

第十四次习题课讲义

① 上课内容回顾

1. 本征空间分解

2. 整环上多项式环的因式分解①(不可约元, 与素元性质讨论)

② 唯一因式分解 整环定义与性质

(高斯引理)

③ 特殊的UFD上的多项式环

④ Eisenstein 判别法

3. 复数域定义与一些基本性质

② 习题讲解

③ 拓展内容

1. 整环与 UFD 的关系 (留作这题思考题)
2. $\mathbb{Z}[X]$ 上不可约多项式判定法 (留作这题思考题)

3. $\mathbb{R}[X]$ 上多项式可约性与在 $\mathbb{C}[X]$ 里可约性何时等价?

④ 复习 I

1. 线性方程组

2. 行列式

2. $\mathbb{Z}[X]$ 上不可约多项式判定方法举例

1) 试值同法

为了说明 f 是否不可约, 试值同法十分有效 (对于低次多项式)

例 1. 判断 $X^5 - X - 1$ 的不可约性

我们知道 若 $f = X^5 - X - 1$ 在 $\mathbb{Z}[X]$ 上可约 记为 $f = gh$

则在 $\mathbb{Z}[X]$ 上 $\bar{f}$ 也是可约的

注意到 $X^5 - X - 1 \equiv (X^3 + X^2 + 1)(X^2 + X + 1) \pmod{2}$

这说明 $\bar{f} = \bar{g}\bar{h} = (X^3 + X^2 + 1)(X^2 + X + 1)$ 在 $\mathbb{Z}[X]$ 中

利用 $\mathbb{Z}[X]$ UFD 性以及 $X^3 + X^2 + 1, X^2 + X + 1$ 不可约性

$$\Rightarrow \bar{g} \sim \overline{X^3 + X^2 + 1}$$

or

$$\bar{g} \sim \overline{X^2 + X + 1}$$

$$\bar{h} \sim \overline{X^2 + X + 1}$$

$$\bar{h} \sim \overline{X^3 + X^2 + 1}$$

$$\text{不妨 } \bar{g} \sim \overline{X^3 + X^2 + 1}$$

$$\text{因为 } \mathbb{Z}_2^\times = \{1\}$$

$$\bar{h} = \overline{X^2 + X + 1}$$

$$\bar{h} \sim \overline{X^2 + X + 1}$$

$$\text{从而 } \bar{g} = \overline{X^3 + X^2 + 1}$$

$$\bar{h} = \overline{X^2 + X + 1}$$

$$\text{代入 } X^5 - X - 1 = (X^3 + X^2 + 1 + 2u)(X^2 + X + 1 + 2v)$$

其中 u 为 2 次多项式 v 为 1 次多项式

分析 4 次 X^4 系数为 0, 从而为 1 次多项式

再看 X^3 系数左边为 0 右边为奇数矛盾

故 $X^5 - X - 1$ 为 $\mathbb{Z}[X]$ 上不可约多项式

ii) 试根法 这种主要是为了排除有一次因式的可能性
 13.12 $X^{105} - 9$ 的不可约性判定

1. 其根为 q_{105}^i $0 \leq i \leq 104$ (q_{105} 为 $X^{105} - 1$ 的根)
 只需要 $\prod_{m=1}^k (X - q_{105}^{im}) \in \mathbb{Z}[X]$ 即可 $\forall i \in \{0, 1, \dots, 104\} \forall k \in \{0, 1, 2, \dots, 104\}$

注意到上述式子的常数项 $q_{105}^{\sum_{m=1}^k im} \in \mathbb{Z} \iff 105 \mid \sum_{m=1}^k im$ 且 $105 \mid k$ 矛盾

从而 $X^{105} - 9$ 不可约

iii) Eisenstein 判别法

13.13: $X^p + pX + 1$ (p 为奇素数)

pf: $f = X^p + pX + 1$ $f(X-1) = X^p + \sum_{k=1}^{p-2} (-1)^k \binom{p}{k} X^{p-k} + 2pX - p$

由 Eisenstein 判别法知 f 不可约

但有时候我们也会用其推广版本.

