A computational approach to Drinfeld modules

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

[1]Univ. Lille, CNRS, UMR 8524 - Laboratoire Paul Painlevé, F-59000 Lille, France
[2]CNRS; IMB, Université de Bordeaux, France
[3]University of Calgary, Canada
[4]CNRS; Univ Rennes, IRMAR - UMR 6625, F-35000 Rennes, France
[5]Department of Mathematical Sciences, University of Copenhagen,
Universitetsparken 5, 2100 Copenhagen, Denmark

Abstract

This survey provides a practical and algorithmic perspective on Drinfeld modules over $\mathbb{F}_q[T]$. Starting with the construction of the Carlitz module, we present Drinfeld modules in any rank and some of their arithmetic properties. We emphasise the analogies with elliptic curves, and in the meantime, we also highlight key differences such as their rank structure and their associated Anderson motives.

This document is designed for researchers in number theory, arithmetic geometry, algorithmic number theory, cryptography, or computer algebra, offering tools and insights to navigate the computational aspects of Drinfeld modules effectively. We include detailed SageMath implementations to illustrate explicit computations and facilitate experimentation. Applications to polynomial factorisation, isogeny computations, cryptographic constructions, and coding theory are also presented.

Contents

2020 Mathematics Subject Classification. Primary 11G09, Secondary 11R58, 11-04.

Keywords: Drinfeld modules, Carlitz module, Ore polynomials, Anderson motives, computer algebra, cryptography, coding theory.

1 Introduction

Number theory is sometimes depicted as the study of *number fields*, which are finite extensions of $\mathbb{Q}$, together with their Galois properties. The simplest class of number fields are the so-called *cyclotomic fields* obtained from $\mathbb{Q}$ by adjoining roots of unity. Although quite elementary in appearance, they revealed a remarkable structure and numerous applications, including Kummer's proof of many cases of Fermat's Last Theorem. Ultimately, their investigation leads to class field theory. Beyond cyclotomic extensions, one finds nonabelian extensions of $\mathbb{Q}$. Here, the situation is far less understood; nevertheless, algebraic geometry provides powerful tools for building such extensions. As a basic example, the field generated by the coordinates of the n-torsion points of an elliptic curve defined over $\mathbb{Q}$ is a number field whose Galois group naturally sits in $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$. Studying these extensions proved to be fascinating and again led to outstanding applications, including the complete proof of Fermat's Last Theorem due to Wiles and Taylor–Wiles. Nowadays, these developments are encompassed in the far-reaching Langlands programme, which, roughly speaking, aims at understanding all number fields by group-theoretical means.

In parallel with number fields, one often considers function fields, which are finite extensions of $\mathbb{F}_q(T)$ where $\mathbb{F}_q$ is a finite field. However, extending the definitions of cyclotomic fields and elliptic curves to function fields in a straightforward way does not lead to notions exhibiting sufficiently rich arithmetic content. Regarding cyclotomy, for example, we note that the extensions of $\mathbb{F}_q(T)$ generated by roots of unity are simply the fields $\mathbb{F}_{q^m}(T)$—which leaves out many interesting abelian function fields.

In the 1930s, Carlitz [Car35] introduced an analogue of the exponential function in the framework of function fields, resulting in the construction of a new large family of cyclotomic extensions. Roughly speaking, these extensions are defined by adjoining "$f(T)$-th roots of unity" for any *polynomial* $f(T) \in \mathbb{F}_q[T]$. About forty years later, Drinfeld went further and proposed new objects, first called *elliptic modules*, as a meaningful arithmetic replacement of elliptic curves over function fields. Elliptic modules, which are nowadays called *Drinfeld modules*, allow for building extensions with Galois groups sitting in $\mathrm{GL}_r(\mathbb{F}_q[T]/f(T)\mathbb{F}_q[T])$ for any rank r and any polynomial $f(T) \in \mathbb{F}_q[T]$. In rank 1, Drinfeld's theory meets Carlitz's constructions, while in rank 2, it mimics the classical theory of elliptic curves. However, Drinfeld's framework allows one to explore higher ranks similarly—this feature turned out to be of remarkable importance towards the Langlands program for function fields [Dri80], as it allowed Lafforgue [Laf02] to completely establish it in the case of GL_r in 2002.

