第五章　复数域和多项式

5　唯一因子分解整环

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

注解 5.1 设 $a, b \in D$. 则 $a \approx b \iff \exists\, u \in U_D,\ a = ub$.

5.1　不可约元和素元

定义 5.2 设 $a \in D^*$ 不可逆. 如果不存在非可逆元 $b, c \in D^*$ 使得 $a = bc$, 则称 a 是不可约元 *(irreducible element)*.

注解 5.3 设 $a, b \in D$ 且 $a \approx b$. 则 a 不可约当且仅当 b 不可约. 设 $a, b \in D$ 是不可约元. 如果 $a|b$, 则 $a \approx b$.

例 5.4 整数环 $\mathbb{Z}$ 中的不可约元是所有的素数和它们的相反数. 根据上一讲中的结论, 多项式环 $\mathbb{C}[x]$ 中的不可约元是所有的一次多项式; $\mathbb{R}[x]$ 中的不可约元的次数不大于 2; 而 $F[x]$ 中的不可约元就是其中的不可约多项式.

定义 5.5 设 $p \in D^*$ 不可逆. 如果对于任意 $a, b \in D^*$,

$$p|ab \implies p|a \text{ 或 } p|b.$$

则称 p 是素元 *(prime element)*.

注解 5.6 设 $a, b \in D$ 且 $a \approx b$. 则 a 是素元当且仅当 b 是素元.

注解 5.7 设 $p \in D$ 是素元, $a_1, \ldots, a_n \in D$. 如果 $p | a_1 \cdots a_n$, 则存在 $i \in \{1, \ldots, n\}$ 使得 $p | a_i$.

引理 5.8 设 $p, a, b \in D^*$, 其中 p 是素元. 设 $k \in \mathbb{Z}^+$ 使得 $p^k | ab$ 且 $p \nmid b$. 则 $p^k | a$.

证明. 对 k 归纳. 由素元的定义, $k = 1$ 时结论成立. 设 $k > 1$ 且 结论对 $k - 1$ 成立. 因为 $p | ab$ 且 $p \nmid b$, 所以 $p | a$. 故存在 $c \in D^*$ 使得 $a = cp$. 于是, 存在 $d \in D^*$ 使得 $p^k d = cpb$. 根据整环中的消去律, $p^{k-1} d = cb$. 由归纳假设, $p^{k-1} | c$. 由此可知, $p^k | a$. □

引理 5.9 整环中的素元都是不可约元.

证明. 设 $p \in D^*$ 是素元, 且存在 $a, b \in D^*$ 使得 $p = ab$. 则 $p | a$ 或 $p | b$. 不妨设 $p | a$. 则存在 $q \in D^*$ 使得 $a = qp$. 故 $p = pqb$. 由整环中的消去律(第四章第二讲推论 3.26)可知, $1 = qb$. 故 b 可逆. 由此推出 p 不可约. □.

引理 5.10 在 $\mathbb{Z}$ 和 $F[x]$ 中, 不可约元都是素元.

证明. 注意到 $\mathbb{Z}$ 中的不可约元就是正的或者负的素数. 根据第一章第五讲引理 7.14, 它们都是素元.

关于多项式的证明类似, 为了复习 Bezout 关系, 我们重述如下. 设 $f \in F[x] \setminus F$ 是不可约元. 设 $g, h \in F[x] \setminus F$ 满足 $f|gh$. 再设 $f \nmid g$. 我们来证明 $f|h$. 设 $r = \gcd(f, g)$. 则存在 $s \in F[x]$ 使得 $f = sr$. 如果 $s \in F$, 则 $f \approx r$. 故 $f|g$. 矛盾. 故 $\deg(s) > 0$. 于是, $\deg(r) < \deg(f)$. 因为 f 不可约, 所以 $\deg(r) = 0$. 我们可以进一步假设 $r = 1$. 根据上一讲推论 4.13, 存在 $u, v \in F[x]$ 使得

$$uf + vg = 1 \Longrightarrow ufh + vgh = h \Longrightarrow f|h. \quad \square$$

5.2 唯一因子分解整环

定义 5.11 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.

由第一章第五讲例 7.11 可知, 每个绝对值大于 1 的整数都有不可约分解.

