第零周习题课

§1 多元多项式

§1.1 加法、乘法和次数.

例 1.1 设 $f = x_1 - (x_3x_2)(x_2 + x_4^3)^2 - x_3 \in \mathbb{Z}_2[x_1, x_2, x_3, x_4]$. 计算 $\deg(f)$ 和 $\deg_{x_i}(f)$, $i = 1, 2, 3, 4$.

解.

$$\begin{aligned} f &= x_1 - (x_3x_2)(x_2^2 + x_4^6) - x_3 \quad \textit{(Freshmen's dream)} \\ &= x_1 + x_3 + x_3x_2^3 + x_3x_2x_4^6 \quad \textit{(特征 2 时, } 1 = -1\textit{)}. \end{aligned}$$

$\deg_{x_1}(f) = 1, \deg_{x_2}(f) = 3, \deg_{x_3}(f) = 1, \deg_{x_4}(f) = 6$ 且 $\deg(f) = 8$.

§1.2 单项式

设 $M = x_1^{i_1} \cdots x_n^{i_n}$ 和 $N = x_1^{j_1} \cdots x_n^{j_n}$ 是两个单项式. 显然

$$M|N \Longleftrightarrow i_1 \leq j_1, \ldots, i_n \leq j_n.$$

单项式的序.

例 1.2 *(i)* **纯字典序.** 我们说 M 在纯字典序下低于 N, 如果存在 $k \in \{1, 2, \ldots, n\}$ 使得

$$i_1 = j_1, \ \ldots, \ i_{k-1} = j_{k-1}, \ i_k < j_k.$$

(ii) **全次数+纯字典序.** 我们说 M 在全次数+纯字典序下低于 N, 如果或者 $\deg(M) < \deg(N)$, 或者 $\deg(M) = \deg(N)$ 且 M 在纯字典序下低于 N.

把例 *1.1* 中 f 的单项式从高到低排列.

- **纯字典序.** $f = x_1 + x_2^3x_3 + x_2x_3x_4^6 + x_3$.
- **全次数+纯字典序.** $f = x_2x_3x_4^6 + x_2^3x_3 + x_1 + x_3$.

§1.3 齐次多项式和齐次分解

例 1.3 计算例 *1.2* 中 f 的齐次分解得

$$f = \underbrace{x_2x_3x_4^6}_{h_8} + \underbrace{x_2^3x_3}_{h_4} + \underbrace{x_1 + x_3}_{h_1},$$

其它齐次分支都等于零.

例 1.4 设 $f \in R[x_1, \ldots, x_n]$. 证明 f 是齐 d 次多项式当且仅当对于任意的 $p \in R[x_1, \ldots, x_n]$

$$f(px_1, \ldots, px_n) = p^d f(x_1, \ldots, x_n).$$

证明. 设单项式 $M(x_1, \ldots, x_n) = x_1^{d_1} \cdots x_n^{d_n}$ 的次数是 d. 则

$$M(px_1, \ldots, px_n) = (px_1)^{d_1} \cdots (px_n)^{d_n} = p^{d_1+\cdots+d_n} x_1^{d_1} \cdots x_n^{d_n} = p^d M.$$

设 f 是齐 d 次的. 则 $f = \sum_{i=1}^{k} \alpha_i M_i$, 其中 $\alpha_i \in F$, $M_i \in X_n$ 且 $\deg(M_i) = d$, $i = 1, 2, \ldots, n$. 由上式可知,

$$f(px_1, \ldots, px_n) = \sum_{i=1}^{n} \alpha_i p^d M_i = p^d f.$$

反之, 设 $f(px_1, \ldots, px_n) = p^d f(x_1, \ldots, x_n)$ 对任意 $p \in F[x_1, \ldots, x_n]$ 成立. 假设 f 不是齐次的. 则可进一步假设

$$f = h_k + h_m + h_{m-1} + \cdots + h_0,$$

其中 h_k 是 k 齐次的, h_m 是 m 齐次的, $k > m$, $h_k \neq 0$, $h_m \neq 0$, 且 h_i 是 i 齐次的, $i = 0, 1, \ldots, m-1$. 令 $p = x_1$. 由上述证明得到 $f(x_1^2, x_1x_2, \ldots, x_1x_n)$ 的两个齐次分解

$$x_1^d h_k + x_1^d h_m + x_1^d h_{m-1} + \cdots + x_1^d h_0 = x_1^k h_k + x_1^m h_m + x_1^{m-1} h_{m-1} + \cdots + x_1^0 h_0.$$

由齐次分解的唯一性可知 $x_1^d h_k = x_1^k h_k$ 和 $x_1^d h_m = x_1^m h_m$. 于是 $\deg(x_1^d h_k) = \deg(x_1^k h_k)$ 和 $\deg(x_1^d h_m) = \deg(x_1^m h_m)$. 从而有 $d + k = 2k$ 和 $d + m = 2m$, 由此推出 $k = m$. 矛盾. □

§2 Vieta 定理

例 2.1 设 $A \in \mathrm{M}_n(F)$, 其中 F 是域. 令$f(t) = \det(tE - A) \in F[t]$.

