第十五次习题课

一、一元多项式环

1. 设$(R, +, 0, \cdot, 1)$是交换环，则

$$\varphi: R \longrightarrow \tilde{R}$$
$$r \longmapsto (r, 0, 0, \cdots)$$ 是单的环同态.

2. i) $\deg(p)$, $lc(p)$. $p'=0$时 $\begin{cases} \deg(p') = -\infty \\ lc(p') = 0 \end{cases}$

ii) $\deg(p+q) \le \max\{\deg(p), \deg(q)\}$

iii) $\deg(pq) \le \deg(p) + \deg(q)$

当 $lc(p)lc(q) \ne 0$ 时，等号成立且 $lc(pq) = lc(p)lc(q)$.

hw1. $f = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0 \in F[x]$ $a_n \ne 0$

$\therefore \deg(f(x)) = n$.

$f(ax+b) = a_n(ax+b)^n + a_{n-1}(ax+b)^{n-1} + \cdots + a_0$

$= a_n a^n x^n + \cdots$

$\because a_n \ne 0$, $a \ne 0$

$\therefore a_n a^n \ne 0$

$\therefore \deg(f(ax+b)) = n = \deg(f(x))$ 且 $lc(f(ax+b)) = a_n a^n$.

3. i) S是交换环，$\varphi: R \to S$是环同态，且$s \in S$，则$\exists!$的环同态$\varphi_s: R[x] \to S$满足

$$\varphi_s|_R = \varphi \quad 和 \quad \varphi_s(x) = s.$$

称φ_s为φ在s处赋值同态.

$S=R$ 且 $\varphi = id_R$ 时，$\varphi_s: R[x] \to R$ 在s处值.

hw3. (1) $f(2) = 2^2 + 2 - 2 = 4$

(2) $f(\bar{a}) = (\bar{a})^2 + \bar{a} - \bar{2}$

$\because$ $\bar{a} \in \mathbb{Z}_3$

$\therefore$ 当 $\bar{a} = \bar{0}$ 时 $f(\bar{a}) = \overline{-2} = \bar{1}$

当 $\bar{a} = \bar{1}$ 时 $f(\bar{a}) = \bar{0}$

当 $\bar{a} = \bar{2}$ 时 $f(\bar{a}) = \bar{1}$

(3) $f(A) = (A-E)(A+2E)$

$$= \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} 3 & 1 & 0 \\ 0 & 3 & 1 \\ 0 & 0 & 3 \end{pmatrix} = \begin{pmatrix} 0 & 3 & 1 \\ 0 & 0 & 3 \\ 0 & 0 & 0 \end{pmatrix}$$

ii> 设 F 是域, $A \in M_n(F)$. 则

$$\rho_A : F[x] \longrightarrow F[A]$$
$$\sum_{i=0}^{k} p_i x^i \longmapsto \sum_{i=0}^{k} p_i A^i.$$

是环同态, 其中 $k \in \mathbb{N}$, $p_0, p_1, \cdots, p_k \in F$.

iii> $\exists$ 非零多项式 $f \in F[t]$ s.t. $f(A) = O$.

iv> $A \in M_n(F)$, A 可逆 $\Longleftrightarrow$ $\exists$ $f \in F[t]$ f 关于 x^0 的系数非零且 $f(A) = O$.

v> 域上的摄动法

F 是域, $A(t), B(t) \in M_n(F[t])$, $\alpha \in F$. 则

$(A(t)+B(t))(\alpha) = A(\alpha) + B(\alpha)$, $(A(t)B(t))(\alpha) = A(\alpha)B(\alpha)$

和 $\det(A(t))(\alpha) = \det(A(\alpha))$.

hw5. (1) 证明: 由赋值定理可知, $\exists!$ 环同态 $\phi_{a,b}: F[x] \to F[x]$

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

$\therefore \varphi_{ab}$ 是环同态。

或者证环同态：

法一：有单同态 $\varphi: F[x] \to F[x]$

$$a \mapsto a.$$

由赋值定理，$\exists!$ 环同态 $\varphi_{a,b}: F[x] \to F[x]$

s.t. $\varphi_{ab}|_F = \varphi = id_F$. $\varphi_{a,b}(x) = ax+b$.

法二：用环同态定义来证

$\forall f, g \in F[x]$，验证 $\varphi_{a,b}(f+g) = \varphi_{a,b}(f) + \varphi_{a,b}(g)$

$$\varphi_{a,b}(fg) = \varphi_{a,b}(f)\cdot\varphi_{a,b}(g)$$

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

下证 $\varphi_{a,b}$ 是双射。

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

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

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

$\because a \neq 0$

$\therefore a^n \neq 0$，$\therefore f_n = 0$

$\therefore f$ 的首项系数为 0 $\therefore f = 0$ $\therefore \varphi_{a,b}$ 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

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

$\therefore \varphi_{a,b}$ 是满射.

$\therefore \varphi_{a,b}$ 是环同构。

(2). $\because$ $\sigma: F[x] \to F[x]$ 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 $\forall f = f_1 x + f_0 \in F[x]$.

