100

离散数学（2023）作业 17 - 子群与群的分解

万鹏举
221900342

2023 年 4 月 27 日

1 Problem1

A. 若有 H⊆K, 或 K⊆H, 则是子群。否则不是。
B 是，CD 不是。

2 Problem2

首先，e 满足条件属于 N
任取 a，b 属于 N，则对于任意 x 属于 N 有
$(ab^{-1})x = ab^{-1}x = ab^{-1}(x^{-1})^{-1} = a(x^{-1}b)^{-1} = a(bx^{-1})^{-1} = (ax)b^{-1} = (xa)b^{-1} = x(ab^{-1})$
故 ab^{-1} 属于 N，由定理可知，N 是 G 的一个子群。

3 Problem3

首先，e 满足条件属于 xHx^{-1}
任意取 $xh_1x^{-1}, xh_2x^{-1} \in xHx^{-1}$,
又由 $h_1, h_2 \in H$ 知，$h_1h_2^{-1} \in H$，则
$xh_1x^{-1}(xh_2x^{-1})^{-1} = xh_1x^{-1}xh_2^{-1}x^{-1} = xh_1h_2^{-1}x^{-1}$,
其中 $h_1h_2^{-1} \in H$, 故 $xh_1x^{-1}(xh_2x^{-1})^{-1} \in xHx^{-1}$。
则说明 xHx^{-1} 是 G 的子群。

4 Problem4

由题，不妨令
$H =< a >= \{a^0 = e, a^1, \ldots, a^{r-1}\}$
$K =< b >= \{b^0 = e, b^1, \ldots, b^{s-1}\}$

如果 $H \cap K$ 不止有单位元 e，说明有 $a^i = b^j$,(其中 i，j 显然不是 r，s 的倍数，否则两数均等于 e)，
则有 $(a^i)^s = (b^j)^s$, 即 $a^{is} = e$, 即 r|is,
但由于 i 不是 r 的倍数,s 与 r 互质，r|is 不可能成立，则说明假设矛盾，$H \cap K = \{e\}$

5 Problem5

令这个 2 阶元为 a，由题可知 $a^2 = e$，
任取 x 属于 G，则有 $(xax^{-1})(xax^{-1}) = xa^2x^{-1} = xx^{-1} = e$, 即 $|xax^{-1}|$=2 或 1
若 $xax^{-1} = 1$，则有 $xax^{-1} = e$, 即 $xa = x$，则 a=e 与 a 为 2 阶元矛盾。
若 $xax^{-1} = 1$，则有 $xax^{-1} = a$, 即 $xa = ax$, 则 a 可与 G 中任意元素交换。

6 Problem6

假设 g 的阶为 a，h 的阶为 b，则有 $g^a = h^b = 1$,gcd(a,b)=1。
由于满足交换律，可知 $(gh)^i = g^ih^i =$,
则对于 $(gh)^i = e$，需满足 $g^i = e\ h^i = e$,
故 i 的最小值应该是 ab 的最小公倍数，又 gcd(a,b)=1，故 i=ab=|g||h|
故 gh 的阶为 |g||h|，即 |gh|=|g||h|。

7 Problem7

由题，对于 $\forall g \in G, \forall h \in H$, 有：
$ghg^{-1} \in H \Leftrightarrow \exists h(h \in H \wedge ghg^{-1} = h) \Leftrightarrow \exists h(h \in H \wedge gh = hg) \Leftrightarrow gH = Hg$
故原命题成立。

8 Problem8

构造集合 S，其中 p 为素数，满足若 gcd(a,p)=1, 则 $[a]_p \in S$,
这样的集合 S 在乘法下构成群，|S|=p-1, 单位元为 $[1]_p$。
若 $[a]_{pi} \in S$, 则对于其中由 $< [a]_{pi} >$ 构成的子群，其阶数一定是 p-1 的因数。
假设其阶数为 i1，$i2 = \frac{p-1}{i1}$ 为整数，则有 $[a]_{pi}^{p-1} = ([a]_{pi}^{i1})^{i2} = e^{i2} = e$。
根据该集合含义，即 $a^{p-1} \equiv 1(modp)$, 即 $a^p \equiv a(modp)$。
证毕。