第五章　复数域和多项式

3.4　Gauss 引理

定义 3.22 设 D 是唯一因子分解整环, $f \in D[x]^*$. 设

$$f = f_n x^n + f_{n-1}x^{n-1} + \cdots + f_0, \quad f_i \in D.$$

则 $\gcd(f_n, f_{n-1}, \ldots, f_0)$ 称为 f 的容度*(content)*, 记为 $\mathrm{cont}(f, x)$ 或 $\mathrm{cont}(f)$.

设 f=$\mathrm{cont}(f)g$, 其中 g∈$D[x]^*$ 满足 $\mathrm{cont}(g)$=1. 称 g 是 f 的本原部分*(primitive part)*, 记为 $\mathrm{pp}(f, x)$ 或 $\mathrm{pp}(f)$.

设 h∈$D[x]^*$. 如果 $\mathrm{cont}(h)$=1, 则称 h 是本原多项式.

引理 3.23 设 D 是唯一因子分解整环, $f \in D[x]^*$. 再设 $a \in D^*$, $g \in D[x]^*$ 是本原多项式. 如果 $ag = \mathrm{cont}(f)\mathrm{pp}(f)$, 则 $a \approx \mathrm{cont}(f)$ 和 $g \approx \mathrm{pp}(f)$.

证明. 设

$$f = f_n x^n + f_{n-1}x^{n-1} + \cdots + f_0$$

和

$$g = g_n x^n + g_{n-1}x^{n-1} + \cdots + g_0,$$

其中 $f_i, g_i \in D$ 且 $f_n g_n \neq 0$. 注意到 $f = ag$ 且 g 是本原的. 故第五章第二讲例 3.21 蕴含 $\mathrm{cont}(f) \approx a$. 设 $a = u\mathrm{cont}(f)$, 其中 $u \in U_D$. 于是，$ug = \mathrm{pp}(f)$. 即 $g \approx \mathrm{pp}(f)$. □

引理 3.24 *(Gauss)* 设 D 是唯一因子分解整环. 则 $D[x]$ 中的本原多项式之积也是本原多项式.

证明. 设本原多项式

$$f = f_m x^m + f_{m-1}x^{m-1} + \cdots + f_0$$

和

$$g = g_n x^n + g_{n-1}x^{n-1} + \cdots + g_0,$$

其中 $f_m, f_{m-1}, \ldots, f_0, g_n, g_{n-1}, \ldots, g_0 \in D$ 且 f_m, g_n 都非零. 假设 fg 不是本原的. 则存在 D 中不可约元 p 使得 $p|\mathrm{cont}(fg)$. 注意到 $\mathrm{lc}(fg, x)$ 是 $f_m g_n$. 于是, $p|f_m g_n$. 由第五章第二讲命题 3.10 可知, $p|f_m$ 或 $p|g_n$. 不妨设 $p|f_m$. 因为 $\mathrm{cont}(f) = 1$, 所以存在 $i \in \{0, 1, \ldots, m-1\}$ 使得

$$p|f_m, p|f_{m-1}, \ldots, p|f_{i+1}, \text{但} p \nmid f_i.$$

因为 $\mathrm{cont}(g) = 1$, 所以存在 $j \in \{0, 1, \ldots, n\}$ 使得

$$p|g_n, p|g_{n-1}, \ldots, p|g_{j+1}, \text{但} p \nmid g_j.$$

注意到在 fg 中 x^{i+j} 的系数是

$$c = \sum_{k+\ell=i+j} f_k g_\ell \quad \text{且} \quad p|c.$$

如果 $\ell < j$, 则 $k > i$. 故 $p|f_k \Longrightarrow p|f_k g_\ell$. 如果 $\ell > j$, 则 $p|g_\ell$. 故 $p|f_k g_\ell$. 于是, $p|f_i g_j$. 根据第五章第二讲命题 3.10, $p|f_i$ 或 $p|g_j$. 矛盾. □

