# 离散数学

# Discrete Mathematics

吴梅红

厦门大学计算机科学系

**E-mail: wmh@xmu.edu.cn**

# 6.2 群Group与子群Subgroup

- 群在存在对称的领域中都有它的应用。近来, 群论应用出现在编码理论、粒子物理领域和Rubik魔方解法中。

定义 6.5 <G, ∘>是含有一个二元运算的代数系统(封闭), 如果满足以下条件:

(1) ∘运算是可结合的; /*半群

(2) 存在$e \in G$是关于∘运算的单位元; /*独异点

(3) $\forall x \in G$, $x$关于∘运算的逆元$x^{-1} \in G$,

则称G是一个群。 ∎

- 群比半群有更多的结构, 本章的结果比上章更深刻。

例 (1) $<Z, +>$(称为**整数加群**), $<Q, +>$, $<R, +>$都是群,

其中0是单位元, $\forall x \in Z$, $-x$是x的加法逆元。

(2) $<Z_n, \oplus>$是群, 称为**模n整数加群**。其中$Z_n = \{0, 1, 2, \cdots, n-1\}$, $x + y = (x + y) \bmod n$, $\forall x, y \in Z_n$。

0是单位元, $\forall x \in Z_n$, $n - x \bmod n$是x的加法逆元。

(3) 设$n \geq 2$, $<M_n(R), +>$是群, 称为**n阶实矩阵加群**。

n阶全零矩阵是单位元, $-M$是矩阵M的加法逆元。

(4) $<P(B), \oplus>$是群, 其中P(B)是集合B的幂集,

$\oplus$为集合的对称差运算。$\varnothing$是单位元,

$\forall A \in P(B)$, A是它自己的对称差逆元, 即$A \oplus A = \varnothing$。

(5) 设S是$A^A$中所有双射函数的集合, 则S关于函数合成运算构成群。恒等函数$I_A$是单位元, $f^{-1}$是f的逆元。

| * | e | a | b | c |
|---|---|---|---|---|
| e | e | a | b | c |
| a | a | e | c | b |
| b | b | c | e | a |
| c | c | b | a | e |

例 6.4 令 G = {e, a, b, c}, * 运算由表 6.1给出。

容易验证 * 运算是可结合的, e是G中的单位元,

$\forall x \in G$, $x^{-1} = x$ (即 $x^2 = e$), G关于 * 运算构成一个群,

称为Klein(克莱因)四元群。 /*可交换, 运算表对称

- 在a, b, c中, 任两个元素运算结果等于第三个元素。
- 所有多项式 $x^n - 1$ ($n = 1, 2, 3, \ldots$) 的一切复数根

  构成一个群, 称为单位根群。

| $\oplus$ | 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 |

例 6.5 考虑模n加群$<Z_n, \oplus>$，其中$Z_n = \{0, 1, 2, \cdots, n-1\}$，

$\forall x, y \in Z_n$, $x + y = (x + y) \bmod n$。 0是单位元。

上一行循环左移得下一行。

- 例如 模6加群$Z_6$，其 * 运算表如 表 6.2 所示。

例 6.6 设 $K = \{1, 2, 3\}$, 如下定义K上的6个函数:

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

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

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

$$S = \{f_1, f_2, f_3, f_4, f_5, f_6\},$$

则 S关于函数的右复合运算构成(置换)群。

其单位元是恒等函数$f_1$;

$f_1, f_2, f_3, f_4$的逆元都是自身,

$f_5$与$f_6$互为反函数, 即互为逆元。

**定义(1)** 群G的基数称为群G的阶, 若群G的阶是正整数, 称G为n阶群, 记作$|G| = n$; 否则称G为无限群。 ■

**(2)** 若群G中只含有一个元素, 即$G = \{e\}$, 则称G为平凡群.

**(3)** 若群G中运算满足交换律, 则称G为交换群或阿贝尔(Abel)群。 ■

**例** $\langle\{0\}, +\rangle$是平凡群。

整数加群和模n整数加群是Abel群,

Klein四元群也是Abel群。

**例** 整数加群是无限群, 模n整数加群是n阶群,

Klein四元群是4阶群。 ■

**定义** $G$是群, $\forall x \in G$, $x$的$n$次幂 ($n \in Z$)。/*$Z^+$, $N$

$$
x^n = \begin{cases} e, & n = 0; \\ x^{n-1}x, & n > 0; \\ (x^{-1})^m, & n = -m,\ m > 0。 \end{cases}
$$
■

