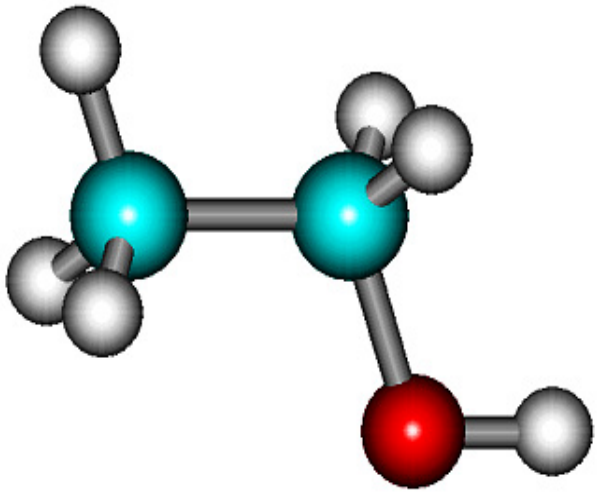
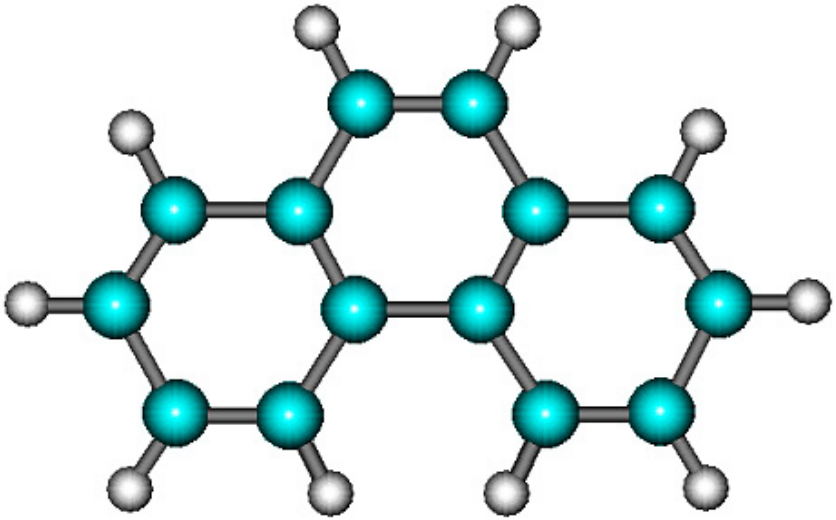
第十章 群与环

北京理工大学 计算机学院
刘琼昕

生物界的对称性

分子中的对称性





美术中的对称性

建筑中的对称性

第十章　群与环

- 主要内容
  - 群的定义与性质
  - 子群与群的陪集分解
  - 循环群与置换群
  - 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

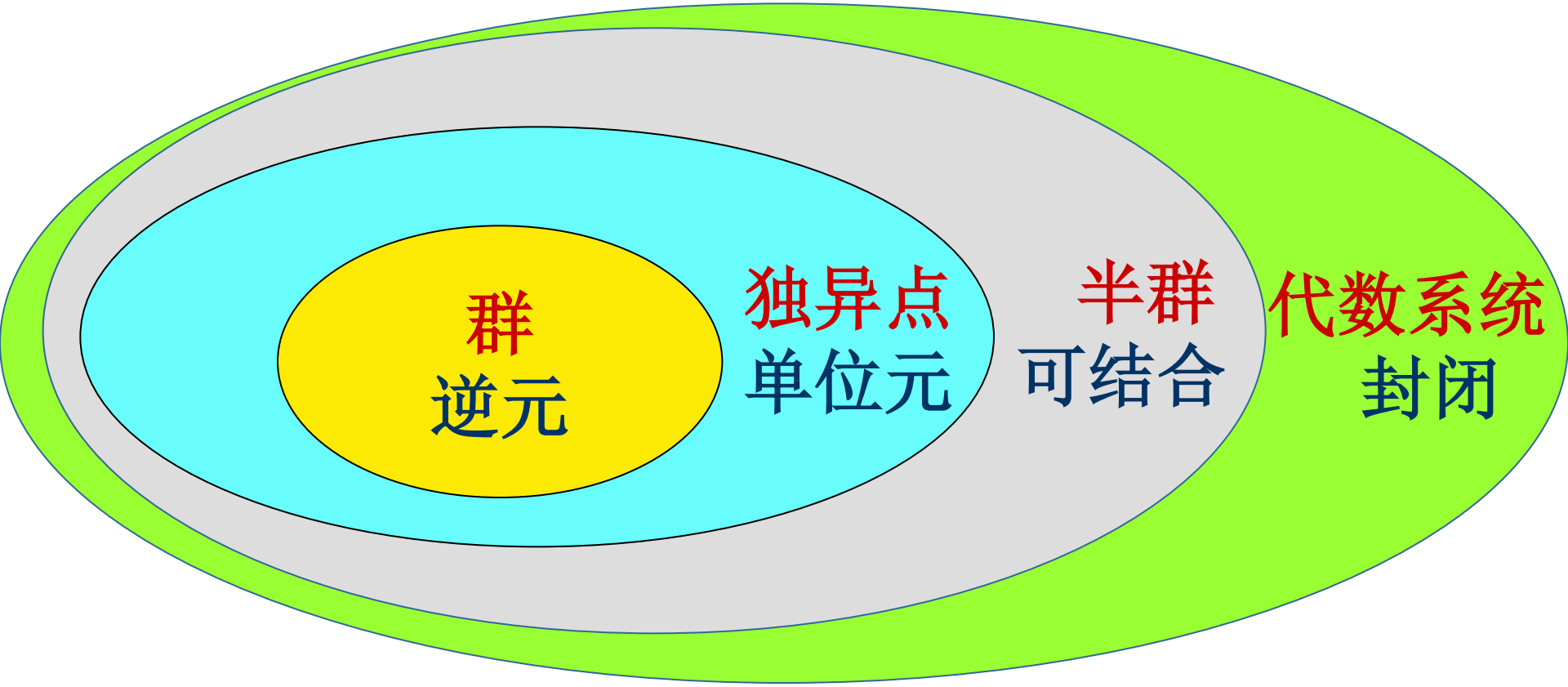
半群、独异点与群的定义

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？

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

实例（续）

- $<M_n(\mathbf{R}),+>$和$<M_n(\mathbf{R}),\cdot>$，其中$M_n(\mathbf{R})$表示所有n 阶($n\geq 2$)实矩阵的集合， +和·分别表示矩阵加法和矩阵乘法
  - 都是半群。
  - 都是独异点。
  - $<M_n(\mathbf{R}),+>$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。

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，单位元为恒等函数。

实例

- 在形式语言中，常称非空有限字符集合为字母表。字母表中字符的 n 重序元为字符串，由 m 个字符所组成的字符串称为长度为 m 的字符串。长度为 0 的字符串称为空串，记为Λ。用◦表示两个字符串的邻接运算。

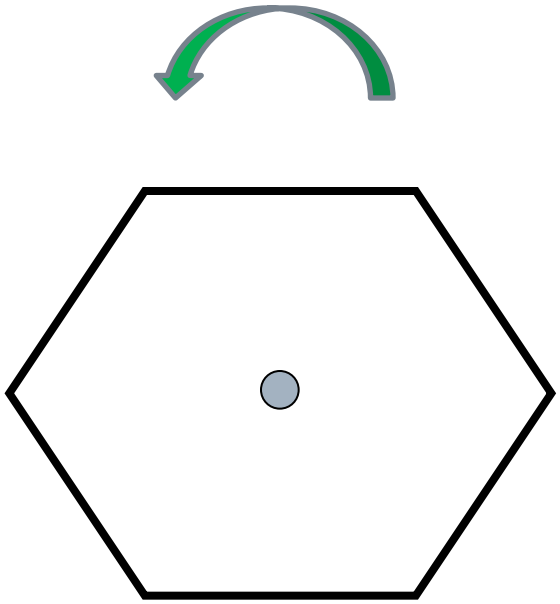
  设 V^* 表示字母表 V 中字符串的集合，

  $V^+ = V^* - \{\Lambda\}$

- 则 $<V^+, \circ>$ 是一个半群（封闭，可结合）
- $<V^*, \circ>$ 是一个独异点（封闭，可结合，单位元为 Λ）。

实例

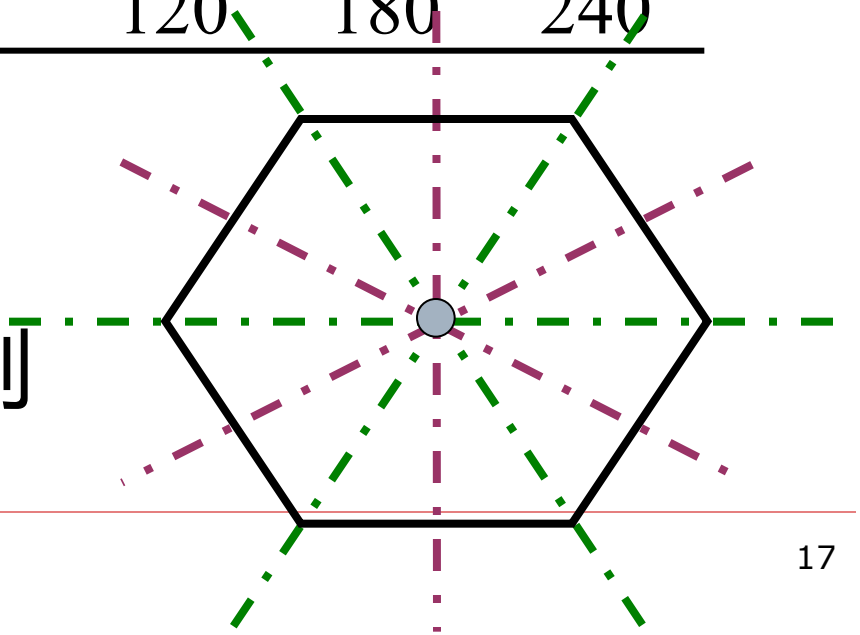
- 设 $R=\{0^\circ, 60^\circ, 120^\circ, 180^\circ, 240^\circ, 300^\circ\}$，$\Delta$ 是 R 上的二元运算，$a \Delta b$表示平面图形连续旋转 a 和 b 得到的总旋转角度。并规定旋转 360° 等于原来的状态。
- 试验证$<R, \Delta>$是一个群。



