Lec5 Note of Abstract Algebra

Xuxuayame

日期：2023 年 3 月 24 日

例 3.1. 在 $\mathbb{Z}$ 中，$k\cdot 1=1+\cdots+1\neq 0,\ \forall\, k>0$，故 1 为无限阶元。

但在 $\mathbb{Z}/n\mathbb{Z}$ 中，$k\cdot\overline{1}=\overline{k}=0\Leftrightarrow n\mid k$，故 $\mathrm{ord}(\overline{1})=n$。

引理 3.1. 设 $g,h\in G,\ \mathrm{ord}(g)=n,\ \mathrm{ord}(h)=m$ 有限，则

(1) $\forall\, k\in\mathbb{Z},\ \mathrm{ord}(g^*)=\frac{n}{(n,k)}$；

(2) $gh=hg,\ (m,n)=1\Rightarrow\mathrm{ord}(gh)=mn$。

证明. (1) $(g^k)^n=(g^n)^k=1\Rightarrow\mathrm{ord}(g^k)\mid n$，记 $\mathrm{ord}(g^k)=r$，由 $(g^k)^{\frac{n}{(n,k)}}=(g^n)^{\frac{k}{(n,k)}}=1\Rightarrow r\mid\frac{n}{(n,k)}$。而 $(g^k)^r=1\Rightarrow\ n\mid kr\Rightarrow\frac{n}{(n,k)}\mid r$，故 $r=\frac{n}{(n,k)}$。

(2) 记 $\mathrm{ord}(gh)=r$，则 $(gh)^r=1\Rightarrow 1=((gh)^r)^n=g^{rn}h^{rn}=h^{rn}\Rightarrow m\mid rn\Rightarrow m\mid r$，同样地，$1=((gh)^r)^m\Rightarrow n\mid r$，那么 $mn\mid r$。又 $(gh)^{mn}=1\Rightarrow r\mid mn$，所以 $r=mn$。

□

评论. $gh=hg\Rightarrow\mathrm{ord}(gh)\mid[m,n]$。

定义 3.2. 设 $\varnothing\neq S\subset G$，包含 S 的最小的 G 的子群，称为 S **生成的子群**，记作 $\langle S\rangle$。

若 $G=\langle S\rangle$，则称 S 为 G 的**一组生成元**。若 $G=\langle\{s\}\rangle$，则 s 为 G 的**一个生成元**。可由一个元素生成的群称为**循环群**。

评论. $\langle S\rangle=\bigcap\limits_{H\leq G,S\subset H}H\leq G$

例 3.2. $\mathbb{Z}=\langle 1\rangle=\langle -1\rangle$。

$\mathbb{Z}/n\mathbb{Z}=\langle\overline{1}\rangle=\langle\overline{-1}\rangle=\langle\overline{a}\rangle\Leftrightarrow(a,n)=1$，于是有 $\varphi(n)$ 个生成元。

$GL_n(\mathbb{F})=\langle T_{ij}(a),P_{ij},D_i(\lambda)\rangle=\langle T_{12}(a),P_{ij},D_1(\lambda)\rangle,\ \mathbb{F}=\mathbb{C},\mathbb{R},\mathbb{Q}\cdots$，且后一组生成元满足 $a\in\mathbb{F},\ 1\leq i<j\leq n,\ \lambda\neq 0$。

引理 3.2. 设 $g\in G$ 为有限阶元，则 $\mathrm{ord}(g)=|\langle g\rangle|$。

证明. g 有限阶，故令 $\mathrm{ord}(g)=n$，下证 $\langle g\rangle=\{1,g,\cdots,g^{n-1}\}$。

对 $\forall\, i\in\mathbb{Z},\ i=qn+r(i)$，那么 $g^i=g^{r(i)}$。而 $\forall\, 0\leq i<j\leq n-1,\ g^i\neq g^j$，否则 $g^{j-i}=1$，矛盾。 □