**例** 设$G = <Z, +>$, 则 $(-4)^{-2} = ((-4)^{-1})^2 = 4^2 = 4 + 4 = 8$

$1^{-3} = (1^{-1})^3 = (-1)^3 = (-1) + (-1) + (-1) = -3$

**定义** $G$是群, $x \in G$, 使得$x^k = e$ 成立的 最小正整数$k$ 称为$x$的阶, 记作 $|x|$。

- 若这样的正整数不存在, 则称a是无穷阶的。 ■
- 在有限群$G$中, 元素的阶是群$G$的阶的因子。 ■

例

(1) 整数加群$<Z, +>$中 $|0| = 1$, 其他元素的阶不存在。

模6整数加群$<Z_6, \oplus>$中,

$|0| = 1$, $|1| = |5| = 6$, $|2| = |4| = 3$, $|3| = 2$。

(2) Klein四元群$G = \{e, a, b, c\}$中, e是1阶元,

$\forall x \in G$, $x^2 = e$, a, b和c 都是2阶元。 ∎

- 下面讨论群的性质。
- 在群论中, 在一般情况下, 可以省略乘法符号* 。

**定理 6.1** G为群, $\forall a, b \in G$有

(1) $(x^{-1})^{-1} = x$ ;　　(2) $(xy)^{-1} = y^{-1}x^{-1}$ ;

(3) $x^n x^m = x^{n+m}$ ;　　(4) $(x^n)^m = x^{nm}$ ;　/*仿定理16.1

(5) 若G为Abel群, $(xy)^n = x^n y^n$ , $n \in Z$。　/* 归纳证明

证 (1) $\forall x \in G$, x是$x^{-1}$的逆元,

由逆元的惟一性得 $(x^{-1})^{-1} = x$。

(2) $(xy)(y^{-1}x^{-1}) = x(yy^{-1})x^{-1} = xex^{-1} = xx^{-1} = e$,

$(y^{-1}x^{-1})(xy) = y^{-1}(x^{-1}x)y = y^{-1}ey = y^{-1}y = e$,

所以 $(xy)^{-1} = y^{-1}x^{-1}$ 。 ∎

归纳证明推广 $(x_1x_2\ldots x_k)^{-1} = x_k^{-1}\ldots x_2^{-1}x_1^{-1}$。

**定理** 元素个数大于1的群G不可能有零元。

**证** 当|G| >1时, 假设(G; •)有零元z, 则对G中任意元素x,

$z \bullet x = x \bullet z = z \neq e$,

这说明 零元z不存在逆元,

与群中每个元素都有逆元的定义矛盾。 ∎

**特例**：群G = {e}, e既是单位元, 又是零元。

定理 6.2 G为群, $\forall a, b \in G$, 方程 (1) $ax = b$ (2) $ya = b$ 在G中有解且有惟一解。 /*必要性

证 (1)$\forall a, b \in G$ 有 $a(a^{-1}b) = (aa^{-1})b = b$,

所以$a^{-1}b$是方程(1)的一个解。

- 假设c是方程 $ax = b$的任一解, 即 $ac = b$, 则

$$c = ec = (a^{-1}a)c = a^{-1}(ac) = a^{-1}b。$$

这就证明 $a^{-1}b$是方程$ax = b$的惟一解。

- 同理 $(ba^{-1})a = b(a^{-1}a) = b$, $ba^{-1}$是方程(2)的一个解,

  可证方程(2)有惟一解$ba^{-1}$。 ∎

- 以上定理给出了群的性质。
- 反过来, 我们也可以利用这条性质来定义群。

*定理 设G是具有一个可结合的二元运算的代数系统，

如果$\forall a, b \in G$方程 $ax = b$ 和 $ya = b$ 在G中有解，

则 G是群。 /*充分性

证 $\forall b \in G$，方程 $bx = b$ 在G中有解，将这个解记为e。

即 $be = b$。

$\forall a \in G$，方程 $yb = a$ 在G中有解，将这个解记为c，

即 $cb = a$。那么有 $ae = (cb)e = c(be) = cb = a$，

e是G中的右单位元。

$\forall a \in G$，方程 $ax = e$ 在G中有解，

恰为a相对于e的右逆元。由定理6.1，G是一个群。 ▌

**定理 6.3 群中运算满足消去律, 即**

(1) 若 $ab = ac$, 则 $b = c$ (左消去律),

(2) 若 $ba = ca$, 则 $b = c$ (右消去律)。 /*必要性

证 (1) $\forall a, b, c \in G$, 由 $ab = ac$,

$$\Rightarrow \quad a^{-1}(ab) = a^{-1}(ac),$$

$$\Rightarrow \quad (a^{-1}a)b = (a^{-1}a)c,$$

$$\Rightarrow \quad b = c。$$

(2) $ba = ca \quad \Rightarrow \quad (ba)a^{-1} = (ca)a^{-1}$

$$\Rightarrow \quad b(aa^{-1}) = c(aa^{-1}) \quad \Rightarrow \quad b = c \qquad \blacksquare$$

