设G是群，$\forall a\in G$，则a的**n次幂**($n\in Z$)：

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

有限群群G的阶：G中元素的个数，记作|G|。

元素的阶

定义 设G是群，$a \in G$，使得等式

$$a^k=e$$

成立的**最小的正整数**k叫做a的**阶**(或**周期**)，记作$|a|=k$，称a为**k阶元**；

如果不存在正整数k，使$a^k=e$，则称a为**无限阶元**。

任何群G中单位元e的阶都是 1，$|e|=1$。

元素的阶

例，

1. $<Z_6,\oplus,0>$中，求

   $|0|, |1|, |2|, |3|$？

2. $<Z,+,0>$中，求

   $|0|$, 其它？

元素的阶

例，

3. 在Klein四元群中,|a|, |b|, |c|, |e|?

∘	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

特点：a,b,c三个元素的阶都是2。

群的性质

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. $\forall a_1,a_2,\ldots,a_n \in G, (a_1a_2\ldots a_n)^{-1} = a_n^{-1}\ldots a_2^{-1}a_1^{-1}$
4. $\forall a \in G$，$a^na^m = a^{n+m}$，$m,n \in Z$
5. $\forall a \in G$，$(a^n)^m = a^{nm}$，$m,n \in Z$
6. 若G为交换群，则$(ab)^n = a^nb^n$，$n \in Z$

群的性质

定理：G为群，$\forall a,b\in G$，方程$ax=b$和$ya=b$在G中有解，且有惟一解。

证明：

1. 存在性：$a^{-1}b\in G$是方程$ax=b$的解。
2. 惟一性：

设存在$c\in G$, 满足$ac=b$，

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

同理证ba^{-1}是方程$ya=b$的惟一解。

群的性质

例：设G=<P({a,b}),⊕>，其中⊕为集合的对称差运算，解下列群方程：

$\{a\}\oplus X=\varnothing$

$Y\oplus\{a,b\}=\{b\}$

解：

$$X = \{a\}^{-1}\oplus\varnothing = \{a\}\oplus\varnothing = \{a\}$$

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

群的性质

定理 群中不可能有零元。

定理 G为群，则G中运算满足**消去律**，即对**任意** $a,b,c \in G$有

(1) 若$ab=ac$，则$b=c$。

(2) 若$ba=ca$，则$b=c$。

群的性质

例：

1. 设G为群，a,b∈G，k∈Z^+，证明

   $(a^{-1}ba)^k=a^{-1}ba \Leftrightarrow b^k=b$

证明：

“$\Rightarrow$”：

“$\Leftarrow$”：

2. 设G为群，a,b∈G，且$(ab)^2=a^2b^2$，证明

   $ab=ba$

3. 设$G=\{a_1,a_2,\ldots,a_n\}$是n阶群， $a_i\in G$， 令

$a_iG=\{a_ia_j|j=1,2,\ldots,n\}$

证明$a_iG=G$

1) $a_iG\subseteq G$

2) $|a_iG|=n$

$a_1,a_2,\ldots,a_n$互不相同，

$a_ia_1, a_ia_2,\ldots,a_ia_n$互不相同，

$|a_iG|=n$

所以， $a_iG=G$。

通过运算表判断群

方法：设G为有限群，则G的运算表中的每一行(每一列)都是G中元素的一个排列。

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

群的性质

定理 一个群中，除了单位元e之外，不存在其它幂等元素。

证明：

若存在$a \in G$，有$a*a = a$成立，

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

$= a*(a*a^{-1}) = a*e = a$，则$e = a$。

问题：其它方法？

$a*a = a = a*e \quad \therefore e = a$

群的性质

定理　设G为群，$a \in G$,且$|a|=r$。设k是**整数**，则

(1) $a^k=e \Leftrightarrow r|k$

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

证明:

(1) “$\Rightarrow$”:

对于整数k，$\exists m,i \in Z$，使得$k=mr+i$, $0 \le i < r$

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

因为$|a|=r$，则$i=0$，所以$r|k$。

群的性质

"$\Leftarrow$":

$r|k \Leftrightarrow \exists m \in Z$，使得$k=mr$，有

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

(2) 设$|a^{-1}| = t$

$(a^{-1})^r = (a^r)^{-1} = e$，则$t|r$；

$a^t = ((a^{-1})^{-1})^t = ((a^{-1})^t)^{-1} = e$，则$r|t$，

所以$r=t$，即$|a^{-1}| = |a|$。

群的性质

例：设G为群，$a,b\in G$是有限阶元，证明

1. $|b^{-1}ab| = |a|$
2. $|ab| = |ba|$

子群

子群就是群的子代数。

定义 设G为群，T是G的非空子集，如果T关于G中的运算构成群，则称T为G的子群，记作$T \leq G$。

若T是G的子群，且$T \subset G$，则称T是G的真子群，记作$T < G$。

例，在群$<Z,+>$中，取

$$2Z=\{2x \mid x \in Z\}$$

则2Z关于加法构成$<Z,+>$的(真)子群。

同样，$\{0\}$也是$<Z,+>$的真子群。

子群

平凡子群：G，{e}

例，Klein四元群G={e,a,b,c}有5个子群，它们是：

{e}, {e,a}, {e,b}, {e,c}, G

- 平凡子群是…
- 真子群是…

子群判定定理

定理一：设G为群，T是G的非空子集。T是G的**子群**当且仅当下面的条件成立：

1. $\forall a,b \in T$，有$ab \in T$，且
2. $\forall a \in T$有$a^{-1} \in T$。

定理二：设G为群，T是G的非空子集。T是G的**子群**当且仅当$\forall a,b \in T$有$ab^{-1} \in T$。

子群判定定理

定理三：设G为群，T是G的非空子集。如果T是有穷集，则T是G的子群当且仅当$\forall a,b \in T$有$ab \in T$。

子群判定

设T，K分别是群G的子群，则$T \cap K$也是G的子群。

1 $T \cap K$非空。

2 $\forall a,b \in T \cap K$，$ab^{-1} \in T \cap K$。

子群判定

例　设G为群，任取$a\in G$，令

$$T=\{a^k|k\in Z\}$$

即a的所有整数次幂的集合。则**T是G的子群**，称为由元素a**生成的子群**，记作$<a>$。

证明：

$a\in<a> \Rightarrow <a>\neq\varnothing$

$\forall a^m,a^l\in<a>$，有

$$a^m(a^l)^{-1}= a^m a^{-l}= a^{m-l} \in <a>$$

所以，$<a>\leq G$

子群判定

如，

1. <Z,+>， 求<i>， i=0,1,2?
2. <P(B),⊕,∅>， 求<X>?
3. $<Z_6,\oplus,0>$， 求<4> = {0,2,4}

群G的中心

例　设G为群，令C是与G中所有的元素都可交换的元素构成的集合，即

$$C=\{a|a\in G\wedge\forall x\in G(ax=xa)\}$$

则C是G的子群，称C为群G的中心。

作业（习题十）

- 5， 9， 15， 16
- 21， 22， 24