arXiv:2602.07237v1 [cs.SC] 6 Feb 2026

LCM 正特征下线性微分算子的分解

Raphaël Pagès
raphael.pages@jku.at
代数研究所 约翰·开普勒
大学 奥地利林茨 4040

摘要

我们提出了一种算法，用于计算系数属于特征为 p、$\mathbb{F}_{p^n}(t)$ 的有理函数域的线性微分算子的最小公倍左倍数分解。我们证明，对于一个阶为 r、系数次数为 d 的算子 L，该算法可在关于 r、d 和 p 的多项式时间内完成。该算法分三个步骤进行。首先，我们证明，可以根据算子 L 的 p-曲率的 Frobenius标准形，轻松确定其因式分解的“类型”；该标准形可使用 [4] 高效计算。随后，利用作者 [18], 的学位论文中的结果，我们能够构造一个与 L 属于同一等价类的算子 L^*，并且已知该算子的最小公倍左倍数分解。最后，通过计算商模 $\mathbb{F}_q(t)\partial/\mathbb{F}_q(t)\partial L^*$ 与 $\mathbb{F}_q(t)\partial/\mathbb{F}_q(t)\partial L$ 之间的同构，我们便能找到 L 的相应最小公倍左倍数分解。

CCS 分类

• **计算方法** → **代数算法**。

关键词

线性微分算子、因式分解、最小公倍数分解、正特征、 p-曲率、Ore 代数

ACM 参考格式:
Raphaël Pagès. 正特征下线性微分算子的最小公倍数分解。发表于. ACM，纽约，美国纽约州，8页。https: //doi.org/10.1145/nnnnnnn.nnnnnnn

1 引言

自微分学发明以来，研究并求解微分方程一直是数学家关注的重要课题，并已获得诸多应用。尽管对微分方程的经典研究本质上涉及实变量或复变量的函数，但该理论存在一种代数对应理论，它在种类繁多的基域上都有意义，包括但不限于数域、p-进域以及正特征域。其应用包括椭圆曲线上的点计数 [17], 同源计算 [9, 16],, 以及更一般地，对许多算术簇（的上同调）的研究。本文关注形如 $L(y) = 0$ 的线性微分方程，其中 $L = f_r(t)\partial^r + f_{r-1}(t)\partial^{r-1} + \cdots + f_0(t)$, 且诸 $f_i(t)$ 为有限域 $\mathbb{F}_q$ 上的有理函数，其中 q 是特征 p 的幂。在此设定下，与 L 形式相同的微分算子可以彼此相乘，但所得的环结构是非交换的，因为乘法遵循法则 $\partial t = t\partial + 1$。在此背景下，因式分解问题不仅是一个有趣的算法挑战，而且也具有重要意义，因为 L 的一个右因子的解空间是 L 的解空间的一个子空间。遗憾的是，与多项式的交换情形不同，若算子 L 可以写成乘积 $L = L'R$，则左因子 L' 并不会自动给出关于 L之解的信息。因此，人们往往更有兴趣尝试将 L写成若干算子 $L_1, \ldots, L_k$的公左倍数，其中诸 L_i尽可能简单，并且使得 L 的解空间是诸 L_i的解空间的直和。这便是所谓 L 的最小公倍左倍数分解，其中 LCLM 表示最小公左倍数。

在特征零下，线性微分方程已得到相当深入的研究，并且已有高效算法可用于回答有关这些方程或其解的各种问题 [15]。关于系数属于$\mathbb{C}(t)$的算子的因式分解算法，已有若干算法被提出（例如 [6, 14, 20, 21, 26]）。这些算法通常依赖于单值群等工具，而这类工具在正特征下并没有明显的对应物。在特征 p下，针对因式分解算法的首项重要工作，是 Marius van der Put 发表的有限维微分模分类 [22]。定理 3.11 和推论 4.3 可视为该分类在微分算子情形下的计算版本。此后，正特征下的因式分解问题曾多次得到研究 [23], , 其中值得一提的是 Thomas Cluzeau [7] , 他提出了一种用于微分系统的因式分解算法，其依据的原理与定理 3.4 相同，但应用于特征环中其他随机选取的元素。遗憾的是，与特征零下不同，特征环元素的特征多项式的系数属于 $\mathbb{F}_q(t^p)$（而非 $\mathbb{F}_q$），在该域上大多数多项式都不分裂，这或许解释了该方法为何在实践中行不通。其他已提出的方法包括 [11] , 其依据是在特征环中寻找零因子。遗憾的是，后来 [13]指出，该算法依赖一些通常不满足的假设；对于定理 3.4 无法给出完整因式分解的算子，这些假设尤其不成立。据我们所知，目前最可靠的因式分解方法依赖于 van der Put 提出的一种方法，用于求解形如$\mathrm{d}^{p-1}/\mathrm{d}t^{p-1}\, f + f^p = a^p$ 的方程，

R. Pages 获奥地利 FWF 项目 10.55776/PAT8258123 资助。

允许免费制作本作品全部或部分内容的数字或纸质副本，用于个人或课堂用途，前提是不得为营利或商业利益制作或分发副本，且副本须附有本声明及首页的完整引文。对于本作品中由 ACM 以外的其他方拥有版权的组成部分，必须尊重其版权。注明出处后允许摘录。以其他方式复制、转载、发布到服务器或向列表重新分发，均须事先获得明确许可和/或支付费用。请通过 permissions@acm.org 申请许可。, © 2025 ACM。
https://doi.org/10.1145/nnnnnnn.nnnnnnn

其中未知变量为 f，且方程定义在 $\mathbb{F}_q(t)$的某个可分扩张中。该方法要求待分解算子不能具有$N(t^p,\partial^p)$的形式，其中 $N\in\mathbb{F}_q(X)[Y]$，并且通常得到的解的规模与 p呈线性关系。在其学位论文 [18],中，本文作者开发了一种算法，无需依赖此类假设，即可求得该方程的解，且解的规模与 p无关。我们在此基础上提出一种新方法，在满足充分可分性假设的条件下计算算子的最小公倍左倍数分解。

在第 2 节重新确立微分算子和最小公倍左倍的一些基本性质后，我们将在第 3 节展示如何利用算子的 p-曲率，完全确定 L 的最小公倍左倍分解的形式及其等价类。第 4 节将展示如何利用 [18] 的结果，构造一个“较小”的算子，其分解已知，且与 L属于同一等价类。最后，我们将在第 5 节介绍最小公倍左倍分解算法。由于需要计算两个循环微分模之间的一组微分同态，目前算法输出规模的上界关于 p 是二次的。实验表明，无需修改算法本身，就可能将该上界降至关于 p 的准线性。

2 预备知识

本节回顾微分算子的基本概念，以及最小公倍数（更准确地说，最小公倍左倍）分解。设 p 为素数，且 $q=p^n$。我们考虑系数属于有理函数域 $\mathbb{F}_q(t)$的线性微分算子，其中 $\mathbb{F}_q$ 是含有 q 个元素的有限域。 $\mathbb{F}_q(t)$上的线性微分算子环记为 $\mathbb{F}_q(t)\partial$，其元素是 ∂ 中的多项式，形式如下：

$$f_r\partial^r+f_{r-1}\partial^{r-1}+\cdots+f_1\partial+f_0$$

其中 $f_i\in\mathbb{F}_q(t)$。该环中的（非交换）乘法由莱布尼茨法则 $\partial f=f\partial+_{\mathrm{d}\,dt}f$导出，对所有 $f\in\mathbb{F}_q(t)$ 均成立。对于任意算子 $L=f_r\partial^r+\cdots+f_0\in\mathbb{F}_q(t)\partial\backslash\{0\}$， L 的阶（记作 $\mathrm{ord}(L)$）是使得 $f_i\neq 0$ 成立的最大 $i\in\mathbb{N}$。我们回顾一下，阶赋予 $\mathbb{F}_q(t)\partial$右（和左）欧几里得除法结构，从而使 $\mathbb{F}_q(t)\partial$ 成为主左（和右）理想整环。两个算子 L_1 和 L_2 生成 $\mathbb{F}_q(t)\partial$ 的同一个左理想，当且仅当存在 $u\in\mathbb{F}_q(t)^\times$ 使得 $L_1=uL_2$。此外，这使我们能够定义最小公左倍数（LCLM）和最大公右因子（GCRD）的概念。

Definition 2.1. *Let $L_1,L_2,L\in\mathbb{F}_q(t)\langle\partial\rangle$. We say that:*

i) $L=\mathrm{LCLM}(L_1,L_2)$ *if and only if* $\mathbb{F}_q(t)\langle\partial\rangle L=\mathbb{F}_q(t)\langle\partial\rangle L_1\cap\mathbb{F}_q(t)\langle\partial\rangle L_2$.

ii) $L=\mathrm{GCRD}(L_1,L_2)$ *if and only if* $\mathbb{F}_q(t)\langle\partial\rangle L=\mathbb{F}_q(t)\langle\partial\rangle L_1+\mathbb{F}_q(t)\langle\partial\rangle L_2$.

