第 6 章　群

前述章节的初等数论主要关注整数、素数、同余等基本性质及其在数学问题中的应用，而后续章节的近世（抽象）代数则迈向了更为抽象与结构化的代数系统研究. 这一转变不仅极大地丰富了数学的研究内容，还提供了更为强大的工具和方法，使得数学能够更深入地探索抽象结构和它们之间的内在联系，为现代数学的发展奠定了坚实的基础.

近世代数的起源与代数方程的求根问题密切相关. 伽罗瓦（Galois）等数学家在研究代数方程的解的过程中，特别是长期困扰数学界的关于高次方程（如 5 次及以上方程）是否存在根式解的问题，提出了群论的思想. 这一思想不仅为代数方程的求解提供了新的视角和方法，还引起代数研究方法和思维方式的深刻变革，逐步发展成为代数研究的主流方法. 后来，随着数学家们对群、环、域等代数结构研究的不断深入，抽象代数逐渐形成了一个完整的数学体系.

本章将从群的定义入手，逐步揭开近世代数的神秘面纱.

本章的知识要点：

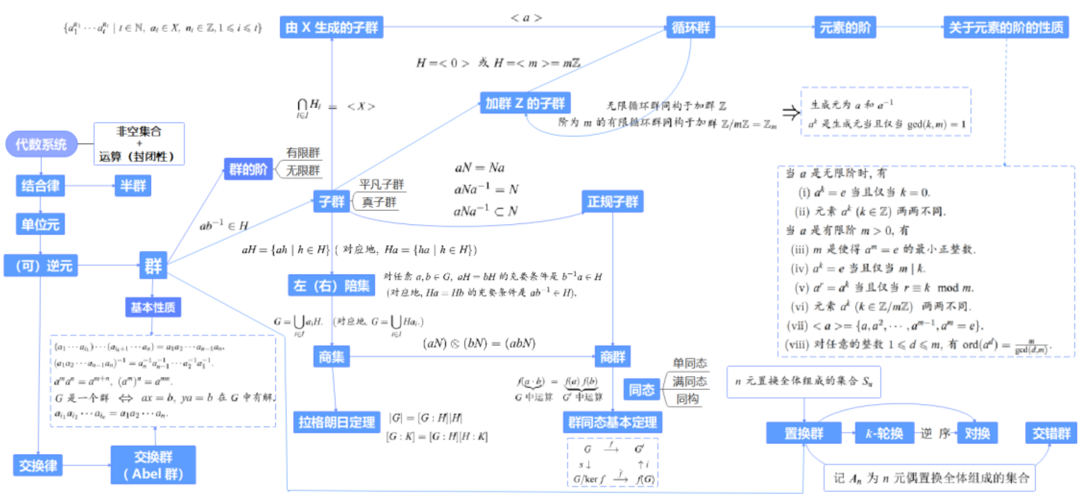

图 6-1 群知识点图谱

6.1 群的定义与性质

首先，给出集合中关于运算的表达.

定义 6.1.1 设 S 是一个非空集合. 那么 $S\times S$ 到 S 的<u>映射</u>叫做 S 的**结合法**或**运算**：

$$S\times S\to S$$
$$(a,b)\to ab$$

注：此时，我们称映射满足封闭性.

对于这个映射，元素对(a, b) 的像叫做 a 与 b 的**乘积**，记作 $a\otimes b$ 或 $a\cdot b$ $a \bullet b$ 或 $a*b$ 等. 为方便起见，该乘积简记为 ab，这个运算叫做**乘法**.

我们常常也把这个运算叫做加法，元素对(a, b)的像叫做 a 与 b 的**和**，记成 $a\oplus b$ 或 $a+b$. 这时 S 叫做**代数系统**.

例 6.1.1 自然数集 $N=\{1,2,\cdots,n,\cdots\}$

① 定义“+”：普通加法，$\forall a,b\in N, a+b\in N$

所以，“+”是 $N\times N$ 到 N 的运算，或称 N 对映射“+”满足封闭性.

② 定义“$\bullet$”：普通乘法，$\forall a,b\in N, a\bullet b\in N$

称 N 对映射“$\bullet$”满足封闭性.

③ 定义“-”：普通减法，

$a=2,b=5,a-b=-3\notin N$，所以，N 对映射“-”不满足封闭性.

定义 6.1.2 设 S 是一个具有运算的非空集合. 如果 a，b，c 都是 S 中的元素，则我们有两种方式得到它们的乘积 $(ab)c$ 和 $a(bc)$，如果对 S 中的任意元素 a，b，c，都有

$$(ab)c=a(bc),$$

则称该运算满足**结合律**.

例 6.1.2 对于 A={所有整数}，

运算+：普通加法，则 $(a+b)+c=a+(b+c)$, 满足结合律；

运算-：普通减法，则 $(a-b)-c\neq a-(b-c)$, 不满足结合律，除非 c=0.

例 6.1.3 对集合 $\{a,b,c\}$，定义 ○ 运算如下

○	**a**	**b**	**c**
a	a	b	c
b	c	b	a
c	b	a	c

验证是否满足结合律？

解：$(xy)z=x(yz)$ 共需验证 $3\times 3\times 3=27$ 个

（i）$(a\circ b)\circ c=b\circ c=a$ ； $a(b\circ c)=a\circ a=a$.

（ii）$(b\circ a)\circ c = c\circ c = c$； $b\circ(a\circ c) = b\circ c = a$.

所以，不满足结合律.

定义 6.1.3 设 S 是一个具有运算的非空集合. 如果 S 满足结合律，那么 S 叫做 S 的**半群**.

定义 6.1.4 设 S 是一个具有运算的非空集合，如果 S 中的一个元素 e，使得对 S 中所有元素 a,

$$ea = ae = a$$

都成立，则称该元素 e 为 S 中的**单位元**.

注：当 S 的运算写作加法时，这个 e 叫做 S 中的零元，通常记作 0.

性质 6.1.1 设 S 是一个具有运算的非空集合，则 S 中的单位元 e 是唯一的.

证 设 e 和 e' 都是 S 中的单位元. 分别根据 e 和 e' 的单位元定义，得到

$$e' = ee' = e.$$

因此，单位元是唯一的.

例 6.1.4 对 $N=\{a,b,c\}$，运算为 ○

○	**a**	**b**	**c**
a	a	b	c
b	b	c	a
c	c	a	b

则，看出元素 a 为 N 中的单位元. 因为

$$a\circ a = a,\quad a\circ b = b,\quad a\circ c = c$$
$$b\circ a = a,\quad c\circ a = c$$

定义 6.1.5 设 S 是一个具有运算的有单位元的非空集合. 设 a 是 S 中的一个元素. 如果 S 中存在一个元素 a' 使得

$$aa' = a'a = e$$

则称该元素 a 为 S 中的**可逆元**，a' 称为 a 的**逆元**，通常记作 a^{-1}.

注：当 S 的运算叫做加法时，这个 a' 叫做元素 a 的**负元**，通常记作 $-a$.

性质 6.1.2 设 S 是一个有单位元的半群. 则对 S 中任意可逆元 a, 其逆元 a' 是唯一的.

证 设 a' 和 a'' 都是 a 的逆元，即

$$aa' = a'a = e, \qquad aa'' = a''a = e.$$

分别根据 a' 和 a'' 是 a 的逆元, 及结合律，得到

$$a' = a'e = a'\left(aa''\right) = \left(a'a\right)a'' = ea'' = a''.$$

因此，a 的逆元 a' 是唯一的.

例 6.1.5 对 $N = \{a,b,c\}$，运算为 $\circ$

$\circ$	***a***	***b***	***c***
a	a	b	c
b	b	c	a
c	c	a	b

则看出元素 a 为 N 中的单位元，

有：$b \circ c = a, \quad c \circ b = a \qquad \therefore b^{-1} = c$.

定义 6.1.6 设 S 是一个具有运算的非空集合. 如果 a, b 都是 S 中的元素，则我们有两种方式得到它们的乘积 ab 和 ba . 如果对 S 中的任意元素 a，b，都有

$$ab = ba,$$

则称该运算满足**交换律**.

例 6.1.6 设 S 是矩阵集合，定义“×”为矩阵乘法，则对 $\forall A, B \in S$ 不总能有 $AB = BA$.

如：

$$A = (1,2), \ B = \begin{pmatrix} 1 \\ 3 \end{pmatrix}$$

$$A \times B = (1,2)\begin{pmatrix} 1 \\ 3 \end{pmatrix} = 1\times1 + 2\times3 = 7.$$

$$B \times A = \begin{pmatrix} 1 \\ 3 \end{pmatrix}(1,2) = \begin{pmatrix} 1 & 2 \\ 3 & 6 \end{pmatrix}$$

即，运算“×”不满足交换律.

定义 6.1.7 设 G 是一个具有运算的非空集合. 如果这个运算满足如下三个条件：

(i) 结合律，即对任意的 $a,b,c \in G$，都有

$$(ab)c = a(bc).$$

(ii) 单位元，即存在一个元素 $e \in G$，使得对任意的 $a \in G$，都有

$$ea = ae = a.$$

(iii) 可逆性，即对任意的$a \in G$，都存在$a' \in G$，使得

$$aa' = a'a = e.$$

那么，G 叫做一个**群**.

注：群满足封闭性、结合律、单位元、逆元.

特别地，当 G 的运算写作乘法时，G 叫做**乘群**；当 G 的运算写作加法时，G 叫做**加群**.

定义 6.1.8 群 G 的元素个数叫做群 G 的**阶**，记作$|G|$.

当$|G|$为有限数时，G 叫做**有限群**，否则，G 叫做**无限群**.

定义 6.1.9 如果群 G 中的运算还满足交换律，即对任意的$a,b \in G$，都有$ab = ba$，那么 G 叫做一个**交换群**或阿贝尔(Abel)群.

注：阿贝尔群是 Camille Jordan 以挪威数学家尼尔斯·阿贝尔命名的.

例 6.1.7 (1) 自然数集 N，运算"+"则

(i) 满足封闭性.

(ii) 具有结合律.

(iii) 没有零元和负元.

所以，N 对"+"是半群.

