第十六次习题课

多项式的除法：F 是域.

定理 1.15 设 $f, g \in F[x]$ 且 $g \neq 0$，则 $\exists!$ 多项式 $q, r \in F[x]$ s.t. $f = q \cdot g + r$ 和 $\deg(r) < \deg(q)$

商：q：$quo(f,g,x)$ $=$ $quo(f,g)$　　余式：r：$rem(f,g,x)$ $=$ $rem(f,g)$

余式定理：设 $a \in F$，$f(x) \in F[x]$. 则 $f(a) = rem(f, x-a)$

3. 多项式 $f(X) = X^5 + 3X^4 + X^3 + 4X^2 - 3X - 1$, $g(X) = X^2 + X + 1$ 可以看作环 $\mathbb{Q}[X]$ 中的多项式或者环 $\mathbb{Z}_5[X]$ 中的多项式. 用带余除法证明:

(i) 在第一种情况下 $f(x)$ 不被 $g(x)$ 整除,

(ii) 而在第二种情况下，$f(x)$ 可以被 $g(x)$ 整除.

3. $f(x) = x^5 + 3x^4 + x^3 + 4x^2 - 3x - 1$

$g(x) = x^2 + x + 1$

辗转相除：$h_1(x) = f(x) - x^3 g(x) = 2x^4 + 4x^2 - 3x - 1$

$h_2(x) = h_1(x) - 2x^2 \cdot g(x) = -2x^3 + 2x^2 - 3x - 1$

$h_3(x) = h_2(x) + 2x \cdot g(x) = 4x^2 - x - 1$

$h_4(x) = h_3(x) - 4g(x) = -5x - 5$

$\Rightarrow q = quo(f,g,x) = x^3 + 2x^2 - 2x + 4$　$r = rem(f,g,x) = -5x - 5$

即 $f - q \cdot g = r$

(1) 在 $\mathbb{Q}$ 中 $f(x) = q(x) \cdot g(x) + r(x)$ 即 $f(x)$ 不被 $g(x)$ 整除.

(2) 在 $\mathbb{Z}_5$ 中 $r(x) = -\bar{5}\bar{x} - \bar{5} = \bar{0}$ 即 $f(x)$ 被 $g(x)$ 整除.

严格证明：定义映射 $\pi: \mathbb{Z}[x] \to \mathbb{Z}_5[x]$

$\sum_{i=0}^{n} a_i x^i \mapsto \sum_{i=0}^{n} \bar{a}_i x^i$　$\bar{a}_i \in \mathbb{Z}_5$.

容易验证 π 是同态. $\forall f(x), g(x) \in \mathbb{Z}[x]$

① $\pi(f(x)+g(x)) = \pi\left(\sum_i (a_i+b_i)x^i\right)$

$= \sum_i (\overline{a_i}+\overline{b_i})x^i$

$= \sum_i \overline{a_i}x^i + \sum_i \overline{b_i}x^i$

$= \pi(f(x)) + \pi(g(x))$

② $\pi(f(x)\cdot g(x)) = \pi\left(\sum_{i,j} a_i b_j x^{i+j}\right)$ 用分配律.

$= \sum_{i,j} \overline{a_i b_j}\, x^{i+j}$ ↘ 用上面证过的保持加法.

$= \sum_{i,j} \overline{a_i}\,\overline{b_j}\, x^{i+j}$

$= \left(\sum_i \overline{a_i}x^i\right)\left(\sum_j \overline{b_j}x^j\right)$

$= \pi(f(x))\cdot\pi(g(x))$

③ $\pi(1) = \pi(\bar{1})$

设 f 在 $\mathbb{Z}[x]$ 中可以被 g 整除 则 $\exists\, h \in \mathbb{Z}[x]$ s.t. $f = gh$

$\Rightarrow \pi(f) = \pi(g)\pi(h)$ $\Rightarrow$ $\pi(f)$ 可以被 $\pi(g)$ 整除 $(\text{若 } \pi(g) \neq \bar{0})$

多项式的根:

设 F 和 K 是域, F 是 K 的子域. 设 $f \in F[x]$ 且 $\alpha \in K$.

如果 $f(\alpha) = 0$, 则称 α 是 f 在 K 中的一个根. 即

α 是方程 $f(x)=0$ 在 K 中的一个解.

