

多项式

秦加俊

2026 年 6 月 20 日

1 代数整数与循环矩阵

知识 1.1: 代数整数

称复数 λ_0 为**代数整数**，如果它是某个首一整系数多项式的根，即存在

$$f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 \in \mathbb{Z}[x]$$

使得

$$f(\lambda_0) = 0.$$

例题 1.1: 代数整数的基本性质 称 λ_0 为代数整数，当且仅当它是一个首一整系数多项式的根。回答下列问题：

1. 设 $r \in \mathbb{Q}$ ，证明： r 是代数整数当且仅当 $r \in \mathbb{Z}$ ；
2. 设 $d \in \mathbb{Z}$ ，证明： $\sqrt{d}$ 是代数整数；
3. 证明：任意单位根都是代数整数；
4. 设 λ_1, λ_2 均为代数整数，证明：

$$-\lambda_1, \quad \overline{\lambda_1}, \quad \lambda_1\lambda_2, \quad \lambda_1 + \lambda_2$$

也都是代数整数。

解答. 1. 设 $r = \frac{a}{b}$ ，其中 $(a, b) = 1$ ， $b > 0$ 。若 r 是代数整数，则存在

$$r^n + c_{n-1}r^{n-1} + \cdots + c_0 = 0, \quad c_i \in \mathbb{Z}.$$

乘以 b^n 得

$$a^n + c_{n-1}a^{n-1}b + \cdots + c_0b^n = 0.$$

故 $b \mid a^n$ ，由 $(a, b) = 1$ 得 $b = 1$ ，即 $r \in \mathbb{Z}$ 。反之，任意整数 r 是首一多项式 $x - r$ 的根，故为代数整数。

2. $\sqrt{d}$ 是首一整系数多项式

$$x^2 - d$$

的根，故是代数整数。

3. 若 ζ 是 n 次单位根, 则

$$\zeta^n = 1.$$

因此 ζ 是首一整系数多项式

$$x^n - 1$$

的根, 故是代数整数。

4. 代数整数对加法、乘法和取相反数封闭。可用有限生成 $\mathbb{Z}$ -模证明: 若 λ_1, λ_2 为代数整数, 则

$$\mathbb{Z}[\lambda_1, \lambda_2]$$

是有限生成 $\mathbb{Z}$ -模, 故其中任意元素都是代数整数。于是

$$-\lambda_1, \quad \lambda_1 + \lambda_2, \quad \lambda_1 \lambda_2$$

都是代数整数。若 λ_1 是首一整系数多项式 $f(x)$ 的根, 则 $\overline{\lambda_1}$ 也是 $f(x)$ 的根, 因为 f 的系数为实数, 故 $\overline{\lambda_1}$ 也是代数整数。

□

例题 1.2: 循环矩阵的特征值 求下列循环矩阵的所有特征值:

$$C = \begin{bmatrix} a_0 & a_1 & a_2 & \cdots & a_{n-1} \\ a_{n-1} & a_0 & a_1 & \cdots & a_{n-2} \\ a_{n-2} & a_{n-1} & a_0 & \cdots & a_{n-3} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a_1 & a_2 & a_3 & \cdots & a_0 \end{bmatrix}.$$

解答. 设

$$\omega_j = e^{2\pi i j/n}, \quad j = 0, 1, \dots, n-1.$$

取向量

$$v_j = (1, \omega_j, \omega_j^2, \dots, \omega_j^{n-1})^T.$$

直接计算可得

$$Cv_j = \lambda_j v_j,$$

其中

$$\lambda_j = a_0 + a_1 \omega_j + \cdots + a_{n-1} \omega_j^{n-1}, \quad j = 0, 1, \dots, n-1.$$

因此循环矩阵的全部特征值为上述 λ_j 。

□

例题 1.3: 反循环矩阵的行列式 求下列反循环矩阵的行列式:

$$A = \begin{bmatrix} a_0 & a_1 & a_2 & \cdots & a_{n-1} \\ -a_{n-1} & a_0 & a_1 & \cdots & a_{n-2} \\ -a_{n-2} & -a_{n-1} & a_0 & \cdots & a_{n-3} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ -a_1 & -a_2 & -a_3 & \cdots & a_0 \end{bmatrix}.$$

解答. 令

$$p(x) = a_0 + a_1x + \cdots + a_{n-1}x^{n-1}.$$

该矩阵对应于商代数

$$\mathbb{C}[x]/(x^n + 1)$$

中乘以 $p(x)$ 的线性变换。因此其特征值为

$$p(\zeta), \quad \zeta^n = -1.$$

故

$$\det A = \prod_{\zeta^n = -1} p(\zeta) = \prod_{\zeta^n = -1} (a_0 + a_1\zeta + \cdots + a_{n-1}\zeta^{n-1}).$$

□

例题 1.4: 上三角特殊矩阵的逆矩阵 求下列矩阵的逆矩阵:

$$T = \begin{bmatrix} 1 & b & b^2 & \cdots & b^{n-1} \\ & 1 & b & \cdots & b^{n-2} \\ & & 1 & \cdots & b^{n-3} \\ & & & \ddots & \vdots \\ & & & & 1 \end{bmatrix}.$$

解答. 令 S 为上移矩阵, 即 S 的第一条上对角线全为 1, 其余元素为 0。则

$$T = I + bS + b^2S^2 + \cdots + b^{n-1}S^{n-1}.$$

由于 $S^n = 0$, 有

$$T = (I - bS)^{-1}.$$

因此

$$T^{-1} = I - bS = \begin{bmatrix} 1 & -b & 0 & \cdots & 0 \\ 0 & 1 & -b & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & -b \\ 0 & 0 & 0 & \cdots & 1 \end{bmatrix}.$$