(2) 自然数集 $N = \{1, 2, \cdots, n, \cdots\}$，映射"•"为普通乘法，则

(i) 满足封闭性.

(ii) 满足结合律.

(iii) 有单位元 1.

(iv) 没有逆元, 因为对$\forall a \in N$，没有a'，使得$a \bullet a' = 1$.

例 6.1.8 请回答：

(1) 整数集$Z = \{\cdots, -n, \cdots -2, -1, 0, 1, 2, \cdots, n, \cdots\}$对于通常意义下的加法，构成交换群吗？

(2) 对$Z^* = Z \setminus \{0\} = \{\cdots, -n, \cdots -2, -1, 1, 2, \cdots, n, \cdots\}$对"•"是通常意义下的乘法，构成群？

答：对于问题(1)：

(i) 满足封闭性: $\forall a, b \in Z, a + b \in Z$.

(*ii*) 满足结合律: $\forall a,b,c\in Z,(a+b)+c=a+(b+c)$.

(*iii*) 有零元 0 : $\forall a\in Z,a+0=0+a=a$.

(*iv*) 有负元: $\forall a\in Z,\exists -a\in Z,a+(-a)=(-a)+a$.

(*v*) 满足交换律: $\forall a,b\in Z,a+b=b+a$.

所以是一个交换加群.

对于问题(2)：

(*i*) 满足封闭性: $\forall a,b\in Z^*,a\bullet b\in Z^*$.

(*ii*) 满足结合律: $\forall a,b,c\in Z^*,(a\bullet b)\bullet c=a\bullet(b\bullet c)$.

(*iii*) 有单位元 1: $\forall a\in Z^*,a\bullet 1=1\bullet a=a$.

(*iv*) 没有逆元: $\forall a\in Z^*,\text{不存在}a'\in Z^*,\text{使得}a\bullet a'=a'\bullet a=1$.

例 6.1.9 有理数集 *Q*，实数集 *R* 和复数集 *C*,

（1）对于通常意义下的加法，（封闭、结合律、单位元 0，逆元-*a*），是交换加群.

（2） 对于"$\bullet$"，普通意义下的乘法， $Q^*=Q\setminus\{0\}$， $R^*=R\setminus\{0\}$和$C^*=C\setminus\{0\}$，满足封闭性，结合律，单位元 1，逆元$a^{-1}=\dfrac{1}{a}$.

因此Q^*， R^*和C^*都是交换乘群.

例 6.1.10 设 *D* 是一个非平方整数，则集合 $Z\left(\sqrt{D}\right)=\left\{a+b\sqrt{D}\mid a,b\in Z\right\}$:

（1）对于加法运算$\oplus$：

$$\left(a+b\sqrt{D}\right)\oplus\left(c+d\sqrt{D}\right)=(a+b)+(b+d)\sqrt{D},$$

验证：

(*i*) 封闭性: $\forall A,B\in Z\left(\sqrt{D}\right),A\oplus B\in Z\left(\sqrt{D}\right)$.

(*ii*) 结合律: $\forall A,B,C\in Z\left(\sqrt{D}\right),(A\oplus B)\oplus C=A\oplus(B\oplus C)$.

(*iii*) 有单位元 0.

(*iv*) 负元: $\forall A=a+b\sqrt{D}\in Z\left(\sqrt{D}\right),A^{-1}=-A=-a-b\sqrt{D}$.

此外满足交换律， 所以$Z\left(\sqrt{D}\right)$对"+"构成一个交换群(Abel 群).

（2）对于乘法运算$\otimes$:

$$\left(a+b\sqrt{D}\right)\otimes\left(c+d\sqrt{D}\right)=\left(ac+bdD\right)+\left(bc+ad\right)\sqrt{D}$$

验证：

(i) 满足封闭性.

(ii) 满足结合律.

(iii) 单位元为 1，即：c=1, d=0, 有

$$\begin{cases} ac+bdD=a \\ bc+ad=b \end{cases}，即单位元为 1.$$

(iv) 至于逆元, 根据

$$\begin{cases} ac+bdD=1 \\ bc+ad=0 \end{cases}，求出 c 与 d.$$

由 $c=-\dfrac{ad}{b}$ 代入， 有 $\dfrac{-a^2d}{b}+bDd=1$.

所以 $\dfrac{-a^2d+b^2D}{b^2}d=1$， 所以 $d=\dfrac{1}{\dfrac{-a^2+b^2D}{b^2}}$.

因为 d 是整数，所以 $\dfrac{-a^2+b^2D}{b^2}=1$.

所以 $-a^2+b^2D=b^2$ ，即 $b^2D=b^2+b^2$.

所以 $D=\dfrac{b^2+a^2}{b^2}=1+(\dfrac{a}{b})^2$ 不是整数，矛盾. 故无逆元.

所有，不构成一个乘群.

例 6.1.11 设 n 是一个正整数，设 $Z/nZ=\{0,1,2,\cdots,n-1\}$，证明：集合 Z/nZ 对于加法

$$a\oplus b=\left(a+b\left(\bmod n\right)\right)$$

构成一个交换加群，其中 $a\left(\bmod n\right)$ 是整数 a 模 n 的最小非负剩余.

证 满足：

(i) 封闭性.

(ii) 结合律.

(iii) 有单位元(零元 0).

(iv) 可逆性(有负元):

$$\forall a\in Z/nZ,\exists n-a\in Z/nZ,\text{使得}a\oplus\left(n-a\right)\equiv 0\left(\bmod n\right).$$

所以是交换加群.

例如，对于 $Z_6=Z/6Z=\{0,1,2,3,4,5\}$：

$a\setminus b$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

注：$Z_n=Z/nZ=\{0,1,2,\cdots,n-1\}$ 叫做**模 *n* 剩余类加群**. 其中：$nZ=\{n,2n,3n,\cdots\}$， 如 $2Z=\{\cdots,-2,0,2,4,6\cdots\}$.

例 6.1.12 设 p 是一个素数， $F_p=Z/pZ$. 设 $F_p^*=F_p\setminus\{0\}$. 证明：集合 F_p^* 对于乘法

$$a\otimes b=(ab(\bmod p))$$

构成一个交换乘群.

证 满足：

(i) 封闭性. (ii) 结合律.

(iii) 有单位元 1. (iv) 交换律成立.

(v) 可逆性，任意元素有逆元.

事实上，根据定理 2.2.9 若 m 是一个正整数，a 满足 $(a,m)=1$，则存在整数 a'，$1\le a'<m$，使得 $aa'\equiv 1(modm)$，所以有

$$F_p^*=\{1,2,\cdots,p-1\}\ \forall a\in F_p^*,(a,p)=1\quad \therefore \exists a'\in F_p^*,\text{使得}aa'=1(\bmod m).$$

所以是交换乘群.

例如，对于 p=7：

$a \setminus b$	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	4	6	1	3	5
3	3	6	2	5	1	4
4	4	1	5	2	6	3
5	5	3	1	6	4	2
6	6	5	4	3	2	1

例 6.1.13 设 n 是一个合数，证明：集合 $Z/nZ\setminus\{0\}$ 对于乘法

$$a \otimes b = (ab(\bmod n))$$

不构成一个乘群.

证明：单位元是 1，但 n 的真因数 d 没有逆元.

例如：n=6，即 $Z_6^* = Z/6Z\setminus\{0\} = \{1,2,3,4,5\}$

则 $1^{-1}=1;\quad 5^{-1}=5;\qquad 2^{-1}, 3^{-1}, 4^{-1}$不存在

$a \setminus x$	1	2	3	4	5
1	1	2	3	4	5
2	2	4	0	2	4
3	3	0	3	0	3
4	4	2	0	4	2
5	5	4	3	2	1

例 6.1.14 设 n 是一个合数，设 $(Z/nZ)^* = \{a \mid a \in Z/nZ, (a,n)=1\}$，则：

集合 $(Z/nZ)^*$ 对于乘法

$$a \otimes b = (ab(\bmod n))$$

构成一个交换乘群.

证明：具有结合律，单位元是 1，a 的逆元是 $a^{-1}(\bmod n)$.

例如：n=15，

$a \setminus x$	1	2	4	7	8	11	13	14
1	1	2	4	7	8	11	13	14
2	2	4	8	14	1	7	11	13
4	4	8	1	13	2	14	7	11
7	7	14	13	4	11	2	1	8
8	8	1	2	11	4	13	14	7
11	11	7	14	2	13	1	8	4
13	13	11	7	1	14	8	4	2
14	14	13	11	8	7	4	2	1

例 6.1.15 元素在数域 K 中的全体 n 级可逆矩阵对于矩阵的乘法成一个群，这个群记为 $GL_n(K)$，称为 n 级**一般线性群**；

$GL_n(K)$ 中全体行列式为 1 的矩阵对于矩阵乘法也成一个群，这个群记为 $SL_n(K)$，称为**特殊线性群**.

下面讨论 n 个元素的乘积.

设 $a_1, a_2, \cdots, a_{n-1}, a_n$ 是群 G 中的 n 个元素. 通常归纳地定义这 n 个元素的乘积为

$$a_1 a_2 \cdots a_{n-1} a_n = (a_1 a_2 \cdots a_{n-1}) a_n .$$

即：两两运算.

当 G 的运算叫做加法时，通常归纳地定义这 n 个元素的和为

$$a_1 + a_2 + \cdots + a_{n-1} + a_n = (a_1 + a_2 + \cdots + a_{n-1}) + a_n .$$

性质 6.1.3 设 $a_1, a_2, \cdots, a_{n-1}, a_n$ 是群 G 中的任意 $n \geq 2$ 个元素，则对任意的 $1 \leq i_1 < \cdots < i_k < n$，有 $(a_1 \cdots a_{i_1}) \cdots (a_{i_k+1} \cdots a_n) = a_1 a_2 \cdots a_{n-1} a_n$.

证 数学归纳法

对 n 作数学归纳法

n=3 时，根据结合律得到 $a_1(a_2 a_3) = (a_1 a_2) a_3 = a_1 a_2 a_3$，结论成立.

假设 n-1 时，结论成立.

