又因为$f$ 是满射，存在$a \in A$，使得$f(a) = b$。由复合映射的定义，有

$$f^{-1} \circ g^{-1}(c) = f^{-1}(g^{-1}(c)) = f^{-1}(b) = a.$$

另一方面，由于

$$g \circ f(a) = g(f(a)) = g(b) = c,$$

可知$(g \circ f)^{-1}(c) = a$。因为c为C中任意一个元素，所以

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

证毕。

3.4 置换

本节介绍一种特殊的双射–有限集合到其自身的双射，称之为置换。置换在本课程以及组合数学中都有重要的作用。

3.4.1 置换的定义与性质

定义 3.9. 设A是有限集合，从A到其自身的双射称为集合A上的置换。若$|A| = n$，则A上的置换称为n 元置换。

设$A = \{a_1, a_2, \cdots, a_n\}$，则$A$上的$n$元置换$\sigma$可以表示成

$$\sigma = \begin{pmatrix} a_1 & a_2 & \dots & a_n \\ \sigma(a_1) & \sigma(a_2) & \dots & \sigma(a_n) \end{pmatrix}.$$

由于置换σ是A上的双射，所以对于$i \neq j$，有$\sigma(a_i) \neq \sigma(a_j)$。事实上，$\sigma(a_1)\sigma(a_2)\dots\sigma(a_n)$是$A$中元素的全排列，所以集合$A$上的置换与$A$中元素的全排列一一对应。特别地，称$A$上的恒等映射为恒等置换，记为

$$\sigma_I = \begin{pmatrix} a_1 & a_2 & \dots & a_n \\ a_1 & a_2 & \dots & a_n \end{pmatrix}.$$

例 3.8. 设$A = \{1,2,3,4,5\}$，$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 1 & 4 & 3 \end{pmatrix}$，其中$\sigma(1) = 2, \sigma(2) = 5, \sigma(3) = 1, \sigma(4) = 4, \sigma(5) = 3$。25143是$A$中元素的全排列。

在研究集合A上的置换时，我们主要关心A中元素间的对应关系，并不关心具体的元素是什么。所以，在介绍置换及其性质时，我们就用$A = \{1, 2, \cdots, n\}$表示一般的n元集合。由于A上的置换σ与A中元素的全排列$\sigma(a_1)\sigma(a_2)\dots\sigma(a_n)$一一对应，所以$n$元置换有$n!$个。

由定理3.2知，双射存在逆映射，而且其逆映射也是双射。由于置换是双射，所以置换存在逆映射，称为逆置换。假设σ是置换，

$$\sigma = \begin{pmatrix} a_1 & a_2 & \dots & a_n \\ \sigma(a_1) & \sigma(a_2) & \dots & \sigma(a_n) \end{pmatrix},$$

则其逆置换为

$$\sigma^{-1}=\begin{pmatrix}\sigma(a_1) & \sigma(a_2) & \dots & \sigma(a_n)\\ a_1 & a_2 & \dots & a_n\end{pmatrix}.$$

例 3.9. 求$\sigma=\begin{pmatrix}1&2&3&4&5\\2&5&1&4&3\end{pmatrix}$的逆置换。

解: $\sigma^{-1}=\begin{pmatrix}1&2&3&4&5\\2&5&1&4&3\end{pmatrix}^{-1}=\begin{pmatrix}2&5&1&4&3\\1&2&3&4&5\end{pmatrix}=\begin{pmatrix}1&2&3&4&5\\3&1&5&4&2\end{pmatrix}$。
事实上，只需要将σ的两行互换，再将第一行从1到n排好序，第二行做与第一行相同的排序就可以了。

例 3.10. 求$A=\{1,2,3\}$上所有的置换。

解: $|A|=3$，所以A上置换有$3!=6$个，它们是

$$\sigma_1=\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix},\ \sigma_2=\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix},\ \sigma_3=\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix},$$

$$\sigma_4=\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix},\ \sigma_5=\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix},\ \sigma_6=\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}。$$

其中，σ_1是恒等映射。A上置换与A中元素的全排列一一对应。例如，$\sigma_5=\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}$对应的全排列是321，也就是置换$\sigma_5$表达式中的第二行。

给定A上的置换σ，$\sigma(a_1)\sigma(a_2)\dots\sigma(a_n)$为$A$中元素的全排列。如果$\sigma(a_1)\sigma(a_2)\dots\sigma(a_n)$中逆序的个数为奇数，则称$\sigma(a_1)\sigma(a_2)\dots\sigma(a_n)$为奇排列，而$\sigma$则称为奇置换；否则，$\sigma(a_1)\sigma(a_2)\dots\sigma(a_n)$中逆序的个数为偶数，称$\sigma(a_1)\sigma(a_2)\dots\sigma(a_n)$为偶排列，而$\sigma$则称为偶置换。例如，在例3.8中，$\sigma$对应的排列为25143，其中有5个逆序，分别为21、51、54、53、43，所以25143是奇排列，σ是奇置换。在例3.10 中，σ_2对应的排列是231，有2个逆序21和31，所以231是偶排列，σ_2是偶置换。

我们知道，任何两个双射的复合映射仍然是一个双射。因此，两个置换σ_i与σ_j 的相继执行也是一个置换，我们称之为σ_i与σ_j的乘积，记为$\sigma_j\cdot\sigma_i$，也经常省略掉“$\cdot$”，直接记为$\sigma_j\sigma_i$。在例3.10中，

$$\sigma_5 \cdot \sigma_4 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 3 & 2 \\ 3 & 1 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$$
$$= \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = \sigma_3,$$
$$\sigma_4 \cdot \sigma_5 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 3 & 2 & 1 \\ 2 & 3 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$
$$= \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \sigma_2.$$

置换作为一种特殊的映射，其复合运算也不满足交换律。例如，在本例中，$\sigma_5\sigma_4 \neq \sigma_5\sigma_4$。

3.4.2 轮换

轮换是一种特殊的置换，轮换在置换的表示与性质分析等方面有重要的作用。

定义 3.10. 设$a_1, a_2, \cdots, a_r$是集合$A = \{1, 2, \cdots, n\}$中r个不同的元素。σ是A上的置换，满足$\sigma(a_1) = a_2$，$\sigma(a_2) = a_3$，...，$\sigma(a_{r-1}) = a_r$，$\sigma(a_r) = a_1$，而且在σ的作用下，其它元素保持不变，即任给$a \in A - \{a_1, a_2, \cdots, a_r\}$，都有$\sigma(a) = a$，我们称$\sigma$为一个长为$r$的轮换，记作

$$\sigma = (a_1 a_2 \cdots a_r).$$

称$a_1, a_2, \cdots, a_r$为σ搬动的元素。

若$\sigma = (a_1 a_2 \cdots a_r)$，则有$\sigma^{-1} = (a_r a_{r-1} \cdots a_1)$。在例3.10中，$\sigma_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = (123)$，$\sigma_2^{-1} = (321) = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = \sigma_3$。

不难看出，$(a_1 a_2 \cdots a_r) = (a_2 a_3 \cdots a_r a_1) = ... = (a_r a_1 \cdots a_{r-1})$。所以，一个长为$r$的轮换有$r$种不同的表示方式。轮换的乘积可用下面列表的形式进行计算。例如，设$\sigma = (134)$、$\tau = (12)$，则有

$$\sigma\tau = (134)(12) = (1234).$$

$$\begin{array}{ccccc} & \sigma & & \tau & \\ 2 & \leftarrow & 2 & \leftarrow & 1 \\ 3 & \leftarrow & 1 & \leftarrow & 2 \\ 4 & \leftarrow & 3 & \leftarrow & 3 \\ 1 & \leftarrow & 4 & \leftarrow & 4 \end{array}$$

$$\tau\sigma = (12)(134) = (1342)$$

$$\begin{array}{ccccc} & \tau & & \sigma & \\ 3 & \leftarrow & 3 & \leftarrow & 1 \\ 1 & \leftarrow & 2 & \leftarrow & 2 \\ 4 & \leftarrow & 4 & \leftarrow & 3 \\ 2 & \leftarrow & 1 & \leftarrow & 4 \end{array}$$

这个例子中，$\sigma\tau \neq \tau\sigma$。

但对于$\sigma = (12)$、$\tau = (34)$来说，通过计算，可以得出$\sigma\tau = \tau\sigma$。这是因为$\sigma = (12)$与$\tau = (34)$所搬动的元素中，没有相同的。我们称这样的两个轮换是不相交的轮换。两个不相交轮换的乘积是可交换的。

定理 3.9. 任何置换都可以表示成若干不相交的轮换之乘积。

证明: 轮换仅与被搬动的元素有关，我们通过对被搬动的元素个数进行归纳，来证明这个定理。若置换没有搬动任何元素，则为恒等置换，可以看作轮换为空，定理成立。而置换不可能仅搬动一个元素，所以若搬动了元素，则至少两个。设置换为σ。

当置换仅搬动两个元素时，设为i与j，则$\sigma = (ij)$，是长为2的轮换。定理成立。

假设当置换搬动的元素个数小于m时，定理成立。现在假设置换σ搬动了m个元素（$m \geq 3$）。σ一定搬动了某个元素，设为i。由于σ是有限集合上的双射，无穷序列i，$\sigma(i)$，$\sigma^2(i)$，...，$\sigma^t(i)$，...中的元素不可能两两互不相同。因此，一定存在两个最小的整数$0 \leq k < l$，使得$\sigma^k(i) = \sigma^l(i) = (\sigma^k\sigma^{l-k})(i) = \sigma^k(\sigma^{l-k}(i))$。由于$\sigma$是置换，$\sigma^k$也是置换，所以由$\sigma^k(i) = \sigma^k(\sigma^{l-k}(i))$可知，$i = \sigma^{l-k}(i)$。由于$k$与$l$是满足$0 \leq k < l$且$\sigma^k(i) = \sigma^l(i)$的两

个最小整数，$i, \sigma(i), \sigma^2(i), ..., \sigma^{l-k-1}(i)$两两不等，故$\pi_0 = (i\sigma(i)\sigma^2(i)...\sigma^{l-k-1}(i))$是一个长为$l-k$的轮换。

现在考虑置换$\sigma_1 = \pi_0^{-1}\sigma$，因为$\pi_0$搬动的元素为$i, \sigma(i), \sigma^2(i), ..., \sigma^{l-k-1}(i)$，而这些元素也被$\sigma$搬动了。所以，$\sigma$没有搬动的元素，$\sigma_1$也没有搬动，而且$\sigma_1$保持$i, \sigma(i), \sigma^2(i), ..., \sigma^{l-k-1}(i)$不动，没有搬动这些元素，所以$\sigma_1$搬动的元素个数小于$m$。由归纳假设知，存在两两不相交的轮换$\pi_1$、$\pi_2$、...、$\pi_s$，使得$\sigma_1 = \pi_1\pi_2...\pi_s$。因此$\sigma = \pi_0\sigma_1 = \pi_0\pi_1...\pi_s$.

这里，π_0只搬动了$i, \sigma(i), ..., \sigma^{l-k-1}(i))$，而$\pi_1$、$\pi_2$、...、$\pi_s$都不搬动这些元素，所以，$\pi_0$与$\pi_1$、$\pi_2$、...、$\pi_s$都不相交，而由归纳假设，$\pi_1$、$\pi_2$、...、$\pi_s$互相不相交，所以$\pi_0$、$\pi_1$、$\pi_2$、...、$\pi_s$互相不相交。这就证明了定理对于搬动了$m$个元素的置换也成立。由归纳法知，定理成立。证毕。

将一个置换表示成不相交的轮换之乘积后，其中的每个轮换称为一个轮换因子。这里要说明的是，不相交的轮换之乘积是可交换的，如果不考虑轮换因子的书写顺序，那么任何置换表示成不相交的轮换之乘积的形式是唯一的。例如，

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 6 & 3 & 5 & 1 & 7 & 4 & 2 & 9 & 8 \end{pmatrix}$$
$$= (164)(2357)(89) = (2357)(164)(89).$$

设σ是置换，使得$\sigma^n = \sigma_I$的最小整数n称为σ的阶。若$\sigma = (a_1a_2...a_r)$是长为r的轮换，那么σ的阶为r。

定理 3.10. 将置换表示成不相交的轮换之乘积，置换的阶为其各轮换因子长度的最小公倍数。

证明: 由定理3.9知，一个置换σ可以表示成不相交的轮换之乘积$\sigma = \pi_1\pi_2...\pi_s$，其中$\pi_1$、$\pi_2$、...、$\pi_s$为互不相交的轮换，设其阶分别为$m_1$、$m_2$、...、$m_s$。设$m$是$m_1$、$m_2$、...、$m_s$的最小公倍数，且设$m = k_1 \times m_1$、$m = k_2 \times m_2$、...、$m = k_s \times m_s$。由于不相交轮换的乘积是可交换的，所以有

$$\sigma^m = \pi_1^m\pi_2^m...\pi_s^m = (\pi_1^{m_1})^{k_1}(\pi_2^{m_2})^{k_2}...(\pi_s^{m_s})^{k_s} = \sigma_I^{k_1}\sigma_I^{k_2}...\sigma_I^{k_s} = \sigma_I.$$

假设，σ的阶为r。下面通过证明$r|m$，并且$m|r$，从而得到$m=r$，说明m是σ 的阶。

一方面，因为$\sigma^m=\sigma_I$，所以$m\geq r$。设$r^{'}\equiv m \mod r$，则有$0\leq r^{'}\leq r-1$。由$\sigma^m=\sigma^r=\sigma_I$ 知，$\sigma^{r^{'}}=\sigma_I$。若$r^{'}\neq 0$，则$1\leq r^{'}\leq r-1$，与r是σ的阶矛盾。因此，$r^{'}=0$，必有$r|m$。

另一方面，由于σ的阶为r，所以有

$$\sigma^r=\pi_1^r\pi_2^r...\pi_s^r=\sigma_I.$$

由于π_1、π_2、...、π_s两两互不相交，必有$\pi_i^r=\sigma_I, 1\leq i\leq s$。而$\pi_i$的阶为$m_i$，与上一段相同的道理可知，$m_i|r, 1\leq i\leq s$。又因为$m$是$m_1$、$m_2$、...、$m_s$的最小公倍数，所以$m|r$。综合$m|r$和$r|m$，可知$m=r$。$m$是$\sigma$的阶。证毕。

3.4.3 对换

两个元素的轮换称之为对换。任何轮换都可以表示成对换之积，比如

$$(a_1a_2...a_r)=(a_1a_r)(a_1a_{r-1})...(a_1a_3)(a_1a_2).$$

由于每个轮换都可以表示成不相交的轮换之积，所以每个置换都可以表示成对换之积，但表示方法不唯一。例如

$\sigma=\begin{pmatrix}1&2&3&4&5\\2&5&4&3&1\end{pmatrix}=(15)(12)(34)=(13)(34)(45)(24)(14)$。

定理 3.11. 对换是奇置换。

证明: 给定对换(ij)，不妨设$i<j$，

$$\begin{pmatrix}1&2&\cdots&i-1&i&i+1&\cdots&j-1&j&j+1&\cdots&n\\1&2&\cdots&i-1&j&i+1&\cdots&j-1&i&j+1&\cdots&n\end{pmatrix}.$$

第二行的数字中，逆序有$j(i+1)$、$j(i+2)$、...、$j(j-1)$、ji；以及$(i+1)i$、$(i+2)i$、...、$(j-1)i$，共有$2\times(j-i)-1$个，为奇数。故(ij)是奇置换。证毕。

给定置换$\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ a_1 & a_2 & \cdots & a_n \end{pmatrix}$，将$\sigma$乘以一个特定的对换$(i\ i+1)$，我们得到

$$\sigma \cdot (i\ i+1) = \begin{pmatrix} 1 & 2 & \cdots & n \\ a_1 & a_2 & \cdots & a_n \end{pmatrix} (i\ i+1)$$
$$= \begin{pmatrix} 1 & 2 & \cdots & i-1 & i & i+1 & i+2 & \cdots & n \\ a_1 & a_2 & \cdots & a_{i-1} & a_{i+1} & a_i & a_{i+2} & \cdots & a_n \end{pmatrix}.$$

其效果是将置换σ中的a_i与a_{i+1}交换位置。如果$a_i < a_{i+1}$，a_i与a_{i+1}交换位置后，$\sigma\cdot(i\ i+1)$中逆序数比σ中逆序数增加1；否则，$a_i > a_{i+1}$，$\sigma\cdot(i\ i+1)$中逆序数比σ中逆序数减少1。无论是$a_i < a_{i+1}$，或$a_i > a_{i+1}$，$\sigma\cdot(i\ i+1)$ 中逆序数的奇偶性与σ相比都发生了变化。所以，一个置换在乘以形如$(i\ i+1)$的对换后，其奇偶性相反。

给定对换$(i\ j)$，不妨假设$i < j$，则有

$$(i\ j) = (i\ i+1)(i+1\ i+2)\cdots(j-1\ j)(j-2\ j-1)\cdots(i\ i+1).$$

如此，$\sigma\cdot(i\ j)$将σ的奇偶性改变了$2\times(j-i)-1$次，从而$\sigma\cdot(i\ j)$的奇偶性与σ的奇偶性相反。

从上面的分析可知，奇置换可以分解成奇数个对换因子的乘积，偶置换可以分解成偶数个对换因子的乘积。

定理 3.12. $n(n \geq 2)$元置换中，奇置换与偶置换各占一半，为$n!/2$个。

证明： n元集合A的置换与A的全排列一一对应，所以A的置换共有$n!$个。每个置换要么是奇置换，要么是偶置换，两者必居其一。令全体n元偶置换的集合为A_n，全体n元奇置换的集合为B_n。定义$f: A_n \to B_n$，使得任给$\sigma \in A_n$，$f(\sigma) = \sigma\cdot(1\ 2)$。下面证明，$f$是$A_n$到$B_n$的双射，从而得出$|A_n| = |B_n| = n!/2$。

任给$\sigma \in A_n$，σ是偶置换，$f(\sigma) = \sigma\cdot(1\ 2)$是奇置换，所以，$f(\sigma) \in B_n$，$f$是$A_n$到$B_n$的映射。任给$\tau \in B_n$，有$\tau\cdot(1\ 2) \in A_n$，而且$f(\tau\cdot(1\ 2)) = (\tau\cdot(1\ 2))\cdot(1\ 2) = \tau$，所以$f$是满射。假设$\sigma_1, \sigma_2 \in A_n$，若$f(\sigma_1) = f(\sigma_2)$，即$\sigma_1\cdot(1\ 2) = \sigma_2\cdot(1\ 2)$，则有$\sigma_1 = \sigma_2$，所以$f$是单射。从而$f$是$A_n$到$B_n$的双射。因为$|A_n \cup B_n| = n!$且$|A_n \cap B_n| = 0$，所以$|A_n| = |B_n| = n!/2$。

表 3.3: 二元开关函数

x_1	x_2	f_0	f_1	f_2	f_3	f_4	f_5	f_6	f_7	f_8	f_9	f_{10}	f_{11}	f_{12}	f_{13}	f_{14}	f_{15}
0	0	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1
0	1	0	0	0	0	1	1	1	1	0	0	0	0	1	1	1	1
1	0	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1
1	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1

3.5 开关函数

3.5.1 开关函数的定义与性质

令$F_2 = \{0,1\}$，n元开关函数$f(x_1, x_2, ..., x_n)$是从F_2^n到F_2的映射，从定理3.1知，n元开关函数又2^{2^n}个。例如，二元开关函数共有$2^{2^2} = 16$个，参见表3.3。

在表3.3中，函数f_1定义了两个布尔量之间的逻辑乘运算，记为$x_1 \cdot x_2$，我们也经常省略“$\cdot$”，简单记为x_1x_2，它的运算规则如表3.4所示，仅当x_1与x_2 都为1 时，$x_1x_2 = 1$。函数f_7定义了两个布尔量之间的逻辑加运算，记为$x_1 + x_2$，它的运算规则如表3.5所示，仅当x_1与x_2都为0时，$x_1 + x_2 = 0$。

表 3.4: 逻辑乘法

x_1	x_2	x_1x_2
0	0	0
0	1	0
1	0	0
1	1	1

表 3.5: 逻辑加法

x_1	x_2	$x_1 + x_2$
0	0	0
0	1	1
1	0	1
1	1	1

逻辑变量的另一个重要运算是逻辑补运算$\overline{x}$，它的运算规则如表3.6，函数$\overline{x}$与x的取值相反。

定义 3.11. 设$f(x_1, x_2, ..., x_n)$与$g(x_1, x_2, ..., x_n)$是两个n元开关函数，定义三个开关函数$\overline{f}$、$f + g$和$f \cdot g$如下。任给$(a_1, a_2, ..., a_n) \in F_2^n$，

表 3.6: 逻辑补

x	$\overline{x}$
0	1
1	0

表 3.7: 开关函数运算

x_1	x_2	$\overline{x}_1$	$\overline{x}_2$	$\overline{x}_1+\overline{x}_2$	f	g	$\overline{f}$	$f+g$	$f\cdot g$
0	0	1	1	1	0	0	1	0	0
0	1	1	0	1	0	1	1	1	0
1	0	0	1	1	0	0	1	0	0
1	1	0	0	0	1	1	0	1	1

(1) $\overline{f}(x_1,x_2,...,x_n)=\overline{f(x_1,x_2,...,x_n)}$，$\overline{f}$称为$f$的补函数，称“$\overline{f}$”为补运算，简称求补。

(2) $(f+g)(x_1,x_2,...,x_n)=f(x_1,x_2,...,x_n)+g(x_1,x_2,...,x_n)$，$f+g$称为$f$与$g$的和函数，称“$+$”为逻辑加，简称加法。

(3) $(f\cdot g)(x_1,x_2,...,x_n)=f(x_1,x_2,...,x_n)\cdot g(x_1,x_2,...,x_n)$，$f\cdot g$ 称为f与g的积函数，称“$\cdot$”为逻辑乘，简称乘法。

为了开关函数的表示起来简单方便，我们规定开关函数运算的优先级依次为求补“$\overline{f}$”、乘法”$\cdot$”、加法“$+$”。

例 3.11. 设$f(x_1,x_2)=x_1x_2$、$g(x_1,x_2)=x_2$。从函数值的计算表*3.7*中可以看出，$(f+g)(x_1,x_2)=x_2=g(x_1,x_2)$，$(f\cdot g)(x_1,x_2)=x_1x_2=f(x_1,x_2)$，$\overline{f}(x_1,x_2)=\overline{x}_1+\overline{x}_2$。

定理 3.13. 设f、g、h是开关函数，开关函数的运算满足下面的性质：

(1) 结合律：$(f+g)+h=f+(g+h)$；$(f\cdot g)\cdot h=f\cdot(g\cdot h)$。

表 3.8: 分配律证明

f	g	h	$g+h$	$f\cdot(g+h)$	$f\cdot g$	$f\cdot h$	$f\cdot g+f\cdot h$
0	0	0	0	0	0	0	0
0	0	1	1	0	0	0	0
0	1	0	1	0	0	0	0
0	1	1	1	0	0	0	0
1	0	0	0	0	0	0	0
1	0	1	1	1	0	1	1
1	1	0	1	1	1	0	1
1	1	1	1	1	1	1	1

(2) 交换律：$f+g=g+f$；$f\cdot g=g\cdot f$。

(3) 分配律：$f+g\cdot h=(f+g)\cdot(f+h)$；$f\cdot(g+h)=f\cdot g+f\cdot h$。

(4) $f+0=f$；$f\cdot 1=f$。

(5) $f+\overline{f}=1$；$f\cdot\overline{f}=0$。

证明： 作为一个例子，我们来证明分配律$f\cdot(g+h)=f\cdot g+f\cdot h$。由于$f$、$g$、$h$的取值都只有0与1两种可能，我们将所有可能的值，列成计算表，参见表3.8。从表3.8可以看出，$f\cdot(g+h)$ 与$f\cdot g+f\cdot h$的取值完全相同，故$f\cdot(g+h)=f\cdot g+f\cdot h$。证毕。

对于数的乘法与加法来说，乘法对于加法满足分配律，但是加法对于乘法不满足分配律。例如，任给实数a,b,c，都有$a\times(b+c)=a\times b+a\times c$，但一般情况下，$a+b\times c\neq(a+b)\times(a+c)$。可是逻辑乘对逻辑加满足分配律，而且逻辑加对逻辑乘也满足分配律。

下面利用定理3.13，来证明开关函数运算满足的一些等式。

例 3.12. 对任意开关函数f，都满足$f+f=f$，$f\cdot f=f$。

证明：

$f+f=(f+f)\cdot 1=(f+f)\cdot(f+\overline{f})=f+(f\cdot\overline{f})=f+0=f$,
$f\cdot f=(f\cdot f)+0=(f\cdot f)+(f\cdot\overline{f})=f\cdot(f+\overline{f})=f\cdot 1=f$。
证毕。

例 3.13. 对任意开关函数f，都满足$f+1=1$，$f\cdot 0=0$。

证明:
$f+1=f+(f+\overline{f})=(f+f)+\overline{f}=f+\overline{f}=1$,
$f\cdot 0=f\cdot(f\cdot\overline{f})=(f\cdot f)\cdot\overline{f}=f\cdot\overline{f}=0$。
证毕。

例 3.14. 对任意开关函数f与g，$f+g=1$且$f\cdot g=0$的充要条件是$g=\overline{f}$。

证明: 若$g=\overline{f}$，则有$f+g=f+\overline{f}=1$且$f\cdot g=f\cdot\overline{f}=0$。
反之，若$f+g=1$且$f\cdot g=0$，那么
$g=g\cdot 1=g\cdot(f+\overline{f})=g\cdot f+g\cdot\overline{f}=0+g\cdot\overline{f}=g\cdot\overline{f}$,
$\overline{f}=\overline{f}\cdot 1=\overline{f}\cdot(f+g)=\overline{f}\cdot f+\overline{f}\cdot g=0+\overline{f}\cdot g=g\cdot\overline{f}$,
所以，$g=\overline{f}$成立。证毕。

例 3.15. 对任意开关函数f与g，$\overline{f+g}=\overline{f}\cdot\overline{g}$。

证明: 证明思路是，先证明$(f+g)\cdot(\overline{f}\cdot\overline{g})=0$，$(f+g)+(\overline{f}\cdot\overline{g})=1$，然后利用例3.14 的结果，可以得知，$\overline{f+g}=\overline{f}\cdot\overline{g}$。

$$\begin{aligned}(f+g)\cdot(\overline{f}\cdot\overline{g}) &= f\cdot(\overline{f}\cdot\overline{g})+g\cdot(\overline{f}\cdot\overline{g})\\ &= (f\cdot\overline{f})\cdot\overline{g}+(g\cdot\overline{g})\cdot\overline{f}\\ &= 0\cdot\overline{g}+0\cdot\overline{f}=0+0=0.\end{aligned}$$

$$\begin{aligned}(f+g)+(\overline{f}\cdot\overline{g}) &= f+[g+(\overline{f}\cdot\overline{g})]\\ &= f+(g+\overline{f})\cdot(g+\overline{g})\\ &= f+(g+\overline{f})\cdot 1\\ &= (f+\overline{f})+g=1+g=1.\end{aligned}$$

由例3.14知，$\overline{f+g}=\overline{f}\cdot\overline{g}$。证毕。

例 3.16. 对任意开关函数f与g，$f+f\cdot g=f$，$f\cdot(f+g)=f$

证明:
$f+(f\cdot g)=f\cdot 1+f\cdot g=f\cdot(1+g)=f\cdot 1=f$,
$f\cdot(f+g)=(f+0)\cdot(f+g)=f+0\cdot g=f$。
证毕。

例 3.17. 设f、g与h是开关函数，如果$f\cdot g=f\cdot h$且$f+g=f+h$，则$g=h$。

证明:（1）当$g=1$时，由$f\cdot g=f\cdot h$且$f+g=f+h$可知，$f\cdot 1=f\cdot h$且$f+1=f+h$，所以$f=f\cdot h$且$1=f+h$。用$\overline{f}$乘以$1=f+h$的两边，可以得出

$$\overline{f}=\overline{f}\cdot(f+h)=\overline{f}\cdot f+\overline{f}\cdot h=0+\overline{f}\cdot h=\overline{f}\cdot h,$$

而$h=h\cdot(f+\overline{f})=h\cdot f+h\cdot\overline{f}=f+\overline{f}=1$。此时，$g=h=1$。

（2）当$g=0$时，由$f\cdot g=f\cdot h$且$f+g=f+h$可知，$f\cdot h=f\cdot 0=0$且$f+h=f+0=f$。用$\overline{f}$乘以$f=f+h$的两边，可以得出

$$0=\overline{f}\cdot f=\overline{f}\cdot(f+h)=\overline{f}\cdot f+\overline{f}\cdot h=0+\overline{f}\cdot h=\overline{f}\cdot h,$$

而$h=h\cdot(f+\overline{f})=h\cdot f+h\cdot\overline{f}=0+0=0$。此时，$g=h=0$。综上，无论$g=1$或者$0$，都有$g=h$，所以$g=h$。证毕。

例3.12、例3.15与例3.16分别证明了n元开关函数满足幂等律、德•摩根律与吸收律。这些定律今后都可以直接引用。

3.5.2 开关函数的小项表达式

通常，一个开关函数可以有多种相互等价的表达方式。为了理论上研究的方便，我们需要一种标准的表达方式，使得每个开关函数有唯一的表达方式，并且不同的开关函数有不同的表达方式。下面介绍的小项表达式就是其中的一种方法。

首先我们说明，对任意n开关函数$f(x_1,x_2,...,x_n)$，都满足

$$f(x_1,x_2,...,x_n)=x_1\cdot f(1,x_2,...,x_n)+\overline{x_1}\cdot f(0,x_2,...,x_n). \tag{3.1}$$

这是因为，当$x_1=0$时，公式(3.1)的右式为

$$0\cdot f(1,x_2,...,x_n)+1\cdot f(0,x_2,...,x_n)=f(0,x_2,...,x_n),$$

而且当$x_1=1$时，公式(3.1)的右式为

$$1\cdot f(1,x_2,...,x_n)+0\cdot f(0,x_2,...,x_n)=f(1,x_2,...,x_n).$$

所以，无论$x_1=0$，还是$x_1=1$，公式(3.1)都成立，所以公式(3.1)成立。

我们将公式(3.1)应用到二元开关函数$f(x_1,x_2)$，可以得出

$$\begin{aligned}f(x_1,x_2)&=x_1\cdot f(1,x_2)+\overline{x_1}\cdot f(0,x_2)\\&=x_1\cdot[x_2\cdot f(1,1))+\overline{x_2}\cdot f(1,0)]+\overline{x_1}\cdot[x_2\cdot f(0,1)+\overline{x_2}\cdot f(0,0)]\\&=f(1,1)x_1x_2+f(1,0)x_1\overline{x_2}+f(0,1)\overline{x_1}x_2+f(0,0)\overline{x_1x_2}.\end{aligned}$$

将这一规律推广到n元开关函数，则有

$$f(x_1,x_2,...,x_n)=\sum_{a_i=0或1,1\le i\le n}f(a_1,a_2,...,a_n)x_1^{a_1}x_2^{a_2}...x_n^{a_n},\tag{3.2}$$

其中，

$$x_i^{a_i}=\begin{cases}x_i & a_i=1,\\ \overline{x_i} & a_i=0.\end{cases}\tag{3.3}$$

公式(3.2)就是n元开关函数的$f(x_1,x_2,...,x_n)$的小项表达式，其中的每一项$x_1^{a_1}x_2^{a_2}...x_n^{a_n}$就是一个小项。因为每个$a_i$都可以取值为0或1，$n$元开关函数有$2^n$个小项。

例 3.18. 给定3元开关函数$f(x_1,x_2,x_3)$，其函数值参见表*3.9*。

它的小项表达式为

$$\begin{aligned}f(x_1,x_2,x_3)=&f(0,0,0)x_1^0x_2^0x_3^0+f(0,0,1)x_1^0x_2^0x_3^1\\&+f(0,1,0)x_1^0x_2^1x_3^0+f(0,1,1)x_1^0x_2^1x_3^1\\&+f(1,0,0)x_1^1x_2^0x_3^0+f(1,0,1)x_1^1x_2^0x_3^1\\&+f(1,1,0)x_1^1x_2^1x_3^0+f(1,1,1)x_1^1x_2^1x_3^1\\=&0\cdot x_1^0x_2^0x_3^0+1\cdot x_1^0x_2^0x_3^1+1\cdot x_1^0x_2^1x_3^0+1\cdot x_1^0\ x_2^1x_3^1\\&+0\cdot x_1^1x_2^0x_3^0+1\cdot x_1^1x_2^0x_3^1+0\cdot x_1^1x_2^1x_3^0+1\cdot x_1^1x_2^1x_3^1\\=&\overline{x}_1\overline{x}_2x_3+\overline{x}_1x_2\overline{x}_3+\overline{x}_1x_2x_3+x_1\overline{x}_2x_3+x_1x_2x_3.\end{aligned}$$

表 3.9: $f(x_1, x_2, x_3)$的函数值表

x_1	x_2	x_3	$f(x_1, x_2, x_3)$
0	0	0	0
0	0	1	1
0	1	0	1
0	1	1	1
1	0	0	0
1	0	1	1
1	1	0	0
1	1	1	1

例 3.19. 求$f(x_1, x_2, x_3) = x_1$的小项表达式。

解:

$$\begin{aligned} f(x_1, x_2, x_3) = x_1 &= x_1 \cdot (x_2 + \overline{x_2}) \cdot (x_3 + \overline{x}_3) \\ &= x_1x_2x_3 + x_1x_2\overline{x}_3 + x_1\overline{x}_2x_3 + x_1\overline{x}_2\overline{x}_3. \end{aligned}$$

3.5.3 集合的特征函数

定义 3.12. 给定集合E，$F_2 = \{0, 1\}$，对于E的每个子集$A \subseteq E$，定义一个函数$\chi_A : E \to F_2$，

$$\chi_A(x) = \begin{cases} 1 & 若x \in A, \\ 0 & 若x \notin A. \end{cases}$$

称χ_A为集合A的特征函数。

显然，E的不同子集对应着不同的特征函数。若E是有限集合，E的子集有$2^{|E|}$个。从E到F_2的映射个数也是$2^{|E|}$。定义$g : \mathscr{P}(E) \to \{f | f : E \to F_2\}$，使得任给$A \in \mathscr{P}(E)$，$g(A) = \chi_A$，则$g$是从$\mathscr{P}(E)$到$\{f | f : E \to F_2\}$的双射。

如果取$E = F_2^n$，F_2^n的2^{2^n}个子集与从F_2^n到F_2的2^{2^n}个开关函数之间可以建立一一对应关系。对应的方法是：对于$A \subseteq F_2^n$，A的特征函数定义为

$$\chi_A(x_1, x_2, ..., x_n) = \begin{cases} 1 & 若(x_1, x_2, ..., x_n) \in A, \\ 0 & 若(x_1, x_2, ..., x_n) \notin A. \end{cases}$$

容易看出，若A_1、A_2的特征函数分别为χ_{A_1}、χ_{A_2}，那么集合$A_1 \cap A_2$、$A_1 \cup A_2$的特征函数分别是$\chi_{A_1} \cdot \chi_{A_2}$和$\chi_{A_1} + \chi_{A_2}$。这样，集合上的三种基本运算补“-”、交“$\cap$”、并“$\cup$”分别对应于开关函数的三种运算–逻辑补、逻辑乘和逻辑加。将集合的运算规则与开关函数的运算规则加以比较，对它们的相似之处就不难理解了。这一点将在第??章有进一步的分析。

习题

1. 下面的对应规则中哪些能够构成映射？请说明理由。其中，$\mathbb{N}$与$\mathbb{R}$分别为自然数集合与实数集合。

（1）$\{(x_1, x_2) | x_1, x_2 \in \mathbb{N}, x_1 + x_2 < 10\}$。

（2）$\{(y_1, y_2) | y_1, y_2 \in \mathbb{R}, y_2 = y_1^2\}$。

（3）$\{(y_1, y_2) | y_1, y_2 \in \mathbb{R}, y_2^2 = y_1\}$。

2. 设$f : A \to B$，其中$A = \{-1, 0, 1\}^2$，B为整数集合。

$$f(x_1, x_2) = \begin{cases} 0 & 若x_1 \times x_2 > 0, \\ x_1 - x_2 & 若x_1 \times x_2 \leq 0. \end{cases}$$

（1）f的值域R_f是什么？

（2）从A到R_f有多少个不同的映射？

3. 下列函数中哪些是单射、满射或双射？说明理由。其中，$\mathbb{Z}$与$\mathbb{Z}^+$分别为整数集合与正整数集合。

（1）$f : \mathbb{Z} \to \mathbb{Z}^+$，$f(n) = |n| + 1$。

（2）$f : \mathbb{Z} \to \mathbb{Z} \cup \{0\}$，$f(j) = j \mod 3$。其中，$j \mod 3$表示$j$除以3的非负余数。

（3）$f : \mathbb{Z} \to \mathbb{Z}$，$f(n) = n + 1$；$g : \mathbb{Z} \to \mathbb{Z}$，$g(n) = n - 1$。

（4）$f:\mathbb{Z}\to\{0,1\}$，$f(j)=\begin{cases}0 & j\text{为奇数},\\ 1 & j\text{为偶数}\end{cases}$。

（5）$f:\mathbb{Z}\to\mathbb{Z}$，$f(j)=j^2+2j-15$。

4. A、B是有限集合，试给出从$A\times B$到$B\times A$的双射，从而证明$|A\times B|=|B\times A|$。

5. 设$R[x]$为所有实数系数的多项式构成的集合，

（1）证明：$\frac{d}{dx}f(x)=f'(x)$是从$R[x]$到$R[x]$的映射。它的值域是什么？是否为满射？是否为双射？

（2）证明：$I(f(x))=\int_0^x f(t)dt$是从$R[x]$到$R[x]$的映射。它的值域是什么？是否为满射？是否为双射？

6. 设$A=\{a_1,a_2,...,a_n\}$、$B=\{b_1,b_2,...,b_m\}$，$S(B)$表示集合B中元素构成的所有有序n元组所构成的集合，即

$$S(B)=\{(b_{i_1},b_{i_2},...,b_{i_n})|b_{i_j}\in B,1\le j\le n\}.$$

用F表示从A到B的所有映射构成的集合，对于F中的每个映射f，令

$$g(f)=(f(a_1),f(a_2),...,f(a_n)),$$

证明：g是从F到$S(B)$的双射，并由此证明从A到B的映射有m^n个。

7. 设f是集合S到T的映射，A与B是S的子集，证明

$$f(A\cup B)=f(A)\cup f(B),$$
$$f(A\cap B)\subseteq f(A)\cap f(B)。$$

并且请给出一个例子，说明$f(A\cap B)\neq f(A)\cap f(B)$。

8. 设f是集合S到T的映射，A是S的子集，A在S中的补集为$\widetilde{A}=S-A$。当f为单射或满射时，分别讨论$f(\widetilde{A})$与$\widetilde{f(A)}$的关系。

9. 设f、g、h都是从$\mathbb{Z}$到$\mathbb{Z}$的映射，$f(x)=3x$，$g(x)=3x+1$，$h(x)=3x+2$，请计算$f\circ g$，$g\circ f$，$g\circ h$，$h\circ g$，$f\circ g\circ h$。

10. 设f是A到B的单射，g是B到C的单射，证明：$g\circ f$是A到C的单射。

11. 设$S=\{1,2,3,...\}$，给出两个从S到S的映射f与g，使得$f\circ g=I_S$，但是$g\circ f\neq I_S$。如果f是双射，会发生什么情况？

12. 设$\sigma=\begin{pmatrix}1&2&3&4&5&6\\3&1&4&5&6&2\end{pmatrix}$，$\tau=\begin{pmatrix}1&2&3&4&5&6\\2&4&1&3&6&5\end{pmatrix}$。计算$\tau\sigma$，$\tau^2\sigma$，$\sigma^2\tau$，$\sigma^{-1}\tau\sigma$。

13. 假设下列为集合$A=\{1,2,3,4,5,6,7,8\}$上的置换，请将其写成不相交的轮换之积。

（1）$(257)(78)(145)$，

（2）$(72815)(21)(476)(12)$。

14. 将下列置换表示成不相交的轮换之积。

（1）$\begin{pmatrix}1&2&3&4&5&6&7&8\\8&2&6&3&7&4&5&1\end{pmatrix}$，

（2）$\begin{pmatrix}1&2&3&4&5&6&7&8\\3&6&4&1&8&2&5&7\end{pmatrix}$，

（3）$\begin{pmatrix}1&2&3&4&5&6&7&8\\3&1&4&7&2&5&8&6\end{pmatrix}$。

15. 假设下列为集合$A=\{1,2,3,4,5,6,7\}$上的置换，请求出各个置换的阶。

（1）$(47)(261)(567)(1234)$，

（2）$(163)(1357)(67)(12345)$。

16. 证明：任何n元置换可以表示成对换(12)、(23)、...、$((n-1)n)$的乘积。

17. 证明下面恒等式：

（1）$x_1=x_1x_2x_3+x_1\overline{x}_2x_3+x_1x_2\overline{x}_3+x_1\overline{x}_2\overline{x}_3$，

（2）$x_1x_2+x_2x_3+\overline{x}_1x_3=x_1x_2+\overline{x}_1x_3$。

18. 假设f与g是开关函数，如果$f+g=g$，证明下面三个等式成立。

（1）$f\cdot g+\overline{f}=1$，

（2）$\overline{f}+g=1$，

（3）$f\cdot\overline{g}=0$。

19. 写出下列二元开关函数的小项表达式：

（1）值恒为1的函数，

（2）当且仅当两个变量的取值相同时，函数的值为1。

第 4 章 二元关系

4.1 基本概念

4.1.1 关系的定义

定义 4.1. 设$A_1, A_2, \cdots, A_n$是集合，$A_1 \times A_2 \times \cdots \times A_n$的子集$R$称为$A_1$、$A_2$、...、$A_n$间的一个$n$元关系。如果$R = \emptyset$，称$R$为空关系或平凡关系；如果$R = A_1 \times A_2 \times \cdots \times A_n$，则称$R$为全关系。

如果R是集合A与集合B间的二元关系，则也称作是从A到B的二元关系。此时，R的定义域定义为

$Dom(R) = \{x | x \in A$，且存在$y \in B$，使得$(x, y) \in R\}$.

而R的值域则定义为

$Ran(R) = \{y | y \in B$，且存在$x \in A$，使得$(x, y) \in R\}$.

