第 1 章　基本概念

这一章介绍群的定义和一些基本概念及性质. 并在 1.2 节中详细介绍置换和置换群的概念，作为进一步研究一般群和置换群的基础.

1.1　群的概念

1　群的定义

定义 1　设 G 是一个非空集合，在 G 中定义了一种代数运算，称为乘法，记作“ $\cdot$ ”. 即对于 G 中任意两个元素 a, b，都唯一确定 G 中一个元素 $a \cdot b$，称为 a, b 的乘积. 如果 G 对这种运算满足下面几个条件：

1) 结合律　对 G 中任意 3 个元素 a, b, c，都有

$$(a \cdot b) \cdot c = a \cdot (b \cdot c);$$

2) 单位元素的存在　G 中存在一个元素 e，对于 G 中任意元素 a，都有

$$e \cdot a = a \cdot e = a;$$

3) 逆元素的存在　对于 G 中任一个元素 a，都可找到 G 中一个元素 a^{-1}，使得

$$a^{-1} \cdot a = a \cdot a^{-1} = e,$$

那么 G 就称为一个群. 元素 e 称为 G 的单位元素，a^{-1} 称为 a 的逆元素.

定义 2 如果群 G 还满足：

4) **交换律** 对于 G 中任意两个元素 a，b，都有

$$a \cdot b = b \cdot a.$$

那么 G 就称作一个交换群或阿贝尔群.

如果群 G 的运算不满足交换律，则称 G 为非交换群.

为了简便起见，在不致混淆的情况下，我们常用 ab 表示 a 与 b 的乘积.

有时候，有些交换群的运算用加法表示，记作“+”，$a+b$ 称为 a 与 b 的和. 那么条件 1)～4)就成为：

1′) **结合律** 对 G 中任意 3 个元素 a，b，c，都有

$$(a+b)+c = a+(b+c);$$

2′) **零元素的存在** G 中存在一个元素 0，对于 G 中任一个元素 a，都有

$$0+a = a+0 = a;$$

3′) **负元素的存在** 对于 G 中任一个元素 a，都可找到 G 中一个元素 $-a$，使得

$$(-a)+a = a+(-a) = 0;$$

4′) **交换律** 对于 G 中任意两个元素 a，b，都有

$$a+b = b+a.$$

0 称为 G 的零元素，$-a$ 称为 a 的负元素.

2 群的例子

例 1 全体整数所成的集合 $\mathbb{Z}$ 对于数的加法成一交换群. 因为 $\mathbb{Z}$ 对数的加法满足条件 1′)～4′)，群 $\mathbb{Z}$ 的零元素就是整数 0，整数 n 的负元素就是 $-n$.

同样地，全体有理数所成集合 $\mathbb{Q}$，全体实数所成集合 $\mathbb{R}$，全体复数所成集合 $\mathbb{C}$，对于数的加法也都成为交换群.

例 2　全体非零有理数$\mathbb{Q}^*$，全体非零实数$\mathbb{R}^*$，全体非零复数$\mathbb{C}^*$对数的乘法都构成交换群.

但是全体非零整数对数的乘法不构成群，因为不满足条件3).全体正整数对数的加法也不构成群，因为不满足条件2)及3).

例 3　n是一个正整数.全部n次单位根所成集合U_n对于数的乘法组成一个交换群.

例 4　用$M_{n,m}(\mathbb{R})$表示全部$n\times m$实矩阵所成的集合.$M_{n,m}(\mathbb{R})$对矩阵的加法构成一个交换群.

例 5　F是一个域,用$GL_n(F)$表示F上全部n阶可逆矩阵所成的集合.$GL_n(F)$对矩阵的乘法构成一个群，称为F上n级一般线性群.当$n\geqslant 2$时,$GL_n(F)$是非交换的.

例 6　用$SL_n(F)$表示域F上全部行列式等于1的矩阵组成的集合.$SL_n(F)$对矩阵的乘法构成一个群，称为F上n级特殊线性群.当$n\geqslant 2$时,$SL_n(F)$是非交换的.

例 7　设V是域F上一个n维线性空间，用$GL_n(V)$表示V的全部可逆线性变换所成的集合.$GL_n(V)$对变换的乘法构成一个群.当$n\geqslant 2$时，这个群是非交换的.