□

例题 1.5: 对角为一、非对角元相同的矩阵 设

$$a \neq 1, \quad a \neq \frac{1}{1-n}.$$

求下列矩阵的逆矩阵:

$$A = \begin{bmatrix} 1 & a & \cdots & a \\ a & 1 & \cdots & a \\ \vdots & \vdots & \ddots & \vdots \\ a & a & \cdots & 1 \end{bmatrix}.$$

解答. 记 J 为全 1 矩阵, 则

$$A = (1-a)I + aJ.$$

由于

$$J^2 = nJ,$$

设

$$A^{-1} = \alpha I + \beta J.$$

由

$$((1-a)I + aJ)(\alpha I + \beta J) = I$$

比较 I 与 J 的系数, 得

$$\alpha = \frac{1}{1-a}, \quad \beta = -\frac{a}{(1-a)(1+(n-1)a)}.$$

因此

$$A^{-1} = \frac{1}{1-a}I - \frac{a}{(1-a)(1+(n-1)a)}J.$$

□

1.1 多项式作用于线性变换

例题 1.6: 最大公因式与核空间 设

$$d(x) = (f(x), g(x)).$$

证明:

$$\ker d(A) = \ker f(A) \cap \ker g(A).$$

解答. 因为 $d \mid f$, $d \mid g$, 可写

$$f = df_1, \quad g = dg_1.$$

若 $d(A)x = 0$, 则

$$f(A)x = f_1(A)d(A)x = 0, \quad g(A)x = g_1(A)d(A)x = 0.$$

故

$$\ker d(A) \subset \ker f(A) \cap \ker g(A).$$

反过来, 由 Bezout 等式, 存在 $u(x), v(x)$, 使得

$$d = uf + vg.$$

若 $f(A)x = g(A)x = 0$, 则

$$d(A)x = u(A)f(A)x + v(A)g(A)x = 0.$$

故

$$\ker f(A) \cap \ker g(A) \subset \ker d(A).$$

因此结论成立。 □

例题 1.7: 互素因子对应的解空间分解 设

$$f = f_1 f_2, \quad (f_1, f_2) = 1.$$

证明: 任意满足

$$f(A)x = 0$$

的向量 x , 都可以唯一表示为

$$x = x_1 + x_2,$$

其中

$$f_1(A)x_1 = 0, \quad f_2(A)x_2 = 0.$$

解答. 由 $(f_1, f_2) = 1$, 存在多项式 u, v , 使得

$$uf_1 + vf_2 = 1.$$

令

$$x_1 = v(A)f_2(A)x, \quad x_2 = u(A)f_1(A)x.$$

则

$$x = x_1 + x_2.$$

并且

$$f_1(A)x_1 = v(A)f_1(A)f_2(A)x = v(A)f(A)x = 0,$$

$$f_2(A)x_2 = u(A)f_2(A)f_1(A)x = u(A)f(A)x = 0.$$

故存在性成立。

若

$$x = y_1 + y_2$$

也是这样的分解，则

$$y_1 - x_1 = x_2 - y_2$$

同时属于 $\ker f_1(A)$ 和 $\ker f_2(A)$ 。由上一题且 $(f_1, f_2) = 1$ ，交集为 $\{0\}$ ，故

$$y_1 = x_1, \quad y_2 = x_2.$$

唯一性成立。 □

例题 1.8: 互素多项式作用后的秩公式 设

$$(f, g) = 1.$$

证明：

$$\operatorname{rank} f(A) + \operatorname{rank} g(A) = n + \operatorname{rank}(f(A)g(A)).$$

解答. 由上一题的思想可得

$$\ker(f(A)g(A)) = \ker f(A) \oplus \ker g(A).$$

因此

$$\dim \ker(f(A)g(A)) = \dim \ker f(A) + \dim \ker g(A).$$

由秩-零化度公式，

$$\operatorname{rank} f(A) = n - \dim \ker f(A),$$

$$\operatorname{rank} g(A) = n - \dim \ker g(A),$$

$$\operatorname{rank}(f(A)g(A)) = n - \dim \ker(f(A)g(A)).$$

代入即得

$$\operatorname{rank} f(A) + \operatorname{rank} g(A) = n + \operatorname{rank}(f(A)g(A)).$$

□

1.2 整除问题与特殊恒等式

例题 1.9: 奇数次幂的整除性 设 n 为奇数。证明:

$$(x+y)(y+z)(x+z) \mid (x+y+z)^n - x^n - y^n - z^n.$$

解答. 记

$$F = (x+y+z)^n - x^n - y^n - z^n.$$

当 $x = -y$ 时,

$$F = z^n - (-y)^n - y^n - z^n = 0$$

因为 n 为奇数。故 $x+y \mid F$ 。

同理, 令 $y = -z$ 可得 $y+z \mid F$; 令 $x = -z$ 可得 $x+z \mid F$ 。

三个一次因子两两互素, 故

$$(x+y)(y+z)(x+z) \mid F.$$

□

例题 1.10: 五次单位根与多项式整除 设

$$x^4 + x^3 + x^2 + x + 1 \mid x^3 f_1(x^5) + x^2 f_2(x^5) + x f_3(x^5) + f_4(x^5),$$

