arXiv:2304.04701v1 [math.NT] 10 Apr 2023

曲线族中出现的伽罗瓦表示的显式计算

Nicolas Mascot*

都柏林圣三一学院

2023年4月11日

摘要

我们将计算曲线雅可比簇除法多项式的方法，从定义在 $\mathbb{Q}$ 上的曲线推广到定义在 $\mathbb{Q}(t)$ 上的曲线，以期计算曲面在 $\mathbb{Q}$ 上的 ´etale 上同调中出现的模 ℓ 伽罗瓦表示。尽管我们得到的除法多项式过于复杂，无法实现这一最终目标，但我们仍然得到了定义在 $\mathbb{P}^1_{\mathbb{Q}}$ 上的伽罗瓦表示显式曲线族，并研究了它们在相应曲线的坏约化赋值点处的退化。

致谢

作者感谢 Jean Gillibert帮助他开始理解第5.2节中介绍的材料。本文中的实验使用 [PlaFRIM] 实验测试平台完成，该平台由 Inria、CNRS（LABRI和 IMB）、波尔多大学、Bordeaux INP 以及阿基坦大区委员会支持（见 https://www.plafrim.fr/）；同时还使用了 EPSRC 计划资助 EP/K034383/1“LMF：L-函数与模形式”提供的Warwick 数学研究所计算机集群。所使用的计算机代数软件包为 [Pari/GP] 和 [Magma]。

关键词：伽罗瓦表示、除法多项式、 ´étale上同调、雅可比簇、曲面、曲线族、退化、分歧、逆伽罗瓦问题。

2020年数学学科分类：11Y40,11F80,14D06, 14H40, 14F20,14Q10。

*mascotn@tcd.ie

1 引言

假设我们给定了一个 S 定义在 $\mathbb{Q}$ 上的曲面，以及一个素数 $\ell \in \mathbb{N}$，使得 ´étale上同调空间 $\mathrm{H}^2_{\text{ét}}(S_{\overline{\mathbb{Q}}}, \mathbb{Z}/\ell\mathbb{Z})$包含一个伽罗瓦子模，该子模给出一个模 ℓ 伽罗瓦表示 ρ，而我们希望对其进行显式计算。这里的意思是计算一个多项式，该多项式按如下意义编码了 ρ：

定义 1.1. 设 K 是一个数域，且 $\rho : \mathrm{Gal}(\overline{K}/K) \longrightarrow \mathrm{GL}(V_\rho)$ 是一个模 ℓ 的伽罗瓦表示，其中 V_ρ 是一个有限维 $\mathbb{F}_\ell$-向量空间。若给定 $V_\rho \setminus \{0\}$ 与 $F(x)$ 在 K 的某个扩张 Ω 中的根之间的一个显式双射，且 $F(x)$ 在该扩张上完全分裂，并且 $F(x)$ 的根上的伽罗瓦作用与其在 V_ρ 上的作用相一致，则称可分多项式 $F(x) \in K[x]$ 编码了 ρ。特别地， $F(x)$ 的分裂域因而与由 ρ 切出的数域 $\overline{K}^{\mathrm{Ker}\,\rho}$ 一致。

在 [Mas22, 2], 中，我们概述了一种基于d ´evissage [SGA4 12, 3.4], 的方法，用于计算 $\rho \subset \mathrm{H}^2_{\text{ét}}(S_{\overline{\mathbb{Q}}}, \mathbb{Z}/\ell\mathbb{Z})$，其可非正式地概括如下。取一个适当的主导态射 $\pi : S \longrightarrow B$ 从 S 到 $\mathbb{Q}$上的一条曲线 B，并记 S_b 为 π 在一点 $b \in B$处的纤维。粗略地说，附着于 π的Leray 谱序列 [MilEC,12.7]表明，$\mathrm{H}^2_{\text{ét}}(S_{\overline{\mathbb{Q}}}, \mathbb{Z}/\ell\mathbb{Z})$ 由$\mathrm{H}^p_{\text{ét}}\left(B_{\overline{\mathbb{Q}}}, \mathrm{H}^q_{\text{ét}}(S_b, \mathbb{Z}/\ell\mathbb{Z})\right)$（$p+q=2$时）组成。由于对于 $p=0, q=2$ 以及对于 $p=2, q=0$ 的项都由无关紧要的部分构成，我们可以期待 ρ出现在$\mathrm{H}^1_{\text{ét}}\left(B_{\overline{\mathbb{Q}}}, \mathrm{H}^1_{\text{ét}}(S_b, \mathbb{Z}/\ell\mathbb{Z})\right)$中。由于 B和 S_b 都是曲线，并且一条曲线的$\mathrm{H}^1_{\text{ét}}$ 本质上就是其雅可比簇的扭点（精确表述见下文定理 1.2的第一部分），因此，合理的希望是通过以下方式计算 $\rho \subset \mathrm{H}^2_{\text{ét}}(S_{\overline{\mathbb{Q}}}, \mathbb{Z}/\ell\mathbb{Z})$:

1. 计算由纤维 S_b 的雅可比簇的 ℓ-扭点所给出的、由 $b \in B$ 参数化的伽罗瓦表示族,

2. 将这些数据拼接成曲线覆盖的一个显式模型 $C \longrightarrow B$，3. 在曲线 C 的雅可比簇的 ℓ-扭点中捕捉 ρ。

策略 1.1：通过考察曲线的雅可比簇的扭点，在曲面的 $\mathrm{H}^2_{\text{ét}}$ 中进行计算。

图 1.1 展示了这一情形。

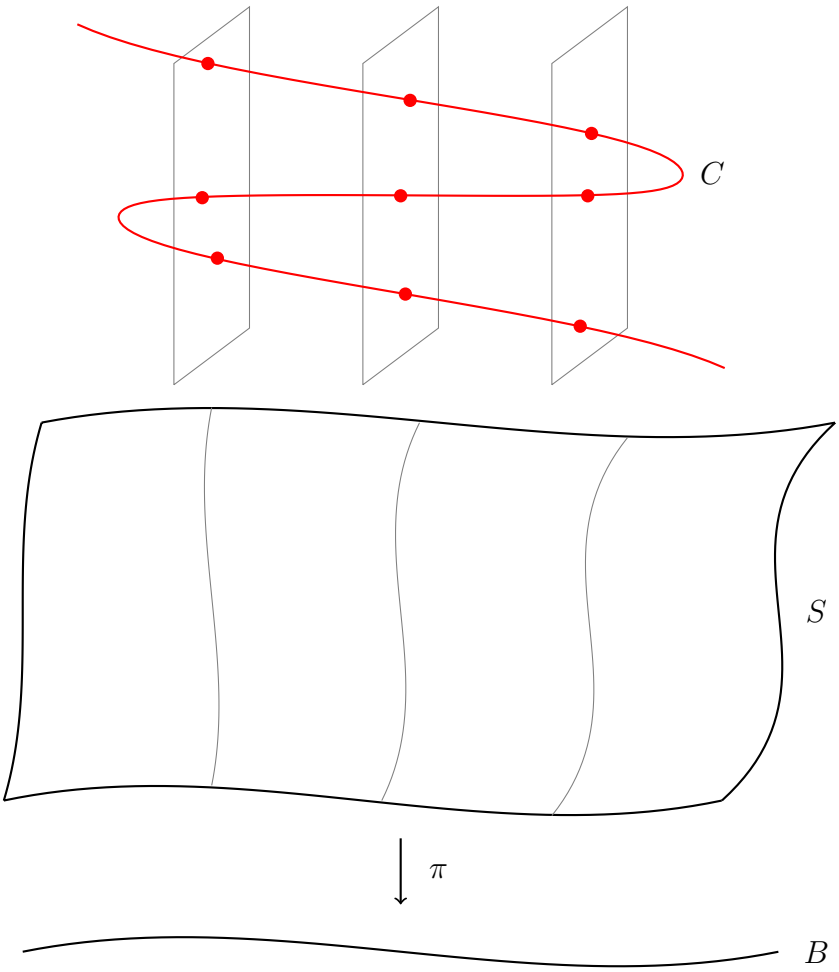


图 1.1：曲面 S 及其部分纤维 S_b（属于 π）。上方的矩形表示这些纤维的雅可比簇，矩形中的红点表示 ℓ-挠点。这些点定义了一条曲线 C，其雅可比簇应当在其 ℓ-挠群中包含 ρ。

更确切地说，我们有以下结果：

定理 1.2. 给定一个 $\mathbb{F}_\ell$-伽罗瓦模 M 和一个整数 $n \in \mathbb{Z}$，记 $M(n)$ 为 M 经模 ℓ 分圆特征的 n 次幂扭曲所得的对象。

1. 设 X 是数域 K 上一条非奇异、几何不可约的曲线，并令 J 为 X 的完备化的雅可比簇。若 X 完备，则 $\mathrm{H}^1_{\acute{e}t}(X_{\overline{K}}, \mathbb{Z}/\ell\mathbb{Z})$ 与 $\simeq J[\ell](-1)$ 作为伽罗瓦模同构。若 X 不完备，则 $\mathrm{H}^1_{\acute{e}t}(X_{\overline{K}}, \mathbb{Z}/\ell\mathbb{Z})$ 是 $J[\ell](-1)$ 的一个扩张，其核为若干个 $(\mathbb{Z}/\ell\mathbb{Z})(-1)$ 的副本。

