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

10.3 循环群与置换群

□ 定义10.10 设G是群，若存在$a \in G$使得

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

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

- 回看旋转群$<G,*>$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

<0>={0}

<60>={0,60,120,180,240,300}

<120>={0,120,240}

<180>={0,180}

<240>={0,120,240}

<300>={0, 60,120,180,240,300}

$G=<Z_9,\oplus>$

$\oplus_9$	0	1	2	3	4	5	6	7	8
0	0	1	2	3	4	5	6	7	8
1	1	2	3	4	5	6	7	8	0
2	2	3	4	5	6	7	8	0	1
3	3	4	5	6	7	8	0	1	2
4	4	5	6	7	8	0	1	2	3
5	5	6	7	8	0	1	2	3	4
6	6	7	8	0	1	2	3	4	5
7	7	8	0	1	2	3	4	5	6
8	8	0	1	2	3	4	5	6	7

- 生成元：**1,2,4,5,7,8**

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$r,s\in Z$，使得

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

$$\begin{aligned} x*y &= a^r * a^s = a^{r+s} = a^{s+r} \\ &= a^s * a^r = y*x \end{aligned}$$

因此群$<G,*>$是阿贝尔群。

循环群一定是阿贝尔群，反之则不一定

- 例如: **Klein四元群 G={e,a,b,c} :**

*	*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}

- **<G,*>是一个阿贝尔群，但不是循环群。**

应用实例

- 证明：阶小于6 的群都是Abel群.

- 证：1 阶群是平凡的，显然是Abel群.
  - 2, 3和5都是素数，由推论2知素数阶群都是循环群，进而都是Abel群.
  - 设G是4阶群.

若G中含有4阶元，比如说a，则$G=\langle a\rangle$，

即G是循环群，故G是Abel群.

若G中不含4阶元，则G中只含1阶和2阶元，

群中元素的阶是群阶的因子

由命题可知G也是Abel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。

循环群的生成元

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

- **定理10.13** 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$\phi(n)$个生成元. 且a^r是G的生成元当且仅当 r是小于n且与 n 互素的自然数.

- 例如 $n=12$，小于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

证明：定理10.13 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}.

- (1) 先证 a^{-1}是G的生成元，即证$G=\langle a^{-1}\rangle$

  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$G \subseteq \langle a^{-1}\rangle$，从而$G=\langle a^{-1}\rangle$，故 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 $b = a^{-1}$

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

证明：定理10.13 设$G=\langle a\rangle$是循环群.

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

- (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互素.
  - 充分性　即证$G = \langle a^r\rangle$

显然有$\langle a^r\rangle \subseteq G$.

设r与n互素，且$r<n$，那么：

存在整数 u 和 v 使得　$ur + vn = 1$

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

对于 $\forall a^k \in G$，　a^k

$= (a^r)^{uk}$

$\in \langle a^r\rangle$

故 $G \subseteq \langle a^r\rangle$

从而 $G = \langle a^r\rangle$.

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

证明：定理10.13 设$G=\langle a\rangle$是循环群.

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

■ 必要性 即证r与n互素（ r与n的最大公约数为1）

设a^r是G的生成元（$r<n$ ），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，$|a^r|$是n/d的因子，即n整除n/d.

从而证明了$d = 1$,

即r与n互素。

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

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.

- 回看旋转群$< G, * >$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

<0>={0}

<60>={0,60,120,180,240,300}

<120>={0,120,240}

<180>={0,180}

<240>={0,120,240}

<300>={0, 60,120,180,240,300}

<0>={0} ={e}=H0

<60>={0,60,120,180,240,300} =G

<120>={0,120,240} =H2

<180>={0,180} = H1

证明：定理10.14 设$G=\langle a\rangle$是循环群.

(1) G的子群仍是循环群.

- (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，

  又$r<m$，则必有$r = 0$.

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

证明：定理10.14 设$G=\langle a\rangle$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.

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

(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.

- (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$H_1 = H$.

求循环子群的方法

- 1. 若$G=\langle a\rangle$是无限循环群，则$\langle a^m\rangle$是G的子群，其中m是自然数, 并且对于不同的自然数m和m', $\langle a^m\rangle$和$\langle a^{m'}\rangle$是不同的子群。
- 2. 若$\langle a\rangle$是 n 阶循环群，则先求出n的所有正因子，对于每一个正因子d, $\langle a^{n/d}\rangle$是G的唯一的d阶子群。

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}, ⊕>，求G_2的所有子群。

$\oplus_{12}$	0	1	2	3	4	5	6	7	8	9	10	11
0	0	1	2	3	4	5	6	7	8	9	10	11
1	1	2	3	4	5	6	7	8	9	10	11	0
2	2	3	4	5	6	7	8	9	10	11	0	1
3	3	4	5	6	7	8	9	10	11	0	1	2
4	4	5	6	7	8	9	10	11	0	1	2	3
5	5	6	7	8	9	10	11	0	1	2	3	4
6	6	7	8	9	10	11	0	1	2	3	4	5
7	7	8	9	10	11	0	1	2	3	4	5	6
8	8	9	10	11	0	1	2	3	4	5	6	7
9	9	10	11	0	1	2	3	4	5	6	7	8
10	10	11	0	1	2	3	4	5	6	7	8	9
11	11	0	1	2	3	4	5	6	7	8	9	10

小于12且与12互素的正整数有4个：1,5,7,11

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

  生成元是1,5,7,11，取$a=1$

12正因子是1,2,3,4,6和12，则G_2的子群:

当d=1时, $<a^{n/d}> =<1^{12/1}>=<12>=<0>=\{0\}$是 1阶子群

当d=2时, $<a^{n/d}> =<1^{12/2}>=<6>=\{0,6\}$是2阶子群

当d=3时, $<a^{n/d}> =<1^{12/3}>=<4>=\{0,4,8\}$是3阶子群

当d=4时, $<a^{n/d}> =<1^{12/4}>=<3>=\{0,3,6,9\}$是4阶子群

当d=6时, $<a^{n/d}> =<1^{12/6}>=<2>=\{0,2,4,6,8,10\}$是6阶子群

当d=12时, $<a^{n/d}> =<1^{12/12}>=<1>=Z_{12}$是12阶子群

回看旋转群<G,*>，求其所有子群

*	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

解：

$G=\langle 60\rangle$是6阶循环群

小于6且与6互素的正整数有2个： 1,5，所以$\phi(6)=2$

有2个生成元：60和300.

