arXiv:2603.00672v1 [math.AG] 28 Feb 2026

奇异曲线上黎曼–罗赫空间的快速计算

DouniaDarkaoui Martin Weimann

LMNO，诺曼底卡昂大学

2026年3月3日

摘要

设 $\mathscr{C}$ 是定义在域 k 上的射影曲线，且 D 是 $\mathscr{C}$的一个除子。黎曼–罗赫空间$\mathscr{L}(D)$是由 $\mathscr{C}$ 上的有理函数构成的集合，这些函数满足一定的零点条件，并允许存在一定的极点，其重数由 D决定。由于Riemann–Roch定理处于核心地位，黎曼–罗赫空间在代数几何中发挥着基础性作用。它们还有重要应用，例如编码理论以及曲线雅可比簇的算术研究。本文介绍一种我们认为迄今为止最快的算法，用于计算具有任意奇点的曲线上的黎曼–罗赫空间的一组基。该算法是确定性的，适用于任意完美域 k，且对 D的支集没有任何假设。

1 引言

设 $\mathscr{C} \subset \mathbf{P}^2_k$ 是定义在完美域 k 上的一条不可约射影平面曲线，其函数域为 $L = k(\mathscr{C})$。与除子 D 在 $\mathscr{C}$ 上对应的黎曼–罗赫空间为

$$\mathscr{L}(D) := \{b \in L \mid \mathrm{div}(b) \geq D\} \cup \{0\}$$

其中，div(b) 表示 b 的主除子。 $\mathscr{L}(D)$ 的元素是 $\mathscr{C}$ 的有理函数，它们允许在指定点处有具有给定重数的极点，并且必须在指定点处有具有给定重数的零点； $\mathscr{L}(D)$ 是一个有限维 k-向量空间。

自 20 世纪 80 年代以来，计算黎曼–罗赫空间的问题引起了广泛关注。当时，Goppa [22, 23, 24] 设计了一类新的纠错码（代数几何码），其构造方法是对黎曼–罗赫空间中的函数进行求值 $\mathscr{L}(D)$，该空间与定义在有限域上的曲线相关（最新进展见 [46] ）。计算特定的黎曼–罗赫空间也是在曲线的雅可比簇 $\mathscr{C}$ [35, 67]上进行运算的基石，在数论和代数几何中有多种应用。黎曼–罗赫空间的其他应用还包括丢番图方程 [18], 、代数函数积分 [19], 、有理曲线参数化 [66], 以及二元多项式分解 [68]。由于黎曼–罗赫空间在代数几何中的广泛应用及其多种用途，在过去四十年里，计算黎曼–罗赫空间已成为计算机代数的一项基础任务，相关文献浩繁，例如参见 [39, 31, 67, 21, 3, 4, 2, 32, 58, 9, 10, 16]。

对于具有结点或普通奇点的曲线，目前已有 Las Vegas 型概率算法，其复杂度接近拟最优 [3, 4]。在本文中，我们提出我们认为是迄今最快的算法，用以计算具有任意奇点的曲线的黎曼–罗赫空间的基（定理1.1）。我们的算法是确定性的，适用于任意完美域 k，且对 D的支集不作任何假设。

我们基本上遵循 Hess 算法 [32], ，该算法基于戴德金环分式理想的整基计算以及对 $k[t]$-模的约化。我们重新审视这一方法，并纳入局部域与整体域算法的最新进展；其基石是 OM 算法，它能够高效地计算、表示和操作戴德金整环的素理想 [50, 27, 28, 53]。

除了复杂度问题之外，本文也注重教学。具体而言，本文旨在厘清我们在此采用的算术观点（将除子视为戴德金环的素理想的 Z 线性组合）与文献中常用的几何观点（将除子视为曲线的光滑模型上点的 Z 线性组合）之间的关系。尽管对专家而言，这种转换早已是经典做法，我们仍希望这番努力能帮助非专家读者理解计算黎曼–罗赫空间的各种方法。

主要结果。我们采用如下代数RAM模型： [37], 仅计算算术运算的次数˜以及零检验次数，其中 k。我们用 $\mathscr{O}(g(n))$ 和 $\mathscr{O}(g(n))$ 分别表示忽略关于 n的常数因子和对数因子。我们假设使用多项式快速乘法。记 $2 \le \omega \le 3$ 为线性代数的常数，使得两个 $n \times n$ 交换环上的矩阵可通过 $\mathscr{O}(n^\omega)$ 次环运算相乘。目前最好的界为 $\omega < 2.37286$ 在 [7]。我们证明：

定理 1.1. 存在一种确定性算法，给定由一个在 X_2 中首一且可分的不可约齐次多项式 $F \in k[X_0, X_1, X_2]$ 定义的次数为 n 的射影曲线 $\mathscr{C} \subset \mathbb{P}^2_k$，以及一个非负次数的除子 $D \in \mathrm{Div}(\mathscr{C})$，其有效部分为 D^+，即可计算 $\mathscr{L}(D)$ 的压缩基，其大小规律为

$$\tilde{\mathscr{O}}(n^\omega(\deg(D^+) + \delta(\mathscr{C}) + n)) \subset \tilde{\mathscr{O}}(n^\omega(\deg(D^+) + n^2))$$

k 中的运算，其中 $\delta(\mathscr{C}) = \frac{(n-1)(n-2)}{2} - g$，其中 g $\mathscr{C}$ 的几何亏格。

除子表示为函数域 $k(\mathscr{C})$ 的赋值的 Z-线性组合，其中每个赋值由适当 Dedekind子环的素理想的 OM 表示给出（定义 3.14）。压缩基（定义 5.4）是一个列表 $(b_1, d_1) \ldots, (b_n, d_n)$，满足 $b_i \in k(t)[x]$，且 $d_i \in \mathbb{Z}$ 使得 k-向量空间 $\mathscr{L}(D)$具有基

$$\left\{ b_i(t, x) t^j,\ i = 1, \ldots, n,\ j = 0, \ldots, d_i \right\},$$

其中 $t = X_1/X_0$ 和 $x = X_2/X_0$ 均视为模 F。若 $D_\infty = \mathrm{div}_\infty(t)$ 是无穷处除子，那么只需将整数 d_i 替换为$d_i + r$，即可直接得到任意整数 $r \in \mathbb{Z}$ 对应的 $\mathscr{L}(D + rD_\infty)$ 的压缩基。写出 $\mathscr{L}(D)$ 的基的所有元素所需的代价见命题 6.5。

据我们所知，定理 1.1 亚者改进了当前最佳界 $\mathscr{O}(n^2 + \deg(D^+)n^\omega)$ 适用于具有任意奇点的曲线 [2]。此外，我们强调，我们的算法是确定性的，不受基域特征的限制，也不要求 D 的支集位于其仿射光滑点上$\mathscr{C}$，这与 [2]不同。若曲线具有普通奇点，我们的界比 n 中得到的（概率性）界差一个因子 [3, 4]。因此仍有改进空间，其中一个关键点是，我们将 $\mathscr{L}(D)$ 的元素表示为分母为一元多项式的有理函数，而 [3, 4]则不同。

数量 $\delta(\mathscr{C})$ 就是所谓的 delta不变量。它衡量 $\mathscr{C}$ 距离光滑有多远：曲线 $\mathscr{C}$的奇点越少， $\delta(\mathscr{C})$ 就越小，我们的算法也就运行得越快。特别地， $\delta(\mathscr{C}) = 0$当且仅当 $\mathscr{C}$ 是非奇异的。如果奇异轨迹和 D 的支集不包含无穷远点，˜我们就能得到稍低的复杂度 $\mathscr{O}(n^\omega(\deg(D^+) + \delta(\mathscr{C}))$ （定理 6.4）。

定理 1.1的更精确表述见定理 5.18，其复杂度以比 $\deg(D^+)$更精细（也可能小得多）的不变量来表示，这些不变量反映了 D 偏离形如$\mathrm{div}(q) + rD_\infty$ 的程度，其中 $q \in k(t)$ 且 $r \in \mathbb{Z}$ （命题 4.16）。

注记 *1.2.* 假设 F 关于 X_2 首一且可分，可以直接替换为存在两个 k-有理点 $P, Q \in P^2_k$，它们不在 $\mathscr{C}$ 上（命题 *6.10*）。如果 *Card(k)* $> n$，这就不是问题。如果 *Card(k)* $\le n$，则可能出现 $\mathscr{C}$ 经过 P^2_k 的所有 k-有理点（填充曲线）的情况，此时我们必须在 k 的有限扩张 k' 上工作，才能归结为可分首一的情形。我们以相同的复杂度（相差一个对数因子 $[k'$）计算 $\mathscr{L}(D)$ 的一个 k'-基： $k] = O(\log(n))$。然而，从 $\mathscr{L}(D)$ 的一个 k'-基恢复 $\mathscr{L}(D)$ 的一个 k-基，涉及概率例程（详见 *[4]* 和第 *6.4* 节）。

证明的主要思路。如前所述，我们主要遵循 Hess 算法 [32]（另见 Bauch 的学位论文 [9]）。函数域 $k(\mathscr{C})$ 自然同构于有理函数域 $k(t)$ 的一个有限扩张 L，该扩张由一个次数为 n 的可分、不可约、首一多项式 $f \in k[t][X]$ 定义。我们可以将 D 与 $I = I$（D）和 $I_\infty = I_\infty$（D）这两个分式理想关联起来，它们分别属于 L 中 $k[t]$ 和 $k[t]_{(1/t)}$ 的整闭包。分式理想 I 是一个秩为 n 的自由 $k[t]$-模，它表示黎曼–罗赫空间 $\mathscr{L}(D)$ 的仿射部分；而 I_∞ 是一个秩为 n 的自由 $k[1/t]_{(1/t)}$-模，它表示无穷远部分。我们有 $\mathscr{L}(D) = I \cap I_\infty$，因此归结为执行以下任务：

- 步骤 1. 计算 I 的一个 $k[t]$-基 $\mathscr{B}$，以及 I_∞ 的一个 $k[1/t]_{(1/t)}$ -基 $\mathscr{B}_\infty$。
- 步骤p 2. 计算p出 k-向量空间的一组基 p间 $I \cap I_\infty$.

第一步，我们采用 Poteaux 和第二作者基于 Okutsu 框架提出的最新快速算法 [54]。该算法结合了同一作者在 [47]中提出的快速 OM 算法（局部域上的多项式分解），以及 Stainsby 出色的 MaxMin 算法 [53]，后者可从 OM 分解计算给定分式理想的三角 [61] -基（参见第 p4.3节）。

这两个集合 $\mathscr{B}$ 和 $\mathscr{B}_\infty$ 构成了 $k(t)$-向量空间 L的一组基，并且文献 [32] （另见 [9]）指出，第 2 步可归结为计算过渡矩阵 $M \in k(t)^{n \times n}$ 在 $\mathscr{B}$ 与 $\mathscr{B}_\infty$之间的行约化形式。为此，我们采用快速算法来乘法、求逆并约化 [44, 64], 多项式矩阵，同时考虑所涉各基的特殊形式。

最新进展。 计算黎曼–罗赫空间基的经典方法源自 Brill 和 Noether 的开创性工作，其历史可追溯至19世纪下半叶。Brill–Noether 算法首先计算一个公分母 H，使得 $\mathscr{L}(D)$ 中的所有元素都可视为同次数齐次多项式之商，并且在模 F 意义下考虑。将 $D = D^+ - D^-$ 写成支撑不相交的有效除子之差后，Brill 和 Noether 证明，只需考虑 $\mathrm{div}_0(H) \geq D^+ + \mathscr{A}$，其中 $\mathscr{A}$ 是所谓的伴随因子。给定这样的 H，计算分子相当于求集合 G 中齐次多项式的基（模 F），使得 $\mathrm{div}_0(G) \geq D - \mathrm{div}_0(H)$。我们有 $D - \mathrm{div}_0(H) \geq D^- + \mathscr{A} \geq 0$。因此，在这两种情况下，我们要寻找具有指定零点的多项式。黎曼–罗赫定理给出了所求多项式 G 次数的上界；将每个条件 $v_P(G) \geq n_P$ 转化为线性方程组后，算法主要归结为线性代数。我们通常称之为几何方法，不过线性代数方法似乎也是一种恰当的说法。

Brill–Noether 方法的第一个缺点是，它最初是为具有节点奇异性的曲线开发的，在这种情况下，伴随因子易于描述。针对节点曲线的高效算法已在 [21] 中利用快速线性代数得到开发，并在 [3] 中基于 $k[t]$-模的结构化线性代数得到改进，从而达到目前已知的最佳复杂度 $\tilde{\mathcal{O}}((n^2 + \deg(D^+))^{\frac{\omega+1}{2}})$（针对节点曲线）。随后，这一结果在 [4] 中推广到了具有普通奇点的曲线。这些算法属于概率型拉斯维加斯型算法，因为为了计算所涉及除子的单变量表示，需要进行各种一般坐标变换。从理论上讲，考虑节点曲线已经足够，因为任意曲线都与一条平面节点曲线双有理等价（必要时可先扩张基域）。然而，计算奇异曲线的节点模型既困难又昂贵。此外，考虑具有任意（非普通）奇点的曲线促成了具有优良性质的新型代数几何码的发现 [39, 65,46]。因此，许多作者通过 [39, 31, 67, 16], 对赋值进行爆破或使用局部参数化，将 Brill–Noether 算法扩展到了具有任意奇点的曲线。这些方法最近在 [2] 的假设下得到了改进，即 k 具有特征零；在这种情况下，我们可以使用快速算法 [52]通过 Puiseux 展开表示奇异点。 [2] 的算法是概率型算法，其复杂度为 $\tilde{\mathcal{O}}((n^2 + \deg(D^+))^\omega)$。据我们所知，在此之前，这一直是具有任意奇点的曲线所能达到的最佳复杂度（假设特征为零）。

布里尔-诺特方法的第二个缺点是，它通常假定 D 的支集位于光滑点。快速算法 [21, 3, 4, 2] 也作此假定。这一假设不能通过变量替换来取消。尽管据我们所知，这一限制对代数几何码的应用并不构成问题，但计算与奇异除子相关联的黎曼–罗赫空间仍是一个相关问题，因为曲线上各种有意义的除子恰恰以奇异点为支集（不同除子或余不同除子、伴随除子、典范除子等）。例如，考虑典范除子可应用于代数函数积分 [19], 有理曲线参数化 [66], 二元多项式分解 [68], 或曲线光滑典范模型的计算，由此可以提取各种双有理不变量，如克利福德指标或戈纳利 [57]。

一些克服Brill-Noether算法缺点的替代方法已被提出，它们更具算术色彩。算术方法不要求一般位置（或许除输入多项式的首一性与可分性外），不要求 D 的支集位于正则点，也不对基域的特征作任何假设。它们使用函数域中分式理想的整基，其精神源自Coates [18] 与Davenport [19]的工作。近几十年来已有若干贡献 [58, 42, 9, 32], , Hess 算法 [32] 自2000年代以来一直是关键参考文献，并已在计算机代数系统Magma [13] 与Singular [62, 12]中实现。已证明它在 [32],中以多项式时间运行，尽管并未给出复杂度估计。2014年，Bauch在其学位论文[9], 中得到了复杂度估计，但函数域中的整基计算当时尚无法与基于线性代数的最快 Brill-Noether型算法相竞争。此后，函数域（以及数域）计算方面取得了重大进展。一个关键工具是 Montes于1999年发展的OM 算法 [50], ，它承袭了Ore [48, 49], 、MacLane [41, 40] 与Okutsu [47]等人长达一个世纪的工作，并在近二十年中由Nart及其合作者 [11, 25, 26, 27, 29, 28, 30, 6] 进一步发展。从完备离散秩一赋值域 K、多项式 $f \in K[x]$ 以及 $K[x]$上的高斯赋值出发，利用Newton 多边形与剩余多项式，OM 算法逐节点构造一棵赋值树，其叶子对应于 f的不可约因子。作为副产品，它返回一些额外数据，从而能够有效地表示并操作戴德金整环中的素理想。一个具有准最优复杂度的版本最近已在 [53]中得到发展。在诸多应用中，OM 算法引出了计算分式理想整基的新算法 [10, 30, 61] ，而最近在 [54] 中获得的准最优复杂度估计则为使算术方法能够与几何方法相竞争打开了大门，这也正是本文所要表明的。

除了整基计算外，Hess 算法（以及快速 Brill-Noether 算法[3, 4, 2]）的另一项特点是对自由 $k[t]$-模进行基约化，也就是对多项式矩阵进行约化。过去二十年间，计算机代数中的这一问题取得了长足发展，如今已有快速算法

可用于多项式矩阵的各种运算（乘法、求逆、约化等），例如参见 [64, 69, 44]及其中的参考文献。本文用到了其中一些成果，我们认为仍有空间利用更精细的结果来改进复杂度界。

文章结构如下。第 2 节以函数域的语言，简要介绍除子和黎曼–罗赫空间。第 3 节阐述戴德金环的赋值与素理想之间的关系，并定义除子的 OM 表示。我们还提及除子的其他一些经典表示。第 4 节专门讨论上述分式理想 I 和 I_∞ 的整基计算。复杂度自然可用与 I 和 I_∞ 相关的不变量来表示，进而用 D 表示。在关键的第 5 节中，我们计算交 $\mathscr{L}(D) = I \cap I_\infty$，这一问题与多项式矩阵的求逆和约化密切相关。第 6 节证明定理 1.1，并将射影曲线 $\mathscr{C}$ 的 δ 不变量与整闭包的指数联系起来。为求完整，我们附上两个附录：首先回顾整闭包的基本事实（附录 A），然后解释函数域$k(\mathscr{C})$的赋值与 $\mathscr{C}$ 的正规化的闭点一一对应的原因（附录 B）。

致谢。 感谢 Vincent Neiger 就多项式矩阵的约化展开了有价值的讨论。

2 除子与黎曼–罗赫空间

定义在代数闭域上的光滑代数曲线的除子通常定义为曲线上各点的有限形式 Z-线性组合。然而，我们希望考虑定义在非代数闭域上的奇异曲线；在这种情况下，必须用更为微妙的赋值概念来替代点的概念。

我们固定 k 一个基域，并假设其为完美域。通常， k 是有限域或数域。关于下文内容的经典参考文献是 [63, 20, 56, 59]。

定义 2.1。 域 L 上的函数域 k （记作 L/k）是 k 的一个有限生成扩张，且超越次数为一。 L/k 的一个赋值是包含 k的离散赋值环 $\mathscr{O} \subset L$ 的极大理想 P。我们用 V_L 表示 L的赋值集合。

回忆一下，环 $\mathscr{O} \subset L$ 是赋值环，当且仅当对于所有 $x \in L$，有 $x \in \mathscr{O}$ 或 $x^{-1} \in \mathscr{O}$。它是一个极大理想为 $P = \mathscr{O} \setminus \mathscr{O}^\times$的局部环。若进一步有 P 是主理想，则赋值环 $\mathscr{O}$ 是离散的。由于 L在 k上的超越次数为一，所有包含 k 的 L的赋值环都是离散赋值环 [63, 定理 1.1。6]

定义 2.2。 设 P 是 L的一个赋值，其赋值环为 $\mathscr{O}_P$。

- P的剩余域是 $k_P = \mathscr{O}_P/P$。它是 k的一个有限扩张。
- P 在 k 上的次数为 $\deg(P) = [k_P : k]$.
- P 的一致化元是主理想 P的一个生成元。

定义 2.3。 函数域 L/k 上的赋值是一个满射 映射 $v : L \to \mathbb{Z} \cup \{\infty\}$，它在 k上为零，并且对于所有 b、$b' \in L$，有：

1. $v(b) = \infty \iff b = 0$,
2. $v(bb') = v(b) + v(b')$
3. $v(b + b') \geq \min(v(b), v(b'))$ 等号成立当且仅当 $v(b) \neq v(b')$。

我们可以为每个赋值关联一个赋值。设 $P \in V_L$ 的赋值环为 $\mathscr{O}$，一致化元为 π。任意$b \in L^\times$ 都可以唯一地写成

$$b = u\pi^n, \quad u \in \mathscr{O}^\times, \quad n \in \mathbb{Z}.$$

整数 n 不依赖于生成元 π 的选择，而映射 $v_P(b) = n$ 在L上定义了一个赋值。反过来， L上的赋值 v 定义了一个赋值环及其极大理想，

$$\mathscr{O} = \{b \in L \mid v(b) \geq 0\} \qquad \text{and} \qquad P = \{b \in L \mid v(b) \geq 1\}$$

并且我们验证了 $v = v_P$。总而言之， L/k的赋值、包含 k 的 L 的（离散）赋值环，以及 L/k 上的赋值之间一一对应（更多细节请参见 [63, 定理 1.1.13] ）。

D定义 2.4. L/k 的除子 D 是 L/k的赋值的有限形式 $\mathbb{Z}$-线性组合，也就是 s,

$$D = \sum_{P \in V_L} n_P \cdot P, \qquad n_P \in \mathbb{Z}, \quad n_P \neq 0 \text{ for finitely many } P.$$

我们称 D 为有效的，如果对于所有 P，都有 $n_P \geq 0$，记作 $D \geq 0$。

- D 的次数为$\deg(D) = \sum_P n_P \deg(P)$。
- D 的支集为$\mathrm{Supp}(D) = \{P \in L \mid n_P \neq 0\}$.