记号 2.2。 令 $L\in\mathbb{F}_q(t)\langle\partial\rangle$。我们将左商模 $\mathbb{F}_q(t)\langle\partial\rangle/\mathbb{F}_q(t)\langle\partial\rangle L$记作 $\mathcal{D}_L$。在某些情况下，我们可能希望将系数域扩张到 $\mathbb{F}_q(t)$的某个可分扩张 K。在不致引起记号混淆时，我们仍将 $K\langle\partial\rangle/K\langle\partial\rangle L$记作 $\mathcal{D}_L$。

我们不加证明地陈述以下结果，它更详细地描述了最小公倍左倍数与最大公右因子之间的关系。

命题 2.3. 以下左 $\mathbb{F}_q(t)\langle\partial\rangle$-模序列是正合的：

$$\begin{array}{ccccccc}0&\to&\mathcal{D}_{\mathrm{LCLM}(L_1,L_2)}&\to&\mathcal{D}_{L_1}\oplus\mathcal{D}_{L_2}&\to&\mathcal{D}_{\mathrm{GCRD}(L_1,L_2)}\to 0\\&&&&(M,N)&\mapsto&M-N\end{array}.$$

特别地：

i) $\mathrm{ord}(\mathrm{LCLM}(L_1,L_2))+\mathrm{ord}(\mathrm{GCRD}(L_1,L_2))=\mathrm{ord}\,L_1+\mathrm{ord}\,L_2$。 *ii)* 若 $\mathrm{GCRD}(L_1,L_2)=1$ 则 $\mathrm{D}_{\mathrm{LCLM}(L_1,L_2)}\simeq\mathrm{D}_{L_1}\oplus\mathrm{D}_{L_2}$。

定义 2.4。 我们称 $L\in\mathbb{F}_q(t)\langle\partial\rangle$ 可分解，当且仅当存在 L_1，$L_2\in\mathbb{F}_q(t)\langle\partial\rangle\backslash\mathbb{F}_q(t)$ 互素的元素（即 最大公右因子$(L_1,L_2)=1$），且 $L=$<*style id='*最小公倍左倍数(L_1,L_2)。这等价于说，$\mathcal{D}_L$ 可分解为左 $\mathbb{F}_q(t)\langle\partial\rangle$-模（即可以写成非平凡子模的直和）。*W*

e say t hat L is in decomposable if it is not decomposable.

备注 2.5. 不可约算子是不可分解的，但反之并不成立。例如，算子 $\partial x\partial=x\partial^2+\partial$ 是不可分解的，但不是不可约的。

定义 2.6. 设 $L\in\mathbb{F}_q(t)\langle\partial\rangle$ 以及 $(L_1,\ldots,L_k)\in\mathbb{F}_q(t)\langle\partial\rangle^k$，其中 $k\in\mathbb{N}$。我们称 $(L_1,\ldots,L_k)$是 L 的最小公倍左倍数分解，当且仅当每个 L_i 都是不可分解的， $L=$最小公倍左倍数$_{i=1}^k L_i$，且 阶$L=\sum_{i=1}^k$阶L_i。

本文的目标是提出一种算法：给定某个 $L\in\mathbb{F}_q(t)\partial$，求出它的最小公倍左倍数分解。

命题 2.7. 设 $L\in\mathbb{F}_q(t)\langle\partial\rangle$ 以及 $L_1,\ldots,L_k$ 是 L 的右因子。$L=$最小公倍左倍数$_{i=1}^k L_i$，且 阶$L=\sum_{i=1}^k$阶L_i，当且仅当典范同态 $\mathcal{D}_L\to\bigoplus_{i=1}^k\mathcal{D}_{L_i}$ 是同构。

证明。我们先假设 $\mathrm{D}_L\to\bigoplus_{i=1}^k\mathrm{D}_{L_i}$ 是一个同构。根据 $L':=\mathrm{LCLM}_{i=1}^k L_i$ 的定义，它是 L 的一个右因子，并且这个典范态射可分解为 $\mathrm{D}_L\twoheadrightarrow\mathrm{D}_{L'}\to\bigoplus_{i=1}^k\mathrm{D}_{L_i}$。因此，只有当两个箭头都是同构时，它才可能是同构，也就是说，当 $L=L'$ 时。通过维数分析，我们得到阶相等。现在假设 $L=\mathrm{LCLM}_{i=1}^k L_i$ 且 $\mathrm{ord}\,L=\sum_{i=1}^k\mathrm{ord}\,L_i$。根据命题 2.3, $k=2$ $k\geq$., 我们知道该结论对 成立。若 , 则可令 $L'=\mathrm{LCLM}_{i=1}^{k-1}L_i$ 。于是有 $L=\mathrm{LCLM}(L',L_k)$。根据命题 2.3(ii)，我们知道 $\mathrm{ord}\,L'\leq\sum_{i=1}^{k-1}\mathrm{ord}\,L_i$ 且 $\mathrm{ord}\,L\leq\mathrm{ord}\,L'+\mathrm{ord}\,L_k\leq\sum_{i=1}^{k}\mathrm{ord}\,L_i$。但由假设可知，这些实际上必须都是等式，因此 $\mathrm{ord}\,L'=\sum_{i=1}^{k-1}\mathrm{ord}\,L_i$。通过归纳，我们推得 $\mathrm{D}_{L'}\simeq\bigoplus_{i=1}^{k-1}\mathrm{D}_{L_i}$ 且 $\mathrm{D}_L\simeq\mathrm{D}_{L'}\oplus\mathrm{D}_{L_k}\simeq\bigoplus_{i=1}^{k}\mathrm{D}_{L_i}$。

■

3 p-曲率

本节回顾 [22]和 [7]中使用的一些结果，这些结果可根据给定算子的 p-曲率，尤其是其 p-曲率的特征多项式，求得该算子的初步分解。 [3]提出了一种高效算法，可在关于算子阶数及其系数次数的多项式时间内，并在 $\sqrt{p}$ 上以准线性时间计算给定算子的p-曲率的特征多项式。随后，我们在定理 3.11 中证明，算子的最小公倍左倍数分解的形式，完全可以从其p-曲率的 Frobenius（或有理）标准形推导出来（关于线性自同态的 Frobenius 标准形，可参见例如 [2, 第 21.4] 节）。为计算该标准形，我们使用 [4]，其复杂度与之相近。

定义 3.1。 *[24,p。329]*令 $L \in \mathbb{F}_q(t)\langle\partial\rangle$。$L$的 p-曲率是由乘以 ∂^p定义的(t)-线性端同态，作用于$\mathcal{D}_L$。我们将此端同态记为 ψ_p^L。

众所周知，对于任意 $L \in \mathbb{F}_q(t)\partial$，存在一个 D_L 的 $\mathbb{F}_q(t)$-基，使得 ψ_p^L 的矩阵系数属于 $\mathbb{F}_q(t^p)$ [8, 命题 2.1.2]。特别地，它的特征多项式和 Frobenius标准形的系数属于 $\mathbb{F}_q(t^p)$。在陈述第一个分解定理之前，我们需要了解关于 p-曲率的特征多项式的另外两个关键信息。

定义 3.2. 如果算子 $L \in \mathbb{F}_q(t)\langle\partial\rangle$ 与 $\mathbb{F}_q(t)\langle\partial\rangle$ 的所有元素在乘法下均可交换，则称其为中心的。等价地， $L \in \mathbb{F}_q(t^p)[\partial^p]$ *[22,*引理 *1.1]*。

引理3.3. *[3,* 引理 *3.9]* 将 $L \in \mathbb{F}_q(t)\langle\partial\rangle$ 映射为其 $\chi \in \mathbb{F}_q\ t^p\ [Y]$ L -曲率的特征多项式 $(\psi_p^L)()$的映射是可乘的。此外，若它是中心的且首一，则 $\chi(\psi_p^L)(\partial^p) = L^p$。

定理 3.4。 令 $L \in \mathbb{F}_q(t)\langle\partial\rangle$。令 N_1、……、 $N_n \in \mathbb{F}_q(t^p)[X]$ 为两两不同的不可约首一多项式，并令 ν_1、……、 $\nu_n \in \mathbb{N}$ 满足 $\chi(\psi_p^L) = N_1^{\nu_1} \dots N_n^{\nu_n}$。对所有 $i \in \{1$、……、 $n\}$，置 L_i：=最大公右因子$(L,\ N_i^{\nu_i}(\partial^p))$。则：

i) L =最小公倍左倍数$_{i=1}^n L_i$。*ii)* 阶 $L = \sum_{i=1}^n$阶 L_i。*iii)* 对所有 $i \in \{1$、……、 $n\}$， $\chi(\psi_p^{L_i}) = N_i^{\nu_i}$。

