第十九次作业

1. $\mathbb{Z}[x]$. $f(x)=(x^2+x-1)g(x)+(-5x+7)$ $\quad quo(f,g,x)=x^2+x-1$, $rem(f,g,x)=-5x+7$

$\mathbb{Z}_5[x]$ $f(x)=(x^2+x-\bar{7})g(x)+(-\bar{5}x+\bar{7})$ $\quad quo(f,g,x)=x^2+x+\bar{4}$, $rem(f,g,x)=\bar{2}$

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

Note: $\varphi: \mathbb{Z}[x] \longrightarrow \mathbb{Z}_5[x]$ 环同态.

$\sum_{i=0}^{n} a_i x^i \longmapsto \sum_{i=0}^{n} \bar{a}_i x^i$

在$\mathbb{Z}[x]$中 $f=qg+r$, 则 $\varphi(f)=\varphi(qg+r)=\varphi(q)\varphi(g)+\varphi(r)$.

在$\mathbb{Z}_5[x]$中:

2. F域. $f,g,h\in F[x]$. $gcd(f,h)=gcd(g,h)=1 \Rightarrow gcd(fg,h)=1$.

Pf: 法一: $gcd(f,h)=1$, $gcd(g,h)=1$ $\quad \exists u_1,u_2,v_1,v_2\in F[x]$ s.t. $u_1f+v_1h=1$, $u_2g+v_2h=1$.

$\Rightarrow 1=(u_1f+v_1h)(u_2g+v_2h)=(u_1u_2)fg+(v_1u_2g+u_1v_2f+v_1v_2h)h$.

$\Rightarrow gcd(fg,h)=1$.

Note: $f,g\in F[x]$. $gcd(f,g)=1 \Leftrightarrow \exists u,v\in F[x]$ s.t. $uf+vg=1$.

法二: (反设法). 设 $gcd(fg,h)\in F[x]\setminus F$, $p\in F[x]$是不可约多项式且$p\mid gcd(fg,h)$

$\Rightarrow p\mid fg$, $p\mid h \Longrightarrow p\mid f$ or $p\mid g$. 与 $gcd(f,h)=gcd(g,h)=1$ 矛盾.

(p也是素元)

Note: UFD中. 不可约元 = 素元. $F[x]$中的不可约多项式是不可约元也是素元.

3. F域. $A\in M_n(F)$ s.t. $A^2=A$. 证: $rank(A)+rank(A-E)=n$.

Pf: 法一: $f(x)=x^2-x=x(x-1)$, $gcd(x,x-1)=1$. 且 $f(A)=A^2-A=0$.

由第五章第二讲推论2.18可得 ~~rand~~ $rank(A)+rank(A-E)=n$.

Note: 推论2.18: 设 $A\in M_n(F)$, $f\in F[x]$, $f(A)=0$. 再设 $f=pq$, $p,q\in F[x]$且 $gcd(p,q)=1$. 则 $sol(p(A)\vec{x}=\vec{0})\oplus sol(q(A)\vec{x}=\vec{0})=F^n$.

特别地, $rank(p(A))+rank(q(A))=n$.

法二： $A^2=A \Rightarrow A(A-E)=0$.

由 Sylvester 不等式得， $\operatorname{rank}(A)+\operatorname{rank}(A-E)-n \le \operatorname{rank}(A(A-E))=0$.

$\Rightarrow \operatorname{rank}(A)+\operatorname{rank}(A-E) \le n$.

$\because n=\operatorname{rank}(E)=\operatorname{rank}(E-A+A) \le \operatorname{rank}(A)+\operatorname{rank}(E-A)$. 且 $\operatorname{rank}(E-A)=$ rank $\operatorname{rank}(A-E)$

$\Rightarrow \operatorname{rank}(A)+\operatorname{rank}(A-E) \ge n$

$\therefore \operatorname{rank}(A)+\operatorname{rank}(A-E)=n$.

Note: ① Sylvester 不等式： $A \in F^{m\times s}$, $B \in F^{s\times n}$. 则

$\operatorname{rank}(A)+\operatorname{rank}(B)-s \le \operatorname{rank}(AB) \le \min(\operatorname{rank}(A), \operatorname{rank}(B))$.

