第十章：群与环

- 第一节：群的定义及其性质
- 第二节：子群
- 第三节：循环群与置换群

第十章：群与环

第一节：群的定义及其性质

第二节：子群

第三节：循环群与置换群

群的定义与性质

定义 设<G,*>是一个代数系统,*是G上的二元运算,如果*在G上成立结合律,
a*(b*c)=(a*b)*c 则称<G,*>为半群。

例

(1)$<Z^+,+>$,<Z,+>,<N,+>,$<Z^+,*>$,<N,*>,<Q,*>等是半群。R^+表示正实数集合,$<R^+,+>$,$<R^+,*>$是半群。

(2)$<M_n(R),+>$是半群, $M_n(R)$ n阶矩阵的全体, +为矩阵加法

(3)<P(A),⊕>是半群。

群的定义与性质

定义　对于*运算，拥有幺元的半群称为独异点。

例：**<N,+,0>,<N,*,1>**均为独异点。

例：设**S**为非空集合，**P(S)**是**S**的幂集，则**<P(S), ∪,Ø>,<P(S), ∩,S>**均为独异点。

而**<Z,max>**，其中**max(x,y)**取二者之大值；**<Z,min>**，其中**min(x,y)**取二者之小值。均不为独异点（不存在幺元）。

<N,max,0>

为独异点，其中幺元为**0**。

群的定义与性质

例:设集合$N_n=\{0,1,\ldots,n-1\}$在N_n上定义运算$+_n$。

$$(a+_n b)+_n c=(a+b+c)(\mathrm{mod}\ n)$$

$$a+_n(b+_n c)=(a+b+c)(\mathrm{mod}\ n)$$

因此,$+_n$在N_n上运算封闭且成立结合律因而$<N_n,+_n>$是半群。

$<N_n,+_n,0>$是独异点。

群的定义与性质

定义 设<G,*>是半群,且二元运算*还满足。

（1）存在$e\in G$, $\forall x\in G, e*x=x*e=x$,即G中存在幺元。

（2） $\forall x\in G, \exists x^{-1}\in G$,使$x*x^{-1}=x^{-1}*x=e$,即每个元素均存在逆元。则称<G,*>是群。

即群<G,*>要求

①运算*满足确定性,封闭性。

②*满足结合律。

③G中存在幺元。

④G中每个元素存在逆元。

群的定义与性质

例1:〈Z,+〉是群,幺元是0,逆元是相反数。

同样〈Q,+〉,〈R,+〉也是群。

例2:〈$M_n(R)$,•〉, •为矩阵乘法运算

不是群,存在幺元是单位矩阵I_n,逆元是逆矩阵,但有的矩阵不存在逆矩阵。

如果$M_n(R)$的子集$S_n(R)$=所有可逆矩阵的全体

〈$S_n(R)$, •〉是群,其运算封闭,且每个矩阵均存在逆矩阵。

群的定义与性质

例3:$<N_6,+_6>$,其中$N_6=\{0,1,2,3,4,5\}$,
幺元是0, $1+_65=0,2+_64=0,3+_63=0$

∴1,5互为逆元,2,4互为逆元,3的逆元是3,0的逆元是0,

∴$<N_6,+_6>$是群。

例4:<P(A),⊕>,P(A)是A的幂集

⊕是环和运算，满足结合律。

因∀B∈P(A),B⊕∅=∅⊕B=B, B⊕B=∅

所以幺元是∅,每个元素的逆元就是其本身。

群的定义与性质

定义

1）若群**G**是有穷集，则称**G**是有限群，否则称为无限群。群**G**的基数称为群**G**的阶。

2）只含单位元的群称为平凡群。

3）若群**G**中的二元运算是可交换的，则称**G**为交换群或阿贝尔群。

群的定义与性质

群中元素的幂次

定义　设<G,*>是一个群，且a∈G,n∈N，则

（1）a的0次幂定义为：$a^0 = \ell, a^1 = a^0 * a, \cdots, a^{n+1} = a^n * a$

（2）a的负幂次定义为：$a^{-n} = \underbrace{a^{-1} * a^{-1} * \mathrm{L} * a^{-1}}_{n\ a^{-1}} = (a^{-1})^n$