We also rapidly mention that, the same way that elliptic curves are related to modular forms, Drinfeld modules are also related to the so-called Drinfeld modular forms *via* modularity theorems [Dri74, GR96]. They are also the source of a rich theory of transcendence over function fields, including algebraic independence [Tha04, Chapter 10].

Algorithms for elliptic curves have been studied for a long time. On the contrary, despite the remarkable impacts of Drinfeld modules, their algorithmic aspects are less known and only a subject of very recent developments [Car18, CGS20, Wes24, Ayo23, CL26, Leu24, CG25, GKK25]. This research was initially driven by the profusion of shared properties with elliptic curves, and more generally, abelian varieties, over number fields, but it has now started to gain its independence and even to go further in certain directions. As a striking example, the problems of computing isogenies or L-functions are basically solved for Drinfeld modules, whereas they are still challenging questions over number fields. Moreover, algorithms for Drinfeld modules also start to find applications in connected domains, including computer algebra [DNS21], cryptography [Sca01, JN19, LS22] and coding theory [BBN15, BDM24].

1.1 Purpose and organisation of the survey

This document is designed as a general introduction to the theory of Drinfeld modules, with a particular look towards computational aspects and applications. Our presentation will be illustrated by many examples handled with the help of the software SageMath, which includes an implementation of Drinfeld modules: the first features were integrated in SageMath 10.0 [ACLM23, Leu24], while the more recent ones were added at the same time as writing the present article.

In practice, our text will be interspersed with SageMath snippets as follows.

SageMath example 1.1.

```
sage: # This is a comment in the SageMath interpretor
sage: # The following is a command and its output
sage: 57.is_prime()
False
sage: # Perfection.
```

We start in Section 2 with Carlitz's *analytic construction* of the so-called *Carlitz module*, and present its applications to cyclotomy. In Section 3, we climb the ladder of ranks and define general Drinfeld modules, moving moreover from an analytic treatment to an algebraic one. There, we also introduce classical algebraic invariants attached to Drinfeld modules, namely their *Tate modules* and their "motives", called *Anderson motives*, the latter being important algorithmic assets.

Section 4 is dedicated to morphisms between Drinfeld modules, a central topic of the theory; we will particularly study the action they induce at the level of Anderson motives and, building on this, will associate meaningful invariants to them. Our goal is to equip the reader with the necessary tools and insights to navigate these structures. In Section 5, we continue drawing parallels between Drinfeld modules and elliptic curves, regarding their arithmetic aspects. We draw in particular a picture of Drinfeld modules over finite fields, underlying the importance of the Frobenius isomorphism, and over function fields, giving an overview of the theory of L-series. We also explore some recent developments related to height theory for Drinfeld modules, a topic which is somewhat less treated in standard references. Finally, Section 6 gives an overview of the applications of Drinfeld modules to polynomial factorisation, cryptography and coding theory.

Although the material presented in the survey is somewhat standard, our presentation deviates from the classical ones by being clearly algorithm-oriented. In particular, we give a prominent role to Anderson motives, as they provide a concrete incarnation of Drinfeld modules with which it is easier to handle computations. Indeed, unlike Drinfeld modules, Anderson motives are actually modules in the classical sense, allowing explicit calculations *via* standard linear algebra methods and polynomial arithmetic. While emphasising similarities between Drinfeld modules and elliptic curves, this point of view also allows one to touch upon some of their key differences: Anderson motives embody Grothendieck motives, but unlike them, can be described using only elementary algebraic definitions. They thus played a key role in recent algorithmic developments, allowing for solving computational problems in greater generality (higher rank, notably), and being used in new coding theory constructions.

For a more comprehensive treatment of Drinfeld modules and their generalisations (Anderson motives, abelian modules, shtukas), with complementary perspectives, we refer the reader to [Gos96, Ros02, Tha04, BP20, Poo22, Pap23] (in chronological order, this list not being exhaustive).

