arXiv:2601.02162v1 [math.NT] 5 Jan 2026

Drinfeld模的计算方法

Cécile Armana[1], Elena Berardini[2],Xavier Caruso[2],Antoine Leudière[3],Jade Nardi[4], 和 Fabien Pazuki[5]

[1]里尔大学，法国国家科学研究中心，UMR 8524 - 保罗·潘勒韦实验室，F-59000 里尔，法国[2]法国国家科学研究中心；波尔多大学数学研究所，法国[3]卡尔加里大学，加拿大 [4]法国国家科学研究中心；雷恩大学，雷恩数学研究所 - UMR 6625，F-35000 雷恩，法国[5]哥本哈根大学数学科学系，Universitetsparken 5，2100 哥本哈根，丹麦

摘要

本综述从实用和算法的角度介绍了 $\mathbb{F}_q[T]$ 上的 Drinfeld 模。我们从 Carlitz 模的构造入手，介绍任意秩的 Drinfeld 模及其部分算术性质。我们着重阐述它们与椭圆曲线之间的类比，同时也指出关键差异，例如它们的秩结构及其相关的 Anderson 动机。

本文面向数论、算术几何、算法数论、密码学或计算机代数领域的研究者，提供工具与见解，帮助他们有效探索 Drinfeld 模的计算方面。我们还提供详尽的 SageMath 实现，以展示具体计算并便于开展实验。文中还介绍了多项式因式分解、同源计算、密码学构造和编码理论方面的应用。

目录

1 引言 **2**

1.1 综述的目的与组织.3 1.2 背景与记号.4

2 探索 Carlitz 模 **5**

2.1 寻找指数函数.6 2.2 Carlitz 模的解析构造.7 2.3 圆分理论的应用.10 2.4 Carlitz ζ 函数.10

3 Drinfeld 模及其 Anderson 动机 1 **2**

3.1 Ore 多项式.13 3.2 代数 Drinfeld 模.16 3.3 解析一致化.17 3.4 Drinfeld 模的实现：Tate 模与 Anderson 动机 . . 19

2020 年数学主题分类。主要分类 11G09，次要分类 11R58，11-04。关键词：Drinfeld 模、Carlitz 模、Ore 多项式、Anderson 动机、计算机代数、密码学、编码理论。

4 Drinfeld 模的态射 **23**
4.1 形式定义.23 4.2 可分性.26

4.3 同构与j-不变量.28 4.4 Anderson 动机上的作用及其结果.30

5 Drinfeld 模的算术方面 36
5.1 有限域上的情形.36 5.2 全局函数域上的情形.47

6 Drinfeld 模的一些应用 53
6.1 Drinfeld 模与计算代数.53 6.2 Drinfeld 模与密码学.58 6.3 Drinfeld 模与线性码.60

1 引言

数论有时被描述为对数域及其伽罗瓦性质的研究；数域是 $\mathbb{Q}$ 的有限扩张。最简单的一类数域是所谓的分圆域，它们由 $\mathbb{Q}$ 添加入单位根得到。尽管这些域乍看之下相当初等，但它们揭示了引人注目的结构，并带来了众多应用，包括库默尔对费马大定理许多情形的证明。最终，对它们的研究导向了类域论。在分圆扩张之外，还可以发现 $\mathbb{Q}$ 的非阿贝尔扩张。在这里，情况远未得到充分理解；然而，代数几何为构造此类扩张提供了强有力的工具。一个基本例子是：由定义在 $\mathbb{Q}$ 上的椭圆曲线的n-挠点的坐标生成的域是一个数域，其伽罗瓦群自然地嵌入 $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$ 中。对这些扩张的研究十分引人入胜，并再次带来了杰出的应用，包括怀尔斯和泰勒–怀尔斯对费马大定理的完整证明。如今，这些发展被囊括在影响深远的朗兰兹纲领之中；粗略地说，该纲领旨在通过群论方法理解所有数域。

与数域相对应，人们通常也会考虑函数域，即 $\mathbb{F}_q(T)$ 的有限扩张，其中 $\mathbb{F}_q$ 是一个有限域。然而，以直接的方式将分圆域和椭圆曲线的定义扩展到函数域，并不能得到具有足够丰富算术内容的概念。以分圆理论为例，我们注意到，由单位根生成的 $\mathbb{F}_q(T)$ 的扩张不过是域 $\mathbb{F}_{q^m}(T)$——这遗漏了许多有趣的阿贝尔函数域。

20世纪30年代，Carlitz [Car35] 在函数域框架下引入了指数函数的一种类似物，由此构造出一个全新的庞大循环扩张族。粗略地说，这些扩张是通过对任意多项式$f(T) \in \mathbb{F}_q[T]$添加“$f(T)$次单位根”来定义的。约四十年后，Drinfeld 更进一步，提出了一类新对象，最初称为椭圆模，将其作为函数域上椭圆曲线的一种有意义的算术替代物。椭圆模如今称为***Drinfeld*** 模，它们可以构造伽罗瓦群包含于 $\mathrm{GL}_r(\mathbb{F}_q[T]/f(T)\mathbb{F}_q[T])$ 的扩张，其中秩r可任取，多项式$f(T) \in \mathbb{F}_q[T]$也可任取。在秩 1 的情形，Drinfeld 理论与 Carlitz构造相契合；而在秩 2 的情形，它则模仿了椭圆曲线的经典理论。不过，Drinfeld 的框架还允许人们以类似方式探索高秩——这一特点后来被证明对 Langlands纲领具有非凡的重要性

函数域的纲领 [Dri80], , 因为它使 Lafforgue [Laf02] 得以在2002年彻底证明 GL_r 的情形。

我们还简要提及，与椭圆曲线和模形式的关系类似，Drinfeld 模也与所谓的 Drinfeld 模形式相关通过模性定理 [Dri74,GR96]。它们也是函数域上丰富的超越理论的源头，其中包括代数独立性 [Tha04, Chapter 10]。

椭圆曲线算法的研究由来已久。相比之下，尽管 Drinfeld 模影响深远，其算法方面却鲜为人知，直到最近才成为研究热点 [Car18, CGS20, Wes24, Ayo23, CL26, Leu24, CG25, GKK25]。这项研究最初受到 Drinfeld 模与椭圆曲线，乃至更广泛地说与数域上的阿贝尔簇之间诸多共同性质的推动，但如今已开始走上独立发展的道路，甚至在某些方向上有所超越。一个显著的例子是：计算 Drinfeld 模的同源或L-函数的问题基本上已得到解决，而在数域上，这些问题仍然颇具挑战性。此外，Drinfeld 模算法也开始在相关领域中得到应用，包括计算机代数 [DNS21], 密码学 [Sca01, JN19, LS22] 以及编码理论 [BBN15, BDM24]。

1.1 本综述的目的与组织结构

本文旨在概述 Drinfeld 模理论，尤其关注其计算方面与应用。文中将通过许多实例加以说明，这些实例借助 SageMath 软件处理；该软件包含 Drinfeld 模的实现：首批功能已集成于 SageMath 10.0 [ACLM23, Leu24], , 而较新的功能则是在撰写本文的同时加入的。

实际上，本文将穿插如下 SageMath 代码片段。

SageMath 示例 1.1。

```
sage: # 这是 SageMath 解释器中的一条注释sage: #
以下是一条命令及其输出sage: 57.is_prime()False
sage: # 完善。
```

我们从第 2 节开始，介绍 Carlitz 对所谓 *Carlitz* 模的解析构造 ，并展示其在分圆理论中的应用。在第 3 节中，我们逐步提升秩，定义一般的 Drinfeld 模，并进一步从解析处理转向代数处理。此外，我们还将介绍与 Drinfeld 模相关的经典代数不变量，即其 *Tate* 模 及其“动机”，后者称为*Anderson* 动机，是重要的算法工具。

第 4 节专门讨论 Drinfeld 模之间的态射，这是该理论的核心课题；我们将特别研究它们在 Anderson 动机层面所诱导的作用，并在此基础上为它们赋予有意义的不变量。我们的目标是为读者提供理解这些结构所需的工具和见解。第 5 节将继续探讨 Drinfeld 模与椭圆曲线之间的类比，着眼于它们的算术方面。我们将描绘有限域上的 Drinfeld 模概貌，阐明 Frobenius 同构的重要性；同时也会介绍函数域上的情形，概述 L-级数理论。我们还将探讨一些最新

的进展，这些进展与 Drinfeld 模的高度理论有关；这一主题在标准参考文献中的讨论相对较少。最后，第 6 节将概述 Drinfeld 模在多项式因式分解、密码学和编码理论中的应用。

尽管本综述所介绍的内容相当标准，但我们的论述与经典论述有所不同，明显以算法为导向。具体而言，我们着重介绍 Anderson 动机，因为它们为 Drinfeld 模提供了一种具体的实现形式，便于处理计算。事实上，与 Drinfeld 模不同，Anderson 动机实际上是经典意义上的模，因此可以借助标准线性代数方法和多项式算术进行显式计算。在强调 Drinfeld 模与椭圆曲线之间相似性的同时，这种视角也让我们得以探讨它们的一些关键区别：Anderson 动机体现了 Grothendieck 动机，但与后者不同，它们只需用初等代数定义即可描述。因此，它们在近期的算法发展中发挥了关键作用，使得人们能够以更一般的方式（尤其是更高的秩）解决计算问题，并用于构造新型编码理论。

关于 Drinfeld 模及其推广（Anderson 动机、阿贝尔模、shtuka）的更全面论述，以及互为补充的不同视角，请读者参阅 [Gos96、Ros02、Tha04、BP20、Poo22、Pap23]（按时间顺序排列，此列表并不穷尽）。

1.2 设定与记号

令p 为素数，令q 为p的幂。令 $\mathbb{F}_q$ 为含有q 个元素的有限域。记$A := \mathbb{F}_q[T]$ 为系数属于 $\mathbb{F}_q$ 的一元多项式环，并记$K = \mathbb{F}_q(T)$ 为其分式域。域K 是 $\mathbb{F}_q$上的全局函数域。

注 1.1. 在最一般的情形下，Drinfeld 模定义于这样的K 上：它是有限域上某条光滑曲线的有理函数域。不过，在本文中，我们始终将范围限制在$A = \mathbb{F}_q[T]$ 的情形（对应于曲线 $\mathbb{P}^1$），因为我们认为这对于本文的论述而言理论已经足够丰富。为了便于研究一般环上的 Drinfeld 模，我们将指出假设$A = \mathbb{F}_q[T]$ 至关重要的部分。

与 $1/T$ 对应的K 的赋值点记为 ∞。置$K_\infty := \mathbb{F}_q((1/T))$，这是一个与$K$ 在 ∞处的完备化同构的域。我们赋予K_∞ 绝对值$q^{\deg(\cdot)}$。固定的K的一个代数闭包的完备化记为C_∞，且绝对值唯一延拓到C_∞。域K_∞ 和C_∞ 都是非阿基米德的。域C_∞ 是完备且代数闭的。

图 1 展示了函数域与数域情形之间的一组经典类比，其中 $\mathbb{Z}$ 和 A 发挥着相同的作用。然而，与 $\mathbb{C}/\mathbb{R}$不同，扩张 C_∞/K_∞ 的次数是无限的。C_∞ 中的元素可能难以理解，尤其是在计算应用中。注意，对于特征为 0 的域 K，$K((t))$ 的代数闭包与 Newton–Puiseux 域$\bigcup_{i=1}^{\infty} K((t^{1/i}))$同构。在我们的情形中，由于$K_\infty$ 具有正特征，其代数闭包包含的不仅仅是 Newton–Puiseux 级数——更多详情请参阅 [Ked01]。

SageMath 示例 1.2. 在本文中，我们将在 SageMath 的所有示例中使用基环 $A = \mathbb{F}_7[T]$。下面的代码会创建 A 及其在无穷远处的完备化 K_∞。

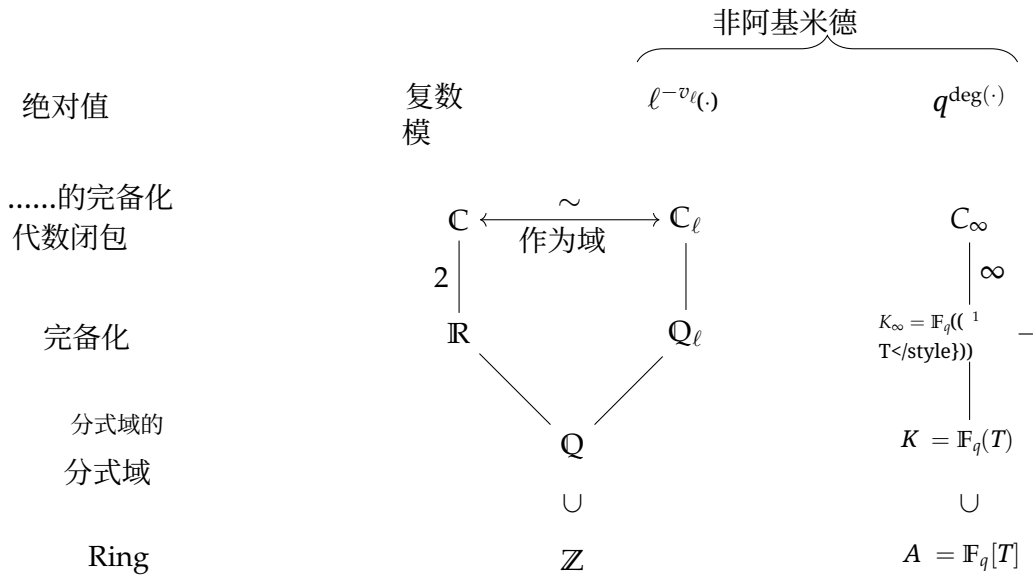


图 1：开始研究 Drinfeld 模时值得牢记的类比。

```
sage: F7 = GF(7)
sage: A.<T> = F7['T']
sage: A.completion(infinity)
Completion of Fraction Field of Univariate Polynomial Ring in T over Finite
    Field of size 7 at infinity
```

欧拉-庞加莱特征。 我们还回顾主理想整环 A 上的以下分类结果：任意有限生成的 A-模 M 都同构于如下形式的直和

$$M \simeq A^n \oplus A/a_1A \oplus \cdots \oplus A/a_mA$$

其中 n 是一个非负整数，通常称为 M 的秩，而 a_i 属于 A。此外，n 是唯一确定的；若要求它们为首一多项式，且对于所有 i，a_i 整除 a_{i+1}，则 a_i 也唯一确定。

特别地，如果M 是有限的，那么n 必为零，且M 同构于$A/a_1A \oplus \cdots \oplus A/a_mA$。由乘积$a_1 \cdots a_m$生成的理想不依赖于这种表示：它就是所谓的欧拉–庞加莱特征或*Fitting* 理想，即M[的特征 Lan02，第 3 章，第 § 8] 节。本文中我们将始终用 $|M|$ 表示它，并以此衡量M的大小。与数域情形类似，它就是对应的基数。

2 探索 Carlitz 模

Drinfeld 模的第一个实例由 Leonard Carlitz 于 1935年提出[Car35]。当时，他的工作鲜少受到关注，几乎被遗忘，直到20世纪70年代 Drinfeld 的研究问世后才重新受到关注 [Dri77]。Carlitz 的构造如今称为*Carlitz* 模。我们通过*Carlitz* 指数 来说明引入它的动机：在特征p下，借助与特征 0 下经典指数函数之间的类比与差异来展开。以下内容主要受[Tha04, § 2.1], 启发，并补充了一些细节。

2.1 寻找一个指数函数

Carlitz 模理论的出发点，是希望在函数域中找到圆分理论的类比。回顾一下，在经典数论中， $\mathbb{Q}$ 的分圆扩张是形如 $\mathbb{Q}(\zeta_n)$ 的扩张，其中 ζ_n 是n次本原单位根，且$n \geqslant 2$ 为整数。理解 ζ_n有多种方式。其中一种是从解析角度出发，通过经典指数函数 $\exp : \mathbb{C} \to \mathbb{C}$:

$$\zeta_n = \exp\left(\frac{2i\pi}{n}\right).$$

构造相关的$K = \mathbb{F}_q(T)$ 分圆扩张的一种方法，是推广上述构造。于是，我们要寻找一个函数$e : C_\infty \to C_\infty$，使它在我们的设定中发挥指数函数的作用。这也将引导我们定义一个与 π类似的概念。

定义经典指数函数 $\exp$ 的第一种方法，是通过它的微分方程 $\exp' = \exp$。该方程的幂级数解必然具有$c\sum_{n\geqslant 0} x^n\, n!$ 的形式，其中c是某个常数。然而，这在C_∞ 中没有意义，因为当$n \geqslant p$时，$\overline{n!} = 0$。理解指数函数的第二种方法是通过它的函数方程

$$\exp(x+y) = \exp(x)\exp(y).$$

遗憾的是，这种方法再次行不通。事实上，任何定义在C_∞ 上且满足上述函数方程的函数 e ，也会满足$e(0) = e(0)^2,$，因此$e(0) \in \{0,1\}$。由于$e(0) = e(px) = e(x)^p$，这是因为 C_∞ 的特征为p，最终可推得e 恒等于零或恒等于一。

这个后来证明可行、最初由 Carlitz 提出的想法，是利用特征p 下存在加性函数这一事实，并通过将右侧的乘积替换为和来修改函数方程：现在我们要寻找满足下式的函数e : $C_\infty \to C_\infty$

$$\forall x, y \in C_\infty, \quad e(x+y) = e(x) + e(y),$$

也就是说，*</style}*就是加性函数。由于我们的情形本质上不仅具有加性，而且是-线性的（所有对象都定义在 上），因此我们将更具体地关注 -线性函数e。

与经典指数函数的情形一样，我们预期函数e 是整函数，也就是说，它由一个在C_∞上处处收敛的幂级数给出。超度量分析中的一个标准结果（在 [Pap23，第 2.7 号命题12], 中回顾）指出，任意非常数整函数$f : C_\infty \to C_\infty$ 都是满射。因此，我们的指数函数e也将是满射。令 Λ 为其零点集。它是C_∞中的离散 $\mathbb{F}_q$-线性子空间，也就是说，它与C_∞ 中任意正半径闭球的交集都是有限集。如果这样的函数e 存在，我们便得到如下形式的 $\mathbb{F}_q$-向量空间正合列

$$0 \longrightarrow \Lambda \longrightarrow C_\infty \xrightarrow{e} C_\infty \longrightarrow 0, \tag{1}$$

这需要与经典指数函数的 $\mathbb{Z}$-模正合列进行比较

$$0 \longrightarrow 2i\pi\mathbb{Z} \longrightarrow \mathbb{C} \xrightarrow{\exp} \mathbb{C}^\times \longrightarrow 0. \tag{2}$$

比较这两个正合列，可以进一步推测 Λ 应该是什么。事实上，回想一下，在我们的情形中， $\mathbb{Z}$ 的对应物是环 $A = \mathbb{F}_q[T]$。因此，我们的目标是

将 Λ 表示为秩 1 的 A-格 $\Lambda = \tilde{\pi}$A，它由某个常数 $\tilde{\pi}$ 生成，而这个常数仍有待确定。此外，类比来看，我们希望 (1) 是 A-模的正合列，其中需要在 Λ 以及 C_∞ 的两个副本上定义某些 A-模结构。首先，我们需要将 $e : C_\infty \to C_\infty$ 理解为 A-模同态。我们已经知道，对于 C_∞ 中任意的 x 和 y，都有 $e(x + y) = e(x) + e(y)$。然而，对于 $a \in A$，我们不能令 $e(az) = ae(z)$，因为函数 $z \mapsto e(az)$ 和 $z \mapsto ae(z)$ 的零点集并不相同。Carlitz 的这一思想是 Drinfeld 模理论的核心：为陪域中的 C_∞ 副本赋予一种与 e 相容的新 A-模结构。

注记 2.1。继续之前，我们强调一下它与经典指数函数的相似之处，参见公式 (2)：后者的陪域不是 $\mathbb{C}$，而是配备了乘法结构的 $\mathbb{C}^\times$。在函数域的情形下，也需要改变陪域上的结构，但修改方式有所不同：我们保留加法结构，但改变 A 的作用。

具体而言，对于任意多项式 $a \in A$，我们寻找如下形式的函数方程

$$\forall z \in C_\infty, \quad e(az) = \phi_a(e(z)) \tag{3}$$

其中 $\phi_a : C_\infty \to C_\infty$ 是一个待确定的函数（取决于 a），它将在 C_∞ 上定义一种新的 A-模结构，记作 ${}^{\phi}C_\infty$，其运算规则为

$$\forall a \in A, \forall z \in C_\infty, \quad a \star z = \phi_a(z).$$

由此我们将得到一族由 A-模构成的交换图：

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \Lambda & \longrightarrow & C_\infty & \xrightarrow{e} & {}^{\phi}C_\infty & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \mathrm{mult}_a} & & \downarrow{\scriptstyle \mathrm{mult}_a} & & \downarrow{\scriptstyle \phi_a} & & \\ 0 & \longrightarrow & \Lambda & \longrightarrow & C_\infty & \xrightarrow{e} & {}^{\phi}C_\infty & \longrightarrow & 0 \end{array}$$

其中 mult_a 表示通常的乘法，即乘以 $a \in A$。

2.2 Carlitz 模的解析构造

2.2.1 为函数 e 寻找一个公式

现在我们旨在构造函数 e，使其具有第 2.1 小节中强调的性质。具体来说，我们固定一个形如 $\Lambda = cA$ 的秩为 1 的 A-格，其中 $c \in C_\infty^\times$，并寻找一个 $\mathbb{F}_q$-线性整函数 $e_\Lambda : C_\infty \to C_\infty$，其核为格 Λ。

为了构造 e_Λ，我们回顾超度量分析中的另一条标准结果：任意整函数 $f : C_\infty \to C_\infty$ 都由其按重数计数的零点集唯一确定，但相差一个非零常数；这是超度量版本的魏尔斯特拉斯“准备定理”的推论（更多细节见 [Pap23, § 2.7.2] ）。

在我们的情形中，最终得到如下表达式

$$e_\Lambda(z) = z \prod_{\lambda \in \Lambda \setminus \{0\}} \left(1 - \frac{z}{\lambda}\right). \tag{4}$$

上述乘积确实收敛到一个 $\mathbb{F}_q$-线性整函数 e_Λ，这是由 Λ 在 C_∞ [中的离散性所致 Pap23，命题 5.1。3]。

2.2.2 在C_∞上重新定义A-模

现在我们来说明函数方程 (3) 中态射 ϕ_a 的构造。首先，我们注意到，由于 $A = \mathbb{F}_q[T]$ 是由 T 在 $\mathbb{F}_q$ 上生成的，只需知道不定元 T 对应的 ϕ_T，便足以还原所有函数 ϕ_a。例如，我们有，

$$\phi_{T^2}(e(z)) = e(T^2 z) = e(T(Tz)) = \phi_T(e(Tz)) = (\phi_T \circ \phi_T)(e(z)),$$

通过同一化可得 $\phi_{T^2} = \phi_T \circ \phi_T$。更一般地，对于任意整数$m \geqslant 1$，我们得到

$$\phi_{T^m} = \underbrace{\phi_T \circ \cdots \circ \phi_T}_{m \text{ times}}.$$

利用e_Λ的 $\mathbb{F}_q$-线性，函数 ϕ_a 可通过对 ϕ_{T^m}取适当的 $\mathbb{F}_q$-线性组合得到。

现在我们专注于 ϕ_T的构造。我们知道，映射$z \mapsto e_\Lambda(Tz)$ 定义了一个零点集为 ${}^1{}_T\Lambda$ 且所有零点均为单零点的整函数。我们来考察映射

$$z \mapsto \prod_{\lambda \in \frac{1}{T}\Lambda/\Lambda} (e_\Lambda(z) - e_\Lambda(\lambda)).$$

回忆一下，e_Λ 的核为 Λ，因此$e_\Lambda(\lambda)$ 对 $\lambda \in {}^1{}_T\Lambda/\Lambda$是良定义的。注意到 $\mathrm{Card}\left({}^1{}_T\Lambda/\Lambda\right) = q$，我们看到上述乘积是有限的，并在$e_\Lambda(z)$ 中定义了一个次数为q的多项式。由于e_Λ 是整函数，它也定义了一个整函数。此外，其零点集为 ${}^1{}_T\Lambda$，且所有零点均为单零点。因此，存在$k \in C_\infty^\times$ 使得 [-]

$$e_\Lambda(Tz) = k \prod_{\lambda \in \frac{1}{T}\Lambda/\Lambda} (e_\Lambda(z) - e_\Lambda(\lambda)). \tag{5}$$

鉴于我们的目标是得到 $\phi_T(e_\Lambda(z)) = e_\Lambda(Tz)$，于是我们定义

$$\phi_T(x) = k \prod_{\lambda \in \frac{1}{T}\Lambda/\Lambda} (x - e_\Lambda(\lambda)) \in C_\infty[x]. \tag{6}$$

由如下规则定义的 A-模结构作用在 C_∞ 上

$$\forall a \in A, \forall z \in C_\infty, \quad a \star z = \phi_a(z) \tag{7}$$

如前所述，记作 ${}^\phi C_\infty$。

由于零点集 ${}^1\mathrm{T}\Lambda/\Lambda$是 C_∞ 中的一维 $\mathbb{F}_q$-线性子空间，我们推得 $\phi_T(\mathrm{x})$ 是一个次数为 q 的 $\mathbb{F}_q$- 线性多项式，即它具有如下形式：$\phi_T(\mathrm{x}) = \mathrm{k}_1\mathrm{x} + \mathrm{k}_2\mathrm{x}^q$，其中 $\mathrm{k}_1, \mathrm{k}_2 \in \mathrm{C}_\infty$ 且 $\mathrm{k}_2 \neq 0$。由方程（4），我们得到估计 $\mathrm{e}(\mathrm{z}) = \mathrm{z} + \mathrm{O}(\mathrm{z}^2)$。将函数方程 $\mathrm{e}_\Lambda(\mathrm{Tz}) = \phi_T(\mathrm{e}_\Lambda(\mathrm{z}))$ 中关于 z 的系数对应起来，得到 $\mathrm{k}_1 = \mathrm{T}$。类似地，将方程（6）中关于 x^q 的系数对应起来，可得 $\mathrm{k}_2 = \mathrm{k}$。因此，我们得到如下简洁公式：

$$\phi_T(x) = Tx + kx^q.$$

2.2.3 格的归一化 Λ

我们仍然不知道常数k 是什么，但事实证明，我们可以通过重新缩放格 Λ来自由选择它的值。事实上，如果我们不从 Λ开始，而是从$u\Lambda$

对于$u \in C_\infty^\times$，我们得到指数函数$e_{u\Lambda}$，它与原指数函数e_Λ之间满足以下关系

$$e_{u\Lambda}(z) = ue_\Lambda(z/u).$$

事实上，两边的函数具有相同的零点集和重数，且其展开式中的首项相同，均为z。我们得到的与格$u\Lambda$相关联的多项式$\phi_T^{u\Lambda}$的最终公式为

$$\phi_T^{u\Lambda}(x) = Tx + u^{1-q}kx^q.$$

标准做法是将我们的指数映射标准化，最终得到标准化形式$\phi_T(x) = Tx + x^q$。

相应的格通常记作$\tilde{\pi}A$；此时，常数$\tilde{\pi}$被理解为$2i\pi$在函数域中的类比（例如参见[Pap23，第317]页）。采用这种标准化后，我们得到 Carlitz 指数映射，记作e_C，其核为$\tilde{\pi}A$，并满足函数方程

$$\forall z \in C_\infty, \quad e_C(Tz) = \phi_T(e_C(z)) = Te_C(z) + e_C(z)^q. \tag{8}$$

采用这种选择的另一个优点是，e的系数全都是有理函数，也就是说，它们是K中的元素。利用函数方程 (8) 可以迭代计算这些系数（更多细节见第 3.3 小节）。

SageMath 示例 2.1。SageMath 提供了直接计算 Carlitz z 指数函数。

```
sage: eC = carlitz_exponential(A, prec=100)
sage: eC
z + (1/(T^7 + 6*T))*z^7 + (1/(T^98 + 6*T^56 + 6*T^50 + T^8))*z^49 + O(z^100)
```

现在我们可以验证函数方程：

```
sage: z = parent(eC).gen()
sage: eC(T*z) == T*eC + eC^7
True
```

次数为q的多项式$\phi_T(x) = Tx + x^q$以及后续所有函数ϕ_a共同构成所谓的*Carlitz*模。

SageMath 示例 2.2。我们在$\mathbb{F}_7$上实例化 Carlitz 模，并计算$a = T^2 + T + 1$对应的ϕ_a。

```
sage: φ = CarlitzModule(A)
sage: φ(T^2 + T + 1)
τ^2 + (T^7 + T + 1)*τ + T^2 + T + 1
```

在上述输出中，τ表示 Frobenius 映射$x \mapsto x^q$。这一记法在 Drinfeld 模理论中至关重要，将在第 3.1 小节中作更详细的解释。

根据 Carlitz 的一项工作[Car35]，，可以推导出以下结果

$$\tilde{\pi} = T\sqrt[q-1]{-T}\prod_{i=1}^{+\infty}\left(1 - \frac{1}{T^{q^i-1}}\right)^{-1}. \tag{9}$$

尽管我们用不到它，但我们还要提到，Wade [Wad41] 证明了$\tilde{\pi}$在K上是超越的。

2.3 圆分理论的应用

构造 Carlitz 指数的一个动机，是在函数域框架下寻找分圆理论的类比。经典地说，分圆域是通过添加 n 次单位根而得到的域（其中 $n \geqslant 2$ 为一个整数），即 群态射 $\mathbb{C}^\times \to \mathbb{C}^\times$ 的核，$x \mapsto x^n$。在函数域的情形下，这些态射的类比是定义 Carlitz 模的映射 ϕ_a。因此，我们自然会考虑扩张 $K(\phi[a])/K$，其中，按定义，

$$\phi[a] = \left\{ z \in {}^{\phi}C_\infty \,,\ a \star z = \phi_a(z) = 0 \right\}.$$

这就是所谓的 Carlitz 模的 a-挠，即 ${}^{\phi}C_\infty$ 的 a-挠子模，因此也是 ${}^{\phi}C_\infty$ 的一个 A-子模。

定理 2.2（Carlitz，参见 [Ros02，命题 12。5]）。对于所有 $a \in A$，扩张 $K(\phi[a]) / K$ 都是伽罗瓦扩张，其伽罗瓦群与 $(A/aA)^\times$ 典范同构。

证明概要。映射 $\alpha : \mathrm{Gal}(K(\phi[a])/K) \to (A/aA)^\times$ 的构造与经典情形类似。设 σ 是 $K(\phi[a])$ 上保持 K 不变的一个自同构。那么 σ 作用于 $\phi[a]$，，因为后者是多项式 ϕ_a 的根集。接着注意到，$\phi[a]$ 是 A/aA 上的秩 1 自由模，且 σ 线性作用。因此，σ 必须通过乘以 A/aA 中的一个元素来作用；由于 σ 是同构，该元素必须可逆。由此得到一个唯一确定的标量，属于 $(A/aA)^\times$，按定义即为 $\alpha(\sigma)$。