2.假设 ρ 是包含于$\mathrm{H}^2_{\acute{e}t}(S_{\overline{\mathbb{Q}}}, \mathbb{Z}/\ell\mathbb{Z})$ 中的模 ℓ 伽罗瓦表示（在半单化意义下）。设 $B' = B \setminus Z$，其中 $Z \subset B$ 是 π 的坏纤维轨迹。假设 ρ 不含有任何形如$(\mathbb{Z}/\ell\mathbb{Z})(n)$的约当-赫尔¨德分量（对任意 $n \in \mathbb{Z}$），并且与 $\eta(-1)$ 没有公共分量，其中 η 是由伽罗瓦作用于 π的坏纤维的几何不可约分量所诱导的模 ℓ 置换表示。那么， ρ 也包含于$\mathrm{H}^1_{\acute{e}t}(C_{\overline{\mathbb{Q}}}, \mathbb{Z}/\ell\mathbb{Z})(-1)$中（在半单化意义下），其中 C 是由 B' 的非零 ℓ-扭点构成的覆盖的完备化，而这些扭点属于 S_b 的雅可比簇。

第1部分是标准的（参见 [MilEC，第14.2、14.4、16.2] 节），第 2 部分则是 [Mas22 的定理 7]。特别地，如果 ρ 满足第2 部分的假设，并且如果 C 是几何不可约的，那么就可以求得 ρ

（经过扭曲）位于 C的雅可比簇的 ℓ-扭点中。更一般地，如果 C 不是几何不可约的，则考虑一个 Galois数域 $K \subset \overline{\mathbb{Q}}$ ，使得 C 的几何不可约分支 C_i 定义在 K上；然后，在将$\overline{\mathbb{Q}}/K$ 的雅可比簇的 ℓ-扭点所赋予的 Gal($\overline{\mathbb{Q}}/K$) 表示诱导到 Gal($\overline{\mathbb{Q}}/\mathbb{Q}$) 的过程中，将会找到 ρ 。

现在让我们更详细地解释如何将这些观察转化为一个用于显式计算 ρ 的算法，并为简单起见，假设 C 是几何不可约的。在 [Mas19],中，我们描述了一种算法：给定一个定义在数域[1] K 上的适当、非奇异且几何不可约的曲线 C 以及一个素数 $\ell \in \mathbb{N}$，该算法计算出一个可称为 ℓ-除法多项式 $R_{C,\,\ell}(x) \in K[x]$ 的 C，也就是说，一个编码了由 ℓ-扭点所赋予的表示的多项式，其中 J 是 C 的雅可比簇，其含义见定义 1.1。只要存在一个 K 的素数 $\mathfrak{p} \nmid \ell$ ，使得 C 具有良约化，并且 $V \subset J[\ell]$可以由作用于 V上的 Frob$_\mathfrak{p}$ 的特征多项式刻画，该算法还能够计算由 $J[\ell]$的一个伽罗瓦子模 V 所赋予的子表示。

假设为了说明方便，给定方程 $f(x,y,t) \in \mathbb{Q}[x,y,t]$，使得我们的曲面 S 是由 $f(x,y,t) = 0$ 所定义的局部片的射影闭包经消奇点得到的。于是，自然可以选取 $B = \mathbb{P}^1_{\mathbb{Q}}$ 和 π，并取投影 $(x, y, t) \mapsto t$，从而将曲面 S 视为定义在 $\mathbb{Q}(t)$ 上的曲线 $\mathcal{S}$。此外，假设我们将除法多项式算法 [Mas19] 推广到定义在 $\mathbb{Q}(t)$ 上的曲线。这样，我们便能计算出 $\mathcal{S}$ 的一个除法多项式 $R_{\mathcal{S},\ell}(x,t) \in \mathbb{Q}(t)[x]$ ；它在 π 的任意良好纤维 $t = t_0 \in B$ 上的特化 $R_{\mathcal{S},\ell}(x,t_0) \in \mathbb{Q}(t_0)[x]$，将是该纤维 S_{t_0} 的一个 ℓ-除法多项式。于是，方程 $R_{\mathcal{S},\ell}(x,t) = 0$ 定义了曲线 C，使得 ρ （相差一个圆分特征的扭转）出现在 C 的雅可比簇的 ℓ-扭点中。因此，我们可以通过对 C 应用原始版本的 [Mas19] 来计算 ρ ：利用 ρ(Frob$_\mathfrak{p}$) 的特征多项式知识，从曲线 C 的雅可比簇 J_C 中分离出 ρ 的扭转，其中 $\mathfrak{p}$ 如上所述（有关这一方法的一个成功实例，参见 [Mas22] ）。

特别是，我们甚至无需计算 $J_C[\ell]$ 的全部 ℓ^{2g_C} 点；当 C 的亏格 g_C 适度增大时，即使对于 $\ell = 2$，这也不切实际。我们只需计算包含于 $J_C[\ell]$ 中、实现了 ρ 扭曲的子空间的 $\ell^{\deg \rho}$ 点。另一方面，为了得到 C 的一个方程，此方法迫使我们计算 $\mathcal{S}$ 的雅可比簇上的全部 ℓ-扭点，因此仅适用于 $\mathcal{S}$ 的亏格相当小时。

本文旨在说明， [Mas19] 确实可以推广到 $\mathbb{Q}(t)$ 上的曲线，从而在理论上能够明确计算出出现在曲面的 $\mathrm{H}^2_{\text{ét}}$ 中的模 ℓ 伽罗瓦表示。

注1.3。 [MO15] 和 [PTvL15]中介绍了用于计算 ´étale上同调的非常一般但遗憾的是不切实际的算法。相比之下，我们的目标是针对曲面的 $\mathrm{H}^2_{\text{ét}}$ 这一特定情形获得一种实用的方法。

我们展示了如何在第2节将 [Mas19] 推广到 $\mathbb{Q}(t)$上的曲线。由于 [Mas19]要求曲线以黎曼–罗赫空间的形式给出，因此我们在第3节简要回顾如何对平面代数曲线执行各种计算，包括确定黎曼–罗赫空间以及验证曲线是否几何不可约。

作为应用，在第 4 节中，我们计算了三条定义在 $\mathbb{Q}(t)$ 上、亏格分别为 1、2 和 3 的曲线 $\mathcal{S}$ 的除法多项式 $R_{\mathcal{S},\ell}(x,t)$。原则上，这使得我们能够利用 $\mathrm{H}^2_{\text{ét}}$ 计算相应曲面在 $\mathbb{Q}$ 上的情形；但遗憾的是，我们得到的亏格为 2 和 3 的曲线方程过于复杂，难以实际应用。不过，我们得到的数据仍值得关注，因为它编码了伽罗瓦表示族。

[1]目前，该算法仅针对 $K = \mathbb{Q}$ 实现，但将其推广到数域是很直接的。

在 $B = \mathbb{P}^1_{\mathbb{Q}}$ 上，并且研究这些族如何在坏纤维处退化尤为有趣，我们将在第5节中探讨这一点；尤其是，我们力求为这些退化的分歧找到几何解释。

2 $\mathbb{Q}(t)$上的除法多项式

2.1 $\mathbb{Q}$上的算法概述

仍设 $\ell \in \mathbb{N}$ 为素数。本节旨在说明，如何将我们的算法 [Mas19]（用于计算 $\mathbb{Q}$ 上的曲线的 ℓ-除法多项式）推广到 $\mathbb{Q}(t)$上的曲线。为此，我们先回顾该算法如何处理 $\mathbb{Q}$上的曲线 C：

1. 选取一个使 C具有良约化的素数 $p \neq \ell$。确定 $a \in \mathbb{N}$，使得曲线 C 的雅可比簇 J 的 ℓ-扭点定义在 $\mathbb{F}_q$上，其中 $q = p^a$。 2. 生成 $J(\mathbb{F}_q)[\ell]$ 中的点，使其张成 $J[\ell]$ 作为一个 $\mathbb{F}_\ell[\mathrm{Frob}_p]$-模。 3. 将这些点提升到 $J(\mathbb{Z}_q/p^e)[\ell]$，其中 $\mathbb{Z}_q$ 是具有剩余域 $\mathbb{F}_q$的 $\mathbb{Q}_p$ 的非分歧扩张的整数环，而 $e \in \mathbb{N}$ 是精度参数。 4. 构造求值映射 $\alpha \in \mathbb{Q}(J)$。 5. 展开 $\tilde{F}(x) = \prod_{0 \neq t \in J[\ell]} \big(x - \alpha(t)\big) \in (\mathbb{Z}/p^e\mathbb{Z})[x]$，并将其识别为 $\mathbb{Q}[x]$中的一个元素 $F(x)$。

算法 2.1： $\mathbb{Q}$ 上曲线的除法多项式。

因此，思路是选取一个辅助素数 p，并利用 $J[\ell]$ 在 p处是 ´艾塔莱的事实，来构造 $J[\ell]$中点的 p-进近似值。

多项式 $F(x)$随后就是 C 的一个 ℓ-除法多项式，其含义见定义 1.1。这假设 α 在 $J[\ell]$ 上有定义且是单射；如果情况并非如此，我们就换一个 α 重新开始。这还假设精度参数 e 足够大，从而可以根据其模 p^e 近似值 $F(x)$ 识别出 $F(x)\tilde{}$。特别地，尽管可以通过确认 $J(\mathbb{Z}_q/p^e)[\ell]$的元素确实是定义在 $F(x)$的不可约因子的茎域上的 ℓ-挠点的 p-进近似值来做到这一点，但这种方法的正确性并没有得到严格保证。此外，在大多数情况下，我们很容易确信输出 $F(x)$ 正确无误，例如检查它具有适当的伽罗瓦群和分歧。

为了在 J 中进行计算，该算法依赖于Makdisi算法 [KM04、KM07]。这些算法最初设计用于在域上工作，因此在 [Mas19] 中，我们将其推广到了局部环上，例如 $\mathbb{Z}_q/p^e$。这些算法还要求已知 C 的次数足够高的黎曼–罗赫空间的一个显式基，以便在内部表示 C（参见 [Mas19] 第1421页底部），因此，下面我们将在第3节中解释如何从 C 的一个（可能是奇异的）平面模型计算出这样的基。