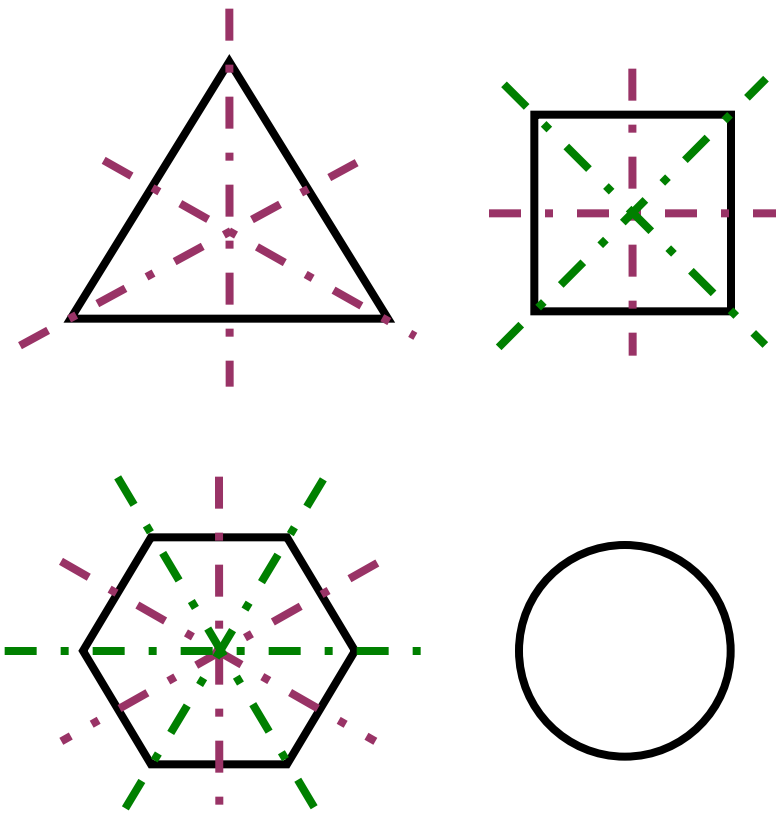
解：由题意，运算Δ的运算表如下：

Δ	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

Δ 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

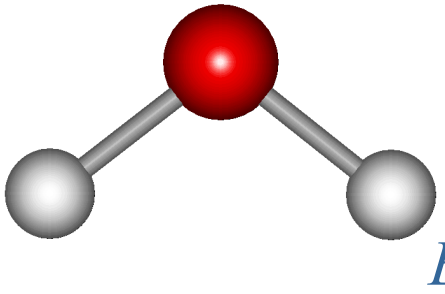


对称变换构成的群



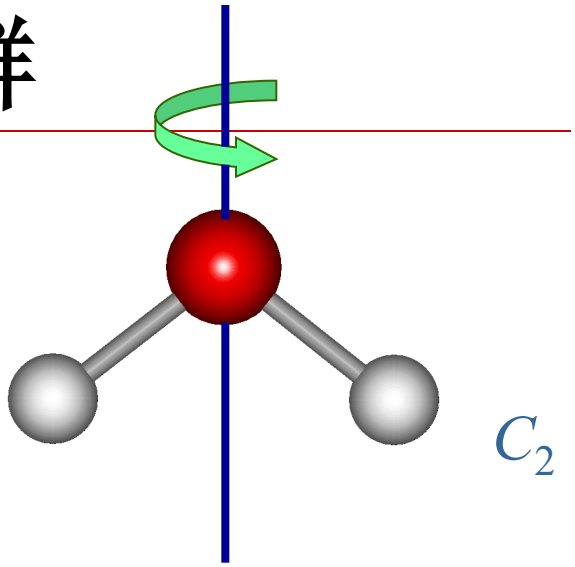
- 左侧图形的所有对称变换，在连续变换的运算下都构成群，显然圆具有最好的对称性。

水分子对称群

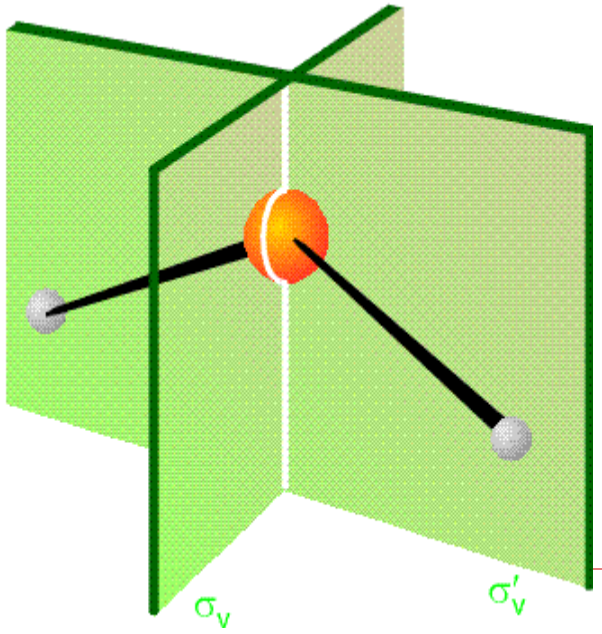


E

旋转180度



C_2



C_{2v}	$\hat{E}$	$\hat{C}_2$	$\hat{\sigma}_v$	$\hat{\sigma}_v'$
$\hat{E}$	$\hat{E}$	$\hat{C}_2$	$\hat{\sigma}_v$	$\hat{\sigma}_v'$
$\hat{C}_2$	$\hat{C}_2$	$\hat{E}$	$\hat{\sigma}_v'$	$\hat{\sigma}_v$
$\hat{\sigma}_v$	$\hat{\sigma}_v$	$\hat{\sigma}_v'$	$\hat{E}$	$\hat{C}_2$
$\hat{\sigma}_v'$	$\hat{\sigma}_v'$	$\hat{\sigma}_v$	$\hat{C}_2$	$\hat{E}$

方程根构成的群

$$G = \{1, \frac{-1+i\sqrt{3}}{2}, \frac{-1-i\sqrt{3}}{2}\}$$

$$= \{1, \varepsilon_1, \varepsilon_2\} \text{为} x^3 = 1 \text{的解}$$

则<*G*,·>为群。

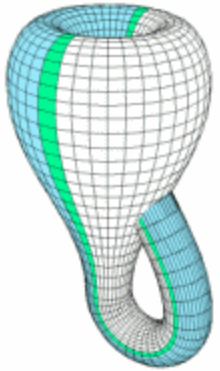
	1	ε_1	ε_2
1	1	ε_1	ε_2
ε_1	ε_1	ε_2	1
ε_2	ε_2	1	ε_1

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，$<Z_n,\oplus>$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.

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

群中元素可以定义负整数次幂.

实例

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

  同理 $(ab)(b^{-1}a^{-1})=e$,

  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$r \mid k$

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

- 证明：(1) 充分性.

  由于$r|k$，必存在整数m使得$k = mr$，所以有

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

证明

- (1) 必要性.

  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

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

  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，由于 $a = b(b^{-1}ab)b^{-1}$

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

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

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）。

实例

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

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

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

$$= a(ba)^t b = aeb = ab$$

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　$a^{-1}b$ 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：

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

- 解

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

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

$=\{a\}$　　$=\{a\}$

群的性质——无零元（补充）

- 试证明：群$<G,*>$（$|G|>1$）中不可能有零元。

证明 假设当$|G|>1$且群$<G,*>$中有零元，

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。

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$ab\in H$

  (2) $\forall a\in H$有$a^{-1}\in H$.

- 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$e\in H$.

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$ab\in H$.
- 证：必要性显然.
  为证充分性，只需证明$\forall a\in H$有$a^{-1}\in H$.
  任取$a\in H$, 若$a=e$, 则$a^{-1}=e\in H$.
  若$a\neq e$，令$S=\{a,a^2,\ldots\}$，则$S\subseteq H$.
  由于H是有穷集，必有$a^i=a^j(i<j)$,即$a^ie=a^ia^{j-i}$
  根据G中的消去律得 $a^{j-i}=e$,
  由$a\neq e$可知 $j-i>1$,
  由此得$a\,a^{j-i-1}a=e$ 和 $a\,a^{j-i-1}=e$
  从而证明了$a^{-1}=a^{j-i-1}\in H$.

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。

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.
  因为H非空，必存在$a\in H$.
  根据给定条件得$aa^{-1}\in H$，即$e\in H$.
  任取$a\in H$, 由$e,a\in H$ 得 $ea^{-1}\in H$，即$a^{-1}\in H$.
  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$ab\in H$.
  综合上述，可知H是G的子群.

典型子群的实例:生成子群

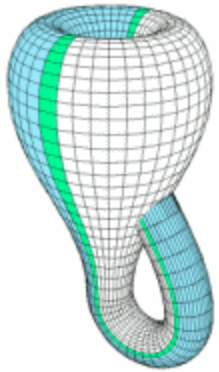
- 定义10.6 设G为群，$a\in G$，令$H=\{a^k \mid k\in \mathbf{Z}\}$，则$H$是$G$的子群，称为由 a 生成的子群，记作$<a>$.
- 证：
  - 首先由$a\in<a>$知道$<a>\neq\varnothing$.
  - 任取$a^m, a^l\in<a>$，则

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

根据判定定理二可知$<a>\leq G$.

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



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:
  - $ae=ea$, 所以$e\in C$，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

$$\begin{aligned}(ab^{-1})x &= ab^{-1}x = ab^{-1}(x^{-1})^{-1}\\ &= a(x^{-1}b)^{-1} = a(bx^{-1})^{-1} = a(xb^{-1})\\ &= (ax)b^{-1} = (xa)b^{-1} = x(ab^{-1})\end{aligned}$$

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

- 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) 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

- (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.

  假设 $H\not\subseteq K$ 且$K\not\subseteq H$，那么存在 h 和 k 使得

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

  推出 $hk\notin H$. 否则由$h^{-1}\in H$ 得 $k=h^{-1}(hk)\in H$，
  与假设矛盾.

  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。

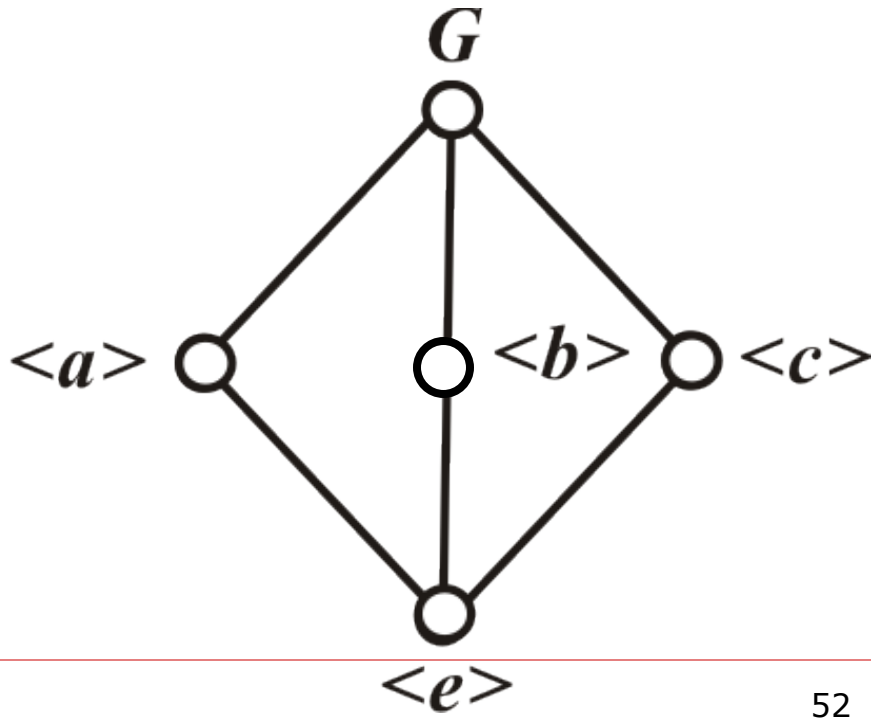
□例：Klein四元群

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

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.