证明 α 的单射性是例行的：由于根据定义，$K(\phi[a])$ 由 $\phi[a]$，的元素在 K 上生成，因此一个 $K(\phi[a])$ 的 K-自同构由其在 $\phi[a]$ 上的作用唯一确定。相反，α 的满射性更难证明；要证明这一点，基本上需要研究 ϕ_a 的因式分解性质。完整证明请参见 [Ros02, Theorem 12.8]。 □

在数域的情形下，关于分圆扩张的一个显著结果是，它们涵盖了 $\mathbb{Q}$ 的所有阿贝尔扩张：这就是著名的克罗内克–韦伯定理。Hayes [Hay74] 在函数域的背景下证明了这一结果的类似结论。不过，这种情形稍微更微妙，因为以下两个事实都与分歧有关。首先，与 $\mathbb{Q}$ 相反，基域 $K = \mathbb{F}_q(T)$ 确实存在处处非分歧扩张：这些扩张的形式为 $F(T)$，其中 F 是 $\mathbb{F}_q$ 的有限扩张。这些扩张是阿贝尔扩张，但并非形如 $K(\phi[a])$。第二个困难来源是，Carlitz 的构造 $K(\phi[a])$ 只产生在 ∞ [Hay74, Theorem 3.1] 处温和分歧的扩张。从某种意义上说，这是由于我们选择了 $\mathbb{F}_q(T)$ 中的整数环 $\mathbb{F}_q[T]$。例如，如果我们一开始选择 $]T^{\mathbb{F}_q}[^{1}$ 而不是 $]T, \mathbb{F}_q[$，最终得到的将是另一族分圆扩张，它们在零点处温和分歧。在 [Hay74], Hayes 证明，将这两族扩张与前面讨论过的处处非分歧扩张结合起来，克罗内克–韦伯定理的类似结论便成立。

Hayes 定理是一项杰出的成果，充分彰显了 Carlitz 模及其后续的 Carlitz 圆分扩张在函数域算术理论中的关键作用。此外，Hayes 定理常被视为函数域背景下类群理论显式版本的开端。

2.4 Carlitz zeta 函数

我们之前已经看到，经典指数函数有一个有趣且相关的函数域类比。事实证明，这并非孤例：实际上，

一些值得关注的算术函数在函数域世界中也有对应物（参见例如， [Pap23，第 5.4] 节）。

作为一个例子，这里给出黎曼 ζ 函数在函数域中的对应物，即所谓的 *Carlitz ζ 函数*。它定义为

$$\begin{aligned} \zeta_C : \quad \mathbb{N} &\to K_\infty \\ s &\mapsto \sum_{\mathfrak{a}\in A_+} \frac{1}{\mathfrak{a}^s}, \end{aligned} \tag{10}$$

其中，A_+ 表示由首一多项式构成的$A = \mathbb{F}_q[T]$ 子集。

与数域的情形类似，Carlitz ζ 函数可以表示为欧拉乘积

$$\zeta_C(s) = \prod_{\mathfrak{p}} \frac{1}{1-\mathfrak{p}^{-s}}, \tag{11}$$

其中，乘积遍历A的所有不可约首一多项式 $\mathfrak{p}$。与经典情形一样，在表达式 (10) 和 (11) 之间转换，归根结底就是写出每个 $\mathfrak{a} \in A_+$ 分解为不可约因子的形式，并对所得公式进行因式分解。

SageMath 示例 2.3。 下面的代码可直接计算 Carlitz ζ 函数的值。

```
sage: carlitz_zeta(A, s=1, prec=40)
1 + 6*T^-7 + 6*T^-13 + 6*T^-19 + 6*T^-25 + 6*T^-31 + 6*T^-37 + O(T^-40)
sage: carlitz_zeta(A, s=2, prec=40)
1 + T^-14 + 2*T^-20 + 3*T^-26 + 4*T^-32 + 5*T^-38 + O(T^-40)
sage: carlitz_zeta(A, s=6, prec=100)
1 + T^-42 + 6*T^-48 + T^-84 + 6*T^-90 + O(T^-100)
```

Carlitz 在 [Car35] 中证明，当s 是$q-1$的倍数时，有

$$\zeta_C(s) = \frac{\mathrm{BC}_s}{\Pi(s)} \cdot \widetilde{\pi}^s, \tag{12}$$

它似乎是欧拉公式的一个类比，欧拉公式给出了黎曼 ζ 函数在正偶数处的值。在公式 (12) 中，常数 $\widetilde{\pi}$ 是我们在第 2.2 小节末尾遇到的 Carlitz 周期。记号 BC_s 指的是伯努利–Carlitz 数，而 $\Pi(s)$ 是 Carlitz 阶乘 [Gos96，第 9]章。

SageMath 示例 2.4。 我们使用由公式 (9) 推导出的以下关于 $\widetilde{\pi}^{q-1}$ 的显式同余式，验证 $s = q-1$ 时的公式 (12)：

$$\widetilde{\pi}^{q-1} = -\frac{T^q}{\prod_{i=1}^{+\infty}\left(1-\frac{1}{T^{q^i}-1}\right)^{q-1}} \equiv -\frac{T^q}{\prod_{i=1}^{n-1}\left(1-\frac{1}{T^{q^i}-1}\right)^{q-1}} \pmod{T^{q+1-q^n}}.$$

```
sage: # 这里q = 7sage: BC6 = carlitz_bernoulli(A, 6)
sage: Π6 = carlitz_factorial(A, 6)
sage: π6 = -T^7 / prod((1 - T^(1-7^i))^6 for i in range(1, 3)) + O(1/T^100)
sage: BC6 / Π6 * π61 + T^-42 + 6*T^-48 + T^-84 + 6*T^-90 + O(T^-100)
```

3 Drinfeld 模及其 Anderson 动机

在第 2 节中，我们通过显式构造同构$C_\infty/\ \tilde{\pi}A\ \to\ ^{\phi}C_\infty$，仿照标准双射 $\mathbb{C}/2i\pi\mathbb{Z}\ \exp\ \longrightarrow \mathbb{C}^\times$，将指数函数的构造推广到了函数域情形。在经典情形中，对秩为 2 的格取商也十分有用，因为这会引出椭圆曲线理论。此时，指数函数由 Weierstraß $\wp$ 函数取代，从而诱导出映射

$$\begin{array}{rcl} \mathbb{C}/\Lambda & \to & \mathbb{P}^2(\mathbb{C}) \\ z & \mapsto & (\wp(z) : \wp'(z) : 1), \\ 0 & \mapsto & (0 : 1 : 0), \end{array}$$

它将 $\mathbb{C}/\Lambda$ 与椭圆曲线的复点对应起来。在函数域的世界中，也有类似的构造：可以考虑一般格 $\Lambda \subset C_\infty$，以及商 C_∞/Λ，它具有自然的 A-模结构。这里，我们要求 Λ 是离散的，以便在商上获得适当的拓扑，尽管它可以具有任意秩，因为与经典情形不同，扩张 C_∞/K 是无限的。尽管如此，我们在第 2.2 小节中进行的所有构造都可以原样推广：对于每个这样的格 Λ（秩任意），都可以关联一个指数映射 e_Λ，其定义如下

$$\begin{array}{rccl} e_\Lambda : & C_\infty & \to & C_\infty \\ & z & \mapsto & z \displaystyle\prod_{\lambda \in \Lambda \setminus \{0\}} \left(1 - \frac{z}{\lambda}\right), \end{array}$$

它处于正合列中

$$0 \longrightarrow \Lambda \longrightarrow C_\infty \xrightarrow{e_\Lambda} C_\infty \longrightarrow 0.$$

此外，对于每个 $a \in A$，函数 e_Λ 满足函数方程

$$e_\Lambda(az) = \phi_a(e_\Lambda(z)),$$

其中 ϕ_a 是形如 $\phi_a(x)\ = ax\ + c_1 x^q + \cdots + c_r x^{q^r}$ 的多项式（其中 $c_i \in C_\infty$ 和 $c_r \neq 0$）由下式显式定义

$$\phi_a(x) := ax \prod_{\lambda \in (\frac{1}{a}\Lambda/\Lambda)^\times} \left(1 - \frac{x}{e_\Lambda(\lambda)}\right). \tag{13}$$

族（ϕ_a）$_{a\in A}$ 赋予C_∞ 一个A-模结构，记为 $^{\phi}C_\infty$。对于任意$a\ \in A$ 和$z\ \in\ ^{\phi}C_\infty$，该结构由 $a \star z\ =\ \phi_a$（z）给出，如公式（7）所示。这正是我们所称的秩为r、定义在C_∞上的 Drinfeld 模。借助指数映射e_Λ，我们得到A-模$C_\infty/\Lambda \simeq\ ^{\phi}C_\infty$之间的同构。

与椭圆曲线的情形类似，来自 ϕ_a 的描述有一个决定性优势，那就是它的代数性：ϕ_a 并非一般的解析函数，而是多项式。因此，它们在一般的基上也有意义，无需再要求在 C_∞ 上工作。Drinfeld 模的一般定义正是基于这一基本观察。我们将在对 Ore 多项式作一些介绍之后，于第 3.2 小节中精确写出该定义；相关介绍见第 3.1 小节。接着，我们会在第 3.3 小节中比较代数定义与解析定义。最后，在第 3.4 小节中，我们将说明如何为一个 Drinfeld 模关联一个 Anderson 模：这将在后续阶段使我们能够使用特征多项式和约化定理。

3.1 Ore 多项式

如上所述，Drinfeld 模的代数定义将由多项式 $\{\phi_a\}_{a\in A}$ 这一数据集来刻画。在这个预备小节中，我们将介绍由这些多项式构成的环，并归纳其基本性质。

显然，式（13）中定义的函数 ϕ_a 具有鲜明的形式：它们是 $\mathbb{F}_q$-线性函数，也就是说，只包含形如 $c_i x^{q^i}$ 的项，其中 $i \in \mathbb{N}$。从某种意义上说，ϕ_a 是 q-Frobenius 自同态 $x \mapsto x^q$ 的多项式。下面定义的 Ore 多项式这一概念刻画了这一性质。

定义 3.1（Ore 多项式）. 设 F 是一个 $\mathbb{F}_q$-代数。记 $F\{\tau\}$ 为 Ore 多项式（亦称斜多项式或扭曲多项式）构成的非交换环。

$$F\{\tau\} = \left\{ \sum_{i=0}^{n} c_i \tau^i \,\middle|\, n \geqslant 0, c_i \in F \right\},$$

其加法采用经典的加法运算，乘法定义为 $\tau c = c^q \tau$，对每个$c \in F$均成立。

记 $f = \sum_i c_i \tau^i$，定义 τ-次数（分别为 τ-赋值）为 f 中使 $c_i \neq 0$ 成立的最大（分别为最小）整数 i。

在定理 3.1 中，字母 τ 只是一个形式变量，并无其他含义。不过，当然应将其理解为 Frobenius 自同态：如此一来，Ore 多项式便对应于先前所述的 q-Frobenius 多项式。非交换乘法法则也令人联想到这种解释；事实上，先乘以标量 c，再施加 q-Frobenius，等同于先施加 q-Frobenius，再乘以 c^q。

SageMath 示例 3.1。在 SageMath 中，Ore 多项式环可以按如下方式构造。

```
sage: F.<z> = F7.extension(2)
sage: frob = F.frobenius_endomorphism()
sage: Ftau.<τ> = OrePolynomialRing(F, frob)
sage: Ftau
Ore Polynomial Ring in τ over Finite Field in z of size 7^2 twisted by z
    |--> z^7
```

我们来展示 $F\{\tau\}$ 的非交换性：

```
sage: z * τ
z*τ
sage: τ * z
(6*z + 1)*τ
```

Ore 多项式的一个优点是，尽管其环是非交换的，但相对于 τ次数 [Ore33b]，它是左欧几里得的。这意味着可以进行右欧几里得除法，而且所有左理想都有唯一的首一生成元。对于任意非空的 Ore 多项式族 S，可以计算它们的右最大公因子（简称右最大公因子）$\mathrm{rgcd}(S)$ 以及它们的左最小公倍元（简称左最小公倍元）$\mathrm{llcm}(S)$。实际应用中，可以使用长除法和欧几里得算法的变体；复杂度方面的论述见 [LS24, § 3.1]。更高级的基本运算

已在 [CLB17b, CLB17a] 中介绍：这些方法基于更快速的算法，用于将系数属于有限域的两个 Ore 多项式相乘。

SageMath 示例 3.2。右最大因子可以轻松地按如下方式计算：

```
sage: f = (1 + τ) * (z + τ)
sage: g = (1 - τ) * (z + τ)
sage: f.right_gcd(g)
τ + z
```

需要强调的是，左侧存在公共因子并不意味着右最大公因子非平凡：

```
sage: f = (1 + τ) * (z + τ)
sage: g = (1 + τ) * (z - τ)
sage: f.right_gcd(g)1
```

3.1.1 Ore 多项式的核

为了继续将 τ 识别为q-Frobenius，我们将$F\{\tau\}$ 中的 Ore 多项式视为实际的自同态，即定义在F的可分闭包F^s 上的自同态：对于元素$nf = \sum c_i \tau^i \in F\{\tau\}$，我们关联变换$i=0$

$$\begin{aligned} F^s &\to F^s \\ x &\mapsto \sum_{i=0}^{n} c_i x^{q^i}, \end{aligned}$$

尽管稍微滥用了记号，我们仍将其记为f。该变换是$\mathbb{F}_q$-线性的，且是F-代数的，因为它由F上的一个多项式给出。可以证明，F^s 上的任意 $\mathbb{F}_q$-线性代数自同态都来自一个唯一确定的 Ore 多项式 [Pap23，引理 3.1.4]。下面的命题也很好地展示了这种对应关系。

命题3.2。 存在一个双射：

$$\begin{array}{ccc} \left\{ \begin{array}{c} \text{Ore polynomials } f \in F\{\tau\} \\ \text{with constant term 1} \end{array} \right\} & \longrightarrow & \left\{ \begin{array}{c} \text{finite dimensional } F\text{-linear subspaces} \\ V \subset F^s \text{ stable by } \mathrm{Gal}(F^s/F) \end{array} \right\} \\ f & \longmapsto & \ker f. \end{array}$$

关于该命题的证明，请参见 [Gos96, § 1.2] 。这里我们仅指出，逆双射可以明确描述如下。给定一个子空间 $V \subset F^s$，我们构造经典多项式

$$\widetilde{f}(x) = x \prod_{v \in V \setminus \{0\}} \left(1 - \frac{x}{v}\right).$$

$\widetilde{}$在伽罗瓦作用下保持稳定，确保f 的系数属于 F。此外，经过计算可知，它定义了一个 $\mathbb{F}_q$-线性函数。因此，经典多项式$\widetilde{f} \in F[x]$ 可以视为 $F\{\tau\}$中的 Ore 多项式。这个 Ore 多项式是 V 在定理 3.2 的双射下的原像。

命题 3.3。 定理 *3.2* 中的双射是递增的，具体而言，f 右整除 g 当且仅当$\ker f \subset \ker g$。这特别意味着，左侧 *Ore* 多项式的右最大公因子（分别为左最小公倍数）对应于右侧子空间的交集（分别为和）。

注 3.4. 在定理 3.2 中将讨论范围限制为常数项等于 1 的 Ore 多项式，这一点有两个重要原因。首先，这样可以对 Ore 多项式进行归一化，因为显然，f和cf（其中$c \in F^\times$）具有相同的核。其次，这样可以舍弃所有常数项为零的 Ore 多项式。事实上，我们注意到f 和 $f\tau$也具有相同的核，因为q-Frobenius 在F^s的每个伽罗瓦稳定 $\mathbb{F}_q$-线性子空间上都诱导出一个双射。

~注 3.5. 上述定义的多项式f 可以用初等对称函数表示。若将f 视为通常的多项式，它的大多数系数都为~零点；我们还希望定义f 的根—系数关系能表示为仅含核基元素的表达式。因此，我们引入以下对象。设整数$n \geqslant 0$，以及形式变量X_1,.....X_n、X。族$(X_1$,.....$X_n)$ 的*Moore* 行列式 定义为

$$\Delta(X_1, \ldots, X_n) = \det \begin{pmatrix} X_1 & \cdots & X_n \\ X_1^q & \cdots & X_n^q \\ \vdots & \vdots & \vdots \\ X_1^{q^{n-1}} & \cdots & X_n^{q^{n-1}} \end{pmatrix}.$$

它是关于 X_1,. . .、X_n 的一个多项式，由 Moore [Moo96] 引入，作为经典 *Vandermonde* 行列式 的一个 $\mathbb{F}_q$-线性类比。该多项式满足（参见 [Ore33a，定理 10]或 [Elk99，命题 1]）

$$\Delta(X_1, \ldots, X_n) = \prod_{i=1}^{n} \prod_{(k_1,\ldots,k_{i-1}) \in \mathbb{F}_q^{i-1}} \left(X_i + \sum_j k_j X_j \right),$$

这意味着，当且仅当 $\Delta(x_1, \ldots、x_n) = 0$时，族 $(x_1$,. . .、$x_n)$ 是 $\mathbb{F}_q$-线性相关的。特别地，如果 $(\omega_1$、...、$\omega_n)$ 是 $\ker f$的一个基，则单变量多项式 $\Delta(x$、ω_1、...、$\omega_n)$ 恰好在 $\ker f$ 上为零。重新归一化后，我们得到

$$\widetilde{f}(x) = \frac{\Delta(x, \omega_1, \ldots, \omega_n)}{\Delta(\omega_1^q, \ldots, \omega_n^q)}.$$

Sim同样，零点集为 $\ker f$ 的唯一首一可分多项式由 b 给出 y

$$\bar{f}(x) := \frac{\Delta(x, \omega_1, \ldots, \omega_n)}{\Delta(\omega_1, \ldots, \omega_n)}.$$

展开行列式，可以证明存在通用多项式$\lambda_0^{(n)}$、.....、$\lambda_n^{(n)} \in \mathbb{F}_q[X_1$,.....、$X_n]$，使得 $\bar{f}(x) = \sum_{i=0}^{n} \lambda^{(n)}{}_i x^{q^i}$。每个 $\lambda^{(n)}{}_i$都是次数为$q^n - q^i$的齐次多项式。总而言之，它们构成了 $\mathbb{F}_q$-线性初等对称函数集。

3.2 代数 Drinfeld 模

现在我们可以定义一般基上的 Drinfeld 模，该基可能不同于C_∞。这个定义具有代数性质。粗略地说，域F 上的 Drinfeld 模，是指在F上赋予一种A-模的代数结构。这里，代数性意味着对任意元素$a \in A$ 的乘法都由一个 Ore 多项式 $\phi_a \in F\{\tau\}$给出。

我们先介绍本文关注的基域。

定义 3.6. A-域 是一个域F，并配备环同态 $\gamma : A \to F$。F 的A–特征 是由 $\mathrm{char}_A(F) = \ker \gamma$ 定义的A 的理想。

在全文中，我们设$z = \gamma(T)$。由于我们假设$A = \mathbb{F}_q[T]$，，因此z 的数据完全确定了 γ。除了$F = C_\infty$之外，文献中考虑的最重要的A-域如下。

- F 是 $\mathbb{F}_q(T)$ 的有限扩张，且 $\gamma : A \to F$ 是典范嵌入（因此A-特征为零）；这种选择导向了有理 Drinfeld 模理论。
- F 是 $\mathbb{F}_q$ 的有限扩张，且 $\gamma : A \to F$ 是将F 表示为$A = \mathbb{F}_q[T]$ 之商的表示（因此A-特征非零，且它是F的定义多项式）；这种选择导向了有限Drinfeld 模理论。

我们将在第 5 节回到这两个特殊的基及其上的 Drinfeld 模。

定义 3.7。 一个*Drinfeld* 模定义在A-域(F, γ) 上，是一个 $\mathbb{F}_q$-代数同态

$$\begin{array}{rccc} \phi : & A & \to & F\{\tau\} \\ & a & \mapsto & \phi_a \end{array}$$

使得:

(i) 对于至少一个元素 $a \in A$， ϕ_a 非常数，

(ii) 对于所有 $a \in A$， ϕ_a 的常数项是 $\gamma(a)$。

定理 3.7 中的条件 (i) 并非必不可少：它只是排除平凡情形，而这些情形可能会在某些时候引发问题。另一方面，条件 (ii) 是一个归一化条件，它反映了指数映射在零点处的导数为 1 这一事实（参见方程 (13)）。从某种意义上说，它表示 ϕ_a 在切空间上的作用，即 $\phi_a(x)$ 的导数的作用，应当是乘以 a。这一要求是椭圆曲线理论（或者更一般地说，阿贝尔簇理论）中的一个标准事实：曲线上的乘以 a 总是通过乘以 a 这一标量乘法在李代数上作用。

备注 3.8。 也可以不借助 γ 来定义 Drinfeld 模，然后再通过令 $\gamma := \phi \bmod \tau$ 来定义 γ。不过，更标准的做法是像定理 3.7 中那样进行。这种观点还有一个优点，就是凸显了切向作用的重要性。

由于我们假设 $A = \mathbb{F}_q[T]$，，Drinfeld 模 ϕ 完全由 Ore 多项式 $\phi_T \in F\{\tau\}$ 确定。反过来，任意选取一个次数为正且常数项等于 z 的 ϕ_T，都会唯一确定一个定义在 A 上的 Drinfeld 模。

τ次的 ϕ_T 称为 ϕ的秩，记作r。对于任意$a \in A$，可以证明， ϕ_a 在 τ 中的次数等于$r\deg a$。

SageMath 示例 3.3。 在 SageMath 中，我们通过指定多项式环A 以及 ϕ_T 的系数来创建一个 Drinfeld模（回顾一下，在 SageMath 示例 3.1 中，z 被定义为 $\mathbb{F}_{7^2}$的生成元）。

```
sage: φ = DrinfeldModule(A, [z, z, z, z+1])
sage: φ
Drinfeld module T |--> (z + 1)*τ^3 + z*τ^2 + z*τ + z
```

```
sage: φ.rank()3sage: φ(T + 1)
(z + 1)*τ^3 + z*τ^2 + z*τ + z + 1
```

Drinfeld 模 $\phi: A \to F\{\tau\}$ 通过公式 $a \star x = \phi_a(x)$，为任意 F-代数$\mathcal{F}$ 赋予一个 A-模结构，其中 $a \in A$ 且 $x \in \mathcal{F}$。我们将用记号 ${}^{\phi}\mathcal{F}$表示 $\mathcal{F}$ 配备了这种奇异作用的[1]。

3.3 解析一致化

当 $F = C_\infty$时，我们对 Drinfeld 模有两种并行的观点：第一种是解析观点，如第 2 节及本节引言所述；第二种是代数观点，如第 3.2 小节所述。本文旨在调和这两种观点，并说明它们实际上定义的是同一类对象。

“解析到代数”这一方向已在第 3 节的引言中讨论过。我们将其概括为以下定理。

定理 3.9 ([Pap23，命题 5.2。2])。 设 Λ 是 C 中的一个离散 A-子模$_\infty$，并令

$$\begin{array}{rccc} e_\Lambda: & C_\infty & \to & C_\infty \\ & z & \mapsto & z\displaystyle\prod_{\lambda\in\Lambda,\lambda\neq 0}\left(1-\frac{z}{\lambda}\right) \end{array}$$

为相应的指数函数。则函数 e_Λ 是整函数、满射且 $\mathbb{F}_q$-线性的。其零点恰为 Λ，并且全都是单零点。此外，对于每个 $a \in A$，都存在唯一的 *Ore* 多项式 $\phi_a^\Lambda \in C_\infty\{\tau\}$，使得

$$\forall z \in C_\infty, \quad e_\Lambda(az) = \phi_a^\Lambda(e_\Lambda(z)). \tag{14}$$

最后，映射

$$\begin{array}{rccc} \phi^\Lambda: & A & \to & C_\infty\{\tau\} \\ & a & \mapsto & \phi_a^\Lambda \end{array} \tag{15}$$

是定义在 C_∞ 上的一个 *Drinfeld* 模，其秩等于 Λ 作为 A-模的秩。

相反方向的“从代数到解析”对应于 Drinfeld 模的所谓解析一致化定理。其表述如下。

定理 3.10。 设 $\phi: A \to C_\infty\{\tau\}$ 是 C_∞上的一个 *Drinfeld* 模。那么，存在一个格Λ 位于 C_∞ 中，使得 $\phi = \phi^\Lambda$。

[1]在文献中，我们常见到记号 $\phi(\mathcal{F})$；不过在本文中，为尽量避免混淆，我们倾向于使用 ${}^{\phi}\mathcal{F}$。

证明概要。 第一步是将指数函数 e_Λ 重构为 C_∞上的 Ore 级数，即 形如以下形式的一个元素

$$e_\Lambda = \sum_{n=0}^{\infty} c_n \tau^n \qquad (c_n \in C_\infty).$$

为了求出系数c_n，我们回到带有$a = T$的函数方程（14）。用我们的语言来说，它表示为 $e_\Lambda T = \phi_T e_\Lambda$，这是形式 Ore 幂级数环$C_\infty\{\{\tau\}\}$中的一个等式。写作

$$\phi_T = g_0 + g_1\tau + \cdots + g_r\tau^r \qquad (g_i \in C_\infty,\ g_0 = T)$$

然后比较系数（注意非交换关系），便得到递推关系

$$c_n = \frac{1}{T^{q^n} - T} \sum_{i=1}^{\min(n,r)} g_i c_{n-i}^{q^i}$$

由此可以递归地计算出所有c_n （从$c_0 = 1$开始）。最后，一旦知道函数e_Λ，就可以通过取其核来重构 Λ。证明的细节见 [Pap23，定理 5.2。8]。

□

定理 3.10 的证明为指数函数提供了一种代数视角，并且这一视角可推广到任意基的A-特征为零的情形。具体而言，若 $\phi : A \to F\{\tau\}$ 是(F,γ)上的 Drinfeld 模，则定义指数函数e_ϕ 为 Ore 级数

$$e_\phi = \sum_{n=0}^{\infty} c_n \tau^n$$

其中系数$c_n \in F$ 由递推关系确定

$$c_n = \frac{1}{z^{q^n} - z} \sum_{i=1}^{\min(n,r)} g_i c_{n-i}^{q^i}.$$

F 具有A-特征零这一事实确保分母

$$z^{q^n} - z = \gamma(T^{q^n} - T)$$

永不为零。

类似地，可以将对数 函数 $\ell_\phi = \sum_{n=1}^{\infty} \ell_n \tau^n \in F\{\{\tau\}\}$ 定义为方程 $\ell_\phi \phi_T = z\ell_\phi$的解。通过比较系数，我们现在得到关系

$$\ell_n = \frac{1}{z - z^{q^n}} \sum_{i=1}^{\min(n,r)} g_i^{q^{n-i}} \ell_{n-i},$$

这同样足以递归地计算所有 ℓ_n。除了这些恒等式之外，

$$\begin{aligned} e_\phi \gamma(a) &= \phi_a e_\phi, \\ \ell_\phi \phi_a &= \gamma(a)\ell_\phi, \end{aligned}$$

对于所有$a \in A$都成立，我们有$e_\phi \ell_\phi = \ell_\phi e_\phi = 1$ 在$F\{\{\tau\}\}$中的形式关系。

SageMath 示例 3.4。 指数函数和对数函数已在 SageMath 中实现。不过，由于 SageMath 中不存在 Ore 级数，结果以实际级数的形式给出，其中 τ^n 被x^{q^n}替代。

```
sage: ϕ = DrinfeldModule(A, [T, T, 1])
sage: exp = ϕ.exponential(prec=100, name='x')
sage: exp
x + (1/(T^6 + 6))*x^7 + ((T^42 + T + 6)/(T^91 + 6*T^49 + 6*T^43 + T))*x^49 +
     O(x^100)
sage: log = ϕ.logarithm(prec=100, name='x')
sage: log
x + (6/(T^6 + 6))*x^7 + ((T^7 + 6*T^6 + 1)/(T^55 + 6*T^49 + 6*T^7 + T))*x^49
     + O(x^100)
```

我们可以验证它们互为逆运算。

```
sage: exp(log)
x + O(x^100)
sage: log(exp)
x + O(x^100)
```

3.4 Drinfeld 模的实现：Tate 模与 Anderson 动机

Drinfeld 模的定义可能听起来相当令人困惑，因为它们无论如何都不是某个环上的模。更糟糕的是，它们不是 SageMath 意义下的“父对象”，也就是说，我们没有任何可以选取并进行操作的元素。

在本小节中，我们将解释如何把 Drinfeld 模与线性代数中的实际对象联系起来。除了让我们更容易理解之外，这还将使我们能够在之后轻松引入线性代数中的经典工具，例如特征多项式、约化定理等。

3.4.1 挠点与 Tate 模

我们将介绍的第一个构造是 Tate 模：在我们的语境中，它是椭圆曲线经典 Tate 模的直接类比。我们首先定义挠点。

定义 3.11。 设 $\phi: A \to F\{\tau\}$ 是定义在(F, γ)上的 Drinfeld 模。对于一个理想 $\mathfrak{a} \subset A$， $\mathfrak{a}$-挠 的 ϕ 定义为 ${}^{\phi}F^{s}$的 $\mathfrak{a}$-挠，即

$$\phi[\mathfrak{a}] = \left\{ x \in {}^{\phi}F^{s} \mid \forall a \in \mathfrak{a},\ \phi_a(x) = 0 \right\}.$$

注记 3.12。 由于在我们的设定中$A = \mathbb{F}_q[T]$， A 的每个理想 $\mathfrak{a}$ 都是主理想，即 $\mathfrak{a} = aA$，因此 $\mathfrak{a}$-挠就是 ϕ_a 的根的集合。多项式 ϕ_a 有时被称为 ϕ的a-除法 *Ore* 多项式。

$\mathfrak{a}$-挠 $\phi[\mathfrak{a}]$ 自然是 ${}^{\phi}F^{s}$ 的一个A-子模，它被 $\mathfrak{a}$湮没，因此是商环$A/\mathfrak{a}$上的一个模。此外，它带有伽罗瓦群 $\mathrm{Gal}(F^s/F)$的作用。由此得到伽罗瓦群 $\mathrm{Gal}(F^s/F)$的一个$A/\mathfrak{a}$-线性表示。

命题 3.13 ([Pap23，推论 3.5。3])。 设 $\phi: A \to F\{\tau\}$ 是秩为 r 的 *Drinfeld* 模。设 $\mathfrak{l}$ 是 A 的一个素理想，且不同于 ϕ的 A-特征。那么，对所有非负整数 n， $\phi[\mathfrak{l}^n]$ 都是 $A/\mathfrak{l}^n$上的秩为 r 的自由模。

