第三部分 代数结构


3代数结构
ch9 代数系统
9.1二元运算及其性质
9.2代数系统
9.3代数系统的同态与同构
ch10 群与环
10.1群G的定义与性质
10.2子群H与群G的陪集分解
10.3循环群与置换群
10.4环与域
ch11 格与布尔代数
11.1格的定义及性质
11.2分配格、有补格与布尔代数

第十章　群与环

- 主要内容
  - **10.1群的定义与性质**
  - **10.2子群与群的陪集分解**
  - **10.3循环群与置换群**
  - **10.4环与域**

10.1 群的定义与性质

- 半群、独异点与群的定义
- 群中的术语
- 群的基本性质

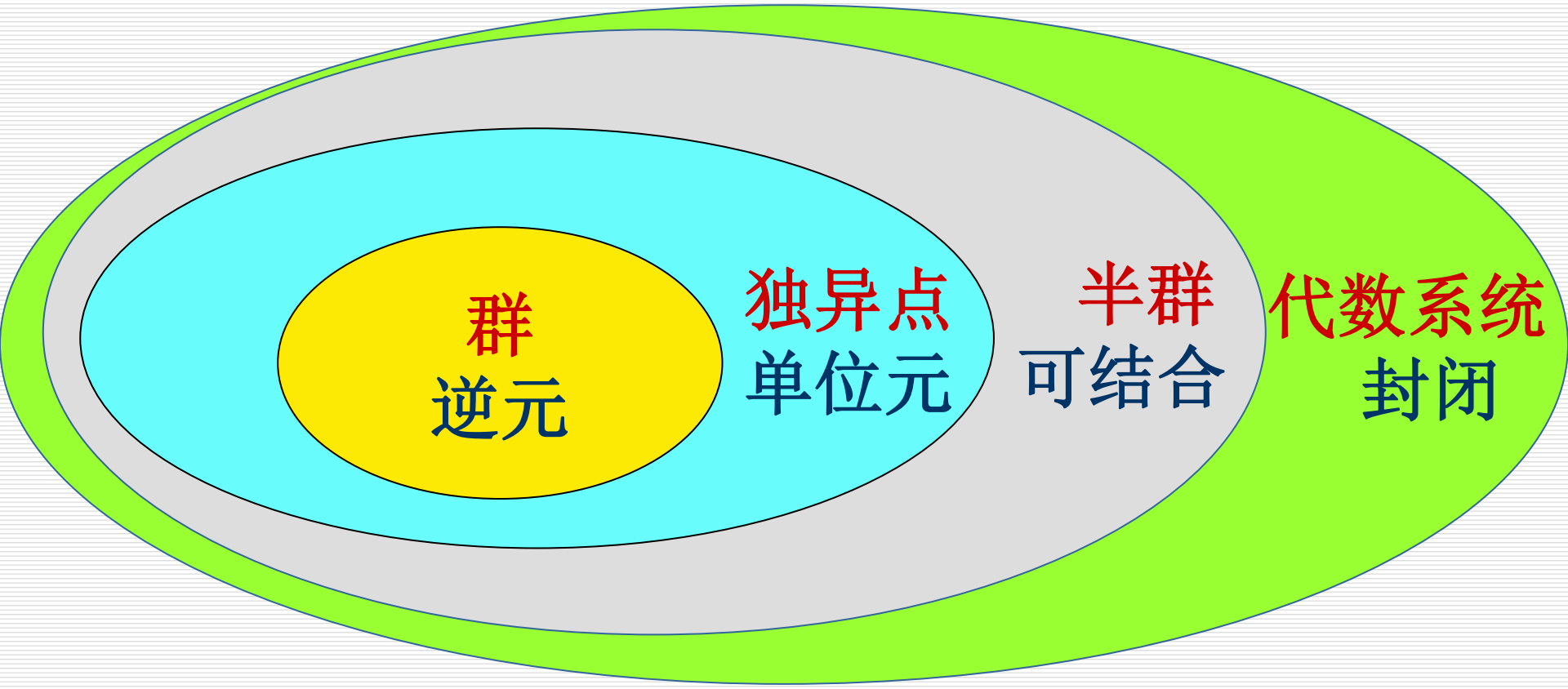
半群、独异点与群的定义

定义10.1

(1) 设$V=<S, \circ>$是代数系统，$\circ$为二元运算，如果$\circ$运算是可结合的，则称V为半群.

(2) 设$V=<S,\circ>$是半群，若$e \in S$是关于$\circ$运算的单位元，则称V是含幺半群，也叫做独异点. 有时也将独异点V 记作$V=<S,\circ,e>$.

(3) 设$V=<S,\circ>$是独异点，$e \in S$关于$\circ$运算的单位元，若$\forall a \in S$，$a^{-1} \in S$，则称V是群. 通常将群记作G.


群
逆元
独异点
单位元
半群
可结合
代数系统
封闭

实例

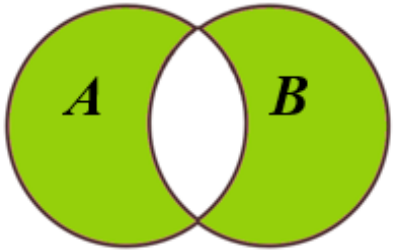
判断下列代数系统是否为半群、独异点、群？

- $\langle Z^+,+\rangle$, $\langle N,+\rangle$, $\langle Z,+\rangle$,$\langle Q,+\rangle$,$\langle R,+\rangle$ ，+是普通加法.
  - 都是半群。
  - 除$\langle Z^+,+\rangle$外都是独异点。
  - $\langle Z,+\rangle$,$\langle Q,+\rangle$,$\langle R,+\rangle$是群。

实例（续）

$\oplus$	$\varnothing$	$\{a\}$	$\{b\}$	$\{a,b\}$
$\varnothing$	$\varnothing$	$\{a\}$	$\{b\}$	$\{a,b\}$
$\{a\}$	$\{a\}$	$\varnothing$	$\{a.b\}$	$\{b\}$
$\{b\}$	$\{b\}$	$\{a,b\}$	$\varnothing$	$\{a\}$
$\{a,b\}$	$\{a,b\}$	$\{b\}$	$\{a\}$	$\varnothing$

- $<P(B),\oplus>$，其中$\oplus$为集合对称差运算
  - 是半群。
  - 是独异点，单位元为$\varnothing$。
  - 是群。