容易得知，$Dom(R) \subseteq A$，$Ran(R) \subseteq B$。如果$(a, b) \in R$，我们称a与b有关系R，记作aRb；如果$(a, b) \notin R$，我们称a与b没有关系R，记作$a \not R b$。如果$A = B$，则称R为A上的二元关系。

例 4.1. 将整数集合$\mathbb{Z}$上的小于关系记为L。因为$4 < 6$，所以$(4, 6) \in L$，或者$4L6$，但是$(6, 4) \notin L$。

例 4.2. 定义自然数集合$\mathbb{N}$上的整数倍关系M，$(x, y) \in M$当且仅当x是y的整数倍，即

$$xMy \Leftrightarrow \text{存在} k \in \mathbb{N}, \text{使得} x = ky.$$

如果$x \in \mathbb{N}$且$x \not M 2$，则x为奇数。设$p \in \mathbb{N}$且$p > 1$，若任给$q \neq 1$且$q \neq p$，都有$p \not M q$，则意味着p是素数。

例 4.3. 实数集合上的二元关系对应于笛卡尔坐标平面的点集合。例如关系$R = \{(x, y) | |x| + |y| \leq 1\}$ 对应于图*4.1*中画阴影的部分。

对比集合A到集合B的映射f与$A \times B$上的二元关系R，尽管它们都可以写成如下的有序对集合的形式：

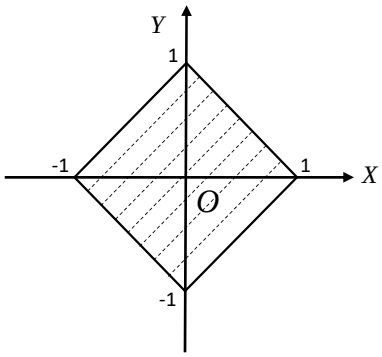


图 4.1: 例4.3对应的图

$f = \{(x, y)|x \in A, y \in B, 并且 f(x) = y\}$,
$R = \{(x, y)|x \in A, y \in B, 并且 xRy\}$。

两者看上去非常类似，但是，从映射的定义可知，在f的作用下，A中的每个元素在B中都有一个对应的像。因此，f的定义域是$Dom(f) = A$，但是R的定义域$Dom(R) \subseteq A$。另一方面，对于任给$x \in A$，在f 的作用下，x在B中的像是唯一的，也就说，若$(x, y_1) \in f$且$(x, y_2) \in f$，则有$y_1 = y_2$。但是对于关系R来说，完全有可能存在$x \in A$，$y_1, y_2 \in B$且$y_1 \neq y_2$，使得$(x, y_1) \in R$且$(x, y_2) \in R$。所以，关系是函数的延伸，相对于函数来说，关系表达了集合间更广泛的联系。

由于n元关系可以表达成有序n元组的集合的形式，有些关系也可以采用归纳定义。例如，自然数集合$\mathbb{N}$上的小于关系“L”可以通过下面的形式进行归纳定义：

(1) 基础语句：$(0, 1) \in L$;

(2) 归纳语句：如果$(x, y) \in L$，则$(x, y + 1) \in L$，$(x + 1, y + 1) \in L$;

(3) 终结语句：L由有限次使用规则(1)与(2)生成的有序二元组组成。

4.1.2 关系的性质

定义 4.2. 设R是A上的二元关系，

(1) 如果对于任意$x \in A$，都有xRx，则称R是自反的;

(2) 如果对于任意$x \in A$，都有$x \not R x$，则称R是反自反的；

(3) 如果对于任意$x, y \in A$，若xRy，则一定有yRx，那么称R是对称的；

(4) 如果对于任意$x, y \in A$，若xRy且yRx，则一定有$x = y$，那么称R 是反对称的；

(5) 如果对于任意$x, y, z \in A$，若xRy且yRz，则一定有xRz，那么称R是传递的。

对于集合A上的二元关系R来说，可能存在$x, y \in A$，使得xRx，但$y \not R y$。所以，从上面的定义可以看出，存在二元关系，既不是自反的，也不是反自反的，自反与反自反的性质并不是互补的。其次，对于反对称关系来说，主要指的是，若$x, y \in A$且$x \neq y$，则xRy与yRx不能同时成立。

例 4.4. 将英文字母表记为$\Sigma = \{a, b, \cdots, x, y, z\}$，$\Sigma^*$为$\Sigma$中字母组成的字符串集合，假定$\alpha, \beta \in \Sigma^*$，定义$\Sigma^*$上的二元关系$R_1$、$R_2$、$R_3$，其中：

$\alpha R_1 \beta$，当且仅当α与β长度相等，

$\alpha R_2 \beta$，当且仅当α比β长，

$\alpha R_3 \beta$，当且仅当α的某个真前缀是β的一个真后缀。

例如，设$\alpha = abc$，$\beta = xyz$，$\gamma = xyzab$，则有$\alpha R_1 \beta$，$\alpha \not R_1 \gamma$，$\gamma R_2 \beta$，$\alpha \not R_2 \beta$，$\alpha R_3 \gamma$，$\alpha \not R_3 \beta$。其中，ab是α的真前缀，同时又是γ的真后缀。

由定义知，R_1是自反的；R_2是反自反的；R_3既不是自反的，也不是反自反的。比如说，aaR_3aa，但是$ab \not R_3 ab$。

例 4.5. Σ^*的定义如例*4.4*。设$\alpha, \beta \in \Sigma^*$，定义$\Sigma^*$ 上的二元关系R_4、R_5、R_6，其中：

$\alpha R_4 \beta$，当且仅当α是β的子串，

$\alpha R_5 \beta$，当且仅当α与β有一个相同的非空前缀，

$\alpha R_6 \beta$，当且仅当α与β相等。

例如，设$\alpha = abc$，$\beta = xyz$，$\gamma = xyzab$，$\delta = xyz$，则有$\alpha R_4 \alpha$，$\beta R_4 \gamma$，$\alpha \not R_4 \beta$，$\beta R_5 \gamma$，$\alpha \not R_5 \beta$，$\beta R_6 \delta$，$\alpha \not R_b \beta$。

由定义知，R_4是反对称的；R_5是对称的；R_6既是对称的，也是反对称的。假设二元关系R 既是对称的，也是反对称的，那么若$\alpha \neq \beta$，则α与β一定不满足关系R，即$\alpha \not R \beta$。

例 4.6. Σ^*的定义如例4.4。设$\alpha, \beta \in \Sigma^*$，定义$\Sigma^*$ 上的二元关系R_7、R_8、R_9，其中：

$\alpha R_7 \beta$，当且仅当α是β的前缀，

$\alpha R_8 \beta$，当且仅当α是β的子字，

$\alpha R_9 \beta$，当且仅当α与β有相同的字符。

由定义知，R_7与R_8是传递的；但R_9不是传递的。例如，设$\alpha = abc$，$\beta = xyzab$，$\gamma = xyz$，则有$\alpha R_9 \beta$，$\beta R_9 \gamma$，但是，$\alpha \not R_9 \gamma$。

4.1.3 关系的表示

在关系的定义中，我们曾用有序二元组的形式来表示二元关系。假设R是集合A到B上的二元关系，可以将R表示为

$$R = \{(x, y) | x \in A, y \in B, xRy\}.$$

本节介绍另外两种二元关系的表达形式，即关系矩阵与关系图。

定义 4.3. 设R是从有限集合A到有限集合B的二元关系，其中$A = \{a_1, a_2, \cdots, a_m\}$、$B = \{b_1, b_2, \cdots, b_n\}$，定义矩阵$M_R = (m_{ij})_{m \times n}$，其中

$$m_{ij} = \begin{cases} 0 & \text{当} a_i \not R b_j \text{时}, \\ 1 & \text{当} a_i R b_j \text{时}. \end{cases}$$

我们称M_R是关系R的关系矩阵，M_R的行数与列数分别为集合A中的元素个数与集合B中的元素个数。

例 4.7. 设$A = \{a_1, a_2, a_3, a_4\}$、$B = \{b_1, b_2, b_3\}$，$R$是集合$A$到集合$B$上的关系，

$$R = \{(a_1, b_1), (a_1, b_2), (a_2, b_2), (a_3, b_1), (a_3, b_3), (a_4, b_1), (a_4, b_2)\}.$$

R的关系矩阵M_R是4×3阶矩阵，

$$M_R = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix}.$$

例 4.8. 设R是$A=\{a_1,a_2,a_3,a_4\}$上的二元关系，$R=\{(a_1,a_1),(a_1,a_2),(a_1,a_4),(a_2,a_2),(a_2,a_3),(a_3,a_1),(a_3,a_3),(a_3,a_4),(a_4,a_1),(a_4,a_2),(a_4,a_3)\}$，则$R$的关系矩阵$M_R$是4阶方阵，

$$M_R=\begin{pmatrix}1&1&0&1\\0&1&1&0\\1&0&1&1\\1&1&1&0\end{pmatrix}.$$

从关系矩阵的定义可以看出：对于有限集合$A=\{a_1,a_2,\cdots,a_n\}$上的二元关系R，如果R 是自反的，那么M_R的主对角线上所有元素都是1；如果R是反自反的，那么M_R 的主对角线上所有元素都是0；如果R是对称的，那么M_R是对称矩阵；如果R是反对称的，那么M_R中关于主对角线对称的两个位置不能同时为1，即在$i\neq j$时，若$m_{ij}=1$，一定有$m_{ji}=0$。但是，关系R 的传递性不容易从M_R中直接看出。

定义 4.4. 给定有限集合$A=\{a_1,a_2,\cdots,a_n\}$上的二元关系R，我们可以用一个有向图G_R来表示R。G_R 的定义是：用n个点分别表示A中的每个元素，其中代表a_i的点标记为a_i，也称为节点a_i；如果$a_iRa_j(i\neq j)$，那么从节点a_i向节点a_j画一条有向弧；如果a_iRa_i，则在节点a_i上画一条有向圈。

例 4.9. 例*4.8*中关系对应的关系图参见图*4.2*。

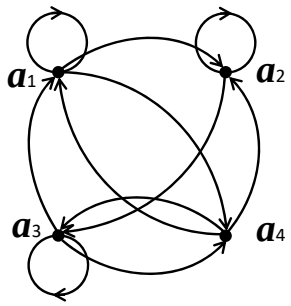


图 4.2: 例4.8对应的关系图

有限集合上的二元关系可以用关系图来表示，从关系图可以直观地看出关系的一些性质。如果关系R 是自反的，那么关系图中的每个节点都有

一个圈。如果一个关系是反自反的，则关系图中的每个节点上都没有圈。设a_i与a_j是两个不同的节点，如果关系是对称的，a_i到a_j有有向弧，则a_j到a_i一定有向弧；如果关系是反对称的，a_i到a_j有有向弧，则a_j到a_i一定没有有向弧。设a_i、a_j与a_k是三个不同的节点，如果关系是传递的，a_i到a_j、a_j到a_k都有有向弧，则a_i到a_k一定有有向弧。

关系矩阵可以表示有限集合A到有限集合B上的二元关系，也可以表示有限集合A上的二元关系。关系图用来表示有限集合A上的二元关系。一般情况下，不用关系图表示有限集合A到另一个有限集合B上的二元关系。

4.1.4 关系的运算

从集合A到集合B的二元关系R，等价于$A \times B$的一个子集。集合之间的相等与包含等关系，以及集合间的并、交与补等运算，都可以直接定义成关系之间的相互关系以及关系的运算。

定义 4.5. 设R_1与R_2都是集合A到集合B的二元关系。作为$A \times B$的子集而言，如果$R_1 \subseteq R_2$，则称R_1小于等于R_2，记作$R_1 \leq R_2$。

如果$R_1 \leq R_2$且$R_1 \neq R_2$，则称R_1小于R_2，记作$R_1 < R_2$。

类似地，可以定义关系间的“大于等于”与“大于”关系，分别记作“$\geq$”与“$>$”。

对于两个集合A与B而言，若满足$A \subseteq B$，其含义是：任给$a \in A$，则必有$a \in B$。而对于集合A到集合B的两个二元关系R_1与R_2而言，若满足$R_1 \leq R_2$，可以刻划成：若xR_1y，则必有xR_2y；类似地，若满足$R_1 < R_2$，可以刻划成：若xR_1y，则必有xR_2y，并且存在$x_0 \in A$、$y_0 \in B$，使得$x_0 \not R_1 y_0$，但是$x_0 R_2 y_0$。

定义 4.6. 设R、R_1与R_2都是集合A到集合B的二元关系。定义R的补$\overline{R}$、R_1与R_2的并$R_1 \cup R_2$，以及R_1与R_2的交$R_1 \cap R_2$如下：

（1）任给$x \in A$、$y \in B$，若$x\overline{R}y$，当且仅当$x \not R y$；

（2）任给$x \in A$、$y \in B$，若$x(R_1 \cup R_2)y$，当且仅当xR_1y或xR_2y；

（3）任给$x \in A$、$y \in B$，若$x(R_1 \cap R_2)y$，当且仅当xR_1y且xR_2y。

例 4.10. 设R_1与R_2是实数集合$\mathbb{R}$上的二元关系。它们的定义分别为：任给$x, y \in \mathbb{R}$，（*1*）xR_1y，当且仅当$x = y$；（*2*）xR_2y，当且仅当$x = -y$。那么

$x(R_1 \cup R_2)y$，当且仅当$|x| = |y|$。

例 4.11. 设R_1与R_2是实数集合$\mathbb{R}$上的二元关系。它们的定义分别为：任给$x, y \in \mathbb{R}$，（*1*）xR_1y，当且仅当$x \geq y$；（*2*）xR_2y，当且仅当$x \leq y$。那么

$x(R_1 \cap R_2)y$，当且仅当$x = y$，

$x\overline{R}_1y$，当且仅当$x < y$。

因为从集合A到集合B的二元关系R等价于$A \times B$的一个子集，所以集合间运算“$\cup$”、“$\cap$”、“$\overline{A}$”所满足的基本规则也完全适合于关系间的运算。例如，

（1）交换律：$R_1 \cup R_2 = R_2 \cup R_1$，$R_1 \cap R_2 = R_2 \cap R_1$；

（2）结合律：$(R_1 \cup R_2) \cup R_3 = R_1 \cup (R_2 \cup R_3)$，$(R_1 \cap R_2) \cap R_3 = R_1 \cap (R_2 \cap R_3)$。

除了与集合运算类比的几个关系运算“$\cup$”、“$\cap$”、“$\overline{A}$”之外，还有两个特殊的关系运算：关系的合成与关系的闭包。

定义 4.7. 设R_1是从集合A到集合B上的关系，R_2是从集合B到集合C上的关系，定义R_1与R_2 的复合关系$R_2 \circ R_1$为从集合A到集合C上的关系，具体定义如下：

任给$x \in A$、$z \in C$，$x(R_2 \circ R_1)z$，当且仅当存在$y \in B$，使得xR_1y且yR_2z。

例 4.12. 设R与S都是集合$A = \{1, 2, 3, 4, 5\}$上的关系，其中，

$R = \{(1, 2), (2, 2), (3, 4)\}$，

$S = \{(1, 3), (2, 5), (3, 1), (4, 2)\}$，

那么

$R \circ S = \{(1, 4), (3, 2), (4, 2)\}$，

$S \circ R = \{(1, 5), (2, 5), (3, 2)\}$。

$R \circ S$与$S \circ R$都是集合A到其自身上的二元关系，但是$R \circ S \neq S \circ R$，可见关系的复合运算不满足交换律。

定理 4.1. 关系的复合运算满足结合律。

证明: 设R_1是从集合A到集合B上的关系，R_2是从集合B到集合C上的关系，R_3 是从集合C到集合D上的关系。我们要证明$R_3 \circ (R_2 \circ R_1) = (R_3 \circ R_2) \circ R_1$。

先证明$R_3 \circ (R_2 \circ R_1) \subseteq (R_3 \circ R_2) \circ R_1$。任给$a \in A$、$d \in D$，若$(a,d) \in R_3 \circ (R_2 \circ R_1)$，根据复合关系的定义可知，存在$c \in C$，使得$(a,c) \in R_2 \circ R_1$且$(c,d) \in R_3$。又由于$(a,c) \in R_2 \circ R_1$，由复合关系定义知，存在$b \in B$，使得$(a,b) \in R_1$且$(b,c) \in R_2$。而由$(b,c) \in R_2$和$(c,d) \in R_3$，可知$(b,d) \in R_3 \circ R_2$，再由$(b,d) \in R_3 \circ R_2$和$(a,b) \in R_1$ 知，$(a,d) \in (R_3 \circ R_2) \circ R_1$。因此，$R_3 \circ (R_2 \circ R_1) \subseteq (R_3 \circ R_2) \circ R_1$。

同理可证，$(R_3 \circ R_2) \circ R_1 \subseteq R_3 \circ (R_2 \circ R_1)$。因此，$(R_3 \circ R_2) \circ R_1 = R_3 \circ (R_2 \circ R_1)$。证毕。

利用关系的复合运算，以及关系复合运算满足的结合律，可以构成关系的幂运算。设R是集合A 上的二元关系，可以递归定义R的幂：$R^1 = R$、$R^2 = R \circ R$、$R^3 = R^2 \circ R = R \circ R^2$、...、$R^n = R^{n-1} \circ R = R \circ R^{n-1}$、...。由关系复合运算满足结合律可知，对于$n > m > 0$，满足

$$R^n = R^m \circ R^{n-m}.$$

注意，R必须是某个集合A到其自身上的二元关系，才可以定义R的幂。

定义 4.8. 设R是集合A上的二元关系，如果存在A上的二元关系R_1，R_1满足以下三个条件:

（*1*）R_1是自反的，

（*2*）$R \subseteq R_1$,

（*3*）任给A上的二元关系R_2，若R_2是自反的，且$R \subseteq R_2$，则一定有$R_1 \subseteq R_2$，

那么称R_1是R的自反闭包。

事实上，R的自反闭包就是包含R且满足自反性质的最小关系。类似地，可以定义R的对称闭包与传递闭包。但是，仿照定义4.8，不能定义R的反自反闭包与反对称闭包。

定理 4.2. 设R是集合A上的二元关系，定义集合A上的二元关系R^+：任给$a_1, a_2 \in A$，

$$a_1 R^+ a_2，当且仅当存在 n > 0，使得 a_1 R^n a_2，$$

则R^+是关系R的传递闭包。

证明： 首先证明R^+是传递的。任给$a, b, c \in A$，如果aR^+b且bR^+c，则存在$n_1 > 0$、$n_2 > 0$，使得$aR^{n_1}b$、$bR^{n_2}c$，由复合关系的定义知，$a(R^{n_2} \circ R^{n_1})c = aR^{n_1+n_2}c$，所以$aR^+c$，从而$R^+$是传递的。

再证明$R \leq R^+$。任给$a, b \in A$，若aRb，即aR^1b，所以aR^+b。因此，$R \leq R^+$。

最后证明R^+是包含R的最小传递关系。假设R^*是A上任意一个包含R的传递关系。任给$b, c \in A$，若cR^+b，那么存在着某个$n > 1$，使得cR^nb。由幂关系的定义知，存在$a_1, a_2, \cdots, a_{n-1} \in A$，使得

$$cRa_1, a_1Ra_2, \cdots, a_{n-2}Ra_{n-1}, a_{n-1}Rb,$$

因为$R \leq R^*$，所以有

$$cR^*a_1, a_1R^*a_2, \cdots, a_{n-2}R^*a_{n-1}, a_{n-1}R^*b.$$

因为R^*满足传递性，所以cR^*b。从而$R^+ \leq R^*$，R^+是包含R的最小传递关系。

综上分析知，R^+是关系R的传递闭包。证毕。

定理 4.3. 设R是集合A上的二元关系，则$R' = I_A \cup R$是关系R的自反闭包。其中，I_A是A 上的恒等关系，即对任给$a \in A$，都有aI_Aa，而对于任给$a, b \in A$且$a \neq b$，aI_Ab都不成立。

证明： 留作习题5。

定理 4.4. 设R是集合A上的二元关系，定义A上的二元关系R'如下

$$R' = \{(y, x) | x, y \in A且(x, y) \in R\},$$

则$\widetilde{R} = R \cup R'$是$R$的对称闭包。

证明： 首先，由于$\widetilde{R} = R \cup R' \supseteq R$，所以$R \leq \widetilde{R}$。

下面证明$\widetilde{R}$是对称的。任给$a, b \in A$，若$a\widetilde{R}b = a(R \cup R')b$，由关系的并运算的定义可知，$aRb$或$aR'b$。若$aRb$，由$R'$的定义知，$bR'a$，所以$b(R \cup R')a$，即$b\widetilde{R}a$；若$aR'b$，由$R'$的定义知，$bRa$，同样也可以得到$b(R \cup R')a$，即$b\widetilde{R}a$。所以，无论是$aRb$或$aR'b$，都可以得到$b\widetilde{R}a$。所以$\widetilde{R}$是对称的。

最后证明$\widetilde{R}$是包含R的最小对称关系。假设R^*是包含R的对称关系。任给$a, b \in A$，若$a\widetilde{R}b$，则有aRb或$aR'b$。（1）若aRb，因为R^* 包含了R，所以aR^*b；（2）若$aR'b$，则由R'的定义知，bRa。因为R^*包含了R，所以bR^*a。再因为R^*是对称关系，可得aR^*b。所以，无论是aRb，还是$aR'b$，都有aR^*b。因此，aR^*b。R^*包含了$\widetilde{R}$。

综上可知，$\widetilde{R}$是R的对称闭包。证毕。

4.2 等价关系

定义 4.9. 设R是集合A上的二元关系，如果R是自反的、对称的、传递的，则称R是等价关系。

设R是集合A上的等价关系，$a, b \in A$。如果aRb，则称a与b等价。如果aRb，由R 的对称性可知，bRa，我们称a与b彼此等价。由R的自反性可知，任给$a \in A$，aRa，所以A 中每个元素与其自身等价。又由R的传递性可知，若a与b等价，且b与c等价，则a与c等价。

定义 4.10. 设R是集合A上的等价关系。任给$a \in A$，记$[a]_R$为A中所有与a等价的元素构成的集合，即

$$[a]_R = \{x | x \in A, aRx\}.$$

由于a与其自身等价，$a \in [a]_R$，称$[a]_R$为元素a所属的等价类，也称元素a是等价类$[a]_R$的代表元。

定理 4.5. 设R是集合A上的等价关系，则等价类满足：

（1）任给$a, b \in A$，要么$[a]_R = [b]_R$，要么$[a]_R \cap [b]_R = \emptyset$。

（2）$\bigcup_{a \in A}[a]_R = A$。

证明： （1）任给$a, b \in A$，要么aRb，要么$a\not Rb$，两者必居其一。

先看aRb的情况。由R的对称性可知，bRa。任取$x \in [a]_R$，由等价类的定义知，aRx，再由R的传递性知，bRx，所以$x \in [b]_R$。故$[a]_R \subseteq [b]_R$。同理可得，$[b]_R \subseteq [a]_R$。所以$[a]_R = [b]_R$。

再看$a\not Rb$的情况。如果$[a]_R \cap [b]_R \neq \emptyset$，则存在$x \in [a]_R \cap [b]_R$，即$x \in [a]_R$且$x \in [b]_R$。由等价类的定义知，$aRx$且$bRx$。因为$R$是对称的，由$bRx$得出$xRb$。又因为$R$是传递的，由$aRx$和$xRb$得出$aRb$。与假设$a\not Rb$矛盾，故$[a]_R \cap [b]_R = \emptyset$。

由上面的证明可知，彼此等价的元素属于同一个等价类，彼此不等价的元素所属的等价类没有公共元素。

（2）任取$x \in \bigcup_{a\in A}[a]_R$，存在$a \in A$，使得$x \in [a]_R$。因为$[a]_R$是$A$的子集，故$x \in A$。由此得出，$\bigcup_{a\in A}[a]_R \subseteq A$。

反之，任取$x \in A$，显然$x \in [x]_R \subseteq \bigcup_{a\in A}[a]_R$。所以，$A \subseteq \bigcup_{a\in A}[a]_R$。

综上可得，$A = \bigcup_{a\in A}[a]_R$。证毕。

定义 4.11. 设A是一个非空集合。如果集合族$\mathbb{A} = \{A_1, A_2, \cdots, A_k, \cdots\}$满足：

（1）任给i，$A_i \subseteq A$，即A_i是A的子集，

（2）任给$i \neq j$，$A_i \cap A_j = \emptyset$或者$A_i = A_j$，

（3）$\bigcup_{i=1}^{+\infty} A_i = A$，

则称集合族$\mathbb{A}$是A的一个划分。

若R是集合A上的等价关系，则由定理4.5知，等价类集合$\{[a]_R | a \in A\}$是集合A的一个划分，我们称之为集合A关于等价关系R的商集，记作A/R。

例 4.13. 设$\mathbb{Z}$是整数集合，R_n是$\mathbb{Z}$上的模n同余关系，即任给$a, b \in \mathbb{Z}$，

$$xR_ny, \quad \text{当且仅当} \quad n|x-y, \text{也即} x \equiv y \mod n.$$

我们曾经在第二章介绍过，同余关系是自反的、对称的与传递的，所以R_n是$\mathbb{Z}$上的等价关系。$[0]_{R_n}, [1]_{R_n}, \cdots, [n-1]_{R_n}$是$R_n$所确定的全部等价类。

例 4.14. 设R是复数集合$\mathbb{C}$上的二元关系，任给$x, y \in \mathbb{C}$，xRy当且仅当$|x| = |y|$，其中$|x|$、$|y|$分别为复数x与y的模。则R是$\mathbb{C}$上的等价关系。任给$x \in \mathbb{C}$，x所在的等价类$[x]_R$就是以坐标原点O为圆心，半径为$|x|$的圆，参见图4.3。所有以O 为圆心的圆构成$\mathbb{C}$关于R的所有等价类。正数轴$[0, +\infty)$上所有的数是所有等价类的代表元，这是因为每个等价类中都有且仅有一个元素在正数轴上。

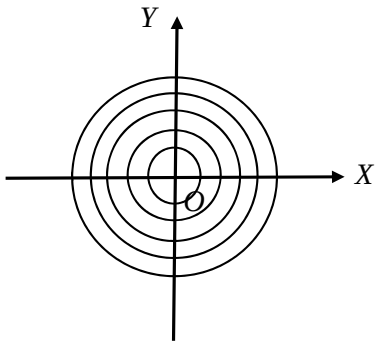


图 4.3: 例4.14中等价类的示意图

例 4.15. 在平面几何中，设A是各种几何图形构成的集合，如果一个几何图形经过平移或旋转，可以与另一个几何图形完全重合，则称这两个几何图形“全等”。这种“全等”关系是等价关系。彼此全等的几何图形构成一个等价类。

如果一个几何图形经过成比例放大或缩小，可以与另一个几何图形完全重合，则称这两个几何图形“相似”。几何图形间的“相似”关系也是等价关系。彼此相似的几何图形构成一个等价类。例如，所有的圆就是属于同一个相似的等价类。

由定理4.5知，集合A上的等价关系决定了A的一个划分，该划分由各个不同的等价类构成。反过来，给定集合A的一个划分，也决定了集合A的一个等价关系。

定理 4.6. 设集合族$\mathbb{A} = \{A_1, A_2, \cdots, A_k, \cdots\}$是非空集合$A$的一个划

分。定义集合A上的二元关系R，任给$x, y \in A$，

$$xRy \quad \text{当且仅当存在} i, \text{使得} x \in A_i \text{且} y \in A_i,$$

则关系R是集合A上的等价关系。

证明： 因为$\mathbb{A} = \{A_1, A_2, \cdots, A_k, \cdots\}$是集合$A$的一个划分，所以$\bigcup_{i=1}^{+\infty} A_i = A$，任给$x \in A$，存在$i$，使得$x \in A_i$。由$R$的定义知，$xRx$，所以$R$是自反的。任给$x, y \in A$，如果$xRy$，则存在$i$，使得$x \in A_i$ 且$y \in A_i$，所以yRx，故R是对称的。任给$x, y, z \in A$，若xRy且yRz。由xRy得知，存在i，使得$x \in A_i$且$y \in A_i$；而由yRz 又可以得知，存在j，使得$y \in A_j$且$z \in A_j$。因为$\mathbb{A}$是A的划分，所以A中每个元素只能属于某一个A_i。因为y 在A_i与A_j中，所以$i = j$。从而$x, y, z \in A_i = A_j$。由R的定义知，xRz，所以R是传递的。

综上分析知，R是集合A上的等价关系，它所确定的等价类集合就是$\mathbb{A}$。证毕。

在一个集合上，用不同方式定义的两个等价关系可能产生同一个集合划分。例如，设$A = \{1, 2, \cdots, 9\}$。在A上定义等价关系R_1和R_2，其中R_1的定义为：任给$x, y \in A$，

$$xR_1y \quad \text{当且仅当} 3|x - y.$$

而R_2则通过下面的矩阵来定义

$$\begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{pmatrix}。$$

任给$x, y \in A$，xR_2y当且仅当x与y在上述矩阵的同一列中。则R_1与R_2都是集合A 上的等价关系，它们产生的等价类都是

$$[1]_{R_1} = [1]_{R_2} = \{1, 4, 7\}, [2]_{R_1} = [2]_{R_2} = \{2, 5, 8\}, [3]_{R_1} = [3]_{R_2} = \{3, 6, 9\}.$$

这时我们称$R_1 = R_2$。事实上，集合的划分与集合上的等价关系一一对应，两个等价关系对应的集合划分相同，意味着两个等价关系本质上相同。

4.3 序关系

序关系是另一类重要的二元关系。

4.3.1 偏序关系

定义 4.12. 设$\preceq$是集合A上的二元关系，如果$\preceq$是自反的、反对称的、传递的，则称$\preceq$ 是集合A上的偏序关系，或叫偏序。集合A和A上的一个偏序$\preceq$构成偏序集，记作$< A, \preceq >$。

例 4.16. 实数集合$\mathbb{R}$上的大于等于关系“$\geq$”和小于等于关系“$\leq$”都是偏序。$< \mathbb{R}, \geq >$ 与$< \mathbb{R}, \leq >$都是偏序集。

例 4.17. 假设A是一个集合，在A的幂集$\mathscr{P}(A)$上定义包含关系“$\supseteq$”与被包含关系“$\subseteq$”，则“$\supseteq$”与“$\subseteq$”都是$\mathscr{P}(A)$上的偏序关系，$< \mathscr{P}(A), \supseteq >$、$< \mathscr{P}(A), \subseteq >$都是偏序集。

设$\preceq$是集合A上的偏序，a与b是A中两个元素。如果$a \preceq b$或者$b \preceq a$，则称a与b是可比较的；若$a \npreceq b$且$b \npreceq a$，则称a 与b是不可比较的。由偏序$\preceq$的自反性可知，A中每个元素与其自身都是可比较的。一般来说，集合中任取两个元素a与b，可能a与b不可比较。例如，假设$A = \{1, 2, 3\}$，幂集$\mathscr{P}(A)$上的包含关系“$\supseteq$”是偏序。但是，A的两个子集$\{1, 2\}$与$\{2, 3\}$之间就不可比较。

4.3.2 线序关系

定义 4.13. 设$\preceq$是集合A上的偏序。如果A中任意两个元素a与b都是可比较的，即$a \preceq b$ 或$b \preceq a$成立，那么称$\preceq$是线序关系或完全序关系，简称线序或完全序。$< A, \preceq >$称为线序集。

注意，在定义4.13中，若$a = b$，因为$\preceq$是自反的，当然有$a \preceq b$ 与$b \preceq a$同时成立；但是若$a \neq b$，则$a \preceq b$与$b \preceq a$只能有一个成立。

例4.16中的$< \mathbb{R}, \geq >$与$< \mathbb{R}, \leq >$都是线序集。

例 4.18. 设$< A, \preceq >$是线序集。为了方便，我们用$a \preceq_{\neq} b$表示$a \preceq b$且$a \neq b$。现在定义A^n上的二元关系$\preceq'$。任给$(a_1, a_2, \cdots, a_n), (b_1, b_2, \cdots, b_n) \in A^n$，$(a_1, a_2, \cdots, a_n) \preceq' (b_1, b_2, \cdots, b_n)$，当且仅当下面三个条件之一成立：

（1）$(a_1, a_2, \cdots, a_n) = (b_1, b_2, \cdots, b_n)$，

（2）$a_1 \preceq_{\neq} b_1$，

（3）存在$1 \leq i \leq n-1$，使得对任意$1 \leq j \leq i$，都满足$a_j = b_j$，而且$a_{i+1} \preceq_{\neq} b_{i+1}$。

则$\preceq'$是A^n上的偏序，也是线性序。

证明： 事实上，$(a_1, a_2, \cdots, a_n) \in A^n$等价于$a_1 a_2 \cdots a_n$是$A$中元素构成的长为$n$ 的字符串。如果将$\preceq$看作A中元素之间的一种顺序，则关系$\preceq'$就是由A 中元素构成长为n的字符串之间的字典序。对于非数值字符串来说，这是一种常见的排序方式，在计算机科学中有重要应用。

首先，由条件（1）可知，$\preceq'$是自反的。

其次，若$(a_1, a_2, \cdots, a_n) \preceq' (b_1, b_2, \cdots, b_n)$，则由定义中的三个条件知，要么$a_1 = b_1$，要么$a_1 \preceq_{\neq} b_1$，都满足$a_1 \preceq b_1$。同理，如果$(b_1, b_2, \cdots, b_n) \preceq' (a_1, a_2, \cdots, a_n)$，则有$b_1 \preceq a_1$。因为$\preceq$ 是偏序，满足反对称性，可以得出$a_1 = b_1$。在得到$a_1 = b_1$ 之后，条件（2）不成立，因此要么条件（1）成立，得到$(a_1, a_2, \cdots, a_n) = (b_1, b_2, \cdots, b_n)$；要么条件（3）成立，则由$(a_1, a_2, \cdots, a_n) \preceq' (b_1, b_2, \cdots, b_n)$ 知，$a_2 = b_2$或者$a_2 \preceq_{\neq} b_2$，都可以得出$a_2 \preceq b_2$。同理，由$(b_1, b_2, \cdots, b_n) \preceq' (a_1, a_2, \cdots, a_n)$可以得出，$b_2 \preceq a_2$。由$\preceq$ 的反对称性，知$a_2 = b_2$；...；如此递归可以得出$a_1 = b_1$、$a_2 = b_2$、...、$a_n = b_n$，即$(a_1, a_2, \cdots, a_n) = (b_1, b_2, \cdots, b_n)$。故$\preceq'$是反对称的。

最后证明$\preceq'$是传递的。设$(a_1, a_2, \cdots, a_n) \preceq' (b_1, b_2, \cdots, b_n)$，则满足前面的三个条件（1）、（2）和（3）。假设$(b_1, b_2, \cdots, b_n) \preceq' (c_1, c_2, \cdots, c_n)$，则满足下面的三个条件之一：

（I）$(b_1, b_2, \cdots, b_n) = (c_1, c_2, \cdots, c_n)$，

（II）$b_1 \preceq_{\neq} c_1$，

（III）存在$1 \leq i' \leq n-1$，使得对任意$1 \leq j \leq i'$，都满足$b_j = c_j$，而且$b_{i'+1} \preceq_{\neq} c_{i'+1}$。

我们可以综合分析，在满足三个条件（1）、（2）、（3）之一和满足

三个条件（I）、（II）、（III）之一的各种组合，来证明$(a_1, a_2, \cdots, a_n) \preceq' (c_1, c_2, \cdots, c_n)$。这里，只给出满足条件（3）与（III）时的证明。

假设条件（3）与（III）成立，分两种情况。首先，若$i \geq i' + 1$，那么对任意$1 \leq j \leq i'$，都满足$a_j = b_j = c_j$，而且$a_{i'+1} = b_{i'+1}$、$b_{i'+1} \preceq_{\neq} c_{i'+1}$，所以有$a_{i'+1} \preceq_{\neq} c_{i'+1}$。由$\preceq'$的定义知，$(a_1, a_2, \cdots, a_n) \preceq' (c_1, c_2, \cdots, c_n)$。再者，若$i < i' + 1$，则对任意的$1 \leq j \leq i$，都满足$a_j = b_j = c_j$，而且$b_{i+1} = c_{i+1}$、$a_{i+1} \preceq_{\neq} b_{i+1}$，从而$a_{i+1} \preceq_{\neq} c_{i+1}$。由$\preceq'$的定义知，$(a_1, a_2, \cdots, a_n) \preceq' (c_1, c_2, \cdots, c_n)$。所以$\preceq'$满足传递性。

综上可知，$\preceq'$是A^n上的偏序。

事实上，$\preceq'$也是A^n上的线序。任给A中两个元素$(a_1, a_2, \cdots, a_n)$和$(b_1, b_2, \cdots, b_n)$，我们只需从左至右，逐个比较两个n元组的元素即可。比较过程是：若$a_1 \neq b_1$，由于$\preceq$是线序，必有$a_1 \preceq b_1$或$b_1 \preceq a_1$，所以有$a_1 \preceq_{\neq} b_1$或$b_1 \preceq_{\neq} a_1$，由条件（2）知，$(a_1, a_2, \cdots, a_n) \preceq' (b_1, b_2, \cdots, b_n)$或者$(b_1, b_2, \cdots, b_n) \preceq' (a_1, a_2, \cdots, a_n)$。如果，$a_1 = b_1$，就比较$a_2$和$b_2$。一般地，若$a_1 = b_1$、$a_2 = b_2$、...、$a_i = b_i$，而$a_{i+1} \neq b_{i+1}$，则$a_{i+1} \preceq_{\neq} b_{i+1}$或$b_{i+1} \preceq_{\neq} a_{i+1}$，从而$(a_1, a_2, \cdots, a_n) \preceq' (b_1, b_2, \cdots, b_n)$或者$(b_1, b_2, \cdots, b_n) \preceq' (a_1, a_2, \cdots, a_n)$。最后，若$(a_1, a_2, \cdots, a_n) = (b_1, b_2, \cdots, b_n)$，也同样满足$(a_1, a_2, \cdots, a_n) \preceq' (b_1, b_2, \cdots, b_n)$。所以，$\preceq'$是$A^n$上的线序，是$A^n$中元素的字典序。

4.3.3 极大元与极小元

定义 4.14. 设$< A, \preceq >$为偏序集，$x, y \in A$，如果$x \preceq_{\neq} y$，并且不存在$z \in A$，使得$x \preceq_{\neq} z$且$z \preceq_{\neq} y$，则称元素y控制元素x，或者说元素x 被元素y 控制，记作$x \widehat{\preceq} y$。

在偏序集中，不是每个元素都能控制着某个其它元素，也不是每个元素都被别的元素所控制。例如，偏序集$< \mathbb{R}, \leq >$中，每个元素都不控制别的元素，而且每个元素也不被其它元素所控制。

定理 4.7. 设$< A, \preceq >$为偏序集。当A是有限集合时，对于A中元素a，如果有元素$b \in A$，使得$a \preceq_{\neq} b$，则一定存在b'，使得$a \widehat{\preceq} b'$，即a的控制元素一定存在。

证明： 设$< A, \preceq >$为偏序集，对于$a \in A$，存在$b \in A$，使得$a \preceq_{\neq} b$，则有两种可能。(1) 若b是a的控制元素，$a \widehat{\preceq} b$，取$b' = b$ 即可；(2) b不是a的控制元素，那么由定义4.14可知，存在$b_1 \in A$，使得$a \preceq_{\neq} b_1$且$b_1 \preceq_{\neq} b$。这里仍然有两个可能，一个是b_1是a的控制元素，另一个是存在$b_2 \neq b_1$，使得$a \preceq_{\neq} b_2$且$b_2 \preceq_{\neq} b_1$。这里我们可以得出$b_2 \neq b$。否则，若$b_2 = b$，那么$b_2 \preceq_{\neq} b_1$就是$b \preceq_{\neq} b_1$，再加上$b_1 \preceq_{\neq} b$，由$\preceq$ 的反对称性可知，$b_1 = b$。这与$b_1 \neq b$矛盾。故$b_2 \neq b$。

如果我们一直找不到元素a的控制元素，上述过程就可以无限地进行下去，得到无限序列$b_1, b_2, \cdots, b_n, \cdots$，其中$b_i \in A$，满足$a \preceq_{\neq} \cdots$、$b_n \preceq_{\neq} b_{n-1}$、$b_{n-1} \preceq_{\neq} b_{n-2}$、...、$b_3 \preceq_{\neq} b_2$、$b_2 \preceq_{\neq} b_1$、$b_1 \preceq_{\neq} b$，而且$b_1, b_2, \cdots, b_n, \cdots$ 互不相同，与A是有限集合矛盾。于是，存在某个i，使得上述过程终止，即$a \preceq_{\neq} b_i$，且b_i是a的控制元素。证毕。

从这个定理可以看出，若$\preceq$是有限集合A上的偏序关系，则对于任意$a \in A$，要么不存在元素b，使得$a \preceq_{\neq} b$；要么a存在控制元素。同样的道理可知，要么不存在元素b，使得$b \preceq_{\neq} a$；要么a控制某个元素。

例 4.19. 设$S = \{1, 2, 3, 4, 6, 12\}$。$S$上的整除关系是偏序关系。元素1的控制元素为2与3。元素2 的控制元素为4与6，元素3的控制元素为6，元素4与6的控制元素为12。元素12没有控制元素。

定义 4.15. 设$< A, \preceq >$为偏序集，对于$a \in A$，如果不存在元素$b \in A$，使得$a \preceq_{\neq} b$，则称a为偏序集$< A, \preceq >$的极大元；如果不存在元素$b \in A$，使得$b \preceq_{\neq} a$，则称a 为偏序集$< A, \preceq >$的极小元。

根据定理4.7，每个有限偏序集都可以绘成一个图，称为哈希（Hasse）图。假设$< A, \preceq >$为偏序集，且A是有限集合。将A中的每个元素用一个点来表示，对于$a, b \in A$，如果b是a的控制元素，即$a \widehat{\preceq} b$，则将b画在a的上方，且在a 与b之间画一条线。这样就得到了$< A, \preceq >$ 对应的哈希图。哈希图可以直观地将偏序关系表示出来，对研究偏序集的结构提供方便。在哈希图中，位于最上方的元素是极大元，位于最下方的元素是极小元，其余每个元素用线段向上连至它的全部控制元素，向下用线段连至全部被它控制的元素。

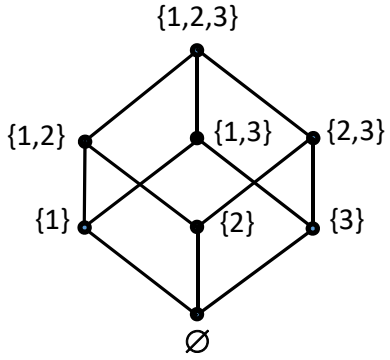


图 4.4: 例4.20对应的哈希图

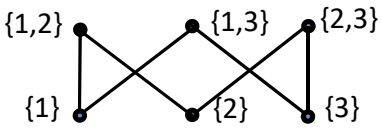


图 4.5: 例4.21对应的哈希图

例 4.20. 设$S = \{1, 2, 3\}$。偏序集$< \mathscr{P}(S), \subseteq >$的哈希图参见图*4.4*。其中$\{1, 2, 3\}$是极大元，$\emptyset$是极小元。

例 4.21. $< \{\{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}\}, \subseteq >$是偏序集，对应的哈希图参见图*4.5*，其中，$\{1, 2\}, \{1, 3\}, \{2, 3\}$都是极大元，$\{1\}, \{2\}, \{3\}$都是极小元。

例 4.22. $B = \{1, 2, 3, 5, 6, 10, 15, 30\}$，$B$与其上的整除关系构成偏序集$< B, | >$，对应的哈希图参见图*4.6*，其极大元是30，极小元是1。

例4.20与例4.22中两个偏序集的哈希图相同。这表明，尽管$< \mathscr{P}(S), \subseteq >$与$< B, | >$的具体含义不同，但它们元素之间的序结构完全相同。若两个偏序集的哈希图相同，我们称其是**序同构**的。

例 4.23. $< \{1, 2, 4, 5, 10\}, \leq >$是偏序集，对应的哈希图参见图*4.7*，它的哈希图是一条链。不难看出，若A是有限集合，则A上的偏序集是线序集，当且仅当它的哈希图是一条链。

4.3.4 最大元与最小元

定义 4.16. 设$< A, \preceq >$为偏序集，$a \in A$。若任给$b \in A$，都有$b \preceq a$，则称a为$< A, \preceq >$ 的最大元；若任给$b \in A$，都有$a \preceq b$，则称a为$< A, \preceq >$的最小元。

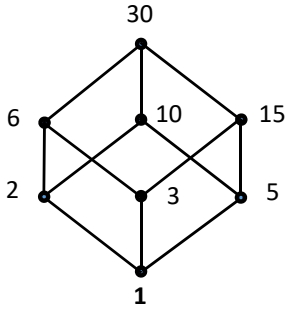


图 4.6: 例4.22对应的哈希图

图 4.7: 例4.23对应的哈希图

在例4.20中，$\{1,2,3\}$是最大元，$\emptyset$是最小元。例4.21中没有最大元与最小元。例4.22中，30是最大元，1 是最小元。在例4.23中，10是最大元，1是最小元。

下面分析极大元、极小元、最大元与最小元的性质。

定理 4.8. 偏序集$< A, \preceq >$的最大元一定是极大元。

证明: 用反证法。设a是偏序集$< A, \preceq >$的最大元，若a不是$< A, \preceq >$的极大元，则存在$b \in A$，使得$a \preceq_{\neq} b$，即$a \neq b$且$a \preceq b$。由于a 是$< A, \preceq >$ 的最大元，所以必然有$b \preceq a$。再从$\preceq$的反对称性，可以推出$a = b$，与$a \neq b$矛盾。所以偏序的最大元必是极大元。证毕。

定理 4.9. 偏序集$< A, \preceq >$的最大元最多只有一个。

证明: 从前面的例子可以看出，偏序集不一定有最大元，比如说例4.21中的偏序集就没有最大元。

如果偏序集$< A, \preceq >$有最大元，设$a, b \in A$都是最大元。因为a是最大元，则任给$x \in A$，都满足$x \preceq a$，所以有$b \preceq a$。同理，由b是最大元，可以得出$a \preceq b$。由于$\preceq$满足反对称性，$b \preceq a$且$a \preceq b$，所以$a = b$。这说明当$< A, \preceq >$有最大元时，一定唯一。证毕。

定理 4.10. 假设A是有限集合，偏序集$< A, \preceq >$存在最大元，当且仅当$< A, \preceq >$只有一个极大元。

证明: 设a是$< A, \preceq >$的最大元。由定理4.8 知，a 是$< A, \preceq >$的极大元。假如存在$b \in A$且$b \neq a$，b也是极大元。由于a 是最大元，所以$b \preceq a$。而且$b \neq a$，所以$b \preceq_{\neq} a$，这与b是极大元矛盾。所以说，$< A, \preceq >$ 只有一个极大元。

反之，设a是$< A, \preceq >$唯一的极大元，我们要证明a是$< A, \preceq >$的最大元。任给$b \in A$ 且$b \neq a$。因为b不是极大元，所以存在$c_1 \in A$，使得$b \preceq_{\neq} c_1$。下面分两种情况来讨论。

其一是$c_1 = a$，则由于$b \preceq_{\neq} c_1$，可以得到$b \preceq a$。

另一种情况是$c_1 \neq a$。因为a是唯一极大元，故c_1也不是极大元，从而存在$c_2 \in A$ 且$c_2 \neq c_1$，使得$c_1 \preceq_{\neq} c_2$。这时又有两种情况:（1）$c_2 = a$，那么从$b \preceq_{\neq} c_1$、$c_1 \preceq_{\neq} c_2$以及$c_2 = a$，可以得出$b \preceq a$;（2）$c_2 \neq a$，那么c_2也不是极大元，存在$c_3 \in A$，使得$c_2 \preceq_{\neq} c_3$，而且由$b \preceq_{\neq} c_1$、$c_1 \preceq_{\neq} c_2$、$c_2 \preceq_{\neq} c_3$ 可知，b, c_1, c_2, c_3 互不相等。这样一直分析下去，得到元素序列c_1, c_2, c_3, $\cdots$,，而且这个序列中的元素两两不同。由于A是有限集合，这一过程一定会终止。也就是说，存在某个i，使得

$$b \preceq_{\neq} c_1, c_1 \preceq_{\neq} c_2, c_2 \preceq_{\neq} c_3, \cdots, c_{i-1} \preceq_{\neq} c_i, c_i \preceq_{\neq} c_{i+1},$$

而且$c_{i+1} = a$。由于$\preceq$满足传递性，可以得出$b \preceq a$。

综上可以得出，任给$b \in A$，都满足$b \preceq a$，所以a是$< A, \preceq >$的最大元。

因此，若A是有限集合，偏序集$< A, \preceq >$存在最大元，当且仅当$< A, \preceq >$只有一个极大元。证毕。

类似，可以证明下面的定理:

定理 4.11. 假设A是有限集合，偏序集$< A, \preceq >$存在最小元，当且仅当$< A, \preceq >$只有一个极小元。

4.3.5 上界与下界

定义 4.17. 设$< A, \preceq >$为偏序集，$M \subseteq A$，$a \in A$。如果对于任意$m \in M$，都有$m \preceq a$，则称a是子集M的上界；如果对于任意$m \in M$，都有$a \preceq m$，则称a是子集M的下界。

集合A的任意子集M不一定有上界或下界。即使有上界或下界，也不一定唯一。例如，$< \{1,2,3,4,5,6\}, | >$是偏序集，它的哈希图参见图4.8。$< \{1,2,3,4,5,6\}, | >$的最小元是1，无最大元，$4,5,6$是极大元。子集$\{1,2,4\}$的上界是4，子集$\{1,3\}$的上界是3和6，子集$\{3,4\}$无上界。

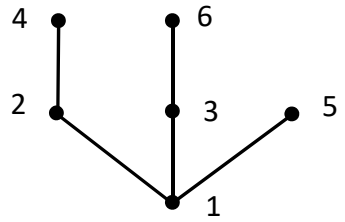


图 4.8: 上下界示例

一般的上界与下界对研究问题的意义不是很大，人们往往更关注的是最小上界与最大下界。参见定义4.18。

定义 4.18. 设$< A, \preceq >$为偏序集，$a \in A$是$M \subseteq A$的上界。如果任给M的上界a'，都有$a \preceq a'$，则称a是M的最小上界或上确界。

$b \in A$是$M \subseteq A$的下界。如果任给M的下界b'，都有$b' \preceq b$，则称b 是M的最大下界或下确界。

4.4 集合的势

对于有限集合来说，我们可以数出其中元素的个数，得到有限集合的阶，从而可以比较两个有限集合中元素的多少。但对于无限集合来说，我们就无法数出其中元素的个数。为了比较无限集合在元素个数上的差异，本节引入集合势的概念。集合势适用于有限集合与无限集合。

定义 4.19. 如果存在从集合A到集合B的双射，那么称集合A与集合B等势，记作$A \sim B$。

例 4.24. 集合$\mathbb{N} = \{0,1,2,3,\cdots\}$，$\mathbb{N}_2 = \{0,2,4,6,\cdots\}$。定义映射$f : \mathbb{N} \to \mathbb{N}_2$，任给$n \in \mathbb{N}$，$f(n) = 2n$，则$f$ 是$\mathbb{N}$到$\mathbb{N}_2$的双射。从而$\mathbb{N}$与$\mathbb{N}_2$等势。

定理 4.12. 设E是万有集合，$\mathscr{P}(E)$是所有集合构成的集合族。集合间的等势关系$\sim$是$\mathscr{P}(E)$ 上的等价关系。

证明: 任给集合$A \in \mathscr{P}(E)$，定义映射$I_A : A \to A$。任给$a \in A$，$I_A(a) = a$，则I_A是A到其自身的双射，所以$A \sim A$，故$\sim$满足自反性。任给$A, B \in \mathscr{P}(E)$，若$A \sim B$，则存在A到B的双射$f : A \to B$，则f的逆映射$f^{-1} : B \to A$是B到A的双射，所以$B \sim A$，故$\sim$满足对称性。任给$A, B, C \in \mathscr{P}(E)$，若$A \sim B$且$B \sim C$，则存在双射$f : A \to B$和双射$g : B \to C$，由复合映射的性质（定理3.8）可知，$g \circ f : A \to C$是集合$A$到集合$C$的双射，所以$A \sim C$。故$\sim$满足传递性。

综上，$\sim$是$\mathscr{P}(E)$上的等价关系。证毕。

利用等势关系，可以对所有的集合进行等价分类，在同一个等价类中的集合是等势的。

4.4.1 有限集合与可数集合

定义 4.20. 记$|0, n| = \{0, 1, 2, \cdots, n\}$，称为自然数集合的一个断片。与自然数的某个断片等势的集合称为有限集合。空集合$\emptyset$也称为有限集合。不是有限集合的集合叫作无限集合。

如果集合A与$|0, n|$等势，则存在双射$f : |0, n| \to A$，对于$0 \leq i \leq n$，记$f(i) = a_i$，则有$A = \{a_0, a_1, a_2, \cdots, a_n\}$。可以将有限集合中的元素一个一个地数出来，所以有限集合的势可以用其中的元素个数来表示，也就是有限集合的阶。空集合的势为0。