例 8　设F是一个域,F对F的加法构成一个交换群.F中非零元素的集合F^*对F的乘法也成为一个交换群.

例 9　设V是域F上一个线性空间.V对向量的加法构成一

个交换群.

例 10　设 $G=\{a,b,c,d\}$. 用下列乘法表定义 G 的运算：

	a	b	c	d
a	a	b	c	d
b	b	a	d	c
c	c	d	a	b
d	d	c	b	a

表中第 i 行第 j 列处的元素表示左边的第 i 个元素与表上边第 j 个元素之积. 例如，上表说明

$$a \cdot a = a, \quad b \cdot c = d,$$

等等.

请读者自己验证 G 对这个运算构成一个交换群.

用乘法表来给出一个群是常常采用的方法，我们在以后还会遇到.

3　简单性质

从群的定义，可以推出下面的一些性质：

1) 群中单位元素是唯一的.

证　明　设 G 是一个群，e 是 G 的单位元素. 如果 e' 也是 G 的单位元素，那么，因为 e 是单位元素，所以

$$e \cdot e' = e'.$$

又因 e' 也是单位元素，所以

$$e \cdot e' = e.$$

因此，必须有

$$e' = e,$$

所以 G 的单位元素是唯一的. ▌

2) 在群中，每个元素只有一个逆元素.

证 明 设 a 是群 G 中的一个元素，e 是 G 的单位元素，a^{-1} 是 a 的逆元素.如果 a 也是 a 的逆元素，那么，根据逆元素的定义，有

$$(a' \cdot a)a^{-1} = e \cdot a^{-1} = a^{-1},$$
$$a' \cdot (a \cdot a^{-1}) = a' \cdot e = a'.$$

由结合律，即得

$$a' = a^{-1}.$$

所以逆元素是唯一的. ▌

由逆元素的唯一性，可得

3) $(a^{-1})^{-1} = a.$

4) 群中消去律成立，即 如果 $ab = ac$，则有 $b = c$ 如果 $ba = ca$，则有 $b = c.$

证 明 设 $ab = ac.$ 用 a^{-1} 左乘等式两端，得

$$a^{-1}(ab) = a^{-1}(ac).$$

于是

$$(a^{-1}a)b = (a^{-1}a)c.$$

从而

$$eb = ec, \quad b = c.$$

同样可证第二个等式. ▌

5) 在群中,对于任意两个元素 a,b,方程

$$ax = b \quad 及 \quad ya = b$$

都有解，而且解是唯一的.

证明　显然，元素 $a^{-1}b$ 及 ba^{-1} 分别是这两个方程的解，解的唯一性可由消去律得出. ▌

需要注意的是，因为群中交换律不一定成立，所以上面两个方程的解一般是不相等的，只有在 a 与 b 可交换,即 $ab=ba$ 时,这两个解才相等.

对于群中一个元素 a,我们把 $n(n>0)$ 个 a 相乘所得的元素记作 a^n,即

$$\underbrace{a \cdot a \cdot \cdots \cdot a}_{n\text{个}} = a^n.$$

对于负整数一 $n(n>0)$,规定

$$a^{-n} = (a^{-1})^n,$$

并约定 a^0 表示群的单位元素. a^n(n 为任意整数)称为 a 的方幂. 根据结合律,可知

6) 群中指数律成立,即

$$a^n \cdot a^m = a^{n+m}, \quad n,m \text{ 为任意整数;}$$

$$(a^n)^m = a^{nn}, \quad n,m \text{ 为任意整数.}$$

如果 $ab=ba$,则有

$$(ab)^n = a^n b^n, \quad n \text{ 为任意整数.}$$

如果所讨论的群是交换群，而且群的运算用加法表示，那么，上面的一些性质可以叙述为：

1′) 群中只有一个零元素.

2′) 在群中，每个元素只有一个负元素 .

3′) $-(-a)=a$.

以后,常用 $a-b$ 表示 $a+(-b)$.

4′) 如果 $a+b=a+c$,则有 $b=c$.