② $A, B \in F^{m\times n}$. $\operatorname{rank}(A+B) \le \operatorname{rank}(A)+\operatorname{rank}(B)$

4. F 域， $f \in F[x]$, $A \in M_n(F)$ s.t. $f(A)=0$. 设 $g \in F[x]$ s.t. $\gcd(f,g)=1$. 证：$g(A)$ 是可逆矩阵：

赋值同态 $\varphi_A: F[x] \to F[A]$

Pf: 法一： $\because \gcd(f,g)=1 \therefore \exists u, v \in F[x]$ s.t. $uf+vg=1$. $\Rightarrow u(A)f(A)+v(A)g(A)=E$

$\because f(A)=0 \therefore v(A)g(A)=E \therefore g(A)$ 可逆且逆是 $v(A)$.

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

另注意 $F[A]$ 是交换环.

错误写法： $uf+vg=1 \overset{①}{\Rightarrow} uf(A)+v\cdot g(A)=1$ ✗.

② $u\circ f(A)+v\circ g(A)=$ $u(f(A))+v(g(A))=E$ ✗.

多项式乘积与多项式复合是不同的.

eg: $f(x)=x^2$. $u(x)=x+1$.

$u(x)f(x)=(x+1)x^2=x^3+x^2$

$u\circ f(x)=u(f(x))=u(x^2)=x^2+1$.

法二：令 $h(x)=f(x)g(x)$，则 $h(A)=f(A)g(A)=0$，且 $\gcd(f,g)=1$。

由推论2.18可知，$\operatorname{rank}(f(A))+\operatorname{rank}(g(A))=n$。

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

5. D是UFD，$a_1,\cdots,a_m,b\in D^*$，证 $\gcd(a_1b,\cdots,a_mb)=\gcd(a_1,\cdots,a_m)b$。

Pf：设 $g=\gcd(a_1,\cdots,a_m)$，则 $a_i=c_ig$，$c_i\in D^*$，$i=1,\cdots,m$。

$\Rightarrow a_ib=c_igb$，$\therefore gb$ 是 $a_1b,\cdots,a_mb$ 的公因子。

设 d 是 $a_1b,\cdots,a_mb$ 的公因子，p 是 d 中重数为 m 的不可约因子且 $m>0$。

设 p 在 a_i 中重数为 $k_i\in\mathbb{N}$ $(i=1,\cdots,m)$，在 b 中重数为 $k\in\mathbb{N}$，$\because D$ 是UFD

$\therefore m\le \min(k_1,\cdots,k_m)+k$

$\because p^{\min(k_1,\cdots,k_m)}\mid g \Rightarrow p^{\min(k_1,\cdots,k_m)+k}\mid gb \Rightarrow p^m\mid gb$

从而 $d\mid gb$，$\therefore \gcd(a_1b,\cdots,a_mb)=\gcd(a_1,\cdots,a_m)b$。

Note：Bezout关系只有在有除法的整环里才成立，有的整环中是没有除法的，

∴在一般的整环 or UFD中不能直接用Bezout关系。

目前已学过的Bezout关系成立的UFD有：$\mathbb{Z}$，$F[x]$（F域）

$\mathbb{Z}$：带余除法，$m=qn+r$，$r\in\{0,1,\cdots,n-1\}$。

Bezout关系：① $\gcd(m,n)=g$，则 $\exists u,v\in\mathbb{Z}$ s.t. $um+vn=g$。

② $\gcd(m,n)=1 \Leftrightarrow \exists u,v\in\mathbb{Z}$ s.t. $um+vn=1$。

$F[x]$：除法，$f=qg+r$，$\deg(r)<\deg(g)$。

Bezout关系：① $\gcd(f_1,\cdots,f_n)=g$，则 $\exists u_1,\cdots,u_n\in F[x]$ s.t. $u_1f_1+\cdots+u_nf_n=g$

② $\gcd(f,g)=1 \Leftrightarrow \exists u,v\in F[x]$ s.t. $uf+vg=1$

期末复习.