命题 1.21. 设 F 是域, $f \in F[x]$ 且 $\deg(f) = n > 0$. 则

(1) $\alpha \in F$ 是 f 的根 $\Leftrightarrow \operatorname{rem}(f, x-\alpha) = 0$

K 是 F 子域 (2) f 在 F 中至多有 n 个互不相同的根.

K K

- $f(x) \in F[x]$, $\deg(f) = n$, $\alpha_1, \cdots, \alpha_n \in F$ 是 f 的 n 个互不相同的根.
  则 $f(x) = lc(f)(x-\alpha_1)\cdots(x-\alpha_n)$

多元多项式环：R 交换环。 $R[x_1,\cdots,x_n] := R[x_1][x_2]\cdots[x_n]$

性质：当 R 是整环时，$R[x_1,\cdots,x_n]$ 是整环。

次数：$X_n = \{x_1^{d_1}\cdots x_n^{d_n} \mid d_1,\cdots,d_n \in \mathbb{N}\}$

$M = x_1^{d_1}\cdots x_n^{d_n}$ 是单项式 $\deg(M) = d_1+\cdots+d_n$

其中 $d_i = \deg_{x_i}(M)$. $i=1,\cdots,n$. $\deg(0) = -\infty$.

性质：$M,N \in X_n$ $\deg(M\cdot N) = \deg(M)+\deg(N)$

定理 2.6：设 $p \in R[x_1,\cdots,x_n]$ 且 $p\neq 0$. 则 $\exists!\ k\in\mathbb{Z}^+$.

$\alpha_1,\cdots,\alpha_k \in R\setminus\{0\}$ 和两两不同单项式 $M_1,\cdots,M_k \in X_n$

s.t. $p = \alpha_1 M_1+\cdots+\alpha_k M_k$ "分布式".

$\Rightarrow \deg(p) = \max(\deg(M_1),\cdots,\deg(M_k))$

齐次多项式：$h\in R[x_1,\cdots,x_n]$. $\exists \beta_1,\cdots,\beta_l \in R$ 和 d 次单项式 $N_1,\cdots,N_l \in X_n$.

s.t. $h = \beta_1 N_1+\cdots+\beta_l N_l$. $\Rightarrow h$ 是齐次多项式.

齐次分解：$p = h_d + h_{d-1}+\cdots+h_0$ $h_i \to$ 齐 i 次多项式.

性质：(1) $\deg(h_d+h_e) \le \max(d,e)$ 当且仅当 $d=e$ 时等号成立.

(2) $\deg(\underset{p}{h_d}\ \underset{q}{h_e}) \le d+e$ 当且仅当 R 是整环时等号成立 (无零因子律)

单项式成立 $\Rightarrow$ 多项式成立.

赋值定理的多变量多项式版本：R,S 交换环，$\phi: R\to S$ 环同态

$\forall s_1,\cdots,s_n \in S$. $\exists!$ 环同态 $\phi_{s_1,\cdots,s_n}: R[x_1,\cdots,x_n]\to S$

s.t. $\phi_{s_1\cdots s_n}(x_i) = s_i$ 且 $\phi_{s_1\cdots s_n}|_R = \phi$.

对称多项式：$\sigma\in S_n$, $\phi: R\to R[x_1,\cdots,x_n]$ 是嵌入 ($\forall r\in R.\ \phi(r)=r$)

则 $\phi_\sigma: R[x_1,\cdots,x_n]\to R[x_1,\cdots,x_n]$ 满足 $\phi_\sigma(x_i) = x_{\sigma(i)}$ 且 $\phi_\sigma|_R = \phi$ 是环同态. 若 $\phi_\sigma(p) = p$ $\Rightarrow p$ 对称.

对称多项式的和与积 ⇒ 对称多项式.

定理3.3: F 域. $f \in F[x]$, $\deg(f) = n > 0$, $\mathrm{lc}(f) = a_n$

(Vieta定理推广版)

令 $f = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0 = a_n (x-\alpha_1) \cdots (x-\alpha_n)$

则 $\frac{a_i}{a_n} = (-1)^{n-i} \epsilon_{n-i}(\alpha_1, \cdots, \alpha_n)$

$\epsilon_1 = x_1 + \cdots + x_n$, $\cdots$, $\epsilon_n = x_1 x_2 \cdots x_n$. ⇒ 初等对称多项式.