证明。根据核分解引理，我们可以写成 D_L =核 $N_1^{\nu_1}(\psi_p^L)$ ⊕ · · · ⊕核 $N_n^{\nu_n}(\psi_p^L)$。令 $i \in \{1, \dots, n\}$。 V_i:=核 $N_i^{\nu_i}(\psi_p^L)$ 同构于 D_L 的一个商模，因此同构于某个 $\mathrm{D}^{L_i'}$（作为一个 $\mathbb{F}_q(t)\partial$-模），其中 L_i' 是 L 的一个右因子。此外，由于 $\psi_{p|V_i}^L = \psi_p^{L_i'}$通过此同构，并根据 V_i 的定义， $N_i^{\nu_i}(\psi_p^{L_i'})(1) = 0 = N_i^{\nu_i}(\partial^p) \bmod L_i'$，由此可知 L_i' 也是 $N_i^{\nu_i}(\partial^p)$ 的一个因子，因而是 L_i 的一个因子。最后我们知道 $\chi(\psi_p^{L_i'}) = \chi(\psi_{p|V_i}^L) = N_i^{\nu_i}$。设 $L_i = Q_i L_i'$ 为某个 $Q_i \in \mathbb{F}_q(t)\partial$。由于根据定义$L_i$是 L 的一个因子，根据引理 3.3， $\chi(\psi_p^{L_i})|\chi(\psi_p^L)$。此外，$\chi(\psi_p^{L_i}) = \chi(\psi_p^{Q_i})\chi(\psi_p^{L_i'}) = \chi(\psi_p^{Q_i})$ $N_i^{\nu_i}$。但由于 Q_i 是 L_i 的一个因子，它必定是 $N_i^{\nu_i}(\partial^p)$ 的一个因子。再次利用乘法性，并且由于 $\chi(\psi^{N_i^{\nu_i}(\partial^p)p}) = N_i^{p\nu_i}$，可知 $\chi(\psi_p^{Q_i})$ 必须是 N_i 的幂。如果 $Q_i \notin \mathbb{F}_q(t)$，这意味着该幂非零，并且 $\chi(\psi_p^L)$ 必须被 N_i 的更高次幂整除，这是不可能的。因此可以假设 $L_i' = L_i$。结论现在由命题 2.7 得出

∎

从现在起，我们所考虑的所有算子都将满足以下假设，即使未明确说明：

假设 3.5. 令 $L \in \mathbb{F}_q(t)\langle\partial\rangle$。我们假设 $\chi(\psi_p^L)$在 $\mathbb{F}_q(t^p)$上没有不可分不可约因子。

由定理 3.4 可知，现在可以假设我们研究的算子 L 是某个 $N(\partial^p)^\nu$ 的因子，其中 $N \in \mathbb{F}_q(t^p)[Y]$ 不可约，且 $\nu \in \mathbb{N}$。在 $\nu = 1$ 的情形下，这使得 D_L 成为左 $\mathrm{D}_{N(\partial^p)}$-模。我们可以证明，$\mathrm{D}_{N(\partial^p)}$ 是一个中心单代数 $C_N := \mathbb{F}_q(t^p)[Y]/N(Y)$-代数，其维数为 p^2 [22, 引理 1.2]。由韦德伯恩定理 [12,定理 2.1.3] 可推得，$\mathrm{D}_{N(\partial^p)}$ 要么是除法代数，要么同构于 $M_p(C_N)$。在第一种情形下，可知 $N(\partial^p)$ 不可约，因为任何非平凡因子都会是 $\mathrm{D}_{N(\partial^p)}$ 中的零因子。在后一种情形下，我们知道所有简单的 $M_p(C_N)$-模都同构于C_N^p，由此可知， $N(\partial^p)$ 的因子不可约，当且仅当它们的阶为 $\deg(N)$。

这种二分法在寻找 L 的不可约右因子时对我们很有帮助；正如我们接下来要展示的，它现在仍然十分有用。

从现在起直到第 6 页，我们假设 L、 N和 ν固定。我们还假设 N在 $\mathbb{F}_q(t^p)$ 上可分，也就是说， L 满足假设 3.5。

记号 3.6. 我们按前文所述，将 $C_N \simeq \mathbb{F}_q(t^p)[Y]/N(Y)$记为……。此外，我们将 Y 在 C_N 中的像记为 y_N，于是 $N(y_N) = 0$。我们将 $K_N = \mathbb{F}_q(t)[y_N]$ 记为……。这是 $\mathbb{F}_q(t)$的一个微分扩张，因为 N在 $\mathbb{F}_q(t^p)$上可分。

注 3.7. 请注意， K_N 与 C_N 并不相同，因为它是由 N的根生成的 $\mathbb{F}_q(t)$的扩张，而不是 $\mathbb{F}_q(t^p)$。

从计算角度来看，用多项式 N_*在 $\mathbb{F}_q(t)$上表示 N在计算上更为合适，其中$N_*^p(Y) = N(Y^p)$，N的系数属于 $\mathbb{F}_q(t^p)$。采用这些记号， $N_*(y_N^{1/p}) = 0$，并且我们使用表示 $K_N = \mathbb{F}_q(t)[y_N^{1/p}] \simeq \mathbb{F}_q(t)[Y]/N_*(Y)$。

引理 3.8. 设 $F \in K_N[\partial^p]$。则$(\partial - F)^p = \partial^p - F_{(p-1)} - F^p$ 其中，对 F的导数是逐系数作用的。

证明。我们将 [22, 引理 1.4.2(1)] 应用于系数属于 $K_N[T]$ 且配备了 K_N的导子的逐系数扩张的算子。于是，对于任意 $F \in K_N[T]\partial$，$(\partial - F)^p = \partial^p - \tau(F) = \partial^p - F_{(p-1)} - F^p$，这里使用了 [22,引理 1.4.2]的记号。然后我们在 $T = \partial^p$中计算该等式。∎

Theorem 3.9. $\mathcal{D}_{N(\partial^p)^\nu} \simeq \mathcal{D}_{N(\partial^p)}[T]/T^\nu$.

证明。注意，典范单射 $\mathbb{F}_q(t)\partial \hookrightarrow K_N\partial$ 诱导出一个环同构 $\mathrm{D}_N(\partial^p)^\nu \xrightarrow{\sim} K_N\partial/(\partial^p - y_N)^\nu$.。将算子写成 $\mathbb{F}_q(t)\partial$ 中的$\mathbb{F}_q(t^p)[\partial^p]$基 $(x^i\partial^j)_{0\le i,j<p}$，并利用 N 是 y_N 在 $\mathbb{F}_q(t^p)$ 上的最小多项式这一事实，即可看出其单射性。满射性则由维数分析得出。因此，扩张基域后，不失一般性地假设 $N = Y - y_N$。我们构造一个环同态，从 $\mathrm{D}_N(\partial^p)$ 映到 $\mathrm{D}_{N(\partial^p)^\nu}$，并将 K_N 映到自身。这样的态射由 ∂ 的像唯一确定；该像是 $A \in K_N\partial$ 中满足 $A^p - y_N \equiv 0 \bmod N(\partial^p)^\nu$ 的一个元素。我们寻求形如 $\partial + x^{p-1}F$ 的 A，其中 $F \in C_N[\partial^p]$。假设我们已找到满足 $(\partial + x^{p-1}F_0)^p - y_N \equiv 0 \bmod N(\partial^p)^m$ 的 $F_0 \in K_N[\partial^p]$，其中某个 $m \ge 1$。那么存在 $P \in C_N[\partial^p]$ 使得 $(\partial + x^{p-1}F_0)^p - y_N = PN(\partial^p)^m$。令 $F_1 = F_0 + PN(\partial^p)^m$。于是

$$\begin{aligned}(\partial + x^{p-1}F_1)^p - y_N &= \partial^p - F_1 + x^{p(p-1)}F_1 - y_N\\ &= \partial^p - F_0 - PN(\partial^p)^m + x^{p(p-1)}F_0\\ &\quad + x^{p(p-1)}P^pN(\partial^p)^{pm} - y_N\\ &\equiv (\partial + x^{p-1}F_0)^p - y_N - PN(\partial^p)^m \mod N(\partial^p)^{m+1}\\ &\equiv 0 \mod N(\partial^p)^{m+1}\end{aligned}$$

从 $F_0 = 0$ 和 $m = 1$ 出发，我们可以构造 F，使得 $N(\partial + x^{p-1}F)^p) \equiv 0 \bmod N(\partial)^\nu$，从而得到一个非零态射 $\mu\colon \mathrm{D}_N(\partial^p) \to \mathrm{D}_N(\partial^p)^\nu$。由于 $\mathrm{D}_N(\partial^p)$ 是一个中心单 C_N-代数，它没有非平凡双边理想，因此该态射是单射。我们将 T 映到 $N(\partial^p)$，得到态射 $\mathrm{D}_N(\partial^p)\ [T]/T^\nu \to \mathrm{D}_N(\partial^p)^\nu$。这个态射也是单射。事实上，若 $A = \sum_{k=0}^{\nu-1} A_k T^k$ 满足 $A_K \in$，其中 $\mathrm{D}_N(\partial^p)$，且其像为零，则 $\sum_{k=0}^{\nu-1} \mu(A_k) N(\partial^p)^k \equiv 0 \bmod N(\partial^p)^\nu$。如果 A_k 并非全为零，这意味着存在最小的 k，使得 A_k 不为零。但这样一来，$\mu(A_k)$ 就必须能被 $N(\partial^p)$ 整除。这不可能，因为 $\mu^{-1}(\mathrm{D}_N(\partial^p)_m N(\partial^p))$ 是 $\mathrm{D}_N(\partial^p)$ 的双边理想，且不包含 1，因此只能是零理想。于是，对所有 k 都有 $A_k = 0$，从而得到一个单射环同态。最后，由 C_N 上维数相等即可得出结论。 ∎