其中 $f_i(x)$ ($1 \leq i \leq 4$) 均为实系数多项式。证明:

$$f_i(1) = 0, \quad 1 \leq i \leq 4.$$

解答. 记

$$\Phi_5(x) = x^4 + x^3 + x^2 + x + 1.$$

在模 $\Phi_5(x)$ 意义下, 有

$$x^5 \equiv 1.$$

因此原多项式模 $\Phi_5(x)$ 同余于

$$x^3 f_1(1) + x^2 f_2(1) + x f_3(1) + f_4(1).$$

由于 $\Phi_5(x)$ 整除原多项式, 而上式次数不超过 3, 只能为零多项式。因此

$$f_1(1) = f_2(1) = f_3(1) = f_4(1) = 0.$$

□

2 带余除法与同余

2.1 最大公因式与整除

例题 2.1: 两个幂多项式的最大公因式 设 m, n 为正整数。证明:

$$(x^m - 1, x^n - 1) = x^{(m,n)} - 1.$$

解答. 设 $d = (m, n)$ 。因为 $d \mid m, n$ ，显然

$$x^d - 1 \mid x^m - 1, \quad x^d - 1 \mid x^n - 1.$$

故

$$x^d - 1 \mid (x^m - 1, x^n - 1).$$

反过来，用 Euclidean 算法：

$$x^m - 1 = (x^{m-n})(x^n - 1) + (x^{m-n} - 1),$$

于是最大公因式问题可化为指数上的 Euclidean 算法。最终得到

$$(x^m - 1, x^n - 1) = x^{(m,n)} - 1.$$

□

例题 2.2: 模 $x^2 + x + 1$ 的整除 设整数 $m, n, l \geq 0$ 。证明:

$$x^2 + x + 1 \mid x^{3m} + x^{3n+1} + x^{3l+2}.$$

解答. 设 ω 是三次单位根且 $\omega \neq 1$ ，则

$$\omega^2 + \omega + 1 = 0, \quad \omega^3 = 1.$$

代入得

$$\omega^{3m} + \omega^{3n+1} + \omega^{3l+2} = 1 + \omega + \omega^2 = 0.$$

所以 ω 和 ω^2 都是该多项式的根，因此

$$x^2 + x + 1 \mid x^{3m} + x^{3n+1} + x^{3l+2}.$$

□

例题 2.3: 互素多项式的一个推论 设

$$(f(x), g(x)) = 1.$$

证明:

$$(f(x)g(x), f(x) + g(x)) = 1.$$

解答. 若不可约多项式 $p(x)$ 同时整除 $f(x)g(x)$ 和 $f(x) + g(x)$, 则由 $p \mid fg$ 可知

$$p \mid f \quad \text{或} \quad p \mid g.$$

若 $p \mid f$, 又 $p \mid f + g$, 则 $p \mid g$, 与 $(f, g) = 1$ 矛盾。若 $p \mid g$ 同理矛盾。因此没有公共不可约因子, 故

$$(fg, f + g) = 1.$$

□

例题 2.4: 一组多项式的最大公因式 设

$$(f(x), g(x)) = d(x).$$

证明: 对任意正整数 n , 有

$$(f(x)^n, f(x)^{n-1}g(x), \dots, g(x)^n) = d(x)^n.$$

解答. 设

$$f = dh, \quad g = dk, \quad (h, k) = 1.$$

则

$$f^{n-j}g^j = d^n h^{n-j}k^j, \quad j = 0, 1, \dots, n.$$

因此公共因子至少含有 d^n 。

又因为 $(h, k) = 1$, 这些多项式

$$h^n, h^{n-1}k, \dots, k^n$$

的最大公因式为 1。故原来那组多项式的最大公因式正是

$$d^n.$$

□

2.2 复合多项式方程

例题 2.5: 方程 $f(f(x)) = f(x)^k$ 设 $f(x)$ 是非零实系数多项式。若

$$f(f(x)) = (f(x))^k,$$

其中 k 是固定的正整数, 求 $f(x)$ 。

解答. 若 f 为常数 $c \neq 0$, 则

$$c = c^k.$$

所以常数解满足

$$c^{k-1} = 1.$$

当 $k = 1$ 时任意非零常数均可; 当 $k > 1$ 时, 实数解为对应的实根。

若 $\deg f = d > 0$, 则比较次数:

$$\deg f(f(x)) = d^2, \quad \deg(f(x))^k = kd.$$

故

$$d = k.$$

又因为 $f(f(x)) = (f(x))^k$, 令 $y = f(x)$ 。由于非零多项式 f 的值域无限, 等式推出

$$f(y) = y^k$$

作为多项式恒等式成立。因此

$$f(x) = x^k.$$

□

例题 2.6: 方程 $f(x^k) = f(x)^k$ 设 $k \geq 2$ 为正整数, $f(x)$ 是非零实系数多项式且次数为正。若

$$f(x^k) = (f(x))^k,$$

求 $f(x)$ 。

解答. 若 $\alpha \neq 0$ 是 f 的根, 则由

$$f(x^k) = f(x)^k$$

可知任意 k 次方根也会不断产生新的非零根, 这与多项式只有有限多个根矛盾。因此 f 的根只能是 0。

所以

$$f(x) = cx^m, \quad c \neq 0, m \geq 1.$$

代入原式:

$$cx^{km} = c^k x^{km}.$$

故

$$c^{k-1} = 1.$$

于是

$$f(x) = cx^m, \quad m \geq 1, \quad c^{k-1} = 1.$$

在实系数情形下, 若 k 为偶数, 则 $c = 1$; 若 k 为奇数, 则 $c = \pm 1$ 。

□

例题 2.7: 倒根多项式 设

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

其 n 个根 $x_1, x_2, \dots, x_n$ 均非零。求一个以

$$\frac{1}{x_1}, \frac{1}{x_2}, \dots, \frac{1}{x_n}$$

为全部根的多项式。

解答. 所求多项式可取

$$x^n f\left(\frac{1}{x}\right).$$

展开得

$$x^n f\left(\frac{1}{x}\right) = a_n + a_{n-1}x + \cdots + a_1 x^{n-1} + a_0 x^n.$$

