高等代数 (II) 第二次习题课

李卓远　　数学科学学院

zy.li@stu.pku.edu.cn

1　内容概要

- 重因子的判断 (辗转除法和结式);
- 不可约性的判断 (Eisenstein 方法和 mod p 方法).

2　补充知识

2.1　素性/不可约性/唯一分解

在初等数论中, 素数有以下两个常用的性质:

- 若素数 p 整除 ab, 则 p 必定整除 a 或 b;
- 素数 p 不含非平凡因子.

在代数学中我们将它们抽象成为交换环上的两种性质. 设 p 为交换环 R 中一非零, 非单位元.

- 称 p 为素元 (prime element), 若 $p \mid ab$ 蕴含着 $p \mid a$ 或 $p \mid b$;
- 称 p 为不可约元 (irreducible element), 若 p 不能表示成为非单位元的乘积.

容易证明所有的素元一定是不可约的, 但是不可约元不一定具有素性. 例如在 $\mathbb{Z}[\sqrt{-5}]$ 中

$$2 \mid 6 = (1+\sqrt{-5})(1-\sqrt{-5}),\ 2 \nmid (1 \pm \sqrt{-5}).$$

教材 P25 性质 2 实际上阐述了当 $R = \mathbb{F}[x]$ 时不可约元一定是素元, 这一性质在唯一分解定理证明过程中至关重要. 事实上整环 R 为唯一分解整环 (Unique Factorization Domain, UFD), 即 R 上任意非零元在相伴意义下可分解为唯一一组不可约元的乘积, 当且仅当 R 满足

- 主理想升链稳定 (真包含关系只有有限多个), 这对应唯一分解定理中存在性的证明对于多项式次数的讨论, 即分解的乘积项只有有限多个.
- 不可约元都是素元, 这是唯一分解定理中唯一性证明的关键.

Remark 2.1.1. *利用上述等价刻画可立即得到: 主理想整环必定为唯一分解整环.*

2.2 环同态与 Gauss 引理

Theorem 2.2.1. *本原多项式 (primitive polynomials) 的乘积也为本原多项式.*

证明. 考虑更为一般的唯一分解整环 R 上的多项式. 令 $f, g \in R[x]$ 为本原多项式, 若不然, 设素元 $p \in R$ 满足 $p \mid fg$, 令 $\pi : R \to R/pR$ 并扩充至多项式环上:

$$\bar{\pi} : R[x] \to R/pR[x].$$

于是

$$\bar{\pi}(f)\bar{\pi}(g) = \bar{\pi}(fg) = 0.$$

又由于 p 的素性保证了 R/pR 没有零因子, 故而上式蕴含了 $\bar{\pi}(f) = 0$ 或 $\bar{\pi}(g) = 0$, 这与 f, g 是本原多项式矛盾. □

2.3 可约性的判断

考虑 $f \in R = \mathbb{Z}[x]$ 或 $\mathbb{Q}[x]$. 由代数基本定理可知

- f 在 $\mathbb{C}$ 上可分解为一次因式的乘积;
- f 在 $\mathbb{R}$ 上可分解为至多二次因式的乘积.

而一般地, 存在任意次数的多项式在 $\mathbb{Q}$ 上不可约, 例如 $(x^n + 2)$. $\mathbb{Z}[x]$ 上不可约性的判定有以下充分条件:

- (Eisenstein) $p \mid a_k$ for $0 \le k < n$, $p \nmid a_n$, $p^2 \nmid a_0$, 则不可约;
- ("reversed" Eisenstein) $p \mid a_k$ for $0 < k \le n$, $p \nmid a_0$, $p^2 \nmid a_n$, 则不可约;
- (mod p) $\overline{f(x)}$ 在 $\mathbb{Z}/p\mathbb{Z}[x]$ 中不可约, 则 $f(x)$ 在 $\mathbb{Z}[x]$ 中不可约. $\pi : \mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$ 可诱导环同态 $\bar{\pi} : \mathbb{Z}[x] \to \mathbb{Z}/p\mathbb{Z}[x]$, 于是 f 在 $\mathbb{Z}[x]$ 上可约蕴含着 $\bar{f}$ 在 $\mathbb{Z}/p\mathbb{Z}[x]$ 上可约.