在陈述本节最后将要给出的结构定理（稍后我们将用它来计算等价类 L的受控代表元）之前，我们必须先陈述一个不加证明的范畴等价结果；这是环之间 Morita 等价的一个经典例子。我们在基环为交换环这一较受限的情形下给出该结果，尽管这并非实际所需的条件，这样便不会对张量积的含义产生歧义。关于环的 Morita 等价，更多信息例如可见 [1, 第 6]章。

定理 3.10（莫里塔）。设 R 是一个交换环，且 $n \in \mathbb{N}$。协变函子

$$\begin{aligned} \mathcal{M}\mathrm{or}: \quad \mathrm{Mod}_R &\to \mathrm{Mod}_{M_n(R)} \\ M &\mapsto R^n \otimes_R M \end{aligned} .$$

是一个保直和的范畴等价。

定理 3.11。设 $L \in \mathbb{F}_q(t)\langle\partial\rangle$ 是某个$N(\partial^p)^\nu$的首一因子，其中 $N \in \mathbb{F}_q(t^p)[Y]$ 是一个首一不可约多项式，在 $\mathbb{F}_q(t^p)$上可分，且 $\nu \in \mathbb{N}$。

- 若 $N(\partial^p)$ 在 $\mathbb{F}_q(t)\langle\partial\rangle$ 中不可约，则 $L = N(\partial^p)^m$ 其中 $m \le \nu$，且不可分解。
- 否则，令 $N^{\nu_1}|N^{\nu_2}|\dots|N^{\nu_k}$ 为 ψ_p^L 的 *Frobenius* 不变量。那么存在 $L_1, \dots, L_k \in \mathbb{F}_q(t)\langle\partial\rangle$，使得 *i)* $L = LCLM_{i=1}^k L_i$ 且 *ord* $L = \sum_{i=1}^k$ *ord* L_i。 *ii)* 对所有 $i \in \{1, \dots, k\}$，*ord* $L_i = \nu_i$*deg* N。 *iii)* 每个 L_i 都不可分解

证明。先假设 $N(\partial^p)$ 不可约。我们可以将 L除以 $N(\partial^p)$ 的最高次幂（该幂整除 L），因此不妨假设 L N ∂^p $L \in$ 与 ( ) 互素，$\mathbb{F}_q$ t N ∂^p N ψ_p^L 并证明 ( )。于是，乘以 ( )（即 ( )）会在 D_L 上诱导一个自同构。然而，由于 $N(\partial^p)^\nu$是L的倍数，$N(\psi_p^L)$ 是幂零的；这只有在 $\mathrm{D}_L = \{0\}$ 时才可能，也就是说 $L \in \mathbb{F}_q(t)$。由于 L 的任意两个非平凡右因子也必然是 $N(\partial^p)$ 的幂，它们的最大公右因子永远不会是 1，这就证明了 L 不可分解。

现在我们假设 $N(\partial^p)$ 是可约的，也就是说，$\mathrm{D}_{N(\partial^p)} \simeq M_p(C_N)$。因此，根据定理 3.9，$\mathrm{D}_{N(\partial^p)^\nu} \simeq \mathrm{D}_{N(\partial^p)}\ [T]/T^\nu \simeq M_p(C_N[T]/T^\nu)$。由于 D_L 是左 $\mathrm{D}_{N(\partial^p)^\nu}$-模，通过莫里塔等价，它对应于一个有限维（在 C_N 上的） $C_N[T]/T^\nu$-模，也就是说，一个有限维 C_N-向量空间 V，配备一个幂零端同态。因此，存在 $k' \in \mathbb{N}$ 和 $m_1 \le \cdots \le m_{k'}$，使得$V \simeq C_N[T]/T^{m_1} \oplus \cdots \oplus C_N[T]/T^{m'_k}$，并且根据定理 3.10，$\mathrm{D}_L \simeq R^p \otimes_R C_N[T]/T^{m_1} \oplus \cdots \oplus R^p \otimes_R C_N[T]/T^{m'_k}$作为一个 $M_p(R)$-模，其中 $R = C_N[T]/T^\nu$。我们将 M_i设为该分解中对应于 $R^p \otimes_R C_N[T]/T^{m_i}$ 的 D_L 子模。它典范地同构于某个 D_{L_i}，其中 L_i 是 L 的右因子。由命题 2.7 可得$L = \mathrm{LCLM}_{i=1}^{k'} L_i$，且 ord $L = \sum_{i=1}^{k'}$ ord L_i。由于定理 3.10 中的函子 Mor 保持直和，且 $C_N[T]/T^{m_i}$ 是一个不可分解的 $C_N[T]$-模，因此 L_i 是不可分解的。此外，映射 $N(\psi^L_{p|M_i})$ 对应于 $R^p \otimes_R C_N[T]/T^{m_i}$ 上乘以 T，故 $\psi^L_{p|M_i}$ 的最小多项式为 N^{m_i}。由于

$$\begin{aligned} \dim_{\mathbb{F}_q(t)} M_i &= p^{-1} \dim_{\mathbb{F}_q(t^p)} M_i \\ &= p^{-1} \deg(N) \dim_{C_N} R^p \otimes_R C_N[T]/T^{m_i} \\ &= \deg(N) p^{-1} p m_i = m_i \deg(N), \end{aligned}$$

由此可知 $\psi^L_{p|M_i}$ 是循环的。因此 $N^{m_1}|\dots|N^{m_{k'}}$ 符合 ψ_p^L 的 Frobenius 不变量的判定条件，并且由唯一性可得，对所有 i，均有 $k' = k$ 和 $m_i = \nu_i$。 ∎

4 等价类与代表元

定理 3.11 使我们能够准确地知道，给定 $L \in \mathbb{F}_q(t)\partial$，其某个最小公倍左倍数分解应当是什么样子，也就是说，我们准确地知道其系数的次数。众所周知，同一算子的两个最小公倍左倍数分解必定具有次数相同的因子。在正特征下，这实际上可以看作定理 3.11 的一个推论，因为 L 的一个最小公倍左倍数分解也给出了 ψ_p^L 的 Frobenius标准形。事实上，正如我们下面将要证明的，ψ_p^L 的等价类完全决定了 D_L 作为 $\mathbb{F}_q(t)\partial$-模的同构类。

定义 4.1。设 $L_1, L_2 \in \mathbb{F}_q(t)\langle\partial\rangle$。称 L_1 与 L_2 等价，当且仅当 $\mathcal{D}^{L_1}$ 与 $\mathcal{D}^{L_2}$ 作为 $\mathbb{F}_q(t)\langle\partial\rangle$-模同构。

引理 4.2。如果 L_1 和 L_2 是满足假设 *3.5* 的 $\mathbb{F}_q(t)\langle\partial\rangle$ 中的两个不可分解算子，那么当且仅当 $\chi(\psi_p^{L_1}) = \chi(\psi_p^{L_2})$时，它们等价。

证明。$\mathrm{D}_{L_1} \simeq \mathrm{D}_{L_2}$推出 $\chi(\psi_p^{L_1}) = \chi(\psi_p^{L_2})$这一事实是显然的。反过来，假设 $\chi(\psi_p^{L_1}) = \chi(\psi_p^{L_2})$。这尤其意味着 $\mathrm{ord}(L_1) = \mathrm{ord}(L_2)$。由于 L_1和 L_2不可分解，根据定理 3.4，$\chi(\psi_p^{L^*})$具有N^ν的形式，其中 N是 $\mathbb{F}_q(t^p)$上的不可约多项式。于是，若$N(\partial^p)$不可约，根据定理 3.11，我们知道必有 $L_i = N(\partial^p)^{m_i}$，其中 m_i以及 $i \in \{1, 2\}$。由次数相等可得 $m_1 = m_2$和 $L_1 = L_2$。如果此时 $N(\partial^p)$可约，则根据定理 3.9，$\mathrm{D}_N(\partial^p) \simeq M_p(C_N)$且$\mathrm{D}_N(\partial^p)^\nu \simeq M_p(C_N[T]/T^\nu)$。因此，$\mathrm{D}_{L_1}$和$\mathrm{D}_{L_2}$通过莫里塔等价对应于两个不可分解的（见定理 3.10，莫里塔等价保持直和） $C_N[T]/T^\nu$-模，分别为 $C_N[T]/T^{\nu_1}$和 $C_N[T]/T^{\nu_2}$。由此可得，对 $i \in \{1, 2\}$，$\mathrm{D}_{L_i} \simeq R^p \otimes_R C_N[T]/T^{\nu_i}$，且 $R = C_N[T]/T^\nu$。由阶相等，进而维数相等，必有 $\nu_1 = \nu_2$。 ∎

推论 4.3。 两个算子 $L_1, L_2 \in \mathbb{F}_q(t)\langle\partial\rangle$ （不一定是 $N(\partial^p)^\nu$的因子）满足假设 *3.5*，当且仅当$\psi_p^{L_1}$和$\psi_p^{L_2}$作为 $\mathbb{F}_q(t)$-线性映射等价时，它们等价。