R is UFD $K = \text{Frac}(R)$

~~if~~ $f = a_0 + a_1X + \dots + a_{N-1}X^{N-1} + X^N \in R[X]$

and p is prime element in R

if $p \mid a_i$ but $p^2 \nmid a_0$ then f is irreducible in $R[X]$

Moreover f is irreducible in $K[X]$

13.14. $X^2 + Y^2 + Z^2 \in K[X, Y, Z]$ 若 $\text{char } K \neq 2$ 则其不可约

pf $\text{char } K = 2$ 时 $X^2 + Y^2 + Z^2 = (X+Y)^2 - Z^2 = (X+Y+Z)(X+Y-Z)$ 可约

若 $\text{char } K \neq 2$ 把 $X^2 + Y^2 + Z^2 \in K[X, Y, Z] \cong K[Y, Z][X]$ 看成 $K[Y, Z]$ 上的多项式

足需证 $Y^2 + Z^2$ 不能被 $K[X, Z]$ 中一个元素整除, 但不被其平方整除

在 $K(Z)[Y]$ 证明此事即可

$R(Z)[Y]$ 是一个域上的多项式环
故只需证 Y^2+Z^2 无重根 不是单位即可

$$\frac{\partial(Y^2+Z^2)}{\partial Y} = 2Y \text{ 与 } Y^2+Z^2 \text{ 在 } K(Z)[Y] \text{ 中互素}$$

故无重根

不是单位 因为次数 > 0

从而由 Eisenstein 判别法 $X^2+Y^2+Z^2$ 为 $K(X, Y, Z)$ 上不可约多项式

3. $R[X]$ 上的不可约多项式 f 何时一定在 $K[X]$ 上也不可约?

我们知道 $Z[X]$ 上不可约多项式 f 在 $Q[X]$ 上一定不可约
其证明核心在于 Z 的 UFD 性

所以我们要证: $R[X]$ 在 R 为 UFD 条件下与 $K[X]$ 的不可约多项式有类似 $Z[X]$ 与 $Q[X]$ 的关系

即 $\forall f \in R[X], f$ 在 $K[X]$ 上不可约 $\Leftrightarrow f$ 在 $R[X]$ 上不可约

证明类似于 $R=Z$

Pf: 若 f 在 $R[X]$ 上不可约 但在 $K[X]$ 上可约

$$f = gh, \quad g, h \in K[X] \text{ 非单位}$$

$$\text{记 } g = \frac{\tilde{g}}{a}, \quad h = \frac{\tilde{h}}{b}$$

$$\text{则 } abf = \tilde{g}\tilde{h}$$

$$c(\tilde{h})ab = 1$$

$$\text{由于 Gauss 引理 } c(\tilde{g}\tilde{h}) = c(\tilde{g})c(\tilde{h})$$

$$\text{故 } c(abf) = ab c(f) = c(\tilde{g})c(\tilde{h})$$

$$\text{这与 } (c(\tilde{g}), ab) = 1, (c(\tilde{h}), ab) = 1 \text{ 矛盾}$$

从而 f 一定在 $K[X]$ 上也不可约

~~而 $R[X]$ 上不可约多项式在 $K[X]$ 上也不可约~~

上面证明中用到了 Gauss 引理 (一般 UFD 上)

我们也能证明

$$f = gh, \quad f, g, h \in R[x]$$

$$\Leftrightarrow c(f) = c(g) c(h) \quad (c(f) \text{ 为 } f \text{ 系数在 } R \text{ 中的最大公因子})$$

$$g = g_0 + g_1 x + \dots + g_n x^n$$

$$f = g_0 h_0 + (g_1 h_0 + h_1 g_0) x + \dots + g_n h_n x^{m+n}$$

$$h = h_0 + h_1 x + \dots + h_m x^m$$

$$= f_0 + f_1 x + \dots + f_{m+n} x^{m+n}$$

有

$$c(g) c(h) \mid f_i \quad \text{故} \quad c(g) c(h) \mid c(f)$$

$$\text{其次} \quad c(f) \mid g_0 h_0 \quad c(f) \mid g_n h_n$$

说明 $c(f) = (g_0, g_n)$ 的一些因子 $\times (h_0, h_m)$ 的一些因子 (由 R UFD 性)

$$\text{Pf: } f = c(f) \tilde{f}$$

$$g = c(g) \tilde{g} \quad h = c(h) \tilde{h}$$

只需证 $\tilde{g} \tilde{h}$ 为本原多项式即可

若存在 $u \in R^* \text{ 使得 } u \mid \tilde{g} \tilde{h}$ 取 u 分解中任意一个素元 π 则 $\pi \mid \tilde{g} \tilde{h} \Rightarrow \pi \mid \tilde{g} \text{ or } \pi \mid \tilde{h}$
 这与 $\tilde{g}, \tilde{h}$ 本原矛盾 故 $\tilde{g} \tilde{h}$ 本原 从而 $c(fg) = c(f)c(g)$.

利用高斯引理, 我们很容易证明 R UFD 则 $R[x]$ 也是 UFD