Remark 2.3.1. *注意以上条件均不为必要条件, See https://math.stackexchange.com/questions/3398787 for Eisenstein, https://math.stackexchange.com/questions/77155 for mod p.*

3 典型例题

Lemma 3.1. *Let $f,\ g,\ h \in \mathbb{F}[x]$, then*

$$(g, h) = 1 \Rightarrow (f, gh) = (f, g)(f, h).$$

证明. 取多项式的标准分解

$$f = p_1^{m_1} \cdots p_s^{m_s},\ g = p_1^{n_1} \cdots p_s^{n_s},\ h = p_1^{l_1} \cdots p_s^{l_s},$$

其中 $\{m_k\}_{k=1}^s$, $\{n_k\}_{k=1}^s$, $\{l_k\}_{k=1}^s$ 中元素均为非负整数. 利用最小多项式的性质可知只需验证

$$nl = 0 \Rightarrow \min(m, n + l) = \min(m, n) + \min(m, l)$$

对所有的非负整数 m, n, l 均成立. 不妨令 $m = 0$, 直接计算可得上述命题是显然的. □

Problem 3.2. $p^k \mid f \Rightarrow p^{k-1} \mid f'$ *for* $k \ge 1$. *反之不一定成立.*

证明. 由 $p^k \mid f$ 可设

$$f = qp^k,\, q \in \mathbb{F}[x].$$

那么

$$f' = q'p^k + kqp^{k-1}p' = (q'p + kqp')p^{k-1},$$

故 $p^{k-1} \mid f'$. 反之由于 f' 对应的 f 可能相差一个零次多项式, 故而若成立, 则 p^k 必定整除 $\mathbb{F}$ 中任意元素, 即 $p \in \mathbb{F}$. □

Problem 3.3. 设 $p, f \in \mathbb{F}[x]$, p 不可约, $k \geq 1$, 那么

$$p^k \mid f,\, p^{k+1} \nmid f \iff p \mid f, \cdots, p \mid f^{(k-1)}, p \nmid f^{(k)}.$$

证明. $\Rightarrow$) 设 $f = qp^k$, $p \nmid q$, 有

$$f^{(l)} = \sum_{s=0}^{l} \binom{l}{s} q^{(l-s)} (p^k)^{(s)}.$$

下面采用归纳法证明

$$p^{k-s} \mid (p^k)^{(s)},\, p^{k-s+1} \nmid (p^k)^{(s)},\, 0 \leq s \leq k.$$

对 s 归纳, 当 $s = 0$ 时显然成立, 现假设命题对 $s = t$ 成立, $r < k$, 则当 $s = t + 1$ 时设 $(p^k)^{(t)} = p^{k-t}r$, $p \nmid r$, 那么

$$(p^k)^{(t+1)} = (p^{k-t}r)' = (k-t)p^{k-t-1}r + p^{k-t}r' = p^{k-t-1}((k-t)r + pr'),$$

其中由 $p \mid pr'$, $p \nmid (k-t)r$ 知命题对 $s = t + 1$ 也成立. 由归纳原理可得命题对所有满足条件的 s 和 k 均成立. 由此可将 $f^{(l)}$ 改写为

$$f^{(l)} = \sum_{s=0}^{l} \binom{l}{s} q^{(l-s)} p^{k-s} r_{m,s},\, p \nmid r_{m,s}.$$

立即可得 $p \mid f, \cdots, p \mid f^{(k-1)}$, 且

$$p \nmid f^{(k)} \iff p \nmid \left(qr_k + p \sum_{s=0}^{k-1} \binom{k}{s} q^{(k-s)} p^{k-s-1} r_{m,s} \right) \iff p \nmid qr_k$$

显然成立.