证明。显然，若 D_{L_1} 和 D_{L_2} 作为$\mathbb{F}_q(t)\partial$-模同构，则 $\psi_p^{L_1}$ 和 $\psi_p^{L_2}$ 等价。反过来，现在假设 $\psi_p^{L_1}$ 和 $\psi_p^{L_2}$ 等价。特别地，它们具有相同的特征多项式，且 L_1 和 L_2 的阶相同。我们可以应用定理 3.4，将问题化归为 L_1 和 L_2 都是 $N(\partial^p)^\nu$ 的因子的情形。于是根据定理 3.11，要么 L_1 和 L_2 都等于 $N(\partial^p)$ 的同一个幂（因为它们的阶相同），要么它们的最小公倍左倍数分解中各因子的阶由其 p-曲率的 Frobenius 不变量给出。由于 $\psi_p^{L_1}$ 和 $\psi_p^{L_2}$ 等价，这些不变量相同，因此存在

$k \in \mathbb{N}$ $L_{i\,j} \in$ 和，$\mathbb{F}_q\ t\ \partial$ $i\ j\ \in\ 1,2\ \times\ 1\ \ldots\ k$ ( ) 中不可分解的元素，使得对于 (,) { } { , , }，$\mathrm{D}_{L_i} = \mathrm{D}_{L_{i,1}} \oplus \cdots \oplus \mathrm{D}_{L_{i,k}}$，此外，对所有 j，$\operatorname{ord} L_{1,j} = \operatorname{ord} L_{2,j}$。根据引理 4.2，对所有 j，$\mathrm{D}_{L_{1,j}} \simeq \mathrm{D}_{L_{2,j}}$，因此 $\mathrm{D}_{L_1} \simeq \mathrm{D}_{L_2}$。

■

既然我们现在已经知道如何根据其 p-曲率的 Frobenius 标准形计算 D_L 的同构类（对于这一计算，已有高效算法，例如参见 [4]），我们的目标便是展示如何计算任意选定的同构类的代表元，其中已知一个最小公倍左倍数分解。由于一旦确定 $N(\partial^p)$ 是否可约，不可约情形便是平凡的，因此在本节余下部分中，我们假设 $N(\partial^p)$ 是可约的。注意，在其学位论文中，本文作者提出了一种多项式时间方法，用于确定 $N(\partial^p)$ 是否可约（参见 [18, 第 3.3 节3] 或 [19, 定理 3.9]）。

引理 4.4。 令 $n \in \mathbb{N}$。算子 $(x\partial)^n$ 在 $K\langle\partial\rangle$ 中是不可分解的，其中 K 是 $\mathbb{F}_q$ 的任意可分扩张(t)。

证明。根据 $L \mapsto \chi(\psi_p^L)$的乘法性（见引理3.3），并且由于 $\chi(\psi_p^\partial)(Y) = Y$，可知 $\chi(\psi_{(x\partial^n)})(Y) = Y^n$，因此$\psi_p^{(x\partial)^n}$是幂零的。根据定理 3.11，只需证明 $\chi_{min}(\psi_{(x\partial^n)}) = Y^p$，也就是说，$\psi_{(x\partial^n)}$是最大秩幂零的。这等价于说 $\ker \psi_p^{(x\partial)^n} = 1$。此外，根据 [24, 引理13.2],，我们知道 $\dim_K \ker \psi_{(x\partial^n)}$ di $\mathrm{m}_C\{f \in K | (x\partial)^n(f) = 0\}$，其中 C是 K的常数域。由于 K是 $\mathbb{F}_q(t)$的可分扩张，C是 K中所有 p次幂的集合，并且 $1, x, \ldots, x^{p-1}$是 K的 C-基。因此，若$f \in K = \sum_{i=0}^{p-1} f_i x^i$，其中 $f_i \in C$，则有 $(x\partial)^n(\sum_{i=0}^{p-1} f_i x^i) = \sum_{i=1}^{p-1} i^n f_i x^i$，而这只有在对所有 $i > 0$ 都有 $f_i = 0$ 时才可能为零，也就是说 $f \in C$。

■

在其学位论文 [18, 3 4], $N \in \mathbb{F}_q\ t^p\ [Y]$ $f_N \in K_N$ $\partial - f_N$ 节中，作者说明了，给定 ( )，如何计算一个“小的”对象，使得 ( ) 是 $\partial^p - y_N$的因子，当 $N(\partial^p)$ 可约时。由于我们假定情况如此，我们为命题 4.5 固定这样一个 f_N。

命题 4.5. 设 $(m_1, \ldots, m_p) \in (\mathbb{N} \cup \{0\})^p$。对每个 $i \in \{1, \ldots, p\}$ 设 $L_i \in \mathbb{F}(t)\langle\partial\rangle$ 是 $(x\partial - x f_N + i)^{m_i}$的一个左倍，其阶为 $m_i \deg(N)$。设 $L =$最小公倍左倍数$_{i=1}^p L_i$。则

i) L_i 不可分解。

ii) $\chi(\psi_p^{L_i}) = N^{m_i}$。*iii)* $\operatorname{ord} L = \sum_{i=1}^p \operatorname{ord} L_i$。也就是说，$L_i$ 给出了 L 的一个最小公倍左倍数分解。

证明。我们断言，$L_i' := (x\partial - x f_N + i)^{m_i}$ 作为 $(x\partial)^{m_i}$ 在 $K_N\partial$ 上的环自同构的像是不可分解的；该环自同构在 K_N 上为恒等映射，并将 ∂ 映到 $\partial - f_N + \frac{i}{x}$。此外，$(\partial - f_N + \frac{i}{x})^p = \partial^p - (f_N + \frac{i}{x})^{(p-1)} - (f_N + \frac{i}{x})^p = \partial^p - y_N$（见 [22, 引理 1.4.2]）。由于它不可分解，$\chi_{min}(\psi_p^{L_i'})(Y) = (Y - y_N)^{m_i}$。注意到 $(Y - y_N)^{m_i} | \chi_{min}(\psi_p^{L_i})$，因为 L_i 是 L_i' 的倍数。由于 $L_i \in \mathbb{F}_q(t)\partial$，且 N 是 y_N 在 $\mathbb{F}_q(t^p)$ 上的最小多项式，因此可得 $N^{m_i} | \chi_{min}(\psi_p^{L_i})$。由于 L_i 的阶恰为 $m_i \deg(N)$，因此 $\psi_p^{L_i}$ 是循环的；这意味着根据定理 3.11，L_i 不可分解。

剩下要证明的是 $\operatorname{ord} L = \sum_{i=1}^p \operatorname{ord} L_i$。我们用归纳法。设 $L' = \mathrm{LCLM}_{i=1}^{p-1} L_i$，并假设我们已经证明了 $\operatorname{ord} L' = \sum_{i=1}^{p-1} \operatorname{ord} L_i$。我们要证明 $\operatorname{ord} L = \operatorname{ord} L' + \operatorname{ord} L_p$。根据命题 2.7，只需证明 L'和 L_p互素。设 K_S是 N在$\mathbb{F}_q(t)$上的分裂域。它是 K_N的伽罗瓦扩张。若 L'和 L_p不互素，我们可以取 $L^* \in K_S\partial \backslash K_S$作为 L_p和 L'的一个不可约因子。由于 $N(\partial^p) = \prod_{\sigma \in \mathrm{Gal}(K_S/\mathbb{F}_q(t))} \partial^p - \sigma(y_N)$且 $L^* | N(\partial^p)$，由定理 3.4 可知，对于某个 $\sigma \in \mathrm{Gal}(K_S/\mathbb{F}_q(t))$，$L^*$必定整除 $\partial^p - \sigma(y_N)$。不失一般性，我们可以假设 L^*是 $\partial^p - y_N$的一个因子。于是 L^*必定是 $\mathrm{GCRD}(L_p, \partial^p - y_N) = \partial - f_N$的因子，从而 $L^* = \partial - f_N$。我们断言 $\mathrm{GCRD}(\partial^p - y_N, L') = \mathrm{LCLM}_{i=1}^{p-1} \partial - f_N + \frac{i}{x}$。事实上，根据归纳假设，$\mathrm{D}_{L'} \simeq \bigoplus_{i=1}^{L} \mathrm{D}_{L_i}$，因此 $\mathrm{D}_{L'(\partial^p - y_N)} = \bigoplus_{i=1}^{p-1} \mathrm{D}_{L_i \partial^p - y_N}$。由最大公右因子的定义可得，$\mathrm{GCRD}(L', \partial^p - y_N) = \mathrm{LCLM}_{i=1}^{p-1} \mathrm{GCRD}(\partial^p - y_N, L_i) = \mathrm{LCLM}_{i=1}^{p-1} \partial - f_N + \frac{i}{x}$。我们将 f_N平移，从而可以假设 $f_N = 0$ 和 $L^* = \partial$，并证明它不是 $\mathrm{LCLM}_{i=1}^{p-1} \partial + \frac{i}{x}$ 的因子。这很容易看出，因为 $\mathrm{LCLM}_{i=1}^{p-1} \partial - \frac{i}{x}$ 在 K_S 中的解空间是 $\bigoplus_{i=1}^{p-1} C_S x^i$，其中不包含 C_S，而后者是 ∂的解空间（其中 C_S是 K_S的常数域）。 ■

