85

离散数学（2023）作业

吴煜
221900360

2023 年 4 月 28 日

Problem 1

A. 是子群：

$\forall x, y, z \in H, \forall a, b, c \in K, x, y, z, a, b, c \in H \cup K$

$\because \forall x, y, z \in H, \forall a, b, c \in K$ 满足结合律，有单位元，且都有逆元

$\therefore \forall x, y, z, a, b, c \in H \cup K$ 也满足结合律，有单位元，且都有逆元

$\therefore (H \cup K, \circ)$ 为子群

−5

B. 是子群

设 $H \cap K \neq \varnothing, \forall x, y, z \in H \cap K$

$\therefore x, y, z \in H, x, y, z \in K$

假设 $x \circ y = a, a \in K, a \notin H$

$\therefore H$ 不封闭，矛盾

同理：$a \notin H - K$

$\therefore x \circ y = z \in H \cap K$

$\therefore$ 封闭性成立

$\because H, K$ 都为群

$\therefore H \cap K$ 满足结合律，有单位元，都有逆元

$\therefore (H \cap K, \circ)$ 为子群

$C.D.$:

如果 $H \cap K = \varnothing, H - K = H, K - H = K$, 都为群

否则都不是子群

Problem 2

$\because a, x, y \in G$

$\therefore N(a)$ 满足结合律

$\because xa = ax$

$\therefore axy = xay = x(ay) = x(ya)$

$\therefore a(xy) = (xy)a$

$\therefore N(a)$ 满足封闭性

$\because xe = ex = x$

$\therefore N(a)$ 有单位元

$\because \forall x \in N(a), x^{-1}a = x^{-1}ae = x^{-1}(ax)x^{-1} = x^{-1}xax^{-1} = eax^{-1} = ax^{-1}$

$\therefore x^{-1} \in N(a)$

$\therefore N(a)$ 是 G 的子群

Problem 3

1)$e_G = e_H = e$

$\therefore e \in H$

$\therefore xex^{-1} = e \in xHx^{-1}$

$\because exhx^{-1} = xhx^{-1}e$

$\therefore e$ 为 xHx^{-1} 的单位元素

2)$\forall a, b \in H, ab \in H$

$\because xax^{-1} \cdot xbx^{-1} = x(ab)x^{-1}$

$\therefore xabx^{-1} \in xHx^{-1}$

$\therefore xHx^{-1}$ 满足封闭性

3)$\because \forall h \in H, h^{-1} \in H, (xhx^{-1})^{-1} = xh^{-1}x^{-1}$

$\therefore xh^{-1}x^{-1} \in xHx^{-1}$

$\therefore H$ 存在逆元

4)$\forall xax^{-1}, xbx^{-1}, xcx^{-1} \in xHx^{-1}$

$(xax^{-1}xbx^{-1})xcx^{-1} = xax^{-1}(xbx^{-1}xcx^{-1}) = xabcx^{-1}$

$\therefore$ 满足结合律

$\therefore xHx^{-1}$ 为 G 的子群

Problem 4

$e_H = e_K = e_G = e$

若 $H \cup K \neq \{e\}, a \in H \cup K, a \neq e$

$\therefore |a| > 1$

$\therefore |a|||H|, |a|||K|$

$\because |H| = r, |S| = s, r, s$ 互素

$\therefore$ 矛盾

$\therefore H \cup K = \{e\}$

Problem 5

设 a 是 G 中的二阶元

$\therefore a^2 = e, a = a^{-1}$

$\therefore \forall x \in G, (xax^{-1})^2 = e$

若 $xax^{-1} = e$

$\therefore xa = x, a = e$

$\therefore$ 不成立

$\therefore xax^{-1} \neq e$

$\therefore xax^{-1}$ 为二阶元

$\therefore xax^{-1} = a$

$\therefore xa = ax$

$\therefore$ 得证

Problem 6

$\because g,h \in G, hg = gh$
$\therefore (gh)^{|g||h|} = g^{|g||h|}h^{|h||g|} = e^{|h|}e^{|g|} = e$
$\therefore e = e^{|h|} = (gh)^{|gh||h|} = g^{|gh||h|}h^{|h||gh|} = g^{|gh||h|}$
$\therefore |g|||gh||h|$
$\because gcd(|g|,|h|) = 1$
$\therefore |g|||gh|$
同理：$|h|||gh|$
$|g||h|||gh|$
$\therefore |g||h| = |gh|$

Problem 7

设 e 为 G 上的单位元
$\therefore gh = ghe = (ghg^{-1})g$
$\because ghg^{-1} \in H, g \in G, H$ 为 G 的子群
$\therefore (ghg^{-1})g \in Hg$
$\because (ghg^{-1})g = gh \in gH$
同理, 对 hg 有:$g(g^{-1}hg) \in gH$
$g(g^{-1}hg) = hg \in Hg$
$\therefore \forall h \in H, gh, hg \in Hg, gh, hg \in gH$
$\therefore gH = Hg$

Problem 8

设 $p \in \mathbb{P}, a \in \mathbb{Z}, gcd(a,p) = 1, \mathbb{Z}_p^* = \{x \in \mathbb{Z}_p : gcd(x,p) = 1\}$
$\therefore (\mathbb{Z}_p^*, \cdot)$ 是一个群
$\therefore |\mathbb{Z}_p^*| = p - 1$
$\because a \in \mathbb{Z}_p^*$
$\therefore |a| \mid |\mathbb{Z}_p^*|$(拉格朗日定理)
$\therefore \exists k \in \mathbb{N}^+, s.t. a^k = 1(mod\ p)$
$\because k|p-1$
$\therefore a^{p-1} = 1(mod\ p)$
$\therefore a^p = a(mod\ p)$