6的正因子是1,2,3,6，则G的子群（取a=60）：

当d=1时, $\langle a^{n/d}\rangle=\langle 60^{6/1}\rangle=\langle 0\rangle=\{0\}$是 1阶子群

当d=2时, $\langle a^{n/d}\rangle=\langle 60^{6/2}\rangle=\langle 180\rangle=\{0,180\}$是2阶子群

当d=3时, $\langle a^{n/d}\rangle=\langle 60^{6/3}\rangle=\langle 120\rangle=\{0,120,240\}$是3阶子群

当d=6时, $\langle a^{n/d}\rangle=\langle 60^{6/6}\rangle=\langle 60\rangle=G$是6阶子群

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

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

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

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：任意置换都可以唯一地表示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，$\sigma$可以进一步表示成对换之积，即$(i_1\ i_2\ \ldots\ i_k)=(i_1\ i_2)\ (i_1\ i_3)\ \ldots\ (i_1\ i_k)$

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

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

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.

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

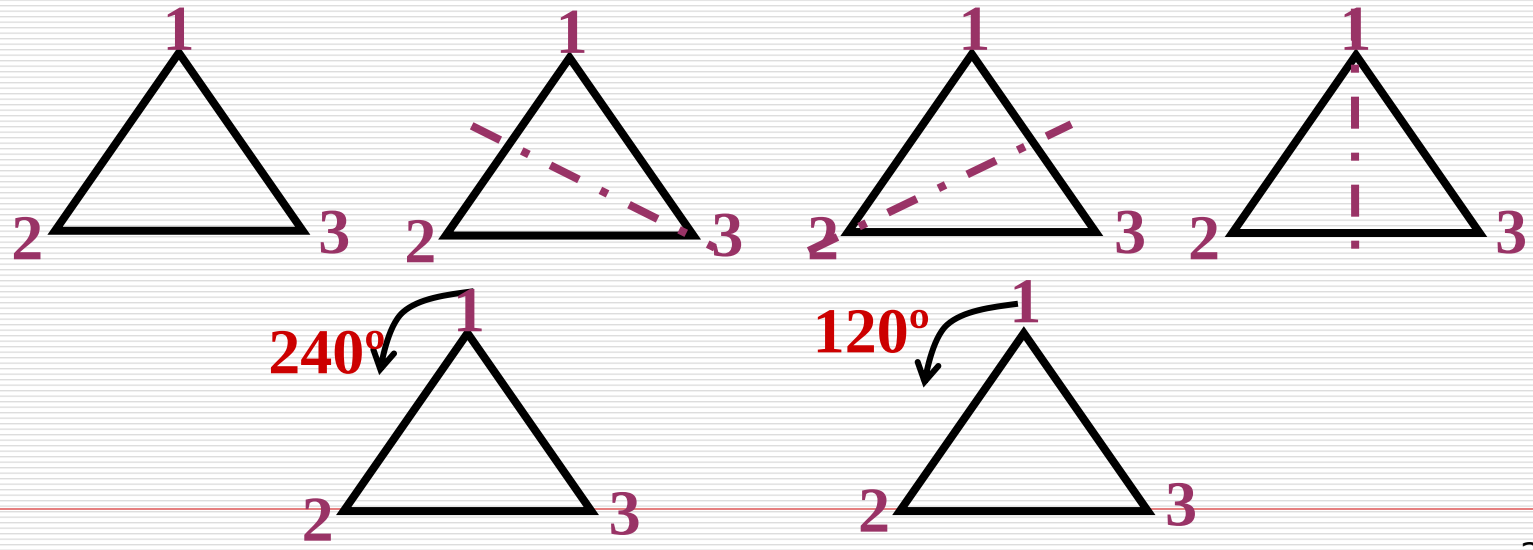
$\sigma=(1\ 2)(1\ 3)$

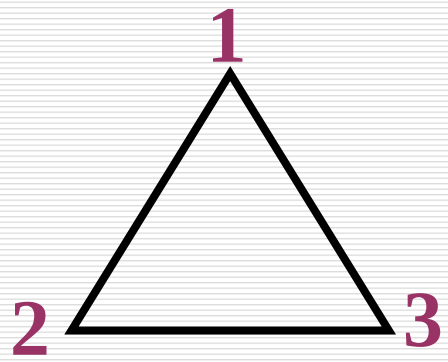
$\sigma=(1\ 4)(2\ 4)(3\ 4)(1\ 4)$

- 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.