任何有限集合不能与其真子集等势。这是因为，若A、B是有限集合且$A \subset B$，则必有$|A| < |B|$。A与B之间不可能存在双射，故$A \not\sim B$。然而，无限集合可以与其真子集等势。例如，在例4.24 中，$\mathbb{N}_2$ 是$\mathbb{N}$的真子集，但是$\mathbb{N} \sim \mathbb{N}_2$。

定义 4.21. 与自然数集合$\mathbb{N}$等势的集合叫作可数无限集合。

有限集合与可数无限集合统称为可数集合，非可数集合称为不可数集合。

若集合A与自然数集合$\mathbb{N}=\{0,1,2,\cdots\}$等势，那么存在双射$f:\mathbb{N}\to A$。记$f(i)=a_i$，则$A=\{a_0,a_1,a_2,\cdots\}$，所以无限可数集合中的元素可以逐个枚举出来，自然数集合的势记为$\aleph_0$。

下面来看一个不可数集合的例子。

例 4.25. 集合$(0,1)=\{x|x\in\mathbb{R},0<x<1\}$是不可数集合。

证明： 首先证明$(0,1)$是无限集合。取$(0,1)$的子集$C=\{\frac{1}{2},\frac{1}{3},\cdots,\frac{1}{n},\cdots\}\subset(0,1)$，定义映射$f:C\to\mathbb{N}$，$f(\frac{1}{n})=n-2$，则$f$是$C$到$\mathbb{N}$的双射，故$C\sim\mathbb{N}$。因为$C$是无限集合，而且$C\subset(0,1)$，所以$(0,1)$是无限集合。

下面证明$(0,1)$是不可数集合。假设$(0,1)$是可数集合，将$(0,1)$中所有的元素逐个枚举出来，记为$(0,1)=\{b_1,b_2,\cdots,b_n,\cdots\}$。将$(0,1)$中的每个元素表示成小数，设为

$$\begin{aligned}
&b_1=0.a_{11}a_{12}\cdots a_{1n}\cdots,\\
&b_2=0.a_{21}a_{22}\cdots a_{2n}\cdots,\\
&\cdots\quad\cdots\quad\cdots\quad\cdots,\\
&b_n=0.a_{n1}a_{n2}\cdots a_{nn}\cdots,\\
&\cdots\quad\cdots\quad\cdots\quad\cdots,
\end{aligned}$$

我们取$d=0.d_1d_2\cdots d_n\cdots$，其中，任给$i=1,2,\cdots,n,\cdots$，$d_i\neq a_{ii},0,9$，也就是说，$d_i$可以任取$\{1,2,3,4,5,6,7,8\}$中某个不等于$a_{ii}$的数字，这是一定可以取到的。因为$d_i\neq 0,9$，所以$d\in(0,1)$。另一方面，对于任意$i\geq 1$来说，$d_i\neq a_{ii}$，也就是$d$的第$i$位小数不等于$b_i$的第$i$位小数，所以有$d\neq b_i$，从而$d\notin\{b_1,b_2,\cdots,b_n,\cdots\}=(0,1)$。矛盾。所以，$(0,1)$ 是不可数集合。

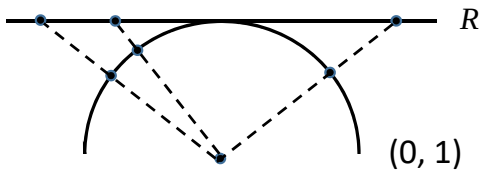


图 4.9: $(0,1)$与$\mathbb{R}$等势证明示意图

可以证明，集合$(0,1)$与实数集合$\mathbb{R}$是等势的。图4.9给出了其证明的示意图。我们将开区间$(0,1)$的有限长线段弯曲成一个半圆，用无限长的横坐

标轴来表示实数R，横坐标轴与半圆弧相切于半圆弧的中点。如果从半圆的圆心引出直线，使之与半圆弧，以及横坐标轴相交，这两个交点必定成对出现，从而形成从$(0,1)$到$\mathbb{R}$的双射。故$(0,1)$与$\mathbb{R}$的势相同，记为$\mathscr{N}_1$。

4.4.2 势的大小

定义 4.22. 如果集合A与集合B的一个子集等势，则称B支配A，记为$A \preceq B$，并且说A的势小于等于B的势，记为A的势$\leq B$的势。

如果$A \preceq B$，并且$A \not\sim B$，则称$A \prec B$，也说A的势小于B的势，记为A的势$< B$的势。

例如，自然数集合是实数集合的子集，即$\mathbb{N} \subseteq \mathbb{R}$，故自然数集合$\mathbb{N}$ 的势$\mathscr{N}_0 \leq$实数集合$\mathbb{R}$的$\mathscr{N}_1$。又因为$\mathbb{N} \not\sim \mathbb{R}$，所以$\mathscr{N}_0 < \mathscr{N}_1$。

定理 4.13. 将集合A的幂集记为$\mathscr{P}(A)$，那么A的势小于$\mathscr{P}(A)$的势，即$A \prec \mathscr{P}(A)$。

证明： 首先证明$A \preceq \mathscr{P}(A)$。记$\overline{\mathscr{P}}(A) = \{\{a\} | a \in A\}$，则$\overline{\mathscr{P}}(A) \subset \mathscr{P}(A)$。定义$f : A \to \overline{\mathscr{P}}(A)$，任给$a \in A$，$f(a) = \{a\}$，则易知$f$是$A$到$\overline{\mathscr{P}}(A)$的双射，而且$\overline{\mathscr{P}}(A) \subset \mathscr{P}(A)$，所以$A \preceq \mathscr{P}(A)$。

下面证明$A \prec \mathscr{P}(A)$。因为已经证明$A \preceq \mathscr{P}(A)$，只需证明$A \not\sim \mathscr{P}(A)$。假设$A \sim \mathscr{P}(A)$，则存在双射$g : A \to \mathscr{P}(A)$。我们把集合$A$中的元素分成两类：内部成员与外部成员。任给$a \in A$，如果$a \in g(a)$，则称$a$为内部成员，否则称$a$为外部成员。令$B = \{x | x \in A, x \notin g(x)\}$，即$B$是全体外部成员构成的集合，是$A$的子集，$B \in \mathscr{P}(A)$。

因为g是双射，所以是满射，因此存在$b \in A$，使得$g(b) = B$。如果b是内部成员，则有$b \in g(b) = B$。而B为外部成员集合，与$b \in g(b)$矛盾。如果b是外部成员，应该$b \notin g(b) = B$。另一方面B是所有外部成员构成的集合，b是外部成员，应该$b \in B$，但$b \notin B$，故矛盾。

综上所述，$A \sim \mathscr{P}(A)$不成立，即$A \not\sim \mathscr{P}(A)$，加之$A \preceq \mathscr{P}(A)$，得到$A \prec \mathscr{P}(A)$。证毕。

定理 4.14. 设E是万有集合。$\mathscr{P}(E)$中集合间的支配关系“$\preceq$”是偏序关系。

证明： （1）对任意集合$A \in \mathscr{P}(E)$，定义映射$f : A \to A$，使得任意$a \in A$，$f(a) = a$。则f是A到A的双射，且$A \subseteq A$，所以$A \preceq A$。“$\preceq$”是自反的。

（2）任给$A, B, C \in \mathscr{P}(E)$，如果$A \preceq B$、$B \preceq C$，则存在子集$B_1 \subseteq B$、$C_1 \subseteq C$，以及双射$f : A \to B_1$和$g : B \to C_1$。因为$B_1 \subseteq B$，所以$f(B_1) \subseteq f(B)$，而且因为$g$是集合$B$到集合$C_1$的双射。所以$f(B) = C_1$。综上，记$f(B_1) = C_2$，则有$C_2 \subseteq C_1$。将$g$的原像限制到$B_1$上，则$g$ 也是B_1到C_2的双射，所以复合映射$g \circ f : A \to C_2$是A 到C_2的双射。而$C_2 \subseteq C$，所以$A \preceq C$。“$\preceq$”是传递的。

（3）下面证明支配关系“$\preceq$”是反对称的。假设$A, B \in \mathscr{P}(E)$，$A \preceq B$且$B \preceq A$，则存在$A_1 \subseteq A$与$B_1 \subseteq B$，以及双射$f : A \to B_1$和$g : B \to A_1$，从而A与B_1等势，B与A_1等势，即$A \sim B_1$且$B \sim A_1$。令$g(B_1) = A_2 \subseteq A_1 \subseteq A$，将$g$的原像限制到$B_1$ 上，$g : B_1 \to A_2$ 是双射，$B_1 \sim A_2$。由等势关系的传递性，得出$A \sim A_2$，即存在双射$h : A \to A_2$。类似，我们可以得到，存在A的子集合序列$A_1, A_2, A_3, \cdots$，满足

$$h(A) = A_2，其中A_2 \subseteq A_1, \tag{1}$$

$$h(A_1) = A_3，其中A_3 \subseteq A_2, \tag{2}$$

$$h(A_2) = A_4，其中A_4 \subseteq A_3, \tag{3}$$

$$h(A_3) = A_5，其中A_5 \subseteq A_4, \tag{4}$$

$$\cdots \quad \cdots$$

从而$A \supseteq A_1 \supseteq A_2 \supseteq \cdots \supseteq A_{n-1} \supseteq A_n \cdots$。因为$h$ 是一一映射，由（1）式与（2）式，可得$h(A - A_1) = h(A) - h(A_1) = A_2 - A_3$，于是有

$$A - A_1 \sim A_2 - A_3 \tag{5}$$

同理，由（3）式与（4）式，可得$h(A_2 - A_3) = h(A_2) - h(A_3) = A_4 - A_5$，于是有

$$A_2 - A_3 \sim A_4 - A_5 \tag{6}$$

$$\cdots \quad \cdots$$

记集合$C = A_1 \cap A_2 \cap \cdots \cap A_{n-1} \cap A_n \cdots$。任取$a \in A$，记$A_0 = A$，有以下两种可能性：

（1）$a \in C$，则任给$i = 1, 2, \cdots$，都满足$a \in A_i$；

（2）$a \notin C$，则存在某个$n \in \{1, 2, \cdots\}$，使得$a \in A_{n-1}$，但是$a \notin A_n$，所以$a \in A_{n-1} - A_n$。

从上面的分析可知，

$$A = C \cup (A - A_1) \cup (A_1 - A_2) \cup (A_2 - A_3) \cup \cdots,$$

$$A_1 = C \cup (A_1 - A_2) \cup (A_2 - A_3) \cup (A_3 - A_4) \cup \cdots。$$

又由（5）、（6）、...诸式，可以得到

$$(A - A_1) \cup (A_2 - A_3) \cup \cdots \sim (A_2 - A_3) \cup (A_4 - A_5) \cup \cdots,$$

即存在双射

$$f_0 : (A - A_1) \cup (A_2 - A_3) \cup \cdots \to (A_2 - A_3) \cup (A_4 - A_5) \cup \cdots。$$

再定义一个双射$f_1 : A \to A_1$，任给$a \in A$，

$$f_1(a) = \begin{cases} f_0(a), & a \in (A - A_1) \cup (A_2 - A_3) \cup \cdots, \\ a & a \in C \cup (A_1 - A_2) \cup (A_3 - A_4) \cup \cdots。 \end{cases}$$

不难看出，f_1是双射，即$A \sim A_1$。再由$B \sim A_1$，得出$A \sim B$，即A的势等于B的势。所以，支配关系“$\preceq$”满足反对称性。

综上所述，集合间的支配关系“$\preceq$”是偏序关系。证毕。

4.4.3 无限集合

定理 4.15. 每个无限集合都含有一个可数无限子集。

证明： 因为A是无限集合，所以不是空集合，存在$a_1 \in A$。而$A - \{a_1\}$仍是无限集合。同理，必存在$a_2 \in A - \{a_1\}$，显然$a_2 \neq a_1$。$\{a_1, a_2\}$是A的子集，$A - \{a_1, a_2\}$也是无限集合。如此进行下去，得到$S = \{a_1, a_2, \cdots, a_n, \cdots\}$是$A$的子集。而且，当$i \neq j$时，$a_i \neq a_j$，所以说，$S$就是无限集合$A$ 的可数无限子集。证毕。

定理 4.16. 每个无限集合都与它的某个真子集等势。

证明： 假设A是无限集合，由定理4.15知，A有一个可数无限子集$S = \{a_1, a_2, \cdots, a_n, \cdots\}$。构造映射$f : A \to A - \{a_1\}$，

$$f(a) = \begin{cases} a & a \in A - S, \\ a_{i+1} & a \in S \text{且} a = a_i, \end{cases}$$

则f是A到$A-\{a_1\}$的双射，所以$A \sim A-\{a_1\}$。证毕。

从这个定理可知，若一个集合与其真子集等势，则一定是无限集合；否则就一定是有限集合。

习题

1. 设E是万有集合，在$\mathscr{P}(E)$上定义下列关系，请说明这些关系具有什么性质?

（1）SR_1T，当且仅当$S \cap T = \emptyset$，

（2）SR_2T，当且仅当$S \cap T \neq \emptyset$，

（3）SR_3T，当且仅当$S \subset T$，

（4）SR_4T，当且仅当$S \subseteq T$，

（5）SR_5T，当且仅当$S = T$。

2. 请在整数集合$\mathbb{Z}$上给出三个二元关系，这三个关系分别具有以下性质:

（1）自反的、对称的，但不是传递的，

（2）自反的、传递的，但不是对称的，

（3）对称的、传递的，但不是自反的。

3. 设$\{a,b,c,d\}$，R_1、R_2是A上的关系，其中

$$R_1 = \{(a,a),(a,b),(b,d)\},$$

$$R_2 = \{(a,d),(b,c),(b,d),(c,b)\}。$$

求$R_1 \circ R_2$，$R_2 \circ R_1$，R_1^2，R_2^3。

4. R_1是集合B到集合C的关系，R_2与R_3是集合A到集合B的关系。证明:

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

5. 设R是集合A上的二元关系，I_A是A上的恒等关系。证明：$R' = R \cup I_A$是R的自反闭包。

6. $\mathbb{N}$是自然数集合，“$\sim$”是$\mathbb{N}\times\mathbb{N}$上的关系。任给$(a,b),(c,d) \in \mathbb{N}\times\mathbb{N}$，

$$(a,b) \sim (c,d), \quad 当且仅当 \quad a+d = b+c。$$

证明:“$\sim$”是$\mathbb{N}\times\mathbb{N}$上的等价关系，并在二维坐标平面上画出“$\sim$”确定的等价类。

7. 设$A=\{1,2,3,4\}$，在$\mathscr{P}(A)$上定义关系“$\sim$”。任给$S,T\in\mathscr{P}(A)$，

$$S\sim T,\quad \text{当且仅当}\quad |S|=|T|。$$

证明:“$\sim$”是$\mathscr{P}(A)$上的等价关系，并写出它的商集$\mathscr{P}(A)/\sim$。

8. 将非零实数集合记为$\mathbb{R}^*$，定义$\mathbb{R}^*$上的二元关系R。任给$x,y\in\mathbb{R}^*$，

$$xRy,\qquad \text{当且仅当}\quad x\times y>0。$$

证明：R是$\mathbb{R}^*$上的等价关系，列出所有等价类的代表元。

9. $\mathbb{R}$是实数集合，在$\mathbb{R}$上定义关系R。任给$x,y\in\mathbb{R}$，

$$xRy,\qquad \text{当且仅当}\quad x\text{与}y\text{相差一个整数}。$$

证明：R是$\mathbb{R}$上的等价关系，列出所有等价类的代表元。

10. 设R是集合X上的偏序，A是X的子集。证明：$R\cap(A\times A)$是A上的一个偏序关系。

11. 设A是非空集合，$\mathscr{B}$是A上所有二元关系构成的集合。在$\mathscr{B}$上定义二元关系$\preceq$。任给$R_1,R_2\in\mathscr{B}$，$R_1\preceq R_2$，当且仅当，对所有的$x,y\in A$，若xR_1y，则必有xR_2y。证明；$<\mathscr{B},\preceq>$是偏序集。

12. 设画出下列集合上整除关系的哈希图:

（1）$S=\{1,2,3,4,6,8,12,14\}$,

（2）$S=\{1,2,3,4,5,6,7,8,9,10,11,12\}$。

13. 假定图4.10给出的是不同偏序关系的关系图，请画出每个关系对应的哈希图。

14. 设$A=\{a,b,c\}$，说明A的偏序集只有五种不同的哈希图。

15. $\mathbb{Z}$是整数集合，在$\mathbb{Z}^*=\mathbb{Z}-\{0\}$上定义关系$R$。任给$m,n\in\mathbb{Z}^*$，

$$mRn,\qquad \text{当且仅当}\qquad m\times n>0\text{且}m|n.$$

证明：$<\mathbb{Z}^*,R>$是偏序集，它是否有最大元、最小元、极大元、极小元?

16. $A=\{a_1,a_2,\cdots,a_n,\cdots\}$是任意集合。在偏序集$<\mathscr{P}(A),\subseteq>$中取子集序列$\{a_1\},\{a_1,a_2\},\{a_1,a_2,a_3\},\cdots,\{a_1,a_2,\cdots,a_n,\},\cdots$，它们的并集是否是$\mathscr{P}(A)$的一个极大元? 为什么?

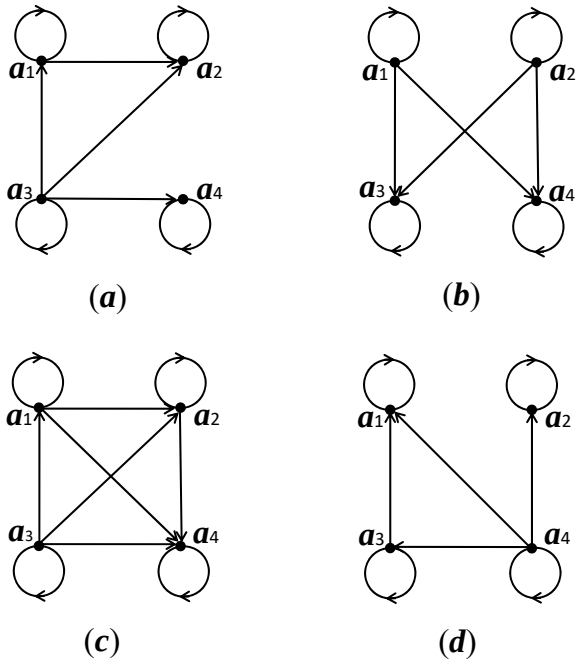


图 4.10: 习题13对应的图

17. 设$< S, \preceq >$是偏序集。证明：S的任意非空子集M均含有极小元，当且仅当S的任意递降序列$a_1 \succ a_2 \succ \cdots \succ a_n \succ \cdots$必终止于有限项。

18. 证明：一个有限集合与一个可数集合的并是可数集合。

19. 设$\mathbb{N}$是自然数集合。证明$\mathbb{N} \times \mathbb{N}$是可数集合。

20. 证明：实数集合$\mathbb{R}$与笛卡尔积$\mathbb{R} \times \mathbb{R}$等势。

第 5 章 群论初步

从本章起开始讲述群、环、域、格等代数对象的基本性质，它是学习和研究理论计算机科学不可缺少的工具.

今后我们主要研究对象不是代数结构中的元素特性，而是各种代数结构本身和不同代数结构之间的相互联系(同态). 掌握其中体现的丰富的数学思想和方法，比背诵定义和名词要重要得多.

5.1 群的定义与简单性质

定义 5.1. G是非空集合，$*$是G上的乘法运算，如果他们满足如下要求：

1° G对于乘法$*$是封闭的，即$\forall a,b\in G$，$a*b\in G$；

2° 对$\forall a,b,c\in G$，$a*(b*c)=(a*b)*c$. $*$满足结合律；

3° 存在$e\in G$，$\forall a\in G$，$e*a=a*e=a$. e称为单位元；

4° $\forall a\in G$，存在$a'\in G$，使得$a'*a=a*a'=e$. a'称为a的逆元.

那么G连同$*$称为一个**群**，记为$\langle G,*\rangle$.

如果只满足1°，2°，则称$\langle G,*\rangle$为**半群**.

如果只满足1°，2°，3°，则称$\langle G,*\rangle$为带1半群.

定义 5.2. 在群$\langle G,*\rangle$中，如果对任意$a,b\in G, a*b=b*a$，则称$\langle G,*\rangle$为**交换群**(或称为**阿贝尔群**).

例 5.1. A是非空集合. $\langle\mathscr{P}(A),\cup\rangle$是带1半群. $\varnothing\in\mathscr{P}(A)$是单位元.

例 5.2. 字母表Σ上的所有非空字组成集合Σ^+，对于字的连接运算$\bullet$构成半群$\langle\Sigma^+,\bullet\rangle$.

例 5.3. 有理数集合Q，在普通加法运算下形成交换群$\langle Q,+\rangle$. 其单位元为0，每个元素的逆元就是它的负数.

例 5.4. 非零实数集合R^*，在普通乘法运算下形成交换群$\langle R^*,\bullet\rangle$. 其单位元为1. 每个元素的逆元就是它的倒数.

例 5.5. 令$G=\{1,-1,\mathrm{i},-\mathrm{i}\}$，对于复数乘法构成的有限交换群$\langle G,*\rangle$. G中的任意两个元素的乘积可用下面的群表示.

$*$	1	-1	i	$-\mathrm{i}$
1	1	-1	i	$-\mathrm{i}$
-1	-1	1	$-\mathrm{i}$	i
i	i	$-\mathrm{i}$	-1	1
$-\mathrm{i}$	$-\mathrm{i}$	i	1	-1

例 5.6. 令$Z_n=\{[0],[1],\cdots,[n-1]\}$，其中$[i]$是模$n$同余$i$的所有整数构成的集合，规定$Z_n$上的$+$运算，$[a]+[b]=[a+b]$. 由模$n$同余定义知，如果$[a_1]=[a_2]$，$[b_1]=[b_2]$，那么$[a_1+b_1]=[a_2+b_2]$，即同余类的加法定义与同余类的代表元选取无关，所以这样的加法定义是确定的，我们称它是“可定义”的. 不难验证$\langle Z_n,+\rangle$是交换群，$[0]$是他的单位元，$[a]$的逆元是$[-a]$.

根据群的定义，我们可以定义群G中元素的方幂

$$a^n=\overbrace{a*a*\cdots*a}^{n}$$

显然$a^m*a^n=a^{m+n}$，$(a^m)^n=a^{m*n}$. 如果将G中元素a的逆元$a^{'}$记为a^{-1}，那么

$$a*a^{'}=a*a^{-1}=a^0,$$

即$a^0=e$. 显然$a^{-n}=(a^{-1})^n=(a^{'})^n$.

在群$\langle G,*\rangle$中的运算$*$不一定满足交换律. 当运算$*$满足交换律时，一般写作“$+$”. 群的单位元称为零元，元素的逆元称为负元. 在交换群中，

$$\begin{aligned}na&=\overbrace{a+a+\cdots+a}^{n},\\ ma+na&=(m+n)a,\\ m(na)&=(m\cdot n)a.\end{aligned}$$

定理 5.1. 在群$\langle G,*\rangle$中，左消去律和右消去律成立，即$\forall a,b\in G$，如果$a*b=a*c$，则必有$b=c$，如果$b*a=c*a$，则必有$b=c$.

证明: 如果$a*b=a*c$，由群定义中4°知，G中每个元素都有逆元. 令元素a的逆元为$a^{'}$. 我们用$a^{'}$左乘这个等式，

$$a^{'}*(a*b)=a^{'}*(a*c)$$

又由群定义中的2°知，运算*满足结合律，得到$(a^{'}*a)*b=(a^{'}*a)*c$. 从逆元的定义和单位元e的定义知$a^{'}*a=e$，$e*b=b$，$e*c=c$，于是最后得到$b=c$. 这表明在群G的等式中可以消去等式两边最左的公因子，即左消去律成立.

同理可以证明右消去律成立.

定理 5.2. 在群$\langle G,*\rangle$中，方程$a*x=b$与$y*a=b$有唯一解.

证明: 令$x=a^{'}*b$代入方程$a*x=b$中，使得

$$a*(a^{'}*b)=(a*a^{'})*b=e*b=b$$

它说明$x=a^{'}*b$是方程$a*x=b$的解.

现假设x_1和x_2都是方程$a*x=b$的解，即$a*x_1=b$，$a*x_2=b$. 于是有$a*x_1=a*x_2$，利用左消去律可得$x_1=x_2$. 这就是说如果方程$a*x=b$有两个解，那么它们必须相等.

综上知在群$\langle G,*\rangle$中方程$a*x=b$有解，并且解是唯一的.

同理可以证明方程$y*a=b$有唯一解.

定理 5.3. 群$\langle G,*\rangle$中单位元和逆元是唯一的.

证明: 假设e_1和e_2都是群G的单位元. 因为e_1是单位元，$\forall a\in G$，$a*e_1=a$，特别取$a=e_2$，那么$e_2*e_1=e_2$. 又因e_2是单位元，$\forall a\in G$，$e_2*a=a$. 特别取$a=e_1$，那么$e_2*e_1=e_1$. 从而$e_1=e_2$，即群G的单位元是唯一的.

假设$a_1,a_2\in G$都是a的逆元. 由逆元定义知$a_1*a=e$，$a_2*a=e$，即$a_1*a=a_2*a$. 再用右消去律得到$a_1=a_2$，即群G中元素a的逆元是唯一的.

定理 5.4. 在群$\langle G,*\rangle$中，$\forall a,b\in G$，则有

1° $(a^{'})^{'}=a$;

2° $(a*b)^{'}=b^{'}*a^{'}$.

证明:

1° $(a^{'})^{'}$是$a^{'}$的逆元，$a^{'}$是a的逆元，由逆元的定义知$(a^{'})^{'}*a^{'}=e$，$a*a^{'}=e$，即$(a^{'})^{'}*a^{'}=a*a^{'}$. 由右消去律知$(a^{'})^{'}=a$.

2° $(a*b)*(b^{'}*a^{'})=a*(b*b^{'})*a^{'}=a*a^{'}=e$,

$(b^{'}*a^{'})*(a*b)=b^{'}*(a^{'}*a)*b=b^{'}*b=e$.

由逆元的唯一性知$(a*b)^{'}=b^{'}*a^{'}$.

注意，在群中乘积求逆满足脱衣规则.

定义 5.3. 在群$\langle G,*\rangle$中，G是有限集合，则称$\langle G,*\rangle$是**有限群**，其阶数为$|G|$.

定义 5.4. 在群$\langle G,*\rangle$中，$a\in G$，如果存在n，它是满足$a^n=e$的最小正整数，则称元素a是n**阶**的. 如果那样的n不存在，则称元素a是**无限阶**的.

我们考虑集合A，其中$a\in G$，Z^*为非零整数集合

$$A=\{i|i\in Z^*,\ a^i=e\}.$$

当$A=\varnothing$时，a是无限阶元. 当$A\neq\varnothing$时，那么A中必有正整数. (这是因为如果$-m<0$，且$-m\in A$即$a^{-m}=e$，那么必有$a^m=e$，即$m>0$且$m\in A$.)这时a是有限阶的，其阶数是A中的最小正整数n. 集合A有如下性质:

1° 若$m,l\in A$，则$m\pm l\in A$.

2° 若$m\in A,c\in Z^*$，则$cm\in A$.

不难证明:

$$A=\{kn|k\in Z^*\}.$$

也就是说，如果$a^m=e$，那么m必是元素a阶的整数倍数.

例 5.7. 在整数加群$\langle Z,+\rangle$中，除零元0的阶为1以外，所有元素的阶都是无限的.

例 5.8. 模6同余类群$\langle Z_6,+\rangle$中，[0]是1阶元，[1],[5]是6阶元，[2],[4]是3阶元，[3]是2阶元.

例 5.9. 在群$\langle G,*\rangle$中，$a,b\in G$，它们分别是m阶、n阶元，$(m,n)=1$. 如果$a*b=b*a$，则$a*b$是$m\cdot n$阶元.

证明： 设$a*b$的阶为k，

$$(a*b)^{mn}=a^{mn}*b^{mn}=(a^m)^n*(b^n)^m=e*e=e,$$

得知$k|mn$.

由于$a*b$的阶是k，$(a*b)^k=e$，

$$e=(a*b)^{km}=(a^m)^k*(b^k)^m=b^{km}.$$

因为b的阶为n，故$n|km$，又由$(m,n)=1$知$n|k$. 同理可以证明$m|k$. 从而$[m,n]|k$，即$mn|k$.

综上知$k=m\cdot n$.

5.2 群定义的进一步讨论

本节介绍群的几个等价的定义，从而更进一步探讨群的性质.

定理 5.5. G是非空集合，$*$是G上的运算. 如果

(1) $\forall a,b\in G,a*b\in G$;

(2) $\forall a,b,c\in G,a*(b*c)=(a*b)*c$;

(3) 存在$e_r\in G$，对一切$a\in G$, $a*e_r=a$. e_r称为右单位元;

(4) $\forall a\in G$，存在$a'\in G$使得$a*a'=e_r$. a'称为a的右逆，那么$\langle G,*\rangle$为群.

证明： 对照定义5.1，我们只要证明右单位元一定是左单位元，右逆一定是左逆.

先证右逆一定是左逆，即已知$a*a'=e_r$，证明$a'*a=e_r$. 现设a''是a'的右逆，$a'*a''=e_r$.

$$a'*a=(a'*a)*e_r=(a'*a)*(a'*a'')=e_r.$$

a'也是a的左逆.

再证右单位元一定是左单位元，a'是a的逆元

$$e_r * a = (a * a^{'}) * a = a * (a^{'} * a) = a * e_r = a.$$

定理 5.6. G是非空集合，$*$是G上的运算，如果

(1) $\forall a, b \in G, a * b \in G$;

(2) $\forall a, b, c \in G, (a * b) * c = a * (b * c)$;

(3) $\forall a, b \in G$，方程$a * x = b$和$y * a = b$在G中都有解. 那么$\langle G, * \rangle$为群.

证明: 与定理5.5比较，我们要证明从(3)推出G中有右单位元并且任意元素均有右逆.

由(3)知方程$a * x = a$在G中有解，我们选取其中一个解记为e_r，即$a * e_r = a$. 任取G的任意元素b，由(3)知$y * a = b$在G中有解，我们选取一个解记为d，即$d * a = b$. 那么

$$b * e_r = (d * a) * e_r = d * (a * e_r) = d * a = b.$$

这说明e_r是G的右单位元. 又由(3)知$a * x = e_r$在G中有解，并记为$a^{'}$，即$a * a^{'} = e_r$，那么$a^{'}$是a的右逆.

定理5.5和定理5.6是与定义5.1等价的两个群定义. 它们的等价性证明过程图5.1所示.

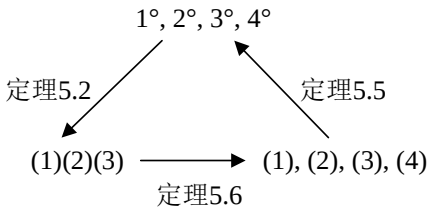


图 5.1: 等价性证明过程

定理 5.7. G是非空集合，$*$是G上的运算. 如果

1° $\forall a, b \in G, a * b \in G$;

2° $\forall a, b, c \in G, (a * b) * c = a * (b * c)$;

3° $\forall a \in G$，$a * x_1 = a * x_2$推出$x_1 = x_2$，并且$\forall a \in G, y_1 * a = y_2 * a$推出$y_1 = y_2$. 那么$\langle G, * \rangle$为群.

证明： 令$G=\{a_1,a_2,\cdots,a_n\}$. 任取G中的元素a，用a左乘G中的每个元素，所有乘积构成一个集合G'，

$$G'=\{a*a_1,a*a_2,\cdots,a*a_n\}.$$

由1°知$a*a_i\in G$，$1\le i\le n$，即$G'\subseteq G$. 又由3°知当$i\ne j$时，$a*a_i\ne a*a_j$，于是$|G'|=|G|=n$. 显然得出$G=G'$. 这表明任取G的元素a，b，方程$a*x=b$均有解.

同样，考虑$G''=\{a_1*a,a_2*a,\cdots,a_n*a\}$，可以证明任取$G$的元素$a$，$b$，方程$y*a=b$均有解.

由定理5.6知$\langle G,*\rangle$为群.

在定理5.1中指出，群中左、右消去律成立. 在定理5.7中，如果非空集合G上的运算满足封闭性、结合律和左右消去律，那么该代数结构是群. 也就是说，当G是有限集合时. 定义5.1的1°，2°，3°，4°与定理5.7的中1°，2°，3°是等价的. 从而定理5.7可以看成有限群的定义.

一个有限群的乘法可以用一个群表来表示. 群的一些性质可以从群表(5.1节例5.5)上直接看出：由于存在单位元，表中有一行与横线边上的元素一样，表里有一列与竖线左边的元素一样. 又由消去律知，全体元素必在每行出现一次，必在每列出现一次. 下面我们来看几个低阶群.

1阶群$G_1,|G_1|=1$. 由于群必有单位元e，故$G_1=\{e\}$. 2阶群$G_2,|G_2|=2$. G_2中除去单位元之外还有一个元素a. $G_2=\{e,a\},a\ne e$. 由于运算$*$的封闭性，$a*a\in\{e,a\}$. 假设$a*a=a$. 由$a*e=a$推出$a=e$，矛盾，故不可. 所以$a*a=e$. G_1和G_2的乘法表如下

$*$	e
e	e

G_1

$*$	e	a
e	e	a
a	a	e

G_2

3阶群$G_3=\{e,a,b\},a\ne b,a,b\ne e,a*a$不能是$a$或$e$，否则推出$a=e$，所以$a*a=b$. 再根据每个元素在一行或一列中出现且只出现一次，得到$a*b=e,b*a=e,b*b=a$. 我们看到元素$b=a*a=a^2$，$e=b*a=a^3$，从而$G_3=\{e,a,a^2\}$，并且a是3阶元，$a^3=e$. 4阶群在同构的意义下只有两

个: $C_4 = \{e, a, a^2, a^3\}$且$a^4 = e$, $K_4 = \{e, a, b, c\}$且$a^2 = b^2 = c^2 = e$. 3阶群G_3和4阶群C_4, K_4的乘法表如下.

$*$	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

G_3

$*$	e	a	b	c
e	e	a	b	c
a	a	b	c	e
b	b	c	e	a
c	c	e	a	b

C_4

$*$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

K_4

例 5.10. 设G是有限群, 则G的每个元素的阶必是有限的.

证明: 群G的单位元e显然是1阶元. 若$a \in G$且$a \neq e, a, a^2, a^3, \cdots, a^n, \cdots \in G$. 由于$G$是有限集合, 必然存在$i > j$, $a^i = a^j$. 等式两边同时乘以a^j的逆元$(a^j)'$,

$$a^i * (a^j)' = a^j * (a^j)' = e.$$

由$a^i = a^{i-j} * a^j$及$*$运算的结合律得到

$$a^{i-j} = e, i - j > 0.$$

那么$i - j$是上节末才提到的集合$A = \{k | k \in Z^*, a^k = e\}$的元素$A \neq \varnothing$, 这表明元素$a$是有限阶元, 其阶数是$A$中的最小正整数.

下面再给出两个非交换群的例子.

例 5.11. 全体n阶有理数方阵记为Q_n. 令$G = \{A | A \in Q_n, |A| \neq 0\}$. G对于矩阵乘法$\bullet$构成群. 若$A, B \in G$, 即$|A|, |B| \neq 0$, 而$|A \bullet B| = |A| \bullet |B| \neq 0$, 则$A \bullet B \in G$. 乘法$\bullet$在$G$中是封闭的. 矩阵乘法是可结合的.

$$I_n = \begin{pmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{pmatrix}$$

是G的单位元. 当$A \in G$时, $|A| \neq 0$, A有逆矩阵A^{-1}, 且$|A^{-1}| \neq 0$, 即$A^{-1} \in G$, 且$A \bullet A^{-1} = I_n$, 故A^{-1}是A在G中的逆元. 所以$\langle G, \bullet \rangle$为群. 由于矩阵乘法是非交换的, 于是$\langle G, \bullet \rangle$为非交换群.

例 5.12. Q是有理数集合. 令

$$G = \{f_{a,b} | f_{a,b} : Q \to Q, f_{a,b}(x) = ax + b, a \neq 0, a, b \in Q\}.$$

G对于映射的合成运算构成群. 若$f_{a,b}, f_{c,d} \in G$，其中$f_{a,b}(x) = ax + b, f_{c,d}(x) = cx + d$，且$a, c \neq 0, a, b, c, d \in Q$.

$$(f_{a,b} \circ f_{c,d})(x) = f_{a,b}(cx + d) = a(cx + d) + b = f_{ac,ad+b}(x),$$

其中$a \cdot c \neq 0$，$ac, cd + b \in Q$，故$f_{a,b} \circ f_{c,d} \in G$，即$G$中$\circ$运算是封闭的. 映射合成运算是可结合的. $f_{1,0} \in G$是G的单位元，$f_{\frac{1}{a},-\frac{b}{a}}$是$f_{a,b}$的逆元. $\langle G, \circ \rangle$是群. 由于运算$\circ$不满足交换律，所以$\langle G, \circ \rangle$是非交换群.

5.3 子群

定义 5.5. $\langle G, * \rangle$是群，H是G的非空子集. 如果

1° $\forall a, b \in H$，$a * b \in H$;

2° $\forall a \in H$，$a^{'} \in H$;

则称$\langle H, * \rangle$是$\langle G, * \rangle$的**子群**，并记为$H \leqslant G$.

定理 5.8. 若$\langle H, * \rangle$是$\langle G, * \rangle$的子群，则$\langle H, * \rangle$也是群.

证明: 从$\langle H, * \rangle$是$\langle G, * \rangle$的子群的定义知运算$*$在集合H中是封闭的. H是G的子集，即H中的每个元素都是G中的元素. 而$\langle G, * \rangle$为群，$*$运算满足结合律，从而$\forall a, b, c \in H \subseteq G$，$(a * b) * c = a * (b * c)$. H是G的非空子集，它至少有一个元素$h \in H$，由子群定义中2°知，$h^{'} \in H$那么$h * h^{'} = e \in H$. 故G中的单位元e在H中并且也是H的单位元. 综上知$\langle H, * \rangle$本身也是群.

由此看出，群G的子群，如果对该群的运算及求逆运算是封闭的，那么该子集对原来群的运算也构成群.

定理 5.9. H是群G的有限非空子集. 如果$\forall a, b \in H$，$a * b \in H$，则$H \leqslant G$.

证明: 任取$a \in H$，$a^2 = a * a \in H$，$a^3 = a^2 * a \in H, \cdots$. 由于$H$是$G$的有限非空子集，$a, a^2, a^3, \cdots$不可能是完全不同的元素，必存在$1 \leq i \leq j$，使得$a^i = a^j = a^i * a^{j-i}$. 用左消去律得到$a^{j-i} = e \in H$，

$$e = a^{j-i} = a * a^{j-i-1},\ j - i - 1 \geq 0.$$

$a^{'} = a^{j-i-1} \in H$，这表明H中任意元素a在H中均有逆. 对照定义5.5知$\langle H, * \rangle$是$\langle G, * \rangle$的子群.

例 5.13. $\langle G, \bullet \rangle = \langle \{1, -1, i, -i\}, \bullet \rangle$中，$H = \{-1, 1\} \subset G$. H对复数乘法封闭，$\langle H, \bullet \rangle$是$\langle G, \bullet \rangle$的子群.

例 5.14. 全体非零复数集合C^*，对复数乘法构成群$\langle C^*, \bullet \rangle$. 令

$$H = \{x | x \in C^*, \exists n \in N 使 x^n = 1\},$$

则$H \leqslant C^*$.

证明: 1是群$\langle C^*, \bullet \rangle$的单位元. $1^1 = 1,\ 1 \in H$. H是C^*的非空子集. 若$x, y \in H$，即存在$n, m \in N$，使$x^n = y^m = 1$，而$(x \bullet y)^{mn} = (x^n)^m \bullet (x^m)^n = 1$，故$x \bullet y \in H$. 又若$x \in H$，存在$n \in N, x^n = 1$. 而$(x^{'})^n = (x^n)^{'} = 1^{'} = 1$，故$x^{'} \in H$. 这就证明了$H \leqslant C^*$.

例 5.15. 设$H_1 \subseteq H_2 \subseteq \cdots \subseteq H_n \subseteq \cdots$是由群$G$的子群$H_i$组成的升链. 令$H = \bigcup_i H_i$，则$H \leqslant G$.

证明: H_i是群G的子群. 即$H_i \neq \varnothing$且$H_i \subseteq G$，显然$H = \bigcup_i H_i \neq \varnothing$且$H \subseteq G$. 若$a, b \in H$，存在$i, j, i > j$使$a \in H_i, b \in H_j \subseteq H_i$，由于$H_i \leqslant G$，则$a * b \in H_i \subseteq H$. 又若$a \in H$，存在$i, a \in H_i$. 再由$H_i \leqslant G$，则$a^{'} \in H_i \subseteq H$. 综上知$H \leqslant G$.

例 5.16. $\langle G, * \rangle$为群. S是G的非空子集，令

$$A = \{H | H \leqslant G, 且 S \subseteq H\},$$

即A是G中包含S所有子群构成的集合. 显然$G \in A$，即A是非空的. 定义$K = \bigcap_{H \in A} H$. 证明$K \leqslant G$.

证明: 任取$H \in A$，H是G的子群，群G的单位元$e \in H$且$H \subseteq G$，所以$e \in \bigcap_{H \in A} H = K$ 且$K \subseteq G$，即K是G的非空子集. 若$a, b \in K$，对任何$H \in A$均有$a, b \in H$，H是G的子群，故$a * b \in H$. 所以$a * b \in K$，又

若$a \in K$，对任何$H \in A$均有$a \in H$，H是G的子群，故$a^{'} \in H$. 所以$a^{'} \in K$，综上知$K \leqslant G$.

A中每个H均满足$S \subseteq H$. 显然$S \subseteq \bigcap_{H \in A} H = K$. 从而$K$是$G$中包含$S$的最小子群. 我们记$\langle S \rangle = K = \bigcap_{H \in A} H$，并称$\langle S \rangle$为$S$生成的子群，如果$S$本身就是$G$的子群，那么$K = \langle S \rangle = S$，否则$S \subseteq \langle S \rangle$.

下面讨论$\langle S \rangle$是哪些元素组成的. 我们先引入集合T.

$$T = \{a_1^{e_1} * a_2^{e_2} * \cdots * a_n^{e_n} \mid a_1, a_2, \cdots, a_n \in S, e_1, e_2, \cdots, e_n = \pm 1, n = 1, 2, \cdots\}.$$

S是非空集合. S中的任意元素a，$a = a^1$，故$a \in T$，也就是说$S \subseteq T$，T是非空集合. 由T的定义知$T \subseteq G$. 若$x = a_{i1}^{e_{i1}} * a_{i2}^{e_{i2}} * \cdots * a_{im}^{e_{im}}, y = a_{j1}^{e_{j1}} * a_{j2}^{e_{j2}} * \cdots * a_{jn}^{e_{jn}} \in T$, 那么$x * y = a_{i1}^{e_{i1}} * a_{i2}^{e_{i2}} * \cdots * a_{im}^{e_{im}} * a_{j1}^{e_{j1}} * a_{j2}^{e_{j2}} * \cdots * a_{jn}^{e_{jn}} \in T$, $x^{'} = a_{i1}^{-e_{i1}} * a_{i2}^{-e_{i2}} * \cdots * a_{im}^{-e_{im}} \in T$, 所以$T$是$G$的包含$S$的子群. 前面已经知道$\langle S \rangle$是$G$中包含$S$的最小子群，于是$\langle S \rangle \subseteq T$.

另一方面，任取$x = a_{i1}^{e_{i1}} * a_{i2}^{e_{i2}} * \cdots * a_{im}^{e_{im}} \in T$，其中$a_{ik} \in S, e_{ik} = \pm 1, 1 \leq k \leq m$. 由于$\langle S \rangle$是$G$中包含$S$的群，$a_{ik}^{e_{ik}} \in \langle S \rangle, 1 \leq k \leq m$，所以$x \in \langle S \rangle$，由此推出$T \subseteq \langle S \rangle$.

综上知$T = \langle S \rangle$.

特别地，当$S = \{a\}$时，$\langle S \rangle = \{a^n | n \in Z\} = \langle a \rangle$. 整数加群$\langle Z, + \rangle$是由整数1生成的群，即$\langle Z, + \rangle = \langle 1 \rangle$. $\langle 2 \rangle = \{2k | k \in Z\}$，$\langle 2, 3 \rangle = \{2a + 3b | a, b \in Z\} = \{k \cdot 1 | k \in Z\} = Z$. 一般地，$\langle m, n \rangle = \{(m, n) \cdot k | k \in Z\}$.

5.4 循环群

有一类群，它的每个元素都可以写成某个固定元素的幂，a^i或a^{-i}，这样的群称之为循环群.

定义 5.6. 在群$\langle G, * \rangle$中，如果存在一个元素$g \in G$，使$G = \{g^n \mid n \in \mathbf{Z}\}$，则称该群为**循环群**，记作$\langle g \rangle$，其中$g$称为循环群的**生成元**.

若群中的运算用“+”表示，循环群$\langle G, + \rangle$写成$\langle g \rangle = \{ng \mid n \in \mathbf{Z}\}$，$g$是该循环群的生成元.

每个循环群都是交换群，这是因为$g^r * g^s = g^{r+s} = g^s * g^r$.

例 5.17. $\langle G,*\rangle=\langle\{1,-1,\mathrm{i},-\mathrm{i}\},\cdot\rangle$是由i生成的四阶循环群.

$$\mathrm{i}^0=1,\mathrm{i}^1=\mathrm{i},\mathrm{i}^2=-1,\mathrm{i}^3=-\mathrm{i},\mathrm{i}^4=1,\cdots$$

所以该群可以写成$\langle\left\{1,\mathrm{i},\mathrm{i}^2,\mathrm{i}^3\right\},\bullet\rangle$.

定理 5.10. g是群$\langle G,*\rangle$中的k阶元. 令$H=\{g^r\mid r\in\mathbf{Z}\}$，那么$\langle H,*\rangle$是$\langle G,*\rangle$的一个$k$阶子群.

证明: $\forall r,s\in\mathbf{Z},g^r*g^s=g^{r+s}\in H,\left(g^r\right)'=g^{-r}\in H$. 故$H\leqslant G$. g是G的k阶元，$g^0=e,g^1,\cdots,g^{k-1}$是k个两两互不相同的元素. 对于任意整数t，$t=uk+v$，其中$0\leqslant v<k$，那么

$$g^t=g^{uk+v}=(g^k)^u*g^v=g^v$$
$$H=\{g^r\mid r\in\mathbf{Z}\}=\left\{g^0,g^1,\cdots,g^{k-1}\right\}.$$

$\langle H,*\rangle$是$\langle G,*\rangle$的k阶子群.

特别地，G是n阶群. G的某个元素g是n阶元，那么G必定是由g生成的一个循环群.

定理 5.11. 循环群的每个子群必是循环群.

证明: 令G是由元素a生成的循环群. $G=\langle a\rangle$. H是群G的子群. 如果$H=\{e\}=\langle e\rangle$，显然H是循环群. 如果$H\neq\{e\}$. 那么至少存在一个元素$b\in H$且$b\neq e$. 设m是使$a^m\in H$的最小正整数，任取H中的元素b，b也是群G的元素，则$b=a^n$. 令$n=mu+v$，$0\leqslant v<m$.

$$b=a^n=a^{mu+v}=(a^m)^u*a^v,$$
$$a^v=a^n*(a^m)^{-u}.$$

由于$b=a^n\in H$，$a^m\in H$，而H是群，$(a^m)^{-u}\in H$，从而$a^v\in H$. 假若$v>0$，那么这就与m是使$a^m\in H$的最小正整数相矛盾，故不可. 这说明必须$v=0$，即$b=a^{mu}=(a^m)^u$，也就是说H中的每个元素都可以表示成a^m的方幂. 于是a^m是子群H的生成元，H是循环群.