1.2 Setting and notation

Let p be a prime number and q be a power of p. Let $\mathbb{F}_q$ be a finite field with q elements. We denote by $A := \mathbb{F}_q[T]$ the ring of univariate polynomials with coefficients in $\mathbb{F}_q$ and $K = \mathbb{F}_q(T)$ its field of fractions. The field K is a global function field over $\mathbb{F}_q$.

Remark 1.1. In full generality, Drinfeld modules are defined for K being the field of rational functions over a smooth curve defined over a finite field. Nonetheless, throughout this text, we will restrict ourselves to the case where $A = \mathbb{F}_q[T]$ (corresponding to the curve $\mathbb{P}^1$), considering that the theory is already rich enough for our exposition. In order to facilitate the study of Drinfeld modules over general rings, we point out parts where the assumption $A = \mathbb{F}_q[T]$ is crucial.

The place of K corresponding to $\frac{1}{T}$ is denoted by ∞. We set $K_\infty := \mathbb{F}_q((\frac{1}{T}))$, which is a field isomorphic to the completion of K at ∞. We equip K_∞ with the absolute value $q^{\deg(\cdot)}$. The completion of a fixed algebraic closure of K_∞ is denoted by C_∞, and the absolute value uniquely extends to C_∞. Both fields K_∞ and C_∞ are non-archimedean. The field C_∞ is complete and algebraically closed.

A set of classical analogies between the function field and the number field settings, in which $\mathbb{Z}$ and A play the same role, is given in Figure 1. However, contrary to $\mathbb{C}/\mathbb{R}$, the extension C_∞/K_∞ has infinite degree. The elements of C_∞ may be difficult to apprehend, especially for computational applications. Note that for a field K of characteristic 0, the algebraic closure of $K((t))$ is isomorphic to the Newton–Puiseux field $\bigcup_{i=1}^{\infty} K((t^{1/i}))$. In our case, as K_∞ has positive characteristic, its algebraic closure contains more than Newton–Puiseux series—we refer to [Ked01] for more details.

SageMath example 1.2. Throughout this article, we shall use the base ring $A = \mathbb{F}_7[T]$ for all our examples in SageMath. The code below creates A and its completion at infinity K_∞.

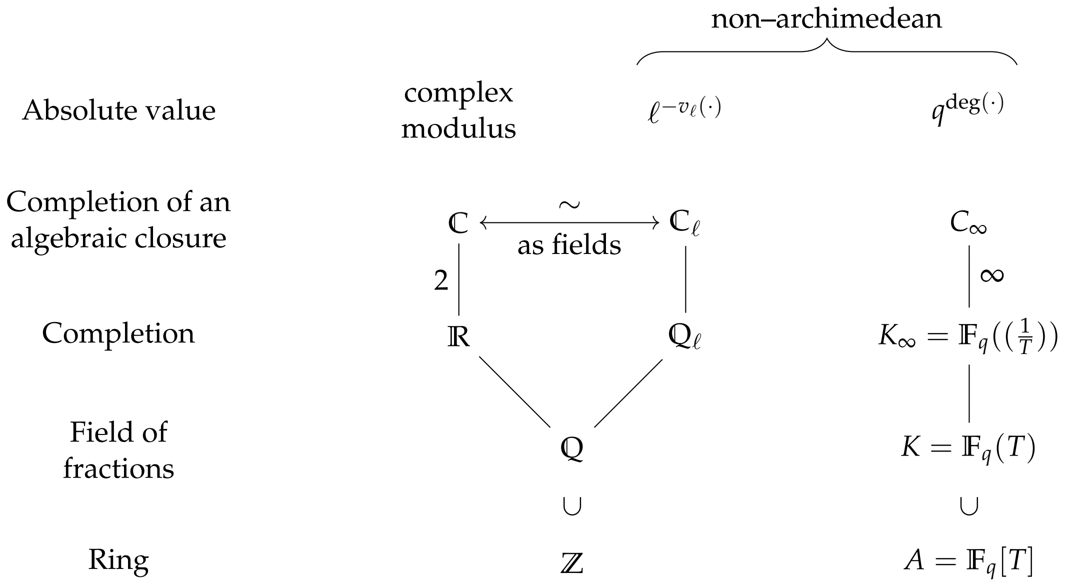

Figure 1: An analogy to keep in mind when starting to work with Drinfeld modules.

```
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
```