注 3.14。 当 $\mathfrak{l} = \mathfrak{p}$ 等于 ϕ的A-特征时， $\phi[\mathfrak{p}^n]$ 仍然是 $\mathrm{A}A/\mathfrak{p}^n$ 上的自由模，但其秩总是小于r。亏格 $\mathrm{h}(\phi) := r - \mathrm{rk}^{A/\mathfrak{p}^n}(\phi[\mathfrak{p}^n])$不依赖于$n$ ，称为 ϕ的弗罗贝尼乌斯高度，通常简称高度。它也可以解释为 Ore 多项式 $\phi_{\mathfrak{p}}$ 的 τ-赋值除以 $\mathfrak{p}$的次数。这个高度概念不同于 Drinfeld 模所附带的其他高度。

取逆极限后，我们得到一族定义在$A_{\mathfrak{l}}$上的自由模。

定义 3.15。 设 $\phi : A \to F\{\tau\}$ 是一个 Drinfeld 模，并设 $\mathfrak{l}$是A的一个极大理想。 ϕ 在 $\mathfrak{l}$ 处的*Tate* 模为

$$\mathbf{T}_{\mathfrak{l}}(\phi) = \varprojlim_{n\in\mathbb{N}} \phi[\mathfrak{l}^n].$$

由此可知，当 $\mathfrak{l}$ 不同于 ϕ的A-特征时， ϕ 在 $\mathfrak{l}$ 处的 Tate 模在$A_{\mathfrak{l}}$ 上秩为r ；否则，其秩为$r - h(\phi)$ 。

3.4.2 Anderson 动机

第二个重要的构造是 Anderson 动机。正如我们将看到的，这是一个非常强大的概念，它涵盖了 Drinfeld 模中所包含的全部信息，同时也易于处理和运用，尤其是从算法的角度来看。从更抽象的观点而言，按照 Grothendieck 的构想，Anderson 动机应被视为 Drinfeld 模的动机。迄今为止，在椭圆曲线和阿贝尔簇的框架下，尚无已知的类似概念。

定义 3.16。 设 $\phi : A \to F\{\tau\}$ 是一个 Drinfeld 模。其*Anderson* 动机 $\mathbf{M}(\phi)$ 是$F\{\tau\}$ ，并带有以下附加结构:

- 一个由下式给出的 A-模结构:

$$\forall a \in A, \forall m \in \mathbf{M}(\phi), \quad a \bullet m = m\phi_a,$$

其中右边的乘积是$F\{\tau\}$中的乘法,

- 一个由下式给出的F-模结构:

$$\forall \lambda \in F, \forall m \in \mathbf{M}(\phi), \quad \lambda \bullet m = \lambda m,$$

- 一个算子 $\tau_{\mathbf{M}(\phi)} : \mathbf{M}(\phi) \to \mathbf{M}(\phi)$ ，定义为 $m \mapsto \tau m$。

下文中，我们将省略符号 $\bullet$ ，只写作 am 或 λm。注意，同时具有A-模和F-模结构，等价于成为$A \otimes_{\mathbb{F}_q} F$上的模。此外，由于在我们的设定中$A = \mathbb{F}_q[T]$ ，因此有$A \otimes_{\mathbb{F}_q} F \simeq F[T]$。所以，动机$\mathbf{M}(\phi)$ </style}不过是一个配备了额外自同态 的$\mathrm{F}[T]$ 模。还要注意，后者是半线性的，具体而言，

$$\forall f \in F[T], \forall m \in \mathbf{M}(\phi), \quad \tau_{\mathbf{M}(\phi)}(fm) = \tau(f)\,\tau_{\mathbf{M}(\phi)}(m),$$

其中 $\tau : F[T] \to F[T]$ 是环同态，在T 上作用平凡，并将所有系数提升到q次幂。

命题 3.17。 若 $\phi : A \to F\{\tau\}$ 是一个秩为 r 的 *Drinfeld* 模，则 $\mathbf{M}(\phi)$ 是 $F[T]$ 上的秩为 r 的自由模，其基为 $(1, \tau, \ldots, \tau^{r-1})$。

证明。 我们说明如何将元素 $m \in \mathbf{M}(\phi)$ 按给定的基分解。回忆一下，根据定义，m 是 $F\{\tau\}$中的一个 Ore 多项式。由于后者是右欧几里得的，我们可以将m 按基 ϕ_T 分解如下：

$$m = m_0 + m_1\phi_T + \cdots + m_k\phi_T^k,$$

对于某个非负整数k 以及某些唯一确定的m_0,....., $m_k \in F\{t\}$，其次数至多为$r-1$，其中 r $\deg_\tau \phi_T$ 是 ϕ的秩。事实上，m_0 是m 被 ϕ_T 右除法所得的余式，接下来的m_i 则通过依次对商进行除法而类似地得到。现在写成

$$m_i = \lambda_{i,0} + \lambda_{i,1}\tau + \cdots \lambda_{i,r-1}\tau^{r-1},$$

我们得到公式：

$$m = \sum_{i=0}^{k}\sum_{j=0}^{r-1}\lambda_{i,j}\tau^j\phi_T^i = \sum_{j=0}^{r-1}\left(\sum_{i=0}^{k}\lambda_{i,j}T^i\right)\tau^j,$$

这恰好是m 在基$(1, \tau, \ldots, \tau^{r-1})$下的分解。

前面的计算表明，族$(1, \tau, \ldots, \tau^{r-1})$ 生成$\mathbf{M}(\phi)$。证明它是自由的留作读者的一道简单练习。 □

我们称$(1, \tau, \ldots, \tau^{r-1})$ 为$\mathbf{M}(\phi)$的典范基 。上面详细给出的证明表明，将$\mathbf{M}(\phi)$ 中的元素写成典范基的形式并不困难，而且完全可以通过计算机实现。

SageMath 示例 3.5. 可以按如下方式创建附属于 Drinfeld 模的动机。

```
sage: φ = DrinfeldModule(A, [z, z, z, z+1])
sage: M = φ.anderson_motive()
sage: M
Anderson motive of Drinfeld module T |--> (z + 1)*τ^3 + z*τ^2 + z*τ + z
```

现在，我们可以通过传入一个 Ore 多项式来创建$\mathbf{M}(\phi)$ 中的元素，并观察到软件会自动将其分解到典范基上。

```
sage: τ = φ.ore_variable()
sage: M(τ)
(0, 1, 0)
sage: M(τ^2)
(0, 0, 1)
sage: M(τ^3)
((4*z + 6)*T + 4*z + 5, 4*z + 5, 4*z + 5)
sage: M(φ(T))
(T, 0, 0)
```

$\mathbf{M}(\phi)$ 的典范基使我们能够用矩阵表示线性态射。按照 SageMath 的惯例，我们将向量写成行向量——特别地，态射f的矩阵 $\mathrm{Mat}(f)$ 定义为一个矩阵，其i行是基的第i个元素经f 映射后的像的系数。

使用完全相同的定义，也可以为半线性算子，尤其是自同态 $\tau_{\mathbf{M}(\phi)}$，赋予一个矩阵。简单计算可得，

如果 $\phi_T = z + g_1\tau + \cdots + g_r\tau^r$，那么

$$\mathrm{Mat}\left(\tau_{\mathbf{M}(\phi)}\right) = \begin{pmatrix} 0 & 1 & & & \\ & 0 & 1 & & \\ & & \ddots & \ddots & \\ & & & 0 & 1 \\ \frac{T-z}{g_r} & \frac{-g_1}{g_r} & \cdots & \frac{-g_{r-2}}{g_r} & \frac{-g_{r-1}}{g_r} \end{pmatrix} \in F[T]^{r\times r}. \tag{16}$$

SageMath 示例 3.6。我们可以通过以下语法访问上面的矩阵。

```
sage: M.matrix()
[                     0                      1                      0]
[                     0                      0                      1]
[(4*z + 6)*T + 4*z + 5              4*z + 5              4*z + 5]
```

例 3.18。一个重要的例子是 Carlitz 模的动机（见第 2.2 节）。简要回顾一下，相应的 Carlitz 模是由态射 $c : A \to F\{\tau\}, T \mapsto z + \tau$ 给出的秩 1 Drinfeld 模。其动机 M(c) 是一个秩 1 的 F[T]-模，也就是说，作为一个模，有 $M(c) = F[T]e$，其中我们用字母 e 表示 M(c) 的典范基。此外，应用公式 (16)，可得$\tau_{\mathbf{M}(c)}$ 的矩阵就是 $(T - z)$。因此，算子 $\tau_{\mathbf{M}(c)}$ 可明确表示为

$$\tau_{\mathbf{M}(c)}(f\,\mathbf{e}) = \tau(f)\,(T - z)\,\mathbf{e}.$$

3.4.3 Anderson 动机与 Tate 模的比较

我们先前介绍的两种构造在某种意义上互为对偶。为了准确说明这一点，我们考虑双线性映射

$$\mathbf{M}(\phi) \times F^s \to F^s,\ (m, z) \mapsto m(z).$$

对于 A 的所有理想 $\mathfrak{a}$，可以验证它会在挠点层面诱导出如下第二个双线性映射：

$$\mathbf{M}(\phi)/\mathfrak{a}\mathbf{M}(\phi) \times \phi[\mathfrak{a}] \to F^s. \tag{17}$$

于是，上述映射实际上是一个“完美对偶”，也就是说，它使 $\phi[\mathfrak{a}]$ 成为$\mathbf{M}(\phi)/\mathfrak{a}\mathbf{M}(\phi)$ 的对偶，反之亦然*viceversa*。具体而言，有如下定理。

定理 3.19. 设 $\phi : A \to F\{\tau\}$ 是一个 *Drinfeld* 模，且 $\mathfrak{a}$ 是 A 的一个理想。若 ϕ 的 A-特征不为零，则假设 $\mathfrak{a}$ 与之互素。于是，双线性映射(17)诱导出一个同构

$$\phi[\mathfrak{a}] \simeq \mathrm{Hom}_{F,\tau}\left(\mathbf{M}(\phi)/\mathfrak{a}\mathbf{M}(\phi),\ F^s\right),$$

其中$\mathrm{Hom}_{F,\tau}(\cdot,\cdot)$ 表示与 τ-作用可交换的 F-线性映射所构成的 A-模，其中τ 在 F^s 上的作用为 $x \mapsto x^q$。

证明. </style}参见 [Gos96, §5.4], 或 [CL26, §2.1]，以了解一种更为直观的证明方法。 □

注记 3.20. 定理 3.19 可视为 Katz 关于 Galois 表示与 Frobenius 模之间范畴等价的著名结果的一种实现 [Kat73, 命题 4.1.1]：它准确地说明了 $\phi[\mathfrak{a}]$ 与 $\mathbf{M}(\phi)/\mathfrak{a}\mathbf{M}(\phi)$ 在这一等价关系下相对应。

取极限后，我们由定理 3.19 推得 Tate 模$\mathbf{T}_{\mathfrak{l}}(\phi)$ 关于 $\mathbf{M}(\phi)$的一个公式。为了将其写成简洁的形式，引入 $\mathbf{M}(\phi)$的对偶动机$\mathbf{M}(\phi)^{\vee}$ 较为方便。它按通常的公式定义为

$$\mathbf{M}(\phi)^{\vee} = \mathrm{Hom}_{F[T]}\big(\mathbf{M}(\phi), F[T]\big).$$

在典范对偶基下， τ对它的作用由矩阵定义

$$\mathrm{Mat}\big(\tau_{\mathbf{M}(\phi)}\big)^{-1} = \frac{1}{T-z}\begin{pmatrix} g_1 & 1 & & \\ g_2 & 0 & 1 & \\ \vdots & & \ddots & \ddots \\ g_r & & & 0 \quad 1 \end{pmatrix}. \tag{18}$$

不过，我们注意到，后者的系数并不属于$F[T]$ ，而是属于$F[T][\ \frac{1}{T-z}]$。这意味着$\tau_{\mathbf{M}(\phi)^{\vee}}$ 不是$\mathbf{M}(\phi)^{\vee}$ 的自同态，而只定义了一个映射

$$\tau_{\mathbf{M}(\phi)^{\vee}} : \mathbf{M}(\phi)^{\vee} \to \mathbf{M}(\phi)^{\vee}\left[\frac{1}{T-z}\right].$$

我们称$\mathbf{M}(\phi)^{\vee}$ 是非有效的。

对于A的一个极大理想 $\mathfrak{l}$，它不同于 ϕ的A-特征，此时我们有一个同构

$$\mathbf{T}_{\mathfrak{l}}(\phi) \otimes_{\mathbb{F}_q} F^{\mathrm{s}} \simeq \mathbf{M}(\phi)^{\vee} \otimes_{A\otimes F} (A_{\mathfrak{l}} \otimes F^{\mathrm{s}}), \tag{19}$$

它与 τ作用相容（在陪域上将$T-z$ 求逆之后）。最后，通过取 τ作用下的不动点，我们得到$\mathbf{T}_{\mathfrak{l}}(\phi)$ 的一个公式。

4 Drinfeld 模的态射

在本节中，我们沿用第 3.2 小节的记号。特别地，回顾一下，F 通过环同态 $\gamma: A \to F$ 成为一个A-域，并且我们令$z = \gamma(T)$。

4.1 正式定义

在(F,γ) 上的 Drinfeld 模旨在刻画A-模在F-代数上的代数结构；类似地，两个 Drinfeld 模之间的态射对应于代数化的A-线性映射，即由 Ore 多项式编码的映射*i.e.,* 。

Drinfeld 模之间态射的正式定义只保留底层的 Ore 多项式，可表述如下。

定义 4.1。 设 $\phi,\psi: A \to F\{\tau\}$ 是(F,γ)上的两个A-Drinfeld 模。一个态射 $u: \phi \to \psi$ 是一个 Ore 多项式$u \in F${v28>，满足$u\phi_a = \psi_a u$ 对所有$a \in A$均成立。非零态射称为同源。

我们用 $\mathrm{Hom}(\phi,\psi)$ 表示从 ϕ 到 ψ 的态射集合。当 $\phi = \psi$ 时，我们简写为 $\mathrm{End}(\phi)$ ，表示 $\mathrm{Hom}(\phi,\phi)$。

由于 A 是 $\mathbb{F}_q[T],$ ，定理 4.1 的条件等价于要求 $u\phi_T = \psi_T u$；换言之，只需检查条件对 $a = T$ 成立即可。另一个值得注意的事实是，两个同源 Drinfeld 模必然具有相同的秩。事实上，关系式 $u\phi_T = \psi_T u$ 意味着在 τ 次数下，$\deg u + \deg \phi_T = \deg \psi_T + \deg u$，因此 $\deg \phi_T = \deg \psi_T$。

注记 4.2。 提醒读者，表示态射集和自同态集的方式有多种约定。例如，当需要区分普通 Drinfeld 模和超奇异 Drinfeld 模（我们将在小节 5.1.4 中定义）时，考虑定义在可分闭包上的态射会很有用，也就是说，元素 $u \in F^s\{\tau\}$ 满足 $u\phi_T = \psi_T u$。此时，我们将其集合记作 $\mathrm{Hom}_{F^s}(\phi,\psi)$，而 $\mathrm{End}_{F^s}(\phi) = \mathrm{Hom}_{F^s}(\phi,\phi)$。这种记法不同于[Pap23，命题 3.3 中引入的记法，10], 但与 SageMath 的实现一致（参见 SageMath 示例 5.4）。

我们注意到，当仅给出 ϕ 和 u 时，可以通过求解方程 $u\phi_T = \psi_T u$轻松推断出陪域 ψ。这一观察也引出了下面的命题。

命题 4.3. 设 $\phi : A \to F\{\tau\}$ 是一个 *Drinfeld* 模。设 $u \in F\{\tau\}$ 是一个非零 *Ore* 多项式。那么，u 定义了一个定义域为 ϕ 的同源，当且仅当 u 右整除 $u\phi_T$。

证明。 我们假设命题中的条件成立。由关系式 $u\phi_T = \psi_T u$定义 Ore 多项式 ψ_T。考察右侧次数最低的项的系数，可知 ψ_T 的常数项为 z。因此，可以将 ψ_T 延拓为 Drinfeld 模 $\psi : A \to F\{\tau\}$，且 u 定义了一个从 ϕ 到 ψ的同源。反向的证明类似。

□

SageMath 示例 4.1. 只需传入定义该态射的 Ore 多项式，即可创建一个态射：如果未给出陪域，系统会自动计算。

```
sage: φ = DrinfeldModule(A, [z, z, 1])
sage: u = φ.hom(τ + 1)
sage: u
Drinfeld Module morphism:
  From: Drinfeld module T |--> τ^2 + z*τ + z
  To:   Drinfeld module T |--> τ^2 + (6*z + 1)*τ + z
  Defn: τ + 1
sage: ψ = u.codomain()
sage: ψ
Drinfeld module T |--> τ^2 + (6*z + 1)*τ + z
sage: (τ + 1) * φ(T) == ψ(T) * (τ + 1)
True
```

态射上的算术运算。 所有基本的态射算术运算均通过引入 Ore 多项式上的标准算术运算来定义。具体而言，态射可以：

- 相加。若 u、v：$\phi \to \psi$ 是两个态射，则 Ore 多项式 $u+v$ 也定义了一个态射。事实上，我们有

$$(u+v)\cdot\phi_T = u\phi_T + v\phi_T = \psi_T u + \psi_T v = \psi_T \cdot (u+v).$$

- 乘以 $\mathbb{F}_q$ 中的标量。注意，由于 $\mathbb{F}_q$ 位于 $F\{\tau\}$ 的中心，对于 ϕ 上的任意同源 u 以及任意标量 $\lambda \in \mathbb{F}_q$，则 λu 和 $u\lambda$ 定义的是同一个同源。
- 与A中的元素相乘。给定u：$\phi \to \psi$ 以及$a \in A$，乘积au 由 Ore 多项式$u\phi_a = \psi_a u$定义；我们很容易检查出，它仍然是从ϕ 到 ψ的同源。

- 复合。给定$u:\ \phi \to \psi$ 以及$v:\ \psi \to \mu$，Ore 多项式uv的乘积定义了一个从 ϕ 到 μ的态射。事实上，立即可验证$uv\phi_T = u\psi_T v = \mu_T uv$。恒等态射同样是有意义的：它由常 Ore 多项式 1 表示。

可以将上述性质概括为：固定基 (F,γ) 上的 Drinfeld 模构成一个A-线性范畴；特别是，集合 $\mathrm{Hom}(\phi,\psi)$ 是 A 上的模，而 $\mathrm{End}(\phi)$ 是 A上的代数。

SageMath 示例 4.2。 我们构造另一个同源v，并将它与u复合。

```
sage: v = ψ.hom(τ + z - 1)
sage: v
Drinfeld Module morphism:
  From: Drinfeld module T |--> τ^2 + (6*z + 1)*τ + z
  To:   Drinfeld module T |--> τ^2 + z*τ + z
  Defn: τ + z + 6
sage: u * v
Endomorphism of Drinfeld module T |--> τ^2 + (6*z + 1)*τ + z
  Defn: τ^2 + (6*z + 1)*τ + z + 6
sage: v * u
Endomorphism of Drinfeld module T |--> τ^2 + z*τ + z
  Defn: τ^2 + z*τ + z + 6
sage: u * v == T - 1
True
sage: v * u == T - 1
True
```

在上面的代码中，最后两行验证复合$u\circ v$和$v\circ u$都是由$T-1$给出的标量乘法。不过我们注意到，定义它们的 Ore 多项式并不相同。事实上，第一个是 ψ_{T-1}（因为$u\circ v$是 ψ的一个自同态），而第二个是 ϕ_{T-1}。我们将在后面的第 4.4.3 小节中看到，$T-1$ 是u的范数，而v 是它的对偶同源。

命题 4.4。 设 $\phi:A\to F\{\tau\}$ 是一个 *Drinfeld* 模。设 $u_1,\dots,u_n$ 是定义域为 ϕ的同源。则 *Ore* 多项式 最大公右因式$(u_1,\dots,u_n)$ 和 最小公右倍式$(u_1,\dots,u_n)$ 都定义了定义域为 ϕ的同源。

证明。我们令 ψ_i 表示每个同源u_i $(1\leqslant i\leqslant n)$ 的陪域。对每个指标i，都有关系$u_i\phi_T = \psi_{i,T}u_i$。

现在记$u =$最大公右因式$(u_1,\dots,u_n)$。由于$F\{\tau\}$是左欧几里得的，存在贝祖关系$u = \sum_{i=1}^n m_i u_i$，其中$m_i\in F\{\tau\}$。由此可得$u\phi_T = \sum_{i=1}^n m_i\psi_{i,T}u_i$。因此$u\phi_T$ 属于由这些u_i生成的左理想，因而可被它们的右最大公因子u右整除。根据定理 4.3，我们得出u 定义了一个定义域为 ϕ 的同源。

现在令$v =$最小公右倍式$(u_1,\dots,u_n)$。根据定义，u_i 右整除v。因此，我们可以写成 $v = m_i u_i$，其中$m_i\in F\{\tau\}$，并得到关系$v\phi_T = m_i u_i\phi_T = m_i\psi_{T,i}u_i$，这证明$u_i$ 也右整除 $v\phi_T$。由于这对所有u都成立，我们得到v 也右整除$v\phi_T$。同样，根据定理 4.3 得出结论。□

对 F^s-点的作用。 研究 Drinfeld 模在 F-代数上的作用，是研究 Drinfeld 模态射的另一种途径。事实上，按照前述意义，任意 Drinfeld 模态射$u:\ \phi\to\psi$ 都会诱导映射，我们仍将其记作u

$$\begin{array}{ccc} {}^{\phi}\mathcal{F} & \to & {}^{\psi}\mathcal{F} \\ x & \mapsto & u(x), \end{array}$$

对每个F-代数 $\mathcal{F}$均如此。当 $\mathcal{F}$ 是F^s时，这种构造尤其重要。事实上，可以证明，两个同源$u,v:\ \phi \to \psi$ 相等，当且仅当它们诱导相同的态射 ${}^{\phi}F^s \to {}^{\psi}F^s$。

我们将在下文第 4.4 小节进一步阐述这一观点。

4.2 可分性

关于椭圆曲线的同源，可分与不可分同源之间存在一个重要区别：前者对应有限子群，而后者通常由 Frobenius 态射来刻画。这种二分法也适用于 Drinfeld 模，下面我们将对此进行讨论。

4.2.1 可分同源及其核

我们先定义 Drinfeld 模语境下可分性的概念。 .

定义 4.5。若同源 $u:\ \phi \to \psi$ is可分，则其 τ-赋值为零；也就是说，将其视为 Ore 多项式时，其常数项不为零。

我们回顾定理 3.2，其中定义了态射 u 的核：

$$\ker u = \left\{ x \in {}^{\phi}F^s \mid u(x) = 0 \right\}.$$

它是 ${}^{\phi}F^s$ 的一个 A-子模，当且仅当 u 是同源时，它是有限的。此外，作为 F^s 的子集，它带有 $\mathrm{Gal}(F^s/F)$ 的作用。

命题 4.6。设 $\phi : A \to F\{\tau\}$ 是一个 *Drinfeld* 模。设 G 是 ${}^{\phi}F^s$ 的一个有限 A-子模，且在 *Gal*$\mathrm{Gal}(F^s/F)$ 的作用下稳定。则存在一个 *Drinfeld* 模 $\psi : A \to F\{\tau\}$，以及一个可分同源 $u:\ \phi \to \psi$，使得 $\ker u = G$。

证明。应用定理 3.2，可得一个常数项为 1 的 Ore 多项式 $u \in F\{\tau\}$，使得 $\ker u = G$。此外，由于 G 是一个 A-子模，故 $\phi_T(G) \subset G$，由此可得 $\ker u \subset \ker(u\phi_T)$。因此，由注记 3.3 可知，$u$ 右整除 $u\phi_T$，也就是说，存在一个 Ore 多项式 $\psi_T \in F\{\tau\}$，使得 $u\phi_T = \psi_T u$。这个 Ore 多项式 ψ_T 定义了一个 Drinfeld 模 ψ，使得 u 成为同源 $\phi \to \psi$。□

注记 4.7. 定理 4.6 中的同源 ψ 在 ψ 的同构意义下唯一确定，也就是说，差一个 $\mathbb{F}_q$ 的非零元素的乘法（见第 4.3 小节）。因此，我们可以通过要求其常数项为 1（如定理 3.2 中所示）或要求其为首一多项式来对其进行规范化。

结合前文来看，重新诠释定理 4.4 很有意思。事实上，回顾定理 3.3，右最大公因子（分别地，左最小公倍数）对应于取交（分别地，取和）。因此，当同源 u_i 可分时，Ore 多项式 最大公右因式$(u_1,\ldots,u_n)$ 和 最小公右倍式$(u_1,\ldots,u_n)$ 分别定义了核为 $\ker(u_1)\cap\cdots\cap\ker(u_n)$ 和 $\ker(u_1)+\cdots+\ker(u_n)$ 的同源。

4.2.2 不可分同源与 Frobenius 态射

当A的F 特征为零点时，可以验证所有同源都是可分的，因此对应于有限的A-子模 ${}^{\phi}F^s$。

相反，当F的A特征为极大理想 $\mathfrak{p}$时，确实存在不可分同源。事实上，由 $\mathrm{char}_A(F) = \mathfrak{p}$这一事实，我们可推出$z^{q^{\deg \mathfrak{p}}} = z$。因此，若写作 $\phi_T = z + g_1\tau + \cdots + g_r\tau^r$，Ore 多项式 $\tau^{\deg \mathfrak{p}} \in F\{\tau\}$ 满足以下交换关系：

$$\tau^{\deg \mathfrak{p}}\phi_T = z\tau^{\deg \mathfrak{p}} + \sum_{i=1}^{r} g_i^{q^{\deg \mathfrak{p}}}\tau^{i+\deg \mathfrak{p}} = \phi'_T\tau^{\deg \mathfrak{p}}$$

其中

$$\phi'_T = z + g_1^{q^{\deg \mathfrak{p}}}\tau + \cdots + g_r^{q^{\deg \mathfrak{p}}}\tau^r. \tag{20}$$

换句话说，$\tau^{\deg \mathfrak{p}}$ 定义了一个从 ϕ 到由方程（20）定义的 Drinfeld 模 ϕ'的非可分同源。

定义 4.8. 同源 $\tau^{\deg(\mathfrak{p})}\colon \phi \to \phi'$ 称为 ϕ的相对 *Frobenius* 态射。

SageMath 示例 4.3. 在下面的例子中，我们有 $\gamma(T) = 1$，因此相对 Frobenius 由 Ore 多项式 τ表示。

```
sage: ϕ = DrinfeldModule(A, [1, z, z])
sage: ϕ.frobenius_relative()
Drinfeld Module morphism:
  From: Drinfeld module T |--> z*τ^2 + z*τ + 1
  To:   Drinfeld module T |--> (6*z + 1)*τ^2 + (6*z + 1)*τ + 1
  Defn: τ
```

相反，当 $\gamma(T)$ 生成 F时，相对 Frobenius 是一个自同态。它就是所谓的*Frobenius* 自同态，将在小节 5.1.1 中作更详细的讨论。

```
sage: ϕ = DrinfeldModule(A, [z, z, 1])
sage: ϕ.frobenius_relative()
Endomorphism of Drinfeld module T |--> τ^2 + z*τ + z
  Defn: τ^2
```

事实证明，Frobenius 态射是不可分同源的典型例子，以下命题对此作了强调。

命题 4.9。 任意非可分同源 $u\colon \phi \to \psi$ 在 A-特征为 $\mathfrak{p}$的 *Drinfeld* 模之间都可通过 ϕ 的相对 *Frobenius* 分解，即存在一个同源 $u'\colon \phi' \to \psi$，使得 $u = u'\tau^{\deg \mathfrak{p}}$。

任意同源 $u\colon \phi \to \psi$都可以写成 $u = v\tau^{m\deg \mathfrak{p}}$，其中 v 是可分的，m 是非负整数。

证明。 只需证明 τ-赋值的 u 至少为 $\deg \mathfrak{p}$。这可通过写出交换关系 $u\phi_T = \psi_T u$ 并比较最低次数项的系数得到。第二个结论通过反复应用第一个结论即可得到。 □

注 4.10。 我们强调，反方向的分解，即 $u = \tau^{\deg \mathfrak{p}}u'$ 在一般情形下可能不存在。然而，当 F 是有限域时，它总是存在。

与椭圆曲线的情形一样，Frobenius 态射在有限域上 Drinfeld 模的研究中起着主要作用。我们将在第 5.1 小节中进一步阐述这一点。

4.3 同构与j-不变量

当然，同构是一类重要的态射。回到定义可知，同构 $u\colon \phi \to \psi$ 由一个可逆 Ore 多项式 u编码。由于次数具有可加性，可逆 Ore 多项式恰好就是非零常 Ore 多项式。因此，同构仅由$F^\times$中的元素给出。尽管如此，我们也可以考虑任意扩张F'/F上的同构：$F'\{\tau\}$ 上的常 Ore 多项式u，满足$u\phi_T = \psi_T u$。本小节将介绍一种检验同构的方法，并给出用于编码同构类的不变量（在F^s上）。

4.3.1 判定两个 Drinfeld 模是否同构

固定一个 Drinfeld 模 $\phi\colon A \to F\{\tau\}$，其秩为$r$，并记

$$\phi_T = z + g_1\tau + g_2\tau^2 + \cdots + g_r\tau^r.$$

现在，任意元素$u \in (F^s)^\times$ 都定义了一个同源$u\colon \phi \to \psi$，其中 ψ 是秩为r 的 Drinfeld 模，由下式显式定义：

$$\psi_T = z + u^{1-q}g_1\tau + u^{1-q^2}g_2\tau^2 + \cdots + u^{1-q^r}g_r\tau^r.$$

这一计算的另一个结果是，我们可以通过一个过程来判定两个 Drinfeld 模ϕ 和 ψ 是否同构：当且仅当将 ϕ_T 的系数乘以u^{1-q^i} 后可以得到 ψ_T 的系数时，它们才同构（其中i 是相应的 τ-次数）。虽然这一判据看起来很容易检验，但必须谨慎处理系数可能为零的情况。不过，只要妥善处理这一稍显棘手的情形，最终便能得到一种高效的同构检验算法（更多细节另见[Leu24, § 3.2.3.5] ）。

SageMath 示例 4.4。 我们提到的同构检验已实现。此方法甚至可以判定 Drinfeld 模是否在基域上或在可分闭包上同构，默认情况下是在基域上判定。

```
sage: φ = DrinfeldModule(A, [z, 1, 1])
sage: ψ = DrinfeldModule(A, [z, 2*z + 1, 1])
sage: φ.is_isomorphic(ψ)
True
```

在这里，我们可以手动验证，同构由常 Ore 多项式$z + 1$给出。

```
sage: u = φ.hom(z + 1)
sage: u.codomain() is ψ
True
sage: u.is_isomorphism()
True
```

下面是第二个例子：ϕ 和 ψ 在底A-域F上不同构，但在F^s上同构。

```
sage: ψ = DrinfeldModule(A, [z, z, 3])
sage: φ.is_isomorphic(ψ)
False
sage: φ.is_isomorphic(ψ, absolutely=True)
True
```

4.3.2 j-不变量

一个重要事实是，F^s 上的同构类可以由代数不变量刻画。在秩 1 的情形下，情况很简单：所有秩 1 的 Drinfeld模都与 $T \mapsto z+\tau$ 上的 Carlitz 模同构。

秩-2 Drinfeld 模。由第 4.3.1 小节中的推导可知，由以下关系定义的秩 2 Drinfeld 模 ϕ 和 ψ，

$$\begin{aligned}\phi_T &= z + g_1\tau + g_2\tau^2 \qquad (g_2 \neq 0),\\ \psi_T &= z + h_1\tau + h_2\tau^2 \qquad (h_2 \neq 0),\end{aligned}$$

当且仅当存在 $u \in (F^s)^\times$ 使得 $h_1 = u^{q-1}g_1$ 且$h_2 = u^{q^2-1}g_2$时，它们才是F^s-同构的。将第一个方程两边提升到$q+1$次幂，得到$h_1^{q+1} = u^{q^2-1}g_1^{q+1}$；再与第二个方程结合，可得必要条件

$$\frac{g_1^{q+1}}{g_2} = \frac{h_1^{q+1}}{h_2}. \tag{21}$$

事实证明，这个条件也是充分的。事实上，如果$g_1 \neq 0$（因此$h_1 \neq 0$ 也如此），我们解第一个方程$h_1 = u^{q-1}g_1$，并验证任一解也是第二个方程的解。反之，如果$g_1 = h_1 = 0$，我们只需求解第二个方程，第一个方程便会自动成立。

定义 4.11。式（21）中出现的量 g_1^{q+1}/g_2 称为 ϕ 的j 不变量，记作$j(\phi)$。

它刻画了 ϕ 在F^s上的同构类。

SageMath 示例 4.5。我们重新使用 SageMath 示例 4.4 中的 Drinfeld 模（它们在可分闭包上同构，但在基域上不同构），并验证它们具有相同的j不变量。

```
sage: φ.j_invariant()
1sage: ψ.j_invariant()
1
```

注记 4.12。对于 K 中的任意j，若$j = 0$，令 $\phi_T = z + \tau^2$；否则令 $\phi_T = z + \tau + j^{-1}\tau^2$。则由 ϕ_T 定义的 Drinfeld 模$A \to F\{\tau\}$ 具有j不变量j。

高秩 Drinfeld 模。高秩 Drinfeld 模的同构不变量由 Potemine [Pot98]引入。

定义 4.13. 设 $\phi : A \to F\{\tau\}$ 是一个秩为 r 的 Drinfeld 模。记 $\phi_T = z + g_1\tau + \cdots + g_r\tau^r$，其中 $g_r \neq 0$。设 $\ell < r$ 和 $k = (k_1, \ldots, k_\ell)$ 是一个多重指标，满足$1 \leqslant k_1 \leqslant \ldots \leqslant k_\ell \leqslant r-1$；再设 $s = (s_1, \ldots, s_\ell, s_r)$ 是一个 $(\ell+1)$ 元整数元组，满足以下条件：

- $0 \leqslant s_i \leqslant \dfrac{q^r-1}{q^{\gcd(k_i,r)}-1}$ for every $i \in \{1, \ldots, \ell\}$,
- $s_1\left(q^{k_1}-1\right) + \cdots + s_\ell\left(q^{k_\ell}-1\right) = s_r\left(q^r-1\right)$.

