

在第 2 节中我们已经知道循环群是指由一个元素生成的群，
因而，循环群是交换群，循环群的子群是正规子群，
本节将进一步讨论循环群的结构及其子群和生成元的一些简单性质，

定理 5.1 设循环群 $G=\langle a \rangle$ ，若 a 的所有不同的整数幂都互不相等，

即 $a^k \neq a^l$, k, l 都属于 $\mathbb{Z}$ ，且 $k \neq l$

则 $\langle a \rangle$ 含有无穷多个元素，即 $\langle a \rangle = \{\dots, a^{-2}, a^{-1}, a^0, a^1, a^2, \dots\}$ ，进而 $\langle a \rangle = \{\mathbb{Z}; +\}$

证： 只需证 $\varphi: G \rightarrow \mathbb{Z}, a^k \mapsto k$ 是群同构，

定理 5.2 设循环群 $G=\langle a \rangle$ ，若 a 的不同的整数幂中有两个是相等的，

则存在正整数 n ，使得 $\langle a \rangle = \{a^0, a^1, a^2, \dots, a^{n-1}\}$ ，进而 $\langle a \rangle \cong \{\mathbb{Z}_n; +\}$ ，

证： 由于 a 的整数幂中有两个是相等的，

所以不妨设 s 大于 t 时，有 $a^s = a^t$ ，即 $a^{s-t} = e$ ，其中 e 是循环群 $\langle a \rangle$ 中的单位元，

这就是说，存在一正整数 m ，使得 $a^m = e$ ，

所以我们可以找到一个使得 $a^m = e$ 成立的最小正整数 n ，

$n = \min\{m | a^m = e, m > 0, m \in \mathbb{Z}\}$ ，那么， $\langle a \rangle = \{a^0, a^1, a^2, \dots, a^{n-1}\}$ ，

事实上，若 a^k 属于 $\langle a \rangle$ ，则 $k = nq + r$ ，其中 $0 \leq r < n$ ，

于是 $a^k = a^{nq+r} = (a^n)^q a^r = e a^r = a^r$ ，即 $\langle a \rangle$ 包含于 $\{a^0, a^1, a^2, \dots, a^{n-1}\}$ ，

反之，有 $\{a^0, a^1, a^2, \dots, a^{n-1}\}$ 包含于 $\langle a \rangle$ ，所以 $\langle a \rangle = \{a^0, a^1, a^2, \dots, a^{n-1}\}$ ，

另外，在集合 $\{a^0, a^1, a^2, \dots, a^{n-1}\}$ 中没有两个相等的元素，

如若不然，则存在 $a^i = a^j, 0 \leq i < j \leq (n-1)$ ，即 $a^{j-i} = e$ ，

但是，此时 $0 < (j-i) < n$ ，矛盾，

至于 $\langle a \rangle$ 与 $\mathbb{Z}_n$ 的同构性，只需考虑映射 $\varphi: \langle a \rangle \rightarrow \mathbb{Z}, a^k \mapsto \bar{k}$ 即可，

由上述定理我们知道：

若 a 的整数幂中有两个是相等的，

则循环群 $\langle a \rangle$ 含有有限个元素，称其为有限循环群；

否则， $\langle a \rangle$ 含无穷多个元素，称其为无限循环群，

推论 5.1 n 阶有限循环群同构于 Z_n , 无限循环群同构于 Z ,
当且仅当两个有限循环群阶相同时它们互同构,

在定理 5.2 中, 我们注意到, 当循环群 $\langle a \rangle$ 含有有限个元素时,
其所含元素的个数与满足 $a^m = e$ 成立的最小正整数 n 联系密切,

定义 5.1 设 a 是群 G 中的元素, 若存在最小正整数 n 使得 $a^n = e$,
则称 a 的阶为 n , 否则称 a 是无限阶的,
显然, 群 G 的循环子群 $\langle a \rangle$ 的阶就是元素 a 的阶,