例: 三次: $f = ax^3 + bx^2 + cx + s \in \mathbb{R}[x]$, $a \neq 0$, $\alpha, \beta, \gamma \in \mathbb{C}$

$\Rightarrow \alpha+\beta+\gamma = -\frac{b}{a}$ $\alpha\beta+\beta\gamma+\alpha\gamma = \frac{c}{a}$ $\alpha\beta\gamma = -\frac{s}{a}$.

2. 设域 $\mathbb{Z}_3 = \{\bar{i} \mid i = 0, 1, 2\}$, $f(x) = x^2 + \bar{2}$, 和

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

计算 $f(A)$. 确定 $f(A)$ 是否可逆. 当 $f(A)$ 可逆时, 计算 $f(A)^{-1}$. .

2. $f(A) = A^2 + \bar{2}E$

$$= \begin{pmatrix} \bar{2} & \bar{0} & \bar{2} \\ \bar{0} & \bar{1} & \bar{0} \\ \bar{2} & \bar{0} & \bar{2} \end{pmatrix} + \begin{pmatrix} \bar{2} & \bar{0} & \bar{0} \\ \bar{0} & \bar{2} & \bar{0} \\ \bar{0} & \bar{0} & \bar{2} \end{pmatrix} = \begin{pmatrix} \bar{1} & \bar{0} & \bar{2} \\ \bar{0} & \bar{0} & \bar{0} \\ \bar{2} & \bar{0} & \bar{1} \end{pmatrix}$$

$$(f(A) \mid E) = \left(\begin{array}{ccc|ccc} \bar{1} & \bar{0} & \bar{2} & \bar{1} & \bar{0} & \bar{0} \\ \bar{0} & \bar{0} & \bar{0} & \bar{0} & \bar{1} & \bar{0} \\ \bar{2} & \bar{0} & \bar{1} & \bar{0} & \bar{0} & \bar{1} \end{array}\right) \longrightarrow \left(\begin{array}{ccc|ccc} \bar{1} & \bar{0} & \bar{2} & \bar{1} & \bar{0} & \bar{0} \\ \bar{2} & \bar{0} & \bar{1} & \bar{0} & \bar{0} & \bar{1} \\ \bar{0} & \bar{0} & \bar{0} & \bar{0} & \bar{1} & \bar{0} \end{array}\right)$$

$\Rightarrow f(A)$ 不可逆. $r(f(A)) = 1$

4. 设数域 $\mathbb{F}$ 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}.

4. 设 $A=kE+cH$，$H=\begin{pmatrix} 0 & 1 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 0 & 1 \\ 0 & 0 & 0 & \cdots & 0 & 0 \end{pmatrix}$

计算可得 $H^2=\begin{pmatrix} 0 & 0 & 1 & 0 & \cdots & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & \cdots & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & \cdots & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & \cdots & 0 & 0 & 0 \end{pmatrix} \Rightarrow H^n=0$

$\Rightarrow (E-\frac{1}{k}A)^n=(-\frac{c}{k}H)^n=0$

利用：$(1-x)(1+x+\cdots+x^{n-1})=1-x^n$

令 $B=E-\frac{1}{k}A \Rightarrow B^n=0$

$\Rightarrow (\frac{1}{k}A)^{-1}=(E-B)^{-1}=E+B+B^2+\cdots+B^{n-1}=\begin{pmatrix} 1 & r & r^2 & \cdots & r^{n-2} & r^{n-1} \\ 0 & 1 & r & \cdots & r^{n-3} & r^{n-2} \\ \vdots & \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & r \\ 0 & 0 & 0 & \cdots & 0 & 1 \end{pmatrix}$

其中 $r=-\frac{c}{k}$，$B=-\frac{c}{k}H$.