Euler-Poincaré characteristic. We also recall the following classification result over the principal ideal domain A: any finitely generated A-module M is isomorphic to a direct sum of the form

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

where n is a nonnegative integer, often referred to as the *rank* of M, and the a_i lie in A. Besides, n is uniquely determined, and the a_i are too, if we impose the condition that they are monic and that a_i divides a_{i+1} for all i.

In particular, if M is finite then n is necessarily zero and M becomes isomorphic to $A/a_1A \oplus \cdots \oplus A/a_mA$. The ideal generated by the product $a_1 \cdots a_m$ does not depend on this presentation: it is the so-called *Euler–Poincaré characteristic* or the *Fitting ideal* of M [Lan02, Chapter 3, § 8]. We will denote it by $|M|$ throughout this article and use it to measure the size of M. In analogy with the number field setting, it simply corresponds to the cardinality.

2 Discovering the Carlitz module

The first instance of a Drinfeld module was introduced by Leonard Carlitz in 1935 [Car35]. At the time, his work received little attention and was mostly forgotten until it was rediscovered in the 1970s, following the work of Drinfeld [Dri77]. Carlitz's construction is now called the *Carlitz module*. We motivate its introduction with the *Carlitz exponential* in characteristic p, by building on analogies and differences with classical exponential functions in characteristic 0. The following presentation is largely inspired by [Tha04, § 2.1], with additional details.

2.1 Looking for an exponential function

The starting point of the theory for the Carlitz module is the desire to find an analogue of the cyclotomic theory in function fields. Recall that, in classical number theory, the cyclotomic extensions of $\mathbb{Q}$ are the extensions of the form $\mathbb{Q}(\zeta_n)$ where ζ_n is a primitive n-th root of unity, with $n \geqslant 2$ an integer. There are several ways to think of ζ_n. One of them is of an analytic nature, through the classical exponential function $\exp : \mathbb{C} \to \mathbb{C}$:

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

An approach to construct relevant cyclotomic extensions of $K = \mathbb{F}_q(T)$ is to generalise the above construction. We are then looking for a function $e : C_\infty \to C_\infty$ which would play the role of an exponential function in our setting. This will also lead us to define an analogue of π.

A first way to define the classical exponential function exp is through its differential equation $\exp' = \exp$. Power series solutions to this equation would necessarily be of the form $c \sum_{n\geqslant 0} \frac{x^n}{n!}$ for some constant c. However, this does not make sense in C_∞ since $n! = 0$ when $n \geqslant p$. A second way to look at the exponential is *via* its functional equation

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

Unfortunately, this fails again. Indeed, any function e defined over C_∞ satisfying the above functional equation would also satisfy $e(0) = e(0)^2$, and therefore $e(0) \in \{0,1\}$. Since $e(0) = e(px) = e(x)^p$ because C_∞ has characteristic p, we would finally derive that e is identically zero or identically one.

The idea, which turns out to work, originally developed by Carlitz, is to take advantage of the existence of additive functions in characteristic p and to modify the functional equation by replacing the product on the right-hand side by a sum: we are now looking for functions $e : C_\infty \to C_\infty$ satisfying

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

i.e., simply additive functions. Since our setting is by nature not only additive but $\mathbb{F}_q$-linear (everything is defined over $\mathbb{F}_q$), we will focus more specifically on $\mathbb{F}_q$-*linear* functions e.

