第五章　多项式和复数域

例 1.14 设 F 是域, $A, B \in \mathrm{M}_n(F)$. 证明 $(AB)^\vee = B^\vee A^\vee$.

证明. 设 A 和 B 都可逆. 则 AB 可逆. 我们有

$$(AB)^\vee = \det(AB)(AB)^{-1} = \det(B)B^{-1}\det(A)A^{-1} = B^\vee A^\vee.$$

设 t 是 F 上的未定元. 则

$$M := tE + A \quad 和 \quad N := tE + B$$

是域 $F(t)$ 上的矩阵. $\det(M)$ 和 $\det(N)$ 都是 $F[t]$ 中的 n 次多项式. 故它们都不等于零. 于是, M 和 N 都可逆. 由上述结论可知

$$(MN)^\vee = N^\vee M^\vee.$$

注意到 $M^\vee, N^\vee, (MN)^\vee$ 中的每个元素在 $F[t]$ 中. 故对应元素相等是两个多项式相等. 于是

$$(MN)^\vee|_{t=0} = MN^\vee|_{t=0}.$$

而从 M 通过定义计算 $M^\vee$ 的过程只需要加法和乘法. 又因为把 t 赋值为零是同态, 所以 $M^\vee|_{t=0} = (M|_{t=0})^\vee$. 换言之, $A^\vee = M^\vee|_{t=0}$. 同理 $B^\vee = (N^\vee)_{t=0}$. 类似可证 $(AB)^\vee = (MN)^\vee|_{t=0}$. 综上可知, $(AB)^\vee = B^\vee A^\vee$. □

1.4 多项式的除法

在本节中 F 是域.

定理 1.15 设 $f, g \in F[x]$ 且 $g \neq 0$. 则存在唯一的多项式 $q, r \in F[x]$ 满足

$$f = qg + r \quad 和 \quad \deg(r) < \deg(g).$$

证明. *(存在性)* 当 $\deg(f) < \deg(g)$ 时, 令 $q = 0$ 和 $r = f$ 即可. 否则, 设

$$f = f_{n+k}x^{n+k} + f_{n+k-1}x^{n+k-1} + \cdots + f_0, \; g = g_n x^n + g_{n-1}x^{n-1} + \cdots + g_0,$$

其中 $k \geq 0$, $f_i, g_j \in F$ 且 g_n 可逆.

我们对 k 归纳. 当 $k = 0$ 时, 计算

$$\begin{aligned} f - f_n g_n^{-1} g &= (f_n - f_n g_n^{-1} g_n)x^n + (f_{n-1} - f_n g_n^{-1} g_{n-1})x^{n-1} + \cdots + f_0 - f_n g_n^{-1} g_0 \\ &= \underbrace{(f_{n-1} - f_n g_n^{-1} g_{n-1})x^{n-1} + \cdots + f_0 - f_n g_n^{-1} g_0}_{r} \end{aligned}$$

再令 $q = f_n g_n^{-1}$. 则 $f = qg + r$ 且 $\deg(r) < n$ 即可.

设 $k > 0$ 且存在性对小于 k 的值都成立. 计算

$$\begin{aligned} & f - f_{n+k} g_n^{-1} x^k g \\ &= (f_{n+k} - f_{n+k} g_n^{-1} g_n)x^{n+k} + (f_{n+k-1} - f_{n+k} g_n^{-1} g_{n-1})x^{n+k-1} + \\ & \cdots + (f_k - f_{n+k} g_n^{-1} g_0)x^k + f_{k-1}x^{k-1} + \cdots + f_0 \\ &= \underbrace{(f_{n+k-1} - f_{n+k} g_n^{-1} g_{n-1})x^{n+k-1} + \cdots + (f_k - f_{n+k} g_n^{-1} g_0)x^k + f_{k-1}x^{k-1} + \cdots + f_0}_{h}. \end{aligned}$$

则 $\deg(h) < n + k$. 由归纳假设或证明中第一段的结论可得, 存在 $\tilde{q}, r \in R[x]$ 满足

$$h = \tilde{q} g + r \quad 和 \quad \deg(r) < n.$$

则

$$f = \underbrace{(f_n g_n^{-1} x^{n-k} + \tilde{q})}_{q} g + r.$$

存在性成立.

