

## 2.2 第 5 讲 理想运算、主开集与谱映射

理想上的包含关系经  $I \mapsto V_A(I)$  反转为闭集的包含关系. 和、积与交使这项对应具体可算; 商映射、中国剩余定理与环同态则把这些运算转化为素谱上的几何关系.

### 2.2.1 理想的和、交与积

**定义 2.15** (三种理想运算). 设  $I, J \subseteq A$  为理想. 它们的和、交与积分别为

$$I + J = \{a + b : a \in I, b \in J\}, \quad I \cap J = \{a : a \in I \text{ 且 } a \in J\},$$

以及

$$IJ = \left\{ \sum_{\nu=1}^r a_\nu b_\nu : r \geq 0, a_\nu \in I, b_\nu \in J \right\}.$$

须注意  $IJ$  不是单纯的乘积集合  $\{ab : a \in I, b \in J\}$ , 而是由两者元素乘积生成的理想.

逐项验证可知, 这三个集合都是理想. 和  $I + J$  是同时包含  $I, J$  的最小理想, 交  $I \cap J$  是同时包含于  $I, J$  的理想中最大的一个. 对积则有

$$IJ \subseteq I \cap J,$$

因为每个  $a_\nu b_\nu$  同时属于  $I$  与  $J$ . 这个包含一般不是等号(见下文尖点曲线的例子). 另一方面, 中国剩余定理给出等式成立的条件. 对任意一族理想  $(I_\lambda)_{\lambda \in \Lambda}$ , 定义它们的和  $\sum_{\lambda \in \Lambda} I_\lambda$  为同时包含每个  $I_\lambda$  的最小理想; 这样的理想存在, 因为所有满足条件的理想之交仍是理想, 而  $A$  本身满足条件. 这个定义给出具体公式

$$\sum_{\lambda \in \Lambda} I_\lambda = \left\{ a_1 + \cdots + a_r : r \geq 0, \lambda_j \in \Lambda, a_j \in I_{\lambda_j} \right\}.$$

事实上, 记右端为  $S$ . 空和为 0, 而有限和的加法、取负以及乘以  $A$  中的元素仍是同类的有限和, 所以  $S$  是理想. 取  $r = 1$  可见它包含每个  $I_\lambda$ ; 反过来, 任何包含所有  $I_\lambda$  的理想都包含  $S$ . 因此  $S$  正是上述最小理想.

**命题 2.16** (理想与闭集运算). 设  $I, J \subseteq A$  为理想, 并设  $(I_\lambda)_{\lambda \in \Lambda}$  为任意一族理想. 则

$$V_A(I + J) = V_A(I) \cap V_A(J), \quad \bigcap_{\lambda \in \Lambda} V_A(I_\lambda) = V_A\left(\sum_{\lambda \in \Lambda} I_\lambda\right),$$

而且

$$V_A(IJ) = V_A(I \cap J) = V_A(I) \cup V_A(J).$$

特别地, 理想的和对应闭集之交; 理想的积与交都对应闭集的并.

证明. 对  $\mathfrak{p} \in \text{Spec} A$ , 有

$$\begin{aligned}\mathfrak{p} \in V_A(I+J) &\iff I+J \subseteq \mathfrak{p} \\ &\iff I \subseteq \mathfrak{p} \text{ 且 } J \subseteq \mathfrak{p} \\ &\iff \mathfrak{p} \in V_A(I) \cap V_A(J).\end{aligned}$$

由最小性,  $\sum_{\lambda} I_{\lambda} \subseteq \mathfrak{p}$  当且仅当每个  $I_{\lambda}$  都包含于  $\mathfrak{p}$ , 这给出第一行公式中的第二个.

若  $\mathfrak{p}$  包含  $I$  或  $J$ , 则它包含  $I \cap J$ , 进而由  $IJ \subseteq I \cap J$  包含  $IJ$ . 只需证明最后一个条件推出第一个条件. 设  $IJ \subseteq \mathfrak{p}$  而  $I \not\subseteq \mathfrak{p}$ , 并取  $a \in I \setminus \mathfrak{p}$ . 对每个  $b \in J$ , 都有  $ab \in IJ \subseteq \mathfrak{p}$ ; 由  $\mathfrak{p}$  的素性以及  $a \notin \mathfrak{p}$ , 可得  $b \in \mathfrak{p}$ . 因此  $J \subseteq \mathfrak{p}$ . 三个条件于是等价, 从而  $V_A(IJ) = V_A(I \cap J) = V_A(I) \cup V_A(J)$ .  $\square$

整数环中的计算. 对正整数  $m, n$ , 令  $d = \gcd(m, n)$ ,  $\ell = \text{lcm}(m, n)$ . 由 Bézout 等式

$$(m) + (n) = (d), \quad (m) \cap (n) = (\ell), \quad (m)(n) = (mn).$$

例如

$$(12) + (18) = (6), \quad (12) \cap (18) = (36), \quad (12)(18) = (216).$$

后两个理想不同, 但 36 与 216 具有相同的素因子 2, 3, 所以  $V_{\mathbb{Z}}((36)) = V_{\mathbb{Z}}((216)) = \{(2), (3)\}$ . 这正说明闭集只看见理想的根, 而看不见素因子的重数.

