第五章　复数域和多项式

3　唯一因子分解整环

在本节中 D 是整环, $D^* = D \setminus \{0\}$, U_D 代表 D 中可逆元, F 代表域.

3.2　唯一因子分解整环

定义 3.7 设 $a \in D^*$ 是不可逆元. 如果存在不可约元 $p_1, \ldots, p_n$ 使得

$$a = p_1 \cdots p_n.$$

则称 a 有不可约分解. 而上式称为 a 的一个不可约分解.

由第二章第一讲中例 7.20 可知, 每个绝对值大于 1 的整数都有不可约分解.

例 3.8 $44 = 2^2 \cdot 11$, $-45 = -3^2 \cdot 9$.

$$242340461377689532 = 41 \cdot 11 \cdot 2^2 \cdot 13 \cdot 3214571^2.$$

例 3.9 设 $f \in F[x] \setminus F$. 证明: f 有不可约分解.

证明. 设 $n = \deg(f)$. 我们对 n 归纳. 当 $n = 1$ 时, f 是不可约多项式. 结论成立. 设 $n > 1$ 且结论对任何次数大于零且小于 n 的多项式都成立. 考虑次数等于 n 的情形. 如

果 f 是不可约的, 则结论成立. 否则, 存在次数为正且小于 n 的多项式 $g, h \in F[x]$ 使得 $f = gh$ *(见第五章第一讲命题 2.3)*. 由归纳假设可知, g 和 h 都是若干个不可约多项式之积. 故 f 也是.

定义 3.10 设 D 整环. 我们称 D 是唯一因子分解整环*(unique factorization domain, UFD)*, 如果 D 中每个非零非单位的元素 a 都满足下列两个条件.

(i) a 可以写成 D 中有限多个不可约元素之积;

(ii) 设

$$a = p_1 \cdots p_m = q_1 \cdots q_n,$$

其中 $p_1, \ldots, p_m, q_1, \ldots, q_n$ 是 D 中的不可约元, 则 $m = n$ 且适当调整下标后, 我们有

$$p_1 \approx q_1, \ \ldots, \ p_m \approx q_m.$$

命题 3.11 设 D 满足上述定义中的条件 *(i)*. 则 D 是唯一因子分解整环当且仅当 D 中的不可约元都是素元.

证明. 先设上述定义中的条件 (ii) 也成立. 我们证明 D 中的不可约元都是素元.

设 $q \in D$ 是不可约元且 $q|st$, 其中 $s, t \in D^*$. 则存在 $r \in D^*$ 使得 $rq = st$. 因为 D 是唯一因子分解整环, 所以

$$r = ur_1 \cdots r_k, \ s = vs_1 \cdots s_m, \ t = wt_1 \cdots t_n,$$

其中 $u, v, w \in U_D$, $r_1, \ldots, r_k, s_1, \ldots, s_m, t_1, \ldots, t_n \in D$ 是不可约元. 则

$$ur_1 \cdots r_k q = (vw)s_1 \cdots s_m t_1 \cdots t_n.$$

故

$$r_1 \cdots r_k q = (u^{-1}vw)s_1 \cdots s_m t_1 \cdots t_n.$$

由上述定义条件 (ii) 可知, q 与 $s_1, \ldots, s_m, t_1, \ldots, t_n$ 中某个元素相伴. 故 $q|s$ 或 $q|t$. 即 q 是素元.

再设 D 中的不可约元都是素元. 我们证明上述定义中的条件 (ii) 成立. 设 $x \in D^*$ 不可逆. 由上述定义中条件 (i) 可知, 存在不可约元 $p_1, \ldots, p_m$ 使得

$$x = p_1 \cdots p_m.$$

再设 x 的另一个不可约分解是

$$x = q_1 \cdots q_n,$$

其中 $q_1, \ldots, q_n$ 是 D 中的不可约元. 不妨设 $m \leq n$. 则

$$p_1 | q_1 q_2 \cdots q_n = q_1(q_2 \cdots q_n).$$

因为 p_1 是素元, 所以 $p_1|q_1$ 和 $p_1|q_2 \cdots q_n$. 故 p_1 整除某个 q_i. 适当调整下标, 我们不妨假设 $p_1|q_1$. 于是, 存在 $a \in D$ 使得 $q_1 = up_1$. 因为 q_1 是不可约元且 p_1 不可逆, 所以 u 可逆. 由此可知, $p_1 \approx q_1$ 且