5′) 对于任意两个元素 a,b,方程

$$a+x=b$$

有唯一解 $x=b-a$.

对于加法交换群来说，一个元素的方幂就是这个元素的倍数. 当 $n>0$ 时,我们用 na 表示 n 个 a 相加所得之和,即

$$\underbrace{a+a+\cdots+a}_{n\text{个}}=na.$$

规定

$$(-n)a=-(na).$$

并约定 $0a$ 表示群的零元素. 于是下列倍数律成立：

6′) $na+ma=(n+m)a$， n,m 为任意整数；

$m(na)=mna$， n,m 为任意整数；

$n(a+b)=na+nb$， n 为任意整数.

4 阶

定义 3 如果群 G 包含的元素个数有限，则称 G 为有限群.否则称 G 为无限群. 有限群 G 所包含的元素个数称为 G 的阶.

定义 4 设 a 是群 G 中一个元素，如果存在正整数 k 使得 $a^k=e$,则 a 称为有限阶元素. 满足 $a^k=e$ 的最小正整数 k 叫做 a 的阶.如果不存在正整数 k 使得 $a^k=e$,则 a 称为无限阶元素.

定义中的条件 $a^k=e$ 在加法群时应改为 $ka=e$. 以后我们只讨

论乘法群，而对加法群的情形就不另外说明了.

例如,在前面所举的群例中,例 3 中的群的阶等于 n;例 10 中的群的阶等于 4 其余的群,除例 8 外,都是无限群. 至于例 8 中的群则要根据域 F 来决定 当 F 是无限域时，加法群 F 及乘法群都是无限群. 当 F 是有限域时，加法群 F 的阶等于 F 中元素数 $|F|$；而乘法群 F^* 的阶 $|F^*|$ 等于 $|F|-1$.

在例 1 中，除去零元素的阶等于 1 外，其他元素都是无限阶元素. 在例 10 中,单位元素 a 是 1 阶元素，其他元素的阶都等于 2.

从定义可以看出，在一个群中，单位元素 (零元素,如果是加法群)是唯一的一个 1 阶元素.

我们以后主要讨论有限群. 有限群中的元素一定都是有限阶元素. 这个事实可以这样来证明，设 a 是有限群 G 中一个元素. 考虑下列元素

$$a, a^2, a^3, \cdots.$$

由于 G 是一个有限群，所以这些元素中一定有相同的. 即有正整数 $k_1 < k_2$,使得

$$a^{k_1} = a^{k_2}.$$

于是

$$a^{k_2-k_1} = e, \qquad k_2 - k_1 > 0.$$

根据定义,a 是一个有限阶元素.

如果一个群中的所有元素都是有限阶元素，那么这个群称为周期群. 有限群一定是周期群.

关于元素的阶有下述重要性质.

定理 1 如果 a 是群 G 的一个 k 阶元素,e 是 G 的单位元素. 那么

1) $a^l = e \Leftrightarrow k \mid l$;

2) $a^l = a^m \Leftrightarrow k \mid l-m$.

如果 a 是一个无限阶元素，那么

$$a^l=a^m\Leftrightarrow l=m.$$

证明　1) 如果 $k\mid l$，那么可设 $l=kd$，d 是一个整数.

于是

$$a^l=a^{kd}=(a^k)^d=e^d=e.$$

反之，如果 $k\nmid l$，可设

$$l=kd+r,\quad 0<r<k.$$

于是

$$a^l=a^{kd+r}=a^{kd}\cdot a^r=e\cdot a^r=a^r\neq e.$$

2 因为

$$a^l=a^m\Leftrightarrow a^{l-m}=e,$$

故由 1)即得

$$a^l=a^m\Leftrightarrow k\mid l-m.$$

关于无限阶元素的结论可以从定义直接得到. ▌

关于群及元素的阶还有一些重要的性质，请读者参考本章习题.

1.2 置　　换 群

置换群是一类最重要的有限群，作为群的例子，这一节介绍置换及置换群的概念. 关于置换的进一步性质，将在第 3 章中讨论.