群的定义与性质

定义　设<G,*>是一个群，且a∈G，若存在一个正整数n，能使$a^n=e$，则称元素a的阶是有限的，而最小的n称为元素a的阶。若不存在这样的元素n，则称元素a拥有无限阶。

幺元的阶为1，

∵$e^1=e$。

四元群中，e的阶为1；

a,b,c的阶都为2。

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

群的定义与性质

定理 设**G**为群，则**G**中的幂运算满足:

1) $\forall a \in G, (a^{-1})^{-1} = a$

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

3) $\forall a \in G, a^n a^m = a^{n+m}, n, m \in Z$

4) $\forall a \in G, (a^n)^m = a^{nm}, n, m \in Z$

5) 若G为交换群，则 $(ab)^n = a^n b^n$

群的定义与性质

2）证明：

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

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

所以$(a*b)^{-1}=b^{-1}*a^{-1}$成立。

推广到一般形式有：

$$(a_1*a_2*\cdots*a_n)^{-1}=a_n^{-1}*\cdots*a_2^{-1}*a_1^{-1}$$

群的定义与性质

定理　**<G,*>**是群，**∀a,b∈G,**方程**a*x=b**和**y*a=b,**在**G**中存在唯一解。

说明:

因为群未必成立交换律

∴ $a^{-1}*b$和$b*a^{-1}$未必相等

∴**a*x=b**和**y*a=b**的解未必相等

群的定义与性质

例：代数系统$G=<P(\{a,b\}), \oplus>$是群。解下列方程：

$$\{a\} \oplus x = \varnothing,\ y \oplus \{a,b\} = \{b\}$$

解：$x = \{a\}^{-1} \oplus \varnothing = \{a\} \oplus \varnothing = \{a\}$

$$y = \{b\} \oplus \{a,b\}^{-1} = \{b\} \oplus \{a,b\} = \{a\}$$

群的定义与性质

定理 设<G,*>是群,则∀a,b,c∈G

(1) 如a*b=a*c 则b=c。

(2) 如b*a=c*a 则b=c。

证明:因为群中的每一个元素都有逆元，因此只要两边同左乘a^{-1},即可得(1)

(2)也同理

问题：如果a*b=c*a,是否可以得到b=c?

群的定义与性质

例：设**G**为群，**a,b**∈**G**，且 $(ab)^2=a^2b^2$

证明**ab=ba**。

证： $(ab)^2=(ab)(ab)=abab$

$=a^2b^2=aabb$

因为群的运算满足消去律，所以有

ab=ba 。

群的定义与性质

定理 若群<G,*>的元素a拥有有限阶n，则

1）$a^k=e$，当且仅当k是n的整数倍。

2）群中的元素和它的逆元具有相同的阶，$|a^{-1}|=|a^1|$。

证明：1）

- 充分性，由于k是n的整数倍，必存在整数m使得k=mn, 所以有$a^k= a^{mn}= (a^n)^m= e$。
- 必要性，存在整数m和i，使得k=mn+i, 从而有$e= a^{mn+i}= a^{mn}\ a^i= a^i$,因为a的阶是n，并且$0\le i\le n-1$，所以i=0。

则k是n的整数倍

群的定义与性质

2） 由于$(a^{-1})^n = (a^{-n})^1 = e^{-1} = e$。

可知a^{-1}的阶是存在的。令$|a^{-1}| = t$，根据上面的证明有n是t的整数倍。这说明a的逆元的阶是a的阶的因子。而a又是a^{-1}的逆元，所以a的阶也是a^{-1}的阶的因子，故有t是n的整数倍。从而证明了$n=t$，即$|a^{-1}| = |a^1|$。

