4.3 循环群与置换群

4.3.1 循环群

定义11 设$< G,* >$是一个群，若存在元素$a \in G$，使得

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

称$< G,* >$为**循环群**，记作$G =< a >$，称a为此群的**生成元**。

例 $<Z,+>$ 是循环群，其生成元是 1 或 -1

因为 $\forall i \in Z$ ，若 $i>0$ 有

$$i=\underbrace{1+1+\cdots+1}_{i}=1^{i}\ ;\quad -i=\underbrace{1^{-1}+1^{-1}+\cdots+1^{-1}}_{i}=1^{-i}$$

$$i=\underbrace{(-1)^{-1}+(-1)^{-1}+\cdots+(-1)^{-1}}_{i}=(-1)^{-i}\ ;\quad -i=(-1)^{i}$$

特别的，对于0来说，需特殊对待。

个别教科书上说：0可以看成是1的0倍

例10 群$<Z_6,\oplus>$是循环群，生成元是1或5。

因为

$$1^1=1，1^2=2，1^3=3，1^4=4，1^5=5，1^6=0$$

$$5^1=5，5^2=4，5^3=3，5^4=2，5^5=1，5^6=0$$

例11 设 $G=\{\alpha,\beta,\gamma,\delta\}$，在 G 上定义二元运算 $*$ 如表所示

$*$	α	β	γ	δ
α	α	β	γ	δ
β	β	α	δ	γ
γ	γ	δ	β	α
δ	δ	γ	α	β

说明 $<G,*>$ 是一个循环群。

解　由运算表可知运算 $*$ 是封闭的；α 是幺元；β,γ,δ 的逆元分别是 β,δ,γ；可以验证运算 $*$ 是可结合的；所以 $<G,*>$ 是一个群。

在这个群中，由于

$$\gamma*\gamma=\gamma^2=\beta，\gamma^3=\delta，\gamma^4=\alpha$$

$$\delta*\delta=\delta^2=\beta，\delta^3=\gamma，\delta^4=\alpha$$

一个循环群的生成元不一定唯一

故群 $<G,*>$ 是由 γ 或 δ 生成的，因此 $<G,*>$ 是一个循环群。

定理8 任何一个循环群必是阿贝尔群

证明 设 a 是循环群 $<G,*>$ 的生成元，

$\forall x, y \in G$，必存在 $r, s \in Z$，使得 $x = a^r, y = a^s$，

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

即运算 $*$ 是可交换的，故该群是阿贝尔群。

证毕

定理9 设 $<G,*>$ 是由元素 a 生成的 n 阶有限循环群，即 $|G|=n$，则 $a^n=e$，且

$$G=\{e,a,a^2,\cdots,a^{n-1}\}$$

证明 利用反证法（略）

循环群中生成元的阶数与群的阶数相同

例 $<Z,+>$ 是无限阶循环群；

$<Z_n,\oplus>$ 是 n 阶循环群。

对无限阶循环群 $G=<a>$ ，其生成元是 a 和 a^{-1}。

对 n 阶循环群 $G=<a>=\{e,a,a^2,\cdots a^{n-1}\}$，其生成元是 a^t，当且仅当 t 与 n 互质。

例 $<Z,+>$ 的生成元是1和-1，-1是1的逆元。

$<Z_6,\oplus>$是6阶循环群，1和5都与6互质，故1和5是生成元。

定理10 循环群的子群仍是循环群。

定理11 无限循环群的子群除 $< e >$ 外，均为无限循环群。

（证明略）

例12 $G=<Z,+>$ 是无限阶的循环群，则 G 的子群除 $<\{0\},+>$ 外，均为无限阶循环群。

如 $<2Z,+>,<3Z,+>,\cdots,<nZ,+>,\cdots$

均为其子群，其中

$$nZ=\{nz \mid z\in Z\}=\{\cdots,-2n,-n,0,n,2n,\cdots\}$$

定理12 n阶循环群$G=\langle a\rangle$的子群的阶数均为n的因子。对于n的每个正因子d，有且只有一个d阶循环子群，生成元为 $a^{\frac{n}{d}}$。

（证明略）

例13　求12阶循环群 $<G,*>$ 的所有子群，其中 $G=\{e,a,a^2,\cdots,a^{11}\}$ 。

解　12的正因子为 1,2,3,4,6,12，子群为

$$<a^{\frac{12}{1}}>=<e>=<\{e\},*>$$

$$<a^{\frac{12}{2}}>=<a^6>=<\{e,a^6\},*>$$

$$<a^{\frac{12}{3}}>=<a^4>=<\{e,a^4,a^8\},*>$$

$$< a^{\frac{12}{4}} > = < a^3 > = < \{e, a^3, a^6, a^9\}, * >$$

$$< a^{\frac{12}{6}} > = < a^2 > = < \{e, a^2, a^4, a^6, a^8, a^{10}\}, * >$$

$$< a^{\frac{12}{12}} > = < a > = < G, * >$$

4.3.2 置换群

定义12 设 S 是一个非空集合，从集合 S 到 S 的任何一个双射 $\sigma: S \to S$，称为 S 到 S 的一个**置换**。

集合 S 上的每一次置换产生一个 S 中元素的全排列，每一个全排列对应着一个置换。

例如　对于集合 $S=\{a,b,c,d\}$, 将 a 映射到 b, 将 b 映射到 d, 将 c 映射到 a, 将 d 映射到 c, 是从 S 到 S 的一个双射 σ，也称为置换，可以用置换表表示

$$\sigma=\begin{pmatrix} a & b & c & d \\ b & d & a & c \end{pmatrix}$$

表中上一行中按任何次序写出集合中的全部元素, 而在下一行中写每个对应元素的像, 此置换称为4元置换。

n 元置换也可以用不交的轮换之积表示

例　σ 是 $\{1,2,3,4,5,6\}$ 上的置换，定义为

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

它表示

$$\sigma: \quad 1 \mapsto 6, 2 \mapsto 5, 3 \mapsto 3, 4 \mapsto 4, 5 \mapsto 2, 6 \mapsto 1$$