备注 2.5。定义在 k 上的曲线 $\mathscr{C}$ 的除子就是有理函数域 $k(\mathscr{C})$的除子，其中 $\mathscr{C}$ 确实是一个函数域，详情参见第 6 节。

我们省略对基域 k 的依赖，简单地将 Div(L) 记作 L/k的除子集合。这是一个群，即由 L/k的位构成的自由阿贝尔群。该群具有偏序：若 $E - D \geq 0$，则令 $E \geq D$。

定义 2.6。设 $b \in L^\times$。对于有限多个赋值 $[63, (b) \neq 0$，有 v_P推论 *1.3*。*4]*。的除子为

$$\mathrm{div}(b) = \sum_{P \in V_L} v_P(b) \cdot P.$$

我们称 P是 b的零点，如果 $v_P(b) > 0$；称 P是 b的极点，如果 $v_P(b) < 0$。形如 $\mathrm{div}(b)$ 的除子称为主除子。

对于任意 $b \in \mathscr{O}_P$，我们可以通过令下式成立来“在 P处取 b的值”:

$$b(P) := b \bmod P \ \in k_P,$$

并且 P是 b的零点，当且仅当 $b(P) = 0$。如果 $b \notin \mathscr{O}_P$，则有 $v_P(b) < 0$，并令 $b(P) = \infty$。如果 k是代数闭的，那么对所有 P都有 $k_P \simeq k$，且任意 $b \in L$ 定义一个函数 $b\colon V_L \to k \cup \{\infty\}$。这解释了“函数域”这一术语。

定义 2.7. 除子 D 的黎曼–罗赫空间为:

$$\mathscr{L}(D) := \{b \in L \mid \mathrm{div}(b) + D \geq 0\} \cup \{0\}.$$

它是一个 k-向量空间，维数有限；如果 $\deg(D) < 0$ *[63,*，则 $\mathscr{L}(D) = \{0\}$。参见命题 *1.4.9* 和推论 *1.4.12]*。

我们可以唯一地将 D 写成支集不相交的有效除子之差，即

$$D = D^+ - D^-, \qquad \text{where} \quad D^+ = \sum_{n_P > 0} n_P \cdot P, \quad \text{and} \quad D^- = -\sum_{n_P < 0} n_P \cdot P.$$

同样地，对于元素 $b \in L$，我们定义 $\mathrm{div}_0(b) := \mathrm{div}(b)^+$ 的零点除子 b 以及 $\mathrm{div}_\infty(b) := \mathrm{div}(b)^-$ 的极点除子 b。因此有

$$b \in \mathscr{L}(D) \iff \mathrm{div}_\infty(b) \leq D^+ \quad \text{and} \quad \mathrm{div}_0(b) \geq D^-.$$

换句话说，我们要寻找至多具有那么多个极点且至少具有那么多个零点的有理函数 b。

我们希望计算 $\mathscr{L}(D)$ 的 k-基。首先要问的是:

- 我们如何表示域 L 及其元素?
- 我们如何表示赋值 $P \in V_L$？
- 我们如何计算元素 $b \in L$ 的赋值 $v_P(b)$?

对于这些问题，可能有多种答案，具体取决于我们如何看待赋值。通常主要有两种观点。几何观点将赋值视为射影平面曲线的解奇异化 $\mathscr{C}$上的闭点。在这种情形下，赋值通常用爆破 [39], Puiseux 展开 [2, 58] 或 Hamburger-Noether 展开 [16]来表示。我们将在此采用算术观点，它将赋值视为戴德金环的素理想。在这种情形下，赋值可以用素理想的生成元、OM 表示或展开来表示，下一节将对此进行介绍。关于这两种观点之间的关系，请参阅附录B。

3 函数域赋值点的表示

我们令 Spec R 表示环 R的素理想集合。对于 $p \in$ Spec R，我们令 R_p 表示 R 在 p处的局部化，也就是关于乘法子集 $R \setminus p$的局部化。

3.1 有理函数域的赋值点。

Defi定义 3.1. 函数域 K 是 k 上的有理函数域，当且仅当 $K = k(t)$ 对某个 $t \in$成立 K.

设 $K = k(t)$ 是一个有理函数域。设 $A = k[t]$ 和 $p \in$ Spec A。由于 A 是整闭的一维环，局部环 A_p 是主理想环且整闭，因此是 K的离散赋值环，从而定义了 K的一个赋值 $P = pA_p$ 。我们称 P 为有限处（相对于生成元 t的选择）。注意， p 由 $k[t]$ 的唯一首一不可约多项式生成（为方便起见，仍记作 p），且赋值 v_P 与通常的 p-进赋值 v_p一致。

在 K 中还有另一个包含 k的赋值环，即局部环 $A_\infty = k[1/t]_{(1/t)}$，其极大理想 $(1/t)$ 称为无穷远赋值点，记作 $P = \infty$。相应的赋值 v_∞ 是负次数赋值（注意符号）。

$$v_\infty(g/h) = -\deg(g/h) := \deg(h) - \deg(g).$$

命题 3.2. *[63, 定理 1.2.2]* 属于 K/k 的位恰好是位 $P = pA_p$ ，其中 $p \in$ 谱 A 以及无穷远赋值点 $P = \infty$。

因此， K 的位与 $\mathscr{P}_A :=$ 谱 $A \cup \{\infty\}$之间存在一一对应。此外，给定$p \in \mathscr{P}_A$，相应的赋值 v_p 易于描述。注意，从几何上看，我们可以将 $\mathscr{P}_A$ 视为射影直线 $\mathbf{P}^1_k = \mathbf{A}^1_k \cup \{\infty\}$的闭点集合。

3.2 位与戴德金环的素理想。

设 L/k 为任意函数域。设 $t \in L$ 在 k上是超越的。因此 L 是有理函数域 $K = k(t)$的有限扩张。

引理 3.3. 设 t P为 L的一个赋值。限制 $P' = P \cap K$ 是 K的一个赋值。我们称 P位于 P之上 $'$.

证明。 显然， $\mathscr{O}_P \cap K$ 是包含 k的 K 的赋值环。 $\mathscr{O}_P$ 的极大理想是 $P = \{x \in L, x^{-1} \notin \mathscr{O}_P\}$，而极大理想 P' 是集合 $P' = \{x \in K, x^{-1} \notin \mathscr{O}_P \cap K\}$，即 $P' = P \cap K$。 □

定义 3.4。 如果 L 的一个赋值位于 K的某个有限处之上，我们就称它为有限赋值；如果它位于 ∞之上，则称它为无穷赋值（此概念取决于 t的选取）。

设 B 和 B_∞ 分别是 A 和 A_∞ 在 L 中的整闭包（定义 A.1）。简记为

$$\mathscr{P}_0 = \text{Spec } B, \quad \mathscr{P}_\infty = \text{Spec } B_\infty \quad \text{and} \quad \mathscr{P} = \mathscr{P}_0 \cup \mathscr{P}_\infty.$$

我们称 $\mathscr{P}$ 为 L/K 的素理想集合（注意，在我们的语境中，极大理想与非零素理想相同）。如果 $p = \mathfrak{p} \cap K$，则称 $\mathfrak{p} \in \mathscr{P}$ 整除 $p \in \mathscr{P}_A$ （或称其位于 p之上），记作 $\mathfrak{p}|p$。

命题 3。 **5.** L/k 的赋值与 L/K的素理想一一对应。更确切地说 $:$

1. L 的有限处集合为 $V_L(B) = \{\mathfrak{p}B_\mathfrak{p} \mid \mathfrak{p} \in \mathscr{P}_0\}$。
2. L 的无限处集合为 $V_L(B_\infty) = \{\mathfrak{p}B_{\infty,\mathfrak{p}} \mid \mathfrak{p} \in \mathscr{P}_\infty\}$。
3. 位于 $pA_p \in V_K$ 之上的 $P \in V_L$ 赋值与位于 $p \in \mathscr{P}_A$ 之上的 $\mathfrak{p} \in \mathscr{P}$ 素理想一一对应。

证明。由于 B 和 B_∞ 都是整闭的，它们在各自极大理想处的局部化是 L的不同赋值环，因而定义了 L的不同赋值。反之，如果 $P \in V_L$ 是一个有限处，那么根据引理 3.3， $P \cap K$ 是 K 的一个有限处，即由命题 3.2可知，对于某个素理想 $p \in$ Spec A ，有 $\mathscr{O}_P \cap K = A_p$ 。因此$\mathscr{O}_P$包含 A，从而由于 $\mathscr{O}_P$是整闭的，$\mathscr{O}_P$包含 B。令 $\mathfrak{p} = P \cap B$。于是 $\mathfrak{p} \cap A = p$ ，因而 $\mathscr{O}_P$包含 $B_\mathfrak{p}$。由于离散赋值环是其分式域的极大子环，我们得到 $\mathscr{O}_P = B_\mathfrak{p}$ 和$P = \mathfrak{p}B_\mathfrak{p}$。对于无穷远位，同样的推理也适用。 □

如果 $P \in V_L$，我们令 $\mathfrak{p} \in \mathscr{P}$ 为对应的素理想，称为 P 的素理想。反之，如果 $\mathfrak{p} \in \mathscr{P}$，我们令 $P \in V_L$ 为对应的赋值。我们有

$$P = \mathfrak{p}B_\mathfrak{p} \quad \text{and} \quad \mathfrak{p} = P \cap B$$

for 个有限处和素理想，无穷远位也类似。回顾以下事实：

Lemma 3.6. 若 $\mathfrak{p}$、$\mathfrak{q}$ 是整环 R 的两个不同极大理想，则 $\mathfrak{p}\cap\mathfrak{q}=\mathfrak{p}\mathfrak{q}$ 和 $\mathfrak{q}R_{\mathfrak{p}}=R$ $_{\mathfrak{p}}$.

证明。 由于 $\mathfrak{p}$，$\mathfrak{q}$ 是 R的不同极大理想，因此必有 $\mathfrak{p}+\mathfrak{q}=R$，即 $\mathfrak{p}$ 和 $\mathfrak{q}$ 互素。因此交与乘积相等。此外，存在 $y\in\mathfrak{q}$ 使得 $y\notin\mathfrak{p}$。因此 y 在 $R_{\mathfrak{p}}$ 中可逆，由此可得 $1\in\mathfrak{q}R_{\mathfrak{p}}$，也就是说 $\mathfrak{q}R_{\mathfrak{p}}=R_{\mathfrak{p}}$。 □

环 B 是整闭的一维环，因此是戴德金环 [8, 定理 9。3]。因此， B 的所有分式理想都是可逆的 [8, 定理 9。8], ， B 的分式理想集合是由素理想生成的自由阿贝尔乘法群 $\mathfrak{p}\in\mathscr{P}_0$ [8, 推论 9。8], ，且 I 中的任意分式理想 B 都存在唯一分解 [8,推论 9。4]

$$I=\prod_{\mathfrak{p}\in\mathscr{P}_0}\mathfrak{p}^{n_{\mathfrak{p}}},\qquad \text{with}\ \ n_{\mathfrak{p}}\in\mathbb{Z}\ \ \text{and}\ \ n_{\mathfrak{p}}=0\ \ \text{for almost all}\ \ \mathfrak{p}.$$

我们定义 $v_{\mathfrak{p}}(I)=n_{\mathfrak{p}}$，约定 $v_{\mathfrak{p}}(0)=\infty$。这诱导出 $\mathfrak{p}$-进赋值

$$v_{\mathfrak{p}}:L\to\mathbb{Z}\cup\{\infty\},\quad v_{\mathfrak{p}}(b):=v_{\mathfrak{p}}(bB).$$

同理， B_∞ 是一个戴德金环，我们类似地定义附属于任意素理想$\mathfrak{p}\in\mathscr{P}_\infty$的 $\mathfrak{p}$-进赋值。

引理 3.7。 设 $P\in V_L$ 具有素理想 $\mathfrak{p}\in\mathscr{P}$。赋值 v_P 和$v_{\mathfrak{p}}$ 相同。

证明。 由引理 3.6， $v_{\mathfrak{p}}(b)$ 等于满足 n 的最大整数 $b\in\mathfrak{p}^n$，也等于满足 $b\in\mathfrak{p}^nB_{\mathfrak{p}}$的最大整数。由于 $\mathfrak{p}B_{\mathfrak{p}}=P$，结论得证。 □

我们以几个经典定义和结果结束本节。

定义 3.8。 设 $\mathfrak{p}\in\mathscr{P}$ 是一个有限处，并设 $p=\mathfrak{p}\cap K$。

- $\mathfrak{p}$ 的次数为$\deg(\mathfrak{p}):=[B/\mathfrak{p}B:\ k]$。
- $\mathfrak{p}/p$ 的剩余次数为 $f_{\mathfrak{p}}:=[B/\mathfrak{p}B:\ \ A/pA]$。

$\mathfrak{p}/p$ 的分歧指数为 $e_{\mathfrak{p}}:=v_{\mathfrak{p}}\ (p)$ 。

我们将此定义平凡地扩展到无穷远位，将 A， B替换为 A_∞， B_∞。注意，在这种情况下，$p=\infty$ 且 $A_\infty/pA_\infty=k$。因此，次数与剩余次数一致。如果 p 是有限的，我们将 p 与其唯一的首一生成元 $p\in A=k[t]$等同起来。

P命题 3.9。 设 P是 L 的一个有限赋值，其上的素理想为 $\mathfrak{p}$，且位于 $p\in$ 谱 A之上。我们有

$$\deg(P)=\deg(\mathfrak{p})=f_{\mathfrak{p}}\deg(p).$$

证明。 第一个等式是显然的，因为 $\mathscr{O}_P/P=B_{\mathfrak{p}}/\mathfrak{p}B_{\mathfrak{p}}\simeq B/\mathfrak{p}B$。第二个等式由乘法性质 $[B/\mathfrak{p}B:\ k]=[B/\mathfrak{p}B:\ A/pA][A/pA:\ k]$ 以及 $[A/pA:\ k]=\deg(p)$ 得出。 □

T以下结果称为基本不等式 [20, 定理 3.3.4 和定理 3.3。5] :

命题 3.10。 我们有 $\sum_{\mathfrak{p}|p}e_{\mathfrak{p}}f_{\mathfrak{p}}\le[L:\ \ K]$，且当扩张可分时等号成立。

3.3 赋值的 OM 表示

从现在起，我们假设对于某个不可约首一可分多项式 $f\in A[X]$， $L=K[X]/(f)$。令$n=\deg(f)=[L:\ K]$。记 $x=X\bmod f$，则可写为

$$L=K(x)=k(t,x)=k(t)[x]$$

任意 $b\in L$ 都可唯一写成 $b=a_0+a_1x+\cdots+a_{n-1}x^{n-1}$，其中 $a_i\in k(t)$。

根据命题 3.5，只需表示 L/K 的素理想，即可表示 L/k的赋值。给定 $p\in\mathscr{P}_A$， $\widehat{}$我们记 A_p p-进完备化 A_p。

命题 3.11。 素数 $\mathfrak{p}$ （整除 p ）与 $A_p[X]$ 中 f 的首一不可约因子 $\widehat{}$ $F_{\mathfrak{p}}$ 之间存在一一对应。

证明。 这由 [45, 命题 82] 结合命题 3.5 得出。 □

给定任意 $p \in \mathscr{P}_A$，OM 算法可以计算因子 $F_{\mathfrak{p}}$，精度可达到任意 p-进制精度。这一强大的算法由 Montes 在 [50] 延续 Ore 的开创性工作时[48, 49], MacLane [41, 40] 和 Okutsu [47]的基础上发展而来。过去十年间，该算法在多篇论文中得到改进和推广，例如参见 [26, 27, 28, 30, 11, 29, 53, 6]。

简而言之，OM 算法在每次迭代中，都会在更高阶的牛顿多边形和更高阶的剩余多项式上检测 f 的部分因式分解（双重剖分过程），直至完成因式分解。作为副产品，它会为每个素理想 $\mathfrak{p}$ 返回一个类型 $t_{\mathfrak{p}}$（也称为 Okutsu 框架或 OM 表示）。该对象是一个序列

$$t_{\mathfrak{p}} = [p, \phi_1, \ldots, \phi_{r_{\mathfrak{p}}}, \phi_{\mathfrak{p}}] \tag{1}$$

其中有 $p = \mathfrak{p} \cap A$，而 $\phi_i \in A[X]$ 是一些特殊的不可约首一多项式，其次数 $d_1 | \cdots | d_{r_{\mathfrak{p}}}$ 严格递增，称为关键多项式。最后一个关键多项式 $\phi_{\mathfrak{p}}$ 是 $F_{\mathfrak{p}}$ 的 p-进近似，且精度足够高，因而可以将 $F_{\mathfrak{p}}$ 与 f 的其余因子 $F_{\mathfrak{q}}$ 区分开来；详见例如 [11, 第 3] 节。

注 3.12。*Mac Lane 于 20 世纪 30 年代引入了关键多项式 [41, 40]。当 k 的特征为零或足够大时，f 的某些适当的“近似根”可发挥关键多项式的作用。Abhyankhar [5] 最初引入近似根，以便在不使用 Puiseux 级数的情况下研究复平面曲线芽（关于这一主题的精彩综述，参见例如 [51]）。*

我们给出两个简单的例子。

例 3.13。 • 令 $f = X^3 - X^2 + t^2$，并令 $p = (t)$。我们假设$\mathrm{char}(k) \neq 2$。f 在 $k[[t]][X]$ 中的分解为 $f = f_1 f_2 f_3$，其中 $f_1 = X - t + O(t^2)$、$f_2 = X + t + O(t^2)$ 和 $f_3 = X - 1 + O(t^2)$。位于(t) 之上的素理想 $\mathfrak{p}_1$、$\mathfrak{p}_2$、$\mathfrak{p}_3$ 的一些 *OM* 表示为

$$t_{\mathfrak{p}_1} = [t, X - t], \qquad t_{\mathfrak{p}_2} = [t, X + t], \qquad t_{\mathfrak{p}_3} = [t, X - 1].$$

• 令 $f = (X^2 + 1)^2 + tX + t + t^2$。该多项式在 $k((t))[X]$中不可约。因此，位于(t)之上的素理想$\mathfrak{p}$ 唯一。一个 *OM* 表示为

$$t_{\mathfrak{p}} = [t, X, X^2 + 1, (X^2 + 1)^2 + t].$$

在实际应用中，类型 $t_{\mathfrak{p}}$、$\mathfrak{p}|p$ 还附带额外的数值数据，可用于计算各种算术量（例如分歧、剩余次数、指数、交数），参见 [28]。对我们而言，一个重要事实是，这些数据可用于快速计算任意$v_{\mathfrak{p}}(b)$ 的赋值 $b \in L$。具体而言，此任务归结为计算$(\phi_1, \ldots, \phi_{r_{\mathfrak{p}}})$多进展开 b，这可在准线性时间内完成。OM 表示的另一个重要特点是，它还可快速计算分式理想的整基（参见 [30, 54] 和第4节），这是使用算术方法计算黎曼–罗赫空间的关键。

需要强调的是，$\mathfrak{p}$的 OM 表示是预先以较低精度给出的。如有需要，我们可以使用单因子提升过程 $\phi_{\mathfrak{p}}$将其提升至任意精度，[29] 也可以使用多因子提升过程[53], ；借助赋值亨泽尔引理，后一种方法具有准线性复杂度。计算赋值、计算理想的二元素表示，或计算分式理想的整基等任务，都需要更高的精度。

OM 算法已在 [53] 中得到改进。这个快速版本能够计算所有整除 p 的素理想 $\mathfrak{p}$ 的 OM 表示：当剩余特征为零或足够大时，需要在剩余域 k_p 中进行 $\tilde{\mathcal{O}}(n\delta_p)$ 次运算（相对于输出规模为准线性）；否则，需要在 k_p 中进行 $\tilde{\mathcal{O}}(n\delta_p + \delta_p^2)$ 次运算。其中，$\delta_p \leq v_p(\mathrm{disc}(f))$ 即所谓的奥库苏不变量。关于复杂度问题的更多细节，请参阅 [11, 53, 54] 。

3.4 除子的 OM 表示

定义 3.14. 设 $D = \sum_P n_P \cdot P$ 是 L 的一个除子。D 的 *OM* 表示是一个列表

$$t_D = \{(t_P, n_P),\ P \in \mathrm{Supp}(D)\}$$

其中 $t_P = t_{\mathfrak{p}}$ 是与 (1) 中类型相同的 *OM* 表示，该表示对应于素理想 $\mathfrak{p} \in \mathscr{P}$，后者与 P 相关联。

需要强调的是，计算黎曼–罗赫空间 $\mathscr{L}(D)$ 并不只涉及位 $P \in \mathrm{Supp}(D)$：我们还需要控制 $v_P(b)$ 在所有其余位 $P \notin \mathrm{Supp}(D)$ 处的情况。特别是，这要求计算射影曲线 f 的奇点处所有中心的位的 OM 表示。我们不假设这些数据已知。不过，如果需要计算与多个除子相关的黎曼–罗赫空间，这项工作只需完成一次。

注 3.15. 在许多有趣的情形中，我们可能希望计算一个除子的 *OM* 表示 D，该除子属于 L，具有特别重要的意义，并且由其内在性质简单地定义。例如，曲线的典范除子、曲线的伴随因子、L/K 的导子、不同、余不同等。对于这类除子，存在显式公式，可用 $v_{\mathfrak{p}}(D)$ 的 *OM* 不变量表示 f（例如参见 *[43]*）；由 *[53]*可知，我们可以在准线性时间内计算 D 的 *OM* 表示。

3.5 赋值点的其他常用表示

为求完整起见，我们提及文献中经典使用的另外两种赋值点表示。

3.5.1 通过 Puiseux 展开表示赋值点。

这种赋值点表示在代数几何中广泛使用，尤其用于计算黎曼–罗赫空间 [2]。从几何上看，f 的不可约因子 $F_{\mathfrak{p}}$ 给出了由 f定义的仿射平面曲线 C 的一个分支 $C_{\mathfrak{p}}$ 的局部方程。在此情形下，赋值$v_{\mathfrak{p}}$ 对应于与$F_{\mathfrak{p}}$的交数，通常借助结式计算。也就是说：

命题 3.16. 设 $h \in L = K[x]$。h 的 $\mathfrak{p}$-赋值由下式给出

$$v_{\mathfrak{p}}(h) = \frac{v_p(\mathrm{Res}(h, F_{\mathfrak{p}}))}{f_{\mathfrak{p}}}, \tag{2}$$

其中，我们仍用 h 表示 h 到 $K[X]$的典范提升。

证明。设 θ 是 $F_{\mathfrak{p}}$ 的一个根，取在 K 的 p-进完备化的固定代数闭包 K 中。由亨泽尔性质，赋值 v_p 可唯一延拓为 K 上的赋值 $\bar{v}$，并且有等式 $v_{\mathfrak{p}}(h) = e_{\mathfrak{p}}\bar{v}(h(\theta))$（例如参见 [45, 第 165] 页）。令 $d_{\mathfrak{p}} = \deg F_{\mathfrak{p}}$，并令 $\theta_1 = \theta$，θ_2，……，$\theta_{d_{\mathfrak{p}}}$ 为 $F_{\mathfrak{p}}$ 的根。由结果式的泊松公式，得到 $v_p(\mathrm{Res}(h, F_{\mathfrak{p}})) = \sum_{i=1}^{d_{\mathfrak{p}}} \bar{v}(h(\theta_i)) = d_{\mathfrak{p}}\bar{v}(h(\theta))$，结合等式 $d_{\mathfrak{p}} = e_{\mathfrak{p}} f_{\mathfrak{p}}$ 即可得出结论。 □

