第十四周习题课

李文桥

2023 年 12 月 22 日

1 回忆与习题

回忆: 群的定义, 单位元与可逆元. 设 G 为一个群, 单位元为 e.

- 群的定义: 二元运算(乘法), 结合律, 有单位元, 有逆元.
- 乘法交换的群称为交换群, 或者阿贝尔群. 所含元素个数有限的群称为有限群.
- 单位元唯一, 逆元唯一。

  证: 以单位元为例, 设 $e, e' \in G$ 为单位元, 则 $ee' = e', ee' = e$, 从而 $e = e'$. $\square$
- 消去律: 设 $x, y, g \in G$, 且 $xg = yg$, 则 $x = y$. (g 在左侧的情形也一样).

回忆: 子群, 群的生成元, 元素的阶.

- 子群的定义: 子集且是群.
- 子群的判别法: 设 H 为 G 的非空子集, 且 $\forall x, y \in H$, $xy^{-1} \in G$, 则 H 成为 G 的子群.
- Lagrange 定理: 设 G 为有限群, H 为 G 的子群, 则 $\mathrm{card}(H) \,|\, \mathrm{card}(G)$.
- 设 S 为 G 的非空子集, 定义 $\langle S\rangle := \{x_1^{e_1} x_2^{e_2} \cdots x_m^{e_m} \,|\, m \in \mathbb{N}^+,\ x_1, \cdots, x_m \in S,\ e_1, \cdots, e_m \in \mathbb{Z}\}$, 这是一个 G 的子群, 称为 S 生成的子群. 若 $G = \langle S\rangle$, 则称 S 为 G 的一组生成元.
- 设 $g \in G$, 定义 g 的阶 $\mathrm{ord}(g) := \min_{m\in\mathbb{N}^+}\{g^m = e\}$.(可以是 ∞)
- 设 $g^k = e$, 则 $\mathrm{ord}(g) \,|\, k$.
- $\mathrm{card}(\langle g\rangle) = \mathrm{ord}(g)$.

  证: 设 $m = \mathrm{ord}(g)$, 则 $\langle g\rangle = \{e, g, \cdots, g^{m-1}\}$ $(m < \infty)$ 或 $\{\cdots, g^{-1}, e, g, \cdots, g^n, \cdots\}$ $(m = \infty)$.
- $g^{\mathrm{card}(\langle g\rangle)} = e$, 或者 $\mathrm{ord}(g) \,|\, \mathrm{card}(\langle g\rangle)$.
- 设 $k \in \mathbb{N}$, 则 $\mathrm{ord}(g^k) = \dfrac{\mathrm{ord}(g)}{\gcd(k, \mathrm{ord}(g))}$.

回忆: 同态与同构设 G, H 为两个群, 单位元为 e_G, e_H. $\phi: G \to H$ 为映射.

- 群同态: ϕ 保持乘法, 即 $\phi(ab) = \phi(a)\phi(b)$, $\forall a, b \in G$; 群同构: ϕ 为群同态且为双射.
- 若 ϕ 为群同态, 则 $\phi(e_G) = e_H$, $\phi(g^{-1}) = (\phi(g))^{-1}$.
- 若 ϕ 为群同态, 则 $\mathrm{im}(\phi)$ 为 H 的子群.

回忆: 循环群.

- 定义: 由一个元素生成的群称为循环群.
- 循环群的子群是循环群, 循环群同构于 $\mathbb{Z}$ 或者 Z_n, $\exists\, n \in \mathbb{N}^+$.
- 素数阶群一定是循环群.

习题1: 按照定义验证即可, 需验证乘法的封闭性, 结合律以及单位元和逆元的存在性.

注: 实际上, 任取 $a, b \in \mathbb{R}$, $a \neq 0$, 令 $f_{a,b}(x) = ax + b$. 考虑: $H = f_{a,b}(x) \,|\, a, b \in \mathbb{R}, a \neq 0$. 则容易验证 H 在函数复合运算下成为一个群, 且 $(a, b) \mapsto f_{a,b}$ 给出同构 $G \cong H$.

