第五章　多项式和复数域

3　多元多项式环

3.1　单项式与分布式表示

定义 3.1 设 R 是交换环. 交换环 $R[x_1][x_2]\cdots[x_n]$ 称为 R 上的 n 元多项式环, 记为 $R[x_1,\ldots,x_n]$.

定理 3.2 当 R 是整环时, $R[x_1,\ldots,x_n]$ 是整环.

证明. 设 R 是整环. 当 $n=1$ 时 $R[x_1]$ 是整环(上一讲定理 1.8). 对 n 归纳可直接得出 $R[x_1,\ldots,x_n]$ 也是整环. □

定义 3.3 设 $R[x_1,\ldots,x_n]$ 是交换环 R 上的多项式环. 令

$$X_n=\left\{x_1^{d_1}\cdots x_n^{d_n}\mid d_1,\ldots,d_n\in\mathbb{N}\right\},$$

其中元素 $M=x_1^{d_1}\cdots x_n^{d_n}$ 称为 单项式, $d_1+\cdots+d_n$ 称为 M 的*(总)*次数, 记为 $\deg(M)$. 而 d_i 称为 M 关于 x_i 的次数, 记为 $\deg_{x_i}(M)$, $i=1,\ldots,n$.

注解 3.4 设 $M,N\in X_n$. 则 $MN\in X_n$ 且

$$\deg(MN)=\deg(M)+\deg(N).$$

下面我们研究如何用单项式表示多项式. 由分配律可知, 通过 $R[x_1,\dots,x_n]$ 中的运算, $R[x_1,\dots,x_n]$ 中的任何元素 f 可以写成

$$f=\alpha_1M_1+\cdots+\alpha_kM_k, \tag{1}$$

其中 $k\in\mathbb{Z}^+$, $\alpha_1,\dots,\alpha_k\in R$, $M_1,\dots,M_k\in X_n$. 通过合并同类项, 我们可进一步假设上式中 $M_1,\dots,M_k$ 两两不同.

引理 3.5 设 (1) 中 $M_1,\dots,M_k$ 两两不同且 $f=0$. 则

$$\alpha_1=\cdots=\alpha_k=0.$$

证明. 对 n 归纳. 当 $n=1$ 时, 结论成立(见定理 2.1 (i)). 设 $n>1$ 且结论在 $n-1$ 时成立. 设

$$d=\max(\deg_{x_n}(M_1),\dots,\deg_{x_n}(M_k)).$$

如果 $d=0$, 则 x_n 在 $M_1,\dots,M_k$ 中都不出现. 由归纳假设 $\alpha_1=\cdots=\alpha_k=0$.

考虑 $d>0$ 的情形. 假设 $\alpha_1,\dots,\alpha_k$ 都不等于零. 再设 $i\in\{1,\dots,n\}$ 使得 $M_1,\dots,M_{i-1}$ 关于 x_n 的次数都小于 d, 而 $\deg_{x_n}(M_i)=\deg_{x_n}(M_{i+1})=\cdots=\deg_{x_n}(M_k)=d$. 则 $M_i=N_ix_n^d,\dots,M_k=N_kx_n^d$, 其中 $N_i,\dots,N_k\in X_{n-1}$. 于是

$$0=\underbrace{\alpha_1M_1+\cdots+\alpha_{i-1}M_{i-1}}_{P}+\underbrace{(\alpha_iN_i+\cdots+\alpha_kN_k)}_{Q}x_n^d.$$

注意到 P 作为关于 x_n 的多项式有 $\deg_{x_n}(P)<d$. 根据定理 2.1, $Q=0$. 根据归纳假设, $\alpha_i=\cdots=\alpha_k=0$, 矛盾. □

定理 3.6 设 $p \in R[x_1, \ldots, x_n]$ 且 $p \neq 0$. 则存在唯一的 $k \in \mathbb{Z}^+$, $\alpha_1, \ldots, \alpha_k \in R \setminus \{0\}$ 和两两不同的单项式 $M_1, \ldots, M_k \in X_n$ 使得

$$p = \alpha_1 M_1 + \cdots + \alpha_k M_k. \tag{2}$$

(有时称上述表达式为 p 的"分布式".)

证明. 存在性由交换环的运算规律直接可得.

