Homework 01

DarkSharpness

2023.09.21

目录

T5

由题，因为交换群，所以 $\forall a, b \in G$, $(a \circ b)^m = (a^m) \circ (b^m) = ee = e$, 因此 $a \circ b \in G$ 。对于任意的 $a \in G$, $a^m = e$, $e = a \circ {a^{-1}}^m = a^m \circ (a^{-1})^m = e \circ (a^{-1})^m = (a^{-1})^m$. 所以 $a^{-1} \in G$ 。因此 H 是 G 的子群。

T6

$\forall a, b \in H$, 设 $a = gXg^{-1}$, $b = gYg^{-1}$, 则 $ab = gXg^{-1}gYg^{-1} = gXYg^{-1} \in H$ 。且 $a^{-1} = g^{-1}X^{-1}g = gX^{-1}g^{-1} \in H$ 。因此 H 是 G 的子群。

注: 由群的性质，显然 X^{-1}, XY 也在群内。

T7

$\forall x, y \in C(a)$, $xya = xay = axy$ ，因此 $xy \in C(a)$ 。同时，$x^{-1}a^{-1} = (ax)^{-1} = (xa)^{-1} = a^{-1}x^{-1}$ ，因此 (左右分别乘以 a 之后) $ax^{-1} = x^{-1}a$ ，因此 $x^{-1} \in C(a)$ 。

T8

$C(G) = \{g \in G | gx = xg, \forall x \in G\}$ 因此显然，$\forall a \in G$ ，$C(G) \subseteq C(a)$ ，因此显然 $C(G) \subseteq \bigcap\limits_{a \in G} C(a)$ 。而由定义，$\forall x \in \bigcap\limits_{a \in G} C(a)$ ，$\forall a \in G, xa = ax$ ，因此 $x \in C(G)$ ，所以 $\bigcap\limits_{a \in G} C(a) \subseteq C(G)$ 。

综上 $\bigcap\limits_{a \in G} C(a) = C(G)$ 。

T18

在整数加群中，$\forall a \in \langle m \rangle, b \in \langle n \rangle \exists x, y$ ，满足 $\forall a = xm, y = bn$ 。记 $m_0 = \frac{m}{d}, n_1 = \frac{n}{d}$ ，则 $a + b = xm + yn = d(xm_0 + yn_0) \in \langle d \rangle$ 。因此 $\langle m, n \rangle \subseteq \langle d \rangle$ 。而因为 $(m_0, n_0) = 1$ ，所以当

$xm_0 + yn_0 = 1$ 可以取遍 $\mathbb{Z}$ 。因此 $\forall x \in \langle d \rangle$ ，必定满足 $x \in \langle m, n \rangle$ 。因此 $\langle d \rangle \subseteq \langle m, n \rangle$ 。因此 $\langle m, n \rangle = \langle d \rangle$ 。

T19

充分性显然。下证明其必要性。若 $\langle m \rangle = \langle n \rangle$ ，考虑群中绝对值非零且最小的一项，分别为 $|m|$ 和 $|n|$ 。因为 $\langle m \rangle = \langle n \rangle$ ，所以 $|m| = |n|$ ，所以 $m = \pm n$ 。

补充

如果 $N = n_1 \cdot n_2$ 且 $gcd(n1, n2) = 1$ 。则

$$\mathbb{Z}_N^* = \mathbb{Z}_{n_1}^* \times \mathbb{Z}_{n_2}^*$$

证明: $\mathbb{Z}_N^* = \{1, 2, \ldots, N-1\}$。而 $\mathbb{Z}_{n_1}^* \times \mathbb{Z}_{n_2}^* = \{d | xn_1 + yn_2 \equiv d(modN), 0 < d < N, \forall x, y\}$ 。

因为 $(n_1, n_2) = 1$ ，故存在 x, y 使得 $xn_1 + yn_2 \equiv 1(modN)$ 。因此 d 可以取遍 $1, 2, \ldots, N-1$ ，因此

$$\mathbb{Z}_N^* = \mathbb{Z}_{n_1}^* \times \mathbb{Z}_{n_2}^*$$