尖点曲线. 设  $k$  为域, 并在  $k[t]$  中取子环 (因而是整环)  $A = k[t^2, t^3]$ . 考虑环同态

$$\varphi: k[X, Y] \rightarrow A, \quad \text{由 } X \mapsto t^2, Y \mapsto t^3 \text{ 给出.}$$

它是满的. 我们来计算这个环同态的核. 每个多项式  $f(X, Y) \in k[X, Y]$  模掉  $Y^2 - X^3$  都有形如  $a(X) + Yb(X)$  的唯一余式. 若此余式代入  $(t^2, t^3)$  后为零, 则  $a(t^2) + t^3b(t^2) = 0$ . 两项所含的  $t$ -次数一偶一奇, 故  $a(t^2) = b(t^2) = 0$ , 这说明

$$a(X) \text{ 和 } b(X) \text{ 在变量替换 } k[X] \rightarrow k[t^2], \quad X \mapsto t^2$$

的环同态像均为 0. 但该代换是单射, 所以  $a = b = 0$ , 核  $\ker(\varphi) = (Y^2 - X^3)$ , 从而

$$A \cong k[X, Y]/(Y^2 - X^3).$$

令  $\mathfrak{m} = (t^2, t^3)$ . 由  $A/\mathfrak{m} \cong k$  可知  $\mathfrak{m}$  是极大理想, 但它不是主理想. 为此, 对非零  $f \in A$  以  $\nu(f)$  表示  $f$  中出现的最低  $t$ -次数. 其可能值为  $0, 2, 3, \dots$ , 且  $\nu(fg) = \nu(f) + \nu(g)$ . 若  $\mathfrak{m} = (f)$ , 则  $f \in \mathfrak{m}$  使  $\nu(f) \geq 2$ ; 由  $t^2 = fg$  必有  $\nu(f) = 2$ , 再由

$t^3 = fh$  得  $v(h) = 1$ , 矛盾. 因而  $A$  不是主理想整环 (principal ideal domain, PID), 即  $A$  中存在不能由一个元素生成的理想.

现取  $I = (t^2), J = (t^3)$ . 直接计算得

$$I + J = \mathfrak{m}, \quad IJ = (t^5), \quad I \cap J = (t^5, t^6).$$

实际上,  $t^2A$  中可出现的单项式次数为  $2, 4, 5, 6, \dots$ , 而  $t^3A$  中的次数为  $3, 5, 6, 7, \dots$ . 两者共有的次数正是  $5, 6, 7, \dots$ , 它们由  $t^5, t^6$  生成. 特别地,  $t^6 \in I \cap J$  却不属于  $(t^5)$ , 因为否则必有  $t \in A$ . 于是  $IJ \subsetneq I \cap J$ .

然而  $(t^3)^2 = (t^2)^3$ , 故一个素理想包含  $t^2$  当且仅当它包含  $t^3$ . 由此得到

$$V_A(I) = V_A(J) = V_A(I + J) = V_A(IJ) = V_A(I \cap J) = \{\mathfrak{m}\}.$$

这一例也能看出, 虽然理想  $IJ$  与  $I \cap J$  不同, 但它们确定相同的 Zariski 闭子集.

**命题 2.17** (商环的素谱). 设  $L \subseteq A$  是理想, 且  $\rho: A \rightarrow A/L$  是商同态. 则

$$\rho^*: \operatorname{Spec}(A/L) \rightarrow V_A(L), \quad \bar{\mathfrak{p}} \mapsto \rho^{-1}(\bar{\mathfrak{p}})$$

是双射, 其逆映射为  $\mathfrak{p} \mapsto \mathfrak{p}/L$ . 赋予  $V_A(L)$  从  $\operatorname{Spec} A$  继承的子空间拓扑后,  $\rho^*$  是同胚.

**证明.** 由商同态的满射性,  $J \mapsto J/L$  与  $\bar{J} \mapsto \rho^{-1}(\bar{J})$  给出  $A$  中包含  $L$  的理想与  $A/L$  的理想之间的互逆对应. 又因为  $(A/L)/(J/L) \cong A/J$ , 所以  $J$  是素理想当且仅当  $J/L$  是素理想, 这就给出所述双射. 现在证明  $\rho^*$  是同胚. 对每个包含  $L$  的理想  $J$ , 有

$$\rho^*(V_{A/L}(J/L)) = V_A(J).$$

左端遍历  $\operatorname{Spec}(A/L)$  的全部闭集在此双射下的像, 而  $V_A(L)$  中的每个闭集都形如  $V_A(I) \cap V_A(L) = V_A(I + L)$ . 因而这个双射对应两边的全部闭集, 所以是同胚.  $\square$

**闭集无法辨别幂零元.** 对任意理想  $I$  与整数  $n \geq 1$ , 命题 2.16 给出  $V_A(I^n) = V_A(I)$ . 例如  $k[T]/(T^2)$  与  $k[T]/(T)$  的素谱沿相应商映射在  $\operatorname{Spec} k[T]$  中的像均为  $V(T^2) = V(T) = \{(T)\}$ ; 前一个商环中却仍有非零元素  $\bar{T}$  满足  $\bar{T}^2 = 0$ .

### 2.2.2 中国剩余定理

约成书于公元三至五世纪的《孙子算经》卷下记述著名的“物不知数”问题, 其处理模  $3, 5, 7$  的具体问题及算法. 1247 年, 秦九韶在《数书九章》卷一“大衍类”中系统整理

余数问题. 例如, 当  $a, m$  互素时, “大衍求一术”求解满足  $au \equiv 1 \pmod{m}$  的乘数  $u$ , 即求  $a$  在模  $m$  意义下的乘法逆元; “大衍总术”再用这些乘数合成同时满足各项余数条件的数. 1801 年, Gauß 在《算术研究》第 36 条中以同余语言写出同一类构造. 以下定理则把整数中的除数替换为环中的理想.<sup>1</sup>

环  $A$  的理想  $I$  和  $J$  若满足  $I + J = A$ , 则称  $I, J$  互素 (comaximal). 这等价于存在  $u \in I, v \in J$  使  $u + v = 1$ . 这推广了整数环  $\mathbb{Z}$  中通常的互素概念.

