第五章　复数域和多项式

4　复数

4.3　单位根

设 $n \in \mathbb{Z}^+$. 方程 $z^n = 1$ 在 $\mathbb{C}$ 中的根称为 n 次单位根.

命题 4.5 *方程 $z^n = 1$ 在 $\mathbb{C}$ 中有 n 个互不相同的根*

$$\epsilon_k = e^{\frac{2k\pi\mathbf{i}}{n}}, \quad k = 0, 1, \ldots, n-1.$$

证明. 直接计算得

$$\epsilon_k^n = e^{2k\pi\mathbf{i}} = 1.$$

故 $\epsilon_0, \epsilon_1, \ldots, \epsilon_{n-1}$ 都是单位根. 设 $k, m \in \{0, 1, \ldots, n-1\}$ 且 $k \leq m$. 如果 $\epsilon_k = \epsilon_m$, 则

$$1 = \epsilon_m \epsilon_k^{-1} = e^{\frac{2(m-k)\pi\mathbf{i}}{n}}.$$

因为 $m-k \in \{0, 1, \ldots, n-1\}$, 所以 $m = k$. 故 $\epsilon_0, \epsilon_1, \ldots, \epsilon_{n-1}$ 两两不同. □

根据第五章第二讲定理 3.19, 方程 $z^n = 1$ 在 $\mathbb{C}$ 中的至多有 n 个根. 于是, $\mathbb{C}$ 中恰有 n 个互不相同的单位根. 记 U_n 是这些单位根的集合.

命题 4.6 三元组 $(U_n, \cdot, 1)$ 是循环群. $U_n = \langle \epsilon_\ell \rangle$ 当且仅当 $\gcd(\ell, n) = 1$.

证明. 先证 U_n 是群. 因为 $(\mathbb{C}^*, \cdot, 1)$ 是群且 $U_n \subset \mathbb{C}^*$, 所以只要证明对任意 $a, b \in U_n$, $ab^{-1} \in U_n$ (上学期第四章第一讲命题 2.24). 注意到 $(ab^{-1})^n = a^n(b^n)^{-1} = 1$. 故 U_n 是群. 因为 $\epsilon_k = \epsilon_1^k$, $k = 0, 1, \ldots, n-1$, 所以 $U_n = \langle \epsilon_1 \rangle$. 故 U_n 是循环群. 特别地 $\mathrm{ord}(\epsilon_1) = n$.

根据上学期第四章第二讲推论 2.38, $\mathrm{ord}(\epsilon_\ell) = n/\gcd(\ell, n)$. 而 ϵ_ℓ 是 U_n 的生成元当且仅当 $\mathrm{ord}(\epsilon_\ell) = n$, 即 $\gcd(\ell, n) = 1$. □

当 $U_n = \langle \epsilon_\ell \rangle$ 时, ϵ_ℓ 称为 n 次本原单位根.

例 4.7 设循环矩阵

$$A = \begin{pmatrix} a_0 & a_1 & \cdots & a_{n-2} & a_{n-1} \\ a_{n-1} & a_0 & \cdots & a_{n-3} & a_{n-2} \\ a_{n-2} & a_{n-1} & \cdots & a_{n-4} & a_{n-3} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ a_1 & a_2 & \cdots & a_{n-1} & a_0 \end{pmatrix} \in \mathrm{M}_n(\mathbb{C}).$$

计算 A 的行列式. 当矩阵 A 可逆时, 求 A^{-1}.

解. 设 $\epsilon_0, \ldots, \epsilon_{n-1}$ 是 n 个 n 次单位根. 令 $f = a_0 + a_1 x + \cdots + a_{n-2}x^{n-2} + a_{n-1}x^{n-1} \in \mathbb{C}[x]$. 对 $k \in \{0, 1, \ldots, n-1\}$,

