第八章 群论

在研究代数系统时，可以将结合律看成是代数系统的基本性质，并且将具有相同性质的代数集中研究，从而形成了很多特定的代数系统，如半群，群，环，域，格，布尔代数等等。

而群是最早被研究的代数系统，半群的概念则是群的理论发展之后才引进的。

8.1 半群

- **1. 概念**
- **定义8.1：设<S, *>是代数系统，*是二元运算，如果*运算满足结合律，则称它为半群(Semigroups)**

例：$<N,+>$，$<Z,\times>$，$<P(S),\oplus>$，$<S^S,\circ>$ 是半群 $<Z,->$ 不是

- **例8-1：（1）设** $S=\left\{\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} \middle| a,b\in R, a\neq 0\right\}$ **，则<S, *>是半群(*矩阵乘法)**

证：对任意的 $\begin{pmatrix} a_1 & b_1 \\ 0 & 0 \end{pmatrix}\in S,\begin{pmatrix} a_2 & b_2 \\ 0 & 0 \end{pmatrix}\in S$，有 $\begin{pmatrix} a_1 & b_1 \\ 0 & 0 \end{pmatrix}*\begin{pmatrix} a_2 & b_2 \\ 0 & 0 \end{pmatrix}$

$=\begin{pmatrix} a_1a_2 & a_1b_2 \\ 0 & 0 \end{pmatrix}$ 且 $a_1a_2\neq 0$， $\therefore \begin{pmatrix} a_1a_2 & a_1b_2 \\ 0 & 0 \end{pmatrix}\in S$

$\therefore$ *封闭，又 $\because$ 矩阵乘法满足结合律，$\therefore <S,*>$ 是半群。

(2) $<S,+>$ 不是半群，$\begin{pmatrix} a_1 & b_1 \\ 0 & 0 \end{pmatrix}+\begin{pmatrix} -a_1 & b_2 \\ 0 & 0 \end{pmatrix}=\begin{pmatrix} 0 & b_1+b_2 \\ 0 & 0 \end{pmatrix}\notin S$，不封闭

8.1 半群

- **2. 半群的幂运算**

设x为半群<S, *>中的元素，x的n次幂定义如下：

$$(1): x^1 = x \quad (2) x^{n+1} = x^n * x \quad n \in Z^+$$

由于半群满足结合律，所以可用归纳法证明

$x^m * x^n = x^{m+n} \quad (x^m)^n = x^{mn}$，如果 $x^2 = x$，则称x是<S, *>的幂等元。

- **定理8.1**：若<S, *>是半群，S是有限集合，则称S中必含有幂等元。

8.1 半群

证明：因为$<S,*>$是半群，则$\forall a \in S$，有$a^2, a^3, \cdots \in S$

而S是有限集合，所以必有$j > i$，使得$a^i = a^j$。

令$p = j - i$，则有$a^i = a^j = a^p * a^i$，

所以：$a^q = a^p * a^q (q \geq i)$

因为$p \geq 1$，所以存在$k \geq 1$，使得$kp \geq i$，则

$$a^{kp} = a^p * a^{kp} = a^p * (a^p * a^{kp}) = a^{2p} * a^{kp} = \cdots = a^{kp} * a^{kp}$$

即在S中存在元素$b = a^{kp}$，使得$b * b = b$

8.1 半群

- 3. 特殊半群
- 定义8.2：如果半群<S, *>中二元运算*是可交换的，则称<S, *>是可交换半群；如：<Z, +>，<Z, ×>，<P(S), ⊕>可交换半群，$<S^S,\circ>$ 不是。
- 定义8.3：含有关于*运算幺元的半群<S, *>，称它为独异点(monoid)，或含幺半群，常记作<S, *, e>

例：<Z, +, 0>，<Z, ×, 1>，<P(S), ⊕, ∅>是独异点，$<S^S,\circ,I_A>,<Z_E,\times>$ 不是。

➢对于独异点，一般规定，$a^0=e(\forall a\in S)$

8.1 半群

- 定义8. 4：（1）设<S, *>为一半群，若$T \subseteq S$，*在T中封闭，则<T, *>称为子半群；（2）设<S, *, e>为一独异点，若$T \subseteq S$，*在T中封闭，且幺元 $e \in T$，则<T, *, e>称为子独异点。

8.1 半群

- **4. 性质**
- **定理8. 2：一个有限独异点，<S, *, e>的运算表中不会有任何两行或两列元素相同。**

证明：$\forall a,b \in S$，且$a \neq b$时，有：

$e*a=a\neq b=e*b$和$a*e=a\neq b=b*e$

$\therefore$命题成立

但这个性质对有限半群不一定成立。

- **例8-2：(1) S={a，b，c}，*运算的定义如表，判断<S, *>的代数结构；**

(2) 判断$<Z_4,+_4>$的代数结构。

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

8.1 半群

解:(1),i): 封闭性：$\forall x,y\in S, x*y\in S$；ii): 可结合：

$\forall x,y,z\in S$，有$x*(y*z)=x*z=z,(x*y)*z=y*z=z$

$\therefore <S,*>$是半群，a,b,c均有左幺元，该表中任何两行元素相同

$\therefore <S,*>$不是独异点

(2), i)：封闭性：（画表），

i i)：可结合性：有的定义可知，

i i i)：幺元：[0]，

$+_4$	**[0]**	**[1]**	**[2]**	**[3]**
[0]	[0]	[1]	[2]	[3]
[1]	[1]	[2]	[3]	[0]
[2]	[2]	[3]	[0]	[1]
[3]	[3]	[0]	[1]	[2]

表中没有人员两行或两列元素完全相同。

8.1 半群

- 定理8.3：设<S,*>，<T,∘>是半群，f为S到T的同态，这时称f为半群同态，对半群同态，有(1)：同态像<f(S),∘>为一半群；(2)：当<S,*>为独异点时，则<f(S),∘>为一独异点。

证：由7.10，7.11可得。

8.2 群的定义与性质

- **1. 概念**

独异点中含有幺元，可以考虑其中每个元素是否有逆元，由此引出一个特殊的独异点，即群的概念

- 定义8.5：如果代数系统<G, *>满足：（1）<G, *>为一半群；（2）<G, *>中有幺元；（3）<G, *>中每个元素 $x \in G$ 均有逆元 x^{-1} ；则称代数系统<G, *>为群（Groups）。