可将其写成 $\sigma = (16)(25)(3)(4)$，简化为 $\sigma = (16)(25)$

例 定义{1,2,3,4,5,6}上的置换如下

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

写成轮换之积为

$\tau=(14325)(6)$ 或 $\tau=(14325)$

定义13 设 $S=\{1,2,\cdots,n\}$，将 S 上的 $n!$ 个不同置换组成的集合记为 S_n，关于置换的复合∘运算构成一个群 $<S_n,\circ>$，称为 S 上的 n **元对称群**，它的任何子群称为 S 上的 n **元置换群**。

说明 在 S_n 上规定置换的复合运算∘，运算封闭，幺元为恒等置换 $I_S=(1)\in S_n$，复合运算满足结合律，$\forall\sigma\in S_n$，其逆元为逆置换，即

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

故 $<S_n,\circ>$ 构成群。

例14 $S_3=\{(1),(12),(13),(23),(123),(132)\}$，其运算表如下

$\circ$	(1)	(12)	(13)	(23)	(123)	(132)
(1)	(1)	(12)	(13)	(23)	(123)	(132)
(12)	(12)	(1)	(132)	(123)	(23)	(13)
(13)	(13)	(123)	(1)	(132)	(12)	(23)
(23)	(23)	(132)	(123)	(1)	(13)	(12)
(123)	(123)	(13)	(23)	(12)	(132)	(1)
(132)	(132)	(23)	(12)	(13)	(1)	(123)

$<S_3\circ>$为 $S=\{1,2,3\}$ 上的 3 元对称群。

说明 按两个函数进行复合运算

$$(12)\circ(13)=\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}\circ\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}=\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}=(132)$$

先作

$$(23)\circ(123)=\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}\circ\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}=\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}=(13)$$

因为 $(13)\circ(12)\neq(12)\circ(13)$

故 $<S_3,\circ>$ 不是阿贝尔群。

在 $<S_3,\circ>$ 中，$(12),(13),(23)$ 均为 2 阶元

而 $(123),(132)$ 是 3 阶元。

如 $(12)\circ(12)=(1)$

$$(123)\circ(123)\circ(123)=(1)$$

$<S_3,\circ>$ 有 6 个子群：

$<(1)>=<\{(1)\},\circ>$； $<(12)>=<\{(1),(12)\},\circ>$；

$<(13)>=<\{(1),(13)\},\circ>$； $<(23)>=<\{(1),(23)\},\circ>$；

$<(123)>=<(132)>=<\{(1),(123),(132)\},\circ>$； $<S_3,\circ>$

其中$<(1)>$和$<S_3,\circ>$是平凡子群，其余均为真子群。

定理13 任一有限群均与一个置换群同构。

证明 设 n 阶有限群 $<G,*>$，其中 $G=\{a_1,a_2,\cdots,a_n\}$，则存在一个映射 φ：

$$\varphi(a_i)=\begin{pmatrix} a_1 & a_2 & \cdots & a_n \\ a_i*a_1 & a_i*a_2 & \cdots & a_i*a_n \end{pmatrix}=p_{k_i} \quad (i=1,2,\cdots,n)$$

由这些置换组成的集合 $P=\{p_{k_1},p_{k_2},\cdots,p_{k_n}\}$

对于复合运算构成一个置换群$<P,\circ>$，由于

$$\varphi(a_i * a_j) = \begin{pmatrix} a_1 & a_2 & \cdots & a_n \\ a_i * a_j * a_1 & a_i * a_j * a_2 & \cdots & a_i * a_j * a_n \end{pmatrix}$$

$$\varphi(a_i)\circ\varphi(a_j) = \begin{pmatrix} a_1 & a_2 & \cdots & a_n \\ a_i * a_1 & a_i * a_2 & \cdots & a_i * a_n \end{pmatrix} \circ \begin{pmatrix} a_1 & a_2 & \cdots & a_n \\ a_j * a_1 & a_j * a_2 & \cdots & a_j * a_n \end{pmatrix}$$

$$= \begin{pmatrix} a_1 & a_2 & \cdots & a_n \\ a_i * a_j * a_1 & a_i * a_j * a_2 & \cdots & a_i * a_j * a_n \end{pmatrix}$$

故 $\varphi(a_i * a_j) = \varphi(a_i)\circ\varphi(a_j)$

因此，有限群 $<G,*>$ 与置换群 $<P,\circ>$ 同构。

证毕

由此定理可知，对有限群的研究问题，可以转换为对置换群的研究，而置换群是一类目前解决的比较好的群。

内容小结

1.循环群的判断及子群的求法

2.置换群的概念

课下练习 P66 习题4.3 1,2,3