4.2 群与子群

4.2.1 群

定义4 设$<S,*>$是一个代数系统，$*$是S上的一个二元运算，若满足

（1） 运算$*$是可结合的；------半群

（2） 存在幺元e；------独异点

（3） 对于每一个元素$x \in S$，存在它的逆元$x^{-1} \in S$，称$<S,*>$是一个群。

例3　设$G=\{e,a,b,c\}$，$\circ$为G上的二元运算

运算表如下

$\circ$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

说明$<G,\circ>$是一个群。

解　由$\circ$的运算表知，运算封闭且满足结合律，e是幺元，且

$$e^{-1}=e,\ a^{-1}=a,\ b^{-1}=b,\ c^{-1}=c$$

故$<G,\circ>$是一个群。

此群有下面特征：

1）e 为 G 的幺元；

2）$\circ$ 是可交换的；

3） G 中的任何元素与自己运算的结果是幺元，即自己是自己的逆元；

4） 除幺元外的三个元素 a,b,c ，任何两个元素运算的结果都是另一个元素。

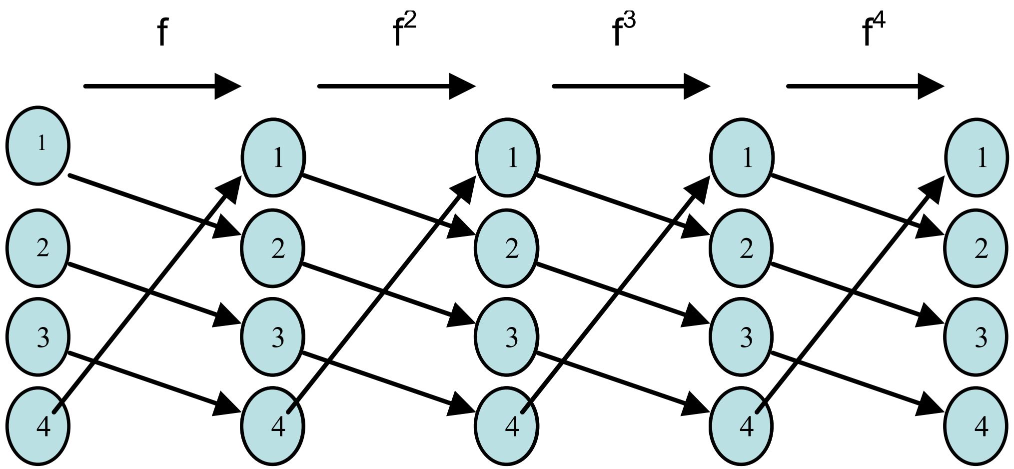
一般称这种群为 *Klein* （克莱因）四元群。

例4　设 $X=\{1,2,3,4\}$，函数 $f:X\to X$ 定义

$$f=\{<1,2>,<2,3>,<3,4>,<4,1>\}$$

设 f^0 是 X 上的恒等函数，构造

$$f\circ f=f^2,\ f^2\circ f=f^3,\ f^3\circ f=f^4$$



则 $f^4 = f^0$， 令 $F = \{f^0, f^1, f^2, f^3\}$

可以验证，复合运算在 F 上是封闭的，并满足结合律，f^0是关于复合运算$\circ$的幺元，f^0的逆元是自身，$f^i(i=1,2,3)$ 的逆元是 f^{4-i}，所以$<F,\circ>$是一个群。

下表是它的复合运算表

$\circ$	f^0	f^1	f^2	f^3
f^0	f^0	f^1	f^2	f^3
f^1	f^1	f^2	f^3	f^0
f^2	f^2	f^3	f^0	f^1
f^3	f^3	f^0	f^1	f^2

从上表可知，任何不同的两行或两列均不相同；每一行或每一列中均不出现重复的元素换句话说，表中每一行或每一列都是属于群的全部元素的一个全排列（群的普遍性质）。

定义5　设$<G,*>$是一个群，若G是一个有限集，称$<G,*>$是有限群，G中元素的个数称为该有限群的阶数，记为$|G|$；若G是无限集，称$<G,*>$是无限群。