$A \oplus B$

实例（续）

$\oplus_4$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

- $<Z_n, \oplus>$，其中$Z_n=\{0,1,\ldots,n-1\}$，$\oplus$为模n加法。
  - 是半群。
  - 是独异点，单位元为0。
  - 是群。

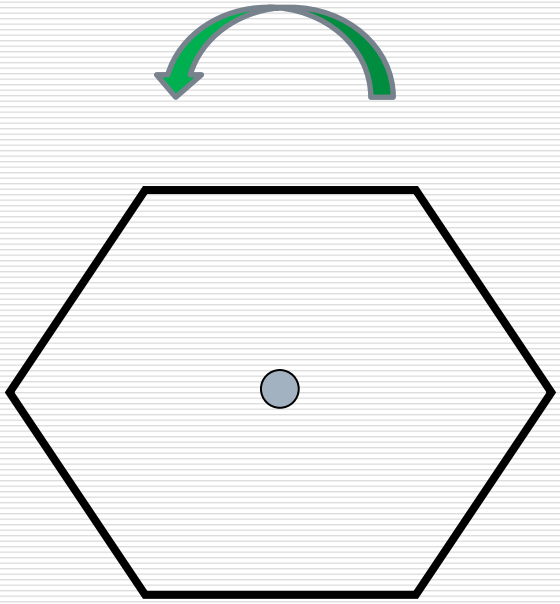
实例（续）

$\circ$	f_1	f_2	f_3	f_4
f_1	f_1	f_2	f_3	f_4
f_2	f_2	f_2	f_3	f_3
f_3	f_3	f_2	f_3	f_2
f_4	f_4	f_2	f_3	f_1

- $<A^A,\circ>$，其中$\circ$为函数的复合运算。
  - 是半群。
  - 是独异点，单位元为f_1

实例

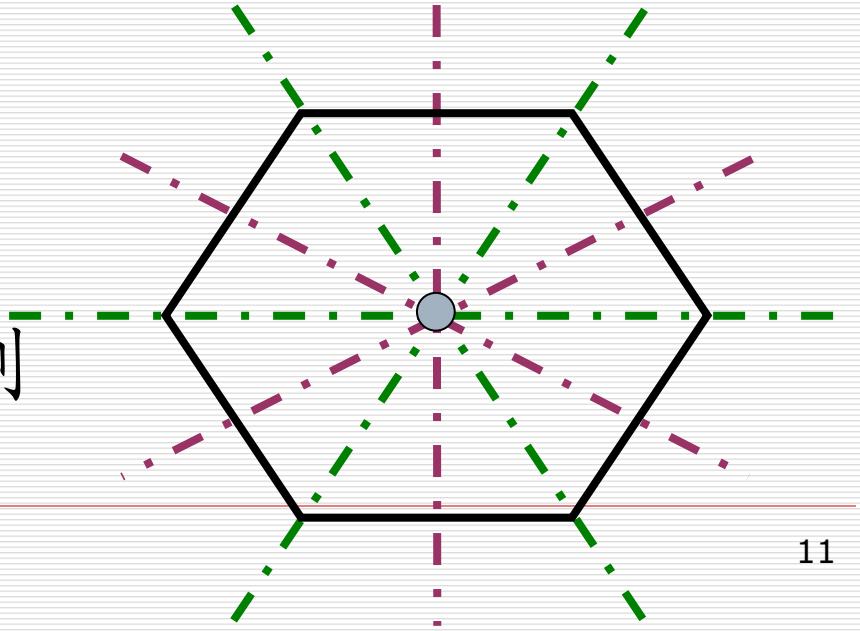
- 设 $R=\{0^\circ, 60^\circ, 120^\circ, 180^\circ, 240^\circ, 300^\circ\}$，*是 R 上的二元运算，$a * b$表示平面图形连续旋转 a 和 b 得到的总旋转角度。并规定旋转 360° 等于原来的状态。
- 试验证$<R, * >$是一个群。



解：由题意，运算*的运算表如下：

*	0	60	120	180	240	300
0	0	60	120	180	240	300
60	60	120	180	240	300	0
120	120	180	240	300	0	60
180	180	240	300	0	60	120
240	240	300	0	60	120	180
300	300	0	60	120	180	240

* 是封闭的，满足结合律，幺元是0，60,120,180的逆元分别是300,240,180



Klein四元群

- 设$G=\{e, a, b, c\}$，G上的运算由下表给出，称为**Klein四元群**。

1. 满足交换律。
2. 每个元素都是自己的逆元。
3. a, b, c中任何两个元素运算结果都等于剩下的第三个元素。

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

有关群的术语

定义10.2

(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，有限群G的阶记作$|G|$.

(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 (Abel) 群.

实例

- <Z,+>和<R,+>是无限群，$\langle Z_n, \oplus \rangle$是有限群，也是 n 阶群.
- Klein四元群是4阶群.
- <{0},+>是平凡群.
- 上述群都是交换群，n阶($n \geq 2$)实可逆矩阵集合关于矩阵乘法构成的群是非交换群.

挪威青年数学家——阿贝尔

挪威 阿贝尔
N.H.Abel
1802－1829

- 主要成就：五次方程无解证明、阿贝尔积分、阿贝尔函数、阿贝尔积分方程、阿贝尔群、阿贝尔级数、阿贝尔部分和公式、阿贝尔基本定理、阿贝尔极限定理、阿贝尔可和性等。
- 为了纪念挪威天才数学家阿贝尔诞辰200周年，挪威政府于2003年设立了一项数学奖——阿贝尔奖。

群中元素的幂

定义10.3 设G是群，$a\in G$，$n\in Z$，则a 的 n次幂.

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

只有群中元素可以定义负整数次幂.

