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$\overbrace{m\times m\times\cdots\times m}^{n\text{个}}=m^n=|B|^{|A|}$ 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

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

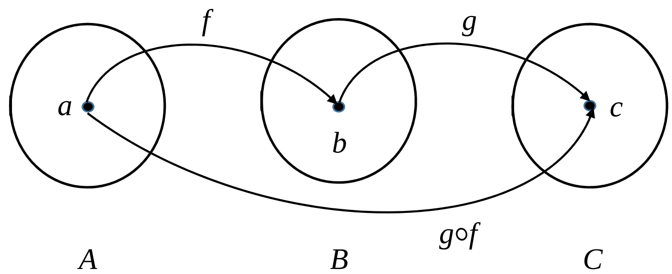

图 3.1: 复合映射的示意图

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$\sigma_j \bullet \sigma_i$，也经常省略掉“•”，直接记为$\sigma_j\sigma_i$。在例3.10中，

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

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，

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

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	$\overline{f}$	$f+g$	$f\bullet g$
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) $(f\bullet g)(x_1,x_2,...,x_n)=f(x_1,x_2,...,x_n)\bullet g(x_1,x_2,...,x_n)$，$f\bullet g$ 称为f与g的积函数，称“$\bullet$”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”$\bullet$”、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，$(f+g)(x_1,x_2)=x_2=g(x_1,x_2)$，$(f\bullet g)(x_1,x_2)=x_1x_2=f(x_1,x_2)$，$\overline{f}(x_1,x_2)=\overline{x}_1+\overline{x}_2$。

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：$(f+g)+h=f+(g+h)$；$(f\bullet g)\bullet h=f\bullet(g\bullet h)$。

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

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

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:

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

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“∩”、并“∪”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

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

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

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$g\circ f\ne I_S$。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。