循环群：群 G 是循环群，若 $\exists\, a\in G$ s.t. $G=\langle a\rangle=\{a^k\cdot(a^{-1})^s \mid k\geq 0,\ s\geq 0\}$ （$\langle a\rangle$ 表示：G 被由 a 生成）

$=\{a^t \mid t\in\mathbb{Z}\}$

注 若 $G=G_a$，则称 $\langle G,*\rangle$ 为循环群

eg: $\langle\mathbb{Z},+\rangle$ 生成元 ± 1

$\langle\mathbb{Q},+\rangle$ 不是

$\langle\mathbb{Q}\setminus\{0\},\times\rangle$ 不是

$\langle 1\text{的}n\text{次单位根},\times\rangle$ 是循环群 生成元 $e^{\pm i\frac{2\pi}{n}k}$ $(k,n)=1$

循环群生成元是否唯一？ Nope. 不唯一.

i) $\langle 1\text{的}n\text{次单位根},\times\rangle$ 生成元 $e^{\pm\frac{2\pi}{n}\cdot k}$，只须 $\exists\, b$ s.t. $bk\equiv 1 \bmod n$

$\Leftarrow (k,n)=1$ 即可

$\Rightarrow$ 其生成元有 $\varphi(n)$ 个

ii) $\langle\mathbb{Z}_m,+\rangle$ （$\mathbb{Z}_m=\{0,1,2,\cdots m-1\}$ 为模 m 的完全剩余系）

$a\in\mathbb{Z}_m$ 为生成元 $\Leftrightarrow \forall\, b\in\mathbb{Z}_m.\ \exists\, k\in\mathbb{Z}$ s.t. $ka\equiv b \bmod m$

$\Leftrightarrow \exists\, k\in\mathbb{Z}$ s.t. $ka\equiv 1 \bmod m$

$\Leftrightarrow (a,m)=1$

$\langle\mathbb{Z}_m,+\rangle$ 的生成元有 $\varphi(m)$ 个

那 $\langle\mathbb{Z}_n,\times\rangle$，模 m 的乘法群的性质呢？

结论：$\forall$ 有限循环群 G_m，G_m 中有 $\varphi(m)$ 个生成元

$\forall$ 无限循环群 G，G 中只有两个生成元 $\langle a\rangle,\langle a^{-1}\rangle$

引入群同构来证明

群同构：分两个群 $\langle G_1, *_1\rangle \cong \langle G_2, *_2\rangle$，若存在映射 $f: G_1 \to G_2$ 为一一映射

$f: \forall a, b \in G_1,\ f(a), f(b) \in G_2$ 且 $f(a *_1 b) = f(a) *_2 f(b)$

eg: $\langle Z_n, +\rangle$ 与 $\langle$ 1的n次单位根, $\times\rangle$ 同构.

取 $f: k \to e^{\frac{2\pi i}{n}\cdot k}$

则 $f(k_1+k_2) = e^{\frac{2\pi i}{n}(k_1+k_2)} = e^{\frac{2\pi i}{n}k_1} \cdot e^{\frac{2\pi i}{n}k_2} = f(k_1)\cdot f(k_2)$

够么？

群同构的主要性质

1. 同构映射保持单位元

e_1 为 G_1 单位元，e_2 为 G_2 单位元. 则 $f(e_1) = e_2$

$\forall a \in G_1,\ e_1 *_1 a = a$

则 $\begin{cases} f(e_1 *_1 a) = f(a) = f(e_1) *_2 f(a) \\ f(a *_1 e_1) = f(a) = f(a) *_2 f(e_2) \end{cases}$

由单位元定义. $f(e_1)$ 为 G_2 中单位元 则 $f(e_1) = e_2$

$A\ A^2 = A \not\Rightarrow A = 1$.

eg: $A = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$

2.1 无限循环群同构于 $\langle Z, +\rangle$

$G = \langle a, *\rangle = \{a^k \mid k \in Z\}$ 其中 $a^0 = e$. a^{-1} 为 a 的逆

def: $f: \langle Z, +\rangle \to G$. $\forall k \in Z,\ f(k) = a^k$

f 显然为一一映射

$\forall i, j \in Z$ 有 $f(i+j) = a^{i+j} = a^i * a^j = f(i) * f(j)$

则无限循环群 G_a 与 $\langle Z, +\rangle$ 同构

2.2 G的生成元个数与Z的生成元一一对应，仅有两个 $f(1) = a$，$f(-1) = a^{-1}$

反证：设 $\exists b \in G \setminus \{a, a^{-1}\}$，$b = a^k$ 也为 G 的生成元

则 $G = \{(a^k)^j \mid j \in Z\}$

$f^{-1}(G) = \{k\ \ 2k\ \ 3k \cdots$

$\quad -k\ \ -2k\ \ -3k \cdots\}$ $= Z$，$k \neq \pm 1$ 显然矛盾.

or: a^k 为 G 的生成元. 则 $\exists m$ s.t. $a = (a^k)^m \Rightarrow f^{-1}(a^{km}) = km = f^{-1}(a) = 1$

$\Rightarrow k \mid 1$ 与 $k \neq \pm 1$ 矛盾.