然而，实际中使用结果式并不方便。另一种方法是用对应分支 $C_{\mathfrak{p}}$ 的有理参数化来表示素理想 $\mathfrak{p}$，即用一对 $(a, b) \in k_{\mathfrak{p}}((u))$（实际中会截断）表示，使得 $F_{\mathfrak{p}}(a(u)\ b(u)) = 0$。如果 k 的特征为零或足够大，则这种参数化可以由形如 $(\lambda u^e, S(u))$ 的“有理普伊瑟展开”给出。等式 (2) 变为

$$v_{\mathfrak{p}}(h) = \mathrm{ord}_u\, h(\lambda u^e, S(u)), \tag{3}$$

可通过霍纳法则快速计算 [2]。将赋值表示为 Puiseux 展开，对于计算黎曼–罗赫空间尤其方便，因为这使我们能够将条件 $v_{\mathfrak{p}}(h) \geq n_{\mathfrak{p}}$ 转化为关于 k 的有限线性方程组，前提是我们已知 h 的总次数上界（例如参见 [2]）。然而，线性方程组求解的复杂度高于我们对一般奇异曲线给出的复杂度界。尽管如此，利用一些额外的 $k[t]$-模结构（本文将采用这种方法），文献 [21, 3, 4]表明，我们可以加快一般位置下节点曲线或普通曲线的计算。

注 3.17。 如果 k 的特征较小，我们可以用 *Hamburger-Noether* 参数化 *[15, 16]*替代 *Puiseux* 展开。不过，我们尚未发现针对这一任务的任何实现或复杂度估计。

注 3.18。 *OM* 算法可计算截断因子 $F_{\mathfrak{p}}$，但无法计算对应分支的参数化。我们认为这是一个很有意思的开放问题。

3.5.2 赋值的二元素表示。

它基于以下经典结果：

引理 3.19。任意素理想 $\mathfrak{p} \subset B$ 都可由两个元素 $\mathfrak{p} = (p, q)$ 生成，其中 $p \in A$ 是 $\mathfrak{p} \cap A$ 和 $q \in B$的首一生成元。如果 $\mathfrak{p} \subset B_\infty$，则存在 $q \in B_\infty$ 使得 $\mathfrak{p} = (1/t, q)$。

这大概是表示函数域或数域中素理想的最经典方法，例如在 SageMath 或 PariGP 等计算机代数系统中便采用这种方法。

定义 3.20。有序对 (p, q) 称为素理想 $\mathfrak{p}$（或赋值 P）的双元素表示。

分式理想的 $\mathfrak{q}$-进赋值等于其生成元的最小赋值。特别地，如果$\mathfrak{p}=(p,q)$，则有 $\min(v_{\mathfrak{p}}(p)v_{\mathfrak{p}}(q))=v_{\mathfrak{p}}(\mathfrak{p})=1$，因此 p 或 q必须是赋值 $P=P_{\mathfrak{p}}$的一致化元。然而，这个条件并不充分。事实上，生成元 $q\in L$ 需要确保所有条件

$$v_{\mathfrak{p}}(\mathfrak{p})=1 \quad \text{and} \quad v_{\mathfrak{q}}(\mathfrak{p})=0 \ \ \forall\, \mathfrak{q}\in\mathscr{P}_0,\ \mathfrak{q}\neq\mathfrak{p}$$

均得到满足。这对 q 施加了涉及 L的所有有限处的先验条件。

例 3.21。 设 $f=X^3-X^2+t^2$ 如例 *3.13*中所述，其因子为 $f_1=X-t+O(t^2)$ 、 $f_2=X+t+O(t^2)$ 和 $f_3=X-1+O(t^2)$ 在 $p=(t)$ 之上。我们断言

$$\mathfrak{p}_1=(t,q) \qquad \text{where} \qquad q=\frac{(x-1+t)(x-t)}{t}.$$

设 $\mathfrak{p}=(t,q)$。注意，对于所有有限素理想 $\mathfrak{q}$，有 $v_{\mathfrak{q}}(\mathfrak{p})=\min(v_{\mathfrak{q}}(t)v_{\mathfrak{q}}(q))$。我们需要检查，对于所有 $\mathfrak{q}\neq\mathfrak{p}_1$，$v_{\mathfrak{p}_1}(\mathfrak{p})=1$ 以及$v_{\mathfrak{q}}(\mathfrak{p})=0$。如果 $\mathfrak{q}$ 不整除 t，则 $v_{\mathfrak{q}}(t)=0$ 且 $v_{\mathfrak{q}}(q)\geq 0$ （该不等式成立是因为 $x\in B\subset B_{\mathfrak{q}}$，而 f 是首一的）。因此，$v_{\mathfrak{q}}(\mathfrak{p})=0$。如果 $\mathfrak{q}=\mathfrak{p}_i$，则有 $v_{\mathfrak{p}_i}(t)=1$。让我们计算 $v_{\mathfrak{p}_i}(q)$。对于 $i=1$，我们以更高的精度 $f_1=X-t-t^2/2+O(t^3)$ 计算f_1。命题 *3.16* 给出

$$v_{\mathfrak{p}_1}(q)=v_p\left(\mathrm{Res}((X-1+t)(X-t),X-t-\frac{t^2}{2}+O(t^3)\right)-1=2-1=1.$$

因此 $v_{\mathfrak{p}_1}(\mathfrak{p})=1$。对于 $i=2,3$ 我们发现

$$v_{\mathfrak{p}_2}(q)=v_p(\mathrm{Res}((X-1+t)(X-t),X+t+O(t^2))-1=1-1=0$$

类似地，$v_{\mathfrak{p}_3}(q)=0$。因此 $v_{\mathfrak{p}_2}(\mathfrak{p})=v_{\mathfrak{p}_3}(\mathfrak{p})=0$，如所需。类似地，我们可以得到双元素表示 $\mathfrak{p}_2=(t,(x-1+t)(x+t)/t)$ 和 $\mathfrak{p}_3=(t,x-1)$。

更一般地，我们可以从素理想的 OM 表示轻松推导出它的双元素表示，参见 $\mathfrak{p}$，见 [28]。然而，双元素表示不适合快速计算 $\mathfrak{p}$-进赋值，也不包含足够的信息来计算整基。因此，我们更倾向于使用 OM 表示，尽管我们不排除将两种表示结合起来用于各种任务可能会有所裨益，例如计算两个分式理想之乘积的整基。

4 从除子到整基

我们沿用上一节的记号。仍假设对于某个次数为 n 的不可约首一可分多项式 $f\in A[X]$，有 $L=K[X]/(f)$。

4.1 除子作为分式理想对

设 $D=\sum_{P\in V_L}n_P\cdot P$ 为 L/k 的一个除子。记 $\mathfrak{p}\in\mathscr{P}$ 为 P 的素理想，并设 $n_{\mathfrak{p}}=n_P$。我们定义

$$I(D)=\prod_{\mathfrak{p}\in\mathscr{P}_0}\mathfrak{p}^{-n_{\mathfrak{p}}} \qquad \text{and} \qquad I_\infty(D)=\prod_{\mathfrak{p}\in\mathscr{P}_\infty}\mathfrak{p}^{-n_{\mathfrak{p}}}. \tag{4}$$

因此 $I(D)\subset L$ 是 B 的一个分式理想，而 $I_\infty(D)$ 是 B_∞ 的一个分式理想。设 $\mathscr{I}$（相应地 $\mathscr{I}_\infty$）表示 B（相应地 B_∞）的分式理想的乘法群，并设 $\mathscr{I}\times\mathscr{I}_\infty$ 为它们的直积。

命题 4.1. 映射 $D\mapsto(I(D)\ I_\infty(D))$ 是从 $\mathrm{Div}(L)$ 到 $\mathscr{I}\times\mathscr{I}_\infty$ 的群同构。此外，我们有

$$\mathscr{L}(D)=I(D)\cap I_\infty(D).$$

证明。第一点由命题 3.5 以及 $\mathscr{I}$ 与 $\mathscr{I}_\infty$ 是由 $\mathscr{P}_0$（相应地 $\mathscr{P}_\infty$）生成的自由阿贝尔群这一事实显然可得。对于第二点，我们注意到按定义有 $\mathscr{L}(D)=\cap_{P\in V_L}P^{-n_P}$。由命题 A.6，我们有 $B=\bigcap_{\mathfrak{p}\in\mathscr{P}_0}B_{\mathfrak{p}}$ 以及 $B_\infty=\bigcap_{\mathfrak{p}\in\mathscr{P}_\infty}B_{\infty,\mathfrak{p}}$。因此由引理 3.5 可知，$\mathscr{L}(D)$ 是 B 的分式理想 $\bigcap_{\mathfrak{p}\in\mathscr{P}_0}\mathfrak{p}^{-n_{\mathfrak{p}}}$ 与 B_∞ 的分式理想 $\bigcap_{\mathfrak{p}\in\mathscr{P}_\infty}\mathfrak{p}^{-n_{\mathfrak{p}}}$ 的交。由引理 3.6，这些交可以用乘积代替。 □

我们希望计算 $\mathscr{L}(D)$ 的一个基，使用命题 4.1。第一步是计算分式理想 $I(D)$ 和 $I_\infty(D)$的整基。为此，我们采用 [53]的最新结果。

4.2 分式理想的三角基

设 $R \subset K = k(t)$ 是戴德金环，其分式域为 K（通常是 $R = A$ 或 $R = A_\infty$）。

定义 4.2。设 M、$N \subset L$ 是秩为 n 的自由 R-模。我们记 $[M\colon N]$ 为 R 的分式理想，它由 N 的一个 R-基到 M 的一个 R-基的过渡矩阵的行列式生成。它称为 M 在 N 中的指数理想。

这个定义不依赖于基的选取，因为行列式只相差 R 的一个单位。指数理想满足以下经典性质（例如参见 [59]）：

引理 4.3。设 L、M 和 N 是秩为 n 的自由 R-模。我们有

1. $[L\colon N] = [L\colon M][M\colon N]$ 以及 $[M\colon N] = [N\colon M]^{-1}$,
2. 若 $N \subset M$，则存在 a_1、.....、$a_n \in R$，使得 $a_1 | \cdots | a_n$ 并且

$$M/N \cong R/a_1R \times \cdots \times R/a_nR.$$

于是 $[M\colon N] = (a_1 \cdots a_n) \subset R$ 当且仅当 $N = M$ $[M\colon N] = R$。

令 $\overline{R} \subset L = k(t)[x]$ 为 R 在 L 中的整闭包（通常是 $R = B$ 或 $R = B_\infty$）。因此，R 仍是一个戴德金环。由于假设 L/K 是可分的，R 的所有分式理想都是秩为 $n = [L$ 的自由 R-模$\colon K]$。关于以下结果，参见 [60, Thm.1.16]：

命题 4.4。R 的任意分式理想 I 都存在一个形如 $\mathscr{B} = (q_0, q_1h_1(x), \ldots, q_{n-1}h_{n-1}($ 的 R-基 $x))$，使得满足条件：

1. 对所有 $1 \le i < n$、$q_i \in K$ 和 $h_i(x) \in R[x]$，其次数为 i，且为首一多项式。
2. 我们有 $q_0R \subset q_1R \subset \cdots \subset q_{n-1}R$，它们是 R 的分式理想之间的包含关系。

我们称 $\mathscr{B}$ 为 I 的三角形 R-基。元素 q_i 在相差一个 R 的单位倍数意义下唯一确定，并且有

$$[I : R[x]] = (q_0 \cdots q_{n-1})^{-1}R.$$

注 4.5. 根据高斯消元，任意秩为 n 的自由 R-模 $I \subset L$ 都有一个满足第一条条件的 R-基，但第二条条件未必满足。事实上，如果 I 是戴德金环的分式理想，那么条件 *2* 会由条件 *1* 自动推出。

记号。对于 $R = A$ 或 $R = A_\infty$，R 的任意分式理想 J 都是主理想，因此由唯一的元素 $h = a/b$ 生成，其中 a, $b \in k[t]$ 为首一且互素。为简便起见，我们记作

$$\deg(J) := \deg(h) = \deg(a) - \deg(b).$$

4.3 有限处的三角基计算

我们在此考虑 $R = A = k[t]$。我们希望计算 B 的分式理想 I 的整基。I 的指数不能很好地反映 I 的大小，因此我们将用 I 的规范化理想的指数来表示算法的复杂度。

定义 4.6. 设 I 是 B 的分式理想。设 $q_I \in K$ 满足 $I \cap K = q_IA$。

- I 的规范化理想为 $I^* = q_I^{-1}I$。
- I 的标准化指数为 $\delta_I = \deg [I^*\colon A[x]]$。
- I 的标准化指数幂为 $\exp(I) := \min\{\deg(a) \mid a \in A, aI^* \subset A[x]\}$。

引理 4.7. 我们有 $A[x] \subset B \subset I^*$。特别地，$0 \le \delta_B \le \delta_I$ 且 $0 \le \exp(B) \le \exp(I)$。此外，

$$\exp(I) \le \delta_I \le n \exp(I).$$

证明。由于 f 是首一的，x 在 A上是整的，因此 $A[x] \subset B$。我们有 $I \cap K = qA$，故 $I^* \cap K = q^{-1}qA = A$。于是 $1 \in I^*$ 和 $B \subset I^*$。由这些包含关系可推出 $0 \le \mathsf{exp}(B) \le \mathsf{exp}(I)$；利用 $[I^*\colon A[x]] = [I^*\colon B][B\colon A[x]]$ 和 $A[x] \subset B \subset I^*$，由引理 4.3 可得不等式 $0 \le \delta_B \le \delta_I$。同样由引理 4.3，我们得到分解 $I^*/A[x] \simeq A/a_1A \times \cdots \times A/a_nA$，其中 $a_i \in A$ 且 $a_i | a_{i+1}$。因此，$\mathsf{exp}(I) = \mathsf{deg}\ a_n$。此外，$[I^*\colon A[x]] = a_1 \cdots a_nA$，故 $\delta_I = \mathsf{deg}\ a_1 + \cdots + \mathsf{deg}\ a_n$。由于 $\mathsf{deg}\ a_i \le \mathsf{deg}\ a_{i+1}$，最后一个结论得证。 □

在函数域中计算整基是计算机代数的一项经典任务，已有多种算法可用于此目的。几何方法以 Puiseux 级数为基础（参见 [1]，其中介绍了情形 $I = B$下的最新进展），此外还有算术方法（[10, 30, 61, 54] 及其中的参考文献），这些方法主要遵循 Okutsu 框架 [47]，并像本文一样使用 OM 算法。这种方法的优点在于适用于任意特征，并且经适当调整后也适用于 数域的情形。下面简要概述主要步骤。设 $I = \prod_{\mathfrak{p}\in\mathscr{P}_0} \mathfrak{p}^{n_\mathfrak{p}}$ 是 B的一个分式理想。

1. 对于每个有限素理想 $p \in \mathscr{P}_A$，我们计算自由 A_p-模 $I_p = I \otimes_A A_p$ 的一个三角 A_p-基。若 p 不整除指数 $[B\colon A[x]]$ 且对于所有 $\mathfrak{p}|p$，$n_\mathfrak{p} = 0$，则三角基为 1，x，……，x^{n-1}。否则：

   (a) 我们运行上述 [53] OM 算法 p，以足够高的精度计算每个 $\mathfrak{p}|p$ 的 OM 表示（即素因子 $F_\mathfrak{p} \in A_p[x]$ 的关键多项式列表，其中 $\widehat{\ }$）。(b) 我们应用 Stainsby 的简单而强大的 MaxMin 算法 [61]，针对每个 $i = 0$，……，$n-1$，检测一个次数为 i 的关键多项式乘性组合 h_i，使某个半赋值 $w_{I,\,p}$ 最大化。于是 $h_0/p^{\lfloor w_{I,\,p}(h_0)\rfloor}$，……，$h_{n-1}/p^{\lfloor w_{I,\,p}(h_{n-1})\rfloor}$ 是 I_p 的一个三角 A_p-基，见 [61, 定理 3.4]。

2. 我们使用中国剩余定理将所有 A_p-基拼接起来，从而得到 I 的三角形 A-基（这里使用了 A_p-基是三角形的这一事实）。

我们使用记号 $\mathscr{O}_\epsilon(g(n)) = \mathscr{O}(g(n)^{1+\epsilon(n)})$，其中 $\epsilon(n) \to 0$。简记为 $\delta = \delta_B$。我们得到如下复杂度估计：

定理 4.8。 *[54, 定理 7]* 设 f 可分且首一。令 $I = \prod \mathfrak{p}^{n_\mathfrak{p}}$ 为 B 的一个分式理想，其中素理想 $\mathfrak{p}$ 以 *OM* 表示给出。存在一种确定性算法，可以计算 I 的三角形 A-基，其

- $\mathscr{O}_\epsilon(n\delta_I)$ 次 k 中的运算，若 $char(k) = 0$ 或 $char(k) > n$，
- $\mathscr{O}_\epsilon(n\delta_I + \delta^2)$ 次 k 中的运算，若 $char(k) \le n$。

返回的基表示为一对 $\mathscr{B} = (q, \mathscr{B}^*)$，其中 $q = q_I \in k(t)$ 如定义 4.6 所示，且 $\mathscr{B} = q\mathscr{B}^*$，其中

$$\mathscr{B}^* = \left(1, \frac{g_1(t,x)}{p_1(t)}, \ldots, \frac{g_{n-1}(t,x)}{p_{n-1}(t)}\right) \tag{5}$$

是规范化理想 I^* 的一个 A-基，使得：
(i) $p_i \in k[t]$ 是首一的，$p_1|p_2|\cdots|p_{n-1}$。(ii) $g_i \in k[t][x]$ 是 x 中次数为 i 的首一多项式，且 $\deg_t(g_i) < \deg(p_i)$。
p_i由此唯一确定。我们有 $\delta_I = \deg(p_1) + \cdots + \deg(p_{n-1})$，且 $\exp(I) = \deg(p_{n-1})$。不计因子 q，输出的算术稠密规模为 $\sum_{i=1}^{n-1} i\deg(p_i) = \mathscr{O}(n\delta_I)$，且此界是紧的。因此，该算法在特征零或特征足够大时具有准线性复杂度。元素$q = q_I$ 表示为素数的乘积 $q = \prod_{p\in\mathscr{P}_A} p^{-m_p}$（未计算），其中 m_p由 I显式确定，见下文。

注 4.9。 定理 7 *[54]* 要求我们知道整除 $p \in \mathscr{P}_A$ 的素数集合 $[I^*\colon A[x]]$。其中一部分素数可以从 I 的 *OM* 表示（已知）中直接推出。剩余的素数是 $[B$ 的素因子$\colon A[x]]$。它们可以通过 $k[t]$ 中 f的判别式的不可约因式分解推出。使用动态求值 *[34]*，实际上只需计算判别式的无平方因子部分，其计算成本符合预期的上界。

4.4 计算无穷远处的三角基

现在，我们将命题 4.4 专门应用于 $R = A_\infty = k[1/t]_{(1/t)}$这一情形。我们希望计算分式理想 A_∞的三角 I_∞ -基，它属于 B_∞。需要注意的是，$A_\infty[x]$ 通常并不包含在 B_∞中。令 $f = \sum_{i=0}^{n} c_i X^i$，其中 $c_i \in A = k[t]$。根据 [32]，，我们考虑

$$y = xt^{-\lambda} \qquad \text{where} \qquad \lambda = \lambda(f) := \max_{i<n}\left(\left\lceil \frac{\deg(c_i)}{n-i}\right\rceil\right). \tag{6}$$

引理 4.10. 元素 $y \in L$ 在 A_∞ 上整。

证明。多项式 $f_\infty(Y)\colon = t^{-n\lambda}f(t^\lambda Y)$ 是一个次数为 n 的首一多项式，根据（6）它属于$k[t^{-1}][Y]$。由于 $f_\infty(y) = t^{-n\lambda}f(x) = 0$ 且 $k[t^{-1}] \subset A_\infty$，得证。 □

记 $u = t^{-1}$。注意，对于所有 $a \in K$，$\deg_u(a) = -\deg(a)$。理想 $I_\infty \cap K$ 现在是 $A_\infty = k[u]_{(u)}$的一个分式理想。

定义 4.11. 设 I_∞ 是 B_∞ 的分式理想，且 $m_{I_\infty} \in \mathbb{Z}$ 满足 $I_\infty \cap K = u^{m_{I_\infty}} A_\infty$。

- I_∞ 的规范化理想为 $I_\infty^* = u^{-m_{I_\infty}} I_\infty$。
- I_∞ 的标准化指数为 $\delta_{I_\infty} = \deg_u [I_\infty^* : A_\infty[y]]$。
- I_∞ 的标准化指数幂为 $\exp(I_\infty) := \min\{\deg_u(a) \mid a \in A_\infty, aI^* \subset A_\infty[y]\}$。

引理 4.12. 我们有 $A_\infty[y] \subset B_\infty \subset I_\infty^*$。特别地，$0 \le \delta_{B_\infty} \le \delta_{I_\infty}$ 且 $0 \le \exp(B_\infty) \le \exp(I_\infty)$。此外，

$$\exp(I_\infty) \le \delta_{I_\infty} \le n \exp(I_\infty).$$

证明. 与引理 4.7的证明类似，不同之处在于我们是在环 $A_\infty = k[u]_{(u}$上进行讨论).