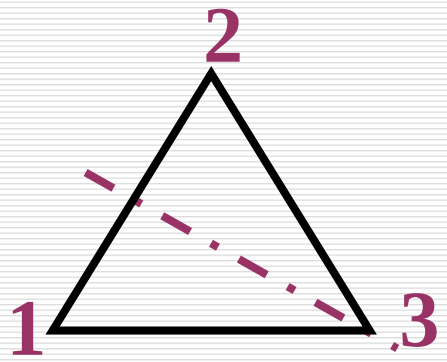
n元对称群

- 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
  $S_3=\{ (1), (1\ 2), (1\ 3), (2\ 3), (1\ 2\ 3), (1\ 3\ 2) \}$

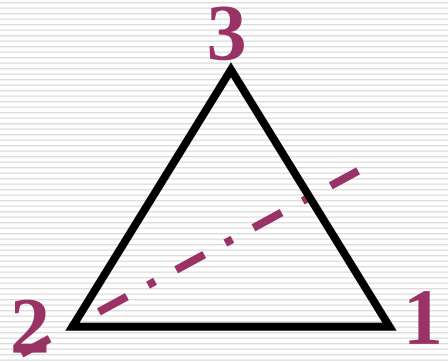




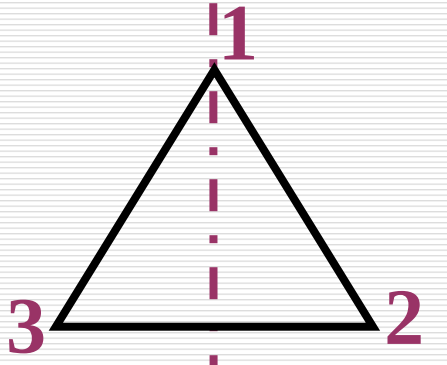
f_1={<1,1>,<2,2>,<3,3>} (1)



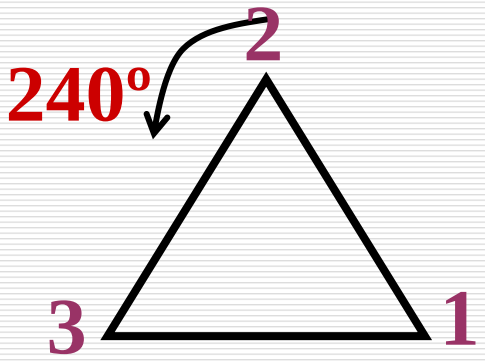
f_2={<1,2>,<2,1>,<3,3>} (1 2)



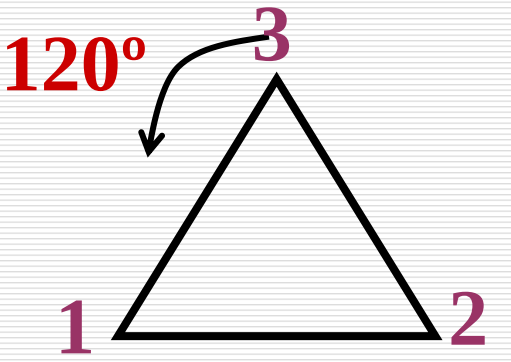
f_3={<1,3>,<2,2>,<3,1>} (1 3)



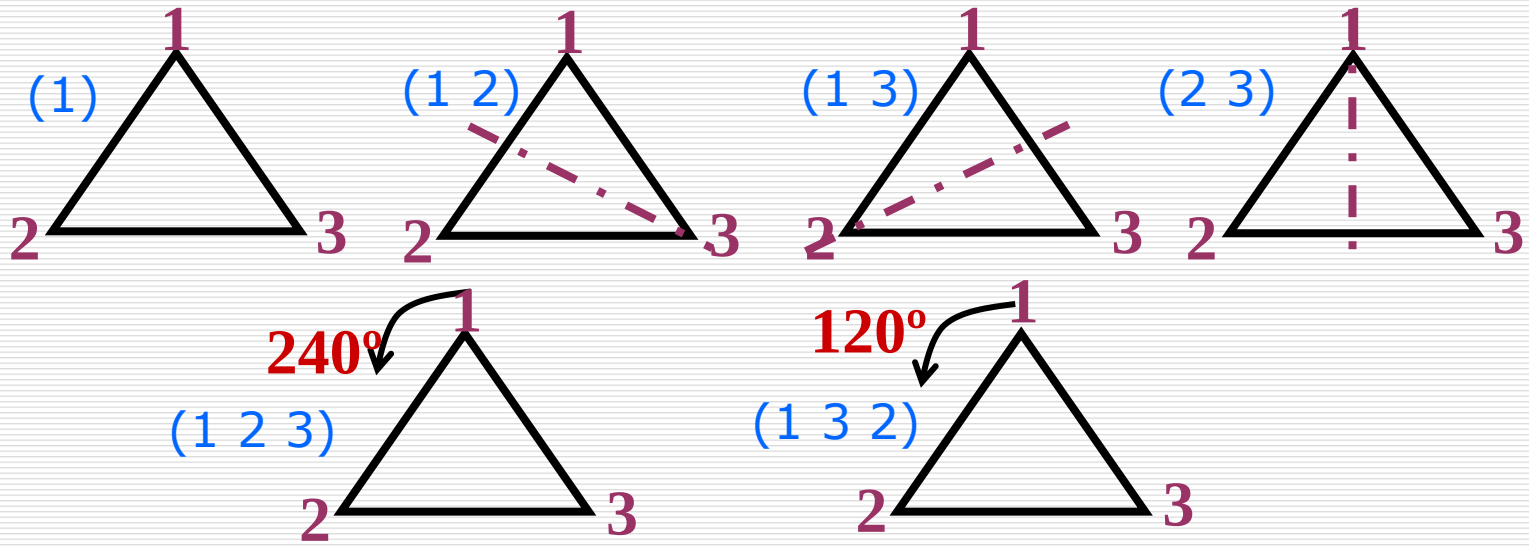
f_4={<1,1>,<2,3>,<3,2>} (2 3)



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.