利用 $\epsilon_k^n = 1$ 得到

$$f(\epsilon_k) = a_0 + a_1\epsilon_k + \cdots + a_{n-2}\epsilon_k^{n-2} + a_{n-1}\epsilon_k^{n-1},$$

$$\epsilon_k f(\epsilon_k) = a_{n-1} + a_0\epsilon_k + \cdots + a_{n-3}\epsilon_k^{n-2} + a_{n-2}\epsilon_k^{n-1},$$

$$\epsilon_k^2 f(\epsilon_k) = a_{n-2} + a_{n-1}\epsilon_k + \cdots + a_{n-4}\epsilon_k^{n-2} + a_{n-3}\epsilon_k^{n-1},$$

$$\vdots$$

$$\epsilon_k^{n-1} f(\epsilon_k) = a_1 + a_2\epsilon_k + \cdots + a_{n-1}\epsilon_k^{n-2} + a_0\epsilon_k^{n-1}.$$

利用矩阵写成

$$f(\epsilon_k)\begin{pmatrix} 1 \\ \epsilon_k \\ \epsilon_k^2 \\ \vdots \\ \epsilon_k^{n-1} \end{pmatrix} = A\begin{pmatrix} 1 \\ \epsilon_k \\ \epsilon_k^2 \\ \vdots \\ \epsilon_k^{n-1} \end{pmatrix}, \quad k = 0, 1, \ldots, n-1.$$

设

$$V = \begin{pmatrix} 1 & 1 & \cdots & 1 \\ \epsilon_0 & \epsilon_1 & \cdots & \epsilon_{n-1} \\ \vdots & \vdots & \ddots & \vdots \\ \epsilon_0^{n-1} & \epsilon_1^{n-1} & \cdots & \epsilon_{n-1}^{n-1} \end{pmatrix}.$$

则 $V\mathrm{diag}(f(\epsilon_0), \ldots, f(\epsilon_{n-1})) = AV$. 换言之,

$$A = V\mathrm{diag}(f(\epsilon_0), \ldots, f(\epsilon_{n-1}))V^{-1}.$$

两边取行列式得

$$\det(A) = f(\epsilon_0) \cdots f(\epsilon_{n-1}).$$

进而 A 可逆当且仅当 $\gcd(f, x^n - 1) = 1$. 此时,

$$A^{-1} = V \mathrm{diag}(f(\epsilon_0)^{-1}, \ldots, f(\epsilon_{n-1})^{-1}) V^{-1}.$$

注解 4.8 设上例中 $a_0 = 1, a_1 = 2, \ldots, a_{n-1} = n$. 则矩阵 A 是上学期第十周作业中第 5 题的矩阵. 用当时的知识得

$$\det(A) = (-1)^{n+1} n^{n-1} \frac{n+1}{2}$$

和

$$A^{-1} = \frac{1}{sn} \begin{pmatrix} 1-s & 1+s & 1 & 1 & \cdots & 1 \\ 1 & 1-s & 1+s & 1 & \cdots & 1 \\ 1 & 1 & 1-s & 1+s & \cdots & 1 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 1+s & 1 & 1 & 1 & \cdots & 1-s \end{pmatrix},$$

其中 $s = n(n-1)/2$.

4.4 代数学基本定理

定理 4.9 *(代数学基本定理)* 设 $f \in \mathbb{C}[x] \setminus \mathbb{C}$. 则 f 在 $\mathbb{C}[x]$ 有根.

上述定理的证明要用到超出本课程范围的知识. 这里不给出证明. 但它的两个推论对下学期的学习比较重要.

推论 4.10 设 $f \in \mathbb{C}[x] \setminus \mathbb{C}$. 则存在互不相同的复数 $\alpha_1, \cdots, \alpha_k$ 和非零正整数 $m_1, \ldots, m_k$ 使得

$$f = \mathrm{lc}(f)(x-\alpha_1)^{m_1} \cdots (x-\alpha_k)^{m_k}.$$

证明. 设 $n = \deg(f), \ell = \mathrm{lc}(f)$. 我们对 n 归纳.