简记为 $\delta_\infty = \delta_{B_\infty}$。与定理 4.8类似，我们由 [54] 推出：

定理 4.13。 设 I_∞ 是由 *OM* 表示给出的 B_∞ 的一个分式理想。存在一种确定性算法，可计算 I_∞ 的一个三角形 A_∞ 基，满足：

- $\mathcal{O}_\epsilon(n\delta_{I_\infty})$ 次 k 运算，当 $char(k) = 0$ 或 $char(k) > n$ 时，
- $\mathcal{O}_\epsilon(n\delta_{I_\infty} + \delta_\infty^2)$ 次 k 运算，当 $char(k) \le n$ 时。

The 返回的基具有如下形状 $\mathscr{B}_\infty = u^m \mathscr{B}_\infty^*$，其中 $m = m_{I_\infty} \in \mathbb{Z}$ 如定义 4.11 所示，且

$$\mathscr{B}_\infty^* = \left(1, \frac{h_1(u,y)}{u^{m_1}}, \ldots, \frac{h_{n-1}(u,y)}{u^{m_{n-1}}}\right) \tag{7}$$

是规范化理想 I_∞^* 的一个 A_∞ 基，满足：
(i) $0 \le m_1 \le m_2 \cdots \le m_{n-1}$。(ii) $h_i \in k[u][y]$ 在 y 中是次数为 i 的首一 u，且 $\deg_u(h_i) < m_i$。
m_i 唯一确定。我们有 $\delta_{I_\infty} = m_1 + \cdots + m_{n-1}$，且 $\exp(I_\infty) = m_{n-1}$。复杂度相对于输出大小仍为准线性。

4.5 指数的各种界

我们需要给出指数 $\exp(I)$ 和 $\exp(I_\infty)$ 关于除子 D 的上界。以下显式公式是关键。

引理 4.14. 设 $I = \prod_{\mathfrak{p} \in \mathscr{P}_0} \mathfrak{p}^{-n_\mathfrak{p}}$ 和 $I_\infty = \prod_{\mathfrak{p} \in \mathscr{P}_\infty} \mathfrak{p}^{-n_\mathfrak{p}}$。对于 $p \in \mathscr{P}_A \cup \{\infty\}$，令 $m_p :=$ 最小值 $\left\{ \left\lfloor \frac{n_\mathfrak{p}}{e_\mathfrak{p}} \right\rfloor \mid \mathfrak{p} | p \right\}$。
采用定义 *4.6* 和定义 *4.11*：

1. 我们有 $q_I = \prod_{p \in \mathscr{P}_A} p^{-m_p}$ 和 $I^* = \prod_{p \in \mathscr{P}_A} \prod_{\mathfrak{p}|p} \mathfrak{p}^{e_\mathfrak{p} m_p - n_\mathfrak{p}}$
2. 我们有 $m_{I_\infty} = -m_\infty$ 和 $I_\infty^* = \prod_{\mathfrak{p}|\infty} \mathfrak{p}^{e_\mathfrak{p} m_\infty - n_\mathfrak{p}}$。

证明。这由 [54, 引理2]得出。

对于 $q = a/b \in K = k(t)$，在 a，$b \in k[t]$ 互素时，我们将 $h(q) = \deg(a) + \deg(b)$ 记为 q 的高度。

命题 4.15. 设 $D \in \mathrm{Div}(L)$，并设 $I = I(D)$ 与 $I_\infty = I_\infty(D)$。我们有

$$\exp(B) + \exp(B_\infty) \le \exp(I) + \exp(I_\infty) \le \deg(D^+) + \deg(D^-) + \exp(B) + \exp(B_\infty) \tag{8}$$

且 $h(q_I) + |m_{I_\infty}| \le \deg(D^+) + \deg(D^-)$。
证明。我们先证明第二点。根据引理 $h(q_I) + |m_{I_\infty}| = \sum_{p \in \mathscr{P}_K} |m_p|$ 次数 p 4.14 (约定 次数 $\infty = 1$)。设 $p \in \mathscr{P}$ 并设 $\mathfrak{p}_0 | p$ 使得 $m_p = \left\lfloor \frac{n_{\mathfrak{p}_0}}{e_{\mathfrak{p}_0}} \right\rfloor$。

- 如果 $n_{\mathfrak{p}_0} > 0$ 那么 $0 < n_{\mathfrak{p}_0}/e_{\mathfrak{p}_0} \le n_{\mathfrak{p}_0}$。因此，$0 \le \lfloor n_{\mathfrak{p}_0}/e_{\mathfrak{p}_0} \rfloor \le n_{\mathfrak{p}_0}$ 且 $|m_p| \le |n_{\mathfrak{p}_0}|$。
- 如果 $n_{\mathfrak{p}_0} < 0$，那么 $0 > n_{\mathfrak{p}_0}/e_{\mathfrak{p}_0} \ge n_{\mathfrak{p}_0}$。因此，$0 \ge \lfloor n_{\mathfrak{p}_0}/e_{\mathfrak{p}_0} \rfloor \ge n_{\mathfrak{p}_0}$ 和 $|m_p| \le |n_{\mathfrak{p}_0}|$。

由于 次数 $p \le$ 次数 $\mathfrak{p}_0$ 根据命题 3.9，我们得到 $|m_p|$次数 $p \le |n_{\mathfrak{p}_0}|$次数 $\mathfrak{p}_0 \le \sum_{\mathfrak{p}|p} |n_{\mathfrak{p}}|$次数 $\mathfrak{p}$。对所有 $p \in \mathscr{P}_K$求和，得到

$$h(q_I) + |m_{I_\infty}| \le \sum_{\mathfrak{p} \in \mathscr{P}_K} |n_{\mathfrak{p}}| \deg \mathfrak{p} = \deg(D^+) + \deg(D^-),$$

如所要求的。

现在证明不等式 (8)。由于 $A[x] \subset B \subset I^*$，显然 $\exp(B) \le \exp(I)$。取 $a, b \in A$ 使得 $aI^* \subset B$且 $bB \subset A[x]$。我们有 $abI^* \subset A[x]$。因此，$\exp(I) \le \deg(a) + \deg(b)$。考虑次数最小的 b，我们得到 $\exp(I) \le \deg(a) + \exp(B)$，剩下的就是用 D 来界定 $\deg a$。我们先构造这样的 a。记 $l_p = \max\{\lceil n_{\mathfrak{p}}/e_{\mathfrak{p}} \rceil \mid \mathfrak{p}|p\}$ （对 $p \in \mathscr{P}_A$），并考虑 $a = \prod_{p \in \mathscr{P}_A} p^{l_p - m_p}$。由于 $l_p \ge m_p$，我们有 $a \in A$。对于所有 $p \in \mathscr{P}_A$ 和所有 $\mathfrak{p}|p$，都有 $v_{\mathfrak{p}}(p) = e_{\mathfrak{p}}$ （定义 3.8），而引理 4.14 给出

$$v_{\mathfrak{p}}(aI^*) = e_{\mathfrak{p}}(l_p - m_p) + e_{\mathfrak{p}} m_p - n_{\mathfrak{p}} = e_{\mathfrak{p}} l_p - n_{\mathfrak{p}} \ge 0.$$

由此可得 $aI^* \subset B$，接下来只需对 $\deg a$ 进行界定。我们有

$$l_p \le \max_{\mathfrak{p}|p, n_{\mathfrak{p}} > 0} \left\lceil \frac{n_{\mathfrak{p}}}{e_{\mathfrak{p}}} \right\rceil \le \max_{\mathfrak{p}|p, n_{\mathfrak{p}} > 0} n_{\mathfrak{p}} \qquad \text{and} \qquad m_p \ge \min_{\mathfrak{p}|p, n_{\mathfrak{p}} < 0} \left\lfloor \frac{n_{\mathfrak{p}}}{e_{\mathfrak{p}}} \right\rfloor \ge \min_{\mathfrak{p}|p, n_{\mathfrak{p}} < 0} n_{\mathfrak{p}}.$$

再次利用对所有 $\mathfrak{p}|p$ 都有 $\deg p \le \deg \mathfrak{p}$，可得

$$\deg(a) = \sum_{p \in \mathscr{P}_A} (l_p - m_p) \deg(p) \le \sum_{\mathfrak{p} \in \mathscr{P}_0 | n_{\mathfrak{p}} > 0} n_{\mathfrak{p}} \deg \mathfrak{p} - \sum_{\mathfrak{p} \in \mathscr{P}_0 | n_{\mathfrak{p}} < 0} n_{\mathfrak{p}} \deg \mathfrak{p} = \deg(D_0^+) + \deg(D_0^-)$$

其中 D_0 是 D 的有限部分。因此 $\exp(I) \le \deg(D_0^+) + \deg(D_0^-) + \exp(B)$。同理可证明 $\exp(I_\infty) \le \deg(D_1^+) + \deg(D_1^-) + \exp(B_\infty)$，其中 D_1 是 D 的无穷部分。由于 $D = D_0 + D_1$，结论得证。 □

命题 4.15 的上界在某些情况下是紧的，但在另一些情况下则相当粗糙。下面我们根据由规范化理想定义的除子，给出另一种估计。

命题 4.16。 设 D^* 是由以下分式理想对定义的除子 (I^*, I_∞^*)，遵循命题*4.1*。

1. 我们有 $D^* \ge 0$，且 $D^* = D + \operatorname{div}(q) + rD_\infty$，其中某个 $q \in K = k(t)$ 以及某个 $r \in \mathbb{Z}$。
2. 我们有 $q = q_I$和 $r = m_{I_\infty} +$ 次数 q_I。
3. 如果 $D_0^* \ne D^*$ 对某些 q_0、r_0满足第 *1* 点，那么 $D_0^* > D^*$、$r < r_0$ 和 $q_0/q \in k[t]$，且非常数。
4. 以下不等式成立：

$$\exp(I) + \exp(I_\infty) \le \deg(D^*) + \exp(B) + \exp(B_\infty) \tag{9}$$

证明。第 1 点。由于 $B \subset I^*$ 和 $B_\infty \subset I_\infty^*$ 分别由引理 4.7 和引理 4.12 得出，每个 $\mathfrak{p}$ 都以负指数出现在 I^* 和 I_∞^*中，因此由 (4) 可推得 $D^* \ge 0$。考虑 $q = q_I$ 和 $m = m_{I_\infty}$。我们有 $I(D) = I = qI^* = qI(D^*) = I(D^* - \operatorname{div}(q))$，第二个等式由定义 4.6 得出，第三个等式由 D^* 的定义得出，第四个等式由 (4) 得出。因此，

$$D = D^* - \operatorname{div}(q) + D' \tag{10}$$

对于某个 D' 由（4）支撑于无穷远处。同理，$I_\infty = u^m I_\infty^* = t^{-m} I_\infty^*$（定义 4.11）蕴含$I_\infty(D) = I_\infty(D^* + \operatorname{div}(t^m))$，因此

$$D = D^* + \operatorname{div}(t^m) + D'' \tag{11}$$

对某个支集位于有限处的 D''。令 $D_\infty = \operatorname{div}_\infty(t) = \operatorname{div}_0(t^{-1}) \ge 0$ 为无穷处除子。由于$q \in K$，$-\operatorname{div}(q)$的无穷部分恰为$\deg(q)D_\infty$，而$\operatorname{div}(t^m)$的无穷部分为 $-mD_\infty$。通过比较(10)和(11)中的无穷处部分，我们推得 $D' = -(m + \deg q)D_\infty$。再次利用(10)，得到 $D^* = D + \operatorname{div}(q) + rD_\infty$，其中 $r = m + \deg q$。这证明了第1点，并且 $q = q_I$ 和$m = m_{I_\infty}$ 是解。我们同时证明第2点和第3点。沿用记号 $q = q_I$ 和 $m = m_{I_\infty}$，且$r = m + \deg q$。令 $D_0^* = D + r_0 D_\infty + \operatorname{div}(q_0)$，其中 $D_0^* \ge 0$、$q_0 \in K$ 且 $m_0 \in \mathbb{Z}$。因此

$$q_0 \in \mathscr{L}(D + r_0 D_\infty) \cap K. \tag{12}$$

根据命题 4.1，特别得到 $q_0 \in I(D + r_0D_\infty) \cap K = I(D) \cap K = qA$；第一个等式由(4)得出，因为 r_0D_∞ 支集位于无穷远处；第二个等式则由 $q = q_I$的定义 4.6 得出。因此，对于某个$a \in A = k[t]$，有 $q_0 = aq$。特别地，a 在有限处没有极点，且$\operatorname{div}(q_0) - \operatorname{div}(q) = \operatorname{div}(a) = \operatorname{div}_0(a) - \deg(a)D_\infty$。我们得到

$$D = D_0^* - r_0D_\infty - \operatorname{div}(q_0) = D^* - rD_\infty - \operatorname{div}(q) \quad \Longrightarrow \quad D_0^* = D^* + \operatorname{div}_0(a) + (r_0 - r - \deg a)D_\infty. \tag{13}$$

另一方面，(12) 和命题 4.1 给出 $q_0 \in I_\infty(D + r_0D_\infty) \cap K$。由于 r_0D_∞ 是$\operatorname{div}(t^{-r_0})$的无穷部分，我们得到

$$I_\infty(D + r_0D_\infty) \cap K = I_\infty(D + \operatorname{div}(t^{-r_0})) \cap K = t^{r_0}I_\infty(D) \cap K = t^{r_0-m}A_\infty,$$

根据定义 4.11，最后一个等式成立，因为 $m = m_{I_\infty}$。因此 $q_0t^{m-r_0} \in A_\infty$，即 $\deg q_0 + m - r_0 \leq 0$。由于 $m = r - \deg(q)$，我们得到 $r_0 - r - \deg a \geq 0$。结合 (13)，我们推得 $D_0^* \geq D^*$，当且仅当 $a \in k$ 和 $r = r_0$时等号成立。这就证明了第 2 点和第 3 点。最后，根据定义 4.6，我们有 $\exp(I) = \exp(I^*)$，并且根据 D^*的定义，$I(D^*) = I^*$。因此，$\exp(I) = \exp(I(D^*))$，在无穷远处同样成立。第 4 点由命题 4.15 应用于有效除子 D^*得出。 □

简言之，命题 4.16 表明：

- 除子 D^* 是与 D 模 D_∞ K-线性等价的次数最小的有效除子。
- 量 $\exp(I) + \exp(I_\infty)$度量了 D 模 D_∞的 K-主性的缺陷。
- 量 $r_D = \deg(q_I) + m_{I_\infty}$ 满足以下关系：

$$\deg D^* = \deg D + nr_D \qquad \text{and} \qquad r_D = \min\{r \in \mathbb{Z},\ \mathscr{L}(D + rD_\infty) \cap K \neq \{0\}\},$$

第一次等式由第 1 点得出，因为 $\deg(\operatorname{div}(q)) = 0$ 且 $\deg D_\infty = n$；第二次等式则由结合第 1、2、3 点得到。

注 *4.17*。界 *(9)* 可能比 *(8)* 好得多。特别地，如果对于某个 $q \in K$ 以及某个 $r \in Z$，有 $D = \operatorname{div}(q) + rD_\infty$，那么 $D^* = 0$，且 *(9)* 给出了 $\exp(I) + \exp(I_\infty) = \exp(B) + \exp(B_\infty)$ 的最小可能值，该值不依赖于 $\deg(D)$；而当 $h(q)$ 增大时，上界 *(8)* 可能变得任意大。

另一方面，如果 D 为负且远非 K模 D_∞主，则界 (8) 更好。一个例子是 $D = -N\mathfrak{p}$ 其中 $N > 0$，$e_\mathfrak{p} = f_\mathfrak{p} = 1$。由引理 $\deg D = -N$，$r_D = \deg q_I + m_{I_\infty} = N$，可得 *4.14*，因此 $\deg D^* = \deg D + nr_D = (n-1)N > N = \deg D^+ + \deg D^-$。

5 从整基到黎曼–罗赫空间

给定 $I(D)$ 和 $I_\infty(D)$ 的一些整基，现在我们要计算 $\mathscr{L}(D) = I(D) \cap I_\infty(D)$ 的一个 k-基。我们遵循 Hess 的算法 [32]（另见 Bauch 的学位论文 [9]），沿用 Schmidt[58] 的开创性工作。回顾一下，无穷处除子是 $D_\infty = \operatorname{div}_\infty(t)$。它的支集位于无穷位。对于任意整数 r，我们将计算 $\mathscr{L}(D + rD_\infty)$ 的一个k-基。

5.1 Hess 算法

一个关键概念是约化基，我们将用行约化矩阵来表述。对于$b \in k(t)^n$，令 $\deg(b)$ 表示 b 各项的最大次数。

定义 5.1. 设 $b_0, \ldots, b_{n-1} \in k(t)^n$。我们将由行 b_i 组成的矩阵记作 $\mathbf{M} = (b_0, \ldots, b_{n-1}) \in k(t)^{n\times n}$。

- $\mathbf{M}$ 的行次数为 $\operatorname{rdeg}(\mathbf{M}) = (\deg(b_0), \ldots, \deg(b_{n-1})) \in \mathbb{Z}^n$。
- 若$\mathbf{M}$满足以下条件，则称其为行约化矩阵：

$$\deg\left(\sum \lambda_i b_i\right) = \max_i \deg(\lambda_i b_i) \quad \textit{for all } \lambda_i \in k(t).$$

引理 5. **2.** 对于 $s \in \mathbb{Z}^n$，记 $|s| \in \mathbb{Z}$ 为 s各项之和。若 $\mathbf{M} \in k(t)^{n\times n}$ 非奇异 r.

1. 矩阵 $\mathbf{M}$ 是行约化的，当且仅当 $\deg\det(\mathbf{M}) = |\operatorname{rdeg}(\mathbf{M})|$。

2. 存在么模矩阵 $\mathbf{U} \in k[t]^{n\times n}$，使得 $\mathbf{UM}$ 是行约化的。

证明。这是标准结论，参见例如 [36, 第 6 章3], [69, 第 2 节7] 或 [32,引理 41]。 □

与上一节一样，我们假设 $L = k(t)[X]/(f)$ 是某个不可约首一可分多项式f，其次数为 n。因此 $L = k(t)[x]$ 是一个 $k(t)$-向量空间，其维数为 n。以下是 [32]的关键结果。

命题 5.3. 设 $D \in \mathrm{Div}(L)$。设 $\mathscr{B} = (b_0, \ldots, b_{n-1})$ 为 $I(D)$ 的一个 A-基，且 $\mathscr{B}_\infty$ 为$I_\infty(D)$的一个 A_∞-基。

- $\mathscr{B}$ 与 $\mathscr{B}_\infty$ 都构成 $k(t)$-向量空间 L的一个基。
- 设$\mathbf{P} \in k(t)^{n\times n}$ 为基 $\mathscr{B}$ 在基 $\mathscr{B}_\infty$下表示的矩阵。若$\mathbf{P}$ 是行约化的，则对所有$r \in \mathbb{Z}$，黎曼–罗赫空间 $\mathscr{L}(D + rD_\infty)$ 具有 k-基

$$(b_i t^j,\ 0 \le i \le n-1,\ 0 \le j \le d_i + r)$$

  其中$(d_0, \ldots, d_{n-1}) = -\operatorname{rdeg}(\mathbf{P})$。
- 整数 s $d_i \in \mathbb{Z}$ 由子环 $A \subset L$ 与除子 D唯一确定（在置换意义下）.

证明。这由 [32] 中的定理 5.1 和算法 6.1 得出（细微区别在于，这里我们处理行向量，而 [32] 处理列向量）。该定理源于以下基的存在性： $I = I(D)$ 的基 $(b_0, \ldots, b_{n-1})$，以及 $I_\infty = I_\infty(D)$ 的基 $(v_0, \ldots, v_{n-1})$，使得 $b_i = t^{-d_i} v_i$ 对唯一的有理整数 $d_0 \ge \cdots \ge d_{n-1}$ 成立。考虑这些基和命题 4.1，通过将 L 中的元素分别用两组基表示，我们很容易理解如何得到这样的 $\mathscr{L}(D)$ 的 k-基。关于 b_i 的条件，源于将 P 对角化的方法；P 是从 I 的一组基到 I_∞ 的一组基的过渡矩阵。我们对 P 进行行化简，这对应于对 I 作基变换；再对 P 进行列化简，这对应于对 I_∞ 作基变换。所得矩阵为对角矩阵。在我们的情形中，我们只需寻找族 $(b_0, \ldots, b_{n-1})$，因此只需进行行化简。

□

定义 5.4。 一族 $((b_0, d_0)\ldots\ldots, (b_{n-1}, d_{n-1}))$ 如命题 5.3 中所述，称为 $\mathscr{L}(D$ 的压缩基).

