第五章　复数域和多项式

3　复数

3.4　代数学基本定理

定理 3.7 *(代数学基本定理)* 设 $f \in \mathbb{C}[x] \setminus \mathbb{C}$. 则 f 在 $\mathbb{C}$ 中有根.

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.

首先我们定义不可约多项式的概念.

定义 3.8 设 F 是域, $f \in F[x] \setminus F$. 如果存在 $g, h \in F[x] \setminus F$ 使得 $f = gh$, 则称 f 是 $F[x]$ 中的可约*(reducible)*多项式, 也称 f 在 F 上可约. 否则称 f 是 $F[x]$ 中的不可约*(irreducible)*多项式, 也称 f 在 F 上不可约.

显然, 一次多项式在它系数所在的域上都是不可约的.

例 3.9 设 $f = x^2 - 2$ 和 $g = x^2 + 2$.

- 如果把 f, g 看成 $\mathbb{Q}[x]$ 中的多项式, 则它们都是不可约的.
- 如果把 f, g 看成 $\mathbb{R}[x]$ 中的多项式, 则

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

是可约的, 但 g 仍不可约.

- 如果把 g 看成 $\mathbb{C}[x]$ 中的多项式, 则

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

是可约的. 因为 $\mathbb{R}[x] \subset \mathbb{C}[x]$, 所以 f 在 $\mathbb{C}$ 上也可约.

- 如果把 f, g 看成 $\mathbb{Z}_2[x]$ 中的多项式, 则 $f = g = x^2$. 故它们都是可约的.

引理 3.10 设 F 是域, $f \in F[x] \setminus F$. 则存在一次多项式 $g \in F[x]$ 满足 $\mathrm{rem}(f, g, x) = 0$ 当且仅当 f 在 F 中有根.

证明. 设 $\alpha \in F$ 满足 $f(\alpha) = 0$. 根据余式定理(上学期第五章第一讲定理 1.21), $\mathrm{rem}(f, x - \alpha) = f(\alpha) = 0$.

设 $f = (\alpha x - \beta)q$, 其中 $\alpha, \beta \in F$, $\alpha \neq 0$ 和 $q \in F[x]$. 则 $-\beta/\alpha$ 是 f 的根. □

推论 3.11 设 $f \in \mathbb{C}[x] \setminus \mathbb{C}$. 如果 f 在 $\mathbb{C}$ 上不可约, 则 $\deg(f) = 1$.

证明. 根据代数学基本定理, 存在 $\alpha \in \mathbb{C}$ 使得 $f(\alpha) = 0$. 由引理 3.10, 存在 $g \in \mathbb{C}[x]$ 使得

$$f = (x - \alpha)g.$$

因为 f 不可约, 所以 $g \in \mathbb{C} \setminus \{0\}$. 由此得出 $\deg(f) = 1$. □

推论 3.12 设 $f \in \mathbb{R}[x] \setminus \mathbb{R}$. 如果 f 在 $\mathbb{R}$ 上不可约, 则 $\deg(f) \leq 2$.

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 有复根 α. 注意到 $\alpha \notin \mathbb{R}$. 否则引理 3.10 蕴含 f 在 $\mathbb{R}$ 上可约, 与 f 的不可约性矛盾. 特别地, $\bar{\alpha} \neq \alpha$.

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 有两个互不相同的复根 α 和 $\bar{\alpha}$.

令 $g(x) = (x - \alpha)(x - \bar{\alpha})$. 则 $g \in \mathbb{R}[x]$. 由多项式除法可知, 存在 $q, r \in \mathbb{R}[x]$ 使得

$$f(x) = q(x)g(x) + r(x)$$

且 $\deg(r) \leq 1$. 于是, $r(\alpha) = r(\bar{\alpha}) = 0$. 故 $r = 0$. 我们得到 f 在 $\mathbb{R}$ 上可约, 矛盾. □

3.5 复数应用举例

例 3.13 设循环矩阵

$$A=\begin{pmatrix} a_0 & a_1 & \cdots & a_{n-2} & a_{n-1} \\ a_{n-1} & a_0 & \cdots & a_{n-3} & a_{n-2} \\ a_{n-2} & a_{n-1} & \cdots & a_{n-4} & a_{n-3} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ a_1 & a_2 & \cdots & a_{n-1} & a_0 \end{pmatrix} \in \mathrm{M}_n(\mathbb{R}).$$

计算 A 的行列式. 当矩阵 A 可逆时, 求 A^{-1}.