*Potemine J*不变量的 ϕ 指标为$(\boldsymbol{k},\boldsymbol{s})$ 时为

$$J_k^{\boldsymbol{s}}(\phi) = \frac{g_{k_1}^{s_1} \cdots g_{k_\ell}^{s_\ell}}{g_r^{s_r}}.$$

先验地 存在无限多个可接受的配对$(\boldsymbol{k},\boldsymbol{s})$。然而，将$\boldsymbol{s}$ 改为$n\boldsymbol{s}$ （其中$n \in \mathbb{N}$），会使相应的J-不变量升至n次幂。因此，我们可以放心地将范围限制在所谓的基本 参数上，即满足附加条件 $\gcd(s_1,\ldots,s_\ell,s_r) = 1$的参数$(\boldsymbol{k},\boldsymbol{s})$。

随着r 增大，基本参数列表会迅速变得很长，但始终是有限的。极端情况下，当$r = 2$时，只有一个基本参数，即$\boldsymbol{k} = (1)$ 和$\boldsymbol{s} = (q+1, 1)$。相应的 Potemine J-不变量就是我们在定理4.11中介绍的j-不变量。

SageMath 示例 4.6. SageMath 提供了用于生成基本参数列表以及计算任意秩下相应J-不变量的方法。我们从下面的示例中已经可以看到，即使在秩为 3 时，Potemine J-不变量的完整列表也可能非常长。

```
sage: φ = DrinfeldModule(A, [z, z+1, z+2, z+3])
sage: φ.basic_j_invariants()
{((1,), (57, 1)): 3*z,
((1, 2), (1, 7, 1)): 4*z + 6,
((1, 2), (9, 6, 1)): 5*z + 5,
((1, 2), (10, 13, 2)): 5,
((1, 2), (11, 20, 3)): 6*z + 2,
((1, 2), (12, 27, 4)): 5*z + 3,
((1, 2), (13, 34, 5)): 6*z, ...,
((1, 2), (53, 29, 5)): 6*z + 2,
((1, 2), (55, 43, 7)): 6*z,
((2,), (57, 8)): 2*z + 4}(35 lines in total)
```

注4.14. 提醒读者，不同文献可能采用不同的不变量命名约定。我们选择遵循 Potemine 的约定，SageMath 也采用这一约定。Papikian 使用不同的记法： [Pap23] 的 j-不变量以及基本 j-不变量，分别对应 Potemine 的基本j-不变量，以及与参数$\boldsymbol{k} = (k)$ 和$\boldsymbol{s} = \frac{1}{q^{\gcd(k,r)-1}} \cdot (q^r - 1, q^k - 1)$相关联的 Potemine$J$-不变量，即

$$\frac{g_k^{(q^r-1)/(q^{\gcd(k,r)-1})}}{g_r^{(q^k-1)/(q^{\gcd(k,r)-1})}}.$$

这些不变量刻画了代数闭包上的 Drinfeld 模的同构类，正如下述定理所示。

定理 4.15 ([Pap23，定理 3.8。11]). 设 $\phi, \psi : A \to F\{\tau\}$ 是两个秩相同的 *Drinfeld* 模。假设 F 是可分闭的。那么，当且仅当 ϕ 和 ψ 具有相同的基本 *Potemine J*不变量时，它们同构。

4.4 Anderson 动机上的作用及其后果

我们之前已经提到过，Drinfeld 模之间的态射 $u : \phi \to \psi$ 可以实现为一个实际的 A-线性映射 $u : {}^{\phi}F^s \to {}^{\psi}F^s$。然而， ${}^{\phi}F^s$ 作为 A-模的结构并不容易描述和处理；例如，它通常不是

有限型（参见 [Poo95]）。可以通过用 Tate 模 $\mathbf{T}_{\mathfrak{l}}(\phi)$ 替代 ${}^{\phi}F^{s}$来解决这个问题。正确选取素理想 $\mathfrak{l}$后，我们便知道 $\mathbf{T}_{\mathfrak{l}}(\phi)$ 是一个秩为 $r := \mathrm{rank}(\phi)$的 $A_{\mathfrak{l}}$ 上的自由模。尽管这一改动确实带来了许多有益的应用，但它仍有一个令人不快的缺点：引入了辅助素数 $\mathfrak{l}$ 以及与之相关的完备化 $A_{\mathfrak{l}}$。接下来我们将说明，用 Anderson 动机（见第 3.4.2 小节）取代 Tate 模，能够巧妙地解决所有这些问题。

给定一个同源 $u : \phi \to \psi$，我们定义

$$\begin{array}{rccc} \mathbf{M}(u): & \mathbf{M}(\psi) & \longrightarrow & \mathbf{M}(\phi) \\ & m & \mapsto & mu \end{array},$$

其中，乘积 mu 是在 $F\{\tau\}$ 中计算的。容易验证，$\mathbf{M}(u)$ 是 $F[T]$-线性的，并且与 τ-作用可交换，也就是说，它满足

$$\mathbf{M}(u) \circ \tau_{\mathbf{M}(\psi)} = \tau_{\mathbf{M}(\phi)} \circ \mathbf{M}(u).$$

我们强调，这一构造是逆变的，也就是说，箭头方向相反：若 u 从 ϕ 指向 ψ，则 $\mathbf{M}(u)$ 从 $\mathbf{M}(\psi)$ 指向 $\mathbf{M}(\phi)$。

已知 $\mathbf{M}(u)$ 是一个线性映射，可以分别考虑它在 $\mathbf{M}(\psi)$ 和 $\mathbf{M}(\phi)$的典范基下的矩阵。具体而言，$\mathrm{Mat}(\mathbf{M}(u))$ 的第i行由 $\tau^i u$ 在 $\mathbf{M}(\phi)$中的系数组成。

SageMath 示例 4.7。

```
sage: φ = DrinfeldModule(A, [z, z, z, 1])
sage: u = φ.hom(τ + 5)
sage: Mu = u.anderson_motive()
sage: Mu
Morphism:
  From: Anderson motive of Drinfeld module
           T |--> τ^3 + (6*z + 1)*τ^2 + (2*z + 3)*τ + z
  To:   Anderson motive of Drinfeld module T |--> τ^3 + z*τ^2 + z*τ + z
sage: Mu.matrix()
[      5       1       0]
[      0       5       1]
[T + 6*z     6*z 6*z + 5]
```

4.4.1 全忠实性定理

关于 Anderson 动机的第一个重要结果如下定理，它表明函子 $\mathbf{M}$ 是完全忠实的。

定理 4.16. 设 $\phi, \psi : A \to F\{\tau\}$ 是两个 *Drinfeld* 模。那么，存在一个典范双射

$$\begin{array}{rccc} \mathrm{Hom}(\phi,\psi) & \xrightarrow{\sim} & \mathrm{Hom}_{F[T],\tau}(\mathbf{M}(\psi), \mathbf{M}(\phi)) \\ u & \mapsto & \mathbf{M}(u) \end{array},$$

其中，$\mathrm{Hom}_{F[T],\tau}$ 由所有与 τ-作用可交换的 $F[T]$-线性映射组成。

证明。 只需证明逆映射由 $f \mapsto f(1)$ 给出，这可以通过直接验证得出。

□

利用 Anderson 动机决定 Tate 模（见等式（19））这一事实，我们从定理 4.16 推导出 Tate 模层面上的一个全忠实性结果，这可视为 Tate定理在阿贝尔簇上的一个类似结果。

定理 4.17. 设 $\mathfrak{l}$ 是 A 的一个极大理想，且不同于（F，γ）的 A-特征。那么，对于所有 *Drinfeld* 模 ϕ，ψ：$A \to F\{\tau\}$，典范映射

$$A_{\mathfrak{l}} \otimes_A \mathrm{Hom}(\phi, \psi) \to \mathrm{Hom}_{A_{\mathfrak{l}}}\big(\mathbf{T}_{\mathfrak{l}}(\phi), \mathbf{T}_{\mathfrak{l}}(\psi)\big)$$

它是单射，且其像恰好由在 $\mathrm{Gal}(F^s/F)$作用下保持等变的态射 $\mathbf{T}_{\mathfrak{l}}(\phi) \to \mathbf{T}_{\mathfrak{l}}(\psi)$ 组成。

4.4.2 特征多项式

Anderson 模对于引入线性代数中的经典构造，并为 Drinfeld 模的态射附加有意义的不变量，也十分有用。这方面的一个典型例子是构造 Drinfeld 模的自同态的特征多项式，其定义如下。

定义 4.18。 设 u 是 Drinfeld 模 ϕ的一个自同态。u的特征多项式记为 χ_u，定义为 $F[T]$-线性映射 $\mathbf{M}(u)$：$\mathbf{M}(\phi) \to \mathbf{M}(\phi)$的特征多项式，即

$$\chi_u(X) = \det\big(X \cdot \mathrm{id} - \mathbf{M}(u)\big).$$

根据定义，$\chi_u(X)$ 是一个次数为 r 的多项式，其中 的秩为 $\mathbf{r}$。它的系数起初属于 $F[T] \simeq A \otimes_{\mathbb{F}_q} F$，但由 $\mathbf{M}(u)$ 与 τ-作用交换这一事实可知，$\chi_u(X)$ 的系数实际上属于 A。此外，Cayley–Hamilton 定理断言 $\chi_u(\mathbf{M}(u)) = 0$，由此根据定理 4.16 可得 $\chi_u(u) = 0$。

定理 4.18 与定理 3.17 相结合，可直接得出一种计算自同态特征多项式的算法。目前，SageMath 默认采用此方法。[CL26] 中提供了更多详情，包括复杂度说明和各种优化。

SageMath 示例 4.8。

```
sage: φ = DrinfeldModule(A, [z, z, 1])
sage: u = φ.hom(τ^4 + z*τ^3 + (z + 1)*τ^2)
sage: χ = u.characteristic_polynomial()
sage: χ
X^2 + (5*T^2 + 3*T + 5)*X + T^4 + T^3 + 2*T^2 + 5*T + 3
```

下面，我们将 χ 的计算分为两步：首先，计算作用于$\mathbf{M}(\phi)$ 上的 Frobenius 自同态的矩阵；其次，计算其特征多项式。

```
sage: Mu = u.anderson_motive()
sage: Mu.matrix()
[    T^2 + (6*z + 1)*T + 6*z                 6*z*T + 6*z]
[(z + 6)*T^2 + (z + 2)*T + 3     T^2 + (z + 3)*T + z + 2]
sage: Mu.matrix().charpoly()
x^2 + (5*T^2 + 3*T + 5)*x + T^4 + T^3 + 2*T^2 + 5*T + 3
```

从这个例子可以验证，特征多项式 χ 确实消去了 u。

```
sage: χ(u)Endomorphism of Drinfeld module T |--> τ^2 + z*τ + zDefn: 0
sage: u^2 + (5*T^2 + 3*T + 5)*u + T^4 + T^3 + 2*T^2 + 5*T + 3
Endomorphism of Drinfeld module T |--> τ^2 + z*τ + zDefn: 0
sage: φT = φ.gen()sage: μ = u.ore_polynomial()
sage: μ^2 + (5*μ*φT^2 + 3*μ*φT + 5*μ) + (φT^4 + φT^3 + 2*φT^2 + 5*φT + 3)
零点
```

注释4.19。 Musleh 和 Schost 也提出了一种通用方法，用于计算自同态 [MS23] 的特征多项式。该方法不依赖 Anderson 动机，而是利用 Drinfeld 模 [Ang97] 的晶体上同调（另见 [Mus23，第 5] 章）。这两种方法都将特征多项式作为多项式矩阵的经典特征多项式来计算。这两类算法首次实现了在相当广泛的情形下计算 Drinfeld 模的自同态的特征多项式；而此前的方法通常仅限于 Frobenius 自同态这一情形，正如我们将在小节 5.1.2 中讨论的那样。

在公式（19）中比较 Anderson 动机和 Tate 模之后，还可以发现，对于任意不同于 A-特征的素理想 $\mathfrak{l}$， $\chi_u(X)$ 等于$\mathbf{T}_{\mathfrak{l}}(u)$ 作用于 Tate 模$\mathbf{T}_{\mathfrak{l}}(\phi)$上的特征多项式。实际上，这种重新诠释是椭圆曲线框架下的经典定义，而其中并没有 Anderson 动机这一概念。由此我们清楚地看到 Anderson 动机的优势：它们提供了一个更简单的定义，一方面不依赖辅助素数 $\mathfrak{l}$（因而无需证明关于 $\mathfrak{l}$ 的独立性结果），另一方面也更适合计算。特别是，该定义不涉及F的可分闭包，而这在计算机上难以处理。

4.4.3 范数与对偶同源

类似地，也可以定义范数与对偶同源。

定义4.20。 设 $u:\ \phi \to \psi$ 是 $(F,\ \gamma)$上的 Drinfeld 模态射。u 的范数定义为

$$\operatorname{norm}(u) := \frac{\det \mathbf{M}(u)}{\operatorname{lc}(\det \mathbf{M}(u))}$$

其中，行列式在 $F[T]$ 上计算，lc 表示首项系数。

我们强调，$\mathbf{M}(u)$ 从 $\mathbf{M}(\psi)$ 映射到 $\mathbf{M}(\phi)$，因此一般而言它不是自同态。因此，计算其行列式时需要谨慎，因为其值取决于定义域与陪域的基的选择。然而，改变基只会使行列式乘以 $F[T]^{\times} = F^{\times}$中的一个元素。于是，行列式与其首项系数之商是良定义的。实际上，我们可以选取由定理 3.17 给出的 $\mathbf{M}(\phi)$ 和 $\mathbf{M}(\psi)$的典范基来完成计算。

注 4.21。 当A 不是 $\mathbb{F}_q[T]$, 时，就无法再除以 $\det \mathbf{M}(u))$的首项系数。相反，可以考虑由 $\det\mathbf{M}(u)$生成的 A 的理想，该理想仍然是规范定义的。

与特征多项式的情形一样，可以证明u 的范数总是属于A。此外，范数关于同源的复合具有乘法性。

此外，与特征多项式的情形相同，定理 4.20 直接给出了计算范数的算法。关于复杂度的详细说明，仍请参阅 [CL26] 。

SageMath 示例 4.9。 我们计算先前定义的u 的范数，并发现它是 χ_u 的常数项。注意，SageMath 的函数 `norm` 返回的是理想，而不是生成元（参见注 4.21）。

```
sage: u.norm()
Principal ideal (T^4 + T^3 + 2*T^2 + 5*T + 3) of Univariate Polynomial Ring
    in T over Finite Field of size 7
sage: χ.constant_coefficient()
T^4 + T^3 + 2*T^2 + 5*T + 3
```

与特征多项式不同，对于不同 Drinfeld 模之间的同源，范数仍有意义。在下面的例子中，我们重新得到了 SageMath 示例 4.2 中手动进行的计算。

```
sage: φ = DrinfeldModule(A, [z, z, 1])
sage: u = φ.hom(τ + 1)
sage: u
Drinfeld Module morphism:
  From: Drinfeld module T |--> τ^2 + z*τ + z
  To:   Drinfeld module T |--> τ^2 + (6*z + 1)*τ + z
  Defn: τ + 1
sage: u.norm()
Principal ideal (T + 6) of Univariate Polynomial Ring in T over Finite Field
     of size 7
```

与椭圆曲线的情形一样，同源u 的范数与其核有关

$$\ker u = \{\, x \in F^{\mathrm{s}} \mid u(x) = 0 \,\}.$$

更确切地说，与其 Fitting 理想 $|\ker u|$ 有关（定义见第 1.2 小节）。

命题 4.22。 设 u 是定义在(F,γ)上的 *Drinfeld* 模之间的一个同源。

1. 若 u 可分，则有理想的等式

$$\operatorname{norm}(u)A = |\ker u|.$$

2. 若 u 不可分，则

$$\operatorname{norm}(u)A = \mathfrak{p}^{h/\deg \mathfrak{p}} \cdot |\ker u|,$$

其中 h 是 u 的 τ-赋值，而 $\mathfrak{p}$ 是(F,γ) 的 A-特征。

证明概要。 当u 可分时，该公式由定理 3.19 得出，其中取一个消去 $\ker u$ 的理想 $\mathfrak{a}$。一般情形可通过在u 中尽可能多次提取 $\tau^{\deg \mathfrak{p}}$，由前一种情形推得（另见下一节的定理 4.9）；并独立证明 $\operatorname{norm}(\tau^{\deg \mathfrak{p}}) = \mathfrak{p}$。更多细节请参见 [CL26，定理 3.2]。

□

命题 4.23。 设 ϕ 和 ψ 是定义在 $(F,\ \gamma)$ 上的两个 *Drinfeld* 模，且 $u:\ \phi \to \psi$ 是一个范数为 a 的同源。则存在一个同源 $\hat{u}:\ \psi \to \phi$，使得 $\hat{u}\,u = \phi_a$ 且 $u\hat{u} = \psi_a$。

证明概要。 利用定理 4.16 定义同源 $\hat{u}$：令 $\mathbf{M}(\hat{u})$ 为 $\mathbf{M}(u)$ 的伴随矩阵（即余子式矩阵的转置）。 □

同源 $\hat{u}$ 称为u的对偶同源。计算它同样很容易：先计算范数，再通过 Ore 欧几里得除法求出对偶同源。

SageMath 示例 4.10. 我们计算 SageMath 示例 4.8 中同源 u 的对偶同源，并认出它就是我们在 SageMath 示例 4.2 中已经引入的同源v。

```
sage: u.dual_isogeny()
Drinfeld Module morphism:
  From: Drinfeld module T |--> τ^2 + (6*z + 1)*τ + z
  To:   Drinfeld module T |--> τ^2 + z*τ + z
  Defn: τ + z + 6
```

注记 4.24. 对偶同源是椭圆曲线语境下经典对偶同源的类比：若 $\varphi : E \to E'$ 是两个椭圆曲线之间范数为n 的同源，则存在一个同源 $\hat{\varphi} : E' \to E$，其范数为n，并且 $\hat{\varphi}\varphi$ （分别为 $\varphi\hat{\varphi}$）是 E （分别为 E') 上乘以n 的自同态。

我们以指出对偶同源的存在性保证“同源”是一种等价关系来结束本小节。

4.4.4 Hom 空间和自同态环的结构

Anderson 动机还有助于描述两个 Drinfeld 模之间的态射空间的结构。

定理 4.25([Pap23，定理 3.4。1])。 设 ϕ 和 ψ 是域 F 上的两个 *Drinfeld* 模，且二者的秩均为 r。那么，$\mathrm{Hom}(\phi, \psi)$ 是秩至多为 r^2 的自由 A-模。

证明概要。 由定理 4.16 可知，$\mathrm{Hom}(\phi, \psi)$ 同构于 $\mathrm{Hom}_{F[T],\tau}\big(\mathbf{M}(\psi), \mathbf{M}(\phi)\big)$，而后者本身属于 $\mathrm{Hom}_{F[T]}\big(\mathbf{M}(\psi), \mathbf{M}(\phi)\big)$ 这是一个在 $F[T]$ 上秩为 r^2 的自由模。为了从 $F[T]$ 下降到 $A = \mathbb{F}_q[T]$，关键观察是自然态射

$$F \otimes_{\mathbb{F}_q} \mathrm{Hom}_{F[T],\tau}\big(\mathbf{M}(\psi), \mathbf{M}(\phi)\big) \to \mathrm{Hom}_{F[T]}\big(\mathbf{M}(\psi), \mathbf{M}(\phi)\big)$$

是单射，这是关于 τ-模的一个经典一般性结论。更多细节请参阅 [Pap23, 命题 3.4.6]。 □

注 4.26. 上述证明不仅阐明了 $\mathrm{Hom}(\phi, \psi)$ 的结构，而且还可用于开发高效的算法方法来计算这个同态空间。事实上，将 $F[T]$-线性态射 $\mathbf{M}(\psi) \to \mathbf{M}(\phi)$ 表示为 $r \times r$ 矩阵后，我们只需解以下方程

$$M \cdot \mathrm{Mat}\big(\tau_{\mathbf{M}(\psi)}\big) = \mathrm{Mat}\big(\tau_{\mathbf{M}(\phi)}\big) \cdot \tau(M), \tag{22}$$

其中 $M \in F[T]^{r\times r}$ 是未知量，另外两个矩阵由方程（16）给出。当F 是有限域时，这为计算该同态空间提供了高效的算法。我们将在小节 5.1.3 中对此进行更详细的介绍。

定义 4.27。 给定一个 Drinfeld 模 ϕ，我们定义

$$\begin{aligned}\mathrm{End}^0(\phi) &= K \otimes_A \mathrm{End}(\phi),\\ \mathrm{End}^0_{F^s}(\phi) &= K \otimes_A \mathrm{End}_{F^s}(\phi),\end{aligned}$$

其中我们回顾一下，$K = \mathbb{F}_q(T)$ 是A的分式域。

对偶等源的存在性保证了 $\mathrm{End}^0(\phi)$ 是一个除法代数；事实上，对于一个同源 u：$\phi \to \phi$，若其范数为a 且对偶同源为 $\hat{u}$，那么它在 $\mathrm{End}^0(\phi)$ 中的逆元就是$a^{-1}\hat{u}$。此外，定理 4.25 告诉我们，$\mathrm{End}^0(\phi)$ 的维数至多为r^2，且是在K上的；而 $\mathrm{End}(\phi)$ 可以看作其中的一个序。$\mathrm{End}^0_{F^s}(\phi)$也同样如此。当$F$ 为有限域时，我们将在第 5.1.5 小节中进一步详细讨论 $\mathrm{End}^0(\phi)$ 和 $\mathrm{End}^0_{F^s}(\phi)$ 的结构。

5 德林费尔德模的算术方面

椭圆曲线的研究根据我们所处的基的不同而分为截然不同的分支。粗略地说，主要有三种情况。

- 在 $\mathbb{C}$ 上，主要工具是魏尔施特拉斯一致化定理和解析几何。
- 在有限域上，Frobenius 自同态发挥着核心作用。
- 在数域上，椭圆曲线可以视为定义在 $\mathbb{C}$上的椭圆曲线，但也可以对素数取模，将其约化为有限域上的椭圆曲线。因此，这种情形兼具前两种情形的特点。

在 Drinfeld 模理论中，也存在类似的三分法。我们已经讨论过解析理论（见第 3.3 小节），即 定义在 C_∞上的 Drinfeld 模。本节将探讨剩下的两种情形：定义在有限域上的 Drinfeld 模，以及定义在函数域上的 Drinfeld 模。

5.1 有限域上的情形

我们假设 F 是有限域 $\mathbb{F}_q$的有限扩张。这意味着与 A-特征相关联的态射$\gamma : A \to F$ （见定理 3.6）不是单射。我们记作$\mathfrak{p} = \mathrm{char}_A(F)$，它是一个素理想。记 $\mathbb{F}_\mathfrak{p}$ 为商 $A/\mathfrak{p}$；它是一个含有 $q^{\deg \mathfrak{p}}$ 个元素的有限域，并且我们有一个扩张塔

$$\mathbb{F}_q \xrightarrow{\pi_\mathfrak{p}} \mathbb{F}_\mathfrak{p} \xrightarrow{\iota_\mathfrak{p}} F \xrightarrow{\iota_F} F^s \ ,$$
$$\mathbb{F}_\mathfrak{p} \xrightarrow{\gamma} F$$

其中 $\iota_\mathfrak{p}$ 和 ι_F 是单射。我们还令 d 表示 F 在 $\mathbb{F}_q$上的次数。于是它是 $\deg \mathfrak{p}$的倍数。在本小节中，我们还固定一个秩为 r 的 Drinfeld 模$\phi : A \to F\{\tau\}$，其定义为 $\phi_T = z + g_1\tau + \cdots + g_r\tau^r$，其中 $g_i \in F$。

5.1.1 Frobenius 自同态及其特征多项式

我们回顾一下，Ore 多项式 $\tau^{\deg \mathfrak{p}}$ 定义了一个定义域为 ϕ的同源，称为 ϕ 的相对 Frobenius（见定理 4.8）。

命题 5.1. 同源 τ^d 是 ϕ 的一个自同态，称为 ϕ 的Frobenius 自同态。

自同态 τ^d 通常记作 π。

正如我们将看到的，与 ϕ 相关的一个极其重要的不变量是 π 的特征多项式。由于它具有核心作用，我们略微滥用记号，将其记作 $\chi_\phi(X)$，而非 $\chi_\pi(X)$（见定理 4.18）。

例 5.2. 回顾一下，(F, γ) 上的 Carlitz 模 c 定义为 $\mathrm{c}_T = \mathrm{z} + \tau$，其中按惯例 $\mathrm{z} = \gamma(\mathrm{T})$。我们在定理 3.18 中已经看到，c 的 Anderson 动机在 $\mathrm{F}[\mathrm{T}]$，上是一维的，即 $\mathrm{M(c)} = \mathrm{F}[\mathrm{T}]\cdot\mathrm{e}$，其中 τ-作用由公式 $\tau_{\mathbf{M}(c)}(\mathrm{e}) = (\mathrm{T}-\mathrm{z})\mathrm{e}$ 明确给出。利用 $\tau_{\mathbf{M}(c)}$ 的半线性，我们通过归纳可得

$$\tau^n_{\mathbf{M}(c)}(\mathbf{e}) = (T-z)(T-z^q)\cdots(T-z^{q^{n-1}})\cdot\mathbf{e}$$

对所有正整数n均成立。因此

$$\chi_c(X) = X - (T-z)(T-z^q)\cdots(T-z^{q^{d-1}}),$$

其中 $d = [F : \mathbb{F}_q]$。特别地，如果z 生成F 在 $\mathbb{F}_q$ 上的扩张，则有 $\chi_c(X) = X - \mathfrak{p}$，其中 $\mathfrak{p}$ 是A特征(F, γ)的一个生成元。更一般地，我们总有$\chi_c(X) = X - \mathfrak{p}^m$，其中$m = [F : \mathbb{F}_q(z)]$。

特别地，我们注意到，$\chi_c(1)$ 与定义 Carlitz ζ 函数的局部因子存在某种联系（见公式 (11)）。稍后在介绍L-级数理论时，我们将再次回到这一观察（见小节 5.2.1）。

SageMath 示例 5.1。 我们计算 Carlitz 模的 Frobenius 的特征多项式，并注意到确实得到了上面例 5.2 中给出的公式。

```
sage: c = CarlitzModule(A, F)
sage: c.characteristic()
T^2 + 6*T + 3
sage: c.frobenius_charpoly()
X + 6*T^2 + T + 4
```

下面给出另一个秩更高的 Drinfeld 模示例。我们注意到，系数的T-次数增长缓慢；这是一个普遍现象，正如下面的定理 5.4 所述。

```
sage: φ = DrinfeldModule(A, [z, z^2, z^3, z^4, z^5, z^6])
sage: χ = φ.frobenius_charpoly()
sage: χ
X^5 + 3*X^4 + 6*X^3 + (3*T + 5)*X^2 + (6*T + 3)*X + 6*T^2 + T + 4
```

以下三个定理凸显了 χ_ϕ 的重要性。第一个定理类似于椭圆曲线中的一条著名定理，该定理指出，有理点的数量可通过在 1 [处求 Frobenius 自同态的特征多项式的值来得到Sil09, 第五章, 定理 2.3.1]。对于 Drinfeld 模而言，有理点群所起的作用由 A-模 ϕ_F 承担。与阿贝尔簇不同，