群的定义与性质

《定理》 一个群中，除了幺元e之外，不存在其它等幂元素。

证明：若任一a∈G，有a*a=a的话，则a=e。

$$\because \quad e = a*a^{-1} = (a*a)*a^{-1} = a*(a*a^{-1}) = a*e = a$$

《定理》 群<G,*>的运算表中的每一行或每一列都是G中元素的一个置换。

群的定义与性质

根据群的以上性质，可得出下列结论：

一阶群只有一个：

$*$	ℓ
ℓ	ℓ

二阶群也仅有一个：

$*$	ℓ	a
ℓ	ℓ	a
a	a	ℓ

三阶群也为一个：

$*$	ℓ	a	b
ℓ	ℓ	a	b
a	a	b	ℓ
b	b	ℓ	a

群的定义与性质

四阶群有二个：

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

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

五阶群仅有一个：

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

群的定义与性质

六阶群有二个：

$*$	e	a	b	c	d	f
e	e	a	b	c	d	f
a	a	b	c	d	f	e
b	b	c	d	f	e	a
c	c	d	f	e	a	b
d	d	f	e	a	b	c
f	f	e	a	b	c	d

$*$	e	a	b	c	d	f
e	e	a	b	c	d	f
a	a	e	d	f	b	c
b	b	f	e	d	c	a
c	c	d	f	e	a	b
d	d	c	a	b	f	e
f	f	b	c	a	e	d

群的定义与性质

七阶群有一个：

$*$	e	a	b	c	d	f	g
e	e	a	b	c	d	f	g
a	a	b	c	d	f	g	e
b	b	c	d	f	g	e	a
c	c	d	f	g	e	a	b
d	d	f	g	e	a	b	c
f	f	g	e	a	g	c	d
g	g	e	a	b	c	d	f

证明可根据群的定义。任何一阶，二阶，……，七阶群均和以上的群同构。

群的定义与性质

例,设有代数系统<Z,*>运算*的定义如下：

a,b∈Z,a*b=a+b-2,试证<Z,*>是群。

证明:

*满足确定性，唯一性，是Z上代数运算。

*满足结合律：a,b,c∈Z,(a*b)*c=(a+b-2)*c=a+b+c-4

a*(b*c)=a*(b+c-2)=a+b+c-4 ∴*满足结合律

*有幺元：a∈Z,a*2=a+2-2=a, 2*a=a ∴幺元是2

Z中每个元素有逆元： a∈Z,(4-a)*a = a*(4-a)=(4-a)+a-2=2

∴a的逆元是4-a

∴<Z,*>是群。

第十章：群与环

第一节：群的定义及其性质

第二节：子群

第三节：循环群与置换群

子群

- 子群
  - <G,*>是群,H是G的(非空)子集,如果H关于G的运算*构成群,则称H为G子群
  - 记作H≤G

子群

说明:

(1)<H,*>是子群, 要求

①H对于运算*是封闭的

②G的幺元e在H内

③H的每个元素的逆元仍在H内(对逆运算封闭)

