

第五章 复数域和多项式

5 多元多项式环

5.1 多元多项式环的构造

设 R 是(含幺)交换环. 则 R 上的一元多项式环 $R[x]$ 是交换环. 特别地, 当 R 是整环时, $R[x]$ 也是整环.

把 $R[x]$ 看作系数环, $R[x][y]$ 是 $R[x]$ 上的关于 y 的一元多项式环.

例 5.1 设

$$\begin{aligned} f &= (x^2 + 1)y^3 - (x + 1)y^2 - x^5 + 2x \in \mathbb{Z}[x][y] \\ &= x^2y^3 + y^3 - xy^2 - y^2 - x^5 + 2x \quad (\text{分配律}) \\ &= -x^5 + y^3x^2 + (2 - y^2)x + y^3 - y^2 \in \mathbb{Z}[y][x]. \end{aligned}$$

由此可知, $\mathbb{Z}[x][y] = \mathbb{Z}[y][x] =: \mathbb{Z}[x, y]$ 并称之为 \mathbb{Z} 上的二元多项式环.

定义 5.2 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 $R[x_1, \dots, x_n]$.

定理 5.3 当 R 是整环时, $R[x_1, \dots, x_n]$ 是整环. 当 R 是唯一因子分解整环时, $R[x_1, \dots, x_n]$ 是唯一因子分解整环.

证明. 当 $n = 1$ 时 $R[x_1]$ 是整环(见上学期第五章第一讲定理 1.8). 对 n 归纳可直接得出 $R[x_1, \dots, x_n]$ 也是整环. 类似地, 利用上学期第五章第三讲定理 3.30 和数学归纳法可知, 当 R 是唯一因子分解整环时, $R[x_1, \dots, x_n]$ 也是唯一因子分解整环. \square

定义 5.4 设 $R[x_1, \dots, x_n]$ 是交换环 R 上的多项式环. 令

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

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 $\deg_{x_i}(M)$, $i = 1, \dots, n$.

注解 5.5 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. 由例 5.1 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

$$f = \alpha_1 M_1 + \cdots + \alpha_k M_k, \quad (1)$$

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, 我们进一步假设上式中 M_1, \dots, M_k 两两不同.

引理 5.6 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(上学期第五章第一讲注释 1.3). 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 $\alpha_1 = \dots = \alpha_k = 0$. 现在考虑 $d > 0$ 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

$$\deg_{x_n}(M_i) = \deg_{x_n}(M_{i+1}) = \dots = \deg_{x_n}(M_k) = d.$$

则 $M_i = N_i x_n^d, \dots, M_k = N_k x_n^d$, 其中 $N_i, \dots, N_k \in X_{n-1}$. 于是

$$0 = \underbrace{\alpha_1 M_1 + \dots + \alpha_{i-1} M_{i-1}}_P + \underbrace{(\alpha_i N_i + \dots + \alpha_k N_k)}_Q x_n^d.$$

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, $\alpha_i = \dots = \alpha_k = 0$, 矛盾. \square

定理 5.7 设 $p \in R[x_1, \dots, x_n]$ 且 $p \neq 0$. 则存在唯一的 $k \in \mathbb{Z}^+$, $\alpha_1, \dots, \alpha_k \in R \setminus \{0\}$ 和两两不同的单项式 $M_1, \dots, M_k \in X_n$ 使得

$$p = \alpha_1 M_1 + \dots + \alpha_k M_k. \quad (2)$$

(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 $\beta_1, \dots, \beta_\ell \in R \setminus \{0\}$ and $N_1, \dots, N_\ell \in X_n$ 两两不同.

再设 $i \in \{1, 2, \dots, \min(k, \ell)\}$ 使得 $M_1 = N_1, \dots, M_i = N_i$,

且对任意的 $s, t \in \{i+1, \dots, \max(k, \ell)\}$, $M_s \neq N_t$. 则:

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

根据引理 5.6, $i = k = \ell$ 且 $\alpha_1 = \beta_1, \dots, \alpha_k = \beta_k$. \square

定义 5.8 设 $p \in R[x_1, \dots, x_n] \setminus \{0\}$ 的分布式表示为 (2).