$\Rightarrow A^{-1}=\begin{pmatrix} \frac{1}{k} & -\frac{c}{k^2} & \cdots & (-1)^{n-1}\frac{c^{n-1}}{k^n} \\ 0 & \frac{1}{k} & \cdots & (-1)^{n-2}\frac{c^{n-2}}{k^{n-1}} \\ \vdots & \vdots & & \\ 0 & 0 & \cdots & \frac{1}{k} & -\frac{c}{k^2} \\ 0 & 0 & \cdots & 0 & \frac{1}{k} \end{pmatrix}$

1. 设 F 是域, $A \in \mathrm{M}_n(F)$ 且 $A^2=E$. 证明:

(i) 如果 F 的特征不等于 2, 则 $\mathrm{rank}(A-E)+\mathrm{rank}(A+E) \le n$,

(ii) 如果 F 的特征等于 2, 则 $\mathrm{rank}(A-E) \le n/2$.

1. 设 $f(x)=x^2-1 \in F[x]$. $\Rightarrow f(x)=(x+1)(x-1)$ 且 $f(A)=0$

(1) $\mathrm{char}(F) \neq 2 \Rightarrow \mathrm{ord}(1) \neq 2 \Rightarrow E^2 \neq E$

$(A+E)\cdot(A-E)=0$

由矩阵的 Sylwester 不等式 $\mathrm{rank}(A)+\mathrm{rank}(B)-s \le \mathrm{rank}(AB) \le \min\{r(A), r(B)\}$

$\Rightarrow 0 \ge \mathrm{rank}(A-E)+\mathrm{rank}(A+E)-n$

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

(2) $\operatorname{char}(F)=2$ 由 Freshmen's dream $(x+y)^p=x^p+y^p$

$\Rightarrow f(x)=x^2-1=(x-1)^2 \Rightarrow (A-E)^2=0$

$\Rightarrow$ 利用矩阵秩的 Sylvester 不等式

$0\ge \operatorname{rank}(A-E)+\operatorname{rank}(A-E)-n$

$\Rightarrow \operatorname{rank}(A-E)\le \frac{n}{2}$

期末复习:

- 一般域上的线性映射.

  例 2.1 设 $\phi:\ \mathbb{Z}_2^3\to\mathbb{Z}_2^2$ 为线性映射, 取 $\mathbb{Z}_2^3$ 中标准基为 $\boldsymbol{e}_1,\boldsymbol{e}_2,\boldsymbol{e}_3$, Z_2^2 中的标准基为 $\boldsymbol{\epsilon}_1,\boldsymbol{\epsilon}_2$. 已知 $\phi(\boldsymbol{e}_1)=\boldsymbol{\epsilon}_2,\ \phi(\boldsymbol{e}_2)=\boldsymbol{\epsilon}_1+\boldsymbol{\epsilon}_2,\ \phi(\boldsymbol{e}_3)=\boldsymbol{\epsilon}_1$.

  (a) 写出 ϕ 在标准基下的矩阵;

  (b) 求 $\ker(\phi)$ 和 $\operatorname{im}(\phi)$.

- 矩阵求逆.

  ① 行变换.

  ② 多项式法.

  ③ $A^{-1}=\frac{A^V}{|A|}$.

  例 2.2 *(a)* 求 $\begin{pmatrix}\bar2&\bar3&\bar1\\ \bar1&\bar0&\bar2\\ -\bar1&-\bar1&-\bar2\end{pmatrix}\in \mathrm{M}_3(\mathbb{Z}_5)$ 的逆;

- 求行列式:

3. 三线型: 设 $a,b,c\in\mathbb{R},\ A_n=\begin{pmatrix}a&b&0&\cdots&0&0&0\\ c&a&b&\cdots&0&0&0\\ 0&c&a&\cdots&0&0&0\\ \vdots&\vdots&\vdots&&\vdots&\vdots&\vdots\\ 0&0&0&\cdots&a&b&0\\ 0&0&0&\cdots&c&a&b\\ 0&0&0&\cdots&0&c&a\end{pmatrix}\in \mathrm{M}_n(\mathbb{R})$, 则: $A_n=aA_{n-1}-bcA_{n-2}$.

4. 三爪型: 设 $a_i\neq 0\in\mathbb{R},\ i=1,\cdots n,\ b_i,c_i\in\mathbb{R},\ i=2,\cdots n.\ A=\begin{pmatrix}a&b_2&b_3&\cdots&b_{n-1}&b_n\\ c_2&a_2&0&\cdots&0&0\\ c_3&0&a_3&\cdots&0&0\\ \vdots&\vdots&\vdots&&\vdots&\vdots\\ c_{n-1}&0&0&\cdots&a_{n-1}&0\\ c_n&0&0&\cdots&0&a_n\end{pmatrix}$, 则:

- 分块矩阵:

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

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

- 群中元素的阶.