实例

⊕	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

在$<Z_3,\oplus>$中

$2^{-3}=(2^{-1})^3$

$=1^3=1\oplus1\oplus1$

$=0$

在$<Z,+>$中

$(2)^{-3}=(2^{-1})^3$

$=(-2)^3=(-2)+(-2)+(-2)$

$=-6$

元素的阶

- 定义10.4 设G是群，$a \in G$，使得等式 $a^k=e$ 成立的最小正整数k 称为a 的阶，记作$|a|=k$，称 a 为 k 阶元. 若不存在这样的正整数 k，则称 a 为无限阶元.
- 例如：在<Z,+>中，0是1阶元，其它整数都是无限阶元。

实例

⊕	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

- 在<Z_6,⊕>中，
  - 0是1阶元，
  - 1和5是6阶元，
  - 2和4是3阶元，
  - 3是2阶元。

群的性质：幂运算规则

- **定理10.1** 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) $\forall a \in G$，$a^n a^m = a^{n+m}$，$n, m \in \mathbf{Z}$

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

  (5) 若G为交换群，则 $(ab)^n = a^n b^n$.

证明

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

  证明：$(a^{-1})^{-1}$是a^{-1}的逆元，a也是a^{-1}的逆元.

  根据逆元唯一性，等式得证.

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

  证明：$(b^{-1}a^{-1})(ab)$

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

  $= e$

  $(ab)(b^{-1}a^{-1})$

  $= a(bb^{-1})a^{-1} = aa^{-1}$

  $= e$

  故$b^{-1}a^{-1}$是ab的逆元.

  根据逆元的唯一性，等式得证.

群的性质：元素的阶

- **定理10.2** G为群，$a \in G$且 $|a| = r$. 设k是整数，则

  (1) $a^k = e$当且仅当$r \mid k$　　// $r \mid k$ 表示r整除k

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

- 证明：(1) 充分性. //已知$|a| = r$ ($a^r = e$), $r \mid k$

  由于 $r \mid k$，必存在整数m使得$k = mr$，所以有

  a^k

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

  $= e$

证明

定理10.2 G为群，$a \in G$且$|a| = r$. 设k是整数，则

(1) $a^k = e$当且仅当$r \mid k$　　// $r \mid k$ 表示r整除k

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

- (1) 必要性.　//已知$a^k = e$，　$|a| = r$

  根据除法，存在整数 m 和 i 使得

  $$k = mr+i,\ 0 \le i \le r-1$$

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

  因为$|a| = r$，必有$i = 0$.

  这就证明了$r \mid k$.

证明

定理10.2 G为群，$a \in G$且 $|a| = r$. 设k是整数，则

(1) $a^k = e$当且仅当$r \mid k$　　// $r \mid k$ 表示r整除k

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

- (2) 由 $(a^{-1})^r = (a^r)^{-1} = e^{-1} = e$　　// $a^r = e$

  可知 a^{-1} 的阶存在.

  令$|a^{-1}| = t$，根据上面的证明有$t \mid r$.

  a又是a^{-1}的逆元，所以 $r \mid t$.

  从而证明了$r = t$，即$|a^{-1}| = |a|$

实例

- 设G是群，$a,b\in G$是有限阶元.

  证明：$|b^{-1}ab| = |a|$

- 证：设 $|a| = r$，$|b^{-1}ab| = t$，则有

$$(b^{-1}ab)^r = \underbrace{(b^{-1}ab)(b^{-1}ab)\ldots(b^{-1}ab)}_{r\text{个}}$$

$$= b^{-1}a^r b = b^{-1}eb = e$$

从而有$t \mid r$.

实例（续）

- 另一方面，$|a| = r$，由于 $a = b(b^{-1}ab)b^{-1}$

$$(b(b^{-1}ab)b^{-1})^t = (\underbrace{b(b^{-1}ab)b^{-1})(b(b^{-1}ab)b^{-1})\ldots(b(b^{-1}ab)b^{-1}}_{t个})$$

$$= b(b^{-1}ab)^t b^{-1} = beb^{-1} = e$$

可知$r \mid t$.

- 综上所述，可知 $|b^{-1}ab| = |a|$.

群的性质：消去律

- **定理10.3** G为群，则G中适合消去律，即对任意$a,b,c \in G$有

  (1) 若 $ab = ac$，则 $b = c$.

  (2) 若 $ba = ca$，则 $b = c$.

- 证明略

实例

- 设$G = \{a_1, a_2, \ldots, a_n\}$是$n$阶群，令

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

  证明：$a_iG = G$.

- 证：由群中运算的封闭性有 $a_iG \subseteq G$.

  假设$a_iG \subset G$，即 $|a_iG| < n$.

  必有$a_j, a_k \in G$使得

  $$a_ia_j = a_ia_k \quad (j \neq k)$$

  由消去律得 $a_j = a_k$, 与 $|G| = n$矛盾.

群G的运算表中的每一行（列）

都是G中元素的一个排列（置换）

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

实例

$\oplus$	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

- 设群G为有限群，

  则G中阶大于2的元素有偶数个。

- 证：对于任意元素$a \in G$，根据消去律有

$$a^2=e \Leftrightarrow a^{-1}a^2=a^{-1}e$$

$$\Leftrightarrow a=a^{-1}$$

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

因此G中阶大于2的元素必有$a \neq a^{-1}$.

又由于$|a|=|a^{-1}|$，所以G中阶大于2的元素一定成对出现。

所以，如果G中有阶大于2的元素，一定是偶数个，

如果G中没有阶大于2的元素，0也是偶数。故结论成立。

判断: 有限群G的阶数是偶数，则在 G 中阶等于 2 的元素的个数一定是奇数

实例

- 设G是群，$a,b\in G$是有限阶元.
  证明：$|ab|=|ba|$
- 证： 设 $|ab|=r$，$|ba|=t$，则有

$$(ab)^{t+1}=\underbrace{(ab)(ab)\ldots(ab)}_{t+1个}$$

$$=a\underbrace{(ba)(ba)\ldots(ba)}_{t个}b$$

$$=a(ba)^tb=aeb=ab$$

由消去律得 $(ab)^t=e$，从而可知，$r\mid t$.
同理可证 $t\mid r$. 因此 $|ab|=|ba|$.

群的性质：方程存在惟一解（补充）

□ **定理10.4** 设G为群，$\forall a,b\in G$，方程$ax=b$和$ya=b$在G中有解且仅有惟一解.

证明 $a^{-1}b$ 代入方程左边的x 得

$$a(a^{-1}b) = (aa^{-1})b = eb = b$$

所以$a^{-1}b$ 是该方程的解.

下面证明惟一性：

假设c是方程$ax=b$的解，必有$ac=b$，

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

同理可证ba^{-1}是方程 $ya=b$的惟一解.

实例

- 设群$G=<P(\{a,b\}),\oplus>$，其中$\oplus$为对称差.