**定理 2.18** (中国剩余定理). 若理想  $I, J \subseteq A$  满足  $I + J = A$ , 则环同态

$$\Phi: A \longrightarrow A/I \times A/J, \quad a \longmapsto (a + I, a + J)$$

是满射, 且

$$\ker \Phi = I \cap J = IJ.$$

因此  $A/(IJ) \cong A/I \times A/J$ . 更一般地, 若  $I_1, \dots, I_r$  两两互素, 则

$$A/(I_1 \cdots I_r) \cong \prod_{j=1}^r A/I_j, \quad I_1 \cdots I_r = \bigcap_{j=1}^r I_j.$$

证明. 显然  $\ker \Phi = I \cap J$ . 取  $u \in I, v \in J$  使  $u + v = 1$ . 对任意  $x, y \in A$ , 元素  $xv + yu$  模  $I$  等于  $x$ , 模  $J$  等于  $y$ , 故  $\Phi$  为满射. 第一同构定理于是给出  $A/(I \cap J) \cong A/I \times A/J$ .

我们已有  $IJ \subseteq I \cap J$ . 若  $a \in I \cap J$ , 则

$$a = a(u + v) = au + av.$$

这里  $a \in J, u \in I$  给出  $au \in IJ$ , 而  $a \in I, v \in J$  给出  $av \in IJ$ , 故  $a \in IJ$ . 因而  $I \cap J = IJ$ .

对有限多个两两互素的理想作归纳. 若  $J = I_1 \cdots I_{r-1}$ , 则对每个  $j < r$  可写  $1 = u_j + v_j$ , 其中  $u_j \in I_j, v_j \in I_r$ . 相乘后  $\prod_{j < r} u_j \in J$ , 其余各项均含某个  $v_j$ , 因而属于  $I_r$ . 所以  $J + I_r = A$ . 二理想情形与归纳假设遂给出一般结论.  $\square$

**推论 2.19** (中国剩余定理的几何形式). 若  $I + J = A$ , 则  $V_A(IJ)$  有拓扑不交分解

$$V_A(IJ) = V_A(I) \sqcup V_A(J).$$

其中  $V_A(I)$  与  $V_A(J)$  在  $V_A(IJ)$  中都是既开又闭的子集.

证明. 先说明积环的素谱. 设  $R = B \times C$ , 并记  $e = (1, 0), f = (0, 1)$ . 因为  $ef = 0$  且  $e + f = 1$ , 任意  $\mathfrak{P} \in \operatorname{Spec} R$  都包含  $e, f$  中恰好一个: 素性说明至少包含一个, 而真理想

<sup>1</sup>《孙子算经》的作者与确切成书年代未定, 今本可能汇集了不同时期的材料. 原文见《孙子算经》卷下; 历史演变可参见 Shen Kangsheng, “Historical Development of the Chinese Remainder Theorem,” *Archive for History of Exact Sciences* 38 (1988), 285–305, 电子版.

不能同时包含二者. 因此  $\text{Spec } R = V_R((e)) \sqcup V_R((f))$  两部分既开又闭. 又有

$$R/(e) \cong C, \quad R/(f) \cong B.$$

命题 2.17 遂给出

$$\text{Spec}(B \times C) \cong \text{Spec } B \sqcup \text{Spec } C.$$

更具体地,  $B \times C$  的素理想恰为  $\mathfrak{p} \times C$  与  $B \times \mathfrak{q}$ , 其中  $\mathfrak{p} \in \text{Spec } B, \mathfrak{q} \in \text{Spec } C$ .

现令  $B = A/I, C = A/J$ . 中国剩余同构诱导素谱同胚; 再用商环的素谱命题, 得

$$V_A(IJ) \cong \text{Spec}(A/(IJ)) \cong \text{Spec}(A/I) \sqcup \text{Spec}(A/J) \cong V_A(I) \sqcup V_A(J).$$

命题 2.16 给出  $V_A(IJ) = V_A(I) \cup V_A(J)$ , 而  $V_A(I) \cap V_A(J) = V_A(I+J) = V_A(A) = \emptyset$ . 因此上述两块正是原来的闭子集; 它们在  $V_A(IJ)$  中互为补集, 所以也都是开集.  $\square$

《孙子算经》的“物不知数”. 古题原文是:“今有物, 不知其数. 三三数之, 賸二; 五五数之, 賸三; 七七数之, 賸二. 问: 物几何? 答曰: 二十三.”用现代记号, 它要求解

$$x \equiv 2 \pmod{3}, \quad x \equiv 3 \pmod{5}, \quad x \equiv 2 \pmod{7}.$$

三个模数两两互素, 而且  $105 = 3 \cdot 5 \cdot 7$ , 故中国剩余定理给出

$$\mathbb{Z}/105\mathbb{Z} \cong \mathbb{F}_3 \times \mathbb{F}_5 \times \mathbb{F}_7.$$

