

柯P127.1. 证明: 记群  $(G, \cdot, e)$ , 有  $H_i \subset G (\forall i \in I)$

则  $\forall h_1, h_2 \in \bigcap_{i \in I} H_i$ , 有  $h_1, h_2 \in H_i (\forall i \in I)$

又  $H_i$  是子群, 则  $h_1 h_2^{-1} \in H_i (\forall i \in I)$

即  $h_1 h_2^{-1} \in \bigcap_{i \in I} H_i$ , 则  $\bigcap_{i \in I} H_i$  也是子群.  $\square$

P128.5. 证明: 记  $G$  中单位元  $e$ .

~~令  $a=e, \forall b \in G$ , 方程  $b=x=y$ , 即  $x, y \in G$ .~~

令  $b=e, \forall a \in G$ , 方程  $ax=e, ya=e$

设其唯一解为  $x_0, y_0 \in G$ ,

则  $x_0 = ex_0 = (y_0 a) x_0 = y_0 (ax_0) = y_0 e = y_0$

即  $x_0 a = ax_0 = e, x_0 = a^{-1} \in G$

即  $\forall a \in G, a$  有逆. 则  $G$  是群.  $\square$

P128.15. 证明: 由  $H \subset G, H \neq \emptyset$ , 则  $\exists h \in H, \Rightarrow h \in G$

由  $G$  是有限群,  $\text{ord}(h) < +\infty$ , 设  $k = \text{ord}(h)$

记  $G$  中单位元  $e$ , 则  $h^k = e$ .

由  $H$  乘法封闭,  $h \in H \Rightarrow \dots \Rightarrow h^{k-1} \in H \Rightarrow h^k \in H$ .

即  $h^k = e \in H$ .

又对  $\forall h \in H, h^{k-1} \cdot h = h \cdot h^{k-1} = e, h^{k-1} = h^{-1} \in H$

则  $H$  是子群.  $\square$

2. 解.  $(\mathbb{Z}_{30}, \cdot, 1)$  构成群.  $\mathbb{Z}_{30} = \{0, 1, \dots, 29\}$ .  $\bar{a} \in \mathbb{Z}_n, \bar{a}$  关于乘法可逆  $\Leftrightarrow \gcd(a, n) = 1$

则  $\forall \bar{a} \in \mathbb{Z}_{30}, \bar{a}$  可逆  $\Leftrightarrow \gcd(a, 30) = 1$ .

则可逆元 =  $1, 7, 11, 13, 17, 19, 23, 29$ , 设它们构成集合  $G$ .

下证  $G$  关于乘法构成群.

结合律:  $\forall \bar{a}, \bar{b}, \bar{c} \in G, \overline{a(b \cdot c)} = \overline{abc} = (\overline{a \cdot b}) \bar{c}$ , 成立

单位元:  $1 \in G, \forall \bar{a} \in G, \bar{a} \cdot 1 = 1 \cdot \bar{a} = \bar{a}$ , 成立

可逆元:  $\forall \bar{a} \in G, \gcd(a, 30) = 1, \bar{a}$  必有逆, 成立.

可逆元:  $\forall \bar{a} \in G, \bar{a}$  可逆  $\therefore \exists \bar{b} \in \mathbb{Z}_{30}$   $\bar{a}^{-1}$  也可逆, 则  $\bar{a}^{-1} \in G$

s.t.  $\bar{a} \bar{b} = \bar{b} \bar{a} = 1$  故  $\bar{b}$  可逆  $\therefore \bar{b} \in G$

$G$  对乘法封闭:  $\forall \bar{a}, \bar{b} \in G$ , 则  $\exists \bar{a}^{-1}, \bar{b}^{-1} \in G$ , 若  $\bar{a}, \bar{b}$  可逆, 则  $\bar{a}\bar{b}$  也可逆  
 $(\bar{a}\bar{b})(\bar{b}^{-1}\bar{a}^{-1}) = (\bar{b}^{-1}\bar{a}^{-1})(\bar{a}\bar{b}) = I$ , 即  $\bar{a}\bar{b}$  有逆. 且逆是  $\bar{b}^{-1}\bar{a}^{-1}$

又  $\bar{a}, \bar{b} \in \mathbb{Z}_{30}$ ,  $\bar{a}\bar{b} = \bar{a}\bar{b} \in \mathbb{Z}_{30}$  有逆, 则  $\bar{a}\bar{b} \in G$ , 成立.