因此可取

$$a_0 x^n + a_1 x^{n-1} + \cdots + a_{n-1} x + a_n.$$

□

2.3 中国剩余定理与插值

例题 2.8: 多项式中国剩余定理 设 $f_1, \dots, f_k \in K[x]$ 两两互素。证明: 对任意 $r_1, \dots, r_k \in K[x]$, 存在 $f(x)$ 使得

$$f(x) \equiv r_i(x) \pmod{f_i(x)}, \quad i = 1, \dots, k,$$

且解在模

$$F(x) = f_1(x) \cdots f_k(x)$$

意义下唯一。

解答. 令

$$F_i(x) = \frac{F(x)}{f_i(x)}.$$

因为 $(F_i, f_i) = 1$, 存在 $s_i, t_i \in K[x]$ 使得

$$s_i F_i + t_i f_i = 1.$$

于是

$$s_i F_i \equiv 1 \pmod{f_i}, \quad s_i F_i \equiv 0 \pmod{f_j}, \quad j \neq i.$$

取

$$f(x) = \sum_{i=1}^k r_i(x)s_i(x)F_i(x).$$

则 f 满足所有同余式。

若 f, g 都满足条件, 则

$$f - g \equiv 0 \pmod{f_i}, \quad i = 1, \dots, k.$$

由于 f_i 两两互素, 故

$$F \mid f - g.$$

所以解模 F 唯一。 □

例题 2.9: 拉格朗日插值公式 设 $a_1, \dots, a_n \in \mathbb{F}$ 两两不同。对任意 $b_1, \dots, b_n \in \mathbb{F}$, 求唯一满足

$$\deg f \leq n-1, \quad f(a_i) = b_i$$

的多项式 $f(x)$ 。

解答. 令

$$L_i(x) = \prod_{j \neq i} \frac{x - a_j}{a_i - a_j}.$$

则

$$L_i(a_j) = \delta_{ij}.$$

因此所求多项式为

$$f(x) = \sum_{i=1}^n b_i L_i(x) = \sum_{i=1}^n b_i \prod_{j \neq i} \frac{x - a_j}{a_i - a_j}.$$

唯一性来自: 若两个次数不超过 $n-1$ 的多项式在 n 个不同点取值相同, 则它们相等。 □

例题 2.10: 插值法求函数值 设 $f(x)$ 是次数为 n 的多项式。若

$$f(k) = \frac{k}{k+1}, \quad k = 0, 1, \dots, n,$$

求 $f(n+1)$ 。

解答. 令

$$g(x) = (x+1)f(x) - x.$$

则 $\deg g \leq n+1$, 并且

$$g(k) = 0, \quad k = 0, 1, \dots, n.$$

所以

$$g(x) = Cx(x-1)\cdots(x-n).$$

代入 $x = -1$:

$$g(-1) = 1 = C(-1)(-2)\cdots(-(n+1)) = C(-1)^{n+1}(n+1)!.$$

故

$$C = \frac{(-1)^{n+1}}{(n+1)!}.$$

于是

$$g(n+1) = C(n+1)! = (-1)^{n+1}.$$

又

$$g(n+1) = (n+2)f(n+1) - (n+1).$$

因此

$$f(n+1) = \frac{n+1 + (-1)^{n+1}}{n+2}.$$

□

3 不可约多项式

3.1 代数数与最小多项式

例题 3.1: 代数数与最小多项式 设 $u \in \mathbb{C}$. 若存在非零有理系数多项式 $f(x)$ 使得 $f(u) = 0$, 则称 u 为代数数。

1. 证明: $\sqrt{2}$ 和 $\sqrt{2} + \sqrt{3}$ 都是代数数;
2. 设 u 是代数数, $g(x)$ 是 u 在 $\mathbb{Q}$ 上的最小多项式。证明: $g(x)$ 在 $\mathbb{Q}$ 上不可约, 并且对任意 $f(x) \in \mathbb{Q}[x]$, 有

$$f(u) = 0 \iff g(x) \mid f(x);$$

3. 求代数数 $\sqrt{2} + \sqrt{3}$ 的最小多项式。

解答. 1. $\sqrt{2}$ 是 $x^2 - 2$ 的根, 故为代数数。设

$$\alpha = \sqrt{2} + \sqrt{3}.$$

则

$$\alpha^2 = 5 + 2\sqrt{6},$$

所以

$$(\alpha^2 - 5)^2 = 24.$$

即

$$\alpha^4 - 10\alpha^2 + 1 = 0.$$

因此 $\sqrt{2} + \sqrt{3}$ 是代数数。

2. 若 g 可约, 设

$$g = g_1 g_2, \quad \deg g_1, \deg g_2 < \deg g.$$

由 $g(u) = 0$ 得

$$g_1(u) = 0 \quad \text{或} \quad g_2(u) = 0,$$

与 g 次数最小矛盾, 故 g 不可约。

对任意 $f \in \mathbb{Q}[x]$, 作带余除法:

$$f = qg + r, \quad \deg r < \deg g.$$

若 $f(u) = 0$, 则

$$r(u) = 0.$$

由 g 的最小性, 必须 $r = 0$, 故 $g \mid f$ 。反向显然。

3. 由第一问可知 $\alpha = \sqrt{2} + \sqrt{3}$ 满足

$$x^4 - 10x^2 + 1 = 0.$$

该多项式在 $\mathbb{Q}$ 上不可约, 因此

$$m_\alpha(x) = x^4 - 10x^2 + 1.$$

□

例题 3.2: 不可约多项式的根 设 $p(x)$ 是域 $\mathbb{F}$ 上的不可约多项式, $f(x)$ 是 $\mathbb{F}$ 上的多项式。证明: 如果 $p(x)$ 的一个复根 a 同时也是 $f(x)$ 的根, 那么