在  $\mathbb{Z}/105\mathbb{Z}$  中令

$$e_3 = 70, \quad e_5 = 21, \quad e_7 = 15.$$

元素  $e_3$  模 3 为 1, 模 5, 7 为 0, 元素  $e_5$  模 5 为 1, 模 3, 7 为 0, 元素  $e_7$  模 7 为 1, 模 3, 5 为 0. 这些元素构成  $\mathbb{Z}/105\mathbb{Z}$  中的正交投影算子: 对  $j, k \in \{3, 5, 7\}$  且  $j \neq k$ , 有

$$e_j^2 = e_j, \quad e_j e_k = 0, \quad e_3 + e_5 + e_7 = 106 \equiv 1 \pmod{105}.$$

《孙子算经》的算法写道:“三三数之, 賸二, 置一百四十; 五五数之, 賸三, 置六十三; 七七数之, 賸二, 置三十. 并之, 得二百三十三, 以二百一十减之, 即得.”其中“置”意为列出该数, 原本指置筹演算; “并之”即相加. 用上面的选择元素  $e_i$  来看, 这一计算即为

$$2e_3 + 3e_5 + 2e_7 = 2 \cdot 70 + 3 \cdot 21 + 2 \cdot 15 = 233 \equiv 23 \pmod{105}.$$

从 233 减去  $210 = 2 \cdot 105$ , 得到最小正代表 23; 全体整数解为  $23 + 105\mathbb{Z}$ .



同时指定函数值与导数. 设  $k$  为域. 对多项式  $G(T) = \sum_{n=0}^N g_n T^n$ , 定义其形式导数为  $G'(T) = \sum_{n=1}^N n g_n T^{n-1}$ . 给定任意  $a, b, c, d \in k$ , 我们要找  $F \in k[T]$ , 使

$$F(0) = a, \quad F'(0) = b, \quad F(1) = c, \quad F'(1) = d.$$

这些条件可以用理想的平方来表达. 在任意  $\alpha \in k$  处展开得  $G(T) = u + v(T - \alpha) + (T - \alpha)^2 H(T)$ , 其中  $u, v \in k, H \in k[T]$ , 且有  $u = G(\alpha)$  以及  $v = G'(\alpha)$ . 因此, 模  $(T - \alpha)^2$  的余式恰好记录  $G$  在  $\alpha$  处的值与导数, 而所求的四个条件等价于

$$F \equiv a + bT \pmod{T^2}, \quad F \equiv c + d(T - 1) \pmod{(T - 1)^2}.$$

这就成了中国剩余定理所处理的问题. 理想  $I = (T^2)$  与  $J = ((T - 1)^2)$  互素, 因为

$$1 = (1 + 2T)(T - 1)^2 + (3 - 2T)T^2.$$

中国剩余定理保证解存在, 且任意两个解之差属于  $I \cap J = IJ = (T^2(T - 1)^2)$ ; 反之, 加上这个理想中的任意元素仍是解. 再对首一的四次多项式  $T^2(T - 1)^2$  作带余除法, 便得到唯一的次数至多为 3 的解. 因此, 四项数据  $a, b, c, d$  可以独立指定.

实际构造时, 先令  $F(T) = a + bT + T^2(u + v(T - 1))$ , 便已满足 0 处的两个要求. 再由  $F(1) = a + b + u = c$  及  $F'(1) = b + 2u + v = d$ , 依次得到  $u = c - a - b$  和  $v = d - b - 2u$ . 将它们代入并按  $a, b, c, d$  整理, 得到

$$\begin{aligned} F(T) = & a(2T^3 - 3T^2 + 1) + b(T^3 - 2T^2 + T) \\ & + c(-2T^3 + 3T^2) + d(T^3 - T^2). \end{aligned}$$

上述构造没有除以 2 或 3, 因而在任意特征下都成立.

### 2.2.3 主开集

对  $f \in A$ , 其主开集记为

$$D_A(f) = \text{Spec } A \setminus V_A((f)) = \{\mathfrak{p} \in \text{Spec } A : f \notin \mathfrak{p}\}.$$

若环已经明确, 下标  $A$  省略. 因而  $D_A(f)$  完全由素理想与  $f$  的包含关系刻画.

**命题 2.20** (主开集的基本性质). 对  $f, g \in A$ , 有

$$D(0) = \emptyset, \quad D(1) = \text{Spec } A, \quad D(fg) = D(f) \cap D(g), \quad D(f^n) = D(f) \quad (n \geq 1).$$

主开集构成  $\text{Spec } A$  的一组拓扑基: 若  $U$  是开集且  $\mathfrak{p} \in U$ , 则存在  $f \in A$  使  $\mathfrak{p} \in D(f) \subseteq U$ .

$U$ . 此外:

- (i)  $D(f) = \emptyset$  当且仅当  $f$  是幂零元;
- (ii)  $D(f) = \text{Spec} A$  当且仅当  $f$  是单位;
- (iii)  $D(f) \subseteq D(g)$  当且仅当  $f \in \sqrt{(g)}$ .

证明. 前四个等式来自素理想的定义; 其中  $fg \notin \mathfrak{p}$  当且仅当  $f, g \notin \mathfrak{p}$ . 任意开集可写成

$$\text{Spec} A \setminus V_A(I) = \bigcup_{f \in I} D(f).$$

若  $\mathfrak{p}$  位于这个开集内, 则  $I \not\subseteq \mathfrak{p}$ , 可取  $f \in I \setminus \mathfrak{p}$ , 于是  $\mathfrak{p} \in D(f) \subseteq \text{Spec} A \setminus V_A(I)$ . 这证明基的性质.