综上,  $G$  是群.  $\square$

$\bar{a}\bar{b}$

3. 证明: 由  $\forall x \in G, x^2 = x \cdot x = e$ , 即  $x^{-1} = x \in G$ .

则  $\forall x, y \in G, x \cdot y = x^{-1} \cdot y^{-1} = (yx)^{-1}$ .

又  $yx \in G, yx = (yx)^{-1} = xy$ .

即  $G$  是交换群.  $\square$

4. 证明 (1)  $GL_n(\mathbb{R}) = \{A \in M_n(\mathbb{R}) \mid A \text{ 可逆}\}$ .

同态:  $\forall A, B \in GL_n(\mathbb{R}), \phi(AB) = ((AB)^{-1})^t = (B^{-1}A^{-1})^t = (A^{-1})^t(B^{-1})^t = \phi(A)\phi(B)$ . 即  $\phi$  是同态

单射: 若  $\exists A, B \in GL_n(\mathbb{R})$ , s.t.  $\phi(A) = \phi(B)$ , 即  $(A^{-1})^t = (B^{-1})^t$ ,  
 则  $((A^{-1})^t)^t = ((B^{-1})^t)^t, A^{-1} = B^{-1}, \Rightarrow (A^{-1})^{-1} = (B^{-1})^{-1}$  i.e.  $A = B$   
 又  $A \cdot A^{-1} = A \cdot B^{-1} = E_n$ ,  $E_n$  是单位元  
 则  $(B^{-1})^{-1} = A, B = A$ .  $\phi$  是单射.

满射: 由  $\forall B \in GL_n(\mathbb{R}), B$  可逆,  $\exists A = (B^t)^{-1} \in GL_n(\mathbb{R})$   
 s.t.  $\phi(A) = ((B^t)^{-1})^t = (((B^t)^{-1})^{-1})^t = B$ .  $\phi$  是满射.

则  $\phi$  是同构.  $\square$

(2)  $(G, \cdot, e)$  是群,  $g \in G$ .

同态:  $\forall a, b \in G, \phi_g(ab) = g^{-1}abg = g^{-1}agg^{-1}bg = \phi_g(a)\phi_g(b)$

单射: 若  $\exists a, b \in G$ , s.t.  $\phi_g(a) = \phi_g(b)$ ,  $g^{-1}ag = g^{-1}bg$ ,

由  $g \in G, \exists g^{-1} \in G, gg^{-1}agg^{-1} = gg^{-1}bgg^{-1}, a = b$ .

满射:  $\forall b \in G, \exists a = gbq^{-1} \in G$ , s.t.  $\phi_g(a) = g^{-1}gbq^{-1}g = b$

则  $\phi_g$  是同构.  $\square$

# 群

群:  $G$  集合.

(G0) 封闭性:  $\forall a, b \in G, a \cdot b \in G$ . ( $\cdot$  是  $G$  上二元运算)

(G1) 结合律:  $\forall a, b, c \in G, (a \cdot b) \cdot c = a \cdot (b \cdot c)$

(G2) 单位元:  $\exists e \in G$  s.t.  $\forall a \in G, a \cdot e = e \cdot a = a$ .

(G3) 逆元:  $\forall a \in G, \exists b_a \in G$  s.t.  $a \cdot b_a = b_a \cdot a = e$ .

群  
含么群  
群

交换群:  $\forall a, b \in G, a \cdot b = b \cdot a$

子群:  $(G, \cdot, e)$  群,  $H \subset G$ , 若  $(H, \cdot, e)$  也是群, 则称  $H$  是  $G$  子群, 记为  $H \leq G$

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

同态:  $\varphi: (G, \cdot, e) \rightarrow (H, *, \varepsilon)$  满足  $\forall a, b \in G, \varphi(a \cdot b) = \varphi(a) * \varphi(b)$ .

同构:  $\varphi$  同构 =  $\varphi$  同态 +  $\varphi$  双射, 记为  $G \cong H$

嵌入:  $\varphi: (G, \cdot, e) \rightarrow (H, *, \varepsilon)$  单同态. 称  $\varphi$  把  $G$  嵌入到  $H$  中.  $G \cong \text{im}(\varphi)$

命题:  $\varphi: (G, \cdot, e) \rightarrow (H, *, \varepsilon)$  群同态, 则  $\text{im}(\varphi) \leq H, \ker(\varphi) \leq G$ .