解. 设 $\epsilon_0,\ldots,\epsilon_{n-1}$ 是 n 个 n 次单位根. 令

$$f=a_0+a_1x+\cdots+a_{n-2}x^{n-2}+a_{n-1}x^{n-1}\in\mathbb{C}[x].$$

对 $k\in\{0,1,\ldots,n-1\}$, 利用 $\epsilon_k^n=1$ 得到

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

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

$$\epsilon_k^2 f(\epsilon_k)=a_{n-2}+a_{n-1}\epsilon_k+\cdots+a_{n-4}\epsilon_k^{n-2}+a_{n-3}\epsilon_k^{n-1},$$

$$\vdots$$

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

利用矩阵写成

$$f(\epsilon_k)\begin{pmatrix}1\\ \epsilon_k\\ \epsilon_k^2\\ \vdots\\ \epsilon_k^{n-1}\end{pmatrix}=A\begin{pmatrix}1\\ \epsilon_k\\ \epsilon_k^2\\ \vdots\\ \epsilon_k^{n-1}\end{pmatrix},\quad k=0,1,\ldots,n-1.$$

设

$$V=\begin{pmatrix}1 & 1 & \cdots & 1\\ \epsilon_0 & \epsilon_1 & \cdots & \epsilon_{n-1}\\ \vdots & \vdots & \ddots & \vdots\\ \epsilon_0^{n-1} & \epsilon_1^{n-1} & \cdots & \epsilon_{n-1}^{n-1}\end{pmatrix}.$$

则 $V\mathrm{diag}(f(\epsilon_0),\ldots,f(\epsilon_{n-1}))=AV$. 由 *Vandermonde* 行列式可知, V 可逆. 故

$$A=V\mathrm{diag}(f(\epsilon_0),\ldots,f(\epsilon_{n-1}))V^{-1}.$$

两边取行列式得

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

而 A 可逆当且仅当任何 n 次单位根都不是 f 的根. 此时,

$$A^{-1}=V\mathrm{diag}(f(\epsilon_0)^{-1},\ldots,f(\epsilon_{n-1})^{-1})V^{-1}.$$

例 3.14 设

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

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)*, 称为 *Hamilton* 四元数系.

验证如下:

(i) 设 $W=\begin{pmatrix} u & v \\ -\bar{v} & \bar{u} \end{pmatrix}$ 和 $Z=\begin{pmatrix} x & y \\ -\bar{y} & \bar{x} \end{pmatrix}$, 其中 $u,v,x,y\in\mathbb{C}$.

我们有

$$W-Z=\begin{pmatrix} u-x & v-y \\ -\bar{v}+\bar{y} & \bar{u}-\bar{x} \end{pmatrix}=\begin{pmatrix} u-x & v-y \\ -\overline{v-y} & \overline{u-x} \end{pmatrix}\in H.$$

故 $(H,+,O)$ 是 $(\mathrm{M}_2(\mathbb{C}),+,O)$ 的子群.

计算

$$WZ=\begin{pmatrix} ux-v\bar{y} & uy+v\bar{x} \\ -\bar{v}x-\bar{u}\bar{y} & -\bar{v}y+\bar{u}\bar{x} \end{pmatrix}=\begin{pmatrix} ux-v\bar{y} & uy+v\bar{x} \\ -\overline{(uy+v\bar{x})} & \overline{ux-v\bar{y}} \end{pmatrix}\in H.$$

注意到

$$E_2=\begin{pmatrix} 1 & 0 \\ -\bar{0} & \bar{1} \end{pmatrix}\in H.$$

故 H 是 $\mathrm{M}_2(\mathbb{C})$ 的子环.

(ii) 设 $A=\begin{pmatrix} \mathbf{i} & 0 \\ 0 & -\mathbf{i} \end{pmatrix}$ 和 $B=\begin{pmatrix} 0 & \mathbf{i} \\ \mathbf{i} & 0 \end{pmatrix}$. 则 $A,B\in H$.