(唯一性) 再设 $q', r' \in F[x]$ 满足

$$f = q'g + r' \quad 和 \quad \deg(r') < \deg(g).$$

则

$$(q - q')g = r' - r. \tag{1}$$

因为 $\deg(r) < \deg(g)$ 且 $\deg(r') < \deg(g)$, 所以

$$\deg(r' - r) < \deg(g).$$

因为 $\mathrm{lc}(g)$ 可逆, 所以

$$\deg((q - q')g) = \deg(q - q') + \deg(g).$$

由此可知, (1) 蕴含 $q = q'$. 进而, $r = r'$. 唯一性成立. □

沿用定理 1.15 的符号, 我们称 q 是被除式 f 关于除式 g 的商, r 是余式. 记为 $\mathrm{quo}(f, g, x)$ 和 $\mathrm{rem}(f, g, x)$. 有时也可以省略未定元 x.

例 1.16 设 $f = x^3 + 3x + 1$ 和 $g = 2x^2 + 1$ 是 $\mathbb{Q}[x]$ 中的多项式. 计算 $\mathrm{rem}(f, g, x)$.

解. 直接计算得

$$h := f - \frac{1}{2}xg = \frac{5}{2}x + 1.$$

因为 $\deg(h) < \deg(g)$, 所以

$$\operatorname{rem}(f,g,x) = \frac{5}{2}x + 1 \quad \text{和} \quad \operatorname{quo}(f,g,x) = \frac{1}{2}x.$$

例 1.17 设 $f = \bar{3}x^3 + \bar{2}x^2 + \bar{1}$ 和 $g = \bar{2}x^2 + \bar{4}$ 是 $\mathbb{Z}_5[x]$ 中的多项式. 计算 $\operatorname{quo}(f,g,x)$ 和 $\operatorname{rem}(f,g,x)$.

解. 注意到 $\bar{2}^{-1} = \bar{3}$. 于是

$$h_1 := f - \bar{3}\cdot\bar{3}xg = f - \bar{4}xg = \bar{2}x^2 - x + \bar{1} = \bar{2}x^2 + \bar{4}x + \bar{1}.$$

$$h_2 := h_1 - g = \bar{4}x - \bar{3} = \bar{4}x + \bar{2}.$$

于是,

$$f - \bar{4}xg - g = \bar{4}x + \bar{2} \implies f = (\bar{4}x + 1)g + (\bar{4}x + \bar{2}).$$

我们得到 $\operatorname{quo}(f,g,x) = \bar{4}x + 1$ 和 $\operatorname{rem}(f,g,x) = \bar{4}x + \bar{2}$.

定理 1.18 *(余式定理)* 设 $a \in F$ 和 $f(x) \in F[x]$. 则

$$f(a) = \operatorname{rem}(f, x - a).$$

证明. 根据定理 1.15, 存在 $q \in F[x]$ 和 $r \in F$ 使得

$$f(x) = q(x)(x - a) + r.$$

注意到把 x 代换为 a 是环同态. 于是, $f(a) = q(a)(a-a)+r$. 故 $f(a) = r$. $\square$

1.5 多项式的根

定义 1.19 *设 F 和 K 是域, 且 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(root), 即 α 是方程 $f(x) = 0$ 在 K 中的一个解.*

例 1.20 *多项式 $x^2 - 2 \in \mathbb{Q}[x]$ 在 $\mathbb{R}$ 中有根 $\pm\sqrt{2}$, 但它在 $\mathbb{Q}$ 中无根.*

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

(i) $\alpha \in F$ 是 f 的根当且仅当 $\mathrm{rem}(f, x - \alpha) = 0$;

(ii) f 在 F 中至多有 n 个互不相同的根.

