17.3 循环群

- 循环群的定义
- 循环群的分类
- 生成元
- 子群
- 循环群的实例

循环群的定义及其分类

定义　设G是一个群，若存在$a \in G$使得

$G=<a>=\{a^k \mid k \in Z\}$, 则称$G$为循环群，$a$为$G$的生成元.

分类:

生成元的阶无限，则G为无限循环群

生成元a为n阶元，则$G=\{e, a, a^2, \ldots, a^{n-1}\}$为

n阶循环群

实例　$<Z, +>$为无限循环群

$<Z_n, \oplus>$为n阶循环群

循环群的生成元

定理1 $G=\langle a\rangle$是循环群

(1) 若G是无限循环群，则G的生成元是a和a^{-1};

(2) 若G是n阶循环群，则G有$\phi(n)$个生成元，

当$n=1$时$G=\langle e\rangle$的生成元为e;

当$n>1$时, $\forall r(r\in Z^{+}\wedge r<n)$, a^r是G的生成元$\Leftrightarrow(n,r)=1$.

若$n=p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k}$，则
$\phi(n)=n(1-\frac{1}{p_1})(1-\frac{1}{p_2})\cdots(1-\frac{1}{p_k})$

证明思路:

(1) 证明a^{-1}是生成元;
证明若存在生成元b，则$b=a$或a^{-1}.

(2) 只需证明若$(n,r)=1$，则a^r是生成元
反之，若a^r是生成元，则$(n,r)=1$.

证明

(1) 若G是无限循环群，则G的生成元是a和a^{-1}
(2) 若G是n阶循环群，则G有$\phi(n)$个生成元: $n=1$时$G=\langle e\rangle$的生成元为e； 当$n>1$时,$\forall r(r\in Z^+\wedge r<n)$, a^r是G的生成元$\Leftrightarrow(n,r)=1$

证 (1) a是生成元，$\langle a^{-1}\rangle\subseteq G$,

任取 $a^l\in G$, $a^l=(a^{-1})^{-l}\in\langle a^{-1}\rangle \Rightarrow G\subseteq\langle a^{-1}\rangle$

假设 b为生成元，$b=a^j$, $a=b^t$,

$a=b^t=(a^j)^t=a^{jt}\Rightarrow a^{jt-1}=e$. 若$jt-1\neq0$与$a$为无限阶元矛盾,

因此 $j=t=1$或 $j=t=-1$

(2) $n=1$结论为真. 下面考虑$n>1$

$(n, r)=1 \Leftrightarrow \exists u,v\in Z$ s.t. $un+rv=1\Rightarrow a=a^{un+rv}=(a^r)^v$

$\Rightarrow a^r$为生成元

反之，若a^r为生成元，则$|a^r|=n$. 另一方面，由$|a|=n$知，$|a^r|=\frac{n}{(n,r)}$，故$(n,r)=1$.

循环群的子群

定理2 $G=\langle a\rangle$是循环群，那么

(1) G的子群也是循环群.

(2) 若G是无限阶，则G的子群除$\{e\}$外也是无限阶.

(3) 若G是n阶的，则G的子群的阶是n的因子.

(4) 对于n的每个正因子d, 在G中有且仅有一个d阶子群.

证明思路:

(1) 子群H中最小正方幂元a^m为H的生成元

(2) 若子群$H=\langle a^m\rangle$有限，$a\neq e$, 则推出 $|a|$ 有限.

(3) $H=\langle a^m\rangle$, $|H|=|a^m|$, $(a^m)^n=e$. 从而 $|a^m|$ 是n的因子.

(4) $\langle a^{n/d}\rangle$是d阶子群，然后证明唯一性.

证明 (1) G的子群是循环群 (2) 若G无限阶，则G的子群除$\{e\}$外也是无限阶

证 (1) 设H是$G=\langle a \rangle$的子群，不妨设$H\neq\{e\}$.

取H中最小正方幂元a^m, $\langle a^m \rangle \subseteq H$.

对于任意整数i, $i = lm+r$, $r\in\{0, 1, \ldots , m-1\}$

$$a^i \in H \Rightarrow a^r=a^i(a^m)^{-l}\in H \Rightarrow r=0 \Rightarrow a^i\in \langle a^m \rangle$$

$$H\subseteq \langle a^m \rangle$$

(2) 设H为G的子群，若$H\neq\{e\}$, 必有$H=\langle a^m \rangle$, a^m为H中最小正方幂元.

假设$|H|=t$, 则$(a^m)^t=e \Rightarrow a^{mt}=e$，与$a$为无限阶元矛盾.

证明(续)

(3) 若G是n阶的，则G的子群的阶是n的因子;
(4) 对于n的每个正因子d, 在G中有且仅有一个d阶子群.

(3) 设$G=\{e, a, \ldots, a^{n-1}\}$，$H=\{e\}$命题显然成立.

若$H\neq\{e\}$, 必有$H=<a^m>$, a^m为H中最小正方幂元.