习题2: 容易计算 $AB = -\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, 从而 $(AB)^n = (-1)^n \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}$, $n \in \mathbb{Z}$. 所以 $(AB)^m \neq (AB)^n$, 若 $m \neq n$. 故 AB 生成的子群是无限群. 而在阿贝尔群中, 设 $\mathrm{ord}(a), \mathrm{ord}(b) < \infty$, 则 $(ab)^{\mathrm{ord}(a)\mathrm{ord}(b)} = e$, 从而有限阶.

习题3: 我们只需验证 H 中有单位元和逆元即可. 任取 $h \in H$, 由乘法封闭性知 $h^k \in H$, $\forall k \in \mathbb{N}^+$. 由于 H 是有限集合, 故存在 $i \neq j$ 使得 $h^i = h^j$. 不妨设 $j > i$, $t = j - i$, 则 $h^t = e \in H$, 且 $h^{-1} = h^{t-1} \in H$.

习题4: (a) 按照定义验证. 先验证乘法封闭性: 设 $a, b \in \ker(\phi)$, 则 $\phi(ab) = \phi(a)\phi(b) = e_G e_G = e_G$, 从而 $ab \in \ker(\phi)$.

任取 $a, b \in \ker(\phi)$, $\phi(ab^{-1}) = \phi(a)\phi(b^{-1}) = \phi(a)(\phi(b))^{-1} = e_G$, 从而 $ab^{-1} \in G$, 由子群判别法知 $\ker(\phi)$ 为子群.

(b) 我们证明 $g\ker(\phi) \subseteq \ker(\phi)g$, 另一个方向方法是一样的. 设 $x \in g\ker(\phi)$, 则存在 $t \in \ker(\phi)$ 使得 $x = gt$. 则 $\phi(x) = \phi(g)\phi(t) = \phi(g)$. 这说明 $e_H = \phi(x)(\phi(g))^{-1} = \phi(x)\phi(g^{-1}) = \phi(xg^{-1})$, 从而 $xg^{-1} \in \ker(\phi)$. 故存在 $s \in \ker(\phi)$ 使得 $xg^{-1} = s$, 则 $x = sg \in \ker(\phi)g$. 这表明 $g\ker(\phi) \subseteq \ker(\phi)g$.

(c) 只证充分性. 若 $\ker(\phi) = \{e_G\}$, 则任取 $x, y \in G$, 若 $\phi(x) = \phi(y)$, 则 $e_H = \phi(x)(\phi(y))^{-1} = \phi(x)\phi(y^{-1}) = \phi(xy^{-1})$, 从而 $xy^{-1} \in \ker(\phi) = \{e_G\}$, 故 $xy^{-1} = e_G$, $x = y$.从而 ϕ 为单射.

习题5: 必要性: 反证法, 若 G 中不含二阶元, 则除单位元外, 所有元素与其逆不相等. 将单位元外的每个元素与其逆配对, 设有 n 对, 我们就知道 G 中有 $2n + 1$ 个元素, 这与 $\mathrm{card}(G)$ 为偶数矛盾.

充分性: 设 $g \in G$ 为二阶元, 则 $2 = \mathrm{ord}(g) \,|\, \mathrm{card}(G)$.

习题6: (2) 可由 (1) 直接得到. 关于 (1) 我们只证必要性: 反证法, 设 A, B 不相互包含, 则存在 $a \in A\backslash B$, $b \in B\backslash A$. 由于 $A \cup B$ 为子群, 故 $ab \in A \cup B$. 令 $c = ab$. 若 $c \in A$, 则 $b = a^{-1}c \in A$, 矛盾; 若 $c \in B$, 则 $a = cb^{-1} \in B$ 矛盾. 故 A 为 B 的子群或 B 为 A 的子群.

2 陪集与商群

设 G 为一个群, H 为 G 的子群. 任取 $g \in G$, L_g 为左平移. 定义 $gH := L_g(H)$, 称为 G 关于 H 的一个左陪集.

命题 2.1 $\forall g_1, g_2 \in G$, $g_1H = g_2H$ 或者 $g_1H \cap g_2H = \emptyset$.

证: 若存在 $x \in g_1H \cap g_2H$, 则存在 $h_1, h_2 \in H$ 使得 $x = g_1h_1 = g_2h_2$, 从而 $g_1 = g_2h_2h_1^{-1}$, $g_1H = g_2h_2h_1^{-1}H = g_2(h_2h_1^{-1}H) \subseteq g_2H$. 同理, $g_2H \subseteq g_1H$, 从而 $g_1H = g_2H$.