2.2 算法在 $\mathbb{Q}(t)$ 上的概要

类比于将 $\mathbb{Q}$ 嵌入其完备化 $\mathbb{Q}_p$，自然可以通过将 $\mathbb{Q}(t)$ 嵌入 p-进劳朗级数域 $\mathbb{Q}_p((t))$，将算法 2.1 扩展到 $\mathbb{Q}(t)$ 上的曲线。这引出了以下计算 $\mathbb{Q}(t)$ 上曲线 $\mathcal{C}$ 的 ℓ-除法多项式的思路：

1.如有必要，平移参数 t，使得 $\mathcal{C}$ 在 $t=0$处具有良约化 C_0。选取 C_0的一个良约化素数 $p \neq \ell$，并确定 $a \in \mathbb{N}$，使得雅可比簇 J_0 的 ℓ 扭点定义在 $\mathbb{F}_q$上，其中 $q = p^a$。2.生成 $J_0(\mathbb{F}_q)[\ell]$ 的点，使其作为一个 $\mathbb{F}_\ell[\mathrm{Frob}_p]$-模张成 $J_0[\ell]$。3. 将这些点提升到 $\mathcal{J}(R)[\ell]$，其中 $\mathcal{J}$ 是 $\mathcal{C}$ 的雅可比簇，而 R 是形式幂级数环 $\mathbb{Z}_q[[t]]$的有限商。4. 构造一个求值映射 $\alpha \in \mathbb{Q}(t)(\mathcal{J})$。5. 展开 $\tilde{F}(x) = \prod_{0 \neq t \in J[\ell]} \big(x - \alpha(t)\big) \in R[x]$，并将其识别为 $\mathbb{Q}(t)$中的元素 $F(x)$。

算法 2.2：曲线在 $\mathbb{Q}(t)$ 上的除法多项式。

这假设我们能够将 Makdisi 算法推广到 $\mathbb{Z}_q[[t]]$ 的有限商环。这实际上不是问题，因为我们在 [Mas19] 中设计的推广适用于任意有限局部环 R，只要能在“良约化情形”下进行线性代数，具体如下：

定义 2.1。设 $R = \mathcal{O}/\mathfrak{a}$ 是局部整环 $\mathcal{O}$ 的有限商环。设 K 是 $\mathcal{O}$ 的分式域，且 k 是 $\mathcal{O}$ 的剩余域。我们称在良约化情形下可以在 R 上进行线性代数，是指：给定 $\mathcal{O}$ 上矩阵 A 模 $\mathfrak{a}$ 的约化，且 A 在 K 和 k 上的秩相同，我们能够在 $\mathcal{O}/\mathfrak{a}$ 中计算 K 的核 A 的一个基的近似值。

类似地，求值映射 α 的构造 [Mas19, 2.2.3] 可以直接推广到 $\mathbb{Q}(t)$ 上的曲线的雅可比簇。

最后，我们可以通过结合 p-进有理重构（正如我们在 [Mas19]的原始版本中所做的那样）和Padé 逼近（实际细节见下文的注2.2），将 $F(x)$ 的系数识别为 $\mathbb{Q}(t)$ 的元素。

2.3 扭点提升 (p,t)-进

为了将这些想法转化为一个完善的算法，我们仍需说明我们将使用何种有限商环 R of $\mathbb{Z}_q[[t]]$，以及如何将一个扭点从 $\mathbb{F}_q$ 提升到 R。

对于 R，第一个自然选择可以是 $R_e = \mathbb{Z}_q[[t]]/\mathfrak{m}^e$，其中 $\mathfrak{m} = (p,t)$ 是 $\mathbb{Z}_q[[t]]$ 的极大理想，而 $e \in \mathbb{N}$ 是算法 2.1 中所述的精度参数。乍看之下，这个选择颇具吸引力，因为它让我们有望同时提高挠点的 p-进精度和 t-进精度；但遗憾的是，我们将在下文看到，R_e 的克鲁尔维数为 2，实际上会给扭点提升带来算法障碍。此外，R_e 的元素具有 $\sum_{j<e} \lambda_j t^j$ 的形式，其中 $\lambda_j \in \mathbb{Z}/p^{e-j}\mathbb{Z}$ 的精度较低，

˜很大的 j；因此，在 $F(x)$ 中， t 的高次幂的系数将只有较低的 p-进精度，这会迫使我们增大 e 的值以便识别这些系数。这样一来，在整个计算过程中，我们都不得不携带 t 的高次幂，直到最后阶段才将它们丢弃，因为它们的 p- 进精度太低，无法将其识别为有理数，从而造成大量时间浪费。

因此，我们决定使用商 $R = R_{e,h} = (\mathbb{Z}_q/p^e\mathbb{Z}_q)[t]/(t^h)$，其中 $h \in \mathbb{N}$ 是第二个精度参数。引入这一新参数使我们能够独立设置 p-进精度和 t-进精度，事实证明这在实践中很有用。此外，这使得我们能够将算法推广到提升挠点。为了理解其中的原因，回顾一下我们在 $\mathbb{Q}$ 上于 [Mas19]中所采用的方法:

设 $\mathcal{O} = \mathbb{Z}_q$、 $\varpi = p$、 $\mathfrak{m} = \varpi\mathcal{O}$、 $K = \mathbb{Q}_q$，并设 J 是一个定义在 K上、在 $\mathfrak{m}$处具有良约化的曲线的雅可比簇。给定 $e \in \mathbb{N}$，点 $x \in J(\mathcal{O}/\mathfrak{m}^e)$在 Makdisi 算法中（如 [Mas19]中所推广）由一个矩阵 W_x 表示，其元素属于 $\mathcal{O}/\mathfrak{m}^e$；但反过来，这类矩阵中的大多数并不表示 J 的任何点。因此，我们从算法 [Mas19、算法 9] 开始：该算法给定一个整数 $e \in \mathbb{N}$ 和一个表示 $x \in J(\mathcal{O}/\mathfrak{m}^e)$ 的矩阵 W_x，计算 W_x 到 $\mathcal{O}/\mathfrak{m}^{2e}$ 的一个提升，该提升表示 x 到 $J(\mathcal{O}/\mathfrak{m}^{2e})$ 的一个提升。

由于 J 在 x 处的切空间，这个 x 的提升并不唯一；事实上，如果需要，该算法可以返回多个矩阵，分别表示 x 的不同随机提升。但这也意味着，即使 x 在 $J(\mathcal{O}/\mathfrak{m}^e)$ 中是 ℓ-扭点，这些到 $J(\mathcal{O}/\mathfrak{m}^{2e})$ 的提升也都无法保证（甚至不太可能）是 ℓ-扭点。

为了解决这个问题，我们展示了如何构造一个代数“坐标图” $\kappa : U \hookrightarrow \mathcal{O}^n$，其中 n 是一个不小于曲线 g 亏格的固定整数。这个坐标图定义在原点 $0 \in J(\mathcal{O})$ 的一个 $\mathfrak{m}$-进邻域 U 上，并将点 $x \in U$ 的 Makdisi 形式的模 $\mathfrak{m}^e$ 表示转化为向量 $\kappa(x) \in (\mathcal{O}/\mathfrak{m}^e)^n$，使得对所有 $e' \leqslant e$， $\kappa(x) = 0$ 模 $\mathfrak{m}^{e'}$ 当且仅当 $x = 0$ 属于 $J(\mathcal{O}/\mathfrak{m}^{e'})$。此外，由于 $\mathcal{O}$ 是主理想且其一致化参数为 $\varpi = p$，我们设计了第二种算法 [（Mas19，算法 11], ），如下计算点 $x \in J(\mathcal{O}/\mathfrak{m}^e)[\ell]$ 到 $J(\mathcal{O}/\mathfrak{m}^{2e})[\ell]$ 的唯一提升:

1. 使用算法 [Mas19，算法 9] 生成矩阵 $g+1$ $W_0, \cdots, W_g$，表示 $x_0, \cdots, x_g$ 到 $J(\mathcal{O}/\mathfrak{m}^{2e})$ 的随机提升 x。 2. 对于这些提升中的每一个，计算向量 $k_i = \frac{1}{\varpi^e}\kappa([\ell]x_i) \in (\mathcal{O}/\mathfrak{m}^e)^n$。 3. 尝试找到标量 $\lambda_1, \cdots, \lambda_g \in \mathcal{O}/\mathfrak{m}^{2e}$，使得 $\sum_{i=0}^{g} \lambda_i k_i = 0$ 模 $\mathfrak{m}^e$ 且 $\sum_{i=0}^{g} \lambda_i = 1$ 模 $\mathfrak{m}^{2e}$，并返回矩阵 $\sum_{i=0}^{g} \lambda_i W_i$。

算法 2.3：以 Makdisi 形式提升一个 ℓ-扭点。

其想法是， x_i 提升以很高的概率构成 J 在 x处的仿射坐标框架，从而保证 λ_i 的存在性与唯一性（否则，我们就用其他随机提升 x_i重新开始）。注意，由于假设 x模 $\mathfrak{m}^e$为 ℓ-扭点，对于所有 i，都有 $\kappa(x_i) = 0$模 $\mathfrak{m}^e$，因此除以 ϖ^e 确实会使 k_i 成为整数。进行这一除法是必要的，这样我们才能通过在局部环 $\mathcal{O}/\mathfrak{m}^{2e}$上求解线性系统来求出 λ_i，因为只要 x_i 确实构成仿射框架，就能保证该系统具有良约化（其含义见定义 2.1）。