由第四讲的根理想判别,  $V((f)) = \text{Spec} A$  当且仅当  $f \in \sqrt{(0)}$ , 即  $f$  幂零; 这证明 (i). 若  $f$  是单位, 它不属于任何真理想. 反之, 若  $f$  不是单位, 则  $(f)$  是真理想, 因而包含于某个极大理想; 于是  $D(f) \neq \text{Spec} A$ . 这证明 (ii). 同一根理想判别给出

$$D(f) \subseteq D(g) \iff V((g)) \subseteq V((f)) \iff f \in \sqrt{(g)},$$

从而得到 (iii). □

若  $\varphi: A \rightarrow B$  是环同态, 第四讲定义的谱映射  $\varphi^*: \text{Spec} B \rightarrow \text{Spec} A$  还满足

$$(\varphi^*)^{-1}(D_A(f)) = D_B(\varphi(f)).$$

事实上,  $f \notin \varphi^{-1}(\mathfrak{q})$  当且仅当  $\varphi(f) \notin \mathfrak{q}$ .

## 2.2.4 从 Gauß 整数环到整数环的谱映射

Gauß 整数环是复数域的子环

$$B = \mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\} \cong \mathbb{Z}[T]/(T^2 + 1),$$

其中同构把  $T$  的剩余类送到  $i$ . 包含同态  $\iota: \mathbb{Z} \hookrightarrow B$  诱导连续映射

$$\pi = \iota^*: \text{Spec} B \longrightarrow \text{Spec} \mathbb{Z}, \quad \mathfrak{q} \longmapsto \mathfrak{q} \cap \mathbb{Z}.$$

例 2.21 (Gauß 整数谱到整数谱). 映射  $\pi$  是满射. 泛点  $(0)$  的原像只有  $(0)$ . 对每个正素数  $p$ , 点  $(p)$  的原像如下. 当  $p \equiv 1 \pmod{4}$  时,  $r \in \mathbb{F}_p$  满足  $r^2 = -1$ ,  $\tilde{r} \in \mathbb{Z}$  是它的任一整数提升:

| $p$                   | $\pi^{-1}(\{(p)\})$                          | $(p)B$ 的分解                                   |
|-----------------------|----------------------------------------------|----------------------------------------------|
| 2                     | $\{(1+i)\}$                                  | $(2) = (1+i)^2$                              |
| $p \equiv 1 \pmod{4}$ | $\{(p, i - \tilde{r}), (p, i + \tilde{r})\}$ | $(p) = (p, i - \tilde{r})(p, i + \tilde{r})$ |
| $p \equiv 3 \pmod{4}$ | $\{(p)\}$                                    | $(p)$ 是极大理想                                  |

第一行成立是因为生成元相差单位:  $(1+i)^2 = 2i$ , 故  $((1+i)^2) = (2)$ .

证明. 环  $B \subseteq \mathbb{C}$  是整环, 故  $(0)$  是素理想并收缩为  $(0)$ . 反过来, 若  $0 \neq \mathfrak{q} \in \text{Spec } B$ , 取非零的  $a + bi \in \mathfrak{q}$ . 因为

$$(a + bi)(a - bi) = a^2 + b^2 \in \mathfrak{q} \cap \mathbb{Z}$$

且  $a^2 + b^2 > 0$ , 其收缩非零. 因此只有  $(0)$  位于  $(0)$  之上.

现在固定正素数  $p$ . 一个素理想  $\mathfrak{q}$  收缩为  $(p)$ , 当且仅当它包含  $pB$ : 一方面收缩为  $(p)$  显然蕴含这一点; 另一方面, 包含  $pB$  的真素理想之收缩是包含  $(p)$  的真素理想, 只能等于  $(p)$ . 由上述多项式表示, 有商环同构

$$B/pB \cong \mathbb{F}_p[T]/(T^2 + 1)$$

于是把这些  $\mathfrak{q}$  与右端的素理想一一对应. 具体地, 包含  $pB$  的素理想先取商; 反过来, 把商环中的素理想沿商映射取原像. 这两个操作互为逆.

当  $p = 2$  时,  $T^2 + 1 = (T + 1)^2$ . 每个包含  $(T + 1)^2$  的素理想都包含  $T + 1$ , 故商环只有素理想  $(T + 1)/(T + 1)^2$ , 其原像为  $(2, 1 + i) = (1 + i)$ .

设  $p$  为奇素数. 若  $r^2 = -1$  在  $\mathbb{F}_p$  中有解, 则  $r$  在  $\mathbb{F}_p^\times$  中的阶为 4, 由 Lagrange 定理知  $4 \mid p - 1$ . 反过来, 若  $p \equiv 1 \pmod{4}$ , 在  $\mathbb{F}_p^\times$  中把每个非  $\pm 1$  的元素与其逆元配对, 先得到 Wilson 同余式  $(p - 1)! \equiv -1 \pmod{p}$ . 再把  $(p - 1)!$  的前后两半配对, 得到

$$-1 \equiv (p - 1)! \equiv (-1)^{(p-1)/2} \left( \left( \frac{p-1}{2} \right)! \right)^2 = \left( \left( \frac{p-1}{2} \right)! \right)^2 \pmod{p}.$$

因此  $-1$  是平方, 且  $T^2 + 1 = (T - r)(T + r)$  拆成互异一次因子. 中国剩余定理给出

$$B/(p) \cong \mathbb{F}_p[T]/(T - r) \times \mathbb{F}_p[T]/(T + r) \cong \mathbb{F}_p \times \mathbb{F}_p.$$

乘积环右端恰有两个素理想  $\mathbb{F}_p \times (0)$  与  $(0) \times \mathbb{F}_p$ . 因而  $B$  中相应的两个素理想为

$$\mathfrak{q}_+ = (p, i - \tilde{r}), \quad \mathfrak{q}_- = (p, i + \tilde{r}).$$

更换  $\tilde{r}$  的整数提升只会改变生成元一个  $p$  的倍数, 故不改变理想. 由于  $\gcd(p, 2\tilde{r}) = 1$ ,

而  $2\tilde{r} = (i + \tilde{r}) - (i - \tilde{r})$ , 可得  $q_+ + q_- = B$ . 上述商同态的核又给出  $(p) = q_+ \cap q_-$ ; 互素理想的交等于积, 因此  $(p) = q_+ q_-$ . 若  $p \equiv 3 \pmod{4}$ , 则  $T^2 + 1$  没有根, 因而作为二次多项式不可约; 商环是含  $p^2$  个元素的域, 所以  $(p)$  本身是  $B$  的极大理想.