(i) 证明: $\deg_t(f) = n$ 且首一.

(ii) 证明: $f(0) = (-1)^n \det(A)$.

(iii) 设: f 在 F 中有 n 个根 $\alpha_1, \ldots, \alpha_n$. 证明: $\alpha_1 \cdots \alpha_n = \det(A)$.

证明. 设 $A = (a_{i,j})_{n\times n}$. 则

$$f(t) = \begin{vmatrix} t - a_{1,1} & -a_{1,2} & \cdots & -a_{1,n} \\ -a_{2,1} & t - a_{2,2} & \cdots & -a_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ -a_{n,1} & -a_{n,2} & \cdots & t - a_{n,n} \end{vmatrix}.$$

(i) 由行列式的定义可知, $f(t)$ 中关于 t 的最高项出现在 $(t-a_{1,1})\cdots(t-a_{n,n})$, 而在其它乘积中 t 的最高次数至多是 $n-1$. 于是 f 是次数为 n 的首一多项式.

(ii) 由 $f(t)$ 的行列式表示和一元多项式赋值同态可知, $f(0)=\det(-A)$. 于是

$$f(0)=(-1)^n\det(A).$$

(iii) 由 *(i)* 可设 $f(t)=t^n+\beta_{n-1}t^{n-1}+\cdots+\beta_0$, 其中 $\beta_{n-1},\beta_{n-2},\ldots,\beta_0\in F$. 由 *(ii)* 可知 $\beta_0=(-1)^n\det(A)$. 根据 *Vieta* 定理,

$$\alpha_1\cdots\alpha_n=(-1)^n\beta_0=(-1)^n(-1)^n\det(A)=\det(A). \quad \square$$

§3 无平方部分

例 3.1 设 $f=x^n+a\in\mathbb{Q}[x]$, 其中 $n>1, a\in\mathbb{Q}$. 证明 f 是无平方的当且仅当 $a\neq 0$.

证明. 注意到 $f'=nx^{n-1}$. 于是

$$f+\frac{-x}{n}f'=a.$$

当 $a\neq 0$ 时, 由 *Bezout* 关系可知, $\gcd(f,f')=1$. 于是 f 无平方. 反之, 设 f 无平方. 因为 $n>1$, 所以 x^n 不是无平方的. 于是 $a\neq 0$. $\square$

例 3.2 设 p 是素数, $f\in\mathbb{Z}_p[x]$. 证明 $f'=0$ 当且仅当 存在 $g\in\mathbb{Z}_p[x]$ 使得 $f=g^p$.

证明. 如果 $f=g^p$, 则 $f'=pg^{p-1}g'=0$. 这是因为 $\mathbb{Z}_p$ 的特征等于 p.

反之. 设

$$f=f_nx^n+f_{n-1}x^{n-1}+\cdots f_1x+f_0,$$

其中 $f_n,f_{n-1},\ldots,f_1,f_0\in\mathbb{Z}_p$. 由

$$f'=nf_nx^{n-1}+(n-1)f_{n-1}x^{n-2}+\cdots+f_1=0.$$

于是, 我们有 $kf_k=0$, $k=1,2,\ldots,n$. 如果 $f_k\neq 0$, 则 $p|k$. 由此可知

$$f=f_{i_1}x^{j_1p}+\cdots+f_{i_\ell}x^{j_\ell p},$$

其中 $f_{i_1},\ldots,f_{i_\ell}\in\mathbb{Z}_p\setminus\{\bar{0}\}$ 且 $i_1=j_1p,\ldots,i_\ell=j_\ell p$. 由 *Fermat* 小定理, 对任意 $a\in\mathbb{Z}_p\setminus\{\bar{0}\}$, 我们有 $a^{p-1}=1$. 于是, $a^p=a$. 从而,

$$f=f_{i_1}^px^{j_1p}+\cdots+f_{i_\ell}^px^{j_\ell p}=\left(f_{i_1}x^{j_1}\right)^p+\cdots+\left(f_{i_\ell}x^{j_\ell}\right)^p.$$