前面所讨论的$<F,\circ>$群和$Klein$ 4元群都是有限群，且阶数均为4。

例5 验证代数系统 $<Z,+>$ 是一个群，此处 Z 是整数集， $+$ 是普通加法运算。

解 二元运算 $+$ 在 Z 上封闭且满足结合律，幺元是0，对于任一 $\alpha \in Z$，其逆元 $-\alpha \in Z$，故 $<Z,+>$ 是一个群，且是一个无限群。

3/31/2020 9:55 AM

由于群$<G,*>$中有逆元，定义负幂

$$\forall x \in G \quad (n \in Z^{+})$$

$$x^{-n} = (x^{-1})^{n} \quad ; \quad x^{0} = e \quad ; \quad x^{n+1} = x^{n} * x$$

定义6 设$<G,\circ>$是群，$x\in G$，使得$x^k=e$成立的**最小正整数**k称为x的**阶数**（或**周期**）记为$|x|$。

若不存在正整数k，使得$x^k=e$成立，称x是**无限阶**的。

例 在群 $<Z,+>$ 中，只有 0 的阶数是1，其余元素都是无限阶的。

例 在 ***Klein*** 四元群中，a,b,c 的阶数均为2，e 的阶数是1。

例 在模 6 的加群 $<Z_6,\oplus>$ 中，0是幺元

$$2\oplus 2\oplus 2=0\Rightarrow |2|=3\,;\quad 3\oplus 3=0\Rightarrow |3|=2\,;$$

同理 $|1|=|5|=6\,;\ |4|=3\,;\ |0|=1$

定义7 若群$<G,*>$中的运算$*$是可交换的称该群为**交换群**，也称为**阿贝尔群**。

例 整数集 Z 上的加法群$<Z,+>$、非零实数 $R-\{0\}$ 上的乘法群$<R-\{0\},\times>$，均是交换群。

不是所有的群都是交换群

例6 设 G 为所有 n 阶非奇异（满秩）矩阵的集合，矩阵乘法运算 $\bullet$ 作为定义在集合 G 上的二元运算，试说明 $<G,\bullet>$ 是一个不可交交换群。

解 1）运算 $\bullet$ 是封闭的；（任意两个 n 阶非奇异矩阵相乘后，仍然是一个非奇异矩阵）

2）运算是可结合的；（矩阵乘法满足结合律）

3）存在幺元;（n 阶单位矩阵 E 是 G 的幺元）

4）每个元素存在逆元。（任意一个非奇异矩阵 A，逆元是其逆矩阵 A^{-1}，$A^{-1} \bullet A = A \bullet A^{-1} = E$）

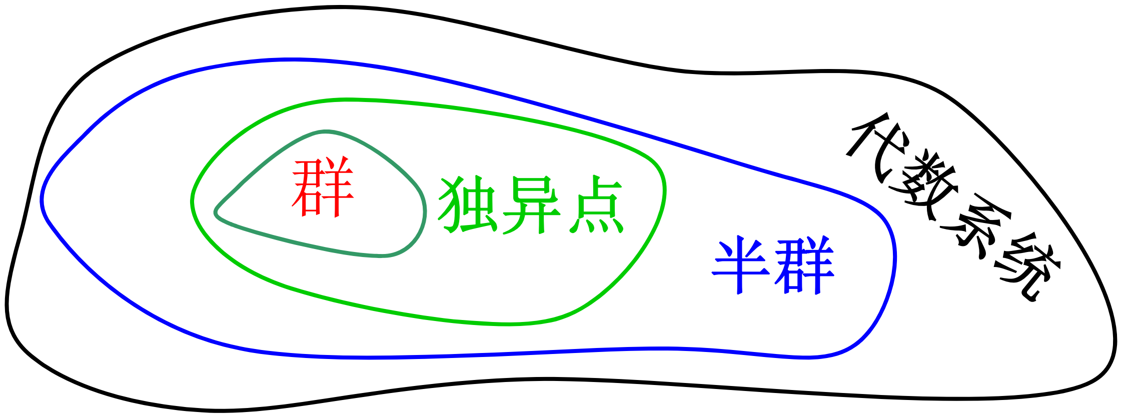
因此 $<G,\bullet>$ 是群。

由于矩阵的乘法不满足交换律，故该群是一个不可交换群。

概括地说，代数系统仅仅是一个具有封闭二元运算的非空集合；半群是一个满足结合律的代数系统；独异点是带有幺元的半群；群是每个元素都有逆元的独异点。

{群}$\subset${独异点}$\subset${半群}$\subset${代数系统}

如图所示



群中任何一个元素的逆元必定是唯一的，由群中逆元的唯一性，有以下几个定理

已学定理　　设 $*$ 是定义在集合 A 上的二元运算，且 A 中的元素的个数大于1，若集合 A 中存在幺元 e 和零元 θ ，则 $e \neq \theta$ 。