$$p_2 \cdots p_m = uq_2 q_3 \cdots q_n.$$

重复同样的推理和适当调整下标, 我们可得

$$p_2 \approx q_2, \ldots, p_m \approx q_m.$$

从而我们有

$$1 = uq_{n-m-1} \cdots q_n.$$

故当 $m < n$ 时, $q_{n-m-1}, \ldots, q_n$ 是都是可逆元. 矛盾. 由此可知, $m = n$. $\square$

注解 3.12 设 D 是唯一因子分解整环, $a \in D$, 且

$$a = p_1 \cdots p_n,$$

其中 $p_1, \ldots, p_n$ 是不可约元. 如果 $p_1 \approx p_n$, 则存在 $u_1 \in U_D$ 使得 $p_n = u_1 p_1$. 故

$$a = u_1 p_1^2 \cdots p_{n-1}.$$

重复上述步骤并适当置换下标, 我们有

$$a = u p_1^{m_1} \cdots p_\ell^{m_\ell}, \tag{1}$$

其中 $u \in U_D$, $p_1, \ldots, p_\ell$ 是两两互不相伴的不可约元, 且 $m_1, \ldots, m_\ell$ 是正整数. 特别地, 如果 q 是 a 的不可约因子, 则存在 $i \in \{1, \ldots, \ell\}$ 使得 $q \approx p_i$. 我们称 (1) 是 a 的一个标准不可约分解.

定理 3.13 整数环 $\mathbb{Z}$ 是唯一因子分解整环.

证明. 根据上学期第二章第一讲引理 7.23 可知, 整数环中每个素数(不可约元)都是素元. 根据命题 3.11, $\mathbb{Z}$ 是唯一因子分解整环. □

例 3.14 $44 = 2^2 \cdot 11,\ -45 = -3^2 \cdot 9.$

$$242340461377689532 = 41 \cdot 11 \cdot 2^2 \cdot 13 \cdot 3214571^2.$$

定理 3.15 设 F 是域. 则多项式环 $F[x]$ 是唯一因子分解整环.

证明. 根据例 3.9 和命题 3.11, 我们只要证明 $F[x]$ 中的次数大于零的不可约多项式都是素元即可. 设 f 是这样一个多项式. 再设 $g, h \in F[x]$ 满足 $f|gh$. 我们要证明 $f|g$ 或者 $f|h$. 假设 $f \nmid g$. 我们证明 $f|h$ 即可. 因为 f 不可约, 所以 f 和 g 互素. 根据上学期第十七讲定理 2.13, 存在 $u, v \in F[x]$ 使得

$$uf + vg = 1 \implies ufh + vgh = h.$$

因为 $f|(fh)$ 和 $f|(gh)$, 所以 $f|h$ (上学期第十七讲命题 2.3 (ii)). □

例 3.16 设

$$f = \underbrace{(2x-1)}_{q_1}\underbrace{(10x-5)}_{q_2}\underbrace{\left(\frac{1}{2}x^2 - \frac{1}{3}x + 2\right)}_{q_3} \in \mathbb{Q}[x].$$

一次多项式 q_1 和 q_2 是 $\mathbb{Q}[x]$ 中的不可约多项式. 二次多项式 q_3 的判别式小于零. 故 q_3 也是 $\mathbb{Q}[x]$ 中的不可约多项式. 计算每个因子的首一部分得到

$$f = 10 \underbrace{\left(x - \frac{1}{2}\right)}_{p_1}{}^2 \underbrace{\left(x^2 - \frac{2}{3}x + 4\right)}_{p_2}.$$

例 3.17 证明: $f(x) = x^4 + 1$ 在 $\mathbb{Q}[x]$ 中不可约但在 $\mathbb{R}[x]$ 中可约.

证. 因为 $f(x)$ 在实数上恒正, 所以 $f(x)$ 没有有理根. 根据余式定理, $f(x)$ 没有一次因子. 假设

$$f(x) = (x^2 + ax + b)(x^2 + cx + d),$$

其中 $a, b, c, d \in \mathbb{Q}$. 根据待定系数法可知

$$\begin{cases} a + c = 0 \\ ac + b + d = 0 \\ ad + bc = 0 \\ bd = 1 \end{cases} \Longrightarrow \begin{cases} a^2 - \left(b + \frac{1}{b}\right) = 0 \\ a\left(b - \frac{1}{b}\right) = 0. \end{cases}$$

于是, $a = 0$ 或 $b^2 = 1$. 前者意味着 $b + 1/b = 0$, 而后者蕴含 $a^2 = \pm 2$. 这在有理数域中都不可能.