As in the case of the classical exponential function, one expects the function e to be *entire*, that is, given by a power series which converges everywhere on C_∞. A standard result of ultrametric analysis, recalled in [Pap23, Proposition 2.7.12], states that any entire and non-constant function $f : C_\infty \to C_\infty$ is surjective. Thus, our exponential function e would also be surjective. Let Λ be the set of its zeros. It is a discrete $\mathbb{F}_q$-linear subspace of C_∞, meaning that the intersection of Λ with any closed ball of positive radius in C_∞ is finite. If such a function e existed, we would get an exact sequence of $\mathbb{F}_q$-vector spaces of the form

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

which is to be compared to the exact sequence of $\mathbb{Z}$-modules for the classical exponential function

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

Comparing those two exact sequences provides additional hints of what Λ should be. Indeed, recall that the analogue of $\mathbb{Z}$ in our setting is the ring $A = \mathbb{F}_q[T]$. We thus aim at expressing Λ as a rank-1 A-lattice $\Lambda = \widetilde{\pi} A$ generated by some constant $\widetilde{\pi}$, that we still need to determine. Furthermore, by analogy, we would like (1) to be an exact sequence of *A-modules*, for some A-module structures to be defined on Λ and on both copies of C_∞. First, we need to interpret $e : C_\infty \to C_\infty$ as a homomorphism of A-modules. We already know that $e(x+y) = e(x) + e(y)$ for any x and y in C_∞. However, we cannot have $e(az) = ae(z)$ for $a \in A$, as the functions $z \mapsto e(az)$ and $z \mapsto ae(z)$ do not have the same set of zeros. The idea of Carlitz, which is central to the theory of Drinfeld modules, is to equip the copy of C_∞ in the codomain with a new structure of A-module compatible with e.

Remark 2.1. Before proceeding, we underline the similarity with the classical exponential function, see Equation (2): the codomain of the latter is not $\mathbb{C}$, but $\mathbb{C}^\times$ equipped with its multiplicative structure. In the function field setting, changing the structure on the codomain is also required, but the modification is of a different nature: we keep the additive structure but modify the action of A.

Concretely, for any polynomial $a \in A$, we look for a functional equation of the form

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

where $\phi_a : C_\infty \to C_\infty$ is a function (dependent on a) to determine, which will define a new structure of A-module on C_∞, denoted by ${}^\phi C_\infty$, through the rule

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

We will thus get a family of commutative diagrams of A-modules:

$$\begin{tikzcd}
0 \arrow[r] & \Lambda \arrow[r] \arrow[d, "\mathrm{mult}_a"] & C_\infty \arrow[r, "e"] \arrow[d, "\mathrm{mult}_a"] & {}^\phi C_\infty \arrow[r] \arrow[d, "\phi_a"] & 0 \\
0 \arrow[r] & \Lambda \arrow[r] & C_\infty \arrow[r, "e"] & {}^\phi C_\infty \arrow[r] & 0
\end{tikzcd}$$

where mult_a denotes the usual multiplication by $a \in A$.

2.2 Analytic construction of the Carlitz module

2.2.1 Finding a formula for the function e

We now aim at constructing the function e with the properties highlighted in Subsection 2.1. Namely, we fix a rank-1 A-lattice of the form $\Lambda = cA$, with $c \in C_\infty^\times$, and we are looking for an $\mathbb{F}_q$-linear entire function $e_\Lambda : C_\infty \to C_\infty$ whose kernel is the lattice Λ.

To build e_Λ, we recall another standard result of ultrametric analysis: any entire function $f : C_\infty \to C_\infty$ is determined, up to multiplication by a nonzero constant, by its set of zeros counted with multiplicity; this is a consequence of an ultrametric version of the Weierstraß "preparation theorem" (see [Pap23, § 2.7.2] for more details).

In our case, we end up with the expression

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

The fact that the above product indeed converges to an $\mathbb{F}_q$-linear entire function e_Λ is a consequence of the discreteness of Λ in C_∞ [Pap23, Proposition 5.1.3].

2.2.2 Setting a new structure of A-module on C_∞

We now explain the construction of the morphisms ϕ_a in the functional Equation (3). First of all, we observe that since $A = \mathbb{F}_q[T]$ is generated by T over $\mathbb{F}_q$, knowing ϕ_T for the indeterminate T is enough to recover all the functions ϕ_a. Indeed, we have, for instance,

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

which would give $\phi_{T^2} = \phi_T \circ \phi_T$ by identification. More generally, for any integer $m \geqslant 1$, we get

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

Using the $\mathbb{F}_q$-linearity of e_Λ, the function ϕ_a is obtained by taking the suitable $\mathbb{F}_q$-linear combinations of the ϕ_{T^m}.