➢群：每个元素都可逆的独异点，常用G表示；封闭，可结合，含幺元，元素可逆。

例：$<Z,+,>$, $<Q_+,\times>$, $<P(A),\oplus>(A \neq \emptyset)$为群；

$<Z,\times,>$, $<Q,\times>$, $<P(A),\cup>(A \neq \emptyset)$不是。

8.2 群的定义与性质

- **例8-3：** 设G={a，b，c，e}，*为G上的二元运算，满足下表。

*	**e**	**a**	**b**	**c**
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

则G是一个群，且满足：

(1)e是幺元；

(2)G中任何元素的逆元就是它自己；

(3)a，b，c三元素中，任何两个元素运算的结果都等于另一个元素。

这样的群称为Klein四元群，简称四元群。

8.2 群的定义与性质

- **例8-4：设<G, *>是一个独异点，并且每个元素都有右逆元，证明<G, *>为群。**

证：设e是$<G,*>$中的幺元。每个元素都有右逆元，

即$\forall x \in G, \exists y \in G$, 使得$x * y = e$，对于$y$，又$\exists z \in G$，

使得$y * z = e$，而$\forall x \in G$有$x * e = e * x = x$.

因此：$z = e * z = x * y * z = x * e = x$，即

$x * y = e = y * z = y * x = e$.

即y既是x的右逆元，又是x的左逆元，即$\forall x \in G$均可逆，

$\therefore <G,*>$为群。

8.2 群的定义与性质

- **2. 群的幂运算**

对于群<G, *>中的任意元素a，可以类似半群一样来定义它的幂：

$$a^n = \begin{cases} e & n = 0 \\ a^{n-1} * a & n > 0 \\ (a^{-1})^m & n < 0, n = -m \end{cases}$$

即在群中，可以定义负数次幂

- **定理8.4：** 对于群<G, *>的任意元素a，b有：

$$(1):(a^{-1})^{-1} = a, \quad (2)(a * b)^{-1} = b^{-1} * a^{-1}$$

$$(3):a^n * a^m = a^{n+m}, \quad (4):(a^n)^m = a^{nm}(m, n \in Z)$$

8.2 群的定义与性质

证：(1) $\because a*a^{-1}=a^{-1}*a=e \therefore (a^{-1})^{-1}=a$

(2) $(a*b)*(b^{-1}*a^{-1})=a*(b*b^{-1})*a^{-1}=e$

$(b^{-1}*a^{-1})*(a*b)=b^{-1}*(a^{-1}*a)*b=e$

$\therefore (a*b)$的逆元为$b^{-1}*a^{-1}$，即$(a*b)^{-1}=b^{-1}*a^{-1}$

(3) 当$m,n\geq 0$时：用归纳法(对m归纳)

$m=0$时，$a^{n}*a^{0}=a^{n}*e=a^{n}=a^{n+0}$，显然成立

设$m=k$时，有$a^{n}*a^{k}=a^{n+k}$，则$m=k+1$时，

$a^{n}*a^{k+1}=a^{n}*(a^{k}*a)=(a^{n}*a^{k})*a=a^{n+k}*a=a^{n+k+1}$

$\therefore m.n\geq 0$时，有$a^{n}*a^{m}=a^{n+m}$

8.2 群的定义与性质

当$n<0, m\geq 0$时，令$n=-t$，则$t>0$ $a^n*a^m=a^{-t}*a^m=(a^{-1})^t*a^m$

$$=\begin{cases} a^{-t+m}*\underbrace{a^{-1}*a^{-1}*\cdots*a^{-1}}_{m个}*\underbrace{a*a*\cdots*a}_{m个}=a^{-t+m}=a^{n+m} & (t\geq m) \\ \underbrace{a^{-1}*a^{-1}*\cdots*a^{-1}}_{t个}*\underbrace{a*a*\cdots*a}_{t个}*a^{m-t}=a^{m-t}=a^{n+m} & (t<m) \end{cases}$$

同理，其它情况均有$a^n*a^m=a^{n+m}$

(4) 当$m,n\geq 0$时，由归纳法，易得$(a^n)^m=a^{nm}$

当$m<0$时，令$m=-t$，则$t>0$

$$(a^n)^m=(a^n)^{-t}=((a^n)^{-1})^t=((\underbrace{a*a*\cdots*a}_{n个})^{-1})^t=(\underbrace{a^{-1}*a^{-1}*\cdots*a^{-1}}_{n个})^t$$

$$=((a^{-1})^n)^t=(a^{-1})^{nt}=a^{-nt}=a^{mn}$$

当$n<0$时，令$n=-t$，则$t>0$

$$(a^n)^m=(a^{-t})^m=((a^{-1})^t)^m=(a^{-1})^{tm}=a^{-tm}=a^{mn}$$

8.2 群的定义与性质

- **3. 群的性质**
- **定理8.5：** 设<G,*>为群，则

(1)：方程a*x=b，y*a=b在G中有解且有唯一解；

(2)：当 $G \neq \{e\}$时，无零元；

(3)：G中所有元素都是可约的，即$\forall a, x, y \in G$，有 a*x=a*y=>x=y，x*a=y*a=>x=y；

(4)：运算表中任意一行(列)都没有两个相同的元素；

(5)：群G中除幺元e外无其它幂等元。

8.2 群的定义与性质

证：(1)先证$a^{-1}*b$是方程$a*x=b$的解：代入，则

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

再证唯一性：设c为方程$a*x=b$的解，即$a*c=b$，则

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

同理$b*a^{-1}$是方程$y*a=b$的唯一解

(2)若G有零元，且$G\neq\{e\}$，则$|G|\geq 2$，由定理7.5，知零元无逆元与G为群矛盾

(3)$x=e*x=(a^{-1}*a)*x=a^{-1}*(a*x)=a^{-1}*(a*y)=(a^{-1}*a)*y=e*y$

(4)反证法：设某一行有两个相同元素，设为a，行的表头为b，列的表头分别为c_1,c_2，显然$c_1\neq c_2$，而$a=bc_1=bc_2\Rightarrow c_1=c_2$，矛盾

(5)反证法：设a是G中非幺的幂等元，即$a*a=a$，且$a\neq e$，因此$a*a=a*e$，由(3)得$a=e$，矛盾

8.2 群的定义与性质

- 定义8.6：若群G为有限集合，则称G为有限群(Finite Group)，否则称为无限群(Infinite Group)，群G的基数称为群的阶(Order)。

