17.2 子群

- 子群定义
- 子群判别定理
- 重要子群的实例
  - 生成子群
  - 中心
  - 正规化子
  - 共轭子群
  - 子群的交
- 子群格

子群定义

定义 设G为群, H是G的非空子集，若H关于G中运算构成群，则称H为G的子群，记作$H \le G$.

如果子群H是G的真子集，则称为真子群，记作$H<G$.

说明： 子群H就是G的子代数.

假若H的单位元为e', 且x在H中相对e'的逆元为x',

则

$$xe' = x = xe \Rightarrow e' = e$$

$$xx' = e' = e = xx^{-1} \Rightarrow x' = x^{-1}$$

子群判定定理一

定理1　G 是群，H 是G 的非空子集，则

$$H \le G \Leftrightarrow \forall a,b \in H,\ ab \in H,\ b^{-1} \in H$$

证：　只证充分性.(即证H构成群）

H 非空，存在$a \in H$，由已知得$a^{-1} \in H$，

由已知有$e=aa^{-1} \in H$, 即$e \in H$

由已知可得H关于G中的运算是封闭的，

且H中的每个元素的逆元都存在H中。

又G是群，H是G的非空子集，故H关于G中的

运算是可结合的.

子群判定定理二和三

定理2　G是群，H是G的非空子集，则

$$H \le G \Leftrightarrow \forall a,b \in H,\ ab^{-1} \in H$$

证 充分性. $H \ne \varnothing \Rightarrow \exists b \in H$

$b \in H \Rightarrow bb^{-1} \in H \Rightarrow e \in H$（存在单位元）

$\forall a,\ a \in H \Rightarrow ea^{-1} \in H \Rightarrow a^{-1} \in H$（每个元素可逆）

$\forall a,b,\ a,b \in H \Rightarrow a \in H, b^{-1} \in H \Rightarrow a(b^{-1})^{-1} \in H \Rightarrow ab \in H$

（封闭）

定理3 G是群，H 是G 的有限非空子集，则

$$H \le G \Leftrightarrow \forall a,b \in H,\ ab \in H \qquad // \text{运算封闭}$$

证明见教科书.

重要子群

*a*生成的子群　$<a> = \{ a^k \mid k \in Z \}$， $a \in G$

*B*生成的子群　$<B> = \cap\{ H \mid H \leq G, B \subseteq H \}, B \subseteq G$

$$< B >= \{b_1^{e_1} b_2^{e_2} \cdots b_n^{e_n} \mid b_i \in B, e_i = \pm 1, i = 1,2,\cdots,n, n \in Z^+\}$$

中心　$C = \{ a \mid a \in G, \forall x \in G(ax=xa) \}$

a 的正规化子群　$N(a) = \{ x \mid x \in G, xa=ax \}, a \in G$

H 的正规化子群　$N(H) = \{ x \mid x \in G, xHx^{-1}=H \}, H \leq G$

共轭子群　$xHx^{-1} = \{ xhx^{-1} \mid h \in H \}$

其中 $H \leq G, x \in G$

子群的交

$H, K \leq G$, 则

(1) $H \cap K \leq G$

(2) $H \cup K \leq G \Leftrightarrow H \subseteq K \vee K \subseteq H$

生成子群的实例

(1) 整数加群，由2生成的子群是

$<2>=\{2k|k\in Z\}=2Z$

(2) 群$<Z_6, +_6>$中，由2生成的子群由

$2^0=0$，$2^1=2$，$2^2=4$，$2^3=0$，…构成，

即 $<2>=\{0,2,4\},<3>=\{0,3\},<1>= Z_6$,

(3) Klein四元群$G=\{e,a,b,c\}$的所有生成子群是：

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

关于子群的证明

证明 中心C为子群

证 由于e属于C, C非空.

任取$a, b\in C$，对于任意$x\in G$有

$$(ab^{-1})x = a(b^{-1}x) = a(x^{-1}b)^{-1} = a(bx^{-1})^{-1}$$

$$= a(xb^{-1}) = (ax)b^{-1} = (xa)b^{-1} = x(ab^{-1})$$

因此ab^{-1}属于C. 由判定定理2，命题得证

分析：H非空， $H \le G \Leftrightarrow \forall a,b \in H, ab^{-1} \in H$

重要子群的证明（续）

设$H,K \leq G$, 则

(1) $H \cap K \leq G$

(2) $H \cup K \leq G \Leftrightarrow H \subseteq K \vee K \subseteq H$

证 (1) 略.