至此每个  $(p)$  都至少有一个原像, 故  $\pi$  满射. 复共轭  $a + bi \mapsto a - bi$  交换  $p \equiv 1 \pmod{4}$  时的两个素理想, 并固定  $(0)$ 、 $(1+i)$  以及  $p \equiv 3 \pmod{4}$  时的  $(p)$ .  $\square$

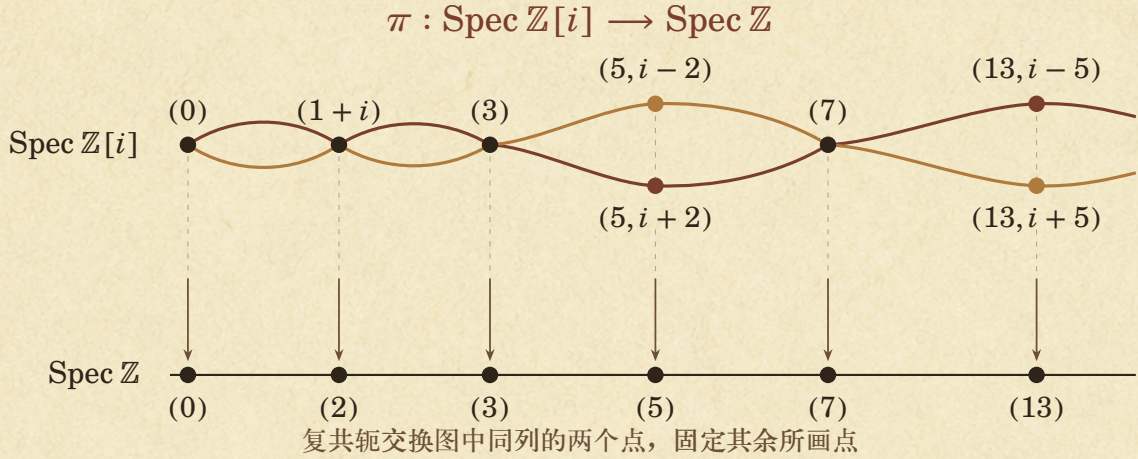


图 2.1: 谱映射  $\pi : \text{Spec } B \rightarrow \text{Spec } \mathbb{Z} (B = \mathbb{Z}[i])$  的曲线示意. 每个基点的全部原像由其正上方的实心点表示, 箭头表示理想的收缩; 红、金曲线仅辅助排布. (2) 上方只有  $(1+i)$ , (3)、(7) 上方分别只有  $(3)$ 、 $(7)$ ; (5) 与 (13) 上方各有两个点, 泛点的原像仍只有泛点.

对任意  $n \in \mathbb{Z}$ , 连续性的主开集公式为

$$\pi^{-1}(D_{\mathbb{Z}}(n)) = D_B(n).$$

当  $n \neq 0$  时, 从整数谱删去整除  $n$  的闭点, 恰好会从 Gauß 整数谱删去上表中位于这些闭点之上的所有点.

### 2.2.5 仿射直线的平方映射

令  $A$  为环, 并用两个不同的变量区分源与目标. 环同态

$$\sigma : A[U] \rightarrow A[T], \quad U \mapsto T^2, \quad a \mapsto a \quad (a \in A)$$

诱导谱映射

$$s_A : \text{Spec } A[T] \rightarrow \text{Spec } A[U].$$

把  $\text{Spec} A[T]$  记作  $A$  上的仿射直线时, 这就是平方映射. 分开使用  $U, T$  很重要: 谱映射的方向与环同态的方向相反. 每个  $H(T) \in A[T]$  都能唯一写成

$$H(T) = H_0(T^2) + TH_1(T^2), \quad H_0, H_1 \in A[U].$$

这由偶数次项与奇数次项的分组直接得到, 也说明  $\sigma$  是单射. 若  $\mathfrak{p} \in \text{Spec} A$  且  $a \in A$ , 则  $(\mathfrak{p}, T - a)$  是素理想, 因为相应商环同构于整环  $A/\mathfrak{p}$ . 对多项式除以  $U - a^2$  所得的余数作计算, 可得

$$s_A((\mathfrak{p}, T - a)) = (\mathfrak{p}, U - a^2).$$

例 2.22 (平方映射下的点). 设  $k$  为域. 对  $a \in k$ , 有

$$s_k((T - a)) = (U - a^2), \quad s_k((0)) = (0).$$

给定  $b \in k$ , 收缩为  $(U - b)$  的素理想恰好来自  $T^2 - b$  在  $k[T]$  中的不可约因子. 具体地:

- (i) 若  $\text{char } k \neq 2$  且  $b = a^2 \neq 0$ , 则有两个点  $(T - a), (T + a)$ ;
- (ii) 若  $b = 0$ , 则只有一个点  $(T)$ , 而  $T^2$  是重复因子;
- (iii) 若  $\text{char } k \neq 2$  且  $b$  不是平方, 则只有一个点  $(T^2 - b)$ , 且商域  $k[T]/(T^2 - b)$  是  $k$  的二次扩张;
- (iv) 若  $\text{char } k = 2$ , 则平方情形满足  $T^2 - b = (T - a)^2$ , 非平方情形仍给出不可约二次多项式.