注记 5.5. 注意，即使 $\mathscr{L}(D) = \{0\}$，压缩基仍然存在，这对应于对所有 i 均有 $d_i < 0$ 的情形。若要针对某个 $r \in \mathbb{Z}$ 计算 $\mathscr{L}(D + rD_\infty)$，则在这种情形下计算压缩基是有意义的。

在下文中，我们将 $b \in L = k(t)[x]$ 自由地等同于它在 $k(t)$-向量空间 L 的基 1，x，……，x^{n-1} 下的系数行向量。由此我们得到如下算法：

算法 1 Hess 算法

输入： $L = k(t)[X]/(f)$，其中 $f \in k[t][X]$ 为首一且可分，以及 $D \in \mathrm{Div}(L)$。**输出：** $\mathscr{L}(D)$ 的一个压缩基。

1: 计算 $\mathbf{M}$，使其各行构成 A-基 $\mathscr{B}$，即 $I(D)$ 的基。2: 计算 $\mathbf{N}$，使其各行构成 A_∞-基 $\mathscr{B}_\infty$，即 $I_\infty(D)$ 的基。3: 计算 $\mathbf{U} \in k[t]^{n\times n}$ 幺模矩阵，使得 $\mathbf{UMN}^{-1}$ 为行约化。4: 计算 $\mathbf{UM}$，记作 $\mathbf{UM} = (b_0, \ldots\ldots, b_{n-1})$。5: **返回** $((b_i,\ d_i)\ 0 \le i \le n-1)$，其中 $(d_0, \ldots\ldots, d_{n-1}) = -\operatorname{rdeg}(\mathbf{UMN}^{-1})$。

定理 5.6. 该算法是正确的。

证明。 存在性：$\mathbf{U}$ 的存在性由引理 5.2 保证。由于 $\mathbf{U} \in k[t]^{n\times n} = A^{n\times n}$ 是幺模的，$\mathbf{UM}$ 的各行仍构成一个 A-基 $\mathscr{B}'$，即 $I(D)$。 $\mathscr{B}'$ 在基 $\mathscr{B}_\infty$ 下的矩阵由 $\mathbf{P} = \mathbf{UMN}^{-1}$ 给出，且该矩阵是行约化的。因此该结果由命题 5.3 得出。

□

步骤 1 和 2 的复杂度已在上一节中分析。我们需要研究其余步骤的复杂度。一个棘手的问题是，如果使用由 $(\mathbf{MN}^{-1}$ 和 $\mathbf{UM}$ 的计算开销过大，其中矩阵 $\mathbf{N}$ 是由 (A_∞-基构成的三角形 $I_\infty(D)$) 给出的7)。我们需要先计算 $\mathbf{N}$的一个合适的标准形。先给出一些关于多项式矩阵的辅助复杂度结果。

5.2 多项式矩阵的乘法、求逆与化简

下文中，矩阵的次数是指其各项的最大次数。

命题 5.7。 设 $\mathbf{E}$、$\mathbf{F} \in k[t]^{n\times n}$，且 $d = \deg \mathbf{E}$ 和 $e = \deg \mathbf{F}$。则：

1. $\deg(\mathbf{EF}) \le d + e$。
2. 我们可以在 $\mathscr{O}_\epsilon(n^\omega(d + e + 1))$ 时间内计算 $\mathbf{EF}$。

证明。 将 $\mathbf{E}$、$\mathbf{F}$ 视为以 t 为系数所在的 $k^{n\times n}$中的多项式，不等式 $\deg(\mathbf{EF}) \le d+e$ 显然成立。第二点由 [17]得出。 □

接下来，我们需要估算计算多项式矩阵的行约化形式（定义 5.1）的代价。

命题 5.8. 设 $\mathbf{E} \in k[t]^{n\times n}$ 的次数为 d。我们可以在 $\mathscr{O}(n^\omega(d+1))$ 的时间内计算出 $\mathbf{E}$ 的行约化形式 $\mathbf{E}_{\text{red}}$。于是有 $\deg\mathbf{E}_{\text{red}} \le \deg\mathbf{E}$。

证明。 第一点可由例如 [44, 定理 1.4]得出。我们有 $\operatorname{rdeg}(\mathbf{E}) \ge \operatorname{rdeg}(\overline{\mathbf{E}_{\text{red}}})$，参见 [69, 引理 2.14],其中 a是 $a \in \mathbb{Z}^{\overline{n}}$ 中各项按递增顺序排列所得的列表。特别地，这意味着 $\deg(\mathbf{E}_{\text{red}}) \le \deg(\mathbf{E})$。 □

最后，我们将使用以下关于多项式矩阵求逆的关键事实：

命题 5.9. 设 $\mathbf{F} \in k[t]^{n\times n}$ 是一个行约化矩阵，并设 $d \in \mathbb{N}$ 满足：

$$\deg \mathbf{F} \le d \qquad \text{and} \qquad t^d\mathbf{F}^{-1} \in k[t]^{n\times n}.$$

则$\deg(t^d\mathbf{F}^{-1}) \le d$，且$\mathbf{F}^{-1}$ 可在 $\mathscr{O}_\epsilon(n^\omega d)$ 的时间内计算得到。

证明。我们遵循 [55]。根据行列式公式，F 的余子式矩阵满足 $\deg({}^t\mathrm{com(F)}) \le \operatorname{rdeg(F)}$。由于 F 是行约化的，我们有 $\deg(\det\mathrm{(F)}) = |\operatorname{rdeg(F)}|$（引理 5.2）。利用 $\mathrm{F}^{-1} = {}^t\mathrm{com(F)}/\det\mathrm{(F)}$，可得 $\deg(\mathrm{F}^{-1}) \le 0$。因此，$t^d\mathrm{F}^{-1}$ 的次数至多为 d。结合 [55,引理 3.8] 和 [55, 引理 3.6] 可得成本估计（第一个条件用列次数表示为 [55]，但对于我们的目的而言，转置后这一点无关紧要）。策略如下：我们计算 F^{-1} 模 $(t-1)$，并使用快速高阶提升 [64] 推导出 F^{-1} 模 $(t-1)^{d+1}$。由此推导出 $t^d\mathrm{F}^{-1}$ 模 $(t-1)^{d+1}$，再使用快速基数转换推导出 t-进制展开的 $t^d\mathrm{F}^{-1}$。 □

注 5.10. 关于多项式矩阵的乘法与约简，已有更精细的复杂度结果，这些结果考虑了输入矩阵各行（或各列）的平均次数（例如参见 [44]）。我们的目的并不需要这些改进。

5.3 重新审视 Hess 算法

从现在起，我们分别用 $I = I(D)$ 和 $I_\infty = I_\infty(D)$ 表示，并令 $\mathscr{B}, \mathscr{B}^*$ 和 $\mathscr{B}_\infty, \mathscr{B}_\infty^*$ 分别表示由式（5）和（7）定义的三角基。简记为

$$d = \exp(I) \qquad \text{and} \qquad e = \exp(I_\infty). \tag{14}$$

（参见定义 4.6 和定义 4.11）。因此有 $d =$ 次数 p_{n-1} 以及 $e = m_{n-1}$，采用式（5）和（7）中的记号。

引理 5.11. 设 $\mathbf{M}^*$ 是基 $\mathscr{B}^*$ 在基 $1, x, \ldots, x^{n-1}$下表示的矩阵。矩阵 $\mathbf{M}^*$ 是下三角矩阵，并且有

$$p_{n-1}\mathbf{M}^* = \tilde{\mathbf{M}}, \quad \tilde{\mathbf{M}} \in k[t]^{n\times n}, \quad \deg(\tilde{\mathbf{M}}) = d.$$

证明。 这可由（5）和（14）直接得出。 □

回想一下，我们记作 $u = t^{-1}$。因此 $\deg_u = -\deg_t$。

引理 5.12. 设 $\mathbf{N}^*$ 是基 $\mathscr{B}_\infty^*$ 在基 $1, x, \ldots, x^{n-1}$ 下的矩阵，并令 λ 如 (6)中所示。我们有

$$u^e\mathbf{N}^* = \tilde{\mathbf{N}} \quad \textit{where} \quad \tilde{\mathbf{N}} \in k[u]^{n\times n}, \quad \deg_u(\tilde{\mathbf{N}}) \le e + n\lambda.$$

此外，我们有 $u^{e+n\lambda}\,\tilde{}\,\mathbf{N}^{-1} \in k[u]^{n\times n}$。

证明。令 $\mathbf{N}'$ 为 $\mathscr{B}_\infty^*$ 在基 $\mathbf{1}, y, \ldots, y^{n-1}$下的矩阵。由于 $y = xu^\lambda$，$\mathscr{B}_\infty^*$ 在基 $\mathbf{1}, x, \ldots, x^{n-1}$ 下的矩阵为 $\mathbf{N}^* = \mathbf{N}'\mathbf{D}$，其中 $\mathbf{D} = \operatorname{diag}(1, u^\lambda, \ldots, u^{(n-1)\lambda})$。由（7）和（14）可直接推出 $\tilde{}$ $\tilde{}$that $u^e\mathbf{N}' \in k[u]^{n\times n}$，$\deg_u(u^e\mathbf{N}') = e$。因此，$\mathbf{N} = u^e\mathbf{N}'\mathbf{D} \in k[u]^{n\times n}$ 且 $\deg_u \mathbf{N} \le \deg(u^e\mathbf{N}') + \deg \mathbf{D} \le e + n\lambda$，证毕。对于第二点，我们有 $u^{e+n\lambda}\,\tilde{}\,\mathbf{N}^{-1} = u^{n\lambda}\mathbf{D}^{-1}\mathbf{N}'^{-1}$。由于 $u^{n\lambda}\mathbf{D}^{-1} \in k[u]^{n\times n}$，只需证明 $\mathbf{N}'^{-1} \in k[u]^{n\times n}$。由（7）可得 $\mathbf{N}' = \mathbf{D}'\mathbf{T}$，其中 $\mathbf{T} \in k[u]^{n\times n}$ 是对角线上全为 1 的下三角矩阵（特别地，$\mathbf{T}$ 是幺模矩阵），而 $\mathbf{D}'$ 是一个对角矩阵，其元素属于 $k[u^{-1}]$。因此，$\mathbf{T}^{-1}$ 和 $\mathbf{D}'^{-1}$ 都属于 $k[u]^{n\times n}$，故 $\mathbf{N}'^{-1} \in k[u]^{n\times n}$，如所需。 □

~

~**引理 5.13.** 设 $\mathbf{N}_{\text{red}} \in k[u]^{n\times n}$ 为 $\mathbf{N}$ 的行约化形式。我们有：

(i) $\deg_u(\tilde{\mathbf{N}}_{\text{red}}) \le e + n\lambda$

(ii) $u^{e+n\lambda}\tilde{\mathbf{N}}_{\mathrm{red}}^{-1} \in k[u]^{n\times n}$

(iii) $\deg_u(u^{e+n\lambda}\tilde{\mathbf{N}}_{\mathrm{red}}^{-1}) \le e+n\lambda.$

给定 $\tilde{\mathbf{N}}$，我们可以同时计算矩阵 $\tilde{\mathbf{N}}_{\mathrm{red}}$ 及其逆矩阵 $\tilde{\mathbf{N}}^{-1}{}_{\mathrm{red}}$，时间为 $\tilde{O}(n^\omega(e+n\lambda))$。

证明。由引理 5.12 和命题 5.8 可得 (i) 以及计算 $\mathrm{N}_{\mathrm{red}}$ 的复杂度。我们有 $\tilde{\mathrm{N}}_{\mathrm{red}} = \mathrm{U}\tilde{\mathrm{N}}$，其中 $\mathrm{U} \in k[u]^{n\times n}$ 是幺模矩阵，因此 $\tilde{\mathrm{N}}^{-1}\,\mathrm{red} = \tilde{\mathrm{N}}^{-1}\mathrm{U}^{-1}$，且 $\mathrm{U}^{-1} \in k[u]^{n\times n}$，由引理 5.12 可得 (ii)。最后，由 (i)、(ii) 和命题 5.9 可得 (iii) 以及计算 $\tilde{\mathrm{N}}^{-1}\,\mathrm{red}$ 的复杂度。 □

在接下来的两个引理中，我们将重新讨论坐标 $t = u^{-1}$。

引理 5.14。 设 $\mathbf{P} = \tilde{\mathbf{M}}\,\tilde{\mathbf{N}}^{-1}{}_{\mathrm{red}}$。则 $\mathbf{P} \in k[t]^{n\times n}$ 且 $\deg_t \mathbf{P} \le d+e+n\lambda$。我们可以在时间 $\tilde{O}(n^\omega(d+e+n\lambda))$ 内计算 $\mathbf{P}$。

证明。由引理 5.11，我们有 $\mathbf{M} \in k[t]^{n\times n}$，$\deg_t \mathbf{M} = d$。由引理 5.13 (ii) 和 (iii)，我们推出 $\tilde{\mathbf{N}}^{-1}{}_{\mathrm{red}} \in k[u^{-1}]^{n\times n} = k[t]^{n\times n}$ 且 $\deg_t \tilde{\mathbf{N}}^{-1}{}_{\mathrm{red}} \le e+n\lambda$。因此该结果由命题 5.7。 □

引理 5.15。 我们可以计算行约化形式 $\mathbf{P}_{\mathrm{red}} \in k[t]^{n\times n}$（即 $\mathbf{P}$ 的行约化形式），所需时间为 $\tilde{O}(n^\omega(d+e+n\lambda))$。我们有 $\deg_t(\mathbf{P}_{\mathrm{red}}) \le d+e+n\lambda$。

证明。这由命题 5.8 和引理 5.14 得出。 □

引理 5.16。 设 $\mathbf{U} \in k[t]^{n\times n}$ 为幺模矩阵，使得 $\mathbf{P}_{\mathrm{red}} = \mathbf{UP}$。我们可以计算 $\mathbf{MUM} \in k[t]^{n\times n}$，所需时间为 $\tilde{O}(n^\omega(d+e+n\lambda))$。

证明。根据引理 $\mathbf{P}$ 的定义，在引理 5.14 中，我们有 $\mathbf{UM} = \mathbf{UPN}_{\mathrm{red}} = \mathbf{P}_{\mathrm{red}}\mathbf{N}_{\mathrm{red}}$. 根据引理 5.13 (i)，且由于 $u = t^{-1}$，我们可推得 $t^{e+n\lambda}\tilde{\mathbf{N}}_{\mathrm{red}} \in k[t]^{n\times n}$ 的次数至多为 $e+n\lambda$ 在 t 中。因此，计算 $t^{e+n\lambda}\mathbf{P}_{\mathrm{red}}\tilde{\mathbf{N}}_{\mathrm{red}}$ 根据引理 5.15 和命题 5.7，其复杂度符合预期的上界。接下来只需将所得矩阵除以 $t^{e+n\lambda}$，这一步可以免费完成。 □

注 5.17。 显然，我们本可以更仔细地研究各个步骤的复杂度，尤其是考虑到 $\tilde{\mathbf{N}}_{\mathrm{red}}$ 是对角矩阵 $\mathbf{D} = (1, u^\lambda, \ldots, u^{(n-1)\lambda})$ 的左倍数。一般来说，这不会改善总体成本估计，但当无穷远处的指标为零时，可以略微改进，见小节 *5.4*。

我们现在可以重新审视 Hess 算法，以得到复杂度估计。

算法 2 黎曼–罗赫

输入： $L = k(t)[X]/(f)$，其中 $f \in k[t][X]$ 为首一且可分，且 $D \in \mathrm{Div}(L)$ 由 OM 表示给出。**输出：** $\mathscr{L}(D)$ 的压缩基。

1：计算 $\mathbf{M} \in k[t]^{n\times n}$，如引理 5.11 所述，利用定理 4.8。2：计算 $\mathbf{N} \in k[u]^{n\times n}$，如引理 5.12 所述，利用定理 4.13。3：计算行约化形式 $\tilde{\mathbf{N}}_{\mathrm{red}}$，即 $\tilde{\mathbf{N}}$ 在 $k[u]^{n\times n}$ 中的行约化形式，并用引理 5.13 计算 $\tilde{\mathbf{N}}^{-1}\,\mathbf{red}$。4：计算 $\mathbf{P} = \tilde{\mathbf{M}}\,\tilde{\mathbf{N}}^{-1}\,\mathbf{red} \in k[t]^{n\times n}$，用引理 5.14。5：计算行约化形式 $\mathbf{P}_{\mathrm{red}} = \mathbf{UP}$，在 $k[t]^{n\times n}$ 中用引理 5.15。6：计算 $\mathbf{M}_{\mathrm{red}} = \mathbf{UM}$，在 $k[t]^{n\times n}$ 中用引理 5.16。7：计算 $\mathbf{M}_{\mathrm{red}} = \frac{q}{p_{n-1}}\mathbf{M}_{\mathrm{red}} \in k(t)^{n\times n}$，其中 $q \in k(t)$ 与 $p_{n-1} \in k[t]$ 如 (5) 中所述。8：令 $\delta = m_{n-1} - m - \deg(q/p_{n-1})$，其中 $m_{n-1} \in \mathbf{N}$ 与 $m \in \mathbf{Z}$ 如 (7) 中所述。9：返回

$$((b_i, d_i),\ 0 \le i \le n-1)$$

其中 $(b_0, \ldots, b_{n-1}) = \mathbf{M}_{\mathrm{red}}$ 且 $(d_0, \ldots, d_{n-1}) = -\mathrm{rdeg}\,\mathbf{P}_{\mathrm{red}} + (\delta, \ldots, \delta)$。

回顾 $b_i \in k(t)^n$ 被等同于 $k(t)[x]$ 在第 9 步中的一个元素。利用定义 4.6 与定义 4.11 的记号，我们得到：

定理 5.18. 该算法返回正确答案。它至多执行

- $\tilde{O}(n^\omega(\exp(I) + \exp(I_\infty) + n\lambda) + n^2h(q_I))$ 次运算（在 k 中），若 $\mathrm{char}(k) = 0$ 或 $\mathrm{char}(k) > n$，
- $\tilde{O}(n^\omega(\exp(I) + \exp(I_\infty) + n\lambda) + n^2h(q_I) + \delta^2 + \delta_\infty^2)$ k 中的运算。

证明。正确性。设$\mathbf{M}$和$\mathbf{N}$分别为$\mathscr{B}$和$\mathscr{B}_\infty$在规范基 1，x，……，x^{n-1}中的矩阵。根据记号（5）和（7），以及引理5.11 和引理5.12的记号，我们因此有

$$\mathbf{M} = q\mathbf{M}^* = \frac{q}{p_{n-1}}\tilde{\mathbf{M}} \qquad \text{and} \qquad \mathbf{N} = u^m\mathbf{N}^* = u^{m-e}\tilde{\mathbf{N}}. \tag{15}$$

~ ~根据构造，对于某个幺模矩阵 V，有 $\mathbf{N}_{\text{red}} = \mathbf{VN} \in k[u]^{n\times n}$。因此，V 在 $A_\infty = k[u]_u$ 上是幺模的，并且 $\mathbf{N}_{\text{red}} := u^{m-e}\,\tilde{}\mathbf{N}_{\text{red}} = \mathbf{VN}$ 的各行仍构成 $\mathscr{B}_\infty$的 A_∞-基。由于矩阵 $\mathbf{P}_{\text{red}} = \mathbf{U}\,\tilde{}\mathbf{M}\,\tilde{}\mathbf{N}^{-1}$ red 在第 5 步（相对于 $\deg_t$）是行约化的，由定义 5.1 可知，矩阵 $\mathbf{P}_0 := \mathbf{UMN}^{-1}$ red 也同样是行约化的，因为它是 $\mathbf{P}_{\text{red}}$ 的一个 K-倍。由算法 1 和定理 5.6 可知，$\mathscr{L}(D)$ 的一个压缩基由 $(b_0, \ldots, b_{n-1}) := \mathbf{UM}$ 以及 $(d_0, \ldots, d_{n-1}) := -\operatorname{rdeg}(\mathbf{P}_0)$ 给出。结合 (15)、$e = \exp(I_\infty) = m_{n-1}$（由 (7)）和 $u = t^{-1}$，我们得到

$$\mathbf{UM} = \frac{q}{p_{n-1}}\mathbf{U}\tilde{\mathbf{M}} = \mathbf{M}_{\text{red}} \qquad \text{and} \qquad \mathbf{P}_0 = \frac{qt^{m-m_{n-1}}}{p_{n-1}}\mathbf{P}_{\text{red}},$$

因此 $(b_0, \ldots, b_{n-1}) = \mathbf{M}_{\text{red}}$ 以及 $(d_0, \ldots, d_{n-1}) = -\operatorname{rdeg}\mathbf{P}_{\text{red}} + (\delta, \ldots, \delta)$，其中 $\delta = m_{n-1} - m - \deg(q/p_{n-1})$，由算法2返回。

复杂度。借助定理 4.8 和定理 4.13，结合引理 4.7 和引理 4.12 分别给出的不等式 $n\delta_I \le n^2\exp(I)$ 和 $n\delta_{I_\infty} \le n^2\exp(I_\infty)$，我们在目标界内计算 $\mathbf{M}^*$ 和 $\mathbf{N}^*$。由于 $\deg p_{n-1} = \exp(I)$，且 $\mathbf{M}^*$ 的 n^2 个元素的高度为 $\mathscr{O}(\exp(I))$，我们在目标界内计算 $\tilde{}\mathbf{M} = p_{n-1}\mathbf{M}^*$。从 $\mathbf{N}^*$ 可免费得到 N（乘以 t的某个幂）。步骤 3、4、5、6 的复杂度分别由引理 5.13、引理 5.14、引理 5.15 和引理 5.16 保证在目标界内。~根据引理 5.16（的证明），多项式矩阵 $\mathbf{M}_{\text{red}}$ 的次数至多为 $\exp(I) + \exp(I_\infty) + n\lambda$。由于$q = q_I$ 且 $\deg p_{n-1} = \exp(I)$，我们推得步骤 7 中计算 $\mathbf{M}_{\text{red}}$ 符合目标界。

□

再者，在考察用 $K = k(t)$ 的元素进行各种矩阵乘法时，我们本可以更仔细地分析其复杂度。不过，这并不会降低总体成本估计。

注 5.19. 我们也可以不在第 7 步执行乘积运算，而是返回一个（未展开的）乘积列表 ~ ~ ~ ~ ~(qb0, qb1/p1, . . . , qbn−1/pn−1) 其中 b_i 由 $\mathbf{M}_{\text{red}}$的各行给出。在这种情况下，复杂度估计中就不需要额外项 $h(q_I)$。如果 $\exp(I) << h(q_I)$，也就是说，当 D接近成为 K-主模 D_∞ 时（见注 *4.17*），这一点尤其重要。

5.4 无穷远处的平凡指数情形

如果我们假设 $\exp(I_\infty) = 0$，那么定理 $n\lambda$ 5.18 的复杂度估计中那个令人烦恼的额外项就会消失:

T定理 5.20。 假设$\exp(I_\infty) = 0$。我们可以计算出 $\mathscr{L}(D)$ w 的压缩基 ith

- $\tilde{\mathscr{O}}(n^\omega\exp(I) + n^2h(q_I))$ 次 k 如果 $\operatorname{char}(k) = 0$ 或 $\operatorname{char}(k) > n$,
- $\tilde{\mathscr{O}}(n^\omega\exp(I) + n^2h(q_I) + \delta^2)$ 运算于 k 其他情况。

T证明需要使用矩阵的移位约化，而不是通常的次数约化。

定义 5.21。 令 $\vec{s} = (s_0, \ldots, s_{n-1}) \in \mathbb{Z}^n$ 为一个移位，且$\mathbf{E} \in k(t)^{n\times n}$。若矩阵$\mathbf{E}$ 经 $\vec{s}$ 处理后为行约化，则称其为行约化，其中$\mathbf{D} = \operatorname{diag}(t^{s_0}, \ldots, t^{s_{n-1}})$。

该移位用作列权重。

定理 5.22(~[44])。设$\mathbf{E} \in k[t]^{n\times n}$ 的次数为 d。我们可以在 $\mathscr{O}(n^\omega d$时间内计算$\mathbf{E}$ 的行 $\vec{s}$约化形式).