(2) 只证必要性（ $H \cup K \leq G \Rightarrow H \subseteq K \vee K \subseteq H$ ）

假若 $\exists h(h \in H, h \notin K)$, $\exists k(k \in K, k \notin H)$,

则 $hk \notin H$，否则 $k=h^{-1}(hk) \in H$, 矛盾.

同理 $hk \notin K$, 从而 $hk \notin H \cup K$

但是$h,k \in H \cup K$, 与$H \cup K \leq G$矛盾.（不满足封闭性）

AB 构成子群的条件

命题 设$A,B\le G$，定义$AB = \{ ab \mid a\in A, b\in B \}$, 则

(1) $AB\le G \Leftrightarrow AB=BA$.

(2) $AB\le G \Rightarrow AB=\langle A\cup B\rangle$

证(1) 略.

(2) $A\subseteq AB,\ B\subseteq AB \Rightarrow A\cup B\subseteq AB \Rightarrow \langle A\cup B\rangle\subseteq AB$

$\forall ab,\ ab\in AB \Rightarrow a\in A,\ b\in B \Rightarrow a,b\in A\cup B$

$\Rightarrow a,b\in\langle A\cup B\rangle \Rightarrow ab\in\langle A\cup B\rangle$

例 Klein四元群$G =\{ e, a, b, c \}$,

$\langle a\rangle=\{ e, a \}, \langle b\rangle=\{ e, b \}, \langle c\rangle=\{ e, c \}$

$\langle a\rangle\langle b\rangle=\{ e, a, b, c \}$

$\langle\{ a, e \}\cup\{ b, e\}\rangle = \langle\{ a, b, e \}\rangle=\{ e, a, b, c \}$

子群格

- G 为群，$S=\{\,H \mid H\le G\,\}$,偏序集$<S,\subseteq>$构成格，称为G 的子群格
- Klein 四元群，Z_{12} 的子群格.

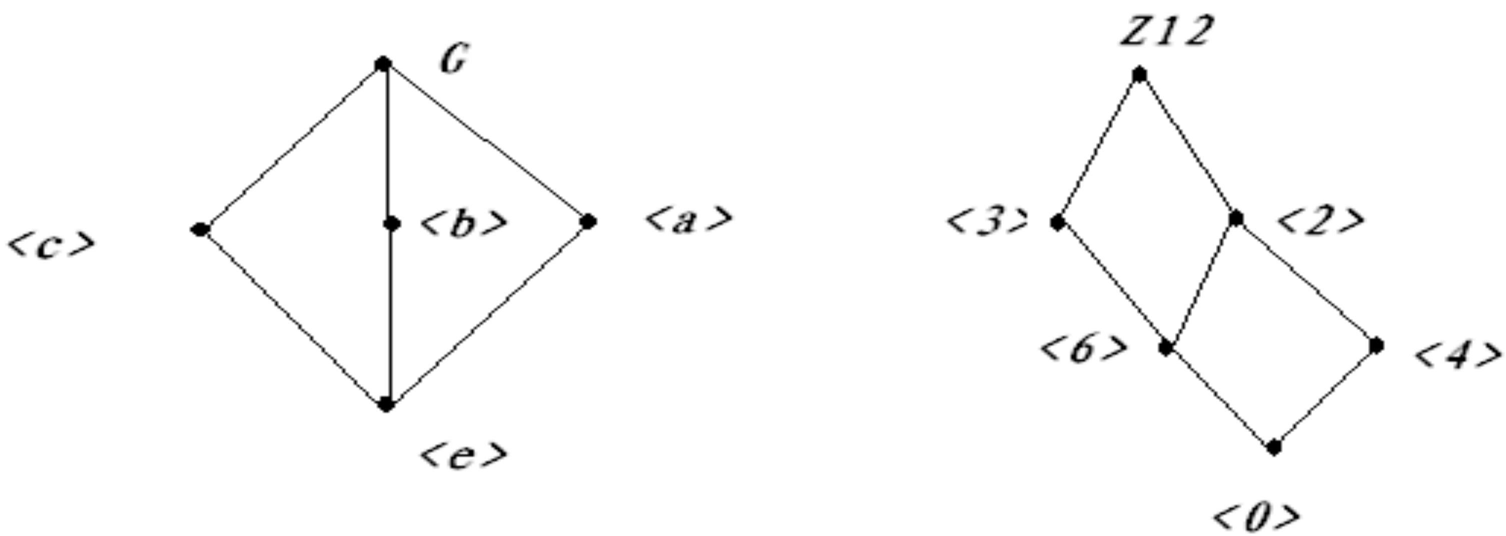

图11.1

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

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$G=\{e,a,a^2,\cdots,a^{n-1}\}$为**$n$阶循环群**