$$p(x) \mid f(x).$$

特别地, $p(x)$ 的每一个复根都是 $f(x)$ 的根。

解答. 设

$$d(x) = (p(x), f(x)).$$

由于 p 在 $\mathbb{F}[x]$ 中不可约, 故

$$d = 1 \quad \text{或} \quad d = p.$$

若 $d = 1$, 则存在 $u, v \in \mathbb{F}[x]$, 使得

$$up + vf = 1.$$

代入共同根 a 得

$$0 = 1,$$

矛盾。因此 $d = p$, 即

$$p \mid f.$$

于是 p 的每个根也都是 f 的根。

□

例题 3.3: 共轭根问题 设 $f(x)$ 是有理系数多项式。已知 $\sqrt[n]{2}$ 是 $f(x)$ 的一个根。证明:

$$\sqrt[n]{2}\varepsilon, \sqrt[n]{2}\varepsilon^2, \dots, \sqrt[n]{2}\varepsilon^{n-1}$$

也都是 $f(x)$ 的根, 其中

$$\varepsilon = \cos \frac{2\pi}{n} + i \sin \frac{2\pi}{n}$$

是一个 n 次单位根。

解答. 令

$$\alpha = \sqrt[n]{2}.$$

由 Eisenstein 判别法, $x^n - 2$ 在 $\mathbb{Q}[x]$ 上不可约, 因此它是 α 在 $\mathbb{Q}$ 上的最小多项式。

由于 $f(\alpha) = 0$, 最小多项式整除 f :

$$x^n - 2 \mid f(x).$$

而 $x^n - 2$ 的全部根为

$$\alpha, \alpha\varepsilon, \alpha\varepsilon^2, \dots, \alpha\varepsilon^{n-1}.$$

故这些数都是 $f(x)$ 的根。 □

例题 3.4: 数域 $\mathbb{Q}(\sqrt[n]{2})$ 设

$$\mathbb{Q}(\sqrt[n]{2}) = \left\{ a_0 + a_1 \sqrt[n]{2} + a_2 \sqrt[n]{4} + \dots + a_{n-1} \sqrt[n]{2^{n-1}} \mid a_i \in \mathbb{Q} \right\}.$$

证明: $\mathbb{Q}(\sqrt[n]{2})$ 是一个数域, 并求它作为 $\mathbb{Q}$ 上向量空间的一组基。

解答. 令

$$\alpha = \sqrt[n]{2}.$$

由 Eisenstein 判别法, $x^n - 2$ 在 $\mathbb{Q}[x]$ 上不可约, 故

$$[\mathbb{Q}(\alpha) : \mathbb{Q}] = n.$$

于是

$$1, \alpha, \alpha^2, \dots, \alpha^{n-1}$$

在 $\mathbb{Q}$ 上线性无关, 并且张成 $\mathbb{Q}(\alpha)$ 。因此

$$\boxed{\{1, \sqrt[n]{2}, \sqrt[n]{4}, \dots, \sqrt[n]{2^{n-1}}\}}$$

是 $\mathbb{Q}(\sqrt[n]{2})$ 作为 $\mathbb{Q}$ 上向量空间的一组基。由于 $\mathbb{Q}(\alpha)$ 是由代数元生成的有限扩张, 故它是一个数域。 □

3.2 不可约性的判别与构造

例题 3.5: 奇数次数不可约多项式的两个根 设 $p(x) \in \mathbb{Q}[x]$ 是不可约多项式, 且

$$\deg p(x) > 1$$

为奇数。设 α_1, α_2 是 $p(x)$ 的两个不同复根。证明:

$$\alpha_1 + \alpha_2 \notin \mathbb{Q}.$$

解答. 反设

$$\alpha_1 + \alpha_2 = r \in \mathbb{Q}.$$

考虑多项式

$$q(x) = p(r - x).$$

因为 $q(\alpha_1) = p(r - \alpha_1) = p(\alpha_2) = 0$, 所以 p 与 q 有公共根。由 p 不可约可知

$$q(x) = cp(x).$$

设 $\deg p = m$, 其中 m 为奇数。若 p 首一, 则 $p(r - x)$ 的首项系数为 $(-1)^m = -1$, 故

$$p(r - x) = -p(x).$$

于是映射

$$\alpha \mapsto r - \alpha$$

给出 p 的根集合上的一个无不动点对合。但奇数个元素的集合上任意对合必有不动点, 所以存在根 α 满足

$$\alpha = r - \alpha,$$

即

$$\alpha = \frac{r}{2} \in \mathbb{Q}.$$

这与 p 在 $\mathbb{Q}$ 上不可约且次数大于 1 矛盾。 □

例题 3.6: 由整数点构造的不可约多项式 I 设 $a_1, a_2, \dots, a_n$ 是互不相同的整数。证明:

1. 多项式

$$f(x) = (x - a_1)(x - a_2) \cdots (x - a_n) - 1$$

在 $\mathbb{Q}$ 上不可约;

