第五章　复数域和多项式

2　整环中的最大公因子和最小公倍式

2.3　一元多项式的最大公因子和最小公倍式

本节中 F 代表域.

命题 2.11 设 $f_1, \ldots, f_n \in F[x]$ 不全为零. 则 $f_1, \ldots, f_n$ 的最大公因子存在. 设 g 是 $f_1, \ldots, f_n$ 最大公因子. 则存在 $a_1, \ldots, a_n \in F[x]$ 使得

$$a_1 f_1 + \cdots + a_n f_n = g. \tag{1}$$

证明. 设 $I = \{u_1 f_1 + \cdots u_n f_n \,|\, u_1, \ldots, u_n \in F[x]\}$. 令 g 是 I 中次数最小的非零多项式. 则存在 $a_1, \ldots, a_n \in F[x]$ 使得 (1) 成立. 我们只要证明 g 是 $f_1, \ldots, f_n$ 的最大公因子.

对任意 $i \in \{1, 2, \ldots, n\}$, 设 $r_i = \mathrm{rem}(f_i, g, x)$. 则

$$f_i = q_i g + r_i,$$

其中 $q_i \in F[x]$. 由 (1) 可知,

$$r_i = f_i - q_i a_1 f_1 - \cdots - q_i a_n f_n \in I.$$

于是, $r_i \in I$. 因为 $\deg(r_i) < \deg(g)$, 所以 $r_i = 0$. 故 $g | f_i$, $i = 1, 2, \ldots, n$. 我们证明了 g 是 $f_1, \ldots, f_n$ 的公因子.

再设 a 是 $f_1, \ldots, f_n$ 的公因子. 由第五章第一讲命题 2.3(ii) 和 (1) 可知, $a|g$. 于是, g 是 $f_1, \ldots, f_n$ 的最大公因子. □

定义 2.12 设 $f, g \in F[x]$ 不全为零. 如果 1 是 f 和 g 的最大公因子, 则称 f 和 g 互素.

定理 2.13 设 $f, g \in F[x]$. 则 f, g 互素当且仅当存在 $u, v \in F[x]$ 使得 $uf + vg = 1$.

证明. 设 f, g 互素. 根据命题 2.11, 存在 $u, v \in F[x]$ 使得 $uf + vg = 1$ (取 $n = 2$). 反之, 设 h 是 f, g 的一个最大公因子. 由第五章第一讲命题 2.3(ii), $h|1$. 故 $h \in F^*$. 从而 $\gcd(f, g) = 1$. □

利用 $F[x]$ 中的除法, 我们可以设计 Euclid 算法来计算两个多项式的最大公因子.

扩展的辗转相除法(Extended Euclidean Algorithm)

输入: $a, b \in F[x]^*$

输出: $g \in F[x]^*$, $u, v \in F[x]$ 使得 $g = \gcd(a, b)$ 和 $ua + vb = g$.

1. [初始化] 令 $r_0 := a$; $r_1 := b$; $i = 1$; $u_0 := 1$; $v_0 := 0$; $u_1 = 0$; $v_1 := 1$;
2. [循环] while $r_i \neq 0$ do
   (a) $i := i + 1$;

(b) $q_i := \mathrm{quo}(r_{i-2}, r_{i-1}, x)$; $r_i := \mathrm{rem}(r_{i-2}, r_{i-1}, x)$;

(c) $u_i := u_{i-2} - q_i u_{i-1}$; $v_i := v_{i-2} - q_i v_{i-1}$;

end do;

3. [准备返回] $g := r_{i-1}$; $u := u_{i-1}$; $v := v_{i-1}$;

4. [返回] return g, u, v;

证明. 首先验证该算法在有限步内必然终止. 注意到算法中的循环产生一个关于余式序列满足:

$$\deg(r_1) > \deg(r_2) > \cdots .$$

因为非零多项式的次数都非负, 所以该序列有限步必然终止. 此时最后一个余式一定是零. 由此可知, 算法终止.