注 4.6。 引理 *4.4* 和命题 *4.5* 在将 x替换为任意非恒定的 $g \in K$ 或 $\mathbb{F}_q(t)$时仍然成立。证明相同，只需改用 K的基 1、g、.....、g^{p-1}。

我们不再假设 L、N和 ν是第 3 页中固定的那些对象。

命题 4.4 可以使用 5 来设计一种算法：给定多项式序列 $P_1 | \ldots | P_m \in \mathbb{F}_q(t^p)[Y]$（根据推论 4.3，该序列唯一确定一个算子等价类），计算该等价类的一个代表元，使得 P_i 是其 p-曲率的 Frobenius 不变量。我们仅考虑满足假设 4.7 的多项式；其他情形将在最终的最小公倍左倍数分解算法（算法 2）中另行处理。

假设 4.7。 设 $Q \in \mathbb{F}_q(t)[Y]$。我们假设 Q 的所有不可约因子 N 在 $\mathbb{F}_q(t)$ 上都是可分的，并且 $N^p(\partial)$ 在 $\mathbb{F}_q(t)\langle\partial\rangle$ 中是可约的。

定义 4.8. 令 $L \in \mathbb{F}_q(t)\langle\partial\rangle$。我们称 L的次数（小于） d，如果存在多项式 $D, p_0, \ldots, p_{\operatorname{ord}(L)} \in \mathbb{F}_q[t]$

算法 1 nice_repr输入：$Q_1|Q_2\ldots|Q_m \in \mathbb{F}_q(t)[Y]$满足 $m \le p$ 且 Q_m符合假设 4.7。输出：

- $L^* \in \mathbb{F}_q(t)\partial$，使得 $\psi_p^{L^*}$的 Frobenius 不变量为 $P_1|P_2\ldots|P_m$，其中对于所有 i，都有 $P_i(X^p) = Q_i^p(X)$。
- $L_1^*, \ldots, L_k^*$ 是 L_*的最小公倍左倍数分解。(1) 将列表 _factor 设为 Q_m的不可约因子列表。(2) 对于 list_factor 中的 N：（a）设 a_N 为 N 在 $\mathbb{F}_q(t)$ 的可分闭包中的一个根。（b）使用 [18, 算法 9]计算 $f_N \in \mathbb{F}_q(t)[a_N]$，使得 $f(N)^{p-1} + f_N^p = a_N^p$。(3) 将 LCLM_decomp 设为空列表。(4) 对于 $\{1, \ldots, m\}$ 中的 i：（a）对于 list_factor 中的 N：（i）计算 $v_N(Q_i)$，即 Q_i 在 N 中的重数。（ii）计算 $N_{i,N}$，即 $(x\partial - xf_N)^{v_N(Q_i)}$ 在 $\mathbb{F}_q(t)\partial$ 中的最小倍数。（iii）将 $N_{i,N}(\partial + \frac{i}{x})$ 添加到 LCLM_decomp。(5) 使用 [5] 以及 LCLM_decomp 计算并返回 LCLM_decomp 中各元素的最小公倍左倍数。

_

次数小于 d $L = D^{-1}\, p_{\mathrm{ord}(L)}\, t\, \partial^{\mathrm{ord}(L)} + \cdots + p_1\, t\, \partial + p_0\, t$，使得 $(()\cdots())$。

定理 4.9。算法 *1* 是正确的。此外，如果 Q_m 是 $\mathbb{F}_q[t, Y]$ 中一个双次数为 d_t, d_Y 的多项式，那么算法 *1* 会在关于 d_t、d_Y 和 m 的多项式时间内终止，并且关于 p 是准线性的。它会输出次数关于 d_t、d_Y 和 m 为多项式的算子 L_*，而它在 L_* 的最小公倍左倍数分解中输出的算子 L_1^*、…、L_k^* 的次数关于 d_t 和 d_Y 为多项式。

证明。算法 1 的正确性直接来自定理 3.4 和命题 4.5。假设 4.7 确保对于列表_因子中的每个 N，命题 4.5 均适用。

步骤 (3a) 中的每个 f_N 都可表示为

$$f_N = D_{f_N}^{-1}(f_{N,\deg_y(N)-1} a_N^{\deg_y(N)-1} + \cdots + f_{N,0})$$

其中某些多项式 $D_{f_N}, f_N, 0, \ldots, f_{N,\deg_y(N)-1}$ 的次数小于某个关于 $\deg_t(N) \le d_t$、$\deg_Y(N) \le d_Y$ 的多项式（见 [18, 定理 3.4.29]）。那么，对于每个整数 $n \in \mathbb{N}$，$(\partial - f_N)^n$，其系数属于 $\mathbb{F}_q(t)[a_N]$，并且也可表示为关于 $\mathbb{F}_q[t]$ 的 $\deg_Y(N)$ 次多项式，且公分母的次数小于关于 $\deg_t(N)$、$\deg_Y(N)$ 和 n 的多项式（事实上，由于通常 $\deg_t(N)\deg_Y(N) = O(d')$，这个多项式通常为 $O(nd')$）。$(\partial - f_N)^n$ 在 $\mathbb{F}_q(t)\partial$ 中的一个倍数是自然 $\mathbb{F}_q(t)$-线性映射的核的生成元

$$\pi_N : \mathbb{F}_q(t)\langle\partial\rangle_{\le n\deg_Y(N)} \to K_N\langle\partial\rangle / K_N\langle\partial\rangle(\partial - f_N)^n.$$

在 $\mathbb{F}_q(t)$-基$(1, \partial, \ldots, \partial^{n\deg_Y(N)})$与$(1, a, \ldots, a^{\deg_Y(N)-1}, \partial, a\partial, \ldots, a^{\deg_Y(N)-1}\partial^{n-1})$下，$\pi_N$的矩阵 M由下式给出

$$[v, \theta(v), \ldots, \theta^{n\deg_Y(N)}(v)]$$

其中 $v = {}^t(1, 0, \ldots, 0)$，且 $\theta = \mathrm{d}\frac{}{\mathrm{d}t} + T$，而 T是矩阵$(A_N' D_a) \otimes I_n + C((\partial - f_N)^n)$，其中 A_N'是在 $\mathbb{F}_q(t)[a]$中乘以 a_N'的矩阵，D_a是$\mathrm{d}\frac{}{\mathrm{d}a}$的矩阵，并且

$$C((\partial - f_N)^n) = \begin{pmatrix} & & & -F_0 \\ I_{\deg_Y(N)} & & & -F_1 \\ & \ddots & & \vdots \\ & & I_{\deg_Y(N)} & -F_{n-1} \end{pmatrix}$$

其中 $(\partial - f)^n = \partial^n + f_{n-1}\partial^{n-1} + \cdots + f_0$ 和 F_i是 $\mathbb{F}_q(t)[a]$ 中乘以 f_i 的矩阵。T 的每个条目，其大小关于 n，$\deg_t(N)$ 和 $\deg_Y(N)$ 均为多项式，因此核 M 中的元素也同样如此。

由于 $n\deg_Y(N) \le d_Y$，因此每个 L_i^*的次数都是关于 d_t 和 d_Y 的多项式。L^* 的系数次数是关于 d_t，d_Y 和 m 的多项式，这一事实可由 [5] 以及 $\mathrm{ord}\, L^* = \sum_{i=1}^k \mathrm{ord}\, L_i^* \le md_Y$ 这一事实得出。∎

注 4.10. 我们从定理的证明中看到，寻找 $\mathbb{F}_q(t)\langle\partial\rangle$ 中 $(\partial - f_N)^n$ 的一个倍数这一问题，实际上是 *[10, 问题 1]* 的一个特例，尽管这里处于正特征情形。通过同类型的分析，或许可以得到更紧的界。

5 同构与最小公倍左倍数分解的传播

本节旨在寻找两个等价算子的商模之间的同构。回顾一下，$\mathbb{F}_q(t)\partial$-模的态射 $\varphi : \mathrm{D}_{L_1} \to \mathrm{D}_{L_2}$，其中 L_1，$L_2 \in \mathbb{F}_q(t)\partial$，完全由 $\varphi(1)$ 决定。为了使 φ 定义良好，必须存在 $Q \in \mathbb{F}_q(t)\partial$，使得 $L_1\varphi(1) = QL_2$。因此，在 D_{L_1} 和 D_{L_2} 之间寻找态射，是一个典型例子：寻找混合微分方程的有理解；Mark van Hoeij 在 [25]中研究了这一问题。遗憾的是，他们的工作仅限于特征零的情形。在特征零中，通常通过将问题转化为寻找某个线性微分系统 $Y' = AY$ 的有理解来求解，其中 A 是一个有理系数矩阵。随后，我们可以根据 A的系数，对有理解的极点及其重数进行界定。遗憾的是，在特征 p 下无法做到这一点，因为常数域是 $\mathbb{F}_q(t^p)$，这使得解可以有任意多个极点，且赋值可以任意高。或许，假设 p 相对于A 的参数足够大，就能让我们使用特征零时的相同方法，并找到 D_{L_1} 与 D_{L_2} 之间的“小”同构（也就是说，由次数不依赖于 p的算子给出的同构）。然而，L_1 与 L_2 等价，并不保证存在“小”同构。此外，尽管“小”同构的存在结合前几节的工作可以保证存在“小”的最小公倍左倍数分解（“小”的含义类似），反过来却不成立。