例 5.18. 模6同余类加群$\langle\mathbf{Z}_6,+\rangle=\langle[1]\rangle$是循环群. $[0]$是1阶元，$\langle[0]\rangle=\{[0]\}$是$\mathbf{Z}_6$的1阶子群，$[3]$是2阶元，$\langle[3]\rangle=\{[0],[3]\}$是$\mathbf{Z}_6$的2阶子群. $[5]$是6阶元，$\langle[5]\rangle=\{[0],[5],[4],[3],[2],[1]\}$是$\mathbf{Z}_6$的6阶子群.

定理 5.12. G是n阶循环群，$G=\langle a\rangle$且$|G|=n$，H是G的一个子群，$H=\langle b\rangle$，且$b=a^s$，则

$$|H|=\frac{n}{(n,s)}.$$

证明： 令H是G的m阶子群，m是使$b^m=e$的最小正整数. $b^m=a^{sm}=e$，而a是n阶元$a^n=e$，故$n\mid ms$. 设$(n,s)=d, n=dn_0, s=ds_0$，且$(n_0,s_0)=1$，于是$n_0\mid ms_0$，进而得到$n_0\mid m$，即$m=n_0\cdot k$. m是满足此式的最小正整数，从而$k=1$. 最后得出

$$m=n_0=\frac{n}{(n,s)}$$

例 5.19. 求模18同余类加群的所有子群.

解： $\langle[1]\rangle=\langle[5]\rangle=\langle[7]\rangle=\langle[11]\rangle=\langle[13]\rangle=\langle[17]\rangle$是$\mathbf{Z}_{18}$的18阶子群.
$\langle[2]\rangle=\langle[4]\rangle=\langle[8]\rangle=\langle[10]\rangle=\langle[14]\rangle=\langle[16]\rangle$是$\mathbf{Z}_{18}$的9阶子群.
$\langle[3]\rangle=\langle[15]\rangle$是$\mathbf{Z}_{18}$的6阶子群.
$\langle[6]\rangle=\langle[12]\rangle$是$\mathbf{Z}_{18}$的3阶子群.
$\langle[9]\rangle$和$\langle[0]\rangle$分别为$\mathbf{Z}_{18}$的2阶和1阶子群.

例 5.20. 在集合$\{1,2,\cdots,p-1\}$上定义运算$*$:

$$a*b=c\Longleftrightarrow a\cdot b\equiv c(\mathrm{mod}\ p),$$

其中p为素数. 若$a\in\{1,2,\cdots,p-1\}$，显然$(a,p)=1$，a的阶为l，那么$l\mid(p-1)$，即a是$x^l\equiv 1(\mathrm{mod}\ p)$的一个解. 于是$\{1,a,a^2,\cdots,a^{l-1}\}$都是$x^l\equiv 1(\mathrm{mod}\ p)$的解，而且是全部解. 它是以$a$为生成元的$l$阶循环群，是$\{1,2,\cdots,p-1\}$的$l$阶子群. 元素$a^k$的阶为$\frac{l}{(k,l)}$.

5.5 置换群

定理 5.13. n元集合$A=\{1,2,\cdots,n\}$上的全体置换构成集合S_n，S_n在合成运算之下构成一个群. 称之为n次对称群，其阶数为$n!$.

证明： 集合A上的置换是从A到A的双射. 由于两个双射的合成映射仍是双射. 所以S_n中的置换在合成运算下是封闭的. 并且映射的合成满足结合

律. S_n的单位元是恒同置换$\sigma_I = \begin{pmatrix} 1 & 2 & \cdots & n \\ 1 & 2 & \cdots & n \end{pmatrix}$置换$\sigma$的逆元是它的逆置换$\sigma^{-1}$. 根据群的定义知$\langle S_n, \bullet \rangle$是群. n元置换共有$n!$个. 故$|S_n| = n!$.

定义 5.7. 集合A上的双射全体对于映射的合成运算构成群. 该群叫做**对称群**. 对称群的子群为置换群.

由于置换的合成运算不满足交换律，所以置换群通常是非交换群.

例如，$S_2 = \{\sigma_I, (1\ 2)\}, S_3 = \{\sigma_I, (1\ 2\ 3), (1\ 3\ 2), (1\ 2), (1\ 3), (2\ 3)\}$.

例 5.21. 图5.2中的等边三角形经旋转和反射使之三个顶点与原来的顶点重合在一起，一共有六种情况：

$$\rho_0 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = \sigma_1, \qquad \mu_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = (1\ 2),$$

$$\rho_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = (1\ 2\ 3), \quad \mu_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = (1\ 3),$$

$$\rho_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = (1\ 3\ 2), \quad \mu_3 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = (2\ 3),$$

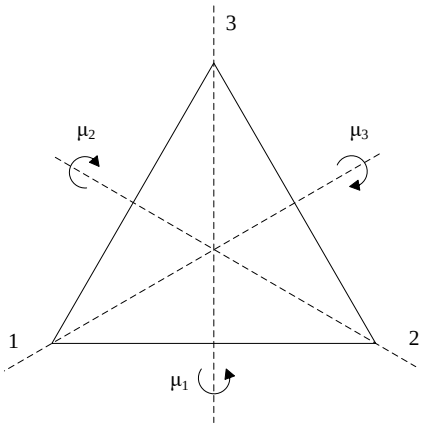


图 5.2: 等边三角形的顶点置换示意图

令ρ_0, ρ_1, ρ_2分别是绕等边三角形中心旋转$0°, 120°, 240°$的结果. μ_1, μ_2, μ_3分别是对三个对称轴反射的结果.

令$D_3=\{\rho_0,\rho_1,\rho_2,\mu_1,\mu_2,\mu_3\}$，$D_3$在合成运算之下形成一个置换群. 它的乘法表如下:

$*$	ρ_0	ρ_1	ρ_2	μ_1	μ_2	μ_3
ρ_0	ρ_0	ρ_1	ρ_2	μ_1	μ_2	μ_3
ρ_1	ρ_1	ρ_2	ρ_0	μ_2	μ_3	μ_1
ρ_2	ρ_2	ρ_0	ρ_1	μ_3	μ_1	μ_2
μ_1	μ_1	μ_3	μ_2	ρ_0	ρ_2	ρ_1
μ_2	μ_2	μ_1	μ_3	ρ_1	ρ_0	ρ_2
μ_3	μ_3	μ_2	μ_1	ρ_2	ρ_1	ρ_0

我们注意到$\rho_1\cdot\mu_3=\mu_1,\mu_3\cdot\rho_1=\mu_2$，$D_3$不是交换群，称它为三次二面体. $|D_3|=6$，恰好$D_3=S_3$.

例 5.22. 正方形通过旋转和反射使之顶点与原来顶点重合. 共有如下八种情况:

$$\rho_0=\begin{pmatrix}1&2&3&4\\1&2&3&4\end{pmatrix}=\sigma_1,\qquad \mu_1=\begin{pmatrix}1&2&3&4\\2&1&4&3\end{pmatrix}=(1\ 2)(3\ 4),$$
$$\rho_1=\begin{pmatrix}1&2&3&4\\2&3&4&1\end{pmatrix}=(1\ 2\ 3\ 4),\quad \mu_2=\begin{pmatrix}1&2&3&4\\4&3&2&1\end{pmatrix}=(1\ 4)(2\ 3),$$
$$\rho_2=\begin{pmatrix}1&2&3&4\\3&4&1&2\end{pmatrix}=(1\ 3)(2\ 4),\quad \delta_1=\begin{pmatrix}1&2&3&4\\3&2&1&4\end{pmatrix}=(1\ 3),$$
$$\rho_3=\begin{pmatrix}1&2&3&4\\4&1&2&3\end{pmatrix}=(1\ 4\ 3\ 2),\quad \delta_2=\begin{pmatrix}1&2&3&4\\1&4&3&2\end{pmatrix}=(2\ 4).$$

其中$\rho_0,\rho_1,\rho_2,\rho_3$是正方形绕中心旋转$0^\circ,90^\circ,180^\circ,270^\circ$的结果. μ_1,μ_2是关于两个对边中心点连线反射的结果. δ_1,δ_2是关于两条对角线反射的结果*(*图*5.3)*.

令$D_4=\{\rho_0,\rho_1,\rho_2,\rho_3,\mu_1,\mu_2,\delta_1,\delta_2\}$, D_4在合成运算之下形成一个置换群. 它的乘法表如下:

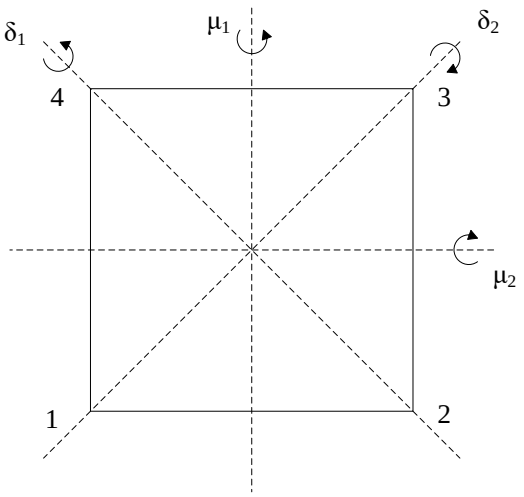


图 5.3: 正方形的顶点置换示意图

$*$	ρ_0	ρ_1	ρ_2	ρ_3	μ_1	μ_2	δ_1	δ_2
ρ_0	ρ_0	ρ_1	ρ_2	ρ_3	μ_1	μ_2	δ_1	δ_2
ρ_1	ρ_1	ρ_2	ρ_3	ρ_0	δ_1	δ_2	μ_2	μ_1
ρ_2	ρ_2	ρ_3	ρ_0	ρ_1	μ_2	μ_1	δ_2	δ_1
ρ_3	ρ_3	ρ_0	ρ_1	ρ_2	δ_2	δ_1	μ_1	μ_2
μ_1	μ_1	δ_2	μ_2	δ_1	ρ_0	ρ_2	ρ_3	ρ_1
μ_2	μ_2	δ_1	μ_1	δ_2	ρ_2	ρ_0	ρ_1	ρ_3
δ_1	δ_1	μ_1	δ_2	μ_2	ρ_1	ρ_3	ρ_0	ρ_2
δ_2	δ_2	μ_2	δ_1	μ_1	ρ_3	ρ_1	ρ_2	ρ_0

D_4称为四次二面体. $|D_4| = 8$. 它是四次对称群S_4的子群.

例 5.23. 证明$S_n = \langle (1\ 2), (1\ 3), \cdots, (1\ n)\rangle$，即对换$(1\ 2)$，$(1\ 3)$，$\cdots$，$(1\ n)$是$S_n$的生成元系.

证明: $\langle (1\ 2), (1\ 3), \cdots, (1\ n)\rangle$是由$(1\ 2)$，$(1\ 3)$，$\cdots$，$(1\ n)$是$S_n$生成的群. 由5.3例5.16知,

$$\langle (1\ 2), (1\ 3), \cdots, (1\ n)\rangle = \{\sigma_1\sigma_2\cdots\sigma_m \mid \sigma_i \in \{(1\ 2), (1\ 3), \cdots, (1\ n)\},$$
$$1 \leqslant i \leqslant m, m = 1, 2, \cdots\}.$$

显然$\langle(1\ 2),(1\ 3),\cdots,(1\ n)\rangle \subseteq S_n$.

下面证明每个n元置换均可以写成$(1\ 2),(1\ 3),\cdots,(1\ n)$这些基本元素的乘积. 对$n$进行归纳证明. 当$n=2$时,

$$\begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix} = (1\ 2)(1\ 2), \qquad \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} = (1\ 2),$$

该命题成立. 假设$n=k$时命题成立，现设$n=k+1$,

$$\sigma = \begin{pmatrix} 1 & 2 & \cdots & k & k+1 \\ \sigma(1) & \sigma(2) & \cdots & \sigma(k) & \sigma(k+1) \end{pmatrix}$$

有如下两种可能:

1° $\sigma(k+1)=k+1$，这时σ本身变成k元置换. 由归纳假设命题成立.

2° $\sigma(k+1)\neq k+1$，必定存在$l, 1\leqslant l\leqslant k, \sigma(l)=k+1$. 用对换$(l\quad k+1)$右乘$\sigma$得到$\sigma_1$,

$$\begin{aligned} &\sigma_1 = \sigma(l\quad k+1) \\ &= \begin{pmatrix} 1 & 2 & \cdots & l-1 & l & l+1 & \cdots & k+1 \\ \sigma(1) & \sigma(2) & \cdots & \sigma(l-1) & k+1 & \sigma(l+1) & \sigma(k+1) & \end{pmatrix} (l\quad k+1) \\ &= \begin{pmatrix} 1 & 2 & \cdots & l-1 & l & l+1 & \cdots & k & k+1 \\ \sigma(1) & \sigma(2) & \cdots & \sigma(l-1) & \sigma(k+1) & \sigma(l+1) & \cdots & \sigma(k) & k+1 \end{pmatrix}, \end{aligned}$$

σ_1变为k元置换. 由归纳假设σ_1可以写成$(1\ 2)$，$(1\ 3)$，$\cdots$，$(1\ k)$的乘积. 而$\sigma=\sigma_1(l\quad k+1)=\sigma_1(1\ l)(1\ k+1)(1\ l)$，故$\sigma$可以写$(1\ 2)$，$(1\ 3)$，$\cdots$，$(1\ k)$，$(1\ k+1)$的乘积. 命题对$n=k+1$也成立.

例如

$$\begin{aligned} S_3 &= \{\sigma_I,(1\ 2\ 3),(1\ 3\ 2),(1\ 2),(1\ 3),(2\ 3)\} \\ &= \{(1\ 2)(1\ 2),(1\ 3)(1\ 2),(1\ 2)(1\ 3),(1\ 2),(1\ 3),(1\ 2)(1\ 3)(1\ 2)\} \end{aligned}$$

5.6 群的同构

本节讨论两个群之间的关系.

我们在习题中曾经讨论过$\langle S,*\rangle$，其中$S=\{\alpha,\beta,\gamma,\delta\}$，乘法表为

$*$	α	β	γ	δ
α	β	δ	α	γ
β	δ	γ	β	α
γ	α	β	γ	δ
δ	γ	α	δ	β

$\langle S, * \rangle$是群，把该表的行与列适当地调换次序得到

$*$	γ	α	β	δ
γ	γ	α	β	δ
α	α	β	δ	γ
β	β	δ	γ	α
δ	δ	γ	α	β

再与5.2节的C_4的乘法表比较，只要把$\gamma, \alpha, \beta, \delta$分别换名为$e, a, b, c$，它们是完全相同的. 也就是说群$S$和群$C_4$的元素之间的有一种一一对应关系. 我们研究群时并不关心元素本身是什么，关心的是元素与元素间的关系. 所以，从这个意义上群S与群C_4是一回事.

为了刻画上述思想，我们引出同构的概念.

定义 5.8. $\langle G_1, * \rangle$与$\langle G_2, \bullet \rangle$是两个群，如果存在着从集合$G_1$到集合$G_2$的双射$\varphi$，对于任何$a, b \in G_1$，

$$\varphi(a * b) = \varphi(a) \bullet \varphi(b).$$

则称G_1与G_2同构，记作$G_1 \cong G_2$. 双射φ称作**同构映射**.

φ作为同构映射，除了要求它是双射外，还要求它保持运算. 即$\forall a, b \in G_1$，$\varphi(a * b) = \varphi(a) \bullet \varphi(b)$. 形象地说，同构映射$\varphi$满足如图5.4所示交换图表.

如果群G_1与群G_2同构，那么两个群的单位元之间以及元素和它的逆元之间有什么联系呢? 这是下面定理要讨论的内容.

定理 5.14. φ是从群G_1到群G_2的同构映射，e_1和e_2分别是群G_1和G_2的单位元，必有$\varphi(e_1) = e_2$，并且对任何G_1中的元素a，$\varphi(a') = \varphi'(a)$.

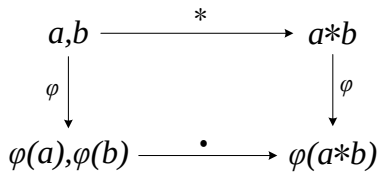


图 5.4: 同构映射φ的交换图表

证明： e_1和e_2分别是群G_1和G_2的单位元. 对任意G_1中的元素a,

$$\varphi(a) = \varphi(e_1 * a) = \varphi(e_1) \bullet \varphi(a).$$

等式两边同时右乘$\varphi^{'}(a)$得到

$$e_2 = \varphi(a) \bullet \varphi^{'}(a) = \varphi(e_1) \bullet \varphi(a) \bullet \varphi^{'}(a) = \varphi(e_1),$$

即群G_1的单位元e_1的同构映射像是G_2的单位元e_2.

又对于G_1的任意元素a,

$$\varphi^{'}(a) = \varphi^{'}(a) \bullet e_2 = \varphi^{'}(a) \bullet \varphi(e_1) = \varphi^{'}(a) \bullet \varphi(a) \bullet \varphi(a^{'}) = \varphi(a^{'}),$$

即G_1任意元素a的逆元的像等于该元素同构映射像的逆元.

例 5.24. 证明正实数乘群与实数加群同构.

证明： $\langle \mathbf{R}^+, \bullet \rangle$与$\langle \mathbf{R}, + \rangle$分别为正实数乘群与实数加群. $\varphi : \mathbf{R} \to \mathbf{R}^+$, $\varphi(x) = \mathrm{e}^x$. 显然$\varphi$是双射. 对任意$x, y \in \mathbf{R}$,

$$\varphi(x + y) = \mathrm{e}^{x+y} = \mathrm{e}^x \bullet \mathrm{e}^y = \varphi(x) \bullet \varphi(y),$$

故φ为同构映射. 从而$\langle \mathbf{R}^+, \bullet \rangle \cong \langle \mathbf{R}, + \rangle$.

这里要指出的是并非每个从G_1到G_2的双射都是同构映射. 例如：$\psi : \mathbf{R} \to \mathbf{R}^+, \psi(x) = \mathrm{e}^{x-1}$，显然$\psi$是双射. 但是对任意$x, y \in \mathbf{R}$,

$$\psi(x + y) = \mathrm{e}^{x+y-1}$$
$$\phi(x) \bullet \psi(y) = \mathrm{e}^{x-1} \bullet \mathrm{e}^{y-1} = \mathrm{e}^{x+y-2}$$

故ψ不是从$\mathbf{R}$到$\mathbf{R}^+$的同构映射.

例 5.25. 在同构的意义下循环群$G = \langle a\rangle$只有两类：若a是无限阶元，则$G \cong \langle \mathbf{Z}, +\rangle$. 若$a$是$n$阶元，则$G \cong \mathbf{Z}_n$.

证明： 若循环群$G = \langle a\rangle$的生成元a是无限阶元，对任何$m_1 \neq m_2$均有$a^{m_1} \neq a^{m_2}$. f 是从G到整数集合$\mathbf{Z}$的映射，$f : G \to \mathbf{Z}, f(a^m) = m$. 显然$f$是双射. 对任意$a^{m_1}, a^{m_2} \in G$，

$$f(a^{m_1} * a^{m_2}) = f(a^{m_1+m_2}) = m_1 + m_2 = f(a^{m_1}) + f(a^{m_2}).$$

f是同构映射，故$G \cong \langle \mathbf{Z}, +\rangle$.

若生成元a是n阶元，则$G = \left\{a^0, a^1, a^2, \cdots, a^{n-1}\right\}$. f是从G到模n同余类集合$\mathbf{Z}_n$的映射，$f : G \to \mathbf{Z}_n, f(a^i) = [i]$. 显然$f$是双射. 对任意$a^i, a^j \in G$，

$$f(a^i * a^j) = f(a^{i+j}) = [i + j] = [i] + [j] = f(a^i) + f(a^j).$$

f是同构映射，故$G \cong \langle \mathbf{Z}_n, +\rangle$.

例 5.26. 任意一个群都与一个置换群同构.

证明： 对于任意群$\langle G, *\rangle$构造一个新的集合

$$G^{'} = \{f_a \mid a \in G, f_a : G \to G, f_a(x) = a * x\}.$$

容易证明f_a是G上的双射，$G^{'}$上的运算$\bullet$是映射的合成运算.

$$(f_a \bullet f_b)(x) = f_a(b * x) = (a * b) * x = f_{a*b}(x),$$

即$f_a \bullet f_b = f_{a*b}$. 该运算在$G^{'}$中封闭且满足结合律. f_e是$G^{'}$的单位元，$f_{a'}$是f_a的逆元，从而$\langle G^{'}, \bullet\rangle$ 是置换群.

在群G与$G^{'}$之间定义映射$h : G \to G^{'}, h(a) = f_a$，显然$h$是双射. 对任意$a, b \in G$，

$$h(a * b) = f_{a*b} = f_a \bullet f_b = h(a) \bullet h(b),$$

故h是同构映射. 从而$G \cong G^{'}$.

例 5.27. 求出与n阶循环群同构的置换群.

解： 令$G=\langle a\rangle$是循环群，$f:G\to G'$是同构映射. 任取$x\in G'$，必存在$g=a^i\in G$使

$$x=f(g)=f(a^i)=(f(a))^i.$$

这说明G'是以$f(a)$为生成元的循环群. 现G是n阶循环群，$G=\{a^0,a^1,\cdots,a^{n-1}\}$，从例5.26可知$G'=\{f_{a^0},f_{a^1},\cdots,f_{a^{n-1}}\}$. 也是$n$阶循环群. 其生成元是$f_a$，它对应$G$上长为$n$的轮换$(a^0\ a^1\ \cdots\ a^{n-1})$. 令$G''=\langle(a^0\ a^1\ \cdots\ a^{n-1})\rangle$，则$G\cong G''$.

定理 5.15. $\langle G,*\rangle$为群，另有一个集合G'，$\bullet$是G' 上的运算. 如果存在从G到G'上的双射f，对G中的任意元素a,b有$f(a*b)=f(a)\bullet f(b)$. 那么$\langle G',\bullet\rangle$也是群，并且$G\cong G'$.

证明： 任取$x,y\in G'$，f是从G到G'的满射，存在$a,b\in G$使得$f(a)=x$. $f(b)=y$. 由于f保持运算，

$$x\bullet y=f(a)\bullet f(b)=f(a*b)\in G',$$

可知运算$\bullet$在G'中是封闭的，任取$x,y,z\in G'$. 对于满射f在G中有原像. $f(a)=x$，$f(b)=y$，$f(c)=z$，

$$\begin{aligned}(x\bullet y)\bullet z&=(f(a)\bullet f(b))\bullet f(c)=f((a*b)*c)\\&=f(a*(b*c))=f(a)\bullet(f(b)\bullet f(c))=x\bullet(y\cdot z),\end{aligned}$$

即G'中运算$\bullet$满足结合律. 容易看出$f(e)$是G'的单位元. 任取$x\in G',a\in G$是它的原像，易知$f(a')\in G'$是x的逆元.

综上知$\langle G',\bullet\rangle$是群. f就是从G到G'的同构映射，从而$G\cong G'$.

习题

1. 如下代数系统$\langle S,*\rangle$哪些是群? 如果是群，它是否是交换群? 指出它的单位元以及如何计算其逆元.

(1) $S=\{z|z\in\mathbf{C},|z|=1\}$，其中$\mathbf{C}$是复数集合，$*$是普通的复数加法.

(2) $S=\{a+b\sqrt{2}\mid a,b\in\mathbf{Q}\}$，其中$\mathbf{Q}$是有理数集合. $*$是普通的加法.

(3)

$$S=\left\{\begin{pmatrix}1&0\\0&1\end{pmatrix},\begin{pmatrix}-1&0\\0&-1\end{pmatrix},\begin{pmatrix}1&0\\0&-1\end{pmatrix},\begin{pmatrix}-1&0\\0&1\end{pmatrix}\right\}$$

$*$是矩阵乘法.

(4) $S=\{\alpha,\beta,\gamma,\delta\}$

$*$	α	β	γ	δ
α	β	δ	α	γ
β	δ	γ	β	α
γ	α	β	γ	δ
δ	γ	α	δ	β

(5) $S=\mathbf{R}-\{0\}$是非零实数集合，在S 上定义运算$*$:

$$x*y=\begin{cases}x\cdot y & x>0,\\ x/y & x<0.\end{cases}$$

(6) p为素数，$S=\{1,2,\cdots,p-1\}$. 在S上定义运算$*$:

$$a*b=c\Longleftrightarrow a\cdot b\equiv c(\mathrm{mod}\ p).$$

2. 令$S=\mathbf{R}-\{-1\}$，在S上定义运算$*$:

$$a*b=a+b+ab$$

(1) 证明$\langle S,*\rangle$是群;

(2) 在S中求解方程$2*x*3=7$.

3. 在群G中，如果对G有任意元素a均有$a^2=e$，证明G必是交换群.

4. G是交换群当且仅当对G中任意元素$a,b,(a*b)^2=a^2*b^2$.

5. g是群G中的任意元素，那么，

(1) g与它的逆元$g^{'}$同阶;

(2) $(g^k)^{'}=(g^{'})^k$，k是非负整数.

6. a与b是群G中的两个任意元素. 证明$a*b$与$b*a$是同阶的.

7. 如果群G中只有一个2阶元a，那么a与G中任意元素都是可交换的，即$\forall x \in G, a * x = x * a$.

8. G是群，G中的元素个数为偶数，证明：存在$a \in G, a$是2阶元.

9. H是群G的非空子集. $\langle H, * \rangle$是$\langle G, * \rangle$的子群当且仅当$\forall a, b \in H, a * b' \in H$.

10. G是群.

$$H = \{a \mid a \in G, \forall g \in G, a * g = g * a\},$$

称为群G的中心. 证明：$\langle H, * \rangle$是$\langle G, * \rangle$的子群.

11. H, K是群G的子群. 证明$H \cap K$也是G的子群. $H \bigcup K$是G的子群吗? 证明你的结论.

12. 找出K_4群的所有子群.

13. 令$G = \{f_{a,b} \mid f_{a,b} : \mathbf{Q} \to \mathbf{Q}, f(x) = ax + b, a \neq 0, a, b \in \mathbf{Q}\}, G$对合成运算构成群. 证明$H = \{f_{1,b} \mid b \in \mathbf{Q}\}$是$G$的子群.

14. 指出下列群中哪个是循环群? 对循环群写出它的全部生成元.

(1) $G_1 = \langle \mathbf{Q}, + \rangle$;

(2) $G_2 = \langle 6Z, + \rangle$;

(3) $G_3 = \langle \{6^n \mid n \in \mathbf{Z}\}, \bullet \rangle$.

15. G是6阶循环群，找出G的全部生成元并列出G的所有子群.

16. 证明：只有一个生成元的循环群至多含有两个元素.

17. 如果n阶群G的某个元素g是n阶的，那么G是由g生成的循环群.

18. G是n阶循环群，d是n的因子，G存在且仅存在一个d阶子群.

19. 找出S_3的所有子群.

20. A_4是全体4元偶置换构成的群，请列出它的全部元素.

21. $S_n (n \geqslant 2)$的每个子群或者全部由偶置换构成，或者其中奇、偶置换各占一半.

22. 证明：整数加群与偶数加群同构.

23. 证明：群的同构关系是一种等价关系.

24. 找出所有与K_4群同构的S_n的子群.

25. 证明：无限循环群的子群，除$\{e\}$以外都是无限循环群.

26. 在群$\langle G, * \rangle$中定义新的二元运算$\bullet$，

$$a \bullet b = b * a.$$

证明：$\langle G, \bullet \rangle$是群，并且$\langle G, * \rangle$与$\langle G, \bullet \rangle$同构.

第 6 章 商群

为了深入探讨群的结构，需要进一步研究子群的作用.

6.1 陪集与Lagrange定理

定义 6.1. $\boldsymbol{H}$是$\boldsymbol{G}$的子群. 在$\boldsymbol{G}$上定义模$\boldsymbol{H}$同余关系，$\forall a,b\in\boldsymbol{G}$，如果$a*b'\in\boldsymbol{H}$，则称$a$与$b$**模**$H$**同余**，记作$a\equiv b(\mathrm{mod}\ \boldsymbol{H})$.

定理 6.1. 模$\boldsymbol{H}$同余关系是$\boldsymbol{G}$上的等价关系. 对于$\boldsymbol{G}$中的元素a，a所在的等价类为

$$\boldsymbol{H}a=\{h*a|h\in\boldsymbol{H}\},$$

称为$\boldsymbol{G}$中$\boldsymbol{H}$的右陪集，元素a是陪集$\boldsymbol{H}a$的代表元.

证明 任取$a\in\boldsymbol{G}$，$a*a'=e\in\boldsymbol{H}$，故$a\equiv a\,(\mathrm{mod}\boldsymbol{H})$. 模$\boldsymbol{H}$同余关系是自反的. 如果$a,b\in\boldsymbol{G}$，$a\equiv b(\mathrm{mod}\,\boldsymbol{H})$，即$a*b'\in\boldsymbol{H}$. 因$\boldsymbol{H}$是群，$(a*b')'=b*a'\in\boldsymbol{H}$. 故$b\equiv a\,(\mathrm{mod}\boldsymbol{H})$. 模$\boldsymbol{H}$同余关系是对称的. 如果$a,b,c\in\boldsymbol{G}$，$a\equiv b\,(\mathrm{mod}\boldsymbol{H})$，$b\equiv c\,(\mathrm{mod}\boldsymbol{H})$，即$a*b'\in\boldsymbol{H}$，$b*c'\in\boldsymbol{H}$. $\boldsymbol{H}$是$\boldsymbol{G}$的子群，$\boldsymbol{H}$对群$\boldsymbol{G}$的运算$*$封闭，$(a*b')*(b*c')=a*c'\in\boldsymbol{H}$，故$a\equiv c\,(\mathrm{mod}\ \boldsymbol{H})$. 模$\boldsymbol{H}$同余关系是传递的. 综上分析知模$\boldsymbol{H}$同余关系是$\boldsymbol{G}$上的等价关系.

$\boldsymbol{G}$中的元素a的等价类，

$$\begin{aligned}[a]&=\{b|b\in G,b*a'\in\boldsymbol{H}\}\\&=\{h*a|h\in\boldsymbol{H}\}=\boldsymbol{H}a.\end{aligned}$$

显然$a\in\boldsymbol{H}a$，a是该等价类的代表元.

模$\boldsymbol{H}$同余关系有如下性质：

1° $\boldsymbol{H}e=\boldsymbol{H}$;

2° $a\equiv b\,(\mathrm{mod}\ \boldsymbol{H})\Longleftrightarrow\boldsymbol{H}a=\boldsymbol{H}b$;

3° $a\in\boldsymbol{H}\Longleftrightarrow\boldsymbol{H}a=\boldsymbol{H}$.

例 6.1. 非零有理数乘法群$\langle \boldsymbol{Q}^*, \bullet \rangle$，$\boldsymbol{H} = \{-1, 1\} \subset \boldsymbol{Q}^*$，是该乘法群的子群. $\boldsymbol{Q}^*$中元素a所在的右陪集$\boldsymbol{H}a = \{a, -a\}$. 当$a \equiv b \pmod{\boldsymbol{H}}$时，$b = \pm a$，显然$\boldsymbol{H}a = \boldsymbol{H}b$.

例 6.2. 三次二面体群$\langle \boldsymbol{D}_3, \bullet \rangle$，$\boldsymbol{H} = \{\rho_0, \rho_1, \rho_2\}$是$\boldsymbol{D}_3$的子群，因$\rho_i \in \boldsymbol{H}$，$0 \leqslant i \leqslant 2$，故$\boldsymbol{H}\rho_0 = \boldsymbol{H}\rho_1 = \boldsymbol{H}\rho_2 = \boldsymbol{H}$. 又因$\mu_i * \mu_j^{'} \in \boldsymbol{H}$，$1 \leqslant i, j \leqslant 3$，故$\boldsymbol{H}\mu_1 = \boldsymbol{H}\mu_2 = \boldsymbol{H}\mu_3 = \{\mu_1, \mu_2, \mu_3\}$. $\boldsymbol{H}$有两个不同的右陪集$\boldsymbol{H}$和$\boldsymbol{H}\mu_1$，$\boldsymbol{D}_3 = \boldsymbol{H} \cup \boldsymbol{H}\mu_1$且$\boldsymbol{H} \cap \boldsymbol{H}\mu_1 = \varnothing$.

例 6.3. $\boldsymbol{G}$是以g为生成元的9阶循环群，$\boldsymbol{G} = \{g^0, g^1, \cdots, g^8\}$，$g^9 = e$. $\boldsymbol{H} = \{g^0, g^3, g^6\}$是$\boldsymbol{G}$的3阶子群.

$$\begin{aligned} \boldsymbol{H}g^0 = \boldsymbol{H}g^3 = \boldsymbol{H}g^6 = \{g^0, g^3, g^6\} = \boldsymbol{H}, \\ \boldsymbol{H}g^1 = \boldsymbol{H}g^4 = \boldsymbol{H}g^7 = \{g^1, g^4, g^7\}, \\ \boldsymbol{H}g^2 = \boldsymbol{H}g^5 = \boldsymbol{H}g^8 = \{g^2, g^5, g^8\}. \end{aligned}$$

$\boldsymbol{H}$有三个不同的右陪集$\boldsymbol{H}$，$\boldsymbol{H}g$，$\boldsymbol{H}g^2$. $\boldsymbol{G} = \boldsymbol{H} \bigcup \boldsymbol{H}g \bigcup \boldsymbol{H}g^2$，且这些右陪集两两非交.

对于群$\boldsymbol{G}$的子群$\boldsymbol{H}$也可以定义它的左陪集，先在$\boldsymbol{G}$上定义等价关系. $\forall a, b \in \boldsymbol{G}$,

$$a \equiv b \pmod{\boldsymbol{H}} \Longleftrightarrow a^{'} * b \in \boldsymbol{H}.$$

$\boldsymbol{G}$中元素a所在的等价类$[a] = \{b | b \in \boldsymbol{G}, a^{'} * b \in \boldsymbol{H}\} = \{a * h | h \in \boldsymbol{H}\} = a\boldsymbol{H}$，称为$a$所在的左陪集.

定理 6.2. $\boldsymbol{H}$是群$\boldsymbol{G}$的子群，$\boldsymbol{H}$的所有左陪集集合$\boldsymbol{S}_L = \{a\boldsymbol{H} | a \in \boldsymbol{G}\}$和所有右陪集集合$\boldsymbol{S}_R = \{\boldsymbol{H}a | a \in \boldsymbol{G}\}$是等势的.

证明 令$f : \boldsymbol{S}_L \to \boldsymbol{S}_R$，$f(a\boldsymbol{H}) = \boldsymbol{H}a^{'}$. 这里首先要说明该映射与代表元选取无关，即若$a\boldsymbol{H} = b\boldsymbol{H}$，必有$\boldsymbol{H}a^{'} = \boldsymbol{H}b^{'}$. 由$a\boldsymbol{H} = b\boldsymbol{H}$知$a^{'} * b \in \boldsymbol{H}$，$\boldsymbol{H}$是群，$(a^{'} * b)^{'} = b^{'} * (a^{'})^{'} \in \boldsymbol{H}$从而$\boldsymbol{H}a^{'} = \boldsymbol{H}b^{'}$. 显然$f$是满射. 如果$a_1\boldsymbol{H}, a_2\boldsymbol{H} \in \boldsymbol{S}_L$都是$\boldsymbol{H}a$的原像，$f(a_1\boldsymbol{H}) = f(a_2\boldsymbol{H}) = \boldsymbol{H}a$，得出$\boldsymbol{H}a_1^{'} = \boldsymbol{H}a_2^{'}$，故有$(a_1^{'}) * (a_2^{'})^{'} = a_1^{'} * a_2 \in \boldsymbol{H}$. 由此可知$a_1\boldsymbol{H} = a_2\boldsymbol{H}$. 这说明$f$是单射.

综上分析，在$\boldsymbol{S}_L$和$\boldsymbol{S}_R$之间存在一个双射，故$\boldsymbol{S}_L$与$\boldsymbol{S}_R$等势.

注意:在定理6. 2证明中定义的映射是$f(a\boldsymbol{H}) = \boldsymbol{H}a^{'}$，而不是$\boldsymbol{H}a$. 后者它不是映射. 当$a\boldsymbol{H} = b\boldsymbol{H}$时，不能保证$\boldsymbol{H}a = \boldsymbol{H}b$.

定义 6.2. 群$\boldsymbol{G}$关于它的子群$\boldsymbol{H}$的左(右)陪集个数叫做$\boldsymbol{H}$在$\boldsymbol{G}$中的**指数**，记为$[\boldsymbol{G} : \boldsymbol{H}]$.

定理 6.3. ***(Lagrange定理)***
若$\boldsymbol{G}$是有限群，$\boldsymbol{H}$是$\boldsymbol{G}$的子群，那么

$$|\boldsymbol{G}| = [\boldsymbol{G} : \boldsymbol{H}]|\boldsymbol{H}|.$$

证明 $\boldsymbol{H}a$是$\boldsymbol{G}$中$\boldsymbol{H}$的一个右陪集. 定义映射$f : \boldsymbol{H} \to \boldsymbol{H}a$，$f(h) = h * a$，显然$f$是双射. $\boldsymbol{G}$是有限群，$\boldsymbol{H}$是$\boldsymbol{G}$的子群，所以$\boldsymbol{H}$也是有限群，得出$|\boldsymbol{H}| = |\boldsymbol{H}a|$. 由定理6.1知，$\boldsymbol{G}$中$\boldsymbol{H}$的右陪集全体构成$\boldsymbol{G}$的一个分划，令$\boldsymbol{G}$关于子群$\boldsymbol{H}$的右陪集个数$[\boldsymbol{G} : \boldsymbol{H}] = k$，$k$个不同的右陪集的代表元分别为$a_1, a_2, \cdots, a_k$，那么$\boldsymbol{G} = \boldsymbol{H}a_1 \bigcup \boldsymbol{H}a_2 \cdots \bigcup \boldsymbol{H}a_k$，其中$\boldsymbol{H}a_i \bigcap \boldsymbol{H}a_j = \varnothing, (i \neq j)$. 从而

$$\begin{aligned} |\boldsymbol{G}| &= |\boldsymbol{H}a_1| + |\boldsymbol{H}a_2| + \cdots + |\boldsymbol{H}a_k| \\ &= k \bullet |\boldsymbol{H}| = [\boldsymbol{G} : \boldsymbol{H}] \bullet |\boldsymbol{H}| \end{aligned}$$

由此定理可以得到两个非常有用的推论.

推论 6.1. 有限群$\boldsymbol{G}$中元素的阶是$|\boldsymbol{G}|$ 的因子.

证明 在有限群中所有元素的阶必然是有限的. 设$\boldsymbol{G}$中元素a的阶为m，令$\boldsymbol{H} = \{a^0, a^1, \cdots, a^{m-1}\}$，显然$\boldsymbol{H}$是$\boldsymbol{G}$的$m$阶子群. 由Lagrange定理知$|\boldsymbol{G}| = [\boldsymbol{G} : \boldsymbol{H}] \bullet |\boldsymbol{H}| = [\boldsymbol{G} : \boldsymbol{H}] \bullet m$，故$m \,|\, |\boldsymbol{G}|$.

推论 6.2. 素数阶群都是循环群.

证明 设$\boldsymbol{G}$是p阶群，p是素数，它的因子只有1和p. 由推论6. 1知$\boldsymbol{G}$中的元素的阶是1或p. 显然群$\boldsymbol{G}$的单位元的阶为1，非单位元元素a的阶为p，从而$\boldsymbol{G} = \langle a \rangle$.

例 6.4. 证明*4*阶群$\boldsymbol{G}$或者是*4*阶循环群$\boldsymbol{C}_4$或者是*Klein-4*群$\boldsymbol{K}_4$.

证明 4阶群$\boldsymbol{G}$中元素的阶可能为1,2,4. 如果$\boldsymbol{G}$中包括4阶元a，那么$\boldsymbol{G}=\langle a\rangle=\{a^0,a^1,a^2,a^3\}$，即$\boldsymbol{G}$是4阶循环群$\boldsymbol{C}_4$. 如果$\boldsymbol{G}$中没有4阶元，那么除单位元$e$外，其他元素均是2阶元，即$\boldsymbol{G}=\{e,a,b,c\}$，$a^2=b^2=c^2=e$. 由前面的习题知该群必是交换群. $a*b$不能是a,b,e，否则推出$b=e$，$a=e$，$a=b$. 从而$a*b=c$. 同理可知$a*c=b$，$b*c=a$. 据此得出该群的乘法表：

$*$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

故$\boldsymbol{G}$是Klein-4群$\boldsymbol{K}_4$.

例 6.5. *$\boldsymbol{G}$是6阶群，$\boldsymbol{G}$至少含有一个3阶子群.*

证明 $\boldsymbol{G}$是6阶群. $\boldsymbol{G}$中元素的阶可能是1，2，3，6. 如果$\boldsymbol{G}$中有3阶元a，那么$\langle a\rangle$就是$\boldsymbol{G}$的3阶子群. 如果$\boldsymbol{G}$中有6阶元a，那么$\langle a^2\rangle$为3阶子群. 下面证明$\boldsymbol{G}$中不可能既无3阶元也无6阶元. 也就是说$\boldsymbol{G}$中不可能除掉单位元e外都是2阶元. 用反证法，假设$\boldsymbol{G}=\{e,a,b,c,d,f\}$，且$a^2=b^2=c^2=d^2=f^2=e$. 由于$a*b$不可为a,b,e，取$\boldsymbol{K}=\{e,a,b,a*b\}$，其中$a*b\in\{c,d,f\}$，显然$\boldsymbol{K}$是Klein-4群. 而$\boldsymbol{K}\subseteq\boldsymbol{G}$. 故$\boldsymbol{K}$是$\boldsymbol{G}$的子群. $|\boldsymbol{K}|=4$. 而$4\nmid 6$，与Lagrange定理矛盾. 故不可. 综上知六阶群必有三阶子群.

6.2 正规子群与商群

本节介绍一类特殊的子群—正规子群.

定义 6.3. *$\boldsymbol{H}$是群$\boldsymbol{G}$的子群. 如果对所有的$\boldsymbol{G}$中元素g 和$\boldsymbol{H}$中元素h都有$g'*h*g\in\boldsymbol{H}$，那么称$\boldsymbol{H}$是$\boldsymbol{G}$的**正规子群**，并记为$\boldsymbol{H}\lhd\boldsymbol{G}$.*

定理 6.4. *$\boldsymbol{H}$是群$\boldsymbol{G}$的子群. $\boldsymbol{H}$是$\boldsymbol{G}$的正规子群当且仅当对$\boldsymbol{G}$中任意元素g，$\boldsymbol{H}g=g\boldsymbol{H}$.*

证明 若$\boldsymbol{H}$是$\boldsymbol{G}$的正规子群. 任取$x \in g\boldsymbol{H}$，存在$h_1 \in \boldsymbol{H}$使$x = g * h_1$. 而$x = (g^{'})^{'} * h_1 * g^{'} * g$，由正规子群的定义，$(g^{'})^{'} * h_1 * g^{'} \in \boldsymbol{H}$，故$x \in \boldsymbol{H}g$，于是$g\boldsymbol{H} \subseteq \boldsymbol{H}g$. 反过来，任取$y \in \boldsymbol{H}g$，存在$h_2 \in \boldsymbol{H}$使$y = h_2 * g$，而$y = g * g^{'} * h_2 * g$，由正规子群的定义$g^{'} * h_2 * g \in \boldsymbol{H}$，故$y \in g\boldsymbol{H}$. 于是$\boldsymbol{H}g = g\boldsymbol{H}$. 综上知，$\boldsymbol{H}g = g\boldsymbol{H}$.

又若对$\boldsymbol{G}$中任意元素g均有$\boldsymbol{H}g = g\boldsymbol{H}$，任取$h_3 \in \boldsymbol{H}$，必存在$h_4 \in \boldsymbol{H}$使$h_3 * g = g * h_4$，于是$g^{'} * h_3 * g = h_4 \in \boldsymbol{H}$，从而$\boldsymbol{H}$是$\boldsymbol{G}$的正规子群.

例 6.6. 三次二面体$\boldsymbol{D}_3$的子群$\boldsymbol{H} = \{\rho_1, \rho_2, \rho_3\}$是正规子群，

$$\rho_0\boldsymbol{H} = \rho_1\boldsymbol{H} = \rho_2\boldsymbol{H} = \boldsymbol{H}\rho_0 = \boldsymbol{H}\rho_1 = \boldsymbol{H}\rho_2 = \{\rho_0, \rho_1, \rho_2\},$$
$$\mu_1\boldsymbol{H} = \mu_2\boldsymbol{H} = \mu_3\boldsymbol{H} = \boldsymbol{H}\mu_1 = \boldsymbol{H}\mu_2 = \boldsymbol{H}\mu_3 = \{\mu_1, \mu_2, \mu_3\}.$$

$\widetilde{\boldsymbol{H}} = \{\rho_0, \mu_1\}$是$\boldsymbol{D}_3$的子群，但不是正规子群. 例如

$$\mu_2\widetilde{\boldsymbol{H}} = \{\mu_2, \rho_1\},\ \ \widetilde{\boldsymbol{H}}\mu_2 = \{\mu_2, \rho_2\}.$$

$\mu_2\widetilde{\boldsymbol{H}} \neq \widetilde{\boldsymbol{H}}\mu_2$.

例 6.7. 指数为2的子群是正规子群.

证明 $\boldsymbol{H}$是群$\boldsymbol{G}$的子群且$[\boldsymbol{G} : \boldsymbol{H}] = 2$，即$\boldsymbol{G} = \boldsymbol{H} \bigcup \boldsymbol{H}a_1$，其中$a_1 \notin \boldsymbol{H}$，并且$\boldsymbol{H} \bigcap \boldsymbol{H}a_1 = \varnothing$. 我们任取群$\boldsymbol{G}$的元素$a$，有两种可能性：若$a \in \boldsymbol{H}$，由于$a\boldsymbol{H} = \boldsymbol{H}$，$\boldsymbol{H}a = \boldsymbol{H}$，故$a\boldsymbol{H} = \boldsymbol{H}a$；若$a \notin \boldsymbol{H}$，$\boldsymbol{G} = \boldsymbol{H} \bigcup \boldsymbol{H}a = \boldsymbol{H} \bigcup a\boldsymbol{H}$. $\boldsymbol{H}a = \boldsymbol{G} - \boldsymbol{H} = a\boldsymbol{H}$. 所以不管是哪种情况均有$a\boldsymbol{H} = \boldsymbol{H}a$. $\boldsymbol{H}$是$\boldsymbol{G}$的正规子群.

显然交换群的任何子群都是正规子群.

下面研究在$\boldsymbol{G}$中$\boldsymbol{H}$的所有右陪集构成的集合上的运算及相应的代数结构.

定义 6.4. $\boldsymbol{A}$，$\boldsymbol{B}$是群$\boldsymbol{G}$的非空子集，定义

$$\boldsymbol{A} \bullet \boldsymbol{B} = \{a * b | a \in \boldsymbol{A}, b \in \boldsymbol{B}\}.$$

该运算满足结合律. 任取$x \in \boldsymbol{A} \bullet (\boldsymbol{B} \bullet \boldsymbol{C})$，存在$a \in \boldsymbol{A}$，$b \in \boldsymbol{B}$，$c \in \boldsymbol{C}$使$x = a*(b*c)$. 群$\boldsymbol{G}$中乘法满足结合律$x = (a*b)*c$，故$x \in (\boldsymbol{A} \bullet \boldsymbol{B}) \bullet \boldsymbol{C}$. 从而$\boldsymbol{A} \bullet (\boldsymbol{B} \bullet \boldsymbol{C}) \subseteq (\boldsymbol{A} \bullet \boldsymbol{B}) \bullet \boldsymbol{C}$. 同理也可证明$(\boldsymbol{A} \bullet \boldsymbol{B}) \bullet \boldsymbol{C} \subseteq \boldsymbol{A} \bullet (\boldsymbol{B} \bullet \boldsymbol{C})$. 最后得到$\boldsymbol{A} \bullet (\boldsymbol{B} \bullet \boldsymbol{C}) = (\boldsymbol{A} \bullet \boldsymbol{B}) \bullet \boldsymbol{C}$.

