MA150 Algebra

homework 2

Problem 1 *Page 25-5*

Solution: 首先根据题设，显然有 $H \subseteq G$。

对$\forall a, b \in H$, 因G是交换群，则有 $(ab^{-1})^m = a^m \cdot (b^{-1})^m = e \to ab^{-1} \in H$。

所以H是G的子群。

Problem 2 *Page 25-6*

Solution: $gHg^{-1} \subseteq G, \forall a, b \in H, gag^{-1}, gbg^{-1} \in gHg^{-1}$。

$$gag^{-1} \cdot (gbg^{-1})^{-1} = gag^{-1} \cdot gb^{-1}g^{-1} = g(ab^{-1})g^{-1} \tag{1}$$

$H < G \to ab^{-1} \in H \to g(ab^{-1})g^{-1} \in gHg^{-1} \to gHg^{-1} < G$。

Problem 3 *Page 25-7*

Solution: 显然$C(a) \subseteq G$,

(1) $\forall g \in C(a), ga = ag$, 等式两边变换后得到

$g^{-1}(ga)g^{-1} = g^{-1}(ag)g^{-1} \to ag^{-1} = g^{-1}a$。

所以$g^{-1} \in C(a)$。

(2) $\forall x, y \in C(a)$,

$xya = x(ya) = xay = axy \to xy \in C(a)$。

综上 $C(a) < G$。

Author(s): 于峥

Problem 4 *Page 25-8*

Solution: 此题分两步分别证明：

(1) $C(G) \subseteq \bigcap_{a \in G} C(a)$

$\forall x \in C(G)$, 根据$C(G)$的定义，

有$\forall a \in G, x \in C(a)$, 所以$a \in \bigcap_{a \in G} C(a)$，结论得证。

(2) $C(G) \supseteq \bigcap_{a \in G} C(a)$。

$\forall x \in \bigcap_{a \in G} C(a)$，则$\forall g \in G, gx = xg$, 所以$x \in C(g)$。

综上 $C(G) = \bigcap_{a \in G} C(a)$。

Problem 5 *Page 26-18*

Solution: 首先 $\langle m, n \rangle = \{am + bn | a, b \in \mathbb{Z}\}$, $\langle d \rangle = \{kd | k \in \mathbb{Z}\}$。

下证$ax + by = m$有解当且仅当m为$d = \gcd(a, b)$的整数倍。

(1) 如果有$a = 0$或$b = 0$, 则显然成立。

(2) 若a, b都不为0, $\forall x, y \in \mathbb{Z}$，有 $d|(ax + by)$。

设$s > 0$为$ax + by$的最小值,因为$d|(ax + by)$,则必有$d|s$。

令 $q = \left\lfloor \frac{a}{s} \right\rfloor$，$r = a \mod s$。

容易发现 $r = a - q(ax + by) = a(1 - qx) + b(-qy)$。

又s为最小值，所以$r = 0$。得到$s|a$的结论。

同理得到$s|b$, 那么$s|d$所以有$s = d$。

所以$ax + by = d$存在解，进而$ax + by = kd, k \in Z$有解。

综上所述，$\forall x \in \langle m, n \rangle, x \in \langle d \rangle$。反之亦然。得出结论$\langle m, n \rangle = \langle d \rangle$。

Problem 6 *Page 26-19*

Solution: **必要性**：当$m = \pm n$,显然有 $\langle m \rangle = \langle n \rangle$。

充分性: 反证法，若$m \neq \pm n$，且$\langle m \rangle = \langle n \rangle$。

令$m = pn + r$, 因为$\langle m \rangle = \{km | k \in \mathbb{Z}\}$。

因为 $kn \in \langle m \rangle$, 所以 $kpn + kr = kn$均有解。那么$r = 0$。

因为 $n \in \langle m \rangle$, 所以 $kp = 1$有解。那么$p = \pm 1$。

这与假设矛盾。

综上所述，$\langle m \rangle = \langle n \rangle$ 当且仅当 $m = \pm n$。

Problem 7 **证明**：若$N = n_1 n_2, \gcd(n_1, n_2) = 1$ 那么 $\mathbb{Z}_N^* \cong \mathbb{Z}_{n_1}^* \times \mathbb{Z}_{n_2}^*$。

Solution: *(1)* 构造$\mathbb{Z}_N^*$到$\mathbb{Z}_{n_1}^* \times \mathbb{Z}_{n_2}^*$的映射$\phi(x)$。

$$\phi(x) = (x \mod n_1, x \mod n_2)$$

(2) **双射性质**：$\forall x, y \in \mathbb{Z}_N$, 使得 $\phi(x) = \phi(y)$。若$x \neq y$, 即

$$\begin{cases} x \mod n_1 = a \\ x \mod n_2 = b \end{cases}$$

有至少两个解，然而$\gcd(n_1, n_2) = 1$, $0 < x, y < N$。根据中国剩余定理，矛盾。所以$\phi(x)$为单射。同时由于该方程必有解，所以$\phi(x)$为满射。

(3) **保持运算**： $\forall x, y \in \mathbb{Z}_N^*, \phi(x) = (a, b), \phi(y) = (c, d)$。

$$\begin{aligned} \phi(xy) &= (xy \mod n_1, xy \mod n_2) \\ &= (ac \mod n_1, bd \mod n_2) \,. \\ &= \phi(x)\phi(y) \end{aligned}$$

。综上所述,得证。