对于 n，如果 $i_{k+1} = n$，则根据归纳假设，

$$\left(a_1\cdots a_{i_1}\right)\cdots\left(a_{i_k+1}\cdots a_n\right)=\left(a_1a_2\cdots a_{n-1}\right)a_n=a_1a_2\cdots a_{n-1}a_n$$

如果$i_{k+1}<n$，则根据归纳假设和结合律，

$$\begin{aligned}\left(a_1\cdots a_{i_1}\right)\cdots\left(a_{i_{k-1}+1}\cdots a_{i_k}\right)\left(a_{i_k+1}\cdots a_n\right)&=\left(a_1\cdots a_{i_k}\right)\left(a_{i_k+1}\cdots a_{n-1}\right)a_n\\&=\left(a_1a_2\cdots a_{n-1}\right)a_n\\&=a_1a_2\cdots a_{n-1}a_n\end{aligned}$$

因此，结论对于 n 成立. 根据数学归纳法原理，结论对任意 n 成立.

性质 6.1.4 设$a_1,a_2,\cdots,a_{n-1},a_n$是交换群 G 中的任意$n\geq 2$个元素，则

$$(a_1\ a_2\ldots a_{n-1}\ a_n)^{-1}=a_n^{-1}\ a_{n-1}^{-1}\ldots a_2^{-1}\ a_1^{-1}.$$

证 数学归纳法（略）.

性质 6.1.5 设$a_1,a_2,\cdots,a_{n-1},a_n$是交换群 G 中的任意$n\geq 2$个元素，则对 1, 2, …, n 的任一排列$i_1,i_2,\cdots,i_n$，有

$$a_{i_1}a_{i_2}\cdots a_{i_n}=a_1a_2\cdots a_n.$$

证 数学归纳法.

n=2 时，根据交换得到$a_2a_1=a_1a_2$，结论成立.

假设 n-1 时，结论成立，

对于 n，如果$i_n=n$，则根据结合律和归纳假设，

$$a_{i_1}\cdots a_{i_{n-1}}a_{i_n}=\left(a_{i_1}\cdots a_{i_{n-1}}\right)a_{i_n}=\left(a_1a_2\cdots a_{n-1}\right)a_n=a_1a_2\cdots a_{n-1}a_n.$$

如果$i_n<n$，$i_k=n$，则根据结合律，交换律及前面的结果，

$$\begin{aligned}a_{i_1}\cdots a_{i_k-1}a_{i_k}a_{i_k+1}\cdots a_{i_n}&=\left(a_{i_1}\cdots a_{i_k-1}\right)a_n\left(a_{i_k+1}\cdots a_{i_n}\right)\\&=\left(a_{i_1}\cdots a_{i_k-1}\right)\left(a_{i_k+1}\cdots a_{i_n}\right)a_n.\\&=a_1a_2\cdots a_{n-1}a_n\end{aligned}$$

因此，结论对于 n 成立. 根据数学归纳法原理，结论对于任意 n 成立.

定义 6.1.10 设 n 是正整数，如果$a_1=a_2=\cdots=a_n=a$，则记$a_1a_2\cdots a_n=a^n$称之为 a 的 n 次幂.

特别地，定义$a^0=e$为单位元，$a^{-n}=\left(a^{-1}\right)^n$为逆元$a^{-1}$的 n 次幂.

性质 6.1.6 设 a 是群 G 中的任意元，则对任意的整数 m，n，我们有

$$a^m a^n = a^{m+n}, \qquad \left(a^m\right)^n = a^{mn}.$$

证 我们分如下几种情况证明：

(i) $m>0, n>0$，根据性质 6.1.4，有

$$a^m a^n = a^{m+n}, \left(a^m\right)^n = a^{mn}.$$

(ii) $m=0, n>0$，有

$$a^m a^n = ea^n = a^{m+n}, \left(a^m\right)^n = \left(a^0\right)^n = e = a^{mn}.$$

(iii) $m<0, n>0$，有

$$a^m a^n = \left(a^{-1}\right)^{-m} a^n = \begin{cases} \left(a^{-1}\right)^{-m} a^{-m} a^{n-(-m)} = a^{n-(-m)} = a^{m+n} & \text{如果} -m<n \\ e = a^{m+n} & \text{如果} -m=n \\ \left(a^{-1}\right)^{-m-n} = a^{m+n} & \text{如果} -m>n \end{cases}.$$

$$\left(a^m\right)^n = \left(\left(a^{-1}\right)^{-m}\right)^n = \left(a^{-1}\right)^{-mn} = a^{mn}.$$

（iv）$n=0$，有 $a^m a^n = a^m e = a^m = a^{m+n}$, $\quad \left(a^m\right)^n = e = a^{mn}$.

(v) $m>0,\quad n<0$，有

$$a^m a^n = a^m \left(a^{-1}\right)^{-n} = \begin{cases} a^{m-(-n)} = a^{m+n} & \text{如果} m>-n \\ e = a^{m+n} & \text{如果} m=-n \\ \left(a^{-1}\right)^{-n-m} = a^{m+n} & \text{如果} m<-n \end{cases}.$$

$$\left(a^m\right)^n = \left(\left(a^m\right)^{-1}\right)^{-n} = \left(\left(a^{-1}\right)^m\right)^{-n} = \left(a^{-1}\right)^{-mn} = a^{mn}.$$

（vi）$m<0, n<0$，有

$$a^m a^n = \left(a^{-1}\right)^{-m} \left(a^{-1}\right)^{-n} = \left(a^{-1}\right)^{-m-n} = a^{m+n}.$$

$$\left(a^m\right)^n = \left(\left(a^m\right)^{-1}\right)^{-n} = \left(a^{-m}\right)^{-n} = a^{mn}.$$

因此，结论成立.

定理 6.1.1 设 G 是一个具有运算的非空集合. 如果 G 是一个群，则方程

$$ax=b, \quad ya=b$$

在 G 中有解. 反过来，如果上述方程在 G 中有解，并且运算满足结合律，则 G 是一个群.

证：$\Rightarrow$ 设 G 是一个群. 在方程 $ax=b$ 两端左乘 a^{-1}，得到

$$a^{-1}(ax)=a^{-1}b\ ,$$

即 $x=a^{-1}b$ 是方程 $ax=b$ 的解．同理， $y=ba^{-1}$ 是方程 $ya=b$ 的解.

$\Leftarrow$ 由已知，

1) 封闭性满足；

2) 结合律成立；

3) 有单位元：设方程 $ax=b, ya=b$ 在 G 中有解.

因为 G 非空，所以 G 中有元素 c, 并且 $cx=c$ 有解 $x=e_r$.

这个 e_r 是 G 中的（右）单位元.

事实上，对任意 $a\in G$，因为 $yc=a$ 有解，所以

$$ae_r=(yc)e_r=y(ce_r)=yc=a\ .$$

同理， $yc=c$ 的解 $y=e_l$ 是 G 中的（左）单位元.

事实上，对任意 $a\in G$，因 $cx=a$， $yc=a$ 有解，所以

$$e_l a=e_l(cx)=(e_l c)x=cx=a\ .$$

因此， $e_r=e_l e_r=e_l=e$ 是 G 中的单位元.

4) 有逆元：对 G 中任意元素 a，

设方程 $ax=e$， $ya=e$ 在 G 中的解分别为 $x=a', y=a''$．则

$$a'=ea'=(a''a)a'=a''(aa')=a''e=a''\ .$$

因此， a' 是 a 在 G 中的唯一逆元.

因此，G 是一个群.

6.2 子群

6.2.1 子群的定义与性质

讨论具有运算的子集合.

定义 6.2.1 设 H 是群 G 的一个子集合，如果对于群 G 的运算，H 成为一个群，那么 H 叫做群 G 的子群，记作 $H\le G$.

$H=\{e\}$ 和 $H=G$ 都是群 G 的子群，叫做群 G 的**平凡子群**.

群 G 的子群 H 叫做群 G 的**真子群**，如果 H 不是群 G 的平凡子群.

例 6.2.1 设 n 是一个正整数，运算为+，则 $nZ=\{nk\mid k\in Z\}$ 是 Z 的子群.

证：(0) nZ 是 Z 的一个子集合

（下证，nZ 对 Z 的运算“+”满足 4 条）

(1) 封闭性 $\forall nk_1,nk_2\in nZ,nk_1+nk_2=n(k_1+k_2)\in nZ,k_1+k_2\in Z$.

(2) 结合律 因为 Z 是群，所以运算“+”在 Z 中满足结合律. nZ 是 Z 的一个子集合，所以在 nZ 集合中，运算“+”仍然满足结合律.

(3) 单位元（零元）0. 因为 $0\in nZ$，有 $nk+0=0+nk=nk$.

事实上，群与子群的单位元是同一个

$$\forall nk\in Z,nk+0=0+nk$$
$$n(k+0)=(0+k)n$$

所以，0 是 Z 中的单位元， 0+k=k+0=k.

(4) 逆元： $\forall nk\in Z$,

$\because k\in Z,Z$为群$,\therefore \exists$-$k\in Z$，使得$k+(-k)=(-k)+k=0$.

对于 $nk\in nZ$，$\exists n(\text{-}k)\in nZ$,

使得 $nk+n(-k)=n(-k)+nk=n[k+(-k)]=n\cdot 0=0$.

综上，$nZ=\{nk\mid k\in Z\}$ 是 Z 的子群.

定理 6.2.1 设 H 是群 G 的一个非空子集合，则 H 是群 G 的子群的充要条件是：对任意的 $a,b\in H$，有 $ab^{-1}\in H$.

证 $\Rightarrow$ 必要性是显然的.

（对任意的 $a,b\in H$，因为 H 是群，b^{-1} 存在且 $b^{-1}\in H$，

再由群的封闭性，$ab^{-1}\in H$ 成立）

$\Leftarrow$ (证明 H 是群 G 的子群，下证 4 条)

(1) 结合律: 结合律在 G 中成立，在 H 中自然成立.

(2) 单位元: 因为 H 非空，所以 H 中有元素 a.

根据假设，我们有 $e=aa^{-1}\in H$. 因此，H 中有单位元 e.

(3) 对于任意 $a\in H$，由 $e\in H$，再应用假设，我们有 $a^{-1}=ea^{-1}\in H$，即 H 中每个元素 a 在 H 中有逆元.