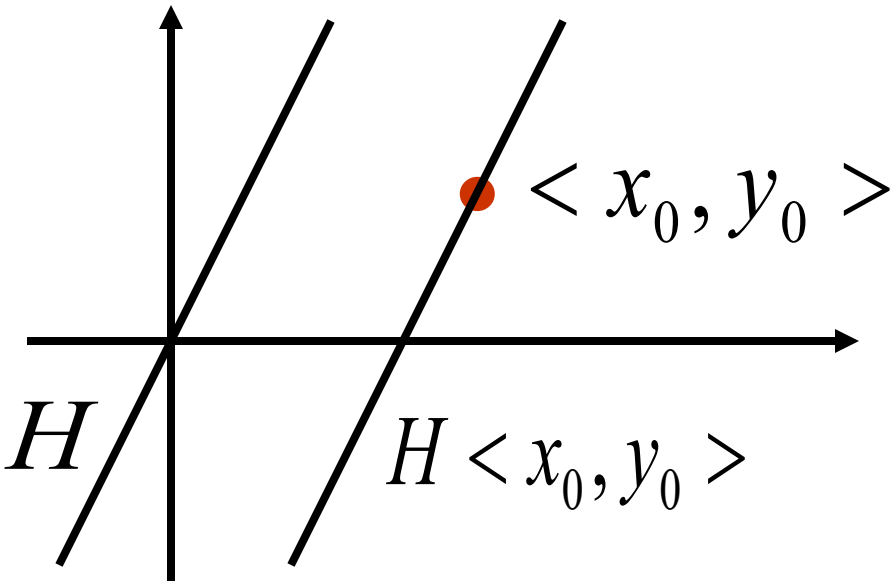
- 令 $aH=\{ah \mid h\in H\}$

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$G=\mathbf{R}\times\mathbf{R}$，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，$\langle G, +\rangle$是一个具有幺元$\langle 0, 0\rangle$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：
  - $H0=\{0,2\}$
  - $H1=\{1,3\}$
  - $H2=\{0,2\}$
  - $H3=\{1,3\}$
- 不同的右陪集只有两个：
  - $H0= H2=\{0,2\}=H$
  - $H1= H3=\{1,3\}$

实例

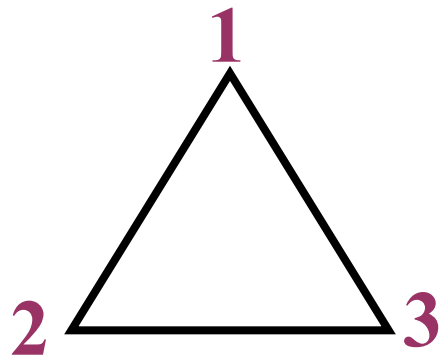
(3)设$A=\{1,2,3\}$，$f_1, f_2, \ldots, f_6$是A上的双射函数.
其中：

$f_1=\{<1,1>,<2,2>,<3,3>\}$，$f_2=\{<1,2>,<2,1>,<3,3>\}$

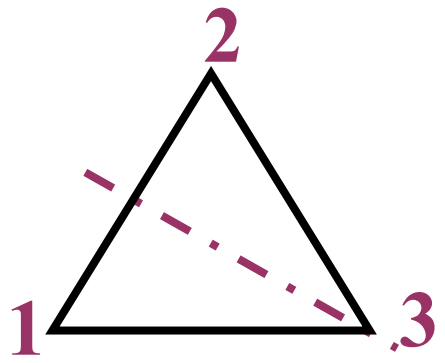
$f_3=\{<1,3>,<2,2>,<3,1>\}$，$f_4=\{<1,1>,<2,3>,<3,2>\}$

$f_5=\{<1,2>,<2,3>,<3,1>\}$，$f_6=\{<1,3>,<2,1>,<3,2>\}$

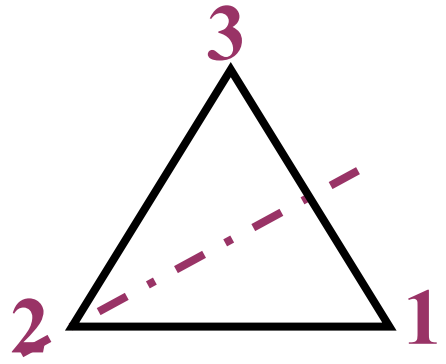
令 $G=\{f_1, f_2, \ldots, f_6\}$，则$G$关于函数的复合运算构成群. 考虑$G$的子群$H=\{f_1, f_2\}$. 做出 H的全体右陪集。



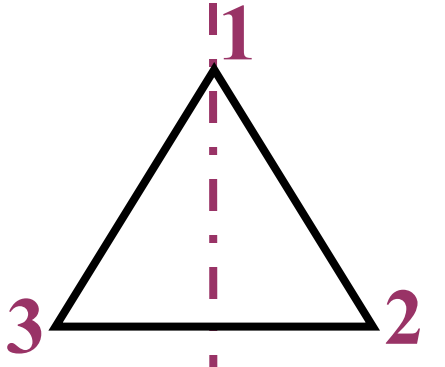
f_1={<1,1>,<2,2>,<3,3>}



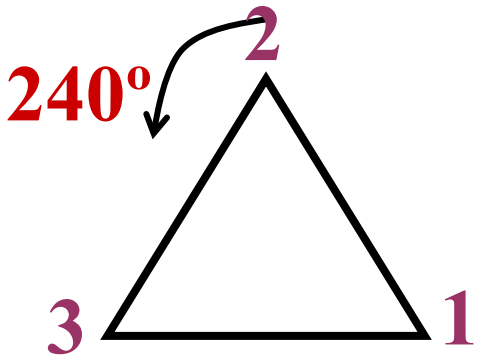
f_2={<1,2>,<2,1>,<3,3>}



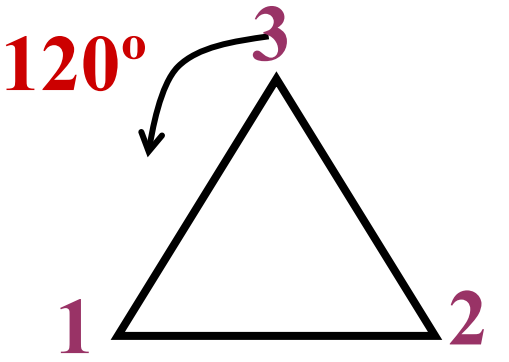
f_3={<1,3>,<2,2>,<3,1>}



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：
  $Hf_1=\{f_1\circ f_1, f_2\circ f_1\}=H$,
  $Hf_2=\{f_1\circ f_2, f_2\circ f_2\}=H$
  $Hf_3=\{f_1\circ f_3, f_2\circ f_3\}=\{f_3, f_5\}$
  $Hf_5=\{f_1\circ f_5, f_2\circ f_5\}=\{f_5, f_3\}$
  $Hf_4=\{f_1\circ f_4, f_2\circ f_4\}=\{f_4, f_6\}$,
  $Hf_6=\{f_1\circ f_6, f_2\circ f_6\}=\{f_6, f_4\}$
- 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$a\in Hb \Leftrightarrow ab^{-1}\in H$

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

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

证明

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.

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 $Ha \subseteq Hb$.

反之，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10.10** 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　先证明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

传递性. 任取$a,b,c \in G$，则

$$<a,b> \in R \wedge <b,c> \in R \Rightarrow ab^{-1} \in H \wedge bc^{-1} \in H$$

$$\Rightarrow ac^{-1} \in H \Rightarrow <a,c> \in R$$

- 下面证明：$\forall a \in G$，$[a]_R = Ha$.

  任取$b \in G$,

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

  $\Leftrightarrow Ha = Hb \Leftrightarrow b \in Ha$

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.

- **定理10.11** 设H是群G的子群，则

  $\forall a\in G$，$H \approx Ha$

  - 证明 略

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.

证明

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.

  $<a>$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$a^n = e$.

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.

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，
  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 $H=\{e, a, b, ab\}$，则H 是G的子群，
  但 $|H|=4$，$|G|=6$，与拉格朗日定理矛盾.

Lagrange定理的应用

- 证明阶小于6 的群都是Abel群.
- 证明：1 阶群是平凡的，显然是阿贝尔群.
  - 2, 3和5都是素数，由推论2它们都是单元素生成的群，都是Abel群.
  - 设G是4阶群. 若G中含有4阶元，比如说a，则$G=\langle a\rangle$，由上述分析可知G是Abel群. 若G中不含4阶元，G中只含1阶和2阶元，由命题可知G也是Abel群.

陪集的应用——线性分组码

- 七位二进制的码字$x=x_1x_2x_3\ldots x_7$，设G是所有这样的码字构成的集合，

  在G上定义二元运算，其中$\oplus$是模2加法：

  $\forall x,y\in G,\ x\circ y=z_1z_2z_3\ldots z_7$，$z_i=x_i\oplus y_i$，$i=1\sim7$
- 证明$<G,\circ>$构成群。

证明

- 任取 $x=x_1x_2x_3\ldots x_7$，$y=y_1y_2y_3\ldots y_7 \in G$，$x\circ y=z_1z_2z_3\ldots z_7$，$z_i=x_i\oplus y_i$，$i$=1~7 仍是一个七位二进制码字，所以$x\circ y\in G$。
- 任取 $x, y, z \in G$，

  $(x\circ y)\circ z=a_1a_2a_3\ldots a_7$　$x\circ(y\circ z)=b_1b_2b_3\ldots b_7$

  由于$a_i=(x_i\oplus y_i)\oplus z_i$　$b_i=x_i\oplus(y_i\oplus z_i)$

  所以$(x\circ y)\circ z = x\circ(y\circ z)$
- 幺元：0000000
- $\forall x\in G, x^{-1} = x$

综上所述，$<G, \circ>$构成群。

陪集的应用——线性分组码

- 某二进制的码字$x=x_1x_2x_3\ldots x_7$，其中$x_1x_2x_3x_4$数据位，$x_5x_6x_7$是校验位，并且满足：

  $x_5=x_1\oplus x_2\oplus x_3$ $x_6=x_1\oplus x_2\oplus x_4$ $x_7=x_1\oplus x_3\oplus x_4$

  $\oplus$是模2加法。

  设C是所有这样的码字构成的集合，

  在C上定义二元运算：

  $\forall x,y\in C,\ x\circ y=z_1z_2z_3\ldots z_7$，$z_i=x_i\oplus y_i$，$i=1\sim7$

- 证明$<C,\circ>$构成G的子群，称为[7, 4]线性分组码。

证明

- 幺元：0000000 $\in C$，C非空
- 任取 $x=x_1x_2x_3\ldots x_7$, $y=y_1y_2y_3\ldots y_7 \in C$, 验证 $x\circ y=z_1z_2z_3\ldots z_7\in C$

$z_1\oplus z_2\oplus z_3=(x_1\oplus y_1)\oplus(x_2\oplus y_2)\oplus(x_3\oplus y_3)$

$=(x_1\oplus x_2\oplus x_3)\oplus(y_1\oplus y_2\oplus y_3)$

$=x_5\oplus y_5$

$=z_5$

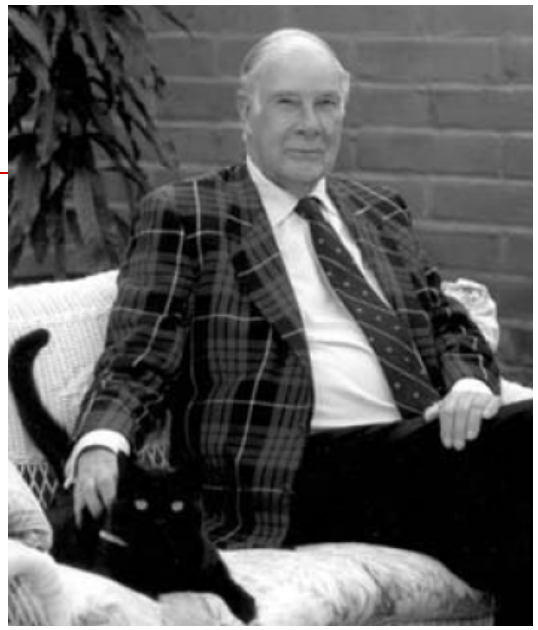
同理可证$z_1\oplus z_2\oplus z_4=z_6$和$z_1\oplus z_3\oplus z_4=z_7$