例 5.1 写出四次单位根群中所有元素的阶,

解: 令四次单位根群为 $G = \{1, -1, i, -i\}$,

因为 $1^1 = 1$,

$(-1)^1 \neq 1, (-1)^2 = 1$,

$i^1 = i, i^2 = -1, i^3 = -i, i^4 = 1$,

$(-i)^1 = -i, (-i)^2 = -1, (-i)^3 = i, (-i)^4 = 1$,

所以, 1 的阶为 1 , -1 的阶为 2 , $\pm i$ 的阶为 4 ,

例 5.2 在一般线性群 $GL_2(R)$ 中, 求 $A = \begin{pmatrix} 0 & 1 \\ -1 & 1 \end{pmatrix}$, $B = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ 和 AB 的阶,

解: 计算可知 A^2, A^3, A^4, A^5 都不为 E , 而 $A^6 = E$, 所以 A 的阶是 6 ,

B^2, B^3 都不为 E , 而 $B^4 = E$, 所以 B 的阶是 4 ,

$(AB)^n = \begin{pmatrix} 0 & 1 \\ -1 & 1 \end{pmatrix} \neq E$, 所以 AB 是无限阶的,

关于元素的阶我们有如下简单性质，

命题 5.1 设 a 是群 G 中的元素， a 的阶为 n ，则

(1) $a^k=e \Leftrightarrow n|k$;

(2) 若 G 是有限阶群，则 $n||G|$ 且 $a^{|G|}=e$;

(3) 设 r 是正整数，则 a^r 的阶为 $\frac{n}{(n,r)}$ ，这里 (n,r) 表示 n 和 r 的最大公因数，

证: (1) 若 $a^k=e$ ，则由 $h=nq+r$ ，其中 $0 \leq r < n$ ，

得 $a^r=(a^n)^qa^r=a^{nq+r}=a^k=e$ ，所以 $r=0$ ，

因此， $k=nq$ ， $n|k$ ，若 $n|k$ ，则显然有 $a^k=e$ ，

(2) 根据拉格朗日定理可知， $\langle a \rangle$ 的阶是 G 的阶的因数，

从而 a 的阶是 G 的阶的因数，即 $n||G|$ ，从而 $a^{|G|}=e$ ，

(3) 设 a^r 的阶为 q ，则 $a^{rq}=(a^r)^q=e$ ，从而 $n|rq$ ， $\frac{n}{(n,r)}|q$ ，

再由 $(a^r)^{\frac{n}{(n,r)}}=(a^n)^{\frac{r}{(n,r)}}=e$ 可知， $q|\frac{n}{(n,r)}$ ，于是， $q=\frac{n}{(n,r)}$ ，结论得证，

命题 5.2 设 a, b 是群 G 的阶分别为 n, m 的元素，

若 $(\langle a \rangle \cap \langle b \rangle) = \{e\}$ 且 $ab=ba$ ，则 ab 的阶为 $[n, m]$ ，

这里 $[n, m]$ 表示 n 和 m 的最小公倍数，

证: 设 ab 的阶为 q ，则 $(ab)^q=e$ ，再由 $ab=ba$ 得 $a^qb=e$ ，

从而 $a^q=b^{-q}$ 属于 $(\langle a \rangle \cap \langle b \rangle) = \{e\}$ ，即 $a^q=b^q=e$ ，

故 $n|q, m|q$ ，因此 $[n, m]|q$ ，

而 $(ab)^{[n, m]}=e$ ，因此 $q|[n, m]$ ，

于是 $q=[n, m]$ ，结论得证，

推论 5.2 设 a, b 是群 G 的阶分别为 n, m 的元素，则下列结论成立:

(1) 若 s 是 n 的一个正因数，则 $a^{\frac{n}{s}}$ 的阶为 s ;

(2) 设 r 是正整数，则 a^r 的阶为 $n \Leftrightarrow (n, r)=1$;