$\Leftarrow$) 反之可设 $f = qp^m$, $p \nmid q$, $m \geq 1$. 根据上述结论有

$$f^{(l)} = \sum_{s=0}^{l} \binom{l}{s} q^{(l-s)} p^{m-s} r_{m,s},\, p \nmid r_{m,s},\, 0 \leq l \leq m.$$

取 $l = 1$, 由 $p \mid f^{(1)}$ 结合上式展开的最后一项得 $m \geq 2$; 再取 $l = 2$, 由 $p \mid f^{(2)}$ 结合上式展开的最后一项得 $m \geq 3$, 以此类推, 最终得到 $m \geq k$. 最后取 $l = k$ 由 $p \nmid f^{(k)}$ 结合上式展开的最后一项得 $m = k$. □

Problem 3.4. 求 $f(x) = x^4 + ax^2 + b$ 有重因式的充要条件.

证明. 计算

$$\begin{aligned}
(f, f') &= (x^4 + ax^2 + b, 4x^3 + 2ax) \\
&= \left(x^4 + ax^2 + b, x^3 + \frac{1}{2}ax \right) \\
&= \left(\frac{a}{2}x^2 + b, x^3 + \frac{a}{2}x \right) \\
&= \left(\frac{a}{2}x^2 + b, x(x^2 + \frac{a}{2}) \right)
\end{aligned}$$

当 $a=0$ 时有

$$(f,f')=(b,x^2),$$

即 $(f,f')\neq 1$ 当且仅当 $b=0$; 当 $a\neq 0$ 时, 由于 $(x,x^2+a/2)=1$,

$$(f,f')=\left(\frac{a}{2}x^2+b,x\right)\left(\frac{a}{2}x^2+b,x^2+\frac{a}{2}\right)=(b,x)(b-a^2/4,x^2+a/2),$$

即 $(f,f')\neq 1$ 当且仅当 $b=0$ 或 $a^2=4b$. 综上所述, 无论 a 取何值, $(f,f')\neq 1$ 当且仅当 $b=0$ 或 $a^2=4b$.
另法: (结式, resultant)

$$\begin{aligned}
R(f,f') &= R(x^4+ax^2+b,4x^3+2ax)\\
&= \begin{vmatrix}
1 & 0 & a & 0 & b & & \\
 & 1 & 0 & a & 0 & b & \\
 & & 1 & 0 & a & 0 & b\\
4 & 0 & 2a & 0 & & & \\
 & 4 & 0 & 2a & 0 & & \\
 & & 4 & 0 & 2a & 0 & \\
 & & & 4 & 0 & 2a & 0
\end{vmatrix}\\
&= b\begin{vmatrix}
1 & 0 & a & 0 & b & \\
 & 1 & 0 & a & 0 & b\\
4 & 0 & 2a & 0 & & \\
 & 4 & 0 & 2a & 0 & \\
 & & 4 & 0 & 2a & 0\\
 & & & 4 & 0 & 2a
\end{vmatrix}\\
&= b\begin{vmatrix}
1 & 0 & a & 0 & b\\
0 & 2a & 0 & & \\
4 & 0 & 2a & 0 & \\
 & 4 & 0 & 2a & 0\\
 & & 4 & 0 & 2a
\end{vmatrix}+4b\begin{vmatrix}
0 & a & 0 & b & \\
1 & 0 & a & 0 & b\\
4 & 0 & 2a & 0 & \\
 & 4 & 0 & 2a & 0\\
 & & 4 & 0 & 2a
\end{vmatrix}
\end{aligned}$$