由定理8.5知：G为有限群时，*运算的运算表中每一行(列)都是G中元素的一个全排列，因此，当G分别为1,2,3阶群时，*运算都只有一种定义方式：如下

*	e
e	e

*	e	a
e	e	a
a	a	e

*	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

8.2 群的定义与性质

- **4. 元素的阶及性质**
- 定义8.7：设<G,*>为群，$a \in G$，满足等式 $a^n = e$ 的最小正整数n称为a的阶(Order)或周期，记作|a|=n，若不存在这样的正整数n，称a是无限阶。

例：(1)任何群G的幺元e的阶为1，且只有幺元的阶为1；

(2)<Z,+>中幺元0的阶为1，其它整数均为无限阶元

(3) $<Z_4,+_4>$ 中[1]的阶为4，[2]的阶为2，[3]的阶为4。

- 定理8.6：有限群G的每个元素都有有限阶，且其阶数不超过群G的阶数|G|。

8.2 群的定义与性质

证：设a为G的任一元素，考虑$e=a^0,a^1,a^2,\cdots,a^{|G|}$这$|G|+1$个$G$中的元素，由于$G$中只有$|G|$个元素，由鸽巢原理，它们中至少有2个是同一元素，不妨设：$a^s=a^t(0\le s<t\le|G|)$于是$a^{t-s}=e$，因此a有有限阶，且阶数是$t-s$，且不超过$|G|$.

- **定理8.7：设<G, *>为群，**$a\in G$，且$|a|=r$**，设k为整数，则**

(1) $a^k=e$当且仅当$r\,|\,k$

(2) $|a^{-1}|=|a|$

8.2 群的定义与性质

证 (1)先证充分性：设$a^r=e$且$r\mid k$，设$k=mr$(m为整数)，则

$a^k=a^{mr}=(a^r)^m=e^m=e$

再证必要性：设$a^k=e$且$k=mr+i, (0\le i<r)$则

$e=a^k=a^{mr+i}=a^{mr}*a^i=a^i$,

由r的最小性得$i=0$，即$r\mid k$

(2) $(a^{-1})^r=(a^r)^{-1}=e^{-1}=e$，$\therefore a^{-1}$的阶存在，令$|a^{-1}|=t$，由(1)知

$t\mid r$，而$(a^{-1})^{-1}=a$，则$a^t=((a^{-1})^{-1})^t=((a^{-1})^t)^{-1}=e^{-1}=e$

$\therefore r\mid t, \therefore r=t$，即$|a|=|a^{-1}|$

8.2 群的定义与性质

- **例8-5：设G是n阶有限群，证明：**

(1) G中阶大于2的元素个数一定是偶数；

(2) 若n是偶数，则G中阶等于2的元素个数一定是奇数。

证：(1)设$A=\{x \mid x\in G, x$的阶大于$2\}$，则：$\forall a\in A, a^{-1}\neq a$，否则

$a^2=a^{-1}*a=e$与$a\in A$矛盾

因为a与a^{-1}的阶相同，且a^{-1}相对于a是唯一的，所以

$\forall a\in A$，a与a^{-1}成对出现，故G中阶大于2的元素个数一定是偶数。

(2)当n是偶数时，因为G中阶大于2的元素个数一定是偶数，所以G中阶小于等于2的元素个数也是偶数，由于阶为1的元素是唯一的幺元e，因此G中阶等于2的元素一定是奇数。

8.2 群的定义与性质

- 定义8.8：设<G,*>为一群，若*运算满足交换律，则称G为交换群，或阿贝尔群(Abel group)，阿贝尔群又称加群，常表示为<G,+>，加群的幺元常用0表示，常用-x表示x的逆元。

例：<Z,+>，<Q,+>，<R,+>。

- 定理8.8：设<G,*>为一群， <G,*>为阿贝尔群的充要条件是对 $\forall x, y \in G$，有(x*y)*(x*y)=(x*x)*(y*y).

8.2 群的定义与性质

证：必要性：设$<G,*>$为阿贝尔群，则$\forall x,y\in G$，

有$x*y=y*x \quad \therefore (x*x)*(y*y)=x*(x*y)*y$

$=x*(y*x)*y=(x*y)*(x*y)$

充分性：设$\forall x,y\in G$，有$(x*y)*(x*y)=(x*x)*(y*y)$

而$x*(x*y)*y=(x*x)*(y*y)=(x*y)*(x*y)=x*(y*x)*y$

由消去律，可得$x*y=y*x$

$\therefore <G,*>$为阿贝尔群

8.3 子群

- 定义8.9：设<G, *>为群，$H \neq \emptyset$，如果<H, *>为G的子代数，且<H, *>为一群，则称<H, *>为G的子群(Subgroups)，记作H≤G。若H是G的子群，且 $H \subset G$ 则称H是G的真子群，记作H<G。

例：<Z, +>是<Q, +>的子群，<Q, +>是<R, +>的子群，<R, +>是<C, +>的子群。

- 1. 子群的判定定理

- 定理8.9（判定定理一）：设<G, *>为群，那么<H, *>为<G, *>的子群的充要条件是：

(1).G的幺元$e \in H$，(2)若$a, b \in H$，则$a * b \in H$，

(3)若$a \in H$，则$a^{-1} \in H$

8.3 子群

证：必要性：设H为子群

(1).设$<H,*>$的幺元为e'，对$\forall x \in H \subseteq G$，则$e' * x = x = e * x$

由于$*$满足消去律，故$e' = e \therefore e \in H$.

(2)H是子代数，由定义知，(2)成立

(3)设$<H,*>$中任一元素a在H中的逆元为b，则$a * b = b * a = e$

而$H \subseteq G$，则$a,b \in G$，由逆元的唯一性，b是a在G中的逆元，

即$b = a^{-1} \in H$

充分性：事实上仅(2),(3)可得$<H,*>$为$<G,*>$的子群，

H为非空时，(2),(3)蕴含(1).

8.3 子群

- **定理8. 10（判定定理二）：设<G, *>为群，H是G的非空子集，那么<H, *>为<G, *>的子群的充要条件是：** $\forall a,b\in H$，有$a*b^{-1}\in H$

证：必要性：任取$a,b\in H$，由于H是G的子群，

则$b^{-1}\in H, \therefore a*b^{-1}\in H$

充分性：H非空，必存在$a\in H$，取$b=a$，则$a*a^{-1}\in H$，

即$e\in H$

任取$a\in H$，由$e,a\in H$，有$e*a^{-1}\in H$，即$a^{-1}\in H$

任取$a,b\in H$，则$b^{-1}\in H$，则$a*(b^{-1})^{-1}\in H$，即$a*b\in H$

由定理8.9知：$<H,*>$为$<G,*>$的子群。

8.3 子群

- **定理8. 11 （判定定理三）：设<G, *>为群，H是G的非空有限子集，那么<H, *>为<G, *>的子群的充要条件是：**$\forall a,b \in H$，有$a*b \in H$

证：必要性：显然

充分性：H为非空有限集，设$|H|=k$，$a \in H$，考虑

$S=\{a^1,a^2,\cdots,a^{k+1},\cdots\} \subseteq H$

由鸽巢原理，因此必有$a^i=a^j(0 \le i < j \le k+1)$，从而由消去律，

得$a^{j-i}=e$，故$e \in H$.