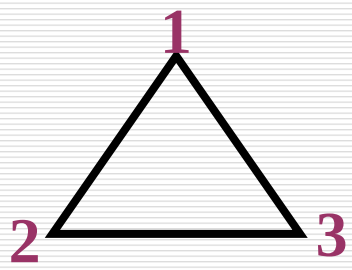
- 证 恒等置换(1) 是偶置换，所以A_n非空.

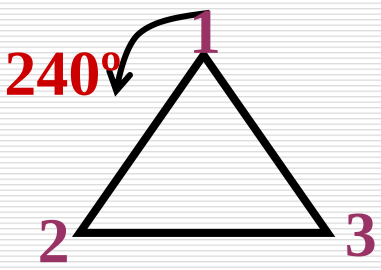
  根据判定定理三，只需证明封闭性：

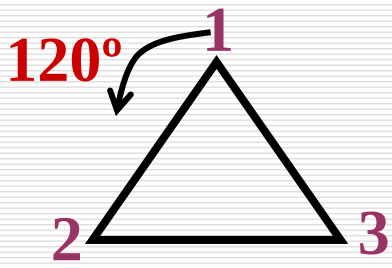
  - 任取$\sigma,\tau \in A_n$， σ, τ 都可以表成偶数个对换之积，那么$\sigma\tau$也可以表成偶数个对换之积，所以$\sigma\tau \in A_n$.

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)}

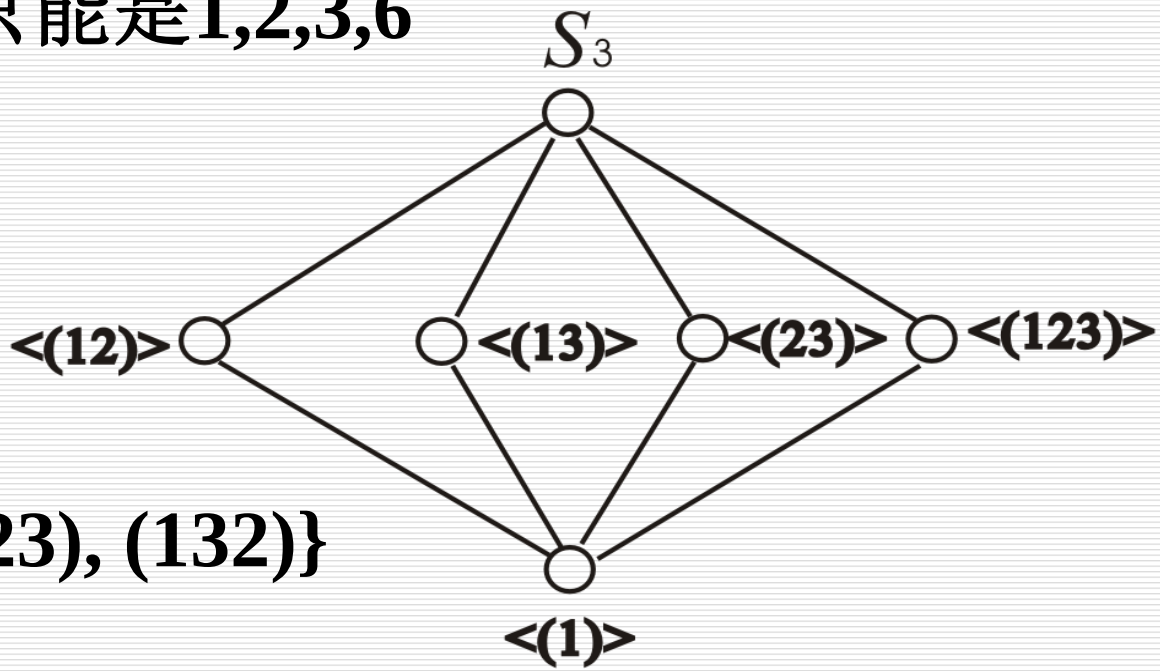
2阶：{(1), (12)}

{(1), (13)}

{(1), (23)}

3阶：A_3 ={(1), (123), (132)}

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

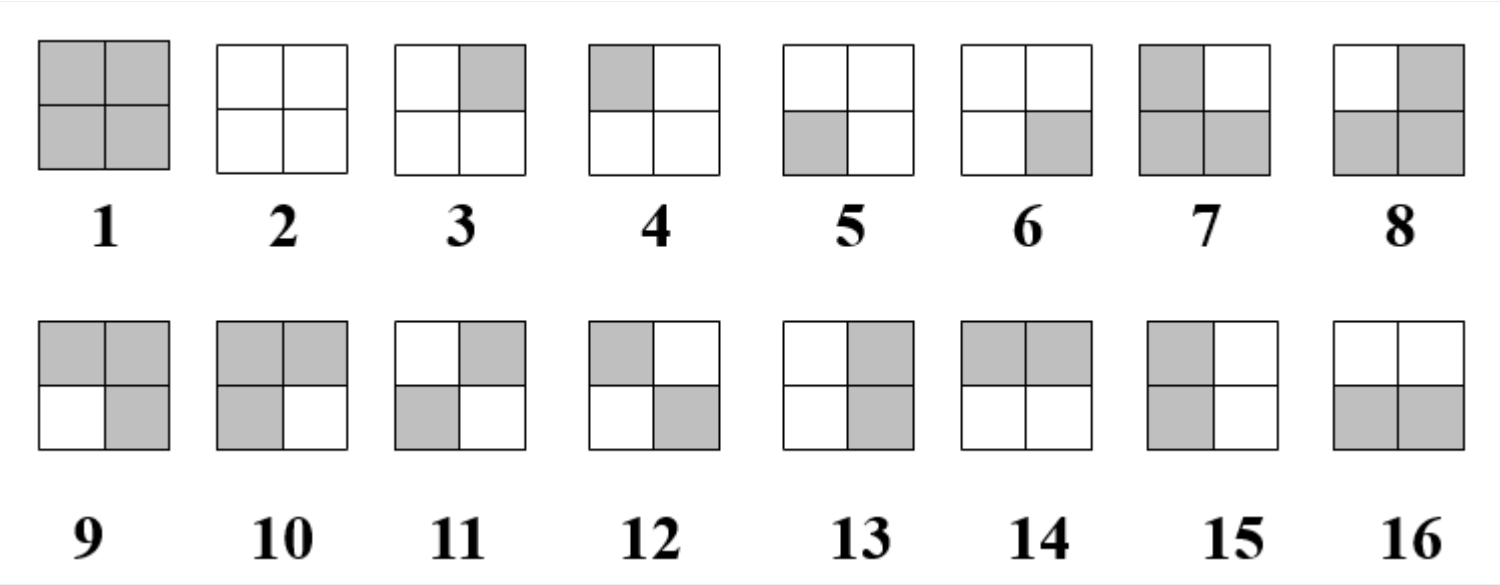
$$M=\frac{1}{|G|}\sum_{k=1}^{g}m^{c(\sigma_k)}$$