- 这条性质也可以用来定义群。

**定理 设G是具有一个二元运算的不含零元的有限代数系统, 且该运算适合结合律和消去律, 则G是群。

证 令 $G = \{a_1, a_2, \ldots, a_n\}$。 $\forall a \in G$, 令

$aG = \{aa_i \mid i = 1, 2, \ldots, n\}$, 则 $aG \subseteq G$, /*封闭性

- 且 aG中元素两两不同。

  若不然有 $aa_i = aa_j$, 则 $a_i = a_j$, 与G有n个元素矛盾。

  因此 aG中有n个元素， $aG = G$ 。

- $\forall b \in G$, $ax = b$, 必存在 $a_i \in G$, 使得 $aa_i = b$,

  方程 $ax = b$ 在G中有解。

- 同理可证方程 $ya = b$ 在G中也有解。 /*先证 $Ga = G$

- 根据定理6.2, G是群。 /*充分性 ∎

| * | e | a | b | c | d |
|---|---|---|---|---|---|
| e | e | a | b | c | d |
| a | a | b | c | d | e |
| b | b | c | d | e | a |
| c | c | d | e | a | b |
| d | d | e | a | b | c |

**定理** 设<S, *, e>为独异点(或群), e是单位元, 则关于运算*的运算表中没有两行或两列是相同的。

**证** $\forall$ a, b $\in$S, 当a $\neq$ b时,

总有 a*e = a $\neq$ b = b*e,  /*两行在e列处不同

和 e*a = a $\neq$ b = e*b,  /*两列在e行处不同

结论成立。 ▌

**定理 设$G = \{a_1, a_2, \ldots, a_n\}$为群, 则G的运算表的每行每列都是G中元素的一个置换。 /*有穷集合一一变换

证 $\forall$ $i = 1, 2, \ldots, n$, 设 $a_{i1}, a_{i2}, \ldots, a_{in}$ 是运算表的第i行,

假设 $a_{ij} = a_{il}$, 根据运算表的定义有 $a_i a_j = a_i a_l$。

由于群中运算满足消去律, 因此有$a_j = a_l$,

与G中有n个元素矛盾。这就证明

G中任何元素在运算表的每一行至多出现一次。

- $\forall a_j \in G$ $(i = 1, 2, \ldots, n)$, 方程 $a_i x = a_j$ 在G中有解。

若 $x = a_k$, 则 $a_j$ 出现在第i行第k列上。因此

G中任何元素在运算表的每一行至少出现一次。

- 综上所述, 运算表的每一行是G中元素的一个置换。
- 同理可证运算表的每一列也是G中元素的一个置换. ▌

定理 6.4 G是群, $a \in G$ 且 $|a| = r$, 则 /*$a^r = e$,

(1) $a^k = e$ 当且仅当 $r \mid k$, $k \in Z$; /*最小正整数r

证 (1) 充分性 已知 $r \mid k$, 即存在整数$l$, 使得$k = l\,r$。

所以有 $$a^k = a^{l\,r} = (a^r)^l = e^l = e。$$

- 必要性 根据除法有 $k = l\,r + i$, 其中$l \in Z$, $0 \leqslant i < r$,

因为 $a^k = e$, 所以有

$$e = a^k = a^{l\,r + i} = (a^r)^l \bullet a^i = e \bullet a^i = a^i,$$

a的阶是r, 且 $i < r$, 因此 $i = 0$, 这就证明了$r \mid k$ 。 ▌

定理 6.4 G是群, $a \in G$ 且 $|a| = r$,

则 (2) $|a| = |a^{-1}|$ ;

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

可知 $a^{-1}$的阶存在。

令 $|a^{-1}| = t$, $t \mid r$, /* 由(1)

- 而 $a = (a^{-1})^{-1}$,

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

所以有 $r \mid t$。 /* $|a| = r$, 由(1)