反复应用 *Freshmen's dream* 可得

$$f=\left(f_{i_1}x^{j_1}+\cdots+f_{i_\ell}x^{j_\ell}\right)^p. \quad \square$$

§4 补充内容: 对称多项式基本定理

我们利用纯字典序排列 X_n 中的单项式. 设 $f \in R[x_1, \ldots, x_n] \setminus 0$. 则存在唯一的 $\alpha_1, \ldots, \alpha_k \in R \setminus \{0\}$ 和 $M_1, \ldots, M_k \in X_n$, 两两不同, 使得

$$f = \alpha_1 M_1 + \cdots + \alpha_k M_k.$$

设 M_1 是 $M_1, \ldots, M_k$ 中序最高的单项式, 称为 f 的头项, 记为 $\mathrm{hm}(f)$. 由纯字典序的定义可直接验证

$$\forall\ f, g \in R[x_1, \ldots, x_n] \setminus 0, \quad \mathrm{hm}(fg) = \mathrm{hm}(f)\mathrm{hm}(g).$$

例 4.1 设 $\epsilon_k = \sum_{1 \le i_1 < \cdots < i_k \le n} x_{i_1} \cdots x_{i_k}$. 则 $\mathrm{hm}(\epsilon_k) = x_1 x_2 \cdots x_k$.

引理 4.2 设 $\epsilon_1, \epsilon \ldots, \epsilon_n$ 是关于 $x_1, \ldots, x_n$ 的初等对称多项式. 则

$$\mathrm{hm}\left(\epsilon_1^{d_1} \epsilon_2^{d_2} \cdots \epsilon_n^{d_n}\right) = x_1^{d_1 + \cdots + d_n} x_2^{d_2 + \cdots + d_n} \cdots x_n^{d_n}.$$

证明. 由例 4.1 可知, $\mathrm{hm}\left(\epsilon_k^{d_k}\right) = x_1^{d_k} \cdots x_k^{d_k}$. 而

$$\mathrm{hm}\left(\epsilon_1^{d_1} \epsilon_2^{d_2} \cdots \epsilon_n^{d_n}\right) = \mathrm{hm}\left(\epsilon_1^{d_1}\right) \mathrm{hm}\left(\epsilon_2^{d_2}\right) \cdots \mathrm{hm}\left(\epsilon_n^{d_n}\right) = x_1^{d_1 + \cdots + d_n} x_2^{d_2 + \cdots + d_n} \cdots x_n^{d_n}. \quad \square$$

在设 f 的齐次分解为

$$f = h_d + h_{d-1} + \cdots + h_0.$$

对任意 $\sigma \in S_n$, 设 $\phi_\sigma : R[x_1, \ldots, x_n] \longrightarrow R[x_1, \ldots, x_n]$ 使得 $\phi_\sigma(x_i) = x_{\sigma(i)}$, $i = 1, \ldots, n$ 和 $\phi_\sigma(r) = r$ 对任意的 $r \in R$. 则

$$\phi_\sigma(f) = \phi_\sigma(h_d) + \phi_\sigma(h_{d-1}) + \cdots + \phi_\sigma(h_0).$$

可直接看出 $\phi_\sigma(h_i)$ 是齐 i 次的. 由此可知, 当 f 关于 $x_1, \ldots, x_n$ 对称时, 我们有 $h_i = \phi_\sigma(h_i)$. 从而, f 对称的当且仅当 f 的每个齐次分支是对称的.

引理 4.3 设 $f \in R[x_1, \ldots, x_n] \setminus \{0\}$ 和 $\mathrm{hm}(f) = x_1^{k_1} x_2^{k_2} \cdots x_n^{k_n}$. 如果 f 对称, 则

$$k_1 \ge k_2 \ge \cdots \ge k_n.$$

证明. 设 $\sigma \in S_n$. 因为 $\phi_\sigma(f) = f$, 所以 $x_{\sigma(1)}^{k_1} \cdots x_{\sigma(n)}^{k_n}$ 出现在 f 分布式表示中且不高于 $\mathrm{hm}(f)$. 由 σ 的任意性可知 $k_1 \ge \max(k_2, \ldots, k_n)$. 否则会存在 $\tau \in S_n$ 使得 $\phi_\tau(f)$ 的头项与 f 的头项不同, 与 f 的对称性矛盾. 同理可证

$$k_i \ge \max(k_{i+1}, \ldots, k_n), \quad i = 2, 3, \ldots, n-1. \quad \square$$

有了上述的准备, 我们来叙述和证明对称多项式基本定理.