值得注意的是，复杂度估计不依赖于移位 $\vec{s}$。

定理 5.20 的证明。根据引理 4.12，假设 $\exp(I_\infty) = 0$ 等价于 $\delta_{I_\infty} = 0$，也就是说，由定义 4.11 可得 $\deg[A_\infty[y] : I^*_\infty] = 0$。由于 $A_\infty[y] \subset I^*_\infty$，根据引理 4.3 可得 $A_\infty[y] = I^*_\infty$。因此，$\tilde{}\mathbf{N} = \mathbf{D} = \operatorname{diag}(1, u^\lambda, \ldots, u^{(n-1)\lambda})$ 是对角矩阵（因此是约化的），所以算法得以简化。算法 2 中第 6 步的矩阵 $\tilde{}\mathbf{M}_{\text{red}}$ 与 M 的行 $\vec{s}$-约化形式一致，其中 $\vec{s} = (1, \lambda, \ldots, (n-1)\lambda)$，因此我们可以直接计算 M 的行 $\vec{s}$-约化形式，以此替代步骤 3、4、5、6。根据定理 5.22，其复杂度为 $\mathscr{O}(n^\omega\exp(I))$。注意，$\tilde{}\mathbf{N}_{\text{red}} = \mathbf{D}$，因此 $\mathbf{P}_{\text{red}} = \tilde{}\mathbf{M}_{\text{red}}\mathbf{D}^{-1}$。由此可直接从 $\mathbf{M}_{\text{red}}$ 的行次数推出 $\operatorname{rdeg}\mathbf{P}_{\text{red}} = \operatorname{rdeg}\tilde{}\mathbf{M}_{\text{red}} + (1, \lambda, \ldots, (n-1)\lambda)$~。 □

5.5 一个例子

让我们说明　算法2 通过一个具体例子说明。设 $f = X^3 - X^2 + t^2 \in \mathbb{F}_5(t)[X]$ 如例3.1　　3.

- 令 $p = tA_0$。我们在例 3.13 中看到，位于 p上方的有三个素理想，$\mathfrak{p}_1$，$\mathfrak{p}_2$，$\mathfrak{p}_3$ 其 OM 表示为 $t_{\mathfrak{p}_1} = [t, x-t]$，$t_{\mathfrak{p}_2} = [t, x+t]$ 以及 $t_{\mathfrak{p}_3} = [t, x-1]$。例如，我们有 $tB = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3$ 以及$(x-1)B = \mathfrak{p}_3^2$。
- 令 $p' = (t-1)A_0$。位于 p'上方的素理想恰有两个：$\mathfrak{p}'_1$，$\mathfrak{p}'_2$，其 OM 表示为 $t_{\mathfrak{p}'_1} = [t-1, x+3]$和 $t_{\mathfrak{p}'_2} = [t-1, x, x^2+x+2]$。我们有 $(t-1)B = \mathfrak{p}'_1\mathfrak{p}'_2$。
- 令 $p_\infty = t^{-1}A_{\infty 0}$。根据（6），我们有 $\lambda = 1$，$y = xt^{-1}$ 以及 $y^3 - t^{-1}y^2 + t^{-1} = 0$。存在唯一一个素理想 $\mathfrak{p}_\infty$ 位于 p_∞上方，其 OM 表示为 $\mathfrak{p}_\infty = [t^{-1}, y, y^3 + t^{-1}]$。我们有 $t^{-1}B_\infty = \mathfrak{p}_\infty^3$ 以及 $yB_\infty = \mathfrak{p}_{\infty 0}$。

我们来计算　　与除子 $D = 2\mathfrak{p}_1 + 3\mathfrak{p}_2 - \mathfrak{p}'_1 - \mathfrak{p}'_2 + \mathfrak{p}_\infty \in \mathrm{Div}(\mathbb{F}_5(t)[X]/f$ 相关的黎曼–罗赫空间　　).

步骤 1. 我们有 $I = I(D) = \mathfrak{p}_1^{-2}\mathfrak{p}_2^{-3}\mathfrak{p}'_1\mathfrak{p}'_2$。使用计算机代数系统 SageMath，我们发现这个分式理想的基为

$$\mathscr{B} = (t-1)\mathscr{B}^*, \qquad \text{with} \qquad \mathscr{B}^* = \left(1, \frac{x-1}{t^2}, \frac{x^2 - (t+1)x + t(1+t-t^2)}{t^4}\right).$$

我们有 $I^* = \mathfrak{p}_1^{-2}\mathfrak{p}_2^{-3}$, $q = t-1$, $p_{n-1} = t^4$ 和

$$\tilde{\mathbf{M}} = \begin{pmatrix} t^4 & 0 & 0 \\ -t^2 & t^2 & 0 \\ t(1+t-t^2) & -(t+1) & 1 \end{pmatrix}.$$

步骤 2.　我们有 $I_\infty = I_\infty(D) = \mathfrak{p}_\infty^{-1}$。这个分式理想已正规化，SageMath 给出了一个基　　sis

$$\mathscr{B}_\infty = \mathscr{B}^*_\infty = (1, y, ty^2) = \left(1, \frac{x}{t}, \frac{x^2}{t}\right).$$

我们有 $m = 0$、$m_{n-1} = 1$ 以及

$$\tilde{\mathbf{N}} = \begin{pmatrix} 1/t & 0 & 0 \\ 0 & 1/t^2 & 0 \\ 0 & 0 & 1/t^2 \end{pmatrix}.$$

˜**步骤 3.** 矩阵$\mathbf{N}$ 是对角的，因此是行约化的，其逆矩阵显而易见。

步骤 4. 我们计算

$$\mathbf{P} = \tilde{\mathbf{M}} \times \tilde{\mathbf{N}}^{-1} = \begin{pmatrix} t^5 & 0 & 0 \\ -t^3 & t^4 & 0 \\ t^2(1+t-t^2) & -t^2(t+1) & t^2 \end{pmatrix}.$$

步骤 5. 矩阵$\mathbf{P}$ 不是行约化的。事实上，$\deg(\det(\mathbf{P})) = 11 < |\mathrm{rdeg}(\mathbf{P})| = 13$。我们计算$\mathbf{P}$的行约化形式：

$$\mathbf{P}_{\mathrm{red}} = \begin{pmatrix} t^3+t^2 & -2t^3-t^2 & t^2(t+1) \\ -t^3 & t^4 & 0 \\ 0 & -t^4 & t^4+t^2 \end{pmatrix}.$$

˜　　˜**步骤 6.** 我们计算乘积$\mathbf{M}_{red} = \mathbf{P}_{\mathrm{red}} \times \mathbf{N}_{\mathrm{red}}$：

$$\tilde{\mathbf{M}}_{\mathrm{red}} = \begin{pmatrix} t^2+t & -2t-1 & t+1 \\ -t^2 & t^2 & 0 \\ 0 & -t^2 & t^2+1 \end{pmatrix}.$$

˜**步骤 7.** 我们得到以下元素，对应于$\mathbf{M}_{\mathrm{red}} = {}_{p_{n-1}}^{q}\mathbf{M}_{\mathrm{red}}$的各行　　——　　：

$$b_0 = \frac{t^2-1}{t^2} + x\frac{(3t-1)(t-1)}{t^4} + x^2\frac{t^2-1}{t^4}, \quad b_1 = \frac{1-t}{t^2} + x\frac{t-1}{t^2} \quad \text{and} \quad b_2 = x\frac{1-t}{t^2} + x^2\frac{(t^2+1)(t-1)}{t^4}.$$

步骤 8. 我们有 $\delta = 4$，且 $\mathrm{rdeg}(\mathbf{P}_{\mathrm{red}}) = (3, 4, 4)$，因此 $(d_0, d_1, d_2) = (1, 0, 0)$。

结果： $\mathscr{L}(D)$ 的一个 k-基为（b_0，tb_0，b_1，b_2）。

6 算术与几何（定理1.1的证明）

定理 1.1 中给出的复杂度是用射影平面曲线的 δ 不变量来表述的。为此，我们需要将曲线与函数域联系起来。更多细节见附录 B。

6.1 曲线与函数域

设 $\mathscr{C} \subset \mathbf{P}^2_k$ 是由次数为 n 的齐次多项式$F \in k[X_0, X_1, X_2]$定义的次数为 n 的不可约射影平面曲线。我们用 $k(\mathscr{C})$ 表示 $\mathscr{C}$ 的有理函数域。$k(\mathscr{C})$ 中的元素是同次数齐次多项式的商 G/H，并按 $H \bmod F \neq 0$ 取模；若 $GH' - G'H = 0 \bmod F$，则按等价关系$G/H \sim G'/H'$ 取商。域 $k(\mathscr{C})$ 是 k 上的函数域（每个函数域都可以这样得到）。

定义 6.1。$\mathscr{C}$ 的除子是函数域 $k(\mathscr{C})$ 的除子，其中该函数域属于 $\mathscr{C}$。

等价地，$\mathscr{C}$ 的除子可以看作 $\mathbb{Z}$-正规化 $\mathscr{C}$ 上的闭点的线性组合，$\mathscr{C}$（定理 B.10）。如果 $\mathscr{C}$ 是光滑的，且 k 是代数闭的，那么除子就是曲线上点的$\mathbb{Z}$-线性组合，这也是通常理解除子的方式。

假设 $F \neq X_0$。记 $t = X_1/X_0$ 和 $X = X_2/X_0$，则 $\mathscr{C}$ 在仿射图$U_0 = \{X_0 \neq 0\} \simeq \mathbf{A}^2_k$ 上的限制可识别为由下式定义的仿射曲线 $C \subset \mathbf{A}^2_k$

$$C = \operatorname{Spec} k[t, X]/(f) \quad \text{where} \quad f(t, X) = F(1, t, X) \in k[t, X].$$

C的坐标环为 $k[C] := k[t, X]/(f)$，其函数域为 $k(C) = \operatorname{Frac} k[C]$。采用前几节中使用的记号$A = k[t]$、$K = k(t)$ 和 $x = X \bmod f$，我们便有

$$k[C] = A[x] \quad \text{and} \quad k(C) = K(x).$$

去齐次化诱导出一个同构 $k(\mathscr{C}) \simeq k(C)$。它将 $\mathscr{C} \cap U_0$ 的闭点与 C 的闭点对应起来，并对这样的点诱导出局部环的同构 $\mathscr{O}_{\mathscr{C},\,P} \simeq \mathscr{O}_{C,\,P}$。注意，闭点 $P \in C$ 按定义是 $k[C]$ 的一个极大理想，而 C 在 P 处的局部环为 $\mathscr{O}_{C,\,P} = k[C]_P$（见第 B.1节）。

6.2 B 和 B_∞ 的指标界

为了证明定理 1.1，还需将定义 4.6 和定义 4.11 中定义的 f 的指标 $\delta = \deg[B : A[x]]$ 和 $\delta_\infty = \deg[B_\infty : A_\infty[y]]$ 与输入射影平面曲线$\mathscr{C}$的 delta不变量（定义 B.14）联系起来。我们用 $\mathscr{O}_{\mathscr{C},P}$ 表示 $\mathscr{O}_{\mathscr{C},P}$ 的整闭包。

命题 6.2. 假设 F 在 X_2 中首一且可分。采用上述记号，我们有：

1. $\delta = \sum_{P \in \mathscr{C} \cap U_0} \dim_k \overline{\mathscr{O}_{\mathscr{C},P}}/\mathscr{O}_{\mathscr{C},P}$.
2. $\delta_\infty = \sum_{P \in \mathscr{C} \setminus \mathscr{C} \cap U_0} \dim_k \overline{\mathscr{O}_{\mathscr{C},P}}/\mathscr{O}_{\mathscr{C},P}$.

注意，根据命题 B.2，$\mathscr{O}_{\mathscr{C},P} = \mathscr{O}_{\mathscr{C},P}$ 当且仅当 P 是 $\mathscr{C}$ 的正则点，因此这些求和是在 $\mathscr{C}$ 的有限奇点集合上进行的。

证明。我们来证明第 1 点。令 B 为 $L = k(C)$ 中 A 的整闭包。由于 $A \subset A[x] = k[C]$，我们有$B \subset k[C]$。根据假设，$f(t, X) = F(1, t, X)$ 在 X 中首一且可分。因此 x 在 A 上整，这就推出 $A[x] \subset B$，也就是说 $k[C] \subset B$。由于 B 是整闭的，因此 $k[C] \subset B$，进而 $k[C] = B$。换言之，B 与 C 的正规化 C 的坐标环一致。因此我们有

$$\delta := \deg[B : A[x]] = \dim_k(B/A[x]) = \dim_k(\overline{k[C]}/k[C]). \tag{16}$$

根据定义，闭点 $P \in \mathscr{C} \cap U_0 \simeq C$ 是 $k[C] = A[x]$ 的极大理想，并且我们有 $\mathscr{O}_{\mathscr{C},\,P} \simeq k[C]_P = A[x]_P$（在 P处局部化）。由于整闭包与局部化可交换，我们得到半局部环的一个同构 $\mathscr{O}_{\mathscr{C},\,P} \simeq k[C]_P = B_P$，从而得到

$$\dim_k(\overline{\mathscr{O}_{\mathscr{C},P}}/\mathscr{O}_{\mathscr{C},P}) = \dim_k(B_P/A[x]_P). \tag{17}$$

现在我们沿用 [38, 定理 4 的证明。17]令 $a \in A[x]$ 使得 $aB \subset A[x]$。因此 $aA[x]$ 和 aB 都是 $A[x]$的理想，并且有包含关系 $aA[x] \subset aB$。k-代数 $A[x]/aA[x]$ 是有限生成的，并且

它是零维的，因此有有限个极大理想。于是，中国剩余定理（参见 [38,推论 D4]）保证

$$A[x]/aA[x] = \prod_{P\in \operatorname{Spec} A[x]} A[x]_P/aA[x]_P$$

并且 $aB/aA[x]$ 与 $\prod_{P\in 谱\ A[x]} aB_P/aA[x]_P$. 回想一下，$C =$ 谱 $A[x]$。我们得到

$$\dim_k(B/A[x]) = \dim_k(aB/aA[x]) = \sum_{P\in C} \dim_k(aB_P/aA[x]_P) = \sum_{P\in C} \dim_k(B_P/A[x]_P)$$

结合式（16）和（17），即可得出关于第一个点的结论。

下面证明第 2 点。由于 F 在 X_2中是首一的，因此 $F(0:0:1) \neq 0$。于是，$(0:0:1) \notin \mathscr{C}$，且 $\mathscr{C} \setminus \mathscr{C} \cap U_0 = \mathscr{C} \cap (X_0 = 0)$ 的所有点（即无穷远点）都属于仿射图 $U_1 = \{X_1 \neq 0\}$。记 $u = X_0/X_1 = t^{-1}$ 和 $Y = X_2/X_1 = Xt^{-1}$，则在图 $U_1 \simeq \mathbb{A}_k^2$ 中，$\mathscr{C}$ 的仿射方程由多项式

$$f_\infty \in k[u, Y], \quad f_\infty(u, Y) := u^d f(u^{-1}, u^{-1}Y).$$

剩余类 y Y模 f_∞满足 $y = xt^{-1}$在 $L = k(t, x) = k(u, y)$。由于 f的总次数为 n，式（$\lambda = \lambda(f)$ 中定义的整数（6）满足 $\lambda = 1$，定义 4.11 变为

$$\delta_\infty = \deg[B_\infty : A_\infty[y]],$$

其中 $u = t^{-1}$, $y = xt^{-1}$, $A_\infty = k[u]_{(u)}$ 和 B_∞ 是 L中 A_∞ 的整闭包。无穷远直线 $X_0 = 0$的局部方程为 $u = 0$，而 $\mathscr{C} \setminus \mathscr{C} \cap U_0 = \mathscr{C} \cap (X_0 = 0)$的点与包含 u的 $k[u, y]$ 的极大理想一一对应，因此也与 $A_\infty[y]$的极大理想 P 一一对应。按照上述相同的推理，我们得到

$$\dim_k(B_\infty/A_\infty[y]) = \sum_{P\in\mathscr{C}\setminus\mathscr{C}\cap U_0} \dim_k(B_{\infty,P}/A_\infty[y]_P).$$

借助同构 $A_\infty[y]_P \simeq \mathscr{O}_{\mathscr{C},\ P}$和 $B_{\infty,\ P} \simeq \mathscr{O}_{\mathscr{C},\ P}$，即可得出结论。 □

记 $\delta($ $\mathscr{C})$ 为 $\mathscr{C}$的 δ 不变量，记 $g(\mathscr{C})$ 为其几何亏格，定义见第 B.6节。我们有 et:

推论 6.3。假设 F在 X_2中是首一且可分的。那么 $\delta + \delta_\infty = \delta(\mathscr{C}) = (n-1(n-2)\ 2 - g(\mathscr{C})$。

证明。第一个等式由命题 6.2 和定义 B.14得出。第二个等式由亏格公式（推论 B.16）得出。

□

6.3 定理1.1 的证明

定理 1.1 可由稍一般的结果立即推出。

定理 6.4。设 $\mathscr{C} \subset \mathbb{P}_k^2$ 是次数为 n 由齐次多项式 F 定义的不可约曲线，且该多项式在 X_2中首一且可分。设 $D \in Div(\mathscr{C})$。存在一个确定性算法，可以计算 （定义 5.4）的压缩基 $\mathscr{L}(D)$，其所需

$$\tilde{\mathscr{O}}(n^\omega(\deg(D^+) + \deg(D^-) + \delta(\mathscr{C}) + n)) \subset \tilde{\mathscr{O}}(n^\omega(\deg(D^+) + \deg(D^-) + n^2))$$

算术运算次数为 k。若 $\deg D \geq 0$，复杂度为

$$\tilde{\mathscr{O}}(n^\omega(\deg(D^+) + \delta(\mathscr{C}) + n)).$$

此外，若 $\mathscr{C}$ 的奇异轨迹和 D 的支集均包含于仿射图 $X_0 \neq 0$中，则复杂度为

$$\tilde{\mathscr{O}}(n^\omega(\deg(D^+) + \delta(\mathscr{C}))).$$

证明。在这种情况下，我们有 $\lambda(f) = 1$。因此，结合定理 5.18、命题4.15 和推论 6.3，第一个结论可直接得出。第二个结论（即定理 1.1）也立即成立，因为 $\deg D \geq 0$ 意味着 $\deg D^- + \deg D^+ \leq 2\deg D^+$。最后一个估计由定理5.20得出。

□

我们可能希望存储 $\mathscr{L}(D)$ 的一个 k-基的所有元素。由此可得以下大小估计。

命题 6.5。假设 $\mathscr{C}$ 在 k 上不可约。给定 $\mathscr{L}(D)$ 的一个压缩基，我们可以在以下时间内计算出 $\mathscr{L}(D)$ 的一个 k-基

$$\mathscr{O}(n(\deg(D) + 1)(\deg(D^+) + \delta(\mathscr{C}) + n))$$

（也就是说，如果 $\deg D < 0$，则成本为零）。

证明。复杂度取决于写出集合 $\{t^j b_i,\ 0 \le j \le d_i, 0, i \le n-1\}$ 中的所有元素。该集合的基数为 $\ell(D) := \dim \mathscr{L}(D)$。如果 $\ell(D) = 0$，则无需进行任何操作。否则，$\deg D \ge 0$，因此 $\deg D^+ + \deg D^- \le 2\deg D^+$。于是，根据定理 5.18 和推论 6.3（的证明），每个元素 $t^j b_i \in \mathscr{L}(D)$ 的算术规模为 $n(\deg D^+ + \delta(\mathscr{C}) + n)$。假设 $\mathscr{C}$ 在 k 上不可约，等价于 k 在 L中代数闭。在这种情况下，众所周知，$\ell(D) \le \deg(D) + 1$（例如参见 [63, Prop.1.4.9 和 Eq.1.21]），证明完毕。 □

备注 *6.6.* 若 $\mathscr{C}$仅在 k上不可约，则它在 k上的不可约因子数为 $\rho = [k_0 : k] = \dim \mathscr{L}(0)$，其中 $k \subset k_0 \subset L$ 是 L中 k 的代数闭包，即常数域。在这种情况下，由（ [63, 命题 *1.4* 的）证明可得不等式$\ell(D) \le \deg D + \rho$，并且在命题 *6.5* 中，我们必须将因子 $\deg D + 1$ 替换为 $\deg D + \rho$。例如，由 $f = X^2 - 2t^2$ 定义的曲线在 Q 上不可约，但在 Q 上有 $\rho = 2$ 个不可约分支。常值函数空间为 $\mathscr{L}(0) = k_0 \simeq k(\sqrt{2})$，其 k-基为 $(1, x/t)$，维数为$\ell(0) = 2$。

6.4 化归为首一可分情形

为完整起见，我们说明如何从任意射影平面曲线出发，得到定理6.4 中的首一可分假设。

引理 6.7. 设 $F \in k[X_0, X_1, X_2]$ 是次数为 $n > 0$ 的不可约齐次多项式。假设 $\mathrm{Card}(k) > n$。我们可以在 $\mathscr{O}(n^2)$ 时间内计算出两个不同的有理点 $P, P' \in \mathbb{P}^2(k)$，使得 $F(P) \ne 0$ 且 $F(P') \ne 0$。

证明。令 $f(t, X) = F(1, t, X)$。我们可以将 $f = \sum f_i(t) X^i$ 写成次数为 $f_i \le n - i$ 的形式。用霍纳法则在 $t = 0$ 和 $t = 1$ 处对 f_i 求值，需要 $\mathscr{O}(n)$ 次运算。对 i 求和后，我们可以在 $\mathscr{O}(n^2)$ 时间内计算出 $f(0, X)$ 和 $f(1, X)$。令 $\alpha_0, \ldots, \alpha_n$ 为 k 中互不相同的元素。利用快速多点求值，在 $\alpha_0, \ldots, \alpha_n$ 处计算 $f(0, X)$ 和 $f(1, X)$，需要 $\mathscr{O}(n)$ 次运算。由于每个多项式的次数至多为 n，因此存在 $\alpha = \alpha_i$ 和 $\alpha' = \alpha_j$，使得 $f(0, \alpha) \ne 0$ 且 $f(1, \alpha') \ne 0$。点 $P = (1 : 0 : \alpha)$ 和 $P' = (1 : 1 : \alpha')$ 满足所需假设。 □

引理 6.8. 设 P, P' 如上。存在一个射影自同构 $\tau : \mathbb{P}^2_k \to \mathbb{P}^2_k$，它将$(0, 1, 0)$ 映到P，并将$(0, 0, 1)$ 映到 P'。我们可以在 $\tilde{\mathscr{O}}(n^2)$的时间内计算出 $\tilde{F} = F \circ \tau$。多项式 $\tilde{F}$是齐次、不可约的，且关于 X_1 和 X_2的次数均为 n，并且是首一的（相差一个非零标量因子）。

