第五章　复数域和多项式

2　整环中的因子和倍式

记号. 在本节中, 设 D 是整环. 则 $D^* = D \setminus \{0\}$ 和 U_D 是 D 中所有可逆元的集合. 由第四章第三讲命题 3.24, U_D 关于 D 中的乘法是交换群.

2.1　整除和相伴

定义 2.1 设 $a \in D^*$ 和 $b \in D$. 如果存在 $c \in D$ 使得

$$b = ca,$$

则称 a 是 b 的因子*(divisor)*, b 是 a 的倍式*(multiple)*. 此时, 我们称 a 在 D 中整除 b, 记为 $a|b$.

例 2.2 在 $\mathbb{Z}$ 中, $2|4$ 但 $2 \nmid 5$. 在 $\mathbb{Q}[x]$ 中, $(x+1)|(x^2-1)$ 但 $(x+1) \nmid (x^2+1)$. 在 $\mathbb{Z}_2[x]$ 中, $(x+\bar{1})|(x^2+\bar{1})$ *(Freshmen's dream)*.

命题 2.3 设 $a, b \in D^*$, $c, f, g \in D$. 则

(i) 如果 $a|b$ 和 $b|c$, 则 $a|c$;

(ii) 如果 $a|f$ 和 $a|g$, 则对任意 $u, v \in D$, $a|(uf+vg)$.

证明. (i) 设 $b = pa$ 和 $c = qb$, 其中 $p, q \in D^*$. 则 $c = (qp)a$. 于是, $a|c$. (ii) 与第一章第四讲引理 7.1 的证明类似. □

定义 2.4 设 $a, b \in D$. 如果存在 $u, v \in U_D$ 使得 $ua = vb$, 则称 a 和 b 在 D 上相伴, 记为 $a \approx b$.

下面验证 $\approx$ 是等价关系. 对任意 $a \in D$, $1a{=}1a \implies a{\approx}a$. 自反性成立. 设 $a \approx b$. 则存在 $u, v \in U$ 使得 $ua = vb$. 故 $vb = ua$. 于是, $b \approx a$. 对称性成立. 设 $a \approx b$ 和 $b \approx c$. 则存在 $s, t, u, v \in U$ 使得 $sa = tb$ 和 $ub = vc$. 于是

$$usa = utb = tvc.$$

因为 U_D 是群, 所以 $us, tv \in U_D$. 故 $a \approx c$. 传递性成立.

例 2.5 在 $\mathbb{Z}$ 中, $U_{\mathbb{Z}} = \{1, -1\}$. 故 $a \approx b \iff a = \pm b$. 设 F 是域. 则 $U_{F[x]} = F^*$. 故在 $F[x]$ 中,

$$f \approx g \iff \exists\ \alpha, \beta \in F^*,\ \alpha f = \beta g.$$

特别地, 当 $f \neq 0$ 时, $f \approx \mathrm{lc}(f)^{-1} f$. 这里, $\mathrm{lc}(f)^{-1} f$ 是首项系数等于 *1* 的多项式, 简称首一多项式*(monic polynomial)* 而 $\mathrm{lc}(f)^{-1} f$ 称为 f 的首一部分.

例 2.6 设 $f, g \in F[x]^*$. 证明*:* $f \approx g$ 当且仅当 f 和 g 的首一部分相同.

证明. 设 $f \approx g$. 则存在 $u, v \in F^*$ 使得 $uf = vg$. 则

$$f = u^{-1}vg \Longrightarrow \mathrm{lc}(f) = u^{-1}v\mathrm{lc}(g)$$
$$\Longrightarrow \mathrm{lc}(f)^{-1}f = (u^{-1}v)^{-1}\mathrm{lc}(g)^{-1}(u^{-1}v)g = \mathrm{lc}(g)^{-1}g.$$

故 f 和 g 的首一部分相同.

反之, 我们有 $\mathrm{lc}(f)^{-1}f = \mathrm{lc}(g)^{-1}g$. 故 $f \approx g$. □

命题 2.7 设 $a, b \in D^*$. 则 $a \approx b$ 当且仅当 $a|b$ 和 $b|a$ 同时成立.