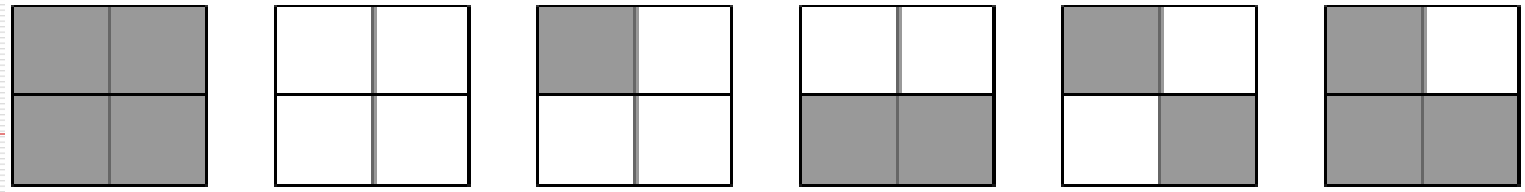
其中$c(\sigma_k)$是置换σ_k的轮换表示中（包含1阶轮换在内）的轮换个数.

- 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.





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.

1	2
4	3

解：群G中的所有置换是（每次顺时针转90°）

1	2
4	3

$\sigma_1=(1)$

4	1
3	2

$\sigma_2=(1432)$

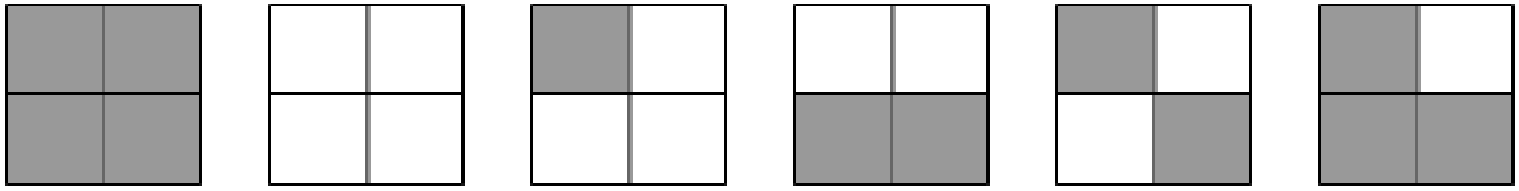
3	4
2	1

$\sigma_3=(13)(24)$

2	3
1	4

$\sigma_4=(1234)$

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



用 2 种颜色涂色 3×3 的方格棋盘，每个方格一种颜色. 如果允许棋盘任意旋转或者翻转，则不同的着色方案数是_____.

答案：群 G 的置换结构为：恒等置换：1 个

绕中心转 90、270 度：（****）（****）（*）2 个

绕中心转 180 度：（**）（**）（**）（**）（*）1 个

翻转 180 度：（**）（**）（**）（*）（*）（*）4 个

带入 Polya 定理： $M=(2^9+2*2^3+2^5+4*2^6)/8=102$

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

其中$c(\sigma_k)$是置换σ_k的轮换表示中包含1阶轮换在内的轮换个数.

答案：群 G 的置换结构为：恒等置换：1 个

绕中心转 90、270 度：（****）（****）（*）2 个

绕中心转 180 度：（**）（**）（**）（**）（*）1 个

翻转 180 度：（**）（**）（**）（*）（*）（*）4 个

带入 Polya 定理： $M=(2^9+2*2^3+2^5+4*2^6)/8=102$

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

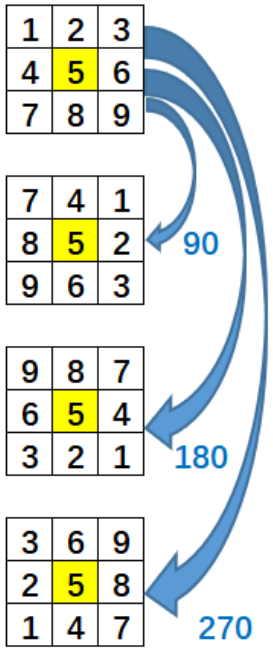
其中$c(\sigma_k)$是置换σ_k的轮换表示中包含1阶轮换在内的轮换个数.