其中

$$\begin{aligned}
\begin{vmatrix}
1 & 0 & a & 0 & b\\
0 & 2a & 0 & & \\
4 & 0 & 2a & 0 & \\
 & 4 & 0 & 2a & 0\\
 & & 4 & 0 & 2a
\end{vmatrix}
&= \begin{vmatrix}
2a & 0 & & \\
0 & 2a & 0 & \\
4 & 0 & 2a & 0\\
 & 4 & 0 & 2a
\end{vmatrix}+4\begin{vmatrix}
0 & a & 0 & b\\
2a & 0 & & \\
4 & 0 & 2a & 0\\
 & 4 & 0 & 2a
\end{vmatrix}\\
&= 16a^4-8a\begin{vmatrix}
a & 0 & b\\
0 & 2a & 0\\
4 & 0 & 2a
\end{vmatrix}\\
&= 16a^4-8a(4a^3-8ab)=-16a^4+64a^2b
\end{aligned}$$

$$
\begin{vmatrix} 0 & a & 0 & b & \\ 1 & 0 & a & 0 & b \\ 4 & 0 & 2a & 0 & \\ & 4 & 0 & 2a & 0 \\ & & 4 & 0 & 2a \end{vmatrix} = -\begin{vmatrix} a & 0 & b & \\ 0 & 2a & 0 & \\ 4 & 0 & 2a & 0 \\ & 4 & 0 & 2a \end{vmatrix} + 4\begin{vmatrix} a & 0 & b & \\ 0 & a & 0 & b \\ 4 & 0 & 2a & 0 \\ & 4 & 0 & 2a \end{vmatrix}
$$

$$
\begin{aligned}
&= -2a\begin{vmatrix} a & 0 & b \\ 0 & 2a & 0 \\ 4 & 0 & 2a \end{vmatrix} + 4a\begin{vmatrix} a & 0 & b \\ 0 & 2a & 0 \\ 4 & 0 & 2a \end{vmatrix} + 16\begin{vmatrix} 0 & b & \\ a & 0 & b \\ 4 & 0 & 2a \end{vmatrix} \\
&= 2a(4a^3 - 8ab) - 16b(2a^2 - 4b) = 8a^4 - 48a^2b + 64b^2.
\end{aligned}
$$

故

$$
\begin{aligned}
R(f, f') &= b(-16a^4 + 64a^2b) + 4b(8a^4 - 48a^2b + 64b^2) \\
&= 16a^4b - 128a^2b^2 + 256b^3 \\
&= 16b(a^4 - 8a^2b + 16b^2) = 16b(a^2 - 4b)^2
\end{aligned}
$$

即 $(f, f') \neq 1$ 当且仅当 $b = 0$ 或 $a^2 = 4b$. □

Problem 3.5. *求 $f(x) = x^4 + ax^2 + b \in \mathbb{Q}[x]$ 可约的充要条件.*

证明. 由于 f 的次数为 4, 若 f 可约, 则必定包含一次因式或二次因式. 若 f 有一次因式, 即存在有理零点 $x_0 \in \mathbb{Q}$, 那么

$$
x_0^2 = \frac{-a \pm \sqrt{a^2 - 4b}}{2} \in \mathbb{Q} \Rightarrow a^2 - 4b \in \mathbb{Q}_2 := \{x^2 \mid x \in \mathbb{Q}\}.
$$

若 f 有二次因式, 可设

$$
x^4 + ax^2 + b = (x^2 + ux + v)(x^2 + sx + t),\ u, v, s, t \in \mathbb{Q}.
$$

有

$$
u + s = 0,\ us + v + t = a,\ ut + vs = 0,\ vt = b,
$$

得

$$
s = -u,\ -u^2 + v + t = a,\ u(t - v) = 0,\ vt = b.
$$

当 $u = 0$ 时, $s = -u = 0$, 且 $v + t = a$, $vt = b$, 即方程 $z^2 + az + b = 0$ 关于 $z \in \mathbb{Q}$ 有解, 于是 $a^2 - 4b \in \mathbb{Q}_2$; 当 $t = v$ 时,

$$
x^4 + ax^2 + b = (x^2 + ux + v)(x^2 - ux + v),\ v = t = \frac{a + u^2}{2},\ b = vt = \frac{(a + u^2)^2}{4}.
$$

得

$$
\pm\sqrt{b} = v = t \in \mathbb{Q},\ u = \pm\sqrt{2v - a} = \pm\sqrt{2\sqrt{b} - a} \in \mathbb{Q}.
$$