证明. 设 $a \approx b$. 则存在 $u, v \in U_D$ 使得 $ua = vb$. 则 $a = u^{-1}vb$. 故 $b|a$. 同理, $a|b$.

反之, 设 $b|a$ 和 $a|b$. 则存在 $c, d \in D^*$ 使得 $a = cb$ 和 $b = da$. 则 $a = cda$. 由整环中的消去律(第四章第二讲推论 3.24)可知, $cd = 1$. 故 $c, d \in U_D$, 即 $a \approx b$. □

2.2 最大公因子和最小公倍式

定义 2.8 设 $a, b_1, \ldots, b_n \in D^*$. 如果 a 是每个 $b_1, \ldots, b_n$ 的因子, 则称 a 是 $b_1, \ldots, b_n$ 的一个公因子. 再设 g 是 $b_1, \ldots, b_n$ 的一个公因子. 如果对于 $b_1, \ldots, b_n$ 的任意公因子 a, 我们有 $a|g$. 则称 g 是 $b_1, \ldots, b_n$ 的一个最大公因子.

设 $c, d_1, \ldots, d_n \in D^*$. 如果 c 是每个 $d_1, \ldots, d_n$ 的倍式, 则称 c 是 $d_1, \ldots, d_n$ 的一个公倍式. 再设 ℓ 是 $d_1, \ldots, d_n$

的一个公倍式. 如果对于 $d_1, \ldots, d_n$ 的任意公因子 c, 我们有 $\ell | c$. 则称 ℓ 是 $d_1, \ldots, d_n$ 的一个最小公倍式.

命题 2.9 设 $b_1, \ldots, b_n \in D^*$.

(i) 设 g 是 $b_1, \ldots, b_n$ 的最大公因子. 则 $h \in D^*$ 也是 $b_1, \ldots, b_n$ 的最大公因子当且仅当 $h \approx g$.

(ii) 设 ℓ 是 $b_1, \ldots, b_n$ 的最小公倍式, 则 $h \in D^*$ 也是 $b_1, \ldots, b_n$ 的最小公倍式当且仅当 $h \approx \ell$.

证明. (i) 设 h 也是 $b_1, \ldots, b_n$ 的最大公因子. 则 $g|h$ 且 $h|g$. 则命题 2.7 蕴含 $g \approx h$.

反之, 设 $h \approx g$. 则命题 2.7 蕴含 $h|g$ 和 $g|h$. 因为 $g|b_i$, 所以 $h|b_i$ (命题 2.3 (i)). 故 h 是 $b_1, \ldots, b_n$ 的公因子. 再设 d 是 $b_1, \ldots, b_n$ 的公因子. 则 $d|g$. 于是, $d|h$. 故 h 是 $b_1, \ldots, b_n$ 的最大公因子.

(ii) 设 h 也是 $b_1, \ldots, b_n$ 的最小公倍式. 则 $\ell|h$ 且 $h|\ell$. 则命题 2.7 蕴含 $g \approx \ell$. 反之, 设 $h \approx \ell$. 则命题 2.7 蕴含 $h|\ell$ 和 $\ell|h$. 因为 $b_i|\ell$, 所以 $b_i|h$ (命题 2.3 (i)). 故 h 是 $b_1, \ldots, b_n$ 的公倍式. 再设 q 是 $b_1, \ldots, b_n$ 的公倍式. 则 $\ell|q$. 于是, $h|q$. 故 h 是 $b_1, \ldots, b_n$ 的最小公倍式. □

如果 $b_1, \ldots, b_n \in D^*$ 的最大公因子存在, 则它们的最大公因子记为 $\gcd(b_1, \ldots, b_n)$. 该记号在相伴的意义下是唯一的. 类似地, 如果 $b_1, \ldots, b_n \in D^*$ 的最小公倍式存在,

则它们的最小公倍式记为 $\operatorname{lcm}(b_1,\ldots,b_n)$. 该记号在相伴的意义下也是唯一的.

由第一章第四讲可知 $\mathbb{Z}$ 中的有限个非零元的最大公因子和最小公倍式都存在. 它们的最大公因子和最小公倍式通常是指正的整数.

下面的推论说明多个元素的最大公因子和最小公倍式的计算可以化成两个元素的情形.