至于运算的确定性和结合律,由于在G中成立,对于H必然成立。

(2)如H构成子群,必然是非空的,至少有幺元e。

(3)<G,*>有两个平凡子群,

H′={e},<H′,*>是子群,还有是G本身。

子群

例:$<R,+>$是群,$<Z,+>$是子群。$<N,+>$不是子群。

例:$<N_6,+_6>$是群。$H_1=\{0,2,4\}$

则$<H_1,+_6>$是子群,

因$2+_62=4\in H_1,4+_64=2\in H_1$,2,4互为逆元等等。

但$H_2=\{0,1,5\}$,$< H_2,+_6>$不是子群

$1+_61=2\notin H_2,5+_65=4\notin H_2$,$H_2$对运算$+_6$不封闭。

可以验证$<\{0,3\},+_6>$也是子群。

子群

- 子群的判定定理一

设<G,*>是群，H⊆G,<H,*>是子群的充要条件是以下三条同时成立

（1） H非空

（2） 如果a∈H,b∈H,则a*b∈H

（3） 若a∈H,则a^{-1}∈H

证明：必要性是显然成立。

充分性，因H非空,取a∈H, 知a^{-1}∈H,

由条件(2)有$a*a^{-1}$∈H

∴e∈H, 从而<H,*>是子群。

子群

- 子群的判定定理二

<G,*>是群,H⊆G,<H,*>是子群的充要条件是

(1)H非空　(2)∀x,y∈H, 均有$x*y^{-1}\in H$

证明：必要性。

任取x,y∈H.由于H是G的子群，必有$y^{-1}\in H$ ，从而$x*y^{-1}\in H$ 。

充分性。因为H非空，必存在x∈H，根据给定条件得$x*x^{-1}\in H$，即e∈H 。

设a是H的任一元素，即a∈H ,由e,a∈H得$e*a^{-1}\in H$,即$a^{-1}\in H$。任取a,b∈H,由刚才的证明知$b^{-1}\in H$。根据给定条件知$a*(b^{-1})^{-1}\in H$,即a*b∈H

根据上一定理可知<H,*>是<G,*>的子群。

子群

子群的判定定理三

<G,*>是群,H⊆G,如果H是有穷集，<H,*>是子群的充要条件是

(1)H非空　(2)∀x,y∈H, 均有x*y∈H

证明：设**a**是**H**的任一元素，即**a∈H**，据判断定理一，只需证明$a^{-1}\in H$。

若**a＝e**，则$a^{-1}= e^{-1} = e \in H$。

若**a≠e**，令 $S=\{a,a^2,\ldots\}$

则**S ⊆H**。由于**H**是有穷集，必有$a^i= a^j\ (i<j)$。根据消去律得$a^{j-i}= e$，由**a≠e**可知**j-i>1**，由此得

$a^{j-i-1} *a = e$和$a*a^{j-i-1} = e$

从而证明了$a^{-1}=a^{j-i-1}\in H$。

子群

例：设G为群，a∈G，令

$$H=\{a^k \mid k \in Z\}$$

即a的所有的幂构成的集合，证明H是G是子群，称为由a生成的子群，记作<a>。

证明：首先由a∈<a>知道<a>不为空，任取$a^m, a^l \in <a>$，则$a^m(a^l)^{-1} = a^m a^{-l} = a^{m-l} \in <a>$

根据判断定理二可知。

例如整数加群，由2生成的子群是

$$<2>=\{2k \mid k \in Z\}=2Z$$

子群

例：设G为群，已知$a^{-1}=a$，证明G中与a可交换的元素构成G的子群.

证　　令$H=\{x \mid x\in G \wedge xa=ax\}$, 下面证明$H$是$G$的子群.
首先e属于H，H是G的非空子集.
任取$x, y \in H$，有

$$(xy^{-1})\,a = x(y^{-1}a) = x(a^{-1}y)^{-1} = x(ay)^{-1}$$
$$= x(ya)^{-1} = xa^{-1}y^{-1} = xay^{-1} = axy^{-1} = a(xy^{-1})$$

因此 xy^{-1}属于H. 由判定定理二命题得证.