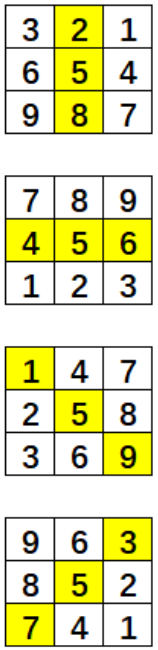
$$\sigma=\begin{pmatrix}1&2&3&4&5&6&7&8&9\\1&2&3&4&5&6&7&8&9\end{pmatrix}=(1)(2)(3)(4)(5)(6)(7)(8)(9)$$

$$\sigma=\begin{pmatrix}1&2&3&4&5&6&7&8&9\\7&4&1&8&5&2&9&6&3\end{pmatrix}=(1793)(2486)(5)$$

$$\sigma=\begin{pmatrix}1&2&3&4&5&6&7&8&9\\9&8&7&6&5&4&3&2&1\end{pmatrix}=(19)(28)(37)(46)(5)$$

$$\sigma=\begin{pmatrix}1&2&3&4&5&6&7&8&9\\3&6&9&2&5&8&1&4&7\end{pmatrix}=(1397)(2684)(5)$$





$$\sigma=\begin{pmatrix}1&2&3&4&5&6&7&8&9\\3&2&1&6&5&4&9&8&7\end{pmatrix}=(13)(46)(79)(2)(5)(8)$$

$$\sigma=\begin{pmatrix}1&2&3&4&5&6&7&8&9\\7&8&9&4&5&6&1&2&3\end{pmatrix}=(17)(28)(39)(4)(5)(6)$$

$$\sigma=\begin{pmatrix}1&2&3&4&5&6&7&8&9\\1&4&7&2&5&8&3&6&9\end{pmatrix}=(24)(37)(68)(1)(5)(9)$$

$$\sigma=\begin{pmatrix}1&2&3&4&5&6&7&8&9\\9&6&3&8&5&2&7&4&1\end{pmatrix}=(19)(26)(48)(3)(5)(7)$$

恒等置换：1个

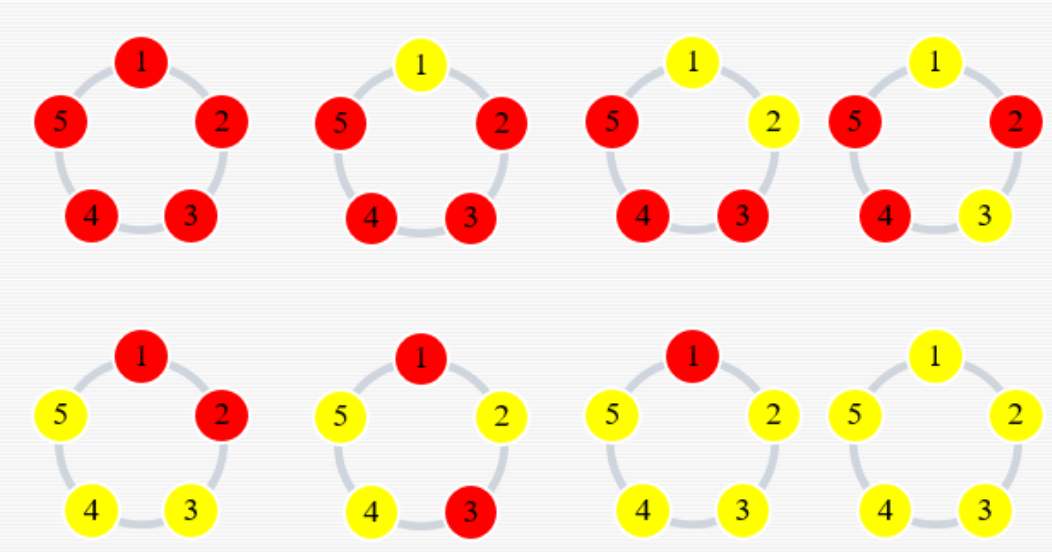
绕中心转90、270度：（****）（****）（*）2个

绕中心转180度：（**）（**）（**）（**）（*）1个

翻转180度：（**）（**）（**）（*）（*）（*）4个

带入Polya定理： $M=(2^9+2*2^3+2^5+4*2^6)/8=102$

例：考察从红、黄两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：

$$M = \frac{1}{5}(2^5 + 2^1 + 2^1 + 2^1 + 2^1) = 8$$

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

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

S_4相关（补充）

- 设 S = {1, 2, 3, 4}，4元对称群　　$|S_4|=4!$

S_4={ (1), (12),(13),(14),(23),(24),(34),
(123),(124),(132),(134),(142),(143),(234),(243),
(12)(34),(14)(23),(13)(24),
(1234),(1243),(1324),(1342),(1423),(1432)}

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.　　$|A_4|=4!/2=12$

A_4={(1),(123),(124),(132),(134),(142),(143),(234),(243),
(12)(34),(14)(23),(13)(24) }

S_4相关（补充）

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

$$\frac{1}{8}\left(2^4 + 2*2^3 + 3*2^2 + 2*2^1\right) = 6$$

8阶置换群:{ (1), (1234), (13)(24), (1432), (12)(34), (14)(23),(2 4) ,(1,3)}　包括旋转和翻转

o	(1)	(1234)	(13)(24)	(1432)	(12)(34)	(14)(23)	(24)	(13)
(1)	(1)	(1234)	(13)(24)	(1432)	(12)(34)	(14)(23)	(24)	(13)
(1234)	(1234)	(13)(24)	(1432)	(1)	(24)	(13)	(14)(23)	(12)(34)
(13)(24)	(13)(24)	(1432)	(1)	(1234)	(14)(23)	(12)(34)	(13)	(24)
1432	(1432)	(1)	(1234)	(13)(24)	(13)	(24)	(12)(34)	(14)(23)
(12)(34)	(12)(34)	(13)	(14)(23)	(24)	(1)	(13)(24)	(1432)	(1234)
(14)(23)	(14)(23)	(24)	(12)(34)	(13)	(13)(24)	(1)	(1234)	(1432)
(24)	(24)	(12)(34)	(13)	(14)(23)	(1234)	(1432)	(1)	(13)(24)
(13)	(13)	(14)(23)	(24)	(12)(34)	(1432)	(1234)	(13)(24)	(1)

