NIS2312-01 Fall 2023-2024

信息安全的数学基础 (1)

Answer 16

2023 年 12 月 4 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.

解: 有

$$F = \frac{\mathbb{R}[x]}{\langle p(x) \rangle} = \{a + bx : a, b \in \mathbb{R}\}.$$

故构造映射

$$\begin{aligned} \phi : \quad & \mathbb{R}[x] \to \mathbb{C} \\ & f(x) = \sum_{i=1} a_i x^i \mapsto f(\imath) = \sum_{i=1} a_i \imath^i, \end{aligned}$$

1. 显然是个映射;

2. 是一个同态: 对于任意 $f(x) = \sum_{i=0} a_i x^i, g(x) = \sum_{i=0} b_i x^i$, 有

$$\begin{aligned} \phi(f(x) + g(x)) &= \phi(\sum_{i=0} (a_i + b_i) x^i) = \sum_{i=0} (a_i + b_i) \imath^i = \phi(f_1(x)) + \phi(f_2(x)) \\ \phi(f_1(x) f_2(x)) &= \phi\left(\sum_{k=0} \left(\sum_{i=0}^{k} a_i b_{k-i} \right) x^k \right) = \sum_{k=0} \left(\sum_{i=0}^{k} a_i b_{k-i} \right) \imath^k \\ &= \phi(f_1(x)) \phi(f_2(x)) \end{aligned}$$

3. 是一个满映射: $\forall a + b\imath \in \mathbb{C}$, 都有对应的 $a + bx \in \mathbb{R}[x]$;

4. $ker(\phi) = \{f(x) \in \mathbb{R}[x] \mid \phi(f(x)) = 0\} = \{f(x) \in \mathbb{R} \mid (x^2 + 1) \mid f(x)\} = \langle f(x) \rangle$;

综上利用环同态基本定理有 $\frac{\mathbb{R}[x]}{\langle p(x) \rangle} \cong \mathbb{C}$.

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

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

到域 F 的一个同构映射.

解:

1. 显然 "+" 是满足封闭性且满足交换律;
2. 加法结合律成立: 对任意 $x_1, x_2, x_3 \in F$, $x_1 + (x_2 + x_3) = (x_1 + x_2) + x_3$;
3. 零元是 0;
4. 任意元素 $a_0 + a_1\alpha$ 的负元是其自身, 即 $a_0 + a_1\alpha + a_0 + a_1\alpha = 0$;
5. 显然 "$\cdot$" 是满足封闭性的且满足交换律;
6. 乘法也是满足结合律的: 对任意 $a_0 + a_1\alpha, b_0 + b_1\alpha, c_0 + c_1\alpha \in F$, 有

$$\begin{aligned}
&(a_0 + a_1\alpha)(b_0 + b_1\alpha)(c_0 + c_1\alpha)\\
=\ &\big[(a_0b_0 + a_1b_1) + (a_1b_0 + a_0b_1 + a_1b_1)\alpha\big](c_0 + c_1\alpha)\\
=\ &(a_0b_0c_0 + a_1b_1c_0 + a_1b_0c_1 + a_0b_1c_1 + a_1b_1c_1) + (a_0b_0c_1 + a_1b_1c_1 + a_1b_0c_1 + a_0b_1c_1 + a_1b_1c_1)\,\alpha\\
&(a_0 + a_1\alpha)\big[(b_0 + b_1\alpha)(c_0 + c_1\alpha)\big]\\
=\ &(a_0 + a_1\alpha)\big[\,(b_0c_0 + b_1c_1) + (b_0c_1 + b_1c_0 + b_1c_1)\alpha\big]\\
=\ &(a_0b_0c_0 + a_1b_1c_0 + a_1b_0c_1 + a_0b_1c_1 + a_1b_1c_1) + (a_0b_0c_1 + a_1b_1c_1 + a_1b_0c_1 + a_0b_1c_1 + a_1b_1c_1)\,\alpha
\end{aligned}$$

7. 存在单位元 1;
8. 每个非零元均可逆: $1 \cdot 1 = 1$, $\alpha \cdot (1 + \alpha) = 1$;
9. 乘法和加法满足分配律的: 对任意 $a_0 + a_1\alpha, b_0 + b_1\alpha, c_0 + c_1\alpha \in F$, 有

$$\begin{aligned}
&(a_0 + a_1\alpha)(b_0 + b_1\alpha + c_0 + c_1\alpha)\\
=\ &(a_0 + a_1\alpha)((b_0 + c_0) + (b_1 + c_1)\alpha)\\
=\ &(a_0b_0 + a_0c_0 + a_1b_1 + a_1c_1) + (a_1b_0 + a_1c_0 + a_0b_1 + a_0c_1 + a_1b_1 + a_1c_1)\alpha\\
=\ &(a_0 + a_1\alpha)(b_0 + b_1\alpha) + (a_0 + a_1\alpha)(c_0 + c_1\alpha),
\end{aligned}$$

同理另一个分配率也成立.

综上, F 是一个域.

同构映射是

$$\begin{aligned}\phi : \frac{\mathbb{F}_2[x]}{\langle x^2+x+1\rangle} &\to F\\ \overline{a_0+a_1x} &\mapsto a_0+a_1\alpha\end{aligned}$$

Problem 3

设

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

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

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

请利用映射

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

证明 $R/J\cong\mathbb{Q}$.

解:

1. 显然是一个同态: 对任意 $r_1=\begin{bmatrix}a_1 & b_1\\ 0 & a_1\end{bmatrix}, r_2=\begin{bmatrix}a_2 & b_2\\ 0 & a_2\end{bmatrix}\in R$ 且 $a_1,a_2,b_1,b_2\in\mathbb{Q}$,

   我们有

$$\phi(r_1+r_2)=\phi\left(\begin{bmatrix}a_1+a_2 & b_1+b_2\\ 0 & a_1+a_2\end{bmatrix}\right)=a_1+a_2=\phi(r_1)+\phi(r_2)$$

$$\phi(r_1r_2)=\phi\left(\begin{bmatrix}a_1a_2 & a_1b_2+a_2b_1\\ 0 & a_1a_2\end{bmatrix}\right)=a_1a_2=\phi(r_1)\phi(r_2);$$

2. 对任意 $a\in\mathbb{Q}$, 都有 $r=\begin{bmatrix}a & b\\ 0 & a\end{bmatrix}\in R$ 满足 $\phi(r)=a$, 故 ϕ 是一个满射;

3. $ker(\phi)=\{r\in R\mid\phi(r)=0\}=\left\{\left. r\in R\right| r=\begin{bmatrix}0 & b\\ 0 & 0\end{bmatrix}\right\}=J$

故利用环同态基本定理有 $R/J\cong\mathbb{Q}$.