We now focus on the construction of ϕ_T. We know that the map $z \mapsto e_\Lambda(Tz)$ defines an entire function whose set of zeros is $\frac{1}{T}\Lambda$, and that all zeros are simple. Let us look at the map

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

Recall that e_Λ has Λ for kernel so $e_\Lambda(\lambda)$ is well defined for $\lambda \in \frac{1}{T}\Lambda/\Lambda$. Observing that $\mathrm{Card}\big(\frac{1}{T}\Lambda/\Lambda\big) = q$, we see that the above product is finite and defines a polynomial in $e_\Lambda(z)$ of degree q. As e_Λ is entire, it also defines an entire function. Moreover, its set of zeros is $\frac{1}{T}\Lambda$ and all its zeros are simple. Therefore, there exists $k \in C_\infty^\times$ such that

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

Given that we aim at obtaining $\phi_T(e_\Lambda(z)) = e_\Lambda(Tz)$, we then define

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

The A-module structure on C_∞ defined by the rule

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

will be denoted by ${}^\phi C_\infty$, as announced previously.

Since the set of zeros $\frac{1}{T}\Lambda/\Lambda$ is a one-dimensional $\mathbb{F}_q$-linear subspace of C_∞, we deduce that $\phi_T(x)$ is an $\mathbb{F}_q$*-linear* polynomial of degree q, *i.e.*, it has the form $\phi_T(x) = k_1 x + k_2 x^q$ for some $k_1, k_2 \in C_\infty$ with $k_2 \neq 0$. From Equation (4), we derive the estimation $e(z) = z + O(z^2)$. By identifying the coefficients in z in the functional equation $e_\Lambda(Tz) = \phi_T(e_\Lambda(z))$, we then get $k_1 = T$. Similarly, by identifying the coefficients in x^q in Equation (6), we find $k_2 = k$. Therefore, we end up with the simple formula

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

2.2.3 Normalising the lattice Λ

We still do not know what the constant k is, but it turns out that we can freely choose its value by rescaling the lattice Λ. Indeed, if instead of starting with Λ, we start with $u\Lambda$

for $u \in C_\infty^\times$, we get the exponential function $e_{u\Lambda}$, which is connected to the original one e_Λ by the relation

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

Indeed, on both sides, the functions have the same set of zeros with multiplicities and the same first term z in their expansion. The final formula we get for the polynomial $\phi_T^{u\Lambda}$ attached to the lattice $u\Lambda$ reads

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

The standard choice is to normalise our exponential map, to finally obtain the normalised form $\phi_T(x) = Tx + x^q$.

The corresponding lattice is usually denoted by $\tilde{\pi}A$; the constant $\tilde{\pi}$ is then understood as the function field analogue of $2i\pi$ (see [Pap23, p. 317] for instance). With this normalization, we get the *Carlitz exponential* map, denoted by e_C, whose kernel is $\tilde{\pi}A$ and with functional equation

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

Another advantage of this choice is that the coefficients of e are all rational functions, *i.e.*, elements of K. They can be computed iteratively by using the functional equation (8) (see Subsection 3.3 for more details).

SageMath example 2.1. SageMath provides direct functionalities for computing the Carlitz exponential.

```
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)
```

We can now check the functional equation:

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

The datum of the degree-q polynomial $\phi_T(x) = Tx + x^q$ and all the subsequent functions ϕ_a forms the so-called *Carlitz module*.

SageMath example 2.2. We instantiate the Carlitz module over $\mathbb{F}_7$ and compute ϕ_a for $a = T^2 + T + 1$.

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

In the output above, τ represents the Frobenius map $x \mapsto x^q$. This notation is of primary importance in the theory of Drinfeld modules and will be explained in more detail in Subsection 3.1.