定理 6.5. $\boldsymbol{N}$是群$\boldsymbol{G}$的正规子群，$\langle \{\boldsymbol{N}g | g \in \boldsymbol{G}\}, \bullet \rangle$是群，称为$\boldsymbol{G}$模$\boldsymbol{N}$的**商群**，记为$\boldsymbol{G}/\boldsymbol{N}$.

证明 首先研究两个正规子群的右陪集怎样做乘法.

$$\boldsymbol{N}g_1 \bullet \boldsymbol{N}g_2 = \{(n_1 * g_1) * (n_2 * g_2) | n_1, n_2 \in \boldsymbol{N}\}.$$

因$\boldsymbol{N}$是$\boldsymbol{G}$的正规子群，对于$\boldsymbol{G}$中元素g_1，有$g_1\boldsymbol{N} = \boldsymbol{N}g_1 . g_1 * n_2 \in g_1\boldsymbol{N}$，那么存在$n_3 \in \boldsymbol{N}$使$g_1 * n_2 = n_3 * g_1$，代入上式，

$$\begin{aligned} \boldsymbol{N}g_1 \bullet \boldsymbol{N}g_2 &= \{n_1 * (n_3 * g_1) * g_2 | n_1, n_2 \in \boldsymbol{N}\} \\ &= \{n * (g_1 * g_2) | n \in \boldsymbol{N}\} \\ &= \boldsymbol{N}g_1 * g_2. \end{aligned}$$

这里定义的正规子群右陪集间的乘法运算与右陪集代表元的选取无关. 这是因为，如果$\boldsymbol{N}g_1 = \boldsymbol{N}a_1$，$\boldsymbol{N}g_2 = \boldsymbol{N}a_2$，即$g_1 * a_1', g_2 * a_2' \in \boldsymbol{N}$，那么

$$(g_1 * g_2) * (a_1 * a_2)' = g_1 * (g_2 * a_2') * a_1'.$$

令$n_1 = g_2 * a_2'$，$n_1 * a_1' = a_1' * n_2$，$n_3 = g_1 * a_1'$

$$(g_1 * g_2) * (a_1 * a_2)' = n_3 * n_2 \in \boldsymbol{N}.$$

于是$\boldsymbol{N}g_1 * g_2 = \boldsymbol{N}a_1 * a_2$.

在集合$\{\boldsymbol{N}g | g \in \boldsymbol{G}\}$上的乘法运算显然是封闭的. 并且满足结合律. $\boldsymbol{N} = \boldsymbol{N}e$是单位元，$\boldsymbol{N}g'$是$\boldsymbol{N}g$的逆元. 所以$\langle \boldsymbol{N}g | g \in \boldsymbol{G}, \bullet \rangle$是群.

当$\boldsymbol{G}$是有限群时，$\boldsymbol{G}$模$\boldsymbol{N}$的商群$\boldsymbol{G}/\boldsymbol{N}$中的元素个数就是$\boldsymbol{N}$在$\boldsymbol{G}$中的指数，故

$$|\boldsymbol{G}/\boldsymbol{N}| = |\boldsymbol{G}|/|\boldsymbol{N}|.$$

例 6.8. 整数加群$\langle \boldsymbol{Z}, + \rangle$是交换群. 每个子群都是正规子群. $\boldsymbol{Z}$模正规子群$\langle n \rangle = \{kn | k \in \boldsymbol{Z}\} = n\boldsymbol{Z}$的商群.

$$\boldsymbol{Z}/n\boldsymbol{Z}=\{n\boldsymbol{Z},1+n\boldsymbol{Z},\cdots,(n-1)+n\boldsymbol{Z}\}.$$

若映射$f:\boldsymbol{Z}/n\boldsymbol{Z}\to\boldsymbol{Z}_n$，$f(i+n\boldsymbol{Z})=[i]$，显然$f$是双射，故

$$\boldsymbol{Z}/n\boldsymbol{Z}\cong\boldsymbol{Z}_n.$$

例 6.9. 三次二面体$\boldsymbol{D}_3$中，子群$\boldsymbol{H}=\{\rho_0,\rho_1,\rho_2\}$的指数为2. $\boldsymbol{H}$是$\boldsymbol{D}_3$的正规子群，$\boldsymbol{D}_3$模$\boldsymbol{H}$的商群

$$\boldsymbol{D}_3/\boldsymbol{H}=\{\boldsymbol{H},(12)\boldsymbol{H}\}$$

是2阶循环群.

例 6.10. $\boldsymbol{G}$是有限交换群. 素数p是$|\boldsymbol{G}|$的因子，那么群$\boldsymbol{G}$中必有一个p阶元.

证明 我们对群$\boldsymbol{G}$的阶数进行归纳证明. 当$|\boldsymbol{G}|=2$时，$\boldsymbol{G}=\{e,a\}$且$a^2=e$. 素数$2||\boldsymbol{G}|$. a是2阶元，命题成立. 假设$|\boldsymbol{G}|<k$时，命题成立. 现设$|\boldsymbol{G}|=k$，某素数$p|k$. 任取$\boldsymbol{G}$的某个非单位元素g，它的阶为t，显然$t|k$且$t>1$. 如果$p|t$，即$t=rp$，则g^r是$\boldsymbol{G}$中的p阶元. 如果$p\nmid t$，考虑$\boldsymbol{G}$模正规子群$\langle g\rangle$的商群$\boldsymbol{G}/\langle g\rangle$.

$$|\boldsymbol{G}/\langle g\rangle|=|\boldsymbol{G}|/t<|\boldsymbol{G}|=k,$$

$\boldsymbol{G}/\langle g\rangle$仍是有限交换群. 由于$p|k$，$p\nmid t$，故$p||\boldsymbol{G}/\langle g\rangle|$. 由归纳假设知在$\boldsymbol{G}/\langle g\rangle$中有$p$阶元$a\langle g\rangle$. 假设$a$在$\boldsymbol{G}$中的阶为$u$，显然有$(a\langle g\rangle)^u=\langle g\rangle$. 从而$p|u$. 由前面讨论知，$a^{u/p}$是$\boldsymbol{G}$的$p$阶元. 命题对$|\boldsymbol{G}|=k$也成立.

一般地，n阶群$\boldsymbol{G}$，对n的因子d，在$\boldsymbol{G}$中不一定有d阶子群. 例如:全体四元偶置换构成$\boldsymbol{A}_4$，$|\boldsymbol{A}_4|=12$. 6是12的因子，但$\boldsymbol{A}_4$没有6阶子群，这是因为$\boldsymbol{A}_4$中有1个1阶元，8个3阶元，3个2阶元. 若$\boldsymbol{H}$是$\boldsymbol{A}_4$的6阶子群，因2阶元只有3个. 故$\boldsymbol{H}$中至少有1个3阶元，不妨假设是$(abc)\in\boldsymbol{H}$. 3阶元的逆元仍是3阶元，故3阶元必须成对出现. 单位元$e\in\boldsymbol{H}$，所以$\boldsymbol{H}$中至少有一个2阶元，不妨假设是$(ab)(cd)\in\boldsymbol{H}$. 由$(abc)\in\boldsymbol{H}$，$(ab)(cd)\in\boldsymbol{H}$推出$(abc)'=(acb)\in\boldsymbol{H}$，$(abc)(ab)(cd)=(acd)\in\boldsymbol{H}$，$(acd)'=(adc)\in\boldsymbol{H}$，$(ab)(cd)(abc)=(bdc)\in\boldsymbol{H}$，$(bdc)'=(bcd)\in\boldsymbol{H},\cdots,\boldsymbol{H}$中的元素个数已超过6个，与$\boldsymbol{H}$是$\boldsymbol{A}_4$的6阶子群矛盾. 所以$\boldsymbol{A}_4$没有6阶子群.

6.3 群的同态

本节继续讨论两个群的关系.

定义 6.5. 在群$\langle \boldsymbol{G}_1, * \rangle$和$\langle \boldsymbol{G}_2, \bullet \rangle$之间存在映射$f : \boldsymbol{G}_1 \to \boldsymbol{G}_2$，对任意$a, b \in \boldsymbol{G}_1$，$f(a * b) = f(a) \bullet f(b)$，则称$f$是从$\boldsymbol{G}_1$到$\boldsymbol{G}_2$的**同态映射**(简称**同态**). 如果$f$是满射(单射，双射)，则称$f$是**满同态映射(单一同态映射，同构映射)**.

若f是从群$\boldsymbol{G}_1$到$\boldsymbol{G}_2$的同态映射，$\boldsymbol{G}_1$，$\boldsymbol{G}_2$单位元分别为e_1和e_2，那么$f(e_1) = e_2$. 对任意$a \in \boldsymbol{G}$，$f(a^{'}) = (f(a))^{'}$. 此结论证明方法与群同构映射相应性质证明方法相同.

定义 6.6. f是从群$\boldsymbol{G}_1$到$\boldsymbol{G}_2$的群同态映射，f的**核**是$\boldsymbol{G}_1$中通过f映到$\boldsymbol{G}_2$的单位元e_2的那些元素组成的集合，记为$Kerf$，

$$Kerf = \{a | a \in \boldsymbol{G}_1, f(a) = e_2\}.$$

.

定理 6.6. f是从群$\boldsymbol{G}_1$到$\boldsymbol{G}_2$的群同态映射.

1° $Kerf$是群$\boldsymbol{G}_1$的正规子群.

2° f为单射而且仅当$Kerf = \{e_1\}$.

证明

1° f是从群$\boldsymbol{G}_1$到$\boldsymbol{G}_2$的群同态映射. 由于$f(e_1) = e_2$，$e_1 \in$Ker$f$，所以Ker$f$是$\boldsymbol{G}_1$的非空子集. 任取$g_1, g_2 \in$ Ker$f$，$f(g_1) = f(g_2) = e_2$，而

$$f(g_1 * g_2) = f(g_1) \bullet f(g_2) = e_2 \bullet e_2 = e_2,$$
$$f(g_1^{'}) = (f(g_1))^{'} = e_2^{'} = e_2.$$

故$g_1 * g_2 \in$ Ker$f$，$g_1^{'} \in$ Ker$f$，从而Ker$f$是$\boldsymbol{G}_1$的子群，任取$g \in \boldsymbol{G}_1$，$k \in$ Ker$f$，

$$\begin{aligned} f(g^{'} * k * g) &= (f(g))^{'} \bullet f(k) \bullet f(g) \\ &= (f(g))^{'} \bullet e_2 \bullet f(g) = e_2, \end{aligned}$$

故$g^{'} * k * g \in \mathrm{Ker}f$. $\mathrm{Ker}f$是$\boldsymbol{G}_1$的正规子群.

2° 当f为单射时，只有e_1的像为e_2，故$\mathrm{Ker}f = \{e_1\}$，反过来，当$\mathrm{Ker}f = \{e_1\}$时，如果存在$g_2 \in \boldsymbol{G}_2$，它有两个不同的原像$g_{11}, g_{12} \in \boldsymbol{G}_1$，$g_{11} \neq g_{12}$，$f(g_{11}) = f(g_{12}) = g_2$.

$$f(g_{11} * g_{12}^{'}) = f(g_{11}) \bullet (f(g_{12}))^{'} = g_2 \bullet g_2^{'} = e_2.$$

那么$g_{11} * g_{12}^{'} \in \mathrm{Ker}f = \{e_1\}$，即$g_{11} * g_{12}^{'} = e_1$. 从而得到$g_{11} = g_{12}$，矛盾. 这说明如果$\boldsymbol{G}_2$中的元素有原像，那么原像是唯一的，所以$f$是单射.

例 6.11. $\boldsymbol{G}_1$和$\boldsymbol{G}_2$是任意两个群，令$f : \boldsymbol{G}_1 \to \boldsymbol{G}_2$，对任意$g \in \boldsymbol{G}_1$，$f(g) = e_2$. 任取$g_1, g_2 \in \boldsymbol{G}_1$，

$$f(g_1 * g_2) = e_2 = e_2 \bullet e_2 = f(g_1) \bullet f(g_2),$$

f是群同态映射. $\mathrm{Ker}f = \boldsymbol{G}_1$，我们称这个特殊的同态映射为零同态映射.

例 6.12. $\boldsymbol{G}_1 = \langle \boldsymbol{Z}, + \rangle$，$\boldsymbol{G}_2 = \langle \boldsymbol{C}, \bullet \rangle$，令$f : \boldsymbol{Z} \to \boldsymbol{C}$. $f(m) = \mathrm{i}^m$. $f(k+l) = \mathrm{i}^{k+l} = \mathrm{i}^k \bullet \mathrm{i}^l = f(k) \bullet f(l)$. f是从$\boldsymbol{G}_1$到$\boldsymbol{G}_2$的同态映射. $\mathrm{Ker}f = \{n | \mathrm{i}^n = 1\} = \{4m | m \in \boldsymbol{Z}\}$. f的像集$\mathrm{Im}f = \{1, -1, \mathrm{i}, -\mathrm{i}\}$.

定理 6.7. f是群$\boldsymbol{G}_1$到$\boldsymbol{G}_2$的一个同态映射.

1° 若$\boldsymbol{H}_1 \leqslant \boldsymbol{G}_1$，则$f(\boldsymbol{H}_1) \leqslant \boldsymbol{G}_2$，特别地$f(\boldsymbol{G}_1) \leqslant \boldsymbol{G}_2$;

2° 若$\boldsymbol{H}_1 \lhd \boldsymbol{G}_1$，则$f(\boldsymbol{H}_1) \lhd f(\boldsymbol{G}_1)$;

3° 若$\boldsymbol{H}_2 \leqslant f(\boldsymbol{G}_1)$，则$f^{-1}(\boldsymbol{H}_2) \leqslant \boldsymbol{G}_1$;

4° 若$\boldsymbol{H}_2 \lhd f(\boldsymbol{G}_1)$，则$f^{-1}(\boldsymbol{H}_2) \lhd \boldsymbol{G}_1$且$\boldsymbol{G}_1 / f^{-1}(\boldsymbol{H}_2) \cong f(\boldsymbol{G}_1)/\boldsymbol{H}_2$.

证明 这里只证2°，3°，其他留作练习题.

2° $\boldsymbol{H}_1$是$\boldsymbol{G}_1$的正规子群，由1°知$f(\boldsymbol{H}_1) \leqslant \boldsymbol{G}_2$. 而$f(\boldsymbol{H}_1) \subseteq f(\boldsymbol{G}_1) \subseteq \boldsymbol{G}_2$，$f(\boldsymbol{G}_1)$为群，故$f(\boldsymbol{H}_1)$是$f(\boldsymbol{G}_1)$的子群. 任取$y \in f(\boldsymbol{G}_1)$，$x \in f(\boldsymbol{H}_1)$，存在$g \in \boldsymbol{G}_1$，$h \in \boldsymbol{H}_1$使$f(g) = y$，$f(h) = x$.

$$y^{'} \bullet x \bullet y = f(g^{'}) \bullet f(h) \bullet f(g) = f(g^{'} * h * g).$$

由于$\boldsymbol{H}_1$是$\boldsymbol{G}_1$的正规子群，$g^{'} * h * g \in \boldsymbol{H}_1$，故$y^{'} \bullet x \bullet y \in f(\boldsymbol{H}_1)$，$f(\boldsymbol{H}_1)$是$f(\boldsymbol{G}_1)$的正规子群.

3° $\boldsymbol{H}_2$是$f(\boldsymbol{G}_1)$的子群. $f^{-1}(\boldsymbol{H}_2)=\{x|x\in\boldsymbol{G}_1,f(x)\in\boldsymbol{H}_2\}\subseteq\boldsymbol{G}_1$, $f(e_1)=e_2\in\boldsymbol{H}_2$, 显然$e_1\in f^{-1}(\boldsymbol{H}_2).f^{-1}(\boldsymbol{H}_2)$是$\boldsymbol{G}_1$的非空子集. 若$x_1,x_2\in f^{-1}(\boldsymbol{H}_2)$, 存在$h_1,h_2\in\boldsymbol{H}_2$, 使$f(x_1)=h_1$, $f(x_2)=h_2$.

$$f(x_1*x_2)=f(x_1)\bullet f(x_2)=h_1\bullet h_2\in\boldsymbol{H}_2,$$
$$f(x_1^{'})=(f(x_1))^{'}=h_1^{'}\in\boldsymbol{H}_2.$$

可知$x_1*x_2\in f^{-1}(\boldsymbol{H}_2)$, $x_1^{'}\in f^{-1}(\boldsymbol{H}_2)$. 从而$f^{-1}(\boldsymbol{H}_1)$是$\boldsymbol{G}_1$的子群.

定理 6.8. f是从$\boldsymbol{G}_1$到$\boldsymbol{G}_2$的群同态映射, 对任意$a\in\boldsymbol{G}_1$, $f^{-1}(f(a))=aKerf$.

证明 任取$a\in\boldsymbol{G}_1$, f是从$\boldsymbol{G}_1$到$\boldsymbol{G}_2$的群同态映射, $f(a)\in\boldsymbol{G}_2$. 由f^{-1}定义知$f^{-1}(f(a))=\{x|x\in\boldsymbol{G}_1,f(x)=f(a)\}$. 任取$x\in f^{-1}(f(a))$, $f(a^{'}*x)=f(a^{'})\bullet f(x)=(f(a))^{'}\bullet f(a)=e_2$, 故$a^{'}*x\in\mathrm{Ker}f$, 即$x\in a\mathrm{Ker}f$. 从而得到$f^{-1}(f(a))\subseteq a\mathrm{Ker}f$. 又任取$y^{'}\in a\mathrm{Ker}f$, 存在$k\in\mathrm{Ker}f$使$y=a*k$, $f(y)=f(a)\bullet f(k)=f(a)\bullet e_2=f(a)$, 所以$y\in f^{-1}(f(a))$. 又得出$a\mathrm{Ker}f\subseteq f^{-1}(f(a))$. 综上分析知

$$f^{-1}(f(a))=a\mathrm{Ker}f.$$

这个定理说明了, 若f是从$\boldsymbol{G}_1$到$\boldsymbol{G}_2$的满同态, 则$\boldsymbol{G}_2$中每个元素的原像集正好是f的同态核$\mathrm{Ker}f$的一个陪集. 据此, 我们可以在$\boldsymbol{G}_1/\mathrm{Ker}f$和$\boldsymbol{G}_2$之间建立起一个一一对应关系.

定理 6.9. ***(群同态基本定理)***

群$\boldsymbol{G}_1$的任何商群都是$\boldsymbol{G}_1$的同态像. 若$\boldsymbol{G}_2$是$\boldsymbol{G}_1$的同态像, 则$\boldsymbol{G}_1/Kerf\cong\boldsymbol{G}_2$.

证明 设$\boldsymbol{H}$是群$\boldsymbol{G}_1$的正规子群. 定义$\varphi:\boldsymbol{G}_1\to\boldsymbol{G}_1/\boldsymbol{H}$, $\varphi(a)=a\boldsymbol{H}$. 显然$\varphi$是满同态映射, $\varphi(\boldsymbol{G}_1)=\boldsymbol{G}_1/\boldsymbol{H}$, 这就证明了群$\boldsymbol{G}_1$的任何商群都是$\boldsymbol{G}_1$的同态像.

若$\boldsymbol{G}_2$是$\boldsymbol{G}_1$的同态像, 即$f:\boldsymbol{G}_1\to\boldsymbol{G}_2$, $f(\boldsymbol{G}_1)=\boldsymbol{G}_2$. 定义$\tilde{f}:\boldsymbol{G}_1/\mathrm{Ker}f\to\boldsymbol{G}_2$, $\tilde{f}(a\mathrm{Ker}f)=f(a)$. 首先说明$\tilde{f}$是映射, 就是说如果$a_1\mathrm{Ker}f=a_2\mathrm{Ker}f$,

那么$a_1^{'}*a_2 \in \mathrm{Ker}f$. 而$(f(a_1))^{'} \bullet f(a_2) = f(a_1^{'}*a_2) = e_2$，得出$f(a_1) = f(a_2)$，即映射$\tilde{f}$与代表元选取无关.

任取$y \in \boldsymbol{G}_2 = f(\boldsymbol{G}_1)$，存在$a \in \boldsymbol{G}_1$使$y = f(a)$，那么$a\mathrm{Ker}f \in \boldsymbol{G}_1/\mathrm{Ker}f$是$y$的原像. 又若$a_1\mathrm{Ker}f, a_2\mathrm{Ker}f \in \boldsymbol{G}_1/\mathrm{Ker}f$都是$y \in f(\boldsymbol{G}_1)$的原像，那么$f(a_1) = f(a_2)$. 而$f(a_1^{'} * a_2) = (f(a_1))^{'} \bullet f(a_2) = e_2$，故$a_1^{'} * a_2 \in \mathrm{Ker}f$，即$a_1\mathrm{Ker}f = a_2\mathrm{Ker}f$. 由上面分析知$\tilde{f}$是双射.

$$\begin{aligned}\tilde{f}(a\mathrm{Ker}f \bullet b\mathrm{Ker}f) &= \tilde{f}((a*b)\mathrm{Ker}f)\\ &= f(a*b) = f(a) \bullet f(b)\\ &= \tilde{f}(a\mathrm{Ker}f) \bullet \tilde{f}(b\mathrm{Ker}f).\end{aligned}$$

故$\tilde{f}$保持运算，是群同构映射. 最后得到

$$\boldsymbol{G}_1/\mathrm{Ker}f \cong f(\boldsymbol{G}_1)$$

例 6.13. $\boldsymbol{H}$是群$\boldsymbol{G}$的正规子群. 令$\varphi : \boldsymbol{G} \to \boldsymbol{G}/\boldsymbol{H}$，$\varphi(a) = a\boldsymbol{H}$，称$\varphi$为自然同态. φ的同态核

$$\begin{aligned}Ker\varphi &= \{x | x \in \boldsymbol{G}, \varphi(x) = \boldsymbol{H}\}\\ &= \{x | x \in \boldsymbol{G}, x\boldsymbol{H} = \boldsymbol{H}\} = \boldsymbol{H}.\end{aligned}$$

例 6.14. 令$\boldsymbol{G}_1 = \langle \boldsymbol{Z}, + \rangle$，$\boldsymbol{G}_2 = \langle a \rangle = \{a^0, a^1, \cdots, a^{n-1}\}$且$a^n = e$. 定义$f : \boldsymbol{Z} \to \langle a \rangle$，$f(m) = a^m$，$f$是从$\boldsymbol{G}_1$到$\boldsymbol{G}_2$的满同态映射，它的同态核

$$Kerf = \{m | m \in \boldsymbol{Z}, a^m = a^0\} = \{kn | k \in \boldsymbol{Z}\} = n\boldsymbol{Z}.$$

由群同态基本定理知

$$\boldsymbol{Z}/n\boldsymbol{Z} \cong \langle a \rangle.$$

而$\boldsymbol{Z}/n\boldsymbol{Z} \cong \boldsymbol{Z}_n$，所以$\langle a \rangle \cong \boldsymbol{Z}_n$. 我们再次得到“$n$阶循环群同构于模$n$同余类群”这个结论.

例 6.15. 用同态基本定理证明定理*6. 7*中的*4°*.

证明 已知$\boldsymbol{H}_2$是$f(\boldsymbol{G}_1)$的正规子群. 定义$\tilde{f} : \boldsymbol{G}_1 \to f(\boldsymbol{G}_1)/\boldsymbol{H}_2.\tilde{f}(a) = f(a)\boldsymbol{H}_2$. 由于$f : \boldsymbol{G}_1 \to f(\boldsymbol{G}_1)$是满同态映射，易知$\tilde{f}$也是满同态映射.

$$\begin{aligned}\mathrm{Ker}\tilde{f} &= \{x|x \in \boldsymbol{G}_1, f(x)\boldsymbol{H}_2 = \boldsymbol{H}_2\} \\ &= \{x|x \in \boldsymbol{G}_1, f(x) \in \boldsymbol{H}_2\} = f^{-1}(\boldsymbol{H}_2),\end{aligned}$$

由定理6. 6知$f^{-1}(\boldsymbol{H}_2)$是$\boldsymbol{G}_1$的正规子群. 再由群同态基本定理知

$$\boldsymbol{G}_1/f^{-1}(\boldsymbol{H}_2) \cong f(\boldsymbol{G}_1)/\boldsymbol{H}_2.$$

定理 6.10. *$\boldsymbol{H}$，$\boldsymbol{K}$均是群$\boldsymbol{G}$的正规子群，且$\boldsymbol{K} \subseteq \boldsymbol{H}$，那么*

$$\boldsymbol{G}/\boldsymbol{H} \cong \frac{\boldsymbol{G}/\boldsymbol{K}}{\boldsymbol{H}/\boldsymbol{K}}.$$

证明 $\boldsymbol{K}$是群$\boldsymbol{G}$的子群. $\boldsymbol{K}$对于$\boldsymbol{G}$中的运算构成群. $\boldsymbol{K} \subseteq \boldsymbol{H}$，$\boldsymbol{H}$对于$\boldsymbol{G}$中的运算也构成群，从而$\boldsymbol{K}$也是$\boldsymbol{H}$的子群. 任取$h \in \boldsymbol{H} \subseteq \boldsymbol{G}$，$k \in \boldsymbol{K}$，由于$\boldsymbol{K}$是$\boldsymbol{G}$的正规子群，$h' * k * h \in \boldsymbol{K}$，所以$\boldsymbol{K}$是$\boldsymbol{H}$的正规子群，从而$\boldsymbol{H}/\boldsymbol{K}$是群.

令$f : \boldsymbol{G}/\boldsymbol{K} \to \boldsymbol{G}/\boldsymbol{H}$，$f(a\boldsymbol{K}) = a\boldsymbol{H}$，容易证明$f$与代表元选取无关，$f$是映射，并且是满射.

$$\begin{aligned}f(a\boldsymbol{K} \bullet b\boldsymbol{K}) &= f(a * b\boldsymbol{K}) = a * b\boldsymbol{H} = a\boldsymbol{H} \bullet b\boldsymbol{H} \\ &= f(a\boldsymbol{K}) \bullet f(b\boldsymbol{K}),\end{aligned}$$

f是满同态映射，它的同态核

$$\begin{aligned}\mathrm{Ker}f &= \{a\boldsymbol{K}|a\boldsymbol{K} \in \boldsymbol{G}/\boldsymbol{K}, f(a\boldsymbol{K}) = \boldsymbol{H}\} \\ &= \{a\boldsymbol{K}|a\boldsymbol{K} \in \boldsymbol{G}/\boldsymbol{K}, a\boldsymbol{H} = \boldsymbol{H}\} \\ &= \{a\boldsymbol{K}|a \in \boldsymbol{H}\} = \boldsymbol{H}/\boldsymbol{K}.\end{aligned}$$

由同态基本定理知

$$\frac{\boldsymbol{G}/\boldsymbol{K}}{\boldsymbol{H}/\boldsymbol{K}} \cong \boldsymbol{G}/\boldsymbol{H}.$$

习题

1. $\boldsymbol{H}$是交换群$\boldsymbol{G}$的子群，证明$\boldsymbol{H}$的每个左陪集也是一个右陪集.
2. $\boldsymbol{H}$是$\boldsymbol{G}$的子群，a, b是$\boldsymbol{G}$中的元素，证明以下六个命题是等价的:

(1)$a' * b \in \boldsymbol{H}$; (2)$b' * a \in \boldsymbol{H}$; (3)$b \in a\boldsymbol{H}$;

(4)$a \in b\boldsymbol{H}$; (5)$a\boldsymbol{H} = b\boldsymbol{H}$; (6)$a\boldsymbol{H} \bigcap b\boldsymbol{H} \neq \varnothing$.

3. 写出$\boldsymbol{A}_4$中关于$\boldsymbol{H} = \{e, (1\,2)(3\,4), (1\,3)(2\,4), (1\,4)(2\,3)\}$的左陪集分解与右陪集分解.

4. $\boldsymbol{H}$是群$\boldsymbol{G}$的指数为2的子群. 证明:对于$\boldsymbol{G}$的任意元素a必有$a^2 \in \boldsymbol{H}$, 若$\boldsymbol{H}$的指数为3, 是否对$\boldsymbol{G}$的任意元素a有$a^3 \in \boldsymbol{H}$? 证明你的断言.

5. $\boldsymbol{H}$,$\boldsymbol{K}$是$\boldsymbol{G}$的两个子群, $[\boldsymbol{G} : \boldsymbol{H}] = m$, $[\boldsymbol{G}, \boldsymbol{K}] = n$, 证明子群$\boldsymbol{H} \bigcap \boldsymbol{K}$在$\boldsymbol{G}$中的指数$\leqslant m \bullet n$.

6. 群$\boldsymbol{G}$的阶数为$p \bullet q$, 其中p, q均为素数且$p < q$. 证明:群$\boldsymbol{G}$不可能有两个不同的q阶子群.

7. $\boldsymbol{H}$是$\boldsymbol{G}$的正规子群. 如果a和b属于$\boldsymbol{H}$的同一个陪集中, c和d属于$\boldsymbol{H}$的同一个陪集中, 那么$a * c$和$b * d$属于$\boldsymbol{H}$的同一个陪集中.

8. $\boldsymbol{G}$是整数加群, $\boldsymbol{H} = \{mk | k \in \boldsymbol{Z}\}$. 商群$\boldsymbol{G}/\boldsymbol{H}$含有哪些元素? 它的单位元是什么? 写出该商群的乘法表.

9. 如果群$\boldsymbol{G}$中含有一个某阶子群, 那么该群必是正规子群.

10. $\boldsymbol{H}_1$和$\boldsymbol{H}_2$是群$\boldsymbol{G}$的正规子群. 证明: $\boldsymbol{H}_1 \bigcap \boldsymbol{H}_2$, $\boldsymbol{H}_1 \bullet \boldsymbol{H}_2$ 也是$\boldsymbol{G}$的正规子群.

11. $\boldsymbol{H}_1, \boldsymbol{H}_2, \boldsymbol{N}$都是$\boldsymbol{G}$的正规子群, 并且$\boldsymbol{H}_1 \subset \boldsymbol{H}_2$, 证明$\boldsymbol{H}_1 \bullet \boldsymbol{N}$是$\boldsymbol{H}_2 \bullet \boldsymbol{N}$的正规子群

12. $\boldsymbol{H}$,$\boldsymbol{K}$都是群$\boldsymbol{G}$的正规子群并且$\boldsymbol{H} \bigcap \boldsymbol{K} = \{e\}$. 证明:对任意$h \in \boldsymbol{H}$, $k \in \boldsymbol{K}$, 都有$h * k = k * h$.

13. 在$\boldsymbol{G} = \{f | f : \boldsymbol{Z} \to \boldsymbol{Z}/(2)\}$上定义运算$+$.

$$(f + g)(x) = f(x) + g(x).$$

证明: $\langle \boldsymbol{G}, + \rangle$是交换群, 并且非零元素的阶为2.

14. 在非零实数乘法群中, 如下定义的映射f中, 哪些是同态映射, 并且找出它的同态核.

(1)$f_1(x) = |x|$; (2)$f_2(x) = 2x$; (3)$f_3(x) = x^2$;

(4)$f_4(x) = \frac{1}{x}$; (5)$f_5(x) = -x$; (6)$f_6(x) = -\dfrac{1}{x}$.

15. 令$\boldsymbol{G} = \{\boldsymbol{A} | \boldsymbol{A} \in (\boldsymbol{Q})_n, |\boldsymbol{A}| \neq 0\}$, $\boldsymbol{G}$对于矩阵乘法构成群. $f : \boldsymbol{G} \to \boldsymbol{R}^*$, $f(\boldsymbol{A}) = |\boldsymbol{A}|$. 证明: f 是从群$\boldsymbol{G}$到非零实数乘群$\boldsymbol{R}^*$的同态映射. 求$f(\boldsymbol{G})$和$\mathrm{Ker} f$.

16. $\boldsymbol{G}$是交换群，k是取定的正整数. $f:\boldsymbol{G}\to\boldsymbol{G}$，$f(a)=a^k$. 证明:$f$是同态映射. 求出$f(\boldsymbol{G})$和$\mathrm{Ker}f$.

17. $\boldsymbol{G}=\langle a\rangle$是$n$阶循环群，$\boldsymbol{G}'=\langle b\rangle$是$m$阶循环群，证明:

$$m|nk\Leftrightarrow\exists\varphi:\boldsymbol{G}\to\boldsymbol{G}'\text{是同态映射并且}\varphi(a)=b^k.$$

18. $\boldsymbol{H}$是$\boldsymbol{G}$的正规子群，$[\boldsymbol{G}:\boldsymbol{H}]=m$. 证明:对于$\boldsymbol{G}$的任意元素$x,x^m\in\boldsymbol{H}$.

19. $\boldsymbol{H},\boldsymbol{K}$是$\boldsymbol{G}$的正规子群. 如果$\boldsymbol{G}/\boldsymbol{H}$，$\boldsymbol{G}/\boldsymbol{K}$是交换群，那么$\boldsymbol{G}/\boldsymbol{H}\bigcap\boldsymbol{K}$也是交换群.

20. 在群$\boldsymbol{G}$中，a,b是$\boldsymbol{G}$中的元素，称$a'*b'*a*b$为$\boldsymbol{G}$的换位元. 证明:

(1)$\boldsymbol{G}$的所有有限个换位元乘积构成$\boldsymbol{G}'$，$\boldsymbol{G}'$是$\boldsymbol{G}$的正规子群;

(2)$\boldsymbol{G}/\boldsymbol{G}'$是交换群;

(3)若$\boldsymbol{N}$是$\boldsymbol{G}$的正规子群且$\boldsymbol{G}/\boldsymbol{N}$是交换群，那么$\boldsymbol{G}'$是$\boldsymbol{N}$的子群.

第 7 章 环和域

实数或复数系统包含两个基本的二元运算：加法和乘法。群论仅仅处理一个二元运算，更没有涉及两个二元运算之间的关系——乘法对加法的分配律。本章将介绍一种新的代数结构——环和域。

7.1 环的定义

定义 7.1. 在具有两个二元运算加法$+$和乘法$\bullet$的集合R中，如果

(1) $\langle R,+\rangle$是交换群;

(2) $\langle R,\bullet\rangle$是含幺半群；

(3) 乘法对加法有左、右分配律，即对任意的三个元素$a,b,c\in R$，都有

$$a\bullet(b+c)=a\bullet b+a\bullet c,$$
$$(b+c)\bullet a=b\bullet a+c\bullet a.$$

则称$\langle R,+,\bullet\rangle$为**环**。

如果在环$\langle R,+,\bullet\rangle$中，对任意的两个元素$a,b\in R$，都有$a\bullet b=b\bullet a$，则称该环是交换环。

从环的定义中可以看出，环中的两个运算$+$和$\bullet$的地位是不同的。集合R对$+$构成交换群，而对$\bullet$只构成含幺半群。加法运算的单位元称为零元，记为0；乘法运算的单位元称为乘法单位元，记为1。R中的任意元素$a\in R$都有加法逆元，称为负元，记为$-a$；但不一定都有乘法逆元。有乘法逆元的元素称为环中的可逆元。

下面是环的几个例子。

例 7.1. $\langle\mathbb{R},+,\bullet\rangle$，$\langle\mathbb{C},+,\bullet\rangle$和$\langle\mathbb{Q},+,\bullet\rangle$分别是实数环、复数环和有理数环，其中$+$和$\bullet$运算是普通的加法和乘法运算。这些环统称为数环。

例 7.2. 全体n阶整数方阵$M_n(\mathbb{Z})$对矩阵加法和矩阵乘法构成n阶矩阵环$\langle M_n(\mathbb{Z}),+,\bullet\rangle$。全部元素都为$0$的$n$阶方阵为零元，$n$阶单位矩阵为乘法单位元，该环是非交换环。

例 7.3. $\langle G,+\rangle$是交换群，$E=\{f|f:G\to G$ 是同态映射$\}$。在E上定义二元运算$+$和$\bullet$如下：对E中的任意两个映射f,g，以及任意的$x\in G$，

$$(f+g)(x)=f(x)+g(x),$$
$$(f\bullet g)(x)=f(g(x)).$$

证明$\langle E,+,\bullet\rangle$是环，被称为交换群$G$上的自同态环。

证明： 对于任意的$f,g\in E$，以及$x\in G$，定义$(f+g)(x)=f(x)+g(x)$。显然，$f+g$是G上的映射。由于f和g都是G上的自同态映射，所以有

$$\begin{aligned}(f+g)(x+y)&=f(x+y)+g(x+y)\\&=(f(x)+f(y))+(g(x)+g(y))\\&=(f(x)+g(x))+(f(y)+g(y))\\&=(f+g)(x)+(f+g)(y).\end{aligned}$$

可见，$f+g$保持加法运算，因此$f+g$是G上的自同态映射，即$f+g\in E$。由于$\langle G,+\rangle$是交换群，所以E中的$+$运算满足结合律和交换律。令$f_0:G\to G$，对任意的$x\in G$，$f_0(x)=0_G$，其中0_G是交换群$\langle G,+\rangle$的零元。显然，f_0是E的零元。对于E中的任意元素$f:G\to G$，定义$f_-:G\to G$，对任意的$x\in G$，$f_-(x)=-f(x)$。易见f_-是f的负元。综上所述可知，$\langle E,+\rangle$是交换群。

对于任意的$f,g\in E$，以及$x\in G$，定义$(f\bullet g)(x)=f(g(x))$。显然，$f\bullet g$是G上的映射。由于f和g都是G上的自同态映射，所以有

$$\begin{aligned}(f\bullet g)(x+y)&=f(g(x+y))=f(g(x)+g(y))\\&=f(g(x))+f(g(y))=(f\bullet g)(x)+(f\bullet g)(y).\end{aligned}$$

可见，$f\bullet g$保持加法运算，因此$f\bullet g$是G上的自同态映射，即$f\bullet g\in E$。映射的复合运算满足结合律。令$f_1:G\to G$，对任意的$x\in G$，$f_1(x)=x$。显然，f_1是E的乘法单位元。综上可知，$\langle E,\bullet\rangle$是含幺半群。

对任意的$f,g,h\in E$和$x\in G$，有

$$\begin{aligned}(f\bullet(g+h))(x)&=f((g+h)(x))=f(g(x)+h(x))\\&=f(g(x))+f(h(x))=(f\bullet g+f\bullet h)(x).\end{aligned}$$

$$((g+h)\cdot f)(x) = (g+h)(f(x)) = g(f(x)+h(f(x))$$
$$= (g\cdot f + h\cdot f)(x),$$

即$f\cdot(g+h) = f\cdot g + f\cdot h$，$(g+h)\cdot f = g\cdot f + h\cdot f$，$\cdot$对$+$满足左、右分配律。因此，$\langle E, +, \cdot\rangle$是环，并且是非交换环。证毕。

例 7.4. 在$\mathbb{Z}_n = \{[0], [1], \cdots, [n-1]\}$上定义

$$[i] + [j] = [i+j],$$
$$[i]\cdot[j] = [i\cdot j].$$

易证如此定义的同余类加法和乘法与代表元的选取无关，即当$[i_1] = [i_2]$，$[j_1] = [j_2]$，则$[i_1 + j_1] = [i_2 + j_2]$，$[i_1\cdot j_1] = [i_2\cdot j_2]$。显然，$\langle\mathbb{Z}_n, +\rangle$是交换群，其中$[0]$为零元，$[-i]$是$[i]$的负元；$\langle\mathbb{Z}_n, \cdot\rangle$是含幺半群，其中$[1]$为乘法单位元。此外，$\cdot$对$+$满足左、右分配律。注意到$\mathbb{Z}_n$中的$\cdot$满足交换律，因此，$\langle\mathbb{Z}_n, +, \cdot\rangle$是环，而且是交换环，被称为模$n$同余类环。

从环的定义知，$\langle R, +\rangle$是交换群，满足左、右消去律。因此，

$$x + a = a \Rightarrow x = 0,$$
$$a + x = 0 \Rightarrow x = -a,$$
$$a + b = a + c \Rightarrow b = c.$$

对环的两个运算$+$和$\cdot$，有以下结论。

定理 7.1. 在环$\langle R, +, \cdot\rangle$中，0和1分别是零元和乘法单位元。对于$R$中的任意元素$a$和$b$，有

(1) $a\cdot 0 = 0\cdot a = 0$；

(2) $a\cdot(-b) = (-a)\cdot b = -(a\cdot b)$，特别地，$(-1)\cdot a = -a$；

(3) $(-a)\cdot(-b) = a\cdot b$，特别地，$(-1)\cdot(-1) = 1$。

证明： (1) $a\cdot 0 = a\cdot(0+0) = a\cdot 0 + a\cdot 0$，由消去律得到$a\cdot 0 = 0$。同理可证，$0\cdot a = 0$。

(2) $a\cdot(-b)+a\cdot b=a\cdot((-b)+b)=a\cdot 0=0$，因此$a\cdot(-b)=-(a\cdot b)$。同理可证，$(-a)\cdot b=-(a\cdot b)$。特别地，取$b=1$，即得$(-1)\cdot a=-a$。

(3) $(-a)\cdot(-b)=-(a\cdot(-b))=-(-(a\cdot b))=a\cdot b$。特别地，取$a=b$，即有$(-1)\cdot(-1)=1$。证毕。

在环$\langle R,+,\cdot\rangle$中，如果零元0_R等于乘法单位元1_R，即$0_R=1_R$，任取$r\in R$，

$$r=r\cdot 1_R=r\cdot 0_R=0_R,$$

即$R=\{0_R\}$。

定义 7.2. 在环$\langle R,+,\cdot\rangle$中，如果$|R|=1$，则$R=\{0_R\}$，称该环为**平凡环**。如果$|R|>1$，那么必有$0_R\neq 1_R$，称这样的环为**非平凡环**。

例 7.5. 环$\langle R,+,\cdot\rangle$中所有可逆元关于$\cdot$构成群。

证明： 令$H=\{r|r\in R,\exists r'\in R,r\cdot r'=r'\cdot r=1_R\}$。任取$r_1,r_2\in H$，存在$r_1',r_2'\in R$，使得$r_1\cdot r_1'=r_1'\cdot r_1=1_R$，$r_2\cdot r_2'=r_2'\cdot r_2=1_R$。由于$(r_1\cdot r_2)\cdot(r_2'\cdot r_1')=(r_2'\cdot r_1')\cdot(r_1\cdot r_2)=1_R$，因此，$r_2'\cdot r_1'\in R$是$r_1\cdot r_2$的乘法逆元，故$r_1\cdot r_2\in H$，即$H$对$\cdot$运算是封闭的。因为$\langle R,\cdot\rangle$是含幺半群，而$H\subseteq R$，显然，$\cdot$运算在$H$中也满足结合律。因为$1_R$的乘法逆元就是自身，即$1_R'=1_R$，所以$1_R\in H$。任取$r\in H$，$r$是$r'$的乘法逆元，故$r'\in H$。综上所述，$\langle H,\cdot\rangle$是群。证毕。

7.2 整环和域

本节介绍两类特殊的环——整环和域。先观察下面的两个例子。

例 7.6. 在整数环$\langle\mathbb{Z},+,\cdot\rangle$中，0是零元。对任何$m,n\in\mathbb{Z}$，如果$m\cdot n=0$，则必有$m=0$或$n=0$。换句话说，如果$m\neq 0$，$m\cdot n=0$，则必有$n=0$。这个性质允许我们在等号两边消去非零元素。这是因为如果$a\cdot b=a\cdot c$且$a\neq 0$，那么$a\cdot(b-c)=0$。由此推出$b-c=0$，即$b=c$。

例 7.7. 在模4同余类环中，$[0]$是零元。$[2]\neq[0]$，但是$[2]\cdot[2]=[0]$，从$[2]\cdot[1]=[2]\cdot[3]$ 推不出$[1]=[3]$。

定义 7.3. 在环$\langle R,+,\cdot\rangle$中，对于非零元素$a\in R$，如果存在一个非零元素$b\in R$，使得$a\cdot b=0$，则称a为**左零因子**。如果存在一个非零元素$c\in R$，使得$c\cdot a=0$，则称a为**右零因子**。若a既是左零因子又是右零因子，则称a为**零因子**。

定理 7.2. 环$\langle R,+,\cdot\rangle$中没有左零因子当且仅当环中的乘法有左、右消去律。

证明: 如果环$\langle R,+,\cdot\rangle$中没有左零因子，对于R中的非零元素a，如果$a\cdot b=a\cdot c$，即$a\cdot(b-c)=0$，可得$b-c=0$，即$b=c$，故左消去律成立。

假如环$\langle R,+,\cdot\rangle$中存在右零因子$b\in R$且$b\neq 0$，那么必然存在非零元素c使得$c\cdot b=0$。则c是R的左零因子，与环R中无左零因子矛盾。换句话说，在环R中无左零因子，那么也一定没有右零因子。用与上面相同的方法同理可证右消去律成立。

反之，环R中的乘法存在左、右消去律。任取环R中的非零元素a，如果$a\cdot b=0$，由于$a\cdot b=0=a\cdot 0$，根据左消去律可得$b=0$，所以a不是左零因子。由a 的任意性可知，环R中没有左零因子。证毕。

定义 7.4. 非平凡交换环$\langle R,+,\cdot\rangle$中，如果没有零因子，则称之为**整环**。

显然在整环中，对于任意元素$a,b\in R$，若$a\cdot b=0$，则必有$a=0$或$b=0$。由定理7.2知，整环中有左、右消去律。

定理 7.3. 在整环中，每个非零元素关于加法运算的阶*(*简称加阶*)*或者是无限的，或者是素数。

证明: 整环$\langle R,+,\cdot\rangle$乘法单位元1_R的加阶有两种情况。

(1) 1_R的加阶是无限的。假设R的某个非零元素a的加阶为m，即$ma=0_R$。

$$ma=\underbrace{a+a+\cdots+a}_{m}=(\underbrace{1_R+1_R+\cdots+1_R}_{m})\cdot a=0_R.$$

因为$a\neq 0_R$，所以$m1_R=\underbrace{1_R+1_R+\cdots+1_R}_{m}=0_R$，这与$1_R$的加阶是无限的矛盾，故$R$中所有非零元素的加阶都是无限的。

(2) 1_R的加阶是有限数k。假设k不是素数，设$k = mn$，即$(mn)1_R = 0_R$。而

$$\begin{aligned}(mn)1_R &= \underbrace{1_R + 1_R + \cdots + 1_R}_{mn} \\ &= \underbrace{(\underbrace{1_R + 1_R + \cdots + 1_R}_{m}) + (\underbrace{1_R + 1_R + \cdots + 1_R}_{m}) + \cdots (\underbrace{1_R + 1_R + \cdots + 1_R}_{m})}_{n} \\ &= \underbrace{(m1_R) + (m1_R) + \cdots + (m1_R)}_{n} \\ &= (\underbrace{1_R + 1_R \cdots + 1_R}_{n}) \cdot (m1_R) = (n1_R) \cdot (m1_R),\end{aligned}$$

且R 是整环，因此有$m1_R = 0_R$或者$n1_R = 0_R$。这与1_R的加阶为$k = mn$矛盾，因此1_R的加阶必为素数。令1_R的加阶为素数p，任取R中的非零元素a,

$$pa = \underbrace{a + a + \cdots + a}_{p} = (\underbrace{1_R + 1_R + \cdots + 1_R}_{p}) \cdot a = 0_R \cdot a = 0_R.$$