3.1 任意m阶有限循环群均同构于$\langle \mathbb{Z}_m, + \rangle$

记 $G = \langle a, * \rangle = \langle \{e, a^1, a^2, \cdots a^{m-1}\}, * \rangle$

先证 G 与 $\mathbb{Z}_m$ 之间存在一一映射　　$a^r \equiv 1 \mod m$

a 为 G 的生成元. $\exists$ 最小正整数 r s.t. $a^r = e$ 则 $r = m$

否则 G 的阶为 m ($r < m$. 则 $a^{m+1} = a^r * a = a$ 已回归. $|G| < m$, $r > m$ 同理)

同时构建 $f: \mathbb{Z}_m \to G$., $\forall k \in \mathbb{Z}$, $f(k) = a^k \in G$. f 为一一映射

$\forall i, j \in \mathbb{Z}$, $f(i+j) = a^{i+j} = a^i * a^j = f(i) * f(j)$ 则同构.

3.2 $\langle G_m, * \rangle$ 的生成元个数与 $\langle \mathbb{Z}_m, + \rangle$ 生成元个数相等, 均为 $\varphi(m)$

证: 在 $\mathbb{Z}_m$ 中取生成元 k 则 $(k, m) = 1$.

先证 $f(k) = a^k \in G$ 为 G 的生成元.

由 $(k, m) = 1$ 则 $\forall i \in \mathbb{Z}_m$ $\exists b \in \mathbb{Z}$ $bk \equiv i \mod m$

则 $f(i) = f(\underbrace{k + k + \cdots + k}_{b\text{个}}) = f(k) * f(k) \cdots * f(k) = (a^k)^b$　　(注: 加法在 mod m 下进行)

则 $\forall a^i \in G$. $\exists b \in \mathbb{Z}$ 有 $a^{kb} = a^i$ 故 a^k 是 G 的生成元

再证 除 $a^k [(k, m) = 1]$ 以外, $\langle G_m, + \rangle$ 无其余生成元

设 $\exists k$ 满足 $(k, m) \neq 1$ s.t. a^k 仍为 G_m 生成元

则 $\forall a^i \in G_m$, $\exists b \in \mathbb{Z}$. s.t $(a^k)^b = a^i$ 则 $kb \equiv i \mod m$. $\forall i \in \mathbb{Z}$

则 $(k, m) = 1$. 矛盾

4. 同构保持生成元 / 同构的两群间的映射为同构映射 $\Longleftrightarrow$ 生成元一一对应

证: $G_m = \{e, a^1, a^2, \cdots, a^{m-1}\}$, 考虑 $\langle G_m, * \rangle$ 与 $\langle \mathbb{Z}_m, + \rangle$ 之间的映射

$\forall a \in G_m$ 为生成元, 有 $a^m = e$

记 $f: G_m \to \mathbb{Z}_m$. $f(e) = 0$ $f(a) = b$ $f(a^2) = 2b$ $\cdots$

则 $\mathbb{Z}_m = \{0, b, 2b, \cdots (m-1)b\}$

其中 $jb = lm + (m-1)b$

故 $\forall j \in \{0, 1, \cdots m-1\}$ $\exists i \in \mathbb{Z}$ s.t $ib \equiv j \mod m$

即 $(b, m) = 1 \Rightarrow b$ 为 $\langle \mathbb{Z}_m, + \rangle$ 的生成元

由4) $\langle G_m, * \rangle \longleftrightarrow \langle Z_m, + \rangle$ 的映射，本质上可以看成 $\langle Z_m, + \rangle \longleftrightarrow \langle Z_m, + \rangle$ 的映射

记 $\langle Z_m, + \rangle \longleftrightarrow \langle Z_m, + \rangle$ 的所有映射：$\{f_{p_1}, f_{p_2}, \cdots f_{p_{\varphi(m)}}\}$

$f_{p_k}(1) = p_k$，$(p_k, m) = 1$，$1 \le k \le \varphi(m)$

故假设 f_a 为 $\langle Z_m, + \rangle \longleftrightarrow \langle Z_m, + \rangle$ 的一种同构映射，f_b 为另一种同构映射。

则 $f_a \circ f_b$ 也是一种同构映射

记 $A(\langle Z_m, + \rangle) = \{f : \langle Z_m, + \rangle \longleftrightarrow \langle Z_m, + \rangle$ 同构映射$\}$

$f_a \circ f_b = f_{ab} \in A$　$(a, m) = 1$，$(b, m) = 1 \Rightarrow (ab, m) = 1$

$\Rightarrow \langle A(\langle Z_m, + \rangle), \circ \rangle$ 成群，且与 $\langle Z_m^*, \times \rangle$ 同构

δ_1：$1 \to 1$，$2 \to 2$，… 则 $f(\delta_1) = 1$

δ_i：$1 \to a$，$(a, m) = 1$　$f(\delta_i) = a$

$2 \to 2a$

$\vdots$

$m-1 \to m-1a$

乘法可视作加法运算的自同构