近世代数作业 5

cycleke

November 23, 2020

Contents

1 课后习题

1.1 第一题

证明 设 $U_n = \{x^n = 1 | x \in C\}$。

显然 $U_n = \{x_i | 0 \le i < n, i \in N, x_i = e^{\frac{2\pi i}{n}}\}$ 且对于复数的乘法构成群。$x_1 = e^{\frac{2\pi i}{n}}$，而 $\forall 1 \le i \le n-1, x_i = x_1^i = e^{\frac{2\pi i}{n}} \ne 1$，而 $x_1^n = 1$，所以 $|x_1| = n$，$U_n = (x_1)$，即 U_n 为一个循环群。 □

1.2 第二题

真子群如下：

- $\{[0]\}$
- $\{[0], [6]\}$
- $\{[0], [4], [8]\}$
- $\{[0], [3], [6], [9]\}$
- $\{[0], [2], [4], [6], [8], [10]\}$

1.3 第三题

证明 首先 $\forall x \in (a^r), x = (a^r)^k = a^{rk} \in G$，所以 $(a^r) \subseteq G$。

又有因为 $G = (a)$，所以 $\forall x \in G, x = a^k, 1 \le k \le n 且 a^n = e$，又因为 $(r, n) = 1$，所以 $\exists p, q \in Z, pr + qn = 1$

$$\begin{aligned} x &= a^k \\ &= a^{k(pr+qn)} \\ &= a^{kpr} \circ a^{kqn} \\ &= (a^r)^{kp} \circ (a^n)^{kn} \\ &= (a^r)^{kp} \end{aligned}$$

所以 $G \subseteq (a^r)$。

综上所述，$G = (a^r)$。 □

1.4 第四题

证明 因为 $a^n = e, (r, n) = d$，所以 $(a^r)^{\frac{n}{d}} = (a^n)^{\frac{r}{d}} = e$，所以 $|a^r| \le \frac{n}{d}$。

$\forall 1 \le k < \frac{n}{d}$，若 $(a^r)^k = e$，因为 $(r, n) = d$，所以 $\exists p, q \in Z, pr + qn = d$。

$$\begin{aligned} a^d &= a^{pr+qn} \\ &= (a^r)^p \circ (a^n)^q \\ &= (a^r)^p \\ (a^d)^k &= ((a^r)^k)^p \\ &= e \end{aligned}$$

所以 $|a| \le dk < n$，这与 $|a| = n$ 矛盾。所以 $|a^r| \ge \frac{n}{d}$。

综上所述，$|a^r| = \frac{n}{d}$。 □

1.5 第五题

证明 设 G 是一个六阶群，所以 $\forall a \in G, |a| \in \{6, 3, 2, 1\}$。

若 $\exists a, |a| = 6$，则 e, a^2, a^4 是一个三阶群。

若 $\exists a, |a| = 3$，则 e, a, a^2 是一个三阶群。

若 $\forall a \in G, |a| \leq 2$，因为有且只有 $|e| = 1$，则 $\forall a \in G, a^2 = e$。由前面的作业有，此时 G 是一个交换群且每个元素的拟元为自身。不妨设 $a, b \in G, |a| = |b| = 2, a \neq b \neq e$，设 $S = \{e, a, b, ab\}$，则 $\forall x, y \in S, xy^{-1} \in S$，所以 S 为 G 的一个四阶子群，产生矛盾。

综上所述，六阶群里必有一个三阶子群。 □

1.6 第六题

证明 设 G 是一个 p^m 阶群，$\forall a \in G, |a| = p^k, 0 \leq k <= m$。

$$\therefore a^{p^k} = e$$
$$(a^{p^{k-1}})^p = e$$
$$\therefore |a^{p^{k-1}}| \leq p$$

因为 $p \geq 2$，所以 $\exists b \in G, |b^{p^{k-1}}| = p$，所以存在一个 p 阶子群 $(b^{p^{k-1}})$. □

1.7 第七题

$$H = \{(1\ 2\ 3), (2\ 1\ 3)\}$$
$$(3\ 2\ 1)H = \{(3\ 2\ 1), (3\ 1\ 2)\}$$
$$H(3\ 2\ 1) = \{(3\ 2\ 1), (2\ 3\ 1)\}$$

1.8 第八题

不一定。

由于 $(3\,2\,1)$ 在 S_3 中是一个双射，所以 $(3\,2\,1)S_3 = S_3(3\,2\,1)$。但是 $(3\,2\,1)(2\,1\,3) = (3\ 1\ 2), (2\ 1\ 3)(3\ 2\ 1) = (2\ 3\ 1)$。

1.9 第九题

证明 设 $\varphi : S_l \to S_r, \forall a \in G, aH \in S_l, \varphi(aH) = Ha^{-1}$。

首先证明 φ 是满射：

$$\forall Hb \in S_r, b, b^{-1} \in G$$
$$\exists b^{-1}H \in S_l, 即\varphi(b^{-1}H) = Hb$$

再证明 φ 是单射：

$$\forall a_1H, a_2H \in S_l, a_1H \neq a_2H$$
$$\varphi(a_1H) = Ha_1^{-1}$$
$$\varphi(a_2H) = Ha_2^{-1}$$
$$\text{若} Ha_1^{-1} = Ha_2^{-1} \text{则} a_1a_2^{-1} \in H$$
$$\text{则} a_1H = a_2H, \text{产生矛盾}$$

所以 φ 是一个单射。

所以 φ 是一个双射，$|S_l| = |S_r|$。 □

1.10 第十题

证明 若 $x \in H, x \circ x \in H, x^2 \in H$。

若 $x \notin H, x^{-1} \notin H$，所以 $xH \neq H, x^{-1}H \neq H$。因为 $[G : H] = 2$，所以 $xH = x^{-1}H, x \circ xH = H, x^2 \in H$。 □

举例：

- 有限群：G 为模 n 同余类，H 为偶余数子群
- 无限群：G 为 $(Z, +)$，H 为偶数加群