NIS2312-01 Fall 2023-2024

信息安全的数学基础 (1)

Assignment 16

2023 年 11 月 24 日

Problem 1

考虑实数域 $\mathbb{R}$ 和 $\mathbb{R}$ 上的二次不可约多项式 $p(x) = x^2 + 1$, 构造域

$$F = \frac{\mathbb{R}[x]}{\langle p(x) \rangle}.$$

证明域 F 和复数域 $\mathbb{C}$ 同构.

Problem 2

考虑有限域 $\mathbb{F}_2$ 上的不可约多项式 $f(x) = x^2 + x + 1$, 如果 α 是 $f(x) = 0$ 的根, 即 $f(\alpha) = \alpha^2 + \alpha + 1 = 0$.

证明 $F = \{a_0 + a_1\alpha : a_0, a_1 \in \mathbb{F}_2\}$ 是一个域并直接给出域

$$\frac{\mathbb{F}_2[x]}{\langle x^2 + x + 1 \rangle} = \left\{a_0 + a_1 x + \langle x^2 + x + 1\rangle : a_0, a_1, \in \mathbb{F}_2\right\} = \{\overline{a_0 + a_1 x} : a_0, a_1 \in \mathbb{F}_2\}$$

到域 F 的一个同构映射.

Problem 3

设

$$R = \left\{ \begin{bmatrix} a & b \\ 0 & a \end{bmatrix} \middle| \, a, b \in \mathbb{Q} \right\},$$

则在通常的矩阵加法和矩阵乘法下, R 构成一个环. 给定 R 的一个理想

$$J = \left\{ \begin{bmatrix} 0 & b \\ 0 & 0 \end{bmatrix} \middle| \, b \in \mathbb{Q} \right\}.$$

请利用映射

$$\phi : R \to \mathbb{Q}$$
$$\phi\left(\begin{bmatrix} a & b \\ 0 & a \end{bmatrix} \right) = a$$

证明 $R/J \cong \mathbb{Q}$.