因此当  $k$  代数闭且特征不为 2 时, 非零闭点各有两个原像, 原点只有一个原像, 而泛点仍映到泛点.

证明. 对  $F(U) \in k[U]$ , 有  $F(U) \in \sigma^{-1}((T - a))$  当且仅当  $F(a^2) = 0$ , 故收缩为  $(U - a^2)$ . 同态  $\sigma$  是单射, 因为不同的  $U$ -次数变成不同的偶数次  $T$ -幂, 所以  $(0)$  收缩为  $(0)$ .

一个素理想  $\mathfrak{q} \subseteq k[T]$  收缩为  $(U - b)$ , 当且仅当  $T^2 - b = \sigma(U - b) \in \mathfrak{q}$ . 这里反向成立是因为收缩为真素理想, 而  $(U - b)$  已是极大理想. 为说明  $k[T]$  中的非零素理想, 取其中次数最低的首一非零多项式  $h$ . 对理想中任意多项式作带余除法, 余式仍在该理想中且次数低于  $h$ , 故余式为零; 于是该理想等于  $(h)$ . 若  $h$  可约, 素性又会迫使一个次数更低的非单位因子属于该理想, 矛盾. 因此  $h$  不可约, 包含  $T^2 - b$  的素理想恰由它的不可约因子生成. 对  $T^2 - b$  作上述四种因式分解即得结论. 在第一种情形, 中国剩余定理还给出

$$k[T]/(T^2 - b) \cong k[T]/(T - a) \times k[T]/(T + a) \cong k \times k;$$

在第二种情形则得到  $k[T]/(T^2)$ , 其中  $T$  的剩余类非零而平方为零. 因而点的数目相同并不意味着商环相同, 重复因子仍由环结构保存.  $\square$

当  $\text{char } k = 2$  时, 先用变量改名  $k[U] \cong k[T]$  识别两个多项式环. 平方映射固定  $k$  中的系数. 它只有在每个  $c \in k$  都满足  $c^2 = c$  时才与环的绝对 Frobenius (absolute Frobenius)  $F(\sum c_j T^j) = \sum c_j^2 T^{2j}$  相同. 对域而言, 这一条件等价于  $k = \mathbb{F}_2$ .

## 习题

- (1) 直接验证定义 2.15 中的  $IJ$  是理想, 并证明  $I(J+L) = IJ + IL$  以及  $(I+J)L = IL + JL$ .
- (2) 对正整数  $m, n$ , 在  $\mathbb{Z}$  中证明  $(m) + (n) = (\gcd(m, n))$ ,  $(m) \cap (n) = (\text{lcm}(m, n))$ . 求  $V((84)) \cap V((90))$  与  $V((84)) \cup V((90))$ .
- (3) 在  $k[X, Y]$  中求  $V(X) \cap V(Y)$  与  $V(X) \cup V(Y)$ , 并分别把它们写成某个理想的消失集.
- (4) 给出理想  $I, J$  使  $IJ \subsetneq I \cap J$ . 证明尽管理想不同,  $V(IJ) = V(I \cap J)$  仍成立.
- (5) 考察同态  $\mathbb{Z} \rightarrow \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$ . 证明它的像恰由满足  $x \equiv y \pmod{2}$  的有序对  $(x, y)$  组成, 并求其核. 这说明互素条件在中国剩余定理的满射结论中不可删去.
- (6) 求同余方程组  $x \equiv 2 \pmod{3}$ ,  $x \equiv 3 \pmod{5}$ ,  $x \equiv 4 \pmod{7}$  的一个解, 并证明其解集是  $\mathbb{Z}$  中模 105 的一个剩余类.
- (7) 利用正文中的四个三次多项式, 构造  $F \in \mathbb{Z}[T]$  使  $F(0) = 1, F'(0) = 0, F(1) = 0, F'(1) = 0$ . 再把这四个等式分别约化到特征 2 与特征 3, 说明同一公式是否仍成立.
- (8) 证明  $D(f) \cup D(g) = \text{Spec } A \setminus V((f, g))$ . 给出一个例子说明这个开集未必等于  $D(f+g)$ .
- (9) 证明  $D(f) = D(g)$  当且仅当  $\sqrt{(f)} = \sqrt{(g)}$ . 据此计算  $D_{\mathbb{Z}}(12), D_{\mathbb{Z}}(18)$  及它们的交与并.
- (10) 设  $A$  为整环且  $0 \neq f \in A$ . 证明泛点  $(0)$  属于  $D(f)$ , 并由此说明  $\text{Spec } A$  的任意两个非空主开集相交.
- (11) 对  $p = 2, 3, 5, 7, 13$ , 逐一描述商环  $\mathbb{F}_p[T]/(T^2 + 1)$  ( $p = 5, 13$  时写成直积), 并写出  $\text{Spec } \mathbb{Z}[i] \rightarrow \text{Spec } \mathbb{Z}$  中位于  $(p)$  之上的所有素理想. 同时求每个上述素理想  $\mathfrak{q}$  的商域  $\mathbb{Z}[i]/\mathfrak{q}$ , 并说明复共轭怎样作用于这些素理想.
- (12) 设  $a, b \in \mathbb{Z}$ , 证明若素数  $p = a^2 + b^2$ , 则  $p = 2$  或  $p \equiv 1 \pmod{4}$ . 提示: 先说明奇素数情形不可能有  $p \mid b$ , 再在  $\mathbb{F}_p$  中考察  $(ab^{-1})^2$ .