(4) 封闭性: 对任意的 $a,b\in H$，由(3)可知 $b^{-1}\in H$，再应用假设，有

$a(b^{-1})^{-1}\in H$，由于 ab=$a(b^{-1})^{-1}$ ，所以 $ab\in H$.

因此，H 是群 G 的子群.

例 6.2.2 证明群 G 的两个子群的交集也是 G 的子群.

证 设 G 的两个子群 H_1与H_2.要证 $H_1 \bigcap H_2$ 是 G 的子群，只需证

$$ab^{-1} \in H_1 \bigcap H_2; \forall a,b \in H_1 \bigcap H_2 .$$

令 $\forall a,b \in H_1 \bigcap H_2$,

$\therefore a \in H_1, b \in H_1, a \in H_2, b \in H_2$.

又因为 H_1 是子群，H_2 是子群，

所以 $ab^{-1} \in H_1$，$ab^{-1} \in H_2$.

所以 $ab^{-1} \in H_1 \bigcap H_2$,

所以 $H_1 \bigcap H_2$ 是 G 的子群.

例 6.2.3 设 G 是一个群，$\left\{H_i\right\}_{i\in I}$ 是 G 的一族子群. 则 $\cap_{i\in I} H_i$ 是 G 的一个子群.

证明：对任意的 $a,b \in \cap_{i\in I} H_i, i \in I$.

因为 H_i 是 G 的子群，根据定理 6.2.1，我们有 $ab^{-1} \in H_i, i \in I$.

进而，$ab^{-1} \in \cap_{i\in I} H_i$，根据定理 6.2.1，$\cap_{i\in I} H_i$ 是 G 的一个子群.

定义 6.2.2 设 G 是一个群，X 是 G 的子集，设 $\left\{H_i\right\}_{i\in I}$ 是 G 的包含 X 的所有子集. 则 $\cap_{i\in I} H_i$ 叫做 G 的由 X **生成的子群**. 记为 $< X >$.

X 的元素称为子群 $< X >$ 的**生成元**. 如果 $X = \left\{a_1, \cdots, a_n\right\}$，则记为 $< X >$ 为 $< a_1, \cdots, a_n >$.

如果 $G =< a_1, \cdots, a_n >$，则称 G 为**有限生成的**. 特别地，如果 $G =< a >$，则称 G 为 a 生成的**循环群**.

定义 6.2.3 若群 G 的每一个元都能表示成一个元素 g 的方幂，则 G 称为由 g 生成的**循环群**，记作 $G =< g >$，g 称为循环群 G 的生成元.

循环群 $G =< g >$ 共有两种类型:

(1) 无限阶循环群 G.

(2) 由 g 所生成的 n 阶循环群.

设 $G =< g >= \left\{g^r \mid g^r \neq 1,\quad 0 \le r < n,\quad g^n = 1\right\}$

$$=\left\{1,g,g^2,g^3,\cdots g^{n-1}\right\}.$$

则 G 是 n 阶循环群. 其中, 单位元为 1, g^r 的逆元为 g^{n-r}, $g^{n\text{-}r}=g^n g^{-r}=1g^{-r}=g^{-r}$.

例 6.2.4 设 $G=<g>=\left\{g^r \mid g^r\neq 1, 0\le r<n, g^n=1\right\}$, G 是 n 阶循环群, 则 $<g^d>=\left\{g^{dk}\mid k\in Z\right\}$是 G 的子群.

证明:(i) 非空 k=0, $1\in<g^d>$

(ii) $\forall a=g^{dk_1}, b=g^{dk_2}\in<g^d>$, 则

$b^{-1}=g^{-dk_2}=g^{d(-k_2)}$,

$ab^{-1}=g^{dk_1}g^{d(-k_2)}=g^{d(k_1-k_2)}\in<g^d>$.

所以, $<g^d>=\left\{g^{dk}\mid k\in Z\right\}$是 G 的子群.

6.2.2 正规子群和商群

群的正规子群是一种重要的子群,它在群论中起着很重要的作用,从群的正规子群还可以构造出新的群,即商群:在讨论正规子群、商群之前,先给出陪集的概念.

定义 6.2.4 设 H 是 G 的子群,a 是 G 中任意元. 那么集合 $aH=\left\{ah\mid h\in H\right\}$(对应地 $Ha=\left\{ha\mid h\in H\right\}$)分别叫做 G 中 H 的左(右)**陪集**.

其中:

(1) aH(对应地 Ha)中的元素叫做 aH(对应地 Ha)的代表元.

(2) 如果 aH=Ha, aH 叫做 G 中 H 的**陪集**.

例 6.2.5 设 $n>1$ 是整数. 则 $H=nZ$ 是 Z 的子群,子集

$a+nZ=\left\{a+nk\mid k\in Z\right\}$ 就是 nZ 的一个陪集.

定理 6.2.2 设 H 是群 G 的子群,则

(i) 对任意 $a\in G$, 有 $aH=\left\{c\mid c\in G, c^{-1}a\in H\right\}$(对应地 $Ha=\left\{c\mid c\in G, ac^{-1}\in H\right\}$);

(ii) 对任意 $a,b\in G$, $aH=bH$ 的充要条件是 $b^{-1}a\in H$(对应地 $Ha=Hb$ 的充要条件 $ab^{-1}\in H$);

(iii) 对任意 $a,b\in G$，$aH\cap bH=\varnothing$ 的充要条件是 $b^{-1}a\notin H$（对应地 $Ha\cap Hb=\varnothing$ 的充要条件 $ab^{-1}\notin H$）；

(iv) 对任意 $a\in H$，有 $aH=H=Ha$.

证 (i) 令 $H_{al}=\left\{c\,|\,c\in G,c^{-1}a\in H\right\}$，要证明：$aH=H_{al}$，

i）对任意的 $c\in aH$（当然 $c\in G$），存在 $h\in H$ 使得 $c=ah$.

从而，$c^{-1}a=h^{-1}\in H$.

由定义 $H_{al}=\left\{c\,|\,c\in G,c^{-1}a\in H\right\}$，即 $c\in H_{al}$，因此 $aH\subset H_{al}$.

ii）反过来，对任意 $c\in H_{al}$，有 $c^{-1}a\in H$，

从而存在 $h\in H$，使得 $c^{-1}a=h$，

由此，$c=ah^{-1}\in aH$，因此，$H_{al}\subset aH$.

综上，故 $aH=\left\{c\,|\,c\in G,c^{-1}a\in H\right\}$.

同理可得，$Ha=\left\{c\,|\,c\in G,ac^{-1}\in H\right\}$.

(ii) $\Rightarrow$ 设 $aH=bH$，则 $b=be\in bH=aH$，

故 $\exists h$，使得 $b=ah$，所以 $b^{-1}a=h^{-1}\in H$.

$\Leftarrow$ 反过来，设 $b^{-1}a=h_1\in H$，

对任意 $c\in aH$，存在 $h_2\in H$ 使得 $c=ah_2$.

进而 $c=b\left(b^{-1}a\right)h_2=b\left(h_1h_2\right)\in bH$，因此，$aH\subset bH$.

同样，对任意 $c\in bH$，存在 $h_3\in H$ 使得 $c=bh_3$，

进而 $c=a\left(b^{-1}a\right)^{-1}h_3=a\left(h_1^{-1}h_2\right)\in aH$，因此，$bH\subset aH$，

综上，有 $aH=bH$.

同理可得，$Ha=Hb$ 的充要条件 $ab^{-1}\in H$.

(iii) $\Rightarrow$ 由(ii)知必要性成立.

$\Leftarrow$ 再证充分性. 反证法.

假设 $aH\cap bH\neq\varnothing$，则存在 $c\in aH\cap bH$.

根据(i)，我们有 $c^{-1}a\in H$ 及 $c^{-1}b\in H$.

进而，$b^{-1}a=\left(c^{-1}b\right)^{-1}\left(c^{-1}a\right)\in H$. 这与假设条件矛盾.

同理可得，$Ha\cap Hb=\varnothing$ 的充要条件 $ab^{-1}\in H$.

(iv) 因为 $e,a^{-1}\in H$，所以由结论（ii）可以得到结论 $aH=H=Ha$ 成立.

例 6.2.6 两个正规子群的交集是正规子群.

证　设群G的两个正规子群H_1与H_2，

可知，$H_1 \bigcap H_2$是G的子群.

设$\forall h \in H_1 \bigcap H_2, \forall g \in G$，

所以$h \in H_1, h \in H_2$.

$\because H_1$是正规子群，$\therefore g^{-1}hg \in H_1$，

$\because H_2$是正规子群，$\therefore g^{-1}hg \in H_2$

$\therefore g^{-1}hg \in H_1 \bigcap H_2$，

$\therefore H_1 \bigcap H_2$是正规子群.

根据定理 6.2.2 可以进一步得到：

定理 6.2.3　设 H 是群 G 的子群. 则群 G 可以表示为不相交的左（对应右）**陪集的并集**.

例 6.2.7　令 n=3，则$H = 3Z = \{\ldots, -6, -3, 0, 3, 6, 9, \cdots\}$，已经证明：$H$ 是 Z 的子群.

$\forall a \in Z$，

(1)　若 a=0,则$0 + H = \{\ldots, -3, 0, 3, 6, 9, 12, \cdots\} = H$.

若 a=3,则$3 + H = \{\ldots, -3, 0, 3, 6, 9, 12, \cdots\} = H$.

也就是说，若$a \in H$，则$aH = H$.

(2)　若 a=1，则$1 + H = \{\ldots, -5, 1, 4, 7, 10, 13, \cdots\}$.

即此集合是模 3 余 1 的集合，记作$[1]$，（模 3 余 1 剩余类）

当然：H，记作$[0]$.

(3)　若 a=2，则得到$[2] = 2 + H$.

因此，Z 被分为 3 个互不相交的集合$[0]$，$[1]$，$[2]$，即剩余类集合{$[0]$，$[1]$，$[2]$}.

或者说，Z 被子群 H 分为了 3 个互不相交的左陪集的集合 H，　1+H，　2+H.

同时，Z 也可以被子群 H 分为了 3 个互不相交的右陪集的集合 H，　H+1，　H+2.