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：$\sigma(x) = ax + b$ $(a \neq 0)$ 则由(1)可知 $\sigma = \varphi_{a,b}$.

当 $n=0$ 时：$\sigma(x) = k$. 常数

$\therefore$ 对 $\forall f \in F[x]$，$\sigma(f)$ 为常数与 σ 是满射矛盾。

法二：令 $f(x) = \sigma(x) \in F[x]$. 则 $f(x) \notin F$. 否则 σ 不是满射

从而 $\deg f(x) \geq 1$.

设 σ^{-1} 是 σ 的逆映射，且 $g(x) = \sigma^{-1}(x)$.

同理 $\deg g(x) \geq 1$.

设 $\sigma(x) = f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0$, $a_n \neq 0$, $n \geq 1$.

$\sigma^{-1}(x) = g(x) = b_m x^m + b_{m-1} x^{m-1} + \cdots + b_0$, $b_m \neq 0$, $m \geq 1$.

$$\Longrightarrow x = \sigma^{-1}(\sigma(x)) = \sigma^{-1}(a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0)$$

$$= a_n (\sigma^{-1}(x))^n + a_{n-1} (\sigma^{-1}(x))^{n-1} + \cdots + a_0$$

$$= a_n (b_m x^m + \cdots + b_0)^n + \cdots + a_0$$

$$\deg = mn$$

$\therefore mn = 1 \Longrightarrow m = n = 1 \Longrightarrow f(x) = ax + b$, $a \neq 0$

4. 多项式除法：

i) 设 $f, g \in R[x]$ 且 $g \neq 0$. 再设 $lc(g)$ 可逆. 则 $\exists!$ 的多项式 $q, r \in R[x]$ 满足

$$f = qg + r \quad 和 \quad \deg(r) < \deg(g).$$

ii) 余式定理:

$$f(a)=rem(f,\ x-a,\ x).$$

hw2.

$$
\begin{array}{r|l}
 & x^3+2x^2-2x+4 \\
\hline
x^2+x+1 & x^5+3x^4+x^3+4x^2-3x-1 \\
 & x^5+x^4+x^3 \\
\hline
 & 2x^4 \qquad +4x^2-3x-1 \\
 & 2x^4+2x^3+2x^2 \\
\hline
 & -2x^3+2x^2-3x-1 \\
 & -2x^3-2x^2-2x \\
\hline
 & 4x^2-x-1 \\
 & 4x^2+4x+4 \\
\hline
 & -5x-5
\end{array}
$$

$g(x)\nmid f(x)$ $\quad quo(f,g,x)=x^3+2x^2-2x+4$ $\quad rem(f,g,x)=-5x-5$

第二种: $f(x)=(x^3+\bar{2}x^2-\bar{2}x+\bar{4})g(x)-\bar{5}x-\bar{5}$

$=(x^3+\bar{2}x^2-\bar{2}x+\bar{4})g(x)$

$\therefore\ g(x)\mid f(x).$

反过来, 在$\mathbb{Z}_5[x]$中$g\nmid f$, 但在$\mathbb{Z}[x]$中$g\mid f$不可能.

设环同态 ϕ: $\mathbb{Z}[x]\longrightarrow\mathbb{Z}_5[x]$

$$\sum_{i=0}^{n}a_ix^i\longmapsto\sum_{i=0}^{n}\bar{a}_ix^i$$

若$g\mid f$. 不妨设 $f=gh$ $\therefore\ \phi(f)=\phi(gh)=\phi(g)\cdot\phi(h)$

$\Longrightarrow\ \phi(g)\mid\phi(f)$ 矛盾.

5. 多项式的根.

F是域, 且 $f\in F[x]$ 且 $deg(f)=n>0$. 则

① $a\in F$ 是 f 的根 $\Longleftrightarrow$ $\mathrm{rem}(f, x-a, x)=0$。

② f 在 F 中至多有 n 个互不相同的根。

eg. F 域，$f\in F[x]$，$A\in M_n(F)$ 满足 $f(A)=0$，再设 $g\in F[x]$ 使得 $\gcd(f,g)=1$. 证明：$g(A)$ 是可逆矩阵。

证：法一：$\because \gcd(f,g)=1$

$\therefore \exists u, v\in F[x]$ s.t. $uf+vg=1$

赋值同态 $\rho_A: F[x]\to F[A]$

$\Longrightarrow u(A)f(A)+v(A)g(A)=E$.

$\because f(A)=0$ $\quad\therefore v(A)g(A)=E$ $\quad\therefore g(A)$ 可逆，逆 $v(A)$.

注：$A\in M_n(F)$ 可逆 $\Longleftrightarrow$ $\exists B\in M_n(F)$ s.t $AB=E$ or $BA=E$.

另注意 $F[A]$ 是交换环。

法二：令 $h(x)=f(x)g(x)$. 则 $h(A)=f(A)\cdot g(A)=0$

且 $\gcd(f,g)=1$

$\mathrm{rank}(f(A))+\mathrm{rank}(g(A))=n$

$\because f(A)=0$ $\quad\therefore \mathrm{rank}(g(A))=n$ $\quad\Rightarrow g(A)$ 可逆.