若$H=\{e\}$, $<H,*>$为G的子群

若$H \ne \{e\}$，设a为H中任意一个不同于e的元素，则$j-i \ge 2$

$\therefore a^{j-i}=a^{j-i-1}*a=e \quad \therefore a*a^{j-i-1}=a^{j-i}=e$，因此$a^{-1}=a^{j-i-1} \in H$

由定理8.9知：$<H,*>$为$<G,*>$的子群。

8.3 子群

- **2. 特殊子群**
- **例8-5：设G为群，**$a \in G$，令$H=\{a^k \mid k \in Z\}$**，即a的所有幂构成的集合，则H是G的子群，称为由a生成的子群，记作<a>，a称为生成元。**

证：$a \in \langle a \rangle, \therefore \langle a \rangle \neq \emptyset$，任取$a^m, a^n \in \langle a \rangle$，有：

$$a^m * (a^n)^{-1} = a^m * a^{-n} = a^{m-n} \in \langle a \rangle$$

由定理8.11知：$H \le G$

➢**由a生成的子群是包含a的最小子群。**

例：对Klein四元群，其每个元素生成的子群分别是：<e>={e}，<a>={e, a}，<b>={e, b}，<c>={e, c}

对<Z, +>而言：<0>={0}, <1>={0, 1, -1, 2, -2, ···}=Z

<2>={0, 2, -2, 4, -4, ···}= $\{2k \mid k \in Z\} = 2Z$

8.3 子群

- **例8-6：设G为群，令C是G中所有元素都可交换的元素构成的元素集合，即：**$C=\{a \mid a\in G\wedge \forall x\in G(ax=xa)\}$ **则C是G的子群，称为G的中心。**

证：首先e与G中所有元素都可交换，$\therefore e\in C$且$C\neq\emptyset$

任取$a,b\in C$，要证$ab^{-1}\in C$，即ab^{-1}与G中所有元素可交换

$\forall x\in G$，有$(ab^{-1})x=ab^{-1}x=ab^{-1}(x^{-1})^{-1}=a(x^{-1}b)^{-1}=a(bx^{-1})^{-1}$

$=a(xb^{-1})=axb^{-1}=xab^{-1}=x(ab^{-1})$

由定理8.10知：C为G的子群

➢ **对于阿贝尔群G，G中所有元素都可交换，G的中心就等于G，对于某些非交换群G，G的中心是{e}。**

8.3 子群

- **例8-7：设G为群，H，K是G的子群，则：**

(1).$H \cap K$是G的子群， (2).$H \cup K$是G的子群当且仅当 $H \subseteq K$或$K \subseteq H$

证： (1)由于$e \in H, e \in K$， $\therefore e \in H \cap K$，即$H \cap K$非空，

任取$a \in H, a \in K, b \in H, b \in K \quad \therefore ab^{-1} \in H, ab^{-1} \in K$

$\therefore ab^{-1} \in H \cap K$

由定理8.10，命题成立；

(2)必要性：用反证法，假设$H \not\subseteq K$且$K \not\subseteq H$，则存在h和k

使得$h \in H \wedge h \notin K, k \in K \wedge k \notin H$,

则$hk \notin H$，否则由$h^{-1} \in H$，可得$k = h^{-1}(hk) \in H$，矛盾

同理$hk \notin K$，则$hk \notin H \cup K$，与$H \cup K$是子群矛盾

充分性：显然

$\therefore$命题成立

8.3 子群

- **3. 构造G的全部子群的方法**
- 1. 第0层：{e}
- 2. 第1层：⟨a⟩：$a \neq e \wedge <a> \neq G \wedge \neg(\exists b)(<b> \subset <a>)$
- 3. 第2层：⟨b⟩：$\exists b(<a> \subset <b>) \wedge \neg(\exists c)(<a> \subset <c> \subset <b>)$
- ……

例：$<Z_{12}, +_{12}>$

0层：{0}；

1层：⟨1⟩= Z_{12}，⟨2⟩=⟨10⟩={0, 2, 4, 6, 8, 10}，⟨3⟩=⟨9⟩={0, 3, 6, 9}，⟨4⟩=⟨8⟩={0, 4, 8}，⟨5⟩=⟨7⟩= Z_{12}，⟨6⟩={0, 6}　∴⟨4⟩, ⟨6⟩;

8.3 子群

2层：〈6〉⊂〈3〉，〈〈4〉∪〈6〉〉=〈2〉=〈10〉 ∴〈2〉,〈3〉

3层：〈〈2〉∪〈3〉〉，即G。

- 子群格：G为群，S={H|H≤G}，$R:\forall A,B\in S$，ARB〈=〉A≤B，〈S, R〉构成偏序集，称为群G的子群格。

8.4 陪集与拉格朗日定理

- **1. 群中子集合的乘积**
- 定义8.10：设<G,*>为群，$A, B \subseteq G$，且A，B非空，则 $AB = \{a * b \mid a \in A, b \in B\}$ 称为A，B的乘积。
- (1)一般地：|AB|≠|A||B|，当G可交换时，AB=BA
- (2)当A={a}时，记{a}B=aB
- (3)性质：设<G,*>为群，$A, B, C \subseteq G$，且A，B，C非空，则：i):(AB)C=A(BC)；ii):eA=Ae=A
- 定义8.11：设<H,*>为<G,*>的子群，任一 $g \in G$，称gH为H的左陪集(Left coset)，称Hg为H的右陪集(Right coset)，这里：