另外，左陪集=右陪集，H=H；　1+H= H+1；　2+H= H+2.

定义 6.2.5 设 H 是群 G 的子群. 则 H 在 G 中不同左（对应右）陪集组成的新集合

$\{aH \mid a \in G\}$，叫做 H 在 G 中的**商集**，记作 G/H.

G/H 中不同左（对应右）陪集的个数叫做 H 在 G 中的**指数**，记为 $[G:H]$.

定理 6.2.4 （i）设 H 是群 G 的子群，则 $|G|=[G:H]|H|$.

（ii）更进一步，如果 K，H 是群 G 的子群，且 K 是 H 的子群，则

$$[G:k]=[G:H][H:K].$$

如果其中两个指数是有限的，则第三个指数也是有限的.

证 (i) 根据定理 6.2.2，我们有

$$G=\bigcup_{i\in I} a_i H \quad 和 \quad |G|=\sum_{i\in I}|a_i H|.$$

对 H 到 $a_i H$ 的映射， $f: h \mapsto a_i h$ 是一一对应的双射.

所以 $|a_i H|=|H|$. 再由 $|G|=\sum_{i\in I}|a_i H|$,

所以 $|G|=[G:H]|H|$.

(ii) 若 K，H 是群 G 的子群，且 K 是 H 的子群，由定理 6.2.2，我们有

$G=\bigcup_{i\in I} a_i H$ 和 $H=\bigcup_{j\in J} b_j K$,

其中 $|I|=[G:H], |H|=[H:K]$. 从而 $G=\bigcup_{i\in I}\bigcup_{j\in J}(a_i b_j)K$.

下面我们证明：$\{(a_i b_j)K\}, i\in I, j\in J$ 是不同的陪集. 假设

$$(a_i b_j)K=(a_{i'} b_{j'})K,$$

由于 K 是群 G 的子群，根据定理 6.2.2 (ii)，$(a_{i'}b_{j'})^{-1}(a_i b_j)\in K\subset H$，即 $b_{j'}{}^{-1}a_{i'}{}^{-1}a_i b_j \in K\subset H$. 而 $b_j, b_{j'}\in H$，故 $a_{i'}{}^{-1}a_i\in H$，即得 $a_i H=a_{i'}H$.

进而，$b_j K=a_i^{-1}a_i b_j K=a_i^{-1}a_{i'}(b_{j'}K)\subset b_{j'}K$.

同理，$b_{j'}K\subset b_j K$，从而 $b_{j'}K=b_j K$.

因此，有 $|G|=\sum_{i\in I}\sum_{j\in J}|(a_i b_j)K|=[G:H][H:K]|K|$.

但我们有 $|G|=[G:K]|K|$,

故 $[G:k]=[G:H][H:K]$.

推论 6.2.1 (Lagrange)设 H 是有限群 G 的子群，则子群 H 阶是 $|G|$ 的因数.

下面考虑群 G 的两个子群组成的集合. 设 G 是一个群，H，K 是 G 的子群，我们用 HK 表示集合

$$HK=\{hk \mid h\in H, k\in K\}$$

如果写成加法，我们用 H+K 表示集合

$$H+K=\{h+k \mid h\in H, k\in K\}$$

例 6.2.8 设 H，K 是交换群 G 的两个子群，则 HK 是 G 的子群.

证:

(i) HK 是群 G 的非空子集，$e\in HK$.

(ii) $\forall a=h_1k_1$，$b=h_2k_2\in HK$，其中 $h_1,h_2\in H$，$k_1,k_2\in K$.

$ab^{-1}=h_1k_1\bullet k_2^{-1}h_2^{-1}$.

因为 G 是交换群，所以 $ab^{-1}=h_1h_2^{-1}\bullet k_1k_2^{-1}$.

又因为 H 是 G 的子群，所以 $h_1h_2^{-1}=h\in H$.

K 是子群，所以 $k_1k_2^{-1}=k\in K$.

即 $ab^{-1}=hk\in HK$. 所以，HK 是 G 的子群.

接下来，我们给出，定理 6.2.5-6.2.7 的相应结论，证明略去.

定理 6.2.5 设 H，K 是群 G 的子群，则 $|HK|=|H||K|/|H\cap K|$.

定理 6.2.6 设 H，K 是群 G 的子群，则 $|H:H\cap K|\le[G:K]$. 如果 $[G:K]$ 是有限的，则 $|H:H\cap K|=[G:K]$ 当且仅当 $G=KH$.

定理 6.2.7 设 H，K 是群 G 的有限子群. 则 $[G:H\cap K]$ 是有限的，且 $[G:H\cap K]|\le[G:H][G:K]$. 进一步，$[G:H\cap K]|=[G:H][G:K]$ 当且仅当 $G=KH$.

下面来讨论商集 G/H 构成一个群的条件.

定理 6.2.8 设 N 是群 G 的子群，则如下条件是等价的：

(i) 对任意 $a\in G$，有 $aN=Na$.

(ii) 对任意 $a\in G$，有 $aNa^{-1}=N$（或者 $a^{-1}Na=N$）.

(iii) 对任意 $a\in G$，有 $aNa^{-1}\subset N$，其中 $aNa^{-1}=\{ana^{-1} \mid n\in N\}$.

证 易知，(*i*)蕴含(*ii*) 及(*ii*)蕴含(*iii*)是显然的. 现从(*iii*)推出(*i*).

证明(*iii*)推出(*i*)：对任意 $a \in G, n \in N$，

因为 $ana^{-1} \in aNa^{-1} \subset N$，所以 $ana^{-1} = n', \quad n' \in N$.

进而 $an = n'a \in Na, \qquad aN \subset Na$.

特别地，也有 $a^{-1}N \subset Na^{-1}$ 或 $Na \subset aN$，故 $aN = Na$. 结论成立.

定义 6.2.5 设 N 是群 G 的子群. 我们称 N 为群 G 的**正规子群**，如果它满足定理 6.2.8 的任一条件，记为 $N \lhd G$.

注：若群 G 没有非平凡的正规子群，则称 G 为**单群**.

例 6.2.9 可以证明 $(nZ,+)$ 是 $(Z,+)$ 的正规子群 $a(nZ)a^{-1} \subset nZ$（因为满足交换律）.

定理 6.2.9 设 N 是群 G 的正规子群，G/N 是由 N 在 G 中的所有（左）陪集组成的集合，则对于运算

$$(aN)(bN) = (ab)N,$$

G/N 构成一个群.

证 首先，我们要证明运算的定义不依赖于陪集的代表元的选择.

即要证明：$aN = a'N, \quad bN = b'N$ 时，$(ab)N = (a'b')N$.

事实上，

$$(ab)N = a(bN) = a(b'N) = a(Nb') = (aN)b' = (a'N)b' = (a'b')N.$$

其次，运用群的定义，证明是一个群.

（0） 满足封闭性: $\forall aN, bN \in \mathrm{G}/H, \quad (aN)(bN) = (ab)N \in \mathrm{G}/H$.

（1） 满足结合律:

$$\forall aN, bN, cN \in \mathrm{G}/H, \quad [(aN)(bN)](cN) = (aN)[(bN)(cN)].$$

（2） $eN = N$ 是单位元. 事实上，对任意 $a \in G$，有

$$(aN)(eN) = (ae)N = aN, (eN)(aN) = (ea)N = aN.$$

（3） aN 的逆元是 $a^{-1}N$. 事实上，

$$(aN)(a^{-1}N) = (aa^{-1}N) = eN, (a^{-1}N)(aN) = (a^{-1}aN) = eN.$$

综上，G/H 对于运算构成一个群.

注：定理 6.2.9 中的这个群 G/N 叫做群 G 对于正规子群 N 的**商群**.

如果群 G 的运算写作加法，则 G/N 中的运算写作

$$(a+N)\oplus(b+N)=(a+b)+N.$$

例 6.2.10 可以证明 $G/H=\{H,aH,bH,\cdots\}$ 商群.

例如，$Z/3Z=\{3Z,\ 1+3Z,\ 2+3Z\}$ 商群, 因为 3Z 是 Z 的一个正规子群.

6.3 同态和同构

近世代数的主要研究对象是代数系统 $(G,\bullet)$，即一个集合及其上的运算. 本节讨论代数系统 $(G,\bullet)$（包括其运算）之间的关系.

定义 6.3.1：设 $(G,\bullet)$ 和 $(G',*)$ 是两个代数系统. 如果存在 G 到 G' 的映射 f，并且保持运算，即

$$f(a\bullet b)=f(a)*f(b)\qquad \forall a,b\in G,$$

则称 f 是 $(G,\bullet)$ 到 $(G',*)$ 的**同态**（同态映射）.

例 6.3.1 例如整数集合上加法 $(Z,+)$ 和正实数集合上乘法 $(R^+,\bullet)$.

令映射 f：$Z\to R^+$，$x\mapsto e^x$（即 $f(x)=e^x$）.

由于

1) f 是映射（每一个元素都有唯一的像存在）.

2) 保持运算：$\forall x,y\in \mathrm{Z}\quad f(x+y)=e^{x+y}=e^x\bullet e^y=f(x)\bullet f(y)$.

所以, f 是 $(G,\bullet)$ 到 $(G',*)$ 的同态映射.

定义 6.3.2：

(1) 如果 G 到 G' 的同态映射 f 是单射，则称 f 为 G 到 G' 的**单同态**.

(2) 如果 G 到 G' 的同态映射 f 是满射，则称 f 为 G 到 G' 的**满同态**.

此时，称 G 与 G' 是同态的.

(3) 如果 G 到 G' 的同态映射 f 是双射(一一对应的)，则称 f 为 G 到 G' 的**同构**映射.

此时，称 G 与 G' 是同构的，记作 $G\cong G'$.

(4) 如果$G=G'$，f是G到G的同（态）构映射，则称f为**自同态（构）**映射.

例 6.3.2 对于$(Z,+)$与$(R^{+},\bullet)$， $f(x)=e^{x}$，则f是$Z\to R^{+}$的单同态.