证明。第一个断言显然：这相当于求一个可逆线性映射，将两个给定的非零向量映到另外两个给定的非零向量。计算 τ 的开销可以忽略不计，第二个断言例如可由中的 [4, Lem.2.5]证明。显然，F 仍是次数为 n的齐次不可约多项式。根据构造，我们有 $F(0,1,0) = F(P) \ne 0$ 且 $F(0,0,1) = F(P') \ne 0$。这恰好意味着单项式和以非零系数出现在 F 中。 □

引理 6.9. 设 $F \in k[X_0, X_1, X_2]$ 是次数为 $n > 0$的齐次不可约多项式，且是关于 X_1和 X_2的次数为 n 的首一多项式。若 k 是完美域，则 F 关于 X_1 可分，或关于 X_2可分。

证明. 反设 F 关于 X_1 和 X_2不可分。由于 F 不可约，因此有$\partial_{X_1} F = \partial_{X_2} F = 0$。由于 F 是关于 X_1的次数为 n 的首一多项式，这就意味着 $p = \mathrm{char}(k)$ 整除 n，而欧拉公式 $\sum X_i \partial_{X_i} F = nF = 0$则推出 $\partial_{X_0} F = 0$。最后，我们得到 $F = G(X_0^p, X_1^p, X_2^p)$，其中某个 G。由于 k是完美域，因此得到 $F = G^p$，这与 F 不可约相矛盾。 □

由此我们得到如下结果。

命题 6.10. 设 $F \in k[X_0, X_1, X_2]$ 不可约，且为次数 $n > 0$ 的齐次多项式。若 $\mathrm{Card}(k) > n$，则可在时间 $\tilde{\mathscr{O}}(n^2)$ 内计算出一个总次数为 n 的多项式 $f \in k[t, X]$，它关于 X 可分，且为首一次数为 n 的多项式，使得 $k(\mathscr{C}) \simeq k(t)[X]/(f)$。

证明。我们按引理 6.7 计算 P、P'，并如引理 6.8 那样考虑 F。依照引理 6.9，若 F关于 X_2可分，则令 $f(t, X) = F(1, t, X)$；若 F关于X_1可分，则令 $f = F(1, X, t)$。 □

如果 $\mathrm{Card}(k) < n$，那么对于所有 $P \in \mathbf{P}^2_k$（填充曲线），我们可能有 $F(P) = 0$，在这种情况下，引理 6.7 可以考虑 k 的一个有限扩张 k'，使得 $\mathrm{Card}(k') > n$ 且 $[k' : k] \in O(\log(n))$。由于 F 在 k 上不可约，它在 k' 上的不可约因子在 k 上共轭，很容易验证引理 6.9 在此情形下仍然成立。因此，我们需要计算以下空间的一组基：

$$\mathscr{L}(D) \otimes k' \simeq \mathscr{L}(D')$$

其中 D' 是曲线 $\mathscr{C}' = \mathscr{C} \otimes k'$ 的除子，该曲线由次数为 n 的齐次多项式 $G \in k'[X_0, X_1, X_2]$ 定义，此多项式在 X_2 中可分且为首一，次数为 n。曲线 $\mathscr{C}'$ 在 k' 上不一定不可约，但整个算法的执行方式完全相同。计算成本至多乘以一个对数因子 $O(\log(n))$。为了从 $\mathscr{L}(D) \otimes k'$ 的一组基恢复 $\mathscr{L}(D)$ 的一组基，我们可以例如使用相对迹映射

$$\mathrm{Tr}_{k'/k} : \mathscr{L}(D) \otimes k' \to \mathscr{L}(D).$$

对 $\mathscr{L}(D) \otimes k'$ 的随机基作一次选取，便可得到一个 k-基，作为 $\mathscr{L}(D)$ 的基，概率为 $\geq 1/4$。我们参阅 [4,第7节。5]以了解详情（另见 [35] 中的确定性方法）。

注 6.11. 由于 $A = k[t]$ 是有限型 k-代数，B 的分式理想总是自由 A-模，秩为 $n = [L : K]$，依据 *[14, 第V章§2，no2，定理2]*。这表明，首一且可分的假设或许可以去掉。为此需要在这一更广的背景下改造 *OM* 算法以及整基计算，而这超出了本文的范围。这将具有重要意义，因为届时我们的算法将对任意不可约多项式 F 适用，从而避免任何坐标变换以及任何基域扩张。

A 赋值环与整闭包

几何方法和算术方法中一个常见的要素是整闭包的概念。下面简要回顾我们需要的主要性质。

定义 A.1. 设 S 是一个环，$R \subset S$ 是一个子环。若元素 $x \in S$ 是多项式 $f \in R[X]$ 的根，则称它在 R 上整。S 在 R 上的整元所成的集合称为 R 在 S 中的整闭包。若 R 与其在 S 中的整闭包相同，则称 R 在 S 中整闭。若 R 在其全商环中整闭，则简称 R 整闭。

命题 A.2. *[8, 推论 5.3 和推论 5.5]* 设 S 是一个环，$R \subset S$ 是一个子环。R 在 S 中的整闭包是 S 的一个子环，包含 R，且在 S 中整闭。

对于环 R，我们用 Spec R 表示 R 的极大理想集合。对于 $\mathfrak{p} \in \mathrm{Spec}\ R$，令 $R_{\mathfrak{p}}$ 为 R 在 $\mathfrak{p}$ 处的局部化（即关于乘法子集 $R \setminus \mathfrak{p}$ 的局部化）。它是一个局部环，其极大理想为 $\mathfrak{p}R_{\mathfrak{p}}$。

命题 A.3。 *[8, 命题 5。13]* 整环 R 是整闭的，当且仅当所有局部环 $R_{\mathfrak{p}}$、$\mathfrak{p} \in$ 谱 R 都是整闭的。

整闭包与赋值环之间的联系始于以下初等结果：

引理 A.4。 赋值环是整闭的。

证明。设 $\mathscr{O}$ 为赋值环。令 $x \in \mathrm{Frac}(\mathscr{O})$ 使得 $x^n = a_{n-1}x^{n-1} + \cdots + a_0$，其中 $a_i \in \mathscr{O}$。若 $x \notin \mathscr{O}$，则根据赋值环的定义，$x^{-1} \in \mathscr{O}$。两边除以 x^{n-1}，得到 $x = a_{n-1} + \cdots + a_0 x^{1-n} \in \mathscr{O}$，矛盾。 □

以下结果给出了函数域的离散赋值环的一种刻画：

命题 A.5。 *[8, 命题 9。2]* 设 $\mathscr{O}$ 为一维诺特局部环。则 $\mathscr{O}$ 是离散赋值环，当且仅当它是整闭的。

整闭环对我们的目的尤为重要，这是由于以下结果（例如参见 [8,推论 5.22]）：

命题 A.6. 域 L 的子环 R 的整闭包是包含 R 的 L 的所有赋值环的交。

现在假设 R 是函数域 L/k 的一个子环，且满足 $k \subset R$。前一命题表明，$b \in L$ 在 R 上整，当且仅当对 L 的所有在 R 上为正的赋值 v，均有 $v(b) \geq 0$。

命题 A.7. R 在 L 中的整闭包 $\overline{R}$ 是一个有限 R-模，且映射

$$\mathrm{Spec}\,\overline{R} \to \mathrm{Spec}\,R, \quad \mathfrak{p} \mapsto \mathfrak{p} \cap R$$

定义良好、满射且有限。此外，对于至少所有满足 $R_{\mathfrak{m}}$ 为赋值环（即整闭）的 $\mathfrak{m} \in$ 谱 R，此映射都是一一对应的。

证明。若 R 是一个域，那么 R 也是一个域，且是 R 的有限扩张，在这种情况下命题显然成立。若 R 不是域，那么 R 是一个有限生成的 k-代数，其 Krull 维数为一，并且根据有限性定理（例如参见 $\overline{R}$，R-模也是有限生成的（参见 [56, 定理 9，第267]页）。由此，所述结论可由 [38, 引理 F.9 和定理 F.10] □

定义 A.8. 赋值 $P \in V_L$ 在 R 上的中心 是集合 $\mathfrak{p} = P \cap R$，也就是在 P处消失的“函数” $b \in R$的集合。

赋值的中心是 R的一个素理想。下文中，若子环 $S \subset L$ 满足$R \subset S$，则称其覆盖 R 。

命题 A.9. 设 R 不是域。令 R 为 R 在 L 中的整闭包，并令 $P \in V_L$。以下条件等价：

(a) 中心 $\mathfrak{p} = P \cap R$ 不是零理想；*(b)* 中心 $\mathfrak{p} = P \cap R$ 是 R的极大理想；*(c)* 赋值环 $\mathcal{O}_P$ 覆盖 R；*(d)* 赋值环 $\mathcal{O}_P$ 覆盖 $\overline{R}$。

于是我们称 P 以 R 为中心，并称 P 覆盖 $\mathfrak{p}$。

证明. $a) \Leftrightarrow b)$由以下事实可得： R 的 Krull 维数为一，因为 $k \subset R \subset L$ 不是域。 $d) \Rightarrow c)$显然，因为 $R \subset \overline{R}$。我们来证明 $c) \Rightarrow d)$。若 $R \subset \mathcal{O}_P$，则 L 中任何在 R 上整的元素也必然在 $\mathcal{O}_P$上整，因此 $R \subset \mathcal{O}_P$。但根据引理 A.4， $\mathcal{O}_P = \mathcal{O}_P$。回忆一下， $\mathcal{O}_P = \{a \in L \mid a^{-1} \notin P\}$。我们来证明 $c) \Rightarrow a)$。令 $R \subset \mathcal{O}_P$。若 $P \cap R = \{0\}$，则对于所有非零的 $a \in R$，都有 $a^{-1} \in \mathcal{O}_P$，这将导致 $L \subset \mathcal{O}_P$。这是不可能的，因此 $P \cap R$ 不是零理想。最后，我们来证明 $b) \Rightarrow c)$。假设存在 $a \in R$使得 $a \notin \mathcal{O}_P$。特别地， $a \notin \mathfrak{p}$。由于 $\mathfrak{p}$ 是 R的极大理想，存在 $b \in R$ 满足 $ab - 1 \in \mathfrak{p}$。然而， $a \notin \mathcal{O}_P$，所以 $b \notin \mathcal{O}_P^\times$，从而可得 $b \in \mathfrak{p}$ 。这导致 $1 \in \mathfrak{p}$，矛盾，因此不存在这样的元素 a。 □

命题 A.10. 设 $V_L(R)$ 为以 R 为中心的位的集合。假设 $\mathrm{Frac}(R) = L$。映射 p

$$V_L(R) \to \operatorname{Spec} \overline{R}, \quad P \mapsto \mathfrak{p} = P \cap \overline{R}$$

是双射，并且有 $\mathcal{O}_P = R_\mathfrak{p}$ 和 $\overline{P} = \mathfrak{p}R_\mathfrak{p}$。

证明。我们有 $V_L(R) = V_L(\overline{R})$根据命题 A.9 的 (c) 和 (d) 项可知，因此我们可以假设 $R = \overline{R}$。结论由 [63, 命题 3.29] 得出。 □

B 几何观点：曲线上的赋值与闭点

警告：这里我们用 P 或 Q 表示曲线的闭点，请勿将其与函数域的位混淆。

B.1 仿射曲线与闭点

设 k是一个完美域， k是它的代数闭包。设 $R = k[X_1, \ldots, X_n]$ 是关于 n个变量的多项式环，并考虑仿射 n 空间

$$\mathbb{A}_k^n = \operatorname{Spec} R.$$

闭点 $P \in \mathbb{A}_n^k$ 按定义是 R的一个极大理想。或者，我们可以将 P 视为点集 $\overline{k}^n$，其中的点位于 k^n 中，且 P中的所有函数都在这些点处取值为零：该集合是在 $\mathrm{Gal}(k/k)$作用下， k^n 中某个点的一个伽罗瓦轨道。反过来，给定 k^n中的一个伽罗瓦轨道，所有在该轨道中任意（因而也在所有）点处取值为零的 R 中的多项式构成 R 的一个极大理想（零点定理）。 k 上的仿射曲线是 $C \subset \mathbb{A}_n^k$的一个一维整子概形，也就是说

$$C = \operatorname{Spec} R/I$$

其中 $I \subset R$是一个高度为 $n-1$的素理想。此时， C的闭点是 R/I的一个极大理想，或者等价地，根据对应定理，是 R 的一个包含 I 的极大理想。同样，闭点 $P \in C$ 可以看作簇（几何曲线）中某个点的伽罗瓦轨道

$$C(\bar{k}) = \{a \in \bar{k}^n,\ f(a) = 0\ \forall\ f \in I\}.$$

C上的正则函数环，或 C的坐标环，是

$$k[C] := R/I.$$

由于假设 I 是素理想， $k[C]$ 是整环。我们将其分式域称为 C的有理函数域，记为 $k(C)$。它是一个函数域，并且每个函数域都同构于形如$k(C)$的域。 C 在闭点 $P \in C$ 处的局部环，是 $k[C]_P$ 在极大理想 P处的局部化，通常记为$\mathcal{O}_{C,\,P}$。因此我们有包含关系

$$k[C] \subset \mathcal{O}_{C,P} \subset k(C).$$

域 $k_P = \mathcal{O}_{C,P}/P\mathcal{O}_{C,P} \simeq k[C]/(P)$ 是 P 的剩余域，而后者是 k 的有限扩张。如果 $h \in \mathcal{O}_{C,P}$，我们就称 h 在 P 处正则。之所以采用这一术语，是因为求值映射

$$ev_P : \mathcal{O}_{C,P} \to k_P, \quad ev_P(h) = h \mod P$$

是良定义的。我们也记 $h(P) = ev_P(h)$。如果 $h(P) = 0$，也就是说，如果 $h \in P$，我们就称 h 在 P 处消失。注意，如果 $k = \bar{k}$，那么 $P = (X_1 - a_1, \ldots, X_n - a_n)$ 可以视为 $a = (a_1, \ldots, a_n) \in C(k)$，而 $h(P)$ 则可自然地视为 $h(a)$，即通常所说的函数在一点处的求值。

注 B.1. 概形 C 带有一个拓扑： C 的闭子集是其自身或有限个闭点的并。它还配有定义在拓扑空间 C 上的结构层 $\mathcal{O}_C$ ；对于开集 $U \subset C$，$\mathcal{O}_C(U) \subset k(C)$ 是由在所有 $P \in U$ 处正则的函数构成的子环。 P 处的茎是局部环 $\mathcal{O}_{C,P}$。这些都是至关重要的数据，尤其是在定义概形之间的态射时。不过，我们在这里有意不深入讨论这些细节，主要将 C 视为一个集合。更多细节请参阅任意一本代数几何教材。

B.2 正则点与奇点。

局部环 $\mathcal{O}_{C,\,P}$ 不一定是赋值环。事实上，我们有以下经典刻画[8, 命题9.2，第94]:

命题 B.2。 设 $P \in C$ 是一个闭点。以下断言等价:
(a) 环 $\mathcal{O}_{C,\,P}$ 是一个离散赋值环。*(b)* 环 $\mathcal{O}_{C,\,P}$ 是整闭的。*(c)* 若 $I = (f_1, \ldots, f_r)$，则 f_i 的偏导数不全在 P 处消失。

如果 P 满足上述任一条件，我们就称其为 正则点 ，属于 C。否则，我们称 P 为奇点。由 (c) 可知， P 是正则点，当且仅当几何曲线 $C(k)$ 在由 P定义的伽罗瓦轨道上的所有点处都光滑（按通常意义）。闭点若非正则点，则为奇点。曲线 C 若没有奇点，则称其为正则（或光滑）。否则，我们称 C 为奇异的。曲线C 上的奇点集合是有限的。结合命题 A.3 和命题 B.2，可得经典结果:

命题 B.3。 仿射曲线 C 光滑，当且仅当 $k[C]$整闭。

请注意，正则点 $P \in C$ 特别定义了一个离散秩一赋值 v_P： $k(C) \to \mathbf{Z} \cup \{\infty\}$。因此，讨论有理函数 $h \in k(C)$ 在正则点处的零点阶数或极点阶数是有意义的。

B.3 奇异曲线的正规化。

曲线在奇点处的局部环不是赋值环。 在这种情况下，函数在 P 处的零点阶数或极点阶数不再有意义。我们需要消解曲线 C的奇点，或者对其进行正规化。

定义 B.4。 C 的正规化是曲线 C =谱 $k[C]$ ，其中 $k[C]$ 表示 $\overline{k(C)}$中 $k[C]$的整闭包。

C 是曲线这一事实源于有限性定理（该定理本身是诺特正规化定理的推论），该定理保证 $k[C]$ 是一个一维整 k-代数（命题 A.7）。也就是说， $k[C] \simeq k[Z_1, \ldots, Z_m]/J$其中 J是高度为$m - 1$的素理想。因此， C确实是某个（可能更大的）仿射空间 $\mathbb{A}^m_k$中的一条仿射曲线。

例 B.5. 考虑仿射平面曲线 C =谱 $k[T, X]/(X^2 - T^2 - T^3)$。它只有一个奇点 $P = (T, X)$ （对应的几何点为 $(0, 0)$）。记 t和 x 为 T和 X的剩余类。因此 $k[C] = k[t, x]$ ，其中 $x^2 = t^2 - t^3$。有理函数 $y = x/t \in k(C)$ 满足 $y^2 - t - 1 = 0$，因此它在 $k[C]$ 上是整的。将此元素添入环 $k[C]$ ，得到更大的环

$$k[t, x, x/t] = \frac{k[T, X, Y]}{(X^2 - T^2 - T^3, X - TY, Y^2 - T - 1)} \simeq k[Y].$$

由于 $k[Y]$ 是整闭的，我们推出$k[C] = \overline{k[t, x, x/t]} \simeq k[Y]$ 且 C 同构于仿射直线$\mathbb{A}^1_k$ = 谱 $k[Y]$ （但请注意， C 在此自然嵌入于$\mathbb{A}^3_k$ 中）。

由命题B.3，仿射曲线 C 是光滑的，且 $\overline{C}=C$ 当且仅当 C 是光滑的。我们有包含关系$k[C]\subset k[C]\subset k(C)$因此曲线 C 与 C 具有相同的函数域 $k(C)=k(C)$。具有同构函数域的两条曲线称为双有理等价。由命题A.7，我们有一个满射（事实上是 k-概形的态射）

$$\pi:\overline{C}\twoheadrightarrow C,\quad \pi(Q)=Q\cap k[C]$$

该映射是有限的，且除 C 上有限个闭点之外均为一一对应；这些点都包含在 C 的奇异轨迹中。如果 $P\in C$ 是奇异的，则 P 上方可能有多个点，也可能没有点。

例 *B.6*。（续例 *B.5*） $\pi:\ C\to C$ 在 $P=(T,X)$ 上方的纤维由包含 $P+(X^2-T^2-T^3,X-TY,Y^2-T-1)=(T,X,Y^2-1)$ 的极大理想 $Q\subset k[T,X,Y]$ 组成。假设 *char(k)* $\neq 2$，则该纤维由两个闭点组成，分别由极大理想 $Q_1=(T,X,Y-1)$ 和 $Q_2=(T,X,Y+1)$ 给出，对应于几何点 *(0, 0,* $\pm$*1)*（这是在节点处对平面曲线进行爆破的一个例子）。如果 *char(k)* $=2$，那么 $Y^2-1=(Y-1)^2$，且 P 上方有唯一一个点 Q，由极大理想 *(T, X, Y* $-$ *1)* 给出。

我们说 $k(C)$的一个赋值以 C 为中心，如果它以 $k[C]$ 为中心（命题A.9）。我们可以在此语境下重新表述命题A.10:

定理 B.7. 设 C 为一条仿射曲线。 $k(C)$的以 C 为中心的位与 C的闭点之间存在一一对应。

~ ~ — ~ ~底层映射为 $Q\mapsto \overline{Q}=Q\cap k[C]$。在 C 上，赋值 Q 的中心是 $P=Q\cap k[C]=\pi(Q)\in C$。若曲线 C 光滑，我们因而可将以 C 为中心的位与 C的闭点等同起来。

B.4 平面曲线的位与分支。

设 $C=$谱 $k[T,X]/(f)$是由不可约多项式 $f\in R=k[T,X]$ 所定义的平面曲线，并^设 $P\in C$ 为一个闭点。我们可以如下描述以 P 为中心的位。设 R_P 为~R 关于 P-进拓扑的完备化。通常， $P=(T,\ X)$且 $R_P=k[[T,X]]$。曲线 C在P 处的芽为

$$(C,P):=\operatorname{Spec}\widehat{R}_P/(f).$$

^局部不可约分解 $f=f_1\cdots f_r\in R_P$给出了如下分解

$$\widehat{R}_P/(f)=\widehat{R}_P/(f_1)\oplus\cdots\oplus\widehat{R}_P/(f_r)$$

其中每个加项现在都是一个整局部环（但一般并非整闭）。由 f_i定义的曲线芽（$C_i,\ P$）的不可约芽称为（$C,\ P$）的一个分支。我们有

$$(C,P)=(C_1,P)\cup\cdots\cup(C_r,P).$$

下面的结果是命题3.11 和命题3.16的局部对应结果。

命题B.8. 具有中心 P 的 $k(C)$ 的赋值 Q_i 与曲线芽(C,P)的分支(C_i,P)之间存在一一对应。赋值v_{Q_i}由 P处与 f_i 的交数诱导。更准确地说，若$h\in\mathscr{O}_{C,\ P}$，则有等式

$$v_{Q_i}(h)=\frac{1}{[k_P:k]}\dim_k\frac{\widehat{R}_P}{(f_i,h)}.$$

^这里仍用 $h\in R_P\subset\widehat{R}_P$表示 h的任意一个提升。

这一观点使我们能够用相应分支的（截断）局部方程 Q_i 来表示赋值 f_i，并且可以通过结式或局部参数化计算交数，详见第3.5.1节。

B.5 无穷远位与紧化。

遗憾的是， C 的闭点无法描述 $k(C)$的所有赋值。换言之，仍有一些赋值没有以 C为中心。这些就是仿射曲线 C的“无穷远处”赋值。

例 *B.9.* 考虑正则曲线 $C =$ 谱 $k[T,X]/(TX-1)$，其坐标环为 $k[C]=k[t,x]$，其中 $tx=1$。因此，$k[C]=k[t,1/t]$ 和 $k(C)=k(t)$。考虑两个赋值 P_1 和 P_2，它们分别由 $k(C)$的离散赋值环 $k[t]_{(t)}$ 和 $k[1/t]_{(1/t)}$ 的极大理想(t)和$(1/t)$给出。我们验证$P_1\cap k[C]=\{0\}$ 和 $P_2\cap k[C]=\{0\}$，因此 P_1 和 P_2 不以 C 为中心（命题 *A.9*）。

