第十六周习题课

李文桥

2024 年 1 月 4 日

1　一元多项式

回忆: 赋值定理, 多项式除法和分式域

- 设 $\phi: R \to S$ 为一个环同态, 则对任意一个 $s \in S$, 存在唯一环同态 $\phi_s: R[X] \to S$ 使得 $\phi_s|_R = \phi$, $\phi_s(X) = s$.
- 赋值定理实际上给出了多项式赋值的一般模式. 我们有两类重要的赋值: 设 $f(X) = x^2 + 7$, 则取 $\bar{3} \in Z_5$, $f(\bar{3}) = \bar{3}^2 + \bar{7} = \bar{1}$; 取 $X = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$, $f(A) = A^2 + 7E_3 = \begin{pmatrix} 8 & 2 & 0 \\ 0 & 8 & 0 \\ 0 & 0 & 8 \end{pmatrix}$.
  直观来讲, 我们需要先将多项式 $f(X)$ 的系数"转换"到与待赋值 s 相同的环里, 再进行计算.
- 设 $f, g \in F[X]$ 为两个非零多项式, 则存在 $q, r \in F[X]$ 使得 $f = qg + r$, 且 $r = 0$ 或 $\deg(r) < \deg(g)$.
- 设 $f \in F[X]$ 非零, 则 f 在 F 上的根至多有 $\deg(F)$ 个.
- 设 D 为整环, 形式上考虑 $\mathrm{Fr}(D) := \{\frac{b}{a} \mid a, b \in D,\ b \neq 0\}$, 并在其中定义与分数类似的加法与乘法, 使得 $\mathrm{Fr}(D)$ 成为一个域, 称为 D 的分式域. 更加严格的定义参照第十五周讲义第二节.
- 分式域的例子: $\mathbb{Z}$ 为整环, $\mathrm{Fr}(\mathbb{Z}) = \mathbb{Q}$. 设 F 为域, 则 $F[X]$ 为整环, 则 $\mathrm{Fr}(F[X])$ 表示 F 系数的有理函数全体, 即 $\{\frac{f(X)}{g(X)} \mid f(X), g(X) \in F[X],\ g(X) \neq 0\}$.

注: 作为环, $F[X]$ 中的加法单位为 0, 即零多项式, 乘法单位为 1, 即 1 多项式. 同样地, 在 $\mathrm{Fr}(F[X])$ 中, 加法单位与乘法单位分别为零函数和 1 函数. 比如 $f(X) = \dfrac{x+2}{x^2+1} \in \mathrm{Fr}(F[X])$, 直观来看 $f(X)$ 的分子有根, 但 $f(X)$ 在 $\mathrm{Fr}(F[X])$ 中确实不为零.

习题2: $f(X) = X^5 + 3X^4 + X^3 + 4X^2 - 3X - 1$, $g(X) = X^2 + X + 1$. 用 g 给 f 降次:

$$\begin{aligned} h_1(X) &= f(X) - X^3 g(X) = 2X^4 + 4X^2 - 3X - 1 \\ h_2(X) &= h_1(X) - 2X^2 g(X) = -2X^3 + 2X^2 - 3X - 1 \\ h_3(X) &= h_2(X) + 2X g(X) = 4X^2 - X - 1 \\ h_4(X) &= h_3(X) - 4g(X) = -5X - 5 \end{aligned}$$

从而 $\operatorname{quo}(f,g,X)=X^3+2X^2-2X+4$, $\operatorname{rem}(f,g,X)=-5X-5$, 不整除. 若将 f,g 视为 $Z_5[X]$ 中的多项式, 重复上述过程, 很容易知道 $\operatorname{rem}(f,g,X)=\bar{0}$. 从而 g 整除 f.

通过上述计算, 我们会有一个感性的认识. 下面来严格化:

设 $n\in\mathbb{N}^+$, 则 $\phi:\ \mathbb{Z}[X]\to\mathbb{Z}_n[X]$, $\sum\limits_i a_iX^i\mapsto\sum\limits_i \bar{a}_iX^i$ 是一个环同态.

证明: 设 $f(X)=\sum\limits_i a_iX^i$, $g(X)=\sum\limits_j b_jX^j$, 则:

$$\begin{aligned}\phi(f(X)+g(X))=&\phi(\sum_i(a_i+b_i)X^i)\\=&\sum_i(\overline{a_i+b_i})X^i\\=&\sum_i(\bar{a}_i+\bar{b_i})X^i\\=&\sum_i\bar{a}_iX^i+\sum_i\bar{b_i}X^i\\=&\phi(f(X))+\phi(g(X)).\end{aligned}$$

并且:

$$\begin{aligned}\phi(f(X)g(X))=&\phi(\sum_{i.j}a_ib_jX^{i+j})\ \text{(分配律, 不是乘法定义)}\\=&\sum_{i.j}\phi(a_ib_jX^{i+j})\ \text{(已证明的保持加法)}\\=&\sum_{i.j}\overline{a_ib_j}X^{i+j}\\=&\sum_{i.j}\bar{a}_i\bar{b_j}X^{i+j}\\=&(\sum_i\bar{a}_iX^i)(\sum_j\bar{b_j}X^j)\\=&\phi(f(X))\phi(g(X)).\end{aligned}$$

且 $\phi(1)=\phi(\bar{1})$. 故 ϕ 为环同态.

所以, 若 $f,g\in\mathbb{Z}[X]$ 且 $g\,|\,f$, 则存在 $q\in\mathbb{Z}[X]$ 使得 $f=qg$. 设 $\phi:\ \mathbb{Z}[X]\to\mathbb{Z}_n[X]$ 是将系数模 5 所给出的环同态, 则 $\phi(f)=\phi(q)\phi(g)$. 这表示 $\phi(g)\,|\,\phi(f)$, 只要 $\phi(g)\neq\bar{0}$.