  例 2.4 *(a)* 计算 $\bar3\in\mathbb{Z}_{21}$ 的加法阶;

  (b) 计算 $\bar2\in\mathbb{Z}_{21}^*$ 的乘法阶.

- 赋值计算.

- 摄动法 构造 λE_n+A.

- 证明：$G \hookrightarrow T_G$ 是单群同态.

$T_G = \{\varphi : G \to G \mid \varphi$ 是双射$\}$

设 $\phi: G \longrightarrow T_G$, φ_g 定义为 g 的左平移，即 $\varphi_g(x) = gx$ $\forall x \in G$.

$g \longmapsto \varphi_g$

$\forall g_1, g_2 \in G$, $\phi(g_1 g_2) = \varphi_{g_1 g_2}$

而 $\forall g \in G$, $\varphi_{g_1} \circ \varphi_{g_2}(g) = \varphi_{g_1}(g_2 g) = g_1 g_2 (g) = \varphi_{g_1 g_2}(g)$

$\Rightarrow \phi(g_1 g_2) = \phi(g_1)\phi(g_2)$ 故 ϕ 是同态.

设 $\phi(g_1) = \phi(g_2) \Rightarrow \varphi_{g_1} = \varphi_{g_2}$

即 $\forall g \in G$ $\varphi_{g_1}(g) = \varphi_{g_2}(g) \Rightarrow \forall g \in G$ $g_1 g = g_2 g \Rightarrow g_1 = g_2$

即 ϕ 是单射.

- 若 $\varphi: R \longrightarrow S$ 是同构，证明 $\varphi^{-1}: S \longrightarrow R$ 也是同构.

群同构：① 保持运算（一个）
② 单射
③ 满射

环同构：① 保持运算（二个）
② 单射
③ 满射.

$\forall x, y \in S$, 设 $a = \varphi^{-1}(x)$, $b = \varphi^{-1}(y)$ 则 $x = \varphi(a)$ $y = \varphi(b)$.

2. 一些证明方法

(1) 最常规的证明方法是反证法和数学归纳法, 它们用在很多证明的命题中.

(2) 扩基方法. 用于维数公式和 Sylvester 不等式的证明, 可能会用在证明矩阵的秩不等关系中.

(3) 分块矩阵和初等变换. 用于证明一些矩阵秩的等式或者不等式, 或者行列式等式.

(4) 利用有限性. 例如第十三周习题 3 和第十四周习题 4.

(5) 配对. 例如第十三周习题 5.

(6) 摄动法.

3. 一些注意事项

(1) 域的特征会给我们的直观带来影响. 比如向量 $(1,1,2)^t$ 和 $(2,2,1)^t$, 若视为 $\mathbb{R}^3$ 中的向量, 则它们线性无关, 而若视为 $\mathbb{Z}_3^3$ 中的向量, 则它们线性相关.

(2) 多项式不是函数. 设 $f, g \in F[X]$, 且 $f(x) = g(x)$ 对无穷多个 $x \in F$ 成立, 则 $f = g$. 这是因为 $f - g \in F[X]$ 要么为零多项式, 要么有有限个根. 但 $f(x) = g(x)$, $\forall x \in F$ 推不出 $f = g$. 比如 $\mathbb{Z}_2[X]$ 中, 确实有 $x^2 = x$, $\forall x \in \mathbb{Z}_2$, 但 X^2 与 X 作为多项式是不同的.

(3) 关于一般域上的摄动法. 习题课中, 我们的摄动法以实数域为例, 实际上依赖于命题“设 $f, g \in F[X]$, 且 $f(x) = g(x)$ 对无穷多个 $x \in F$ 成立, 则 $f = g$.” 而这以命题可以使用的前提条件是域 F 中有无穷多个元素. 那么可想而知, 对于没有附加条件的一般域 F, 习题课版本的摄动法会失效. 我们需要参照第十五周讲义例 2.2, 考虑分式域 $\mathrm{Fr}(F[X])$.