下面证明唯一性. 设

$$p = \beta_1 N_1 + \cdots + \beta_\ell N_\ell,$$

其中 $\beta_1, \ldots, \beta_\ell \in R \setminus \{0\}$ and $N_1, \ldots, N_\ell \in X_n$ 两两不同. 再设 $i \in \{1, 2, \ldots, \min(k, \ell)\}$ 使得 $M_1 = N_1, \ldots, M_i = N_i$, 且对任意的 $s, t \in \{i+1, \ldots, \max(s, t)\}$, $M_s \neq N_t$. 则:

$$\begin{aligned} p - p =& (\alpha_1 - \beta_1)M_1 + \cdots + (\alpha_i - \beta_i)M_i \\ &+ \alpha_{i+1}M_{i+1} + \cdots + \alpha_k M_k + (-\beta_{i+1})N_{i+1} + \cdots + (-\beta_\ell)N_\ell = 0. \end{aligned}$$

根据引理 3.5, $i = k = \ell$ 且 $\alpha_1 = \beta_1, \ldots, \alpha_k = \beta_k$. □

定义 3.7 设 $p \in R[x_1, \ldots, x_n] \setminus \{0\}$ 的分布式表示为 (2). 多项式 p 的*(总)*次数定义为

$$\max(\deg(M_1), \ldots, \deg(M_k)),$$

记为 $\deg(p)$. 此外, 0 的次数定义为 $-\infty$.

注解 3.8 设 $p \in R[x_1, \ldots, x_n]$ 和 $i \in \{1, \ldots, n\}$. 我们把看成 p 在系数环 $R[x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n]$ 上关于 x_i 的元多项式. 多项式 p 关于 x_i 的次数记为 $\deg_{x_i}(p)$.

例 3.9 设: $f = 2(x-y)(x+y)+3y^2-5xyz-(y+z)^2-2y^3 \in \mathbb{Z}[x, y, z]$. 求 $\deg_x(f)$, $\deg_y(f)$, $\deg_z(f)$ 和 $\deg(f)$.

解. 利用交换环中的计算规则可知

$$
\begin{aligned}
f &= 2x^2 - (5yz)x - 2yz - z^2 - 2y^3 && \text{(看成关于 } x \text{ 的元多项式)} \\
&= -2y^3 - (2xz + 2z)y + 2x^2 - z^2 && \text{(看成关于 } y \text{ 的元多项式)} \\
&= -z^2 - (5xy + 2y)z + 2x^2 - 2y^3 && \text{(看成关于 } z \text{ 的元多项式)} \\
&= -(2y^3 + 5xyz) + (2x^2 - 2yz - z^2) && \text{(分布表示)}.
\end{aligned}
$$

于是 $\deg_x(p) = 2$, $\deg_y(p) = 3$, $\deg_z(p) = 2$ 和 $\deg(p) = 3$.

3.2 齐次(homogeneous)多项式与齐次分解

为了研究多元多项式的加法和乘法, 我们引入齐次多项式的概念.

定义 3.10 设 $h \in R[x_1, \ldots, x_n]$. 如果存在 $\beta_1, \ldots, \beta_\ell \in R$ 和 d 次的单项式 $N_1, \ldots, N_\ell \in X_n$ 使得

$$h = \beta_1 N_1 + \cdots + \beta_\ell N_\ell,$$

则称 h 是齐 d 次的. 特别地, 0 认为是齐任意次的多项式.

如果多项式 h 非零, 则它是齐 d 次的当且仅当在它的分布表达式中出现的单项式都是 d 次的. 任何一个非零的 d 次多项式 p 都可以唯一地写成

$$p = h_d + h_{d-1} + \cdots + h_0,$$

其中 h_i 是齐 i 次的多项式且 $h_d \neq 0$. 我们称上式为 p 的齐次（加法）分解.

例 3.11 例 *3.9* 中的多项式 $f = h_3 + h_2 + h_1 + h_0$, 其中

$$h_3 = -(2y^3 + 5xyz),\ h_2 = 2x^2 - 2yz - z^2,\ h_1 = h_0 = 0.$$

引理 3.12 设 h_d 和 h_e 分别是 $R[x_1, \ldots, x_n]$ 中齐 d 次和齐 e 次多项式. 则

(i) $\deg(h_d + h_e) \leq \max(d, e)$, 且当 $d \neq e$ 时等式成立.

(ii) $\deg(h_d h_e) \leq d + e$, 且当 R 是整环时等式成立.

证明. (i) 当 $d > e$ 时, h_d 中出现的单项式不可能与 h_e 中的单项式相等. 由引理 3.5, $\deg(h_d + h_e) = d$. 当 $d = e$ 时, $\deg(h_d + h_e) = d$ 或 0. 结论成立.