所以$x\circ y\in C$。

综上所述，$<C, \circ>$构成G的子群。

汉明码

$$\begin{cases} x_5 = x_1 \oplus x_2 \oplus x_3 \\ x_6 = x_1 \oplus x_2 \oplus x_4 \\ x_7 = x_1 \oplus x_3 \oplus x_4 \end{cases}$$



Hamming, 1915-1998

- 线性分组码中信息码元和监督码元是用线性方程联系起来的。线性码各许用码组的集合构成群,因此,又称群码.
- 这种编码方式是20世纪40年代由R.Hamming和M.Golay提出的第一个实用的差错控制编码方案，通常称为汉明码。

- **[7, 4]线性分组码的全部码字为：**

0	0	0	0	0	0	0		1	0	0	0	1	1	1
0	0	0	1	0	1	1		1	0	0	1	1	0	0
0	0	1	0	1	0	1		1	0	1	0	0	1	0
0	0	1	1	1	1	0		1	0	1	1	0	0	1
0	1	0	0	1	1	0		1	1	0	0	0	0	1
0	1	0	1	1	0	1		1	1	0	1	0	1	0
0	1	1	0	0	1	1		1	1	1	0	1	0	0
0	1	1	1	0	0	0		1	1	1	1	1	1	1

陪集的应用——线性分组码

码字	C_1 (00…0)	C_2	C_i	…	C_{2^k}
禁用码字	E_2	C_2+E_2	C_i+E_2	…	$C_{2^k}+E_2$
	E_3	C_2+E_3	C_i+E_3	…	$C_{2^k}+E_3$
	⋮	⋮	⋮	⋮	⋮
	$E_{2^{n-k}}$	$C_2+E_{2^{n-k}}$	$C_i+E_{2^{n-k}}$	…	$C_{2^k}+E_{2^{n-k}}$

陪集首

$\wp_i$

陪集

陪集的应用——线性分组码

[4，2]线性分组码

$$\begin{cases} x_3 = x_1 \oplus x_2 \\ x_4 = x_2 \end{cases}$$

译码表：

许用码字	$C^{(0)}$ 0000	$C^{(1)}$ 0111	$C^{(2)}$ 1010	$C^{(3)}$ 1101
禁用码组	0001	0110	1011	1100
	0010	0101	1000	1111
	0100	0011	1110	1001

陪集首　　陪集

10.3 循环群与置换群

- 定义10.10 设G是群，若存在$a \in G$使得

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

  则称G是循环群，记作$G=\langle a \rangle$，称 a 为G 的生成元.

例

$\circ$	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

生成元: f^1, f^3

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

生成元: b,c

定理

- 任何一个循环群必定是阿贝尔群。

证明 设$<G,*>$是循环群，它的生成元是a，则对任意$x,y\in G$，必有$r,s\in I$，使得

$$x=a^r, y=a^s$$

$$x*y=a^r*a^s=a^{r+s}=a^{s+r}$$

$$=a^s*a^r=y*x$$

因此群$<G,*>$是阿贝尔群。

循环群的分类

- 循环群的分类：n 阶循环群和无限循环群.
  - 设$G=\langle a\rangle$是循环群，若a是n 阶元，则
    $G = \{ a^0=e, a^1, a^2, \dots , a^{n-1} \}$

  那么$|G| = n$，称 G 为 n 阶循环群.
  - 若a 是无限阶元，则
    $G = \{ a^0=e, a^{\pm 1}, a^{\pm 2}, \dots \}$

  称 G 为无限循环群.
- 例如：$\langle Z, + \rangle = \langle 1 \rangle$ 是无限循环群

  $\langle Z_{12}, \oplus \rangle = \langle 1 \rangle$ 是12阶循环群。

循环群的

$\phi(n)$称为欧拉函数，表示{0,1, …n-1}中与n互质的数的个数。

- **定理10.13** 设$G=\langle a\rangle$是

  (1) 若G是无限循环群，则G只有两个 元，即a和a^{-1}.

  (2) 若G是 n 阶循环群，则G含有$\phi(n)$个生成元. 即a^r是G的生成元当且仅当r是小于n且与 n 互质的自然数.

- 例如 n=12，小于或等于12且与12互素的正整数有4个： 1, 5, 7, 11，所以$\phi(12)=4$.

实例

- $\langle Z, + \rangle$的生成元
  - 1和-1
- $\langle Z_{12}, \oplus \rangle$的生成元
  - 1、5、7、11

定理证明

- (1) 显然$\langle a^{-1}\rangle \subseteq G$. $\forall a^k \in G$,

$$a^k=(a^{-1})^{-k} \in \langle a^{-1}\rangle,$$

因此$G \subseteq \langle a^{-1}\rangle$，$a^{-1}$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 $G=\langle b\rangle$.
由$a \in G$ 可知存在整数 t 使得$a = b^t$.
由$b \in G = \langle a\rangle$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中的消去律得 $a^{mt-1} = e$
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 $b = a^{-1}$

定理证明（续）

- (2) 只须证明：对任何自然数 r ($r<n$)，

  a^r是G的生成元 $\Leftrightarrow$ n与r互质.

  - 充分性. 设r与n互质，且$r<n$，那么存在整数 u 和 v 使得　$ur + vn = 1$

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

这就推出$\forall a^k \in G$，$a^k = (a^r)^{uk} \in <a^r>$,

即$G \subseteq <a^r>$.

另一方面，显然有$<a^r> \subseteq G$. 从而$G = <a^r>$.

定理证明（续）

- 必要性.

设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,

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

所以是$|a^r|$是n/d的因子，即n整除n/d.

从而证明了$d = 1$，即r与n互质。

循环群的子群

- **定理10.14** 设$G=\langle a\rangle$是循环群.

  (1) G的子群仍是循环群.

  (2) 若$G=\langle a\rangle$是无限循环群，则G的子群除$\{e\}$以外都是无限循环群.

  (3) 若$G=\langle a\rangle$是n阶循环群，则对n的每个正因子d，G恰好含有一个d阶子群.

证明

- (1) 设H是$G=\langle a\rangle$的子群，若$H=\{e\}$，显然H是循环群，否则取H中的最小正方幂元a^m，下面证明$H=\langle a^m\rangle$. 易见$\langle a^m\rangle \subseteq H$.
- 下面证明$H\subseteq\langle a^m\rangle$. 任取$a^l\in H$，由除法可知存在整数 q 和 r，使$l = qm+r$，其中 $0\le r\le m-1$

$$a^r = a^{l-qm} = a^l(a^m)^{-q}$$

由$a^l, a^m\in H$ 且 H 是G 的子群可知$a^r\in H$.

因为a^m是H中最小正方幂元，必有$r = 0$.

推出$a^l = (a^m)^q\in\langle a^m\rangle$

证明

- (2) 设$G=\langle a\rangle$是无限循环群，H是G 的子群. 若$H\neq\{e\}$可知$H=\langle a^m\rangle$，其中a^m为H中最小正方幂元. 假若 $|H|=t$，则 $|a^m|=t$，

  从而得到$a^{mt}=e$. 这与a为无限阶元矛盾.

证明

- (3) 设$G=\langle a\rangle$是 n 阶循环群，则 $G=\{a^0=e, a^1, \ldots, a^{n-1}\}$, 下面证明对于$n$的每个正因子$d$都恰好存在一个$d$阶子群.
  - 易见$H=\langle a^{n/d}\rangle$是G的d 阶子群.
  - 假设$H_1=\langle a^m\rangle$也是G的d 阶子群，其中 a^m 为H_1中的最小正方幂元.
    则由 $(a^m)^d=e$ 可知 n 整除md，即 n/d 整除 m.
    令$m=(n/d)\cdot l$，l是整数，则有$a^m=(a^{n/d})^l$
    这就推出$H_1\subseteq H$.
    又由于 $|H_1|=|H|=d$，得$H_1=H$.

实例

- (1)设G_1=<Z,+>是整数加群，求G_1的所有子群。
- 解：

G_1=<Z,+>是无限循环群，其生成元为1和–1.

<0> = {0}是有限子群

对于正整数$m \in Z^+$，1的m次幂是m，

m生成的子群是mZ，$m \in Z^+$. 即

$<m> = \{mz \mid z \in Z, m \in Z^+\}$是无限子群

实例

- (2) 设$G_2=<Z_{12}, \oplus>$，求G_2的所有子群。
- 解：$G_2=<Z_{12}, \oplus>$是12阶循环群.

  12正因子是1,2,3,4,6和12，G 的子群:

  1阶子群　<0>={0}

  2阶子群　<6>={0,6}

  3阶子群　<4>={0,4,8}

  4阶子群　<3>={0,3,6,9}

  6阶子群　<2>={0,2,4,6,8,10}

  12阶子群　<1>=Z_{12}

n 元置换

- 定义10.11 设 $S=\{1, 2, \ldots, n\}$, S上的任何双射函数$\sigma: S \to S$ 称为S上的n元置换.
- 例如 $S=\{1, 2, 3, 4, 5\}$, 下述为5元置换:

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

- n元置换一共有$n!$个。
- 恒等置换：S上的恒等函数。

群的性质——置换性

- 定理：群$< G , * >$的运算表中的每一行或每一列都是 G 的元素的一个置换。

证明

对于任意$a \in G$，

1. 考察对应于$a \in G$的那一行，设b是G中的任一元素，由于$b = a * (a^{-1} * b)$,所以b必定出现在对应于a的那一行中。

2. 若对应于$a \in G$的那一行中有两个元素都是c ,则有 $a * b_1 = a * b_2 = c$ 且$b_1 \neq b_2$，这与消去律矛盾。

综上所述，群$< G , * >$的运算表中的每一行都是 G 的元素的一个置换。

对于列同理可证，所以定理成立。

置换的乘法

- **定义10.12** 设σ,τ是n元置换, σ和τ的复合$\sigma\circ\tau$也是n元置换, 称为σ与τ 的乘积, 记作$\sigma\tau$.
- 例如

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

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

轮换与对换

- 定义10.13 设σ是$S=\{1,2,\ldots,n\}$上的n元置换，若$\sigma(i_1)=i_2, \sigma(i_2)=i_3, \ldots, \sigma(i_{k-1})=i_k, \sigma(i_k)=i_1$，且保持$S$中其他元素不变，则称σ是$S$上的$k$阶轮换，记作$(i_1, i_2, \ldots, i_k)$.
- 如果$k=2$，则称σ是S上的对换。

n元置换的轮换表示

- 设 $S = \{1, 2, \ldots, n\}$，对于任何S上的 n 元置换 σ, 存在着一个有限序列 $i_1, i_2, \ldots, i_k$, $k \geq 1$, (可以取$i_1=1$) 使得

  $\sigma(i_1) = i_2, \sigma(i_2) = i_3, \ldots, \sigma(i_{k-1}) = i_k, \sigma(i_k) = i_1$

  - 令 $\sigma_1 = (i_1\ i_2 \ldots i_k)$, 是 σ 分解的第一个轮换. 将 σ 写作 $\sigma_1\sigma'$, 继续对 σ' 分解. 由于S 只有n 个元素, 经过有限步得到