- 这就证明了 $r = t$,

即 $|a| = |a^{-1}|$ 。

定理 6.4 G是群, $a \in G$ 且 $|a| = r$, 则

(3) 若 $|G| = n$, 则 $r \le n$。　　　/* 元素的阶≤群的阶

证 (3) $e, a, a^2, \dots, a^{r-1}$ 必两两不同。

若不然有 $a^i = a^j$, $0 \le i < j \le r-1$。

由消去律得 $a^{j-i} = e$,　　　/* $r > j-i > 0$

与 $|a| = r$ 矛盾。

- 令 $G' = \{e, a, a^2, \dots, a^{r-1}\} \subseteq G$,　　　/* 封闭性

假设 $r > n$, 则 $|G'| = r > n = |G|$,

与 $G' \subseteq G$矛盾, 所以 $r \le n$。

**例 6.8** $G = \langle P(S), \oplus \rangle$, 其中$S = \{1, 2, 3\}$, $\oplus$为对称差运算。

求方程 $\{1, 2\} \oplus x = \{1, 3\}$ 和 方程 $y \oplus \{1\} = \{2\}$ 的解。

**解**

$$\{1, 2\} \oplus x = \{1, 3\}$$

$$\{1, 2\} \oplus \{1, 2\} \oplus x = \{1, 2\} \oplus \{1, 3\}$$

$$x = \{2, 3\}$$

- $$y \oplus \{1\} = \{2\}$$

$$y \oplus \{1\} \oplus \{1\} = \{2\} \oplus \{1\}$$

$$y = \{1, 2\}$$

例 6.9 证明 单位元e 是群G中惟一的幂等元。

证 $ee = e$, e是群G中的幂等元。

假设 x也是G中的幂等元, 则有 $xx = x$,

由消去律可得 $x = e$ 。 ■

- 群有惟一的单位元e。
- 群中每个元素的逆元也是惟一的。

** 例 G是群, 若$\forall x \in G$都有 $x^2 = e$, 证明G是Abel群。

证 $\forall x, y \in G$, 由 $x^2 = e \Leftrightarrow x = x^{-1}$,

$xy = (xy)^{-1} = y^{-1}x^{-1} = yx$, 所以G是Abel群。 ■

例 Klein群是Abel群。

**定义6.6** G是群, H是G的非空子集, 若H关于G中的运算构成一个群, 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H为G的**真子群**, 记作 $H < G$。 ■

**定义** G是群, $H \le G$, 如果 $H = \{e\}$ 或 $H = G$, 则称H是G的**平凡子群**。G的其余子群均为真子群。 ■ /*平凡子代数

**例** $<Z, +>$是 $<Q, +>$, $<R, +>$ 的真子群,

$<Q, +>$ 是 $<R, +>$ 的真子群。

$<\{0\}, +>$ 和 $<R, +>$都是 $<R, +>$ 的平凡子群。 ■

**例 6.10** $G = \langle Z, +, 0\rangle$是整数加群, 则对任意的$n \in N$,

$nZ = \{nk \mid k \in Z\}$都是G的子群, 且

任何G的子群都具有nZ的形式。

*证 $\forall nk_1, nk_2 \in nZ$, 有$nk_1 + nk_2 = n(k_1 + k_2) \in nZ$, 封闭性.

- $(nk_1 + nk_2) + nk_3 = nk_1 + (nk_2 + nk_3)$, 可结合。
- $0 = n0 \in nZ$ 是nZ中的单位元。
- $\forall nk \in nZ$, $-nk = n(-k) \in nZ$ 是nk的逆元。

  因此 nZ关于G中的加法构成群, 是G的子群。
- 设H是G的任一子群。若 $H = \{0\}$, 则 $H = 0Z$, $0 \in N$;

  否则 存在$a \in H$, $a \neq 0$。

  取H中最小的正整数, 记作n, 则 $nZ \subseteq H$。 /*封闭性

- 任取H中的元素b, 根据除法有 $b = nq + r$,

  其中 $q, r \in Z$ 且 $0 \le r < n$ 。

- 由于 $H \le G$, 所以 $0 \le r = b - nq = b + (-nq) \in H$。

  从而有 $r = 0$, 否则与n是H中最小的正整数矛盾。

  于是 $b = nq \in nZ$, 这就推出 $H \subseteq nZ$。

- 综合上述, $H = nZ$。 ∎

- 考虑 $<Z, +>$ 的子群 $nZ$, $(n \in N)$ :

  当 $n = 0$时, $\{0\}$ 是 $<Z, +>$ 的平凡子群, 也是真子群。

  当 $n = 1$时, $nZ = Z$是 $<Z, +>$ 的另一个平凡子群。

  除此以外, nZ都是Z的非平凡子群。 ∎

- 如果把群看作代数系统$<G, \circ, ^{-1}, e>$, 其中e是G中关于运算$\circ$ 的单位元, 是该代数系统的零元运算。

$\forall x \in G$, $x^{-1}$是x的逆元, 求逆运算$^{-1}$是中的一元运算。

可以证明G的子群就是代数系统$<G, \circ, ^{-1}, e>$的子代数。

- 设$H \leqslant G$, 只需验证: H中单位元e'就是G中的单位元e, 且$\forall x \in H$, x在H中的逆元x' 就是x在G中的逆元$x^{-1}$。
- $\forall x \in H$, 有$x \circ e' = x = x \circ e$, 由G中的消去律得 $e' = e$。再由$x \circ x' = e' = e = x \circ x^{-1}$, 用消去律得到 $x' = x^{-1}$。
- 群G的子群是G的子代数。