其底层子集始终相同，也就是 F 本身。然而，它作为A-模的结构可能有所不同。

定理 5.3([Gek91，定理 5.1])。 欧拉-庞加莱特征 $|^{\phi}F|$ 是由 $\chi_{\phi}(1)$生成的主理想。

SageMath 例 5.2。 定理 5.3 尤其意味着， $^{\phi}F$ 中的所有元素都是 $\chi_{\phi}(1)$ 挠。下面通过一个例子来验证这一点。

```
sage: a = χ(1)
sage: a
6*T^2 + 3*T + 1
sage: [φ(a)(x) for x in F]
[0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
    0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0]
```

第二个定理可以看作是椭圆曲线的哈斯定理的类比 [Sil09，第五章，定理 1。1]。

***r*定理 5.4**。 设 $\chi_{\phi}(X)=\sum a_i X^r$，其中 $a_0,\ldots,a_r \in A = \mathbb{F}_q[T]$。对于任意正整数 $i=0$ $i<r$，我们有

$$\deg(a_i) \leqslant \frac{r-i}{r}\cdot d.$$

在弗罗贝尼乌斯范数这一特殊情形下，也就是说，对于系数 a_0，，我们有一个显式公式：若 $p \in A$ 表示 $\mathfrak{p}$ 的首一生成元，则有

$$a_0 = (-1)^{rd-d-r}\frac{p^{d/\deg(\mathfrak{p})}}{\mathrm{N}_{F/\mathbb{F}_q}(g_r)}.$$

需要指出的是，与椭圆曲线的情形不同，在 Drinfeld 模的框架下，定理 5.4 很容易证明，因为只需明确写出作用于 $\mathbf{M}(\tau^d)$ 上的 $\mathbf{M}(\phi)$ 的矩阵，并估计其系数的次数即可直接得到结论。此外，结合定理 5.3 和定理 5.4 可得以下界

$$\deg\left(|^{\phi}F| - \mathfrak{p}\right) \leqslant \frac{\deg\mathfrak{p}}{2}$$

对于任意形如 $\phi_T = z + g_1\tau + \tau^2$ 且具有 $F = \mathbb{F}_q(z)$ 的秩 2 Drinfeld 模 ϕ。这相当于亏格为 1 的曲线的有理点数的韦伊界。

定理 5.5 ([Pap23, 定理 4.3。2])。 定义在(F,γ) 上的两个 *Drinfeld* 模是 F-同源的，当且仅当它们具有相同的 *Frobenius* 自同态特征多项式。

5.1.2 计算 Frobenius 自同态特征多项式的方法综述

现在，我们来思考自同态特征多项式的计算，重点关注 Frobenius 情形。这个问题是椭圆曲线与同源密码学中的经典课题。对于有限域上的椭圆曲线，有理点的数量由 Frobenius 自同态的迹给出。首个用于计算该数量的确定性算法由 Schoof 提出 [Sch85]。Schoof 算法的工作方式是

利用除法多项式计算迹模若干不同素数的值，再通过中国剩余定理将其还原。

Musleh 和 Schost 等人提出了这种方法的 Drinfeld 模类比 [MS19, Mus18, Mus23]。他们介绍了两个版本：一种确定性方法，以及一种效率更高的蒙特卡罗方法。需要强调的是，这些方法只适用于秩 2 Drinfeld 模。这一限制使我们能够直接将椭圆曲线经典情形中的算法移植过来。

先前的方法还包括 Gekeler 提出的一种方法，该方法通过直接求解由恒等式 $\chi_\phi(\pi) = 0$ [Gek08], 导出的线性方程组来实现，其中 π 是 ϕ的 Frobenius 自同态。Musleh 在 [Mus23, § 4.4.1]中将其推广并实现到高秩情形。另一方面，Narayanan 提出了一种基于序列最小多项式的方法 [Nar18]。Musleh 和 Schost 对 Narayanan 所作部分假设的有效性表示怀疑，并在 [MS19, § 5]中提出了一种替代方案。

在 [CL26, § 4], 中，作者提出了一种适用于任意秩的 Frobenius 自同态计算方法。该方法基于这样一个观察：Frobenius 自同态不仅是 ϕ 的一个重要元素，也是 $F\{\tau\}$ 的一个重要元素：令 $d = [F : \mathbb{F}_q]$，则元素τ^d 是 $F\{\tau\}$ 的中心，而$F\{\tau\}$ 的中心为 $\mathbb{F}_q\{\tau\}$。由此可以证明，π 的特征多项式是 $\phi_T \in F\{\tau\}$ 的约化特征多项式，其中$F\{\tau\}$ 嵌入到一个在其中心上的次数为d^2 的中心单代数中。

定理 4.19 中提到的方法还提供了一种利用 Anderson 动机计算 Frobenius 自同态特征多项式的途径。有趣的是，经过优化及后续变体，上述所有方法各有优势，具体取决于输入参数的相对大小。它们在 [CL26, 图 1] 中进行了比较。

从这些计算中得到的一个重要启示是：椭圆曲线虽为 Drinfeld 模提供了熟悉的视角，但要想在远超秩 2 情形下 Frobenius 自同态这一受限问题的广泛范围内开发算法，关键在于将 Drinfeld 模作为一套独立的理论来理解。

此外，这些 Ore 多项式还赋予了一个中心单代数的结构，从而能够计算 Frobenius 的特征多项式。得益于定理 3.19，这些对象无需计算扭点和 Tate 模。

如需深入研究这一主题，请参阅 [Mus23] 第 4.4 节（仅讨论秩 2 情形下的 Frobenius 自同态）或 [MS19, § 4]（一般情形）。关于渐近复杂度的直接比较，请参阅 [CL26, Appendix A]；关于可复现的基准测试，请参阅 [LS24, § 4.4.2, 5.4.2, 6.4.1] 和 [ACLM23]。

5.1.3 计算同源

与椭圆曲线的情形不同，在有限域上的 Drinfeld 模的同源可以在多项式时间内计算。事实上，正如方程 (22) 所示，计算 $\mathrm{Hom}(\phi, \psi)$ 归结为求解一个关于A的线性方程组；当F 是有限域时，该方程组是有限维的。Wesolowski [Wes24] 和 Musleh [Mus23, § 7.3] 发展了这一思路，并由此得到以下定理。

定理 5.6 ([Mus23, 定理 7.3。1]). 设 ϕ, ψ 是两个秩为 r 的 *Drinfeld* 模。存在用于计算以下对象的算法

1. 一个由次数至多为 N 的同源构成的 $\mathbb{F}_q$-基，位于 $\mathrm{Hom}(\phi, \psi)$ 中，其关于 N 和 d 具有准立方复杂度，关于 r 具有准线性复杂度，

2. 一个 $\mathrm{Hom}(\phi,\psi)$ 的 $\mathbb{F}_q[\tau^d]$-基，其关于 d 具有拟六次复杂度，关于 r 具有准线性复杂度，

3. 以关于 d 和 r 的准立方复杂度求出$\mathrm{Hom}(\phi,\psi)$ 的一个 A-基。

注记 5.7。 Musleh [Mus23] 事实上给出了略低的复杂度，其中涉及矩阵乘法的指数。

SageMath 示例 5.3。 我们计算两个 Drinfeld 模 ϕ 和 ψ之间的同态空间。在此情况下，我们进一步观察到，该同态空间包含一个由常 Ore 多项式定义的同源，因此 ϕ 和 ψ 同构。

```
sage: φ = DrinfeldModule(A, [z, z, 1])
sage: ψ = DrinfeldModule(A, [z, 1-z, 1])
sage: H = Hom(φ, ψ)sage: H.basis()
[Drinfeld Module morphism:
From: Drinfeld module T |--> τ^2 + z*τ + z
To:   Drinfeld module T |--> τ^2 + (6*z + 1)*τ + z
Defn: τ + 1,Drinfeld Module morphism:
From: Drinfeld module T |--> τ^2 + z*τ + z
To:   Drinfeld module T |--> τ^2 + (6*z + 1)*τ + z
Defn: z + 6]
```

```
sage: H.basis_over_frobenius()
[Drinfeld Module morphism:
From: Drinfeld module T |--> τ^2 + z*τ + z
To:   Drinfeld module T |--> τ^2 + (6*z + 1)*τ + z
Defn: τ + 1,Drinfeld Module morphism:
From: Drinfeld module T |--> τ^2 + z*τ + z
To:   Drinfeld module T |--> τ^2 + (6*z + 1)*τ + z
Defn: τ + z]
```

```
sage: H.basis(degree=5)[Drinfeld Module morphism:
From: Drinfeld module T |--> τ^2 + z*τ + z
To:   Drinfeld module T |--> τ^2 + (6*z + 1)*τ + z
Defn: τ + 1,Drinfeld Module morphism:
From: Drinfeld module T |--> τ^2 + z*τ + z
To:   Drinfeld module T |--> τ^2 + (6*z + 1)*τ + z
Defn: τ + z,Drinfeld Module morphism:
From: Drinfeld module T |--> τ^2 + z*τ + z
To:   Drinfeld module T |--> τ^2 + (6*z + 1)*τ + z
Defn: τ^3 + τ^2,Drinfeld Module morphism:
From: Drinfeld module T |--> τ^2 + z*τ + z
To:   Drinfeld module T |--> τ^2 + (6*z + 1)*τ + z
Defn: τ^3 + z*τ^2,Drinfeld Module morphism:
From: Drinfeld module T |--> τ^2 + z*τ + z
To:   Drinfeld module T |--> τ^2 + (6*z + 1)*τ + z
Defn: τ^5 + τ^4,Drinfeld Module morphism:
From: Drinfeld module T |--> τ^2 + z*τ + z
To:   Drinfeld module T |--> τ^2 + (6*z + 1)*τ + z
Defn: τ^5 + z*τ^4]
```

5.1.4 超奇异性

再次令p 表示 $\mathfrak{p} = \ker\gamma$的首一生成元。根据定理 3.14 和定理 3.15， ϕ 在 $\mathfrak{p}$ 处的 Tate 模的秩为$r - \mathrm{h}(\phi)$，其系数环为$A_{\mathfrak{p}}$；其中r 是 ϕ的秩，而 $\mathrm{h}(\phi)$ 是弗罗贝尼乌斯高度。

定义 5.8. ϕ 称为普通，当 $\mathrm{h}(\phi) = 1$；而当 $\mathrm{h}(\phi) = r$时， ϕ 称为超奇异。

定理 5.9 ([Pap23，推论 4.2.14，定理 4.4。1])。以下性质彼此等价：

- ϕ 是超奇异的；
- $\phi[\mathfrak{p}]$ 是平凡的；
- $\phi_{\mathfrak{p}}$ 是纯不可分的；
- $\mathrm{End}_{F_s}(\phi)$ 具有最大 A-秩，即 r^2；
- $\chi_\phi \equiv X^r \pmod{\mathfrak{p}}$。

SageMath 示例 5.4。我们说明，如果在第四项中将 $\mathrm{End}_{F^s}(\phi)$ 替换为 $\mathrm{End}(\phi)$，定理 5.9 就不成立。

```
sage: φ = DrinfeldModule(A, [1, 0, z])
sage: φ.is_supersingular()
True
```

我们首先计算 $\mathrm{End}(\phi)$，并发现其维数为 2。

```
sage: End(φ).basis()
[Identity morphism of Drinfeld module T |--> z*τ^2 + 1,
 Endomorphism of Drinfeld module T |--> z*τ^2 + 1
  Defn: z]
```

然而，在某个扩张上确实存在更多同源。在我们的例子中，它们出现在 $L = F[\sqrt[8]{z}] = \mathbb{F}_{7^{16}}$ 上。

```
sage: L = F.extension(8)sage: φ_L = φ.change_A_field(L)
sage: End(φ_L).basis()
[Identity morphism of Drinfeld module T |--> z*τ^2 + 1,
Endomorphism of Drinfeld module T |--> z*τ^2 + 1
Defn: (z16^14 + z16^13 + 6*z16^11 + 5*z16^10 + z16^9 + 5*z16^8 + 2*z16^7 +
4*z16^6 + 4*z16^5 + 6*z16^4 + 2*z16^3 + 2)*τ,
Endomorphism of Drinfeld module T |--> z*τ^2 + 1
Defn: z16^15 + z16^14 + 3*z16^13 + z16^12 + 2*z16^11 + 5*z16^10 + 5*z16^9
+ 4*z16^8 + 6*z16^7 + 6*z16^6 + 2*z16^5 + 2*z16^4 + 4*z16^3 + 2*z16^2+ z16,
Endomorphism of Drinfeld module T |--> z*τ^2 + 1
Defn: (z16^15 + 2*z16^13 + 5*z16^12 + z16^11 + 2*z16^10 + 5*z16^9 + 2*z16
^8 + 5*z16^7 + 4*z16^5 + 4*z16^3 + z16^2 + z16 + 2)*τ]
```

注记 5.10. 在秩二的情形下，定理 5.9 的第三项表明，当且仅当 $\tau^{\deg(p)}$ 在 ϕ_p 中的系数为零时， ϕ 是超奇异的。类比椭圆曲线理论，这个系数有时称为 ϕ的*Hasse* 不变量 。在 [Gek08 中，

方程 3.6 和命题 3.7], Gekeler 注意到，可以通过 如下递归过程计算 Hasse 不变量。令 $\phi_T = z + g\tau + \Delta\tau^2$，我们设定$r_{\phi,0} = 1, r_{\phi,1} = g$，对于任意整数$k \geqslant 2$，递归定义

$$r_{\phi,k+2} = g^{q^{k+1}} r_{\phi,k+1} - \left(z^{q^{k+1}} - z\right)\Delta^{q^k} r_{\phi,k}.$$

那么， ϕ 的 Hasse 不变量为$r_{\phi,\deg(p)}$。

对于任意秩，超奇异 Drinfeld 模 ϕ 的特征多项式都具有非常特殊的形式：在 $\mathbb{F}_q[T,X]$, 上，我们有如下分解

$$\chi_\phi(X) = \prod_{i=1}^{r/a} \left(X^a - c_i p^b\right)$$

其中，a, b 是分数r $d\deg(\mathfrak{p})$ 的不可约形式，而c_i 属于 $\mathbb{F}_q$。根据定理 5.5，这尤其意味着两个秩相同的超奇异 Drinfeld 模在F^s上同源。

SageMath 示例 5.5。 我们继续前面的例子，并验证 ϕ 的特征多项式具有预期的形式（这里$a = b = 1, p = T - 1, c_1 = 5z$ 和$c_2 = 2z + 5$）。

```
sage: χ = φ.frobenius_charpoly()
sage: χ = χ.change_ring(F['T'])  # 我们将标量扩张到F
sage: χ.factor()
(X + 2*z*T + 5*z) * (X + (5*z + 2)*T + 2*z + 5)
```

我们选取另一个与 ϕ不同源的超奇异 Drinfeld 模。

```
sage: ψ = DrinfeldModule(A, [1, 0, z^2])
sage: φ.is_isogenous(ψ)
False
```

但我们发现，它们在 F 的 $q^2 - 1 = 48$ 次扩张上变为同源。

```
sage: L = F.extension(48)
sage: φ_L = φ.change_A_field(L)
sage: ψ_L = ψ.change_A_field(L)
sage: φ_L.is_isogenous(ψ_L)
True
```

最后，我们提及以下命题。特别是，它说明在 F^s上给定秩的超奇异 Drinfeld 模只有有限多个。

命题 5.11 ([Gek91, 命题 4.2])。 设 $\phi : A \to F^s\{\tau\}$ 是一个秩为 r 的超奇异 *Drinfeld* 模。那么， ϕ 与一个定义在 $\mathbb{F}_\mathfrak{p}$的 r 次扩张上的 *Drinfeld* 模 F^s-同构。

5.1.5 秩二情形下的自同态环

假设秩为 2，超奇异性的信息也可以从自同态环的结构中看出。有限域上的椭圆曲线是普通的，当且仅当它在代数闭包上的自同态环是交换的 [Sil09，第五章，第 § 3] 节。在

这种情况下，椭圆曲线的自同态环是二次数域中的一个序。否则，它是四元数代数中的一个极大序。秩为 2 的 Drinfeld 模也如此。回想一下，$K = \mathrm{Fracc}(A)$ 以及 $\mathrm{End}^0(\phi) = K \otimes_A \mathrm{End}(\phi)$（定理 4.27）。

定理 5.12([Car18，定理 6.4。2])。 设 $\phi\colon A \to F\{\tau\}$ 是一个秩为 2 的普通 *Drinfeld* 模。那么 $\mathrm{End}^0(\phi)$ 是由 ϕ 的 *Frobenius* 自同态生成的虚二次函数域。换言之，我们有一个 A-代数同构

$$\mathrm{End}^0(\phi) \simeq K[X]/(\chi_\phi(X)).$$

由定理 5.12 可知，在普通情形下，$\mathrm{End}(\phi)$ 表现为虚二次函数域中的一个序。我们回顾一下，这类域包含唯一的极大序：它们的整数环，同时也是唯一一个 Dedekind 整环。若将其记为 $\mathcal{O}_{\mathrm{End}^0(\phi)}$，其他序恰好是形如 $\mathcal{O} = A + f\mathcal{O}_{\mathrm{End}^0(\phi)}$ 的集合，其中 f 属于 A。多项式 f 称为 $\mathcal{O}$ 的*导子*。它满足 $\mathcal{O}$ 在 $\mathcal{O}_{\mathrm{End}^0(\phi)}$ 中的指标为 $q^{\deg(f)}$。

SageMath 示例 5.6。 我们考虑以下秩 2 的普通 Drinfeld 模

```
sage: φ = DrinfeldModule(A, [z, z, 1])
sage: φ
Drinfeld module T |--> τ^2 + z*τ + z
sage: φ.is_ordinary()
True
```

并计算其自同态环

```
sage: End(φ).basis()
[Identity morphism of Drinfeld module T |--> τ^2 + z*τ + z,
 Endomorphism of Drinfeld module T |--> τ^2 + z*τ + z
  Defn: z*τ + z]
```

注意到输出的基的第二个自同态为 $T - \pi$，我们得出 $\mathrm{End}(\phi)$ 由 Frobenius 生成，即

$$\mathrm{End}(\phi) \simeq A[X]/(\chi_\phi(X)).$$

这比定理 5.12 更为精确，后者只给出了在标量扩张到 K 之后的这一同构。

在我们的例子中，还可以验证 $\chi_\phi(X)$ 的判别式是无平方因子的，这意味着 $\mathrm{End}(\phi)$ 是 $\mathrm{End}^0(\phi)$ 的极大序。

```
sage: χ = φ.frobenius_charpoly()
sage: χ.discriminant()
5*T + 6
```

相反，当 ϕ 为超奇异时，$\mathrm{End}^0(\phi)$ 仍包含由 Frobenius 自同态生成的二次域，但它可能严格更大。它的次数实际上为 2 或 4；在后一种情况下，它是 K 上的四元数代数，即一个维数为 4 的中心单代数，而 $\mathrm{End}(\phi)$ 是 $\mathrm{End}^0(\phi)$ 中的一个序。SageMath 示例 5.4 展示了这一情形。

无论如何，尽管 $\mathrm{End}(\phi)$ 可能是交换的，且 ϕ 是超奇异的，但由定理 5.9 和定理 5.12 可得以下结论。

命题 5.13. 秩为2 的 *Drinfeld* 模 ϕ 是超奇异的，当且仅当$\mathrm{End}_{F^s}(\phi)$ 是非交换的。

这项研究非常理论化。要进行具体计算，我们必须转而采用截然不同的视角，通过线性代数方法计算基（见小节 5.1.3）。

5.1.6 Picard 群的作用

我们以第 5.1.5 小节中确立的分类为基础，介绍一种情形：其中自同态及其类群可以用超椭圆曲线来描述。有限域上的普通椭圆曲线与有限域上的（某些）普通秩 2 Drinfeld 模具有一个共同性质：自同态环的类群在一个同构类集合上自由且传递地作用。借助这类作用，我们可以将 Drinfeld 模块的同源视为理想类，并且能够非常明确地描述它们。现在，我们将说明如何利用虚超椭圆曲线计算这一群作用的一个具体实例。

和之前一样，仍设 F 是一个有限域，且 ϕ 是 (F, γ) 上的一个秩为 2 的 Drinfeld 模。设 $\chi_\phi \in \mathrm{A}[\mathrm{X}]$ 是 Frobenius 自同态的特征多项式。我们有 $\chi_\phi(\mathrm{X}) = \mathrm{X}^2 + \mathrm{aX} + \mathrm{b}$；根据定理 5.4，我们知道多项式 a、b $\in \mathrm{A} = \mathbb{F}_q[\mathrm{T}]$ 满足 $\deg(\mathrm{a}) \leqslant \mathrm{d}/2$ 且 $\deg(\mathrm{b}) = \mathrm{d}$。由于 a 和 b 都属于 $\mathbb{F}_q[\mathrm{T}],$，多项式 χ_ϕ 可以看作 T 和 X 的二元多项式。因此，它定义了一个代数簇。我们作如下假设。

- 我们假设 ϕ 是普通的。这意味着a 非零（见定理 5.9），因此 χ_ϕ 定义了一条超椭圆曲线，记作 $\mathcal{H}$
- 我们假设 $\mathcal{H}$ 是光滑的，且d 为奇数。在这种情况下， $\mathcal{H}$ 是虚的，亏格为$g = \frac{d-1}{2}$。

事实证明，这些假设完全确定了 ϕ的F-自同态环，以及所有与之F同源的 Drinfeld 模 ϕ的自同态环。事实上，令$A_{\mathcal{H}} = A[X]/(\chi_\phi(X))$表示 $\mathcal{H}$的坐标环，则映射

$$A[X] \to \mathrm{End}(\phi)$$
$$P(T, X) \mapsto P(\phi_T, \pi)$$

通过$A_{\mathcal{H}}$分解，从而得到一个单射态射$A_{\mathcal{H}} \to \mathrm{End}(\phi)$。由于$A_{\mathcal{H}}$ 是 Dedekind 整环，因此它是其所在二次函数域的极大序，由此可得 $\mathrm{End}(\phi) \simeq A_{\mathcal{H}}$。关键的是，这个显式的环同构给出了一个显式的群同构

$$\mathrm{Pic}^0(\mathcal{H}) \simeq \mathrm{Cl}(\mathrm{End}(\phi)),$$

其中 $\mathrm{Pic}^0(\mathcal{H})$ 是 $\mathcal{H}$的零次皮卡群。

作用的抽象定义。 对于自同态环 $\mathrm{End}(\phi)$的理想 $\mathfrak{a}$，我们定义 $u_{\mathfrak{a}} = \mathrm{rgcd}(\{a \in \mathfrak{a}\})$，即属于 $\mathfrak{a}$ 的 Ore 多项式的右最大公因子。设 ψ 是一个与 ϕ 同源的 Drinfeld 模F。由定理 4.4，$u_{\mathfrak{a}}$ 定义了从 ψ 到一个 Drinfeld 模的同源映射，我们将其记为 $\psi^{\mathfrak{a}}$，并记作

$$\mathfrak{a} * \psi = \psi^{\mathfrak{a}}.$$

如果 $\mathfrak{a}$ 是主理想，也就是说，它由 ψ 的一个自同态生成，那么 $u_{\mathfrak{a}}$ 是 $\mathfrak{a}$ 的一个生成元，而 ψ 等于 $\mathfrak{a} * \psi$。

SageMath 示例 5.7。我们用 SageMath 示例 5.6 中的 Drinfeld 模 ϕ来说明上述构造。遗憾的是，SageMath 尚未实现对 $\mathrm{End}(\phi)$ 中理想的运算。我们通过以下方式解决这一问题：将环 $\mathrm{End}(\phi)$ 重构为商 $E = A[X]/(\chi_\phi(X))$，并定义函数 `endomorphism`，将 E 中的元素转换为实际的自同态。

```
sage: E.<X> = A.extension(χ)sage: def endomorphism(elt, ψ):  # ψ是
与 φ...:     π = ψ.frobenius_endomorphism()
....:     return E(elt).lift()(π)同源的 Drinfeld 模
```

现在，我们只需按照定义即可编写函数 `action`。

```
sage: def action(a, ψ):
....:     u = ψ.hom(0)
....:     for elt in a.gens():
....:         v = endomorphism(elt, ψ)
....:         u = u.right_gcd(v)
....:     return u.codomain()
```

我们考虑理想 $\mathfrak{a} = \langle T + 4, X + 3 \rangle$，并计算 $\psi = \mathfrak{a} * \phi$。

```
sage: a = E.ideal([T+4, X+3])
sage: ψ = action(a, φ)
sage: ψ
Drinfeld module T |--> τ^2 + (6*z + 1)*τ + z
```

我们注意到，$\mathfrak{a}^2$ 是由 $T + 4$生成的主理想。因此，它在 ϕ上的作用是平凡的，也就是说，$\mathfrak{a} * \psi = \mathfrak{a}^2 * \phi = \phi$。下面对此进行验证。

```
sage: action(a, ψ)
Drinfeld module T |--> τ^2 + z*τ + z
sage: action(a, ψ) == φ
True
```

由前文可知，映射 $*$ 在与 ϕ同源的 Drinfeld 模同构类集合上定义了一个 $\mathrm{Cl}(\mathrm{End}(\phi))$ 的群作用。稍微滥用一下记号，仍将 $\mathrm{Cl}(\mathrm{End}(\phi))$ 的群作用记为 $*$。后者是自由且传递的。这可以通过繁琐的计算直接证明。更具概念性的做法（但超出了本文档的范围），是将类似的群作用（已知其自由且传递）“模 $\mathfrak{p}$约化”；该群作用存在于C_∞上的 Drinfeld 模中，并且处于函数域类域论的框架下（参见 [Hay11, 定理 9.3] 或 [LS24, § 2.3]）。

群作用的实际计算。我们在 SageMath 示例 5.7 中看到，计算理想在 $\mathrm{End}(\phi)$ 上的作用可以轻松实现。若要进一步计算 $\mathrm{Cl}(\mathrm{End}(\phi))$的作用，只需为 $\mathrm{Cl}(\mathrm{End}(\phi))$的元素找到一种高效的表示。鉴于 $\mathrm{End}(\phi)$ 同构于 $A_{\mathcal{H}}$，且 $A_{\mathcal{H}}$ 是虚超椭圆曲线的坐标环，我们有一个显式的群同构

坐标环，因此我们有一个显式的群同构

$$\mathrm{Pic}^0(\mathcal{H}) \simeq \mathrm{Cl}(\mathrm{End}(\phi)),$$

其中 $\mathrm{Pic}^0(\mathcal{H})$ 是由 $\mathcal{H}$ 的次数为零的除子按有理等价关系构成的群。此外，$\mathrm{Pic}^0(\mathcal{H})$ 的元素可由*Mumford* 坐标 [CFA+12（定理 14）表示，即 满足下列条件的多项式对$(u, v) \in A^2$

$$\deg(u) < \deg(v) \leqslant g,$$

其中$g = d_2^{-1}$是曲线 $\mathcal{H}$的亏格。由(u, v) 表示的元素是 $\langle u, X - v\rangle$的理想类。就 $\mathrm{End}(\phi)$ 而言，这意味着(u, v) 表示由自同态 ϕ_u 和 $\pi - \phi_v$生成的理想类。

回到群作用 $*$的定义，Mumford 坐标使我们能够用两个明确的生成元表示作用群的元素。若(u, v) 是表示理想 $\mathfrak{a}$的理想类的 Mumford 坐标，那么计算 $\mathfrak{a} * \psi$ 仅相当于计算 Ore 多项式 ψ_u 和 $\pi - \psi_v$的右最大公因子。例如，可以使用欧几里得算法的一种变体来完成这一计算，详见 §3.2。这意味着，计算群作用仅相当于计算两个 Ore 多项式的右最大公因子，以及对 Ore 多项式进行右欧几里得除法。 [LS24]中给出了明确的复杂度分析和一种实现。

与椭圆曲线的比较。群作用 $*$ 的计算如此简单，这表明它与椭圆曲线的情形存在深刻的差异。对于椭圆曲线，群作用是通过同源的核来定义的。若E 是有限域 $\mathbb{F}_q$上的一条普通椭圆曲线，则群作用中的同源定义如下。设I 是 $\mathrm{End}(E)$中的一个理想，并考虑

$$V_I = \bigcap_{f \in I} \ker(f).$$

这些核并不局限于有理点。因此，V_I 是E 的点群的一个子群（但不一定是$E(\mathbb{F}_q)$的子群）。因此，存在一条椭圆曲线E^I，以及一个从E 到E^I的同源 ι_I，其核恰好是V_I。

归根结底，截至撰写本文时，计算群作用仍相当复杂 [DFKS18]。这是因为计算需要处理挠点，而这些点可能位于基域的较大扩张中。有鉴于此，我们提出两点理由，解释为什么在 Drinfeld 模的情形下群作用易于计算，而在椭圆曲线的情形下却并非如此。

1. 第一个原因是对 Ore 多项式（其定义所需的信息包含在F中的对象）进行操作，而不是对它们的核（可能存在于F的大型扩张中的对象）进行操作。Ore 多项式作为 Drinfeld 模理论的潜在空间而存在，使我们能够在 Drinfeld 模的几乎所有计算方面利用高效的 Ore 多项式运算。对于 Drinfeld 模的同源核的操作，这与 Ore 多项式的算术相容，具体而言，一族 Ore 多项式的核的交集就是该族右最大公因子的核。

2. 第二个原因与函数域算术有关。正如我们所见，在 Drinfeld 模的情形下，Frobenius 自同态的特征多项式定义了一个代数簇。在我们的假设下，这个代数簇是

一条虚超椭圆曲线，这使我们能够将 Drinfeld模自同态环的类群作为该曲线的零次皮卡群来处理。这是运用函数域算术的直接例证。

注 5.14. 现在我们来说明，此处介绍的群作用是一个更一般构造的实例。在引言中，我们指出，Drinfeld 模可以定义在某个环 A' 上，其中 A 是有限域上某条曲线的函数环。我们还对曲线添加了假设，以确保 A' 是一个 Dedekind 环。我们的情形 $A = \mathbb{F}_q[T]$ 对应于选取曲线 $\mathbb{P}^1_{\mathbb{F}_q}$。但更一般地，我们可以研究定义在 A'上的 Drinfeld 模，称为 *Drinfeld* A'*-模*。在这一框架下，一个经典结果表明，A' 的类群在定义于 C_∞上的秩 1 Drinfeld A'-模的同构类集合上自由且传递地作用。作为简写，我们将这一群作用记为 $\mathrm{GA}(A')$。

在我们的情形中，$\mathbb{F}_q[T]$ 的类群是平凡的，所有秩为 1 的 Drinfeld A-模彼此同构。可以证明，在 (F,γ)上的秩 1 Drinfeld $A_{\mathcal{H}}$-模范畴与 $(F,\ \gamma)$ 上的秩 2 Drinfeld A-模范畴之间存在范畴等价，且后者的自同态环为 $A_{\mathcal{H}}$。利用这一对应关系，我们可以还原本节计算出的群作用（$A_{\mathcal{H}}$ 的类群作用于自同态环为 $A_{\mathcal{H}}$的秩 2 Drinfeld 模的同构类），方法是将 $\mathrm{GA}(A_{\mathcal{H}})$ 模一个素理想“约化”。

