Problem Set 19: 子群与群分解

提交截止时间：5 月 13 日 10:00

Problem 1

设 H 是 G 的子群，证明 H 在 G 中的所有左陪集中有且只有一个是 G 的子群，即 ∃!K ∈ {aH | a ∈ G} 使得 K 是 G 的子群。

```
当a = e, aH = H, H为G的子群
当a != e, a ∈ G - H，即 ∀ x ∈ H, a != e ^ (-1)
所以e ∉ aH
故aH只有在a == e时为G的子群
```

Problem 2

设 G 是有限群，A 与 B 是 G 的两个非空子集，且 |A| + |B| > |G|，求证 G = AB

```
由于 |A| + |B| > |G|，根据鸽巢原理，必然存在 a1, a2 ∈ A 和 b1, b2 ∈ B，使得 a1 ∘ b1 = a2 ∘ b2。
所以存在 g = a1 ∘ b1 = a2 ∘ b2 ∈ G。
所以g ∘ b2^(-1) = a1 ∘ (b1 ∘ b2 ^ (-1)) = a2
因为 a1 和 a2 都在 A 中，所以 a1 ∘ (b1 ∘ b2 ^ (-1)) 和 a2 都在 AB 中。
所以g ∈ AB
由于 g 是任意的群元素，因此 G ⊆ AB。
由于 AB ⊆ G，我们得出 AB = G。
综上所述，命题得证
```

Problem 3

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

令G = xHx^{−1}

封闭性：存在，$\forall a, b \in G, a \circ b = x \circ a \circ x^{-1} \circ x \circ b \circ x^{-1} = x \circ a \circ b \circ x^{-1}$

结合性：存在，$\forall a, b, c \in G, (x \circ a \circ x^{-1} \circ x \circ b \circ x^{-1}) \circ x \circ c \circ x^{-1} = x \circ a \circ x^{-1} \circ (x \circ b \circ x^{-1} \circ x \circ c \circ x^{-1})$

单位元：存在，$\forall a \in G, x \circ e \circ x^{-1} \circ x \circ a \circ x^{-1} = x \circ a \circ x^{-1}$

可逆性：存在，$\forall a \in G, x \circ a \circ x^{-1} \circ x \circ a^{-1} \circ x^{-1} = x \circ e \circ x^{-1}$

故xHx^{-1}为G的子群

Problem 4

设 H 和 K 分别为群 G 的 r, s 阶子群，若 r 与 s 互素，证明 H ∩ K = {e}.

```
设 x ∈ H ∩ k x ∈ H ∩ K
由于 H 和 K 都是 G 的子群，则 x 的阶必须整除 r 和 s。由于 r 和 s 互素，
所以x 的阶只能是 1，故x=e。
```

Problem 5

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。

```
要证：a ∘ b = b ∘ a
需证：a = b ∘ a ∘ b ^ (-1)
需证：(b ∘ a ∘ b ∘ ^ (-1)) ^ 2 = e
(b ∘ a ∘ b ∘ ^ (-1)) ∘ (b ∘ a ∘ b ∘ ^ (-1)) = b ∘ a ∘ a ∘ b ^ (-1) = e
故命题得证
```

Problem 6

证明：在群 G 中，如果 g, h ∈ 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）

$(gh)^{|g||h|} = g^{|g||h|}h|g|h| = e$
$e = (gh)^{|gh||h|} = g^{|gh||h|}h|gh||h| = g|gh||h|$
所以$|g|$整除$|gh||h|$，
因为$gcd(|g|, |h|) = 1$，所以$|g|||gh|$
同理有$|h|$整除$|gh|$
所以$|g||h|$整除$|gh|$

Problem 7

设群 G 有子群 H，H 是正规子群当且仅当
∀g ∈ G, ∀h ∈ H : ghg −1 ∈ H
证明: 如果群 G 有且只有一个 d 阶子群，那么这个子群是正规的。

Problem 8

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$a^p \equiv a(modp)$。

如果a为p的倍数，显然成立
否则$[a]_p$不为零，则$[a]_p \in Z_p^*$的成员，群Z_p^*的阶为$p-1$，故
$[a]_p^{p-1} = [1]_p$