$$gH = \{g * h \mid h \in H\} \quad Hg = \{h * g \mid h \in H\}$$

8.4 陪集与拉格朗日定理

例：G为Klein四元群，H={e，a}是G的子群，则H的所有右陪集为：He={e，a}=H，Ha={a，e}=H，Hb={b，c}，Hc={c，b}

- 2. 陪集的性质
- 定理8.12：设<H, *>为<G, *>的子群，则：

(1). 对任意$g \in G$，$|gH| = |H| \; (|Hg| = |H|)$

(2). 当$g \in H$时，$gH = H \; (Hg = H)$

8.4 陪集与拉格朗日定理

证： (1)只要证H与gH之间存在双射即可。定义函数$f:H\to gH$

如下：对任何$h\in H$，有$f(h)=g*h.$

设$h_1\neq h_2$，则$f(h_1)=g*h_1 \quad f(h_2)=g*h_2$，

若$f(h_1)=f(h_2)$，由消去律得：$h_1=h_2$，与$h_1\neq h_2$矛盾，$\therefore f$为单射

显然f为满射，f为双射，即$|gH|=|H|$

同理：$|Hg|=|H|$

(2)由gH定义知：$gH\subseteq H$，下面证明$H\subseteq gH$，由$g\in H$得$g^{-1}\in H$

设$h\in H$，则$g^{-1}*h\in H$，从而$g*(g^{-1}*h)\in gH$，即$h\in gH$

由h的任意性：得$H\subseteq gH$，即$H=gH$，同理：$Hg=H$

8.4 陪集与拉格朗日定理

- **定理8.13：设<H, *>为<G, *>的子群，有：**

$(1): a \in aH \quad (2):$ 若$b \in aH$，则$bH = aH$

证： $(1):$因为H为G的子群，$\therefore e \in H$，则$a = a * e \in aH$

$(2):$若$b \in aH$，则存在$h \in H$，使$b = ah$，$bH = (ah)H = a(hH)$

由定理8.12中(2)知：$hH = H$， $\therefore bH = aH$

此定理对右陪集也成立。

- **定理8.14：任意两陪集或相同或不相交，即设<H, *>为<G, *>的子群，**

$\forall a, b \in G$，则或者$aH = bH \, (Ha = Hb)$，

或者$aH \cap bH = \emptyset \, (Ha \cap Hb = \emptyset)$

8.4 陪集与拉格朗日定理

证：只要证明$aH \cap bH \neq \emptyset \Rightarrow aH = bH$即可。

设$aH \cap bH \neq \emptyset$，即$\exists c \in aH \cap bH$，$\therefore \exists h_1, h_2 \in H$，使得

$a * h_1 = c = b * h_2$，$\therefore a = b * h_2 * h_1^{-1}$

为证$aH \subseteq bH$，设$x \in aH$，则$\exists h_3 \in H$，使得

$x = a * h_3 = (b * h_2 * h_1^{-1}) * h_3 \in bH$，$\therefore x \in bH$

$\therefore aH \subseteq bH$，同理：$bH \subseteq aH$

于是$aH = bH$，同理：$Ha \cap Hb \neq \emptyset \Rightarrow Ha = Hb$

$\therefore$命题成立

8.4 陪集与拉格朗日定理

- **定理8. 15：设<H, *>为<G, *>的子群，** $\forall a,b\in G$ **，有：a，b属于H的同一左陪集<=>** $a^{-1}*b\in H$

证：设a,b属于H的同一左陪集，则有$g\in G$，设$a,b\in gH$，

因而有$h_1,h_2\in H$，使得：$a=g*h_1$，$b=g*h_2$，

于是$a^{-1}*b=(g*h_1)^{-1}*g*h_2=h_1^{-1}*h_2\in H$

反之，设$a^{-1}*b\in H$，即有$h\in H$，使$a^{-1}*b=h$，因而

$b=a*h\in aH$，而$a\in aH$，即a，b在同一左陪集aH中。

利用陪集还可以定义陪集等价关系。

8.4 陪集与拉格朗日定理

- **定理8.16：设<H, *>为<G, *>的子群，则** $R=\{<a,b>|a,b\in G,a^{-1}*b\in H\}$ **是G上的等价关系，且** $[a]_R=aH$ **，称R为群G上H左陪集等价关系。**

证明：先证R是等价关系

(1)：$\forall a\in G$，$a^{-1}\in G,\therefore a^{-1}*a=e\in H,\therefore <a,a>\in R$，即$R$自反，

(2)：若$<a,b>\in R$，有$a^{-1}*b\in H,\because H$是G的子群$,\therefore (a^{-1}*b)^{-1}\in H$，

即$b^{-1}*a\in H,\therefore <b,a>\in R$，即$R$对称，

(3)：若$<a,b>\in R,<b,c>\in R$，则有$a^{-1}*b\in H,b^{-1}*c\in H$，而

$(a^{-1}*b)*(b^{-1}*c)=a^{-1}*c\in H,\therefore <a,c>\in R,\therefore R$传递，

即R是G上的等价关系；

8.4 陪集与拉格朗日定理

再证$[a]_R = aH$

$b \in [a]_R \Leftrightarrow bRa \Leftrightarrow a^{-1} * b \in H \Leftrightarrow a,b$属于$H$的同一左陪集$\Leftrightarrow b \in aH$

- **定义8.11：设<H, *>为<G, *>的子群，对$\forall a,b \in G$，如果有$a * b^{-1} \in H$，则称a，b为模H同余关系，记为：$a \equiv b \bmod (H)$**

➢ **由定理8.16知：H的所有左陪集构成了G的一个划分，同样地，H的所有右陪集也构成了G的一个划分，令S={Ha|a∈G}，T={aH|a∈G}，还可证明|S|=|T|。**

8.4 陪集与拉格朗日定理

定义$f:S\to T$：$f(Ha)=a^{-1}H$，$\forall a\in G$，则f为双射，因为：

$\forall a,b\in G$，有$Ha=Hb\Leftrightarrow ab^{-1}\in H\Leftrightarrow(ab^{-1})^{-1}\in H\Leftrightarrow$

$(b^{-1})^{-1}a^{-1}\in H\Leftrightarrow a^{-1}H=b^{-1}H$,

$\therefore\forall Ha,Hb\in S$，若$Ha\neq Hb$，则$f(Ha)\neq f(Hb)$，否则

$f(Ha)=f(Hb)\Leftrightarrow a^{-1}H=b^{-1}H\Leftrightarrow Ha=Hb$矛盾，$\therefore f$单射；

$\forall bH\in T$，则$Hb^{-1}\in S$，且有$f(Hb^{-1})=(b^{-1})^{-1}H=bH$，$\therefore f$满射；