一般的群作用非常显式：对于理想 $\mathfrak{a} \subset A'$ 和 Drinfeld A’-模ϕ，相应的同源为 $\mathrm{rgcd}(\{\phi_a : a \in \mathfrak{a}\})$。

5.2 全局函数域上的情形

现在考虑基域为$F = \mathbb{F}_q(z)$的情形，其中z 是一个形式变量，而 $\gamma : A \to F$ 是将T 映到z的环同态。尽管F 当然与其自身 $\mathbb{F}_q(T)$ 同构，但在下文中，使用不同的变量名表示F 将十分重要，以避免记号混淆，尤其是在讨论 Anderson 动机时。

这种情形无疑与有限域的情形密切相关，因为任意一个K 上的 Drinfeld 模都可以模掉K的几乎所有赋值点 $\mathfrak{p}$，从而得到一个有限域上的 Drinfeld 模。另一方面，它也与解析理论有关（见第 3.3 小节）：由于F 嵌入C_∞，一个F 上的 Drinfeld 模可以视为C_∞上的 Drinfeld 模。

5.2.1 L级数

我们从一个 Drinfeld 模 ϕ 开始：$A \to F\{\tau\}$，并记

$$\phi_T = z + g_1\tau + g_2\tau^2 + \cdots + g_r\tau^r$$

对所有i，都有$g_i \in F$。对于F的几乎所有赋值点 $\mathfrak{p}$，都可以将所有g_i约化，因此也可以将 ϕ 模 $\mathfrak{p}$ 约化。我们将此约化记为 $\phi \bmod \mathfrak{p} : A \to \mathbb{F}_{\mathfrak{p}}\{\tau\}$。这里 $\mathbb{F}_{\mathfrak{p}}$ 表示 $\mathfrak{p}$ 处的剩余域，它是 $\mathbb{F}_q$ 的有限扩张，因此是一个有限域。于是可以考虑其 Frobenius 自同态的特征多项式：记为$\chi_{\phi} \bmod \mathfrak{p}(X)$。

ϕ 的L级数由所有这些特征多项式组合而成。为简便起见，我们假设所有g_i 都属于A。在这一额外假设下，约化

ϕ 模 $\mathfrak{p}$ 对所有赋值点 $\mathfrak{p}$ 都有定义，因此χ_ϕ 模 $\mathfrak{p}(X)$ 也有定义。于是L级数由以下无穷乘积给出：

$$L(\phi; X) = \prod_{\mathfrak{p}} \frac{\chi_{\phi \bmod \mathfrak{p}}(0)}{\chi_{\phi \bmod \mathfrak{p}}(X^{\deg \mathfrak{p}})}.$$

上面分数的分子是一个归一化因子：它确保所有因子的常数项都是 1。级数收敛，是因为次数不超过任意给定常数的赋值点只有有限多个。事实上，前面两个观察表明，对于所有n，$L(\phi;X) \mod X^n$ 都由有限个因子的乘积给出；因此该级数在$K[[X]]$中收敛。

可以证明，$L(\phi;X)$ 不只是一个形式级数，而且在C_∞上收敛；换言之，它定义了一个解析整函数。事实证明，与数域情形类似，$L(\phi;1)$ 的值，以及更一般地，$L(\phi;X)$ 在$X = 1$处的泰勒展开，编码了大量算术信息。下面的例子是这种思想的一个初步而惊人的体现。

例 5.15. 我们来计算由$c_T = z + \tau$定义的 Carlitz 模c 的L级数。由例 5.2 可知，$\chi_c \bmod \mathfrak{p}(X) = X - \mathfrak{p}$。将其代入$L$级数的定义，我们得到

$$L(c; X) = \prod_{\mathfrak{p}} \frac{\mathfrak{p}}{X^{\deg \mathfrak{p}} - \mathfrak{p}} = \prod_{\mathfrak{p}} \frac{1}{1 - X^{\deg \mathfrak{p}} \mathfrak{p}^{-1}}$$

其中乘积遍历 F 的所有处，也就是 F 上所有不可约首一多项式。现在我们注意到，上述公式与定义 Carlitz ζ 函数的公式 (11) 的欧拉乘积十分相似；事实上，我们有关系式 $L(c;1) = \zeta_C(1)$。

前面的例子启发我们在一般的L级数定义中引入变量s，如下所示：

$$L(\phi; X, s) = \prod_{\mathfrak{p}} \frac{\chi_{\phi \bmod \mathfrak{p}}(0)}{\chi_{\phi \bmod \mathfrak{p}}(X^{\deg \mathfrak{p}} \mathfrak{p}^{-s})}. \tag{23}$$

事实上，采用这个定义后，对于所有$s \in \mathbb{Z}$，关系式$L(c; 1, s) = \zeta_C(s + 1)$ 现在都成立。

Taelman 类数公式。 除了 Carlitz 模这个例子之外，Taelman 在 [Tae12] 中证明，对于任意 Drinfeld 模 $\phi : A \to F\{\tau\}$，值 $L(\phi; 1)$ 具有一种精彩的算术诠释，其精神与经典类数公式相同。简要回顾一下，该公式将数域的 Dedekind ζ 函数的特殊值与若干算术不变量联系起来：判别式、单位根群、类数和调节子。关于该公式的精确陈述及证明，请参阅 [Neu99, 第七章，推论 5。11]

Taelman公式涉及类数和调节子在函数域中的类比。二者都是通过我们在第 3.3 小节中引入的指数函数e_ϕ 来定义的。简单回顾一下，e_ϕ 是$F\{\{\tau\}\}$中的 Ore 级数。此外，令 $F_\infty := \mathbb{F}_q((1/z))$，$e_\phi$ 在K_∞ 上的限制仍定义了一个解析函数$e_\phi : F_\infty \to F_\infty$，满足函数方程

$$\forall a \in A, \quad \forall x \in F_\infty, \quad e_\phi(\gamma(a)x) = \phi_a(e_\phi(x)).$$

换句话说，它定义了一个A-线性映射$F_\infty \to {}^{\phi}F_\infty$，其中定义域上的$A$-模结构由$\gamma$诱导；并且我们回顾一下，${}^{\phi}F_\infty$是赋予了来自$\phi$的$A$-模结构的$F_\infty$。$\phi$的类模 定义为商$A$-模

$$H_\phi := \frac{{}^{\phi}F_\infty}{{}^{\phi}R + e_\phi(F_\infty)}$$

其中我们设$R := \mathbb{F}_q[z] \subset F$。Taelman [Tae12，命题 5] 证明了H^ϕ是一个有限A-模，因此我们可以考虑其欧拉–庞加莱特征$|H_\phi|$（见第 1.2 小节）。

为了定义调节子的类似物，我们引入 Taelman单位模：

$$U_\phi := e_\phi^{-1}(R) = \left\{x \in F_\infty \mid e_\phi(x) \in R\right\}.$$

Taelman [Tae12，定理 1] 证明了U^ϕ是R中的一条F_∞-直线；记$u_\phi \in K_\infty$为满足$\gamma(u^\phi)$生成U^ϕ的元素。Taelman 的定理现在可表述如下。

定理 5.16（Taelman 类数公式）。对于所有 *Drinfeld* 模$\phi: A \to F\{\tau\}$，有

$$L(\phi;1)A = u_\phi \cdot |H_\phi|.$$

例 5.17。当ϕ是 Carlitz 模时，类模H^ϕ是平凡的，因此有$|H_\phi| = A$。由定理 5.16 可知，Taelman格U^ϕ由$L(\phi;1) = \zeta_C(1)$生成。回到定义，我们得出$\zeta_C(1)$在指数映射e^ϕ下的像是一个多项式；实际上，它是常数多项式 1，即，有$e_\phi\left(\zeta_C(1)\right) = 1$。注意收敛定义域后，我们得到$\zeta_C(1) = \ell_\phi(1)$，其中$\ell_\phi$是 Carlitz 模的对数。

SageMath 示例 5.8。我们可以在 SageMath 中按如下方式检查前面的内容。

```
sage: φ = CarlitzModule(A)
sage: φ.class_polynomial()_1
```

```
sage: lC = φ.logarithm(prec=100)sage: lC
z + (6/(T^7 + 6*T))*z^7 + (1/(T^56 + 6*T^50 + 6*T^8 + T^2))*z^49 + O(z^100)
sage: lC = lC.polynomial()  # 我们去掉O(·)，以便能够计算sage: lC(1) + O(1/T^40)
1 + 6*T^-7 + 6*T^-13 + 6*T^-19 + 6*T^-25 + 6*T^-31 + 6*T^-37 + O(T^-40)
```

根据 Taelman 定理，我们注意到，前一个值与我们在 SageMath 示例 2.3 中计算出的 Carlitz ζ 函数在$s = 1$处的值一致。

Anderson公式。Taelman公式以及关于 Drinfeld 模的L级数的诸多成果，都是 Anderson 一条优美公式的推论 [And00] 。粗略地说，该公式将$L(\phi;X)$表示为一个单一算子σ的余特征多项式，如下所示：

$$L(\phi;X) = \det{}_{K[X]}\left(\mathrm{id} - X\sigma\right). \tag{24}$$

其缺点在于，σ作用的空间不是有限维的；因此，定义其余特征多项式时需要格外谨慎，所得结果是级数而不是

多项式。实际上，Anderson 公式有多种变体。下面我们简要介绍其动机版本，其中算子 σ 是由与 ϕ 相关联的 Anderson 动机 $\mathbf{M}(\phi)$ 构造而成的。

我们回顾一下，$\mathbf{M}(\phi)$ 是一个在$F[T]$上的模。我们考虑对偶动机$M := \mathbf{M}(\phi)^\vee$（见第 3.4.3 小节）。我们进一步引入卡勒微分空间 $\Omega^1_{F/\mathbb{F}_q}$ 以及作用于其上的q-卡蒂埃算子 S。由于$F = \mathbb{F}_q(z)$，我们直接得到 $\Omega^1_{F/\mathbb{F}_q} = F{\cdot}dz$。$q$-卡蒂埃算子还有一个非常显式的描述：在多项式上，它定义为

$$S\Big(\sum_i a_i z^i dz\Big) = \sum_i a_{qi+q-1} z^i dz \qquad (a_i \in \mathbb{F}_q)$$

并借助公式$S(ab^{-1}dz) = S(ab^{q-1})b^{-1}dz$ 将其扩展至 $\Omega^1_{F/\mathbb{F}_q}$，其中$a$、$b \in \mathbb{F}_q[z]$。我们还考虑空间$F[T]{\cdot}dz$，并通过$T$-线性将$S$ 扩展到该空间[2]。

现在我们可以定义方程（24）中出现的算子 σ 了。它作用于空间

$$M^\star = \mathrm{Hom}_{F[T]}\big(M,\, F[T]{\cdot}dz\big)$$

by

$$\sigma : f \mapsto S \circ f \circ \tau_M \quad (f \in M^\star).$$

与S类似，算子 σ 关于变量T是线性的，但关于z 是半线性的，具体来说，对任意$f \in M^\star$，它满足 $\sigma(z^q f) = z{\cdot}\sigma(f)$。后一个性质是定义 σ的余特征多项式的关键。粗略地说，σ 会降低变量z 的幂次，因此z 的较大正幂和负幂所作的贡献可以忽略不计。于是，我们可以考察它在越来越大的有限维空间$\langle z^i \rangle_{|i|\leqslant N}$上的作用，以此近似求出 σ 的余特征多项式；令N趋于无穷，最终便得到所需结果。

在 [And00], Anderson 为这一粗略构想奠定了坚实基础，并为完整证明等式 (24) 铺平了道路。

值得注意的是，Anderson公式也相当明确，非常适合在计算机上实现：在 [CG24], 中，作者将其转化为一种实际的快速算法，用于计算附属于 Drinfeld 模 ϕ 的L级数$L(\phi; X)$，以及更一般的$L(\phi; X,s)$。

SageMath 示例 5.9. 该算法已在 SageMath 中实现，实际表现非常出色，能够在几秒钟内计算任意L级数的数千项。

```
sage: ϕ = DrinfeldModule(A, [T, T^2, 1])sage: ϕ.Lseries(prec=30)
(6*T^-5 + 6*T^-11 + 6*T^-17 + 6*T^-23 + 6*T^-29 + O(T^-30))*X + 1 + O(T^-30)
sage: ϕ.Lseries(1, prec=40)  # 在 1 处的值
1 + 6*T^-5 + 6*T^-11 + 6*T^-17 + 6*T^-23 + 6*T^-29 + 6*T^-35 + O(T^-40)
```

5.2.2 三联图：秩-2Drinfeld 模、数域上的椭圆曲线、函数域上的椭圆曲线

在本段中，我们汇集并比较三种经典情形下同源的最小次数上界：数域上的椭圆曲线、秩 2 的 Drinfeld 模

[2]对于一般的A，我们应改为考虑 $\Omega^1_{A\otimes F/A} = A \otimes \Omega^1_{F/\mathbb{F}_q}$，并以类似的方式通过$A$-线性将$S$ 扩展到其中。

以及函数域上的椭圆曲线。我们希望读者能体会到，至少在这个特定例子中，数域上的椭圆曲线在函数域情形下的最佳类比实际上是秩 2 的 Drinfeld 模，而不是函数域上的椭圆曲线。

我们研究的估计有两类：一类是两个对象之间同源的最小次数上界，另一类是对任一同源类中相关j不变量的高度进行估计。

设L 是一个数域。我们用h 表示对数魏尔高度，对元素 $\alpha \in L$，其定义为

$$h(\alpha) = \frac{1}{[L:\mathbb{Q}]} \sum_{v \in M_L} [L_v : \mathbb{Q}_v] \log \max\{1, \|\alpha\|_v\},$$

其中M_L 是L的赋值点集合；对于$v \in M_L$，我们用 $\|\cdot\|_v$ 表示相应的绝对值，用L_v 表示 L 在v处的完备化。

定理 5.18([GR14])。 设 E 和 E' 是两条 L-同源椭圆曲线。那么存在一个 L-同源 $f\colon E \to \overline{E}'$，使得

$$\deg(f) \leqslant c_0 \cdot [L:\mathbb{Q}] \cdot h(j)^2,$$

其中 j 是椭圆曲线 E 的 j 不变量。

我们强调，E 与E' 之间存在许多同源不满足定理 5.18 给出的次数界。相比之下，以下定理讨论的是一个不同但相关的问题；它适用于任意同源，并且对最小次数同源给出的界更精确。

定理 5.19 ([Paz19，定理 1。1])。 设 $f\colon E \to E'$ 是椭圆曲线 E 和 E' 之间的 L-同源，其 j 不变量分别为 j 和 j'。那么

$$|h(j) - h(j')| \leqslant 10 + 12 \log(\deg f).$$

魏尔高度的 Northcott 性质表明，具有有界高度和有界次数的代数数集合是有限的。因此，结合前两个定理可知，在一个同源类中，定义在固定数域上的椭圆曲线只有有限多个 L-同构类。

本小节余下部分旨在介绍 Drinfeld 模以及定义在函数域上的椭圆曲线的类似结果。本小节介绍的结果总结于图 2 中。

回顾一下，$\mathrm{A} = \mathbb{F}_q[\mathrm{T}]$ 且 $\mathrm{K} = \mathbb{F}_q(\mathrm{T})$。令 M_K 表示 K 的赋值点集合。对于赋值点 $\mathrm{v} \in \mathrm{M}_K$，记 $\|\cdot\|_v$ 为按如下方式归一化的绝对值：若 $\mathfrak{p} \in \mathrm{A}$ 是与 v 对应的有限处，则 $\|\mathrm{x}\|_v = \mathfrak{q}^{-\deg(p)\cdot \mathrm{val}_{\mathfrak{p}}(\mathrm{x})}$；若 $\mathfrak{p} \in \mathrm{A}$ 是与 v 对应的无限处，则 $\|\mathrm{x}\|_v = \mathfrak{q}^{deg(x)}$。设 F/K 是 K 的有限扩张。对于延拓赋值点 $\mathrm{w} \in \mathrm{M}_K$的赋值点 $\mathrm{v} \in \mathrm{M}_F$，记 $\|\cdot\|_v$ 为相应的绝对值，使得对任意 $\mathrm{x} \in \mathrm{K}$，均有 $\|\mathrm{x}\|_v = \|\mathrm{x}\|_w$。对于由 F 中元素组成的 n 元组 $\mathrm{x} = (\mathrm{x}_1, \ldots, \mathrm{x}_n)$，定义其对数魏尔高度 h 如下：

$$h(x) = \frac{1}{[F:K]} \sum_{v \in M_K} [F_v : K_v] \log \max\{\|x_1\|_v, \ldots, \|x_n\|_v\}. \tag{25}$$

注记 5.20。 方程（25）的对数魏尔高度与定理 5.8 中使用的弗罗贝尼乌斯高度是完全不同的概念。在文献中，它们都称为“高度”，并且都记作 $h(\cdot)$。上下文通常能够明确其含义。

定理 5.21 （[DD99，定理 1。3]）。 设 ϕ 和 ϕ' 是定义在 F 上的两个秩为 r 的 F^s-同源 *Drinfeld* 模。那么，存在一个 F^s-同源 $f:\ \phi \to \phi'$，使得

$$\deg(f) \leqslant c_0[F:K] \cdot h(\phi')^{10\cdot 3^7},$$

其中 $h(\phi')$ 是 *Drinfeld* 模 ϕ' 的 *Potemine* 不变量组的高度（参见定理 *4.13*）。

定理 5.22([BPR21，定理 3。1])。 设 $f:\ \phi \to \phi'$ 是两个秩为 r 的 *Drinfeld* 模之间的 F^s-同源。假设核 $f\ \subseteq \phi[N]$。那么

$$|h(\phi') - h(\phi)| \leqslant \deg N + \frac{q}{q-1} - \frac{q^r}{q^r-1},$$

其中 $h(\phi)$ 和 $h(\phi')$ 分别是 *Drinfeld* 模ϕ 和 ϕ'的 *Potemine* 不变量组的高度。

此外，若 $r\ = 2$，则有

$$|h(j') - h(j)| \leqslant q + \frac{q^2-1}{2}\left(\log\deg f + \log\left(1 + \frac{1}{q}h(j')\right)\right),$$

其中 j 和 j' 分别是 *Drinfeld* 模 ϕ 和 ϕ'的 j 不变量。

同样，结合前两个定理和 Northcott 性质可得，秩 2 Drinfeld 模的同源类中仅包含有限多个同构类。

注 5.23. 对于平行四边形构型中的同源，已有更精细的结果，参见近期文章 [BGP25]。

最后，设 F 是定义在完美域上的亏格为g 的光滑射影几何不可约曲线的函数域。对于定义在F上的椭圆曲线，有以下结论。

定理 5.24 ([GP22，定理 B]). 设 E 和 E' 是两条 F^s-同源椭圆曲线，其 j 不变量分别为 j 和 j'。那么，存在一个 F^s-同源 $f: E\ \to E'$，使得

$$\deg(f) \leqslant 49 \cdot \max\{1,g\} \cdot \max\left\{\frac{\deg_{ins} j}{\deg_{ins} j'}, \frac{\deg_{ins} j'}{\deg_{ins} j}\right\},$$

其中$\deg_{ins}$ 表示非可分次数。

定理 5.25 ([GP22，定理 A]). 设 $f: E\ \to E'$ 是两条椭圆曲线 E 和 E' 之间的一个 F^s-同源，它们的 j 不变量分别为 j 和 j'。那么，

$$h(j') = \frac{\deg_{ins} f}{\deg_{ins} \hat{f}} \cdot h(j),$$

其中$\deg_{ins}$ 表示非可分次数。

函数域上椭圆曲线的同源类情况与前两种情形截然不同。这些同源类包含无穷多个同构类！更多详情请参阅 [GP22] 。考察定理 5.25、定理 5.22 和定理 5.19 后可以看出，数域上的椭圆曲线同源类与秩 2 的 Drinfeld 模同源类更为相似，而不像函数域上的椭圆曲线同源类！

Drinfeld 模 秩 2	**椭圆曲线 在数域上**	**函数域上的椭圆曲线 域**
设$f\colon \phi \to \phi'$ 是一个同源，介于两个 *Drinfeld* 模 ϕ 与 ϕ' 秩为2 的 $A = \mathbb{F}_q[t]$。	设$f\colon E \to E'$ 是一个 K–同源，介于两条椭圆曲线 E 以及 E' 上的数域 K。	设 $f\colon E \to E'$ 是一个 K–同源两条椭圆曲线 E之间的以及 E' 在一个 函数域 K 上的光滑射影且几何不可约曲线亏格为g 的完美域上的曲线。
那么我们可以假设同源f 的次数至多为.....		
$c_0(q)(h(j)[K\colon F])^{10\cdot 3^7}$ [DD99，定理 1.3]	$c_0 \cdot [K\colon \mathbb{Q}] \cdot h(j).$ [GR14]	$49 \cdot$ 最大值$\{1, g\} \cdot \max\left\{\frac{\deg_{ins} j}{\deg_{ins} j'}, \frac{\deg_{ins} j'}{\deg_{ins} j}\right\}$。 [GP22，定理 B]
那么 $\lvert h(j) - h(j')\rvert$ 上界为		
$q + \frac{q^2-1}{2} \log(1 + \frac{1}{q h(j')})$ [BPR21]	$10 + 12\log(\deg f)$ [Paz19，定理 1.1]	$h(j') = \frac{\text{度}_{ins}\, f}{\text{次数}_{ins}\, \hat{f}} \cdot h(j).$ [GP22，定理 A]

图 2：椭圆曲线与秩为 2 的 Drinfeld 模的低次数同源及不变量的高度。

6 Drinfeld 模的一些应用

本节旨在概述 Drinfeld 模的各种应用。我们首先在第 6.1 小节讨论其在多项式因式分解中的应用。在第 6.2 小节，我们介绍一些基于涉及 Drinfeld 模的计算问题的密码系统尝试；人们曾认为这些问题足够困难，能够确保系统安全。这两类应用都利用了 Drinfeld 模与椭圆曲线之间的类比。最后，在第 6.3 小节，我们介绍 Drinfeld 模与编码理论之间的联系。

6.1 Drinfeld 模与计算机代数相遇

椭圆曲线在计算机代数中发挥着关键作用。它们可用于素性测试（由 Goldwasser–Killian 提出、经 Altkin 和 Morain 改进的 椭圆曲线素性证明 方法，参见 [GK86, AM93]）或整数因子分解（由 H. Lenstra 提出的椭圆曲线法， [Len87]）。整数因子分解是一个众所周知的困难问题，目前最佳的算法（如一般数域筛法 [Len87]）只能达到亚指数复杂度。另一方面，在代数 $= \mathbb{F}_q[T]$中对多项式进行因式分解，可以利用概率方法非常高效地完成。其中一些方法依赖于 Drinfeld 模。

在下文的第 6.1.1–6.1.3 小节中，我们介绍 Doliskani、Narayanan 和 Schost 提出的算法 [DNS21]。该算法利用了我们在前几节介绍的许多工具（超奇异性、自同态环的结构），渐近复杂度与目前最优方法相当（截至 2025年）。最后，在第 6.1.4 小节中，我们概述其他因式分解算法，并比较它们的性能。

6.1.1 超奇异约化

回忆一下，K 是 $\mathrm{Frac}(A) = \mathbb{F}_q(T)$，并令 $\gamma : A \to K$ 为典范嵌入。令$\phi : A \to K\{\tau\}$ 为一个秩 2 Drinfeld 模，其定义为

$$\phi_T = T + g\tau + \Delta\tau^2, \quad g \in K, \Delta \in K^\times.$$

由于 ϕ 并非定义在有限域上，因此它没有 Frobenius 自同态，所以它不可能是超奇异的。不过，可以考虑它在素多项式 $f_i \in A$ 处约化后是否会成为超奇异（Drinfeld 模的约化见小节 5.2.1）。在这种情况下，我们称 ϕ 在 f_i 处具有超奇异约化 。根据定理 5.9 和定理 5.10，这很容易检验：只需计算 ϕ 模 f_i 的 Hasse 不变量。为此，我们定义数列 $(r_{\phi,k})_{k\geqslant 0}$，使其满足 $r_{\phi,0} = 1$、$r_{\phi,1} = g$ 以及递推关系

$$r_{\phi,k+2} = g^{q^{k+1}} r_{\phi,k+1} - \left(T^{q^{k+1}} - T\right)\Delta^{q^k} r_{\phi,k}.$$

那么，ϕ 模 f_i 的 Hasse 不变量就是 $r_{\phi,\deg(f_i)}$ 在 A/f_iA 中的像。

SageMath 示例 6.1. 以下函数计算模给定模数的 Hasse 数列 $r_{\phi,k}$，直至 $k = n$（回忆一下，$q = 7$）。

```
sage: def hasse_sequence(g, Δ, n, modulus):
....:     r = [1, g] + (n-1) * [None]
....:     for k in range(n-1):
....:         r[k+2] = (g^(7^(k+1)) * r[k+1]
....:                   - (T^(7^(k+1)) - T) * Δ^(7^k) * r[k]) % modulus
....:     return r
```

我们计算 $\phi_T = r_{\phi,2}$ 模$T^{7^2} - T$ $\phi_T = T + T\tau + (T+1)\tau^2$。

```
sage: r = hasse_sequence(T, T+1, 2, T^49 - T)
sage: h = r[2]
sage: h
6*T^7 + T^2 + T
sage: h.factor()
(6) * T * (T^2 + 2*T + 2) * (T^4 + 5*T^3 + 2*T^2 + 3)
```

h 的二次不可约因子，恰好是使 ϕ 具有超奇异约化的二次不可约多项式。我们分两种情况在下面进行检验。

```
sage: F1.<U1> = F7.extension(T^2 + 2*T + 2) # U1 是T 模T^2 + 2T + 2的像;
sage: φ1 = DrinfeldModule(A, [U1, U1, U1 + 1])sage: φ1.is_supersingular()
Truesage: F2.<U2> = F7.extension(T^2 + 1)       # U2 是T 模T^2 + 1的像。
```

在第二种情况下，我们还验证了h 在F_2 中的像是 ϕ_2的 Hasse 不变量，也就是 τ^2 中 $\phi_2(T^2+1)$的系数。

```
sage: F2(h)
2*U2 + 6
sage: φ2(T^2 + 1)
2*U2*τ^4 + 2*U2*τ^3 + (2*U2 + 6)*τ^2
```

在我们的应用场景中，f_i 将是给定多项式 f 的不可约因子，因此其次数先验 未知，无法计算 Hasse 不变量。然而，利用序列 $(r_{\phi,k})_{k\geqslant 0}$ 满足二阶递推关系这一事实，可以证明以下另一种刻画，它仅涉及 f 的次数。

命题 6.1([DNS21，引理 6])。 对于 $f \in A$，$f \neq 0$，我们定义

$$\overline{h}_{\phi,f} = \gcd\left(r_{\phi,\deg(f)} \bmod f,\, r_{\phi,\deg(f)+1} \bmod f\right).$$

设 f_i 是 f 的一个不可约因子，其中 $\underline{\phi}$ 有良约化。那么，当且仅当 f_i 整除 $h_{\phi,\,f}$ 时，ϕ 在 f_i 处有超奇异约化。

定理 6.1 很容易引出一种因式分解 f 的方法：我们计算 f 与 $h_{\phi,f}$ 的最大公因式，并希望它能给出 f 的一个非平凡除子。只要 f 有两个不可约因子 f_1 和 f_2，使得 ϕ 模 f_1 有普通约化，且模 f_2 有超奇异约化，这种情况就会发生。

6.1.2 具有复乘的 Drinfeld 模

为了确保前述情况以较高概率发生，必须谨慎选择 ϕ。事实上，随机选择并不可行。不过，考虑具有复乘的 Drinfeld 模时，情况就大不相同了，其定义如下。

定义 6.2。 秩为 2 的 Drinfeld 模 ϕ：若其自同态代数 $\mathrm{End}^0_{K^s}(\phi) = \mathrm{End}_{K^s}(\phi) \otimes_A K$（见第 5.1.5 小节）作为一个 A-代数同构于某个虚二次函数域，则称其具有复乘。

具有复乘的 Drinfeld 模比其他 Drinfeld 模（即自同态代数同构于 K 的那些模）更为罕见，但它们在超奇异约化方面具有额外的判据。具体来说，若 f_i 在 $\mathrm{End}^0_{K^s}(\phi)$ 中非分歧，则 ϕ 在 f_i 处有良好的超奇异约化，当且仅当 f_i 在 $\mathrm{End}^0_{K^s}(\phi)$ 中惰性。结合定理 6.1，可得以下结论。

命题 6.3。 假设 ϕ 具有复乘，且 f 的不可约除子在 $\mathrm{End}^0_{K^s}(\phi)$ 中均非分歧。那么最大公因式 $(h_{\phi,f}, f)$ 等于 f 的所有首一素因子 f_i（它们在 $\mathrm{End}^0_{K^s}(\phi)$ 中惰性）的乘积。

我们现在的任务是找出一个具有复乘的显式 Drinfeld 模 $\phi\colon A \to K\{\tau\}$。当 q 为奇数时，我们解释如何做到这一点；当 q 为偶数时，参见[DNS21，备注 7]。取一个元素 $a \in \mathbb{F}_q$，我们考虑域 $K(\omega)$，其中 ω 是 $T-a$ 的平方根，并考虑由下式定义的 Drinfeld 模 $\psi\colon A \to K(\omega)\{\tau\}$

$$\psi_T = (\tau+\omega)^2 + a = T + (\omega+\omega^q)\tau + \tau^2.$$

容易验证，Ore 多项式 $\tau+\omega$ 定义了 ψ 的一个自同态 u，其平方是由 $T-a$ 给出的标量乘法。因此我们得到一个环同态 $K(\omega) \to \mathrm{End}^0(\psi)$，$\omega \mapsto u$，从而证明 ψ 具有复乘。然而，ψ 并非定义在 K 上。我们通过注意到其 j-不变量（见第 4.3 小节）为

$$j = (\omega+\omega^q)^{q+1} = \omega^{q+1}(1+\omega^{q-1})^{q+1} = (T-a)^{\frac{q+1}{2}}\left(1+(T-a)^{\frac{q-1}{2}}\right)^{q+1} \tag{26}$$

因此，由于 q 为奇数，它属于 K。于是我们可以考虑 Drinfeld 模

$$\phi : A \to K\{\tau\}, \quad T \mapsto \phi_T = T + \tau + j^{-1}\tau^2.$$

它同构于 ψ K^s；因此它也具有复乘。

SageMath 示例 6.2。 Doliskani、Narayanan 和 Schost 的算法可以按如下方式轻松实现。

```
sage: def factor_DNS(f, a):....:     n = f.degree()
....:     j = (T-a)^4 * (1 + (T-a)^3)^8   #       = 7
....:     _  Δ  _ = j.xgcd(f)   # Δ =  −1
此处q ,,j模f....:     r = hasse_sequence(1, Δ, n+1, f)
....:     return gcd([f, r[n], r[n+1]])
```