证明. (i) 由余式定理可知, $f(\alpha) = 0 \Leftrightarrow \mathrm{rem}(f, x - \alpha) = 0$.

(ii) 对 n 归纳. 当 $n = 1$ 时, $f = f_1 x + f_0$, $f_1, f_0 \in F$ 且 $f_1 \neq 0$. 于是, f 由唯一的根 $-f_0 f_1^{-1}$. 结论成立. 设结论对 $F[x]$ 次数等于 $n - 1$ 次的多项式成立, 其中 $n > 0$. 如果 f 在 F 中没有根, 则结论显然成立. 假设 $\alpha \in F$ 是 f 的一个根. 根据 (i), $f(x) = g(x)(x - \alpha)$, 其中 $g \in F[x]$ 且 $\deg(g) = n - 1$. 由归纳假设 g 在 F 中至多有 $n - 1$ 个不同的根, 故 f 在 F 中至多有 n 个不同的根. □

推论 1.22 *设 F, K 是域且 F 是 K 的子域. 设 $f \in F[x]$ 且 $\deg(f) = n > 0$. 则*

(i) $\alpha \in K$ 是 f 的根当且仅当 $\mathrm{rem}(f, x-\alpha) = 0$;

(ii) f 在 K 中至多有 n 个互不相同的根.

证明. 因为 $F \subset K$, 所以 $F[x] \subset K[x]$. 故推论可由上述命题直接得到(把系数域 F 换为 K). $\square$

例 1.23 设 $f(x) \in F[x]$ 的次数为 $n > 0$, $\alpha_1, \ldots, \alpha_n \in F$ 是 $f(x)$ 的 n 个互不相同的根. 证明:

$$f(x) = \mathrm{lc}(f)(x-\alpha_1)\cdots(x-\alpha_n).$$

证明. 对 n 归纳. 当 $n=1$ 时, $f(x) = q(x-\alpha_1)$ *(*命题 *1.21 (i))* 且 $q \in F$. 故 $q = \mathrm{lc}(f)$. 设 $n-1$ 时结论成立. 当 n 时, 再利用命题 *1.21 (i)*, 我们有

$$f(x) = q(x)(x-\alpha_1),$$

其中 $q(x)$ 是 $F[x]$ 中的 $n-1$ 次多项式. 对 $i = 2, \ldots, n$,

$$0 = f(\alpha_i) = q(\alpha_i)(\alpha_i - \alpha_1).$$

因为 $\alpha_i \neq \alpha_1$, 所以 $q(\alpha_i) = 0$. 由归纳假设可知

$$q(x) = \mathrm{lc}(q)(x-\alpha_2)\cdots(x-\alpha_n).$$

于是,

$$f(x) = \mathrm{lc}(q)(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_n).$$

而 $\mathrm{lc}(q) = \mathrm{lc}(f)$ 是显然的. $\square$

例 1.24 设 p 是素数. 证明: 在 $\mathbb{Z}_p[x]$ 中,

$$x^p - x = x(x-\bar{1})(x-\bar{2})\cdots(x-\overline{p-1}).$$

证明. 根据上周讲义例 *4.12*, 对任意 $\bar{k} \in \mathbb{Z}_p$, $\bar{k}^p - \bar{k} = \bar{0}$. 故多项式 $x^p - x$ 在 $\mathbb{Z}_p$ 中有 p 个不同的根. 由上例可知:

$$x^p - x = x(x-\bar{1})(x-\bar{2})\cdots(x-\overline{p-1}). \quad \square$$

2 多元多项式环

2.1 单项式与分布式表示

定义 2.1 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 2.2 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. $\square$

定义 2.3 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 2.4 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 $R[x_1, \ldots, x_n]$ 中的运算, $R[x_1, \ldots, x_n]$ 中的任何元素 f 可以写成

$$f = \alpha_1 M_1 + \cdots + \alpha_k M_k, \tag{2}$$

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

引理 2.5 设 (2) 中 $M_1, \ldots, M_k$ 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