(3) 若 $ab=ba$ ，且 $(n, m)=1$ ，则 ab 的阶为 nm ，

利用元素阶的性质，我们可以给出低阶群的分类，

例 5.3 证明素数阶群 G 是循环群，

证： 由于对属于 G 的任意 a , a 的阶是 G 的阶的因数，

故若 $a \neq e$ ，则 a 的阶等于 G 的阶，从而 $G = \langle a \rangle$ 是循环群，

由例 5.3，我们很容易知道，2 阶、3 阶、5 阶群都是循环群，

它们分别同构于 $\{Z_2; +\}$ 、 $\{Z_3; +\}$ 和 $\{Z_5; +\}$ ，

例 5.4 确定所有互不同构的 4 阶群，

解： 若 G 是循环群，则 G 同构于剩余类加法群 Z_4 ，

若 G 不是循环群，根据例 1.8 可知， G 是交换群，

不妨设 $G = \{e, a_1, a_2, a_3\}$ 这里 $a_3 = a_1 a_2 = a_2 a_1$, $a_1^2 = a_2^2 = e$ ，

若 G' 是另一个 4 阶非循环群，则 $G \cong G'$ ，

事实上，设 $G' = \{e', a'_1, a'_2, a'_3\}$ ，这里 $a'_3 = a'_1 a'_2$ ，

若定义映射 $\varphi: G \rightarrow G'$ ，使得 $\varphi(e) = e'$, $\varphi(a_i) = a'_i$ ，则这是一个双射，

且容易验证 φ 保持运算，所以 $G \cong G'$ ，

由此可知所有的 4 阶非循环群都是同构的，它是阶数最小的非循环群，

一般地，称 4 阶非循环群为克莱因四元群，

综上，4 阶群有两类：一类是循环群，一类是克莱因四元群，

下面我们来讨论循环群的生成元及其子群的一些简单性质，

例 5.5 求 Z_{12} 中阶为 12 的元素，

解： 令 $\bar{r} \in Z_{12} = \langle \bar{1} \rangle$ ，

则根据推论 5.2， $\bar{r} = r\bar{1}$ 的阶为 12 的充分必要条件是 $(r, 12) = 1$ ，

所以 Z_{12} 中阶为 12 的元素有 $\bar{1}$ ， $\bar{5}$ ， $\bar{7}$ ， $\bar{11}$ ，

这表明 $\bar{1}$ ， $\bar{5}$ ， $\bar{7}$ ， $\bar{11}$ 都是循环群 Z_{12} 的生成元，

例 5.5 说明，循环群的生成元不是唯一的，
那么，在一个循环群中，怎样的元素才能是生成元呢？其生成元又有多少呢？

命题 5.3(1)在无限循环群 $\langle a \rangle$ 中，恰有两个生成元 a 和 a^{-1} ；

(2)在 n 阶循环群 $\langle a \rangle$ 中， a^r (r 是正整数)是 $\langle a \rangle$ 的生成元 $\Leftrightarrow (n, r)=1$ ，

从而 $\langle a \rangle$ 的生成元的个数为 $\varphi(n)$ ，

这里 $\varphi(n)$ 表示欧拉函数(与 n 互素的且小于 n 的正整数的个数)，

证: (1)设 a^r 是 $\langle a \rangle$ 的生成元，

则 $\langle a \rangle$ 的每个元素(包括 a)可以表为 a^r 的方幂，即存在整数 s 使得 $a=a^{sr}$ ，

又因为 $\langle a \rangle$ 是无限循环群，所以 $sr=1, r=\pm 1$ ，即 $\langle a \rangle$ 中恰有两个生成元 a 和 a^{-1} ，

(2)由推论 5.2 可知， a^r 是 $\langle a \rangle$ 的生成元 $\Leftrightarrow (n, r)=1$ ，

当然，满足 $(n, r)=1 (1 \leq r < n)$ 的 r 的个数恰为欧拉函数 $\varphi(n)$ ，

显然，循环群 $\langle a \rangle$ 的任意元素的所有整数方幂 $\langle a^r \rangle$ 都构成该群的一个循环子群，
那么循环群 $\langle a \rangle$ 的任意一个子群是否是循环子群，且其形式为 $\langle a^r \rangle$ 呢？

定理 5.3 循环群 $\langle a \rangle$ 的子群是循环群，

证: 设 H 是 $\langle a \rangle$ 的子群，

不妨设 $H \neq \{e\}$ ，令 $s = \min\{k \in \mathbb{Z}^+ | a^k \in H\}$ ，则 $H = \langle a^s \rangle$ ，