打洞引理之前的内容看期中复习. 具体内容可参考每章习题课讲义. F域和李老师课上讲义 (下面是提纲)

1. 解有限域上的线性方程组.

eg: $A=\begin{pmatrix}\bar{1}&\bar{2}&\bar{3}\\ \bar{0}&\bar{2}&\bar{4}\\ \bar{1}&\bar{4}&\bar{2}\end{pmatrix}\in M_n(\mathbb{Z}_5)$ $V_A=sol(A\vec{x}=\vec{0})=\left\{\lambda\begin{pmatrix}\bar{1}\\ \bar{3}\\ \bar{1}\end{pmatrix}\mid\lambda\in\mathbb{Z}_5\right\}$

2. 矩阵求逆

F域. $A\in M_n(F)$ 可逆. 求 A^{-1}:

① $(A,E)\xrightarrow{\text{初等行变换}}(E,A^{-1})$

② 设 k 是最小正整数 s.t. $\alpha_k A^k+\cdots+\alpha_1 A+\alpha_0 E=0$. $\alpha_i\in F$, $\alpha_k\neq 0$, $\alpha_0\neq 0$.

$$A^{-1}=-\alpha_0^{-1}(\alpha_1 E+\cdots+\alpha_k A^{k-1})$$

③ $AA^*=A^*A=|A|E\Rightarrow A^{-1}=\frac{A^*}{|A|}$

3. 行列式:

计算行列式: [行列式的性质参看讲义] 要用的: $|AB|=|A||B|=|BA|$

A可逆 $\Leftrightarrow$ A满秩 $\Leftrightarrow |A|\neq 0$.

① 初等变换将行列式化成上三角或下三角 (注: 做初等变换时. I: 行列式出来(-1)不要忘; II: 行列式不变; III: 行列式前乘以某个非0数.)

② 按行或列展开

③ 利用分块矩阵.

④ 有递推关系. eg: 第三章第一讲例3.6. or 书上 Prop 6

注: 以上方法可以混合使用. 可以复习下做过的行列式的题, 看看之前用过的方法和技巧. 如所行列式看不出规律时, 不妨先取 $n=2,3$ 之类找找规律. 再回到 n 阶.

4. 伴随矩阵

$A \in M_n(F)$, $A^V = \begin{pmatrix} A_{11} & A_{21} & \cdots & A_{n1} \\ A_{12} & A_{22} & \cdots & A_{n2} \\ \vdots & \vdots & & \vdots \\ A_{1n} & A_{2n} & \cdots & A_{nn} \end{pmatrix}$ A_{ij}是代数余子式

性质：① $AA^V = A^VA = |A|E$. 若A可逆，则 $A^{-1} = \frac{A^V}{|A|}$ $(\Rightarrow |A||A^V| = |A|^n)$

② $\operatorname{rank}(A^V) = \begin{cases} n, & \operatorname{rank}(A) = n \\ 1, & \operatorname{rank}(A) = n-1 \\ 0, & \operatorname{rank}(A) < n-1 \end{cases}$

5. 子式

$A = (a_{ij}) \in F^{m\times n}$. A的k阶子式记为

$$M_A\begin{pmatrix} i_1 & i_2 & \cdots & i_k \\ j_1 & j_2 & \cdots & j_k \end{pmatrix} = \begin{vmatrix} a_{i_1 j_1} & a_{i_1 j_2} & \cdots & a_{i_1 j_k} \\ a_{i_2 j_1} & a_{i_2 j_2} & \cdots & a_{i_2 j_k} \\ \vdots & \vdots & & \vdots \\ a_{i_k j_1} & a_{i_k j_2} & \cdots & a_{i_k j_k} \end{vmatrix}$$

Prop：$A \in F^{m\times n}$. 以下命题等价：

① $\operatorname{rank}(A) = r$；

② A中所有大于r阶的子式都等于0且存在一个r阶子式非0；

③ A中所有$r+1$阶的子式都等于0且存在一个r阶子式非0；

6. 群

Def：G集合，$\cdot : G\times G \to G$

(G0) 封闭性：$\forall a,b \in G,\ ab \in G$.

(G1) 结合律：$\forall a,b,c \in G,\ (ab)c = a(bc)$

(G2) 单位元：$\exists e \in G$ s.t. $\forall a \in G,\ ae = ea = a$

(G3) 逆元：$\forall a \in G,\ \exists b_a \in G$ s.t. $ab_a = b_a a = e$.

