100

离散数学（2023）作业 17

张波
221900326

2023 年 5 月 3 日

1 Problem 1

A. 不一定是子群，因为 $H \cup K$ 可能不满足群的封闭性质，例如 H 和 K 不交时。

B. 是子群，因为 $H \cap K$ 一定满足群的封闭性、结合性、恒等元和逆元的存在性。

C. 不一定是子群，因为 $K - H$ 可能不满足群的封闭性质，例如 H 是 K 的真子集时。

D. 不一定是子群，因为 $H - K$ 可能不满足群的封闭性质，例如 H 不包含恒等元时。

2 Problem 2

1. 封闭性：由于 a 是 G 中的元素，因此存在 $e \in G$ 使得 $ae = ea = a$。对于任意的 $x, y \in N(a)$，有

$$xya = x(ay) = x(ya) = (xy)a,$$

$$axy = a(xy) = (ax)y = (xa)y = x(ay) = xya.$$

因此 $xy \in N(a)$，即 $N(a)$ 对于乘法运算是封闭的。

2. 结合性：由于 G 是一个群，因此对于任意的 $x, y, z \in G$，有 $x(yz) = (xy)z$。因此，对于任意的 $x, y, z \in N(a)$，有

$$x(yz)a = x(ya)z = (xy)az = (xy)(az) = (xy)za,$$

$$ax(yz) = a(xy)z = (ax)yz = (xa)yz = x(ay)z = x(ya)z = (xy)az.$$

因此 $x(yz) \in N(a)$，即 $N(a)$ 对于乘法运算是结合的。

3. 逆元存在性：对于任意的 $x \in N(a)$，由于 a 是 G 中的元素，因此有

$$xa = ax.$$

因此有

$$xax^{-1} = ax^{-1}x = ae = a,$$

$$x^{-1}ax = ax^{-1}x = e.$$

因此 $x^{-1} \in N(a)$，即 $N(a)$ 对于乘法运算存在逆元。

因此 $N(a)$ 是 G 的子群。

3 Problem 3

证明：

1. 封闭性：对于任意的 $xhx^{-1}, xkx^{-1} \in xHx^{-1}$，由于 H 是 G 的子群，因此 $hk^{-1} \in H$，从而有

$$xhx^{-1}xkx^{-1} = xhk^{-1}x^{-1} \in xHx^{-1}.$$

因此 xHx^{-1} 对于乘法运算是封闭的。

2. 结合性：由于 G 是一个群，因此对于任意的 $x, y, z \in G$，有 $x(yz) = (xy)z$。因此，对于任意的 $xhx^{-1}, xkx^{-1}, xmx^{-1} \in xHx^{-1}$，有

$$xhx^{-1}(xkx^{-1}xmx^{-1}) = xh(km)x^{-1} \in xHx^{-1},$$

$$(xhx^{-1}xkx^{-1})xmx^{-1} = xh(kx)mx^{-1} \in xHx^{-1}.$$

因此 xHx^{-1} 对于乘法运算是结合的。

3. 单位元存在性：由于 H 是 G 的子群，因此 $e \in H$。因此有

$$xex^{-1} = ee = e.$$

因此 xHx^{-1} 中存在单位元。

4. 逆元存在性：对于任意的 $xhx^{-1} \in xHx^{-1}$，由于 H 是 G 的子群，因此 $h^{-1} \in H$。因此有

$$(xhx^{-1})^{-1} = xh^{-1}x^{-1} \in xHx^{-1}.$$

因此 xHx^{-1} 中存在逆元。

综上所述，xHx^{-1} 是 G 的子群，称为 H 的共轭子群。

4 Problem 4

证明：

设 H 和 K 分别为 G 的 r 阶子群和 s 阶子群，且 r 与 s 互素。由拉格朗日定理，r 整除 $|G|$，s 整除 $|G|$。

令 $x \in H \cap K$ 且 $x \neq e$，由于 $x \in H$，因此 x 的阶数 r' 整除 r，即 $x^{r'} = e$，同时由于 $x \in K$，因此 x 的阶数 s' 整除 s，即 $x^{s'} = e$。由于 r 和 s 互素，因此存在整数 m 和 n，使得 $mr' + ns' = 1$。从而有

$$x = x^{mr'+ns'} = (x^{r'})^m (x^{s'})^n = e^m e^n = e,$$

这与 $x \neq e$ 矛盾。因此，$H \cap K$ 只能包含单位元 e，即 $H \cap K = \{e\}$。

综上所述，当 H 和 K 是 G 的 r 阶和 s 阶子群，且 r 与 s 互素时，$H \cap K = \{e\}$。

5 Problem 5

证明：

设 a 是 G 中唯一的 2 阶元，即 $a^2 = e$，其中 e 表示 G 的单位元。

对于任意 $g \in G$，我们需要证明 $ag = ga$。首先注意到，$(ag)^2 = a^2g^2 = g^2$，由于 a 是 G 中唯一的 2 阶元，因此 $g^2 = e$ 或 $g^2 = a^2 = e$。