证　反证法　若 $e = \theta$，则对 A 中的任意元素 x，有 $x = e * x = \theta * x = \theta = e$，即每个元素均相同，都等于 e ，集合中只有一个元素，矛盾，证毕

多于1个元素的集合中，幺元一定不是零元

定理1 阶数大于1的群中没有零元。

证明 当群的阶数为1时，它的唯一元素视作幺元，否则不是群。

假设$|G|>1$且群$<G,*>$中有零元θ，则

$$\forall x \in G, \quad x*\theta=\theta*x=\theta \neq e$$

即零元θ不存在逆元，与群的定义矛盾，故群中无零元。证毕

定理2 设$<G,*>$是一个群，对于 $a,b \in G$，必存在唯一的 $x \in G\ (y \in G)$，使得

$$a * x = b \ \ (\ y * a = b\ )$$

证明 1）存在性 设 a 的逆元为a^{-1}

令 $x = a^{-1} * b$，则

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

2）唯一性 若另有x_1满足 $a * x_1 = b$，

则 $a^{-1} * (a * x_1) = a^{-1} * b$，即 $x_1 = a^{-1} * b = x$ 证毕

定理3 设$<G,*>$是一个群，$\forall a,b,c \in G$，

$$a*b=a*c\ (b*a=c*a) \Rightarrow b=c$$

群中消去律成立

证明 $a*b=a*c \Rightarrow$

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

$$\Rightarrow e*b=e*c \Rightarrow b=c$$

同理可证 $b*a=c*a \Rightarrow b=c$ 证毕

由此定理知，群的运算表中没有两行（或两列）的元素是相同的。

4.2.2 子群

定义8 设 $<G,*>$ 是一个群，S 是 G 的非空子集，若 $<S,*>$ 也构成群，称 $<S,*>$ 是群 $<G,*>$ 的一个子群。

定理4 设$<G,*>$是一个群，$<S,*>$ 是$<G,*>$的一个子群，则$<G,*>$中的幺元 e 一定是$<S,*>$中的幺元。

证明 设$<G,*>$中的幺元为 e ，$<S,*>$中的幺元为 e_1，$\forall x \in S \subseteq G$， 必有

$$e_1 * x = x = e * x$$

故 $e_1 = e$ 。 证毕

定义9 设$<G,*>$是一个群,$<S,*>$是$<G,*>$的一个子群，若 $S=\{e\}$ 或 $S=G$ ，称$<S,*>$是$<G,*>$的**平凡子群**。

阶数大于1的群，其平凡子群有2个

例7　设$<Z,+>$是一个群，$Z_E=\{x|x=2n, n\in Z\}$，证明$<Z_E,+>$是$<Z,+>$的一个子群。

证　1）$\forall x,y\in Z_E$，不妨设$x=2n_1$，$y=2n_2$，$n_1,n_2\in Z$，则　$x+y=2n_1+2n_2=2(n_1+n_2)\in Z_E$

即$+$在Z_E上封闭；

2）运算$+$在Z_E上保持结合律；

3）$<Z,+>$的幺元$0\in Z_E$是$<Z_E,+>$的幺元

4） $\forall x \in Z_E$，必有 n 使 $x = 2n$

而 $$-x = -2n = 2(-n) \in Z_E$$

$$x + (-x) = 0$$

即 $$x^{-1} = -x \in Z_E$$

故 $<Z_E,+>$ 是 $<Z,+>$ 的一个子群。证毕

定理5 设$<G,*>$是一个群，B是G的非空子集，若B是一个有限集，则只要运算$*$在B上封闭，$<B,*>$必定是$<G,*>$的子群。

证明（略）

例8 设 $G_4=\{p=<p_1,p_2,p_3,p_4>\mid p_i\in\{0,1\}\}$，$\oplus$ 是 G_4 上的二元运算，定义为：对任意的

$$X=<x_1,x_2,x_3,x_4>,Y=<y_1,y_2,y_3,y_4>\in G_4$$

$$X\oplus Y=<x_1\overline{\vee}y_1,x_2\overline{\vee}y_2,x_3\overline{\vee}y_3,x_4\overline{\vee}y_4>$$