  解下列群方程：

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

$\oplus$	$\varnothing$	$\{a\}$	$\{b\}$	$\{a,b\}$
$\varnothing$	$\varnothing$	$\{a\}$	$\{b\}$	$\{a,b\}$
$\{a\}$	$\{a\}$	$\varnothing$	$\{a.b\}$	$\{b\}$
$\{b\}$	$\{b\}$	$\{a,b\}$	$\varnothing$	$\{a\}$
$\{a,b\}$	$\{a,b\}$	$\{b\}$	$\{a\}$	$\varnothing$

- 解：

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

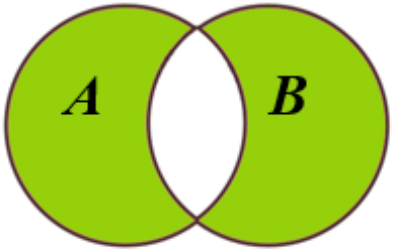
$=\{a\}\oplus\varnothing$

$=\{a\}$

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

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

$=\{a\}$



$A\oplus B$

群的性质——无零元（补充）

- 试证明：群$<G,*>$中不可能有零元。

证明

当群的阶为1时，它的唯一元素视为单位元。

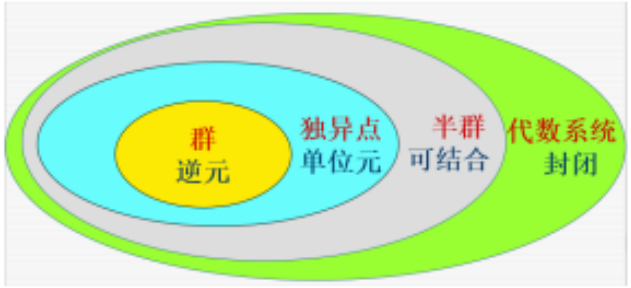
假设：当$|G|>1$且群$<G,*>$中有零元θ，

则对任何$x \in G$，都有$x*\theta=\theta*x=\theta \neq e$。
所以θ不存在逆元。

这与$<G,*>$是群矛盾。

定理9.3 设$\circ$为S上的二元运算，e和θ分别为$\circ$运算的单位元和零元。如果$|S|>1$，则$e \neq \theta$。

10.1 群的定义与性质（回顾）



- 10.1群G的定义与性质
  - 元素的阶
    - $|a|=k$ 即为 $a^k=e$
    - $|a|=r$. 设k是整数
      - (1) $a^k=e$当且仅当$r \mid k$
      - (2) $|a^{-1}|=|a|$
  - 消去律、惟一解、群中无零元等

第十章　群与环

- 主要内容
  - 10.1群的定义与性质
  - 10.2子群与群的陪集分解
  - 10.3循环群与置换群
  - 10.4环与域

10.2 子群与群的陪集分解

- 定义10.5 设G是群，H是G的非空子集，

  (1) 如果H关于G中的运算构成群，则称H是G的子群, 记作 $H \leq G$.

  (2) 若H是G的子群，且$H \subset G$，则称H是G的真子群，记作$H<G$.

- 例如 nZ (n是自然数) 是整数加群$<Z,+>$ 的子群. 当$n \neq 1$时,nZ是Z的真子群.

- 对任何群G都存在子群. G和$\{e\}$都是G的子群，称为G的平凡子群.

子群判定定理1

- **定理10.5**（判定定理一）

  设G为群，H是G的非空子集，则H是G的子群 当且仅当

  (1) $\forall a,b\in H$有$ab\in H$ （封闭）

  (2) $\forall a\in H$有$a^{-1}\in H$ （逆元）

- 证 必要性是显然的.

  为证明充分性，只需证明$e\in H$.

  因为H非空，存在$a\in H$.

  由条件(2) 知$a^{-1}\in H$,

  根据条件(1)$aa^{-1}\in H$,

  即$e\in H$.

群的幺元是子群的幺元

子群判定定理2

- **定理10.6** （判定定理二）
  设G为群，H是G的非空子集.
  H是G的子群 当且仅当 $\forall a,b\in H$有$ab^{-1}\in H$.
- 证　必要性显然.
  只证充分性（已知条件是：$\forall a,b\in H$有$ab^{-1}\in H$）
  因为H非空，必存在$a\in H$.
  根据给定条件得$aa^{-1}\in H$，即$e\in H$. /*找到单位元*/
  任取$a\in H$, 由$e,a\in H$ 得 $ea^{-1}\in H$，即$a^{-1}\in H$. /*逆元*/
  任取$a,b\in H$，知$b^{-1}\in H$. 再利用给定条件得$a(b^{-1})^{-1}\in H$，
  即$ab\in H$. /*封闭*/
  综合上述，可知H是G的子群.

子群判定定理3

- **定理10.7**（判定定理三）
  设G为群，H是G的非空有穷子集，则
  H是G的子群 当且仅当 $\forall a,b\in H$有$ab\in H$.（封闭）

- 证：必要性显然.
  只证充分性（已知条件是：$\forall a,b\in H$有$ab\in H$）
  /*根据子群判定定理1，
  只需证明【H的任何元素都有逆元】*/
  (1)任取$a\in H$, 因为有$\forall a,b\in H$有$ab\in H$
  故：$a^2 = aa$, $a^3 = a^2a$,…,都在 H 中。
  由于 H 是有穷集，所以必存在正整数 i 和 j，设$j>i$,
  使得 $a^i = a^j$, 即$a^i = a^i * a^{j-i}$,
  即a^{j-i}是G 的单位元且在 H 中。
  /*找到单位元，进而由单位元找任意元素a的逆元*/

子群判定定理3(续)

- (2) /* 因为$a^{j-i}=e$ 已经得到证明 */

对于任意$a \in H$
如果$j-i=1$,则 a 是单位元,
而单位元是以其自身为逆元的，故a有逆元。

如果$j-i>1$,则由

$$a^{j-i-1}a = a^{j-i} = e \text{ 和 } aa^{j-i-1} = a^{j-i} = e$$

可知a^{j-i-1}是 a 的逆元且在 H 中。

故，H的任何元素都有逆元

子群判定定理3的应用实例

- 设$<G,*>$是一个有限群，$a\in G$,令$H=\{a^i|i\in Z\}$, 证明$<H,*>$是$<G,*>$的子群。

证明 由于$<G,*>$是一个有限群， 显然$H=\{a^i|i\in Z\}$是有限集。

任取$a^i, a^j \in H$, 有$a^i * a^j = a^{i+j} \in H$,

所以运算*在H上是封闭的。

从而$<H,*>$是$<G,*>$的子群。

上例的进一步解释

- 设$< G , * >$是一个有限群，$a \in G$,令 $H=\{a^i | i \in Z\}$, 证明：$< H , * >$是$< G , * >$的子群。