推论 2.2 *(1)* $g_1H = g_2H \Leftrightarrow g_1 \in g_2H \Leftrightarrow g_2^{-1}g_1 \in H$.

(2) 定义 G 中的关系 $g_1 \sim_H g_2 : g_1H = g_2H$. 这是一个等价关系.

我们称 g 为左陪集 gH 的代表元. 由上述推论知, 陪集中的任何一个元素都能选为代表元.

定义 2.3 $G = \bigcup\limits_{g\in G} gH$. 我们将所有重复出现的陪集去掉, 写为 $G = \coprod\limits_{g\in T} gH$, 其中, 每个互不相同的左陪集取定一个代表元, 它们构成集合 T. 我们称 $G = \coprod\limits_{g\in T} gH$ 为 G 的陪集分解. 若 $\mathrm{card}(T)$ 称为 G 对 H 的指数, 记为 $[G : H]$.

容易看出, 若 G 为有限群, 则 $[G : H] = \dfrac{\mathrm{card}(G)}{\mathrm{card}(H)}$, 这就是 Lagrange 定理.

注: 以上定义和结论均可将“左”换成“右”.

定义 2.4 我们称集合 $G/H := \{gH \mid g \in G\} = \{gH \mid g \in T\}$ 为 G 关于 H 的齐性空间, 则 $\mathrm{card}(G/H) = [G : H]$. 实际上, $G/H = G/\sim_H$.

我们会问: G/H 是否能称为一个群? 设 $g_1H, g_2H \in G/H$, 我们会自然地定义乘法: $g_1H \cdot g_2H := g_1g_2H$. 但这个定义与代表元的选取有关.

定理 2.5 上述定义是良定义的当且仅当 $gH = Hg$, $\forall g \in G$.

证: 任取 $g_1, g_2 \in G$,

$$\begin{aligned}
\text{良定义} &\Leftrightarrow \forall a_1 \in g_1H,\ a_2 \in g_2H,\ a_1a_2H = g_1g_2H \\
&\Leftrightarrow \forall a_1 \in g_1H,\ a_2 \in g_2H,\ a_1a_2 \in g_1g_2H \\
&\Leftrightarrow \forall a_1 \in g_1H,\ a_2 \in g_2H,\ g_2^{-1}g_1^{-1}a_1a_2 \in H \\
&\Leftrightarrow \forall h \in H,\ a_2 \in g_2H,\ g_2^{-1}ha_2 \in H \\
&\Leftrightarrow \forall h \in H,\ a_2 \in g_2H,\ ha_2 \in g_2H \\
&\Leftrightarrow \forall h \in H,\ a_2 \in g_2H,\ g_2 \in ha_2H = h(a_2H) = hg_2H \\
&\Leftrightarrow \forall h \in H,\ hg_2 \in g_2H \\
&\Leftrightarrow \forall h \in H,\ Hg_2 \subset g_2H
\end{aligned}$$

所以

$$\begin{aligned}
\forall g_1, g_2 \in G,\ \text{良定义} &\Leftrightarrow \forall g \in G,\ Hg \subset gH \\
&\Leftrightarrow \forall g \in G,\ Hg^{-1} \subset g^{-1}H \\
&\Leftrightarrow \forall g \in G, gH \subset Hg \\
&\Leftrightarrow \forall g \in G,\ Hg \subset gH \text{ 且 } gH \subset Hg \\
&\Leftrightarrow \forall g \in G,\ Hg = gH.
\end{aligned}$$

□

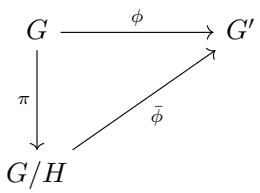
定义 2.6 若 H 为 G 的子群且 $gH = Hg$ 对任意的 $g \in G$ 成立, 则称 H 为 G 的正规子群. 此时, G/H 在上述定义的乘法下构成一个群, 称为 G 对 H 的商群. 此时, G/H 的单位元为 H, gH 的逆元为 $g^{-1}H$.

定义 2.7 记 $\bar{g} := gH \in G/H$, 则 G/H 中的乘法可表示为: $\bar{g_1} \cdot \bar{g_2} = g_1\bar{g}_2$. 映射 $\pi : G \to G/H$, $g \mapsto \bar{g}$ 是群同态, 称为 G 到其商群 G/H 的自然同态.