推论 3.25 设 D 是唯一因子分解整环, $f, g \in D[x]^*$. 则

$$\mathrm{cont}(fg) \approx \mathrm{cont}(f)\mathrm{cont}(g), \quad \mathrm{pp}(fg) \approx \mathrm{pp}(f)\mathrm{pp}(g).$$

证明. 因为 $f = \mathrm{cont}(f)\mathrm{pp}(f)$ 和 $g = \mathrm{cont}(g)\mathrm{pp}(g)$, 所以

$$fg = \mathrm{cont}(fg)\mathrm{pp}(fg) = (\mathrm{cont}(f)\mathrm{cont}(g))\mathrm{pp}(f)\mathrm{pp}(g).$$

根据引理 3.24, $\mathrm{pp}(f)\mathrm{pp}(g)$ 是本原的. 再根据引理 3.23,

$$\mathrm{cont}(fg) \approx \mathrm{cont}(f)\mathrm{cont}(g), \quad \mathrm{pp}(fg) \approx \mathrm{pp}(f)\mathrm{pp}(g). \quad \square$$

定理 3.26 设 D 是唯一因子分解整环, F 是 D 的分式域. 设 $f \in D[x]$ 且 $\deg(f) > 0$. 如果 f 不能写成两个 $D[x]$ 中正次数的多项式之积. 则 f 在 $F[x]$ 不可约.

证明. 假设 $f = gh$, 其中 $g, h \in F[x] \setminus F$. 因为 F 是 D 的分式域, 所以存在 $\alpha, \beta \in D$ 使得 $\alpha f = \beta \tilde{g}\tilde{h}$, 其中 $\alpha, \beta \in D^*$, $\tilde{g}, \tilde{h} \in D[x]$ 是本原多项式, $\deg(\tilde{g}) = \deg(g)$, $\deg(\tilde{h}) = \deg(h)$. 于是, $\alpha\mathrm{cont}(f)\mathrm{pp}(f) = \beta(\tilde{g}\tilde{h})$. 根据推论 3.24, $\mathrm{pp}(f) = u\tilde{g}\tilde{h}$, 其中 $u \in U_D$. 故 $f = \mathrm{cont}(f)\mathrm{pp}(f) = (\mathrm{cont}(f)u\tilde{g})\tilde{h}$. 矛盾. $\square$

定理 3.27 *(Eisenstein 不可约性判别法)* 设 D 是唯一因子分解整环, F 是 D 的分式域,

$$f = f_n x^n + f_{n-1}x^{n-1} + \cdots + f_0,$$

其中 $n > 0$, $f_n, f_{n-1}, \ldots, f_0 \in D$ 且 $f_n \neq 0$. 设 p 是 D 中的不可约元. 如果

$$p \nmid f_n,\ p | f_{n-1},\ \ldots,\ p | f_0,\ p^2 \nmid f_0,$$

则 f 在 $F[x]$ 中不可约.

证明. 由上述定理可知, 我们只要证明 f 不能写成 $D[x]$ 中两个正次数的多项式之积即可. 假设

$$f(x) = (g_k x^k + \cdots + g_1 x + g_0)(h_\ell x^\ell + \cdots + h_1 x + h_0),$$

其中 $k, \ell \in \mathbb{Z}^+$, $g_k, \ldots, g_1, g_0, h_\ell, \ldots, h_1, h_0 \in D$ 且 g_k, h_ℓ 都不等于零.