- 实例：一个有限群$< G , * >$，G={0°, 60°, 120°, 180°, 240°, 300°}， *是 G上的二元运算，$a * b$表示平面图形连续旋转 a 和 b 得到的总旋转角度。并规定旋转 360° 等于原来的状态。运算表如下：

*	0	60	120	180	240	300
0	0	60	120	180	240	300
60	60	120	180	240	300	0
120	120	180	240	300	0	60
180	180	240	300	0	60	120
240	240	300	0	60	120	180
300	300	0	60	120	180	240

上例的进一步解释

- 设$< G , * >$是一个有限群，$a \in G$,令 $H=\{a^i | i \in Z\}$, 证明：$< H , * >$是$< G , * >$的子群。
- 一个有限群$< G , * >$的运算表如下：

*	0	60	120	180	240	300
0	0	60	120	180	240	300
60	60	120	180	240	300	0
120	120	180	240	300	0	60
180	180	240	300	0	60	120
240	240	300	0	60	120	180
300	300	0	60	120	180	240

- $a \in G$,（设a=120）
- $H=\{a^i | i \in Z\} =\{0，120，240\} \subseteq G$

典型子群的实例:生成子群

- 定义10.6 设G为群，$a \in G$，令$H=\{a^k \mid k \in \mathbf{Z}\}$，则$H$是$G$的子群，称为由 a 生成的子群，记作$\langle a \rangle$.
- 证：/*利用子群判定定理二*/
  - 首先由$a \in \langle a \rangle$知道$\langle a \rangle \neq \varnothing$.
  - 任取$a^m, a^l \in \langle a \rangle$，则

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

  根据判定定理二可知$\langle a \rangle \leq G$.

实例

- 整数加群，由2生成的子群是
  $<2>=\{2^k \mid k \in Z\}=2Z$
- $<Z_6,\oplus>$中，由2生成的子群$<2>=\{0,2,4\}$
- Klein四元群 $G=\{e,a,b,c\}$的所有生成子群是：

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

<e>={e}
<a>={e,a}
<b>={e,b}
<c>={e,c}

典型子群的实例:中心C

- 定义10.7 设G为群,令
$$C=\{a \mid a\in G \wedge \forall x\in G(ax=xa)\},$$
则C是G的子群，称为G的中心.
- 证： /*利用子群判定定理二*/
  - 对于$\forall x\in G$，有$ex=xe$, 所以$e\in C$，
    故：C是G的非空子集.
  - 任取$a,b\in C$,
    只需证明ab^{-1}与 G中所有的元素 都可交换.
    $\forall x\in G$，有
$$(ab^{-1})x = ab^{-1}x = ab^{-1}(x^{-1})^{-1}$$
$$= a(x^{-1}b)^{-1} = a(bx^{-1})^{-1} = a(xb^{-1})$$
$$= (ax)b^{-1} = (xa)b^{-1} = x(ab^{-1})$$
    由判定定理二可知$C\leq G$.

说明

- 对于阿贝尔群G，因为G中所有的元素互相都可交换，G的中心就等于G.
- 但是，对某些非交换群G，它的中心是$\{e\}$.

典型子群的实例:子群的交和并

- 设G是群，H,K是G的子群. 证明
  (1) $H\cap K$也是G的子群
  (2) $H\cup K$是G的子群当且仅当 $H\subseteq K$ 或 $K\subseteq H$
- 证明：(1) /*利用子群判定定理二*/
  由 $e\in H\cap K$ 知 $H\cap K$ 非空.
  任取$a, b\in H\cap K$,
  则$a\in H, b\in H, a\in K, b\in K$.
  由于H和K是G的子群，所以
  必有$ab^{-1}\in H$ 和 $ab^{-1}\in K$，从而$ab^{-1}\in H\cap K$.
  因此$H\cap K\leq G$.

典型子群的实例:子群的交和并

- (2) 充分性显然，只证必要性. 即证明：
  如果$H\cup K$是G的子群，则 $H\subseteq K$ 或 $K\subseteq H$。
- 用反证法. /*考查是否具有封闭性*/

  假设 $H\not\subseteq K$ 且$K\not\subseteq H$，那么$\exists h,k\in H\cup K$ 使

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

  $k=ek=(h^{-1}h)k=h^{-1}(hk)$

  因为$h^{-1}\in H$, 若$hk\in H$,

  则 $k=h^{-1}(hk)\in H$与假设矛盾.

  故推出 $hk\notin H$.

  同理可证 $hk\notin K$. 从而得到 $hk\notin H\cup K$.

  与$H\cup K$是子群矛盾.

子群格

□ **定义10.8** 设G为群, 令

$$L(G) = \{H \mid H\text{是}G\text{的子群}\}$$

则偏序集$< L(G), \subseteq >$称为G的子群格。

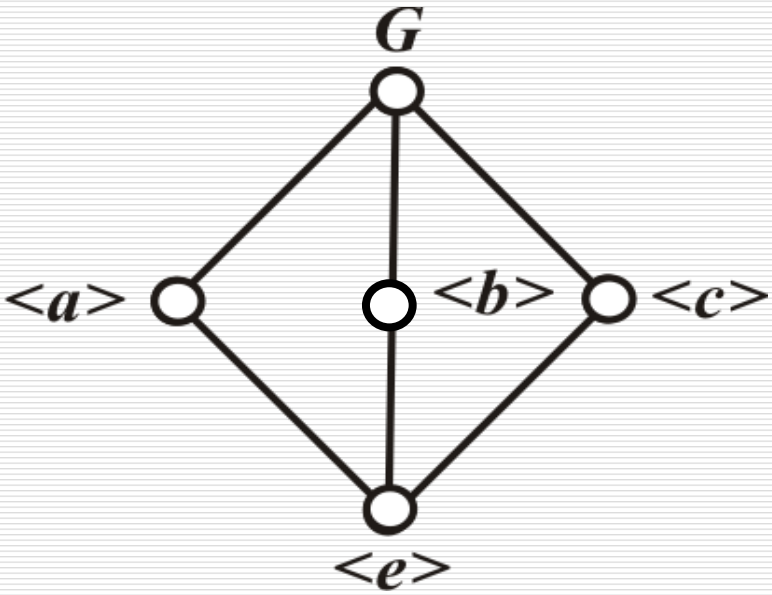
□例：Klein四元群

$G = \{e, a, b, c\}$

的所有生成子群是：

$<e>=\{e\}$, $<a>=\{e, a\}$,

$<b>=\{e, b\}$, $<c>=\{e, c\}$.



