有限群：元素个数有限个的群

阶：有限群中元素个数

eg：$\langle Z_m, + \rangle$

$\langle Z_m^*, \times \rangle$ $\forall a \in Z_m^*, (a, m) = 1$. $a^{\varphi(m)} \equiv 1 \bmod m$, $|G| = \varphi(m)$是一个阶

推广：一般的有限群：$\forall a \in G, a^x \equiv 1_G \bmod m$是否一定有解？

直接暴力 or 找a^{x_1}, a^{x_2}. $a^{x_1} = a^{x_2} \Rightarrow a^{x_2 - x_1} = 1_G$

（从群阶之有限和幂次之无穷）

有阶

$\forall a \in G$. 取$a^1, a^2, \cdots a^k, a^{k+1}, \in G$

$|G| = k \Rightarrow \exists i < j$ s.t $a^i = a^j \Rightarrow a^{j-i} = 1_G$

$|G|$是否为解？ 首先 $i, j \in \{1, 2 \cdots k+1\}$. $j - i \le k$.

设$a^r \equiv 1_G$，r为最小的正数解. 证 $r \mid k$，则所有解.

反证：$r \nmid k$. $k = tr + r'$, $0 < r' < r$. $\Rightarrow a^k = 1_G$. $a^r = 1_G$. $\Rightarrow a^{k-tr} = 1_G = a^{r'}$

与r是最小正整数解矛盾

并给：$H = \{a^1, a^2, a^3, \cdots a^r\}$ $|H| = r$ 是一个子群.

Lagrange定理：对于$\forall$有限群G，对G的任意子群H. 有 $|H| \mid |G|$

陪集分解.

取 $b_1 \in G \setminus H$. 考虑 $b_1 H = \{b_1 a^1, b_1 a^2, \cdots b_1 a^r\}$

证 $b_1 H$中任两个元素互不相等：反证+消去律即可

$|b_1 H| = |H|$

再证 $b_1 H \cap H = \phi$. 反证法假设不为空

$\exists a^{x_1} = b_1 a^{x_2} \Rightarrow b_1 = a^{x_1} (a^{x_2})^{-1} \in H$矛盾

如此往下去，找 b_2、b_3 $\cdots$ 不属于前几个集合. 直有限步可以做完（G有限）

最终：$\begin{cases} H, b_1 H, b_2 H, b_3 H \cdots \text{两两之为空，所均为} |H| \\ \bigcup b_i H = G \end{cases}$

$\Rightarrow |H| \mid |G|$ 引上面的命题得证了

$a^r = 1_G$中，最小的r称为a的阶

G未必有限 再推广：子群 $H \subset G$，作左陪集分解

则 $G = H \cup b_1H \cup b_2H \cup \cdots \cup b_kH$

再假设 G是交换群(Abel群)

def $M = \{bH, b_1H, b_2H, \cdots b_kH\}$

def $*$: $b_iH * b_jH = cH$ $b_i * b_j \in cH$

两个陪集中元素运算应会全落在M中一个陪集中

且陪集间运算可以直接视作代表元间运算

M是一个群，称 G/H 的商群

群的陪集分解：$\forall$ 群 G，关于G的 $\forall$ 子群 $H \subseteq G$

$$G = \bigcup_a a_iH \quad \text{左陪集} \quad (\text{约定 } a_0H = H)$$
$$= \bigcup_b Hb_i \quad \text{右陪集} \quad (Hb_0 = H)$$

特别地：若子交换群 $G = \bigcup_a a_iH = \bigcup_a Ha_i$ $a_0H = Ha_0 = H$

$\langle a_i \rangle * \langle a_j \rangle = \langle a_i \times a_j \rangle$，$G/H$ 商群

eg: $\langle \mathbb{Z}, + \rangle \supset \langle m\mathbb{Z}, + \rangle$

$m\mathbb{Z}$, $1+m\mathbb{Z}$, $2+m\mathbb{Z}$ $\cdots$ $m-1+m\mathbb{Z}$

$\langle 0 \rangle$ $\langle 1 \rangle$ $\langle 2 \rangle$ $\cdots$ $\langle m-1 \rangle$

$\Longleftrightarrow$ $+ \bmod m$ $\langle \mathbb{Z}, + \rangle / \langle m\mathbb{Z}, + \rangle$ 同构于 $\langle \mathbb{Z}_m, + \rangle$

特别地：若有限群 G，$\forall$ 子群 $H \subseteq G$，$|H| \mid |G|$

有限群 G，$\forall a \in G$，$a^{|G|} = 1_G$

陪集分解有什么用？