例 6.3.3 设$(Z,+)$和$(A,\bullet)$，这里$A=\{1,-1\}$，$\bullet$为乘法. 映射f: $Z\to A$

$$f(x)=\begin{cases}1\ , & \text{当}x\text{为偶数（包括负偶数）时}\\ -1, & \text{当}x\text{为奇数（包括负奇数）时}\end{cases}$$

证明：f是$Z\to A$的同态（同态映射）.

证 对$\forall x,y\in Z$,

(1) 当x,y都是偶数时,

$$f(x+y)=1=1\bullet 1=f(x)\bullet f(y).$$

(2) 当x,y都是奇数时,

$$f(x+y)=1=(-1)\bullet(-1)=f(x)\bullet f(y).$$

(3) 当x为奇数，y是偶数时,

$$f(x+y)=-1=(-1)\bullet 1=f(x)\bullet f(y).$$

(4) 当x是偶数，y是奇数时,

$$f(x+y)=-1=1\bullet(-1)=f(x)\bullet f(y).$$

即对$\forall x,y\in Z$，都$f(x+y)=f(x)\bullet f(y)$成立.

所以，f是$Z\to A$的同态，且f是满射（A 中元素都有原像），是满同态.

例 6.3.4 设$M(m\times n,R)=\{\text{实数上的全体}m\times n\text{阶矩阵}\}$，规定映射

$$f:\ M(m\times n;R)\to M(m\times n,R),$$

$$f(A)=A^{T}\ (A^{T}\text{ 为 }A\text{ 的转置矩阵}),\ \forall A\in M(m\times n,R).$$

问：（1）关于矩阵的加法，即($M(m\times n;R)$，+)，f是否是$M(m\times n;R)$的自同构？

（2）关于矩阵的乘法，f是否是$M(m\times n;R)$的自同构？

解：（1）不难证明：f是$M(m\times n;R)\to M(m\times n,R)$的双射.

对$\forall A,B\in M(m\times n,R)$,

$$(A+B)^{T}=A^{T}+B^{T}，\text{即 }f(A+B)=f(A)+f(B).$$

所以，f是$M\left(m\times n;R\right)$的自同构.

（2）当 n>1 时，$\left(AB\right)^{T}=B^{T}A^{T}\neq A^{T}B^{T}$，即

$$f\left(AB\right)\neq f\left(A\right)f\left(B\right).$$

所以，f不是$M\left(m\times n;R\right)$的自同构.

在有了群的定义之后，可知群的几个最基本的性质. 将同态应用到群上，可以随时把一个集合来同一个群比较，或把两个群来比较. 同态(构)用处在于比较两个集合之间的性质.

定理 6.3.1：若$\left(G,\bullet\right)$与$\left(G,*\right)$是同态的，那么

1）若$\bullet$适合结合律，$*$也适合结合律.

2）若$\bullet$适合交换律，$*$也适合交换律.

定理 6.3.2：若 G 是一个群，$\bar{G}$ 是一个不空集合，则若 G 与$\bar{G}$ 对于它们各自的运算来说同态，那么$\bar{G}$ 也是一个群.

事实上，若 G 与$\bar{G}$ 同态，说明存在一个同态满射f. 进而根据同态和群的条件，易得.

例 6.3.5 $\left(R,+\right)$是群，$T=\left\{z\mid z\in C,|z|=1\right\}$，$f$是$R\rightarrow T$ 的一个映射，其中 $f:x\mapsto e^{ix}$，可以证明f是$R\rightarrow T$ 的同态满射，所以$\left(T,\bullet\right)$是群.

1) f是$R\rightarrow T$ 的映射，$\forall x\in R$，$\exists$ 唯一的像 $f\left(x\right)=e^{ix}\in T$.

2) f是$R\rightarrow T$ 的满射，$\forall z\in T,\ \exists\theta\in R$，使得 $f\left(\theta\right)=z$.

3) f是同态映射，对$\forall x,y\in R$,

$$f\left(x+y\right)=e^{i(x+y)}=e^{ix+iy}=e^{ix}\bullet e^{iy}=f\left(x\right)\bullet f\left(y\right).$$

f是$R\rightarrow T$ 的同态满射，又因为$\left(R,+\right)$是群，所以$\left(T,\bullet\right)$是群.

事实上，可以证明$T=\left\{z\mid z\in C,|z|=1\right\}$关于数的乘法构成群.

定理 6.3.3 设f是群 G 到群G'的一个同态，则

(*i*) $f\left(e\right)=e'$，即同态将单位元映到单位元.

(*ii*) 对任意$a\in G,\ f\left(a^{-1}\right)=f\left(a\right)^{-1}$.

(*iii*) $\ker f=\left\{a\mid a\in G,\ f\left(a\right)=e'\right\}$是 G 的子群，则f是单同态的充要条件是

$\ker f = \{e\}$.

(*iv*) $f(G) = \{f(a) \mid a \in G\}$ 是 G' 的子群，且 f 是满同态的充要条件是 $f(G) = G'$.

(*v*) 设 H' 是群 G' 的子群，则集合 $f^{-1}(H') = \{a \in G \mid f(a) \in H'\}$ 是 G 的子群.

证 (*i*) 因为 $f(e)f(e) = f(e^2) = f(e) = f(e)e'$，此式两端同乘 $f(e)^{-1}$，

得到 $f(e) = e'$，结论成立.

(*ii*) 因为 $f(a^{-1})f(a) = f(a^{-1}a) = f(e) = e'$，

$f(a)f(a^{-1}) = f(aa^{-1}) = e'$，所以 $f(a^{-1}) = f(a)^{-1}$.

(*iii*) 对任意 $a, b \in \ker f$，有 $f(a) = e'$， $f(b) = e'$，从而

$$f(ab^{-1}) = f(a)f(b^{-1}) = f(a)f(b)^{-1} = e'.$$

因此，$ab^{-1} \in \ker f$.所以 $\ker f$ 是 G 的子群.

若 f 是单同态，则满足 $f(a) = e' = f(e)$ 的元素只有 $a = e$，因此 $\ker f = \{e\}$.

反过来，设 $\ker f = \{e\}$.则对任意的 $a, b \in G$，使得 $f(a) = f(b)$，有

$$f(ab^{-1}) = f(a)f(b^{-1}) = f(a)f(b)^{-1} = e'.$$

这说明，$ab^{-1} \in \ker f = \{e\}$，有 $a = b$. 因此，f 是单同态.

(*iv*) 对任意 $x, y \in f(G)$，存在 $a, b \in G$ 使得 $f(a) = x, f(b) = y$.

从而，$xy^{-1} = f(a)f(b)^{-1} = f(ab^{-1}) \in f(G)$.

所以 $f(G) = \{f(a) \mid a \in G\}$ 是 G' 的子群,且 f 是满同态的充要条件是 $f(G) = G'$.

(*v*) $f^{-1}(H')$ 非空， e' 的原像 $e \in f^{-1}(H')$.

对任意 $a, b \in f^{-1}(H')$，根据(ii)及 H' 为子群，我们有

$$f(ab^{-1}) = f(a)f(b^{-1}) = f(a)f(b)^{-1} \in H' \text{（因为} H' \text{是子群）}.$$

因此，$ab^{-1} \in f^{-1}(H')$.

所以 $f^{-1}(H')$ 是 G 的子群.

例 6.3.6 加群$\left(Z/nZ,\oplus_n\right)$到乘群$G=\left\{\theta^k \mid \theta=e^{\frac{2\pi i}{n}},k=0,1,2,\cdots n-1\right\}$的映射

$f:k\mapsto\theta^k$，证明f是一个同构.

证

（1）f是一一映射.

(a) 映射，$\forall x\in n\mathrm{Z}$ ，有唯一的像$f\left(x\right)$存在.

(b) 单射，若$x\neq y,f\left(x\right)\neq f\left(y\right)$.

(c) 满射，$\forall z\in G,\exists x\in Z/nZ$，使得$f\left(x\right)=z$，至少有一个$x$存在.

（2）$\forall x,y\in\mathrm{Z}\quad f(x+y)=\theta^{x+y}=\theta^x\bullet\theta^y=f\left(x\right)\bullet f\left(y\right)$.

所以，综上可知f是一个同构.

例 6.3.7 设a是一个元，那么映射$f:b\mapsto aba^{-1}$是G的自同态.

证 （1）因为G是群，由封闭性可知$\forall b\in G$，$f(b)=aba^{-1}\in G$，

所以映射f是G到G的映射.

（2）下证f是同态映射. 因为$\forall b,c\in G$，有

$f\left(bc\right)=a\left(bc\right)a^{-1}=\left(aba^{-1}\right)\left(aca^{-1}\right)=f\left(b\right)f\left(c\right)$.

综上，映射$f:b\mapsto aba^{-1}$是群G的自同态.

在群的研究中，有时候是借助与之同构的群来进行的，这就需要构造相应的同构.但是，直接构造同构并不是很容易的事，因此通常是构造同态，再借助群**同态基本定理**来诱导出同构映射.

定理 6.3.4 设f是群G到群G'的同态，则f的核$\ker f$是G的正规子群，反过来，如果N是群G的正规子群，则映射

$$\begin{gathered}s:G\to G/N\\ a\mapsto aN\end{gathered}$$

是核为N的（自然）同态.

证 $\Rightarrow$ 由前面的定理 6.3.3，知$\ker f\leq G$.

下证$\ker f$是G的正规子群.

对$\forall a\in G,\forall b\in\ker f$，

我们有$f\left(aba^{-1}\right)=f\left(a\right)f\left(b\right)f\left(a^{-1}\right)=f\left(a\right)e'f\left(a\right)^{-1}=e'$.

所以$aba^{-1}\in\ker f$，即 $\ker f$ 是 G 的正规子群.

$\Leftarrow$ 反过来，设 N 是群 G 的正规子群，则 G 到 G/N 的映射 s 满足：

$$s(ab)=(ab)N=(aN)(bN)=s(a)s(b).$$

同时，$s(a)=N$ 的充分必要条件是 $a\in N$. 因此，s 是核为 N 的同态.