多项式 p 的(总)次数定义为

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

记为 $\deg(p)$. 此外, 0 的次数定义为 $-\infty$.

注解 5.9 设 $p \in R[x_1, \dots, x_n]$ 和 $i \in \{1, \dots, n\}$. 我们把看成 p 在系数环 $R[x_1, \dots, x_{i-1}, x_{i+1}, \dots, x_n]$ 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 5.10 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 $\deg(p) = 3$.

例 5.11 设 $d \in \mathbb{N}$. 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 $1, x, x^2, \dots, x^d$, 共 $d+1$ 个.

当 $n = 2$ 时, 这样的单项式的形式是 $x^i y^j$, 其中 $i, j \in \mathbb{N}$ 且 $i + j \leq d$. 于是, 对于取定的 i , j 的取值范围是 $\{0, 1, \dots, d - i\}$, 共 $d - i + 1$ 个. 由此可知, 次数单项式的个数为

$$\sum_{i=0}^d (d - i + 1) = (d + 1)d - \frac{d(d + 1)}{2} + d + 1 = \frac{(d + 2)(d + 1)}{2}.$$

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 $M = x_1^{i_1} \cdots x_n^{i_n}$.

$$\deg(M) \leq d \iff i_1 + \cdots + i_n \leq d,$$

$$(i_1, \dots, i_n \in \mathbb{N}),$$

$$\iff i_0 + i_1 + \cdots + i_n = d,$$

$$(i_0, i_1, \dots, i_n \in \mathbb{N}),$$

$$\iff \underbrace{(i_0 + 1)}_{j_0} + \underbrace{(i_1 + 1)}_{j_1} \cdots + \underbrace{(i_n + 1)}_{j_n} = d + n + 1,$$

$$(i_1, \dots, i_n \in \mathbb{N}),$$

$$\iff j_0 + j_1 + \cdots + j_n = d + n + 1,$$

$$(j_1, \dots, j_n \in \mathbb{Z}^+).$$

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

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

5.2 齐次(homogeneous)多项式

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

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

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

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

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 5.13 例 5.10 中的多项式 $f = h_3 + h_2 + h_1 + h_0$, 其中

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

引理 5.14 设 h_d 和 h_e 分别是 $R[x_1, \dots, x_n]$ 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 5.6, $\deg(h_d + h_e) = d$. 当 $d = e$ 时, $\deg(h_d + h_e) = d$ 或 0 . 结论成立.

(ii) 由注释 5.9 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, $R[x_1, \dots, x_n]$ 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 $\deg(h_d h_e) = d + e$. \square

定理 5.15 设 p 和 q 分别是 $R[x_1, \dots, x_n]$ 中 d 次和齐 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 5.14 (i) 可知, $\deg(p + q) \leq d$.

(ii) 由引理 5.14 (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. \square

5.3 赋值同态

我们把关于一元多项式环的赋值同态定理推广到多元情形.

定理 5.16 设 R 和 S 是两个交换环, $\phi: R \rightarrow S$ 是环同态. 对任意的 $s_1, \dots, s_n \in S$, 存在唯一的环同态 $\phi_{s_1, \dots, s_n}: R[x_1, \dots, x_n] \rightarrow S$ 使得

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

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(见上学期第五章第一讲定理 1.10). 设 $n - 1$ 时定理成立. 即存在唯一的环同态 $\phi_{s_1, \dots, s_{n-1}}: R[x_1, \dots, x_{n-1}] \rightarrow S$ 满足

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

令 $\psi = \phi_{s_1, \dots, s_{n-1}}$. 对 ψ , $R[x_1, \dots, x_{n-1}][x_n]$ 和 s_n 再次利用上学期第五章第一讲定理 1.10 得到唯一的环同态: $\psi_{s_n}: R[x_1, \dots, x_{n-1}][x_n] \rightarrow S$ 满足

$$\psi_{s_n}(x_n) = s_n \quad \text{且} \quad \psi_{s_n}|_{R[x_1, \dots, x_{n-1}]} = \psi.$$

