离散数学（2023）作业 17

周帛岑
221900309

2023 年 5 月 16 日

1 Problem 1

解：A,B

订正：应为 B

A 中可能存在元素不满足封闭性

2 Problem 2

h 证：任取，m，n∈N(a), 我们有 am = ma 且 an = na

对于 an = na, 在两式的左右两侧左右同时运算 n^{-1}, 我们有 $an^{-1} = n^{-1}a$

对于 $mn^{-1}a$，我们在其左侧乘上 a

有 $mn^{-1}a = amn^{-1}nn^{-1} = amn^{-1}nn^{-1} = amn^{-1}a = amn^{-1}$

于是 N(a) 是 G 的子群.

3 Problem 3

证：任取 xax^{-1} 和 $xb^{-1}x$∈H

对于 $xax^{-1}(xb^{-1}x)^{-1}$, 原式等于 $xax^{-1}x^{-1}b^{-1}x = xab^{-1}x$

于是 H 为 G 的子群

4 Problem 4

证：由题可知，H = {x|x$^r = e\}, K = \{x|x^s = e\}$

又 s 与 r 互质，即不存在 r = ms，使 m 为整数

即对于任意 m，若 x≠e,$(x^s)^m \neq$ x^r， k∈K,k≠e, 这样的 k 均不在 H 中，故 H∩K = e.

5 Problem 5

证：由题可知，不妨设这个数为 a，即 aa = e，a = a^{-1}, 任取 m∈G

$mam^{-1}(mam^{-1})$ = e, 故 mam^{-1} 为二阶或一阶元

又由于题设，mam^{-1} 为一个一阶元，即 mam^{-1} = a

故有 ma = am

6 Problem 6

证：

订正：当时未写出

证：

gh$^{|g||h|} = g^{|g||h|}h^{|g||h|} = e$

又 |gh| 能整除 |g||h|

且 e = gh$^{|gh||h|} = g^{|gh||h|}h^{|gh||h|} = g^{|gh||h|}$

故此时 |g| 能整除 |gh||h|, 又 gcd(g,h) = 1 故此时 |g| 能整除 |gh|

同理，|h| 也能整除 |gh|，故 |g||h| 能整除 |gh|

故 |gh| = |g||h|

7 Problem 7

证：任取 h∈H, 我们有 ghg^{-1} ∈ H

即我们有 gHg^{-1} = H

不妨假设 ∃g ∈ G, 有 gH≠ Hg 此时有 $gHg^{-1} \neq$ H

与题意矛盾，故假设不成立，命题得证

8 Problem 8

证: 由题可知，除 p 的非零余数关于同余乘法形成一个运算

显然，由于 p 为质数，故该集合中的元素相乘后仍不能被 p 整除，且结果仍落于集合中，满足封闭性

显然，由于运算为带余除法，故满足结合律

显然，单位元为 1

对于逆元，任取 a 在该集合中，假设我们有 a∘b = 1 即 ab = 1(mod p)

即 ab + kp = 1

又 a 与 p 互质，gcd(a,p) = 1

即有 sa + tp = 1 取 b = s，k = p 即可

故我们总能找到这样的 b，每一个元素均存在逆元

故其构成一个群

由群论的拉格朗日定理，群的阶数为 p-1

对于任意一个元素，其阶为 $\frac{p-1}{k}$, 则 $a^{\frac{p-1}{k}}$ = 1(mod p)

即 a^{p-1} = 1(mod p)