设 $|H|=|a^m|=d$,

$(a^m)^n=(a^n)^m=e \Rightarrow |a^m|\,|n \Rightarrow d|n$.

(4) 设$d|n$，则$H=<a^{\frac{n}{d}}>$是G的d阶子群.

若$H'=\langle a^m\rangle$也是G的d阶子群，其中a^m为最小正方幂元.

则

$$a^{md}=e \Rightarrow n|md \Rightarrow \frac{n}{d}|m \Rightarrow m=\frac{n}{d}t \Rightarrow a^m=\left(a^{\frac{n}{d}}\right)^t \in H$$

$H' \subseteq H, |H'|=|H|=d \Rightarrow H'=H$

实例

例1 (1) $\langle Z_{12}, \oplus \rangle$, 求生成元、子群.

生成元为与12 互素的数：1, 5, 7, 11

12 的正因子为 1, 2, 3, 4, 6, 12,

子群：$\langle 0\rangle, \langle 1\rangle, \langle 2\rangle, \langle 3\rangle, \langle 4\rangle, \langle 6\rangle$

(2) $G=\langle a^2\rangle$为12阶群，求生成元和子群.

生成元为$a^2, a^{10}, a^{14}, a^{22}$

G的子群：$\langle e\rangle, \langle a^2\rangle, \langle a^4\rangle, \langle a^6\rangle, \langle a^8\rangle, \langle a^{12}\rangle$

(3) $\langle a\rangle$为无限循环群，求生成元和子群.

生成元为a, a^{-1}；子群为$\langle a^i\rangle$，$i = 0, 1, 2, \ldots$；

(4) $G=\langle Z,+\rangle$，求生成元和子群.

生成元：1, –1；子群 nZ, $n = 0, 1, \ldots$,

17.4 变换群与置换群

- 变换群
  - 变换群的定义
  - 变换群的实例
- n元置换群
  - 置换的表示
  - 置换的乘法和求逆运算
  - 置换群中元素的阶与子群
  - 置换群的实例

变换群

变换群的定义

A上的变换：　　$f: A \to A$

A上的一一变换：　双射$f: A \to A$

A上的一一变换群：$E(A)=\{ f \mid f: A \to A$为双射$\}$

关于变换乘法构成群

A上的变换群G：　$G \le E(A)$

实例

G为群，$a \in G$，令$f_a: G \to G, f_a(x)=ax$，则f_a为一一变换.

$H=\{ f_a \mid a \in G \}$关于变换乘法构成G上的变换群.

$H \le E(G)$

变换群的实例

例如 $G=\{e, a, b, c\}$，

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

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

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

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

$$H=\{f_e, f_a, f_b, f_c\}$$

思考：怎样证明H同构于G？

与独异点的表示定理进行比较

n元置换群

- 当$|A|$有限时，A上的一一变换称为A上的置换。当$|A| = n$时称A上置换为n元置换。

  置换的表示：令$A = \{1, 2, \dots, n\}$,

$$\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix}$$

- 若σ将A中的k个元素$i_1, i_2, \dots, i_k$进行如下变换：

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

并且保持其它元素不变，则可将σ记为$(i_1 i_2 \cdots i_k)$，称为一个k阶轮换。当k=2时，称为一个对换。

n元置换群

- 设$\boldsymbol{\sigma} = (\boldsymbol{i_1 i_2 \cdots i_k})$和$\boldsymbol{\tau} = (\boldsymbol{j_1 j_2 \cdots j_l})$是两个轮换，若$\{\boldsymbol{i_1, i_2, \cdots, i_k}\} \cap \{\boldsymbol{j_1, j_2, \cdots, j_l}\} = \emptyset$，则称$\boldsymbol{\sigma}$和$\boldsymbol{\tau}$是不相交的。
- 定理：若$\boldsymbol{\sigma}$和$\boldsymbol{\tau}$是两个不相交的n元置换，则$\boldsymbol{\sigma\tau} = \boldsymbol{\tau\sigma}$.

不交轮换的分解式：

$\sigma = \tau_1\tau_2\cdots\tau_t$, 其中 $\tau_1,\tau_2, \ldots,\tau_t$为不交轮换

对换分解式：

对换 $(i\ j) = (j\ i)$

$(i_1 i_2 \cdots i_k) = (i_1\ i_k)\ (i_1\ i_{k-1})\cdots\ (i_1\ i_2)$

n元置换的轮换表示

定理1 任何n元置换都可以表成不交的轮换之积，并且表法是唯一的. 即：

$$\sigma=\sigma_1\sigma_2\cdots\sigma_t,\ \sigma=\tau_1\tau_2\cdots\tau_l \Rightarrow \{\sigma_1, \sigma_2,\ldots, \sigma_t\}=\{\tau_1, \tau_2,\ldots, \tau_l\}$$

证明思路

(1) σ可以表成不交的轮换之积. 归纳证明.