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

如果 $d = 0$, 则 x_n 在 $M_1, \ldots, M_k$ 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 $\alpha_1, \ldots, \alpha_k$ 都不等于零. 再设 $i \in \{1, \ldots, n\}$ 使得 $M_1, \ldots, M_{i-1}$ 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

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

$$0 = \underbrace{\alpha_1 M_1 + \cdots + \alpha_{i-1} M_{i-1}}_{P} + \underbrace{(\alpha_i N_i + \cdots + \alpha_k N_k)}_{Q} x_n^d.$$

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

定理 2.6 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

$$p = \alpha_1 M_1 + \cdots + \alpha_k M_k. \tag{3}$$

(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 2.5, $i = k = \ell$ 且 $\alpha_1 = \beta_1, \ldots, \alpha_k = \beta_k$. $\square$

定义 2.7 设 $p \in R[x_1, \ldots, x_n] \setminus \{0\}$ 的分布式表示为 (3). 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 2.8 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 2.9 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 $\deg(p) = 3$.

2.2 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 2.10 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 2.11 例 *2.9* 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 2.12 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 2.5, $\deg(h_d + h_e) = d$. 当 $d = e$ 时, $\deg(h_d + h_e) = d$ 或 0. 结论成立.

(ii) 由注释 2.8 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 2.13 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 2.16 (i) 可知, $\deg(p + q) \leq d$.

(ii) 由引理 2.16 (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. □

2.3 注记

例 2.14 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 $M = x_1^{i_1} \cdots x_n^{i_n}$.

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

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.

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

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 2.15 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

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

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

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

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 $\phi_{s_1,\ldots,s_n}$. $\square$

3 对称多项式

设 $\sigma \in S_n$, $\phi : R \to R[x_1, \ldots, x_n]$ 是嵌入(满足 $\forall\ r \in R$, $\phi(r) = r$). 则 $\phi_\sigma : R[x_1, \ldots, x_n] \to R[x_1, \ldots, x_n]$ 满

足

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

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

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

$$x_1^i + \cdots + x_n^i$$

是对称多项式.

由对称多项式的定义可知, 两个对称多项式的和与积仍是对称多项式. 进一步可以验证所有 $R[x_1, \ldots, x_n]$ 中的对称多项式构成一个子环. 在该环中有一类重要的对称多项式. 设

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

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 $\epsilon_1, \ldots, \epsilon_{n-1}, \epsilon_n \in R[x_1, \ldots, x_n]$. 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 $\phi_\sigma: R[x_1,\dots,x_n,x_{n+1}]\longrightarrow R[x_1,\dots,x_n,x_{n+1}]$ 是同构. 则

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

另一方面,

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

根据定理 2.1, $\phi_\sigma(\epsilon_1)=\epsilon_1$, …, $\phi_\sigma(\epsilon_{n-1})=\epsilon_{n-1}$ 和 $\phi_\sigma(\epsilon_n)=\epsilon_n$. 于是, ϵ_1, …, ϵ_{n-1}, ϵ_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 3.2 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

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

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 3.3 设 F 是域, $f \in F[x]$, $\deg(f) = n > 0$, $\mathrm{lc}(f) = a_n$. 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 $\alpha_1, \ldots, \alpha_n \in F$, 不必两两不同. 则

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

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

证明. 由定理 2.15 可知, 存在赋值同态

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

满足: $\phi|_F$ 是恒同映射, $\phi(x_i) = \alpha_i, i = 1, 2, \ldots, n$ 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, $a_n(-1)^{n-i}\epsilon_{n-i}(\alpha_1, \ldots, \alpha_n) = a_i$, $i = 0, 1, \ldots, n$. □

例 3.4 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 $f = ax^3 + bx^2 + cx + s \in \mathbb{R}[x]$ 且 $a \neq 0$, $\alpha, \beta, \gamma \in \mathbb{C}$ 是 f 的三个根. 则

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