综上所述, f 可约则必有 $a^2 - 4b \in \mathbb{Q}_2$ 或 $\pm 2\sqrt{b} - a \in \mathbb{Q}_2$. 反之当 $a^2 - 4b = q^2$, $q \in \mathbb{Q}$ 时,

$$
f(x) = \left(x^2 - \frac{-a + q}{2}\right)\left(x^2 - \frac{-a - q}{2}\right);
$$

当 $\pm 2\sqrt{b} - a = r^2$, $r \in \mathbb{Q}$ 时,

$$
f(x) = x^4 + (\pm 2\sqrt{b} - r^2)x^2 + b = (x^2 \pm \sqrt{b})^2 - r^2x^2 = (x^2 + rx \pm \sqrt{b})(x^2 - rx \pm \sqrt{b}).
$$

故 $f(x)$ 可约的充要条件为

$$a^2-4b\in\mathbb{Q}_2,\ \text{ or }\ \pm 2\sqrt{b}-a\in\mathbb{Q}_2.$$

注意比较本题与前一题的结论的差别. □

Problem 3.6. *设 $a_1,\cdots,a_n\in\mathbb{Z}$ 两两不同, 判断下列函数在 $\mathbb{Q}$ 上的可约性:*

- $f_-=\prod_{k=1}^n(x-a_k)-1$;
- $f_+=\prod_{k=1}^n(x-a_k)+1$;
- $f_2=\prod_{k=1}^n(x-a_k)^2+1$.

证明. 对于 f_-, 设 $f_-=g_1g_2$, $g_1,g_2\in\mathbb{Z}[x]$. 由于

$$f(a_k)=g_1(a_k)g_2(a_k)=-1,\,\forall k=1,\cdots,n,$$

而 $g_1(a_k)$ 和 $g_2(a_k)$ 均为整数, 于是有

$$g_1(a_k)=-g_2(a_k)=\pm1,\,k=1,\cdots,n.$$

结合次数关系

$$\deg(g_1+g_2)\le\max(\deg(g_1),\deg(g_2))\le\deg(g_1)+\deg(g_2)=\deg f=n$$

得 $g_1+g_2=0$ 或 $\deg(g_1+g_2)=n$. 比较 f 和 g_1g_2 的最高次项系数知前者始终不成立.

对于 f_+, 设 $f_+=g_1g_2$, $g_1,g_2\in\mathbb{Z}[x]$, 类似地有

$$g_1(a_k)=-g_2(a_k)=\pm1,\,k=1,\cdots,n.$$

结合次数关系

$$\deg(g_1-g_2)\le\max(\deg(g_1),\deg(g_2))\le\deg(g_1)+\deg(g_2)=\deg f=n$$

得 $g_1-g_2=0$ 或 $\deg(g_1-g_2)=n$. 若 $2\nmid\deg f_+=\deg g_1+\deg g_2$, 则 $\deg g_1\ne\deg g_2$, 得 $g_1-g_2\ne0$. 否则若 $2\mid\deg f_+$, f_+ 可约蕴含着 $f_+=g^2$ for $g\in\mathbb{Z}[x]$. 不妨令 $a_1<a_2<\cdots<a_n$, 考虑

$$f_+(a_n-1/2)=\prod_{k=1}^n(a_n-1/2-a_k)+1\le-\frac{1}{2}\cdot\frac{1}{2}\cdots\frac{2n-3}{2}+1.$$

当 $n\ge6$ 时, 上述不等式右端恒小于零, 这与 $f_+=g^2\ge0$ 矛盾. 而若 $n=2$ 或 $n=4$ 时, 存在适当的 $\{a_k\}_{k=1}^n$ 使得 f_+ 可约, 例如

- $(x+1)(x-1)+1=x^2$;
- $(x+2)(x+1)x(x-1)+1=(x^2+x-1)^2$.