(2) 唯一性. 假设

$$\sigma=\sigma_1\sigma_2\cdots\sigma_t,\quad \sigma=\tau_1\tau_2\cdots\tau_l.$$

令$X=\{\sigma_{1,} \sigma_{2,}\ldots, \sigma_t\}$, $Y=\{\tau_{1,} \tau_{2,}\ldots, \tau_l\}$

任取$\sigma_j \in X$, $\sigma_j=(i_1i_2\cdots i_m)$, $m>1$, 证明$\exists\tau_s\in Y$使得$\sigma_j=\tau_s$，

从而$X\subseteq Y$. 同理$Y\subseteq X$.

n元置换的轮换指数

轮换指数： $1^{C_1(\sigma)}2^{C_2(\sigma)}\cdots n^{C_n(\sigma)}$， $C_k(\sigma)$: k-轮换的个数

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

指数为 $1^3 2^1 3^1 4^0 5^0 6^0 7^0 8^0 = 1^3 2^1 3^1$

不同指数的个数是如下方程的非负整数解的个数

$$x_1 + 2x_2 + \ldots + nx_n = n$$

例如：

A={1, 2, 3}上的置换

σ_1=(1), σ_2=(1 2), σ_3=(1 3), σ_4=(2 3), σ_5=(1 2 3), σ_6=(1 3 2)

轮换指数为1^3：σ_1； $1^1 2^1$：$\sigma_2, \sigma_3, \sigma_4$； 3^1：σ_5, σ_6

n元置换的对换表示

任意轮换都可以表成对换之积

对换可以有交

表法不唯一，但是对换个数的奇偶性不变

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 5 & 2 & 3 & 8 & 7 & 6 & 1 & 4 \end{pmatrix} = (1\ 5\ 7)(4\ 8) = (17)(15)(48)$$

$$= (57)(17)(48)$$

奇置换、偶置换

奇置换：表成奇数个对换之积

偶置换：表成偶数个对换之积(恒等置换是偶置换)

奇置换与偶置换之间存在一一对应，因此各有$n!/2$个

置换的乘法与求逆

置换的乘法：函数的合成

例：8元置换σ=(132)(5648)，τ=(18246573), 则

$$\sigma\tau=(15728)(3)(4)(6)=(15728)$$

置换求逆：求反函数

$$\sigma=(132)(5648)，\sigma^{-1}=(8465)(231),$$

令S_n为{1, 2,…, n}上所有n元置换的集合.

S_n关于置换乘法构成群，称为n元对称群.

S_n的子群称为n元置换群.

例: 3元对称群S_3={(1), (12), (13), (23), (123), (132)}

3元交代群(交错群) A_3={(1), (123), (132)}

置换群中元素的阶与子群

元素的阶

k 阶轮换 $(i_1\ i_2 \cdots i_k)$ 的阶为k

若$\sigma=\tau_1\tau_2\cdots\tau_l$是不交轮换的分解式，则$|\sigma|=[|\tau_1|, |\tau_2|,\ldots, |\tau_l|]$

子群

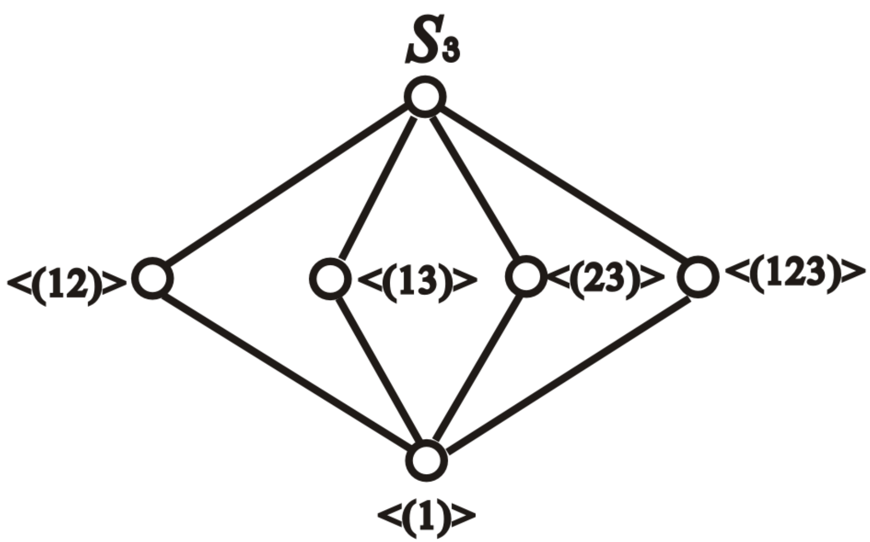
{(1)}，S_n，n元交代群A_n

例如S_3，子群6个

<(1)>, S_3,

<(12)>, <(13)>,

<(23)>, A_3=<(123)>



置换群的实例

Cayley定理 每个群G都与一个变换群同构.

推论 每个有限群都与一个置换群同构.

D_4，4×4的方格图形，在空间旋转、翻转.

二面体群(dihedral group)

4	3
1	2

$$D_4=\{(1),(1234),(13)(24),(1432),(12)(34),$$
$$(14)(23),(13)(2)(4),(24)(1)(3)\}$$

$D_4 \leq S_4$