$\therefore f$为双射，$\therefore|S|=|T|$。

- **H在G中的左陪集数和右陪集数相等，统称为H在G中的陪集数，也叫H在G中的指数，记为[G:H]。**

由以上分析可导出拉格朗日定理。

8.4 陪集与拉格朗日定理

- **定理8. 17：设G是有限群，H是G的子群，则 |G|=|H| · [G:H]。**

证：设$[G:H]=r$，$a_1,a_2,\cdots a_r$分别是H的r个右陪集的代表元素，

由定理8.16知：$G=Ha_1\cup Ha_2\cup\cdots\cup Ha_r$，而这$r$个右陪集不相交，

$\therefore |G|=|Ha_1|+|Ha_2|+\cdots+|Ha_r|$，而$|Ha_i|=|H|$

$\therefore |G|=|H|\cdot r=|H|\cdot[G:H]$

- **拉格朗日逆定理不成立，因此，据此定理只可判别一子代数“非子群”，却不可用它来判别一个子代数“是子群”。**

8.4 陪集与拉格朗日定理

- **推论1：设G是n阶群，则$\forall a \in G$，|a|是n的因子，且$a^n = e$**

证：任取$a \in G$，则$\langle a \rangle$是G的子群，由定理8.17知：

$\langle a \rangle$的阶是n的因子；

而$\langle a \rangle$是由a生成的子群，$|a| = r$，则$\langle a \rangle$

$= \{a^0 = e, a^1, a^2, \cdots, a^{r-1}\} \therefore \langle a \rangle$的阶与$|a|$相等，$\therefore |a| \,|\, n$

由定理8.7知：$a^n = e$

- **推论2：质数阶的群没有非平凡子群。**

证：若有非平凡子群，则其子群的阶必是原来群的阶的一个因子，与原来群的阶是质数矛盾。

8.4 陪集与拉格朗日定理

- **推论3：设<G, *>是群且|G|=4，则G同构与4阶循环群C_4或Klein四元群D_2。**

证：设$G=<e,a,b,c>$，其中e是幺元，因为元素的阶是1,2,4,

若有4阶元a则$|a|=4, <a>=\{e,a,a^2,a^3\}\cong C_4$($\cong$表示同构)

若G中无4阶元，则G中有一个幺元，剩余3个均为2阶元，

即：$a^2=b^2=c^2=e, a*b$不可等于a,b或e，

否则导致：$b=e, a=e$或$a=b \quad \therefore a*b=c$，同样的：

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

因此这个群是Klein 四元群D_2

8.5 正规子群与商群

- **1. 正规子群**
- 定义8.12：设<H,*>为<G,*>的子群，如果对任一 $g \in G$，有gH=Hg，则称H是G的正规子群，记作$H \trianglelefteq G$
- (1)：任何群都有正规子群：G，{e}；
- (2)：当G为阿贝尔群时，G的所有子群都是正规子群；
- (3)：正规子群要求gH=Hg，但并不意味着g与H中的每个元素相乘都是可交换的；
- (4)：正规子群的左陪集和右陪集统称为陪集。

正规子群的判定定理

8.5 正规子群与商群

- **定理8. 17：设<H, *>为<G, *>的子群，<H, *>是<G, *>的正规子群当且仅当** $\forall g \in G, \forall h \in H$，有$g * h * g^{-1} \in H$

证：必要性，任取$g \in G$，$h \in H$，由$gH = Hg$可知，存在$h_1 \in H$，

使得$g * h = h_1 * g$，则有$g * h * g^{-1} = h_1 * g * g^{-1} = h_1 \in H$；

充分性，任取$g * h \in gH$，由$g * h * g^{-1} \in H$，知，存在$h_1 \in H$，

使得$g * h * g^{-1} = h_1$，即$g * h = h_1 * g \in Hg$，则有：$gH \subseteq Hg$

反之，取$h * g \in Hg$，由$g^{-1} \in G$，$g^{-1} * h * (g^{-1})^{-1} \in H$，即

$g^{-1} * h * g \in H$，则存在$h_1 \in H$，使得$g^{-1} * h * g = h_1$，

从而有$h * g = g * h_1 \in gH, \therefore Hg \subseteq gH$

$\therefore \forall g \in G$，有$gH = Hg$

8.5 正规子群与商群

- **2. 商群**

利用群的正规子群可以诱导出一个新的群，这个群比原来的群简单却又保留了原来群的许多性质。

设<H, *>为<G, *>的正规子群，H在G中的所有陪集形成一个集合，即G/H={gH|g∈G}（或{Hg|g∈G}），在G/H上定义运算∘：

$\forall g_1, g_2 \in G$，有$[g_1]\circ[g_2]=[g_1 * g_2]$，即

$$g_1H \circ g_2H = (g_1 * g_2)H \text{或} Hg_1 \circ Hg_2 = H(g_1 * g_2)$$

- **定理8.18：** 设<H, *>为<G, *>的正规子群，群G的商代数系统< G/H, ∘ >构成群。

8.5 正规子群与商群

证：(1).封闭性显然；

(2).$\circ$运算可结合，对$\forall x, y, z \in G$，有$(xH \circ yH) \circ zH = (x * y)H \circ zH$

$= ((x * y) * z)H = (x * (y * z))H = xH \circ (y * z)H = xH \circ (yH \circ zH)$;

(3).含幺元；$eH = H$为幺元，对$\forall g \in G$有，$gH \circ eH = (g * e)H = gH$

$= eH \circ gH$;

(4).含逆元；对$\forall g \in G$有，$gH \circ g^{-1}H = (g * g^{-1})H = eH = H$

$= g^{-1}H \circ gH$;

$\therefore < G / H, \circ >$构成群。

8.5 正规子群与商群

- **定义8.13：群G的正规子群H的所有陪集在运算**
$g_1H\circ g_2H=(g_1*g_2)H$ 下形成的群G/H称为G关于H的商群，显然，当G为有限群时，|G|/|H|=|G/H|。
- **例8-8：H={[0],[3]}，H为群$<Z_6,+_6>$的正规子群，于是H的左右陪集为：**

$[0]+_6H=H+_6[0]$：$\{[0],[3]\}$；$[1]+_6H=H+_6[1]$：$\{[1],[4]\}$；

$[2]+_6H=H+_6[2]$：$\{[2],[5]\}$；则$<Z_6,+_6>$有商群：

$<\{[0],[3]\},\{[1],[4]\},\{[2],[5]\},\oplus>$，其中$\oplus$满足：

$(a+_6H)\oplus(b+_6H)=(a+_6b)H$

8.5 正规子群与商群

- **3. 群同态**

如果存在群 G_1 到群 G_2 上的同态映射，则称群 G_1 与 G_2 同态，若同态映射是双射，则称群 G_1 与 G_2 同构。

- **定理8. 19：设 φ 是群 G_1 到群 G_2 上的同态映射，e_1, e_2 分别为 G_1 和 G_2 的幺元，则：**

$$(1)\varphi(e_1)=e_2,\quad (2)\varphi(a^{-1})=\varphi(a)^{-1},\quad \forall a\in G_1$$