# 子群的判定定理

**定理 6.5 (子群判定定理一)**

G是群, H是G的非空子集, 则H是G的子群 $\Leftrightarrow$

(1) $\forall a, b \in H$ 有 $ab \in H$; /*封闭

(2) $\forall a \in H$, 有 $a^{-1} \in H$。

证 必要性: 由子群的封闭性和每一元素存在逆元得证。

要证明充分性, 只需证明 $e \in H$ 即可 /*H结合律同G

H非空, 存在 $a \in H$。由(2)有 $a^{-1} \in H$。

再由 $a \in H$ 和 $a^{-1} \in H$, 根据 (1) 有 $aa^{-1} = e \in H$。 ▌

定理 6.6 (子群判定定理二) /*最实用

G是群，H是G的非空子集，则H是G的子群

当且仅当 $\forall a, b \in H$有 $ab^{-1} \in H$。

证 必要性 由子群的每一元素存在逆元和封闭性得证。

充分性 由H非空必存在 $b \in H$。

根据充分条件, 则有 $bb^{-1} \in H$，即 $e \in H$。

- 任取$a \in H$, 由$e \in H$ 且 $a \in H$, 则根据充分条件

  有 $ea^{-1} = a^{-1} \in H$。 /*定理6.5 (2)

- 任取$a, b \in H$, 根据上面的证明有 $b^{-1} \in H$。

  再使用充分条件有 $a(b^{-1})^{-1} \in H$,

  即 $ab \in H$， /*定理6.5 (1) 所以H是G的子群。 ∎

## 定理 6.7 (子群判定定理三)

G是群, H是G的有穷非空子集,

则H是G的 子群 当且仅当 $\forall a, b \in H$ 有 $ab \in H$。

证 必要性　由子群封闭性得证。

- 为证明充分性, 根据定理6.5 只需证明$a^{-1} \in H$即可。
- $\forall a \in H$, 若 $a = e$, 则 $a^{-1} = a = e$。设$a \neq e$, 令