可直接看出 ψ_{s_n} 就是所要求的同态 ϕ_{s_1, \dots, s_n} . \square

例 5.17 设 F 是域. ϕ 是 F 上的恒同映射, $\alpha_1, \dots, \alpha_n \in F$. 则存在唯一的赋值同态

$$\begin{aligned} \phi_{\alpha_1, \dots, \alpha_n} : F[x_1, \dots, x_n] &\longrightarrow F \\ p(x_1, \dots, x_n) &\mapsto p(\alpha_1, \dots, \alpha_n). \end{aligned}$$

如果 $p(\alpha_1, \dots, \alpha_n) = 0$, 则称 $(\alpha_1, \dots, \alpha_n)$ 是多项式 p 在 F 上的一个零点. 多项式 $x_1^2 + x_2^2 - 1$ 在 \mathbb{R} 上所有零点的集合是单位圆.

例 5.18 设 $\sigma \in S_n$, $\phi : R \rightarrow R[x_1, \dots, x_n]$ 是嵌入 (满足 $\forall r \in R, \phi(r) = r$). 则 $\phi_\sigma : R[x_1, \dots, x_n] \rightarrow R[x_1, \dots, x_n]$ 满足

$$\phi_\sigma(x_i) = x_{\sigma(i)}, \quad i = 1, \dots, n \quad \text{且} \quad \phi_\sigma|_R = \phi$$

是环同态. 事实上, ϕ_σ 的逆映射是 $\phi_{\sigma^{-1}}$. 于是, ϕ_σ 是同构. 如果 $\sigma = (12)$, 则

$$\phi_\sigma(x_1 + 2x_2^2 - x_3) = x_{\sigma(1)} + 2x_{\sigma(2)}^2 - x_{\sigma(3)} = x_2 + 2x_1^2 - x_3.$$

定义 5.19 设 $p \in R[x_1, \dots, x_n]$. 如果对于任意的 $\sigma \in S_n$, $\phi_\sigma(p) = p$, 则称 p 是关于 x_1, \dots, x_n 的对称多项式.

系数环 R 中的元素都是对称多项式. 对任意 $i \in \mathbb{Z}^+$, $x_1^i + \dots + x_n^i$ 是对称多项式.

命题 5.20 设 T 是 $R[x_1, \dots, x_n]$ 中的所有对称多项式构成的集合. 则 T 是 $R[x_1, \dots, x_n]$ 中的子环.

证明. 设 $f, g \in T$. 则对任意 $\sigma \in S_n$,

$$\phi_\sigma(f - g) = \phi_\sigma(f) - \phi_\sigma(g) = f - g.$$

故 $f - g \in T$. 由此得出, $(T, +, 0)$ 是 $(R[x_1, \dots, x_n], +, 0)$ 的加法子群. 类似地,

$$\phi_\sigma(fg) = \phi_\sigma(f)\phi_\sigma(g) = fg.$$

此外 $1 \in T$. 故 $(T, \cdot, 1)$ 是含幺半群. 故 T 是子环. \square

5.4 初等对称多项式简介

多项式环 $R[x_1, \dots, x_n]$ 中的对称多项式构成一个子环. 在该子环中有一类重要的对称多项式. 设

$$p = (x_{n+1} - x_1) \cdots (x_{n+1} - x_n) \in R[x_1, \dots, x_n, x_{n+1}].$$

把它看成关于 x_{n+1} 的一元多项式, 展开得到:

$$p = x_{n+1}^n - \epsilon_1 x_{n+1}^{n-1} + \cdots + (-1)^{n-1} \epsilon_{n-1} x_{n+1} + (-1)^n \epsilon_n,$$

其中, 其中 $\epsilon_1, \dots, \epsilon_{n-1}, \epsilon_n \in R[x_1, \dots, x_n]$. 直接计算可得

$$\epsilon_1 = x_1 + \cdots + x_n \quad \text{and} \quad \epsilon_n = x_1 \cdots x_n$$

它们都是关于 x_1, \dots, x_n 的对称多项式.