因此元素a的加阶是p的因子，而$a \neq 0_R$，所以a的加阶不是1，只能是素数p。证毕。

定义 7.5. 在整环中，如果每个非零元素的加阶为素数p，则称该整环的**特征**为p。如果每个非零元素的加阶是无限的，则称该整环的特征为0。

在特征为p的整环中，

$$(a + b)^p = a^p + C_p^1 a^{p-1} b + \cdots + C_p^{p-1} a b^{p-1} + b^p,$$

由于$p | C_p^i$，$1 \leq i \leq p - 1$，所以$(a + b)^p = a^p + b^b$。

定义 7.6. 在非平凡交换环R中，如果每个非零元素a都存在乘法逆元$a' \in R$，则称环R为**域**。即，非平凡交换环中，如果所有非零元素关于乘法运算构成交换群，则该环是域。

定理 7.4. 域是整环。

证明： 在域F中，若$a \cdot b = 0_F$且$a \neq 0_F$，那么非零元素a有乘法逆元$a' \in F$，

$$b = 1 \cdot b = (a' \cdot a) \cdot b = a' \cdot (a \cdot b) = a' \cdot 0_F = 0_F.$$

即F中没有零因子，所以域F是整环。证毕。

由定理7.4和定理7.3知，有限域的特征为素数p。

定理 7.5. 有限整环是域。

证明： 设$\langle R, +, \cdot \rangle$是有限整环。令$R = \{r_0, r_1, \cdots, r_n\}$。不妨假设$r_0 = 0_R$，$r_1 = 1_R$。任取$r_i \in R$，$1 \leq i \leq n$，

$$r_i R = \{r_i \cdot r_0, r_i \cdot r_1, \cdots, r_i \cdot r_n\} \subseteq R.$$

由于整环中有左、右消去律，当$k \neq l$时，$r_i \cdot r_k \neq r_i \cdot r_l$，所以$|r_i R| = |R|$，从而有$r_i R = R$。存在$j$使得$r_i \cdot r_j = r_1 = 1_R$，即$r_j$是$r_i$的乘法逆元。这说明$R$中所有非零元素都有乘法逆元，所以$R$是域。证毕。

例 7.8. 设p为素数，则$\langle \mathbb{Z}_p, +, \cdot \rangle$是域。

证明： $\mathbb{Z}_p = \{[0], [1], \cdots, [p-1]\}$。易知，$\langle \mathbb{Z}_p, +, \cdot \rangle$是非平凡交换环，$[0]$是零元，$[1]$是乘法单位元。如果$[a] \neq [0]$ 且$[a] \cdot [b] = [0]$，那么$[a \cdot b] = [0]$，即$p | a \cdot b$。而$p \nmid a$，因此$p | b$，即$[b] = [0]$。这说明$\langle \mathbb{Z}_p, +, \cdot \rangle$是有限整环，所以它是域。证毕。

例 7.9. $\langle \{a + b\sqrt{2} | a, b \in \mathbb{Q}\}, +, \cdot \rangle$是域。

证明： 令$\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} | a, b \in \mathbb{Q}\}$。容易验证，$\langle \mathbb{Q}(\sqrt{2}), + \rangle$是交换群，$\langle \mathbb{Q}(\sqrt{2}), \cdot \rangle$ 是含幺半群。0是零元，$-a - b\sqrt{2}$是$a + b\sqrt{2}$的负元，1是乘法单位元。乘法运算是可交换的，并且乘法对加法有左、右分配律。当$a + b\sqrt{2} \neq 0$ 时，$\frac{a}{a^2 - 2b^2} - \frac{b}{a^2 - 2b^2}\sqrt{2} \in \mathbb{Q}(\sqrt{2})$是$a + b\sqrt{2}$的乘法逆元。故$\langle \mathbb{Q}(\sqrt{2}), +, \cdot \rangle$是域。证毕。

7.3 子环和环同态

定义 7.7. 在环$\langle R,+,\cdot\rangle$中，S是R的非空子集。如果

(1) $\langle S,+\rangle$是$\langle R,+\rangle$的子群；

(2) S对乘法运算$\cdot$封闭；

(3) 环R的乘法单位元$1_R \in S$。

则称$\langle S,+,\cdot\rangle$是$\langle R,+,\cdot\rangle$的**子环**。

显然如此定义的子环$\langle S,+,\cdot\rangle$本身是环。

例 7.10. $\langle \mathbb{Z},+,\cdot\rangle$是$\langle \mathbb{Q},+,\cdot\rangle$的子环。

例 7.11. $\langle R,+,\cdot\rangle$是环，令

$$Z(R)=\{x|x\in R,\forall a\in R,a\cdot x=x\cdot a\},$$

则$\langle Z(R),+,\cdot\rangle$是$\langle R,+,\cdot\rangle$的子环。

证明： $Z(R)$是环R中与所有元素可交换的元素集合。显然，R的乘法单位元$1_R \in Z(R)$，所以$Z(R)$是R的非空子集。任取$x,y\in Z(R)$，$\forall a\in R$，

$$\begin{aligned}(x+y)\cdot a &= x\cdot a+y\cdot a=a\cdot x+a\cdot y=a\cdot(x+y),\\ (-x)\cdot a &= -(x\cdot a)=-(a\cdot x)=a\cdot(-x),\end{aligned}$$

即$x+y,-x\in Z(R)$，故$\langle Z(R),+\rangle$是$\langle R,+\rangle$的子群。

$$\begin{aligned}(x\cdot y)\cdot a &= x\cdot(y\cdot a)=x\cdot(a\cdot y)=(x\cdot a)\cdot y\\ &=(a\cdot x)\cdot y=a\cdot(x\cdot y),\end{aligned}$$

即$x\cdot y\in Z(R)$，因此，$Z(R)$对$\cdot$是封闭的。

综上所述，$\langle Z(R),+,\cdot\rangle$是$\langle R,+,\cdot\rangle$的子环。证毕。

定义 7.8. R_1, R_2是环，f是从R_1到R_2的映射，1_{R_1}和1_{R_2}分别是R_1和R_2的乘法单位元。如果对任意$a, b \in R_1$，有

$$\begin{aligned} f(a+b) &= f(a) + f(b), \\ f(a \cdot b) &= f(a) \cdot f(b), \\ f(1_{R_1}) &= 1_{R_2}, \end{aligned}$$

则称f是从R_1到R_2的**环同态映射**。

如果f是满射(单射、双射)，则称f为满环同态映射(单一环同态映射，环同构映射)。

例 7.12. 从$\mathbb{R}^n$到其自身的线性变换全体对加法和乘法运算构成环$\langle L(\mathbb{R}^n, \mathbb{R}^n), +, \cdot \rangle$。$n$阶实数矩阵环记为$\langle M_n(\mathbb{R}), +, \cdot \rangle$。证明这两个环是同构的。

证明： 从$\mathbb{R}^n$到其自身的线性变换α对于$\mathbb{R}^n$的一组基$\mathbf{x_1}, \mathbf{x_2}, \cdots, \mathbf{x_n}$有

$$\alpha \begin{pmatrix} \mathbf{x_1} \\ \mathbf{x_2} \\ \vdots \\ \mathbf{x_n} \end{pmatrix} = \begin{pmatrix} a_{11}\mathbf{x_1} + a_{12}\mathbf{x_2} + \cdots + a_{1n}\mathbf{x_n} \\ a_{21}\mathbf{x_1} + a_{22}\mathbf{x_2} + \cdots + a_{2n}\mathbf{x_n} \\ \vdots \\ a_{n1}\mathbf{x_1} + a_{n2}\mathbf{x_2} + \cdots + a_{nn}\mathbf{x_n} \end{pmatrix}.$$

定义映射$f : L(\mathbb{R}^n, \mathbb{R}^n) \to M_n(\mathbb{R})$为

$$f(\alpha) = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & & & \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{pmatrix}.$$

在线性代数中已经学习过：给定n维空间的一组基，每个线性变换对应一个n阶方阵，并且线性变换的和对应于矩阵的和，线性变换的积对应于矩阵的乘积。所以，对于任意两个线性变换$\alpha, \beta \in L(\mathbb{R}^n, \mathbb{R}^n)$，

$$\begin{aligned} f(\alpha+\beta) &= f(\alpha) + f(\beta), \\ f(\alpha \cdot \beta) &= f(\alpha) \cdot f(\beta). \end{aligned}$$

若γ是单位线性变换，则$f(\gamma)$是单位矩阵。

反之，对任意n阶实数矩阵都可以定义相应的线性变换。不同的线性变换对应不同的矩阵，所以f是满射和单射，因此f是环同构映射。故环$\langle L(\mathbb{R}^n,\mathbb{R}^n),+,\cdot\rangle$与环$\langle M_n(\mathbb{R}),+,\cdot\rangle$是同构的。证毕。

例 7.13. $\langle\mathbb{Z}_{24},+,\cdot\rangle$与$\langle\mathbb{Z}_4,+,\cdot\rangle$是两个环。令$f:\mathbb{Z}_{24}\to\mathbb{Z}_4$，$f([x]_{24})=[x]_4$。首先指出映射$f$的定义与代表元的选取无关。这是因为若$[x]_{24}=[y]_{24}$，则$24|(x-y)$。而$4|24$，故$4|(x-y)$，即$[x]_4=[y]_4$。容易验证，

$$\begin{aligned}f([x]_{24}+[y]_{24})&=f([x+y]_{24})=[x+y]_4\\&=[x]_4+[y]_4=f([x]_{24})+f([y]_{24}),\\f([x]_{24}\cdot[y]_{24})&=f([x\cdot y]_{24})=[x\cdot y]_4\\&=[x]_4\cdot[y]_4=f([x]_{24})\cdot f([y]_{24}),\\f([1]_{24})&=[1]_4.\end{aligned}$$

所以f是环同态映射。

环同态映射也有类似于群同态映射的一些性质。

定理 7.6. 设f是从环R_1到环R_2的同态映射，0_{R_1}和0_{R_2}分别是环R_1和R_2的零元。则f有以下性质：

(1) $f(0_{R_1})=0_{R_2}$；

(2) $f(-a)=-f(a)$；

(3) 若a是R_1的可逆元，则$f(a)$是R_2的可逆元并且$f(a')=(f(a))'$。

证明： f是从环R_1到环R_2的同态映射，那么f也是从交换群$\langle R_1,+\rangle$到交换群$\langle R_2,+\rangle$群同态映射，所以(1)和(2)显然成立。对于(3)，若a是R_1 的可逆元，即存在$a'\in R_1$，使得$a\cdot a'=a'\cdot a=1_{R_1}$，那么

$$\begin{aligned}f(a)\cdot f(a')&=f(a\cdot a')=f(1_{R_1})=1_{R_2},\\f(a')\cdot f(a)&=f(a'\cdot a)=f(1_{R_1})=1_{R_2}.\end{aligned}$$

因此，$f(a')$是$f(a)\in R_2$的乘法逆元，即$f(a')=(f(a))'$。证毕。

例 7.14. $\langle\mathbb{Z},+,\cdot\rangle$与$\langle\mathbb{Z}_n,+,\cdot\rangle$是环。令$f:\mathbb{Z}\to\mathbb{Z}_n$，$f(m)=[m]$。易证，$f$是满同态映射。$\langle\mathbb{Z},+,\cdot\rangle$是整环，但$\langle\mathbb{Z}_n,+,\cdot\rangle$不一定是整环。事实上，当$n$是合数时，$\langle\mathbb{Z}_n,+,\cdot\rangle$不是整环。这是因为当$n=k\cdot l$时，$[k]\cdot[l]=[0]$且$[k],[l]\neq[0]$，环$\langle\mathbb{Z}_n,+,\cdot\rangle$中有零因子，所以不是整环。

例 7.15. $\langle\mathbb{Z}\times\mathbb{Z},+,\cdot\rangle$与$\langle\mathbb{Z},+,\cdot\rangle$是环。令$f:\mathbb{Z}\times\mathbb{Z}\to\mathbb{Z}$，$f((a,b))=a$。易证，$f$是满同态映射。$\mathbb{Z}\times\mathbb{Z}$中的非零元素$(2,0)$和$(0,1)$是零因子，所以$\langle\mathbb{Z}\times\mathbb{Z},+,\cdot\rangle$不是整环，但$\langle\mathbb{Z},+,\cdot\rangle$是整环。

以上两个例子说明环同态映射并不保持环的全部代数结构。但环同构映射对整环和域则不然。

定理 7.7. *f是从环R_1到环R_2的同构映射，如果R_1是整环(域)，则R_2也是整环(域)。*

证明： 如果R_1是整环，则它是非平凡交换环且没有零因子。令$f:R_1\to R_2$是环同构映射。因为R_1是非平凡环，所以$0_{R_1}\neq 1_{R_1}$，故$0_{R_2}=f(0_{R_1})\neq f(1_{R_1})=1_{R_2}$，于是$R_2$是非平凡环。

任取$x_2,y_2\in R_2$，必存在$x_1,y_1\in R_1$，使$f(x_1)=x_2$，$f(y_1)=y_2$。

$$\begin{aligned}x_2\cdot y_2&=f(x_1)\cdot f(y_1)=f(x_1\cdot y_1)=f(y_1\cdot x_1)\\&=f(y_1)\cdot f(x_1)=y_2\cdot x_2.\end{aligned}$$

所以，R_2是交换环。

如果$x_2,y_2\in R_2$且$x_2\cdot y_2=0_{R_2}$，由于存在$x_1,y_1\in R_1$，使$f(x_1)=x_2$，$f(y_1)=y_2$，故有

$$0_{R_2}=x_2\cdot y_2=f(x_1)\cdot f(y_1)=f(x_1\cdot y_1).$$

而f是单射，所以$x_1\cdot y_1=0_{R_1}$。因为R_1中没有零因子，故有$x_1=0_{R_1}$或$y_1=0_{R_1}$，进而得出$x_2=f(x_1)=0_{R_2}$或$y_2=f(y_1)=0_{R_2}$，即R_2中无零因子，故R_2是整环。

设R_1是域。任取R_2的非零元素x_2，因为f是满射，所以必存在$x_1\in R_1$使$f(x_1)=x_2$。f又是单射，所以x_1是R_1中的非零元素，在R_1中有乘法逆元x_1'。

$$f(x_1)\cdot f(x_1')=f(x_1\cdot x_1')=f(1_{R_1})=1_{R_2}$$

所以$f(x_1') \in R_2$是x_2的乘法逆元。由x_2的任意性知R_2是域。证毕。

定理 7.8. 设$\langle R, +, \bullet\rangle$是环。在非空集合$R_1$上定义两个运算+和•。如果存在满射$f : R \to R_1$，对于任意$a, b \in R$有

$$f(a+b) = f(a) + f(b),$$
$$f(a \bullet b) = f(a) \bullet f(b),$$

则$\langle R_1, +, \bullet\rangle$是环。

证明: $f : R \to R_1$是满射，所以R_1中的元素都可以表示成$f(a)$形式，$a \in R$。由于$\langle R, +\rangle$是交换群，易证，R_1中+运算是封闭的且满足交换律和结合律，$f(0_R) \in R_1$是R_1的零元，$f(-a)$是$f(a)$在R_1中的负元，故$\langle R_1, +\rangle$是交换群。由于$\langle R, \bullet\rangle$是含幺半群，所以，$R_1$ 中•运算是封闭的且满足结合律，$f(1_R) \in R_1$是R_1的乘法单位元，故$\langle R_1, \bullet\rangle$是含幺半群。因为$R$中•对+有左、右分配律，所以$R_1$中• 对+也有左、右分配律。故$\langle R_1, +, \bullet\rangle$是环。证毕。

7.4 理想与商环

本节将用类似商群的方法定义商环，其中与正规子群对应的概念是理想。商环是基于对一个理想的所有陪集组成的集合而定义的。

定义 7.9. 设I是环$\langle R, +, \bullet\rangle$的非空子集。如果$\forall x, y \in I$，$r \in R$，有$x - y \in I$，$x \bullet r \in I$ 并且$r \bullet x \in I$，则称I是环R 的一个**理想**。

根据定义7.9，由于$\forall x, y \in I$，有$x - y \in I$，易得$\langle I, +\rangle$是$\langle R, +\rangle$的子群。

每个环R都有两个理想：R和$\{0_R\}$，称这两个理想为**平凡理想**。非平凡理想称为**真理想**。

设I_1, I_2是环R的理想，定义

$$I_1 \bullet I_2 = \{\sum_{k=1}^{n} r_{1k} \bullet r_{2k} | r_{1k} \in I_1, r_{2k} \in I_2, 1 \le k \le n, n = 1, 2, \cdots\},$$
$$I_1 + I_2 = \{r_1 + r_2 | r_1 \in I_1, r_2 \in I_2\},$$

那么$I_1 \bullet I_2$与$I_1 + I_2$都是R的理想。证明留作习题。

例 7.16. 在模6同余类环$\langle\mathbb{Z}_6,+,\cdot\rangle$中，$I_1=\{[0],[3]\}$是理想。在环$\langle\mathbb{Z}\times\mathbb{Z},+,\cdot\rangle$中，$I_2=\{(0,n)|n\in\mathbb{Z}\}$ 是理想。

在环R中，利用R的理想I建立了一个关系：对环R中任意两个元素x与y，

$$x\text{与}y\text{模}I\text{同余}\quad\text{当且仅当}x-y\in I.$$

不难证明环R中的模I同余关系是等价关系。元素x所在的等价类

$$[x]=\{y|y\in R,x-y\in I\}=\{x+i|i\in I\}=x+I.$$

在商集R/I中定义

$$[x]+[y]=[x+y],$$
$$[x]\cdot[y]=[x\cdot y].$$

首先指出，如此定义的等价类加法和乘法是与代表元选取无关的。这是因为，如果$[x_1]=[x_2]$，$[y_1]=[y_2]$，那么由$x_1-x_2\in I$，$y_1-y_2\in I$知

$$(x_1+y_1)-(x_2+y_2)=(x_1-x_2)+(y_1-y_2)\in I,$$
$$(x_1\cdot y_1)-(x_2\cdot y_2)=x_1\cdot(y_1-y_2)+(x_1-x_2)\cdot y_2\in I.$$

故$(x_1+y_1)+I=(x_2+y_2)+I$，$(x_1\cdot y_1)+I=(x_2\cdot y_2)+I$，即$[x_1+y_1]=[x_2+y_2]$，$[x_1\cdot y_1]=[x_2\cdot y_2]$。

定理 7.9. 设I是环R的理想。$R/I=\{x+I|x\in R\}$中的加法$+$和乘法$\cdot$如上定义。则$\langle R/I,+,\cdot\rangle$是环，被称为$R$模$I$的**商环**。

证明： R/I中的$+$和$\cdot$运算是由等价类代表元的$+$与$\cdot$运算实现的，因此，R/I的$+$运算满足结合律和交换律，0_R+I是R/I的零元，$(-x)+I$ 是$x+I$的负元，故$\langle R/I,+\rangle$是交换群。R/I的$\cdot$运算满足结合律，1_R+I是R/I的乘法单位元，故$\langle R/I,\cdot\rangle$是含幺半群。$\cdot$ 对$+$ 显然有左、右分配律。综上所述，$\langle R/I,+,\cdot\rangle$是环。证毕。

例 7.17. 在例7.16中，

$$\mathbb{Z}_6/I_1=\{[0]+I_1,[1]+I_1,[2]+I_1\},$$
$$\mathbb{Z}\times\mathbb{Z}/I_2=\{(m,0)+I_2|m\in\mathbb{Z}\}.$$

定理 7.10. 如果环R的理想I中有可逆元，则$I = R$。

证明： 设环R的理想I中有R的可逆元r，即其乘法逆元$r' \in R$。由理想的定义知$1_R = r \cdot r' \in I$。任取$\widetilde{r} \in R$，$\widetilde{r} = \widetilde{r} \cdot 1_R \in I$，于是$R \subseteq I$。又知理想$I$是$R$的非空子集，即$I \subseteq R$，因此$I = R$，即该理想是平凡理想。证毕。

在域F中，若I是F的理想且$I \neq \{0_F\}$，则必存在一个非零元素$a \in I$。而域的所有非零元素都有乘法逆元，由定理7.10知，$I = F$。也就是说，域F只有两个平凡理想$\{0_F\}$ 和F，没有真理想。因此，域F的商域或是$F/\{0_F\} = \{r + \{0_F\} | r \in F\} \cong F$，或是$F/F = \{F\} \cong \{0_F\}$。它们的结构很简单，不必深入讨论。

本节最后讨论一种特殊的理想。

定理 7.11. 设R是交换环。$\forall a \in R$，$(a) = \{a \cdot r | r \in R\}$是$R$的理想，称之为由$a$生成的理想。这类特殊的理想叫做**主理想**。

证明： 对于$a \in R, a = a \cdot 1_R \in (a)$。所以$(a)$是$R$的非空子集。$\forall a_1, a_2 \in (a)$，存在$r_1, r_2 \in R$使得$a_1 = a \cdot r_1$，$a_2 = a \cdot r_2$。$a_1 - a_2 = a \cdot (r_1 - r_2) \in (a)$。对任意$r \in R$和$a_1 \in (a)$，$r \cdot a_1 = r \cdot (a \cdot r_1) = a \cdot (r \cdot r_1) \in (a)$，$a_1 \cdot r = a \cdot (r_1 \cdot r) \in (a)$。所以$(a)$是$R$的理想。证毕。

这个概念可以推广到交换环R的子集上。令$S = \{a_1, a_2, \cdots, a_k\} \subseteq R$，

$$(a_1, a_2, \cdots, a_k) = \{a_1 \cdot r_1 + a_2 \cdot r_2 + \cdots + a_k \cdot r_k | r_1, r_2, \cdots r_k \in R\},$$

是R的理想，被称为S生成的理想，也是主理想。

定义 7.10. 如果环R的所有理想都是主理想，则称R是**主理想环**。

例 7.18. 整数环$\langle \mathbb{Z}, +, \cdot \rangle$是主理想环。

证明： 设I是整数环$\langle \mathbb{Z}, +, \cdot \rangle$的理想。如果$I$中没有非零元素，即$I = \{0\}$，则$I$是由0生成的理想。

如果I中有非零元素，那么必有正整数$a \in I$ (如果$b < 0$且$b \in I$，由于I是理想，$-1 \in \mathbb{Z}$，$-b = (-1) \cdot b \in I$，并且$-b > 0$)。这样就可以在I 中找到最小的正整数k。对于I中任意元素n，$n = m \cdot k + q$，$0 \leq q \leq k - 1$。由于I是理想，所以$q = n - m \cdot k \in I$。而k是I中最小的正整数，必有$q = 0$，即$n = m \cdot k \in (k)$。因此$I \subseteq (k)$。又由于$k \in I$，显然$m \cdot k \in I$，故$(k) \subseteq I$。因此，$I = (k)$。即整数环是主理想环。证毕。

7.5 多项式环

7.5.1 环上的多项式

环$\langle R,+,\bullet\rangle$上的多项式定义为

$$p(x)=a_0+a_1x+\cdots+a_nx^n,\quad a_n\neq 0_R, n\geq 0,$$

其中$a_0,a_1,\cdots,a_n\in R$称为系数，x为未定元，n为$p(x)$的次数，即$deg(p(x))=n$。环R上的非零元素称为零次多项式(或常数多项式)，零元素0_R称为零多项式。

环R上的全体多项式组成的集合记为$R[x]$，在其上定义运算$+$和$\bullet$。对任意的$f(x),g(x)\in R[x]$，其中$f(x)=\sum_{i=0}^{n}a_ix^i$，$g(x)=\sum_{j=0}^{m}b_jx^j$，

$$f(x)+g(x)=\sum_{k=0}^{\max\{m,n\}}(a_k+b_k)x^k,$$

$$f(x)\bullet g(x)=\sum_{k=0}^{m+n}c_kx^k,\quad c_k=\sum_{i+j=k}a_i\bullet b_j, 0\leq k\leq m+n,$$

其中$m<n$时$a_k=0$，$n<k\leq m$；$m<n$时$b_k=0$，$m<k\leq n$。不难验证$\langle R[x],+,\bullet\rangle$是环。零多项式是零元，$-f(x)$是$f(x)$的负元，常数多项式$1_R$是乘法单位元。

设R是整环，即R是非平凡交换环并且没有零因子。设$f(x)$与$g(x)$是$R[x]$中的非零多项式，它们的次数分别是$n,m(\geq 0)$，即$f(x)=a_nx^n+\cdots$，$g(x)=b_mx^m+\cdots$，$a_n,b_m\neq 0_R$。由于R是整环，所以$a_n\bullet b_m\neq 0_R$。故

$$f(x)\bullet g(x)=a_nb_mx^{n+m}+\cdots$$

是非零多项式，因此$R[x]$中没有零因子。又$R[x]$是非平凡交换环，故$R[x]$是整环。

7.5.2 域上的多项式

定理 7.12. 设F是域，$f(x),g(x)$是多项式环$F[x]$的元素。如果$g(x)$不是零多项式，则存在唯一的$q(x),r(x)\in F[x]$，使得

$$f(x)=q(x)\bullet g(x)+r(x),$$

其中$r(x)$或是零多项式，或是次数小于$deg(g(x))$的多项式。

证明： 令$g(x)=b_0+b_1x+\cdots+b_mx^m$，$b_m\neq 0_F$，$m\geq 0$。考虑集合

$$S'=\{f(x)-s(x)\cdot g(x)|s(x)\in F[x]\}.$$

有两种可能的情况:

(1) 零多项式$0_F\in S'$。此时存在$q(x)\in F[x]$，使得$f(x)=q(x)\cdot g(x)$。

(2) 零多项式$0_F\notin S'$。记S'中次数最小的多项式为$r(x)$，则存在$q(x)\in F[x]$，使得$r(x)=f(x)-q(x)\cdot g(x)$，即$f(x)=q(x)\cdot g(x)+r(x)$。设$r(x)=c_tx^t+\cdots+c_0$，$c_t\neq 0_F$。假设$deg(r(x))=t\geq deg(g(x))=m$。现构造一个新的多项式，

$$r_1(x)=f(x)-q(x)\cdot g(x)-c_t\cdot b'_mx^{t-m}\cdot g(x)=r(x)-c_tx^t+\cdots,$$

于是$deg(r_1(x))<deg(r(x))$，而

$$r_1(x)=f(x)-[q(x)+c_t\cdot b'_mx^{t-m}]\cdot g(x)]\in S'.$$

这与$r(x)$是S'中次数最低的多项式矛盾，所以必有$deg(r(x))<deg(g(x))$。

下面证明$q(x)$和$r(x)$是唯一的。假设$q_1(x),r_1(x)$及$q_2(x),r_2(x)$均满足:

$$f(x)=q_1(x)\cdot g(x)+r_1(x),$$
$$f(x)=q_2(x)\cdot g(x)+r_2(x),$$

并且$r_1(x)$，$r_2(x)$的次数均小于$g(x)$的次数(即m)。将上面两式相减，可得

$$(q_1(x)-q_2(x))\cdot g(x)=r_2(x)-r_1(x).$$

如果$q_1(x)-q_2(x)$不是零多项式，那么上式左边多项式的次数大于等于m，而右边多项式的次数小于m，矛盾。故必有$q_1(x)=q_2(x)$，由此又可得出$r_1(x)=r_2(x)$。证毕。

定理7.12说明域上的多项式可以做除法，商和余式是唯一确定的。如果$f(x)=q(x)\cdot g(x)$，则称$g(x)$是$f(x)$的因式。特别地，取$g(x)=x-a$，$f(x)$除以$x-a$的余式是域F的元素，即

$$f(x)=q(x)\cdot(x-a)+r_0,\quad r_0\in F.$$

令$x=a$，则$r_0=f(a)$。由此可知，在$F[x]$中，多项式$x-a$是$f(x)$的因式当且仅当$f(a)=0_F$，这时称a是多项式$f(x)$的根。

定理 7.13. 域F上的多项式环$F[x]$是主理想环。

证明： 设I是$F[x]$的一个理想。若I中没有非零多项式，则$I=\{0_F\}$，它是由0_F生成的理想。若I中有非零多项式，其中次数最低的非零多项式记为$g(x)$。根据$g(x)$的次数可以分为两种情况:

(1) $deg(g(x))=0$。即$g(x)=a\in F$且$a\neq 0_F$。a在F中有乘法逆元a'，$a'\in F[x]$。$a'\cdot a=1_F\in I$，与定理7.10 的证明类似，可得$I=F[x]$。I是由1_F生成的理想。

(2) $deg(g(x))\neq 0$。任取$f(x)\in I$，由定理7.12知，存在$q(x),r(x)\in F[x]$使$f(x)=q(x)\cdot g(x)+r(x)$。因为$g(x)\in I$且I是$F[x]$ 的理想，所以$r(x)=f(x)-q(x)\cdot g(x)\in I$。由于$g(x)$是$I$中次数最低的多项式，故必有$r(x)=0_F$，即$f(x)=q(x)\cdot g(x)\in(g(x))$。由$f(x)$的任意性知$I\subseteq(g(x))$。反之，$g(x)\in I$，对任何$q(x)\in F[x]$，$q(x)\cdot g(x)\in I$，所以$(g(x))\subseteq I$。综上，$I=(g(x))$。

所以域F上的多项式环$F[x]$是主理想环。证毕。

7.5.3 域上的多项式商环

域F的多项式环$F[x]$是主理想环。$F[x]$的理想都是$P=(p(x))$形式，其中$p(x)=a_0+a_1x+\cdots+a_nx^n$，$a_n\neq 0_F$，则

$$F[x]/P=\{f(x)+P|f(x)\in F[x]\}.$$

而$f(x)=q(x)\cdot p(x)+r(x)$，$f(x)-r(x)\in(p(x))$，即$f(x)+P=r(x)+P$。所以

$$F[x]/P=\{b_0+b_1x+\cdots+b_{n-1}x^{n-1}+P|b_0,b_1,\cdots,b_{n-1}\in F\}.$$

例 7.19. 写出$\mathbb{Z}_2[x]/(x^2+x+1)$的加法表和乘法表。

解： $\mathbb{Z}_2=\{[0],[1]\}$，简记为$\mathbb{Z}_2=\{0,1\}$。(x^2+x+1)是$\mathbb{Z}_2[x]$的主理想。令$P=(x^2+x+1)$，则有

$$\begin{aligned}\mathbb{Z}_2[x]/P&=\{(ax+b)+P|a,b\in\mathbb{Z}_2\}\\&=\{P,1+P,x+P,1+x+P\}.\end{aligned}$$

表 7.1: $\mathbb{Z}_2[x]/(x^2+x+1)$的加法表和乘法表

$+$	P	$1+P$	$x+P$	$1+x+P$
P	P	$1+P$	$x+P$	$1+x+P$
$1+P$	$1+P$	P	$1+x+P$	$x+P$
$x+P$	$x+P$	$1+x+P$	P	$1+P$
$1+x+P$	$1+x+P$	$x+P$	$1+P$	P

$\cdot$	P	$1+P$	$x+P$	$1+x+P$
P	P	P	P	P
$1+P$	P	$1+P$	$x+P$	$1+x+P$
$x+P$	P	$x+P$	$1+x+P$	$1+P$
$1+x+P$	P	$1+x+P$	$1+P$	$x+P$

它的加法表和乘法表如表7.1所示。

7.6 环同态定理

定义 7.11. 设φ是从环R_1到环R_2的同态映射。0_{R_2}是R_2的零元。$Ker\varphi = \{r|r \in R_1, \varphi(r) = 0_{R_2}\}$称为$\varphi$的**同态核**。

定理 7.14. 设φ是从环R_1到环R_2的同态映射，则$Ker\varphi$是R_1的理想。

证明： φ是从R_1到R_2的环同态映射，所以也是从交换群$\langle R_1, +\rangle$到$\langle R_2, +\rangle$的群同态映射。由定理6.6知，Kerφ是$\langle R_1, +\rangle$的正规子群。任取$x_1, x_2 \in$ Kerφ，$x_1 - x_2 \in$ Kerφ。又若$x \in$ Kerφ，$r \in R_1$，

$$\varphi(x \cdot r) = \varphi(x) \cdot \varphi(r) = 0_{R_2} \cdot \varphi(r) = 0_{R_2},$$

故$x \cdot r \in$ Kerφ。同理可证$r \cdot x \in$ Kerφ。所以，Kerφ是R_1的理想。证毕。

定理 7.15.（环同态基本定理） 环R_1的任意商环都是环R_1的同态像。若φ是从环R_1到环R_2的满同态映射，则

$$R_1/Ker\varphi \cong R_2.$$

证明： 设I_1是环R_1的理想。令$\widetilde{\varphi}: R_1 \to R_1/I_1$，$\widetilde{\varphi} = r + I_1$。显然，$\widetilde{\varphi}$是满射。对任意$r_1, r_2 \in R_1$，

$$\begin{aligned}
\widetilde{\varphi}(r_1 + r_2) &= (r_1 + r_2) + I = (r_1 + I) + (r_2 + I) = \widetilde{\varphi}(r_1) + \widetilde{\varphi}(r_2),\\
\widetilde{\varphi}(r_1 \cdot r_2) &= (r_1 \cdot r_2) + I = (r_1 + I) \cdot (r_2 + I) = \widetilde{\varphi}(r_1) \cdot \widetilde{\varphi}(r_2),\\
\widetilde{\varphi}(1_{R_1}) &= 1_{R_1} + I,
\end{aligned}$$

因此，$\widetilde{\varphi}$是满同态映射，$\widetilde{\varphi}(R_1) = R_1/I_1$。因此，环$R_1$的任意商环都是环$R_1$的同态像。

若φ是从环R_1到环R_2的满同态映射，那么φ也是从$\langle R_1, +\rangle$到$\langle R_2, +\rangle$的群同态映射。由群同态基本定理知$\widetilde{\varphi}: R_1/\mathrm{Ker}\varphi \to R_2$，$\widetilde{\varphi}(r + \mathrm{Ker}\varphi) = \varphi(r)$是群同构映射。另有

$$\begin{aligned}
&\widetilde{\varphi}((r_1 + \mathrm{Ker}\varphi) \cdot (r_2 + \mathrm{Ker}\varphi)) = \widetilde{\varphi}(r_1 \cdot r_2 + \mathrm{Ker}\varphi) = \varphi(r_1 \cdot r_2)\\
&\quad = \varphi(r_1) \cdot \varphi(r_2) = \widetilde{\varphi}((r_1 + \mathrm{Ker}\varphi)) \cdot \widetilde{\varphi}((r_2 + \mathrm{Ker}\varphi)),\\
&\widetilde{\varphi}((1_{R_1} + \mathrm{Ker}\varphi)) = \varphi(1_{R_1}) = 1_{R_2},
\end{aligned}$$

故$\widetilde{\varphi}$是环同构映射，从而$R_1/\mathrm{Ker}\varphi \cong R_2$。证毕。

例 7.20. $\mathbb{Q}[x]$是有理数域$\mathbb{Q}$上的多项式集合。令$\mathbb{Q}(\sqrt{2}) = \{a+b\sqrt{2} | a, b \in \mathbb{Q}\}$。证明

$$\mathbb{Q}[x]/(x^2 - 2) \cong \mathbb{Q}(\sqrt{2}).$$

证明： 令$\psi : \mathbb{Q}[x] \to \mathbb{Q}(\sqrt{2})$，$\psi(f(x)) = f(\sqrt{2})$。易证，$\psi$是从$\mathbb{Q}[x]$到$\mathbb{Q}(\sqrt{2})$的环同态映射。任取$a + b\sqrt{2} \in \mathbb{Q}(\sqrt{2})$，存在$a + bx \in \mathbb{Q}[x]$，使$\psi(a + bx) = a + b\sqrt{2}$，所以$\psi$是满同态映射。

下面求$\mathrm{Ker}\psi$。若$p(x) \in \mathrm{Ker}\psi$，即$p(\sqrt{2}) = 0$。取$g(x) = x^2 - 2$，由定理7.12知，

$$p(x) = q(x)(x^2 - 2) + a_0 + a_1 x,\ a_0, a_1 \in \mathbb{Q}.$$

由$p(\sqrt{2})=0$可得$a_0+a_1\sqrt{2}=0$，因此$a_0=a_1=0$。由此得到$p(-\sqrt{2})=a_0-a_1\sqrt{2}=0$。故，$x^2-2$是$p(x)$的因式。于是，$\mathrm{Ker}\psi=\{p(x)|x^2-2\text{是}p(x)\text{的因式}\}=(x^2-2)$，是$x^2-2$生成的理想。根据环同态基本定理知，$\mathbb{Q}[x]/(x^2-2)\cong\mathbb{Q}(\sqrt{2})$。证毕。

例 7.21. 证明$\mathbb{R}[x]/(x^2+1)\cong\mathbb{C}$。

证明： 令$\psi:\mathbb{R}[x]\to\mathbb{C}$，$\psi(f(x))=f(\mathrm{i})$，其中$\mathrm{i}=\sqrt{-1}$。易证，$\psi$是从$\mathbb{R}[x]$到$\mathbb{C}$ 的环同态映射。任取$a+b\mathrm{i}\in\mathbb{C}$，存在$a+bx\in\mathbb{R}[x]$，使得$\psi(a+bx)=a+b\mathrm{i}$，所以$\psi$是满同态映射。

下面求$\mathrm{Ker}\psi$。任取$p(x)\in\mathrm{Ker}\psi$，即$p(\mathrm{i})=0$。取$g(x)=x^2+1$，由定理7.12知，

$$p(x)=q(x)(x^2+1)+a_0+a_1x,\ a_0,a_1\in\mathbb{R}.$$

由$p(\mathrm{i})=0$可得$a_0+a_1\mathrm{i}=0$，因此$a_0=a_1=0$。由此得到$p(-\mathrm{i})=a_0-a_1\mathrm{i}=0$。故，$x^2+1$是$p(x)$的因式。于是，$\mathrm{Ker}\psi=\{p(x)|x^2+1\text{是}p(x)\text{的因式}\}=(x^2+1)$，是$x^2+1$生成的理想。根据环同态基本定理知，$\mathbb{R}[x]/(x^2+1)\cong\mathbb{C}$。证毕。

定理 7.16. *f是从环R_1到环R_2的同态映射，则*

(1) 若S_1是R_1的子环，则$f(S_1)$是R_2的子环。特别地，$f(R_1)$是R_2的子环。

(2) 若S_1是R_1的理想，则$f(S_1)$是$f(R_1)$的理想。

(3) 若S_2是$f(R_1)$的子环，则$f^{-1}(S_2)$是R_1的子环。

(4) 若S_2是$f(R_1)$的理想，则$f^{-1}(S_2)$是R_1的理想，且$R_1/f^{-1}(S_2)\cong f(R_1)/S_2$。

证明： 这里只证明(1)和(4)，(2)和(3)的证明方法类似，留作习题。

(1) f是从R_1到R_2的环同态映射，那么f是从$\langle R_1,+\rangle$到$\langle R_2,+\rangle$的群同态映射。S_1是R_1的子环，故$\langle S_1,+\rangle$是$\langle R_1,+\rangle$的子群。由定理6.7知$\langle f(S_1),+\rangle$是$\langle R_2,+\rangle$的子群。任取$x_2,y_2\in f(S_1)$，存在$x_1,y_1\in S_1$，使得$f(x_1)=x_2$，$f(y_1)=y_2$。因为$x_1\cdot y_1\in S_1$，所以

$$x_2\cdot y_2=f(x_1)\cdot f(y_1)=f(x_1\cdot y_1)\in f(S_1).$$

$f(S_1)$对乘法$\cdot$是封闭的。$1_{R_1} \in S_1$，$f(1_{R_1}) = 1_{R_2}$，即$1_{R_2} \in f(S_1)$。由此可知，$\langle f(S_1), +, \cdot\rangle$是$\langle R_2, +, \cdot\rangle$的子环。特别地，取$S_1 = R_1$，可得$f(R_1)$是$R_2$的子环。

(4) 因为S_2是$f(R_1)$的理想，所以$f(R_1)/S_2$是环。令$\psi : f(R_1) \to f(R_1)/S_2$，$\psi(f(r_1)) = f(r_1) + S_2$。显然，$\psi$是满射。又因为$f$是从$R_1$ 到$f(R_1)$的满射，所以$\psi \circ f$是从R_1到$f(R_1)/S_2$的满射。对于$r_1, r_2 \in R_1$，

$$\begin{aligned}(\psi \circ f)(r_1 + r_2) &= \psi(f(r_1 + r_2)) = f(r_1 + r_2) + S_2 = (f(r_1) + f(r_2)) + S_2\\ &= (f(r_1) + S_2) + (f(r_2) + S_2) = (\psi \circ f)(r_1) + (\psi \circ f)(r_2),\\ (\psi \circ f)(r_1 \cdot r_2) &= \psi(f(r_1 \cdot r_2)) = f(r_1 \cdot r_2) + S_2 = (f(r_1) \cdot f(r_2)) + S_2\\ &= (f(r_1) + S_2) \cdot (f(r_2) + S_2) = (\psi \circ f)(r_1) \cdot (\psi \circ f)(r_2),\\ (\psi \circ f)(1_{R_1}) &= \psi(f(1_{R_1})) = f(1_{R_1}) + S_2 = 1_{R_2} + S_2,\end{aligned}$$

因此，$\psi \circ f$是从环R_1到环$f(R_1)/S_2$的满同态映射。

$$\begin{aligned}\mathrm{Ker}(\psi \circ f) &= \{r | r \in R_1, (\psi \circ f)(r) = S_2\}\\ &= \{r | r \in R_1, f(r) \in S_2\} = f^{-1}(S_2).\end{aligned}$$

由环同态基本定理可得，$R_1/f^{-1}(S_2) \cong f(R_1)/S_2$。证毕。

定理 7.17. *I_1, I_2是环R的两个理想，$I_2 \subseteq I_1$，则I_1/I_2是R/I_2的理想，且*

$$\frac{R/I_2}{I_2/I_1} \cong R/I_1.$$

证明： I_1, I_2是环R的理想，所以R/I_2和R/I_1是两个商环。因为$I_2 \subseteq I_1 \subseteq R$，商集$I_1/I_2 = \{i + I_2 | i \in I_1\} \subseteq R/I_2$。定义$f : R/I_2 \to R/I_1$，$f(r + I_2) = r + I_1$。当$r_1 + I_2 = r_2 + I_2$时，$r_1 - r_2 \in I_2$，而$I_2 \subseteq I_1$，所以$r_1 - r_2 \in I_1$，从而$r_1 + I_1 = r_2 + I_1$。所以映射$f$与代表元选取无关。显然，$f$是满射。对于$r_1, r_2 \in R$，

$$\begin{aligned}f((r_1 + I_2) + (r_2 + I_2)) &= f((r_1 + r_2) + I_2) = (r_1 + r_2) + I_1\\ &= (r_1 + I_1) + (r_2 + I_1) = f((r_1 + I_2)) + f((r_2 + I_2)),\\ f((r_1 + I_2) \cdot (r_2 + I_2)) &= f((r_1 \cdot r_2) + I_2) = (r_1 \cdot r_2) + I_1\\ &= (r_1 + I_1) \cdot (r_2 + I_1) = f((r_1 + I_2)) \cdot f((r_2 + I_2)),\\ f(1_{R_1} + I_2) &= 1_{R_1} + I_1,\end{aligned}$$

所以，f是从环R/I_2到环R/I_1的满同态映射。

$$\mathrm{Ker}f = \{r + I_2 | r + I_1 = I_1\} = \{r + I_2 | r \in I_1\} = I_1/I_2.$$

由环同态基本定理知，$\frac{R/I_2}{I_1/I_2} \cong R/I_1$。证毕。

7.7 素理想和极大理想

I是环R的理想，则R/I是环。那么什么样的理想能使R/I为整环或者为域呢? 以整数环$\langle \mathbb{Z}, +, \cdot \rangle$为例。整数环$\mathbb{Z}$的所有理想都是主理想。设$p$为素数，$(p) = \{k \cdot p | k \in \mathbb{Z}\}$是$\mathbb{Z}$的理想。

$$\mathbb{Z}/(p) = \{(p), 1 + (p), \cdots, p - 1 + (p)\} \cong \mathbb{Z}_p.$$

如果$(i+(p))\cdot(j+(p)) = (p)$，即$i \cdot j \in (p)$，$p|i \cdot j$，由素数的性质知$p|i$或$p|j$。因此，$i + (p) = (p)$或$j + (p) = (p)$。所以，$\mathbb{Z}/(p)$ 是整环。由此引出素理想的概念。

定义 7.12. I是非平凡交换环R的理想，$I \neq R$。对于R的任意元素a, b，如果$a \cdot b \in I$，必有$a \in I$ 或$b \in I$，那么称I为环R的**素理想**。

定理 7.18. I是非平凡交换环R的理想。R/I是整环当且仅当I是素理想。

证明: 假设R/I是整环。对R中的任意元素a, b，如果$a \cdot b \in I$，则$(a + I) \cdot (b + I) = a \cdot b + I = I$。由于$R/I$中没有零因子，所以必有$a + I = I$或者$b + I = I$ (I是R/I的零元)。于是，$a \in I$ 或者$b \in I$。所以I是素理想。

反之，如果I是环R的素理想。在环R/I中，若$(a+I)\cdot(b+I) = a\cdot b+I = I$，则必有$a \cdot b \in I$。因为$I$是素理想，所以$a \in I$或者$b \in I$，即$a + I = I$ 或者$b + I = I$。这说明R/I中没有零因子。所以R/I是整环。证毕。

例 7.22. 证明主理想环$F[x]$的任意理想(x)都是素理想，其中F是域。

证明: 设(x)是$F[x]$的一个理想，商环

$$F[x]/(x) = \{f(x) + (x) | f(x) \in F[x]\} = \{a + (x) | a \in F[x]\}.$$

定义$\varphi : F[x]/(x) \to F$，$\varphi(a+(x)) = a$，易证φ是环同构映射。因此，$F[x]/(x) \cong F$，$F[x]/(x)$是整环，由定理7.18知，(x)是素理想。证毕。

定义 7.13. I是环R的理想，$I \neq R$。若$I \subset M$，M是R的理想，则必有$M = R$。称这样的理想I是R的**极大理想**。

例 7.23. 整数环$\mathbb{Z}$中，p是素数，(p)是$\mathbb{Z}$的素理想，也是$\mathbb{Z}$的极大理想。这是因为，若M是$\mathbb{Z}$的理想并且$(p) \subset M$，则M中必有元素$m \notin (p)$，即$m = kp + l$，$0 < l < p$。因为$m, p \in M$，所以$l = m - kp \in M$。若$l \neq p$，则l与p互素，存在$a, b \in \mathbb{Z}$使$la + pb = 1$，因此$1 \in M$，与定理7.10的证明类似，可得$M = \mathbb{Z}$。

例 7.24. 域F上的多项式环$F[x]$中，(x)是$F[x]$的素理想，也是$F[x]$的极大理想。这是因为如果M是$F[x]$的理想且$(x) \subset M$，则M中存在$f(x) \notin (x)$，即$f(x) = a_n x^n + \cdots + a_1 x + a_0 \in M$，$a_0 \neq 0$ (因为$f(x) \notin (x)$)。令$f(x) = f_1(x) + a_0$，$f_1(x) \in (x) \subset M$，由此可得$a_0 \in M$。而a_0是域F的非零元素，所以是F的可逆元，也是$F[x]$的可逆元。也就是说，$F[x]$的理想M包含可逆元a_0，由定理7.10知，$M = F[x]$。

定理 7.19. I是非平凡交换环R的理想。R/I是域当且仅当I是极大理想。

证明： 已知R/I是域，$I \neq R$。若$I \subset M$，M是R的理想，那么存在$a \in M$且$a \notin I$。显然，$a + I$是域R/I的非零元素，它的乘法逆元是$x + I$，即$(a + I) \cdot (x + I) = 1_R + I$。因为$a \in M$，$x \in R$，$M$是$R$的理想，所以$a \cdot x \in M$。又$I \subset M$，故$1_R + I = (a + I) \cdot (x + I) = a \cdot x + I \subseteq M$，故有$1_R \in M$，从而$M = R$。即$I$是极大理想。

反之，I是极大理想，任取$a \notin I$，$a + I$是R/I的非零元素。如果$x + I$是$a + I$的乘法逆元，那么x应该满足

$$(a + I) \cdot (x + I) = a \cdot x + I = 1_R + I,$$

即$a \cdot x - 1_R \in I$。考虑集合

$$A = \{-i + a \cdot x | i \in I, x \in R\}.$$

显然，$I \subset A$，A是R的非空子集。任取$-i_1+a\cdot x_1, -i_2+a\cdot x_2 \in A$，$y \in R$，

$$(-i_1 + a\cdot x_1) - (-i_2 + a\cdot x_2) = -(i_1 - i_2) + a(x_1 - x_2) \in A,$$
$$(-i_1 + a\cdot x_1)\cdot y = -i_1\cdot y + a\cdot(x_1\cdot y) \in A,$$

因此，A是R的理想，且$I \subset A$。由于I是极大理想，所以$A = R$，于是R的乘法单位元$1_R \in A$。因此存在$i_0 \in I, x_0 \in R$使得$1_R = -i_0 + a\cdot x_0$，即$a\cdot x_0 - 1_R = i_0 \in I$。因此，$x_0 + I$是$a + I$的乘法逆元。有$a + I$的任意性可知，$R/I$是域。证毕。

如果I是非平凡交换环R的极大理想，那么R/I是域；而域又是整环，所以R/I是整环，进而得出I是R的素理想。故有下面的推论：

推论 7.1. 非平凡交换环的极大理想一定是素理想。

此推论的逆命题不一定成立。例如整数环$\mathbb{Z}$上的多项式环$\mathbb{Z}[x]$，(x)是$\mathbb{Z}[x]$的素理想。$\mathbb{Z}[x]/(x) \cong \mathbb{Z}$，而$\mathbb{Z}$不是域，故$(x)$不是$\mathbb{Z}[x]$的极大理想。

习题

1. 下列代数系统哪些是环?