现在让我们看看如何将算法 2.3 推广到 $\mathcal{O} = \mathbb{Z}_q[[t]$ 的情形。现在我们可以

看看为什么处理形如 $\mathbb{Z}_q[[t]]$ ($\mathbb{Z}_q[[t]]/,p)^e$ 的 $\mathbb{Z}_q[[t]]$ 的商会带来问题：在第2 步中，我们将得到 $\kappa([\ell]x_i)$，其元素属于 $(p,t)^e/(p,t)^{2e}$，但由于理想 (p,t) 不是主理想，我们将无法重新归一化定义 λ_i 的线性系统，使其成为满足定义 2.1 意义下的良约化的系统。

相比之下，通过使用形如 $(\mathbb{Z}_q/p^e\mathbb{Z}_q)[t]/(t^h)$ 的商，我们可以将算法 2.1 推广如下：给定一点 $x \in J_0(\mathbb{F}_q)[\ell]$，我们可以先按照 [Mas19], 中的描述，使用算法 2.3 的原始版本将其 p-进提升到 $J(\mathbb{Z}_q/p^e)[\ell]$，然后应用算法 2.3，以 $\mathcal{O} = (\mathbb{Z}_q/p^e\mathbb{Z}_q)[[t]]$ 和 $\varpi = t$ 为参数，将这次提升再 t-进提升到 $\mathcal{J}\big((\mathbb{Z}_q/p^e\mathbb{Z}_q)[t]/(t^h)\big)[\ell]$。事实上，尽管 $\mathfrak{m} = t\mathcal{O}$ 不再是极大的，但关键在于，商环 $\mathcal{O}/\mathfrak{m}^h = (\mathbb{Z}_q/p^e\mathbb{Z}_q)[t]/(t^h)$ 仍是一个局部环，其“剩余环” $k = \mathbb{Z}_q/p^e$ 仍是局部环，因此我们对 Makdisi 方法在局部环上的推广能够处理在其上进行运算的情形。

因此，我们能够将挠点从 $J_0(\mathbb{F}_q)[\ell]$ 提升到 $\mathcal{J}\big((\mathbb{Z}_q/p^e\mathbb{Z}_q)[t]/(t^h)\big)[\ell]$，从而将我们的方法 [Mas19] 扩展到定义在 $\mathbb{Q}(t)$上的曲线。

注 2.2. 实际上，当我们从 $(\mathbb{Z}/p^e\mathbb{Z})[t]/(t^h$ 中的近似值识别出元素 $c \in \mathbb{Q}(t)$ 时)
在算法2.2结束时，与其先通过 p-进有理重构将 c 识别为 $\mathbb{Q}[t]/(t^h)$的一个元素，再通过在 $\mathbb{Q}$ 上的 Pad´é 逼近将其识别为 $\mathbb{Q}(t)$ 的一个元素，不如反过来进行，也就是说，先使用在 $\mathbb{Q}_p$ 上的 Pad´é 逼近，将 c 识别为 $\mathbb{Q}_p(t)$的一个元素，其系数已知模 p^e，然后再将这些系数重构为有理数。其原因在于，除非 h 相当小，否则 c 截至 $O(t^h)$ 的泰勒系数通常会具有非常大的算术高度，因此识别它们将要求 p-进精度参数 e 非常高，这会大幅降低整个算法2.2的执行速度。例如，在下面的第 4.3节中，识别一个平面四次曲线族的二除法多项式的系数需要 $h = 128$；我们的实验表明，使用第一种方法，这反过来要求 $e = 4096$ ，而使用第二种方法则只需要 $e = 128$ 。

3 平面代数曲线的计算

应用策略 1.1 时，在两次使用我们的算法计算曲线的 ℓ-除法多项式时（第一次借助算法 2.2 在 $\mathbb{Q}(t)$ 上计算，随后借助算法 2.1 在 $\mathbb{Q}$ 上计算），曲线都是以平面方程给出的，而且该方程可能是奇异的。然而，正如上一节所述，我们的 ℓ-除法多项式算法依赖于 Makdisi 算法，而这些算法要求曲线由次数足够高的黎曼–罗赫空间表示。

因此，本节旨在说明如何对由可能奇异的平面模型给出的曲线进行显式计算，例如计算黎曼–罗赫空间。某些计算机代数软件包（如 [Magma],）已提供此类功能，但我们的 ℓ-除法多项式算法基于 [Pari/GP], ，而将数据从 [Magma] 转换到 [Pari/GP] 既繁琐，又容易打断自动化流程。因此，我们在 [Pari/GP], 中自行实现了一个用于计算平面代数曲线的软件包，并针对我们的需求进行了定制。

3.1 表示去奇异化曲线

固定一个基域 K ，在该域上可以通过算法分解多项式并进行线性代数运算。例如， K 可以是 $\mathbb{Q}$ 或 $\mathbb{Q}(t)$。我们还假设 K 具有特征 0，尽管这一假设并非必要（见下文注释 3.4）。

假设给定一个不可约多项式 $f(x,y) \in K[x,y]$。它定义了 K 上的一条仿射曲线 C，但通常我们希望处理的是 C，即的射影闭包 C的去奇异化。C 的非奇点可与 C的点相对应，因此我们只需要为 C 在无穷远处或位于 C的奇点上方的点提供一种特定表示。

一种可能的做法是将 C 的若干仿射模型（例如，由 C 的仿射部分）这种方法将导致涉及许多变量的 Gröbner基计算，可能会非常缓慢。因此，我们转而决定通过形式级数参数化来表示 C的这些点。例如，如果 $f(x,y) = xy + \cdots$，使得 C 在原点处有一个节点，那么 C 中对应于该节点两条分支的两个点可以用如下形式的参数化表示

$$x = t,\ y = t + O(t^2) \quad \text{and} \quad x = t,\ y = -t + O(t^2).$$

为了计算这类参数化，我们可以利用以下事实：域 $\overline{K}\{\{x\}\}$ 上的 Puiseux 级数域 $\overline{K}$ 包含 $K(x)$的一个代数闭包：对于 $f(x,y) \in K(x)[y]$ 的每个根 $y = \sum_{m \geqslant m_0} a_m x^{m/e} \in \overline{K}\{\{x\}\}$，我们得到该参数化

$$x = t^e,\ y = \sum_{m \geqslant m_0} a_m t^m \in \overline{K}((t)). \tag{3.1}$$

因此，人们可能会希望在 C 上的点与形如 $x = t^e$、$y \in \overline{K}((t))$的参数化之间存在一个双射，其中对于任意 $m \geqslant 2$，x 和 y 不同时为 t^m 中的级数；但遗憾的是，事实并非如此，因为(3.1)可以重新参数化为

$$x = t'^e,\ y = \sum_{m \geqslant m_0} \zeta^m a_m t'^m$$

其中 $t = \zeta t'$ 对任意 e 次单位根 $\zeta \in \overline{K}$ 都成立。特别是，采用这种方法，不可能将由系数 a_j 生成的 K 的扩张与相应点[2]的定义域相匹配。

幸运的是，Duval [Duv89]证明，只要允许采用如下形式的参数化 $x = bt^e, y \in \overline{K}((t))$，就可以规避这些问题，其中 $b \in \overline{K}$ 是常数：

定理 3.2。设 $f(x,y) \in K[x,y]$ 在 y 上是次数为 n 的不可约多项式。存在一组有限的参数化

$$x = b_j t^{e_j},\ y = \sum_{m \geqslant m_j} a_{j,m} t^m$$

其中对每个 j，b_j 和$a_{j,m}$ 都属于 $\overline{K}$，并张成 K 的有限扩张 L_j，且 f 在 $\overline{K}\{\{x\}\}$ 中的 n 个根无重复地表示为

$$y = \sum_{m \geqslant m_j} a_{j,m}^{\sigma} (\beta x^{1/e_j})^m$$

其中 σ 遍历 L_j 到 $\overline{K}$ 的 K-嵌入，而 β 遍历 $\{\beta \in \overline{K} \mid \beta^{-e_j} = b_j^{\sigma}\}$（因此 $t = \beta x^{1/e_j}$ 就是解 $x = b_j t^{e_j}$ 关于 t 所得到的结果）。

[2]当然，除非 K 恰好包含所有阶的单位根；不过对于我们所考虑的应用，这种情况通常不会发生，因为我们将在 $K = \mathbb{Q}$ 或 $\mathbb{Q}(t)$ 上进行研究。

这意味着，在这个参数化集合与函数域 $K(C) = K(x)[y]/f(x,y)$在 C上方的赋值点集合之间存在一个伽罗瓦等变双射，因此也与 C 在 $x = 0$上方的点存在一个伽罗瓦等变双射。特别地，我们有

$$\sum_j e_j f_j = n$$

其中， $f_j = [L_j : K]$ 是剩余次数， e_j 是分歧指数，因此~ L_j 是 C中相应点的定义域，并且

$$\prod_{\sigma: L_j \hookrightarrow \overline{K}} \prod_{\beta^{-e_j} = b_j} \left(y - \sum_{m \geqslant m_j} a_{j,m}^{\sigma} (\beta x^{1/e_j})^m \right) \tag{3.3}$$

是 $f(x,y)$ 在 $K((x))$ 上的不可约因子。请注意，这与通过研究定义该数域的多项式在 $\mathbb{Q}_p$ 上的因式分解来确定素数 p 在数域中的分解情况类似。

Duval 解释说，这些参数化可以按如下方式计算：

1.绘制 $f(x,y)$的牛顿多边形，也就是说，点 $(i,j) \in \mathbb{Z}^2$ 的下凸包，使得系数$a_{i,j}$在 $f(x,y)$ 中的 $y^i x^j = \sum_{i,j} a_{i,j} y^i x^j$ 非零。