下面我们来证明每个 ϵ_i 都是对称多项式. 设 $\sigma \in S_n$. 我们可以把 σ 看成 S_{n+1} 中满足 $\sigma(n+1) = n+1$ 的元素. 设 $\phi_\sigma : R[x_1, \dots, x_n, x_{n+1}] \rightarrow R[x_1, \dots, x_n, x_{n+1}]$ 是由例 5.18 定义的同构. 则

$$\phi_\sigma(p) = (x_{n+1} - x_{\sigma(1)}) \cdots (x_{n+1} - x_{\sigma(n)}) = p.$$

另一方面,

$$\phi_\sigma(p) = x_{n+1}^n - \phi_\sigma(\epsilon_1)x_{n+1}^{n-1} + \cdots + (-1)^{n-1}\phi_\sigma(\epsilon_{n-1})x_{n+1} + (-1)^n\phi_\sigma(\epsilon_n).$$

根据上学期第五章第一讲注释 1.3, $\phi_\sigma(\epsilon_1) = \epsilon_1, \dots, \phi_\sigma(\epsilon_{n-1}) = \epsilon_{n-1}$ 和 $\phi_\sigma(\epsilon_n) = \epsilon_n$. 于是, $\epsilon_1, \dots, \epsilon_{n-1}, \epsilon_n$ 都是关于 x_1, \dots, x_n 的对称多项式.

再设 $\epsilon_0 = 1$. 我们称 $\epsilon_0, \epsilon_1, \dots, \epsilon_n$ 是关于 x_1, \dots, x_n 的初等对称多项式.

例 5.21 通过直接计算可得, 当 $n = 2$ 时, $\epsilon_1 = x_1 + x_2, \epsilon_2 = x_1x_2$; 当 $n = 3$ 时, $\epsilon_1 = x_1 + x_2 + x_3, \epsilon_2 = x_1x_2 + x_2x_3 + x_1x_3, \epsilon_3 = x_1x_2x_3$. 一般来讲

$$\epsilon_k = \sum_{1 \leq i_1 < i_2 < \cdots < i_k \leq n} x_{i_1}x_{i_2} \cdots x_{i_k}, \quad k = 1, 2, \dots, n.$$

注意到 ϵ_k 是 k 齐次的.

利用初等对称多项式, 我们可以把关于二次多项式的 Vieta 定理推广到一般情形.

定理 5.22 设 F 是域, $f \in F[x]$, $\deg(f) = n > 0$, $\text{lc}(f) = a_n$. 令

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

其中 $\alpha_1, \dots, \alpha_n \in F$, 不必两两不同. 则

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

其中 ϵ_{n-i} 是第 $n-i$ 个 n 元初等对称多项式, $i = 0, 1, \dots, n$.

证明. 由定理 5.16 可知, 存在赋值同态

$$\phi : F[x_1, \dots, x_n, x_{n+1}] \longrightarrow F[x]$$

满足: $\phi|_F$ 是恒同映射, $\phi(x_i) = \alpha_i, i = 1, 2, \dots, n$ 和 $\phi(x_{n+1}) = x$. 令 $g = (x_{n+1} - x_1) \cdots (x_{n+1} - x_n)$ 和 $h = a_n g$. 则 $\phi(h) = a_n \phi(g) = a_n (x - \alpha_1) \cdots (x - \alpha_n) = f$. 由初等对称多项式的定义可知:

$$\begin{aligned} & a_n (x^n - \phi(\epsilon_1) x^{n-1} + \cdots + (-1)^{n-1} \phi(\epsilon_{n-1}) x + (-1)^n \phi(\epsilon_n)) \\ &= a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0. \end{aligned}$$

根据定理 2.1 可知, $a_n (-1)^{n-i} \epsilon_{n-i}(\alpha_1, \dots, \alpha_n) = a_i, i = 0, 1, \dots, n$. \square

例 5.23 设 $f = ax^2 + bx + c \in \mathbb{R}[x]$ 且 $a \neq 0, \alpha, \beta \in \mathbb{C}$ 是 f 的两个根. 则

$$\alpha + \beta = -\frac{b}{a} \quad \text{且} \quad \alpha\beta = \frac{c}{a}.$$

这就是二次方程的 *Vieta* 定理.