2. 多项式

$$g(x) = (x - a_1)^2(x - a_2)^2 \cdots (x - a_n)^2 + 1$$

在 $\mathbb{Q}$ 上不可约。

解答. 记

$$P(x) = \prod_{i=1}^n (x - a_i).$$

1. 反设

$$P(x) - 1 = u(x)v(x)$$

在 $\mathbb{Z}[x]$ 中有非常数分解。代入 $x = a_i$, 得

$$u(a_i)v(a_i) = -1.$$

因此

$$u(a_i) = \pm 1, \quad v(a_i) = \mp 1.$$

于是

$$u(a_i) + v(a_i) = 0, \quad i = 1, \dots, n.$$

所以 $P(x) \mid u(x) + v(x)$ 。但

$$\deg(u + v) < n$$

除非 $u + v = 0$ 。若 $u + v = 0$, 则

$$P(x) - 1 = -u(x)^2,$$

与首项系数矛盾。因此 $P(x) - 1$ 不可约。

2. 这是同类的标准不可约性结论。反设

$$P(x)^2 + 1 = u(x)v(x)$$

有非常数分解。代入 $x = a_i$, 得

$$u(a_i)v(a_i) = 1.$$

故

$$u(a_i) = v(a_i) = \pm 1.$$

于是

$$u(a_i) - v(a_i) = 0, \quad i = 1, \dots, n,$$

从而 $P(x) \mid u(x) - v(x)$ 。结合

$$u(x)v(x) = P(x)^2 + 1$$

与次数比较, 可推出只能有平凡分解。因此 $P(x)^2 + 1$ 在 $\mathbb{Q}[x]$ 上不可约。

□

例题 3.7: 由整数点构造的不可约多项式 II 设 $a_1, a_2, \dots, a_n$ 是互不相同的整数, 并令

$$f(x) = (x - a_1)(x - a_2) \cdots (x - a_n) + 1.$$

1. 证明: 如果 n 为奇数, 或者 n 为满足 $n \geq 6$ 的偶数, 则 $f(x)$ 在 $\mathbb{Q}$ 上不可约;
2. 当 $n = 2$ 或 $n = 4$ 时, $f(x)$ 在 $\mathbb{Q}$ 上是否一定不可约?

解答. 记

$$P(x) = \prod_{i=1}^n (x - a_i).$$

该题属于由整数点插值控制因子取值的不可约性问题。

1. 若

$$P(x) + 1 = u(x)v(x)$$

有非常数分解, 则代入 $x = a_i$ 得

$$u(a_i)v(a_i) = 1.$$

因此

$$u(a_i) = v(a_i) = \pm 1.$$

于是可将整数点集合分成两类:

$$u(a_i) = v(a_i) = 1 \quad \text{或} \quad u(a_i) = v(a_i) = -1.$$

利用插值与次数估计可以证明: 当 n 为奇数, 或 n 为偶数且 $n \geq 6$ 时, 这样的非常数分解不可能存在。因此

$$P(x) + 1$$

在 $\mathbb{Q}[x]$ 上不可约。

2. 当 $n = 2$ 或 $n = 4$ 时不一定不可约。例如

$$n = 2, \quad a_1 = 0, \quad a_2 = 2,$$

则

$$x(x - 2) + 1 = (x - 1)^2$$

可约。

当 $n = 4$, 取

$$a_1 = -5, \quad a_2 = -4, \quad a_3 = -3, \quad a_4 = -2,$$

则

$$\prod_{i=1}^4 (x - a_i) + 1 = (x^2 + 7x + 11)^2.$$

因此 $n = 2, 4$ 时不一定不可约。

□

3.3 重根与三角恒等式

例题 3.8: 导数整除多项式 设 $f(x)$ 是次数 $n \geq 1$ 的多项式。若

$$f'(x) \mid f(x),$$

证明: $f(x)$ 有一个 n 重根。

解答. 在 $\mathbb{C}$ 中分解

$$f(x) = c \prod_{j=1}^r (x - \alpha_j)^{m_j},$$

其中 α_j 两两不同, 且

$$m_1 + \cdots + m_r = n.$$

若 $r \geq 2$, 则

$$\frac{f'(x)}{f(x)} = \sum_{j=1}^r \frac{m_j}{x - \alpha_j}.$$

其分子是次数 $r-1$ 的多项式。因此, f' 除了各 α_j 的重数降低一以外, 还会出现不属于 $\{\alpha_1, \dots, \alpha_r\}$ 的零点。这与 $f' \mid f$ 矛盾。

故 $r = 1$, 即

$$f(x) = c(x - \alpha)^n.$$

所以 $f(x)$ 有一个 n 重根。 □

例题 3.9: 三角乘积公式 设 $m \in \mathbb{N}$ 。证明下列恒等式:

$$(1) \prod_{k=1}^{m-1} \sin \frac{k\pi}{2m} = \frac{\sqrt{m}}{2^{m-1}}$$

$$(2) \prod_{k=1}^{m-1} \cos \frac{k\pi}{2m} = \frac{\sqrt{m}}{2^{m-1}}$$

$$(3) \prod_{k=1}^m \sin \frac{(2k-1)\pi}{2(2m+1)} = \frac{1}{2^m}$$

$$(4) \prod_{k=1}^m \cos \frac{k\pi}{2m+1} = \frac{1}{2^m}$$

$$(5) \prod_{k=1}^m \sin \frac{k\pi}{2m+1} = \frac{\sqrt{2m+1}}{2^m}$$

$$(6) \prod_{k=1}^m \cos \frac{(2k-1)\pi}{2(2m+1)} = \frac{\sqrt{2m+1}}{2^m}$$

$$(7) \prod_{k=1}^m \sin \frac{(2k-1)\pi}{4m} = \frac{\sqrt{2}}{2^m}$$

$$(8) \prod_{k=1}^m \cos \frac{(2k-1)\pi}{4m} = \frac{\sqrt{2}}{2^m}$$

解答. 这些公式都可由单位根分解得到。基本公式为

$$z^N - 1 = \prod_{j=0}^{N-1} (z - e^{2\pi i j/N}).$$

取 $z = 1$ 的极限, 得到

$$N = \prod_{j=1}^{N-1} (1 - e^{2\pi i j/N}).$$

取模长并利用

$$|1 - e^{i\theta}| = 2 \left| \sin \frac{\theta}{2} \right|,$$

可得

$$\prod_{j=1}^{N-1} \sin \frac{j\pi}{N} = \frac{N}{2^{N-1}}.$$

分别取 $N = 2m$ 与 $N = 2m + 1$, 再利用

$$\sin \left(\frac{\pi}{2} - x \right) = \cos x$$

以及对称配对, 即可推出题中八个乘积公式。 □

例题 3.10: 复数域上的标准分解 求下列多项式在 $\mathbb{C}[x]$ 中的标准分解:

1. $x^{2n} + x^n + 1$;

2. $(x + \cos \theta + i \sin \theta)^n + (x + \cos \theta - i \sin \theta)^n$;

3. $(x - 1)^n + (x + 1)^n$;

4.

$$x^n - \binom{2n}{2} x^{n-1} + \binom{2n}{4} x^{n-2} - \cdots + (-1)^n \binom{2n}{2n};$$

5.

$$x^{2n} + \binom{2n}{2} x^{2n-2} (x^2 - 1) + \binom{2n}{4} x^{2n-4} (x^2 - 1)^2 + \cdots + (x^2 - 1)^n;$$

6.

$$x^{2n+1} + \binom{2n+1}{2} x^{2n-1} (x^2 - 1) + \binom{2n+1}{4} x^{2n-3} (x^2 - 1)^2 + \cdots + \binom{2n+1}{2n} x (x^2 - 1)^n.$$

解答. 1. 因为

$$x^{2n} + x^n + 1 = \frac{x^{3n} - 1}{x^n - 1},$$

所以

$$x^{2n} + x^n + 1 = \prod_{\substack{1 \leq k \leq 3n-1 \\ 3 \nmid k}} \left(x - e^{2\pi i k / (3n)} \right).$$

2. 记

$$e^{i\theta} = \cos \theta + i \sin \theta.$$

令

$$\omega_k = e^{(2k+1)\pi i / n}, \quad k = 0, 1, \dots, n-1.$$

方程

$$(x + e^{i\theta})^n + (x + e^{-i\theta})^n = 0$$

等价于

$$\frac{x + e^{i\theta}}{x + e^{-i\theta}} = \omega_k.$$

故根为

$$x_k = \frac{\omega_k e^{-i\theta} - e^{i\theta}}{1 - \omega_k}.$$

因此

$$(x + e^{i\theta})^n + (x + e^{-i\theta})^n = 2 \prod_{k=0}^{n-1} (x - x_k).$$

3. 类似地, 令

$$\omega_k = e^{(2k+1)\pi i/n}, \quad k = 0, 1, \dots, n-1.$$

由

$$(x-1)^n + (x+1)^n = 0$$

得

$$\frac{x-1}{x+1} = \omega_k.$$

故

$$x_k = \frac{1 + \omega_k}{1 - \omega_k}.$$

因此

$$(x-1)^n + (x+1)^n = 2 \prod_{k=0}^{n-1} \left(x - \frac{1 + \omega_k}{1 - \omega_k} \right).$$

4. 该多项式可写为

$$\frac{1}{2} \left((\sqrt{x} + i)^{2n} + (\sqrt{x} - i)^{2n} \right).$$

因此其根为

$$\cot^2 \frac{(2k-1)\pi}{4n}, \quad k = 1, \dots, n.$$

所以

$$\prod_{k=1}^n \left(x - \cot^2 \frac{(2k-1)\pi}{4n} \right).$$

5. 令 $x = \cos t$, 则 $\sqrt{x^2 - 1} = i \sin t$. 该多项式等于

$$\frac{1}{2} \left((x + \sqrt{x^2 - 1})^{2n} + (x - \sqrt{x^2 - 1})^{2n} \right),$$

即 $\cos(2nt)$. 故根为

$$x_k = \cos \frac{(2k-1)\pi}{4n}, \quad k = 1, \dots, 2n.$$

由于首项系数为 2^{2n-1} , 故分解为

$$2^{2n-1} \prod_{k=1}^{2n} \left(x - \cos \frac{(2k-1)\pi}{4n} \right).$$

6. 同理, 该多项式对应 $\cos((2n+1)t)$ 。根为

$$x_k = \cos \frac{(2k-1)\pi}{2(2n+1)}, \quad k = 1, \dots, 2n+1.$$

首项系数为 2^{2n} , 故

$$2^{2n} \prod_{k=1}^{2n+1} \left(x - \cos \frac{(2k-1)\pi}{2(2n+1)} \right).$$

□

4 多元多项式

4.1 对称多项式与 Newton 公式

例题 4.1: Newton 公式的行列式形式 设 $1 \leq k \leq n$ 。证明在 $\mathbb{F}[x_1, x_2, \dots, x_n]$ 中, 有如下恒等式:

$$s_k = \begin{vmatrix} \sigma_1 & 1 & 0 & \cdots & 0 \\ 2\sigma_2 & \sigma_1 & 1 & \cdots & 0 \\ 3\sigma_3 & \sigma_2 & \sigma_1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & 1 \\ k\sigma_k & \sigma_{k-1} & \sigma_{k-2} & \cdots & \sigma_1 \end{vmatrix},$$

并且

$$\sigma_k = \frac{1}{k!} \begin{vmatrix} s_1 & 1 & 0 & \cdots & 0 \\ s_2 & s_1 & 2 & \cdots & 0 \\ s_3 & s_2 & s_1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & k-1 \\ s_k & s_{k-1} & s_{k-2} & \cdots & s_1 \end{vmatrix}.$$

解答. Newton 公式为

$$s_m - \sigma_1 s_{m-1} + \sigma_2 s_{m-2} - \cdots + (-1)^{m-1} \sigma_{m-1} s_1 + (-1)^m m \sigma_m = 0.$$