设算法终止于 $r_{k+1} = 0$. 则算法输出为 $g = r_k$ 且 $\mathrm{rem}(r_{k-1}, r_k, x) = 0$. 事实上, 算法产生的商序列

$$q_2, \ldots, q_k, q_{k+1}.$$

两序列之间的关系如下

$$r_{i-2} = q_i r_{i-1} + r_i, \quad i = 2, 3, \ldots, k+1. \tag{2}$$

下面我们来验证 $g = \gcd(a, b)$. 根据 (2), 我们有

$$\begin{cases} r_0 = q_2 r_1 + r_2 \\ r_1 = q_3 r_2 + r_3 \\ \vdots \\ r_{k-4} = q_{k-2} r_{k-3} + r_{k-2} \\ r_{k-3} = q_{k-1} r_{k-2} + r_{k-1} \\ r_{k-2} = q_k r_{k-1} + r_k \\ r_{k-1} = q_{k+1} r_k \end{cases} \tag{3}$$

断言 *1.* 对 $j = 1, 2, \ldots, k$, $g | r_{k-j}$.

断言 *1* 的证明. 对 j 归纳. 当 $j = 1$ 时, 由 (3) 中最后一个方程可知, $g | r_{k-1}$. 设 $j > 1$ 且结论对 $1, 2, \ldots, j-1$ 都成立. 注意到 (3) 中的方程

$$r_{k-j} = q_{k-(j-2)} r_{k-(j-1)} + r_{k-(j-2)}.$$

根据归纳假设, 我们有 $g | r_{k-(j-2)}$ 和 $g | r_{k-(j-1)}$. 再根据上述方程和第五章第一讲命题 2.3(ii) 可知, $g | r_{k-j}$. 断言 1 成立.

该断言蕴含 $g | r_0$ 和 $g | r_1$. 于是, g 是 r_0, r_1 的公因子.

再设 $d \in F[x]^*$ 是 r_0 和 r_1 的公因子.

断言 *2.* 对 $j = 2, 3, \ldots, k$, $d | r_i$, $i = 2, 3, \ldots, k$.

断言 *2* 的证明. 对 i 归纳. 当 $i = 2$ 时, 由 (3) 中第一个方程和第五章第一讲命题 2.3(ii) 可知, $d | r_2$. 设 $i > 2$ 且结论对

$2, 3, \ldots, i-1$ 都成立. 注意到 (3) 中的方程

$$r_{i-2} = q_i r_{i-1} + r_i.$$

由第五章第一讲命题 2.3(ii) 可知, $d|r_i$. 断言 2 成立.

该断言蕴含 $d|r_k$. 于是, $d|g$. 我们得出 $g = \gcd(a, b)$.

最后验证 $ua + vb = g$.

断言 *3.* 对 $i = 0, 1, \ldots, k$, $u_i a + v_i b = r_i$.

断言 *3* 的证明. 对 i 归纳. $i = 0, 1$ 时, u_0, v_0, r_0 和 u_1, v_1, r_1 初始值的设定可知, $u_0 a + v_0 b = r_0$ 和 $u_1 a + v_1 b = r_1$. 设 $i > 2$ 且结论对 $2, 3, \ldots, i-1$ 都成立. 由归纳假设可知:

$$u_{i-2} a + v_{i-2} b = r_{i-2} \quad \text{和} \quad u_{i-1} a + v_{i-1} b = r_{i-1}.$$

于是, $q_i u_{i-1} a + q_i v_{i-1} b = q_i r_{i-1}$. 由此得出,

$$(u_{i-2} - q_i u_{i-1}) a + (v_{i-2} - q_i v_{i-1}) b = r_{i-2} - q_i r_{i-1}.$$

根据扩展 Euclid 算法循环中第 (c) 步和 $r_i = \mathrm{rem}(r_{i-2}, r_{i-1}, x)$ 可知:

$$u_i a + v_i b = r_i.$$

断言 3 成立.

在断言 3 中取 i=k 得 $u_k a + v_k b$=r_k, 即 $ua + vb$=g. □

注解 2.14 如果我们只需要计算两个多项式的最大公因子, 则只需执行算法中红色部分.