2. 对于牛顿多边形的每个线段 $pi + qj = r$，其中 p、q、$r \in \mathbb{Z}$，且 gcd(p,q) =1，求 u、$v \in \mathbb{Z}$ 使得 $up + vq = 1$，并令 $f_0 = \sum_{pi+qj=r} a_{i,\ j} x^j y^i$。然后对于每个满足 $f_0(b^{-u}t^q, b^v t^p) = 0$ 的 $b \in \overline{K}$，令 $f_1(x,y) = f\big(b^{-u}x^q \text{、} \ b^q x^p(1+y)\big)$。如果 f_1 在 y 中是非奇异的，则停止；否则，将 f 替换为 f_1，返回步骤 1。

算法 3.1：计算参数化。

其思路是使用牛顿多边形确定 $f(x,y) = 0$ 的根 y的赋值，然后将 f_0 视为“首项”，把其他项看作高阶扰动。经过有限次迭代后，得到的方程关于 y 将是非奇异的，因此可以通过牛顿迭代求出其根。由此，我们得到显式的~参数化，表示 C 上方的点，其中每个点的定义域都是由相应参数化的系数生成的扩张。当然，通过适当地平移变量 x，也可以类似地得到 x 的其他取值上方各点的参数化。

注 3.4。我们假设 K 的特征为 0，唯一原因是为了确保 $f(x,y) \in K(x)[y]$ 在 $\overline{K}\{\{x\}\}$ 上完全分裂。定理 3.2 和算法 3.1 实际上在正特征 π 下仍然成立，只要没有野分歧，也就是说，没有任何赋值点的分歧指数能被 π 整除；这等价于在步骤 1 中考察牛顿多边形的线段 $pi + qj = r$ 时，满足 $\pi \nmid q$。因此，本节介绍的所有算法~在正特征下仍然成立，只要 C 作为 $\mathbb{P}^1_x$ 的覆盖至多是驯分歧的；在实践中，这通常意味着我们只需排除 2、3 或 5 这样很小的特征。此外，在执行算法 3.1 的过程中检查 $\pi \mid q$，我们便能可靠地检测出该算法何时会失败。

3.2 正则微分与亏格

现在我们已经计算出了表示奇点和无穷远点的参数化，˜就可以求出 C上的正则微分基。事实上，众所周知 [DP13, 2.9] 对于所有严格位于 $f(x,y)=\sum_{i,j}a_{i,j}y^ix^j$支撑集的完整（而非低维）凸包内部的$(i,j)\in\mathbb{Z}$，微分$\omega_{i,j}=\frac{x^{j-1}y^{i-1}}{\partial f/\partial y}\mathrm{d}x$除˜可能在奇点处外处处正则，并且 C 上的每个正则微分都是这些微分的 K-线性组合。因此，只需找出这样的线性组合：沿着与奇点对应的参数化展开时，不含极˜部分，即可得到正则微分基。这相当于在 K上进行线性代数。特别地，正则微分基的大小就是 C 的亏格。

虽然有更直接的方法可以计算亏格，但实际求出正则微分基在实践中非常有用。例如，这样就能检验曲线是否为超椭圆曲线；若是 [vH2]，还可以找到一个显式的变量替换，将其化为魏尔斯特拉斯形式。如果曲线不是超椭圆曲线，则可以改为计算其典范像，从而为由复杂且高度奇异的方程定义的曲线寻找更简单的模型（例如，我们在 [Mas22, 3] 中采用的就是这种方法）。

3.3 黎曼–罗赫空间与额外功能

借助表示奇点和无穷远点的参数化，我们还可以计算整闭包

$$\mathcal{O}=\{s\in K(C)\,|\,\text{the only poles of } s \text{ are above } x=\infty\}$$

在 $K[x]$ in $K(C)$ 中，其方法与数域情形类似 [Coh00, 2.4]：对于每个满足 $d(x)^2\,|\,\mathrm{disc}_y f(x,y)$ 的不可约 $d(x)\in K[x]$，我们从近似式 $(\omega_j=y_1^{j-1})_{1\leqslant j\leqslant n}$ 开始构造一个局部基，其中 $y_1=a(x)y$，而 $a(x)$ 是 $f(x,y)\in K(x)[y]$ 的首项系数；随后不断细化，只要能找到标量 $\lambda_j\in K[x]/\big(d(x)\big)$，使得在沿表示 $d(x)=0$ 上方点的参数化代入时，$\frac{\sum_j\lambda_j\omega_j}{d\,x}()$ 没有极部。然后，通过在 $K[x]$ 上计算埃尔米特标准形，将这些局部基合并为 $K[x]$-基的 $\mathcal{O}$。

借助 $\mathcal{O}$ 的这个 $K[x]$-基，我们可以通过找出 $\mathcal{O}$ 中哪些元素在 $x=\infty$ 上方也正则，来检验 C 是否几何不可约。

我们还可以计算黎曼–罗赫空间，因为给定 C 上的一个除子，很容易计算出一个“公分母” $d(x)\in K[x]$，使得相应的黎曼–罗赫空间包含于 $\frac{1}{d\,x}()\mathcal{O}$。

这使得我们能够为亏格为 0 的曲线找到锥模型。如果 K 是一个数域，那么我们可以利用哈塞–明可夫斯基定理的构造性版本，检验该曲线是否有有理点；若有，黎曼–罗赫的另一种应用便能给出该曲线 [vH0] 的一个显式有理参数化。黎曼–罗赫空间还使得我们能够将已知有有理点的亏格为 1 的曲线转化为魏尔斯特拉斯形式的椭圆曲线。

最后，现在我们能够计算黎曼–罗赫空间了，就可以初始化 Makdisi 的˜算法，以便在 C 的雅可比簇中进行计算。

我们已在 [Pari/GP] 中实现了本节所述的所有功能。我们的代码与 [Magma], 相比表现相当出色，可在 [Pari/GP], 的一个开发分支中使用；该分支还包含了第2节中所述的 [Mas19] 到 $\mathbb{Q}(t)$ 的推广。

4 示例

为了展示第2节中所述算法的应用，我们计算了若干在 $\mathbb{Q}(t)$ 上的除法多项式。计算在 [PlaFRIM] 集群上进行。

4.1 热身

作为合理性检查，我们首先使用新算法，求得由 $\mathcal{E}$ 定义的椭圆曲面 3-挠点的方程

$$y^2 = t(1 + 2t - t^2)(x^2 - 1)(t^2x^2 - 1)$$

该曲面曾是我们在 [Mas22] 中关注的对象。尽管在椭圆曲线上使用 Makdisi 算法显然有些小题大做，我们还是立即得到了除法多项式

$$3x^8 + 4t(t^2 + 1)(t^2 - 2t - 1)x^6 + 6t^4(t^2 - 2t - 1)x^4 - t^8(t^2 - 2t - 1)^2 \in \mathbb{Q}(t)[x],$$

它比我们在 [Mas22] 中借助 [Pari/GP] 的 `elldivpol` 函数得到的结果简单得多，甚至比我们在 [Mas22] 中能够得到的最佳模型还要漂亮。更值得一提的是，这个多项式让人联想到 $t = 0$ 和 $t^2 - 2t - 1 = 0$ 是 $\mathcal{E}$ 的坏约化赋值点。

4.2 一个超椭圆族

受这个第一个例子的鼓舞，我们随后计算了由方程定义的超椭圆曲面 H 所对应的亏格为 $g = 2$ 的曲线在 $\mathbb{Q}(t)$ 上的 ℓ 除法多项式 $\ell = 3$

$$y^2 = x^6 - x^4 + (t - 1)(x^2 + x).$$

备注 4.1。方程 $y^2 = x^6 - x^4 + t(x^2 + x)$本来会更自然，但我们对参数 t 进行了平移，以便在 $t = 0$ 处具有良约化。上一个例子中我们也做了同样的处理，但我们在那里展示的多项式是未平移的版本。

我们选择使用辅助素数 $p = 17$，因为要使 ℓ-扭点定义在 $\mathbb{Q}_{p^a}((t))$ 上只需 $a = 6$；并且我们计算了 $e = 48$ 和 $h = 16$的模 (p^e, t^h) ℓ-扭点。计算耗时 2 分钟，我们得到了一个 ℓ-除法多项式 $R_{H,3}(x, t) \in \mathbb{Q}(t)[x]$，其次数为 $\ell^{2g} - 1 = 80$，系数的分子次数最高为 12，系数最多有 27 位小数，公分母为 $d_H(t) = 3^3(t + 1)^2$。

这个分母可能可以由以下事实解释：H 在 $t = -1$处具有坏约化；尽管可以观察到 $d_H(t)$ 不被 $t - 1$ 整除，而 H 显然也在 $t = 1$ 处具有坏约化。

4.3 平面四次曲线族

作为最后一个例子，我们计算了一个 ℓ-除法多项式，用于 $\ell = 2$ 的 Q 平面四次曲线族；该族的一般亏格为 $g = 3$，由方程定义。

$$x^4 + (2 - t)y^4 + 2x^3 + x(x + y) + (t - 1)(y + x^2 + x) = 0.$$

这次，我们采用了 $p = 5$，因为它支持 $a = 7$，精度参数为 $e = h =$128。经过一个半小时，我们得到了一个次数为 $R_{Q,\ 2}(x, t) \in \mathbb{Q}(t)[x]$ 的除法多项式

，公分母为 $d_Q(x) = (t-2)(2t-3)^4 d_{22}(t)$，其中 $d_{22}(t) \in \mathbb{Z}[t]$是一个 22 次不可约多项式，首项系数为 $2^{16},$，其系数分子的次数最高可达 54，系数最多有 39 位。