期末复习

矩阵

1) A可逆 $\Longleftrightarrow \exists B\in M_n(\mathbb{R})$ s.t $AB=E$ or $BA=E$.

$\phi_A: \mathbb{R}^n \longrightarrow \mathbb{R}^n$ 单 $\Longleftrightarrow$ 满 $\Longleftrightarrow$ 双双

2) 幂等、幂零

8、矩阵的初等等价

1) $A, B\in\mathbb{R}^{m\times n}$, $\exists P, Q\in GL(\mathbb{R})$, s.t. $A=PBQ$ $\quad A\sim_e B$.

2) $\text{rank}(A)=\text{rank}(B)$.

3) 初等变换 i) ii) iii)

4) (打洞引理) 设 $A\in\mathbb{R}^{m\times n}$, 则 $\exists P, Q\in GL(\mathbb{R})$ s.t.

$$PAQ=\begin{pmatrix} E_r & O_{r\times(n-r)} \\ O_{(m-r)\times r} & O_{(m-r)\times(n-r)} \end{pmatrix}$$

5) 可逆矩阵是初等矩阵之积.

9. 矩阵求逆

$(A|E)\longrightarrow\cdots\longrightarrow(E|A^{-1})$ 多项式法?

10. 矩阵分块

1)

2). a. $\text{rank}(M)\geqslant\text{rank}(A)+\text{rank}(B)$

b. Sylvester 等式.

3) 矩阵方程求解.

行列式

1. 多重线性斜对称函数

1) 多重. $\mathbb{R}^n\times\cdots\times\mathbb{R}^n\longrightarrow\mathbb{R}$

2) 斜对称:

2. 行列式的定义和基本性质

1). det: $\mathbb{R}^n$ 上 n 重线性斜对称

2) 性质: (初等变换对行列式值的改变?)

3. 行列式性质.

1) 余子式, 代数余子式

2). $\underbrace{\det(A) = \sum_{k=1}^{n} a_{ik} A_{ik}}_{\text{按一行展开}}$ $\underbrace{\det(A) = \sum_{k=1}^{n} a_{kj} A_{kj}}_{\text{按一列展开}}$

3) 行列式的计算 (高阶行列式的计算技巧)

4) 分块矩阵的行列式

a. $\det\begin{pmatrix} A & C \\ 0 & B \end{pmatrix} = \det(A)\det(B)$

b. $\det\begin{pmatrix} C & A \\ B & 0 \end{pmatrix} = (-1)^{mn}\det(A)\det(B)$

c. $\det(AB) = \det(A)\det(B)$

5) 伴随矩阵

a. $A^{\vee}A = AA^{\vee} = |A|E$

b. A 可逆 $A^{-1} = \frac{1}{|A|}A^{\vee}$

4. 行列式的应用

a. Cramer 法则

b. 子式和矩阵的秩

群, 环, 域简介

1. 二元运算

1) 同余运算

2) 单位元和逆元

2. 群

1) 定义

a. 半群

b. 含幺半群

c. 群

2> 群中消去律

3> 同态与同构

a. $\phi: G \to H$ 同态 即 $\phi(e) = \varepsilon$, $\phi(x^{-1}) = \phi(x)^{-1}$.

b. $\phi: G \to H$ 同构, ϕ^{-1} 同构.

c. $\phi: G \to H$ 和 $\psi: H \to M$ $\psi \circ \phi$ 同态(构).

4> 子群.

a. 定义

b. $H \le G \Longleftrightarrow \forall h_1, h_2 \in H$, $h_1 h_2^{-1} \in H$.

c. $\phi: G \to H$ 群同态, $im(\phi)$ 是 H 子群.

d. $H \le G$, $card(H) \mid card(G)$.

5> 群的生成元

a. $g \in G$ $\begin{cases} ord(g) = \infty, & \cdots\cdots \\ ord(g) = k < \infty. & \cdots\cdots \end{cases}$

b. $m = ord(g)$

$$ord(g^k) = \frac{m}{gcd(m,k)}$$

c. $card(\langle g \rangle) = ord(g)$.

d. 循环群

e. $|G| < \infty$, $ord(g) \mid card(G)$, 则 $g^{card(G)} = e$.

6> 循环群结构.

a. $|G| = \infty$ $G \cong (\mathbb{Z}, +, 0)$

b. $|G| = n < \infty$ $G \simeq (\mathbb{Z}_n, +, \bar{0})$

7> Cayley定理

a. $\phi: G \to H$ 群的单同态，则 $G \simeq im(\phi)$.

b. G可被嵌入到 T_G 中.

3. 环.

1> 定义

2> 环同态和子环.

a. 环同态 + 单 环嵌入

环同态 + 双 环同构

b. 子环定义

3> 零因子. 可逆元

4> 消去律

5> 环的特征

4. 域

1> 定义

2> 域上的线性代数.