- 分析：
- 证明子群可以用判定定理，特别是判定定理二.
- 证明的步骤是：
- 验证 H 非空
- 任取 $x, y\in H$，证明$xy^{-1}\in H$

子群

拉格朗日定理 一个有限群的阶一定能被它子群的阶所整除。即 $k = |G| / |H| \quad k \in I_+$

此定理可以确定子群的可能的阶数，但不能确定子群的元素，且同样阶的子群（除平凡子群外）的个数可能很多。

子群

推论

1）质数阶的群没有非平凡子群（<{e},*>和<G,*>叫做群<G,*>的平凡子群）

2）在有限群<G,*>中，任何元素的阶必是|G|的一个因子。因为如果a∈G是r阶的，则<{e,a,a^2,…,a^{r-1}},*>是<G,*>的子群，r必整除|G|。

练习

例：设群G的运算表如表所示，找出群G所有的子群。

	a	b	c	d	e	f
a	a	b	c	d	e	f
b	b	c	d	e	f	a
c	c	d	e	f	a	b
d	d	e	f	a	b	c
e	e	f	a	b	c	d
f	f	a	b	c	d	e

第十章：群与环

第一节：群的定义及其性质

第二节：子群

第三节：循环群与置换群

循环群和置换群

- 循环群
  - 群中存在一个元素$a \in G$,使G中的元素可用$\{a^k \mid k \in Z\}$表示
  - 记作$G=<a>$
- 无限循环群
  - 循环群中不存在一个非零整数n,使得$a^n=e$,则$G=\{e,a,a^2,\ldots a^n \ldots\}$
- 例如$<Z,+>$是循环群,其中1或-1是生成元（生成元可以不唯一）,任意正整数$n=1^n$,负整数$-n=1^{-n}$。

循环群和置换群

- 如果存在一个最小的正整数n,使得$a^n=e$,则G有n个元素,$G=\{e,a,a^2,\ldots a^{n-1}\}$,称<G,*>的周期为n。n阶循环群。

循环群和置换群

例：$<N_4, +_4>$是循环群，运算表为：

$+_4$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

幺元为0，1或3是生成元。

$1^4 = 1 +_4 1 +_4 1 +_4 1 = 0$,周期为4。

$1^3 = 1 +_4 1 +_4 1 = 3$,

$1^2 = 1 +_4 1 = 2$,

$1^1 = 1$。

循环群和置换群

- 循环群必然是交换群

- 交换群未必是循环群
  - 例如四阶群不是循环群,但是它是交换群，在四阶群**G＝｛a,b,c,d｝,$b^2=c^2=d^2=a$,G**不是由某个元素生成的。

$*$	a	b	c	d
a	a	b	c	d
b	b	a	d	c
c	c	d	a	b
d	d	c	b	a

循环群和置换群

例,设有代数系统<Z,*>运算*的定义如下：

a,b∈Z,a*b=a+b-2,试证<Z,*>是循环群。

证明: *满足确定性，唯一性，是Z上代数运算。

a,b,c∈Z,(a*b)*c=(a+b-2)*c=a+b+c-4

a*(b*c)=a*(b+c-2)=a+b+c-4 ∴*满足结合律

a∈Z,a*2=a+2-2=a, 2*a=a ∴幺元是2

a∈Z,(4-a)*a = a*(4-a)=(4-a)+a-2=2

∴a的逆元是4-a

∴<Z,*>是群。

因为，$1^{-2}=(1*1)^{-1}=4, 1^{-1}=3, 1^0=2$，$1^1=1$

，$1^2=1*1=1+1-2=0, 1^3=1*1*1=0+1-2=-1,\ldots,$

∴1是生成元。3也是生成元。

循环群和置换群

定理　设$G=\langle a\rangle$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}。

2）若G是n阶循环群，则G含有h(n)(欧拉函数)个生成元，对于任意小于等于n且与n互素的正整数r，a^r是G的生成元。

例

证明：

1）显然$\langle a^{-1}\rangle \subseteq G$。为证明$G \subseteq \langle a^{-1}\rangle$，只需证明对任意$a^k \in G$，　a^k都可以表示成a^{-1}的幂。由定理11.1有 $a^k=(a^{-1})^{-k}$

循环群和置换群

从而得到$G=<a^{-1}>$，a^{-1}是G的生成元。

再证明G只有a和a^{-1}这两个生成元。假设b也是G的生成元，则$G=<b>$，由$a\in G$可知存在整数t使得$a=b^t$。又由$b\in G=<a>$知存在整数m使得$b=a^m$。