需要注意的是， Q 在 $\mathbb{P}^1_t$ 的一个赋值点处有坏约化，该赋值点在 $\mathbb{Q}$上的次数为 14；由于这必定会以某种方式反映在$R_{Q\text{的特化行为异常上，}2}$ 在 t的这个取值处的情况，这便解释了为什么$R_{Q\text{的系数如此}2}$ 复杂，以及为什么识别它们所需的 t-进精度（$h = 128$）远高于前一个例子。这也解释了为什么这次计算比前一次耗时长得多。

这一次，分母的大部分“几何内容”，也就是说因子$(2t-3)^4$ 和 $d_{22}(t)$，并不对应于 Q 的坏约化赋值点（但 $t-2$ 确实对应），而应当可能被解释为使求值映射 $\alpha \in \mathbb{Q}(t)(\mathcal{J})$ 无法在所有 2-挠点上定义的 t 的值（关于 α的定义及其背景，参见第2节）。然而，值得注意的是，在全部三个例子中，“算术内容”，也就是说公分母的首项系数，都是 ℓ 的幂。

注记 4.2. 我们的计算依赖于 [Pari/GP]的多项式运算，但遗憾的是，它无法利用高次多项式乘法的快速算法。鉴于所需的 t-进精度很高，如果能够使用快速多项式运算，计算 $R_{Q,2}$ 很可能会更快。

注记 4.3. 如引言中所述，我们根据 $\mathbb{Q}_p[[t]]$ 中的近似值，将除法多项式的系数确定为 $\mathbb{Q}(t)$中的元素，这一做法并不严谨。然而，我们很容易确信这些除法多项式正确无误，例如可以检查它们在 t 的良约化非零值处的伽罗瓦群包含于 GSp$(2g, \ell)$，并且其分歧与 Néron-Ogg-Shafarevich [ST68] 的预测相符。我们将在下一节确立这些除法多项式在 t 的坏值处特化所得对象的分歧的几何解释，这也证明其系数已被正确确定。

5 伽罗瓦表示的退化及其分歧性

令人失望的是，我们在前一节得到的除法多项式 $R_{H,3}(x,t)$ 和 $R_{Q,2}(x,t)$ 如此复杂，以至于既不能由 [Magma]，也不能由第3节介绍的平面曲线程序包确定其亏格，更不用说计算使用 Makdisi 算法在其雅可比簇上进行运算所需的黎曼–罗赫空间了。因此，很遗憾，我们无法完成对相应曲面的étale 上同调中出现的伽罗瓦表示的计算。

然而，这些除法多项式仍然是非常有价值的数据，因为每一个多项式都编码了一个由 $\mathbb{P}^1_{\mathbb{Q}}$ 参数化的伽罗瓦表示族。此外，这些表示远非平凡，因为它们具有满像。事实上，利用 [Magma] 很容易检查出，$R_{H,3}(x,t)$在 t 的一个有理良约化值处的特化（例如在 $t=0$处）在 $\mathbb{Q}$ 上的伽罗瓦群为 GSp(4, 3)，这证明了 $R_{H,3}(x,t)$在 $\mathbb{Q}$上的伽罗瓦群为 GSp(4, 3)；因此，根据希尔伯特不可约性，$R_{H,3}(x,t)$ 的大多数特化的伽罗瓦群都将是 GSp(4, 3)，所以 $R_{H,3}(x,t)$可以被看作是一个关于 t的多项式族（多项式变量为 x），其泛伽罗瓦群为 GSp(4,3)。类似地可以检查，$R_{Q,2}(x,t)$定义了一个具有泛伽罗瓦群GSp(6,2) $=$ Sp(6, 2) 的多项式族，而后者恰好是一个单群。

5.1 坏地方的分解

研究这些伽罗瓦表示族在 t 的取值为相应曲线在 $\mathbb{Q}(t)$ 上的坏约化赋值点时如何退化，尤其令人感兴趣。

我们由 H 定义的超椭圆族的坏地方

$$y^2 = x^6 - x^4 + (t-1)(x^2+x)$$

通过考察右侧的判别式，可以轻易确定这些值，结果为 $t=1$、$t=-1$、$t=283/256$ 和 $t=\infty$。

为了分析 $R_{H,3}(x,t)$ 在这些赋值点处的退化，不能简单地将这些值代入 t，就像试图通过模 p 分解多项式来理解有理数域中素数 p 的分解，而不考虑与该多项式关联的整环的指数一样，这样做同样是不正确的。相反，我们必须研究 $R_{H,3}(x,t)$ 的各个版本在 $\mathbb{Q}((t))$ 上的因式分解，这些版本经过平移，使得当前考察的坏赋值点变为 $t=0$。根据 (3.1)，这等价于确定 t 中的分歧，以及曲线 $R_{H,3}(x,t)=0$ 的消奇化上方、位于 $t=0$ 之上的点的定义域；借助我们对第3.1节所述 Duval 方法的实现，我们可以做到这一点。由此得到以下数据：

t	地方分解	伽罗瓦群	分歧
1	$\mathbb{Q}(\sqrt{3})^1 \cdot \mathbb{Q}(\sqrt{-1})^3 \cdot \left(\mathbb{Q}(\zeta_9)^+(\sqrt{-1})\right)^9 \cdot \left(\mathbb{Q}(\zeta_{36})^+\right)^3$	$(\mathbb{Z}/36\mathbb{Z})^\times$	$2,3$
-1	$\mathbb{Q}(\sqrt{-21})^1 \cdot K_6^1 \cdot K_{18}^1 \cdot {K'_{18}}^3$	$C_2 \times C_3 \cdot S_3^2$	$2,3,7,11$
$\frac{283}{256}$	$\mathbb{Q}(\sqrt{-14})^1 \cdot {K''_{18}}^3 \cdot K_{24}^1$	$(C_2 \times C_3 \rtimes S_3) \cdot S_4$	$2,3,7,11$
∞	$\mathbb{Q}^2 \cdot \mathbb{Q}^6 \cdot \mathbb{Q}(\sqrt{3})^4 \cdot \mathbb{Q}(\sqrt[4]{12})^4 \cdot \mathbb{Q}(\sqrt[4]{12})^{12}$	D_4	$2,3$

表 5.1：H 的坏地方分解。

在此表中，第二列显示了赋值点 $\mathbb{Q}(t)$ 在函数域 $\mathbb{Q}(t)[x]/\left(R_{H,3}(x,t)\right)$ 中的分解；例如，在 $t=\infty$ 上方有五个赋值点，其中两个的剩余域为 $\mathbb{Q}$，相应的分歧指数为 2 和 6；一个的剩余域为 $\mathbb{Q}(\sqrt{3})$，分歧指数为 4；另有两个的剩余域为 $\mathbb{Q}(\sqrt[4]{12})$，相应的分歧指数为 4 和 12。第三列显示了这些剩余域的伽罗瓦闭包的复合域的伽罗瓦群，最后一列列出在该伽罗瓦闭包中，或等价地在至少一个剩余域中发生分歧的素数。在此表中，$\mathbb{Q}(\zeta_m)^+$ 表示分圆域 $\mathbb{Q}(\zeta_m)$ 与 $\mathbb{R}$ 的交，而 K_d、K'_d、K''_d 等表示彼此不同构的、次数为 d 的数域。对于伽罗瓦群，C_n、D_{2n} 和 S_n 分别表示循环群、二面体群和对称群，而 $A \cdot B$ 表示一个非分裂群扩张，其正规子群为 A，商群为 B。对于 $t=1$，我们特例地将伽罗瓦群表示为 $(\mathbb{Z}/36\mathbb{Z})^\times$，而不是 $C_6 \times C_2$，因为其伽罗瓦闭包就是 36^{th} 分圆域。

我们将在第5节的5.2节阐明其中一些剩余域的性质，并解释这些分歧素数为何会出现。

对于我们的四次曲线族 Q，坏约化的赋值点为 $t=1$、$t=2$、$t=\infty$，以及上一节提到的 14 次赋值点。由于最后这个赋值点的次数很高，对其进行显式计算并不实际，因此我们从现在起将其忽略。我们得到以下数据：

t	地方分解	伽罗瓦群	分歧
1	$\mathbb{Q}^1 \cdot \mathbb{Q}^1 \cdot \mathbb{Q}^1 \cdot K_8^1 \cdot K_8^1 \cdot K_8'^2 \cdot K_8''^2 \cdot K_{12}^1$	$C_2^3 \rtimes S_4$	$2, 229$
2	$\mathbb{Q}^1 \cdot \mathbb{Q}^2 \cdot \mathbb{Q}^4 \cdot \mathbb{Q}^8 \cdot \mathbb{Q}^8 \cdot \mathbb{Q}(\sqrt{2})^4 \cdot \mathbb{Q}(\sqrt{2}, \sqrt{15})^8$	C_2^2	$2, 3, 5$
∞	$\mathbb{Q}^1 \cdot \mathbb{Q}^2 \cdot \mathbb{Q}^4 \cdot K_3^2 \cdot K_3^4 \cdot K_6^1 \cdot K_8'''^4$	$S_4 \times C_2$	$2, 23$

表 5.2： Q 的部分坏地方的分解。

5.2 特殊纤维上分歧的可视化

我们现在希望为前面表格中观察到的分歧素数找到几何解释。我们还将解释某些剩余域出现的原因。

在 $\mathbb{P}_t^1$ 的良约化处，曲面的纤维是一条良好的曲线 F，N´eron-Ogg-Shafarevich 判据 [ST68] 会让我们预期在 $p = \ell$ 处，以及在 F 的坏约化素数处发生分歧。类比地，在坏处，我们会预期在 $p = \ell$ 处，以及在使坏纤维变得“更糟”的素数 p 处发生分歧。

更具体地说，应将这个坏纤维理解为曲面在 $\mathbb{Q}$ 上的极小正则模型的纤维；而所谓该纤维模 p 后变得更糟，意味着这个特殊纤维模 p 的约化，与曲面模 p 约化后所得极小正则模型的特殊纤维并不一致。更形象地说，可以概括为：除了 $p = \ell$ 之外，这些素数 p 也会使取极小正则模型的特殊纤维这一操作与模 p 约化不交换。

