NIS2312-01 Fall 2023-2024

信息安全的数学基础 (1)

Answer 8-9

2023 年 10 月 20 日

Assignment 8

Problem 1

判断下列映射是否为同态映射:

(1) 定义映射 $\phi : \mathbf{R}^* \to \{\pm 1\}$, 其中 $\phi(x) = \frac{x}{|x|}$, $x \in \mathbf{R}^*$, $|x|$ 代表 x 的绝对值.

(2) 定义映射 $\pi : \mathbf{C}^* \to \mathbf{R}^*$, 其中 $\pi(a + b\sqrt{-1}) = a^2 + b^2$.

(3) 定义映射 $\varphi : \mathbf{R}^2 \to \mathbf{R}$, 其中 $\varphi((x, y)) = x + y$.

解:

(1) 对任意的 $x, y \in \mathbf{R}^*$, 有 $\phi(xy) = \frac{xy}{|xy|} = \frac{x}{|x|} \cdot \frac{y}{|y|} = \phi(x)\phi(y)$ 成立, 故映射是群同态映射.

(2) 对任意的 $a + b\sqrt{-1}, c + d\sqrt{-1} \in \mathbf{C}^*$, 有 $\pi((a + b\sqrt{-1}) \cdot (c + d\sqrt{-1})) = \pi(ac - bd + (ad + bc)\sqrt{-1}) = (ac - bd)^2 + (ad + bc)^2 = a^2c^2 + b^2d^2 + a^2d^2 + b^2c^2$, 同时 $\pi(a + b\sqrt{-1}) \cdot \pi(c + d\sqrt{-1}) = (a^2 + b^2)(c^2 + d^2) = a^2c^2 + b^2d^2 + a^2d^2 + b^2c^2$, 故 $\pi(a + b\sqrt{-1}) \cdot \pi(c + d\sqrt{-1}) = \pi((a + b\sqrt{-1}) \cdot (c + d\sqrt{-1}))$, 故映射是群同态映射.

(3) 对 $\forall (x, y), (x', y') \in \mathbf{R}^2$, 有 $\varphi((x, y) + (x', y')) = \varphi((x + x', y + y')) = x + x' + y + y' = x + y + x' + y' = \varphi((x, y)) + \varphi((x', y'))$, 故映射是群同态映射.

Problem 2

[hint: 考虑单位元的象] 能否找到一个非平凡同态映射 ϕ, 此映射将群 $(\mathbf{Z}_4, +)$ 映射到群 $(\mathbf{Z}_5, +)$. (平凡映射指将任意元素映射为单位元, 见书 82 页例 1).

解: 考虑非单位元 $a \in \mathbf{Z}_4$, 显然 $\mathrm{ord}(a) = 4$, 因此有 $0 = f(0) = f(4 \times a) = 4 \cdot f(a) = 0$, 因此确定 $\mathrm{ord}(f(a)) \mid 4$. 但 $f(a) \in \mathbf{Z}_5$, 故 $\mathrm{ord}(f(a)) \mid 5$, 故 $\mathrm{ord}(f(a)) = 1$ 即 $f(a) = 0$. 因此找不到非平凡同态映射.

Problem 3

假设 G_1 和 G_2 是两个有限群且满足条件 $(|G_1|, |G_2|) = 1$, 同时假设 $\phi : G_1 \to G_2$ 是一个群同态. 证明:

(1) $\forall y \in \phi(G_1)$, $\mathrm{ord}(y) \mid |G_1|$;

(2) $ker(\phi) = G_1$.

解:

(1) 因为 G_1 是有限群, 故 $\mathrm{ord}(y) \mid \mathrm{ord}(\phi^{-1}(a)) \mid |G_1|$(83 页定理 2.3.1(4)).

(2) 由于 $(|G_1|, |G_2|) = 1$, 且 $\mathrm{ord}(y) \mid |G_2|$, 故 $\mathrm{ord}(y) = 1$, 即 $y = e$, 因此 $ker(\phi) = G_1$.

Assignment 9

Problem 1

设 $\mathrm{ord}(a) = 18$, 求 $\langle a^{14} \rangle \cap \langle a^{10} \rangle$ 的生成元.

解: 根据 40 页的定理 1.5.5 的推论 1 可知, 因为 $(18, 14) = 2$, 则 $\langle a^{14} \rangle = \langle a^2 \rangle$, 同理 $\langle a^{10} \rangle = \langle a^2 \rangle$. 因此 $\langle a^{14} \rangle \cap \langle a^{10} \rangle = \langle a^2 \rangle$. 注意到 $\mathrm{ord}(a^2) = 9$, 则 $\langle a^k \rangle$ 是群 $\langle a^2 \rangle$ 的生成元, 其中 $(18, k) = 2$, 解得 $k = 2, 4, 8, 10, 14, 16$.

Problem 2

设 ϕ 是群 G 到群 G' 的同构映射, $a \in G$. 证明:

$$\mathrm{ord}(a) = \mathrm{ord}(\phi(a)).$$

解: 设 $d = \mathrm{ord}(a)$, 故 $a^d = e$, 因此 $\phi(a)^d = \phi(a^d) = \phi(e) = e$, 即 $\mathrm{ord}(\phi(a)) \mid d$;

ϕ 存在逆函数 ϕ^{-1} 同样是同构映射, 设 $k = \mathrm{ord}(\phi(a))$, 故 $\phi(a)^k = e$, 因此 $e = \phi^{-1}(e) = \phi^{-1}(\phi(a)^k) = \phi^{-1}(\phi(g))^k = g^k$.

综上, $\mathrm{ord}(a) = \mathrm{ord}(\phi(a))$.

Problem 3

设 G 是群, $a, b \in G$, $\mathrm{ord}(a) = m$, $\mathrm{ord}(b) = n$. 证明: 如果 $ab = ba$ 且 $\langle a \rangle \cap \langle b \rangle = \{e\}$, 则 $\mathrm{ord}(ab) = [m, n]$.

解: 设 $\mathrm{ord}(ab) = d$, 则 $(ab)^d = e$, 则 $a^d = b^{-d} \in \langle a \rangle \cap \langle b \rangle = \{e\}$, 故 $\mathrm{ord}(a) \mid d$ 和 $\mathrm{ord}(b) \mid d$, 因此 $[m, n] \mid d$;

又因为 $(ab)^{[m,n]} = a^{[m,n]} b^{[m,n]} = e$ 有 $d \mid [m, n]$;

因此有 $\mathrm{ord}(ab) = [m, n]$.

Problem 4

设 p 是素数. 证明每一个 p 阶群都是循环群, 且以每一个非单位元的元素作为它的生成元.

证明: $\forall a \neq e \in G$, 有 $\operatorname{ord}(a) \mid |G|$, 故 $\operatorname{ord}(a) = p$ 恰好等于 G 的阶, 故 $G = \langle a \rangle$.

Problem 5

证明: 任一偶数阶群必含有阶为 2 的元素.

解: 考虑集合 $B = \{x \in G : x^{-1} \neq x\}$, 显然对任意 $x \in B$, $\operatorname{ord}(x) > 2$, 同时 B 的元素可以按照互为逆元素两两划分, 因此 B 中的元素数量必定是偶数. 阶为 1 的元素只有一个单位元, 因此阶不等于 2 的元素数量必是奇数, 而群有偶数个元素, 故一定存在阶为 2 的元素.