100

离散数学（2023）作业 17

邵宇轩
221900406

2023 年 4 月 30 日

1 Problem 1

(2) 是
其余均不是

2 Problem 2

(1) 封闭性：$\forall x, y \in N(a)$:
xa = ax , ya = ay
xya = xay = axy
∴ 是封闭的
(2) ea = ae 显然有单位元
(3) 逆元：
$\forall x, xa = ax$
$x^{-1}a = x^{-1}ae = x^{-1}axx^{-1} = eax^{-1} = ax^{-1}$
∴ 每个元素均有逆元
∴ N(a) 是群，是子群得证

3 Problem 3

设 a = xhx^{-1}
b = xmx^{-1}
b^{-1} = x$m^{-1}x^{-1}$
ab^{-1} = xhx^{-1}x$m^{-1}x^{-1}$
= xh$m^{-1}x^{-1}$

由子群的判定定理可知:
$\because$ m $\in$ H , h $\in$ H
$\therefore$ hm^{-1} $\in$ H
$\therefore$ ab^{-1} $\in$ xHx^{-1}

4 Problem 4

假设 H = { $e, a^2 ... a^{r-1}$ }
K = { e,$b^2, b^3, ... b^{s-1}$ }
$a^r = e, b^s = e$
使用反证法进行证明:
假设存在 i,j ， 使得 $a^i = b^j$
$a^r = b^{\frac{js}{i}}$
$\because$ r,s 互质
$\therefore$ $\frac{js}{i}$ 为整数
当 j > i 时:
$\exists$ 0<k<s , $b^{\frac{js}{i}} = b^k = e$
则 b 的阶数为 k<s
与条件矛盾
j < i 时同理可得到则 b 的阶数 <s
与条件矛盾
$\therefore$ 假设不成立
得证

5 Problem 5

假设 a^2 = e
a-1 = a
考察 xax^{-1} , x 为任意元素
$(xax^{-1})(xax^{-1}) = e$
$\therefore$ xax^{-1} 为二街元素或 xax^{-1} = e
显然 xax^{-1} 为二阶元素
a = xax^{-1}
$\therefore$ ax = xa
满足交换律

6 Problem 6

假设：g 的阶数为 k,h 的结束为 t
则有 k，t 互质
设 m = gh = hg
m 的阶数为 u
$m^{kt} = g^{kt}h^{kt} = (g^k)^t(h^t)^k = e$
∴ u|kt,u<=kt
设 iu = kt
uk = k*kt / i
$m^{uk} = g^{uk}h^{uk} = (g^k)^u h^{uk} = (g^k)^u h^{k*k*t/i} = e$
∴ t|uk
同理可得 k|tu
∵ t,k 互质
∴ kt | u
∴ u = kt 得证

7 Problem 7

gH = $\{gh|h \in H\}$
Hg = $\{gh|h \in H\}$
$\forall h_i,\ gh_ig^{-1} = t_i \in H$
$gh_i = t_ig$
验证单射：
若 $gh_1 = t_1g, gh_2 = t_1g$
$gh_1g^{-1} = gh_2g^{-1}$
由群的消去律可知：$h_1 = h_2$
∴ 是单射
而 h,t ∈ H
∴ 是满射
∴ 是一个双射，对应两个集合中元素相等
gH = Hg 得证

8 Problem 8

考虑集合 Z*:= $\{[m]_n \in Z_n|gcd(m,n) = 1\}$ 在乘法下构成的群
$Z^* = \{[m]_p \in Z_n|gcd(m,p) = 1\}$

$\forall t \in Z^*$ 假设 t 的阶数为 k

则有：$t^k \mod p = 1$

t ∈ { 1,2,...p-1 } 共有 p - 1 个元素

∴ 群的阶数为 p - 1

则 $\forall k_i, k_i | p-1$

令 t = a，有：

p | a^k - 1

k | p - 1

∴ $a^{p-1} - 1 = (a^k - 1) \times M$ ，M 为 a 的一个多项式

∴ p | a^{p-1} - 1

即 $a^p \equiv 1 (\mathrm{mod}\ p)$