(ii) 由注释 3.8 可知, $h_d h_e$ 或者等于零或者是齐 $d + e$ 次多项式. 当 R 整环时, $R[x_1, \ldots, x_n]$ 也是整环. 于是当 h_d 和 h_e 都非零时, $h_d h_e$ 也不等于零. 故 $\deg(h_d h_e) = d + e$. □

定理 3.13 设 p 和 q 分别是 $R[x_1, \ldots, x_n]$ 中 d 次和 e 次多项式. 则

(i) $\deg(p+q) \leq \max(d, e)$, 且当 $d \neq e$ 时整等式成立.

(ii) $\deg(pq) \leq d+e$, 且当 R 是整环时等式成立.

证明. 当 p 或 q 等于零时, 结论显然成立. 设 p 和 q 都不等于零. 令

$$p = g_d + \cdots + g_1 + g_0 \quad \text{和} \quad q = h_e + \cdots + h_1 + h_0,$$

其中 g_i 是齐 i 次的, h_j 是齐 j 次的, 且 h_d 和 g_e 都非零.

(i) 当 $d > e$ 时, g_d 是出现在 $p+q$ 的齐次加法分解中次数最高的齐次多项式, 于是 $\deg(p+q) = d$. 当 $d = e$ 时, 由引理 3.12 (i) 可知, $\deg(p+q) \leq d$.

(ii) 由引理 3.12 (ii) 可知, $pq = g_d h_e + r$, 其中 r 的齐次分解中出现的齐次多项式的次数小于 $d+e$. 于是, $\deg(pq) \leq d+e$. 当 R 是整环时. $\deg(g_d h_e) = d+e$. 这也是 pq 的次数. □

3.3 注记

例 3.14 求 X_n 中次数不高于 d 次的单项式的个数.

解. 当 $n = 1$ 时, 这些单项式是 $1, x, x^2, \ldots, x^d$, 共 $d+1$ 个.

下面我们用一个精彩的组合学技巧来处理一般情形. 设单项式 $M = x_1^{i_1} \cdots x_n^{i_n}$.

$$\begin{aligned}
&\deg(M) \le d \Longleftrightarrow i_1 + \cdots + i_n \le d,\\
&\qquad i_1, \ldots, i_n \in \mathbb{N},\\
&\qquad \Longleftrightarrow i_0 + i_1 + \cdots + i_n = d,\\
&\qquad i_0, i_1, \ldots, i_n \in \mathbb{N},\\
&\qquad \Longleftrightarrow \underbrace{(i_0+1)}_{j_0} + \underbrace{(i_1+1)}_{j_1} \cdots + \underbrace{(i_n+1)}_{j_n} = d+n+1,\\
&\qquad i_1, \ldots, i_n \in \mathbb{N},\\
&\qquad \Longleftrightarrow j_0 + j_1 + \cdots + j_n = d+n+1,\\
&\qquad j_1, \ldots, j_n \in \mathbb{Z}^+.
\end{aligned}$$

于是, 次数小于等于 d 的单项式的个数等于方程

$$z_0 + z_1 + \cdots + z_n = d + n + 1$$

的正整数解的个数. 相当于把 $d+n+1$ 个球排成一排, 然后把它们分成 $n+1$ 个非空组, 一共有多少种不同的分法.

$$\underbrace{\bullet \cdots \bullet}_{z_0} | \underbrace{\bullet \cdots \bullet}_{z_1} | \cdots | \underbrace{\bullet \cdots \bullet}_{z_n},$$

其中有 $d+n+1$ 个 “$\bullet$”, n 个 “$|$”. 因为这些球之间共有 $d+n$ 个空隙, 所以总数等于

$$\binom{n+d}{n}.$$

定理 3.15 设 R 和 S 是两个交换环, $\phi : R \longrightarrow S$ 是环同态. 对任意的 $s_1, \ldots, s_n \in S$, 存在唯一的环同态 $\phi_{s_1,\ldots,s_n} : R[x_1, \ldots, x_n] \longrightarrow S$ 使得

$$\phi_{s_1,\ldots,s_n}(x_i) = s_i,\ i = 1, \ldots, n \quad \text{且} \quad \phi_{s_1,\ldots,s_n}|_R = \phi.$$

证明. 对 n 归纳. 当 $n = 1$ 时, 定理即为一元多项式的赋值同态定理 (见定理 2.3). 设 $n-1$ 时定理成立. 即存在唯一的环同态 $\phi_{s_1,\ldots,s_{n-1}} : R[x_1, \ldots, x_{n-1}] \longrightarrow S$ 满足

$$\phi_{s_1,\ldots,s_{n-1}}(x_i) = x_i,\ i = 1, \ldots, n-1 \quad \text{且} \quad \phi_{s_1,\ldots,s_{n-1}}|_R = \phi.$$