设 $f = ax^3 + bx^2 + cx + d \in \mathbb{R}[x]$ 且 $a \neq 0$, $\alpha, \beta, \gamma \in \mathbb{C}$ 是 f 的三个根. 则

$$\alpha + \beta + \gamma = -\frac{b}{a}, \quad \alpha\beta + \beta\gamma + \gamma\alpha = \frac{c}{a} \quad \text{且} \quad \alpha\beta\gamma = -\frac{d}{a}.$$

定理 5.24 设 F 是域, T_n 是 $F[x_1, \dots, x_n]$ 中对称多项式构成的子环. 则满足

$$\phi_F = \text{id}_F, \quad \phi(x_1) = \epsilon_1, \dots, \phi(x_n) = \epsilon_n$$

是从 $F[x_1, \dots, x_n]$ 到 T_n 的环同构. 特别地, 对任意 $p \in T_n$, 存在唯一的 $f \in F[x_1, \dots, x_n]$ 使得

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

该定理的证明需要用到单项式的排序, 这里不再赘述.

例 5.25 设 $p = x_1^2 + x_2^2 \in T_2$. 则

$$p = (x_1 + x_2)^2 - 2x_1x_2 = \epsilon_1^2 - 2\epsilon_2 = f(\epsilon_1, \epsilon_2),$$

其中 $f(x_1, x_2) = x_1^2 - 2x_2$.

6 一元多项式的无平方部分

设 F 是域, $p \in F[x]$ 的次数为正. 则存在 $c \in F$, F 上两两互不相伴的不可约多项式 $p_1, \dots, p_k \in F[x] \setminus F$ 和唯一

的 $m_1, \dots, m_k \in \mathbb{Z}^+$ 使得

$$p = cp_1^{m_1} \cdots p_k^{m_k}. \quad (3)$$

我们称 p_i 是 p 的 m_i 重因子, $i = 1, 2, \dots, k$. 当 $m_i = 1$ 时, p_i 称为单因子. 因子 $p_1 p_2 \cdots p_k$ 称为 p 的无平方部分 (*squarefree part*). 当 p 的不可约因子都是单因子时, p 称为无平方的. 尽管 p 的无平方部分是通过 p 的不可约因子定义的, 无平方部分可以通过辗转相除法得到. 为此, 我们需要定义多项式的形式导数.

设 $f = f_n x^n + f_{n-1} x^{n-1} + \cdots + f_1 x + f_0 \in F[x]$. 定义 f 关于 x 的导数是

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

由于其运算规律与通常实系数多项式的导数一致, 可直接验证: 对任意 $f, g \in F[x]$,

$$(f+g)' = f' + g' \quad \text{和} \quad (fg)' = f'g + fg'.$$

定理 6.1 设 F 是特征为零的域, $p \in F[x] \setminus F$. 则 p 的无平方部分在 F 上与 $p/\gcd(p, p')$ 相伴.

证明. 由 (3) 可知,

$$\begin{aligned} p' &= c \sum_{i=1}^k m_i \left(p_1^{m_1} \cdots p_{i-1}^{m_{i-1}} p_i^{m_i-1} p'_i p_{i+1}^{m_{i+1}} \cdots p_k^{m_k} \right) \\ &= c \underbrace{\left(p_1^{m_1-1} \cdots p_k^{m_k-1} \right)}_g \underbrace{\sum_{i=1}^k m_i \left(p_1 \cdots p_{i-1} p'_i p_{i+1} \cdots p_k \right)}_h. \end{aligned}$$