例 5.12 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 1.6)*. 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 5.13 我们称 D 是唯一因子整环*(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 5.14 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

$$r = r_1 \cdots r_k, \ s = s_1 \cdots s_m, \ t = t_1 \cdots t_n,$$

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

$$r_1 \cdots r_k q = s_1 \cdots s_m t_1 \cdots t_n.$$

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

$$p_2 \cdots p_m = u q_2 q_3 \cdots q_n.$$

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, $q_{n-m-1} \cdots q_n$ 是都是可逆元. 矛盾. 由此可知, $m = n$. □

注解 5.15 在唯一因子分解整环中, 每个非零非可逆元 a 可表示为

$$a = up_1^{m_1} \cdots p_k^{m_k},$$

其中 $u \in U_D$, $p_1, \ldots, p_k$ 是两两互不相伴的不可约元, m_1, $\ldots$, m_k 是正整数. 称之为 a 的标准不可约分解. 再设

$$a = vq_1^{n_1} \cdots q_\ell^{n_\ell},$$

其中 $v \in U_D$, $q_1, \ldots, q_\ell$ 是两两互不相伴的不可约元, n_1, $\ldots$, n_ℓ 是正整数. 则 $k + \ell$, 并适当调整下标后, 我们有 $p_i \approx q_i$ 和 $m_i = n_i$, $i = 1, \ldots, k$.

例 5.16 $44 = 2^2 \cdot 11 = -(-2)^2 \cdot (-11)$.

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

定理 5.17 *(算术学基本定理)* 设 $n \in \mathbb{Z} \setminus \{0, 1, -1\}$. 则存在唯一的两两不同的素数 $p_1, p_2, \ldots, p_m$ 和正整数 i_1, i_2, $\ldots$, i_m 使得

$$n = \pm p_1^{i_1} p_2^{i_2} \cdots p_m^{i_m}.$$

证明. 根据第二章第一讲例 7.13(第 1 页), 引理 5.10 和命题 5.14, $\mathbb{Z}$ 是唯一因子分解整环. 再由引理 5.10 可知, $\mathbb{Z}$ 中的不可约元就是素数. 此外, $\mathbb{Z}$ 中的单位是 ± 1. 故定理成立. □

例 5.18 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

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

定理 5.19 设 $f \in F[x]$. 则存在唯一的两两不相伴的不可约且首一的多项式 $p_1, p_2, \ldots, p_m \in F[x]$, $i_1, i_2, \ldots, i_m \in \mathbb{Z}^+$, $u \in F^*$ 使得

$$f = \mathrm{lc}(f)p_1^{i_1}p_2^{i_2}\cdots p_m^{i_m}.$$

证明. 根据例 5.12, 引理 5.10 和命题 5.14, $F[x]$ 是唯一因子整环. 注意到相伴的非零多项式的首一部分相同. □

推论 5.20 设 $f \in \mathbb{C}[x] \setminus \mathbb{C}$. 则存在唯一的互不相同的复数 $\alpha_1, \ldots, \alpha_k$ 和唯一的正整数 $m_1, \ldots, m_k$ 使得

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

证明. 根据上一讲推论 3.11, $\mathbb{C}[x]$ 中的不可约元都是一次多项式. 故上述定理直接蕴含推论. □

5.3 重数

定义 5.21 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)*.

引理 5.22 设 D 是唯一因子分解整环, $a \in D^*$, $p_1, \ldots, p_k \in D^*$ 是两两互不相伴的不可约元. 设 $p_1, \ldots, p_k$ 在 a 中的重数分别是 $m_1, \ldots, m_k$. 则 $p_1^{m_1} \cdots p_k^{m_k} | a$.

证明. 我们对 k 归纳. 如果 $k = 1$, 则结论即重数的定义. 设 $k > 1$ 且结论对于 $k - 1$ 成立. 于是, 存在 $b \in D^*$ 使得

$$a = \left(p_1^{m_1} \cdots p_{k-1}^{m_{k-1}}\right) b.$$

由素元的定义可知, $p_k \nmid \left(p_1^{m_1} \cdots p_{k-1}^{m_{k-1}}\right)$. 由引理 5.8 可知, $p_k^{m_k} | b$. 由此可知

$$p_1^{m_1} \cdots p_k^{m_k} | a. \quad \square$$

定义 5.23 设 $f \in F[x]^*$ 和 $x-\alpha \in F[x]$. 设 $x-\alpha$ 在 f 中的重数 m 为正. 则称为 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 5.24 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, $m_1 + \cdots + m_s \leq \deg(f)$.