例 2.15 设 $f = x^4 + \bar{1}$ 和 $g = x^3 + \bar{1}$ 是 $\mathbb{Z}_2[x]$ 中的多项式. 计算 $\gcd(f, g)$.

解. 设 $r_0 = f$ 和 $r_1 = g$. 则 $r_2 = \mathrm{rem}(r_0, r_1, x) = x + \bar{1}$, $r_3 = \mathrm{rem}(r_1, r_2, x) = \bar{0}$. 故 $\gcd(f, g) = x + \bar{1}$.

例 2.16 设 $f, g \in F[x]^*$. 证明:

$$\mathrm{lcm}(f, g) = \frac{fg}{\gcd(f, g)}.$$

证明. 设 $h = \gcd(f, g)$. 则存在 $a, b \in F[x]$ 使得 $f = ah$ 和 $g = bh$. 则 a, b 互素. 由定理 *2.13*, 存在 $u, v \in F[x]$ 使得

$$ua + vb = 1. \tag{4}$$

注意到

$$\ell := \frac{fg}{\gcd(f, g)} = abh = ag = bf.$$

故 ℓ 是 f 和 g 的公倍式.

再设 q 是 f 和 g 的公倍式. 设 $q = cf = dg$, 其中 $c, d \in F[x]$. 根据 (4), 我们有

$$uaq + vbq = q \implies uadg + vbcf = q \implies ud\ell + vc\ell = q.$$

故 $\ell | q$. 由此可知, $\ell = \mathrm{lcm}(f, g)$.

2.4 核核分解

在本节中: 设 F 是域, $\mathcal{A}$ 代表从坐标空间 F^n 到 F^n 的线性映射, 简称线性算子; $\mathcal{O}$ 代表 F^n 上的零算子, $\mathcal{E}$ 是 F^n 上的恒同算子. 则 五元组 $(\mathrm{Hom}(F^n, F^n), +, \mathcal{O}, \circ, \mathcal{E})$ 是环, 它同构于矩阵环 $(\mathrm{M}_n(F), +, O, \cdot, E)$. 特别地, $F[\mathcal{A}]$ 是 $\mathrm{Hom}(F^n, F^n)$ 的交换子环. 它同构于 $F[A]$, 其中 A 是线性算子 $\mathcal{A}$ 在标准基下的矩阵.

定理 2.17 设 $\mathcal{A} \in \mathrm{Hom}(F^n, F^n)$, $f \in F[t]$ 且 $f(\mathcal{A}) = \mathcal{O}$. 再设 $f = pq$, 其中 $p, q \in F[t]$ 且 $\gcd(p, q) = 1$. 则

$$\ker(p(\mathcal{A})) \oplus \ker(q(\mathcal{A})) = F^n.$$

证明. 因为 $\gcd(p, q) = 1$, 所以存在 $u, v \in F[t]$ 使得

$$up + vq = 1.$$

于是,

$$u(\mathcal{A})p(\mathcal{A}) + v(\mathcal{A})q(\mathcal{A}) = \mathcal{E}. \tag{5}$$

设 $\mathbf{v} \in \ker(p(\mathcal{A})) \cap \ker(q(\mathcal{A}))$. 根据 (5), 我们有

$$\left(u(\mathcal{A})p(\mathcal{A}) + v(\mathcal{A})q(\mathcal{A})\right)(\mathbf{v}) = \mathcal{E}(\mathbf{v}).$$

故

$$u(\mathcal{A})p(\mathcal{A})(\mathbf{v}) + v(\mathcal{A})q(\mathcal{A})(\mathbf{v}) = \mathbf{v} \implies \mathbf{0} = \mathbf{v}.$$

于是, $\ker(p(\mathcal{A})) \cap \ker(q(\mathcal{A})) = \{\mathbf{0}\}$.