直接计算得

$$AB=\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix},\quad BA=\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

因为 $AB \neq BA$, 所以 H 不是交换环.

(iii) 设 $W \neq O$. 则 $\det(W) = |u|^2 + |v^2| \neq 0$. 故 W 是可逆矩阵. 在 $\mathrm{M}_n(\mathbb{C})$ 中,

$$W^{-1} = \frac{1}{u\bar{u} + v\bar{v}} \begin{pmatrix} \bar{u} & -v \\ \bar{v} & u \end{pmatrix} \in H.$$

故 W 在 H 中可逆.

4 整环中的最大公因子和最小公倍式

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 3.21, U_D 关于 D 中的乘法是交换群.

4.1 整除和相伴

定义 4.1 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 4.2 在 $\mathbb{Z}$ 中, $2 \mid 4$ 但 $2 \nmid 5$. 在 $\mathbb{Q}[x]$ 中, $(x+1) \mid (x^2-1)$ 但 $(x+1) \nmid (x^2+1)$. 在 $\mathbb{Z}_2[x]$ 中, $(x+\bar{1}) \mid (x^2+\bar{1})$ *(Freshmen's dream)*.

命题 4.3 设 $a, b \in D^*$, $c, f, g \in D$. 则

(i) 如果 $a \mid b$ 和 $b \mid c$, 则 $a \mid c$;

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

证明. (i) 设 $b = pa$ 和 $c = qb$, 其中 $p, q \in D^*$. 则 $c = (qp)a$. 于是, $a \mid c$. (ii) 与第一章第五讲引理 7.1 的证明类似. □

定义 4.4 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 4.5 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 4.6 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 4.7 设 $a, b \in D^*$. 则 $a \approx b$ 当且仅当 $a \mid b$ 和 $b \mid a$ 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 $b \mid a$. 同理, $a \mid b$.

反之, 设 $b \mid a$ 和 $a \mid b$. 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(第四章第三讲推论 3.23)可知, $cd = 1$. 故 $c, d \in U_D$, 即 $a \approx b$. □

4.2 最大公因子和最小公倍式

定义 4.8 设 $a \in D^*$, $b_1, \ldots, b_n \in D$. 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, 有 $a \mid g$. 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 $d_1, \ldots, d_n$ 的任意公倍式 c, 我们有 $\ell \mid c$. 则称 ℓ 是 $d_1, \ldots, d_n$ 的一个最小公倍式.

命题 4.9 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 $g \mid h$ 且 $h \mid g$. 则命题 4.7 蕴含 $g \approx h$.

反之, 设 $h \approx g$. 则命题 4.7 蕴含 $h \mid g$ 和 $g \mid h$. 因为 $g \mid b_i$, 所以 $h \mid b_i$ (命题 4.3 (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 $d \mid g$. 于是, $d \mid h$. 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 $\ell \mid h$ 且 $h \mid \ell$. 则命题 4.7 蕴含 $h \approx \ell$. 反之, 设 $h \approx \ell$. 则命题 4.7 蕴含 $h \mid \ell$ 和 $\ell \mid h$. 因为 $b_i \mid \ell$, 所以 $b_i \mid h$ (命题 4.3 (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 $\ell \mid q$. 于是, $h \mid q$. 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 4.10 *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*

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

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

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 $g \mid \gcd(b_2, \ldots, b_n)$. 于是, g 是 g_1 和 $\gcd(b_2, \ldots, b_n)$ 的公因子. 由此得出 $g \mid h$. 类似地, $h \mid b_i$, $i = 1, 2, \ldots, n$. 故 $h \mid g$. 根据命题 4.7, $g \approx h$. 于是, $h = \gcd(b_1, \ldots, b_n)$ (命题 4.9).

关于最小公倍式的结论类似可证. □

4.3 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 4.11 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 $I = \{u_1 f_1 + \cdots + u_n f_n \mid u_1, \ldots, u_n \in F[x]\}$. 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 $g \mid f_i$, $i = 1, 2, \ldots, n$. 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. 由命题 4.3 和 (1) 可知, $a \mid g$. 于是, g 是 $f_1, \ldots, f_n$ 的最大公因子. □

定义 4.12 设 $f, g \in F[x]$ 不全为零. 如果 $\gcd(f, g) = 1$, 则称 f 和 g 互素.