于是, g 是 p 和 p' 的公因子. 下面证 $\gcd(p, h) = 1$. 假设该结论不成立, 由 (3) 可知存在 $i \in \{1, \dots, k\}$ 使得 $p_i | h$. 不妨设 $p_1 | h$. 则由 h 的定义 $p_1 | m_1(p'_1 p_2 \cdots p_k)$ (见引理 2.1). 因为 $\gcd(p_1, p_i) = 1, i = 2, \dots, k$, 且 m_1 在特征为零的域中非零, 所以 $p_1 | p'_1$ (见引理 3.1). 但这与 $\deg(p_1) > \deg(p'_1)$ 矛盾. 由此可知, $\gcd(p, h) = 1$. 进而 $\gcd(p, p') = g$. 我们得到

$$\frac{p}{g} = p_1 \cdots p_m. \square$$

推论 6.2 设 F 是特征为零的域, $p \in F[x] \setminus F$. 则 p 是无平方的当且仅当 p 和 p' 互素.

证明. 如果 $\gcd(p, p') = 1$, 则由上述定理 p 与它的无平方部分在 F 上相伴. 于是 p 是无平方的. 反之, 若 p 无平方, 则 $m_1 = \cdots = m_k = 1$. 于是上述定理证明中的多项式 $g = 1$, 即 $\gcd(p, p') = 1$. \square

例 6.3 设 $p = x^4 - 2x + 1 \in \mathbb{Q}[x]$. 判断 p 是不是无平方的.

解. 计算 $p' = 4x^3 - 2$. 利用辗转相除法可得 $\gcd(p, p') = 1$. 于是 p 是无平方的.

下面的例子说明, 定理 6.1 对特征大于零的域不成立.

例 6.4 设 F 是分式域 \mathbb{Z}_2 . 令 $p = x^2$. 则 $p' = \bar{2}x = \bar{0}$. 于是 $\gcd(p, p') = p$. 但 p 的无平方部分显然不可能是 $\bar{1}$.

7 中国剩余定理

引理 7.1 设 $m_1, \dots, m_k \in \mathbb{Z}^+ \setminus \{1\}$ 两两互素. 则

(i) $m_1 \cdots m_{k-1}$ 和 m_k 互素.

(ii) $\text{lcm}(m_1, \dots, m_k) = m_1 \cdots m_k$.

证明. (i) 由 Bezout 关系可知. 对任意 $i \in \{1, 2, \dots, k-1\}$ 存在 $u_i, v_i \in \mathbb{Z}$ 使得 $u_i m_i + v_i m_k = 1$. 于是

$$1 = \prod_{i=1}^{k-1} (u_i m_i + v_i m_k) = u(m_1 \cdots m_{k-1}) + v m_k,$$

其中 $u = u_1 \cdots u_{k-1}$ 且 v 是整数. 这个新的 Bezout 关系蕴含 $m_1 \cdots m_{k-1}$ 和 m_k 互素.

(ii) 当 $k = 2$ 时, 结论是上学期第一章中引理 6.1. 设 $k > 2$ 且当 $k-1$ 时我们有

$$\text{lcm}(m_1, \dots, m_{k-1}) = m_1 \cdots m_{k-1}. \quad (4)$$

由 (i) 和 $k = 2$ 的情形可知

$$\text{lcm}(m_1 \cdots m_{k-1}, m_k) = m_1 \cdots m_{k-1} m_k.$$

令

$$\ell = \text{lcm}(m_1, \dots, m_{k-1}, m_k).$$

因为 $(m_1 \cdots m_{k-1} m_k)$ 是 m_1, \dots, m_{k-1}, m_k 的公倍式, 所以 $\ell | (m_1 \cdots m_{k-1} m_k)$. 又因为 ℓ 是 m_1, \dots, m_{k-1} 的公倍式, 所以由 (4) 可知 $(m_1 m_2 \cdots m_{k-1}) | \ell$. 于是, ℓ 是 $(m_1 m_2 \cdots m_{k-1})$ 和 m_k 的公倍式. 从而, $(m_1 \cdots m_{k-1} m_k) | \ell$. 综上所述, $\ell = m_1 \cdots m_{k-1} m_k$. \square .

类似地, 我们有下述引理

引理 7.2 设 $f_1, \dots, f_k \in F[x] \setminus F$ 两两互素. 则

(i) $f_1 \cdots f_{k-1}$ 和 f_k 互素.