因为 $f_n = g_k h_\ell$ 且 $p \nmid g_k h_\ell$, 所以 $p \nmid g_k$ 和 $p \nmid h_\ell$ (第五章第二讲命题 3.10). 因为 $f_0 = g_0 h_0$ 和 $p | f_0$, 所以 $p | g_0$ 或 $p | h_0$. 不妨设 $p | g_0$. 又因为 $p^2 \nmid f_0$, 所以 $p \nmid h_0$. 因为 $p \nmid g_k$ 和 $p | g_0$, 所以存在 $i \in \{0, 1, \ldots, k\}$ 使得

$$p | g_0, \cdots, p | g_{i-1} \quad \text{但} \quad p \nmid g_i.$$

则

$$f_i = h_0 g_i + h_1 g_{i-1} + \cdots + h_i g_0.$$

因为 $i \leq k < n$, 所以 $p | f_i$. 由此可知, $p | h_0 g_i$. 故 $p | h_0$ 或 $p | g_i$. 矛盾. □

例 3.28 证明: 对于 $n > 1$, $x^n - 2x + 2$ 在 $\mathbb{Q}[x]$ 中不可约.

证明. 注意到 $2 \nmid 1$, $2 | -2$, $2 | 2$ 但 $2^2 \nmid 2$. 根据定理 *3.27*, 该多项式不可约.

例 3.29 设 p 是素数. 证明: $x^{p-1} + x^{p-2} + \cdots + x + 1$ 在 $\mathbb{Q}[x]$ 中不可约.

证明. 设 $f(x) = x^{p-1} + x^{p-2} + \cdots + x + 1$. 考虑映射

$$\begin{aligned} \phi : \ \mathbb{Z}[x] &\longrightarrow \quad \mathbb{Z}[x] \\ g(x) &\mapsto \quad g(x+1). \end{aligned}$$

则 ϕ 是由 $\mathbb{Z} \hookrightarrow \mathbb{Z}[x]$ 和 $x \mapsto x + 1$ 诱导的环同态. 同理

$$\begin{aligned} \psi : \ \mathbb{Z}[x] &\longrightarrow \quad \mathbb{Z}[x] \\ g(x) &\mapsto \quad g(x-1) \end{aligned}$$

也是环同态. 因为 $\phi \circ \psi = \psi \circ \phi = \mathrm{id}_{\mathbb{Z}[x]}$, 所以 ϕ 是环同构.

要证明 $f(x)$ 在 $\mathbb{Q}[x]$ 中不可约. 只要证明 $f(x+1)$ 在 $\mathbb{Z}[x]$ 中不可约*(定理 3.26)*. 由于 ϕ 是同构, 只要证明 $f(x+1)$ 在 $\mathbb{Z}[x]$ 中不可约即可. 注意到

$$f(x) = \frac{x^p - 1}{x - 1} \Longrightarrow f(x+1) = \frac{(x+1)^p - 1}{x}.$$

故

$$f(x+1) = x^{p-1} + \binom{p}{1} x^{p-2} + \cdots + \binom{p}{2} x + p.$$

由第二章第一讲例 *7.17* 和定理 *3.27* 可知, $f(x+1)$ 不可约. 故 $f(x)$ 也不可约.

定理 3.30 设 D 是唯一因子分解整环. 则 $D[x]$ 也是.

证明. 根据第五章第一讲定理 1.8, $D[x]$ 是整环. 根据第五章第一讲命题 1.6, D 中的元素只可能是若干个 D 中的元素之积. 因为 D 是唯一因子分解整环, 所以 D^* 中的元素是若干个 D 中不可约元素之积. 类似于第五章第二节例 3.8 中次数推理, 我们可以证明 $D[x] \setminus D$ 中任何本原多项式都是若干 $D[x]$ 中不可约的多项式之积. 注意到任意 $f \in D[x] \setminus D$ 有分解 $f = \mathrm{cont}(f)\mathrm{pp}(f)$. 故 f 是 $D[x]$ 中若干非零多项式之积.

