Lec6 Note of Abstract Algebra

Xuxuayame

日期：2023 年 3 月 29 日

推论. *(Fermat 小定理)*：设 p 素，则

$$a^p \equiv a \mod p, \forall\, a \in \mathbb{Z}.$$

评论. n 为正整数，则 $(a,n)=1 \Rightarrow a^{\varphi(n)}=1 \mod n$。

推论. 素数阶群必为循环群。

证明. 对 $\forall\, G \ni g \neq 1$，$\mathrm{ord} g \mid |G|=p \Rightarrow \mathrm{ord} g = 1$ 或 $p \Rightarrow \mathrm{ord} g = p$，即 $|\langle g\rangle| = |G| \Rightarrow \langle g\rangle = G$。 □

命题 3.8. 非 *Abel* 群最小阶为六。

证明. $2,3,5$ 阶为循环群。

存在 6 阶非 Abel 群 S_3。

当 $|G|=4$ 时，若存在 $g \in G$，使得 $\mathrm{ord}(g)=4$，则 G 为循环群，故交换。或者 $\forall\, g \in G,\ g^2=1$，从而 G 为 Abel 群。 □

命题 3.9. 设 $G=\langle g\rangle$ 为循环群，$|G|=n$，则 $\forall\, 1 \leq d \mid n$，存在唯一的一个 d 阶子群 $G_d=\{1, g^{\frac{n}{d}}, \cdots, g^{\frac{n}{d}(d-1)}\}=\{x \in G \mid x^d=1\}$。特别地，$G$ 的任一子群均为循环群。

证明. 存在性显然，验证即可。

现证唯一性，设 $x=g^i,\ (g^i)^d=1 \Rightarrow n \mid id \Rightarrow \frac{n}{d} \mid i$，于是对任意 $H \leq G,\ |H|=d$，$\forall\, h \in H,\ h^d=1 \Rightarrow h \in G_d \Rightarrow H \subset G_d$，而 $|H|=|G_d|=d$，所以 $H=G_d$。 □

推论. 对 $n \in \mathbb{Z}_+$，

$$n=\sum_{1 \leq d \mid n} \varphi(d).$$

证明. $|\mathbb{Z}/n\mathbb{Z}|$ 中 d 阶元有 $\varphi(d)$ 个，d 阶元恰为 G_d 的所有生成元。

$$\begin{aligned}\mathbb{Z}/n\mathbb{Z} &= \bigsqcup_{1 \leq d \mid n} \{g \in G \mid \mathrm{ord}(g)=d\} \\ \Rightarrow n &= |\mathbb{Z}/n\mathbb{Z}| = \sum_{1 \leq d \mid n} \varphi(d).\end{aligned}$$

□

定理 3.10. $H \le M \le G$，则
$$[G:H] < \infty \Rightarrow [G:M] < \infty,\ [M:H] < \infty.$$
且此时 $[G:H] = [G:M] \cdot [M:H]$。

证明. $G = \bigsqcup\limits_{i \in I} y_i M$，$\{y_i\}_{i \in I}$ 为左陪集代表元系；$M = \bigsqcup\limits_{j \in J} x_j H$，$\{x_j\}_{j \in J}$ 为左陪集代表元系。于是
$$G = \bigsqcup_{i \in I} y_i M = \bigsqcup_{i \in I} \bigsqcup_{j \in J} y_i x_j H = \bigsqcup_{i \in I, j \in J} y_i x_j H.$$
于是 $\{y_i x_j\}_{i \in I, j \in J}$ 为左陪集代表元系。 □

命题 3.11. $|G| < \infty$, $A, B \le G$，则

(1) $|AB| = |A| \cdot |B| / |A \cap B|$；

(2) $[G : A \cap B] \le [G:A][G:B]$，若 $([G:A],[G:B]) = 1$，则 $[G : A \cap B] = [G:A][G:B]$。

这里 $AB = \{ab \mid a \in A,\ b \in B\} = \bigcup_{b \in B} Ab$。

证明. (1) 只需证 $|AB|/|A| = |B|/|A \cap B|$。

设 $B = \bigsqcup\limits_{i \in I} (A \cap B) x_i,\ x_i \in B$，则 $AB = \bigsqcup\limits_{i \in I} A x_i$，这是因为

- $AB = \bigcup_{i \in I} A x_i$。
  $\forall\, ab \in AB,\ a \in A, b \in B \Rightarrow \exists\, i,\ b = c x_i,\ c \in A \cap B \Rightarrow ab = a c x_i,\ ac \in A$。
- $A x_i \cap A x_j = \varnothing,\ \forall\, i \ne j$。
  $a x_i = a' x_i' \Rightarrow a'^{-1} a = x_i' x_i^{-1} \in A \cap B \Rightarrow x_i \in (A \cap B) x_i \Rightarrow x_i' = x_i$。

于是 $|AB| = |A| \cdot |I|,\ |B| = |A \cap B| \cdot |I|$，从而等式成立。

(2) $|G| \cdot |AB| = |G| \cdot |A| \cdot |B| / |A \cap B|$，于是
$$\frac{|G|}{|A|}\frac{|G|}{|B|} \ge \frac{|G|}{|A|}\frac{|AB|}{|B|} = \frac{|G|}{|A \cap B|}.$$
由 $[G : A \cap B] = [G:A][A : A \cap B] \Rightarrow [G:A] \mid [G : A \cap B]$，同理 $[G:B] \mid [G : A \cap B]$，若二者互素，则 $[G:A][G:B] \mid [G : A \cap B]$，从而 $[G:A][G:B] \le [G : A \cap B]$，而我们刚才已经证明 $[G:A][G:B] \ge [G : A \cap B]$，从而二者相等。

□

4 正规子群

设 $H \le G$，G/H 为左陪集的集合。希望
$$aH \cdot bH = abH,$$
$$ah_1 H \cdot bh_2 H = ah_1 bh_2 H.$$
这件事的合理性指出 $abH = ah_1bh_2H, \forall\, a, b \in G, h_1, h_2 \in H \Rightarrow bH = h_1bH, \forall\, b \in G, h_1 \in H \Rightarrow b^{-1}h_1b \in H \Rightarrow b^{-1}Hb \subset H,\ \forall\, b \in G$。于是我们有下面定义。

定义 4.1. 设 $N \leq G$，称 N 为 G 的一个**正规子群 (Normal subgroup)**，记作 $N \triangleleft G$ 或 $G \triangleright H$，若 $gNg^{-1} \subset N, \forall\, g \in G$。

例 4.1. 设 A 为 Abel 群，则 $H \leq A \Rightarrow H \triangleleft A$。

- $\{1\}, G \triangleleft G$，为平凡正规子群。称 G 为**单群**，若 G 没有非平凡正规子群。
- $SL_n(\mathbb{F}) \triangleleft GL_n(\mathbb{F})$，
- 设 $Z(G) = \{g \in G \mid gh = hg, \forall\, h \in G\}$，则 $Z(G) \triangleleft G$，称为 G 的**中心 (Center)**。也写作 $C(G)$。

评论. $N \triangleleft G \Rightarrow gNg^{-1} = N, \forall\, g$。

定义共轭为 $\sigma_g \colon G \xrightarrow{\sim} G,\ x \mapsto g^{-1}xg$，则给出了 G 的一个内自同构。记所有的内自同构为 $\mathrm{Inn}(G)$，那么 $\mathrm{Inn}(G) \triangleleft \mathrm{Aut}(G)$。