其中  $\ker(\varphi) := \{a \in G \mid \varphi(a) = \varepsilon\}$

证: 课本已证  $\text{im}(\varphi) \leq H$ . 下证  $\ker(\varphi) \leq G$ .

$\forall a, b \in \ker(\varphi), \varphi(a) = \varphi(b) = \varepsilon$ , 且  $\varphi(b^{-1}) = \varphi(b)^{-1} = \varepsilon$

$\therefore \varphi(ab^{-1}) = \varphi(a) * \varphi(b^{-1}) = \varphi(a) * \varphi(b)^{-1} = \varepsilon * \varepsilon = \varepsilon$

$\Rightarrow ab^{-1} \in \ker(\varphi) \therefore \ker(\varphi) \leq G$ .

注:  $\varphi$  是单同态 (或嵌入)  $\Leftrightarrow \ker(\varphi) = \{e\}$ . (讲义上引理 2.47)

Lagrange 定理: 设  $G$  是有限群,  $H \leq G$ , 则  $\text{card}(H) \mid \text{card}(G)$

Cor1. 设  $G$  是有限群,  $\forall a \in G, \text{ord}(a) \mid \text{card}(G)$

Cor2. 设  $G$  是有限群,  $\forall a \in G, a^{\text{card}(G)} = e$ .

记号:  $G$  中元素个数 (群的基数) 记为  $\text{card}(G)$  或  $|G|$ .

注：一般 Lagrange 定理的逆命题不成立。

即对  $|G|$  的一个因子  $d$ ，不一定有一个子群  $H$  s.t.  $|H|=d$ .

但如果  $G$  是循环群且有限，该命题成立且  $\forall d \mid |G|, \exists! H \leq G$  s.t.  $|H|=d$ .

群的生成元：

$$\langle S \rangle = \{x_1^{e_1} \dots x_m^{e_m} \mid x_i \in S, e_i \in \mathbb{Z}, m \in \mathbb{Z}^+\} \quad \left( x^n = \begin{cases} \underbrace{x \dots x}_{n \uparrow}, & n > 0 \\ e, & n = 0 \\ \underbrace{x^{-1} \dots x^{-1}}_{-n \uparrow}, & n < 0 \end{cases} \right)$$

$G$  是群  $\Phi S \subset G$ ，若  $G = \langle S \rangle$ ，则称  $S$  是  $G$  的一组生成元。

若  $S$  是有限集，称  $G$  是有限生成的。

注：有限群一定是有限生成的，生成元取所有元素即可。

有限生成的群不一定是有限群，例  $\mathbb{Z} = \langle 1 \rangle = \langle -1 \rangle$  有限生成的。  
不是有限群。

prop:  $G$  群,  $\emptyset \neq S \subset G, H \leq G$ . 则  $S \subset H \Rightarrow \langle S \rangle \subset H$

阶:  $(G, \cdot, e)$  群,  $g \in G$ .

若  $\exists n \in \mathbb{Z}^+$  s.t.  $g^n = e$ ，称  $g$  是有限阶。满足 (\*) 的最小正整数称为  $g$  的阶  
记为  $\text{ord}(g)$ 。

否则称为无限阶

prop:  $(G, \cdot, e)$  群,  $g \in G$ .

(1) 若  $\text{ord}(g) = \infty$ ，则  $\forall i, j \in \mathbb{Z}, g^i = g^j \Leftrightarrow i = j$

(2) 若  $\text{ord}(g) = k < \infty$ ，则  $\forall i, j \in \mathbb{Z}, g^i = g^j \Leftrightarrow k \mid i - j$ 。特别地， $g^m = e \Leftrightarrow k \mid m$

prop 1: 设  $\varphi: (G, \cdot, e) \rightarrow (G', *, e')$  群同态。若  $a^n = e$  ( $n \in \mathbb{Z}$ ) 则  $\text{ord}(\varphi(a)) \mid n$ 。

特别地， $\text{ord}(\varphi(a)) \mid \text{ord}(a)$ 。

若  $\varphi$  是同构，则  $\text{ord}(\varphi(a)) = \text{ord}(a)$ 。

证:  $n=0$ , 自然成立.