令 $\psi = \phi_{s_1,\ldots,s_{n-1}}$. 对 ψ, $R[x_1, \ldots, x_{n-1}][x_n]$ 和 s_n 再次用定理 2.3 得到唯一的环同态: $\psi_{s_n} : R[x_1, \ldots, x_{n-1}][x_n] \longrightarrow S$ 满足 $\psi_{s_n}(x_n) = s_n$ 且 $\psi_{s_n}|_{R[x_1,\ldots,x_{n-1}]} = \psi$. 可直接看出 ψ_{s_n} 就是所要求的同态 $\phi_{s_1,\ldots,s_n}$. □

期末小结

设 F 是域.

矩阵部分

1. 从 F^n 到 F^m 的线性映射, 确定核与像.

2. 矩阵的乘法.

   (a) 设 $A \in F^{m\times s}, B \in F^{s\times n}$. 则

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

   (b) 设 $A \in F^{m\times n}$, $B \in \mathrm{M}_m(F)$ 和 $C \in \mathrm{M}_n(F)$. 如果 B 和 C 都满秩, 则

   $$\mathrm{rank}(BA) = \mathrm{rank}(A) \quad 和 \quad \mathrm{rank}(AC) = \mathrm{rank}(A).$$

   (c) 乘法与转置.

3. $\mathrm{M}_n(F)$ 是非交换环且对任意 $\lambda \in F$, $A, B \in \mathrm{M}_n(F)$,

   $$\lambda(A+B) = \lambda A + \lambda B, \quad \lambda(AB) = (\lambda A)B = A(\lambda B).$$

4. $\mathrm{M}_n(F)$ 中的特殊元素.

   (a) A 可逆当且仅当 A 满秩.

(b) A 是左(右)零因子当且仅当 A 亏秩且 $A \neq O$.

(c) A 是中心元当且仅当 A 是数乘矩阵.

5. 初等等价, 打洞引理, 可逆矩阵是初等矩阵之积

6. 矩阵求逆 (行变换法, 多项式法)

7. 矩阵分块, 利用矩阵分块或核像法证明秩的不等式

行列式部分

1. 定义与性质:

   (a) 行列式定义只需要加法和乘法:

   $$\det((a_{i,j})_{n\times n}) = \sum_{\sigma\in S_n} \epsilon_\sigma a_{1,\sigma(1)} \cdots a_{n,\sigma(n)}.$$

   (b) 行列式多重线性斜对称, 且如果有两行或两列相同, 则行列式的值等于零.

   (c) 转置保持行列式的值.

   (d) 行列式乘积定理.

2. 行列式的计算

   (a) 利用初等行列变换化为上(下)三角形.

   (b) 利用按一行一列展开找递归公式, 并用归纳法证明该公式.

(c) 利用分块矩阵计算行列式.

3. 行列式的应用

(a) 伴随矩阵与原矩阵的逆的关系.

(b) Cramer 法则.

(c) 矩阵的秩和它子式的关系不考.

群、环、域

1. 群

(a) 群、同态、同构、子群的定义, 子群的判别法及其证明.

(b) 最低阶的非循环群，最低阶的非交换群.

(c) 群和子群的生成元.

(d) 群中元素的阶的计算.

(e) 循环群的分类, 确定循环群的所有子群.

(f) 非交换群的例子: S_n, $\mathrm{GL}_n(F)$, $\mathrm{SL}_n(F)$.

(g) Lagrange 定理和 Cayley 定理不考.

2. 环

(a) 环、同态、同构、子环、整环的定义.

(b) 环中的左和右零因子和可逆元, 环中所有可逆元组成的乘法群.

(c) 交换环的例子: $\mathbb{Z}_n$ 和 $F[A]$.

(d) 环中的消去律.

3. 域

(a) 域、同态、同构、子域, 域的特征.

(b) 整环的分式域 (不要求证明).

(c) 域上的线性代数.

一元多项式

1. 次数、首项系数, 加法、乘法.

2. 赋值同态 (证明不要求).

3. $F[x]$ 是整环, $F[x]$ 中的除法.

4. 设 $f \in F[x]$ 和 $A \in \mathrm{M}_n(F)$. 计算 $f(A)$.

5. 多项式的根.