- **定理8. 20：群<G, *>与它的每个商群<G/H, ο>同态**

证：在G与G/H之间建立对应：φ：$g\to gH$，$g\in G$，显然φ是G到G/H的映射，而且对$\forall x,y\in G$，有：$x*y\to(x*y)H=xH\circ yH$，即$\varphi(x*y)=\varphi(x)\circ\varphi(y)$

$\therefore\varphi$是G到G/H上的一个同态映射。

8.5 正规子群与商群

- **定理8. 21：设 φ 是群 $<G_1,*_1>$ 到群 $<G_2,*_2>$ 的同态映射，那么 φ 的核K(φ)构成 $<G_1,*_1>$ 的正规子群**

$(K(f)=\{x \mid x\in G_1 \wedge \varphi(x)=e_2\})$

证：先证: $<K(\varphi),*_1>$ 是 $<G_1,*_1>$ 的子群；

$\because \varphi(e_1)=e_2 \quad \therefore e_1\in K(\varphi)$，$K(\varphi)$ 非空，

任取 $a,b\in K(\varphi)$，则 $\varphi(a*_1 b^{-1})=\varphi(a)*_2\varphi(b)^{-1}=e_2*_2 e_2{}^{-1}=e_2$

$\therefore a*_1 b^{-1}\in K(\varphi), \quad \therefore K(\varphi)\le G$

再证 $K(\varphi)$ 为正规子群

任取 $a\in K(\varphi), x\in G_1$，则 $\varphi(x*_1 a*_1 x^{-1})=\varphi(x)*_2\varphi(a)*_2\varphi(x^{-1})$

$=\varphi(x)*_2 e_2*_2\varphi(x^{-1})=\varphi(x*_1 x^{-1})=\varphi(e_1)=e_2$

$\therefore x*_1 a*_1 x^{-1}\in K(\varphi) \quad \therefore K(\varphi)\trianglelefteq G_1$

8.5 正规子群与商群

- **定理8. 22：** **设 φ 是群 $<G_1,*_1>$ 到群 $<G_2,*_2>$ 的同态映射，K=K（φ），那么商群 $<G_1/K,\circ>$ 与同态像 $<\varphi(G_1),*_2>$ 同构。**

证：在 G_1/K 与 $\varphi(G_1)$ 之间建立如下对应：

σ: $(xK)\to\varphi(x), x\in G_1$

(1): σ 是映射：对 G_1/K 中的任意元素 xK，取 xK 中的任意代表元素 xk，则有 $\varphi(x*_1k)=\varphi(x)*_2\varphi(k)=\varphi(x)*_2e_2=\varphi(x)$

$\therefore$ 在 φ 下，G_1/K 中的任意元素 (xK) 在 $\varphi(G_1)$ 中只有一个像；

(2): σ 是满射：对于 $\varphi(G_1)$ 中任意元素 b，由于 φ 是 G_1 到 $\varphi(G_1)$ 的满射，故 b 在 G_1 中至少存在一个像源 a，即 $\varphi(a)=b$，相应的，对 a 而言，b 在 G_1/K 中就至少存在一个像源 aK，即说明 σ 是满射；

8.5 正规子群与商群

$(3):\sigma$是单射：如果$xK\neq yK$，则$x^{-1}*_1 y\notin K$，从而有，

$\varphi(x^{-1}*_1 y)\neq e_2$，即$\varphi(x)^{-1}*_2\varphi(y)\neq e_2$，即$\varphi(x)\neq\varphi(y)$;

$(4):\sigma$保持运算关系：

$$\sigma(xK\circ yK)=\sigma((x*_1 y)K)=\varphi(x*_1 y)$$

$$=\varphi(x)*_2\varphi(y)=\sigma(xK)*_2\sigma(yK)$$

$\therefore\sigma$为G/K与$\varphi(G_1)$之间的同构映射。

- **例8-9：设h为群$<Z_6,+_6>$到群$<Z_3,+_3>$的同态映射，使得h(x)=2x(mod3)，即h(0)=h(3)=0, h(1)=h(4)=2，h(2)=h(5)=1, 于是K=K(h)={0, 3}，则$<K,+_6>$为$<Z_6,+_6>$的正规子群，所以：**

  $<Z_6/K,\oplus>=<\{0,3\},\{1,4\},\{2,5\},\oplus>$同构于$<Z_3,+_3>$，同构映射

  σ：$Z_6/K\to Z_3$满足：$\sigma(\{0,3\})=0$，$\sigma(\{2,5\})=1$，$\sigma(\{1,4\})=2$

8.6 特殊群：循环群与置换群

- **1. 循环群**
- **定义8.14：** 设G为群，若存在 $a \in G$，使得$G=\{a^k \mid k \in z\}$

则称G为循环群，即G中的任何元素都是a的幂（a^0=e），记为<a>。

例：（1）<Z, +>为循环群，1或-1为生成元；

（2）$A=\{2^i \mid i \in Z\}$，则 $<A,\bullet>$ 为循环群，2是生成元。

➢ 循环群G=<a>分为n阶循环群和无限循环群；

若a是n阶元，则 $G=\{a^0=e, a^1, a^2, \cdots, a^{n-1}\}$，且|G|=n

若a是无限阶元，则$G=\{a^0=e, a^{\pm 1}, a^{\pm 2}, \cdots\}$

8.6 特殊群：循环群与置换群

- 1. 循环群的性质
- 定理8.23：设G=<a>是循环群：

(1) 若G是无限循环群，则G只有两个生成元，即a和a^{-1}，且<G, *>同构于<Z, +>;

(2) 若G是n阶循环群，则G含有$\varphi(n)$（小于或等于n且与n互素的正整数r的个数，欧拉函数）个生成元，即a^r为生成元，且<G, *>与$<Z_n,+_n>$同构。

证：(1)：任取$a^k \in G$，则$a^k=(a^{-1})^{-k}$，即$a^k \in <a^{-1}>$，从而有$G \subseteq <a^{-1}>$