1 置换及对称群

设 Ω 是由 n 个文字组成的集合：

$$\Omega=\{\alpha_1,\alpha_2,\cdots,\alpha_n\}.$$

Ω到自身的一个一一映射称为(作用于)Ω上的一个置换,或n元置换，简称置换.有时候也称为$\alpha_1,\alpha_2,\cdots,\alpha_n$的一个置换.

设σ是$\Omega=\{\alpha_1,\alpha_2,\cdots,\alpha_n\}$上的一个置换.用$\alpha_i^\sigma(i=1,2,\cdots,n)$表示$\alpha_i$在$\sigma$下的象,而把$\sigma$表成

$$\sigma=\begin{pmatrix}\alpha_1 & \alpha_2 & \cdots & \alpha_n\\ \alpha_1^\sigma & \alpha_2^\sigma & \cdots & \alpha_n^\sigma\end{pmatrix},$$

或者可以简单地表成

$$\sigma=\begin{pmatrix}\alpha_i\\ \alpha_i^\sigma\end{pmatrix}.$$

为了简单起见，有时常用$1,2,\cdots,n$表示Ω的n个元素，此时,σ就可表成

$$\sigma=\begin{pmatrix}1 & 2 & \cdots & n\\ 1^\sigma & 2^\sigma & \cdots & n^\sigma\end{pmatrix}=\begin{pmatrix}i\\ i^\sigma\end{pmatrix}.$$

因为σ是一个一一映射，所以$1^\sigma,2^\sigma,\cdots,n^\sigma$是$1,2,\cdots,n$的一个排列.两个不同的置换$\sigma,\tau$所对应的排列$1^\sigma,2^\sigma,\cdots,n^\sigma$与$1^\tau,2^\tau,\cdots,n^\tau$是不同的.而且,任给$1,2,\cdots,n$的一个排列$\alpha_1,\alpha_2,\cdots,\alpha_n$,都有唯一的一个置换$\sigma$使得

$$i^\sigma=\alpha_i,\qquad i=1,2,\cdots,n,$$

即

$$\sigma=\begin{pmatrix}1 & 2 & \cdots & n\\ \alpha_1 & \alpha_2 & \cdots & \alpha_n\end{pmatrix}.$$

因此n元置换与n元排列之间有一个一一对应.我们知道n元排列一共有$n!$个，所以一共有$n!$个n元置换.我们用S_n表示这$n!$个n元置换所成的集合.例如,一共有6个3元置换：

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

$$\sigma_3=\begin{pmatrix}1 & 2 & 3\\ 3 & 2 & 1\end{pmatrix},\quad \sigma_4=\begin{pmatrix}1 & 2 & 3\\ 2 & 1 & 3\end{pmatrix},$$

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

即 $S_3 = \{\sigma_1, \sigma_2, \sigma_3, \sigma_4, \sigma_5, \sigma_6\}$包含 6个元素.

在 S_n 中可以按照映射的乘法定义运算.设 σ, τ是 $1, 2, \cdots, n$ 的两个置换，那么我们规定 σ 与 τ 的乘积 $\sigma\tau$ 为将 σ, τ连续作用,即

$$i^{\sigma\tau} = (i^{\sigma})^{\tau}, \quad i = 1, 2, \cdots, n.$$

例如，4 元置换

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix} 与 \tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$$

的乘积为

$$\sigma\tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 2 & 4 \end{pmatrix}.$$

置换的乘法有下述一些性质：

1）满足结合律

$$(\sigma\tau)\rho = \sigma(\tau\rho), \quad \forall \sigma, \tau, \rho \in S_n;$$

2）n元恒等置换

$$e = \begin{pmatrix} 1 & 2 & \cdots & n \\ 1 & 2 & \cdots & n \end{pmatrix}$$

是 S_n的单位元素

$$e\sigma = \sigma e = \sigma, \quad \forall \sigma \in S_n;$$

3）每个 n元置换在 S_n 中都有逆元素

$$\begin{pmatrix} 1 & 2 & \cdots & n \\ \alpha_1 & \alpha_2 & \cdots & \alpha_n \end{pmatrix}^{-1} = \begin{pmatrix} \alpha_1 & \alpha_2 & \cdots & \alpha_n \\ 1 & 2 & \cdots & n \end{pmatrix}.$$

因此，我们有下面的定理.

