100

# 离散数学（2023）作业 17 - 子群与群的分解

杨辰

221900328

2023 年 4 月 27 日

## 1 Problem 1

解：

A：不是。当且仅当 H$\subseteq K$ 或 $K \subseteq H$ 时 $H \cup K$ 是 G 的子群。若 H$\not\subseteq K$ 且 $K \not\subseteq K$, 那么存在 h,k 使得 $h \in H \vee h \notin K$,$k \in k \vee K \notin H$, 所以 hk$\notin H$. 若不然，则 $h^{-1} \in H$, 所以 $k = h^{-1}(hk) \in K$, 与假设矛盾，同理可证 $hk \not\subseteq K$, 从而 $hk \notin H \cup K$, 这与 $H \cup K$ 是 G 的子群矛盾。

B: 是。由 e$\in H \cap K$ 知 $H \cap K$ 非空。任取 $a, b \in H \cap K$, 则 $a \in H, a \in K, b \in H, b \in K$, 所以 $b^{-1} \in H$, 所以 $ab^{-1} \in H$, 同理 $ab^{-1} \in K$, 所以 $ab^{-1} \in H \cap K$, 所以 $H \cap K$ 是 G 的子群。

C: 不是。因为 e$\in H, e \in K$, 所以 $e \in H \cap K$,$e \notin K - H$, 所以 $K - H$ 无单位元，不构成 G 的子群。

D: 不是。同 C

## 2 Problem 2

证明：任取 $x, y \in N(a)$, 则有 $xa = ax, ya = ay$, 所以 $(xy)a = x(ya) = x(ay) = (xa)y = (ax)y = a(xy)$, 所以 $xy \in N(a)$, 又 $a \in G, x \in G$, 所以 $x = axa^{-1}$, 所以 $x^{-1}a = (a^{-1}x)^{-1} = (a^{-1}axa^{-1})^{-1} = (xa^{-1})^{-1} = ax^{-1}$, 所以 $x^{-1} \in N(a)$, 所以 $N(a)$ 为 G 的子群。

## 3 Problem 3

证明：任取 $h_1, h_2 \in H$, 又 H 是 G 的子群，所以 $h_1, h_2$ 均有逆元且 $h_1 h_2^{-1} \in H$。又 $x \in G$,$xh_1x^{-1}, xh_2x^{-1} \in xHx^{-1}$, 所以 $(xh_1x^{-1})(xh_2x^{-1})^{-1} = (xh_1x^{-1})(xh_2^{-1}x^{-1}) = xh_1h_2^{-1}x^{-1} = x(h_1h_2^{-1})x^{-1} \in xHx^{-1}$, 所以 $xHx^{-1}$ 是 G 的子群。

## 4 Problem 4

证明：先证 $H \cap K \leq H$, 任取 $h_1, h_2 \in H \cap K$, 则 $h_1, h_2 \in H$, 所以 $h_2^{-1} \in H$, 所以 $h_1 h_2^{-1} \in H$, 则 $H \cap K \leq H$, 同理可证 $H \cap K \leq K$, 所以 $|H \cap K|$ 为 r 和 s 的公因子，又 r 与 s 互素，所以 $|H \cap K|$=1, 所以 $H \cap K = \{e\}$。

## 5 Problem 5

证明：设该二阶元为 a，则 $a^2 = e$, 设 $\forall x \in G$, 又 $(xax^{-1})(xax^{-1}) = xaax^{-1} = xx^{-1} = e$, 而 G 中的二阶元只有一个, 所以 $a = xax^{-1}$, 右乘 x 得 $ax = xa$, 所以该二阶元与 G 中元素均可交换。

## 6 Problem 6

证明：设 $|g| = m, |h| = n, |gh| = r$, 则 $(gh)^r = e$, 因为 $gh = hg$, 所以 $(gh)^{mn} = g^{mn}h^{mn} = (g^m)^n(h^n)^m = e$, 所以 $r|mn$, 且 $r \leq mn$, 又 $e = (gh)^{rm} = g^{rm}h^{rm} = h^{rm}$, 所以 $n|rm$, 又 $gcd(m, n) = 1$, 所以 $n|r$, 同理 $m|r$, 所以 $mn|r$, 则 $mn \leq r$, 所以 $mm = r$, 即 $|gh| = |g||h|$。

## 7 Problem 7

证明：对 $\forall g \in G$ 有 $ghg^{-1} \in H$, 任取 $x \in gH$,$\exists h \in H, s.t \quad x = gh$, 且 $xg^{-1} = ghg^{-1} \in H$, 所以 $\exists h' \in H, s.t \quad xg^{-1} = h'$, 所以 $x = h' \in Hg$, 所以 $gH \subseteq Hg$。
另一方面，对 $Hg$ 中任一元素 x，$\exists h \in H, s.t \quad x = hg$, 且 $g^{-1}x = g^{-1}hg = g^{-1}h(g^{-1})^{-1} \in H$, 即 $\exists h' \in H, s.t \quad g^{-1}x = h'$, 所以 $x = gh' \in gH$, 所以 $Hg \subseteq gH$, 所以 $gH = Hg$。

## 8 Problem 8

证明：考虑乘法同余群 $\mathbb{Z}_{|}^* = \{1, 2, ..., p - 1\}$, 其中 p 为质数。对于每一个群元素 a，可以得到一个循环群 $< a >= \{a^m : m \in \mathbb{Z}_{|\ni|}\}$，而 $a^{|a|} \equiv 1 mod p$, 因为 $< a >$ 也是 $\mathbb{Z}_{|}^*$ 的子群，所以由拉格朗日定理得，它的阶数一定可以整除 $|\mathbb{Z}_{|}^*| = p - 1$, 即存在一个整数 n，使得 p-1=$|a| \cdot n$, 又而 $a^{|a|} \equiv 1 mod p$，所以 $a^{p-1} = (a^{|a|})^n \equiv 1 \quad mod \quad p$，证毕。