根据第五章第二讲命题 3.10, 只需证明 $D[x]$ 中任意不可约元都是素元. 设 $f \in D[x]$ 是不可约元且 $f|gh$, 其中 $g, h \in D[x]^*$. 则

$$\mathrm{cont}(f)\mathrm{pp}(f)|\mathrm{cont}(g)\mathrm{cont}(h)\mathrm{pp}(g)\mathrm{pp}(h).$$

如果 $f \in D$, 则 $\mathrm{pp}(f) = 1$. 故 $f = \mathrm{cont}(f)|\mathrm{cont}(g)\mathrm{cont}(h)$ (推论 3.25). 因为 D 是唯一因子分解整环, 所以 f 是 D 中素元 (第五章第二讲命题 3.10). 由此得出, $f|\mathrm{cont}(g)$ 或 $f|\mathrm{cont}(h)$. 故 $f|g$ 或 $f|h$. 即 f 是素元.

如果 $\deg(f) > 0$, 则 f 是本原的. 由定理 3.26 可知, f 在 $F[x]$ 中不可约, 其中 F 是 D 的分式域. 因为 $f|gh$ 在 $D[x]$ 中成立, 所以 $f|gh$ 在 $F[x]$ 中成立. 因为 $F[x]$ 是唯一因子分解整环, 所以 f 是 $F[x]$ 中的素元. 故在 $F[x]$ 中, $f|g$

或 $f|h$. 不妨设 $f|g$. 则存在 $q \in F[x]$ 使得 $g = qf$. 于是, 存在 $\alpha, \beta \in D$ 使得 $\alpha \mathrm{pp}(g) = \beta \mathrm{pp}(q)\mathrm{pp}(f) = \beta \mathrm{pp}(q) f$. 由推论 3.25, $f|\mathrm{pp}(g)$ 在 $D[x]$ 中成立. 故 $f|g$ 在 $D[x]$ 中成立. □

4 复数

4.1 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

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

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 4.1 设

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

由第十三次作业及其习题课讲义可知, $(F, +, O, \cdot, E)$ 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

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

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

注意到

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

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

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 $\bar{}|_{\mathbb{R}} = \mathrm{id}_{\mathbb{R}}$. 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

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

4.2 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 4.3 设复数

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

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

$$\begin{aligned}z_1z_2 &= |z_1||z_2|\\ &\quad(\cos(\theta_1)\cos(\theta_2)-\sin(\theta_1)\sin(\theta_2))+(\cos(\theta_1)\sin(\theta_2)+\sin(\theta_1)\cos(\theta_2))\mathbf{i}\\ &= |z_1||z_2|(\cos(\theta_1+\theta_2)+\sin(\theta_1+\theta_2)\mathbf{i}).\quad\square\end{aligned}$$

命题 4.4 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.

$$\begin{aligned}z^n &= zz^{n-1}\\ &= |z|(\cos(\theta)+\sin(\theta)\mathbf{i})|z|^{n-1}(\cos((n-1)\theta)+\sin((n-1)\theta)\mathbf{i})\\ &\quad(\text{归纳假设})\\ &= |z|^n(\cos(n\theta)+\sin(n\theta)\mathbf{i})\quad(\text{引理 4.3}).\end{aligned}$$

(ii) 直接计算得

$$\begin{aligned}&z|z|^{-1}(\cos(\theta)-\sin(\theta)\mathbf{i})\\ &= |z|(\cos(\theta)+\sin(\theta)\mathbf{i})|z|^{-1}(\cos(-\theta)+\sin(-\theta)\mathbf{i})\\ &= 1\quad(\text{引理 4.3}).\quad\square\end{aligned}$$

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

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

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

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. 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).

对任意 $k \in \{0, 1, \ldots, n-1\}$, $\epsilon_k = \epsilon_1^k$. 于是, $U_n = \langle \epsilon_1 \rangle$.