例5.1。若 $p \ge 3$，算子 ∂和 $\partial + \frac{p-1}{2t}$ 不可约且等价，并且它们的系数的次数与 p无关。然而，同构 φ：$\mathcal{D}_\partial \to \mathcal{D}_{\partial+(p-1)/2t}$ 由 $\varphi(1) = g(t^p)t^{(p-1)/2}$ 给出，其中任意 $g \in \mathbb{F}_q(t)$均成立。无论如何选择 g，同构的系数的次数至少随 p线性增长。

相反，我们将混合微分方程视为一个 $\mathbb{F}_q(t^p)$-线性系统来求解。这使我们将获得的最小公倍左倍数分解的“规模”对 p 呈二次依赖，尽管实验表明这种依赖实际上仅随 p线性增长。

引理 5.2. 设 L, L^* 是 $\mathbb{F}_q(t)\langle\partial\rangle$ 中的等价算子，且 $L_1^*, \ldots, L_k^*$ 是 L^* 的一个最小公倍左倍数 分解。对于任意同构$\varphi: \mathcal{D}_{L^*} \xrightarrow{\sim} \mathcal{D}_L$, L =最小公倍左倍数$_{i=1}^{k}$最大公右因子$(L, \varphi(L_i^*))$是 L 的一个最小公倍左倍数 分解。

证明。由于 φ 是 $\mathbb{F}_q(t)\partial$-模的同构，因此特别也是 $\mathbb{F}_q(t)$-向量空间的同构。特别地，它保持子模的余维数不变。它将由 L_i^* 生成的 $\mathrm{D}_{L^*}L_i^*$ 的子模映射到由 $\varphi(L_i^*)$ 生成的 D_L 的子模；根据最大公右因子的定义，该子模为 D_L最大公右因子$(L, \varphi(L_i^*))$。此外，我们有 $\varphi(\bigcap_{i=1}^{k} \mathrm{D}_{L^*}L_i^*) = \bigcap_{i=1}^{k} \mathrm{D}_L$最大公右因子$(L, \varphi(L_i^*))$ $=\{0\}$。因此，根据最小公倍左倍数的定义， L = 最小公倍左倍数$_{i=1}^{k}$最大公右因子$(L, \varphi_i(L_i^*))$。最后，我们有

$$\sum_{i=1}^{k} \operatorname{ord} \operatorname{GCRD}(L, \varphi(L_i^*)) = \sum_{i=1}^{k} \dim_{\mathbb{F}_q(t)} \mathcal{D}_{\operatorname{GCRD}(L, \varphi(L_i^*))}$$
$$= \sum_{i=1}^{k} \operatorname{codim}_{\mathbb{F}_q(t)} \mathcal{D}_L \operatorname{GCRD}(L, \varphi(L_i^*)) = \sum_{i=1}^{k} \operatorname{codim}_{\mathbb{F}_q(t)} \mathcal{D}_{L^*}L_i^*$$
$$= \sum_{i=1}^{k} \operatorname{ord} L_i^* = \operatorname{ord} L^* = \operatorname{ord} L$$

因此，我们确实得到了 L的最小左公倍数分解。 ∎

现在，我们在算法 2 中给出最小公倍左倍数分解算法。在证明该算法给出正确结果之前，我们先证明以下引理：

引理 5.3. 设 $L \in \mathbb{F}_q(t)\langle\partial\rangle$满足假设 *3.5*。设 $P_1|\ldots|P_m$是 ψ_p^L在 $\mathbb{F}_q(t^p)[Y]$中的 *Frobenius* 不变量。设 $N \in \mathbb{F}_q(t^p)[Y]$是可分且不可约的（在 $\mathbb{F}_q(t^p)$上），并且 $\nu \in \mathbb{N}$是满足 $N(\partial^p)^\nu | L$的最大值。我们将 ν_N记为 N相对于 $\mathbb{F}_q(t^p)[Y]$的赋值。

i) $m \le p$。 *ii)* 若 $\nu > 0$，则 $m = p$且 $\nu_N(P_1) = \nu$。
iii) 若 $\nu_N(P_p) = \nu$，则 L =最小公倍左倍数$(L \cdot N(\partial^p)^{-\nu}, N(\partial^p)^\nu)$

证明。由于 ψ_p^L的 Frobenius 不变量不依赖于基域，并且形如 $\mathrm{D}_{N'(\partial^p)}$ 的任意中心单代数都必须在某个有限维伽罗瓦扩张 K of $\mathbb{F}_q(t)$ 上分裂，因此不失一般性，我们可以假设 L 没有中心不可约因子（特别地，可以假设 N是不可约多项式，而 $N(\partial^p)$ 是可约算子）。我们将 C记为 K的常数域。令 $N' \in C[Y]$为 P_1的一个不可约因子。则 N' 必须出现在每个 P_i中。由于我们假设 $N'(\partial^p)$ 是可约的（否则它将是 L的一个中心不可约因子），根据定理 3.11，这意味着 L的一个最小公倍左倍数分解必须恰好包含 m个不可分解因子，且这些因子都是 $N'(\partial^p)$ 的某个幂的因子。特别地，若 L_1, ..., L_m是它们唯一的右不可约因子，则每个 L_i都是 $N'(\partial^p)$ 的因子，因此 $\operatorname{LCLM}_{i=1}^{m} L_i | N'(\partial^p)$，且 $\operatorname{ord} \operatorname{LCLM}_{i=1}^{m} L_i = \sum_{i=1}^{m} \operatorname{ord} L_i = m \deg(N') \le \operatorname{ord} N'(\partial^p) = p \deg(N')$，这就证明了$m \le p$。

$K\partial$-模 $\mathrm{D}_{N(\partial^p)^\nu}$可识别为以下对象的子模

算法 2 最小公倍左倍数_分解

I 输入： $L \in \mathbb{F}_q(t)\partial$，满足假设 3.5。输出： L_1、.....、 L_k 的最小公倍左倍数分解。(1) 计算 $Q_1|Q_2|\ldots|Q_m$，使得如果 $P_1|\ldots|P_m = \chi_{min}(\psi_p^L)$ 是 ψ_p^L的 Frobenius 不变量，那么使用 [4] (2) 令 列表_因子 为 Q_m的不可约因子列表。(3) 令 最小公倍左倍数_分解 为空列表 (4) **如果** $m == p$ **则执行**：

- 对于 N_* in list_factor：（a）令 ν_{N_*}为与 N_*在 $\mathbb{F}_q(t)[Y]$ 中对应的赋值。（b）如果 $\nu_{N_*}(Q_1) == \nu_{N_*}(Q_m)$，则执行：（i）令 $\nu = \nu_{N_*}(Q_m)$（ii）将 L替换为 $L \cdot N_*^{-p\nu}(\partial)$（iii）对所有 i，将 Q_i替换为 $Q_i \cdot N_*^{-\nu}$。（iv）如果 $N_*^p(\partial)$ 不可约（[18, 算法 6]），则将$N_*^{p\nu}(\partial)$ 添加到最小公倍左倍数分解中。否则：（A）对 $N_*^\nu|\ldots|N_*^\nu$ 使用算法 1。令 L^*为结果，—— —p 次 L_1^*, ..., L_p^*为其最小公倍左倍数分解。（B）将 L_1^*, ..., L_p^* 添加到最小公倍左倍数分解中。（v）从 list_factor 中移除 N_*。（5）对 $Q_1|\ldots|Q_m$ 使用算法 1。令 L^*为输出，L_1^*, ..., L_k^*为其最小公倍左倍数分解。（6）计算 $\mathbb{F}_q(t^p)$-线性映射模 L 的核。（7）选择 M，一个来自 $\ker \Lambda_{L^*,L}$ 的随机元素。（8）当最大公右因子$(M, L) \neq 1$ 时，选择 M 为 $\ker \Lambda_{L^*,L}$ 中另一个随机选取的元素。（9）对于 i in $\{1, \ldots, k\}$，将最大公右因子$(L, L_i^* M)$ 添加到最小公倍左倍数分解中。（10）返回最小公倍左倍数分解。

$$\begin{aligned} \Lambda_{L^*,L}: \quad \mathbb{F}_q(t)\langle\partial\rangle_{<\operatorname{ord} L} &\to \mathcal{D}_L \\ M &\mapsto L^*M \end{aligned}$$

D_L, $\ker N^\nu(\psi_p^L)$。（D_L, ψ_p^L）作为 $K[T]$-模与 $\bigoplus_{i=1}^{m} K[T]/P_i(T)$ 同构。因此，$\ker N(\psi_p^L) \simeq \bigoplus_{i=1}^{m} K[T]/N_{\min(\nu,\ \nu_N(P_i))}(T)$ 作为 $K[T]$-模，并且

$$\dim_K \ker N(\psi_p^L) = \sum_{i=1}^{m} \min(\nu, \nu_N(P_i)) \deg(N) = p\nu \deg(N)$$