陪集定义

- 定义10.9 设H是G的子群，$a \in G$.

  令 $Ha=\{ha \mid h \in H\}$

  称Ha是子群H在G中的右陪集.

  称a为Ha的代表元素.

- 令 $aH = \{ah \mid h \in H\}$

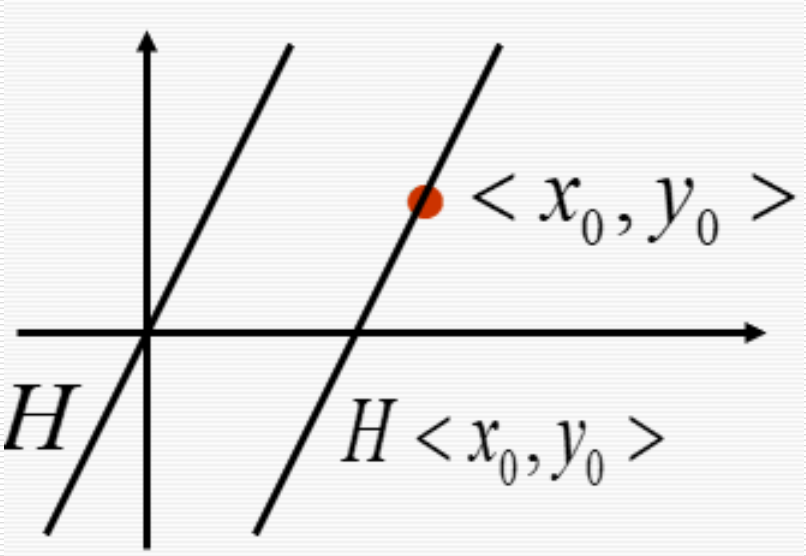
  称aH是子群H在G中的左陪集.

  称a为aH的代表元素.

陪集定义

- 设$G=\mathbf{R}\times\mathbf{R}$，$\mathbf{R}$为实数集，二元运算+定义为：
  $\langle x_1, y_1\rangle + \langle x_2, y_2\rangle = \langle x_1+x_2, y_1+y_2\rangle$
- 显然，$\langle G, +\rangle$是一个具有单位元$\langle 0, 0\rangle$的阿贝尔群。

设 $H=\{\langle x, y\rangle | y=2x\}$
对$\langle x_0, y_0\rangle \in G$, 右陪集
$H\langle x_0, y_0\rangle$的几何意义:



实例

- (1)设$G=\{e,a,b,c\}$是Klein四元群，
  $H=<a>=\{e,a\}$是G的子群.
  H所有的右陪集是：
  $He=\{e,a\}$, $Ha=\{a,e\}$,
  $Hb=\{b,c\}$, $Hc=\{c,b\}$
- 不同的右陪集只有两个：
  - $He=Ha=\{a,e\}=H$
  - $Hb=Hc=\{c,b\}$

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

实例

⊕	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

- (2)已知$G=<Z_4, \oplus>$,
  子群$H=\{0,2\}$
  则H的所有右陪集是:
  - $H0=\{0,2\}$
  - $H1=\{1,3\}$
  - $H2=\{2,0\}$
  - $H3=\{3,1\}$
- 不同的右陪集只有两个:
  - $H0= H2=\{0,2\}=H$
  - $H1= H3=\{1,3\}$

实例

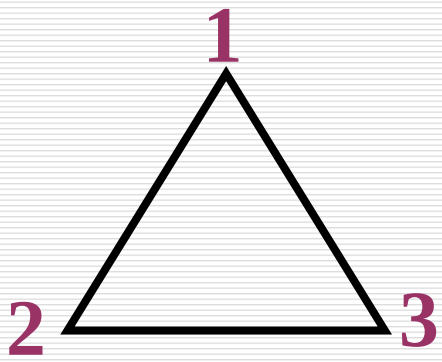
(3)设$A=\{1,2,3\}$，$f_1, f_2, \ldots, f_6$是A上的双射函数.
其中：

$f_1=\{\langle 1,1\rangle,\langle 2,2\rangle,\langle 3,3\rangle\}$，$f_2=\{\langle 1,2\rangle,\langle 2,1\rangle,\langle 3,3\rangle\}$

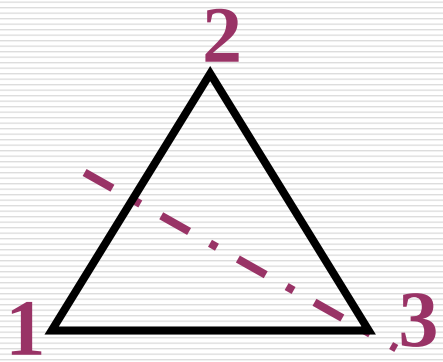
$f_3=\{\langle 1,3\rangle,\langle 2,2\rangle,\langle 3,1\rangle\}$，$f_4=\{\langle 1,1\rangle,\langle 2,3\rangle,\langle 3,2\rangle\}$

$f_5=\{\langle 1,2\rangle,\langle 2,3\rangle,\langle 3,1\rangle\}$，$f_6=\{\langle 1,3\rangle,\langle 2,1\rangle,\langle 3,2\rangle\}$

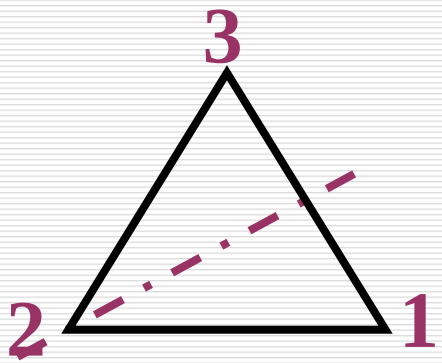
令 $G=\{f_1, f_2, \ldots, f_6\}$，则$G$ 关于函数的复合运算构成群. 考虑G 的子群$H=\{f_1, f_2\}$. 做出 H 的全体右陪集。