$$S = \{a, a^2, \ldots, a^k, \ldots\}$$ , 则 $S \subseteq H$。　/*封闭

H是有穷子集, 则S是有穷子集,

必存在 $a^i = a^j\ (i < j)$。　由消去律得 $a^{j-i} = e$。

因为 $a \neq e$, 所以 $j - i \neq 1$, 即$j - i - 1 > 0$。

故 $e = a^{j-i-1}a$, $a^{-1} = a^{j-i-1} \in H$。 ■

例 6.11 G是群, $a \in G$, 令

$$<a> = \{a^k \mid k \in Z\},$$

则 $<a>$是G的子群, 叫做 由a生成的子群。

证 $a \in <a>$, 所以$<a>$是G的非空子集。

任取 $a^i, a^j \in <a>$, $i, j \in Z$, 有

$$a^i (a^j)^{-1} = a^{i-j} \in <a>。$$

由判定定理二有 $<a> \leq G$。 $\blacksquare$

例 $G = <Z_6, \oplus>$, 则

$<1> = <5> = Z_6 = \{0, 1, 2, 3, 4, 5\}$,

$<2> = <4> = \{0, 2, 4\}$,

$<3> = \{0, 3\}$, $<0> = \{0\}$。

例 6.12 G是群, 令

$$C = \{a \mid a \in G \text{ 且 } \forall x \in G, xa = ax\},$$

则C是 G的子群, 叫做 G的中心。 /*可交换元

证 $\forall x \in G\ (ex = xe)$, 即 $e \in C$, C非空。

$\forall a, b \in C$, $\forall x \in G$有

$(ab^{-1})x = ab^{-1}(x^{-1})^{-1}$

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

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

所以 $ab^{-1} \in C$。由判定定理二有 $C \leq G$。 ∎

- 易见, 当G是Abel群时有 $C = G$,
- 如果群G的中心为$\{e\}$, 则称G是无中心的。

例 6.13 G是群, H和K是G的子群, 则

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

证 (1) $e \in H \cap K$, $H \cap K$ 非空。

- 任取 $a, b \in H \cap K$,

则 $a, b \in H$, $a, b \in K$。

又由于H和K是G的子群,

所以 $b^{-1} \in H$, $b^{-1} \in K$。

- 这就得到 $ab^{-1} \in H$ 和 $ab^{-1} \in K$,

即 $ab^{-1} \in H \cap K$。

由判定定理二有 $H \cap K \leq G$。

例 6.13 G是群, H和K是G的子群, 则

(2) $H \cup K \le G$ 当且仅当 $H \subseteq K$ 或 $K \subseteq H$。

证 (2) 充分性 $H \cup K = H$ (或 $K$) $\le G$。

必要性 反证法 假设 $H \not\subseteq K$ 且 $K \not\subseteq H$,

则存在 $h \in H$ 且 $h \notin K$,

同时存在 $k \in K$ 且 $k \notin H$。

- 如果 $hk \in H$, 则 $k = h^{-1}hk \in H$,

  与假设矛盾, 所以 $hk \notin H$。

- 同理可证 $hk \notin K$。因此 $hk \notin H \cup K$,

- 而 $h, k \in H \cup K$, 与 $H \cup K \le G$矛盾。

**定义** 设G是群, 令 $S = \{ H \mid H$是G的子群$\}$,

在S上定义偏序关系, $\forall A, B \in S$

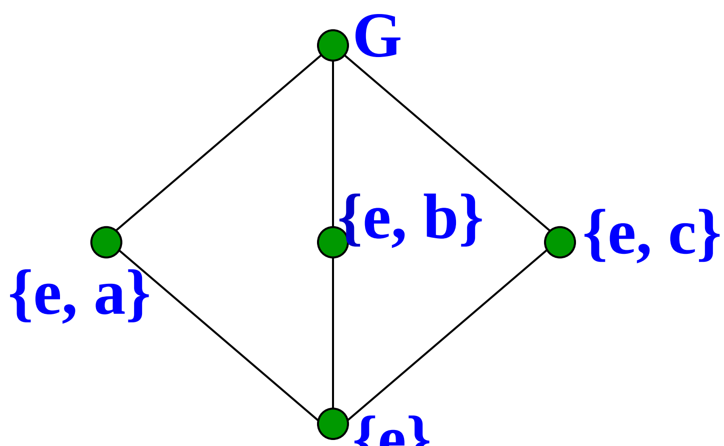
$$A \le B \iff A\text{是}B\text{的子群。} \qquad \blacksquare$$

- 那么$(S, \le)$构成偏序集, 称为群G的子群格(见6.5节格定义)。

**例 6.14.1** $G = \{e, a, b, c\}$是Klein四元群, G的子群是:

<e> = {e}, <a> = {e, a}, <b> = {e, b}, <c> = {e, c}和G,

G的子群格的哈斯图如图6.1所示。



例 6.14.2 $G = \langle Z_{12}, \oplus\rangle$为模12整数加群, G有六个子群:

$H_1 = \{0\} = \langle 0\rangle$,

$H_2 = \{0, 6\} = \langle 6\rangle$,

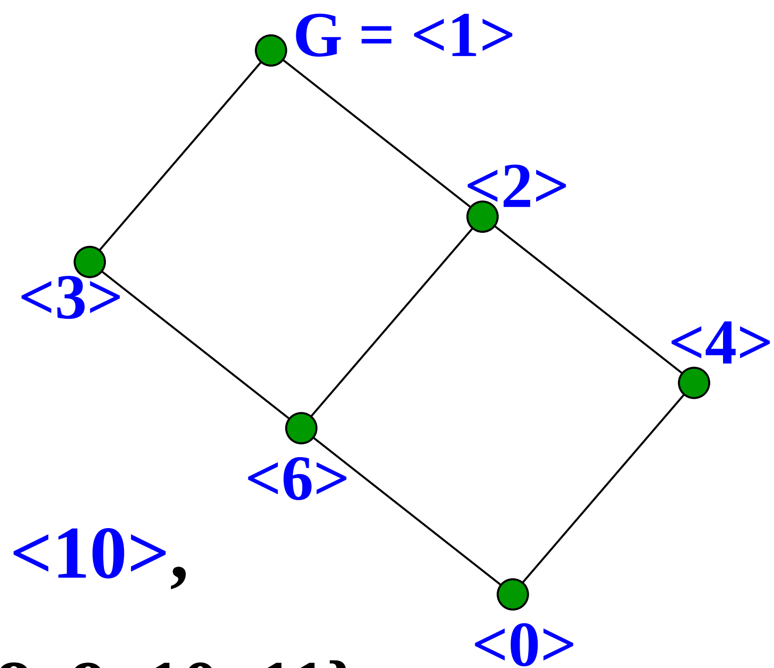
$H_3 = \{0, 4, 8\} = \langle 4\rangle = \langle 8\rangle$,