(G0)(G1)：半群；(G0)(G1)(G2)：含幺半群；(G0)(G1)(G2)(G3)：群.

子群：$H \le G \Leftrightarrow \forall a,b \in H,\ ab^{-1} \in H$

群同态：$\varphi : (G,\cdot,e) \to (H,*,\varepsilon)$, $\forall a,b \in G,\ \varphi(a\cdot b) = \varphi(a) * \varphi(b)$

群同构 = 群同态 + 双射

阶：$(G,\cdot,e)$群，$g\in G$.

若 $\underbrace{\exists n\in\mathbb{Z}^+,\ s.t.\ g^n=e}_{(*)}$，称$g$是有限阶，满足$(*)$最小正整数称为$g$的阶，记为$ord(g)$.

否则称为无限阶

循环群：分类：设$(G,\cdot,e)$是循环群，$|G|>1$

①若$|G|=\infty$，则$G\cong(\mathbb{Z},+,0)$

②若$|G|=n$，则$G\cong(\mathbb{Z}_n,+,\bar{0})$.

其中，$\mathbb{Z}=\langle 1\rangle$，$\mathbb{Z}_n=\langle\bar{1}\rangle=\langle\bar{k}\rangle$，$gcd(k,n)=1$.

7. 环.

Def：$(R,+,0,\cdot,1)$ $0,1\in R$，$0\neq 1$，$+,\cdot$是R上二元运算.

① $(R,+,0)$是交换群

② $(R,\cdot,1)$是含幺半群

③ 分配律：$\forall x,y,z\in R$，$x(y+z)=xy+xz$，$(x+y)z=xz+yz$

子环：设S是R的子环，只需说

①S对$-$封闭

②S对$\cdot$封闭

③ $1_R\in S$

或

① S对$+$封闭

② S对$\cdot$封闭

③ $\pm 1_R\in S$

环同态：$\varphi:(R,+,0_R,\cdot,1_R)\longrightarrow(S,+,0_S,\cdot,1_S)$

$\forall x,y\in R$，$\varphi(x+y)=\varphi(x)+\varphi(y)$，$\varphi(xy)=\varphi(x)\varphi(y)$，$\varphi(1_R)=1_S$.

环同构 = 环同态 + 双射.

整环 = 交换环 + 无零因子

8. 域.

域 = 交换环 + 非零元都可逆

F域 $\mathrm{char}(F) = \begin{cases} 0, & \text{eg: } \mathbb{Q}, \mathbb{R}, \mathbb{C}. \\ p,\ p\text{是素数}. & \text{eg: } \mathbb{Z}_p. \end{cases}$

域上的线性代数

9. 一元多项式环.

R交换环. $R[x] = \{ \sum_{k=0}^{n} r_k x^k \mid n \in \mathbb{N},\ r_k \in R \}$

Prop: ① 赋值定理

② 多项式的除法. $f = qg + r$, $\deg(r) < \deg(g)$

10. 整环中的 gcd, lcm

Def: gcd, lcm.

Prop: ① $f_1, \cdots, f_n \in F[x]$. $\exists\, a_1, \cdots, a_n \in F[x]$ s.t. $\gcd(f_1, \cdots f_n) = a_1 f_1 + \cdots + a_n f_n$

② $f, g \in F[x]$, $\gcd(f, g) = 1 \iff \exists\, u, v \in F[x]$ s.t. $uf + vg = 1$

Note: Bezout 关系在一般的整环中不一定成立, 常见的成立的有: $\mathbb{Z}$, $F[x]$

11. 核核分解.

$(\mathrm{Hom}(F^n, F^n), +, 0, \circ\, \mathrm{Id}) \xrightarrow{\sim} (M_n(F), +, 0, \cdot, E)$ 环同构.