4阶置换群:{ (1), (1234), (13)(24), (1432)}　只是旋转

o	(1)	(1234)	(13)(24)	(1432)
(1)	(1)	(1234)	(13)(24)	(1432)
(1234)	(1234)	(13)(24)	(1432)	(1)
(13)(24)	(13)(24)	(1432)	(1)	(1234)
1432	(1432)	(1)	(1234)	(13)(24)

$$M = \frac{1}{4}\left(2^4 + 2^1 + 2^2 + 2^1\right) = 6$$

10.3循环群与置换群（回顾）

- 10.3循环群与置换群
  - 循环群
    - $G=\langle a\rangle$ — a 为G 的生成元
    - 任何一个循环群必定是阿贝尔群,反之不一定 — 应用：阶小于6 的群都是Abel群
    - 无限循环群 — 只有两个生成元
    - n 阶循环群 — 有$\phi(n)$个生成元 — a^r是G的生成元当且仅当 r是小于n且与 n 互素的自然数
    - 循环群的子群
      - (1) 循环群的子群仍是循环群.
      - (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.
    - 求循环子群的方法
      - 1. 若$G=\langle a\rangle$是无限循环群，则$\langle a^m\rangle$是G的子群，其中m是自然数, 并且对于不同的自然数m和m', $\langle a^m\rangle$和$\langle a^{m'}\rangle$是不同的子群。
      - 2. 若$\langle a\rangle$是 n 阶循环群，则先求出n的所有正因子，对于每一个正因子d, $\langle a^{n/d}\rangle$是G的唯一的d阶子群。
  - 置换群
    - n元置换 — 轮换与对换
    - n元置换的轮换表示 — 置换的对换分解
    - n元对称群 — n元置换群 — n元交错群
    - Polya定理 — $M=\frac{1}{|G|}\sum_{k=1}^{g} m^{c(\sigma_k)}$

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

10.4 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（可结合性）

  (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，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$\mathbf{Z}$，有理数环$\mathbf{Q}$，实数环$\mathbf{R}$ 和复数环$\mathbf{C}$.
- (2)设$\mathbf{Z}_n=\{0,1,\ldots,n-1\}$，$\oplus$和$\otimes$分别表示模$n$的加法和乘法，则$<\mathbf{Z}_n,\oplus,\otimes>$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$<R,+,\bullet>$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

□ (1) $\forall a \in R$，$a0 = 0a = 0$

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

$\forall a,b \in R$，有

$(-a)b+ab = (-a+a)b = 0b = 0$

$ab+(-a)b = (a+(-a))b = 0b = 0$

$?+ab = 0$
$ab+? = 0$

故：$(-a)b$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 $\forall a_1, a_2, \ldots, a_n$ 有

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

同理可证, $\forall b_1, b_2, \ldots, b_m$ 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$<R,+,\bullet>$是环

(1) 若环中乘法 $\bullet$ 适合交换律，则称R是交换环

(2) 若环中乘法 $\bullet$ 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　//没有零因子

(4) 若R既是交换环、含幺环、也是无零因子环，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.

域的定义（补充）

- 定义10.15$^+$ 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-{0}, ●>构成交换群

  (3) ● 运算关于+运算适合分配律

  则称<R,+,●>是一个域

- 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（可结合性）

  (3) ●运算关于+运算适合分配律

  则称<R,+,●>是一个环.

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

⊗	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

实例

- 设$R=Z\times Z$，定义R上的加法+运算和乘法•运算如下：

  对于任意：$\langle x_1,y_1\rangle\in R$，$\langle x_2,y_2\rangle\in R$，

  $$\langle x_1,y_1\rangle + \langle x_2,y_2\rangle = \langle x_1+x_2, y_1+y_2\rangle$$

  $$\langle x_1,y_1\rangle \bullet \langle x_2,y_2\rangle = \langle x_1\bullet x_2, y_1\bullet y_2\rangle$$

  证明：$\langle R, +, \bullet\rangle$是环，并求出该环的所有零因子.

- 证 (一).【$\langle R, +, \bullet\rangle$是环】

  (1) 根据已知条件知，运算+是R上的封闭运算且满足交换律和结合律，其加法单位元是$\langle 0,0\rangle$,任意$\langle x,y\rangle\in R$关于+的逆元为$\langle -x, -y\rangle$，因此, $\langle R, +\rangle$ 是交换群.

  (2) 由于•运算是R上的封闭运算且满足结合律，于是$\langle R, +\rangle$是半群.

  (3) 对于任意$\langle x_1,y_1\rangle\in R$，$\langle x_2,y_2\rangle\in R$，$\langle x_3,y_3\rangle\in R$，有：

  $$\langle x_1,y_1\rangle \bullet (\langle x_2,y_2\rangle + \langle x_3,y_3\rangle) = \langle x_1,y_1\rangle \bullet \langle x_2,y_2\rangle + \langle x_1,y_1\rangle \bullet \langle x_3,y_3\rangle$$

  即•运算对+运算可分配.

  综上所述，$\langle R, +, \bullet\rangle$是环.

  (二).【求出该环的所有零因子】

  对于任意$\langle x,0\rangle\in R(x\neq 0)$及$\langle 0, y\rangle\in R(y\neq 0)$，由于$\langle x,0\rangle \bullet \langle 0, y\rangle=\langle 0,0\rangle$，所以任意$\langle x,0\rangle\in R(x\neq 0)$和$\langle 0, y\rangle\in R(y\neq 0)$是环$\langle R, +, \bullet\rangle$的所有零因子.