当 $n = 1$ 时结论显然成立. 设 $n > 1$ 且结论对 $n-1$ 次复系数多项式都成立. 由代数学基本定理, 存在 $\alpha \in \mathbb{C}$ 使得 $f(\alpha)=0$. 根据余式定理,

$$f(x) = (x-\alpha)g(x),$$

其中 $g \in \mathbb{C}[x]$, $\deg(g) = n-1$ 且 $\mathrm{lc}(g) = \lambda$. 由归纳假设存在互不相同的复数 $\alpha_1, \cdots, \alpha_k$ 和非零正整数 $m_1, \ldots, m_k$ 使得

$$g = \lambda(x-\alpha_1)^{m_1} \cdots (x-\alpha_k)^{m_k}.$$

如果 $\alpha \in \{\alpha_1, \ldots, \alpha_k\}$, 则不妨设 $\alpha = \alpha_1$. 由此得出

$$f(x) = \lambda(x-\alpha_1)^{m_1+1} \cdots (x-\alpha_k)^{m_k}.$$

否则

$$f(x) = \lambda(x-\alpha)(x-\alpha_1)^{m_1} \cdots (x-\alpha_k)^{m_k}. \quad \square$$

该推论说明 $\mathbb{C}[x]$ 中的不可约元是零次或者一次的多项式, 每个复系数多项式在 $\mathbb{C}$ 中的根的个数(计算重数)与其次数相同.

推论 4.11 *在 $\mathbb{R}[x]$ 中的不可约元的次数至多是二次.*

证明. 假设 $f(x) = f_n x^n + f_{n-1}x^{n-1} + \cdots + f_0 \in \mathbb{R}[x]$ 是不可约的且 $n > 2$ 和 $f_n \neq 0$. 因为 f 也是复系数多项式, 所以代数学基本定理蕴含 f 由复根 α. 注意到 $\alpha \notin \mathbb{R}$. 否则由余式定理 f 会有一次实系数因子 $x - \alpha$, 与 f 的不可约性矛盾. 特别地, $\bar{\alpha} \neq \bar{\alpha}$.

因为实数的共轭是它自身, 所以

$$0 = f(\alpha) = \overline{f(\alpha)} = \sum_{i=0}^{n} \bar{f}_i \bar{\alpha}^i = \sum_{i=0}^{n} f_i \bar{\alpha}^i = f(\bar{\alpha}).$$

故 f 由两个互不相同的复根 α 和 $\bar{\alpha}$. 由余式定理, 实二次多项式 $g(x) = (x - \alpha)(x - \bar{\alpha})$ 整除 $\mathbb{R}[x]$. 矛盾. □

该推论说明 $\mathbb{R}[x] \setminus \mathbb{R}$ 中的多项式, 都是 $\mathbb{R}[x]$ 中若干一次或二次不可约多项式的乘积.

4.5 几个关于复数的例子

可直接验证

$$\mathbb{Z}[\sqrt{-5}] = \{x + y\sqrt{-5} \,|\, x, y \in \mathbb{Z}\}$$

是 $\mathbb{C}$ 的子环. 它显然是整环. 可直接验证该环中的可逆元是 ± 1. 注意到

$$9 = 3 \cdot 3 = (2 + \sqrt{-5})(2 - \sqrt{-5}).$$

下面我们证明 3 和 $2 \pm \sqrt{-5}$ 都是 $\mathbb{Z}[\sqrt{-5}]$ 中的不可约元.

设 $3 = (m + n\sqrt{-5})(k + \ell\sqrt{-5})$, 其中 $m, n, k, \ell \in \mathbb{Z}$. 两边取共轭得 $3 = (m - n\sqrt{-5})(k - \ell\sqrt{-5})$. 于是

$$9 = (m^2 + 5n^2)(k^2 + 5\ell^2).$$

但 $m^2+5n^2 = 3$ 无整数解. 故 $m^2+5n^2 = 1$ 或 $m^2+5n^2 = 9$. 前者意味着 $m = \pm 1, n = 0$, 即 $m + n\sqrt{-5} = \pm 1$ 是可逆元. 而后者意味着 $k + \ell\sqrt{-5}$ 是可逆元. 故 3 不可约.