$F[A]$ 是 $\mathrm{Hom}(F^n, F^n)$ 的主接子环. $F[\underset{A}{x}]$ 是 $M_n(F)$ 主接子环. 且 $F[x] \cong F[A]$

Thm: $A \in \mathrm{Hom}(F^n, F^n)$, $f \in F[x]$ 且 $f(A) = 0$. 设 $f = pq$, $p, q \in F[x]$, $\gcd(p, q) = 1$. 则

$$\ker(p(A)) \oplus \ker(q(A)) = F^n$$

Cor: $A \in \overset{M_n(F)}{\cancel{\mathrm{Hom}(F^n, F^n)}}$, $f \in F[x]$ 且 $f(A) = 0$. 设 $f = pq$, $p, q \in F[x]$ 且 $\gcd(p, q) = 1$. 则

$$\mathrm{Sol}(p(A)\vec{x} = \vec{0}) \oplus \mathrm{Sol}(q(A)\vec{x} = \vec{0}) = F^n$$

且 特别地, $\mathrm{rank}(p(A)) + \mathrm{rank}(q(A)) = n$

12. UFD

素元 ⇒ 不可约元. UFD中, 素元 = 不可约元.

Def: 整环 D 中非0非可逆元都能分解成有限多个不可约元之积, 此分解在相伴意义下唯一.

Thm1: $\mathbb{Z}$. $n = \pm p_1^{r_1} p_2^{r_2} \cdots p_m^{r_m}$, p_i 不同素数, $r_i \in \mathbb{Z}^+$. $n \in \mathbb{Z} \setminus \{0, \pm 1\}$

Thm2: $F[x]$. $f = u p_1^{r_1} p_2^{r_2} \cdots p_m^{r_m}$, p_i 为素不可约多项式, $r_i \in \mathbb{Z}^+$, $u \in F^*$. $f \in F[x] \setminus F$

重数: 定义及性质.

Prop: D 是 UFD. $a, b \in D^*$, $\gcd(a,b)$ 和 $\operatorname{lcm}(a,b)$ 都存在.

设 $a = u p_1^{r_1} \cdots p_m^{r_m}$. $b = v p_1^{s_1} \cdots p_m^{s_m}$. p_i 不相伴的不可约元. $r_i, s_i \in \mathbb{N}$, $u, v \in D^*$.

$\gcd(a,b) = p_1^{\min(r_1, s_1)} \cdots p_m^{\min(r_m, s_m)}$

$\operatorname{lcm}(a,b) = p_1^{\max(r_1, s_1)} \cdots p_m^{\max(r_m, s_m)}$

13. 四元数环.

$$H = \left\{ \begin{pmatrix} u & v \\ -\bar{v} & \bar{u} \end{pmatrix} \mid u, v \in \mathbb{C} \right\}$$

① $(H, +, 0, \cdot, E)$ 是 $M_2(\mathbb{C})$ 非交换子环.

子环: $\begin{cases} H \text{ 对 } - \text{ 封闭} \\ H \text{ 对 } \cdot \text{ 封闭} \\ E \in H \end{cases}$ or $\begin{cases} H \text{ 对 } + \text{ 封闭} \\ H \text{ 对 } \cdot \text{ 封闭} \\ \pm E \in H \end{cases}$ 非交换: $\exists a, b \in H$, $ab \neq ba$.

② H 中非0元在 H 中有逆.

设 $A = \begin{pmatrix} u & v \\ -\bar{v} & \bar{u} \end{pmatrix} \in H$. 则

$|A| = u\bar{u} + v\bar{v} = |u|^2 + |v|^2 = 0 \Leftrightarrow |u| = |v| = 0 \Leftrightarrow u = v = 0 \Leftrightarrow A = 0$.

即 $A \neq 0 \Leftrightarrow |A| \neq 0 \Leftrightarrow A$ 在 $M_2(\mathbb{C})$ 中可逆. 下说明 $A^{-1} \in H$ ($A \neq 0$).

$$A^{-1} = \frac{A^*}{|A|} = \frac{1}{|u|^2 + |v|^2} \begin{pmatrix} \bar{u} & -v \\ \bar{v} & u \end{pmatrix} = \begin{pmatrix} \frac{\bar{u}}{|u|^2+|v|^2} & \frac{-v}{|u|^2+|v|^2} \\ \frac{\bar{v}}{|u|^2+|v|^2} & \frac{u}{|u|^2+|v|^2} \end{pmatrix}$$

$\because \overline{\bar{u}} = u$, $-(-\bar{v}) = \bar{v}$, $|u|^2 + |v|^2 \in \mathbb{R}$ 且 $-|_{\mathbb{R}} = id_{\mathbb{R}}$

$\therefore A^{-1} \in H$.