在前文中，我们使用公式（26）定义j，而a是基域中的一个参数 $\mathbb{F}_7$。根据a的取值，该函数可能输出一个非平凡因子，也可能不会。下面我们将看到，当

$$f = (T^2+1)\cdot(T^2+2) = T^4 + 3T^2 + 2$$

当a = 1时，可以找到一个非平凡因子。

```
sage: f = T^4 + 3*T^2 + 2
sage: factor_DNS(f, a=0)
1sage: factor_DNS(f, a=1)
T^2 + 2
sage: factor_DNS(f, a=2)
T^4 + 3*T^2 + 2
```

事实上，当 $a = 1$ 时，我们检查相应的 Drinfeld 模在 f 的第一个因子模下具有普通约化，但在第二个因子模下具有超奇异约化。

```
sage: j = (T-1)^4 * (1 + (T-1)^3)^8
sage: F1.<U1> = F7.extension(T^2 + 1)
sage: ϕ1 = DrinfeldModule(A, [U1, 1, 1/j(U1)])
sage: ϕ1.is_supersingular()
False
sage: F2.<U2> = F7.extension(T^2 + 2)
sage: ϕ2 = DrinfeldModule(A, [U2, 1, 1/j(U2)])
sage: ϕ2.is_supersingular()
True
```

我们再次使用公式（26）定义 j，并使用注记 4.12 中关于 Drinfeld 模的结果。

6.1.3 实现细节和复杂度

将上述策略转化为实际高效的算法还需要一些额外的论证和优化。

首先，需要估计算法成功的概率。根据定理 6.3，可以通过研究 A 中在虚二次函数域 $K(\sqrt{T})$ 中保持惰性的多项式所占的比例来进行估计。反过来，这可以利用函数域算术中的标准结果来完成，例如切博塔廖夫密度定理或黎曼–赫尔维茨亏格公式。总而言之，最终可得算法单轮成功的概率至少为 1 4（参见 [DNS21、引理 8]以及引理 6 之后从 [DNS21]开始的讨论）。 –

另一个重要要素是快速计算$h_{\phi,f}$的方法。事实上，直接采用朴素方法的性能不足以使整体因式分解算法达到最先进水平的复杂度。Doliskani、Narayanan 和 Schost 的一项关键贡献实际上是一种计算$h_{\phi,f}$的新方法。它依赖于模复合，以及对元素属于A/fA的二阶矩阵进行快速乘法。

关于模复合，目前渐近复杂度最佳的算法是 Kedlaya 和 Umans [KU01]提出的算法。这一算法的一项创新是执行位操作，而非仅执行代数运算。不过，目前还没有该算法的高效实现。因此，[DNS21] 的作者选择给出两种复杂度分析：一种只使用代数算法（包括模复合），并以 $\mathbb{F}_q$中的运算次数计量；另一种使用 Kedlaya–Umans 算法，并以位操作次数计量。在第二种情况下，得到的总位复杂度随$n^{\frac{3}{2}+o(1)}$增长（更一般的表述见 [DNS21，定理 2]）。

6.1.4 与其他算法的比较

比较算法时，既要考察渐近复杂度，也要考察实际效率。两者通常存在很大差异。对于在A中分解多项式的问题，渐近上最优（截至2025年）的算法是将 Kaltofen–Schoup 因式分解算法 [KS95] 与用于模复合的 Kedlaya–Umans 算法 [KU01]结合起来。对于A 中次数为n的多项式，该算法的渐近复杂度为$n^{\frac{3}{2}+o(1)}$位操作。正如前文所述，这种算法在实际中很不实用，只有在输入规模非常大时，理论上才可能具有优势。因此，实际实现时通常更倾向于采用 Cantor–Zassenhaus 算法 [CZ81]，它利用了 Berlekamp [Ber67]，提出的思想。该算法分解多项式时的复杂度几乎为二次（以 $\mathbb{F}_q$中的运算次数计），相对于n而言。

我们还要指出，所有多项式时间方法都是概率性的。在有限域上寻找一种用于多项式分解的确定性多项式算法，这一问题仍未解决。

使用 Drinfeld 模的方法。 已知的使用 Drinfeld 模的因式分解方法如下。

- van der Heiden 的方法 [vdH04b, vdH04a]是 Lenstra 椭圆曲线方法用于整数因式分解 [Len87]的一个类似方法。在次数为 n 的多项式上运行该算法，需要在 $\mathbb{F}_q$[中进行 $O(n^2 \log q + dn^3)$ 次算术运算3]vdH04b, 命题 4. [。该方法要求将 f 表示为 k 个互不相同的素多项式的乘积，并且这些多项式具有某个次数 d。通过按照 Berlekamp [Ber67] 和 Cantor–Zassenhaus [CZ81] 算法的前几个步骤计算最大公因式和导数，可以找到 d 并据此进行归一化。van der Heiden 的方法基于以下事实：在给定有限域 K 上，随机 Drinfeld 模的秩为 d 时，端自同态 $x\phi T(x)$ 的特征多项式中可以识别出某些素因子。因而，我们可以利用 Reiner [Rei61] 和 Gerstenhaber [Ger61] 的独立工作，计算一步中找到 f 的一个因子的概率 [vdH04b, 注 4.5]。已知系数属于 $\mathbb{F}_q$ 的 d×d 矩阵中具有不可约特征多项式的矩阵比例的界，van der Heiden 表明，随机选取 ϕ ran- domly $1-$ 时，只要 q 足够大，成功概率约为 $(d-1)k^{+1}$ dk（一般性陈述见 [vdH04b, 命题 4.3] ）。我们还提到 Randrianarisoa 的综述，该综述专门讨论 van der Heiden 的工作[Ran14]。

- 虽然 van der Heiden 提出了第一个已知的、针对基于 Drinfeld 模的因式分解方法的复杂度和成功率分析，但其算法背后的思想可以追溯到 Potemine 和 Panchishkin 的工作 [Pot97, 小节 4.3],[Pan93]。van der Heiden 对此予以承认 [vdH04a]。在 [Pan93], 中，Panchishkin 还提到，可以利用 Drinfeld 模改造经典方法（椭圆曲线素性证明），以便在 A 中进行素性测试。Panchishkin 还讨论了 Schoof 点计数算法的一种可能类似方法 [Sch85]。现在已知其中一种方法在 [MS19, 小节 6]中有所描述（见小节 5.1.2）。

- 在 Doliskani、Narayanan 和 Schost 的工作发表前不久，Narayanan 提出了两种利用 Drinfeld 模进行因式分解的方法 [Nar18]。
  – 第一种方法本身并不是因式分解算法，而是用于计算 f 的最小素因子的次数。得知这一信息后，Kedlaya–Umans 版本的 Kaltofen–Schoup 算法可以显著加速：位复杂度渐近降至 $n^{1+o(1)}(\log q)^{2+o(1)}$。Narayanan 通过随机秩为 2 的 Drinfeld 模在有限域上的“点数”（见定理 5.3）读取这个最小次数。– 第二种方法是 Berlekamp 算法的一个改进版本，其中用 Drinfeld 模的作用取代 Frobenius 自同态的作用。作者未提供复杂度分析。

在这些方法中，只有 Doliskani、Narayanan 和 Schost 的方法 [DNS21] 达到了渐近最先进水平。它也是其中唯一一种不使用一般随机 Drinfeld 模，而使用带复乘的随机 Drinfeld 模的方法。作者使用 NTL C++ 库开发了一个实现 [Sho90], ，该实现采用了更直接的模复合方法。据作者称，由于需要处理二乘二多项式矩阵，其速度比 NTL 的默认函数慢一个常数因子。

6.2 Drinfeld 模与密码学

密码学依赖于计算困难问题，这些问题可用于加密、密钥交换、签名或认证协议。经典的计算困难问题包括整数分解、在有限域上计算离散对数、在有限域上的椭圆曲线上计算离散对数，或计算有限域上椭圆曲线之间的同源。这些问题分别应用于 RSA [RSA78], Diffie-Hellman [DH76], 椭圆曲线 Diffie-Hellman [Kob87, Mil86], 和 SQIsign 密码系统 [DFKL$^+$20]。

为了提高函数域算术的效率，人们曾多次尝试借鉴上述经典构造，引入基于 Drinfeld 模的密码系统。遗憾的是，迄今为止这些尝试都未能成功。

- 在 [Sca01], Scanlon 定义了*Drinfeld* 模块离散对数问题和*Drinfeld* 模块求逆问题，希望据此构造 RSA 和 Diffie-Hellman 密码系统的 Drinfeld 模类比方案。他在同一篇论文中证明了这些问题可以轻易计算。

- 在 [JN19], Joux 和 Narayanan 推导出了 SIDH [JDF11] 和 CSIDH[CLM$^+$18] 密码系统的类似方案，并声称发现了它们的弱点。

- 在 [LS22], Leudière 和 Spaenlehauer 提出了 CRS 密码系统的一种类似方案。Wesolowski 关于计算 Drinfeld 模块的同源的研究

（小节 5.1.3）证明了这一新构造以及 Joux 和 Narayanan 的构造都不能安全使用。

备注 6.4. 我们提到，SIDH 密码系统在 2022年被攻破。此前，Castryck 和 Decru 发起了一系列攻击，随后 Maino 和 Martindale 也加入其中 [CD23], Maino 和 Martindale [MM22],, 最终 Robert 对其进行了无条件密码分析 [Rob23]。截至 2025年，CSIDH 尚未被证明存在安全漏洞。不过，SIDH 和 CSIDH 背后的思想被改编用于构造 SQISign；它是一种签名协议，参与了美国国家标准与技术研究院为后量子密码系统制定标准的竞赛。

设 ϕ 为定义在有限 A-域 (F,γ) 上的 Drinfeld 模。给定 x、y $\in$ F，Drinfeld 模块离散对数问题要求在解存在时，求出一个元素 a $\in$ A，使得 $\phi_a(x) = y$。至于 Drinfeld 模块求逆问题，给定 a $\in$ A，使得 ϕ_a 是 K 上的双射 $\mathbb{F}_q$-线性自同态，要求求出 b $\in$ A，使得 ϕ_b（作为 K 上的 $\mathbb{F}_q$-线性自同态）是 $\iota(\phi_a)$ 的复合逆。Scanlon 指出，这两个问题都可以用线性代数方法解决：映射 a $\mapsto \phi_a(x)$ 和 x $\mapsto \phi_a(x)$ 都是 $\mathbb{F}_q$-线性的。在 [GLPR03], Gillard、Leprévost、Panchishkin 和 Roblot 提出了 Drinfeld 模块求逆问题的一种修正方案。后来 Blackburn、Cid 和 Galbraith 证明该方案并不安全，见 [BCG06]。

就 Joux–Narayanan 和 Leudière–Spaenlehauer 的构造而言，它们都不安全，因为得益于 Wesolowski 的研究（见第 5.1.3 小节），可以高效地计算有限域上 Drinfeld 模之间的同源。

这些攻击的共同点是都涉及 $\mathbb{F}_q$ 上的有限维向量空间。经典情形中不存在这样的对象，因为整数环之下没有域。有关这些尝试的详情，请参阅 [Leu24, Appendix A] 。

注 6.5. Drinfeld 模块求逆问题与 RSA 密码系统之间的关联或许并不显而易见。然而，这两种构造之间存在重要的对称性。两者都涉及一个模（在 $\mathbb{Z}$ 上或在 A 上）。在每种情形下，我们都有一个加密密码系统；现在我们将说明（见表 1），加密函数可以看作该模的挠空间上的一个线性自同态。为简单起见，假设我们处理的是秩为 1 的 Drinfeld 模，并且只考虑 ϕ_a 元素，其中a 不在 A-特征之中。

	经典 RSA	**Drinfeld 模 RSA**
模	$\mathbb{Z}$-模定义为： $\mathbb{Z} \times \mathbb{Q}^* \to \mathbb{Q}^*$ $(n,x) \mapsto n * x = x^n$	由以下方式定义的A-模： $A \times F \to F$ $(a,x) \mapsto a * x = \phi_a(x)$
挠	n-挠（在 $\mathbb{Q}$ 中）：$\mathbb{Z}/n\mathbb{Z}$	a-挠（在 F^s 中）：A/aA
加密函数	线性自同构 $\mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ $x \mapsto e * x$ 其中 e 经过精心选择	线性自同构 $F \to F$ $x \mapsto a * x$ 与精心选择的

表 1：经典 RSA 设置与其 Drinfeld 类比的比较。

人们可能会疑惑，为什么 Drinfeld 模 RSA 加密函数不定义在 A/aA 上。在经典情形中，n-挠与$\mathbb{Z}/n\mathbb{Z}$ 之间的同构是显式的，并由本原n次单位根给出。这使我们能够将其视为

直接定义在 $*$ 上的乘法律 $\mathbb{Z}/n\mathbb{Z}$。在 Drinfeld 模的情形中，其构造并未给出这样的显式同构（见定理 3.13）。话虽如此，鉴于F 是有限的， ${}^{\phi}F$ 中的所有元素都是扭点，即它们全都是$\chi_{\phi}(1)$-挠——其中 χ_{ϕ} 是 Frobenius 自同态的特征多项式——根据定理 5.3， ${}^{\phi}F$ 可以看作挠空间的一个A-子模。

经典 RSA 构造与 Drinfeld 模 RSA 构造之间的这些相似之处，源自分圆数域和函数域的构造。正如我们在第 2.3 小节中看到的，分圆数域是通过向 $\mathbb{Q}$添加单位根得到的，而分圆函数域则是通过向 $\mathbb{F}_q(T)$ 添加定义在C_{∞}上的秩为 1 的 Drinfeld 模的a-挠得到的。

6.3 Drinfeld 模与线性码

纠错码是旨在检测并纠正传输或存储数据中错误的数学工具。数据项在传输或存储之前，通过添加冗余信息进行编码。之后，即使数据在时空传输过程中遭到破坏，也可以通过解码操作恢复原始数据。研究最广泛的纠错码模型是线性码。

本节介绍 Drinfeld 模与编码理论之间的一些已知联系。Drinfeld 模在渐近优良码的构造中发挥了重要作用；从历史上看，这些码使代数几何在编码理论中的地位得以确立。我们将在第 6.3.2 小节简要回顾这段历史。最近，Drinfeld 模再次出现在编码理论中，用于设计秩度量下的局部可恢复码 [BDM24]。我们将在第 6.3.3 小节介绍这一构造；它最初基于 Carlitz 模，并将讨论其向高秩 Drinfeld 模的推广。

6.3.1 汉明度量与秩度量下的线性码

线性码是某个有限维 $\mathbb{F}_q$-线性环境空间中的 $\mathbb{F}_q$-向量子空间。线性码的效率由三个主要参数刻画：其长度，定义为码所在环境空间的维数；其作为向量空间的维数；以及其最小距离，后者取决于环境空间上所定义的度量。值得注意的是，码的维数代表可用其编码的数据量，长度是传输消息的大小，其中包含添加到原始数据中的冗余，而最小距离则与错误检测和纠正能力有关。事实上，众所周知，最小距离为 d 的码最多可以纠正 d 个错误，或 d 个擦除。

—

传统上，线性码定义为赋予汉明距离的 $\mathbb{F}_q$-向量子空间，其中汉明距离用于衡量两个码字作为 $\mathbb{F}_q^n$ 中的向量时，其不同的位置数量。

定义 6.6（**汉明度量中的码**）。汉明距离定义为 x、$y \in \mathbb{F}_q^n$之间的距离

$$d(x,y) = \#\{i \in [n] \ : \ x_i \neq y_i\}.$$

汉明度量中的码 $\mathcal{C}$ 是一个赋予汉明距离的 $\mathbb{F}_q$-线性子空间 $\mathbb{F}_q^n$。其维数 k 为 $\dim_{\mathbb{F}_q}\mathcal{C}$，其最小距离定义为

$$\begin{aligned} d(\mathcal{C}) &:= \min\{d(x,y) \ : \ x,y \in \mathcal{C}, x \neq y\} \\ &= \min\{d(x,0) \ : \ x \in \mathcal{C}, x \neq 0\}. \end{aligned}$$

我们将一个 $\mathcal{C} \subseteq \mathbb{F}_q^n$维数为$k$ 且最小距离为$d(\mathcal{C}) = d$ 的码称为 $[n、k、d]_q$-码。

汉明度量中的一大类码由所谓的求值码组成，顾名思义，这类码通过在一组元素上对函数空间中的函数进行求值得到。这包括*Reed–Solomon* [RS60] 码和*Reed–Muller*码 [Ree54, Mul54],：前者在 $\mathbb{F}_q$ 中选取不同元素对一个变量的多项式进行求值，后者则在 $\mathbb{F}_q^m$ 中选取不同元素对m 个变量的多项式进行求值；还包括代数几何码 [Gop81], ，它通过在一条代数曲线上的点处对有理函数进行求值得到。汉明度量中的一个 $[n、k、d]_q$-码满足所谓的*Singleton*界 $k + d \leqslant n + 1$。达到该界的码称为最大距离可分码（MDS码）。下文将介绍的Reed–Solomon 码就是MDS码的一个例子。

定义 6.7. 设 $k \leqslant n \leqslant q$ 为整数。设 $\mathbf{x} = (x_1, \ldots, x_n)$ 是有限域 $\mathbb{F}_q$ 中两两不同元素组成的元组。支集为 $\mathbf{x}$ 、维数为k 的*Reed–Solomon* 码 定义为

$$\mathsf{RS}_k(\mathbf{x}) = \{(f(x_1), \ldots, f(x_n)) : f \in \mathbb{F}_q[T], \deg f < k\}.$$

它是一个 $[n,k,n-k+1]_q$-码。

近年来，人们还考虑了汉明度量以外的度量，用于更适合解决特定信息论问题的纠错码。其中之一是秩度量 [Del78]。

定义 6.8 （秩度量下的码）。 设 $\mathbb{F}_q^{n\times m}$表示系数属于 $\mathbb{F}_q$ 的$n \times m$ 矩阵空间。M、$N \in \mathbb{F}_q^{n\times m}$之间的秩距离 定义为

$$d_{\mathrm{rk}}(M, N) = \mathrm{rk}(M - N).$$

秩度量码 $\mathcal{C}$ 是一个带有秩距离的 $\mathbb{F}_q$-线性子空间 $\mathbb{F}_q^{n\times m}$。其维数k 为 $\dim_{\mathbb{F}_q} \mathcal{C}$，其最小秩距离定义为

$$\begin{aligned} d_{\mathrm{rk}}(\mathcal{C}) &:= \min\{d_{\mathrm{rk}}(M, N) \ : \ M, N \in \mathcal{C}, M \neq N\} \\ &= \min\{\mathrm{rk}(M) \ : \ M \in \mathcal{C}, M \neq \mathbf{0}\}. \end{aligned}$$

我们将一个维数为k 且最小距离为d 的码$:= d_{\mathrm{rk}}(\mathcal{C})$ 称为一个 $[nm, k, d]_q$秩度量码。

注 6.9。 此处，我们以矩阵形式介绍秩度量码，以便遵循 [BDM24], 一文中的记号；我们将在第 6.3.3 小节介绍该文。不过，秩度量码也可以看作线性态射空间。设V 是一个维数为n的 $\mathbb{F}_q$-子空间。秩距离 可自然定义为f、$g \in \mathrm{Hom}(V, \mathbb{F}_{q^m})$ 之间的$d_{\mathrm{rk}}(f, g) = \mathrm{rk}(f - g)$。于是，秩度量码 $\mathcal{C}$ 是 $\mathrm{Hom}(V, \mathbb{F}_{q^m})$ 的一个 $\mathbb{F}_q$-线性子空间，并配备秩距离。固定V 和 $\mathbb{F}_{q^m}$的 $\mathbb{F}_q$-基，即可恢复矩阵视角。

我们将重点关注秩度量码的一种特殊情形，即所谓的向量秩度量码。选取 $\mathbb{F}_{q^m}$的一个 $\mathbb{F}_q$-基后，可以将任意向量$x \in \mathbb{F}_{q^m}^n$关联到一个矩阵$M_x \in \mathbb{F}_q^{n\times m}$。这样， $\mathbb{F}_{q^m}^n$ 的任意向量子空间都可以赋予秩度量，并视为矩阵码。与矩阵秩度量码相比，这类码自然具有 $\mathbb{F}_{q^m}$-线性这一额外性质。

定义 6.10。 （向量）秩度量码 $\mathcal{C}$ 是一个赋予秩距离的 $\mathbb{F}_{q^m}^n$ 的 $\mathbb{F}_{q^m}$-线性子空间。其维数 k 为 $\dim_{\mathbb{F}_{q^m}} \mathcal{C}$，其最小秩距离定义为

$$d_{\mathrm{rk}}(\mathcal{C}) := \min\{\mathrm{rk}(M_x) \ : \ x \in \mathcal{C}, x \neq \mathbf{0}\}.$$

我们称一个维数为k 且最小距离为$d_{\mathrm{rk}}(\mathcal{C}) = d$ 的 $[n,k,d]_{q^m}$ 秩度量码。

秩度量码在错误可能影响整行或整列而非孤立符号的场景中尤其有效，例如网络编码、空时编码和密码学。有兴趣的读者可参阅 [BHL+22]，了解秩度量码应用的综述。

Ore 多项式理论使得人们能够构造秩度量下的求值码，从而得到上述所有码的对应形式 [Del78, ALR18, ACLN21, BC25, BC24]。特别是，Reed–Solomon码在秩度量领域中的对应形式是 Gabidulin码，由 Delsarte [Del78] 和 Gabidulin[Gab85]提出。

定义 6.11。对于正整数 $\kappa \leqslant m$ 以及 $\mathbb{F}_q$-线性子空间W，其维数为 $\mathbb{F}_{q^m}$，关联的 *Gabidulin* 码 定义为下列映射的像：

$$\begin{array}{rccc} \text{enc}: & \mathbb{F}_{q^m}\{\tau\}_{\leqslant \kappa-1} & \to & \mathrm{Hom}_{\mathbb{F}_q}(W, \mathbb{F}_{q^m}) \simeq \mathbb{F}_q^{n\times m} \\ & f & \mapsto & f|_W \end{array}$$

其中 $\mathbb{F}_{q^m}\{\tau\}_{\leqslant \kappa-1}$ 是次数不超过 $\kappa-1$的 Ore 多项式构成的向量空间；我们回顾第 3.1.1 小节中的内容，稍微滥用一下记号，继续用f 表示在 $\mathbb{F}_{q^m}$上诱导的线性映射。

Gabidulin 码是一个 $[mn,m\kappa、n+1-\kappa]_q$ 秩度量码。也可以将 Gabidulin 码视为 $\mathbb{F}_{q^m}$-线性子空间 $\mathbb{F}_{q^m}^n$，由此得到一个 $[n、\kappa、n+1-\kappa]_{q^m}$（向量）秩度量码。

秩度量码的参数满足秩Singleton界 [Gor21, Theo- rem 3.5]:

$$k \leqslant m(n - d_{\mathrm{rk}}(\mathcal{C}) + 1).$$

参数达到此界的码称为最大秩距离(MRD)码。Gabidulin 码是 MRD 码的实例。

过去四十年来，Ore 多项式已成功应用于编码理论；而直到最近，Drinfeld 模才开始用于这一领域。当时，研究者利用 Carlitz 模构造了具有最优性质、适用于分布式存储的秩度量码 [BDM24]，，从而得到所谓的局部可恢复码。此构造将在第 6.3.3 小节中介绍。在此之前，我们将在下一节简要讨论 Drinfeld 模曲线对于汉明度量中的码的重要性。

6.3.2 汉明度量中渐近优良码的模曲线

给定一列 $(C_s)_{s\in\mathbb{N}}$，其参数为 $[n_s、k_s、d_s]_q$，我们定义其码率 $R := \lim_{s\to\infty} k_s/n_s$，以及相对距离 $\delta := \lim_{s\to\infty} d_s/n_s$。若一列码$(C_s)_{s\in\mathbb{N}}$ 满足渐近优良码的条件，则称其构成一个族，其中$R > 0$ 且 $\delta > 0$。

渐近吉尔伯特–瓦尔沙莫夫界 [Sti09, 命题 8.4.4]指出，长度不断增加的随机码族能够达到 $R > 1 - h_q(\delta) + o(1)$，其中 h_q 是定义如下的 q 元熵函数

$$\forall x \in [0,1], \quad h_q(x) = x\log_q(q-1) - x\log_q(x) - (1-x)\log_q(1-x).$$

长期以来，人们一直认为吉尔伯特–瓦尔沙莫夫界确实是一条界，也就是说，没有任何结构化码族能够在码率和相对距离方面超越随机码，直到 Tsfasman、Vl˘adu,t 和 Zink 构造出代数几何

码，超过了吉尔伯特–瓦尔沙莫夫界 [TVZ82]。由曲线 $\mathcal{X}$ 构造的代数几何码的参数取决于 $\mathcal{X}$的几何性质。例如，长度的上界是 $\mathbb{F}_q$-点数量 $\#\mathcal{X}(\mathbb{F}_q)$ $\mathcal{X}$。Tsfasman、Vl˘adu.t 和 Zink 的构造依赖于一族渐近良好的曲线塔。

一条曲线塔是由曲线和满射组成的无限序列

$$\cdots \twoheadrightarrow \mathcal{X}_3 \twoheadrightarrow \mathcal{X}_2 \twoheadrightarrow \mathcal{X}_1 \twoheadrightarrow \mathcal{X}_0,$$

它们都定义在一个有限域 $\mathbb{F}_q$ 上，且其亏格$g(\mathcal{X}_s)$ 满足

$$\lim_{s\to\infty} g(\mathcal{X}_s) = +\infty. \tag{27}$$

根据哈斯–韦伊定理，每条曲线 $\mathcal{X}_s$ 上的 $\mathbb{F}_q$点数都有上界

$$\#\mathcal{X}_s(\mathbb{F}_q) \leqslant q + 1 + 2\sqrt{q}g(\mathcal{X}_s).$$

如果曲线 $\mathcal{X}_s$上的 $\mathbb{F}_q$点数增长速度显著快于其亏格，则称该曲线塔是渐近良好的，即

$$\limsup_{n\to\infty} \frac{\#\mathcal{X}_n(\mathbb{F}_q)}{g(\mathcal{X}_n)} > 0.$$

根据哈斯–韦伊界，我们知道 $\#\mathcal{X}_n(\mathbb{F}_q)$ $g(\mathcal{X}_n)$ $\leqslant 2\sqrt{q}$。Ihara [Iha81] 注意到，对于大亏格曲线，这个界远未达到，并引入了这个量

$$A(q) = \limsup_{g\to\infty} \frac{\max\{\#\mathcal{X}(\mathbb{F}_q) : \mathcal{X} \text{ curve of genus } g\}}{g},$$

现在称为*Ihara* 常数。他证明了$A(q) \geqslant \sqrt{q} - 1$ 当q 是平方数时成立。后来，Vl˘adu.t 和 Drinfeld 证明了$A(q) \leqslant \sqrt{q} - 1$ [VD83]，这意味着$A(q) = \sqrt{q} - 1$当q 是平方数时成立。¯一条塔$(\mathcal{X}_n)$ 若满足以下条件，则称为最优

$$\limsup_{n\to\infty} \frac{\#\mathcal{X}_n(\mathbb{F}_q)}{g(\mathcal{X}_n)} = \sqrt{q} - 1.$$

模曲线提供了渐近良好的曲线塔，这对于构造具有优异渐近性能的代数几何码至关重要。经典模曲线$X_0(N)$以带有循环N-同源的椭圆曲线为参数，在 $\mathbb{F}_{p^2}$上构成渐近良好的曲线塔，其中p为素数。Tsfasman、Vl˘adu.t 和 Zink 利用这一结果构造了超越吉尔伯特–瓦尔沙莫夫界的代数几何码 [TVZ82]。感兴趣的读者可阅读 [Cou23]，深入了解这一主题。

类似地，Drinfeld 模曲线用于参数化带有层结构的秩 2 Drinfeld 模，也能在任意二次域 $\mathbb{F}_{q^2}$[BBN15]，以及更一般的任意非素域上产生渐近良好的曲线塔。这些曲线在有限域 $\mathbb{F}_q$ 中尤其有用，其中 q 是一个平方数；Garcia 和 Stichtenoth [GS95]构造的最优曲线塔便是例证。Elkies 为此前在编码理论中研究过的某些递归曲线塔（例如 Garcia-Stichtenoth 曲线塔）给出了模解释，从更深层次的结构角度说明了它们为何最优 [Elk01]。更确切地说，他证明了温和情形对应于经典模曲线 [Elk97]，而野情形对应于 Drinfeld 模曲线 [Elk01]。此后，许多已知的显式递归定义曲线塔也获得了模解释。Bassa，

Beelen 和 Nguyen [BBN14, BBN15] 证明，这些（经典或 Drinfeld）模塔的定义方程可以直接从模多项式中读出。因此，模曲线理论被视为一种高效的工具，可用于构造显式定义的曲线族，尤其是优良且最优的曲线塔。更多详情请参阅 Beelen 的综述 [Bee22] 。

6.3.3 秩度量中的局部可恢复码

编码理论的一个主要应用是分布式存储系统中的数据恢复。最初，人们使用数据复制来确保在节点（例如，单台机器）发生故障时的可靠性。过去几十年来，分布式存储系统逐渐转向使用擦除码，因为与之相比，擦除码能够以显著更低的存储成本提供更高的可靠性。很容易验证，一个 $[n、k、d]$ 线性码最多可以恢复$d-1$ 个擦除。例如，2014 年，Facebook 部署了 Hadoop 分布式文件系统（HDFS）的一种版本，该系统依赖于一个 $[14,10,5]$ Reed–Solomon 码，因此最多可以抵抗 4 个节点故障。然而，这需要访问其他 10 个节点并执行高次数多项式插值。

局部可恢复码是一类旨在高效解决这一问题的纠错码，其允许通过仅访问其他符号中的一个很小子集来恢复码字中的每个符号。局部可恢复码最初是在汉明度量中引入的 [GHSY12, PD14]。下面回顾其定义。

定义 6.12。 [BTV17，定义 2] 若码 $\mathcal{C} \subseteq \mathbb{F}_q^n$对每个坐标指标$i \in \{1,\ldots\ldots, n\}$，都存在一个包含$i] \subseteq \{1,\ldots\ldots, n\}$的子集 $\Gamma[$，使得 $|\Gamma(i)| \leqslant t+\delta-1$，并且将码 $\mathcal{C}|_{\Gamma(i)}$ 限制到(i) Γ中的坐标后得到的码 $\mathcal{C}$ 的最小距离为$d(\mathcal{C}|_{\Gamma(i)}) \geqslant \delta$，则称该码具有局部可恢复性，其局部性为$(t,\ \delta)$。