事实上，若 a^k 属于 H ， $k=qs+r, 0 \leq r < s$ ，则 $a^k = a^{qs+r} = (a^s)^q a^r$ ，即 a^r 属于 H ，

由 s 的定义知道必有 $r=0$ ，即 $k=qs$ ，所以 a^k 属于 $\langle a^s \rangle$ ， H 包含于 $\langle a^s \rangle$ ，

因为 a^s 属于 H ，所以 $\langle a^s \rangle$ 包含于 H ，于是 $H = \langle a^s \rangle$ 是循环群，

显然，有限循环群的元素的阶是有限的，有限循环群的子群是有限循环群，
但在无限循环群中，除单位元以外其他元素的阶都是无限的，
无限循环群的非平凡子群是无限循环群，

定理 5.4 设 $\langle a \rangle$ 是 n 阶循环群，若 r 是 n 的一个正因数，
 则 $\langle a \rangle$ 有唯一一个 r 阶循环子群，

证： 首先 $\langle a \rangle$ 有 r 阶循环子群，例如 $\langle a^{\frac{n}{r}} \rangle$ 就是一个 r 阶循环子群，

其次， r 阶循环子群只有一个，

因若另有 a^k 的阶是 r ，则 $n|kr$ ，即 $\frac{n}{r}|k$ ，所以 a^k 属于 $\langle a^{\frac{n}{r}} \rangle$ ， $\langle a^k \rangle$ 包含于 $\langle a^{\frac{n}{r}} \rangle$ ，

但是 $\langle a^k \rangle$ 和 $\langle a^{\frac{n}{r}} \rangle$ 都是 r 阶群，所以 $\langle a^k \rangle = \langle a^{\frac{n}{r}} \rangle$ ，

推论 5.3(1) 若 $\langle a \rangle$ 是无限循环群，则 $\langle a \rangle$ 的全部子群为 $\{\langle a^s \rangle | s=0, 1, 2, \dots\}$ ；

(2) 若 $\langle a \rangle$ 是 n 阶循环群，则 $\langle a \rangle$ 的全部子群为 $\{\langle a^s \rangle | s \text{ 是 } n \text{ 的正因数}\}$

证：(1) 因为 $\langle a \rangle$ 的子群都是无限循环群且形式为 $\langle a^s \rangle$ ，其中 $s=0, 1, 2, \dots$

若 $\langle a^s \rangle = \langle a^r \rangle$ ，则 a^s 属于 $\langle a^r \rangle$ ，于是存在 k ，使得 $a^s = a^{rk}$ ，

但是 a 是无限阶的，所以 $s=rk, r|s$ ，

同理 $s|r$ ，于是 $s=r$ ，因此 $\langle a \rangle$ 的全部子群为 $\{\langle a^s \rangle | s=0, 1, 2, \dots\}$ ，

(2) 设 H 是 $\langle a \rangle$ 的子群，若 H 的阶为 r ，则由拉格朗日定理知 r 是 n 的正因数，

反之，若 r 是 n 的正因数，由定理 5.4 可知 r 阶循环子群是存在且唯一的，

若 H 是 r 阶循环子群，则 $H = \langle a^{\frac{n}{r}} \rangle$ ，

例 5.6 整数加法群 $Z = \langle 1 \rangle$ 的全部子群为 $\{\langle s \rangle | s=0, 1, 2, \dots\}$ ，

剩余类加法群 $Z_n = \langle \bar{1} \rangle$ 的全部子群为 $\{\langle s\bar{1} \rangle | s \text{ 是 } n \text{ 的正因数}\}$ ，

例 5.7 求 Z_{12} 的全部子群

解： Z_{12} 的全部子群为 $\{\langle s\bar{1} \rangle = \langle \bar{s} \rangle | s=1, 2, 3, 4, 6, 12\}$ ，

即 $\langle \bar{1} \rangle, \langle \bar{2} \rangle, \langle \bar{3} \rangle, \langle \bar{4} \rangle, \langle \bar{6} \rangle, \langle \bar{12} \rangle$