第五次习题课

作业

1. 设 $f = x^3 - x + \bar{2}$ 和 $g = \bar{2}x^2 + x$ 是 $\mathbb{Z}_3[x]$ 中的两个多项式. 计算 $\mathrm{quo}(f, g, x)$ 和 $\mathrm{rem}(f, g, x)$.

解:

$$
\begin{array}{r|l}
 & \bar{2}x - \bar{1} \\
\bar{2}x^2 + x & x^3 - x + \bar{2} \\
 & x^3 + 2x^2 \\ \hline
 & -2x^2 - x + \bar{2} \\
 & -\bar{2}x^2 - x \\ \hline
 & \bar{2}
\end{array}
$$

，可知 $\mathrm{quo}(f, g, x) = \bar{2}x - \bar{1}$
$= \bar{2}x + \bar{2}$.

$\mathrm{rem}(f, g, x) = \bar{2}$.

2. 略

3. 设 $f(x) = x^2 + 2x - 3 \in \mathbb{Z}[x]$ 分别求

(a) $f(3) \in \mathbb{Z}$;

(b) $f(\bar{5})$, 其中 $\bar{5} \in \mathbb{Z}_7$;

(c) $f(A)$, 其中 $A = \begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix}$.

解: $f(x) = x^2 + 2x - 3 = (x-1)(x+3)$

(a) $f(3) = (3-1)(3+3) = 12$,

(b) $f(\bar{5}) = (\bar{5} - 1)(\bar{5} + 3) = \bar{4} \times \bar{8} = \bar{4} \times \bar{1} = \bar{4}$.

(c) $f(A) = (A-E)(A+3E)$

$$= \begin{pmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} 4 & 0 & 0 \\ 1 & 4 & 0 \\ 0 & 1 & 4 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 0 \\ 4 & 0 & 0 \\ 1 & 4 & 0 \end{pmatrix}.$$

4. 多项式 $x^2 - 2$ 在 $\mathbb{Z}_{16}$ 中有多少个根?

解: $\mathbb{Z}_{16} = \{0, 1, \cdots, 15\}$

$$\begin{array}{cccccccc} 8k, & 8k+1, & 8k+2, & 8k+3, & 8k+4, & 8k+5, & 8k+6, & 8k+7 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 0 & 1 & 4 & 9 & 0 & 9 & 4 & 1 \end{array}.$$

故没有根

5. 设 $\mathbb{F}$ 是域

(a) 设 $a, b \in \mathbb{F}$ 且 $a \neq 0$. 证明: 映射

$$\phi_{a,b} : \mathbb{F}[x] \to \mathbb{F}[x]$$
$$p(x) \mapsto p(ax+b)$$

$x \longmapsto ax+b$

$\phi(x-5) = a(x-5)+b$

是从 $\mathbb{F}[x]$ 到 $\mathbb{F}[x]$ 的环同构.

(b) 设 $\sigma : \mathbb{F}[x] \to \mathbb{F}[x]$ 是环同构且 $\sigma|_{\mathbb{F}} = \mathrm{id}_{\mathbb{F}}$. 证明: 存在 $a, b \in \mathbb{F}$ 且 $a \neq 0$ 使得 $\sigma = \phi_{a,b}$.

$ax+b-5$

定理1.9. 设 S 是交换环, $\phi: R \to S$ 是环同态, 且 $s \in S$, 则存在唯一的环同态

$$\phi_s : R[x] \longrightarrow S \quad 满足$$

$$\phi_s|_R = \phi \quad 和 \quad \phi_s(x) = s.$$

称 ϕ_s 为 ϕ 在 s 处赋值同态.

$S=R$ 且 $\phi = id_R$ 时, $\phi_s : R[x] \longrightarrow R$ 在 s 处值.

证明 环同态, 双射

(a). $\forall\ p_1(x), p_2(x) \in F[x]$.

$$\phi_{a,b}(p_1(x)+p_2(x)) = \phi_{a,b}(p_1(x)) + \phi_{a,b}(p_2(x))$$

$$\phi_{a,b}(p_1(x)\cdot p_2(x)) = \phi_{a,b}(p_1(x)) + \phi_{a,b}(p_2(x))$$

$$\phi_{a,b}(1) = 1.$$

(1). 直接验证即可.

(2): 利用赋值定理:

$\exists!$ 环同态 $\phi_{a,b} : F[x] \longrightarrow F[x]$ 满足

$$\phi_{a,b}|_F = id_F, \quad \phi_{a,b}(x) = ax+b$$

因此: $\phi_{a,b}$ 是环同态.

双射证明可以构造逆映射.