设 $\ell \in \{0, 1, \ldots, n-1\}$ 使得 $\gcd(\ell, n) = 1$. 对任意 $k \in \mathbb{Z}$, 存在 $u, v \in \mathbb{Z}$ 使得 $u\ell + vn = k$. (Bezout 关系的直接推论). 于是,

$$\epsilon_k = \epsilon_1^k = \epsilon_1^{u\ell + vn} = \left(\epsilon_1^\ell\right)^u (\epsilon_1^n)^v = \epsilon_\ell^u.$$

故 $U_n = \langle \epsilon_\ell \rangle$.

设 $U_n = \langle \epsilon_\ell \rangle$. 则存在 $u \in \mathbb{Z}$ 使得 $\epsilon_\ell^u = \epsilon_1$. 故 $\epsilon_1^{\ell u - 1} = 1$. 因为 $\mathrm{ord}(\epsilon_1) = n$, 所以 $n | (\ell u - 1)$. 故存在 $v \in \mathbb{Z}$ 使得 $\ell u - 1 = vn$ (第四章第二讲命题 2.38 (ii)), 即 $\ell u + vn = 1$. 根据第一章第四讲定理 7.8, $\gcd(\ell, n) = 1$. □

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

例 4.7 设 $f = a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \cdots + a_1 x + a_0 \in \mathbb{C}[x]$. 对 $k \in \{0, 1, \ldots, n-1\}$, 我们有

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

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

$$\epsilon_k^2 f(\epsilon_k) = a_{n-3}\epsilon_k^{n-1} + \cdots + a_1\epsilon_k^3 + a_0\epsilon_k^2 + a_{n-1}\epsilon_k + a_{n-2}.$$

$$\vdots$$

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

利用矩阵写成

$$\mathbf{v}_k := f(\epsilon_k)\begin{pmatrix} 1 \\ \epsilon_k \\ \epsilon_k^2 \\ \vdots \\ \epsilon_k^{n-1} \end{pmatrix} = \underbrace{\begin{pmatrix} a_{n-1} & a_{n-2} & \cdots & a_1 & a_0 \\ a_{n-2} & a_{n-3} & \cdots & a_1 & a_{n-1} \\ a_{n-3} & a_{n-4} & \cdots & a_{n-1} & a_{n-2} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ a_0 & a_{n-1} & \cdots & a_2 & a_1 \end{pmatrix}}_{A}\begin{pmatrix} \epsilon_k^{n-1} \\ \epsilon_k^{n-2} \\ \epsilon_k^{n-3} \\ \vdots \\ 1 \end{pmatrix}.$$

于是,

$$(\mathbf{v}_0, \mathbf{v}_1, \ldots, \mathbf{v}_{n-1}) = A\underbrace{\begin{pmatrix} \epsilon_0^{n-1} & \epsilon_1^{n-1} & \epsilon_2^{n-1} & \cdots & \epsilon_{n-1}^{n-1} \\ \epsilon_0^{n-2} & \epsilon_1^{n-2} & \epsilon_2^{n-2} & \cdots & \epsilon_{n-1}^{n-2} \\ \epsilon_0^{n-3} & \epsilon_1^{n-3} & \epsilon_2^{n-3} & \cdots & \epsilon_{n-3}^{n-3} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 1 & 1 & 1 & \cdots & 1 \end{pmatrix}}_{B}.$$

等式两边取行列式并利用行列式乘积定理得

$$\det((\mathbf{v}_0, \mathbf{v}_1, \ldots, \mathbf{v}_{n-1})) = \det(A)\det(B).$$

即

$$\det(A) = (-1)^{\frac{n(n-1)}{2}} f(\epsilon_0)f(\epsilon_1)\cdots f(\epsilon_{n-1}).$$

4.4 代数学基本定理

定理 4.8 *(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 4.9 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 $\mathbb{C}[x]$ 中的不可约元恰是一次多项式, 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 4.10 *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, $\alpha \neq \bar{\alpha}$.

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 f, 且它们的商也是实系数多项式. 矛盾. $\square$

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. 通过计算 $\mathbb{Z}[\sqrt{-5}]$ 中元素的模长可知, 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

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

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).