- (13) 设  $k = \mathbb{R}$ . 完整描述平方映射  $s_k : \operatorname{Spec} k[T] \rightarrow \operatorname{Spec} k[U]$  中位于  $(U - b)$  之上的点, 分别讨论  $b > 0, b = 0, b < 0$ .
- (14) 设  $k$  的特征为 2. 比较  $k[U] \rightarrow k[T], U \mapsto T^2$  与  $k[T]$  的绝对 Frobenius, 并给出  $k \neq \mathbb{F}_2$  时二者不同的具体例子.

## 拓展阅读:复尖点曲线(选读)

若  $k = \mathbb{C}$ , 记方程  $Y^2 - X^3 = 0$  的零点集为  $C(\mathbb{C}) = \{(x, y) \in \mathbb{C}^2 : y^2 = x^3\}$ . 参数映射  $t \mapsto (t^2, t^3)$  给出  $\mathbb{C}$  到  $C(\mathbb{C})$  的同胚: 原点  $O$  以外的逆映射为  $t = y/x$ , 在  $O$  附近有  $|t|^2 = |x|$ . 但该逆映射在  $O$  处不解析: 任何  $O$  附近的收敛幂级数  $F(x, y)$  代入  $(t^2, t^3)$  后都没有  $t$  的一次项, 不可能得到  $t$ . 因此  $C(\mathbb{C})$  和  $\mathbb{C}$  拓扑同胚但不解析同构.

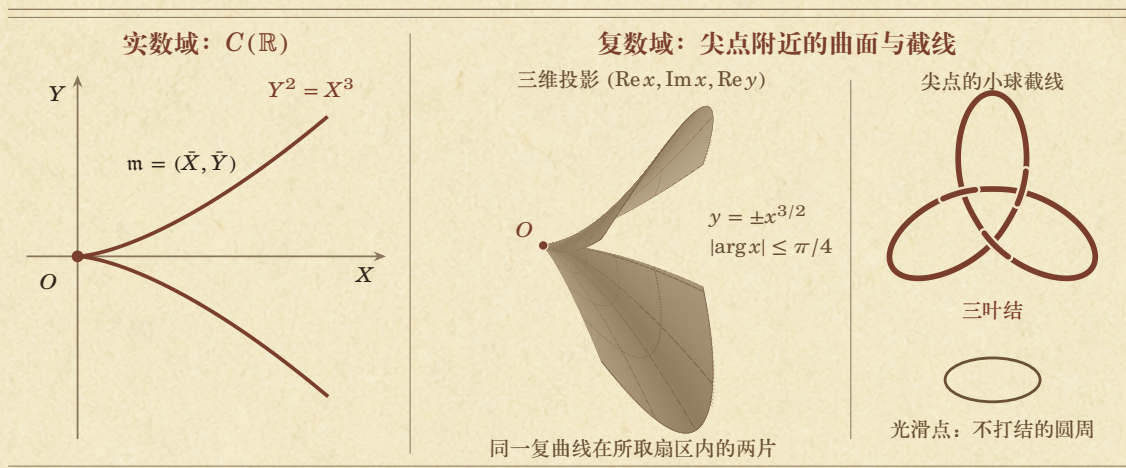


图 2.2: 尖点曲线  $y^2 = x^3$  的实轨迹见左图, 原点对应非主极大理想  $(\bar{X}, \bar{Y})$ . 右侧为尖点曲线的复点在扇区  $|\arg x| \leq \pi/4$  内的三维投影, 两片在  $O$  收于尖点相接; 最右为原点中心小球截得三叶结.

复曲线位于  $\mathbb{C}^2 \cong \mathbb{R}^4$  中. 图中取  $x = \rho e^{i\phi}$ ,  $0 \leq \rho \leq 1$ ,  $|\phi| \leq \pi/4$ , 将  $y = \pm \rho^{3/2} e^{3i\phi/2}$  投影为  $(\rho \cos \phi, \rho \sin \phi, \pm \rho^{3/2} \cos(3\phi/2))$ . 由于  $\cos(3\phi/2) > 0$ , 两片除原点外互不相交, 并在原点相切收尖; 沿  $\phi = 0$  的截面正是实尖点. 这只是一个扇区: 让  $x$  绕原点一周时,  $x^{3/2}$  改变符号, 两片通过图中未画出的部分接在一起.

尖点的嵌入奇性还可由小球截线看出. 将曲线与  $S_\epsilon^3 = \{(x, y) : |x|^2 + |y|^2 = \epsilon^2\}$  相交, 得到  $(x, y) = (r^2 e^{2i\theta}, r^3 e^{3i\theta})$ , 其中  $r^4 + r^6 = \epsilon^2$ ,  $0 \leq \theta \leq 2\pi$ . 这条闭曲线沿两个复坐标的圆周分别绕行两次、三次, 形成三叶结; 它不能在球面内不经自交地解开成圆周, 而光滑点的小球截线是不打结的圆周.<sup>3</sup>

<sup>3</sup>参见 C. McMullen, *Advanced Complex Analysis*, 2017 年讲义, 第 14 页(在线讲义). 图中三叶结由小球截线的立体投影绘制; 取不同的正半径不改变其打结类型.