定理 2 n元置换全体组成的集合 S_n 对置换的乘法构成一个群,称为 n 元对称群,其阶为 $n!$.

需要注意的是，当 $n \geqslant 3$ 时，S_n 是非交换的.例如对上面例子

中的 σ,τ,就有

$$\tau\sigma=\begin{pmatrix}1&2&3&4\\4&2&3&1\end{pmatrix}\neq\sigma\tau.$$

例 1 $S_2=\left\{e,\begin{pmatrix}1&2\\2&1\end{pmatrix}\right\}$ 是一个 2 阶交换群.

例 2 $S_3=\{\sigma_1=e,\sigma_2,\sigma_3,\sigma_4,\sigma_5,\sigma_6\}$($\sigma_i$ 的定义如前)是一个 6 阶非交换群. S_3 的运算可以用下列乘法表给出:

	e	σ_2	σ_3	σ_4	σ_5	σ_6
e	e	σ_2	σ_3	σ_4	σ_5	σ_6
σ_2	σ_2	e	σ_6	σ_5	σ_4	σ_3
σ_3	σ_3	σ_5	e	σ_6	σ_2	σ_4
σ_4	σ_4	σ_6	σ_5	e	σ_3	σ_2
σ_5	σ_5	σ_3	σ_4	σ_2	σ_6	e
σ_6	σ_6	σ_4	σ_2	σ_3	e	σ_5

2 置换的轮换表法

这一小节介绍置换的轮换表法.

首先看几个例子.在 S_3 中,σ_5 将 1 映到 2,2 映到 3,3 映到 1,我们将它表成(1,2,3);σ_2 将 1 保持不变,将 2 映到 3,3 映到 2,我们将它表成(1)(2,3),或简单地表成(2,3).

一般地,如果 n 元置换 σ 把 n 个文字中的一部分 $\alpha_1,\alpha_2,\cdots,\alpha_m$ ($m\leqslant n$)作如下变换:

$$\alpha_1^\sigma=\alpha_2,\quad \alpha_2^\sigma=\alpha_3,\quad \cdots,\quad \alpha_{m-1}^\sigma=\alpha_m,\quad \alpha_m^\sigma=\alpha_1,$$

而把其余 $n-m$ 个文字保持不变,则称 σ 为一个 **m-轮换**,简称轮换,记作

$$\sigma=(\alpha_1,\alpha_2,\cdots,\alpha_m).$$

m称为轮换 σ的长度. 当 $m=1$ 时,σ就是恒等置换. 当 $m=2$ 时,σ 只把两个文字互换,而保持其余的文字不变,称为一个对换.显然有

$$(\alpha_1,\alpha_2,\cdots,\alpha_m)=(\alpha_i,\alpha_{i+1},\cdots,\alpha_m,\alpha_1,\cdots,\alpha_{i-1}),\quad 1<i\leqslant m.$$

两个轮换 $\sigma=(\alpha_1,\alpha_2,\cdots,\alpha_m)$ 与 $\tau=(\beta_1,\beta_2,\cdots,\beta_l)$ 称为不相交的,如果 $\alpha_1,\alpha_2,\cdots,\alpha_m$ 与 $\beta_1,\beta_2,\cdots,\beta_l$ 是各不相同的.

很容易看出,不相交的轮换是可交换的.

定理 3 任何一个置换都可表成一些不相交的轮换的乘积,而且表法(除轮换的次序外)是唯一的.

证明 设 σ 是 $1,2,\cdots,n$ 的一个置换.任取 $1,2,\cdots,n$ 中的一个,设为 α.作序列

$$\alpha=\alpha^{\sigma^0},\alpha^{\sigma^1},\alpha^{\sigma^2},\cdots.$$

因为

$$\alpha^{\sigma^k}\in\{1,2,\cdots,n\}\quad(k=0,1,2,\cdots),$$

因此这个序列一定包含重复的文字.设 α^{σ^m} 是其中第一个在前面出现过的文字,并设它与 α^{σ^i} $(0\leqslant i<m)$相同,于是 $\alpha,\alpha^{\sigma},\cdots,\alpha^{\sigma^{m-1}}$ 各不相同.如果 $i\neq 0$,那么由