而a^{-1}显然满足$<a^{-1}> \subseteq G$，$\therefore G=<a^{-1}>$

再证明只有a和a^{-1}，若$G=<b>$，由$a \in G$知，存在整数s，使得$a=b^s$，

而由$b \in G$和存在整数t，使得$b=a^t$，

$\therefore a=b^s=(a^t)^s$，用消去律得：$a^{ts-1}=e$，

$\because G$是无限群，$\therefore ts-1=0 \quad \therefore t,s=1$或$-1$，即$b=a$或$b=a^{-1}$;

8.6 特殊群：循环群与置换群

(2)：需证：对任何真整数$r(r \le n)$，a^r是G的生成元当且仅当r与n互素，

充分性：设r与n互素，则，存在整数u和v使得：$ur+vn=1$，

则$a=a^{ur+vn}=(a^r)^u(a^n)^v$，由拉格朗日定理推论1知：$a^n=e$

$\therefore a=(a^r)^u \quad \therefore \forall a^k \in G$，有$a^k=(a^r)^{uk} \in <a^r>$，即$G \subseteq <a^r>$

而$<a^r> \subseteq G$(显然) $\quad \therefore G=<a^r>$;

必要性：设a^r是G的生成元，则$|a^r|=n$，令$d=GCD(r,n)$，

则$r=dt$(t为正整数)

$\therefore (a^r)^{\frac{n}{d}}=(a^{dt})^{\frac{n}{d}}=(a^n)^t=e$，$\therefore$由定理8.7得：$n\,|\,\frac{n}{d} \quad \therefore d=1$

8.6 特殊群：循环群与置换群

- **定理8.24：设G=<a>是循环群，则(1)G的子群仍是循环群；(2)若G=<a>为无限循环群，则G的子群除{e}外，都是无限循环群；(3)若G=<a>为n阶循环群，则对n的每个正因子d，G恰好有一个d阶子群**

证：(1)设H是$G=<a>$的子群，$H=\{e\}=<e>$，显然成立

$H\neq\{e\}$，那么H中有$a^k(k\neq 0)$，而H为子群，$\therefore a^{-k}\in H$，

不失一般性,设$k>0$且是H中元素a最小正整数指数,则任意

的$a^m\in H$,有：令$m=pk+q(0\leq q<k)$，则$a^m=a^{pk+q}=a^{pk}*a^q$

$\therefore a^q=a^{-pk}*a^m$，由于$a^{-pk}$，$a^m\in H$，$\therefore a^q\in H$，由$k$的最小性

得$q=0$，$\therefore a^m=a^{pk}=(a^k)^p\in<a^k>$，即$H$为循环群；

(2)设$G=<a>$是无限循环群，H是G的子群，若$H\neq\{e\}$，令

$H=<a^k>$，若$|H|=t$，则$|a^k|=t$，即$a^{kt}=e$，

与a为无限循环元矛盾；

8.6 特殊群：循环群与置换群

(3)设$G=<a>=\{a^0=e,a^1,a^2,\cdots,a^{n-1}\}$，由拉格朗日定理，$G$的每个子群的阶都是$n$的因子，对于$n$的任一个正因子$d$，易知：$H=<a^{\frac{n}{d}}>$是$G$的$d$阶子群，

唯一性：若$H_1=<a^m>$也是G的d阶子群，其中a^m是H_1中最小正次幂元，则$(a^m)^d=e$，$n\mid md$，即$\frac{n}{d}\mid m$，令$m=\frac{n}{d}\cdot l$，

则$a^m=a^{\frac{n}{d}\cdot l}=(a^{\frac{n}{d}})^l\in H$，$\therefore H_1\subseteq H$，又$|H_1|=|H|=d$

$\therefore H_1=H$

- **3. 求循环群子群的方法**

G=<a>：无限：{e}和$<a^m>$，m为自然数；n阶：对每个n的因子d，有$<a^{\frac{n}{d}}>$

8.6 特殊群：循环群与置换群

- **4. 置换群**

在介绍函数时，我们介绍了置换的概念。

➢ **(1) 置换本质上是一个有限集合上的双射函数，例如：**

$$S=\{1,2,3,4,5\},\quad \sigma=\begin{pmatrix}1 & 2 & 3 & 4 & 5\\ 5 & 3 & 2 & 1 & 4\end{pmatrix}$$

➢ **(2)** $S=\{a_1,a_2,\cdots,a_n\}$的n元置换$\sigma=\begin{pmatrix}a_1 & a_2 & \cdots & a_n\\ \sigma(a_1) & \sigma(a_2) & \cdots & \sigma(a_n)\end{pmatrix}$

中 $\sigma(a_1),\sigma(a_2),\cdots,\sigma(a_n)$是$a_1,a_2,\cdots,a_n$ **的一个排列，共有n!个**

➢ **(3)** σ **的逆函数** σ^{-1} **为逆置换**

➢ **(4) 置换的复合就是两个函数的的复合函数，如：**

8.6 特殊群：循环群与置换群

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

$$\sigma\tau(a_i)=\tau(\sigma(a_i))\quad \tau\sigma(a_i)=\sigma(\tau(a_i))$$

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

- **(5) 任何n元置换可以表示成不相交的转换（循环）之积，且表示唯一，如：**

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

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

8.6 特殊群：循环群与置换群

这里补充两个概念：

- **(6) 对换：** $\sigma=(i_1,i_2,\cdots,i_k)=(i_1i_2)(i_1i_3)\cdots(i_1i_k)=\tau$，**每个转换可表示成一些对换之积：**

$$\sigma(i_j)=i_{j+1}$$

$$\tau(i_j)=\tau_2\tau_3\cdots\tau_k(i_j)=\tau_k(\tau_{k-1}(\cdots(\tau_2(i_j))\cdots))$$

$$=\tau_k(\cdots(\tau_j(i_j))\cdots)=\tau_k(\cdots(\tau_{j+1}(i_1))\cdots)$$

$$=\tau_k(\cdots(\tau_{j+2}(i_{j+1}))\cdots)=i_{j+1}$$

$$\sigma(i_k)=i_1 \quad \tau(i_k)=i_1$$

例： σ =(15236) (78)=(15) (12) (13) (16) (78)

8.6 特殊群：循环群与置换群

- **(7) 所有的n元置换构成的集合 S_n，$<S_n, \circ>$ 构成群：封闭，可结合，幺元，恒等置换(1)，逆置换 σ^{-1}**

例：$S_3 = \{(1),(12),(13),(23),(123),(132)\}$

n元置换群：$<\{(1)\},\circ>$，$<\{(1),(23)\},\circ>$，

$<\{(1),(13)\},\circ>$，$<\{(1),(12)\},\circ>$，

$<\{(1),(123),(132)\},\circ>$，$<S_3,\circ>$