通过配方法可知

$$f(x) = (x^2+1)^2 - 2x^2 = (x^2 - \sqrt{2}x + 1)(x^2 + \sqrt{2}x + 1). \quad \square$$

注解 3.18 对任何素数 p, $x^4+\bar{1}$ 在 $\mathbb{Z}_p[x]$ 中可约. 例如: 当 $p=2$ 时,

$$(x^4+\bar{1})=(x+\bar{1})^4 \quad \textit{(大学一年级新生之梦).}$$

当 $p=3$ 时

$$(x^4+\bar{1})=(x^2-x-\bar{1})(x^2+x-\bar{1}) \quad \textit{(直接验证).}$$

3.3 重数

定义 3.19 设 D 是唯一因子分解整环, $a\in D^*$ 和 $p\in D^*$ 是不可约元. 如果非负整数 m 使得 $p^m|a$ 但 $p^{m+1}\nmid a$, 则称 m 是 p 在 a 中的重数*(multiplicity).*

定义 3.20 设 $f\in F[x]^*$ 和 $x-\alpha\in F[x]$. 如果 $(x-\alpha)^m|f$ 但 $(x-\alpha)^{m+1}\nmid f$, 则称 α 是 f 中的 m 重根. 当 $m=1$ 时, α 称为 f 的单根*(simple root);* 当 $m>1$ 时, α 称为 f 的重根*(multiple root).*

定理 3.21 设 $f\in F[x]\setminus F$, $\alpha_1,\ldots,\alpha_s\in F$ 是 f 互不相同的根, 其重数分别是 $m_1,\ldots,m_s$. 则

$$(x-\alpha_1)^{m_1}\cdots(x-\alpha_s)^{m_s}|f.$$

特别地, $m_1+\cdots+m_s\le\deg(f)$.

证明. 由定理 3.15 可知, $F[x]$ 是唯一因子分解整环. 注意到 $x-\alpha_1,\ldots,x-\alpha_s$ 是 $F[x]$ 中两两互不相伴的不可约因子. 故结论由注释 3.12 直接可得. □

命题 3.22 设 D 是唯一因子分解整环, $a,b\in D^*$. 则它们的最大公因子和最小公倍式都存在.

证明. 因为 D 是唯一因子分解整环, 所以存在 $u,v\in U_D$, 互不相伴的不可约元 $p_1,\ldots,p_m$, 非负整数 $i_1,\ldots,i_m,j_1,\ldots,j_m$ 使得

$$a=up_1^{i_1}\cdots p_m^{i_m}\quad\text{和}\quad b=vp_1^{j_1}\cdots p_m^{j_m}.$$

令

$$g=p_1^{\min(i_1,j_1)}\cdots p_m^{\min(i_m,j_m)}\quad\text{和}\quad \ell=p_1^{\max(j_1,i_1)}\cdots p_m^{\max(i_m,j_m)}.$$

则 g 是 a,b 的公因子且 ℓ 是 a,b 的公倍式.

设 d 是 a 和 b 的公因子且 q 是 d 的一个 k 重不可约因子, 其中 $k>1$. 由命题 3.11 可知, q 是素元. 故存在 $s\in\{1,2,\ldots,m\}$ 使得

$$q\approx p_s,i_s>0,j_s>0.$$

适当变换下标后, 不妨设 $s=1$ 和 $q=p_1$. 令 $d=d'q$. 则 q 在 d' 中的重数是 $k-1$, 且 d' 是

$$up_1^{i_1-1}\cdots p_m^{i_m}\quad\text{和}\quad vp_1^{j_1-1}\cdots p_m^{j_m}$$

的公因子. 有限次同样的推理可知, $k \le \min(i_1, j_1)$. 故 $d|g$. 由此可知, $g = \gcd(a, b)$.

类似地, 设 h 是 a 和 b 的公倍式. 因为 $a|h$, 所以对任意 $s \in \{1, \ldots, m\}$, $p_s^{i_s}|h$. 同理 $p_s^{j_s}|h$. 于是, $p_s^{\max(i_s, j_s)}|h$. 故 p_s 在 h 中的重数大于或等于 $\max(i_s, j_s)$. 于是, $\ell|h$. 由此得出 ℓ 是 a, b 的最小公倍式. □

3.4 Gauss 引理

定义 3.23 设 D 是唯一因子分解整环, $f \in D[x]^*$. 设

$$f = f_n x^n + f_{n-1} x^{n-1} + \cdots + f_0, \quad f_i \in D, f_n \neq 0.$$

则 $\gcd(f_n, f_{n-1}, \ldots, f_0)$ 称为 f 的容度*(content)*, 记为 $\mathrm{cont}(f)$. 设 $f = \mathrm{cont}(f)g$, 其中 $g \in D[x]^*$ 满足 $\mathrm{cont}(g) = 1$. 称 g 是 f 的本原部分*(primitive part)*, 记为 $\mathrm{pp}(f)$.

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

例 3.24 设 $f(x) = 6x^2 - 4x + 12$. 则

$$\mathrm{cont}(f) = 2, \quad \mathrm{pp}(f) = 3x^2 - 2x + 6.$$

或

$$\mathrm{cont}(f) = -2, \quad \mathrm{pp}(f) = -(3x^2 - 2x + 6).$$

注解 3.25 一个多项式的容度和本原部分在相伴意义下是唯一的.