若 $g^2 = e$，则 g 是 G 中的 2 阶元，由于 a 是 G 中唯一的 2 阶元，因此 $g = a$。因此，

$$ag = aa = a^2 = e = a^2g^2 = ga.$$

若 $g^2 = a^2 = e$，则 g 是 a 的共轭元，即存在 $x \in G$，使得 $g = xax^{-1}$。因此，

$$ag = axax^{-1} = xaax^{-1} = xae = xe = xax^{-1}a = ga.$$

综上所述，对于任意 $g \in G$，都有 $ag = ga$，即 a 与 G 中所有元素可交换。

6 Problem 6

证明:

设 $|g| = r$，$|h| = s$，则 $|gh|$ 为 $\langle gh \rangle$ 的阶。由于 $gh = hg$，我们有

$$(gh)^{rs} = (g^r)^s(h^s)^r = e.$$

因此，$|gh|$ 必定是 rs 的因数。

另一方面，由于 $gcd(r, s) = 1$，根据扩展欧几里得算法，存在整数 x, y，使得 $xr + ys = 1$。因此，

$$(gh)^{xr+ys} = g^{xr}h^{ys} = h^{ys}g^{xr} = (gh)^1 = gh.$$

因此，$|gh|$ 是 $|g|$ 和 $|h|$ 的倍数，即 $|gh|$ 是 rs 的倍数。综上所述，$|gh|$ 是 rs 的因数，且是 rs 的倍数，因此 $|gh| = rs$。

又因为 g 和 h 可交换，所以有 $|gh| = |hg|$，因此 $|gh| = |hg| = rs = |g||h|$。

因此，证毕。

7 Problem 7

证明:

设 H 是 G 的正规子群，我们需要证明 $\forall g \in G, gH = Hg$。

对于任意 $g \in G$，我们有：

$$gH = \{gh : h \in H\}$$

由于 H 是正规子群，因此 $\forall h \in H, ghg^{-1} \in H$。因此，

$$gh = ghg^{-1}g \in gHg^{-1}$$

也就是说，$gH \subseteq gHg^{-1}$。

同理，$\forall h \in H$，我们有

$$h = geg^{-1}h \in Hg^{-1}$$

也就是说，$H \subseteq g^{-1}Hg$。

综上所述，$gH \subseteq gHg^{-1} \subseteq gH$，且 $H \subseteq g^{-1}Hg \subseteq Hg$，因此 $gH = Hg$。

因此，证毕。

8 Problem 8

证明：

我们考虑集合 $Z_p^* := \{[m]_p \in \mathbb{Z}_p | \gcd(m,p) = 1\}$，其中 $[m]_p$ 表示 m 在模 p 意义下的剩余类，即 $[m]_p = m \bmod p$。显然，Z_p^* 在模 p 意义下构成了一个乘法群。

对于任意 $a \in Z_p^*$，我们考虑它的阶 k，即 $a^k \equiv 1 \pmod p$ 且 k 最小。因为 a 和 p 互质，因此根据欧拉定理，$a^{\varphi(p)} \equiv 1 \pmod p$，其中 φ 是欧拉函数，表示小于 p 的与 p 互质的正整数个数。

因此，我们可以将 k 分解为 $k = r \cdot \varphi(p)$，其中 r 和 $\varphi(p)$ 互质。我们需要证明的是 $k = \varphi(p)$。

假设 $k < \varphi(p)$，则 $r < \frac{\varphi(p)}{r}$，也就是说，存在一个小于 $\varphi(p)$ 且与 $\varphi(p)$ 互质的正整数 q，满足 $r < q$。因此，$a^{qr} \equiv a^k \equiv 1 \pmod p$。

另一方面，根据拉格朗日定理，Z_p^* 中任意元素的阶都是 Z_p^* 的阶的因子。因为 r 和 $\varphi(p)$ 互质，因此 a^r 的阶为 $\varphi(p)$。因此，$a^{qr} \equiv 1 \pmod p$ 意味着 a^r 的阶也是 q 的倍数。

这与我们假设的 $r < q$ 矛盾，因此 k 必须等于 $\varphi(p)$，也就是说 $a^{\varphi(p)} \equiv 1 \pmod p$。

现在我们考虑费马小定理 $a^{p-1} \equiv 1 \pmod p$。因为 a 和 p 互质，因此 $a \in Z_p^*$，根据刚才的结论，$a^{\varphi(p)} \equiv 1 \pmod p$。因为 $\varphi(p) = p - 1$，所以 $a^{p-1} \equiv 1 \pmod p$。

因此，费马小定理得证。