$$\alpha^{\sigma^i}=\alpha^m$$

可推出

$$(\alpha^{\sigma^{i-1}})^{\sigma}=(\alpha^{\sigma^{m-1}})^{\sigma},$$

即 σ 将两个不同的文字 $\alpha^{\sigma^{i-1}}$ 与 $\alpha^{\sigma^{m-1}}$ 映到相同的文字,这是不可能的.所以 $i=0$,即 $\alpha^{\sigma^m}=\alpha$.作轮换

$$\sigma_1=(\alpha,\alpha^{\sigma},\cdots,\alpha^{\sigma^{m-1}}),$$

则 σ 与 σ_1 在 $\alpha,\alpha^{\sigma},\cdots,\alpha^{\sigma^{m-1}}$ 上的作用相同.

如果 $m=n$,那么 $\sigma=\sigma_1$ 是一个轮换.如果 $m<n$,在 $1,2,\cdots,n$ 中去掉 $\alpha,\alpha^{\sigma},\cdots,\alpha^{\sigma^{m-1}}$ 后,在剩下的文字中任取一个 β,仿照上面的方法可以得到一个轮换

$$\sigma_2 = (\beta, \beta^{\sigma}, \cdots, \beta^{\sigma^{r-1}}),$$

σ 与 σ_2 在 $\beta, \beta^{\sigma}, \cdots, \beta^{\sigma^{r-1}}$ 上的作用相同. 因为 σ 是一一映射，所以 σ_1 与 σ_2 不相交.

这样继续下去,直到 $1,2,\cdots,n$ 用完为止，我们就得到一些不相交的轮换 $\sigma_1, \sigma_2, \cdots, \sigma_s$,使

$$\sigma = \sigma_1\sigma_2\cdots\sigma_s.$$

表法的唯一性是很明显的. ▌

例 3

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

置换的这种表法称为置换的轮换表法. 如果在置换 σ 的轮换表法中,α 是一个文字组成一个轮换，那么 $\alpha^{\sigma} = \alpha$,即 σ 保持 α 不变. 为了简单起见，在轮换表法中可以把这样的轮换省略不写. 这种简单的表法,称为 σ 的轮换表法的省略形式. 例如,例 3 中 σ 的轮换表法的省略形式为

$$(1,3,5,2)(6,8).$$

恒等置换保持每个文字都不变，我们可以任取一个文字把它表成一个 1-轮换,例如(1). 不过,我们常用 e 表示恒等置换.

应用置换的轮换表法，可以很容易计算置换的阶. 一个长度为 l 的轮换的阶为 l. 一般地,如果 σ 的轮换表法是

$$\sigma = \sigma_1\sigma_2\cdots\sigma_s,$$

其中 σ_i 的长度为 $l_i (i=1,2,\cdots,s)$,那么 σ 的阶等于 $l_1, l_2, \cdots, l_s$ 的最小公倍数$[l_1, l_2, \cdots, l_s]$. 下面我们来证明这个结论.

设 σ 的阶为 d. 记$[l_1, l_2, \cdots, l_s] = m$. 则因

$$\sigma^m = \sigma_1^m\sigma_2^m\cdots\sigma_s^m = e,$$

所以

$$d \mid m.$$

另一方面，因为

$$\sigma^d = \sigma_1^d \sigma_2^d \cdots \sigma_s^d = e,$$

而 $\sigma_1^d, \sigma_2^d, \cdots, \sigma_s^d$ 没有公共文字，故

$$\sigma_1^d = \sigma_2^d = \cdots = \sigma_s^d = e,$$

因此

$$l_i \mid d, \quad i = 1, 2, \cdots, s,$$

由最小公倍数的性质，知 $m \mid d$.

综上得

$$d = m.$$

例 4　试求置换

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 2 & 8 & 6 & 9 & 1 & 12 & 10 & 4 & 5 & 7 & 3 & 11 \end{pmatrix}$$

的阶.

解　因为 σ 的轮换表法为

$$(1, 2, 8, 4, 9, 5)(3, 6, 12, 11)(7, 10).$$

所以 σ 的阶等于 6,4,2 的最小公倍数,为 12.