设  $n>0$ ,  $a^n = \underbrace{a \cdots a}_n = e$ .  
若

$$\Rightarrow e = \varphi(e) = \varphi(a^n) = \varphi(\underbrace{a \cdots a}_n) = \underbrace{\varphi(a) \cdots \varphi(a)}_n = \varphi(a)^n.$$

$$\Rightarrow \text{ord}(\varphi(a)) \mid n.$$

若  $n<0$ ,  $a^n = \underbrace{a^{-1} \cdots a^{-1}}_{-n} = e$ .

$$\Rightarrow e = \varphi(e) = \varphi(a^n) = \varphi(\underbrace{a^{-1} \cdots a^{-1}}_{-n}) = \underbrace{\varphi(a^{-1}) \cdots \varphi(a^{-1})}_{-n} = \varphi(a^{-1})^{-n} = \varphi(a)^n$$

$\downarrow$   
 $\varphi(a^{-1}) = \varphi(a)^{-1}$

$$\Rightarrow \varphi(a)^{-n} = e. \therefore \text{ord}(\varphi(a)) \mid -n \quad \text{且} \quad \text{ord}(\varphi(a)) \mid n.$$

特别地, 当  $n = \text{ord}(a)$  时, 有  $\text{ord}(\varphi(a)) \mid \text{ord}(a)$ .

若  $\varphi$  是同构, 则  $\varphi^{-1}$  也是群同构.  $\varphi: G \rightarrow H, \varphi^{-1}: H \rightarrow G$

$$a \mapsto \varphi(a) \quad \varphi(a) \mapsto a = \varphi^{-1}(\varphi(a))$$

由上述结论可知:  $\text{ord}(\varphi(a)) \mid \text{ord}(a), \text{ord}(\varphi^{-1}(\varphi(a))) \mid \text{ord}(\varphi(a))$   
 $\quad \quad \quad \parallel$   
 $\quad \quad \quad \text{ord}(a)$

$$\Rightarrow \text{ord}(\varphi(a)) = \text{ord}(a)$$

prop 2:  $(G, \cdot, e)$  群,  $a \in G, \text{ord}(a) = n$ . 则  $\forall k \in \mathbb{Z}, a^k \in G$  且  $\text{ord}(a^k)$

(1) 若  $\text{ord}(a) = \infty$ , 则  $\text{ord}(a^k) = \infty$ .

(2) 若  $\text{ord}(a) = n < \infty$ , 则  $\text{ord}(a^k) = \frac{n}{\gcd(n, k)}$

证: (1) (反证法) 若  $\text{ord}(a^k) = s < \infty$ , 则  $(a^k)^s = a^{ks} = e \Rightarrow a$  是有限阶的, 矛盾.  $\therefore \text{ord}(a^k) = \infty$ .

(2) 令  $d = \gcd(n, k), n = \tilde{n}d, k = \tilde{k}d, \text{ord}(a^k) = \tilde{n}$   
 $\quad \quad \quad \text{gcd}(\tilde{n}, \tilde{k}) = 1$

$$\text{首先, } (a^k)^{\tilde{n}} = a^{k\tilde{n}} = a^{\tilde{k}d\tilde{n}} = a^{\tilde{k}n} = (a^n)^{\tilde{k}} = e^{\tilde{k}} = e \Rightarrow \text{ord}(a^k) \mid \tilde{n}$$

$$\text{其次, } \forall l \in \mathbb{Z}^+ \text{ s.t. } (a^k)^l = e \Rightarrow n \mid kl \Rightarrow \tilde{n} \mid \tilde{k}l \Rightarrow \tilde{n} \mid l$$

即  $\tilde{n}$  是满足  $(a^k)^l = e$  的最小正整数.

$$\downarrow$$

$$\text{gcd}(\tilde{n}, \tilde{k}) = 1$$

$$\therefore \text{ord}(a^k) = \tilde{n}$$

注：上述命题证明过程中用到了广义结合律： $G$  群， $x \in G$

$$\forall m, n \in \mathbb{Z}, (x^m)(x^n) = x^{m+n}, (x^m)^n = x^{mn}$$

Cor: 若  $a \in G$  且  $\text{ord}(a) = n$ ,  $\gcd(n, k) = 1 \Rightarrow \text{ord}(a^k) = n$ . 特别地  $\text{ord}(a^{-1}) = n$ .

eg:  $(\mathbb{Z}_n, +, 0)$   $n$  阶循环群且  $\mathbb{Z}_n = \langle 1 \rangle$ ,  $\text{ord}(1) = n$ .