对于 f_2, 设 $f_2=g_1g_2$, $g_1,g_2\in\mathbb{Z}[x]$. 同理可得

$$g_1(a_k)=g_2(a_k)=\pm1,\,k=1,\cdots,n.$$

又由 f 无零点知 g_1 与 g_2 均无零点, 结合连续函数的性质可知

$$g_1(a_1)=g_1(a_2)=\cdots=g_1(a_n)=g_2(a_1)=g_2(a_2)=\cdots=g_2(a_n)=\pm1,$$

立即可得 $g_1 \mp 1$ 和 $g_2 \mp 1$ 有 n 个互不相同的零点, 故而

$$\deg(g_1), \deg(g_2) \in \{0\} \cup \{n, n+1, \cdots, 2n\}.$$

注意到

$$\deg(g_1) + \deg(g_2) = \deg(g_1 g_2) = 2n,$$

上述关系实际上蕴含着 $\deg(g_1)\deg(g_2) = 0$ 或 $\deg(g_1) = \deg(g_2) = n$. 而若 $\deg(g_1) = \deg(g_2) = n$, 由 g_1 和 g_2 在 n 个不同的整数上的取值可知

$$g_1 = g_2 = \prod_{k=1}^{n}(x - a_k) \pm 1,$$

直接验证可知这与 $f = g_1 g_2$ 矛盾. □

Problem 3.7. *求证 $f_p(x) = x^{p-1} + \cdots + x + 1$ 不可约当且仅当 p 为素数.*

证明. $\Rightarrow$) 若 $p = ab$, $a, b > 1$, 由

$$(x-1)f_p(x) = x^p - 1 = x^{ab} - 1 = (x^b - 1)((x^b)^{a-1} + \cdots + x^b + 1)$$

可知 (注意说明 $(x-1) \mid (x^b - 1)$)

$$f_p(x) = \frac{x^b - 1}{x - 1}((x^b)^{a-1} + \cdots + x^b + 1).$$

$\Leftarrow$) 由于

$$(x-1)f_p(x) = x^p - 1 \Rightarrow x f_p(x+1) = (x+1)^p - 1 \Rightarrow f_p(x+1) = \sum_{k=1}^{p}\binom{p}{k}x^{k-1},$$

利用素数 p 对 $f_p(x+1)$ 使用 Eisenstein 判别法可得 $f_p(x+1)$ 不可约, 进而 $f_p(x)$ 不可约. □

Problem 3.8. *设 f 和 g 为数域 $\mathbb{F}$ 上的多项式, 满足*

$$f(x) = 0 \Leftrightarrow g(x) = 0,\ f(x) = 1 \Leftrightarrow g(x) = 1,\ \forall x \in \mathbb{C},$$

即若看成 $\mathbb{C}$ 上的多项式 f 与 g 的零点集相同, $f-1$ 与 $g-1$ 的零点集也相同. 求证 $f = g$.

证明. 设 f 和 $f-1$ 在 $\mathbb{C}$ 上的标准分解

$$f(x) = a\prod_{k=1}^{p}(x - c_k)^{n_k},\ f(x) - 1 = a\prod_{l=1}^{q}(x - d_l)^{m_l},$$

其中 $\{c_k\}_{k=1}^p$ 互不相同, $\{d_l\}_{l=1}^q$ 互不相同, $\sum_k n_k = \sum_l m_l = \deg f$. 利用代数基本定理只需证明 $p + q > \deg f$ 即可. 利用重因式与导数的联系可知存在 $h \in \mathbb{C}[x]$ 使得

$$f'(x) = (f(x) - 1)' = \prod_{k=1}^{p}(x - c_k)^{n_k - 1}\prod_{l=1}^{q}(x - d_l)^{m_l - 1}h(x).$$

比较等式两端的次数可知

$$\sum_{k=1}^{p}(n_k - 1) + \sum_{l=1}^{q}(m_l - 1) \le \deg(f') = \deg f - 1,$$

而

$$\sum_{k=1}^{p}(n_k - 1) + \sum_{l=1}^{q}(m_l - 1) = \sum_{k=1}^{p}n_k + \sum_{l=1}^{q}m_l - p - q = 2\deg f - (p+q),$$

故而 $p + q \ge \deg f + 1$. □