注 5.1. 与其考察极小正则模型的特殊纤维，考虑半稳定纤维也同样合理。我们姑且接受这种不精确的说法，因为实际上我们考察的是基底 $\mathbb{P}_{\mathbb{Z}}^1$ 上的曲线族，而其维数为 2（一个几何维度和一个算术维度）；据作者所知，此时已不再存在关于雅可比簇的典范良模型（即 N´eron 模型）的概念。

5.2.1 超椭圆曲面

我们先从超椭圆曲面 H 开始。

$t = 1$ 处的纤维

曲面 H 在 $t = 1$上方并不正则，但在特征 $\pi \neq 2$下，经过一次爆破后便变得正则，其特殊纤维随后由两条有理曲线组成，排列方式如图 5.1 所示：

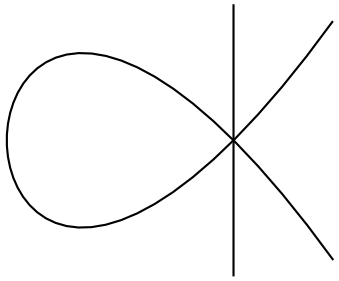


图 5.1： 当 $\pi \neq 2$ 时， $t = 1$ 处 H 的特殊纤维。

相比之下，在特征 $\pi = 2$下，要经过更多次爆破，才能得到 H 在 $t = 1$上方的正则模型。这解释了表 5.1 中观察到的 $t = 1$在 $p = 2$ 处的分歧。至于 $p = 3$处的分歧，只需指出我们考察的是 3-挠点即可解释。

$t = -1$处的纤维

对于 $t = -1$，在特征 $\pi \notin \{2, 7, 11\}$ 下，经过一次吹起后，我们再次得到一个正则曲面。其特殊纤维由一条椭圆曲线和一条有理曲线组成，如图 5.2 所示。第3节中介绍的平面曲线软件包告诉我们，在 $\mathbb{Q}$ 上，椭圆分支是 [LMFDB] 标签 176.a2 对应的曲线，其导子为 $176 = 2^4 \cdot 11$。

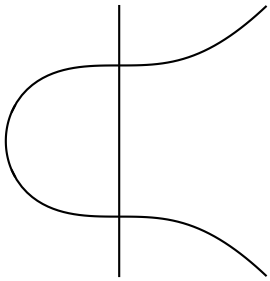


图 5.2：当 $\pi \notin \{2, 7, 11\}$ 时， H 在 $t = -1$ 处的特殊纤维。

因此，在特征 $\pi = 11$ 下，椭圆曲线退化，特殊纤维变成图 5.3 所示的形态：

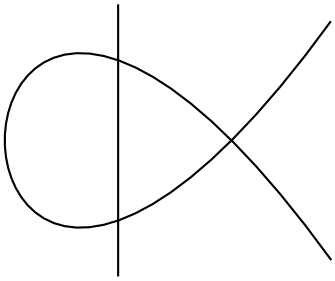


图 5.3： H 模 11 在 $t = -1$ 处的特殊纤维。现在两个分支都是有理曲线。

这解释了为什么我们在 $p = 11$ 处观察到了分歧。至于 $\pi = 2$，其特殊纤维与 $t = 1$ 的相同，因为 t 定义在 $\mathbb{Z}$ 上，且 $-1 \equiv 1$ 模 2。

下面仍需解释在 $p = 7$处的分歧。仔细观察 $\mathbb{Q}$上的特殊纤维（如图 5.2 所示）可以看出，两个分支的交点并非有理点，而是定义在 $\mathbb{Q}(\sqrt{7})$上，并且彼此为伽罗瓦共轭；因此，当我们模 $\pi = 7$ 约化时，这些交点会合并，特殊纤维变成图 5.4 所示的形状，这解释了在 7 处的分歧：

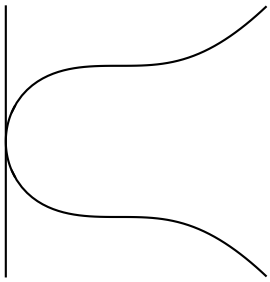


图 5.4: H 模 7 在 $t=-1$ 处的特殊纤维。

注 5.2. 正如预期的那样，我们的剩余域捕捉到了特殊纤维中椭圆曲线部分的 3-挠点。更具体地说，这条椭圆曲线 176.a2 的两个 3-挠点在 $\mathbb{Q}(\sqrt{-1})$ 上定义，而其余六个 3 阶点分别定义在某个次数为 6 的数域 F 的一个伽罗瓦共轭域上。表 5.1 中出现的域 K_6 实际上是 $\mathbb{Q}(\sqrt{-1})$ 的一个次数为 3 的扩张，相对判别式为 $(1+\sqrt{-1})^2\cdot 3^3\cdot 7$；而同一表中出现的域 K_{18} 是 F 的一个次数为 3 的扩张，仅在 2 和 7 之上分歧。这些扩张的次数为 3 这一事实可以用广义雅可比簇来解释，因为我们考察的是 3-挠点。奇怪的是，似乎无法对 K'_{18} 作出类似的解释，但我们仍指出， K_{18} 和 K'_{18} 具有相同的伽罗瓦闭包，其中也包含 K_6。

在 $t=\infty$ 处的纤维

曲面 H 实际上在任意特征下于 $t=\infty$ 已经是正则的，因此我们可以直接将其特殊纤维可视化，结果发现它有一个相当糟糕的奇点:

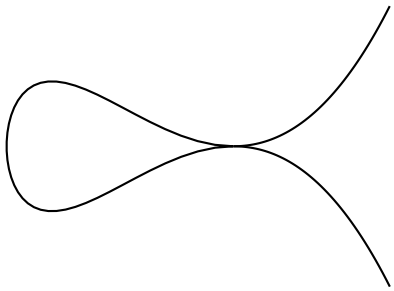


图 5.5: 任意特征下 $t=\infty$ 处 H 的特殊纤维。

H 在 $t=\infty$ 处即使模 $\pi=2$ 仍是正则的这一事实，无法解释我们为何在表 5.1中观察到 $p=2$ 处分歧。然而，我们得到的特殊纤维显然不是半稳定的，所以我们看到的可能是“错误的”纤维。

为了进一步研究，我们可以从半稳定纤维的角度入手，这意味着必须进行一次分歧基变换 [IM98, 3.47]。最简单的候选方案是基变换到 $\mathbb{Q}(t^{1/2})$，也就是在方程中用 t^2 替换 t。结果是 H不再是正则的，即使在特征 $\pi=0$下也是如此；经过几次爆破后，我们发现，在特征 $\pi\neq 2$下，特殊纤维由四条有理曲线构成，其中一条的重数为二，如图 5.6 所示:

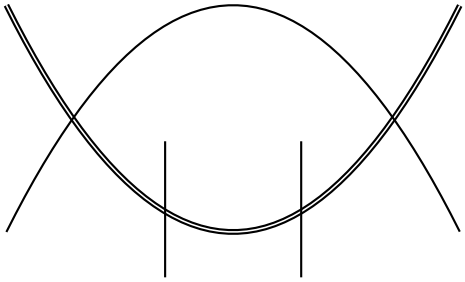


图 5.6：谱　　特征为 $\pi \neq 2$ 时，H 从 $\mathbb{Q}(t^{1/2})$ 到 $t=\infty$ 的基变换的特殊纤维　　.

相反，在特征 $\pi = 2$下，消解奇点需要更多次爆破，这最终解释了我们在 $p = 2$处观察到的分歧。

注 5.3. 由于存在一个重分支，经过基变换到 $\mathbb{Q}(t^{1/2})$ 后得到的特殊纤维仍然不是半稳定的，还需要进一步进行基变换才能解决这一问题。然而，正如注 5.1 中所解释的，由于我们对“良好”模型没有明确的概念，因此我们满足于这个相当令人满意的解释。

$t = 283/256$ 处的纤维

在特征 $\pi \notin \{2, 3, 7, 11\}$下，$H$ 在 $t = 283/256$ 处已经是正则的，其特殊纤维是一条带有节点自交的亏格 1 曲线，如图 5.7 所示：

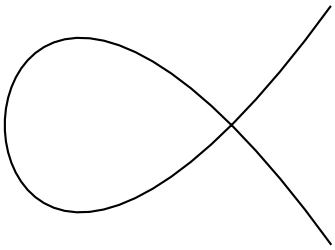


图5.7：当 $\pi \notin \{2, 3, 7, 11\}$ 时，H 在 $t = 283/256$ 处的特殊纤维。

在 $\mathbb{Q}$ 上，这个纤维的消奇异化是椭圆曲线 [LMFDB]，其标签为 528.c2，导子为 $528 = 2^4 \cdot 3 \cdot 11$。正如预期，备注 5.2 中描述的现象再次出现：表 5.1 中列出的数域 K_{24} 是一个次数为 8 的域的三次扩张；该域的伽罗瓦共轭域上定义着这条椭圆曲线的 3 阶点。不过，我们无法对域 K''_{18} 作出类似解释，但注意到它的伽罗瓦闭包与 K_{24} 的伽罗瓦闭包相同，而且还包含表 5.1 相应行中出现的另一个剩余域 $\mathbb{Q}(\sqrt{-14})$。

在特征 $\pi = 2$、3、7、11 下，我们分别得到 $283/256 \equiv \infty$、1、-1、-1；对于这些情形，我们已经找到了相应分歧的解释。