定理 6.3.5 【群同态基本定理】 设 f 是群 G 到群 G' 的同态，则存在惟一的 $G/\ker f$ 到像子群 $f(G)$ 的同构 $\overline{f}:a\ker f\mapsto f(a)$ 使得 $f=i\circ\overline{f}\circ s$，其中 s 是群 G 到商群 $G/\ker f$ 的自然同态，$i:c\mapsto c$ 是 $f(G)$ 到 G' 的恒等同态. 即有如下的交换图：

$$\begin{array}{ccc} G & \xrightarrow{f} & G' \\ s\downarrow & & \uparrow i \\ G/\ker f & \xrightarrow{\overline{f}} & f(G) \end{array}$$

证 首先，证明存在性. 根据定理 6.3.4，$\ker f$ 是 G 的正规子群，所以存在商群.

现在. 要证明：$\overline{f}:a\ker f\mapsto f(a)$ 是 $G/\ker f$ 到像子群 $f(G)$ 的同构.

(1) $\overline{f}$ 是映射，“任一元素有唯一的像”.

若 $a\ker(f)=b\ker(f)\Rightarrow b^{-1}a\in\ker(f)\Rightarrow f(b^{-1}a)=f(b)^{-1}f(a)=e$，

所以 $f(a)=f(b)$，所以像唯一.

(2) 单射“不同的原像，有不同的像”.

若 $a\ker(f)\neq b\ker(f)\Rightarrow b^{-1}a\notin\ker(f)\Rightarrow f(b^{-1}a)=f(b)^{-1}f(a)\neq e$，

所以 $f(a)\neq f(b)$

【或者证明相同的像，有相同的原像.

即若 $f(a)=f(b)$，则 $a\ker(f)=b\ker(f)$】

(3) 满射. 对 $\forall c\in f(G),\exists a\in G$，使得 $f(a)=c$.

从而 $\overline{f}(a\ker f)$=$f(a)=c$，即 $a\ker f$ 是 c 的原像.

(4) 保持同态映射：

$\forall a\ker f,\forall b\ker f\in G/\ker f$，

$$\overline{f}((a\ker f)(b\ker f))=\overline{f}((ab)\ker f)=f(ab)=f(a)f(b)=\overline{f}(a\ker f)\overline{f}(b\ker f).$$

综上，$\overline{f}$ 是同构，并且有 $f=i\circ\overline{f}\circ s$，因为

$$i\circ\overline{f}\circ s(a)=i\left(\overline{f}\left(a\ker f\right)\right)=i\left(f\left(a\right)\right)=f\left(a\right).$$

下证唯一性.

假如还有同构 $g:G/\ker f\mapsto f\left(G\right)$ 使得 $f=i\circ g\circ s$,

则对任意 $a\ker f\in G/\ker f$ ，只需证明 $g\left(a\ker f\right)=\overline{f}\left(a\ker f\right)$，

事实上，我们有

$$g(a\,ker\,f)=i\Big(g\big(s(a)\big)\Big)=(i\circ g\circ s)(a)=f(a)=\overline{f}(a\,ker\,f).$$

因此， $g=\overline{f}$.

例 6.3.8 设 f 是群 N 到群 $G=<a>$ 的同态， $f:n\mapsto a^n$. 我们有

$$Z/\ker f\cong<a>.$$

具体来说，设 f 是群 N 到群 $G=<a>=\{a^n\mid 0\le n<3,\ a^3=1\}=\{1,\ a,\ a^2\}$ 的同态，

有 Kef f =3N，

$N'=N/3N=\{[0],[1],[2]\}$,

$G=<a>=\{a^n\mid 0\le n<3,\ a^3=1\}=\{1,\ a,\ a^2\}$.

6.4 循环群

首先讨论加群 Z 及其子群.

定理 6.4.1 加群 Z 的每个子群 H 是循环群. 并且，有 $H=<0>$ 或 $H=<m>=mZ$ ，其中 m 是 H 中的最小正整数. 如果 $H\neq<0>$，则 H 是无限的.

证 （i）如果 H 是零子群 $\{0\}$，只有一个单位元，则是循环群 $H=<0>$.

（ii）如果 H 是非零子群，则存在非零整数 $a\in H$.

因为 H 是子群，所以 $-a\in H$. 这说明 H 中有正整数.

设 H 中的最小正整数为 m. 则一定有 $H=<m>=mZ$.

事实上，

对任意 $a\in H$ ，根据欧几里德除法，存在整数 q,r 使得

$$a=qm+r,\quad 0\le r<m.$$

如果 $r\neq 0$，则 $r=a-qm\in H$ ，这与 m 的最小性矛盾.

因此 $r=0,\ a=qm\in mZ$.

故 $H\subset mZ$.

但显然有 $mZ \subset H$，因此 $H = mZ$.

例 6.4.1 Z，$3Z$，$4Z$，$6Z$ 是（Z，+）的子群（且为正规子群，因为 Z 是交换群），而 $3Z = <3>, 4Z = <4>, 6Z = <6> = \left\{6^0, 6^1, 6^2, 6^3, \cdots\right\}$.

定理 6.4.2 每个无限循环群同构于加群 Z. 每个阶为 m 的有限循环群同构于加群 Z/mZ.

证 设循环群 $G = <a> = \left\{a^n \mid n \in Z\right\}$，考虑映射

$$f: Z \to G$$
$$n \mapsto a^n,$$

则 f 是映射且为满射，则由群同态基本定理知，

$$\begin{array}{ccc} G & \xrightarrow{f} & G' \\ s\downarrow & & \uparrow i \\ G/\ker f & \xrightarrow{\bar{f}} & f(G) \end{array}$$

有群 G 同构于 $Z/\ker(f)$.

根据定理 6.3.3，$\ker f = <0>$ 或 $\ker f = mZ$.

前者对应于无限循环群，后者对应于 m 阶有限循环群.

定义 6.4.1 设 G 是一个群，$a \in G$. 则子群 $<a>$ 的阶称为**元素 a 的阶**，记为 $ord(a)$.

定理 6.4.3 设 G 是一个群，$a \in G$，

如果 a 是无限阶，则

(*i*) $a^k = e$ 当且仅当 k=0.

(*ii*) 元素 $a^k\ (k \in Z)$ 两两不同.

如果 a 是有限阶 m>0，则

(*iii*) m 是使得 $a^m = e$ 的最小正整数.

(*iv*) $a^k = e$ 当且仅当 $m \mid k$.

(*v*) $a^r = a^k$ 当且仅当 $r \equiv k \pmod{m}$.

(*vi*) 元素 $a^k\ (k \in Z/mZ)$ 两两不同.

(*vii*) $<a> = \left\{a, a^2, a^{m-1}, a^m = e\right\}$.

(*viii*) 对任意整数$1 \le d \le m$，有$ord\left(a^d\right)=\dfrac{m}{(m,d)}$.

证　考虑映射 Z 到群 G 的映射 f:

$$f:n \mapsto a^n$$

f 是同态映射. 根据群同态基本定理，我们有

$$Z/\ker f \cong <a>$$

因为 a 是无限阶元等价于$\ker f$，这说明 f 是一对一的.

因此，(*i*) 和 (*ii*) 成立.

如果 a 是有限阶 m，则$\ker f = mZ$，因此，我们有

(*iii*) m 是使得$a^m = e$的最小正整数.

(*iv*) $a^k = e$等价于$k \in \ker f$，等价于$m \mid k$.

(*v*) $a^r = a^k$等价于$r-k \in \ker f$，等价于$r \equiv k \left(\bmod m\right)$.

(*vi*) 元素a^k对应于$Z/\ker f$ 中的不同元素，两两不同.

(*vii*) $<a>=\left\{a,a^2,a^{m-1},a^m=e\right\}$与$Z/\ker f$ 中最小正剩余系相对应.

(*viii*) $\left(a^d\right)^k = e$等价于$dk \in \ker\left(f\right)$,

等价于$m \mid dk$,

等价于$\dfrac{m}{(m,d)} \mid \dfrac{d}{(m,d)}k$，等价于$\dfrac{m}{(m,d)} \mid k$.

因此，$ord\left(a^d\right)=\dfrac{m}{(m,d)}$.

定理 6.4.4 循环群的子群是循环群.

证　考虑映射 Z 到循环群$G=<a>$的映射 f:

$$f:n \mapsto a^n.$$

f 是同态映射.

根据定理 6.3.3，对于 G 的子群 H，我们有$K = f^{-1}\left(H\right)$是 Z 的子群.

根据定理 6.4.1，K 是循环群，所以$H = f\left(K\right)$是循环群.

例 6.4.2 若 G 是循环群，G 与$\bar{G}$同态，则$\overline{G}$ 是循环群.

证：设 G=<a> ，G 与$\bar{G}$同态，所以存在满同态映射 g.

$$g\left(a^2\right)=g(a\bullet a)=g(a)\bullet g(a)=g(a)^2\in\overline{G}$$

进一步有，任意 $g(b), g(b)=g\left(a^m\right)=\left(g(a)\right)^m$.

所以 $\overline{G}$ 是循环群，生成元 $g(a)$.

例 6.4.3 找到模 12 的剩余类加群的所有子群.

解　12 的因子有 1，2，3，4，6，12.

模 12 的剩余类加群 $G=\{[0],[1],\cdots,[11]\}$ 是循环群，生成元为 $[1]$.

根据循环群的所有子群都是循环群知：

1 阶子群 $([0])=\{[0]\}$，

2 阶子群 $([6])=\{[6],[0]\}$，

3 阶子群 $([4])=([8])=\{[4],[8],[0]\}$，

4 阶子群 $([3])=([9])=\{[3],[6],[9],[0]\}$，

6 阶子群 $([2])=([10])=\{[2],[4],[6],[8],[10],[0]\}$，

12 阶子群 G .

定理 6.4.5　设 G 是循环群.

(i) 如果 G 是无限的，则 G 的生成元为 a 和 a^{-1}.

(ii) 如果 G 是有限阶 m，则 a^k 是 G 的生成元当且仅当 $(k,m)=1$.

证　先证明 (ii).

因为 a^k 的阶为 $\dfrac{m}{(k,m)}$，则 a^k 的阶为 m.

另一个解释：即 $\left\{a^k\right\}=G$.

反之，a^k 是 G 的生成元，则有 $(k,m)=1$.

