第五章　多项式和复数域

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. □

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

$$f=\alpha_1M_1+\cdots+\alpha_kM_k, \tag{1}$$

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, 我们可进一步假设上式中 $M_1,\dots,M_k$ 两两不同.

引理 2.5 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(见定理 2.1 (i)). 设 $n>1$ 且结论在 $n-1$ 时成立. 设

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

如果 $d=0$, 则 x_n 在 $M_1,\dots,M_k$ 中都不出现. 由归纳假设 $\alpha_1=\cdots=\alpha_k=0$.

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 $\deg_{x_n}(M_i)=\deg_{x_n}(M_{i+1})=\cdots=\deg_{x_n}(M_k)=d$. 则 $M_i=N_ix_n^d,\dots,M_k=N_kx_n^d$, 其中 $N_i,\dots,N_k\in X_{n-1}$. 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, $Q=0$. 根据归纳假设, $\alpha_i=\cdots=\alpha_k=0$, 矛盾. □

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

$$p = \alpha_1 M_1 + \cdots + \alpha_k M_k. \tag{2}$$

(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 $\beta_1, \ldots, \beta_\ell \in R \setminus \{0\}$ 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 $\alpha_1 = \beta_1, \ldots, \alpha_k = \beta_k$. □

定义 2.7 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 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 2.12 (i) 可知, $\deg(p+q) \leq d$.

(ii) 由引理 2.12 (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 $M = x_1^{i_1} \cdots x_n^{i_n}$.

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

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.

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

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

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

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

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

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 $\phi_{s_1,\ldots,s_n}$. □

3 复数

3.1 复数域

设

$$\mathbb{C} := \{x + y\sqrt{-1} \,|\, x, y \in \mathbb{R}\}.$$

设 $z = x + y\sqrt{-1}$, 其中 $x, y \in \mathbb{R}$. 则 x 称为 z 的实部, 记为 $\mathrm{Re}(z)$; y 称为 z 的虚部, 记为 $\mathrm{Im}(z)$. 注意到 $\mathbb{R} \subset \mathbb{C}$.

定义

$$\begin{array}{rccc} +: & \mathbb{C}\times\mathbb{C} & \longrightarrow & \mathbb{C} \\ & (x_1+y_1\sqrt{-1}, x_2+y_2\sqrt{-1}) & \mapsto & (x_1+x_2)+(y_1+y_2)\sqrt{-1}. \end{array}$$

可直接验证 $(\mathbb{C}, +, 0)$ 是交换群. 定义

$$\begin{array}{rccc} \cdot: & \mathbb{C}\times\mathbb{C} & \longrightarrow & \mathbb{C} \\ & (x_1+y_1\sqrt{-1}, x_2+y_2\sqrt{-1}) & \mapsto & (x_1x_2-y_1y_2)+(x_1y_2+y_1x_2)\sqrt{-1}. \end{array}$$

可直接验证 $(\mathbb{C}, \cdot, 1)$ 是交换含幺半群.

可直接验证分配律成立. 于是, $(\mathbb{C}, +, 0, \cdot, 1)$ 是交换环.

设 $z = x + y\sqrt{-1}$, 其中 $x, y \in \mathbb{R}$. 则 $\bar{z} = x - y\sqrt{-1}$ 称为 z 的共轭. 注意到

$$z\bar{z} = x^2 + y^2 \in \mathbb{R}.$$

当 $z \neq 0$ 时,

$$z\frac{\bar{z}}{x^2+y^2} = 1.$$

故 $(\mathbb{C}, +, 0, \cdot, 1)$ 是域, 称之为复数域. 它的元素称为复数.

例 3.1 设

$$F = \left\{ \begin{pmatrix} x & y \\ -y & x \end{pmatrix} \mid x, y \in \mathbb{R} \right\}.$$

则 F 是 $\mathrm{M}_2(\mathbb{R})$ 的交换子环, $(F, +, O, \cdot, E)$ 是域. 下面我们验证 F 和 $\mathbb{C}$ 是同构的.