置换的轮换表法有许多方便的地方，读者将在以后看到轮换表法的一些应用.

3　置换的奇偶性　交错群

因为每个轮换都可表成一些对换的乘积：

$$(\alpha_1, \alpha_2, \cdots, \alpha_m) = (\alpha_1, \alpha_2)(\alpha_1, \alpha_3) \cdots (\alpha_1, \alpha_m).$$

因此，每个置换也都可以表成对换的乘积. 但是，一个置换表成对换的乘积的方法不是唯一的. 例如

$$\sigma=\begin{pmatrix}1&2&3&4&5\\2&3&1&5&4\end{pmatrix}=(1,2,3)(4,5)$$
$$=(1,2)(1,3)(4,5)=(2,3)(1,2)(4,5)$$
$$=(2,3)(1,2)(1,3)(4,5)(1,3).$$

然而，我们可以证明下述定理.

定理 4 n 元置换 σ 表成对换的乘积后，乘积中对换个数的奇偶由 σ 唯一确定，而且与 n 元排列 $1^\sigma,2^\sigma,\cdots,n^\sigma$ 的奇偶一致.

证 明 设 σ 表成 m 个对换的乘积：

$$\sigma=\sigma_1\sigma_2\cdots\sigma_m.$$

我们来证明 m 的奇偶与 n 元排列 $1^\sigma,2^\sigma,\cdots,n^\sigma$ 的奇偶一致. σ 将排列 $1,2,\cdots,n$ 变成排列 $1^\sigma,2^\sigma,\cdots,n^\sigma$，因此将 m 个对换 $\sigma_1,\sigma_2,\cdots,\sigma_m$ 依次连续作用于排列 $1,2,\cdots,n$ 也得到排列 $1^\sigma,2^\sigma,\cdots,n^\sigma$. 我们知道对换改变排列的奇偶，所以作 m 次对换就将排列的奇偶改变 m 次. 由于 $1,2,\cdots,n$ 是一个偶排列，所以排列 $1^\sigma,2^\sigma,\cdots,n^\sigma$ 的奇偶与 m 一致. 因此 m 的奇偶由 σ 唯一确定. ∎

根据这个定理，我们可以定义置换的奇偶性.

定义 5 如果 n 元置换 σ 可以表成奇数个对换的乘积，则称 σ 为奇置换 如果 σ 可以表成偶数个对换的乘积，则称 σ 为偶置换.

由定义可知 如果 $1^\sigma,2^\sigma,\cdots,n^\sigma$ 是一个奇排列，则 σ 是一个奇置换 如果 $1^\sigma,2^\sigma,\cdots,n^\sigma$ 是一个偶排列，则 σ 是一个偶置换.

从定义还知，在 $n!$ 个 n 元置换中，奇、偶置换的个数相同，各有 $\frac{n!}{2}$ 个. 恒等置换是偶置换. 两个偶置换之积是偶置换. 偶置换的

逆置换也是偶置换.

因此有下面的定理.

定理 5 n 元偶置换全体对置换的乘法构成一个群，其阶为 $n!/2$.

以后我们用 A_n 表示全部 n 元偶置换所成的群，称为 n 元交错群.

4 置换群

最后来讨论置换群.

由 n 元置换组成的群称为 n 元置换群，简称置换群. 例如，n 元对称群及 n 元交错群都是 n 元置换群. 我们还可举出一些例子，这些例子在以后的讨论中还会用到.

例 5 $G=\{e,(1,2,3),(1,3,2)\}$是一个 3元置换群，它的阶等于 3.

例 6 $G=\{e,(1,2)(3,4),(1,3)(2,4),(1,4)(2,3)\}$是一个 4 阶 4元置换群.

例 7 $G=\{e,(1,2),(3,4),(1,2)(3,4),(1,3)(2,4),(1,4)(2,3),(1,3,2,4),(1,4,2,3)\}$是一个 8 阶 4 元置换群.

例 8 仅由恒等置换组成的群也是一个置换群.

为了确切起见，我们称一个置换实际变动的文字个数为这个置换的次数，而称一个置换群实际变动的文字个数为这个群的次