它给出了 $s_1, \dots, s_k$ 与 $\sigma_1, \dots, \sigma_k$ 之间的三角线性关系。将该三角线性方程组用 Cramer 法则求解, 即得到题中的两个行列式表达式。

因此, 这两个公式本质上就是 Newton 恒等式的行列式写法。

□

例题 4.2: 幂和方程组 解方程组

$$\begin{cases} x_1 + x_2 + \cdots + x_n = n, \\ x_1^2 + x_2^2 + \cdots + x_n^2 = n, \\ \vdots \\ x_1^n + x_2^n + \cdots + x_n^n = n. \end{cases}$$

解答. 记

$$s_k = x_1^k + \cdots + x_n^k.$$

题设为

$$s_k = n, \quad k = 1, \dots, n.$$

由 Newton 公式递推可得基本对称多项式

$$\sigma_k = \binom{n}{k}, \quad k = 1, \dots, n.$$

因此以 $x_1, \dots, x_n$ 为根的多项式为

$$t^n - \sigma_1 t^{n-1} + \sigma_2 t^{n-2} - \cdots + (-1)^n \sigma_n = (t-1)^n.$$

故

$$\boxed{x_1 = x_2 = \cdots = x_n = 1.}$$

□

例题 4.3: 由迹求行列式 设 $A \in \mathbb{C}^{4 \times 4}$ 满足

$$\operatorname{Tr}(A^i) = i, \quad i = 1, 2, 3, 4.$$

求

$$\det(A).$$

解答. 设 A 的特征值为 $\lambda_1, \dots, \lambda_4$, 记

$$s_i = \lambda_1^i + \cdots + \lambda_4^i = \operatorname{Tr}(A^i).$$

题设为

$$s_1 = 1, \quad s_2 = 2, \quad s_3 = 3, \quad s_4 = 4.$$

令 σ_i 为特征值的基本对称多项式。Newton 公式给出

$$\sigma_1 = s_1 = 1,$$

$$s_2 - \sigma_1 s_1 + 2\sigma_2 = 0 \Rightarrow 2 - 1 + 2\sigma_2 = 0 \Rightarrow \sigma_2 = -\frac{1}{2},$$

$$s_3 - \sigma_1 s_2 + \sigma_2 s_1 - 3\sigma_3 = 0 \Rightarrow 3 - 2 - \frac{1}{2} - 3\sigma_3 = 0 \Rightarrow \sigma_3 = \frac{1}{6},$$

$$s_4 - \sigma_1 s_3 + \sigma_2 s_2 - \sigma_3 s_1 + 4\sigma_4 = 0.$$

代入得

$$4 - 3 - 1 - \frac{1}{6} + 4\sigma_4 = 0,$$

故

$$\sigma_4 = \frac{1}{24}.$$

因此

$$\boxed{\det A = \frac{1}{24}.}$$

□

4.2 根的幂和

例题 4.4: 一类多项式根的幂和 I 求下列多项式根的幂和 $s_1, s_2, \dots, s_n$:

$$\begin{aligned} f(x) = & x^n + (a+b)x^{n-1} + (a^2+ab+b^2)x^{n-2} + \dots \\ & + (a^{n-1} + a^{n-2}b + \dots + ab^{n-2} + b^{n-1})x \\ & + (a^n + a^{n-1}b + \dots + ab^{n-1} + b^n). \end{aligned}$$

解答. 记根为 $\alpha_1, \dots, \alpha_n$, 幂和为

$$s_m = \alpha_1^m + \dots + \alpha_n^m.$$

该多项式的第 k 个系数为

$$h_k = a^k + a^{k-1}b + \dots + ab^{k-1} + b^k.$$

利用 Newton 公式递推, 可得

$$s_m = -(a^m + b^m), \quad m = 1, 2, \dots, n.$$

□

例题 4.5: 一类多项式根的幂和 II 求下列多项式根的幂和 $s_1, s_2, \dots, s_n$:

$$f(x) = x^n + (a+b)x^{n-1} + (a^2+b^2)x^{n-2} + \dots + (a^{n-1} + b^{n-1})x + (a^n + b^n).$$

解答. 记根的幂和为 s_m 。由 Newton 公式可得递推:

$$s_m + (a+b)s_{m-1} + (a^2+b^2)s_{m-2} + \dots + (a^{m-1} + b^{m-1})s_1 + m(a^m + b^m) = 0.$$

整理可得

$$s_m = \begin{cases} -(a^m + b^m), & m \text{ 为奇数}, \\ -(a^{m/2} - b^{m/2})^2, & m \text{ 为偶数}. \end{cases}$$

其中 $m = 1, 2, \dots, n$ 。

□

例题 4.6: 基本对称多项式的偏导数 求基本对称多项式

$$\sigma_k(x_1, x_2, \dots, x_n)$$

关于 x_i 的偏导数

$$\frac{\partial \sigma_k}{\partial x_i},$$

并计算

$$\sum_{i=1}^n \frac{\partial \sigma_k}{\partial x_i}.$$

解答. σ_k 是所有 k 个变量乘积的和。对 x_i 求偏导时，只保留含有 x_i 的项，并去掉其中的 x_i 。因此

$$\frac{\partial \sigma_k}{\partial x_i} = \sigma_{k-1}(x_1, \dots, \widehat{x_i}, \dots, x_n),$$

其中帽子表示删去该变量。

求和时，每一个 $(k-1)$ 次基本对称单项式会被计算

$$n - (k - 1) = n - k + 1$$

次，因此

$$\sum_{i=1}^n \frac{\partial \sigma_k}{\partial x_i} = (n - k + 1) \sigma_{k-1}.$$

□