从而得到$a=b^t=(a^m)^t=a^{mt}$

由G中消去律得$a^{mt-1}=e$，因为G是无限群，必有$mt-1=0$。从而证明了$m=t=1$或$m=t=-1$，即$b=a$或$b=a^{-1}$。

2) 只需证明：对任意正整数**r(r≤n)**, **a^r**是**G**的生成元当且仅当**n**与**r**互素。

充分性，设**r**与**n**互素，且**r≤n**，那么存在整数**u**和**v**使得**ur＋vn＝1**

因此由定理**11.1**和拉格朗日定理的推论有

$$a= a^{ur+vn}=(a^r)^u(a^n)^v= (a^r)^u$$

这就推出对任意$a^k \in G$，$a^k=(a^r)^{uk} \in \langle a^r \rangle$，即$G \subseteq \langle a^r \rangle$。另一方面，显然有$\langle a^r \rangle \subseteq G$。所以**$a^r$**是**G**的生成元。

循环群和置换群

必要性: a^r是G的生成元→ n与r互素

a^r是G的生成元，则$|a^r|=n$。令r与n的最大公约数为d，则存在正整数t使得$r=dt$。因此有

$$(a^r)^{n/d}=(a^{dt})^{n/d}=(a^n)^t=e$$

根据定理11.4知$|a^r|$是n/d的因子，即n整除n/d。从而证明了$d=1$。

循环群和置换群

例：$<N_4, +_4>$是循环群，运算表为：

$+_4$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

。幺元为0，已知1为生成元小于等于4且与4互素的数有1，3。所以$1^3=3$也是生成元。

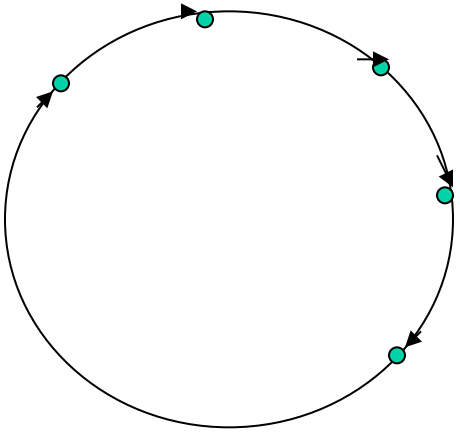
循环群和置换群

- 例： 设$G=\{e, a, \ldots, a^{11}\}$是12阶循环群，小于12且与12互素的数是1, 5, 7, 11,可知 a, a^5, a^7 和 a^{11}是G的生成元

- 例： 设$G=3Z=\{3z \mid z\in Z\}$, G上的运算是普通加法. 那么G只有两个生成元：3和−3

循环群和置换群

循环群的结构图示



有限循环群

无限循环群

循环群和置换群

定义

- **f**是非空集合**A**上的函数，称**f**为集合**A**上的变换
- 若**f**为一对一（双射）函数，则**f**称为一一变换（置换）
- 除一对一函数以外的函数**f**称为多一变换

讨论定义：

（1）**A**到**A**的变换个数为： $|A|^{|A|}$（个）

（2）**A**到**A**的一一变换个数为：$|A|!$（个）

循环群和置换群

例：设**A={1,2}**，定义**f:A→A**，则有四个变换，其中有二个置换，二个多一变换。

即：

$$\left.\begin{array}{l} f_1=\begin{pmatrix}1 & 2\\ 1 & 2\end{pmatrix} \\ f_2=\begin{pmatrix}1 & 2\\ 2 & 1\end{pmatrix}\end{array}\right\rangle$$

置换**2!=2** 个

$$\left.\begin{array}{l} f_3=\begin{pmatrix}1 & 2\\ 1 & 1\end{pmatrix} \\ f_4=\begin{pmatrix}1 & 2\\ 2 & 2\end{pmatrix}\end{array}\right\rangle$$

