# NIS2312-01 Fall 2023-2024

# 信息安全的数学基础 (1)

# Answer 17

# 2023 年 12 月 8 日

---

**Problem 1**

设 $a, b \in \mathbb{R}$, $b \neq 0$. 证明: $\mathbb{R}(a + b\,\mathrm{i}) = \mathbb{C}$.

解: 因为 $[\mathbb{C} : \mathbb{R}] = [\mathbb{C} : \mathbb{R}(a + b\,\mathrm{i})]\,[\mathbb{R}(a + b\,\mathrm{i}) : \mathbb{R}] = 2$, 则 $[\mathbb{R}(a + b\,\mathrm{i}) : \mathbb{R}] \leq 2$. 同时 $\mathrm{i} \notin \mathbb{R}$, 有 $[\mathbb{R}(a + b\,\mathrm{i}) : \mathbb{R}] > 1$, 故 $[\mathbb{R}(a + b\,\mathrm{i}) : \mathbb{R}] = 2$, 即 $\mathbb{R}(a + b\,\mathrm{i}) = \mathbb{C}$.

**Problem 2**

设 $F$ 是个域, $a, b \in F, a \neq 0$. 如果 $c$ 属于 $F$ 的某个扩域, 证明: $F(c) = F(ac+b)$(即 $F$ "吸收" 它自己的元素).

解: 因为 $F(ac + b)$ 是包含 $F$ 和 $ac + b$ 的最小域, 且 $a, b \in F$, $ac + b \in F(c)$, 则 $F(c) \supseteq F(ac + b)$; 同理用 $a, b, ac + b$ 来表示 $c$, 有 $c = a^{-1} \cdot ((ac + b) - b)$, 故可得 $F(c) \subseteq F(ac + b)$. 故 $F(c) = F(ac + b)$.

**Problem 3**

证明: $\mathbb{Q}[\sqrt{2}] \ncong \mathbb{Q}[\sqrt{3}]$.

解: 假设存在同构映射 $\phi : \mathbb{Q}[\sqrt{2}] \to \mathbb{Q}[\sqrt{3}]$.

注意到 $\phi$ 这个映射固定了 $\mathbb{Q}$: 因为单位元必定被映射成单位元, 故 $\phi(1_{\mathbb{Q}[\sqrt{2}]}) = 1_{\mathbb{Q}[\sqrt{3}]}$, 则对任意 $a \in \mathbb{Q} \subset \mathbb{Q}[\sqrt{2}]$, 有 $\phi(a) = a\phi(1_{\mathbb{Q}[\sqrt{2}]}) = a \in \mathbb{Q} \subset \mathbb{Q}[\sqrt{3}]$.

假设 $\phi(\sqrt{2}) = a + b\sqrt{3} \in \mathbb{Q}[\sqrt{3}]$, 其中 $a, b \in \mathbb{Q}$. 故有

$$2 = \phi(2) = \phi((\sqrt{2})^2) = \phi(\sqrt{2})^2 = a^2 + 3b^2 + 2ab\sqrt{3},$$

则

$$a^2 + 3b^2 = 2, 2ab\sqrt{3} = 0.$$

从 $2ab\sqrt{3} = 0$ 得到 $a = 0$ 或 $b = 0$: 假设 $a = 0$, 则 $3b^2 = 2$, 故 $b = \pm\sqrt{\frac{2}{3}} \notin \mathbb{Q}$, 矛盾; 故 $a \neq 0$, 有 $a = \pm\sqrt{2} \notin \mathbb{Q}$, 矛盾. 因此没有同构映射使得 $\mathbb{Q}[\sqrt{2}] \cong \mathbb{Q}[\sqrt{3}]$.