(1) $\langle \mathbb{Z}\times\mathbb{Z}, +, \cdot\rangle$，其中$+$与$\cdot$均是对分量的运算；

(2) $\langle 2\mathbb{Z}\times\mathbb{Z}, +, \cdot\rangle$，其中$+$与$\cdot$同上；

(3) $\langle \mathbb{R}, +, *\rangle$，其中$+$是实数加法，$a * b = |a|\cdot b$。

2. 写出下列各环的全部可逆元。

(1) $\langle \mathbb{Z}, +, \cdot\rangle$；　　(2) $\langle \mathbb{Z}, +, \cdot\rangle$；

(3) $\langle \mathbb{Z}_4, +, \cdot\rangle$；　　(4) $\langle \mathbb{Z}_6, +, \cdot\rangle$。

3. 在环$\langle R, +, \cdot\rangle$中，如果$\langle R, +\rangle$是循环群，则$\langle R, +, \cdot\rangle$是交换环。

4. 在环R中，如果对于任意$a \in R$均有$a^2 = a$，则称该环是布尔环。证明：

(1) $\forall a \in R$，$2a = 0_R$；

(2) R是交换环。

5. 下列环中哪些是整环，哪些是域? 说明理由。

(1) $\langle \mathbb{Z}\times\mathbb{Z}, +, \cdot\rangle$;

(2) $\langle \{a+b\sqrt{2}|a,b\in\mathbb{Z}\}, +, \cdot\rangle$;

(3) $\langle \{a+b\sqrt{3}|a,b\in\mathbb{Q}\}, +, \cdot\rangle$。

6. 若a是环R的可逆元，则

(1) $-a$也是可逆元;

(2) a不是零因子。

7. 在交换环中，若$a\cdot b$是零因子，则a是零因子或b是零因子。

8. E加群$\langle G, +\rangle$的自同态环，如果H是G的子群，那么

$$E_H = \{f|f\in E, f(H)\subseteq H\}$$

是E的子环。

9. 一个环的任意两个子环的交仍是子环。

10. 令$f:\mathbb{Z}\times\mathbb{Z}\to Z$，$f(a,b)=a$。证明$f$是从环$\langle\mathbb{Z}\times\mathbb{Z}, +, \cdot\rangle$到环$\langle\mathbb{Z}, +, \cdot\rangle$的同态映射，并求$\mathrm{Ker}f$。

11. 求出环$\mathbb{Z}_6$的所有理想。

12. 若I_1和I_2是环R的理想，则$I_1\cap I_2$，$I_1\cdot I_2$，I_1+I_2都是R的理想，并且$I_1\cdot I_2\subseteq I_1\cap I_2$。

13. 证明$I=\left\{\begin{pmatrix}0 & 2x\\ 0 & 0\end{pmatrix}\middle| x\in\mathbb{Z}\right\}$是$R=\left\{\begin{pmatrix}a & b\\ 0 & c\end{pmatrix}\middle| a,b,c\in\mathbb{Z}\right\}$的理想。商环$R/I$是由哪些元素构成的?

14. 在高斯整数环$\mathbb{Z}[\mathrm{i}]=\{a+b\mathrm{i}|a,b\in\mathbb{Z}\}$中，$I=(2+\mathrm{i})$含有哪些元素?$\mathbb{Z}[\mathrm{i}]/(2+\mathrm{i})$含有哪些元素?

15. 令$R=\left\{\begin{pmatrix}a & b\\ c & d\end{pmatrix}\middle| a,b,c,d\in\mathbb{Z}\right\}$，$I=\left\{\begin{pmatrix}2m & 2n\\ 2k & 2l\end{pmatrix}\middle| m,n,k,l\in\mathbb{Z}\right\}$。

(1) 证明I是R的理想;

(2) R/I是由哪些元素组成的?

16. $\mathbb{Q}[x]$是有理数域$\mathbb{Q}$上的多项式环，证明$(2,x)$是$\mathbb{Q}[x]$的主理想。

17. $F[x]$是数域F上的多项式环。在$F[x]$上定义运算$f(x)\cdot g(x)=f(g(x))$。则$\langle F[x], +, \cdot\rangle$是否是环? 为什么?

18. $\langle\mathbb{Z}_7, +, \cdot\rangle$上的多项式$f(x)=-4+5x+3x^3$，$g(x)=3-x+4x^3$，试计算$f(x)+g(x)$，$f(x)\cdot g(x)$。

19. 域$\langle \mathbb{Z}_2, +, \bullet \rangle$上的多项式$1+x+x^2+\cdots+x^n$有因式$1+x$当且仅当$n$为奇数。

20. 找出从$\mathbb{Z}$到$\mathbb{Z}$的所有同态映射，并写出其同态核。

21. 找出从$\mathbb{Z}$到$\mathbb{Z}_2$的所有同态映射。

22. 证明：$(3)/(6)$是$\mathbb{Z}/(6)$的理想，并且

$$\frac{\mathbb{Z}/(6)}{(3)/(6)} \cong \mathbb{Z}/(3).$$

23. 给定正整数m和r，且$r|m$。用$\overline{a}$表示$\mathbb{Z}_m$中a所在的同余类，$[a]$表示$\mathbb{Z}_r$中a所在的同余类。令$f : \mathbb{Z}_m \to \mathbb{Z}_r$，$f(\overline{a}) = [a]$。

(1) 证明f是环同态映射；

(2) 求$\mathrm{Ker}f$，并找出与$\mathbb{Z}_m/\mathrm{Ker}f$同构的环。

24. 令$\varphi : \mathbb{R}[x] \to \mathbb{R}$，$\varphi(f(x)) = \varphi(a_0 + a_1x + \cdots + a_nx^n) = a_0$。

(1) 证明φ是从环$\mathbb{R}[x]$到环$\mathbb{R}$的满同态映射；

(2) 求$\mathrm{Ker}\varphi$，并找出与$\mathbb{R}[x]/\mathrm{Ker}\varphi$同构的环。

25. 若φ是从环R_1到环R_2的满同态映射，I_1是R_1的理想。证明：

(1) $\varphi^{-1}(\varphi(I)) = I + \mathrm{Ker}\varphi$；

(2) $\varphi(I) = R_2$ 当且仅当$I + \mathrm{Ker}\varphi = R_1$。

26. 整数环$\mathbb{Z}$中，(n)是$\mathbb{Z}$的素理想当且仅当$|n| = 0$或p，其中p是素数。

27. 证明：在环$\mathbb{Z}[x]$中，(x, n)是极大理想当且仅当n为素数。

第 8 章 格与布尔代数

8.1 格的定义与性质

定义 8.1. 在部分序集$\langle A, \preceq\rangle$中，如果对任意$a, b \in A$，$\{a, b\}$都有一个最大下界和最小上界，则称$\langle A, \preceq\rangle$是**格**。

通常$\{a, b\}$的最大下界称为a与b的积，记作$a * b$；$\{a, b\}$的最小上界称为a与b的和，记作$a \oplus b$。

A的任意子集，如果有最大下界和最小上界，则它们是唯一的。在定义8.1中可以看出$*$与$\oplus$是A上的二元运算。格$\langle A, \preceq\rangle$有时也表示为$\langle A, *, \oplus\rangle$。

不是所有的偏序集都是格。例如，图8.1中的每个偏序集都是格。

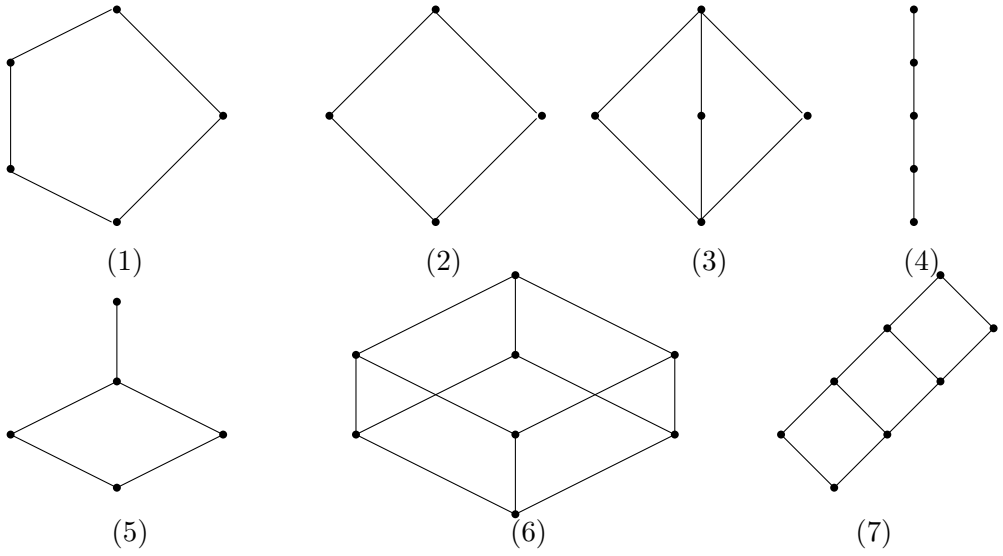


图 8.1: 格的示例

图8.2列出了五个偏序集，其中(1)中$\{x, y\}$没有上界和下界。(2)中$\{x, y\}$有最小上界，无下界。(3)中$\{x, y\}$无上界，有最大下界。(4)中$\{x, y\}$无上界，有下界但无最大下界。(5)中$\{x, y\}$有最小上界，有下界但无最大下界。所以从(1)到(5)都不是格。

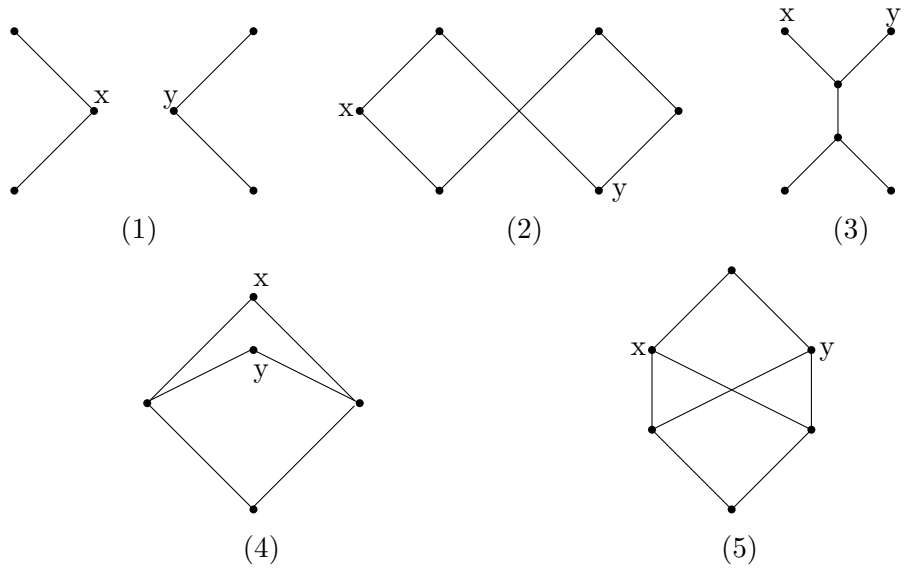


图 8.2: 不是格的偏序集示例

例 8.1. 设A是集合。$\langle \mathscr{P}(A), \subseteq \rangle$是格。格中的运算$*$和$\oplus$分别是$\cap$和$\cup$，原因如下。任取$A_1, A_2 \in \mathscr{P}(A)$。因为$A_1 \cap A_2 \subseteq A_1$，$A_1 \cap A_2 \subseteq A_2$，故$A_1 \cap A_2$是$\{A_1, A_2\}$的下界。设$C$是$\{A_1, A_2\}$ 的任意一个下界，即$C \subseteq A_1$，$C \subseteq A_2$，故$C \subseteq A_1 \cap A_2$。所以$A_1 \cap A_2$是$\{A_1, A_2\}$的最大下界，即$A_1 * A_2 = A_1 \cap A_2$。

因为$A_1 \subseteq A_1 \cup A_2$，$A_2 \subseteq A_1 \cup A_2$，故$A_1 \cup A_2$是$\{A_1, A_2\}$的上界。假设$B$是$\{A_1, A_2\}$的任意一个上界，即$A_1 \subseteq B$，$A_2 \subseteq B$，故$A_1 \cup A_2 \subseteq B$。所以$A_1 \cup A_2$是$\{A_1, A_2\}$的最小上界，即$A_1 \oplus A_2 = A_1 \cup A_2$。

特别地，当$|A| = 2$时，$\langle \mathscr{P}(A), \subseteq \rangle$的*Hasse*图是图*8.1(2)*；当$|A| = 3$时，$\langle \mathscr{P}(A), \subseteq \rangle$的*Hasse*图是图*8.1(6)*。

例 8.2. $\mathbb{Z}$是整数集合。$\langle \mathbb{Z}, | \rangle$是格。格中的运算$*$和$\oplus$分别是求两个整数的最大公约数和最小公倍数运算，原因如下。任取$a, b \in \mathbb{Z}$，a与b 的最大公约数(a, b)满足$(a, b)|a$, $(a, b)|b$，故(a, b)是$\{a, b\}$的下界。若c是$\{a, b\}$的一个下界，即$c|a$，$c|b$，故$c|(a, b)$。所以(a, b)是$\{a, b\}$的最大下界，即$a * b = (a, b)$。

a与b的最小公倍数$[a, b]$满足$a|[a, b]$, $b|[a, b]$，故$[a, b]$是$\{a, b\}$的上界。若c

是$\{a,b\}$的一个上界，即$a|c$，$b|c$，故$[a,b]|c$。所以$[a,b]$ 是$\{a,b\}$的最小上界，即$a \oplus b = [a,b]$。

特别地，图*8.1(2)*是格$\langle\{1,2,3,6\},|\rangle$的*Hasse*图；图*8.1(6)*是格$\langle\{1,2,3,5,6,10,15,30\},|\rangle$的*Hasse* 图；图*8.1(7)*是格$\langle\{1,2,3,4,6,8,12,24\},|\rangle$的*Hasse*图。

例 8.3. 设G是群，$L(G)=\{H|H$是G的子群$\}$，易见$\langle L(G),\subseteq\rangle$是偏序集。任取$A,B \in L(G)$，$A$与$B$均是$G$的子群，故$A\cap B$ 也是G的子群。与例*8.1*类似，$A\cap B$是$\{A,B\}$的最大下界，即$A*B=A\cap B$。

由于A与B都是G的子群，显然$A=\langle A\rangle \subseteq \langle A\cup B\rangle = \langle A,B\rangle$，$B=\langle B\rangle \subseteq \langle A\cup B\rangle = \langle A,B\rangle$。$\langle A,B\rangle$是由$A\cup B$生成的群，$\langle A,B\rangle \subseteq G$，所以$\langle A,B\rangle$是$G$的子群，即$\langle A,B\rangle \in L(G)$。从而$\langle A,B\rangle$是$\{A,B\}$的上界。假设$C$是$\{A,B\}$的任一上界，即$C$ 是G的子群，且$A\subseteq C$，$B\subseteq C$，那么，$A\cup B\subseteq C$。而$\langle A,B\rangle$是包含$A\cup B$的最小的群，因此$\langle A,B\rangle \subseteq C$。所以，$\langle A,B\rangle$是$\{A,B\}$的最小上界，即$A\oplus B=\langle A,B\rangle$。

综上可知$\langle L(G),\subseteq\rangle$是格，被称为子群格。

例 8.4. 设G是群，$N(G)=\{H|H\triangleleft G\}$，易见$\langle N(G),\subseteq\rangle$是偏序集。任取$A,B\in N(G)$，$A$与$B$均是$G$的正规子群，故$A\cap B$也是$G$ 的正规子群。与例*8.1*类似，$A\cap B$是$\{A,B\}$的最大下界，即$A*B=A\cap B$。

由于A与B都是G的正规子群，不难证明AB也是G的正规子群，并且$\langle A,B\rangle = AB$。与例*8.3*类似，$\langle A,B\rangle$是$\{A,B\}$ 的最小上界，即$A\oplus B = AB$。

综上可知$\langle N(G),\subseteq\rangle$是格，被称为正规子群格。

下面研究格的性质。

定理 8.1. 设$\langle A,\preceq\rangle$是格，集合A中的任意元素a,b,c满足：

(1) 幂等律：$a*a=a$，$a\oplus a=a$；

(2) 交换律：$a*b=b*a$，$a\oplus b=b\oplus a$；

(3) 结合律：$a*(b*c)=(a*b)*c$，$a\oplus(b\oplus c)=(a\oplus b)\oplus c$；

(4) 吸收律：$a*(a\oplus b)=a$，$a\oplus(a*b)=a$。

证明： 这里只证明(1)和(3)，(2)和(4)的证明方法类似，留作习题。

(1) $\langle A, \preceq\rangle$是格，$\preceq$是$A$上的偏序关系。由$\preceq$的自反性知，对任意$a \in A$均有$a \preceq a$，所以$a$是$\{a, a\}$的下界。设$x$是$\{a, a\}$ 的任一下界，即$x \preceq a$，所以a是$\{a, a\}$的最大下界，所以$a * a = a$。同理可证$a \oplus a = a$。

(3) 令$d = a * (b * c)$，$d' = (a * b) * c$。所以d是$\{a, b * c\}$的最大下界，故$d \preceq a$，$d \preceq b * c$。后者说明d是$\{b, c\}$的下界，故$d \preceq b$，$d \preceq c$。由$d \preceq a$和$d \preceq b$知，$d \preceq a * b$。再由$d \preceq a * b$和$d \preceq c$知，$d \preceq (a * b) * c = d'$。同理可证$d' \preceq d$。由偏序关系的反对称性可得$d = d'$，即$a*(b*c) = (a*b)*c$。

同理可证$a \oplus (b \oplus c) = (a \oplus b) \oplus c$。证毕。

定理 8.2. 设$\langle A, \preceq\rangle$是格。对于集合$A$中的任意元素$a, b$，以下三个命题是等价的：

(1) $a \preceq b$;

(2) $a * b = a$;

(3) $a \oplus b = b$。

证明： (1) $\Rightarrow$ (2) 已知$a \preceq b$，又由$\preceq$的自反性知$a \preceq a$，所以a是$\{a, b\}$的下界。而$a * b$是$\{a, b\}$的最大下界，所以$a \preceq a * b$。另一方面，由$a * b$ 的定义知$a * b \preceq a$。由偏序关系$\preceq$的反对称性知$a * b = a$。

(2) $\Rightarrow$ (3) 已知$a * b = a$。由定理8.1知，$b = b \oplus (b * a) = b \oplus (a * b) = b \oplus a = a \oplus b$，即$a \oplus b = b$。

(3) $\Rightarrow$ (1) 已知$a \oplus b = b$。由$a \oplus b$的定义知，b是$\{a, b\}$的最小上界，所以$a \preceq b$。

以上证明了三个命题的等价性。证毕。

定理 8.3. 设$\langle A, \preceq\rangle$是格。对于集合$A$中的任意元素$a, b, c$，如果$b \preceq c$，则$a * b \preceq a * c$，$a \oplus b \preceq a \oplus c$。这个性质称为保序性。

证明： 由定理8.2知$b \preceq c$等价于$b * c = b$。另外，格中$*$运算满足幂等律、结合律和交换律，故有

$$(a * b) * (a * c) = (a * a) * (b * c) = a * (b * c) = a * b.$$

由定理8.2知，$a * b \preceq a * c$。

同理可证$a \oplus b \preceq a \oplus c$。证毕。

定理 8.4. 设$\langle A, \preceq\rangle$是格。集合$A$中的任意元素$a, b, c$满足下面的分配不等式：

$$a \oplus (b * c) \preceq (a \oplus b) * (a \oplus c),$$
$$a * (b \oplus c) \succeq (a * b) \oplus (a * c).$$

证明： 由$\oplus$的定义知$a \preceq a \oplus b$，$a \preceq a \oplus c$。再由$*$的定义可得$a \preceq (a \oplus b) * (a \oplus c)$。又因为

$$b * c \preceq b \preceq a \oplus b,$$
$$b * c \preceq c \preceq a \oplus c,$$

和$*$的定义可得，$b * c \preceq (a \oplus b) * (a \oplus c)$。这说明$(a \oplus b) * (a \oplus c)$是$\{a, b * c\}$的上界，而$a \oplus (b * c)$是$\{a, b * c\}$的最小上界，因此

$$a \oplus (b * c) \preceq (a \oplus b) * (a \oplus c).$$

同理可证$a * (b \oplus c) \succeq (a * b) \oplus (a * c)$。证毕。

定理 8.5. 设$\langle A, \preceq\rangle$是格。对于集合$A$中的任意元素$a, b, c$，

$$a \preceq b \Leftrightarrow a \oplus (b * c) \preceq b * (a \oplus c).$$

证明： 已知$a \preceq b$。在定理8.4的第一个分配不等式$a \oplus (b * c) \preceq (a \oplus b) * (a \oplus c)$中代入与$a \preceq b$等价的$a \oplus b = b$，得到$a \oplus (b * c) \preceq b * (a \oplus c)$。

反之，已知$a \oplus (b * c) \preceq b * (a \oplus c)$，由

$$a \preceq a \oplus (b * c),$$

$$b * (a \oplus c) \preceq b,$$

以及偏序关系$\preceq$的传递性知$a \preceq b$。证毕。

定理 8.6. 设$\langle A, \preceq\rangle$是格。集合$A$的任意有限子集$S$均有最大下界和最小上界。

证明： 对A的有限子集S中的元素个数作归纳证明。

(1) 当$|S| = 2$时，因为$\langle A, \preceq\rangle$是格，所以任意二元子集$\{a, b\}$均有最大下界和最小上界，命题成立。

(2) 假设$|S| = n-1$时命题成立。当$|S| = n$时，不妨假设$S = \{a_1, a_2, \cdots, a_{n-1}, a_n\}$。令$S' = \{a_1, a_2, \cdots, a_{n-1}\}$，$|S'| = n-1$。由归纳假设，$S'$有最小上界$b'$。因为$\langle A, \preceq\rangle$是格，$\{b', a_n\}$有最小上界$b$，即$b' \preceq b$，$a_n \preceq b$。而$a_i \preceq b'$，$i = 1, 2, \cdots, n-1$，所以$b$是$S$的上界。若$c$也是$S$的上界，$a_i \preceq c$，$1 \le i \le n$，所以$c$也是$S'$的上界；而$b'$是$S'$的最小上界，故$b' \preceq c$。又$a_n \preceq c$，$b$是$\{b', a_n\}$的最小上界，故$b \preceq c$，即$b$是$S$的最小上界。

同理可证S有最大下界。证毕。

定理8.6的证明实际上给出了一种求集合A的有限子集最大下界和最小上界的方法。这种证明叫做构造性证明。

设$\langle A, \preceq\rangle$是偏序集。在集合$A$上定一个新的关系$\preceq_1$，对于$a, b \in A$，

$$a \preceq_1 b \Leftrightarrow b \preceq a.$$

显然，$\langle A, \preceq_1\rangle$也是偏序集。$\langle A, \preceq_1\rangle$的Hasse图恰好是把$\langle A, \preceq\rangle$的Hasse图上下颠倒过来。$A$的二元子集$\{a, b\}$在$\langle A, \preceq_1\rangle$中的最大下界和最小上界分别是它在$\langle A, \preceq\rangle$中的最小上界和最大下界。如果$\langle A, \preceq\rangle$是格，那么$\langle A, \preceq_1\rangle$也是格。前者的二元运算分别记为$*$和$\oplus$，后者的二元运算分别记为$*'$和$\oplus'$。在$\langle A, \preceq\rangle$中的命题

$$a \preceq b \Leftrightarrow a \oplus b = b,$$

在$\langle A, \preceq_1\rangle$中表示成

$$a \preceq_1 b \Leftrightarrow a \oplus' b = b.$$

把它翻译成$\langle A, \preceq\rangle$中的语言，则是

$$a \succeq b \Leftrightarrow a * b = b.$$

从这个例子，可以看出如下的对偶原理：一个在所有格中都成立的命题，将其中的$\succeq, \preceq, *, \oplus$分别换成$\preceq, \succeq, \oplus, *$，则得到该命题的对偶命题，对偶命题在所有格中也都成立。例如，分配不等式$a \oplus (b * c) \preceq (a \oplus b) * (a \oplus c)$的对偶命题是分配不等式$a * (b \oplus c) \succeq (a * b) \oplus (a * c)$，两者同时成立。

8.2 几种特殊的格

8.2.1 完全格和有界格

定义 8.2. 如果在格$\langle A, \preceq\rangle$中，对于集合$A$的任意子集都有最大下界和最小上界，则称该格是**完全格**。

显然，当A是有限集合时，定理8.6保证了格$\langle A, \preceq\rangle$时完全格。

定义 8.3. 在格$\langle A, \preceq\rangle$中，若存在最大元和最小元，分别记为1和0，即$A$中的任意元素$a$都满足$0 \preceq a \preceq 1$，则称该格是**有界格**，记为$\langle A, \preceq, 0, 1\rangle$。

显然，完全格必是有界格。

在有界格$\langle A, \preceq, 0, 1\rangle$中，对于$A$的任意元素$a$，

$$a \oplus 0 = a, \qquad a * 0 = 0,$$
$$a \oplus 1 = 1, \qquad a * 1 = a.$$

在有界格中，可以引进元素补元的概念。

定义 8.4. 在有界格$\langle A, \preceq, 0, 1\rangle$中，对于$A$中的元素$a, b$，如果$a * b = 0$，$a \oplus b = 1$，则称$a$是$b$的**补元** *($b$也是$a$的补元)*。

一般地，在有界格中，一个元素可能没有补元，也可能有多个补元。例如图8.3中，左图里的a_1, a_2, a_3都没有补元；右图里的a_1, a_2, a_3互为补元，a_1有两个补元a_2, a_3。

在有界格中，最大元1是最小元0的唯一补元，最小元0是最大元1的唯一补元。这是因为1是有界格$\langle A, \preceq, 0, 1\rangle$的最大元，对于$A$中的任意元素$a$，$a \oplus 1 = 1$，$a * 1 = a$。特别地，取$a = 0$，$0 \oplus 1 = 1$，$0 * 1 = 0$，所以0与1互为补元。又若$b \in A$也是0的补元，即$0 \oplus b = 1$；而0是最小元，故有$0 \preceq b$，$0 \oplus b = b$。因此$b = 1$，所以1是0的唯一补元。

8.2.2 有补格

定义 8.5. 在有界格$\langle A, \preceq, 0, 1\rangle$中，如果$A$中每个元素都至少有一个补元，则称该格是**有补格**。

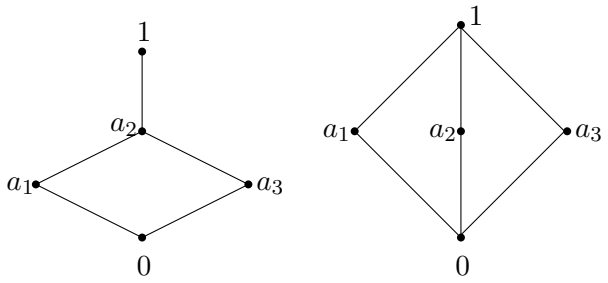


图 8.3: 有界格示例

例 8.5. 令$L = \{0, 1\}$。在集合L^3上定义关系$\preceq_3$，对任意$a_1, a_2, a_3, b_1, b_2, b_3 \in L$，

$$(a_1, a_2, a_3) \preceq_3 (b_1, b_2, b_3) \Leftrightarrow a_1 \preceq b_1, a_2 \preceq b_2, a_3 \preceq b_3.$$

$\langle L^3, \preceq_3\rangle$是有序数组格，其最小元和最大元分别为$(0, 0, 0)$和$(1, 1, 1)$。$L^3$中元素$(a_1, a_2, a_3)$的补元为$(b_1, b_2, b_3)$，其中

$$b_i = \begin{cases} 1 & a_i = 0, \\ 0 & a_i = 1, \end{cases} \quad 1 \le i \le 3.$$

因此，$\langle L^3, \preceq_3\rangle$是有补格，它的*Hasse*图如图*8.4*所示。

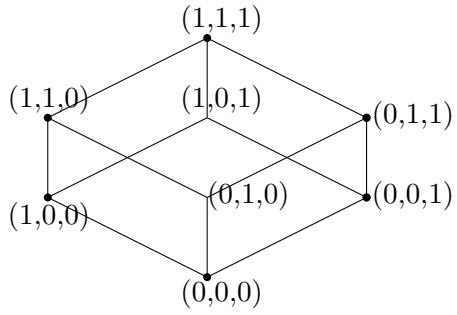


图 8.4: 有序数组格$\langle L^3, \preceq_3\rangle$

例 8.6. 设A是集合，$\langle \mathscr{P}(A), \subseteq\rangle$是有界格，其最小元和最大元分别是$\emptyset$和$A$，$\mathscr{P}(A)$的任意元素$B$的补元是$A-B$。所以$\langle \mathscr{P}(A), \subseteq\rangle$是有补格。

8.2.3 分配格

定义 8.6. 在格$\langle A, \preceq\rangle$中，如果$A$中任意元素$a, b, c$有

$$a * (b \oplus c) = (a * b) \oplus (a * c),$$
$$a \oplus (b * c) = (a \oplus b) * (a \oplus c),$$

则称$\langle A, \preceq\rangle$是**分配格**。

例 8.7. 设A是集合，$\langle \mathscr{P}(A), \subseteq\rangle$的二元运算$*$和$\oplus$分别是集合的交$\cap$和并$\cup$运算。集合的交和并运算满足分配律，故$\langle \mathscr{P}(A), \subseteq\rangle$是分配格。

例 8.8. $\mathbb{Z}^+$是正整数集合，$\langle \mathbb{Z}^+, |\rangle$的二元运算$*$和$\oplus$分别是求最大公因子和最小公倍数运算，它们满足分配律，故$\langle \mathbb{Z}^+, |\rangle$是分配格。

例 8.9. 图*8.5*中，左图是有补格，但不是分配格。这是因为

$$a_1 * (a_2 \oplus a_3) = a_1 * 1 = a_1,$$
$$(a_1 * a_2) \oplus (a_1 * a_3) = 0 \oplus 0 = 0,$$

不满足分配律等式$a_1 * (a_2 \oplus a_3) = (a_1 * a_2) \oplus (a_1 * a_3)$。

图*8.5*的右图是有界分配格，但不是有补格，因为a_1没有补元。

所以，有补格不一定是分配格，分配格也不一定是有补格。

定理 8.7. 任意线性序集都是分配格。

证明： 设$\langle A, \preceq\rangle$是线性序集，$A$中的任意两个元素$a, b$，或者$a \preceq b$，或者$b \preceq a$。故

$$a * b = \begin{cases} a & \text{如果} a \preceq b, \\ b & \text{如果} b \preceq a; \end{cases} \qquad a \oplus b = \begin{cases} b & \text{如果} a \preceq b, \\ a & \text{如果} b \preceq a. \end{cases}$$

因此，$\langle A, \preceq\rangle$是格。

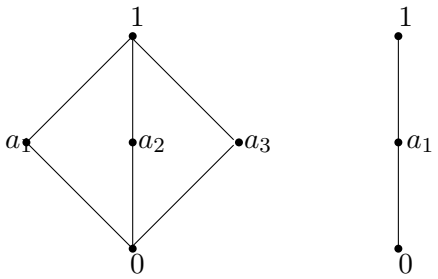


图 8.5: 有补格与分配格示例

对于A的任意元素a, b, c，它们之间的关系可能有以下两种情况:

(1) $a \succeq b$且$a \succeq c$。即a是$\{b, c\}$的上界，所以$b \oplus c \preceq a$。于是，$a*(b \oplus c) = b \oplus c$。又由$a \succeq b$和$a \succeq c$知，$a * b = b$，$a * c = c$，所以$(a * b) \oplus (a * c) = b \oplus c$。因此，$a * (b \oplus c) = (a * b) \oplus (a * c)$。

(2) $a \preceq b$或$a \preceq c$。即a是$\{b, c\}$的下界，所以$a \preceq b * c \preceq b \oplus c$。于是，$a * (b \oplus c) = a$。又由$a \preceq b$和$a \preceq c$知，$a * b = a$，$a * c = a$，所以$(a * b) \oplus (a * c) = a$。因此，$a * (b \oplus c) = (a * b) \oplus (a * c)$。

同理可证$a \oplus (b * c) = (a \oplus b) * (a \oplus c)$。证毕。

定理 8.8. 设$\langle A, \preceq \rangle$是分配格。对于$A$的任意元素$a, b, c$，如果$a * c = b * c$，$a \oplus c = b \oplus c$，则$a = b$。

证明: $\langle A, \preceq \rangle$是分配格。根据$*$和$\oplus$运算的吸收律，分配律和交换律，有

$$\begin{aligned} a &= a * (a \oplus c) = a * (b \oplus c) = (a * b) \oplus (a * c) \\ &= (a * b) \oplus (b * c) = b * (a \oplus c) = b * (b \oplus c) = b. \end{aligned}$$

所以$a = b$。证毕。

推论 8.1. 在有界分配格$\langle A, \preceq, 0, 1 \rangle$中，如果$A$的元素$a$有补元，则它的补元是唯一的。

证明: 假设a'和a''都是元素a的补元，则

$$a \oplus a' = 1, \qquad a * a' = 0,$$
$$a \oplus a'' = 1, \qquad a * a'' = 0.$$

所以，$a \oplus a' = a \oplus a''$，$a * a' = a * a''$。由定理8.8知，$a' = a''$，即$a$的补元是唯一的。证毕。

定理 8.9.（**摩根律**）设$\langle A, \preceq \rangle$是有界分配格，若集合$A$中的元素$a, b$的补元分别为$a', b'$，则

$$(a * b)' = a' \oplus b',$$
$$(a \oplus b)' = a' * b'.$$

证明： 因为

$$(a * b) \oplus (a' \oplus b') = ((a * b) \oplus a') \oplus b' = (a' \oplus b) \oplus b' = 1,$$
$$(a * b) * (a' \oplus b') = a * (b * (a' \oplus b') = a * (b * a') = 0.$$

所以$a' \oplus b'$是$a * b$的补元，再由推论8.1知$a * b$的补元是唯一的，故$(a * b)' = a' \oplus b'$。同理可证，$(a \oplus b)' = a' * b'$。证毕。

定义 8.7. 有补分配格称为**布尔格**。

8.2.4 模格

定义 8.8. 在格$\langle A, \preceq \rangle$中，对于$A$的任意元素$a, b, c$，如果$a \preceq b$均使$a \oplus (b * c) = b * (a \oplus c)$，则称$\langle A, \preceq \rangle$是**模格**。

特别地，在分配格$\langle A, \preceq \rangle$中，若$a \preceq b$，则$a \oplus b = b$，故有

$$a \oplus (b * c) = (a \oplus b) * (a \oplus c) = b * (a \oplus c).$$

所以每个分配格都是模格。

定理 8.10. $\langle A, \preceq \rangle$是模格的充要条件是对于$A$的任意元素$a, b, c$，如果$a \preceq b$且$a * c = b * c$，$a \oplus c = b \oplus c$，则必有$a = b$。

证明： 已知$\langle A, \preceq \rangle$是模格，对于$A$的任意元素$a, b, c$，如果$a \preceq b$且$a * c = b * c$，$a \oplus c = b \oplus c$，那么必有

$$a = a \oplus (a * c) = a \oplus (b * c) = b * (a \oplus c) = b * (b \oplus c) = b.$$

反之，令$x = a \oplus (b * c)$，$y = b * (a \oplus c)$。因为$a \preceq b$，由定理8.5知，$x \preceq y$。下面证明$x \oplus c = y \oplus c$，$x * c = y * c$。

$$x \oplus c = (a \oplus (b * c)) \oplus c = a \oplus ((b * c) \oplus c) = a \oplus c,$$
$$y \oplus c = (b * (a \oplus c)) \oplus c.$$

由于$a \preceq b$和$a \preceq a \oplus c$，所以$a \preceq b * (a \oplus c) \preceq a \oplus c$，从而有

$$a \oplus c \preceq (b * (a \oplus c)) \oplus c \preceq (a \oplus c) \oplus c,$$

即

$$a \oplus c \preceq y \oplus c \preceq a \oplus c.$$

由偏序关系$\preceq$的反对称性知，$y \oplus c = a \oplus c$，因此$x \oplus c = y \oplus c$。

我们已经证明了在格中，当$a \preceq b$时，

$$(a \oplus (b * c)) \oplus c = (b * (a \oplus c)) \oplus c.$$

它的对偶命题是：当$a \succeq b$时，

$$(a * (b \oplus c)) * c = (b \oplus (a * c)) * c.$$

把后者的a与b互换位置，即得，当$b \succeq a$时，

$$(b * (a \oplus c)) * c = (a \oplus (b * c)) * c.$$

这就是说，当$a \preceq b$，$x * c = y * c$。

现在有了$x \preceq y$，$x \oplus c = y \oplus c$，$x * c = y * c$，由已知条件知$x = y$。也就是说，当$a \preceq b$时，$a \oplus (b * c) = b * (a \oplus c)$，所以$\langle A, \preceq \rangle$ 是模格。证毕。

8.3 格——代数系统

集合以及集合上的一个或多个运算所组成的系统叫做代数系统，前几章介绍了群、环、域等代数系统，本章介绍的格是与它们不同的一个新的代数系统。

8.3.1 基本定义

定义 8.9. $*$和$\oplus$是集合A上的两个二元运算。如果集合A的任意元素a,b,c满足下述条件，则称代数系统$\langle A,*,\oplus\rangle$是**格**：

(1) 结合律：$a*(b*c)=(a*b)*c$，$a\oplus(b\oplus c)=(a\oplus b)\oplus c$；

(2) 交换律：$a*b=b*a$，$a\oplus b=b\oplus a$；

(3) 吸收律：$a*(a\oplus b)=a$，$a\oplus(a*b)=a$。

定理 8.11. 定义*8.1*和定义*8.9*中定义的格是等价的。

证明： 设$\langle A,\preceq\rangle$是定义8.1中定义的格，即对集合A中的任意二元子集$\{a,b\}$有唯一的最大下界和最小上界，分别记作$a*b$和$a\oplus b$。$*$和$\oplus$是A上的两个二元运算。定理8.1证明了这两个运算满足结合律、交换律和吸收律，所以$\langle A,*,\oplus\rangle$也是定义8.9中定义的格。

若$\langle A,*,\oplus\rangle$是定义8.9中定义的格，我们在集合$A$上定义关系$\preceq$:

$$a\preceq b\Leftrightarrow a*b=a.$$

当$a*b=a$时，$a\oplus b=(a*b)\oplus b=b$(根据定义8.9中的吸收律)，当$a\oplus b=b$时，$a*b=a*(a\oplus b)=a$。故$a*b=a\Leftrightarrow a\oplus b=b$，因此有

$$a\preceq b\Leftrightarrow a*b=a\Leftrightarrow a\oplus b=b.$$

易证如此定义的关系$\preceq$是集合A上的偏序关系。

任取A中的元素a,b，由$a*(a\oplus b)=a$和$b*(a\oplus b)=b$知，$a\preceq a\oplus b$，$b\preceq a\oplus b$。因此，$a\oplus b$是$\{a,b\}$的上界。如果A 中的元素c 也是$\{a,b\}$的上界，即$a\preceq c$，$b\preceq c$，那么$a\oplus c=c$，$b\oplus c=c$。

$$(a\oplus b)\oplus c=(a\oplus c)\oplus(b\oplus c)=c\oplus c=c.$$

这意味着$a\oplus b\preceq c$，从而$a\oplus b$是$\{a,b\}$的最小上界。同理可证，$a*b$是$\{a,b\}$的最大下界。因此，$\langle A,\preceq\rangle$是定义8.1中定义的格。综上所述，定义8.1和定义8.9是等价的。证毕。

8.3.2 子格和格的直积

定义 8.10. 设$\langle A, *, \oplus\rangle$是格，$B$是$A$的非空子集。如果集合$B$对$*$和$\oplus$运算是封闭的，则称$\langle B, *, \oplus\rangle$是$\langle A, *, \oplus\rangle$ 的**子格**。

易证，子格本身也是格。

例 8.10. 设$\mathbb{Z}^+$是正整数集合。在$\mathbb{Z}^+$上定义二元运算：

$$a * b = (a, b) \qquad a \oplus b = [a, b].$$

$\langle \mathbb{Z}^+, *, \oplus\rangle$是格。令$T$是正偶数集合。两个偶数的最大公因子仍是偶数，两个偶数的最小公倍数也是偶数，所以$\langle T, *, \oplus\rangle$ 是$\langle \mathbb{Z}^+, *, \oplus\rangle$的子格。

例 8.11. 设$\langle A, *, \oplus\rangle$是格。对$A$中的两个元素$a, b$，$a \preceq b$。令

$$I[b, a] = \{x | x \in A, a \preceq x \preceq b\}.$$

任取$x_1, x_2 \in I[b, a]$，即$a \preceq x_1, x_2 \preceq b$，故有

$$a * x_i = a, \qquad x_i * b = x_i,$$
$$a \oplus x_i = x_i, \qquad x_i \oplus b = b,\ 1 \le i \le 2.$$

所以，

$$a * (x_1 * x_2) = (a * x_1) * x_2 = a * x_2 = a,$$
$$(x_1 * x_2) * b = x_1 * (x_2 * b) = x_1 * x_2,$$

即$a \preceq x_1 * x_2 \preceq b$，因此$x_1 * x_2 \in I[b, a]$。

同理可证$a \preceq x_1 \oplus x_2 \preceq b$，因此$x_1 \oplus x_2 \in I[b, a]$。所以，$\langle I[b, a], *, \oplus\rangle$是$\langle A, *, \oplus\rangle$的子格。

例 8.12. $\langle \mathscr{P}(\{1, 2, 3\}), \cap, \cup\rangle$是格。令

$$A_1 = \{\{2\}, \{1, 2\}, \{2, 3\}, \{1, 2, 3\}\},$$
$$A_2 = \{\emptyset, \{1\}, \{3\}, \{1, 3\}\},$$
$$A_3 = \{\emptyset, \{1, 2\}, \{2, 3\}, \{1, 2, 3\}\},$$

$\langle A_1, \cap, \cup\rangle$和$\langle A_2, \cap, \cup\rangle$是$\langle \mathscr{P}(\{1, 2, 3\}), \cap, \cup\rangle$的子格。而$A_3$中$\{1, 2\} \cap \{2, 3\} = \{2\} \notin A_3$，所以$A_3$不是$\mathscr{P}(\{1, 2, 3\})$的子格。由此可见，并非$A$的每个子集都是$\langle A, *, \oplus\rangle$的子格。

定义 8.11. 设$\langle A_1, *, \oplus\rangle$和$\langle A_2, \wedge, \vee\rangle$是两个格。构造一个新的代数系统$\langle A_1 \times A_2, \bullet, +\rangle$，其中$\bullet$和$+$运算的定义是：$(a_1, a_2), (b_1, b_2) \in A_1 \times A_2$，

$$(a_1, a_2) \bullet (b_1, b_2) = (a_1 * b_1, a_2 \wedge b_2),$$
$$(a_1, a_2) + (b_1, b_2) = (a_1 \oplus b_1, a_2 \vee b_2).$$

称$\langle A_1 \times A_2, \bullet, +\rangle$是$\langle A_1, *, \oplus\rangle$和$\langle A_2, \wedge, \vee\rangle$的**直积**。

在此定义中，$A_1 \times A_2$中的$\bullet$和$+$运算是由第一分量按A_1中的$*$和$\oplus$运算，第二分量按A_2中的$\wedge$和$\vee$运算来实现的。$\langle A_1, *, \oplus\rangle$和$\langle A_2, \wedge, \vee\rangle$是格，所以$A_1 \times A_2$中的$\bullet$和$+$运算也满足结合律、交换律和吸收律。因此两个格的直积也是格，并且是用小规模的格构造成的大规模格。

例 8.13. 设$A = \{0, 1\}$。在A上定义关系$\preceq_1$，$a, b \in A$，

$$a \preceq_1 b \Leftrightarrow a \preceq b.$$

$\langle A, \preceq_1\rangle$是格。在$A^2$上定义关系$\preceq_2$，$(a, b), (c, d) \in A^2$，

$$(a, b) \preceq_2 (c, d) \Leftrightarrow a \preceq_1 c, b \preceq_1 d.$$

$\langle A^2, \preceq_2\rangle$是两个格$\langle A, \preceq_1\rangle$与$\langle A, \preceq_1\rangle$的直积。类似地在$A^3$上定义关系$\preceq_3$，$(a, b, c), (d, e, f) \in A^3$，

$$(a, b, c) \preceq_3 (d, e, f) \Leftrightarrow a \preceq_1 d, b \preceq_1 e, c \preceq_1 f.$$

$\langle A^3, \preceq_2\rangle$是两个格$\langle A, \preceq_1\rangle$与$\langle A^2, \preceq_2\rangle$ 的直积。它们的*Hasse*图如图*8.6*所示。