$H_4 = \{0, 3, 6, 9\} = \langle 3\rangle = \langle 9\rangle$,

$H_5 = \{0, 2, 4, 6, 8, 10\} = \langle 2\rangle = \langle 10\rangle$,

$G = Z_{12} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\}$

$= \langle 1\rangle = \langle 5\rangle = \langle 7\rangle = \langle 11\rangle$。




- G的子群格如图6.1所示。
- a 和 逆元 12–a 必在同一子群, $\langle a\rangle = \langle 12-a\rangle$。

# 6.3 循 环Cyclic群 与 置换群

- 循环群是结构简单, 容易掌握且研究较透彻的一类群。

定义 6.7 G是群, 若存在a $\in$ G 使得　/*例6.11 $\langle a\rangle \subseteq G$

$G = \{a^k \mid k \in Z\}$,　/*循环群是Abel群

则称G为循环群, 记作 $G = \langle a\rangle$, 称a是G的生成元。 ▮

- 在循环群$\langle a\rangle$中, 若 $|a| = n$, 则 $\langle a\rangle = \{e, a, a^2, \ldots, a^{n-1}\}$, 叫做 n阶循环群。　/* $|a| = n = |G|$
- 若$|a|$不存在, 则 $\langle a\rangle = \{e, a, a^{-1}, a^2, a^{-2}, \ldots\}$是无限的, 称为 无限阶循环群。　/* $|a| = \infty = |G|$ ▮
- 循环群$G = \langle a\rangle$, $|G| = |a|$。　/*生成元的阶 = 群的阶

例 整数加群$<Z, +>$是无限阶循环群, 1是它的一个生成元;

模n整数加群$<Z_n, \oplus>$是n阶循环群, 1也是它的一个生成元

- 对于循环群, 一个重要问题是它有 几个生成元?

  有 哪些生成元 (generator)?

定义 设n是正整数, 欧拉函数$\varphi(n)$是小于等于n 且与n互质 (relatively prime)的正整数的个数。▌ /*$1 \in \varphi(n)$

例 $\varphi(1) = 1, \varphi(2) = 1, \varphi(3) = 2, \varphi(4) = 2, \varphi(5) = 4, \varphi(6) = 2.$

例 $n = 12$, 小于等于12且与12互质的正整数是1, 5, 7和11,

因此 $\varphi(12) = 4$。

- 若p是素数, 则 $\varphi(p) = p - 1$。

**定理 6.8** G = <a> 是循环群。

(1) 若G是无限阶循环群, 则G只有两个生成元a 和 $a^{-1}$。

**证 (1)** G = <a>是无限阶循环群, a是G的一个生成元。

任取 $a^i \in \langle a \rangle$, $a^i = (a^{-1})^{-i}$, 即 $a^i$ 可以表成$a^{-1}$的整数次幂, 所以$a^{-1}$也是G的一个生成元。

- 设$b \in \langle a \rangle$是G的生成元, 不妨设$b = a^j$。 由于b是<a>的生成元, a也可以用b的幂表出, 即存在整数t,

  使得 $a = b^t = (a^j)^t = a^{jt}$。由消去律得 $a^{jt-1} = e$。

- 注意到a是无限阶元, 则有 $jt - 1 = 0$ 。

  而 j, t都是整数, 从而有 $j = t = 1$ 或 $j = t = -1$。

- 这就证明了无限阶循环群G中只有a和$a^{-1}$ 是生成元。▌

(2) 若G是n阶循环群, 则G有 $\varphi(n)$个生成元。

当$n = 1$时, $G = \langle e \rangle = \{e\}$的生成元是e。

当$n > 1$时, 对于每一个小于[等于]n的正整数 r ,

$a^r$ 是G的生成元 $\Leftrightarrow$ $(n, r) = 1$。

**证 (2) $n = 1$时结论显然为真, 不妨设$n \geqslant 2$。

充分性 若 $(r, n) = 1$, 则存在整数u, v 使得

$ur + vn = 1$, /*高等代数

于是有 $a = a^{ur+vn} = a^{ur} a^{vn} = (a^r)^u (a^n)^v = (a^r)^u$ 。

- 因此 $\forall a^i \in \langle a \rangle$, 都有 $a^i = (a^r)^{ui}$,

即 $a^i$ 可以用$a^r$ 的整数幂表示, $a^r$ 是G的生成元。

必要性 若 $a^r$ 是G的生成元, 设 $(r, n) = d$, $d \mid n$,

且存在非零整数t 使得 $r = dt$。由于

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

所以由定理6.4(1)可知 $a^r$ 的阶是n/d 的因子。

- 而 $a^r$是n阶循环群的生成元, 故 $a^r$的阶是n,

这就推出 n是n/d的因子。

从而必有$d = 1$, 即 $(r, n) = 1$, r与n互质。 ∎

定理 每个循环群都是Abel群。

证 循环群元素都是生成元的幂元, 可结合和交换。

例 G = <a>是12阶循环群, $\varphi(12) = 4$, 与12互质的数有1, 5, 7和11。由定理6.8, $a$, $a^5$, $a^7$和$a^{11}$都是G的生成元。

