离散数学（2023）作业 19 - 子群与拉格朗日定理

离散数学教学组

Problem 1

设 H, K 是群 $\langle G, \circ \rangle$ 的子群，下面哪些代数系统是 $\langle G, \circ \rangle$ 的子群？

A. $\langle H \cup K, \circ \rangle$　　B. $\langle H \cap K, \circ \rangle$　　C. $\langle K - H, \circ \rangle$　　D. $\langle H - K, \circ \rangle$

答案： 答案只有 B。对 A，$H \cup K \Leftrightarrow H \subseteq K \vee K \subseteq H$，故不一定；对 CD，$e_G \notin K - H(H - K)$，故一定不。

Problem 2

设 G 是一个有限群，K 是 G 的子群，H 是 K 的子群。证明：$[G:H] = [G:K] \cdot [K:H]$。

答案： 显然，H 是 G 的子群。由拉格朗日定理有：$|G| = [G:K] \cdot |K|, |G| = [G:H] \cdot |H|, |K| = [K:H] \cdot |H|$，可得 $[G:K] \cdot [K:H] \cdot |H| = [G:H] \cdot |H|$。两边消去 H，可得 $[G:H] = [G:K] \cdot [K:H]$。

Problem 3

设 G 为群，a 是 G 中给定元素，a 的正规化子 $N(a)$ 表示 G 中与 a 可交换的元素构成的集合，即 $N(a) = \{x \mid x \in G \wedge xa = ax\}$。证明：$N(a)$ 是 G 的子群。

答案：
【证法一】
$ea = ae$，$e \in N(a) \neq \emptyset$。$\forall x, y \in N(a)$，则 $ax = xa, ay = ya$。因此

$$a(xy) = (ax)y = (xa)y = x(ay) = x(ya) = (xy)a,$$

所以 $xy \in N(a)$。由 $ax = xa$，得 $x^{-1}axx^{-1} = x^{-1}xax^{-1}, x^{-1}ae = eax^{-1}$，即 $x^{-1}a = ax^{-1}$，所以 $x^{-1} \in N(a)$。根据判定定理，$N(a)$ 是 G 的子群。
【证法二】
$ea = ae$，$e \in N(a) \neq \emptyset$。$\forall x, y \in N(a)$，则

$$(xy^{-1})a = x(y^{-1}a) = x(a^{-1}y)^{-1} = x(ya^{-1})^{-1} = x(ay^{-1}) = (xa)y^{-1} = a(xy^{-1})$$

所以 $xy^{-1} \in N(a)$，得证。

Problem 4

设 H 是群 G 的子群，$x \in G$，令 $xHx^{-1} = \{xhx^{-1} \mid h \in H\}$，证明：$xHx^{-1}$ 是 G 的子群，称为 H 的共轭子群。

答案： $e = xex^{-1} \in xHx^{-1}$，因此 xHx^{-1} 非空。任取 $xh_1x^{-1}, xh_2x^{-1} \in xHx^{-1}$，有 $h_1h_2^{-1} \in H$。因此得

$$(xh_1x^{-1})(xh_2x^{-1})^{-1} = xh_1x^{-1}xh_2^{-1}x^{-1} = x(h_1h_2^{-1})x^{-1} \in xHx^{-1}$$

根据判定定理，xHx^{-1} 是 G 的子群。

Problem 5

设 H 和 K 分别为群 G 的 r, s 阶子群，若 r 与 s 互素，证明：$H \cap K = \{e\}$。

答案： 易见 $H \cap K$ 是 H 的子群，也是 K 的子群。由 Lagrange 定理，子群的阶是群的阶的因子，因此 $|H \cap K|$ 整除 r，也能整除 s，从而，$|H \cap K|$ 整除 r 与 s 的最大公因子。由已知 r 与 s 互素，这就得到 $|H \cap K| = 1$，即 $H \cap K = \{e\}$。