其中 $\overline{\vee}$ 的运算表如下

$\overline{\vee}$	0	1
0	0	1
1	1	0

证明 $<\{<0,0,0,0>,<1,1,1,1>\},\oplus>$ 是群 $<G_4,\oplus>$ 的子群。

证　先证 $<G_4,\oplus>$ 是群。对任意

$$X=<x_1,x_2,x_3,x_4>, Y=<y_1,y_2,y_3,y_4>,$$

$$Z=<z_1,z_2,z_3,z_4>\in G_4$$

因为 $x_i \overline{\vee} y_i \in \{0,1\}$，所以 $X\oplus Y\in G_4$；（封闭）

又因为 $(x_i \overline{\vee} y_i)\overline{\vee} z_i = x_i \overline{\vee}(y_i \overline{\vee} z_i)$，所以

$$(X \oplus Y) \oplus Z = X \oplus (Y \oplus Z) \quad \text{（结合律）}$$

$<0,0,0,0>$ 是幺元；　而 $X \oplus X = <0,0,0,0>$，即任一 X，以它自身为逆元。

故 $<G_4, \oplus>$ 是一个群。

其次，由于 $\{<0,0,0,0>,<1,1,1,1>\} \subset G_4$，且 $\oplus$ 在 $\{<0,0,0,0>,<1,1,1,1>\}$ 上是封闭的，由定理5知，$<\{<0,0,0,0>,<1,1,1,1>\},\oplus>$ 是 $<G_4,\oplus>$ 的一个子群。 证毕

定理6 设$<G,\Delta>$是群，S是G的非空子集，如果对于S中的任意元素a和b，有$a\Delta b^{-1}\in S$，则$<S,\Delta>$是群$<G,\Delta>$的子群。

证 先证G中的幺元e也是S中的幺元

$\forall a\in S\subseteq G$，则$e=a\Delta a^{-1}\in S$，且$a\Delta e=e\Delta a=a$

即e也是S中的幺元。

再证S中的每一元素都有逆元。

$\forall a \in S$，因为 $e \in S$，所以 $e\Delta a^{-1} \in S \Rightarrow a^{-1} \in S$

最后证明，运算 Δ 在 S 上是封闭的

$\forall a,b \in S$，由前面证明知 $b^{-1} \in S$，而 $b = (b^{-1})^{-1}$，所以 $a\Delta b = a\Delta(b^{-1})^{-1} \in S$，即运算封闭。

而 Δ 在 S 上保持结合律，所以 $< S,\Delta >$ 是群 $< G,\Delta >$ 的子群。

例9 设$<H,*>$和$<K,*>$都是群$<G,*>$的子群，证明$<H\cap K,*>$也是$<G,*>$的子群。

证 由于幺元$e\in H\cap K$，则$H\cap K$非空，$\forall a,b\in H\cap K$，因为$<H,*>$和$<K,*>$都是$<G,*>$的子群，由$*$分别在H和K中的封闭性知

$$a*b^{-1}\in H\cap K$$

由定理6，$<H\cap K,*>$是$<G,*>$的子群。证毕

定义10 代数系统$<G,*>$中，如果存在$a \in G$,有 $a*a=a$，称 a 为**等幂元**。

定理7 群$<G,*>$中，除幺元 e 外，没有其它等幂元。

证明 因为$e*e=e$，所以 e 是等幂元。

若 $a \in G, a \neq e$，且 $a*a=a$，则有

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

与假设 $a \neq e$ 矛盾。证毕

内容小结

1. 群的定义

2.群及子群的性质

课下练习 P63 习题4.2 1,2,3,4,5,6