$\forall k \in \mathbb{Z}$ , 若  $\gcd(k, n) = 1$ , 则  $\text{ord}(k) = n$ . ( $k = k \cdot 1$ ) 且

$\mathbb{Z}_n = \langle 1 \rangle = \langle k \rangle$ .  $\gcd(k, n) = 1$   $\mathbb{Z}_n$  中所有  $n$  阶元都是生成元.

~~也是~~  $\mathbb{Z}_n$  中关于乘法的可逆元

事实上:  $\gcd(k, n) = 1 \Leftrightarrow k$  是乘法可逆元  $\Leftrightarrow k$  是  $\mathbb{Z}_n$  的生成元.  
循环群  
(or  $k$  是  $n$  阶元)

循环群:

由一元素生成的群称为循环群.

分类: 设  $(G, \cdot, e)$  是循环群,  $|G| > 1$ .

(1) 若  $|G| = \infty$ , 则  $G \cong (\mathbb{Z}, +, 0)$

(2) 若  $|G| = n$ , 则  $G \cong (\mathbb{Z}_n, +, 0)$

注: 任意两个同阶的循环群是同构的 (特别地, 任意两个无限循环群是同构的)

Prop 3: (循环群的子群是循环群).

$H \leq G = \langle a \rangle$ , 则  $\exists k \in \mathbb{Z}_0$  s.t.  $H = \langle a^k \rangle$ .

Pf: 若  $H = \{e\}$ , 则  $H = \langle a^0 \rangle$ . 下面假设  $H \neq \{e\}$ .

$\forall x \in H, x \neq e$ , 则  $\exists m \in \mathbb{Z} \setminus \{0\}$ , s.t.  $x = a^m$

不妨设  $a^k \in H$  且  $k$  为最小正整数, 显然  $\langle a^k \rangle \subset H$ .

另一方面,  $\forall a^m \in H$ , 带余除法  $m = qk + r$ ,  $r \in \{0, 1, \dots, k-1\}$ ,  $q \in \mathbb{Z}$

$\therefore a^m, a^k \in H, \therefore a^r = a^{m-qk} = a^m \cdot (a^k)^{-q} \in H$ .

由  $k$  的最小性  $\Rightarrow r = 0 \therefore a^m = (a^k)^q \in \langle a^k \rangle \therefore \langle a^k \rangle = H$

prop 4: (无限循环群的非  $\{e\}$  子群都  $\cong \mathbb{Z}$  同构).

$$H \leq G = \langle a \rangle, |G| = \infty, H \neq \{e\}. \text{ 则 } H \cong G.$$

Pf: 由前面命题可知  $\exists k \in \mathbb{Z}^+$  s.t.  $H = \langle a^k \rangle$ . 由子  $\text{ord}(a) = \infty \xRightarrow{\text{prop 2}} \text{ord}(a^k) = \infty$   
 $\therefore |H| = \infty$ . 故  $H \cong (\mathbb{Z}, +, 0)$ . 又  $G \cong (\mathbb{Z}, +, 0) \therefore G \cong H$ .

Thm: 设  $G = \langle a \rangle$  是循环群, 则.

(1) 若  $|G| = n$ , 则  $\forall k \in \mathbb{Z}^+, k | n, \exists! H \leq G$  s.t.  $|H| = k$  且  $H = \langle a^{\frac{n}{k}} \rangle$

(2) 若  $|G| = \infty$ , 则  $G$  有无穷多子群.

Pf: (1)  $|G| = n, k | n$ . 设  $n = kl$  由 prop 2 可知  $\text{ord}(a^l) = \frac{n}{\gcd(n, l)} = \frac{n}{l} = k$

$\therefore \langle a^{\frac{n}{k}} \rangle$  是  $G$  的  $k$  阶子群.