    $\sigma = \sigma_1 \sigma_2 \ldots \sigma_t$

实例

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

σ(1)=5, σ(5)=4, σ(4)=1

第一个轮换(1 5 4)

σ(2)=3, σ(3)=2

第二个轮换(2 3)

σ=(1 5 4)(2 3)

τ(1)=4, τ(4)=2, τ(2)=3,τ(3)=1

第一个轮换(1 4 2 3)

τ(5)=5

第二个轮换(5)

τ =(1 4 2 3)(5)=(1 4 2 3)

实例

- 设$S = \{1, 2, \ldots, 8\}$,

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 5 & 3 & 6 & 4 & 2 & 1 & 8 & 7 \end{pmatrix}$$

$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 8 & 1 & 4 & 2 & 6 & 7 & 5 & 3 \end{pmatrix}$$

则 轮换分解式为：

$\sigma = (1\ 5\ 2\ 3\ 6)\ (4)\ (7\ 8) = (1\ 5\ 2\ 3\ 6)\ (7\ 8)$

$\tau = (1\ 8\ 3\ 4\ 2)\ (5\ 6\ 7)$

轮换分解式的特征

- 定理：任意置换恰有一法写成不相交的轮换乘积。
  - 轮换的不交性
  - 分解的惟一性

    若 $\sigma = \sigma_1\sigma_2 \ldots \sigma_t$ 和 $\sigma = \tau_1\tau_2 \ldots \tau_s$

    则 $\{\sigma_1, \sigma_2, \ldots, \sigma_t\} = \{\tau_1, \tau_2, \ldots, \tau_s\}$
- 通常省略轮换分解式中的1阶轮换，如果其中全是1阶轮换，则需要保留一个1阶轮换。
  - 如恒等置换(1)(2)(3)(4)(5)简记为(1).

置换的对换分解

- 设$S=\{1,2,\ldots,n\}$，$\sigma=(i_1\ i_2\ \ldots\ i_k)$是$S$上的$k$阶轮换，$\sigma$可以进一步表成对换之积，即
$(i_1\ i_2\ \ldots\ i_k)=(i_1\ i_2)\ (i_1\ i_3)\ \ldots\ (i_1\ i_k)$

$$\sigma=\begin{bmatrix}1&2&3\\2&3&1\end{bmatrix}=(1\quad 2\quad 3)$$

$$(1\quad 2)(1\quad 3)$$

$$=\begin{bmatrix}1&2&3\\2&1&3\end{bmatrix}\begin{bmatrix}1&2&3\\3&2&1\end{bmatrix}$$

$$=\begin{bmatrix}1&2&3\\2&3&1\end{bmatrix}=\sigma$$

实例

- 例如 8 元置换

$\sigma = (1\ 5\ 2\ 3\ 6)\ (7\ 8) = (1\ 5)\ (1\ 2)\ (1\ 3)\ (1\ 6)\ (7\ 8)$

$\tau = (1\ 8\ 3\ 4\ 2)\ (5\ 6\ 7)$

$= (1\ 8)\ (1\ 3)\ (1\ 4)\ (1\ 2)\ (5\ 6)\ (5\ 7)$

对换分解的特征

- 对换分解式中对换之间可以有交，分解式也不惟一.

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

$\sigma=(1\ 2)(1\ 3)$,

$\sigma=(1\ 4)(2\ 4)(3\ 4)(1\ 4)$

- 如果n元置换σ可以表示成奇数个对换之积，则称σ为奇置换，否则称为偶置换。
- 表示式中所含对换个数的奇偶性是不变的.
- 可以证明n元置换中奇置换和偶置换各有$n!/2$个.

n元奇置换和偶置换的数量相等

- 定义一个映射f_τ，对任意的n元偶置换σ $f_\tau(\sigma)=\sigma\tau$。

  易见，f_τ是一个双射：

  - 首先是个单射：若$\sigma\tau=\sigma'\tau$，则$\sigma=\sigma'$。
  - 其次是个满射：对于任意的n元奇置换σ，存在$\sigma\tau^{-1}$使得

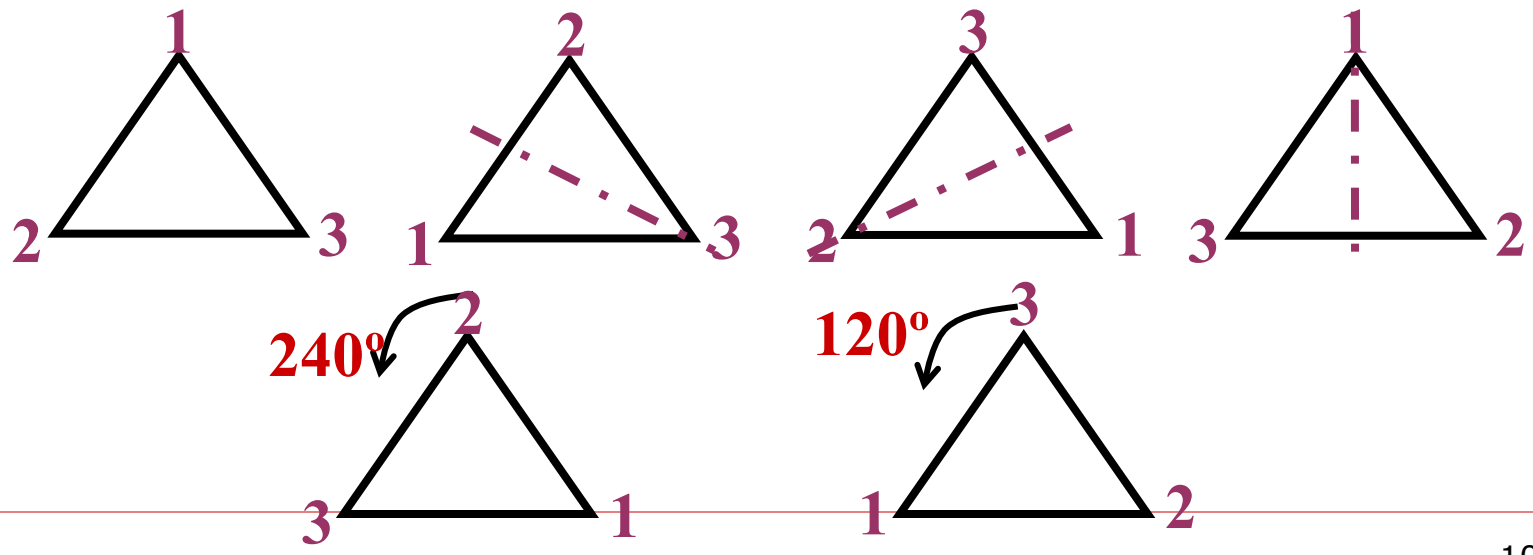
    $$f_\tau(\sigma\tau^{-1})=\sigma$$

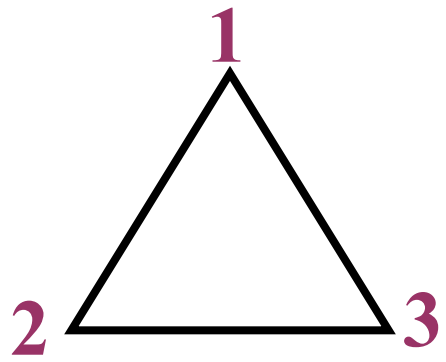
- 故n元奇置换和偶置换的个数相同。

n元对称群

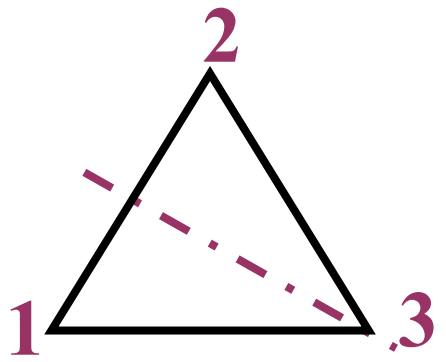
- 所有的 n元置换构成的集合S_n关于置换乘法构成群，称为**n元对称群**. n元对称群的子群叫做**n元置换群**。
- 例 设 $S = \{1, 2, 3\}$，3元对称群

  S_3={ (1), (1 2), (1 3), (2 3), (1 2 3), (1 3 2) }

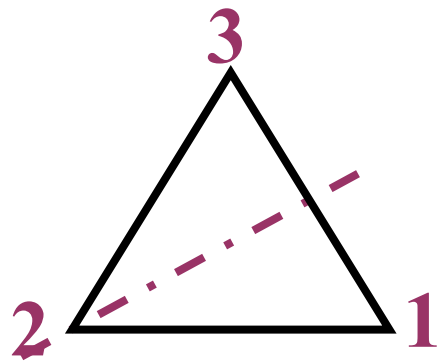




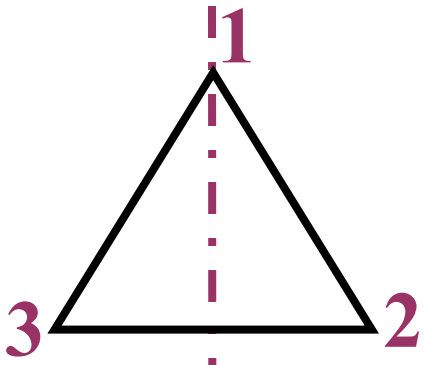
f_1={<1,1>,<2,2>,<3,3>} (1)



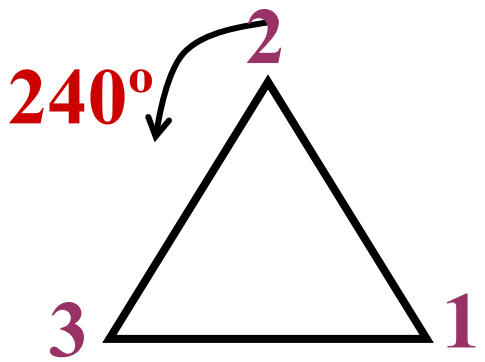
f_2={<1,2>,<2,1>,<3,3>} (1 2)



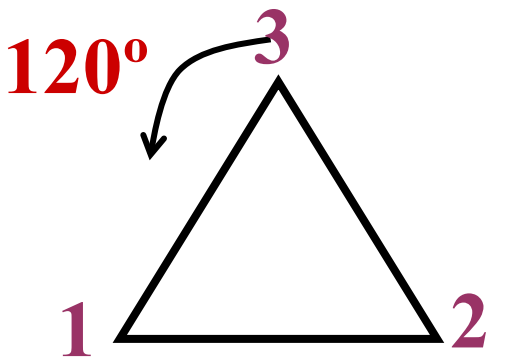
f_3={<1,3>,<2,2>,<3,1>} (1 3)