实例 $\langle Z,+\rangle$为无限循环群,生成元是1和-1

$\langle Z_n,\oplus\rangle$为$n$阶循环群，生成元是1、$n$-1

符号(n,r)与$[n,r]$

(n,r)

定义：n 与r 的最大公约数

性质：$\exists u,v\in Z\,(un+rv=(n,r))$

$(n,r)=1$, n 与r 互质（互素）

$\Leftrightarrow \exists u,v\in Z\,(un+rv=1)$

$[n,r]$

定义：n 与r 的最小公倍数

性质：$[m,n]=\dfrac{mn}{(m,n)}$

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

$\Leftrightarrow(n,r)=1$.

φ(n)：欧拉函数。对于任何正整数n，

φ(n)是小于等于n且与n互质的正整数个数。

例如：$\langle Z_6, +_6\rangle$，其生成元是1，r=1,5，φ(6)＝2，

则1^5=5也是生成元。

循环群的生成元（证明思路）

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 $(r,n)=1$, 则a^r 是生成元

反之，若a^r 是生成元，则 $(r,n)=1$.

(3) 若要证明a是生成元，

则需证明$\forall x\in G$有$x=a^l, l\in Z$.

证明

证 (1) a 是生成元，$<a^{-1}>\subseteq G$,

任取$a^l\in G$, $a^l=(a^{-1})^{-l}\in<a^{-1}>\Rightarrow G\subseteq<a^{-1}>$。故$a^{-1}$是生成元.

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. $n>1$

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

$$\Rightarrow a^r \text{ 为生成元}$$

反之，若a^r 为生成元

$$(a^r)^{\frac{n}{(n,r)}}=e\Rightarrow|a^r|\,\Big|\,\frac{n}{(n,r)}\Rightarrow n\,\Big|\,\frac{n}{(n,r)}\Rightarrow(n,r)=1$$

生成元的举例

(1) 设$G=\{e,a,\ldots,a^{11}\}$是12阶循环群，则φ(12)＝4。

小于或等于12且与12互质的数是1,5,7,11，

根据定理，a,a^5,a^7和a^{11}是G的生成元。

(2)设G＝<Z_9, $+_9$ >是模9的整数加群， |G|=9，则φ(9)＝6。小于或等于9且与9互质的数是1,2,4,5,7,8，

根据定理，G的生成元是1,2,4,5,7和8。

(3)设G＝3Z＝{3z|z∈Z}，G上的运算是普通加法。

那么G只有两个生成元：3和-3。

循环群的子群

定理2 $G=<a>$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，

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$H=<a^m>$有限，$a\neq e$, 则推出 $|a|$ 有限.

(3) $H=<a^m>$, $|H|=|a^m|$, $(a^m)^n=e$. 从而 $|a^m|$ 是n 的因子.

(4) $<a^{n/d}>$是d 阶子群，然后证明唯一性.

证明

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$i(i\geq m)$, $i = lm+r$, $r\in\{0,1,\ldots,m-1\}$

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

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

(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) 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 $|H| =|a^m|=d$,

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

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

若$H'=<a^m>$也是G 的d 阶子群，其中a^m 为H'的最小正方幂元．则

$$a^{md}=e \Rightarrow n \mid md \Rightarrow \frac{n}{d} \mid m \Rightarrow m=\frac{n}{d}t \Rightarrow a^m=a^{\frac{n}{d}t} \in H$$

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

实例

例1 (1) $<Z_{12},\oplus>$, 求生成元、子群.

生成元为与12 互质的数：1, 5, 7, 11

12 的正因子为1, 2, 3, 4, 6, 12,

子群：$<0>,<1>, <2>,<3>, <4>, <6>$

(2) $G=<a^2>$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：$<e>, <a^2>, <a^4>,<a^6>, <a^8>, <a^{12}>$

(3) $<a>$为无限循环群，求生成元和子群.

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

(4) $G=<Z,+>$，求生成元和子群

生成元：1, −1; 子群nZ, $n = 0,1,\ldots$,

作业

- **复习要点：**

  子群的判定定理

  有哪些重要子群，它们之间存在什么关系？

  循环群的定义

  有限循环群与n阶循环群的区别

  怎样求循环群的生成元

  怎样求循环群的子群

- **书面作业：**

  习题十七，14, 16, 19, 20