设 $\mathbf{x} \in F^n$. 令 $\mathbf{y} = u(\mathcal{A})p(\mathcal{A})(\mathbf{x})$ 和 $\mathbf{z} = v(\mathcal{A})q(\mathcal{A})(\mathbf{x})$. 则 (5) 蕴含 $\mathbf{y} + \mathbf{z} = \mathbf{x}$. 注意到:

$$\begin{aligned} q(\mathcal{A})(\mathbf{y}) &= q(\mathcal{A})u(\mathcal{A})p(\mathcal{A})(\mathbf{x}) \quad (\mathbf{y} \text{ 的定义}) \\ &= u(\mathcal{A})q(\mathcal{A})p(\mathcal{A})(\mathbf{x}) \quad (F[\mathcal{A}] \text{ 是交换环}) \\ &= u(\mathcal{A})f(\mathcal{A})(\mathbf{x}) \quad (f = pq)) \\ &= u(\mathcal{A})\mathcal{O}(\mathbf{x}) \quad (f(\mathcal{A}) = \mathcal{O}) \\ &= \mathbf{0}. \end{aligned}$$

故 $\mathbf{y} \in \ker(q(\mathcal{A})$. 同理 $\mathbf{z} \in \ker(p(\mathcal{A}))$. 于是,

$$\ker(q(\mathcal{A})) + \ker(p(\mathcal{A})) = F^n.$$

综上所述, $\ker(p(\mathcal{A})) \oplus \ker(q(\mathcal{A})) = F^n$. □

推论 2.18 设 $A \in \mathrm{M}_n(F)$, $f \in F[t]$ 且 $f(A) = O$. 再设 $f = pq$, 其中 $p, q \in F[t]$ 且 $\gcd(p, q) = 1$. 则

$$\mathrm{sol}(p(A)\mathbf{x} = \mathbf{0}) \oplus \mathrm{sol}(q(A)\mathbf{x} = \mathbf{0}) = F^n,$$

其中 $\mathbf{x} = (x_1, \ldots, x_n)^t$ 是未知向量. 特别地,

$$\mathrm{rank}(p(A)) + \mathrm{rank}(q(A)) = n.$$

证明. 设线性算子

$$\begin{array}{rccc} \mathcal{A}: & F^n & \longrightarrow & F^n \\ & \mathbf{v} & \mapsto & A\mathbf{v}. \end{array}$$

则 $\ker(p(\mathcal{A}))$=sol$(p(A)\mathbf{x}=\mathbf{0})$ 和 $\ker(q(\mathcal{A}))$=sol$(q(A)\mathbf{x}=\mathbf{0})$. 由上述定理

$$\mathrm{sol}(p(A)\mathbf{x}=\mathbf{0}) \oplus \mathrm{sol}(q(A)\mathbf{x}=\mathbf{0}) = F^n.$$

根据第二章第二讲例 2.17,

$$\dim(\mathrm{sol}(p(A)\mathbf{x}=\mathbf{0})) + \dim(\mathrm{sol}(q(A)\mathbf{x}=\mathbf{0})) = n.$$

再根据对偶定理(第二章第三讲定理 4.6),

$$\mathrm{rank}(p(A)) + \mathrm{rank}(q(A)) = n. \quad \square$$

例 2.19 设 $\mathrm{char}(F) \neq 2$, $A \in \mathrm{M}_n(F)$ 满足 $A^2 = E$. 证明:

$$\mathrm{rank}(A+E) + \mathrm{rank}(A-E) = n.$$

证明. 设 $f(x) = x^2-1 = \underbrace{(x-1)}_{p}\underbrace{(x+1)}_{q}$. 因为 $\mathrm{char}(F) \neq 2$. 所以 $\gcd(x-1, x+1) = 1$. 又因为 $f(A) = A^2 - E = O$. 由上述推论可知,

$$\mathrm{rank}(p(A)) + \mathrm{rank}(q(A)) = n.$$

即

$$\mathrm{rank}(A+E) + \mathrm{rank}(A-E) = n.$$

当 $\mathrm{char}(F) = 2$ 时, 上例中的结论一般不成立. 例如: 设 $E_2 \in \mathrm{M}_2(\mathbb{Z}_2)$. 则 $E_2^2 = E_2$. 但 $E_2 + E_2 = E_2 - E_2 = O_2$.

3 唯一因子分解整环

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

3.1 素元和不可约元

定义 3.1 设 $a \in D^*$ 不可逆. 如果对于任意 $b, c \in D^*$,

$$a|bc \implies a|b \text{ 或 } a|c.$$

则称 a 是素元 *(prime element)*. 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)*.