类似地, 设 $2 + \sqrt{-5} = (m + n\sqrt{-5})(k + \ell\sqrt{-5})$, 其中 $m, n, k, \ell \in \mathbb{Z}$. 两边取共轭得

$$2 - \sqrt{-5} = (m - n\sqrt{-5})(k - \ell\sqrt{-5}).$$

于是, $9 = (m^2 + 5n^2)(k^2 + 5\ell^2)$. 同样的推理可知 $2 + \sqrt{-5}$ 不可约. 同理 $2 - \sqrt{-5}$ 也不可约. 这个例子说明 $\mathbb{Z}[\sqrt{-5}]$ 不是唯一因子分解整环.

注意到在该环中, 9 和 $6+3\sqrt{-5}$ 有公因子 3 和 $2+\sqrt{-5}$. 设 d 是 9 和 $6 + 3\sqrt{-5}$ 的最大公因子. 则 $d = 3(x + y\sqrt{-5})$, 其中 $x, y \in \mathbb{Z}$. 因为 $d|9$, 所以 $(x + y\sqrt{-5}) \,|\, 3$. 又因为 3 不可约. 不妨设 $x = 3, y = 0$. 故 $d = 9$. 于是,

$$9 \,|\, (6 + 3\sqrt{-5}) \implies 3 \,|\, (2 + \sqrt{-5}).$$

因为 $2+\sqrt{-5}$ 不可约, 所以 $\pm 3 = 2+\sqrt{-5}$. 矛盾. 由此得出, 9 和 $6+3\sqrt{-5}$ 在 $\mathbb{Z}[\sqrt{-5}]$ 中没有最大公因子.

最后, 我们来看四元数环. 设

$$H = \left\{ \begin{pmatrix} u & v \\ -\bar{v} & \bar{u} \end{pmatrix} \mid u, v \in \mathbb{C} \right\}.$$

则 $(H, +, O, \cdot, E)$ 是 $\mathrm{M}_2(\mathbb{C})$ 中的非交换子环, 且 H 中的每个非零元在 H 中有可逆元. 这是数学史上第一个斜域(skew-field).

验证如下:

(i) 设 $W = \begin{pmatrix} u & v \\ -\bar{v} & \bar{u} \end{pmatrix}$ 和 $Z = \begin{pmatrix} x & y \\ -\bar{y} & \bar{x} \end{pmatrix}$, 其中 $u, v, x, y \in \mathbb{C}$.

我们有

$$W - Z = \begin{pmatrix} u-x & v-y \\ -\bar{v}+\bar{y} & \bar{u}-\bar{x} \end{pmatrix} = \begin{pmatrix} u-x & v-y \\ -\overline{v-y} & \overline{u-x} \end{pmatrix} \in H.$$

故 $(H, +, O)$ 是 $(\mathrm{M}_2(\mathbb{C}), +, O)$ 的子群.

计算

$$WZ = \begin{pmatrix} ux - v\bar{y} & uy + v\bar{x} \\ -\bar{v}x - \bar{u}\bar{y} & -\bar{v}y + \bar{u}\bar{x} \end{pmatrix} = \begin{pmatrix} ux - v\bar{y} & uy + v\bar{x} \\ -\overline{(uy + v\bar{x})} & \overline{ux - v\bar{y}} \end{pmatrix} \in H.$$

注意到

$$E_2 = \begin{pmatrix} 1 & 0 \\ -\bar{0} & \bar{1} \end{pmatrix} \in H.$$

故 H 是 $\mathrm{M}_2(\mathbb{C})$ 的子环.

(ii) 设 $A = \begin{pmatrix} \mathbf{i} & 0 \\ 0 & -\mathbf{i} \end{pmatrix}$ 和 $B = \begin{pmatrix} 0 & \mathbf{i} \\ \mathbf{i} & 0 \end{pmatrix}$. 则 $A, B \in H$. 直接计算得

$$AB = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \quad BA = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

因为 $AB \neq BA$, 所以 H 不是交换环.

(iii) 设 $W \neq O$. 则 $\det(W) = |u|^2 + |v^2| \neq 0$. 故 W 是可逆矩阵. 在 $\mathrm{M}_n(\mathbb{C})$ 中,

$$W^{-1} = \frac{1}{u\bar{u} + v\bar{v}} \begin{pmatrix} \bar{u} & -v \\ \bar{v} & u \end{pmatrix} \in H.$$

故 W 在 H 中可逆.