设  $H \leq G$  且  $|H| = k$ , 由 prop 3,  $\exists m \in \mathbb{N}$  s.t.  $H = \langle a^m \rangle$

$$\text{则 } |H| = \text{ord}(a^m) = \frac{n}{\gcd(n, m)} = k \Rightarrow \gcd(n, m) = \frac{n}{k}$$

$\downarrow$  prop 2                       $\downarrow \because |H| = k$

由 Bezout's 关系,  $\exists l_1, l_2 \in \mathbb{Z}$ , s.t.  $ml_1 + nl_2 = \frac{n}{k}$

$$\therefore a^{\frac{n}{k}} = (a^m)^{l_1} \cdot (a^n)^{l_2} = (a^m)^{l_1} \in \langle a^m \rangle = H \Rightarrow \langle a^{\frac{n}{k}} \rangle \subset H$$

$\downarrow$   
 $\text{ord}(a) = n$

又  $|\langle a^{\frac{n}{k}} \rangle| = |H| = k \therefore \langle a^{\frac{n}{k}} \rangle = H$ . 唯一性得证.

(2)  $|G| = \infty, \{e\}, \langle a \rangle, \langle a^2 \rangle, \dots$  是  $G$  的不同子群且  $\langle a^k \rangle \cong (\mathbb{Z}, +, 0) \quad k \geq 1$ .

注:  $\text{ord}(a^k) = \infty, k \geq 1$ . (prop 2)

Cor: 设  $G$  是  $n$  阶循环群. 则

(1) 若  $n = 1$ , 则  $G$  仅有唯一子群  $G$ .

(2) 若  $n > 1, n = p_1^{k_1} \cdots p_s^{k_s}$  标准素分解, 则  $G$  有  $T(n) = \prod_{i=1}^s (k_i + 1)$  个子群.  
 ( $p_1, \dots, p_s$  素数, 两两不同)  
 ( $k_1, \dots, k_s \in \mathbb{Z}^+$ )

eg: 求  $(\mathbb{Z}_{12}, +, 0)$  中所有元素的阶和所有子群.

①  $\forall k \in \mathbb{Z}_{12}, \text{ord}(k) = \frac{n}{\gcd(n, k)} \quad (\text{已知 } \text{ord}(1) = 12, \mathbb{Z}_{12} = \langle 1 \rangle)$

$$= \frac{12}{\gcd(12, k)}$$

由此公式可得:

$$\text{ord}(\bar{2}) = \frac{12}{2} = 6, \text{ord}(\bar{3}) = \frac{12}{3} = 4, \text{ord}(\bar{4}) = \frac{12}{4} = 3$$

$$\text{ord}(\bar{5}) = \frac{12}{1} = 12, \dots$$

| $k$             | $\bar{0}$ | $\bar{1}$ | $\bar{2}$ | $\bar{3}$ | $\bar{4}$ | $\bar{5}$ | $\bar{6}$ | $\bar{7}$ | $\bar{8}$ | $\bar{9}$ | $\bar{10}$ | $\bar{11}$ | $r$ |
|-----------------|-----------|-----------|-----------|-----------|-----------|-----------|-----------|-----------|-----------|-----------|------------|------------|-----|
| $\text{ord}(k)$ | 1         | 12        | 6         | 4         | 3         | 12        | 2         | 12        | 3         | 4         | 6          | 12         |     |

② 所有子群.

已知  $\forall d | 12, \mathbb{Z}_{12}$  有唯一  $d$  阶子群. 找  $\mathbb{Z}_{12}$  的  $d$  阶元, 其生成的群即为  $d$  阶子群.

$$d = 1, 2, 3, 4, 6, 12$$

$$d=1: \langle \bar{0} \rangle = \{\bar{0}\}$$

$$d=2: \langle \bar{6} \rangle = \{\bar{0}, \bar{6}\}$$

$$d=3: \langle \bar{4} \rangle = \langle \bar{8} \rangle = \{\bar{0}, \bar{4}, \bar{8}\}$$

$$d=4: \langle \bar{3} \rangle = \langle \bar{9} \rangle = \{\bar{0}, \bar{3}, \bar{6}, \bar{9}\}$$

$$d=6: \langle \bar{2} \rangle = \langle \bar{10} \rangle = \{\bar{0}, \bar{2}, \bar{4}, \bar{6}, \bar{8}, \bar{10}\}$$

$$d=12: \langle \bar{1} \rangle = \langle \bar{5} \rangle = \langle \bar{7} \rangle = \langle \bar{11} \rangle = \mathbb{Z}_{12}$$