定理 4.4 设 $\epsilon_1, \ldots, \epsilon_n$ 是关于 $x_1, \ldots, x_n$ 的初等对称多项式, $f \in R[x_1, \ldots, x_n]$. 则 f 关于 $x_1, \ldots, x_n$ 是对称的当且仅当存在唯一的多项式 $p \in R[y_1, \ldots, y_n]$ 使得

$$f(x_1, \ldots, x_n) = p(\epsilon_1, \ldots, \epsilon_n).$$

证明. 设 $\sigma \in S_n$. 我们计算:

$$\begin{aligned} \phi_\sigma\left(p(\epsilon_1, \ldots, \epsilon_n)\right) &= p\left(\phi_\sigma(\epsilon_1), \ldots, \phi_\sigma(\epsilon_n)\right) && (\phi_\sigma \text{ 是环同态}) \\ &= p(\epsilon_1, \ldots, \epsilon_n) && (\epsilon_1, \ldots, \epsilon_n \text{ 是对称多项式.}) \end{aligned}$$

于是, $p(\epsilon_1, \ldots, \epsilon_n)$ 是关于 $x_1, \ldots, x_n$ 的对称多项式.

反之, 设 f 对称. 由上述准备工作中的结果, 我们不妨进一步设 f 是 d 齐次的. 令

$$\mathrm{hm}(f) = x_1^{k_1} x_2^{k_2} \cdots x_n^{k_n}$$

且该项对应的系数是 $a_0 \in R \setminus \{0\}$. 由引理 4.3 可知,

$$p_0 = y_1^{k_1 - k_2} y_2^{k_2 - k_3} \cdots y_{n-1}^{k_{n-1} - k_n} y_n^{k_n} \in R[y_1, \ldots, y_n].$$

再由引理 4.2 可知,

$$\mathrm{hm}\left(p_0(\epsilon_1, \ldots, \epsilon_n)\right) = \mathrm{hm}(f).$$

容易看出 $p_0(\epsilon_1, \ldots, \epsilon_n)$ 是关于 $x_1, \ldots, x_n$ 对称的齐 d 次多项式, 且其头项对应的系数等于 1. 于是, $f - a_0 p_0$ 是对称的齐 d 次多项式, 其头项低于 $\mathrm{hm}(f)$. 对 $f - a_0 p_0$ 重复上述步骤有限次, 我们必然会得到零多项式. 这是因为次数为 d 的单项式只有有限个. 于是存在 $a_0, a_1, \ldots, a_\ell \in R, p_0, p_1, \ldots, p_\ell \in R[y_1, \ldots, y_n]$ 使得

$$f = a_0 p_0(\epsilon_1, \ldots, \epsilon_n) + a_1 p_1(\epsilon_1, \ldots, \epsilon_n) + \cdots + a_\ell p_\ell(\epsilon_1, \ldots, \epsilon_n).$$

令 $p = a_0 p_0 + a_1 p_1 + \cdots + a_\ell p_\ell$. 则 $f = p(\epsilon_1, \ldots, \epsilon_n)$. 存在性成立.

为了证明唯一性, 我们只要证明对任意 $g \in R[y_1, \ldots, y_n]$,

$$g(\epsilon_1, \ldots, \epsilon_n) = 0 \implies g(y_1, \ldots, y_n) = 0.$$

假设 $g \neq 0$. 令 g 的分布式表示是

$$g = \beta_1 N_1 + \cdots + \beta_s N_s,$$

其中 $\beta_1, \ldots, \beta_s \in R \setminus \{0\}$, $N_1, \ldots, N_s$ 是关于 $y_1, \ldots, y_n$ 的单项式, 两两不同. 则

$$0 = g(\epsilon_1, \ldots, \epsilon_n) = \beta_1 N_1(\epsilon_1, \ldots, \epsilon_n) + \cdots + \beta_s N_s(\epsilon_1, \ldots, \epsilon_n).$$

由引理 4.2 可知, $N_1(\epsilon_1, \ldots, \epsilon_n)$, $\ldots$, $N_s(\epsilon_1, \ldots, \epsilon_n)$ 的 s 个头项两两不同. 于是它们中序最高的头项不可能被消去. 矛盾. □