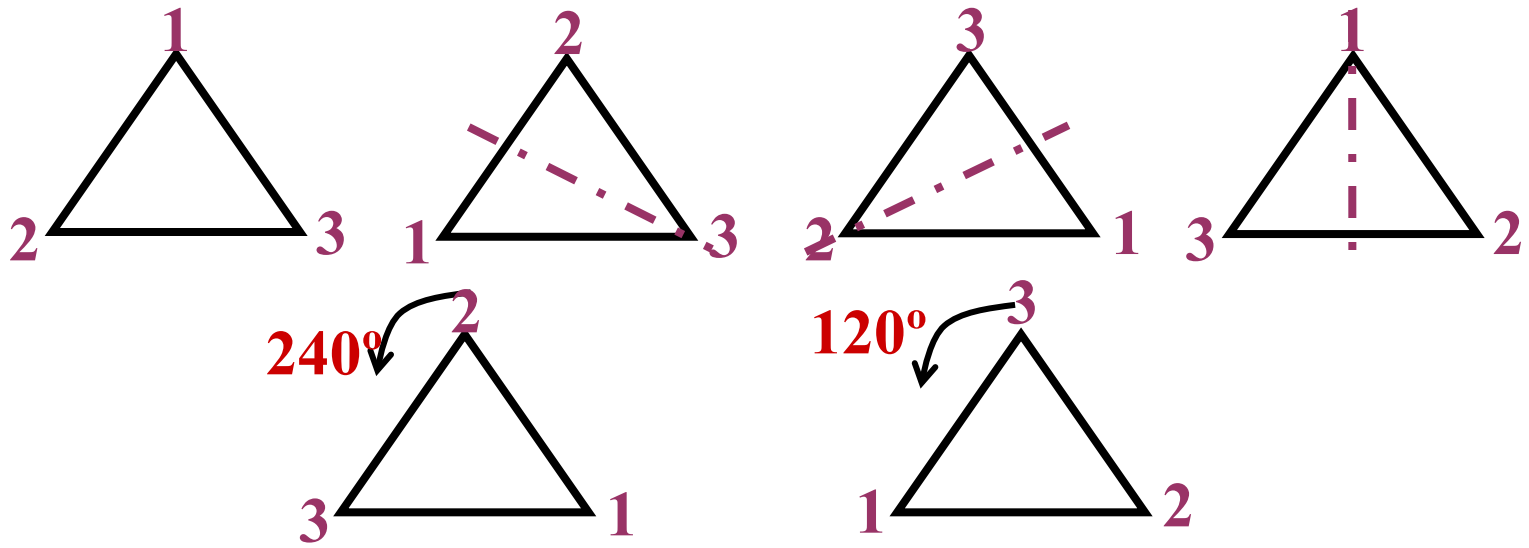
f_4={<1,1>,<2,3>,<3,2>} (2 3)



f_5={<1,2>,<2,3>,<3,1>} (1 2 3)



f_6={<1,3>,<2,1>,<3,2>}(1 3 2)



∘	(1)	(1 2)	(1 3)	(2 3)	(1 2 3)	(1 3 2)
(1)	(1)	(1 2)	(1 3)	(2 3)	(1 2 3)	(1 3 2)
(1 2)	(1 2)	(1)	(1 2 3)	(1 3 2)	(1 3)	(2 3)
(1 3)	(1 3)	(1 3 2)	(1)	(1 2 3)	(2 3)	(1 2)
(2 3)	(2 3)	(1 2 3)	(1 3 2)	(1)	(1 2)	(1 3)
(1 2 3)	(1 2 3)	(2 3)	(1 2)	(1 3)	(1 3 2)	(1)
(1 3 2)	(1 3 2)	(1 3)	(2 3)	(1 2)	(1)	(1 2 3)

n元交错群

- n元交错群A_n是S_n的子群， A_n是所有的n元偶置换的集合.

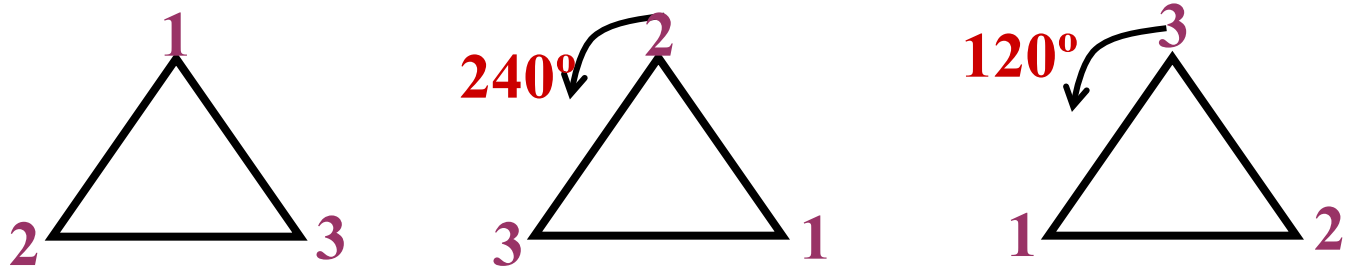
- 证 恒等置换(1) 是偶置换，所以A_n非空.

  根据判定定理三，只需证明封闭性：

  - 任取$\sigma,\tau \in A_n$， σ, τ 都可以表成偶数个对换之积，那么$\sigma\tau$也可以表成偶数个对换之积，所以$\sigma\tau \in A_n$.

实例

- 设 $S = \{1, 2, 3\}$，3元交错群
  $A_3 = \{ (1), (1\ 2\ 3), (1\ 3\ 2) \}$



∘	(1)	(1 2 3)	(1 3 2)
(1)	(1)	(1 2 3)	(1 3 2)
(1 2 3)	(1 2 3)	(1 3 2)	(1)
(1 3 2)	(1 3 2)	(1)	(1 2 3)

实例

- S_3的子群格

S_3是6阶群，根据拉格朗日定理，

S_3的子群的阶数只能是1,2,3,6

1阶：{(1)}

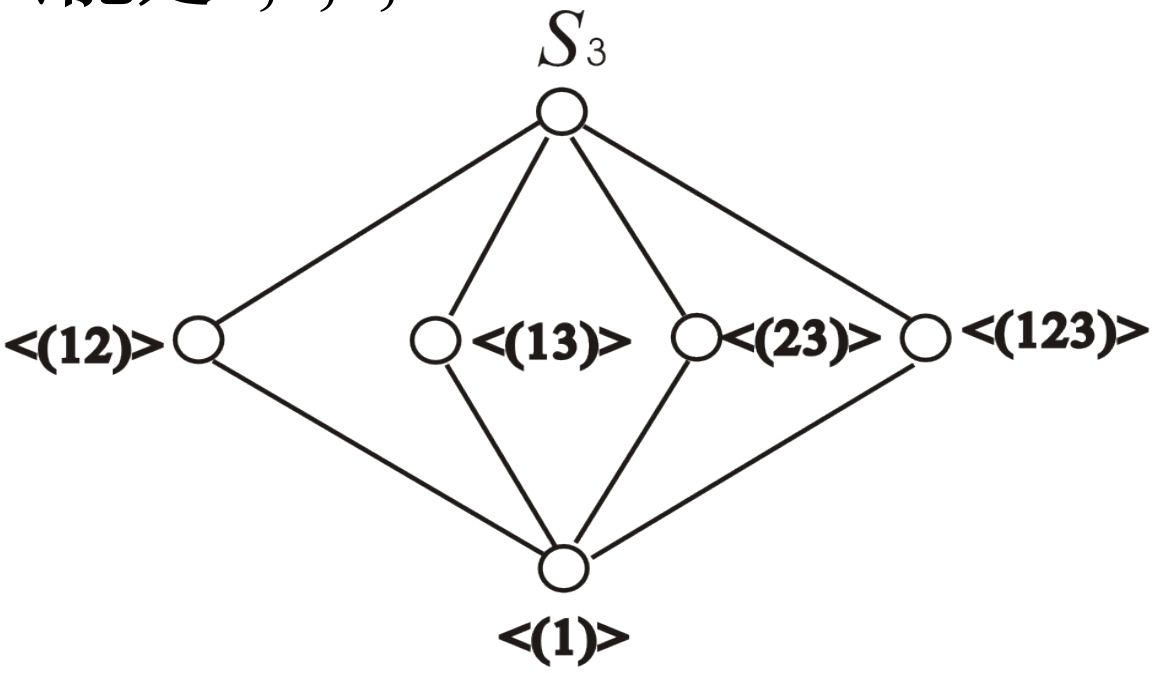
2阶：{(1), (12)}

{(1), (13)}

{(1), (23)}

3阶：A_3

6阶：S_3



Polya定理

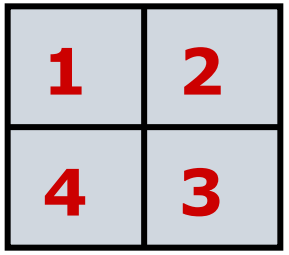
- **定理10.15** 设$N=\{1,2,\ldots,n\}$是被着色物体的集合, $G=\{\sigma_1, \sigma_2, \ldots, \sigma_g\}$是$N$上的置换群. 用$m$种颜色对$N$中的元素进行着色，则在$G$的作用下不同的着色方案数是

$$M = \frac{1}{|G|}\sum_{k=1}^{g} m^{c(\sigma_k)}$$

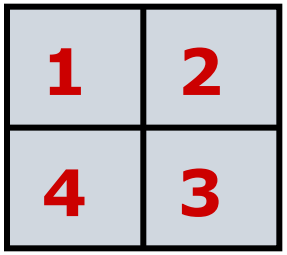
- 其中$c(\sigma_k)$是置换σ_k的轮换表示中包含1-轮换在内的轮换个数.
- Polya定理主要用于等价类的计数.

Polya定理在组合计数中的应用

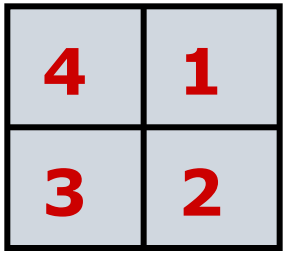
例：用两种颜色着色方格图形，允许方格绕中心转动，求不同的方案数.



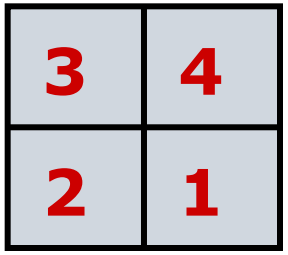
解：群G中的所有置换是（每次顺时针转90°）



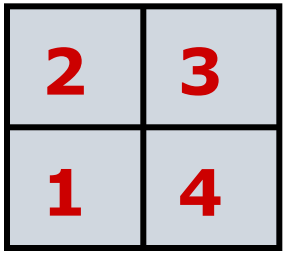
$\sigma_1=(1)$



$\sigma_2=(1432)$

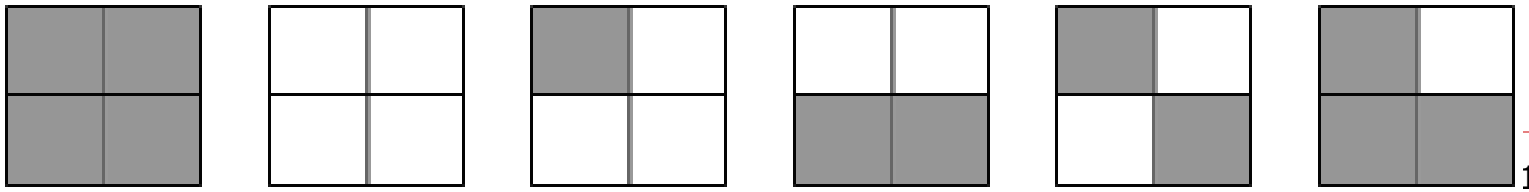


$\sigma_3=(13)(24)$



$\sigma_4=(1234)$

代入Polya定理得 $M=\frac{1}{4}(2^4+2^1+2^2+2^1)=6$



Polya定理练习

- 考察从蓝、黄、白三种颜色的珠子中选取5粒串成手镯，如果将一只手镯经过顺时针旋转得到另一只手镯看作是没有区别的手镯，并称这两只手镯是旋转等价的，那么，在考虑旋转等价的条件下，不同手镯的数目是多少？
- 解：围绕中心旋转的置换为：

0°： (●) (●) (●) (●) (●) 1个

72°、144°、216°、288°：(● ● ● ● ●) 4个

根据Polya定理，不同的着色方案数是

$$M = \frac{1}{5}(3^5 + 3^1 + 3^1 + 3^1 + 3^1) = 51$$

10.4 环与域

- 定义10.14 设<R,+,·>是代数系统，+和·是二元运算. 如果满足以下条件:

  (1) <R,+>构成交换群

  (2) <R,·>构成半群

  (3) · 运算关于+运算适合分配律

  则称<R,+,·>是一个环.