$\phi_{a^{-1}, -\frac{b}{a}}(x) = \frac{x-b}{a}$，则

$$\phi_{a,b}\left(\phi_{a^{-1}, -\frac{b}{a}}(x)\right) = \phi_{a,b}\left(\frac{x-b}{a}\right) = \frac{ax+b-b}{a} = x$$

$$\phi_{a^{-1}, -\frac{b}{a}}\left(\phi_{a,b}(x)\right) = \phi_{a^{-1}, -\frac{b}{a}}(ax+b) = a\left[\frac{x-b}{a}\right]+b = x$$

也可以证明 $\phi_{a,b}$ 即单又满.

设 $f = \sum_{i=0}^{n} f_i x^i$，若 $\phi_{a,b}(f) = 0$

则 $\sum_{i=0}^{n} \phi_{a,b}(f_i)\, \phi_{a,b}(x)^i = \sum_{i=0}^{n} f_i (ax+b)^i = 0$

$\therefore$ $\phi_{a,b}(f)$ 的首项系数 $f_n a^n = 0$

$\because$ $a \neq 0$

$\therefore$ $f_n = 0$ $\quad\therefore$ $f = 0$ $\quad\therefore$ $\phi_{a,b}$ 为单射.

对 $\forall g \in F[x]$，设 $g = \sum_{i=0}^{n} g_i x^i$

令 $g' = \sum_{i=0}^{n} g_i (a^{-1}x - a^{-1}b)^i$，则 $g' \in F[x]$ 且

$$\phi_{a,b}(g') = \sum_{i=0}^{n} g_i x^i = g$$

$\therefore$ $\phi_{a,b}$ 是满射.

故 $\phi_{a,b}$ 是双射，因此 $\phi_{a,b}$ 是环同构.

(b). $\because$ $\sigma: F[x] \to F[x]$ 是环同构，且 $\sigma|_F = id_F$

不妨设

$\sigma(x) = \sum_{i=0}^{n} a_i x^i$ 为 n 次多项式.

当 $n \geq 2$ 时

对于 $\forall f(x) = f_1 x + f_0 \in F[x]$

不存在 $f' \in F[x]$ s.t $\sigma(f') = f$

这与 $\sigma: F[x] \to F[x]$ 环同构矛盾.

当 $n=1$ 时. $\sigma(x) = ax+b \quad (a \neq 0)$，则由 (a) 可知 $\sigma = \phi_{a,b}$

当 $n=0$ 时 $\sigma(x) = k$，常数.

则 对 $\forall f \in F[x]$，$\sigma(f)$ 为常数 与 σ 是满射矛盾.

6. 设域 $\mathbb{F}$ 上的 n 阶矩阵

$$A = \begin{pmatrix} k & c & 0 & 0 & \cdots & 0 & 0 \\ 0 & k & c & 0 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & k & c \\ 0 & 0 & 0 & 0 & \cdots & 0 & k \end{pmatrix},$$

其中 $k, c \in \mathbb{F} \setminus \{0\}$, 求 A^{-1}.

（提示: 考虑一元多项式环 $\mathbb{F}[x]$. 令 $A = kE + cH$, 利用上次作业 3 (a).）

令 $$H = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 & 0 & 0 \\ 0 & 0 & 1 & \cdots & 0 & 0 & 0 \\ 0 & 0 & 0 & \cdots & 0 & 1 & 0 \\ 0 & 0 & 0 & \cdots & 0 & 0 & 1 \\ 0 & 0 & 0 & \cdots & 0 & 0 & 0 \end{pmatrix},$$ 则 $A = kE + cH$.

计算可知 $H^n = O$.

在 $F[x]$ 中有

$$(1-x)(1+x+\cdots+x^{n-1}) = 1-x^n.$$

x用矩阵 $-\frac{c}{k}H$ 代入，得

$$\left(E-\left(-\frac{c}{k}\right)H\right)\left(E+\left(-\frac{c}{k}\right)H+\left(-\frac{c}{k}H\right)^2+\cdots+\left(-\frac{c}{k}\right)H^{n-1}\right)$$

$$= E-\left(-\frac{c}{k}H\right)^n.$$

等价地:

$$(kE+cH)\left(\frac{1}{k}E-\frac{c}{k^2}H+\frac{c^2}{k^3}H^2+\cdots+(-1)^{n-1}\frac{c^{n-1}}{k^n}H^{n-1}\right)=E.$$

故 $A^{-1} = \frac{1}{k}E-\frac{c}{k^2}H+\frac{c^2}{c^3}H^2+\cdots+(-1)^{n-1}\frac{c^{n-1}}{k^n}H^{n-1}$.