多一变换2^2 **-2!=2** 个。

循环群和置换群

代数系统<S, ◇ >，S={f_1,f_2,f_3,f_4}，
“◇”为复合运算

列出运算表：

◇	f_1	f_2	f_3	f_4
f_1	f_1	f_2	f_3	f_4
f_2	f_2	f_1	f_3	f_4
f_3	f_3	f_4	f_3	f_4
f_4	f_4	f_3	f_3	f_4

循环群和置换群

定义

一个**n**个元素的有限集合上的全部置换的集合及其复合运算所构成的群称为**n**元对称群。

一个有限集合上的若干个置换及其右合成运算所组成的群称为**n**元置换群。

置换群一定是对称群的子群。

循环群和置换群

例：设A={1,2,3}（有$3^3=27$种变换，有3!=6种置换），A上所有置换的集合

$$P=\{P_1,P_2,P_3,P_4,P_5,P_6\}$$

$$P_1=\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}\quad P_2=\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}\quad P_3=\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}$$

$$P_4=\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}\quad P_5=\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}\quad P_6=\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}$$

循环群和置换群

$\Diamond$	P_1	P_2	P_3	P_4	P_5	P_6
P_1	P_1	P_2	P_3	P_4	P_5	P_6
P_2	P_2	P_1	P_5	P_6	P_3	P_4
P_3	P_3	P_6	P_1	P_5	P_4	P_2
P_4	P_4	P_5	P_6	P_1	P_2	P_3
P_5	P_5	P_4	P_2	P_3	P_6	P_1
P_6	P_6	P_3	P_4	P_2	P_1	P_5

<P, ◇>是群，3元对称群

$S_1=\{P_1,P_2\}$,$S_2=\{P_1,P_3\}$,

$S_3=\{P_1,P_4\}$,$S_4=\{P_1,P_5,P_6\}$。

则< S_1, ◇> , < S_2,◇>, < S_3,◇>, < S_4,◇>均为置换群

练习

- 设A={1,2}，B是A上的等价关系的集合。
  - 列出B的元素。
  - 给出代数系统V=<B, ∩>的运算表。
  - 求出V的单位元、零元和所有可逆元素的逆元。
  - 说明V是否为半群、独异点和群。

练习

- 1）2个元素集合上只有两种划分，因此只有2个等价关系，即$B=\{I_A, E_A\}$。
- 2）V的运算表如下。
- 3）V的单位元是E_A，零元是I_A，可逆元素只有E_A，其逆元是E_A。
- 4）V为半群，独异点，不是群。

练习

例：设 H_1, H_2分别是群G 的 r, s 阶子群，若r和s互素，证明$H_1 \cap H_2 = \{e\}$.

证 $H_1 \cap H_2 \leq H_1$，$H_1 \cap H_2 \leq H_2$. 由Lagrange定理，$|H_1 \cap H_2|$整除r，也整除s. 从而 $|H_1 \cap H_2|$ 是整除 r与s 的最大公因子. 因为r和s互素, 从而 $|H_1 \cap H_2| = 1$. 即 $H_1 \cap H_2 = \{e\}$.

练习

例：设群G的运算表如表所示，问G是否为循环群？如果是，求出它所有的生成元.

解

易见 a 为单位元.

由于$|G|=6$, $|b|=6$, 所以 b 为生成元. $G=<b>$为循环群. $|f|=6$, 因而 f 也是生成元

$|c|=3$, $|d|=2$, $|e|=3$, 因此 c,d,e不是生成元.

	a	b	c	d	e	f
a	a	b	c	d	e	f
b	b	c	d	e	f	a
c	c	d	e	f	a	b
d	d	e	f	a	b	c
e	e	f	a	b	c	d
f	f	a	b	c	d	e