说明

- 通常称+运算为环中的加法，·运算为环中的乘法,通常可以省略.
- 环中加法单位元记作 0，乘法单位元（如果存在）记作1.
- 对任何元素 x，称 x 的加法逆元为负元，记作$-x$, $(x-y)$表示$x+(-y)$. 若 x 存在乘法逆元的话，则称之为逆元，记作x^{-1}.
- nx表示n个x相加，x^n表示n个x相乘.

环的实例

- (1) 整数集、有理数集、实数集和复数集关于普通的加法和乘法构成环，分别称为整数环Z，有理数环Q，实数环R 和复数环C.
- (2)设$Z_n=\{0,1,\ldots,n-1\}$，$\oplus$和$\otimes$分别表示模n的加法和乘法，则$\langle Z_n,\oplus,\otimes\rangle$构成环，称为模 n的整数环.
- (3) $n(n\geq 2)$阶实矩阵的集合$M_n(\mathbf{R})$关于矩阵的加法和乘法构成环，称为 n 阶实矩阵环.
- (4)集合的幂集$P(B)$关于集合的对称差运算和交运算构成环.

环的运算性质

- **定理10.16** 设$<R,+,\cdot>$是环，则

(1) $\forall a \in R$，$a0 = 0a = 0$

(2) $\forall a,b \in R$，$(-a)b = a(-b) = -ab$

(3) $\forall a,b,c \in R$，$a(b-c) = ab-ac$，

$(b-c)a = ba-ca$

(4) $\forall a_1,a_2,\ldots,a_n,b_1,b_2,\ldots,b_m \in R$ $(n,m \geq 2)$

$$(\sum_{i=1}^{n} a_i)(\sum_{j=1}^{m} b_j) = \sum_{i=1}^{n}\sum_{j=1}^{m} a_i b_j$$

证明

- 证 (1) $\forall a \in R$有 $a0 = a(0+0) = a0+a0$
  由环中加法的消去律得$a0=0$. 同理可证$0a=0$.
  (2) $\forall a,b \in R$，有
  $(-a)b+ab = (-a+a)b = 0b = 0$
  $ab+(-a)b = (a+(-a))b = 0b = 0$
  $(-a)b$是ab的负元. 由负元惟一性
  $(-a)b = -ab$，同理$a(-b) = -ab$

证明

(4) 证明思路：用归纳法证明 $\forall a_1, a_2, \dots, a_n$ 有

$$(\sum_{i=1}^{n} a_i) b_j = \sum_{i=1}^{n} a_i b_j$$

同理可证, $\forall b_1, b_2, \dots, b_m$ 有

$$a_i (\sum_{j=1}^{m} b_j) = \sum_{j=1}^{m} a_i b_j$$

于是 $$(\sum_{i=1}^{n} a_i)(\sum_{j=1}^{m} b_j) = \sum_{i=1}^{n} a_i (\sum_{j=1}^{m} b_j) = \sum_{i=1}^{n} \sum_{j=1}^{m} a_i b_j$$

实例

- 例：在环中计算$(a+b)^3$, $(a-b)^2$
- 解 $(a+b)^3 = (a+b)(a+b)(a+b)$

$$= (a^2+ba+ab+b^2)(a+b)$$

$$= a^3+ba^2+aba+b^2a+a^2b+bab+ab^2+b^3$$

$$(a-b)^2 = (a-b)(a-b) = a^2-ba-ab+b^2$$

特殊的环

□ 定义10.15 设$<R,+,\cdot>$是环

(1) 若环中乘法$\cdot$适合交换律，则称R是交换环

(2) 若环中乘法$\cdot$存在单位元，则称R是含幺环

(3) 若$\forall a,b\in R$，$ab=0 \Rightarrow a=0 \vee b=0$，则称$R$是无零因子环

(4) 若R既是交换环、含幺环、无零因子环，则称R是整环

(5) 设R是整环，且R中至少含有两个元素. 若$\forall a\in R^*$，其中$R^*=R-\{0\}$，都有$a^{-1}\in R$，则称R是域.

实例

(1) 整数环Z、有理数环Q、实数环R、复数环C

- 交换环、含幺环、无零因子环、整环.
  除了整数环以外都是域.

(2) $2\mathbf{Z}=\{2z \mid z\in\mathbf{Z}\}$，$\langle 2\mathbf{Z},+,\cdot\rangle$

- 交换环、无零因子环

(3) 设$n\in\mathbf{Z}$, $n\geq 2$, 则n阶实矩阵的集合$M_n(\mathbf{R})$关于矩阵加法和乘法

- 含幺环

(4) $\langle \mathbf{Z}_6,\oplus,\otimes\rangle$

- 交换环、含幺环

定理（补充）

- 在整环$<A,+,\cdot>$中无零因子当且仅当乘法满足消去律，即对于$c\neq0$和$c\cdot a=c\cdot b$,必有$a=b$。
- 证明 若无零因子并设$c\neq0$和$c\cdot a=c\cdot b$，则有

$$c\cdot a-c\cdot b=c\cdot(a-b)=0$$

所以，必有$a=b$，即乘法满足消去律。

- 反之，若乘法满足消去律，
设$a\neq0$，$a\cdot b=0$则$a\cdot b=a\cdot0$
消去a即得$b=0$，即无零因子。

练习

- 设 p为素数，证明$\mathbf{Z}_p$是域.
- 证　p为素数，所以 $|\mathbf{Z}_p|\geq 2$.

  易见$\mathbf{Z}_p$可交换，单位元是1.

  对于任意的 $i, j\in\mathbf{Z}_p$, 设$i\neq 0$有

  $$i\otimes j=0\Rightarrow p\mid ij\Rightarrow p\mid j\Rightarrow j=0$$

  所以 $\mathbf{Z}_p$ 中无零因子，$\mathbf{Z}_p$为整环.

练习（续）

下面证明每个非零元素都有逆元.

因为Z_p 是有限半群, 且Z_p关于$\otimes$适合消去律

任取 $i \in Z_p$，$i \neq 0$，令

$$i \otimes Z_p = \{ i \otimes j \mid j \in Z_p \}$$

则 $i \otimes Z_p = Z_p$,

否则$\exists\, j, k \in Z_p$，使得 $i \otimes j = i \otimes k$,

由消去律得 $j = k$.

由$1 \in Z_p$，存在 $j \in Z_p$，使得 $i \otimes j = 1$.

由于交换性可知 j 就是i 的逆元.

解域方程

- 在域Z_5中解方程：$3x=2$
- 解：　　$x = 3^{-1} \cdot 2 = 2 \cdot 2 = 4$

第十章 习题课

- 主要内容
  - 半群、独异点与群的定义
  - 群的基本性质
  - 子群的判别定理
  - 陪集的定义及其性质
  - 拉格朗日定理及其应用
  - 循环群的生成元和子群
  - 置换群与Polya定理
  - 环的定义与性质
  - 特殊的环

基本要求

- 判断或证明给定集合和运算是否构成半群、独异点和群
- 熟悉群的基本性质
- 能够证明G的子集构成G的子群
- 熟悉陪集的定义和性质
- 熟悉拉格朗日定理及其推论，能够简单应用
- 会用Polya定理进行计数
- 熟悉循环群的生成元及其子群性质
- 熟悉n元置换的表示方法、乘法以及n元置换群
- 能判断给定代数系统是否为环和域

练习1

- 判断下列集合和运算是否构成半群、独异点和群.

  (1) a 是正整数，$G = \{a^n \mid n \in \mathbf{Z}\}$, 运算是普通乘法.

  (2) $\mathbf{Q}^+$是正有理数集，运算为普通加法.

  (3) 一元实系数多项式的集合关于多项式加法.

练习1解答

(1) 是半群、独异点和群

(2) 是半群但不是独异点和群

(3) 是半群、独异点和群

- 方法：根据定义验证，注意运算的封闭性

练习2

- 设V_1= <Z, +>, V_2 = <Z, ·>,其中Z为整数集合, + 和· 分别代表普通加法和乘法. 显然V_1和V_2是半群和独异点.
  判断下述集合S是否构成V_1和V_2的子半群和子独异点.

  (1) S= {2k | k∈Z}

  (2) S= {2k+1 | k∈Z}

  (3) S= {–1, 0, 1}

练习2解答

- (1) S关于V_1构成子半群和子独异点，但是关于V_2仅构成子半群。
- (2) S关于V_1不构成子半群也不构成子独异点，S关于V_2构成子半群和子独异点。
- (3) S关于V_1不构成子半群和子独异点，关于V_2构成子半群和子独异点。

练习3

- 判断下列集合和给定运算是否构成环、整环和域, 如果不构成, 说明理由.

(1) $A = \{ a+b\mathrm{i} \mid a,b \in \mathbf{Q} \}$, 其中$\mathrm{i}^2 = -1$, 运算为复数加法和乘法.

(2) $A=\{ 2z+1 \mid z \in \mathbf{Z}\}$, 运算为实数加法和乘法

(3) $A=\{ 2z \mid z \in \mathbf{Z}\}$, 运算为实数加法和乘法

(4) $A=\{ x \mid x \geq 0 \wedge x \in \mathbf{Z}\}$, 运算为实数加法和乘法.

(5)

$A = \{a + b\sqrt[4]{5} \mid a,b \in \mathbf{Q}\}$, 运算为实数加法和乘法。

练习3解答

- 解:

  (1) 是环, 是整环, 也是域.

  (2) 不是环, 因为关于加法不封闭.

  (3) 是环, 不是整环和域, 因为乘法没有么元.

  (4) 不是环, 因为正整数关于加法的负元不存在.

  (5) 不是环, 因为关于乘法不封闭.

练习4

- 设Z_{18} 为模18整数加群, 求所有元素的阶.
- 解:

$|0| = 1$

$|9| = 2$

$|6| = |12| = 3$

$|3| = |15| = 6$

$|2| = |4| = |8| = |10| = |14| = |16| = 9$

$|1| = |5| = |7| = |11| = |13| = |17| = 18$

说明

- 群中元素的阶可能存在，也可能不存在.
- 对于有限群，每个元素的阶都存在，而且是群的阶的因子.
- 对于无限群，单位元的阶存在，是1；而其它元素的阶可能存在，也可能不存在.（可能所有元素的阶都存在，但是群还是无限群）.

练习5

(1) 设G为模12加群, 求<3> 在G中所有的左陪集

(2) 设 $X=\{x \mid x\in \mathbf{R}, x\neq 0,1\}$, 在$X$上如下定义6个函数:

$f_1(x)=x$, $f_2(x)=1/x$, $f_3(x)=1-x$,

$f_4(x)=1/(1-x)$, $f_5(x)=(x-1)/x$, $f_6(x)=x/(x-1)$,

则$G=\{f_1,f_2,f_3,f_4,f_5,f_6\}$关于函数合成运算构成群. 求子群$H=\{f_1,f_2\}$ 的所有的右陪集.