推论 2.10 *设 D 中任意有限多个非零元都有最大公因子(最小公倍式). 设 $b_1,\ldots,b_n \in D^*$, 其中 $n>2$. 则*

$$\gcd(b_1,\ldots,b_n)=\gcd(b_1,\gcd(b_2,\ldots,b_n))$$

$$(\ \operatorname{lcm}(b_1,\ldots,b_n)=\operatorname{lcm}(b_1,\operatorname{lcm}(b_2,\ldots,b_n))\ ).$$

证明. 设 $g=\gcd(b_1,\ldots,b_n)$ 和 $h=\gcd(b_1,\gcd(b_2,\ldots,b_n))$. 则 g 是 $b_2,\ \ldots,\ b_n$ 的公因子. 故 $g|\gcd(b_2,\ldots,b_n)$. 于是, g 是 b_1 和 $\gcd(b_2,\ldots,b_n)$ 的公因子. 由此得出 $g|h$. 类似地, $h|b_i,\ i=1,2,\ldots,n$. 故 $h|g$. 根据命题 2.7, $g\approx h$. 于是, $h=\gcd(b_1,\ldots,b_n)$ (命题 2.9).

关于最小公倍式的结论类似可证. □

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) $u_i:=u_{i-2}-q_iu_{i-1};\ v_i:=v_{i-2}-q_iv_{i-1};$

   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

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

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 $i=0,1,\ldots,k$, $u_ia+v_ib=r_i$.

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, $u_0a+v_0b=r_0$ 和 $u_1a+v_1b=r_1$. 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

定理 2.17 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. 记 $V_p = \mathrm{sol}(p(A)\mathbf{x} = \mathbf{0})$ 和 $V_q = \mathrm{sol}(q(A)\mathbf{x} = \mathbf{0})$. 因为 $\gcd(p,q) = 1$, 所以存在 $u, v \in F[t]$ 使得

$$u(t)p(t) + v(t)q(t) = 1.$$

于是,

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

设 $\mathbf{v} \in V_p \cap V_q$. 根据 (5), 我们有

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

故

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

于是, $V_p \cap V_q = \{\mathbf{0}\}$.

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

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

故 $\mathbf{v} \in V_q$. 同理 $\mathbf{w} \in V_p$. 综上所述, $V_p \oplus V_q = F^n$.

根据第二章第二讲例 2.17, $\dim(V_p) + \dim(V_q) = n$. 再利用对偶定理得 $n - \operatorname{rank}(p(A)) + n - \operatorname{rank}(q(A)) = n$. 故

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

例 2.18 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 $f(A) = A^2 - E = O$. 由上述定理可知, $\mathrm{rank}(p(A)) + \mathrm{rank}(q(A)) = n$. 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 $E_2 + E_2 = E_2 - E_2 = O_2$.

设 $\phi \in \mathrm{Hom}(F^n, F^n)$ 和 $f \in F[t]$. 令

$$f(t) = f_m t^m + f_{m-1} t^{m-1} + \cdots + f_1 t + f_0,$$

其中 $f_m, f_{m-1}, \ldots, f_1, f_0 \in F$. 则

$$f(\phi) = f_m \phi^m + f_{m-1} \phi^{m-1} + \cdots + f_1 \phi + f_0 \mathcal{E},$$

其中 $\mathcal{E}$ 代表从 F^n 到 F^n 的恒同映射.

定理 2.19 设 $\phi \in \mathrm{Hom}(F^n, F^n)$, $f \in F[t]$ 且 $f(\phi) = \mathcal{O}$, 其中 $\mathcal{O}$ 代表从 F^n 到 F^n 的零映射. 再设 $f = pq$, 其中 $p, q \in F[t]$ 且 $\gcd(p, q) = 1$. 则

$$\ker(p(\phi)) \oplus \ker(q(\phi)) = F^n.$$

证明. 设 A 是线性映射 $\phi : F^n \to F^n$ 在标准基下的矩阵. 则

$$\ker(p(\phi)) = \mathrm{sol}(p(A)\mathbf{x} = \mathbf{0}) \quad 和 \quad \ker(q(\phi)) = \mathrm{sol}(q(A)\mathbf{x} = \mathbf{0}).$$

于是, 定理 2.17 蕴含定理 2.19. □

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

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