定理（补充）

- 在环<A,+,●>中无零因子 当且仅当 乘法满足消去律（即对于 c≠0 和 ca=cb, 必有a=b）
- 证明：

必要性：若无零因子并设 c≠0 和 ca=cb，

则有：ca-cb=c(a-b)＝0

所以，必有a=b，即乘法满足消去律。

充分性：若乘法满足消去律，

设a≠0，ab=0则ab=a0

消去a即得b=0，即无零因子。

实例

- 设 p为素数，证明Z_p是域.

【证明思路：

先证Z_p为整环，再证每个非零元素都有逆元】

- 证 【先证Z_p为整环】

p为素数，所以 $|Z_p|\geq 2$.

易见Z_p关于乘法可交换，单位元是1.

对于任意的 $i, j \in Z_p$, 设$i \neq 0$有

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

所以 Z_p 中无零因子，Z_p为整环.

⊗	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

实例（续）

【再证每个非零元素都有逆元】

已知：Z_p 是有限半群, 且Z_p关于⊗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，$\exists j, k \in Z_p\ (j \neq k)$，使得 $i \otimes j = i \otimes k$,

而由消去律得 $j = k$, 这是矛盾的。

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

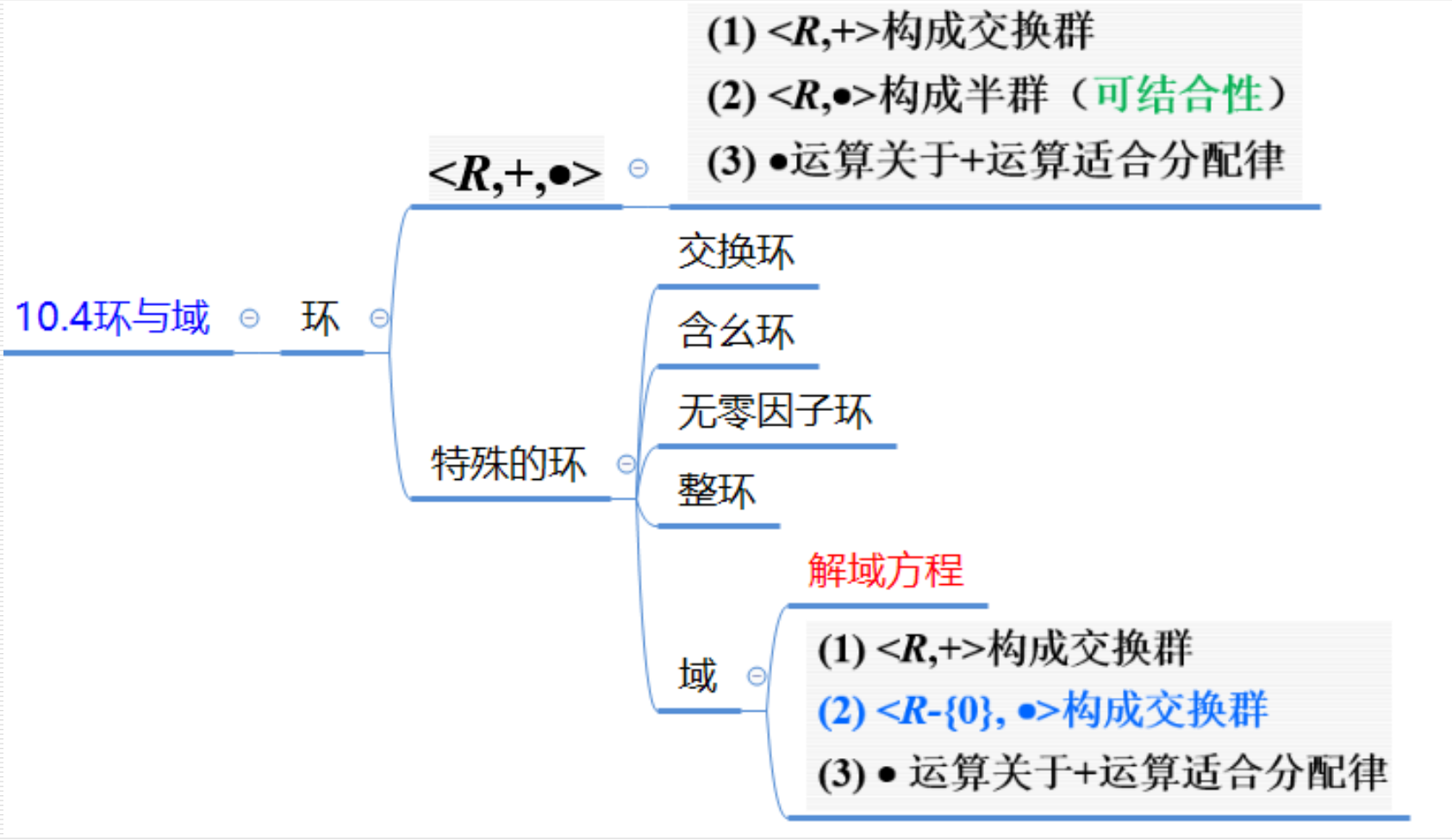
由于交换性可知 j 就是i 的逆元.

解域方程

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

⊗	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

10.4环与域（回顾）


10.4环与域
环
<R,+,•>
(1) <R,+>构成交换群
(2) <R,•>构成半群（可结合性）
(3) •运算关于+运算适合分配律
特殊的环
交换环
含幺环
无零因子环
整环
域
解域方程
(1) <R,+>构成交换群
(2) <R-{0}, •>构成交换群
(3) • 运算关于+运算适合分配律

第十章　群与环（回顾）

- 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