Problem 6

证明：若 G 中只有一个 2 阶元，则这个 2 阶元一定与 G 中所有元素可交换。

答案： 证明：设 2 阶元为 a，任取 G 中元素 x，易证 xax^{-1} 也是 2 阶元，因为

$$(xax^{-1})(xax^{-1}) = xa^2x^{-1} = xex = e$$

因此 $|xax^{-1}| = 2$ 或者 1。如果 $|xax^{-1}| = 1$，那么 $xax^{-1} = e$，从而得到 $xa = x$，根据消去律得 $a = e$，与 a 是 2 阶元矛盾。由已知，只有 1 个 2 阶元，必有 $a = xax^{-1}$，从而得到 $ax = xa$。

Problem 7

证明：在群 G 中，如果 $g, h \in G$ 满足 $gh = hg$，并且 $\gcd(|g|, |h|) = 1$，那么 $|gh| = |g||h|$。
「**提示：** 令 $N = |gh||g|$，使用阶的性质和交换律。」

答案： 证明：由

$$(gh)^{|g||h|} = g^{|g||h|}h|g||h| = e,$$

我们知道 $|gh| \mid |g||h|$。由

$$e = (gh)^{|gh||h|} = g^{|gh||h|}h|gh||h| = g|gh||h|,$$

我们有 $|g| \mid |gh||h|$，因为 $\gcd(|g|, |h|) = 1$，所以 $|g| \mid |gh|$。同理有 $|h| \mid |gh|$。所以 $|g||h| \mid |gh|$。得证。

Problem 8

设群 G 有子群 H，H 是正规子群当且仅当

$$\forall g \in G, \forall h \in H : ghg^{-1} \in H.$$

证明：若子群 H 为正规子群，则左右陪集相等。即证 $\forall g \in G, gH = Hg$。

答案： 令 g 为 G 中任意一元素。$gH = Hg$ 当且仅当 $\forall a \in G, a \in gH \Leftrightarrow a \in Hg$。不失一般性，令 $a \in G$ 且 $a \in gH$，则存在 $h \in H$ 使得 $a = gh$。因为 H 是正规子群，所以 $ghg^{-1} \in H$，设 $ghg^{-1} = h'$。故 $a = gh = h'g$，所以 $a \in Hg$ 成立。故 $gH \subseteq Hg$。另一个方向同理可得。

Problem 9

设 H, K 是群 G 的子群，证明 HK 是 G 的子群的充要条件是：$HK = KH$。

答案:

- 充分性：因为 $e \in H, e \in K$，所以 $e \in HK$，从而 HK 非空。$\forall x = hk, y = h_1k_1 \in HK$，这里 $h, h_1 \in H, k, k_1 \in K$，有 $xy^{-1} = (hk)(h_1k_1)^{-1} = h(kk_1^{-1})h_1^{-1}$，记 $k_2 = kk_1^{-1} \in K$。由 $HK = KH$，存在 $h_3 \in H, k_3 \in K$，使得 $k_2h_1^{-1} = h_3k_3$，从而 $xy^{-1} = h(h_3k_3) = (hh_3)k_3 \in HK$。由子群的判定定理，$HK$ 是 G 的子群。
- 必要性：对任意 $x \in HK$，因 HK 是子群，故 $x^{-1} \in HK$。于是存在 $h \in H, k \in K$，使得 $x^{-1} = hk$，从而 $x = k^{-1}h^{-1}$。而 $k^{-1} \in K, h^{-1} \in H$，故 $x \in KH$。证得 $HK \subseteq KH$，另一方向同理可得。

Problem 10

证明：使用阶的概念证明费马小定理。即对素数 p 和任意整数 a，均有 $a^p \equiv \pmod{p}$。
「**提示：** 考虑集合 $\mathbb{Z}_n^* := \{[m]_n \in \mathbb{Z}_n \mid \gcd(m, n) = 1\}$ 在乘法下构成的群。」

答案: 如果 a 为 p 的倍数，那么立即可得。否则 $[a]_p$ 不为零，因此是 $\mathbb{Z}_p^*$ 的成员，群 $\mathbb{Z}_p^*$ 的阶为 $p-1$，故

$$[a]_p^{p-1} = [1]_p$$

也就是

$$[a]_p^p = [a]_p$$

得证。