/* 例 $G = Z_{12} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\}$

$= \langle 1\rangle = \langle 5\rangle = \langle 7\rangle = \langle 11\rangle$。

- 从同构的观点, 所有的循环群只有两类 —

  整数加群: 无限阶循环群有且仅有两个生成元。

  模n整数加群: n阶有限循环群有且仅有$\varphi(n)$个生成元。

- 一般来说, 求一个群的子群并不是一件容易的事情, 对于循环群, 由下面定理可以直接求出它的所有子群。

**定理6.9** $G = \langle a \rangle$ 是循环群, 那么

(1) G的子群也是循环群;

证 设H是$G = \langle a \rangle$的子群。如果$H = \{e\}$, 则H是循环群;

- 否则取H中 最小正方幂元 $a^m$。$\forall\ a^i \in H$, 根据除法有

  $i = qm + r,\quad q, r \in Z$, 且 $0 \leqslant r < m$, 因此,

  $$a^r = a^i (a^m)^{-q} \in H。$$

  这就推出 $r = 0$, 否则与$a^m$是H中最小正方幂元矛盾。

- $i = qm,\ \ a^i = (a^m)^q$, 即任意 $a^i$ 可由$a^m$ 的幂表出,

  最小正方幂元 $a^m$ 是H 的生成元, 因此 $H = \langle a^m \rangle$。 ∎

**定理 6.9** $G = \langle a \rangle$ 是循环群, 那么

(2) 若G是无限阶的, 则G的子群除{e}外都是无限阶的;

证 设G是无限阶循环群, H是G的子群。

若 $H \neq \{e\}$, 由于H是循环群,

根据(1)有 $H = \langle a^m \rangle$, $a^m \neq e$。

- 假若 $|H| = t$, 则 $(a^m)^t = e$, 即 $a^{mt} = e$,

与a是无限阶元矛盾。

/*无限阶循环群生成元: $|a| = \infty = |G|$

定理6.9 $G = \langle a \rangle$ 是循环群, 那么

(3) 若G是n阶的, 则 ① G的子群的阶是n的因子;

证 设$G = \{e, a, a^2, .., a^{n-1}\}$ 是n阶循环群。

H是G的子群, 不妨设 $H \neq \{e\}$。

- 根据(1) 有 $H = \langle a^m \rangle$,

设 $|a^m| = d$, 则有

$$(a^m)^n = (a^n)^m = e^m = e 。$$

- 由定理6.4(1) 知 $d \mid n$ 。 /*生成元$a^m$的阶 = 群H的阶

所以 子群H的阶d是n的因子;

**定理 6.9** G = <a> 是循环群, 那么(3) 若G是n阶的, 则

②对于n的每个正因子d, 在G中有且只有一个d阶子群。

证 ② 设d是n的正因子, 易见$H = \langle a^{\frac{n}{d}} \rangle$是G的d阶子群。

- 假若 $K = \langle a^m \rangle$也是G的d阶子群, 其中

  $a^m$ 是K中的 最小正方幂元。由于$a^m$的阶是d,

$$a^{md} = (a^m)^d = e。$$

- 根据定理6.4得 n | md, 即 $\frac{n}{d} \mid m$。令$m = \frac{n}{d} \cdot t$, $t \in Z$,

  则有 $a^m = a^{\frac{n}{d}t} = (a^{\frac{n}{d}})^t \in H$。

- 由于$a^m$是$H_1$中的生成元, 所以 $K \subseteq H$。

  又有 $|K| = |H| = d$, 因而 K = H。 ∎

例 $G = \langle a \rangle$ 是无限循环群, $\forall a_i, a_j \in G$, 若 $i \neq \pm j$,

则 $\langle a_i \rangle$ 和 $\langle a_j \rangle$ 是G的不等的子群。

证 若不然必有 $a^i = a^{jt}, t \in Z$, 即$a^{i-jt} = e$, a是有限元,

与$G = \langle a \rangle$ 是无限阶循环群矛盾。

- 所以G有无限多个子群, 分别为

$\langle e \rangle = \{e\}$,

$\langle a \rangle = \langle a^{-1} \rangle = G$,

$\langle a^2 \rangle = \langle a^{-2} \rangle = \{e, a^{\pm 2}, a^{\pm 4}, a^{\pm 6}, \ldots\}$,

$\langle a^3 \rangle = \langle a^{-3} \rangle = \{e, a^{\pm 3}, a^{\pm 6}, a^{\pm 9}, \ldots\}$,

……

例 若G是模15加群<$Z_{15}$, ⊕>。

解 15的正因子为1, 3, 5, 15。G有4个子群:

<0> = {0}, <1> = G ,

<3> = {0, 3, 6, 9, 12, 15}, <5> = {0, 5, 10}。

例 若G是12阶循环群<a>,

12有六个正因子1, 2, 3, 4, 6, 12,

根据定理6.9, G有六个子群,

分别1, 2, 3, 4, 6和0来生成,

正如图6.1的子群格所示。