8.3.3 格的同态与同构

定义 8.12. 设$\langle A_1, *, \oplus\rangle$和$\langle A_2, \wedge, \vee\rangle$是两个格。如果存在从$A_1$到$A_2$的映射$f : A_1 \to A_2$，对于$A_1$中的任意元素$a, b$，

$$f(a * b) = f(a) \wedge f(b),$$
$$f(a \oplus b) = f(a) \vee f(b),$$

则称f是从A_1到A_2的**格同态映射**。

若f是从A_1到A_2的格同态映射，并且为双射，则称f是从A_1到A_2的格同构映射。如果两个格之间存在格同构映射，则称这两个格是同构的。

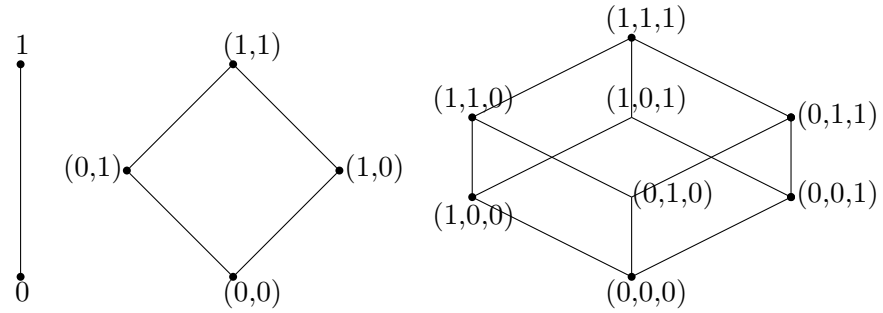


图 8.6: 格的直积示例

设f是从$\langle A_1, *, \oplus\rangle$到$\langle A_2, \wedge, \vee\rangle$的格同态映射，对于$a, b \in A_1$，$a \preceq_1 b$，由于$a \preceq_1 b \Leftrightarrow a * b = a$，故

$$f(a) = f(a * b) = f(a) \wedge f(b).$$

所以$f(a) \preceq_2 f(b)$，即格的同态映射是一种保序映射。反之则不一定成立。例如，令$A_1 = A_2 = \{1, 2, 3, 4, 6, 12\}$，$\langle A_1, |\rangle$和$\langle A_2, \preceq\rangle$是格，它们的Hasse图如图8.7所示。令$f : A_1 \to A_2$，$f(x) = x$是保序映射，但不是格同态映射。这是因为

$$f(3 * 4) = f(1) = 1,$$
$$f(3) \wedge f(4) = 3 \wedge 4 = 3,$$

即$f(3 * 4) \neq f(3) \wedge f(4)$。

定理 8.12. f是从集合A_1到集合A_2的双射。f是从格$\langle A_1, \preceq_1\rangle$到格$\langle A_2, \preceq_2\rangle$的同构映射当且仅当对于$A_1$的元素$a, b$,

$$a \preceq_1 b \Leftrightarrow f(a) \preceq_2 f(b).$$

证明： 已知f是从$\langle A_1, \preceq_1\rangle$到$\langle A_2, \preceq_2\rangle$的格同构映射。在格$\langle A_1, \preceq_1\rangle$中，对$a, b \in A_1$，$a \preceq_1 b \Leftrightarrow a * b = a$。

当$a * b = a$时，$f(a * b) = f(a) \cdot f(b) = f(a)$，故$f(a) \preceq_2 f(b)$。而当$f(a) \preceq_2 f(b)$ 时，$f(a) = f(a) \cdot f(b) = f(a * b)$。因为$f$是单射，所以$a =$

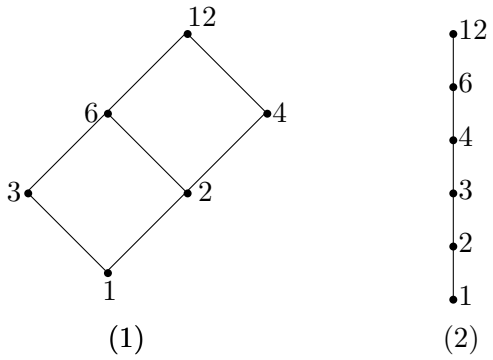


图 8.7: $\{1,2,3,4,6,12\}$上的两个格

$a*b$。从而

$$a*b=a \Leftrightarrow f(a) \preceq_2 f(b).$$

故，$a \preceq_1 b \Leftrightarrow f(a) \preceq_2 f(b)$。

反之，已知$f: A_1 \to A_2$是双射。任取$a,b \in A_1$，$a*b \preceq_1 a$，$a*b \preceq_1 b$。由f的保序性可得，$f(a*b) \preceq_2 f(a)$，$f(a*b) \preceq_2 f(b)$。从而$f(a*b) \preceq_2 f(a)\cdot f(b)$。任取$x,y \in A_2$，由于$f$是满射，存在$a,b \in A_1$，使得$f(a)=x$，$f(b)=y$。$A_2$是格，$x\cdot y = f(a)\cdot f(b) \in A_2$，因此存在$c \in A_1$使$f(c) = x\cdot y = f(a)\cdot f(b)$。于是有$f(c) \preceq_2 f(a)$，$f(c) \preceq_2 f(b)$，由于$f$是保序的，所以$c \preceq_1 a$，$c \preceq_1 b$，从而$c \preceq_1 a*b$。再由$f$的保序性可得$f(a)\cdot f(b) = f(c) \preceq_2 f(a*b)$。综上可得，$f(a)\cdot f(b) = f(a*b)$。同理可证$f(a)+f(b) = f(a\oplus b)$。所以$f$是格同构映射。证毕。

引理 8.1. 格$\langle A,*,\oplus\rangle$是模格当且仅当$A$的每个$I[b,a]=\{x|x\in A, a \preceq x \preceq b\}$中，如果有两个元素可比较且有公共补元，那么这两个元素必相等。

证明： 如果在格$\langle A,*,\oplus\rangle$中，$u \preceq v$，$I[v,u]$中有两个可比较但不相等的元素$a_0,b_0$，不妨假设$a_0 \prec b_0$，它们有一个公共补元$c$，即

$$a_0 * c = b_0 * c = u,$$

$$a_0 \oplus c = b_0 \oplus c = v,$$

那么

$$a_0 \oplus (b_0 * c) = a_0 \oplus u = a_0 \prec b_0 = b_0 * v = b_0 * (a_0 \oplus c),$$

也就是说$a_0 \prec b_0$，但是$a_0 \oplus (b_0 * c) \neq b_0 * (a_0 \oplus c)$，所以$\langle A, *, \oplus \rangle$不是模格。这意味着，如果格$\langle A, *, \oplus \rangle$ 是模格，则A的每个$I[b, a]$中，若有两个元素可比较并且有公共补元，则这两个元素必相等。

如果格$\langle A, *, \oplus \rangle$不是模格，那么必存在$a_0, b_0 \in A$，且$a_0 \prec b_0$，使得$a_0 \oplus (b_0 * c) \prec b_0 * (a_0 \oplus c)$。令$x = a_0 \oplus (b_0 * c)$，$y = b_0 * (a_0 \oplus c)$，显然$a_0 \preceq x, y \preceq b_0$，$b_0 * c \preceq x \prec y \preceq a_0 \oplus c$，$b_0 * c \preceq c \preceq a_0 \oplus c$，

$$c * y = c * (b_0 * (a_0 \oplus c)) = c * b_0.$$

由于$y \preceq a_0 \oplus c$，$a_0 \prec y$，

$$c \oplus y \preceq c \oplus (a_0 \oplus c) = a_0 \oplus c \preceq y_0 \oplus c,$$

得到

$$c \oplus y = a_0 \oplus c.$$

同理可证$x * c = b_0 * c$，$x \oplus c = a_0 \oplus c$。这说明在$I[a_0 \oplus c, b_0 * c]$中$x \prec y$，$x$与$y$有公共补元$c$，与题设矛盾，所以假设不成立，即$\langle A, *, \oplus \rangle$是模格。证毕。

利用引理8.1可以证明下面的定理。

定理 8.13. 格是模格当且仅当它不包含一个与图*8.8(1)*同构的五元子格。

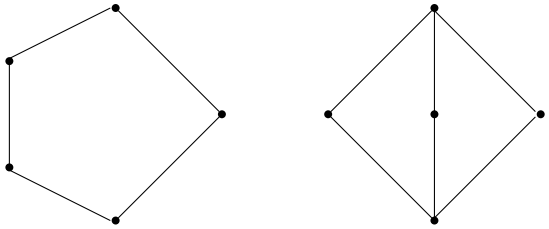
与此定理类似的还有如下定理，其证明略去。

定理 8.14. 格是分配格当且仅当它是模格且不包含一个与图*8.8(2)*同构的五元子格。

8.4 布尔代数

8.4.1 布尔代数

在格中可以定义两个$*$和$\oplus$二元运算。在有补分配格中，每个元素有补元且补元唯一，这样就可以在有补分配格中定义求补元的运算。另外，有补



(1) (2)

图 8.8: 两个五阶格

分配格有最大元1和最小元0。所以布尔格可以看作代数系统$\langle A, *, \oplus, ', 0, 1\rangle$，并称为由布尔格$\langle A, \preceq\rangle$ 诱导出来的代数系统。

定义 8.13. 设A是至少有两个元素的集合，$*$和$\oplus$是集合A上的二元运算。如果集合A的任意元素a, b, c满足下述条件：

(1) $a * b = b * a$，$a \oplus b = b \oplus a$；

(2) $a * (b \oplus c) = (a * b) \oplus (a * c)$，$a \oplus (b * c) = (a \oplus b) * (a \oplus c)$；

(3) $0, 1 \in A$，对A中任意元素a，$a * 1 = a$，$a \oplus 0 = a$；

(4) 对A中任意元素a，存在$a' \in A$，使得$a * a' = 0$，$a * a' = 1$。

则称$\langle A, *, \oplus, ', 0, 1\rangle$为**布尔代数**。

显然，由布尔格诱导出来的代数系统为布尔代数。

定理 8.15. 与布尔代数$\langle A, *, \oplus, ', 0, 1\rangle$相应的$\langle A, *, \oplus\rangle$是布尔格。

证明： 由布尔代数定义可看出，要证明$\langle A, *, \oplus\rangle$是布尔格，只需证明$\langle A, *, \oplus\rangle$是格，并且0和1分别是该格的最小元和最大元。

已知$\langle A, *, \oplus, ', 0, 1\rangle$是布尔代数，在代数系统$\langle A, *, \oplus\rangle$中，二元运算$*$和$\oplus$满足交换律。任取$a, b \in A$，

$$\begin{aligned} a * (a \oplus b) &= (a \oplus 0) * (a \oplus b) = a \oplus (0 * b) = a \oplus ((0 * b) \oplus (b' * b)) \\ &= a \oplus ((0 \oplus b') * b)) = a \oplus (b' * b) = a \oplus 0 = a. \end{aligned}$$

同理可证$a \oplus (a * b) = a$。所以二元运算$*$和$\oplus$满足吸收律。

令$x = a * (b * c)$，$y = (a * b) * c$，显然

$$x = x \oplus 0 = x \oplus (a * a') = (x \oplus a) * (x \oplus a'),$$
$$y = y \oplus 0 = y \oplus (a * a') = (y \oplus a) * (y \oplus a'),$$

其中

$$x \oplus a = (a * (b * c)) \oplus a = a,$$
$$y \oplus a = ((a * b) * c) \oplus a = ((a * b) \oplus a) * (c \oplus a) = a * (a \oplus c) = a,$$
$$x \oplus a' = (a * (b * c)) \oplus a' = (b * c) \oplus a',$$
$$y \oplus a' = ((a * b) * c) \oplus a' = ((a * b) \oplus a') * (c \oplus a') = (b \oplus a') * (c \oplus a') = (b * c) \oplus a'.$$

于是，由$x \oplus a = y \oplus a$和$x \oplus a' = y \oplus a'$推出$x = y$，即

$$a * (b * c) = (a * b) * c.$$

同理可证，$a \oplus (b \oplus c) = (a \oplus b) \oplus c$。所以二元运算$*$和$\oplus$满足结合律。从而$\langle A, *, \oplus\rangle$是格。

在布尔代数$\langle A, *, \oplus, ', 0, 1\rangle$中，对任意元素$a \in A$均有

$$a * 1 = a, \qquad a \oplus 0 = a.$$

在$\langle A, *, \oplus\rangle$中的偏序关系是，对$a, b \in A$，

$$a \preceq b \Leftrightarrow a \oplus b = b \Leftrightarrow a * b = a.$$

于是在格$\langle A, *, \oplus\rangle$中，$0 \preceq a \preceq 1$，即0和1分别是该格的最小元和最大元。

综上分析知，$\langle A, *, \oplus\rangle$是布尔格。证毕。

从这个定理可以看出在有补分配格中，存在最小元和最大元，每个元素有补元，二元运算满足交换律和结合律是其最核心的性质。

8.4.2 布尔代数的子代数

定义 8.14. 设A_1是布尔代数$\langle A, *, \oplus, ', 0, 1\rangle$中集合$A$的子集。如果$0, 1 \in A_1$，并且$A_1$对于$*, \oplus, '$运算是封闭的，那么称$\langle A_1, *, \oplus, ', 0, 1\rangle$是$\langle A, *, \oplus, ', 0, 1\rangle$的**子代数**。

例 8.14. $A=\{1,2,3\}$，$\langle \mathscr{P}(A),\subseteq\rangle$是有补分配格，其上的$*,\oplus,'$运算分别为$\cap,\cup,^-$运算，最小元和最大元分别为$\emptyset$和$A$，故$\langle \mathscr{P}(A),\cap,\cup,^-,\emptyset,A\rangle$是布尔代数。令$A_1=\{\emptyset,\{1\},\{2,3\},A\}$，则$A_1$是$A$的子代数。

例 8.15. $\langle A,*,\oplus,',0,1\rangle$是布尔代数。$a,b\in A$且$a\preceq b$，定义$A$的子集$I[b,a]=\{x|x\in A,a\preceq x\preceq b\}$。易证，$I[b,a]$ 对运算$*$和$\oplus$是封闭的。由于$\langle A,*,\oplus\rangle$是分配格，所以$\langle I[b,a],*,\oplus\rangle$也是分配格。但是$I[b,a]$的最大元是$b$，最小元是$a$，与布尔代数$A$的最大元和最小元不同。另外，$I[b,a]$对求补元运算不一定封闭，所以$I[b,a]$不是$A$的子代数。

对$I[b,a]$中的任意元素x，定义$\overline{x}=(a\oplus x')*b$。显然$\overline{x}\preceq b$。

$$\overline{x}*a=(a\oplus x')*b*a=a,$$

故$a\preceq\overline{x}$。而

$$\overline{x}\oplus x=((a\oplus x')*b)\oplus x=x\oplus b=b,$$
$$\overline{x}*x=((a\oplus x')*b)*x=a*x*b=a,$$

所以$\overline{x}$是x在$I[b,a]$中的补元，因此$\langle I[b,a],*,\oplus,^-,a,b\rangle$是布尔代数，但不是$\langle A,*,\oplus,',0,1\rangle$的子代数。

8.4.3 布尔代数的同态与同构

定义 8.15. $\langle A_1,*,\oplus,',0,1\rangle$与$\langle A_2,\wedge,\vee,^-,\widetilde{0},\widetilde{1}\rangle$是布尔代数。对于映射$f:A_1\to A_2$，如果对于$A_1$中的任意元素$a,b$，

$$f(a*b)=f(a)\wedge f(b),$$
$$f(a\oplus b)=f(a)\vee f(b),$$
$$f(a')=\overline{f(a)}$$

则称f是从布尔代数A_1到布尔代数A_2的**同态映射**。特别地，当f是双射时，称f是同构映射，并称布尔代数A_1与A_2同构。

定理 8.16. $\langle A_1,*,\oplus,',0,1\rangle$是布尔代数，对于$A$的任意元素$a$，布尔代数$I[a',0]$与布尔代数$I[1,a]$是同构的。

证明： 任取$a \in A$，有$a' \in A$且$0 \preceq a' \preceq 1$。

$$I[a', 0] = \{x | x \in A, 0 \preceq x \preceq a'\},$$
$$I[1, a] = \{x | x \in A, a \preceq x \preceq 1\}.$$

当$x \in I[a', 0]$时，$0 \preceq x \preceq a'$，由于$\oplus$运算是保序的，$0 \oplus a \preceq x \oplus a \preceq a' \oplus a$，故$a \preceq x \oplus a \preceq 1$，所以$x \oplus a \in I[1, a]$。令$f : I[a', 0] \to I[1, a]$，$f(x) = x \oplus a$。任取$y \in I[1, a]$，令$x = y * a'$，因为$a \preceq y \preceq 1$并且$*$是保序的，故$a * a' \preceq x = y * a' \preceq 1 * a'$，即$0 \preceq x \preceq a'$。$f(x) = x \oplus a = (y * a') \oplus a = y \oplus a = y$，这表明$x$是$y$的原像，所以$f$是满射。又若$x_1, x_2 \in I[a', 0]$都是$y \in I[1, a]$的原像，即$f(x_1) = x_1 \oplus a = x_2 \oplus a = f(x_2)$。

$$x_1 = x_1 * a' = (x_1 \oplus a) * a' = (x_2 \oplus a) * a' = x_2 * a' = x_2,$$

所以f是单射。从而，f是从$I[a', 0]$ 到$I[1, a]$的双射。

任取$x_1, x_2 \in I[a', 0]$，

$$f(x_1 * x_2) = (x_1 * x_2) \oplus a = (x_1 \oplus a) * (x_2 \oplus a) = f(x_1) * f(x_2),$$
$$f(x_1 \oplus x_2) = (x_1 \oplus x_2) \oplus a = (x_1 \oplus a) \oplus (x_2 \oplus a) = f(x_1) \oplus f(x_2),$$
$$f(\overline{x_1}) = f((0 \oplus x_1') * a') = (x_1' * a') \oplus a = x_1' \oplus a,$$
$$\overline{f(x_1)} = \overline{x_1 \oplus a} = (a \oplus (x_1 \oplus a)') * 1 = a \oplus (x_1' * a') = x_1' \oplus a.$$

所以，f是布尔代数$I[a', 0]$与布尔代数$I[1, a]$的同构映射，且$I[a', 0] \cong I[1, a]$。证毕。

定义 8.16. $\langle A_1, *, \oplus, ', 0, 1\rangle$与$\langle A_2, \wedge, \vee, ^-, \widetilde{0}, \widetilde{1}\rangle$是布尔代数。在$A_1 \times A_2$上定义$\widetilde{*}, \widetilde{\oplus}, ^\circ$运算，对$(a_1, a_2), (b_1, b_2) \in A_1 \times A_2$，

$$(a_1, a_2)\widetilde{*}(b_1, b_2) = (a_1 * b_1, a_2 \wedge b_2),$$
$$(a_1, a_2)\widetilde{\oplus}(b_1, b_2) = (a_1 \oplus b_1, a_2 \vee b_2),$$
$$(a_1, a_2)^\circ = (a_1', \overline{a_2}),$$

称$\langle A_1 \times A_2, \widetilde{*}, \widetilde{\oplus}, ^\circ, (0, \widetilde{0}), (1, \widetilde{1})\rangle$是布尔代数$A_1$和$A_2$的**直积**。

容易证明，两个布尔代数的直积仍是布尔代数。证明留作习题。

定理 8.17. $\langle A,*,\oplus,',0,1\rangle$是布尔代数，$a\in A$，则$A$与直积$\widetilde{(A)}=I[a,0]\times I[1,a]$同构。

证明： 任取$x\in A$，即$0\preceq x\preceq 1$。由于$*$和$\oplus$运算是保序的，故$0=0*a\preceq x*a\preceq 1*a=a$，$a=0\oplus a\preceq x\oplus a\preceq 1\oplus a=1$。定义$f:A\to I[a,0]\times I[1,a]$，$f(x)=(x*a,x\oplus a)$。任取$x_1,x_2\in A$，

$$\begin{aligned}
f(x_1\oplus x_2)&=((x_1\oplus x_2)*a,(x_1\oplus x_2)\oplus a)\\
&=((x_1*a)\oplus(x_2*a),(x_1\oplus a)\oplus(x_2\oplus a))\\
&=(x_1*a,x_1\oplus a)\oplus(x_2*a,x_2\oplus a)=f(x_1)\oplus f(x_2),\\
f(x_1*x_2)&=((x_1*x_2)*a,(x_1*x_2)\oplus a)\\
&=((x_1*a)*(x_2*a),(x_1\oplus a)*(x_2\oplus a))\\
&=(x_1*a,x_1\oplus a)*(x_2*a,x_2\oplus a)=f(x_1)*f(x_2),\\
\overline{f(x_1)}&=(\overline{x_1*a},\overline{x_1*a})=((0\oplus(x_1*a)')*a,(a\oplus(x_1\oplus a)')*1)\\
&=((x_1'\oplus a')*a,a\oplus(x_1'*a'))\\
&=(x_1'*a,x_1'\oplus a)=(f(x_1))',
\end{aligned}$$

所以f是同态映射。

任取$(y,z)\in I[a,0]\times I[1,a]$，$0\preceq y\preceq a$，$a\preceq z\preceq 1$，令$x=y\oplus(z*a')\in A$，

$$\begin{aligned}
f(x)&=f(y\oplus(z*a'))=((y\oplus(z*a'))*a,(y\oplus(z*a'))\oplus a)\\
&=(y*a,y\oplus z\oplus a)=(y,z),
\end{aligned}$$

即x是(y,z)的原像，故f是满射。

设$x_1,x_2\in A$都是$(y,z)\in I[a,0]\times I[1,a]$的原像，即

$$f(x_1)=(x_1*a,x_1\oplus a)=(x_2*a,x_2\oplus a)=f(x_2),$$

所以，

$$\begin{aligned}
x_1&=x_1*(a\oplus a')=(x_1*a)\oplus(x_1*a')\\
&=(x_1*a)\oplus((x_1\oplus a)*a')=(x_2*a)\oplus((x_2\oplus a)*a')\\
&=x_2*(a\oplus a')=x_2,
\end{aligned}$$

即f是单射，所以f是双射，故A与$\widetilde{A}$是同构的。证毕。

例 8.16. 设$A=\{1,2,\cdots,n\}$，$A_1=\{1,2,\cdots,k\}$，$\overline{A_1}=\{k+1,k+2,\cdots,n\}$，$\langle\mathscr{P}(A),\cap,\cup,^-,\emptyset,A\rangle$是布尔代数。

$$I[A_1,\emptyset]=\{x|x\in\mathscr{P}(A),\emptyset\subseteq x\subseteq A_1\}=\mathscr{P}(A_1),$$
$$I[A,A_1]=\{x|x\in\mathscr{P}(A),A_1\subseteq x\subseteq A\}=\mathscr{P}(\overline{A_1}).$$

由定理*8.16*知，$I[\overline{A_1},\emptyset]\cong I[A,A_1]$。由定理*8.17*知，$\mathscr{P}(A)\cong I[A_1,\emptyset]\times I[A,A_1]=\mathscr{P}(A_1)\times\mathscr{P}(\overline{A_1})$。

定理 8.18. 设A是有限布尔代数，$|A|=2^n$。令$B=\{1,2,\cdots,n\}$，则布尔代数A与$\langle\mathscr{P}(B),\cap,\cup,^-,\emptyset,B\rangle$是同构的。

证明： 对集合A的元素个数进行归纳证明。

(1) 当$|A|=2$时，$A=\{0,1\}$，$f:A\to\mathscr{P}(\{1\})$，$f(0)=\emptyset$，$f(1)=\{1\}$。易证，f是同构映射，所以$A\cong\mathscr{P}(\{1\})$。

(2) 假设$|A|<k$时命题成立。现设$|A|=k$。取$a\in A$，且$0\prec a\prec 1$。由定理8.17知，$A\cong I[a,0]\times I[1,a]$。再由定理8.16，$A\cong I[a,0]\times I[a',0]$。注意到$|I[a,0]|<k$，$|I[a',0]|<k$，有归纳假设知，布尔代数$I[a,0]$和$I[a',0]$分别与$\mathscr{P}(B_1)$和$\mathscr{P}(B_2)$同构，其中$|B_1|=k_1$，$|B_2|=k_2$。由例8.16知，如果$A\cong\mathscr{P}(B_1)\times\mathscr{P}(B_2)$，那么存在$k_1+k_2$个元素的集合$B$使得$A\cong\mathscr{P}(B)$。证毕。

从这个定理可以看出，$|A|=n$，$\langle\mathscr{P}(A),\cap,\cup,^-,\emptyset,A\rangle$是有$2^n$个元素的布尔代数，它穷尽了所有的有限布尔代数。

8.4.4 布尔代数的原子表示

如果在格$\langle A,\preceq\rangle$中有最小元0，那么最小元的控制元素称为**原子**。

在格$\langle A,\preceq\rangle$的Hasse图(图8.9)中$a_1,a_2,\cdots,a_k$是原子。显然，$a_i*a_j=0(i\neq j)$。

引理 8.2. 格$\langle A,\preceq\rangle$是有限格，0是它的最小元。对于A中任意非零元素b，至少存在一个原子a使得$a\preceq b$。

证明： 对于A中任意非零元素b，有以下两种情况:

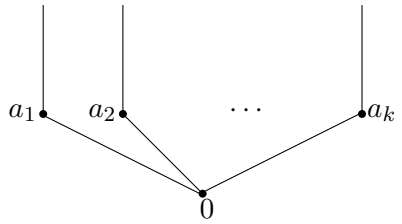


图 8.9: 原子示例图

(1) b是原子。那么显然$b \preceq b$，取$a = b$即可。

(2) b不是原子。0是有限格$\langle A, \preceq\rangle$的最小元，即$0 \prec b$，$b$不是0的控制元素，所以必存在$b_1 \in A$使得$0 \prec b_1 \prec b$。$b_1$又有两种情况:

(2.1) b_1是原子。取$a = b_1$即可。

(2.2) b_1不是原子。0是$\langle A, \preceq\rangle$的最小元，即$0 \prec b_1$，$b_1$不是0的控制元素，那么必存在$b_2 \in A$使得$0 \prec b_2 \prec b_1 \prec b$。这里$b_2 \neq b_1, b$。$b_2$又有两种情况，$\cdots\cdots$。

由于A是有限集合，这个过程不可能无限地进行下去。也就是说，在有限步之后b_i本身就是原子，取$a = b_i$即可。证毕。

引理 8.3. 设$\langle A, *, \oplus, ', 0, 1\rangle$是有限布尔代数。$b$是$A$中的非零元素，假设$a_1, a_2, \cdots, a_k$是$A$中满足$a_i \preceq b$的所有原子，则$b = a_1 \oplus a_2 \oplus \cdots \oplus a_k$。

证明: $a_1, a_2, \cdots, a_k$是A的原子并且$a_i \preceq b$，$1 \preceq i \preceq k$。显然，$a_1 \oplus a_2 \oplus \cdots \oplus a_k \preceq b$。下面证明$b \preceq a_1 \oplus a_2 \oplus \cdots \oplus a_k$。由于在有补分配格中$c \preceq d \Leftrightarrow c * d' = 0$ (证明留作习题)，所以只需证明$b * (a_1 \oplus a_2 \oplus \cdots \oplus a_k)' = 0$。

用反证法进行证明。假设$b * (a_1 \oplus a_2 \oplus \cdots \oplus a_k)' \neq 0$。由引理8.2知，存在原子$a$使得$a \preceq b * (a_1 \oplus a_2 \oplus \cdots \oplus a_k)'$。这里$a$是原子，且$a \preceq b$，$a \preceq (a_1 \oplus a_2 \oplus \cdots \oplus a_k)'$，而$a_1, a_2, \cdots, a_k$是小于等于$b$的全部原子，所以$a \in \{a_1, a_2, \cdots, a_k\}$。故$a \preceq a_1 \oplus a_2 \oplus \cdots \oplus a_k$。因此，$a \preceq (a_1 \oplus a_2 \oplus \cdots \oplus a_k) * (a_1 \oplus a_2 \oplus \cdots \oplus a_k)' = 0$，这与$a$是原子矛盾，所以假设不成立，因此$b * (a_1 \oplus a_2 \oplus \cdots \oplus a_k)' = 0$。

以上证明表明A的任意非零元素b都可以表示成满足$a_i \preceq b$的所有原子$a_1, a_2, \cdots, a_k$之和。下面证明这种表示形式是唯一的。假设$b_1, b_2, \cdots, b_l$是原子并且$b = b_1 \oplus b_2 \oplus \cdots \oplus b_l$。由$\oplus$的定义知$b_1, b_2, \cdots, b_l \preceq b$且$b_1, b_2, \cdots, b_l$是原子，而$a_1, a_2, \cdots, a_k$是小于等于$b$的全部原子，故$\{b_1, b_2, \cdots, b_l\} \subseteq \{a_1, a_2, \cdots, a_k\}$。如果$l < k$，即存在$a_m \notin \{b_1, b_2, \cdots, b_l\}$，

$$\begin{aligned} a_m &= a_m * b = a_m * (b_1 \oplus b_2 \oplus \cdots \oplus b_l) \\ &= (a_m * b_1) \oplus (a_m * b_2) \oplus \cdots \oplus (a_m * b_1), \end{aligned}$$

其中a_m, b_i都是原子，且$a_m \neq b_i$，故$a_m * b_i = 0$，$1 \leq i \leq l$。从而得出，$a_m = 0$，这与a_m是原子矛盾，故假设不成立，所以$l = k$，即b表示成原子之和的形式是唯一的。证毕。

引理 8.4. 在布尔格$\langle A, \preceq \rangle$中若任取非零元素$b$和原子$a$，则$a \preceq b$ 和$b \preceq a$，两者必有一个且只有一个成立。

证明： b和a分别是A的非零元素和原子。显然，$0 \preceq a * b \preceq a$。由于$a$是原子，即$a$是0的控制元素，不可能存在非零元素$b$使得$0 \prec a * b \prec a$。所以$a * b = a$或0。如果$a * b = a$，则$a \preceq b$。又在布尔格中$a \preceq b'$当且仅当$a * (b')' = 0$，即$a * b = 0$。所以当$a * b = 0$ 时，必有$a \preceq b'$。而$a \preceq b$和$a \preceq b'$不可能同时成立，否则$a \preceq b * b' = 0$，与a是原子矛盾。所以$a \preceq b$和$b \preceq a$两者必居其一且只有一个成立。证毕。

定理 8.19. 设$\langle A, *, \oplus, ', 0, 1 \rangle$是有限布尔代数。若$S$是$A$中所有原子构成的集合，那么布尔代数$\langle A, *, \oplus, ', 0, 1 \rangle$与$\langle \mathscr{P}(S), \cap, \cup, ^-, \emptyset, S \rangle$同构。

证明： 在两个布尔代数A与$\mathscr{P}(S)$之间构造映射$f : A \to \mathscr{P}(S)$，对任意$a \in A$，

$$f(a) = \begin{cases} \emptyset & \text{若} a = 0, \\ \{a_1, a_2, \cdots, a_k | a_i \in S, a_i \preceq a, 1 \leq i \leq k\} & \text{若} a \neq 0. \end{cases}$$

由引理8.2知，A中非零元素a的像$f(a)$是唯一确定的。任取$\{a_{i_1}, a_{i_2}, \cdots, a_{i_p}\} \subseteq S$，$\{a_{i_1}, a_{i_2}, \cdots, a_{i_p}\} \neq \emptyset$，令$b = a_{i_1} \oplus a_{i_2} \oplus \cdots \oplus a_{i_p}$。显然，$b \in A$，且$f(b) = \{a_{i_1}, a_{i_2}, \cdots, a_{i_p}\}$，故$b$是$\{a_{i_1}, a_{i_2}, \cdots, a_{i_p}\}$的原像。所以，$f$是满

射。假设a,b都是$\{a_{i_1},a_{i_2},\cdots,a_{i_p}\}$的原像，由引理8.3知，$a=a_{i_1}\oplus a_{i_2}\oplus\cdots\oplus a_{i_p}=b$，所以$f$是单射。因此，$f$是双射。下面证明$f$保持$*,\oplus,'$运算。

(1) $f(a*b)=f(a)\cap f(b)$: 当$a=0$或$b=0$时，$f(a*b)=f(0)=\emptyset$；另一方面，$a=0$或$b=0$意味着$f(a)=\emptyset$或$f(b)=\emptyset$，所以，$f(a)\cap f(b)=\emptyset=f(a*b)$。

当$a\neq 0$且$b\neq 0$时，$f(a)=\{a_1,a_2,\cdots,a_k\}$，$f(b)=\{b_1,b_2,\cdots,b_l\}$。也就是说，$a_1,a_2,\cdots,a_k$是小于等于$a$的所有原子，$b_1,b_2,\cdots,b_l$是小于等于$b$的所有原子。如果$a*b=0$，则有$f(a*b)=\emptyset$。假若$f(a)\cap f(b)\neq\emptyset$，则存在$x\in f(a)\cap f(b)$，即$x$是小于等于$a$ 的原子，同时也是小于等于b的原子，所以$x\preceq a*b=0$，这与x是原子矛盾，故$f(a)\cap f(b)=\emptyset=f(a*b)$。如果$a*b\neq 0$，令$f(a*b)=\{c_1,c_2,\cdots,c_m\}$，所以原子$c_i\preceq a*b\preceq a$，$c_i\preceq a*b\preceq b$，故有$c_i\in\{a_1,a_2,\cdots,a_k\}$且$c_i\in\{b_1,b_2,\cdots,b_l\}$，$1\leq i\leq m$。从而，

$$\{c_1,c_2,\cdots,c_m\}\subseteq\{a_1,a_2,\cdots,a_k\}\cap\{b_1,b_2,\cdots,b_l\}.$$

反之，任取$x\in\{a_1,a_2,\cdots,a_k\}\cap\{b_1,b_2,\cdots,b_l\}$，$x\preceq a$且$x\preceq b$，于是$x\preceq a*b$。所以$x\in\{c_1,c_2,\cdots,c_m\}$。这表明

$$\{a_1,a_2,\cdots,a_k\}\cap\{b_1,b_2,\cdots,b_l\}\subseteq\{c_1,c_2,\cdots,c_m\}.$$

综上，$\{c_1,c_2,\cdots,c_m\}=\{a_1,a_2,\cdots,a_k\}\cap\{b_1,b_2,\cdots,b_l\}$，即

$$f(a*b)=f(a)\cap f(b).$$

(2) $f(a\oplus b)=f(a)\cup f(b)$: 当$a=0$或$b=0$时，$a\oplus b=b$或$a\oplus b=a$，故$f(a\oplus b)=f(b)$或$f(a\oplus b)=f(a)$；另一方面，$a=0$或$b=0$意味着$f(a)=\emptyset$或$f(b)=\emptyset$，故$f(a)\cup f(b)=f(b)$或$f(a)\cup f(b)=f(a)$。于是$f(a\oplus b)=f(a)\cup f(b)$ 。

当$a\neq 0$且$b\neq 0$时，令$f(a\oplus b)=\{d_1,d_2,\cdots,d_n\}$，$d_1,d_2,\cdots,d_n$是满足$d_i\preceq a\oplus b(1\leq i\leq n)$的全部原子。根据引理8.4，对于原子$d_i$和非零元素$a,b$，$d_i\preceq a$和$d_i\preceq a'$有且只有一个成立；$d_i\preceq b$和$d_i\preceq b'$有且只有一个成立。这样就有四种组合: 1) $d_i\preceq a$ 且$d_i\preceq b$，2) $d_i\preceq a$且$d_i\preceq b'$，3) $d_i\preceq a'$且$d_i\preceq b$，4) $d_i\preceq a'$且$d_i\preceq b'$。其中第四种组合不可能，否

则由$d_i \preceq a'$和$d_i \preceq b'$，得到$d_i \preceq a' * b' = (a \oplus b)'$，而$d_i \preceq a \oplus b$，故有$d_i \preceq (a \oplus b)' * (a \oplus b) = 0$，与$d_i$是原子矛盾。在其他三种组合中，或者$d_i \preceq a$成立或者$d_i \preceq b$成立，即$d_i \in \{a_1, a_2, \cdots, a_k\} \cup \{b_1, b_2, \cdots, b_l\}$，所以$\{d_1, d_2, \cdots, d_n\} \subseteq \{a_1, a_2, \cdots, a_k\} \cup \{b_1, b_2, \cdots, b_l\}$。反之，任取$x \in \{a_1, a_2, \cdots, a_k\} \cup \{b_1, b_2, \cdots, b_l\}$，显然$x \preceq a \preceq a \oplus b$，$x \preceq b \preceq a \oplus b$，于是$x \in \{d_1, d_2, \cdots, d_n\}$，从而$\{a_1, a_2, \cdots, a_k\} \cup \{b_1, b_2, \cdots, b_l\} \subseteq \{d_1, d_2, \cdots, d_n\}$。因此，$\{d_1, d_2, \cdots, d_n\} = \{a_1, a_2, \cdots, a_k\} \cup \{b_1, b_2, \cdots, b_l\}$，即

$$f(a \oplus b) = f(a) \cup f(b).$$

(3) $f(a') = \overline{f(a)}$: 当$a = 1$时，$f(a') = f(0) = \emptyset$；而$\overline{f(a)} = \overline{S} = \emptyset$，所以$f(a') = \overline{f(a)}$。

当$a \neq 1$时，$f(a') \neq \emptyset$。这时对于原子x，

$$x \in f(a') \Leftrightarrow x \preceq a' \Leftrightarrow x \preceq a\text{不成立} \Leftrightarrow x \notin f(a) \Leftrightarrow x \in \overline{f(a)},$$

由此得到$f(a') = \overline{f(a)}$。

由以上讨论可知，f是从布尔代数A到$\mathscr{P}(S)$的同构映射，所以两个布尔代数$\langle A, *, \oplus, ', 0, 1\rangle$与$\langle \mathscr{P}(S), \cap, \cup, ^-, \emptyset, S\rangle$同构。证毕。

从以上讨论可知，有限布尔代数中集合A的元素个数是2^n，其中n就是布尔代数A中的原子个数。任何具有2^n个元素的布尔代数都是同构的。

8.4.5 布尔环

在布尔代数$\langle A, *, \oplus, ', 0, 1\rangle$中，现在分别看其中一个二元运算。$\langle A, *\rangle$中，$*$满足交换律和结合律。对于$A$中任意元素$a$均有$a * 1 = a$，所以1是$*$运算的单位元。对于元素$a$，如果存在$b \in A$使$a * b = 1$，那么$a = a \oplus (a * b) = a \oplus 1 = 1$，也就是说集合$A$中只有当$a = 1$时有关于$*$运算的逆元，所以$\langle A, *\rangle$构成含幺半群。$\langle A, \oplus\rangle$中，$\oplus$满足交换律和结合律。对于$A$中任意元素$a$均有$a \oplus 0 = a$，所以0是$\oplus$ 运算的单位元。对于元素a，如果存在$b \in A$使$a \oplus b = 0$，那么$a = a * (a \oplus b) = a * 0 = 0$，也就是说集合$A$中只有当$a = 0$时有关于$\oplus$运算的逆元，所以$\langle A, \oplus\rangle$也是含幺半群。

如果同时看A上的两个二元运算，根据上述分析，$\langle A, *, \oplus\rangle$是布尔格，但不能构成环。为此在$A$上定义新的二元运算$+$，对任意的$a, b \in A$，

$$a + b = (a * b') \oplus (a' * b).$$

易见，$+$运算满足交换律和结合律。0是零元。由于$a+a = (a*a')\oplus(a'*a) = 0 \oplus 0 = 0$，所以$a$是$a$的负元。从而$\langle A, +\rangle$是交换群。又

$$\begin{aligned}
&(a + b) * c = ((a * b') \oplus (a' * b)) * c = (a * b' * c) \oplus (a' * b * c),\\
&(a * c) + (b * c) = ((a * c) * (b * c)') \oplus ((a * c)' * (b * c))\\
&= (a * c * (b' \oplus c')) \oplus ((a' \oplus c') * b * c)\\
&= (a * b' * c) \oplus (a' * b * c),
\end{aligned}$$

所以$(a+b)*c = (a*c)+(b*c)$，即$*$对$+$有右分配律。同理可证$c*(a+b) = (c*a)+(c*b)$，即$*$对$+$有左分配律。

因此，$\langle A, +, *\rangle$是环，称之为**布尔环**。在布尔环中，对A中任意元素a，有$a^2 = a * a = a$。

反之，已知$\langle A, +, *\rangle$是布尔环，重新定义二元运算$\oplus$和一元运算$'$，对$a, b \in A$，

$$a \oplus b = a + b + a * b,$$
$$a' = 1 + a,$$

那么$\langle A, *, \oplus, ', \cdots\rangle$构成布尔代数。该布尔代数最小元和最大元的求解留作习题。

8.4.6 布尔表达式

定义 8.17. 布尔代数$\langle A, *, \oplus, ', 0, 1\rangle$上的**布尔表达式**定义为：

(1) A中任何元素都是布尔表达式；

(2) 任何变元是布尔表达式；

(3) 若e_1和e_2是布尔表达式，则e_1'，$(e_1 \oplus e_2)$，$(e_1 * e_2)$是布尔表达式。

有n个不同变元的布尔表达式叫做n元布尔表达式，记作$E(x_1, x_2, \cdots, x_n)$，其中$x_1, x_2, \cdots, x_n$是变元。用A中元素代替$x_i (1 \le i \le n)$，则$E(x_1, x_2, \cdots, x_n)$就

是A中的一个元素。所以E是从A^n到A的映射。如果$f: A^n \to A$，f能用A上的n元布尔表达式表示，那么f就叫做n元**布尔函数**。

$\langle\{0,1\}, \bullet, +, ^-, 0, 1\rangle$是二元集合上的布尔代数。任何$n$元开关函数$f: \{0,1\}^n \to \{0,1\}$，与函数值1对应的$n$元有序数组都能写出小项表达式。因此，每个开关函数都是布尔函数。可以证明，一般的布尔代数$\langle A, *, \oplus, ', 0, 1\rangle$上的任意布尔表达式$E(x_1, x_2, \cdots, x_n)$ 可以表示成

$$E(x_1, x_2, \cdots, x_n) = \oplus_{(a_1,a_2,\cdots,a_n)} E(a_1, a_2, \cdots, a_n) * x_1^{a_1} * x_2^{a_2} * \cdots * x_n^{a_n},$$

其中$a_i = 0$或1，$x_i^0 = x_i'$，$x_i^1 = x_i$，$1 \le i \le n$。

下面举例说明并非所有从A^n到A的映射都是A上的布尔函数。令$A = \{0,1,2,3\}$，布尔代数$\langle A, *, \oplus, ', 0, 1\rangle$的Hasse图如图8.10，其中2与3互为补元。令映射$g: A^2 \to A$定义如表8.1所示。

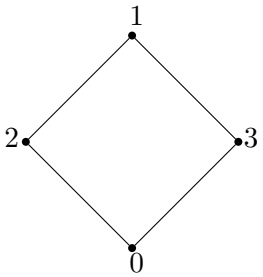


图 8.10: 四阶布尔代数的Hasse图

如果g是布尔函数，应该能有下面的小项表达式

$$\begin{aligned} g(x_1, x_2) &= (g(1,1) * x_1 * x_2) \oplus (g(1,0) * x_1 * x_2') \\ &\quad \oplus (g(0,1) * x_1' * x_2) \oplus (g(0,0) * x_1' * x_2') \\ &= (x_1 * x_2) \oplus (x_1 * x_2') \oplus (x_1' * x_2'). \end{aligned}$$

当$x_1 = x_2 = 3$时，有

$$g(3,3) = (3 * 3) \oplus (3 * 2) \oplus (2 * 2) = 3 \oplus 0 \oplus 2 = 1,$$

与g的定义中$g(3,3) = 2$(见表8.1)不同，矛盾。故g不是布尔函数。

表 8.1: 从A^2到A的映射

g(i, j) i \ j	0	1	2	3
0	1	0	0	3
1	1	1	0	3
2	2	0	1	1
3	3	0	2	2

习题

1. 令$R_1 = \{x|x \in \mathbb{R}, 0 \preceq x \preceq 1\}$，$\preceq$是$R_1$上的小于等于关系。证明$\langle R_1, \preceq\rangle$是格。该格的$*$和$\oplus$运算是什么?

2. $\langle A, \preceq\rangle$是格，$a, b, c$是$A$中任意元素，证明:

(1) $a * b = b * a$，$a \oplus b = b \oplus a$;

(2) $a * (a \oplus b) = a$，$a \oplus (a * b) = a$。

3. 证明: 在格中，如果$a \preceq b$，$c \preceq d$，则有$a * c \preceq b * d$。

4. 证明: 在格中，如果$a \preceq b \preceq c$，则有

(1) $a \oplus b = b * c$;

(2) $(a * b) \oplus (b * c) = b = (a \oplus b) * (b \oplus c)$。

5. 证明: 在格中，

$$(a * b) \oplus (c * d) \preceq (a \oplus c) * (b \oplus d),$$

$$(a * b) \oplus (b * c) \oplus (c * a) \preceq (a \oplus b) * (b \oplus c) * (c \oplus a).$$

6. $\langle A, \preceq\rangle$是格。取$A$中的元素$a, b$，$a \prec b$。令

$$B = \{x|x \in A, a \preceq x \preceq b\},$$

证明: $\langle B, \preceq\rangle$是格。

7. $\langle A, *, \oplus\rangle$是格，$A$的元素个数大于1。如果该格有最小元0和最大元1，那么它们必然是A的不同元素。

8. 设$S = \{1, 3, 5, 15, 25, 75\}$，$\langle S, |\rangle$是格。请列出$S$中有补元的元素并写出它们的补元。

9. 在具有两个或更多个元素的格中，没有元素自身是自身的补元。

10. 具有三个或更多个元素的线性序集不是有补格。

11. 五阶格中哪些是分配格?

12. 证明：格A是分配格当且仅当对任意$a, b, c \in A$，$(a * b) \oplus (b * c) \oplus (c * a) = (a \oplus b) * (b \oplus c) * (c \oplus a)$。

13. 证明：在有补分配格中，

(1) $a \preceq b \Leftrightarrow a * b' = 0$;

(2) $b' \preceq a' \Leftrightarrow a' \oplus b = 1$。

14. f是从集合A到集合B的映射。令$S = \{f(c)|c \in \mathscr{P}(A)\}$。证明：$\langle S, \subseteq\rangle$是$\langle \mathscr{P}(B), \subseteq\rangle$的子格。

15. $\langle A, \preceq\rangle$是分配格。$a, b \in A$且$a \prec b$。令$B = \{x|x \in A, a \preceq x \preceq b\}$。证明：$f(x) = (x \oplus a) * b$是从$A$到$B$的同态映射。

16. $\langle S, \preceq\rangle$是模格，$a, b \in S$。令

$$X = \{x|x \in S, a * b \preceq x \preceq a\},$$

$$Y = \{y|y \in S, b \preceq y \preceq a \oplus b\},$$

$$f = x \oplus b.$$

证明：f是从X到Y的同构映射。

17. 在布尔代数$\langle A, *, \oplus, ', 0, 1\rangle$中，对$A$中任意元素$a, b$，

(1) $a \oplus (a' * b) = a \oplus b$;

(2) $a * (a' \oplus b) = a * b$。

18. 证明：在布尔代数中，$x \preceq y \Leftrightarrow y' \preceq x'$。

19. $\langle A_1, *, \oplus, ', 0, 1\rangle$与$\langle A_2, \wedge, \vee, ^-, \widetilde{0}, \widetilde{1}\rangle$是两个布尔代数。证明它们的直积$\langle A_1 \times A_2, \widetilde{*}, \widetilde{\oplus}, ^\circ, (0, \widetilde{0}), (1, \widetilde{1})\rangle$是布尔代数。

20. A, B是两个不相交的集合。任取$S \subseteq A$，$T \subseteq B$，令$f(S \cup T) = (S, T)$。证明：f是布尔代数$\langle \mathscr{P}(A \cup B), \subseteq\rangle$ 到$\langle \mathscr{P}(A) \times \mathscr{P}(B), \subseteq\rangle$的同构映射。

21. 找出8阶布尔代数的所有子代数。

22. $\langle\{1,2,3,4,6,12\},|\rangle$和$\langle\{1,2,3,4,6,8,12,24\},|\rangle$是布尔代数吗?

23. 若$a,b_1,b_2,\cdots,b_r$是布尔代数$\langle A,*,\oplus,',0,1\rangle$的原子，证明

$$a \preceq b_1 \oplus b_2 \oplus \cdots \oplus b_r \Leftrightarrow \text{存在} i, \text{使得} a = b_i, 1 \leq i \leq r.$$

24. 若$b_1,b_2,\cdots,b_n$是有限布尔代数中的所有原子，证明:

$$y = 0 \Leftrightarrow \forall i, y * b_i = 0, 1 \leq i \leq n.$$

25. $\langle A,+,*\rangle$是布尔环。在A上定义二元运算$\oplus$和一元运算$'$如下，对$a,b \in A$,

$$a \oplus b = a + b + a * b,$$
$$a' = 1 + a,$$

证明: $\langle A,*,\oplus,',\cdots\rangle$构成布尔代数，并确定其最小元和最大元。

Bibliography