引理 3.26 设 D 是唯一因子分解整环, $a_1, \ldots, a_m, b \in D^*$. 证明: $\gcd(a_1 b, \ldots, a_m b) = \gcd(a_1, \ldots, a_m) b$.

证明. 设 $g = \gcd(a_1, \ldots, a_m)$ 和 $h = \gcd(a_1 b, \ldots, a_m b)$. 根据上学期第十七周讲义命题 2.7, 我们只需证明 $h|gb$ 和 $gb|h$.

因为 b 是 $a_1 b, \ldots, a_m b$ 的公因子, 所以 $b|h$. 故存在 $c \in D$ 使得 $h = bc$. 再设 $a_i b = r_i h$, 其中 $r_i \in D$, $i = 1, \ldots, n$. 我们有 $a_i b = r_i bc$. 有消去律可知 $a_i = r_i c$. 故 c 是 $a_1, \ldots, a_n$ 的公因子. 于是,

$$c|g \Longrightarrow cb|gb \Longrightarrow h|gb.$$

再设 $a_i = s_i g$, $s_i \in D$, $i = 1, \ldots, n$. 则

$$a_i b = s_i gb \Longrightarrow gb|a_i b \Longrightarrow gb|h. \quad \square$$

引理 3.27 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 $f = ag$, 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 $f_n g_n \neq 0$. 因为 $f = ag$, 所以

$$\mathrm{cont}(f) = \mathrm{cont}(ag).$$

由引理 3.26 可知, $\mathrm{cont}(f) \approx a$. 设 $a = u\mathrm{cont}(f)$, 其中 $u \in U_D$. 于是，$ug = \mathrm{pp}(f)$. 即 $g \approx \mathrm{pp}(f)$. □

定理 3.28 *(Gauss 引理)* 设 D 是唯一因子分解整环, $f, g \in D[x]^*$ 都是本原多项式. 则 fg 也是本原多项式.

证明. 设

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

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 $p|\mathrm{cont}(fg)$. 因为 $\mathrm{cont}(f) = 1$, 所以存在 $i \in \{0, 1, \ldots, m\}$ 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 在中 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 $p|f_k \Longrightarrow p|f_kg_\ell$. 如果 $\ell>j$, 则 $p|g_\ell$. 故 $p|f_kg_\ell$. 于是, $p|f_ig_j$. 根据命题 3.11, $p|f_i$ 或 $p|g_j$. 矛盾. □

推论 3.29 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

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

根据定理 3.28, $\mathrm{pp}(f)\mathrm{pp}(g)$ 是本原的. 由引理 3.27,

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

定理 3.30 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, $\alpha\mathrm{cont}(f)\mathrm{pp}(f) = \beta(\tilde{g}\tilde{h})$. 根据定理 3.28 可知, $\mathrm{pp}(f) = u\tilde{g}\tilde{h}$, 其中 $u \in U_D$. 故

$$f = \mathrm{cont}(f)\mathrm{pp}(f) = (\mathrm{cont}(f)u\tilde{g})\tilde{h}.$$

矛盾. □

定理 3.31 *(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 $p \nmid f_n = g_k h_\ell$, 所以 $p \nmid g_k$ 和 $p \nmid h_\ell$ (命题 3.11). 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 3.32 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 *3.31*, 该多项式不可约.

例 3.33 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

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

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

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

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 3.30)*. 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 *3.31* 可知, $f(x+1)$ 不可约. 故 $f(x)$ 也不可约.

定理 3.34 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 1.7, D 中的元素只可能是若干个同样环中的元素之积. 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. 类似于例 3.9 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 $D[x]$ 中若干不可约元之积.

根据命题 3.11, 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 3.29). 因为 D 是唯一因子分解整环, 所以 f 是 D 中素元 (命题 3.11). 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 3.30 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

$$\alpha \mathrm{pp}(g) = \beta \tilde{q} f,$$

其中 $\tilde{q} \in D[x]$ 是本原多项式. 由推论 3.29, $f|\mathrm{pp}(g)$ 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

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

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 4.1 设

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

则 F 是 $\mathrm{M}_n(\mathbb{R})$ 的子环, $(F, +, O, \cdot, E)$ 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

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

进而, $\phi(E)=1$. 故 ϕ 是环同态. 显然 ϕ 是满射. 再根据命题第四章第三讲命题 *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 $^-|_{\mathbb{R}} = \mathrm{id}_{\mathbb{R}}$.

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

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

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

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

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

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

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

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

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 $\bar{z} = |z|e^{-\mathbf{i}\theta}$.

Euler "公式"

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