证明. 由定理 5.19 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. 故结论由引理 5.22 直接可得. □

推论 5.25 设 $f \in \mathbb{C}[x] \setminus \mathbb{C}$的所有互不相同的复根是 $\alpha_1, \ldots, \alpha_k$. 这些根的重数是 $m_1, \ldots, m_k$. 则

$$m_1 + \cdots + m_k = \deg(f).$$

证明. 由推论 5.20 和重根的定义直接得出. □

5.4 最大公因子和最小公倍式

命题 5.26 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 $k \geq 1$. 由命题 5.14 可知, q 是素元. 故存在 $s \in \{1, 2, \ldots, m\}$ 使得

$$q \approx p_s.$$

则 $k \leq \min(i_s, j_s)$. 故 $q^k | g$. 由引理 5.22, $d|g$. 故 g 是最大公因子.

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, $p_s^{\max(i_s,j_s)}|h$. 由引理 5.22, $\ell|h$. 即 ℓ 是最小公倍式. □

例 5.27 设 D 是唯一因子分解整环, $a_1, \ldots, a_m, b \in D^*$. 则

$$\gcd(a_1 b, \ldots, a_m b) = \gcd(a_1, \ldots, a_m) b.$$

证明. 设 $g = \gcd(a_1, \ldots, a_m)$. 则 $a_i = c_i g$, 其中 $c_i \in D^*$, $i = 1, 2, \ldots, m$. 于是, $a_i b = c_i g b$. 故 gb 是 $a_1 b, \ldots, a_m b$ 的公因子. 设 d 是 $a_1 b, \ldots, a_m b$ 的公因子, p 是 d 中重数为 m 的因子且 $m > 0$. 再设 p 在 a_i 中的重数是 k_i, $i = 1, 2, \ldots, m$, 和 p 在 b 中的重数是 k. 因为 D 是唯一因子分解整环, 所以

$$m \leq \min(k_1, \ldots, k_m) + k.$$

因为

$$p^{\min(k_1, \ldots, k_m)} | g,$$

所以

$$p^{\min(k_1, \ldots, k_m)+k} | gb \implies p^m | gb.$$

从而 $d|gb$ *(引理 5.22)*. 故

$$\gcd(a_1 b, \ldots, a_m b) = \gcd(a_1, \ldots, a_m) b.$$

5.5 Gauss 引理

定义 5.28 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 $\mathrm{cont}(f, x)$. 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 $\mathrm{pp}(f, x)$.

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

引理 5.29 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

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

和

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

其中 $f_i,g_i\in D$ 且 $f_ng_n\neq 0$. 因为 $f=ag$, 所以 $\mathrm{cont}(f)=\mathrm{cont}(ag)$. 由例 5.27 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 $g\approx\mathrm{pp}(f)$. □

引理 5.30 *(Gauss)* 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

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

和

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

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, $p|f_m g_n$. 由命题 5.14 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 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 $p|f_k \Longrightarrow p|f_k g_\ell$. 如果 $\ell>j$, 则 $p|g_\ell$. 故 $p|f_k g_\ell$. 于是, $p|f_i g_j$. 根据命题 5.14, $p|f_i$ 或 $p|g_j$. 矛盾. □

推论 5.31 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 5.30, $\mathrm{pp}(f)\mathrm{pp}(g)$ 是本原的. 再根据引理 5.29,

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

5.6 Eisenstein 不可约性判别法

定理 5.32 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 5.30 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 5.33 *(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 $p \nmid h_\ell$. 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 5.34 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 *5.33*, 该多项式不可约.

例 5.35 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 5.32)*. 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 *5.33* 可知, $f(x+1)$ 不可约. 故 $f(x)$ 也不可约.

5.7 非UFD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 $(x + y\sqrt{-5}) \mid 3$. 又因为 3 不可约. 不妨设 $x = 3, y = 0$. 故 $d = 9$. 于是,

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

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.