再证明 (i)

考虑映射 Z 到循环群 G 的映射 f：$f:n\mapsto a^n$

f 是同态映射. 根据群同态基本定理，我们有

$$Z/\ker f\cong G.$$

因为 G 中的生成元对应于 $Z/\ker f$ 中的生成元.

当 $\ker f = \{0\}$，$Z/\ker f$ 的生成元是 1 和-1；对应 G 的生成元为 a 和 a^{-1}.

当 $\ker f = mZ$，$m>0$ 时，$Z/\ker f$ 的生成元是 k，$(k,m)=1$.

因此，结论成立.

定理 8.4.6 设 G 是有限交换群. 对任意元素 $a,b\in G$，若 $(ord(a),ord(b))=1$，则

$$ord(ab)=ord(a)ord(b).$$

证 因为

$$\begin{aligned}a^{ord(ab)ord(b)} &= a^{ord(ab)ord(b)}\bullet 1\\ &= a^{ord(ab)ord(b)}\bullet b^{ord(ab)ord(b)}\\ &= (ab)^{ord(ab)ord(b)} = 1\end{aligned}$$

根据定理 6.4.3(iv)，我们有 $ord(a)\mid ord(ab)ord(b)$.

因为 $(ord(a),ord(b))=1$，所以 $ord(a)\mid ord(ab)$.

同理 $ord(b)\mid ord(ab)$.

根据 $(ord(a),ord(b))=1$，我们得到

$$ord(a)ord(b)\mid ord(ab).$$

此外，显然有

$$ord(ab)\mid ord(a)ord(b).$$

事实上，由 $(ab)^{ord(a)ord(b)} = a^{ord(a)ord(b)}\bullet b^{ord(a)ord(b)} = 1$ 及阶的定义立得.

故有

$$ord(a)ord(b)=ord(ab).$$

例 6.4.4 设（G，+）是 6 阶循环群，a, b 分别是 2, 3 阶的元素，则 a+b 是 6 阶的，恰是 G 的生成元.

具体举例如下：$Z_6=\{[0],[1],[2],[3],[4],[5]\}$，生成元为[1]，$(Z_6,\oplus_6)$ 是循环群.

其中，$[2]$ 是 3 阶，$[3]$ 是 2 阶，则 $[2]+[3]=[5]$ 是 2*3=6 阶元素，是生成元.

6.5 置换群

定义 6.5.1 设 S 是一个非空集合，G 是 S 到自身的所有一一对应的映射组成的集合. 则

对于映射的复合运算，G 构成一个群，叫做**对称群**.

注：**单位元：**恒等映射.

G 中的元素叫做 S 的一个**置换**.

当 S 是 n 元有限集时，G 叫做 n 元对称群，记作 S_n.

设 $S=\{1,2,\cdots n-1,n\}$, σ 是 S 上的一个置换，即 σ 是 S 到自身的一一对应的映射：

$$\begin{aligned}\sigma: S &\to S \\ k &\to \sigma(k)=i_k\end{aligned}$$

将 σ 表示成：

$$\sigma=\begin{pmatrix} 1 & 2 & \cdots & n-1 & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n-1) & \sigma(n)\end{pmatrix}.$$

例 6.5.1 对 $S=\{1,2,3,4,5,6\}$, 有

置换 $\sigma=\begin{pmatrix}1&2&3&4&5&6\\6&5&3&1&2&4\end{pmatrix}$.

置换 $\tau=\begin{pmatrix}1&2&3&4&5&6\\6&4&3&1&2&5\end{pmatrix}$.

单位置换 $I=\begin{pmatrix}1&2&3&4&5&6\\1&2&3&4&5&6\end{pmatrix}$.

例 6.5.2 设 $\sigma=\begin{pmatrix}1&2&3&4&5&6\\6&5&4&2&1&3\end{pmatrix}$, $\tau=\begin{pmatrix}1&2&3&4&5&6\\5&6&4&2&3&1\end{pmatrix}$. 计算 $\sigma\tau,\tau\sigma,\sigma^{-1}$.

解:

单位元为： $I=\begin{pmatrix}1&2&3&4&5&6\\1&2&3&4&5&6\end{pmatrix}$.

$$\begin{aligned}\sigma\tau &= \begin{pmatrix}1&2&3&4&5&6\\6&5&4&2&1&3\end{pmatrix}\begin{pmatrix}1&2&3&4&5&6\\5&6&4&2&3&1\end{pmatrix} \\ &= \begin{pmatrix}5&6&4&2&3&1\\1&3&2&5&4&6\end{pmatrix}\begin{pmatrix}1&2&3&4&5&6\\5&6&4&2&3&1\end{pmatrix} \\ &= \begin{pmatrix}1&2&3&4&5&6\\1&3&2&5&4&6\end{pmatrix}.\end{aligned}$$

$$\tau\sigma=\begin{pmatrix}6&5&4&2&1&3\\1&3&2&6&5&4\end{pmatrix}\begin{pmatrix}1&2&3&4&5&6\\6&5&4&2&1&3\end{pmatrix}= \begin{pmatrix}1&2&3&4&5&6\\1&3&2&6&5&4\end{pmatrix}.$$

$$\sigma^{-1}=\begin{pmatrix}6&5&4&2&1&3\\1&2&3&4&5&6\end{pmatrix}=\begin{pmatrix}1&2&3&4&5&6\\5&4&6&3&2&1\end{pmatrix}.$$

定理 6.5.1 n 元置换全体组成的集合 S_n 对置换的乘法构成一个群，且 $|S_n|=n!$.

为了更好地研究置换，先考虑特殊的置换.

定义 6.5.2 (k-轮换)：如果 n 元置换 σ 使得 $\{1,2,\cdots,n-1,n\}$ 中的一部分元素 $\{i_1,i_2,\cdots i_{k-1},i_k\}$ 满足 $\sigma(i_1)=i_2,\sigma(i_{k-1})=i_k,\sigma(i_k)=i_1$，又使得余下的元素保持不变，则称该置换为 ***k*-轮换**，简称轮换，记作 $\sigma=(i_1,i_2,\cdots i_{k-1},i_k)$.

例 6.5.3 （1） $\sigma=\begin{pmatrix}1&2&3&4&5&6\\1&5&3&2&4&6\end{pmatrix}=(2\,5\,4)$.

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

定义 6.5.3 对于定义 6.5.2 中，如果 k=1 时，1-轮换为**恒等置换**；k=2 时，2-轮换 (i_1,i_2) 叫做**对换**. 若两个 k 轮换 $\sigma=(i_1,i_2,\cdots i_{k-1},i_k)$， $\tau=(j_1,j_2,\cdots j_{l-1},j_l)$ 的 $k+l$ 个元素均不同，则称其**不相交**.

例 6.5.4 $\sigma=(2\,5\,4)$ 与 $\tau=(1\,6\,3)$ 是不相交的 3 轮换.

定理 6.5.2 任意一个置换都可以表示为一些不相交轮换的乘积. 在不考虑乘积次序的情况下，该表达式是唯一的.

例 6.5.5 $\sigma=\begin{pmatrix}1&2&3&4&5&6\\6&5&1&2&4&3\end{pmatrix}=(2,5,4)(1,6,3)$

$$=\begin{pmatrix}1&2&3&4&5&6\\1&5&3&2&4&6\end{pmatrix}\begin{pmatrix}1&2&3&4&5&6\\6&2&1&4&5&3\end{pmatrix}.$$

对于轮换来说，可以写成对换.

例 6.5.6 $(2,5,4)=(2,4)(2,5)$， $(1,6,3)=(1,3)(1,6)$.

一般的，轮换 $\sigma=(i_1,i_2,\cdots i_{k-1},i_k)$，有

$$\sigma=\left(i_1,i_2,\cdots i_{k-1},i_k\right)=\left(i_1,i_k\right)\left(i_1,i_{k-1}\right)\cdots\left(i_1,i_3\right)\left(i_1,i_2\right).$$

定义 6.5.4 对于 n 元排列 $i_1,\cdots,i_k,\cdots,i_l,\cdots,i_n$ 的一对有序元素 $\left(i_k,i_l\right)$，如果 $k<l$ 时，$i_k>i_l$，则称其为**逆序**. 排列中逆序的个数叫做该排列的**逆序数**，记为 $\left[i_1,\cdots,i_n\right]$.

例 6.5.7 $\left[1,5,3,2,4,6\right]=0+0+1+2+0=4$.

定理 6.5.3 任意一个置换 σ 都可以表示为一些对换的乘积，且对换个数的奇偶性与排列的逆序数 $\left[\sigma(1),\cdots,\sigma(n)\right]$ 的奇偶性相同.

例 6.5.8 $\begin{pmatrix}1&2&3&4&5&6\\1&5&3&2&4&6\end{pmatrix}=\left(2,5,4\right)=\left(2,4\right)\left(2,5\right)$.

定义 6.5.5 如果一个置换 σ 可以表示为偶数个对换的乘积，则称其为**偶置换**；如果 σ 可以表示为奇数个对换的乘积，则称其为**奇置换**.

记 A_n 为 n 元偶置换全体组合的集合.

定理 6.5.4 A_n 对置换的乘法构成一个群，其阶是 $n!/2$.

证 封闭性：偶置换与偶置换的乘积是偶置换. 易验证结合律. 单位元 I 是恒等置换. 存在逆元，因为偶置换的逆是偶置换.

定义 6.5.6 A_n 叫做 n 元**交错群**. 由 n 元置换构成的群叫做 n 元**置换群**.

例 6.5.9 设 $\sigma=\left(1,2,3\right)$，则循环群 $G=<\sigma>=\left\{e,\left(1,2,3\right),\left(1,3,2\right)\right\}$ 是 3 元置换群.

例 6.5.10 设 $\sigma_1=\left(1,2,3,4\right),\sigma_2=\left(1,3,2,4\right)$，

则循环群 $G_1=<\sigma_1>=\{e,\left(1,2,3,4\right),\left(1,3\right)\ \left(2,4\right),\left(1,4,3,2\right)\}$

和 $G_1=<\sigma_1>=\{e,\left(1,2,3,4\right),\left(1,3\right)\ \left(2,4\right),\left(1,4,3,2\right)\}$

都是 4 元置换群.