

信息安全的数学基础 (1)

Assignment 8

2023 年 10 月 14 日

---

**Problem 1**

判断下列映射是否为同态映射:

- (1) 定义映射  $\phi: \mathbb{R}^* \rightarrow \{\pm 1\}$ , 其中  $\phi(x) = \frac{x}{|x|}$ ,  $x \in \mathbb{R}^*$ ,  $|x|$  代表  $x$  的绝对值.
- (2) 定义映射  $\pi: \mathbf{C}^* \rightarrow \mathbb{R}^*$ , 其中  $\pi(a + b\sqrt{-1}) = a^2 + b^2$ .
- (3) 定义映射  $\phi: \mathbb{R}^2 \rightarrow \mathbb{R}$ , 其中  $\phi((x, y)) = x + y$ .

**Problem 2**

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

**Problem 3 (Problem 2 的一般化结论)**

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  $\phi: G_1 \rightarrow G_2$  是一个群同态. 证明:

- (1)  $\forall y \in \phi(G_1), \text{ord}(y) \mid |G_1|$ ;
- (2)  $\ker(\phi) = G_1$ .