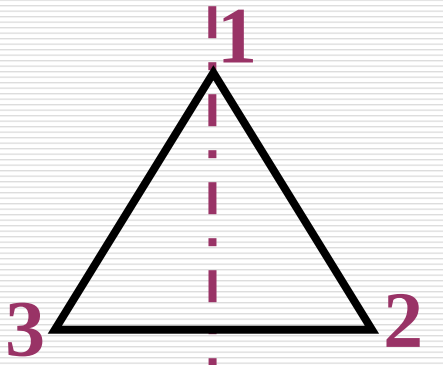
$f_1=\{<1,1>,<2,2>,<3,3>\}$



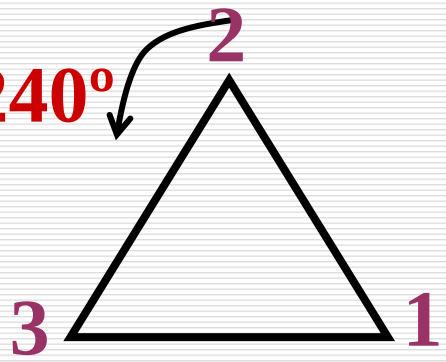
$f_2=\{<1,2>,<2,1>,<3,3>\}$



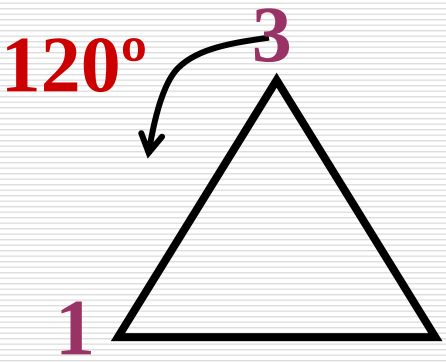
$f_3=\{<1,3>,<2,2>,<3,1>\}$



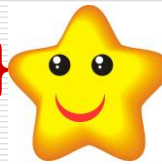
$f_4=\{<1,1>,<2,3>,<3,2>\}$



$f_5=\{<1,2>,<2,3>,<3,1>\}$



$f_6=\{<1,3>,<2,1>,<3,2>\}$



实例（续）

∘	f_1	f_2	f_3	f_4	f_5	f_6
f_1	f_1	f_2	f_3	f_4	f_5	f_6
f_2	f_2	f_1	f_5	f_6	f_3	f_4
f_3	f_3	f_6	f_1	f_5	f_4	f_2
f_4	f_4	f_5	f_6	f_1	f_2	f_3
f_5	f_5	f_4	f_2	f_3	f_6	f_1
f_6	f_6	f_3	f_4	f_2	f_1	f_5

- $H=\{f_1, f_2\}$是G 的子群：
  $Hf_1=\{f_1\circ f_1, f_2\circ f_1\}=H$,
  $Hf_2=\{f_1\circ f_2, f_2\circ f_2\}=H$
  $Hf_3=\{f_1\circ f_3, f_2\circ f_3\}=\{f_3, f_5\}$
  $Hf_4=\{f_1\circ f_4, f_2\circ f_4\}=\{f_4, f_6\}$
  $Hf_5=\{f_1\circ f_5, f_2\circ f_5\}=\{f_5, f_3\}$
  $Hf_6=\{f_1\circ f_6, f_2\circ f_6\}=\{f_6, f_4\}$
- 结论：
  - $Hf_1=Hf_2=\{f_1, f_2\}=H$
  - $Hf_3=Hf_5=\{f_3, f_5\}$
  - $Hf_4=Hf_6=\{f_4, f_6\}$

陪集的基本性质

- **定理10.8** 设H是群G的子群，则

  (1) $He = H$

  (2) $\forall a \in G$ 有$a \in Ha$

- 证 (1) $He = \{ he \mid h \in H \} = \{ h \mid h \in H \} = H$

  (2) 任取 $a \in G$,

  由$a = ea$ 和 $ea \in Ha$ 得 $a \in Ha$

陪集的基本性质

- **定理10.9** 设H是群G的子群，则$\forall a,b\in G$有
  $a\in Hb \Leftrightarrow ab^{-1}\in H \Leftrightarrow Ha=Hb$
- 证 先证$a\in Hb \Leftrightarrow ab^{-1}\in H$

  $a\in Hb \Leftrightarrow \exists h(h\in H\wedge a=hb)$

  $\Leftrightarrow \exists h(h\in H\wedge ab^{-1}=h) \Leftrightarrow ab^{-1}\in H$

定义10.9 设H是G的子群，$a\in G$.

令 $Ha=\{ha \mid h\in H\}$

称Ha是子群H在G中的右陪集.

称a为Ha的代表元素.

证明（续）

定理10.9 设H是群G的子群，则$\forall a,b\in G$有
$a\in Hb \Leftrightarrow ab^{-1}\in H \Leftrightarrow Ha=Hb$

再证 $a\in Hb \Leftrightarrow Ha=Hb$.

- 充分性. 若$Ha=Hb$，由$a\in Ha$ 可知必有 $a\in Hb$.
- 必要性. (即证：若$a\in Hb$则$Ha=Hb$)

由 $a\in Hb$ 可知$\exists h\in H$使得 $a=hb$，从而$b=h^{-1}a$

任取 $h_1a\in Ha$，

则有 $h_1a = h_1(hb) = (h_1h)b\in Hb$ ，从而得到

$Ha\subseteq Hb$

再，任取$h_1b\in Hb$，

则有 $h_1b = h_1(h^{-1}a) = (h_1h^{-1})a\in Ha$ ，从而得到

$Hb\subseteq Ha$

综合上述，$Ha=Hb$ 得证.

陪集的基本性质

定理10.6 （判定定理二）
设G为群，H是G的非空子集.
H是G的子群 当且仅当 $\forall a,b\in H$有$ab^{-1}\in H$.

□ **定理10.10** 设H是群G的子群，在G上定义二元关系R：$\forall a,b\in G$,

$$<a,b>\in R \Leftrightarrow ab^{-1}\in H$$

则 R是G上的等价关系，且 $[a]_R = Ha$.