(ii) $\text{lcm}(f_1, \dots, f_k) = f_1 \cdots f_k$.

证明. (i) 把上述引理关于第一个结论的证明中的 Bezout 关系换成关于域上一元多项式的 Bezout 关系即可.

(ii) 类似的替换可以证明上学期第一章中引理 6.1 对域上一元多项式也成立, 其它的推理类似. \square

注解 7.3 上述两个引理可以利用 *Euclid* 整环的语言统一叙述和证明. 也可以利用 \mathbb{Z} 和 $F[x]$ 都是唯一因子分解整环来证明.

定理 7.4 设 $m_1, \dots, m_k \in \mathbb{Z}^+ \setminus \{1\}$, 两两互素, $r_1, \dots, r_k \in \mathbb{Z}$. 则存在唯一的 $r \in \mathbb{N}$ 满足

$$\begin{cases} r \equiv r_1 \pmod{m_1} \\ \vdots \\ r \equiv r_k \pmod{m_k} \end{cases}$$

且 $r < m_1 \cdots m_k$.

证明. (存在性) 对 k 归纳. 当 $k = 1$ 时令 $r = r_1$ 即可. 设 $k > 1$ 且存在 $s \in \mathbb{Z}$ 使得, $s \equiv r_i \pmod{m_i}, i = 1, 2, \dots, k-1$. 由引理 7.1 (i), 存在 $u, v \in \mathbb{Z}$ 使得 $u(m_1 \cdots m_{k-1}) + vm_k = 1$. 令

$$t = s + u(m_1 \cdots m_{k-1})(r_k - s).$$

则 $t \equiv s \pmod{m_i}$. 由归纳假设 $t \equiv r_i \pmod{m_i}, i = 1, 2, \dots, k-1$. 另一方面

$$t = s + (1 - vm_k)(r_k - s) = r_k - vm_k(r_k - s).$$

于是, $t \equiv r_k \pmod{m_k}$. 再令 $r = \text{rem}(t, m_1 \cdots m_{k-1}m_k)$. 则 $0 \leq r < m_1 \cdots m_{k-1}m_k$ 且 r 满足定理中的同余关系. 我们证明了存在性.

(唯一性) 设 \tilde{r} 也满足定理中同余关系且 $0 \leq \tilde{r} < m_1 \cdots m_{k-1}m_k$. 不妨设 $r \geq \tilde{r}$. 则 $r - \tilde{r} \equiv 0 \pmod{m_i}, i = 1, \dots, k-1, k$. 于是, $r - \tilde{r}$ 是 m_1, \dots, m_{k-1}, m_k 的公

倍式且 $0 \leq r - \tilde{r} < m_1 \cdots m_{k-1} m_k$. 由引理 7.1 (ii) 可知, $r = \tilde{r}$. \square

例 7.5 求正整数 r 满足

$$r \equiv 2 \pmod{3}, r \equiv 3 \pmod{5}, r \equiv 2 \pmod{7}.$$

解. 设 $a = 2$. 计算得 $2 \times 3 + (-1) \times 5 = 1$. 令 $b = a + 2 \times 3 \times (3 - a) = 8$. 计算得 $15 - 2 \times 7 = 1$. 令 $c = 8 + 15 \times (2 - 8) = -82$. 最后, $r = \text{rem}(-82, 105) = 23$. 于是所有的正整数解是

$$\{23 + 105k \mid k = 0, 1, 2, \dots\}.$$

类似地, 关于一元多项式的中国剩余定理如下.

定理 7.6 设 $f_1, \dots, f_k \in F[x] \setminus F$, 两两互素, $r_1, \dots, r_k \in F[x]$. 则存在唯一的 $r \in F[x]$ 满足

$$\begin{cases} r \equiv r_1 \pmod{f_1} & (\text{即 } f_1 \mid (r - r_1)) \\ \vdots \\ r \equiv r_k \pmod{f_k} \end{cases}$$

且 $\deg(r) < \deg(f_1) + \cdots + \deg(f_k)$.

证明. 与定理 7.4 类似, 只要把关于整数的结论和运算换成多项式的即可. \square