在 [KERDS16] 中，定义以如下方式推广到了秩度量。

定义 6.13。 若秩度量码 $\mathcal{C} \subseteq \mathbb{F}_q^{n\times m}$对每个列索引$i \in \{1,\ldots\ldots, m\}$，都存在一个包含$i] \subseteq \{1,\ldots\ldots, m\}$的列集合 $\Gamma[$，使得 $|\Gamma(i)| \leqslant t+\delta-1$，并且将码 $\mathcal{C}|_{\Gamma(i)}$ 限制到(i) Γ中的坐标后得到的码 $\mathcal{C}$ 的最小秩距离为$d_{\mathrm{rk}}(\mathcal{C}|_{\Gamma(i)}) \geqslant \delta$，则称该码具有局部可恢复性，其秩局部性为$(t,\ \delta)$。

注记 6.14. 上述定义是对最初在汉明度量中引入的定义的一种自然扩展。特别地，当秩度量码 $\mathcal{C}$ 是 $\mathbb{F}_{q^m}$-线性的时，它与汉明度量情形下局部可恢复码的经典定义完全一致。局部性的概念与码 puncturing 有关。秩度量矩阵码的 puncturing 是到坐标子空间上的投影；与汉明度量情形不同的是，该投影可以预先复合一个保秩同构 $A \in GL_n(\mathbb{F}_q)$[Ner19，定义 2.15]。定理 6.13 只涉及同构为平凡同构 $A = I_n$的 puncturing。因此，当前秩度量中的局部性概念并未充分利用秩度量的丰富结构，可能会被认为不尽如人意。不过，由于 [BDM24], 采用了这一称法，我们也将沿用。

维数为$m \cdot k$ 且秩局部性为(t,δ) 的局部可恢复秩度量码 $\mathcal{C} \subseteq \mathbb{F}_q^{n\times m}$满足以下 Singleton 型界 [KERDS19，定理 1]

$$d_{\mathrm{rk}}(\mathcal{C}) \leqslant n-k+1-\left(\left\lceil \frac{k}{t} \right\rceil -1\right)(\delta-1). \tag{28}$$

接下来，我们将介绍如何按照 [BDM24], 中所述，从 Carlitz 模构造秩度量下的局部可恢复码，并将其推广到任意秩的 Drinfeld 模。

设 $\phi\colon\ \mathbb{F}_q[T]\to\mathbb{F}_{q^m}\{\tau\}$ 是一个秩为 r 的 Drinfeld 模，其中 $\phi_T:=z+g_1\tau+\cdots+g_r\tau^r$。我们将消息空间视为

$$\mathcal{M}:=\left\{\sum_{k=0}^{s} f_k(\tau)\phi_T^k\ :\ f_k\in\mathbb{F}_{q^m}\{\tau\}_{\leqslant t-1}\right\}.$$

对于某个正整数 ℓ，使得 $\ell\geqslant s+1$，我们选取 $a_1,\ldots,a_\ell\in\mathbb{F}_q^*$，并构造多项式 $h=\prod_{i=1}^{\ell}(T-a_i)$。考虑第 3.4.1 节中定义的 h-挠 $\phi[h]$，我们有 $\phi[h]\simeq\oplus_{i=1}^{\ell}\phi[T-a_i]$。我们提出以下假设：

$$\forall i\in\{1,\ldots,\ell\},\quad \phi[T-a_i]\subseteq\mathbb{F}_{q^m}. \tag{H}$$

由定理 3.13 可知，$\dim_{\mathbb{F}_q}\phi[T-a_i]=r$。

定义 6.15. 考虑编码映射

$$\begin{aligned}\mathrm{enc}:\quad \mathcal{M} &\to \mathrm{Hom}_{\mathbb{F}_q}\left(\phi[h],\mathbb{F}_{q^m}\right)=\bigoplus_{i=1}^{\ell}\mathrm{Hom}_{\mathbb{F}_q}\left(\phi[T-a_i],\mathbb{F}_{q^m}\right)\simeq\mathbb{F}_{q^m}^{\ell r}\\ f &\mapsto f|_{\phi[h]}\end{aligned}$$

其中，最后一个同构是在选取 $\phi[T-a_i]$ 的基之后得到的，对所有的 $i\in\{1,\ldots,\ell\}$ 均成立。我们将码 $\mathcal{C}(\phi,h)$ 定义为 $\mathrm{enc}(\mathcal{M})$ 的像。

使用秩 1 的 Drinfeld 模得到的秩度量下局部可恢复码的参数见 [BDM24，定理 3.4]。这里，我们基本沿用其证明，在下面的定理中说明，我们将 Drinfeld 模推广到更高秩后得到的构造具有相同的参数。

定理 6.16。 设 s，ℓ 为两个满足 $s+1\leqslant\ell$ 的整数。对于 t，δ 设两个满足 $t\geqslant 1$ 和 $\delta\geqslant 2$ 的整数，考虑一个秩为 $r=t+\delta-1>0$ 的 *Drinfeld* 模 ϕ。那么 $\mathcal{C}(\phi,h)$ 是一个 $[m\ell r,\ m(s+1)t,\ \ell r-rs-t+1]$ 码，其秩局部性为 $(t,\ \delta)$。此外，该码是最优的，也就是说，它达到了 *Singleton* 型界。

证明。根据构造，$\mathbb{F}_{q^m}^{\ell r}$ 中的元素是大小为 $\mathrm{m}\cdot\ell\mathrm{r}$ 的矩阵。至于维数，注意到次数为 $\mathrm{sr}+\mathrm{t}-1<(\mathrm{s}+1)\mathrm{r}$ 的 Ore 多项式不可能在 $\mathbb{F}_{q^m}^{\ell r}$ 这个 $\mathbb{F}_{q^m}$-维数为 $\ell\mathrm{r}\geqslant(\mathrm{s}+1)\mathrm{r}$ 的空间上对应零映射，因此编码映射是单射的。由于 $\mathcal{M}$ 的 $\mathbb{F}_{q^m}$-维数为 $(\mathrm{s}+1)\cdot\mathrm{t}$，该码的维数为 $\mathrm{m}\cdot(\mathrm{s}+1)\cdot\mathrm{t}$。现在注意到，$\mathcal{M}$ 包含于次数至多为 $\mathrm{sr}+\mathrm{t}-1$ 的 Ore 多项式环中。因此，$\mathcal{C}(\phi,\mathrm{h})$ 是参数为 $(\ell\mathrm{r},\mathrm{sr}+\mathrm{t})$ 的 Gabidulin 码的子码。由于 Gabidulin 码是最大秩距离码，我们得到

$$d_{\mathrm{rk}}(\mathcal{C}(\phi,h))\geqslant\ell r-sr-t-1. \tag{29}$$

现在，我们要根据定理 6.13 确立秩局部性。对于每个 $i\in\{1,\ldots,r\}$，令 $\Lambda(i)$ 为与直和项 $\mathrm{Hom}_{\mathbb{F}_q}\left(\phi[T-a_i],\mathbb{F}_{q^m}\right)\simeq\mathbb{F}_{q^m}^{r}$ 相对应的列指标集合。我们有 $|\Lambda(i)|=\dim\phi[T-a_i]=r=t+\delta-1$。此外，对于任意 $f\in\mathcal{M}$ 和任意 $x\in\phi[T-a_i]$，我们有

$$f|_{\phi[T-a_i]}(x)=\sum_{k=0}^{s}f_k(a_i^k x)=\sum_{k=0}^{s}a_i^k f_k(x),$$

其中 $f_k(x)\in\mathbb{F}_{q^m}\{\tau\}_{\leqslant t-1}$。由此可得，$\mathcal{C}(\phi,h)|_{\Lambda(i)}$ 包含在一个 $[r,t]_{q^m}$Gabidulin 码中，因此其最小距离至少为 $r+1-t=\delta$。现在，若

$\gamma \in \{1,\ldots,\ell r\}$ 是一个列索引，我们将 $\Gamma(\gamma) := \Lambda(i)$ 设为满足$\gamma \in \Lambda(i)$的唯一指标 i。根据前文， $\mathcal{C}(\phi,h)|_{\Gamma(\gamma)}$ 的最小距离至少为 δ，这证明$\mathcal{C}(\phi,h)$ 具有(t,δ) 秩局部性。由公式（28）的 Singleton 型界可知

$$d_{\mathrm{rk}}(\mathcal{C}(\phi,h)) \leqslant \ell r - rs - t + 1,$$

结合方程 (29)，最终得到 $d_{\mathrm{rk}}(\mathcal{C}(\phi,h)) = \ell r - rs - t + 1$。 □

在任意度量下构造局部可恢复码的一个关键要素，是选择一个良好的多项式，使其满足某些条件，从而能够恢复丢失的数据片段（例如，参见 [TB14，第 A] 节）。本文在秩度量下构造 LR 码也不例外。定理 6.15 中的评价点是通过精心选择多项式$h \in \mathbb{F}_q[T]$ 来确定的，使得h-挠定义在 $\mathbb{F}_{q^m}$ 上，从而满足 **(H)**。对于秩 1 Drinfeld 模，利用狄利克雷定理的有效版本 [BDM24, § 5]，可以保证存在这样的多项式h 。将这一构造推广到任意秩的 Drinfeld 模时，在什么条件下存在这样的多项式h ，值得进一步研究。可以利用小节 5.2.1 中介绍的L级数理论作为主要工具，通过发展 Drinfeld 模的显式切博塔廖夫密度定理来探讨这一问题。

致谢

本报告的灵感源自第二届编码理论、密码学、算术几何与计算机代数巡回研讨会的演讲[3]。作者谨向本届活动的资助方——马赛数学研究所（I2M – UMR7373）和FRUMAM研究联盟（FR 2291 - 法国国家科学研究中心）——表示诚挚谢意。CA获得了ANR*J*不变量（ANR-20-CE40-0003）和ANR*PadLEfAn*（ANR- 22-CE40-0013）的资助。EB获得了ANR-22-CPJ2-0047-01项目的资助。XC和AL感谢ANR*PadLEfAn* （ANR-22-CE40-0013）资助了多次专注于码开发的“结对研究”活动。AL谨此致谢，本研究部分获得了太平洋数学科学研究所的资助。JN获得法国政府未来投资计划ANR-11-LABX-0020-01的资助。FP获得了ANR*J*不变量（ANR-20-CE40-0003）的资助，并感谢波尔多大学的热情接待。本研究部分由ANR-21- CE39-0009-BARRACUDA项目资助。

参考文献

[ACLM23] David Ayotte、Xavier Caruso、Antoine Leudière 和 Joseph Musleh。SageMath 中的 Drinfeld 模。*ACM* 计算机代数通讯，57(2):65–71，2023年。[ACLN 21] Daniel Augot、Alain Couvreur、Julien Lavauzelle 和 Alessandro Neri。任意伽罗瓦扩张上的秩度量码及 Reed–Muller 码的秩类比。*SIAM* 应用代数与几何期刊，5(2):165–199，2021年。

[3]CAIPI: https://caipi_symposium.pages.math.cnrs.fr/page-web/index-en.html

[ALR18] Daniel Augot、Pierre Loidreau 和 Gwezheneg Robert。任意特征的域上的广义Gabidulin码。《设计、码与密码学》，86:1807–1848，2018年。[AM93] Arthur Oliver Lonsdale Atkin 和 François Morain。椭圆曲线与素性证明。《计算数学》，61(203):29–68，1993年。[And00] Greg Anderson。关于模 p 的 L 函数的初等方法。《数论杂志》，80(2):291–303，2000年。[Ang97] Bruno Anglès。关于与有限 Drinfeld 模相关的一些特征多项式。《数学手稿》，93(1):369–379，1997年。[Ayo23] David Ayotte。整体域上模形式的算术与计算方面。博士论文，康考迪亚大学，2023年。[BBN14] Alp Bassa、Peter Beelen 和 Nhut Nguyen。优良函数域塔。《代数曲线与有限域》，《计算与应用数学 Radon 系列》，第23–40页，2014。[BBN15] Alp Bassa、Peter Beelen 和 Nhut Nguyen。Drinfeld 模曲线的优良族。《LMS 计算数学杂志》，18(1):699–712，2015年。[BC24] Elena Berardini 和 Xavier Caruso。和秩度量下的代数几何码。IEEE 信息论汇刊，70(5):3345–3356，2024年。[BC25] Elena Berardini 和 Xavier Caruso。和秩度量下的 Reed–Muller 码。《代数及其应用杂志》，第2541019页，2025年。[BCG06] Simon Blackburn、Carlos Cid 和 Steven Galbraith。基于 Drinfeld 模的密码系统的密码分析。《信息安全》，《电气工程师学会会刊》，153:12–14，2006年。[BDM24] Luca Bastioni、Mohamed O Darwish 和 Giacomo Micheli。利用 Drinfeld 模构造具有秩局部性的最优秩度量码。预印本 arXiv:2407.06081，2024年。[Bee22] Peter Beelen。递归塔与 Ihara 常数综述。预印本 arXiv:2203.03310，2022年。[Ber67] Elwyn Berlekamp。有限域上的多项式因式分解。《贝尔系统技术杂志》，46(8):1853–1859，1967年。[BGP25] Liam Baker、Richard Griffon 和 Fabien Pazuki。Drinfeld 模的平行四边形高度不等式。预印本 arXiv:2512.09526，2025年。[BHL+22] Hannes Bartz、Lukas Holzbaur、Hedongliang Liu、Sven Puchinger、Julian Renner 和 Antonia Wachter-Zeh。秩度量码及其应用。《通信与信息论基础与趋势》，19(3):390–546，2022年。[BP20] W. Dale Brownawell 和 Matthew A. Papanikolas。Drinfeld 模、t模和 t-动机快速导论。载于《t-动机：霍奇结构、超越性及其他动机方面》，第3–30页。欧洲数学会出版有限公司，2020年。ISSN: 2523-515X，2523-5168。

[BPR21] Florian Breuer、Fabien Pazuki 和 Mahefason Heriniaina Razafinjatovo。《Drinfeld 模的高度与同源》。Acta Arithmetica，197:111–128，2021年。[BTV17] Alexander Barg、Itzhak Tamo 和 Serge Vl˘adu ̧t。《代数曲线上的局部可恢复码》。IEEE 信息论汇刊，63(8):4928–4939，2017年。[Car35] Leonard Carlitz。《关于伽罗瓦域中与多项式相关的某些函数》。Duke 数学杂志，1(2):137–168，1935年。[Car18] Perlas Caranay。《秩二 Drinfeld 模的同源火山计算》。博士论文，卡尔加里大学，2018年。[CD23] Wouter Castryck 和 Thomas Decru。《针对 SIDH 的高效密钥恢复攻击》。载于 Carmit Hazay 和 Martijn Stam 编，《密码学进展——EUROCRYPT 2023》，第423–447页。Springer Nature Switzerland，2023年。[CFA+12] Henri Cohen、Gerhard Frey、Roberto Avanzi、Christophe Doche、Tanja Lange、Ki m Nguyen 和 Frederik Vercauteren。《椭圆曲线与双曲曲线密码学手册》。Chapman & Hall/CRC，第2版，2012。[CG24] Xavier Caruso 和 Quentin Gazda。《t-动机的经典与 v-adic L-级数计算》。预印本，arXiv:2401.12618，2024年。[CG25] Xavier Caruso 和 Quentin Gazda。《t-动机的经典与 v-adic L-级数计算》。数论研究，11(1):35，2025年。[CGS20] Perlas Caranay、Matthew Greenberg 和 Renate Scheidler。《有限域上秩二 Drinfeld 模的模多项式与同源计算》。载于《计算数学 75 周年：计算数学 75 周年庆祝研讨会，2018年11月1日至3日，数学计算与实验研究所（ICERM）》，第754卷，第283页。美国数学会，2020年。[CL26] Xavier Caruso 和 Antoine Leudière。《一般 Drinfeld 模上范数与特征多项式的计算算法》。《计算数学》，95(357)，2026年。[CLB17a] Xavier Caruso 和 Jérémy Le Borgne。《斜多项式的快速乘法》。载于《2017年 ACM 国际符号与代数计算研讨会论文集》（ISSAC ’17），第77–84页。计算机协会，2017年。[CLB17b] Xavier Caruso 和 Jérémy Le Borgne。《一种更快的有限域上斜多项式因式分解新算法》。符号计算杂志，79:411–443，2017年。[CLM+18] Wouter Castryck、Tanja Lange、Chloe Martindale、Lorenz Panny 和 Joost Renes。《CSIDH：一种高效的后量子交换群作用》。载于 Thomas Peyrin 和 Steven Galbraith 编，《密码学进展——ASIACRYPT 2018》，第395–427页。Springer International Publishing，2018年。[Cou23] Alain Couvreur。《码与模曲线》。预印本，arXiv:2301.03569，2023年。

[CZ81] David Cantor 和 Hans Zassenhaus。《一种新的有限域上多项式因式分解算法》。《计算数学》，36(154):587–592，1981年。出版方：美国数学会。[DD99] Sinnou David 和 Laurent Denis。《Drinfeld 模之间的最小同源》。《数学年刊》，315:97–140，1999年。[Del78] Philippe Delsarte。《有限域上的双线性型及其在编码理论中的应用》。组合理论杂志，A辑，25(3):226–241，1978年。[DFKL+20] Luca De Feo、David Kohel、Antonin Leroux、Christophe Petit 和 Benjamin Wesolowski。《SQISign：基于四元数与同源的紧凑型后量子签名》。载于 Shiho Moriai 和 Huaxiong Wang 编，《密码学进展——ASIACRYPT 2020》，第64–93页。Springer International Publishing，2020年。[DFKS18] Luca De Feo、Jean Kieffer 和 Benjamin Smith。《迈向基于普通同源图的实用密钥交换》。载于 Thomas Peyrin 和 Steven Galbraith 编，《密码学进展——ASIACRYPT 2018》，《计算机科学讲义》，第365–394页。Springer International Publishing，2018年。[DH76] Whitfield Diffie 和 Martin Hellman。《密码学的新方向》。IEEE 信息论汇刊，22(6):644–654，1976年。[DNS21] Javad Doliskani、Anand Kumar Narayanan 和 Éric Schost。《具有复乘的 Drinfeld 模、Hasse 不变量及有限域上的多项式因式分解》。符号计算杂志，105:199–213，2021年。[Dri74] Vladimir Drinfeld。《椭圆模》。《苏联数学汇刊》，23(4):561，1974年。[Dri77] Vladimir Drinfeld。《某些非交换环的交换子环》。《泛函分析及其应用》，11(1):9–12，1977年。[Dri80] Vladimir Drinfeld。《函数域上 GL(2) 的 Langlands 猜想》。载于《国际数学家大会论文集》（赫尔辛基，1978年），第2卷，第565–574页，1980年。[Elk97] Noam Elkies。《显式模塔》。载于第三十五届 Allerton 通信、控制与计算会议论文集，1997年。[Elk99] Noam Elkies。《线性化代数与李型有限群。一、线性群与辛群》。载于《有限域上的曲线应用》，《当代数学》245卷，第77–107页，1999年。[Elk01] Noam Elkies。《显式 Drinfeld 模曲线塔》。载于 Carles Casacuberta、Rosa Maria Miró-Roig、Joan Verdera 和 Sebastià Xambó-Descamps 编，《欧洲数学大会》，第189–198页，巴塞尔，2001年。Birkhäuser Basel。[Gab85] Ernest Mukhamedovich Gabidulin。《最大秩距离码理论》。《信息传输问题》，21(1):3–16，1985年。[Gek91] Ernst-Ulrich Gekeler。《有限 Drinfeld 模》。代数杂志，141(1):187–203，1991年。

[Gek08] Ernst-Ulrich Gekeler. 有限域上 Drinfeld 模的 Frobenius 分布。美国数学会会刊，360(4):1695–1721，2008。出版者：美国数学会。[Ger61] Murray Gerstenhaber. 有限域上系数为元素的幂零矩阵数量。《伊利诺伊数学杂志》，5(2):330–333，1961。出版者：杜克大学出版社。[GHSY12] Parikshit Gopalan、Cheng Huang、Huseyin Simitci 和 Sergey Yekhanin。论码字符号的局部性。《IEEE 信息论汇刊》，58(11):6925–6934，2012。[GK86] Shafi Goldwasser 和 Joe Kilian。几乎所有素数都可以快速验证。在第十八届 ACM 计算理论研讨会论文集，STOC '86，第 316–329 页。计算机协会，1986年。[GKK25] Filip Głoch、Dawid E. Ke˛dzierski 和 Piotr Kraso´n。确定某些扩张群上的 t-模结构的算法。《国际数论杂志》，21(8):1889–1922，2025年。[GLPR03] Rolland Gillard、Franck Leprévost、Alexei Panchishkin 和 Xavier-François Roblot。Drinfeld 模在密码学中的应用。《数学研究报告》，336(11):879–882，2003。[Gop81] Valerii Denisovich Goppa。代数曲线上的码。载于《苏联数学文摘》，第 24 卷，第 170–172 页，1981。[Gor21] Elisa Gorla。秩度量码。载于《编码理论简明百科全书》，第 227–250 页。Chapman and Hall/CRC，2021年。[Gos96] David Goss。函数域算术的基本结构，《数学及其边界领域成果》第 35 卷（第 3 辑） *[数学及其相关领域成果（第 3 辑）]*。施普林格出版社，柏林，1996年。[GP22] Richard Griffon 和 Fabien Pazuki。函数域上的椭圆曲线同源。《国际数学研究通知》，2022(19):14697–14740，2022年。[GR96] Ernst-Ulrich Gekeler 和 Marc Reversat。Drinfeld 模曲线的雅可比簇。《纯粹与应用数学杂志》，476:27–93，1996年。[GR14] Éric Gaudron 和 Gaël Rémond。周期定理与同源的最小次数。《瑞士数学评论》，89(2):343–403，2014。[GS95] Arnaldo Garcia 和 Henning Stichtenoth。一个达到 Drinfeld-Vladut 界的函数域 Artin-Schreier 扩张塔。《数学新进展》，121(1):211–222，1995年。[Hay74] David Hayes。有理函数域的显式类域论。美国数学会会刊，189(0):77–91，1974年。[Hay11] David Hayes。Drinfeld 模简明导论。载于《Drinfeld 模简明导论》，第 1–32 页。De Gruyter，2011年。[Iha81] Yasutaka Ihara。关于有限域上代数曲线有理点数量的一些评论。《东京大学理学部学报》，28(3):721–724，1981年。

[JDF11] David Jao 和 Luca De Feo。基于超奇异椭圆曲线同源构建抗量子密码系统。在 Bo-Yin Yang（编），《后量子密码学》，第 19–34 页。施普林格，2011年。[JN19] Antoine Joux 和 Anand Kumar Narayanan。Drinfeld 模或许不适用于基于同源的密码学，2019年。[Kat73] Nicholas Katz。模方案与模形式的 p 进性质，《数学讲义》第 350 卷。施普林格，柏林—纽约，1973年。[Ked01] Kiran Kedlaya。正特征下幂级数域的代数闭包。《美国数学会会刊》，129(12):3461–3470，2001年。[KERDS16] Swanand Kadhe、Salim El Rouayheb、Iwan Duursma 和 Alex Sprintson。具有局部可恢复性的秩度量码。载于《2016年第54届 Allerton 通信、控制与计算年会（Allerton）》，第 1033–1040 页。电气电子工程师学会，2016年。[KERDS19] Swanand Kadhe、Salim El Rouayheb、Iwan Duursma 和 Alex Sprintson。秩度量与子空间度量下的局部性码。《IEEE 信息论汇刊》，65(9):5454–5468，2019年。[Kob87] Neal Koblitz。椭圆曲线密码系统。《计算数学》，48(177):203–209，1987年。[KS95] Erich Kaltofen 和 Victor Shoup。有限域上多项式的亚二次时间因式分解。载于第二十七届 ACM 计算理论研讨会论文集，STOC ’95，第 398–406 页。计算机协会，1995年。[KU01] Kiran Kedlaya 和 Christopher Umans。快速多项式因式分解与模复合。《SIAM 计算杂志》，40(6):1767–1802，2011-01。出版者：工业与应用数学学会。[Laf02] Laurent Lafforgue。Drinfeld 束与 Langlands 对应。《数学新进展》，147:1–241，2002年。[Lan02] Serge Lang。《代数》，《数学研究生教材》第 211 卷。施普林格，2002年。[Len87] Henrik Lenstra。利用椭圆曲线分解整数。《数学年刊》，126(3):649，1987年。[Leu24] Antoine Leudière。Drinfeld 模态射及其算法。博士论文，洛林大学，2024年。[LS22] Antoine Leudière 和 Pierre-Jean Spaenlehauer。来自虚双曲函数域类域论的困难齐性空间。《密码学 ePrint 档案》，2022年。[LS24] Antoine Leudière 和 Pierre-Jean Spaenlehauer。根据虚双曲函数域的类域论计算群作用。《符号计算杂志》，125:102311，2024年。

[Mil86] Victor Miller. 密码学中椭圆曲线的应用。载于 Hugh C. Williams 编，《密码学进展——CRYPTO ’85 会议论文集》，第 417–426 页。施普林格，1986年。[MM22] Luciano Maino 和 Chloe Martindale. 使用任意起始曲线对 SIDH 发起攻击。密码学电子印本档案，2022年。[Moo96] Eliakim Hastings Moore. 费马定理的二重推广。《美国数学会通报》，2(7):189–199，1896年。[MS19] Yossef Musleh 和 Éric Schost. 计算有限秩二 Drinfeld 模的特征多项式。2019年国际符号与代数计算研讨会论文集，第 307–314 页，2019年。[MS23] Yossef Musleh 和 Éric Schost. 利用晶体上同调计算有限 Drinfeld 模自同态的特征多项式。载于《 2023 年国际符号与代数计算研讨会论文集》，ISSAC ’23，第 461–469 页。计算机协会，2023年。[Mul54] David Muller. 布尔代数在开关电路设计和错误检测中的应用。《IRE电子计算机专业组汇刊》，EC-3(3):6–12，1954年。[Mus18] Yossef Musleh. 求秩为 2 的 Drinfeld 模特征多项式的快速算法，2018年。硕士论文。[Mus23] Yossef Musleh. Drinfeld 模算法。博士论文，滑铁卢大学，2023年。[Nar18] Anand Kumar Narayanan. 通过计算 Drinfeld 模的欧拉–庞加莱特征对有限域上的多项式进行因式分解。《有限域及其应用》，54:335–365，2018年。[Ner19] Alessandro Neri. 秩度量码的代数理论：表示、不变量与稠密性结果。博士论文，苏黎世大学（瑞士），2019年。[Neu99] Jürgen Neukirch. 代数数论。Norbert Schappacher 从德文翻译，第 322 卷，《数学科学基础丛书》。柏林：施普林格，1999年。[Ore33a] Øystein Ore. 关于一类特殊多项式。《美国数学会会刊》，35(3):559–584，1933年。[Ore33b] Øystein Ore. 非交换多项式理论。《数学年刊》第二辑，34:480–508，1933年。[Pan93] Alexei Panchishkin. 数与多项式因式分解、素性测试、椭圆曲线和 Drinfeld 模的快速算法。卡昂大学数论研讨会，1992–1993 年卷：1–7，1993年。[Pap23] Mihran Papikian. Drinfeld 模，《数学研究生教材》第 296 卷。尚佩恩：施普林格，2023年。

[Paz19] Fabien Pazuki. 模不变量与同源。《国际数论杂志》，15(03):569–584，2019年。[PD14] Dimitris Papailiopoulos 和 Alexandros Dimakis. 局部可修复码。《IEEE信息论汇刊》，60(10):5843–5855，2014年。[Poo95] Bjorn Poonen. Drinfeld 模的局部高度函数与 Mordell–Weil 定理。《数学汇刊》，97(3):349–368，1995年。[Poo22] Bjorn Poonen. Drinfeld 模导论。《算术、几何、密码学与编码理论》，779，2022年。[Pot97] Igor Potemine. 函数全局域的算术与 Drinfeld 模空间概形的几何。博士论文，约瑟夫·傅立叶大学，1997年。[Pot98] Igor Potemine. Drinfeld 粗模空间概形的极小终端 Q-因子化模型。《数学物理、分析与几何：专注于分析与几何在物理学中的理论及应用的国际期刊》，1(2):171–191，1998年。[Ran14] Tovohery Hajatiana Randrianarisoa. 具有不可约特征多项式的矩阵数目。预印本 arXiv:1402.2794，2014年。$\mathbb{F}_q$ Ree[Irving Reed. 一类多重纠错码及其译码方案。《IRE 信息论专业组汇刊》，4(4):38–49，1954年。54] Rei[Irving Reiner. 关于具有给定特征多项式的矩阵数目。《伊利诺伊数学杂志》，5(2):324–329，1961年。出版商：杜克大学出版社。61] Rob[Damien Robert. 在多项式时间内攻破 SIDH。载于 Carmit Hazay 和 Martijn Stam 编，《密码学进展——EUROCRYPT 2023》，第 472–503 页。Springer Nature Switzerland，2023年。23] Ros[Michael Rosen. 函数域数论，第 210 卷。施普林格科学与商业媒体，2002年。02] RS[Irving Reed 和 Gustave Solomon. 某些有限域上的多项式码。《工业与应用数学学会杂志》，8(2):300–304，1960年。60] RSA[Ronald Rivest、Adi Shamir 和 Leonard Adleman. 一种实现数字签名和公钥密码系统的方法。《美国计算机协会通讯》，21(2):120–126，1978年。78] Sca[Thomas Scanlon. 基于 Drinfeld 模的公钥密码系统并不安全。《密码学杂志》，14(4):225–230，2001年。01] Sch[René Schoof. 有限域上的椭圆曲线与模 p 平方根的计算。《计算数学》，44(170):483–494，1985年。85] Sho[Victor Shoup. NTL：用于数论计算的库，1990年。90] Sil[Joseph Silverman. 《椭圆曲线算术》，《数学研究生教材》第 106 卷。施普林格，2009年。

[Sti09] Henning Stichtenoth。《代数函数域与码》。施普林格，2009年。[Tae12] Lenny Taelman。Drinfeld 模的特殊 L 值。《数学年刊》第二辑，175(1):369–391，2012年。[TB14] Itzhak Tamo 和 Alexander Barg。一族最优局部可恢复码。《IEEE 信息论汇刊》，60(8):4661–4676，2014年。[Tha04] Dinesh Thakur。《函数域算术》。新泽西州河边镇：世界科学出版社，2004年。[TVZ82] Michael Tsfasman、Sergey Vl˘adutx 和 Thomas 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年。[VD83] Sergei Georgievich Vl˘adu‚t 和 Vladimir Gershonovich Drinfeld。代数曲线的点数。《泛函分析及其应用》，17(1):68– 69，1983年。[vdH04a] Gert-Jan van der Heiden。《“用 Drinfeld 模分解有限域上的多项式”的补遗》。《计算数学》，73(248):2109– 2109，2004年。[vdH04b] Gert-Jan van der Heiden。用 Drinfeld 模分解有限域上的多项式。《计算数学》，73(245):317–322，2004年。[Wad41] Luther Irwin Wade。某些超越于 GF(p^n, x)之上的量。《Duke 数学杂志》，8:701–720，1941年。[Wes24] Benjamin Wesolowski。计算有限 Drinfeld 模之间的同源。《IACR 密码学通讯》，1(1)，2024年。