定义

$$\begin{array}{rccc} \phi: & F & \longrightarrow & \mathbb{C} \\ & \begin{pmatrix} x & y \\ -y & x \end{pmatrix} & \mapsto & x+y\sqrt{-1}. \end{array}$$

可直接验证对任意 $A, B \in F$, $\phi(A+B)=\phi(A)+\phi(B)$. 设

$$A=\begin{pmatrix} x & y \\ -y & x \end{pmatrix} \quad \text{和} \quad B=\begin{pmatrix} u & v \\ -v & u \end{pmatrix}.$$

则

$$\begin{aligned} \phi(AB) &= \phi\left(\begin{pmatrix} xu-yv & xv+yu \\ -xv-yu & xu-yv \end{pmatrix}\right) \\ &= (xu-yv)+(xv+yu)\sqrt{-1} \\ &= (x+y\sqrt{-1})(u+v\sqrt{-1}) \\ &= \phi(A)\phi(B). \end{aligned}$$

进而, $\phi(E)=1$. 故 ϕ 是环同态. 显然 ϕ 是满射. 再根据命题第四章第三讲命题 *4.4*, ϕ 是同构.

注意到

$$\phi\left(\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}\right)=\sqrt{-1}.$$

因为

$$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}^2=-E,$$

所以 $\sqrt{-1}^2 = -1$ 是合理的.

记 $\sqrt{-1}$ 为 $\mathbf{i}$, 称为虚单位.

命题 3.2 共轭映射 $z \mapsto \bar{z}$ 是从 $\mathbb{C}$ 到 $\mathbb{C}$ 的同构且 $^{-}|_{\mathbb{R}} = \mathrm{id}_{\mathbb{R}}$.

证明. 设 $z = x + y\mathbf{i}$, $x, y \in \mathbb{R}$. 则 $\bar{z} = x - y\mathbf{i}$. 于是, 当 $y = 0$ 时, $\bar{z} = z$. 故 $^{-}|_{\mathbb{R}} = \mathrm{id}_{\mathbb{R}}$. 进而,

$$\bar{\bar{z}} = \overline{x - y\mathbf{i}} = x + y\mathbf{i} = z.$$

故共轭映射的逆是它自身, 从而是双射. 下面只需证明共轭映射是同态. 再设 $z' = x' + y'\mathbf{i}$, 其中 $x', y' \in \mathbb{R}$. 则

$$\begin{aligned}\overline{z + z'} &= \overline{(x + x') + (y + y')\mathbf{i}} = (x + x') - (y + y')\mathbf{i} \\ &= (x - y\mathbf{i}) + (x' - y'\mathbf{i}) = \bar{z} + \bar{z'}. \quad \square\end{aligned}$$

3.2 复数的极表示

设 $z = x + y\mathbf{i}$, 其中 $x, y \in \mathbb{R}$ 不全为零. 则

$$z = \sqrt{x^2 + y^2}\left(\frac{x}{\sqrt{x^2 + y^2}} + \frac{y}{\sqrt{x^2 + y^2}}\mathbf{i}\right).$$

则存在唯一的 $\theta \in [0, 2\pi)$ 使得,

$$\cos\theta = \frac{x}{\sqrt{x^2 + y^2}} \quad \text{和} \quad \sin\theta = \frac{y}{\sqrt{x^2 + y^2}}.$$

称 $\sqrt{x^2+y^2}$ 为 z 的模长, 记为 $|z|$. 称 θ 为 z 的幅角, 记为 $\arg z$. 再设 0 的模长为零, 幅角任意. 则对任意 $z \in \mathbb{C}$,

$$z = |z|(\cos(\theta) + \sin(\theta)\mathbf{i}).$$

称之为 z 的极化公式.

引理 3.3 设复数

$$z_1 = |z_1|(\cos(\theta_1) + \sin(\theta_1)\mathbf{i}),\ z_2 = |z_2|(\cos(\theta_2) + \sin(\theta_2)\mathbf{i}).$$

则

$$z_1 z_2 = |z_1||z_2|(\cos(\theta_1 + \theta_2) + \sin(\theta_1 + \theta_2)\mathbf{i}).$$

证明. 直接计算得

$$\begin{aligned} z_1 z_2 &= |z_1||z_2| \\ &\quad (\cos(\theta_1)\cos(\theta_2) - \sin(\theta_1)\sin(\theta_2)) + (\cos(\theta_1)\sin(\theta_2) + \sin(\theta_1)\cos(\theta_2))\mathbf{i} \\ &= |z_1||z_2|(\cos(\theta_1 + \theta_2) + \sin(\theta_1 + \theta_2)\mathbf{i}). \quad \square \end{aligned}$$

命题 3.4 设 $z = |z|(\cos(\theta) + \sin(\theta)\mathbf{i})$.

(i) 对任意 $n \in \mathbb{N}$, $z^n = |z|^n(\cos(n\theta) + \sin(n\theta)\mathbf{i})$.

(ii) 如果 $z \neq 0$, 则 $z^{-1} = |z|^{-1}(\cos(\theta) - \sin(\theta)\mathbf{i})$.