定理 3.3. 设 $G=\langle g\rangle$ 为循环群，则

(1) 若 G 为无限群，则 $G\simeq\mathbb{Z}$。

(2) 若 G 为有限群，则存在唯一的 $n(=|G|)$ 使得 $G\simeq\mathbb{Z}/n\mathbb{Z}$。

证明. (1) G 无限 $\Rightarrow g^i\neq g^j,\ \forall\, i\neq j\in\mathbb{Z}$。则 $\varphi\colon \mathbb{Z}\to\langle g\rangle=G,\ i\mapsto g^i$ 为同构。

(2) 显然。

□

命题 3.4. $G=\langle g\rangle$，那么

(1) 若 $G\simeq\mathbb{Z}$，则 G 的生成元为 g 或 g^{-1}。

(2) 若 $G\simeq\mathbb{Z}/n\mathbb{Z}$，则 G 的生成元为 $g^a,\ (a,n)=1$。

(3) $\mathrm{Aut}G\simeq\begin{cases}\mathbb{Z}^\times=\{\pm1\}, & G\simeq\mathbb{Z},\\ (\mathbb{Z}/n\mathbb{Z})^\times, & G\simeq\mathbb{Z}/n\mathbb{Z}.\end{cases}$

评论. 若 $G_1\simeq G_2,\ \varphi\colon G_1\xrightarrow{\sim}G_2$，那么 $\mathrm{Aut}G_1\simeq\mathrm{Aut}G_2$，同构由 $f\mapsto\varphi f\varphi^{-1}$ 给出。

设 $H\leq G$。

定义 3.3. $aH=\{ah\mid h\in H\}$ 称为 G 对于子群 H 的一个**左陪集 (Left coset)**，类似可以定义**右陪集 (Right coset)** 为 Ha。

引理 3.5. *(1)*

$$aH\cap bH=\begin{cases}aH, & a^{-1}b\in H,\\ \varnothing, & \textit{else}.\end{cases}$$

(2)

$$Ha\cap Hb=\begin{cases}Ha, & ba^{-1}\in H,\\ \varnothing, & \textit{else}.\end{cases}$$

证明. (1) 若 $x=ah_1=bh_2$，则 $b=ah_1h_2^{-1}\Rightarrow a^{-1}b=h_1h_2^{-1}\in H$，于是 $bH=ah_1h_2^{-1}H=aH$。

(2) 类似可得。

□

评论. G 可写成若干左陪集的无交并，在 G 上可定义等价关系 $\sim$:

$$a\sim b:\Leftrightarrow a^{-1}b\in H.$$

G 在 $\sim$ 下的等价类恰为 G 对于 H 的左陪集。

如果将 $a^{-1}b$ 替换为 ab^{-1}，那么就得到了右陪集。

定义 3.4. 称 $\{a_i\in G\mid i\in I\}$ 为 G 对于子群 H 的一个**左陪集完全代表元系**，若

$$G=\bigcup_{i\in I}a_iH.$$

类似可定义**右陪集完全代表元系**。

引理 3.6. $\{a_i \in G \mid i \in I\}$ 为左陪集完全代表元系 $\Rightarrow \{a_i^{-1} \mid i \in I\}$ 为右陪集完全代表元系。

证明. $\forall\, g \in G,\ \exists!\, i_{(g)} \in I$ 使得

$$g \in a_{i_{(g)}} H \Leftrightarrow g^{-1} \in H a_{i_{(g)}}^{-1}.$$

于是我们知道，$\forall\, g \in G,\ \exists!\, i_{(g^{-1})} \in I$，使得

$$g^{-1} \in a_{i_{g^{-1}}} H \Rightarrow g \in H a_{i_{g^{-1}}}^{-1}.$$

所以 $G = \bigcup H a_i^{-1}$。而 $H a_i^{-1} = H a_j^{-1} \Leftrightarrow a_i H = a_j H \Leftrightarrow i = j$，故彼此不交，从而为不交并。 □

定理 3.7. *(Lagrange)*：$|G| < \infty,\ H \leq G$，则 $|G| = |H| \cdot [G : H]$，特别地，$|H| \mid |G|$。

推论. $|G| < \infty,\ \forall\, g \in G,\ g^{|G|} = 1$。也可等价表为 $\mathrm{ord}(g) \mid |G|$。