5 多元多项式

回忆: 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

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

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.

5.1 多元多项式环

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 $R[x_1,\ldots,x_n]$.

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

证明. 设 R 是整环. 当 $n=1$ 时 $R[x_1]$ 是整环(上学期第十六讲定理 1.8). 对 n 归纳可直接得出 $R[x_1,\ldots,x_n]$ 也是整环. 设 R 是唯一因子分解整环. 当 $n=1$ 时 $R[x_1]$ 是整环(上一讲定理定理 3.33). 对 n 归纳可直接得出 $R[x_1,\ldots,x_n]$ 也是整环. □

定义 5.4 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 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 $R[x_1, \ldots, x_n]$ 中的运算, $R[x_1, \ldots, x_n]$ 中的任何元素 f 可以写成

$$f = \alpha_1 M_1 + \cdots + \alpha_k M_k, \tag{1}$$

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 5.6 设 (1) 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 $\alpha_1 = \cdots = \alpha_k = 0$.

现在考虑 $d>0$ 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 $M_i=N_ix_n^d,\ldots,M_k=N_kx_n^d$, 其中 $N_i,\ldots,N_k\in X_{n-1}$. 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, $Q=0$. 再由归纳假设可知, $\alpha_i=\cdots=\alpha_k=0$, 矛盾. □

定理 5.7 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

$$p=\alpha_1M_1+\cdots+\alpha_kM_k. \tag{2}$$

(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

$$p=\beta_1N_1+\cdots+\beta_\ell N_\ell,$$

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 5.6, $i=k=\ell$ 且 $\alpha_1=\beta_1,\ldots,\alpha_k=\beta_k$. □

定义 5.8 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 5.9 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 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

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

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

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 5.11 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 5.12 例 *5.10* 中的多项式 $f = h_3 + h_2 + h_1 + h_0$, 其中

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

引理 5.13 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) $\deg(h_d h_e) \le d+e$, *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, $R[x_1, \ldots, x_n]$ 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 5.14 *设* p *和* q *分别是* $R[x_1, \ldots, x_n]$ *中* d *次和* e *次多项式. 则*

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

(ii) $\deg(pq) \le d+e$, *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 5.13 (i) 可知, $\deg(p+q) \le d$.

(ii) 由引理 5.13 (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. □

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 5.15 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 $\phi_{s_1,\ldots,s_n}$. □

例 5.16 设 F 是域. $\phi : F \longrightarrow F$ 是恒同映射, $\alpha_1, \ldots, \alpha_n \in F$. 则存在唯一的赋值同态

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

如果 $p(\alpha_1, \ldots, \alpha_n) = 0$, 则称 $(\alpha_1, \ldots, \alpha_n)$ 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 5.17 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

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

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 5.18 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.

5.4 初等对称多项式简介

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:

$$p=x_{n+1}^n-\epsilon_1x_{n+1}^{n-1}+\cdots+(-1)^{n-1}\epsilon_{n-1}x_{n+1}+(-1)^n\epsilon_n,$$

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 $x_1,\ldots,x_n$ 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 $\phi_\sigma: R[x_1,\ldots,x_n,x_{n+1}]\longrightarrow R[x_1,\ldots,x_n,x_{n+1}]$ 是由例 5.17 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,

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

根据定理 2.1,

$$\phi_\sigma(\epsilon_1) = \epsilon_1, \ldots, \phi_\sigma(\epsilon_{n-1}) = \epsilon_{n-1} \quad 和 \quad \phi_\sigma(\epsilon_n) = \epsilon_n.$$

于是, ϵ_1, ..., ϵ_{n-1}, ϵ_n 都是关于 $x_1, \ldots, x_n$ 的对称多项式.

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

例 5.19 通过直接计算可得, 当 $n = 2$ 时,

$$\epsilon_1 = x_1 + x_2, \epsilon_2 = x_1 x_2.$$

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

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

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 5.20 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 5.15 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,

$$a_n(-1)^{n-i}\epsilon_{n-i}(\alpha_1, \ldots, \alpha_n) = a_i, \quad i = 0, 1, \ldots, n. \quad \square$$

例 5.21 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

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