推论 4.13 设 $f, g \in F[x]$ 不全为零. 则 f, g 互素当且仅当存在 $u, v \in F[x]$ 使得

$$uf + vg = 1.$$

证明. 又命题 4.11 可知, f, g 互素蕴含存在 $u, v \in F[x]$ 使得

$$uf + vg = 1.$$

反之, 命题 4.3 (ii) 蕴含 $\gcd(f, g)|1$. □

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 $j = 1, 2, \ldots, k$, $g \mid r_{k-j}$.

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, $g \mid r_{k-1}$. 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 $g \mid r_{k-(j-2)}$ 和 $g \mid r_{k-(j-1)}$. 再根据上述方程和第五章第一讲命题 2.3(ii) 可知, $g \mid r_{k-j}$. 断言 1 成立.

该断言蕴含 $g \mid r_0$ 和 $g \mid r_1$. 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 $j = 2, 3, \ldots, k$, $d \mid r_i$, $i = 2, 3, \ldots, k$.

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, $d \mid r_2$. 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, $d \mid r_i$. 断言 2 成立.

该断言蕴含 $d \mid r_k$. 于是, $d \mid g$. 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 4.14 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 4.15 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 4.16 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. 由命题 *4.11*, 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 $\ell \mid q$. 由此可知, $\ell = \operatorname{lcm}(f, g)$.

4.4 核核分解

在本节中: 设 F 是域, 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 $(\operatorname{Hom}(F^n, F^n), +, \mathcal{O}, \circ, \mathcal{E})$ 是环.

在上学期第二章第四讲中我们定义了映射

$$\begin{aligned} \Psi : \ \mathrm{M}_n(F) &\longrightarrow \operatorname{Hom}(F^n, F^n) \\ A &\mapsto \phi_A =: \mathcal{A}, \end{aligned}$$

其中 $\mathcal{A}$ 是以 A 为矩阵的线性算子, 并证明了 Ψ 是双射. 由矩阵运算的定义可知 Ψ 是环同构.

令

$$F[\mathcal{A}] = \left\{ \sum_{i=0}^{k} f_i \mathcal{A}^i \mid k \in \mathbb{N}, f_i \in F \right\}.$$

则 $\Psi(F[A]) = F[\mathcal{A}]$. 根据上学期第四章第二讲例 3.13 可知, 当 $A \neq O$ 时, $F[A]$ 是 $\mathrm{M}_n(F)$ 的交换子环。因为 Ψ 是环同构, 所以 $F[\mathcal{A}]$ 是 $\mathrm{Hom}(F^n, F^n)$ 的交换子环. 再根据赋值定理(上学期第五章第一讲定理 1.10), 对任意非零线性算子 $\mathcal{A}$, 我们由环同态

$$\begin{array}{ccccc} \rho_{\mathcal{A}}: & F[x] & \longrightarrow & F[\mathcal{A}] \\ & f(x) = \sum_{i=0}^{k} f_i x^i & \mapsto & f(\mathcal{A}) = \sum_{i=0}^{k} f_i \mathcal{A}^i. \end{array}$$

定理 4.17 设 $\mathcal{A} \in \mathrm{Hom}(F^n, F^n)$ 非零, $f \in F[t]$ 且 $f(\mathcal{A}) = \mathcal{O}$. 再设 $f = pq$, 其中 $p, q \in F[t]$ 且 $\gcd(p, q) = 1$. 则

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

进而,

$$\dim\left(\ker(p(\mathcal{A}))\right) + \dim\left(\ker(q(\mathcal{A}))\right) = n.$$

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

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

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, $\ker(p(\mathcal{A})) \oplus \ker(q(\mathcal{A})) = F^n$. 再利用直和的维数公式(上学期第二章第二讲命题 2.18)可知，定理成立. □

推论 4.18 *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 4.19 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 $E_2+E_2=E_2-E_2=O_2$.