5.2.2 Thequartic surface

现在，我们继续对平面四次曲线族 Q 进行同样的分歧分析。

$t = 1$ 处的纤维

在 $t = 1$ 处，于特征 $\pi \notin \{2, 229\}$ 下，我们发现特殊纤维有三个分支，其中两个是有理曲线，而第三个的亏格为 2：

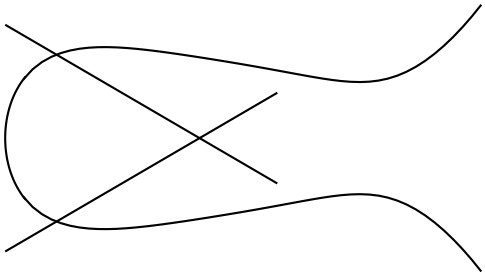


图 5.8：当 $\pi \notin \{2, 229\}$ 时，Q 在 $t = 1$ 处的特殊纤维。

在 $\mathbb{Q}$ 上，我们的平面曲线程序包告知我们，亏格为 2 的分支与方程为超椭圆曲线同构。

$$y^2 = x(x^4 - x + 1)$$

其 [LMFDB] 标签为 29312.a.58624.1；特别是，其雅可比簇的导子为 $29312 = 2^7 \cdot 229$。正如预期的那样，注 5.2 中描述的现象再次出现：表 5.2 中列出的数域 K_8 由不可约多项式 $x^8 - x^2 + 1$ 定义，因此显然是某个域的二次扩张，而在该域上，这条超椭圆曲线的雅可比簇获得一个 2 阶点。我们无法对同一行中出现的数域 K_8'、K_8''和 K_{12} 作出类似解释，但仍要指出，K_8、K_8'和 K_8''具有相同的伽罗瓦闭包，而该闭包是 K_{12}的伽罗瓦闭包的二次扩张。

由于 229 整除这条超椭圆曲线的判别式，当我们模 $\pi = 229$ 约化时，这条曲线退化为一条亏格为 1、带有节点自交的曲线：

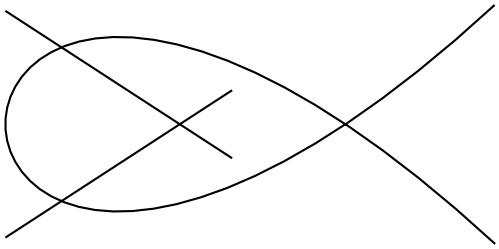


图 5.9：Q 模 229 在 $t = 1$ 处的特殊纤维。

这解释了我们在 $p = 229$ 处观察到的分歧。至于 $p = 2$ 处的分歧，这既是因为我们现在研究的是 2-扭点。

$t = 2$ 处的纤维

在特征为 $\pi \notin \{3, 5\}$ 时，我们得到一个由三个有理分支组成的特殊纤维，其中一个带有尖点，它们的排列如下：

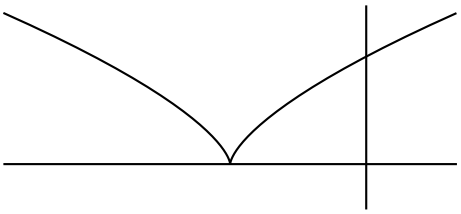


图 5.10：当 $\pi \notin \{3,5\}$ 时， Q 在 $t=2$ 处的特殊纤维。

模 $\pi = 5$ 化简并不需要进行更多次爆破；然而，最右侧的纤维是一条圆锥曲线，它退化为两条曲线的并，这解释了 $p=5$ 处的分歧：

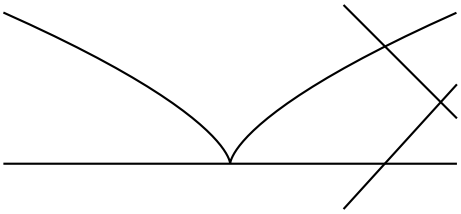


图 5.11： Q 模 5 在 $t=2$ 处的特殊纤维。

在模 $\pi = 3$ 下也会发生相同的退化，而且要解析 Q 在 $t=2$ 处的奇点，在特征 3 下还需要更多次吹胀。这两点都解释了 $p=3$ 处的分歧。

$t=\infty$ 处的纤维

模 $\pi \notin \{2,23\}$，我们的 Q 模型在 $t=\infty$ 处已经是正则的，因此特殊纤维由一个亏格为 1 且存在严重自交的分量构成：

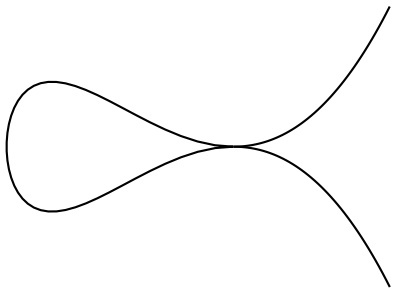


图 5.12：当 $\pi \notin \{2,23\}$ 时 Q 在 $t=\infty$ 处的特殊纤维。

在 $\mathbb{Q}$ 上，我们的平面曲线软件包告知我们，这条曲线的消奇化是椭圆曲线， [LMFDB] 标签为 92.a1，其导子为 $92 = 2^2 \cdot 23$；而表 5.2 中 K_3列出的域是判别式为 -23 的三次域，也是这条椭圆曲线获得一个 2 阶点的域。此外， K_6 是 K_3 的二次扩张，且只在 2 和 23 之上分歧。对于 K_8'''，我们没有类似的解释，不过我们注意到， K_8''' 的伽罗瓦闭包的次数为 48，它包含 K_6，因此也包含 K_3。

23 整除这条椭圆曲线的导子，也导致这条曲线在模 $\pi = 23$ 下出现一个额外的节点，这解释了 $p=23$ 处的分歧：

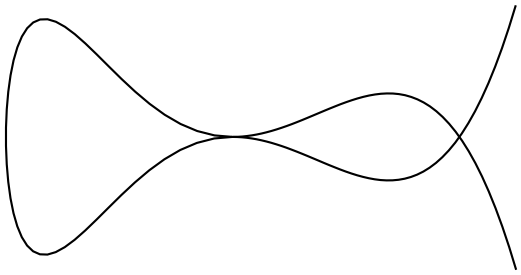


图 5.13： Q 在 $t = \infty$ 处模 23 的特殊纤维。

参考文献

[Coh00] Cohen,Henri, 《计算数论高级主题》。数学研究生教材，193。施普林格出版社，纽约，2000年。ISBN：0-387-98727-4。[DP13] Deconinck,Bernard；Patterson, MatthewS., 《平面代数曲线与黎曼曲面的计算：Maple 软件包“al-gcurves”的算法》。载于《黎曼曲面的计算方法》，2013年，第67–123页。[Duv89] Duval, Dominique, 《有理 Puiseux展开》。Compositio mathematica70，第2期（1989年），119–154。[GT94] van Geemen, Bert；Top, Jaap, 《GL_3 的一个非自对偶自守表示及一个伽罗瓦表示》。Invent. Math. 117（1994），第3期，391–401。[IM98] Harris, Joe；Morrison,Ian, 《曲线模空间》。数学研究生教材，187。施普林格出版社，纽约，1998年。ISBN：0-387-98438-0；0-387-98429-1。[KM04] Khuri-Makdisi, Kamal, 《代数曲线上除子的线性代数算法》。Math. Comp.73（2004），第245期，333–357。[KM07] Khuri-Makdisi, Kamal, 《一般曲线雅可比簇上的渐近快速群运算》。Mathematics ofComputation 76（2007），第260期，2213–2239。[LMFDB] LMFDB 协作组, 《L函数与模形式数据库》。http://www.lmfdb.org。[Magma] Bosma, Wieb；Cannon,John；Playoust, Catherine, 《Magma代数系统。I.用户语言 J》。Symbolic Comput.，24（1997），235–265。[Mas] Mascot, Nicolas, 《个人网页》。https://www.maths.tcd.ie/~mascotn/。[Mas19] Mascot,Nicolas, 《在雅可比簇上进行扭点的 Hensel 提升及伽罗瓦表示》。Mathematicsof Computation，2020年，第89卷，第323期，1417–1455。[Mas22] Mascot,Nicolas, 《显式计算与 SL_3 上的特征形式相关的伽罗瓦表示，该表示来自曲面的 H^2 等》。Foundations ofComputational Mathematics，2022年，1–25。[MilEC] Milne, James S., 《Etale 上同调讲义》，2.21版。https://www.jmilne.org/math/。

[MO15] Madore，David A.；Orgogozo，Fabrice，《模 ℓ 的 étale 上同调的可计算性》。Algebra Number Theory 9 (2015)，第 7 期，1647–1739 页。[Pari/GP]PARI小组，PARI/GP 开发版 2.16.0，波尔多，2023 年。http://pari.math.u-bordeaux.fr/.[PlaFRIM]计算机科学与数学联邦研究平台，超级计算集群，https://www.plafrim.fr/.[PTvL15] Poonen，Bjorn；Testa，Damiano；van Luijk，Ronald，《计算 Néron-Severi 群和循环类群》。Compos. Math. 151 (2015)，第 4 期，713–734 页。[ST68] Serre，Jean-Pierre；Tate，John，《阿贝尔簇的良约化》。Annals of Mathematics (1968)，492–517 页。[SGA$4\frac{1}{2}$]Deligne，Pierre，《étale 上同调》。布瓦-马里代数几何研讨班 (SGA 4 $_{12}$)。数学讲义，569。施普林格出版社，柏林，1977 年。ISBN：3-540-08066-X；0-387-08066-X。[vH0] van Hoeij，Mark，《有理代数曲线参数化的计算》。1994 年国际符号与代数计算研讨会论文集，187–190 页。[vH2] van Hoeij，Mark，《计算超椭圆曲线 Weierstrass标准形的算法》。arXiv:0203130，2002 年。