注: 若 G 为阿贝尔群, 则 G 的任何一个子群都是正规子群.

推论 2.8 若 $\phi : G \to G'$ 为群同态, 则 $\ker(\phi)$ 为 G 的正规子群.

定理 2.9 (第一同态基本定理) 设 $\phi : G \to G'$ 为群同态, 则存在唯一的单同态 $\bar{\phi} : G/\ker(\phi) \to G'$, 使得 $\bar{\phi} \circ \pi = \phi$. 进而 $G/\ker(\phi) \cong \mathrm{im}(\phi)$.



证: 令 $\bar{\phi} : \bar{g} \mapsto \phi(g)$. 容易验证此映射良定义且满足条件. 唯一性是显然的. □

推论 2.10 *若 $\phi: G \to G'$ 为满的群同态, 则 $G/\ker(\phi) \cong G'$.*

注: 若 $\phi: G \to G'$ 为满的群同态, 那么我们可以将 G' 视为 G 的一个商群; 对偶地, 若若 $\phi: G \to G'$ 为单的群同态, 我们可以将 G 视为 G' 的一个子群. 换句话说, 单射对应子对象, 满射对应商对象.

3 4,6 阶群的分类

我们已经知道素数阶群都是循环群. 本节我们讨论 4,6 阶群的全部可能的同构型.

引理 3.1 *若 G 中元素的阶不超过 2, 则 G 为交换群.*

证: 设 $a, b \in G$, 不妨设 a, b 阶均为 2, 则 $a^2b^2 = e = (ab)^2$, 两侧分别消去 a, b 得: $ba = ab$. □

定理 3.2 *设 G 为四阶群, 则 G 同构于 $\mathbb{Z}_4$ 或 $\mathbb{Z}_2 \times \mathbb{Z}_2$.*

证: 若 G 中有四阶元, 则 G 为四阶循环群. 否则, G 中元素的最大阶数为 2, 从而 G 为交换群. 设 $a \neq b \in G\backslash\{e\}$, 则 $G = \{e, a, b, ab\}$. 写出同构如下:

$$\begin{aligned} G &\to \mathbb{Z}_2 \times \mathbb{Z}_2 \\ a &\mapsto (\bar{1}, \bar{0}) \\ b &\mapsto (\bar{0}, \bar{1}) \end{aligned}$$

□

引理 3.3 $S_3 = \langle (12), (123) \rangle$.

定理 3.4 *设 G 为六阶群, 则 G 同构于 $\mathbb{Z}_6$ 或 S_3.*

证: 若 G 中有 6 阶元, 则 G 为六阶循环群. 若 G 中元素最大阶为 3, 则设 $c \in G$ 阶为 3. 设 G 对 $\langle c \rangle$ 的左陪集分解为

$$G = \langle c \rangle \coprod a \langle c \rangle,$$

其中 $a \in G\backslash \langle c \rangle$. 那么 $a^2 \in G$ 但 $a^2 \notin a\langle c \rangle$. 于是我们有三种情形: $a^2 = e, c, c^2$. 这其中, $a^2 = c$ 与 $a^2 = c^2$ 是一样的, 因为 $c^2 = c^{-1}$ 也为 $\langle c \rangle$ 的生成元. 另外, 若 $a^2 = c$, 则 a 的阶为 6, 矛盾. 所以只能是 $a^2 = e$. 接下来考虑 ca. 容易看到 $ca \in a\langle c \rangle$. 那么实际上我们有三种情形:

1. 若 $ca = a$, 则 $c = e$, , 矛盾.
2. 若 $ca = ac$, 则 G 为交换群, 从而 ca 的阶数为 6, 矛盾;

3. 若 $ca = ac^2$, 则有同构:

$$\begin{aligned} G &\to S_3 \\ c &\mapsto (123) \\ a &\mapsto (12) \end{aligned}$$

于是, 若 G 中元素最大阶为 3, 则 G 同构于 S_3.

若 G 中元素最大阶数为 2, 则 G 为交换群. 任取 $a \neq b \in G\backslash\{e\}$, 我们知道 $\{e, a, b, ab\}$ 成为 G 的一个子群. 而 4 不整除 6, 矛盾.

综上所述, G 同构于 $\mathbb{Z}_6$ 或者 S_3.