□ 证 先证：R为G上的等价关系.

自反性：任取$a\in G$，$aa^{-1}=e\in H \Leftrightarrow <a,a>\in R$

对称性：任取$a,b\in G$，则

$<a,b>\in R$

$\Rightarrow ab^{-1}\in H \Rightarrow (ab^{-1})^{-1}\in H \Rightarrow ba^{-1}\in H$

$\Rightarrow <b,a>\in R$

证明（续）

传递性： 任取$a,b,c \in G$，则

$<a,b> \in R \wedge <b,c> \in R$

$\Rightarrow ab^{-1} \in H \wedge bc^{-1} \in H$

$\Rightarrow ac^{-1} \in H$

$\Rightarrow <a,c> \in R$

□ 再证：$\forall a \in G$，$[a]_R = Ha$.

任取$b \in G$,

$b \in [a]_R$

$\Leftrightarrow <a,b> \in R$

$\Leftrightarrow ab^{-1} \in H$

$\Leftrightarrow Ha=Hb$ (定理10.9)

$\Leftrightarrow b \in Ha$

定理10.9 设H是群G的子群，则$\forall a,b \in G$有

$a \in Hb \Leftrightarrow ab^{-1} \in H \Leftrightarrow Ha=Hb$

推论

- 推论 设H是群G的子群, 则

  (1) $\forall a,b\in G$，$Ha = Hb$ 或 $Ha\cap Hb = \varnothing$

  (2) $\cup\{Ha \mid a\in G\} = G$

- 证明：由等价类性质可得.

重要结果：给定群G的一个子群H，H的所有右陪集的集合{Hala∈G}恰好构成G的一个划分。

推论

□ **定理10.11** 设H是群G的子群，则
$\forall a \in G$，$H \approx Ha$

证明： 令$f: H \to Ha$，$f(x) = xa$。

任取$ha \in Ha$，$\exists h \in H$，使得 $f(h) = ha$，

因而f是满射的。

假设 $f(h_1) = f(h_2)$，那么有 $h_1a = h_2a$。

根据消去律得 $h_1 = h_2$，

因而f是单射的。

因此， $H \approx Ha$。

左陪集的定义及性质

- 关于左陪集有下述性质：

  (1) $eH = H$

  (2) $\forall a \in G$，$a \in aH$

  (3) $\forall a,b \in G$，$a \in bH \Leftrightarrow b^{-1}a \in H \Leftrightarrow aH=bH$

  (4) 若在G上定义二元关系R，

  $\forall a,b \in G$，$<a,b> \in R \Leftrightarrow b^{-1}a \in H$

  则R是G上的等价关系，且$[a]_R = aH$.

  (5) $\forall a \in G$，$H \approx aH$

- 正规子群：$\forall a \in G$, $Ha=aH$, 则H称为正规子群，也称为不变子群。

Lagrange定理

拉格朗日（法）
1735~1813
数学家、物理学家

□ **定理10.12** （Lagrange）设G是有限群，H是G的子群，则

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

其中，$[G:H]$ 是H在G中的不同右陪集(或左陪集) 数，称为H在G 中的**指数**.

子群的阶是群阶的因子

证明

定理10.12 （Lagrange）设G是有限群，H是G的子群，则

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

设$[G:H] = r$，

$a_1,a_2,\ldots,a_r$分别是H 的r个右陪集的代表元素，

$$G = Ha_1 \cup Ha_2 \cup \ldots \cup Ha_r$$

因为 $Ha_i \cap Ha_j = \varnothing$

$$|G| = |Ha_1| + |Ha_2| + \ldots + |Ha_r|$$

由$|Ha_i| = |H|$，$i = 1,2,\ldots,r$, 得

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

Lagrange定理的推论1

- 推论1 设G是n阶群，则$\forall a \in G$，$|a|$是n的因子，且有$a^n = e$.
- 证 任取$a \in G$，$<a>$是G的子群，$<a>$的阶是n的因子. (根据拉格朗日定理)

  $<a>$是由a生成的子群，若$|a| = r$，则

  $<a> = \{a^0=e, a^1, a^2, \ldots, a^{r-1}\}$

  即$<a>$的阶与$|a|$相等, 所以$|a|$是n的因子.

  从而$a^n = e$.

群中元素的阶是群阶的因子

Lagrange定理的推论2

- 推论2　对阶为素数的群G，必存在$a \in G$使得$G = \langle a \rangle$.

- 证　设$|G| = p$，p是素数.

  由$p \geq 2$知G中必存在非单位元.
  任取$a \in G$，$a \neq e$，则$\langle a \rangle$是G的子群.
  根据拉格朗日定理，
  $\langle a \rangle$的阶是p的因子，即$\langle a \rangle$的阶是 p或1.
  显然$\langle a \rangle$的阶不是1，
  这就推出$G = \langle a \rangle$.

Lagrange定理的应用

- **命题**：如果群 G 只含 1 阶和 2 阶元，则 G 是Abel群.

- 证

设a为G中任意元素，有$a^{-1} = a$.

任取 $x, y \in G$，则

$$xy = (xy)^{-1} = y^{-1}x^{-1} = yx$$

因此G是Abel群.

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

Lagrange定理的应用

- 证明: 6 阶群中必含有 3 阶元.
- 证　设G是6 阶群，则G中元素只能是1阶、2阶、3阶或6阶.

  若G中含有6 阶元，设为a，则 a^2是3 阶元.

  若G中不含6 阶元，下面证明G中必含有3阶元.

  如若不然，G中只含1阶和2阶元 (反证法)

  即$\forall a \in G$，有$a^2=e$，由命题知G是Abel群.

  取G中2阶元 a 和 b, $a \neq b$,

  令　$H = \{e, a, b, ab\}$,

  易知H 是G的子群,

  但 $|H| = 4$，　$|G| = 6$，与拉格朗日定理矛盾.

	e	a	b	ab
e	e	a	b	ab
a	a	e	ab	b
b	b	ab	e	a
ab	ab	b	a	e

10.2子群与群的陪集分解（回顾）

第十章　群与环

- 主要内容
  - 10.1群的定义与性质
  - 10.2子群与群的陪集分解
  - 10.3循环群与置换群
  - 10.4环与域