习题5: (a) 先证明 σ 为环同态. 实际上, 由赋值定理, 存在唯一环同态 σ 使得 $\sigma|_{\mathbb{F}}=\mathrm{id}_{\mathbb{F}}$ 且 $\sigma(x)=ax+b$, 这个环同态就是题给的映射 $\phi_{a,b}$.

另外, 不难验证 $\phi_{a,b}\circ\phi_{1/a,-b/a}=\phi_{1/a,-b/a}\circ\phi_{a,b}=\mathrm{id}_{\mathbb{F}}$, 这说明 ϕ 是可逆映射, 从而为双射. 故 $\phi_{a,b}$ 为环同构.

(b) 记 $\tau=\sigma^{-1}$, τ 也为环同构. 由 $\sigma(x),\tau(x)\in\mathbb{F}[x]$, 可设 $f(x),g(x)\in\mathbb{F}[x]\backslash\{0\}$ 且 $f(x)=\sigma(x)$, $g(x)=\tau(x)$. 若 $\deg(f(x))=0$, 则 $\operatorname{im}(\sigma)\subseteq\mathbb{F}$, 不是环同构, 所以 $\deg(f(x))\geq 1$, 同理 $\deg(g(x))\geq 1$. 另

一方面, $x=\sigma\circ\tau(x)=\sigma(\tau(x))=\sigma(g(x))$. 设 $g(x)=\sum\limits_i a_ix^i$, 则:

$$\begin{aligned}\sigma(g(x))&=\sigma(\sum_i a_ix^i)\\&=\sum_i\sigma(a_ix^i)\\&=\sum_i\sigma(a_i)\sigma(x)^i\\&=\sum_i a_i\sigma(x)^i\\&=g(\sigma(x)).\end{aligned}$$

从而 $x=g(\sigma(x))=g(f(x))$. 容易知道 $\deg g(f(x))=\deg(g(x))\deg(f(x))$, 故 $\deg(g(x))\deg(f(x))=1$, 从而 $\deg(f(x))=1$. 这说明: 存在 $a,b\in\mathbb{F}$, $a\neq 0$, 使得 $\sigma(x)=f(x)=ax+b$, 也即 $\sigma=\phi_{a,b}$.

习题6: 设 $A=kE+cH$, 其中 $H=\begin{pmatrix}0&1&0&\cdots&0&0\\0&0&1&\cdots&0&0\\\vdots&\vdots&\vdots&&\vdots&\vdots\\0&0&0&\vdots&0&1\\0&0&0&\cdots&0&0\end{pmatrix}$. 计算发现: $H^2=\begin{pmatrix}0&0&1&0&\cdots&0&0&0\\0&0&0&1&\cdots&0&0&0\\\vdots&\vdots&\vdots&\vdots&&\vdots&\vdots&\vdots\\0&0&0&0&\cdots&0&0&1\\0&0&0&0&\cdots&0&0&0\\0&0&0&0&\cdots&0&0&0\end{pmatrix}$, $\cdots$, $H^n=O$. 所以 $(E-\frac{1}{k}A)^n=(-\frac{c}{k}H)^n=O$. 则令 $B=E-\frac{1}{k}A=-\frac{c}{k}H$, $B^n=O$, 则由上次习题 3(a), $(\frac{1}{k}A)^{-1}=(E-B)^{-1}=E+B+B^2+\cdots+B^{n-1}=\begin{pmatrix}1&r&r^2&\cdots&r^{n-2}&r^{n-1}\\0&1&r&\cdots&r^{n-2}&r^{n-1}\\\vdots&\vdots&\vdots&&\vdots&\vdots\\0&0&0&\vdots&1&r\\0&0&0&\cdots&0&1\end{pmatrix}$, 其中 $r=-\dfrac{c}{k}$.

2 期末复习

1. 必考部分:

- 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 $\mathrm{im}(\phi)$.

- 矩阵求逆.

例 2.2 *(a) 求* $\begin{pmatrix} \bar{2} & \bar{3} & \bar{1} \\ \bar{1} & \bar{0} & \bar{2} \\ -\bar{1} & -\bar{1} & -\bar{2} \end{pmatrix} \in \mathrm{M}_3(\mathbb{Z}_5)$ *的逆;*

(b) 本次习题 6.

- 求行列式.

  例 2.3 *三爪型:* $\det\begin{pmatrix} a_1 & b_2 & b_3 & \cdots & b_{n-1} & b_n \\ c_1 & a_2 & 0 & \cdots & 0 & 0 \\ c_2 & 0 & a_3 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & & \vdots & \vdots \\ c_{n-1} & 0 & 0 & \cdots & a_{n-1} & 0 \\ c_n & 0 & 0 & \cdots & 0 & a_n \end{pmatrix}$; *三线型:* $\det\begin{pmatrix} a & b & 0 & \cdots & 0 & 0 \\ c & a & b & \cdots & 0 & 0 \\ 0 & c & a & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & a & b \\ 0 & 0 & 0 & \cdots & c & a \end{pmatrix}$

- 群中元素的阶.

  例 2.4 *(a) 计算* $\bar{3} \in \mathbb{Z}_{21}$ *的加法阶;*

  (b) 计算 $\bar{2} \in \mathbb{Z}_{21}^*$ *的乘法阶.*

- 赋值计算.

  例 2.5 *本次习题3.*

- 其它

  (a) 子群判别法的证明; (b) 期中考试第 5 题重做.

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 $\mathrm{Fr}(F[X])$.