为了赋予无穷远位几何意义，我们需要"紧化" C。一种经典紧化是射影闭包。为完整起见，我们简要说明这一构造。 k 上的射影 n-空间是

$$\mathbb{P}^n_k=\operatorname{Proj}\, k[X_0,\dots,X_n].$$

从集合论角度看，$\mathbf{P}^n_k$是 $R'=k[X_0,X_1,\dots,X_n]$ 中高度为 n、其根不等于无关理想（$X_0,\dots,X_n$）的齐次素理想的集合。底层簇是 k上通常的射影 n-空间，即

$$\mathbb{P}^n(\bar{k})=(\bar{k}^{n+1}\setminus 0)/\sim$$

其中 $\sim$ 是等价的共线关系。$\mathbf{P}^n_k$ 的无穷远超平面是

$$H_0=\operatorname{Proj}\, R'/(X_0)\simeq \operatorname{Proj}\, k[X_1,\dots,X_n]\simeq \mathbb{P}^{n-1}_k,$$

简记为 $H_0=\{X_0=0\}$。 H_0 的闭点对应于$\mathbf{P}^n_k$ 中包含（X_0）的闭点。$\mathbf{P}^n_k$的其余点通过去齐次化与 $R=k[X_1,\dots,X_n]$的极大理想一一对应，即令 $X_0=1$。由此我们得到一个双射

$$\iota_0: U_0=\mathbb{P}^n_k\setminus H_0\longrightarrow \mathbb{A}^n_k.$$

反向映射 ι_0^{-1}是对极大理想 $P\subset k[X_1,\dots,X_n]$ 关于 X_0进行齐次化；将 P 的生成元 f 映为齐次多项式

$$f(X_1,\dots,X_n)\mapsto F(X_0,\dots,X_n)=X_0^d f(X_1/X_0,\dots,X_n/X_0)$$

其中 $d=\deg(f)=\deg(F)$。注意，对每个 $i=0,\dots,n$，关于 X_i 去齐次化会得到一个同构 ι_i：$U_i=\mathbf{P}^n_k\setminus H_i\simeq \mathbf{A}^k_n$，其中 $H_i=\{X_i=0\}$。此外，坐标图 U_i 覆盖整个空间 $\mathbf{P}^n_k$，因此我们可以像在通常的仿射 n-空间中一样，在 $\mathbf{P}^n_k$ 中进行局部研究。

令 $I'\subset R'$ 为定义仿射曲线 C 的理想 $I\subset R$ 的齐次化。闭点 of

$$\mathscr{C}=\operatorname{Proj}\, R'/I'$$

是 R' 中高度为 n、包含 I' 且其根基不等于 $(X_0,\dots,X_n)$ 的齐次素理想。我们有自然包含 $\mathscr{C}\subset\mathbf{P}^n_k$，去齐次化映射 ι_0 导出一个同构

$$\iota_0:\mathscr{C}\cap U_0\longrightarrow C,$$

因此，对所有 $P\in\mathscr{C}\cap U_0$，都有同构$\mathscr{O}_{\mathscr{C},\,P}\simeq\mathscr{O}_{C,\,\iota_0(P)}$。 $\mathscr{C}$中剩余的点集为 $H_0\cap\mathscr{C}$（即"无穷远处"的点），这样的点只有有限个。我们称 $\mathscr{C}$ 为 C 的射影闭包。对于每个图表 U_i，仿射曲线 $C_i=\iota_i(\mathscr{C}\cap U_i)$ 的理想很容易从 C 的理想推导出来。在平面情形 $C=$中，设 Spec $k[X_1,X_2]/(f)$，其中 f的总次数为 d，则有

$$\mathscr{C}=\operatorname{Proj}\, k[X_0,X_1,X_2]/(F)$$

其中 F是 f 的齐次化，并且我们得到 $C_1=$谱$\,k[X_0,X_2]/(f_1)$ 和 $C_2=$谱$\,k[X_0,X_1]/(f_2)$，其中

$$f_1(X_0,X_2)=X_0^d f(1/X_0,X_2/X_0)\quad\text{and}\quad f_2(X_0,X_1)=X_0^d f(1/X_0,X_1/X_0).$$

曲线 $\mathscr{C}$ 自然同构于通过沿交集粘合仿射曲线 C_i 而得到的抽象曲线。每条仿射曲线 $C_i\subset\mathbf{A}^n_k$ 都具有正规化 C_i，如前一段所述。仿射曲线 C_i 可以再次粘合在一起，由此得到的曲线 $\bar{\mathscr{C}}$ 是光滑射影曲线，称为 $\mathscr{C}$ 的正规化。

B.10 定理。设 $C\subset\mathbb{A}^n_k$ 是一条仿射曲线，其射影闭包为 $\mathscr{C}\subset\mathbb{P}^n_k$。$k(C)$ 的赋值与 $\mathscr{C}$的正规化 $\bar{\mathscr{C}}$ 的闭点之间存在一一对应关系。

$k(C)$ 中以 C 为中心的赋值称为仿射赋值。它们对应于 C 的正规化 $\bar{C}$ 的闭点。其余赋值以 $\mathscr{C}$ 的无穷远点为中心，也就是以$\mathscr{C}\setminus C=\mathscr{C}\cap(X_0=0)$ 上的点为中心。请注意，射影闭包 $\bar{\mathscr{C}}$ 的正规化通常不是仿射正规化 $\bar{C}$ 的射影闭包。当且仅当 $\mathscr{C}$ 的无穷远点是正则点时，二者才相同。

例 B.11。（续例 B.9）。相对于新变量 Z， $f = TX - 1$ 的齐次化为 $F = TX - Z^2$，且 $\mathscr{C} = Proj\ k[Z,T,X]/(F)$。$\mathscr{C}$ 与无穷远直线 $Z = 0$ 的交为 $Proj\ k[Z,T,X]/(F,Z) \simeq Proj\ k[T,X]/(TX)$，由两个闭点 $P_1 = (Z,T)$ 和 $P_2 = (Z,X)$ 组成（分别对应几何点 $(0:0:1)$ 和 $(0:1:0)$）。如例 B.9 所述，这两个点对应于两个不以 C 为中心的赋值。

注 B.12. 紧化一条仿射曲线有多种方式。例如，我们可以考虑它在射影空间的乘积中或在完备环面簇中的闭包。例如，考虑由多项式 f 与 $\lambda(f) > 1$ 所定义的平面曲线，便提示我们考虑 f 的仿射平面曲线在某个精心选取的 $\mathbb{A}^2_k$ 的加权射影紧化中的 *Zariski*闭包 $\mathscr{C}$。

仿射赋值与有限处。 设 $C = 谱\ k[T,X]/(f)$ 为一条仿射平面曲线，并设 $\mathscr{C} \subset \mathbb{P}^2_k$ 为 C的射影紧化。记 $K = k(T)$ 与 $L = K[X]/(f)$ 如第 3节，我们可以等同$L = k(\mathscr{C})$。在此情形下， L/k 的仿射赋值（即以 C为中心）与 L/K 的有限处（定义 3.4）未必重合。事实上：

命题 B.13. 以 C 为中心的位的集合包含于 L/K 的有限处的集合。这两个集合重合当且仅当 f 关于 X 是首一的。

证明。根据命题 A.9 (d)，赋值 P 以 C 为中心，当且仅当 $\mathscr{O}_P$ 包含 $k[C]$; 而 P 是有限处，当且仅当 $\mathscr{O}_P$ 包含 $A = k[t]$ 在 $L = k(t,x)$ 中的整闭包 B。由于 $A \subset k[C]$，我们有 $B \subset k[C]$，因此任何以 C 为中心的赋值都是有限处。若 f 是首一的，则 $x \in B$，因此 $B = k[C] = A[x]$，仿射赋值与有限处重合。若 f 不是首一的，则 $x \notin B$ 且 $B \subsetneq k[C] = A[x]$。由于两个环都是整闭的，根据命题 A.6，我们可以推出存在一个赋值 P，使得 $\mathscr{O}_P$ 包含 B 而不包含 $k[C]$，也就是说， P 是有限处，但不以 C 为中心。 □

例如，在例 B.11 中，以 $P_1 =$（Z， T）为中心的赋值 不是仿射赋值，但却是有限处。

B.6 δ不变量与亏格公式

设 $\mathscr{C}$ 是定义在 k 上的射影曲线。设 $P \in \mathscr{C}$ 是一个闭点，其局部环为 $\mathscr{O}_{\mathscr{C},P}$。正规化 $\overline{\mathscr{O}_{\mathscr{C},P}}$ 是一个半局部环，其极大理想对应于正规化 $\mathscr{C}$ 中位于 P 之上的闭点。它是一个有限的 $\mathscr{O}_{\mathscr{C},P}$-模（命题 A.7），因此 $\overline{\mathscr{O}_{\mathscr{C},P}}/\mathscr{O}_{\mathscr{C},P}$ 是一个有限维 k 向量空间。

定义 B.14。 $\mathscr{C}$ 在闭点 $P \in \mathscr{C}$ 处的 *δ*不变量为

$$\delta_P(\mathscr{C}) := \dim_k \overline{\mathscr{O}_{\mathscr{C},P}}/\mathscr{O}_{\mathscr{C},P}.$$

$\mathscr{C}$ 的全局 *δ*不变量为 $\delta(\mathscr{C}) = \sum_{P \in \mathscr{C}} \delta_P(\mathscr{C})$。

注意， $\delta_P(\mathscr{C}) = 0$ 当且仅当 P 是正则点（命题 B.2）。因此，该和式是在奇点的有限集合上取和，全局 δ不变量是良定义的。它衡量曲线 $\mathscr{C}$ 的奇异程度。如果 $\mathscr{C}$ 是节点曲线，则其 δ不变量就是节点的数量（在 k 上），有时也称为“双重点数”。

记 $\mathscr{O}_{\mathscr{C}}$ $\mathscr{C}$ 的结构层为 $\mathscr{C}$，其算术亏格定义为

$$p_a(\mathscr{C}) = 1 - \dim_k H^0(\mathscr{C}, \mathscr{O}_{\mathscr{C}}) + \dim_k H^1(\mathscr{C}, \mathscr{O}_{\mathscr{C}}).$$

若 $\mathscr{C}$ 在 $\bar{k}$ 上不可约，则其算术亏格为 $p_a(\mathscr{C}) = \dim_k H^1(\mathscr{C}, \mathscr{O}_{\mathscr{C}})$。根据定义，几何亏格 $g(\mathscr{C})$ 是 $\mathscr{C}$ 的正规化的算术亏格。与依赖于 $\mathscr{C}$ 的嵌入方式的算术亏格不同，几何亏格是一个双有理不变量。

下一个由 Hironaka 得出的结果 [33] 称为亏格公式。它将射影曲线的 δ 不变量、算术亏格和几何亏格联系起来。

命题 B.15。 *[33, 定理 2]* 设 $\mathscr{C} \subset \mathbb{P}^r_k$ 是一条射影曲线。我们有 $g(\mathscr{C}) = p_a(\mathscr{C}) - \delta(\mathscr{C})$。

换言之，算术亏格与几何亏格之差衡量了曲线的奇异程度。对于次数为 n 的射影平面曲线，亏格次数公式指出

$$p_a(\mathscr{C}) = \frac{(n-1)(n-2)}{2}.$$

结合命题B.15，可得：

推论 B.16. 设 $\mathscr{C} \subset \mathbb{P}^2_k$ 是次数为 n 的射影平面曲线。那么 $g(\mathscr{C}) = \frac{(n-1)(n-2)}{2} - \delta(\mathscr{C})$.

参考文献

[1] S. Abelard. 关于计算函数域整基的复杂度。载于《科学计算中的计算机代数》，第 42–62 页。施普林格国际出版，2020 年。[2] S. Abelard、E. Berardini、A. Couvreur 和 G. Lecerf. 通过 Puiseux 展开计算黎曼–罗赫空间。《复杂性杂志》，73:101666，2022 年。[3] S. Abelard、A. Couvreur 和 G. Lecerf. 黎曼–罗赫空间的次二次时间算法：节点平面射影曲线上光滑除子的情形。载于第 45 届国际符号与代数计算研讨会论文集（ISSAC '20），第 14–21 页，美国纽约州纽约，2020 年。美国计算机协会。[4] S. Abelard、A. Couvreur 和 G. Lecerf. 具有普通奇点的平面曲线的黎曼–罗赫空间高效计算。《工程、通信与计算中的应用代数》，2022 年 12 月。[5] S. S. Abhyankar. 两个复变量解析函数芽的不可约性判据。《数学进展》，74(2):190–257，1989 年。[6] M. Alberich-Carramiñana、J. Guàrdia、E. Nart、A. Poteaux、J. Roé 和 M. Weimann. 亨泽尔域上的多项式因式分解。《计算数学基础》，25(2):631–681，2022 年。[7] J. Alman 和 V. V. Williams. 改进激光法与更快的矩阵乘法，第 522–539 页。[8] M. F. Atiyah 和 I. G. MacDonald.《交换代数导论》。艾迪生-韦斯利出版公司，1969 年。[9] J.-D. Bauch. 多项式环上的格及其在函数域中的应用。arXiv：数论，2014 年。[10] J.-D. Bauch. 整基计算。《数论杂志》，165:382–407，2016 年。[11] J.-D. Bauch、E. Nart 和 H. Stainsby. 局部域上多项式 OM-分解的复杂度。《伦敦数学学会计算与数学杂志》，16:139–171，2013 年。[12] J. Böhm 和 I. Stenger. Brillnoether.lib：一个用于曲线上除子的黎曼–罗赫空间的 Singular 4.1.2 库，2019 年。http://www.singular.uni-kl.de。[13] W. Bosma、J. Cannon 和 C. Playoust. Magma 代数系统 I：用户语言。《符号计算杂志》，24(3):235–265，1997 年。[14] 布尔巴基。《交换代数》第 5 至 7 章。施普林格柏林-海德堡，2006 年。[15] A. Campillo.《正特征代数曲线》，《计算机科学讲义》第 378 卷。施普林格出版社，1980 年。[16] A. Campillo 和 J. I. Farrán. 平面曲线的符号汉堡-诺特表达式及其在代数几何码中的应用。《数学计算》，71(240):1759–1780，2002 年。[17] D. Cantor 和 E. Kaltofen. 任意代数上多项式的快速乘法。《信息学学报》，28(7):693–701，1990 年。[18] J. Coates. 曲线上有理函数的构造。《剑桥哲学学会数学会报》，68(1):105–123，1970 年。[19] J. H. Davenport. 关于代数函数的积分。《计算机科学讲义》，102，1981 年。[20] A. J. Engler 和 A. Prestel.《赋值域》。《施普林格数学专著》。施普林格柏林-海德堡，2005 年。[21] A. L. Gluher 和 P.-J. Spaenlehauer. 一种用于计算黎曼–罗赫空间的快速随机几何算法。《计算数学》，89:2399–2433，2020 年。[22] V. D. Goppa. 与除子相关的码。《信息传输问题》，13(1):33–39，1977 年。[23] V. D. Goppa. 代数几何码。《苏联科学院消息》，21:75–91，1983 年。[24] V. D. Goppa. 码与信息。《俄罗斯数学评论》，39(1):87–141，1984 年。

[25] J. Guàrdia、J. Montes 和 E. Nart。奥库苏不变量与 Newton 多边形。《算术学报》，145：83–108，2010。[26] J. Guàrdia、J. Montes 和 E. Nart。高阶 Newton 多边形在数域判别式计算与素理想分解中的应用。《波尔多数论杂志》，23(3)：667–696，2011。[27] J. Guàrdia、J. Montes 和 E. Nart。代数数论中的高阶 Newton 多边形。《美国数学会汇刊》，364：361–416，2012。[28] J. Guàrdia、J. Montes 和 E. Nart。数域理想理论的一种新计算方法。《计算数学基础》，13(5)：729–762，2013。[29] J. Guàrdia、E. Nart 和 S. Pauli。局部域上多项式的单因子提升与分解。《符号计算杂志》，47(11)：1318–1346，2012。[30] J. Guàrdia、J. Montes 和 E. Nart。高阶 Newton 多边形与整基。《数论杂志》，147：549–589，2015。[31] G. Haché。《有效构造几何码》。博士论文，巴黎第六大学，1996。[32] F. Hess。代数函数域中的黎曼–罗赫空间计算及相关主题。《符号计算杂志》，33(4)：425–445，2002。[33] H. Hironaka。代数曲线的算术亏格与有效亏格。《京都大学理学院纪要 A 数学》，30(2)：177–195，1957。[34] J. v. d. Hoeven 和 G. Lecerf。定向求值。《复杂性杂志》，60：101498，2020。[35] M.-D. Huang 和 D. Ierardi。黎曼–罗赫问题及曲线的雅可比簇上的加法的高效算法。《符号计算杂志》，18(6)：519–539，1994。[36] T. Kailath。《线性系统》。Prentice-Hall，恩格尔伍德克利夫斯，1980。[37] E. Kaltofen。由直线程序给出的多项式的最大公因式。《ACM 杂志》，35(1)：231–264，1988。[38] E. Kunz。《平面代数曲线导论》。Birkauser，2005。[39] D. Le Brigand 和 J. Risler。Brill–Noether 算法与 Goppa 码。《法国数学会通报》，116(2)：231–253，1988。[40] S. Mac Lane。将素理想构造为代数域绝对值的方法。《杜克数学杂志》，2(3)：492–510，1936。[41] S. MacLane。多项式环中绝对值的构造。《美国数学会汇刊》，40(3)：363–395，1936。[42] R. Matsumoto 和 S. Miura。求代数曲线上具有两两不同离散赋值的线性系的一组基。《符号计算杂志》，30(3)：309–324，2000。[43] E. Nart。不同与判别式的局部计算。《计算数学》，83(287)：1513–1534，2014。[44] V. Neiger 和 T. X. Vu。计算一元关系模的典范基。载于 ISSAC ’17——第 42 届国际符号与代数计算研讨会，第 8 页，德国凯撒斯劳滕，2017 年 7 月。[45] J. Neukirch。《代数数论》。施普林格出版社，柏林，1999。[46] H. Niederreiter 和 F. Özbudak。渐近优良码，第 181–220 页。2008。[47] K. Okutsu。整基的构造，I。《日本学士院纪要 A 数学》，58(1)：47–49，1982。[48] Ö. Ore。代数域理论。《数学学报》，44(none)：219–314，1923。[49] Ö. Ore。代数域理论中的 Newton 多边形。《数学年刊》，99：84–117，1928。

[50] J . M. Peral. *Polí*$_{\text{剩线}\,\text{\textcircled{s}}\,\text{\textcircled{s}}\,\text{\textcircled{s}}\,\text{\textcircled{s}}\,\text{\textcircled{s}}\,\text{\textcircled{s}}\,\text{\textcircled{s}}}$ *de Newton de ord*在超 *i*或及 *licaci*一体 *itméticas*. 博士论 esis, Universitat d 文 巴塞罗那，1999。[51] P. Popescu-Pampu。《近似根》。Fields Institute Communiations，33:1–37，2002。[52] A. Poteaux 和 M. Weimann。《计算 Puiseux 级数：一种快速的分治算法》。《亨利·勒贝格年刊》，4:1061–1102，2021。[53] A. Poteaux 和 M. Weimann。《局部多项式因式分解：改进 Montes 算法》。载于《2022 年国际符号与代数计算研讨会论文集》，ISSAC '22，第 149–157 页，纽约，美国，2022。美国计算机协会。[54] A. Poteaux 和 M. Weimann。《快速整基计算》。载于《科学计算中的计算机代数：第 26 届国际研讨会，CASC 2024，法国雷恩，2024 年 9 月 2–6 日，论文集》，第 292–313 页，柏林、海德堡，2024。施普林格出版社。[55] J. Rosenkilde 和 A. Storjohann。《同时 Hermite–Padé 逼近算法》。《符号计算杂志》，102:279–303，2021。[56] P. Samuel。《代数数论》。Hermann，巴黎，1967。[57] J. Schicho、F.-O. Schreyer 和 M. Weimann。《曲线的戈纳尔映射与根式参数化的计算方面》。《工程、通信与计算中的应用代数》，24(5):313–341，2013 年 11 月。[58] W. M. Schmidt。《函数域中基的构造与估计》。《数论杂志》，39(2):181–224，1991。纪念 Theodor Schneider。[59] J. P. Serre。《局部域》。施普林格出版社纽约，第 2 次勘误印刷版，1995。[60] H. D. Stainsby。《整闭包的三角基》。博士论文，2014。[61] H. D. Stainsby。《整闭包的三角基》。《符号计算杂志》，87:140–175，2018。[62] I. Stenger。《Hess.lib：用于计算函数域和曲线上除子的黎曼–罗赫空间的 Singular 4.1.2 库》，2019。http://www.singular.uni-kl.de。[63] H. Stichtenoth。《代数函数域与码》。施普林格出版社，柏林，2009。[64] A. Storjohann。《高阶提升与整性认证》。《符号计算杂志》，36(3):613–648，2003。ISSAC 2002。[65] M. A. Tsfasman、S. G. Vlădutx 和 T. Zink。《模曲线、志村曲线与 Goppa 码：优于 Varshamov–Gilbert 界》。《数学新闻》，109(1):21–28，1982。[66] M. van Hoeij。《利用典范除子对代数曲线进行有理参数化》。《符号计算杂志》，23(2-3):209–227，1997。[67] E. J. Volcheck。《平面代数曲线的雅可比簇上的计算》。载于 L. M. Adleman 和 M.-D. Huang 编，《算法数论》，第 221–233 页，柏林、海德堡，1994。施普林格·柏林·海德堡。[68] M. Weimann。《利用伴随式分解双变量多项式》。《符号计算杂志》，58:77–98，2013。[69] W. Zhou。《阶基与核基的快速计算及相关问题》。博士论文，2013。