引理 3.2 整环中的素元都是不可约元.

证明. 设 $a \in D^*$ 是素元, 且存在 $b, c \in D^*$ 使得 $a = bc$. 则 $a|b$ 或 $a|c$. 不妨设 $a|b$. 则存在 $q \in D^*$ 使得 $b = qa$. 故 $a = aqc$. 由整环中的消去律(第四章第三讲推论 3.25)可知, $1 = qc$. 故 c 可逆. 由此推出 a 不可约. □.

注解 3.3 上述命题的逆命题不成立. 我们将在介绍复数域时给出例子.

引理 3.4 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. 根据第二章第一讲引理 7.16 (第一页), 每个正的或者负的素数都是素元.

关于多项式的证明与第二章第一讲引理 7.16 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 $\deg(r) = 0$. 由第五章第一讲命题 2.9 (i) 可知, 我们可以进一步假设 $r = 1$. 根据定理 2.13, 存在 $u, v \in F[x]$ 使得

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

引理 3.5 *设 $a \in D^*$ 是不可约元(素元), 且 $\tilde{a} \approx a$. 则 $\tilde{a}$ 也是不可约元(素元).*

证明. 设 a 是不可约元且 $\tilde{a} = bc$. 其中 $b, c \in D$. 则 $a = (ub)c$, 其中 $u \in U_D$. 于是, ub 和 c 中至少有一个是可逆元. 故 b, c 中有一个是可逆元.

素元情形可以类似证明. $\square$

引理 3.6 *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, $p^k|a$. □

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.

由第二章第一讲例 7.13 (第一页)和引理 3.2 可知, 每个绝对值大于 1 的整数都有不可约分解.

例 3.8 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 3.9 设 D 整环. 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 3.10 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, $q_{n-m-1} \cdots q_n$ 是都是可逆元. 矛盾. 由此可知, $m = n$. □

定理 3.11 *(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 3.4 和命题 3.10, $\mathbb{Z}$ 是唯一因子分解整环. 再由引理 3.4 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 3.12 $44 = 2^2 \cdot 11$, $-45 = -3^2 \cdot 9$.

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

定理 3.13 设 $f \in F[x]$. 则存在两两互素的不可约多项式 $p_1, p_2, \ldots, p_m \in F[x]$, $i_1, i_2, \ldots, i_m \in \mathbb{Z}^+$, $u \in F^*$ 使得

$$f = up_1^{i_1} p_2^{i_2} \cdots p_m^{i_m}.$$

进而, $p_1, p_2, \ldots, p_m$ 在相伴意义下唯一, $i_1, i_2, \ldots, i_m$ 唯一.

证明. 根据例 3.8, 引理 3.4 和命题 3.10, $F[x]$ 是唯一因子整环. 把 f 的相伴不可约因子取成相同的代表元, 则

$$f = up_1^{i_1} p_2^{i_2} \cdots p_m^{i_m},$$

其中 $u \in F^*, p_1, p_2, \ldots, p_m$ 是 $F[x]$ 中两两互不相伴的不可约因子. 于是, 这些因子两两互素. □

例 3.14 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

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

例 3.15 设 $g = x^2 - 2 \in \mathbb{Q}[x] \subset \mathbb{R}[x]$. 则 g 在 $\mathbb{Q}[x]$ 中不可约. 但

$$g = (x - \sqrt{2})(x + \sqrt{2}).$$

故 g 在 $\mathbb{R}[x]$ 中可约.

3.3 重数

定义 3.16 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 3.17 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 3.6 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 3.18 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 3.19 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 3.13 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 3.17 直接可得. $\square$

命题 3.20 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 3.10 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, $k \leq \min(i_1, j_1)$. 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. □

由上述命题和第五章第一讲推论 2.10 可知, 唯一因子分解整环中有限个非零元素的最大公因子和最小公倍式都存在.

例 3.21 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 $g = \gcd(a_1, \ldots, a_m)$. 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

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

从而 $d | gb$. 故

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