练习5解答

解：(1) <3> = {0, 3, 6, 9}, <3>的不同左陪集有3个，即

$0\langle 3\rangle = \langle 3\rangle$,

$1\langle 3\rangle = \{1, 4, 7, 10\}$

$= 4\langle 3\rangle = 7\langle 3\rangle = 10\langle 3\rangle$

$2\langle 3\rangle = \{2, 5, 8, 11\}$

$= 5\langle 3\rangle = 8\langle 3\rangle = 11\langle 3\rangle$

(2) $\{f_1, f_2\}$有3个不同的陪集，它们是：

H，$Hf_3 = \{f_3, f_5\}$，$Hf_4 = \{f_4, f_6\}$.

练习6

- 设 i 为虚数单位，即 $i^2=-1$, 令

$$G=\left\{\pm\begin{pmatrix}1&0\\0&1\end{pmatrix},\ \pm\begin{pmatrix}\mathrm{i}&0\\0&-\mathrm{i}\end{pmatrix},\ \pm\begin{pmatrix}0&1\\-1&0\end{pmatrix},\ \pm\begin{pmatrix}0&\mathrm{i}\\\mathrm{i}&0\end{pmatrix}\right\}$$

则G关于矩阵乘法构成群. 找出G的所有子群.

练习6解答

- 解 令A, B, C, D分别为

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix},$$

$$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$$

则运算表为

×	*A*	*-A*	*B*	*-B*	*C*	*-C*	*D*	*-D*
A	*A*	*-A*	*B*	*-B*	*C*	*-C*	*D*	*-D*
-A	*-A*	*A*	*-B*	*B*	*-C*	*C*	*-D*	*D*
B	*B*	*-B*	*-A*	*A*	*D*	*-D*	*-C*	*C*
-B	*-B*	*B*	*A*	*-A*	*-D*	*D*	*C*	*-C*
C	*C*	*-C*	*-D*	*D*	*-A*	*A*	*B*	*-B*
-C	*-C*	*C*	*D*	*-D*	*A*	*-A*	*-B*	*B*
D	*D*	*-D*	*C*	*-C*	*-B*	*B*	*-A*	*A*
-D	*-D*	*D*	*-C*	*C*	*B*	*-B*	*A*	*-A*

×	*A*	*-A*	*B*	*-B*	*C*	*-C*	*D*	*-D*
A	*A*	*-A*	*B*	*-B*	*C*	*-C*	*D*	*-D*
-A	*-A*	*A*	*-B*	*B*	*-C*	*C*	*-D*	*D*
B	*B*	*-B*	*-A*	*A*	*D*	*-D*	*-C*	*C*
-B	*-B*	*B*	*A*	*-A*	*-D*	*D*	*C*	*-C*
C	*C*	*-C*	*-D*	*D*	*-A*	*A*	*B*	*-B*
-C	*-C*	*C*	*D*	*-D*	*A*	*-A*	*-B*	*B*
D	*D*	*-D*	*C*	*-C*	*-B*	*B*	*-A*	*A*
-D	*-D*	*D*	*-C*	*C*	*B*	*-B*	*A*	*-A*

*G*的子群有6个，即

平凡子群：$\langle A\rangle = \{A\}$, G

2 阶子群：$\langle -A\rangle = \{A, -A\}$,

4 阶子群：$\langle B\rangle = \{A,B,-A,-B\}$,

$\langle C\rangle = \{A,C,-A,-C\}$,

$\langle D\rangle = \{A,D,-A,-D\}$,

练习7

- 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和子群。

解：$G=\langle b\rangle$是循环群

$|b|=|f|=6$, b和f是生成元.

$|c|=|e|=3$, $|d|=2$,c,d,e不是生成元.

子群：阶数1,2,3,6

1阶：$\langle a\rangle=\{a\}$

2阶：$\langle d\rangle=\{d, a\}$

3阶：$\langle c\rangle=\{c, e, a\}$

6阶：G

$*$	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

练习8

- 设群G为有限群，则G中阶大于2的元素有偶数个。
- 证明：对于任意元素$a \in G$，根据消去律有

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

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。所以结论成立。

练习9

- 证明偶数阶群必含2阶元.
- 证：由 $x^2 = e \Leftrightarrow |x| = 1$ 或2.

  换句话说, 对于G中元素x，如果 $|x| > 2$, 必有 $x^{-1} \neq x$.

  由于 $|x| = |x^{-1}|$，阶大于2的元素成对出现，共有偶数个.

  那么剩下的 1 阶和 2 阶元总共应该是偶数个.

  1 阶元只有 1 个，就是单位元，从而证明了G中必有 2 阶元.

练习10

- 试证：任何一个四阶群只可能是四阶循环群或者Klein四元群。
- 证明：设四阶群为<{*e*,*a*,*b*,*c*},*>。其中*e*是单位元。
  - 当四阶群含有一个四阶元素时，这个群就是循环群。
  - 当四阶群不含有四阶元素时，则由Lagrange定理的推论1可知，除单位元*e*外，*a*,*b*,*c*的阶一定都是2。

练习10（续）

- $a*b$不可能等于a,b,e, 否则将导致$b=e,a=e$或$a=b$的矛盾，所以$a*b=c$。
- 同样可以证明$b*a=c$, $a*c=c*a=b$, $b*c=c*b=a$,

  因此这个群是Klein四元群。

练习11

- 设G为群，a是G中的2 阶元，证明G中与a可交换的元素构成G的子群.
- 证明：令$H=\{x \mid x\in G \wedge xa = ax\}$, 下面证明$H$是$G$的子群. 因为$a$是2阶元，所以$a=a^{-1}$.

  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.

说明

- 判定定理一：
  - 验证 H 非空
  - 任取 $x, y \in H$，证明 $xy \in H$
  - 任取 $x \in H$，证明 $x^{-1} \in H$
- 判定定理二：
  - 验证 H 非空
  - 任取 $x, y \in H$，证明 $xy^{-1} \in H$
- 判定定理三：
  - 验证 H 非空，有限
  - 任取 $x, y \in H$，证明 $xy \in H$

练习12

- 设 H_1, H_2分别是群G 的 r, s 阶子群，若 $\gcd(r,s) = 1$，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 $|H_1 \cap H_2|$ 整除 r与s 的最大公因子.

  因为$(r,s) = 1$, 从而 $|H_1 \cap H_2| = 1$.

  即 $H_1 \cap H_2 = \{e\}$.

练习13

- 设$G=<a>$是循环群,阶为n.试证明：
  对任何自然数 r ($r<n$)，如果a^r是G的生成元,
  则 n与r互质.
- 证明：设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,
  $(a^r)^{n/d} = (a^{dt})^{n/d} = (a^n)^t = e$
  所以是$|a^r|$是n/d的因子，即n整除n/d.
  从而证明了$d = 1$，即r与n互质。

练习14

- 设$G=\langle a\rangle$是循环群，试证G的子群仍是循环群.
- 证明：
  - 设H是$G=\langle a\rangle$的子群，若$H=\{e\}$，显然H是循环群，否则取H中的最小正方幂元a^m，下面证明$H=\langle a^m\rangle$. 易见$\langle a^m\rangle \subseteq H$.
  - 下面证明$H\subseteq\langle a^m\rangle$. 任取$a^l\in H$，由除法可知存在整数 q 和 r，使

    $l = qm+r$，　其中 $0\le r\le m-1$

    $a^r = a^{l-qm} = a^l(a^m)^{-q}$

由$a^l, a^m\in H$ 且 H 是G 的子群可知$a^r\in H$.
因为a^m是H中最小正方幂元，必有$r = 0$.
推出　　$a^l = (a^m)^q\in\langle a^m\rangle$

练习15

- 证明Fermat小定理：设 p为素数，则 $p|(n^p-n)$
- 证：考虑一个圆环上等距离穿有 p个珠子，用 n 种颜色对珠子着色. 考虑围绕中心旋转，则群是：

  $G=\{\sigma_1, \sigma_2, \cdots, \sigma_p\}$

  因为p是素数，所以除了恒等置换外，其他p-1个置换都由1个p阶轮换构成：

  $\sigma_1=(\bullet)(\bullet)\ldots(\bullet)$

  $\sigma_2=(\bullet\ \bullet\ \ldots\ \bullet)$ … $\sigma_p=(\bullet\ \bullet\ \ldots\ \bullet)$

练习15（续）

- 根据Polya定理，不同的着色方案数是

$$M=\frac{1}{p}[n^p+(p-1)n^1]=\frac{1}{p}(n^p-n+pn)$$

- 于是 $p|(n^p-n)$

练习16

- 设 p为素数，证明$\mathbf{Z}_p$是域.
- 证　p为素数，所以 $|\mathbf{Z}_p|\geq 2$.

  易见$\mathbf{Z}_p$可交换，单位元是1.

  对于任意的 $i, j\in\mathbf{Z}_p$, 设$i\neq 0$有

  $$i\otimes j=0\Rightarrow p\mid ij\Rightarrow p\mid j\Rightarrow j=0$$

  所以 $\mathbf{Z}_p$ 中无零因子，$\mathbf{Z}_p$为整环.

练习16（续）

下面证明每个非零元素都有逆元.

因为Z_p 是有限半群, 且Z_p关于$\otimes$适合消去律

任取 $i \in Z_p$，$i \neq 0$，令

$$i \otimes Z_p = \{ i \otimes j \mid j \in Z_p \}$$

则 $i \otimes Z_p = Z_p$,

否则$\exists\, j, k \in Z_p$，使得 $i \otimes j = i \otimes k$,

由消去律得 $j = k$.

由$1 \in Z_p$，存在 $j \in Z_p$，使得 $i \otimes j = 1$.

由于交换性可知 j 就是i 的逆元.

练习17

- 在整数环中定义$*$和$\diamond$两个运算, $\forall a,b\in Z$ 有

$$a*b = a+b-1,\ a\diamond b = a+b-ab.$$

证明<Z, $*$, $\diamond$>构成环

- 证　$\forall a,b\in Z$有$a*b$, $a\diamond b\in Z$, 两个运算封闭.
  任取$a,b,c\in Z$

$$(a*b)*c = (a+b-1)*c = (a+b-1)+c-1 = a+b+c-2$$

$$a*(b*c) = a*(b+c-1) = a+(b+c-1)-1 = a+b+c-2$$

练习17（续）

$(a \diamond b) \diamond c = (a+b-ab) \diamond c$

$= a+b+c-(ab+ac+bc)+abc$

$a \diamond (b \diamond c) = a \diamond (b+c-bc)$

$= a+b+c-(ab+ac+bc)+abc$

$*$与$\diamond$可结合.

$a*b = a+b-1 = b+a-1 = b*a$ 满足交换律

设单位元为e, $a*e = a+e-1=a$, $e=1$

设a的逆元为x , $a*x = a+x-1=1$, $x=2-a$

Z关于$*$构成交换群, 关于$\diamond$构成半群.

练习17（续）

◇关于* 满足分配律.

$$a◇(b*c) = a◇(b+c-1) = 2a+b+c-ab-ac-1$$

$$(a◇b)*(a◇c) = 2a+b+c-ab-ac-1$$

且

$$(b*c)◇a = (b+c-1)◇a = 2a+b+c-ab-ac-1$$

$$(b◇a)*(c◇a) = 2a+b+c-ab-ac-1$$

综上所述，$<Z, *, ◇>$构成环