. 这仅当 $\nu = 0$ 或 $m = p$且 $\nu(P_i) \ge \nu$对所有 i 时才可能发生。特别地， $\nu_N(P_1) \ge \nu$。为证明等式成立，我们可以写成 $L = L'N(\partial^p)^\nu$。于是 $(\mathrm{D}_{L'}, \psi_p^{L'})$ 可等同于 D_L 关于 $\ker N^\nu(\psi_p^L)$ 的商，从而作为 $K[T]$-模同构于 $\bigoplus_{i=1}^{p} K[T]/P_i'$，其中 $P_i' = P_i \cdot N^{-\nu}$。特别地，$P_i'$是 $\psi_p^{L'}$ 的 Frobenius 不变量。若 $\nu_N(P_1') > 0$，则我们可以用证明 $m \le p$ 的同样方式证明 $N(\partial^p)|L'$，这与 ν 的极大性相矛盾。为证明 (iii)，我们可以假设 $\nu > 0$。由于 $N(\partial^p)$ 是中心的， L确实是 $L' = L \cdot N(\partial^p)^{-\nu}$ 与 $N(\partial^p)^\nu$ 的左倍数。此外，由假设，$\nu_N(\chi(\psi_p^L)) = p\nu$。由乘法性可得 $\nu_N(\chi(\psi_p^{L'})) = 0$，从而 L' 与 $N(\partial^p)^\nu$ 互素。由命题 2.7(i) 可得 L =最小公倍左倍数$(L', N(\partial^p)^\nu)$。∎

定理 5.4. 算法 *2* 是正确的。此外，若 $L \in \mathbb{F}_q(t)\langle \partial \rangle$ 的阶为 r 且次数为 d（见定义 *4.8*），则算法 *2* 在关于 r、d 和 p 的多项式时间内终止，并给出 L 的一个 最小公倍左倍数 分解，其中每个因子的次数关于 r 和 d 为多项式，且关于 p 至多为二次。

备注 5.5. p 中的二次复杂度来源于算法 *2* 的第 *(6)* 步。然而，实验表明，$\ker \Lambda_{L^*,L}$ 的基中各元素的系数，其大小并不超过矩阵 $\Lambda_{L_*,L}$ 自身系数的大小。更准确地说，系数的增长似乎并不取决于 p，而只取决于 r 和 d。这表明，算法 *2* 的输出实际上关于 p是准线性规模，而非准二次规模。

证明. 在第 (4) 步结束时， L 不再有任何中心不可约因子，并且 Q_i 满足：若 $P_i(Y^p) = Q_i^p(Y)$，则 P_i 是其 p-曲率的 Frobenius 不变量。这直接由引理 5.3 得出。根据同一引理的 (iii)，要计算输入中 L 的最小公倍左倍数分解，只需在第 4 步计算 L 的最小公倍左倍数分解，并在 $\nu_N(Q_1) = \nu_N(Q_m)$ 且 $m = p$时，计算 $N^p(\partial)$的最小公倍左倍数分解。算法 1 在后一种情况下、当 $N^p(\partial)$ 可约时能够计算出这样的分解，这是命题 4.5 的推论，因为 $N^{p\nu}(\partial)$是右阶的公倍数。

在步骤 (5) 中，算法 1 得到的算子 L^* 与步骤 (4) 中的 L 等价。事实上，根据定理 4.9， $\psi_p^{L^*}$ 和 ψ_p^L 具有相同的 Frobenius 不变量，因此等价；这意味着根据推论 4.3， L^* 和 L 等价。$\Lambda_{L_*,L}$ 的核中的元素都是 D_{L^*} 与 D_L之间的 $\mathbb{F}_q(t)\partial$-模态射。选取一个与 L 互素的元素可确保它是同构；而 L^* 和 L 等价这一事实保证了这样的元素存在。由引理 5.2 即得结论。

由于 $\sum_{i=1}^m \deg_t(Q_i) \leq p^{-1} \deg_t(\chi(\psi_p^L)) \leq d$(见 [3, 引理 3.9])，且 $\sum_{i=1}^m \deg_Y(Q_i) = r$，由定理 4.9 可知， L^* 和 L_i^*都具有关于 r和 d的次数多项式。因此，$\Lambda_{L^*,L}$在基 $(x^i \partial^j)_{0\leq i<p,0\leq j<r}$下的矩阵可表示为 $M_{rp}(\mathbb{F}_q(t^p))$ 中的一个矩阵，其系数是关于 t^p的次数多项式，并且是关于 r和 d的次数多项式。由此可知，核中的元素的系数是关于 t^p的次数多项式、关于 r和 d的次数多项式，并且关于 p是线性的。因此， M 具有关于 t的次数多项式、关于 r和 d的次数多项式，并且关于 p是二次的。

■

参考文献

[1] Anderson，W.，以及 Fuller，K. R.《环与模范畴》。[2] Bhattacharya，P. B.、Jain，S. K. 和 Nagpaul，S.《基础抽象代数》。剑桥大学出版社，1994 年。[3] Bostan，A.、Caruso，X. 和 Schost，E. 一种快速计算 p-曲率特征多项式的算法。载于*ISSAC 2014*——第 *39* 届国际符号与代数计算研讨会论文集（2014 年），ACM，纽约，第 59–66 页。[4] Bostan，A.、Caruso，X. 和 Schost，E. 计算 p-曲率的相似类。载于*2016* 年 *ACM* 国际符号与代数计算研讨会论文集（2016 年），ACM，纽约，第 111–118 页。[5] Bostan，A.、Chyzak，F.、Salvy，B. 和 Li，Z. 快速计算线性常微分算子的公共左倍。载于第 *37* 届国际符号与代数计算研讨会论文集（2012 年 7 月），ISSAC'12，ACM。[6] Chyzak，F.、Goyer，A. 和 Mezzarobba，M. 微分算子的符号-数值分解。载于*2022* 年国际符号与代数计算研讨会论文集（美国纽约州纽约市，2022 年），ISSAC '22，计算机协会，第 73–82 页。[7] Cluzeau，T. 特征 p下微分系统的因式分解。载于*2003* 年国际符号与代数计算研讨会论文集（2003 年），ACM，纽约，第 58–65 页。

[8] Dwork，B. 带幂零 p *112*, -曲 5, 1990，749–786 率的微分算子。《美国数学杂志》（ ），– 。[9] Eid，E. 奇特征下超椭圆曲线同源的快速计算。载于 2021 年国际符号与代数计算研讨会论文集（美国纽约州纽约市，2021 年），ISSAC '21，计算机协会，第 131–138 页。[10] Gaillard，L. 线性微分算子次数界估计的统一方法。载于 2025 年国际符号与代数计算研讨会论文集（美国纽约州纽约市，2025 年），ISSAC '25，计算机协会，第 16–24 页。[11] Giesbrecht，M. 和 Zhang，Y. 在 $\mathbb{F}_q(t)$上对 Ore 多项式进行因式分解与分解。载于 2003 年国际符号与代数计算研讨会论文集（2003 年），ACM，纽约，第 127–134 页。[12] Gille，P. 和 Szamuely，T.《中心单代数与伽罗瓦上同调》。剑桥高级数学研究丛书。剑桥大学出版社，2006 年。[13] Gómez-Torrecillas，J.、Lobillo，F. J. 和 Navarro，G. 计算 Ore 多项式的界及其在因式分解中的应用。《符号计算杂志》92（2019），269–297。[14] Grigor'ev，D. 线性常微分算子的因式分解与最大公因式计算的复杂度。《符号计算杂志》10，1（1990），7–37。[15] Kauers，M.《D-有限函数》。施普林格出版社，2023 年。[16] Lairez，P. 和 Vaccon，T. 关于变量分离的 p-进微分方程。载于 2016 年 ACM 国际符号与代数计算研讨会论文集（2016 年），ACM，纽约，第 319–323 页。[17] Lauder，A. G. 计算有限域上多变量方程的解数。《计算数学基础》4，3（2004），221–267。[18] Pagès，R. 正特征下微分算子的因式分解。博士论文，波尔多大学，2024 年 2 月。[19] Pagès，R. 求解 p-Riccati 方程及其在微分算子因式分解中的应用。工作论文或预印本，2024 年 1 月。[20] van der Hoeven，J. 关于微分伽罗瓦群的数值-符号计算。《符号计算杂志》42（2007），236–264。[21] van der Hoeven，J. 全纯函数的高效加速求和。《符号计算杂志》42，4（2007），389–428。[22] van der Put，M. 特征 p下的微分方程。第 97 卷。1995 年，第 227–251 页。纪念 Frans Oort 的专刊。[23] van der Put，M. 微分方程模 p 约化。《荷兰数学学会杂志》（新辑）7，3（1996），367–387。[24] van der Put，M. 和 Singer，M. F.《线性微分方程的伽罗瓦理论》，《数学科学基础丛书》第 328 卷，*[*《数学科学基础原理》*]*。施普林格出版社，柏林，2003 年。[25] van Hoeij，M. 混合微分方程的有理解及其在微分算子因式分解中的应用。载于 1996 年国际符号与代数计算研讨会论文集（美国纽约州纽约市，1996 年），ISSAC '96，计算机协会，第 219–225 页。[26] Van Hoeij，M. 有理函数系数微分算子的因式分解。《符号计算杂志》24，5（1997），537–561。