证明. (i) 对 n 归纳. 当 $n=0$ 时, 结论显然成立. 设 $n>0$ 且结论对 $n-1$ 时成立.

$$\begin{aligned} z^n &= zz^{n-1} \\ &= |z|(\cos(\theta)+\sin(\theta)\mathbf{i})|z|^{n-1}(\cos((n-1)\theta)+\sin((n-1)\theta)\mathbf{i}) \\ &\quad (\text{归纳假设}) \\ &= |z|^n(\cos(n\theta)+\sin(n\theta)\mathbf{i}) \quad (\text{引理 3.3}). \end{aligned}$$

(ii) 直接计算得

$$\begin{aligned} & z|z|^{-1}(\cos(\theta)-\sin(\theta)\mathbf{i}) \\ &= |z|(\cos(\theta)+\sin(\theta)\mathbf{i})|z|^{-1}(\cos(-\theta)+\sin(-\theta)\mathbf{i}) \\ &= 1 \quad (\text{引理 3.3}). \quad \square \end{aligned}$$

令

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

则, $z=|z|(\cos(\theta)+\sin(\theta)\mathbf{i})$ 可简记为 $z=|z|e^{\mathbf{i}\theta}$. 上述引理和命题中的结论可写为

$$z_1=|z_1|e^{\mathbf{i}\theta_1}, z_2=|z_2|e^{\mathbf{i}\theta_2} \implies z_1z_2=|z_1||z_2|e^{\mathbf{i}(\theta_1+\theta_2)}.$$

当 $z=|z|e^{\mathbf{i}\theta}\neq 0$ 时, 对任意 $n\in\mathbb{Z}$, $z^n=|z|^ne^{\mathbf{i}n\theta}$, 和 $\bar{z}=|z|e^{-\mathbf{i}\theta}$.

Euler “公式”

$$e^{\mathbf{i}\pi}+1=0.$$

3.3 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 3.5 *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 3.6 *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. 设 $\epsilon_k, \epsilon_m \in U_n$. 则 $(\epsilon_k \epsilon_m^{-1})^n = \epsilon_k^n (\epsilon_m^n)^{-1} = 1$. 故 $\epsilon_k \epsilon_m^{-1} \in U_n$. 故 $(U_n, \cdot, 1)$ 是 $(\mathbb{C}^*, \cdot, 1)$ 的子群 (第四章第一讲命题 2.24).

注意到:

$$\begin{aligned} U_n = \langle \epsilon_\ell \rangle &\iff \mathrm{ord}(\epsilon_\ell) = n \\ &\iff \frac{n}{\gcd(n,\ell)} = n \text{ (第四章推论 2.34)} \\ &\iff \gcd(n,\ell) = 1 \quad \square \end{aligned}$$

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

3.4 代数学基本定理

定理 3.7 *(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 3.8 设 $f \in \mathbb{C}[x]\backslash\mathbb{C}$. 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.

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 3.9 *在 $\mathbb{R}[x]$ 中次数大于 2 的多项式必然有非平凡因式分解, 即存在 $f_1, f_2 \in \mathbb{R}[x] \setminus \mathbb{R}$ 使得该多项式等于 $f_1 f_2$.*

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 $\bar{\alpha}$. 根据余式定理 $f(x) = g(x)(x-\alpha)$, 其中 $g \in \mathbb{C}[x]$. 因为 $f(\bar{\alpha}) = 0$, 所以 $g(\bar{\alpha}-\alpha) = 0$. 再因为 $\bar{\alpha} - \alpha \neq 0$. 于是, $g(\bar{\alpha}) = 0$. 故余式定理蕴含 $g(x) = q(x)(x - \bar{\alpha})$. 由此可知,

$$f(x) = q(x)(x-\alpha)(x-\bar{\alpha}).$$

因为 $(x-\alpha)(x-\bar{\alpha}) \in \mathbb{R}[x]$, 所以 $q(x) \in \mathbb{R}[x]$ (两个实系数多项式相除得到的商和余式都是实系数多项式). 故 f 在 $\mathbb{R}[x]$ 中有非平凡因式分解. □

3.5 应用举例

例 3.10 设循环矩阵

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

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 $V\mathrm{diag}(f(\epsilon_0), \ldots, f(\epsilon_{n-1})) = AV$. 由 *Vandermonde* 行列式可知, V 可逆. 故

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

两边取行列式得

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

而 A 可逆当且仅当任何 n 次单位根都不是 f 的根. 此时,

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

例 3.11 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)*, 称为 *Hamilton* 四元数系.

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.