From a work of Carlitz [Car35], one can derive the following

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

Although we will not need it, we also mention that Wade [Wad41] showed that $\tilde{\pi}$ is transcendental over K.

2.3 Application to the cyclotomic theory

One motivation for building the Carlitz exponential was to find an analogue of the cyclotomic theory in the framework of function fields. Classically, the cyclotomic fields are those obtained by adding the n-th roots of unity (for an integer $n \geqslant 2$), *i.e.*, the kernel of the group morphism $\mathbb{C}^\times \to \mathbb{C}^\times, x \mapsto x^n$. In the function field setting, the analogues of these morphisms are the maps ϕ_a defining the Carlitz module. We are then naturally lead to consider the extension $K(\phi[a])/K$ where, by definition,

$$\phi[a] = \{ z \in {}^{\phi}\mathbb{C}_\infty \, , \, a \star z = \phi_a(z) = 0 \}.$$

It is the so-called *a-torsion* of the Carlitz module, which is the a-torsion submodule of ${}^{\phi}\mathbb{C}_\infty$, therefore an A-submodule of ${}^{\phi}\mathbb{C}_\infty$.

Theorem 2.2 (Carlitz, see [Ros02, Proposition 12.5]). *For all $a \in A$, the extension $K(\phi[a])/K$ is Galois and its Galois group is canonically isomorphic to $(A/aA)^\times$.*

Sketch of the proof. The construction of the map $\alpha : \mathrm{Gal}(K(\phi[a])/K) \to (A/aA)^\times$ is similar to the classical case. Let σ be an automorphism to $K(\phi[a])$ preserving K. Then σ acts on $\phi[a]$, as the latter is the set of roots of the polynomial ϕ_a. We then notice that $\phi[a]$ is a free module of rank 1 over A/aA and that σ acts linearly. Therefore σ must act by multiplication by an element of A/aA, which needs to be invertible given that σ is an isomorphism. We thus get a uniquely defined scalar in $(A/aA)^\times$, which is by definition $\alpha(\sigma)$.

Proving the injectivity of α is routine: given that $K(\phi[a])$ is by definition generated over K by the elements of $\phi[a]$, a K-automorphism of $K(\phi[a])$ is uniquely determined by its action on $\phi[a]$. On the contrary, the surjectivity of α is more difficult and showing it amounts more or less to studying the factorisation properties of ϕ_a. We refer to [Ros02, Theorem 12.8] for a complete proof of this statement. □

In the case of number fields, a striking result about cyclotomic extensions is that they exhaust all abelian extensions of $\mathbb{Q}$: it is the famous Kronecker–Weber's theorem. Hayes [Hay74] proved an analogue of this statement in the context of function fields. However, this case is a bit more subtle, due to the two following facts, both related to ramification. First of all, contrary to $\mathbb{Q}$, the base field $K = \mathbb{F}_q(T)$ certainly admits everywhere unramified extensions: these are the extensions of the form $F(T)$ where F is a finite extension of $\mathbb{F}_q$. Those extensions are abelian, and they are not of the form $K(\phi[a])$. The second source of difficulties is that Carlitz's construction $K(\phi[a])$ only produces extensions that are tamely ramified at ∞ [Hay74, Theorem 3.1]. In some sense, this is due to our choice of the integral ring $\mathbb{F}_q[T]$ inside $\mathbb{F}_q(T)$. For instance, had we initially chosen $\mathbb{F}_q[\frac{1}{T}]$ instead of $\mathbb{F}_q[T]$, we would have ended up with a different family of cyclotomic extensions, tamely ramified at 0. In [Hay74], Hayes proves that combining these two families, as well as the previously-discussed everywhere unramified extensions, then an analogue of the Kronecker–Weber's theorem does hold.

Hayes' theorem is an outstanding outcome, which definitely demonstrates the pivotal role of the Carlitz module and of the subsequent Carlitz cyclotomic extensions in the arithmetic theory of function fields. Beyond that, Hayes' theorem is often considered the seed of an explicit version of the class group theory in the context of function fields.

2.4 The Carlitz zeta function

We have seen previously that the classical exponential function has an interesting and relevant function field analogue. It turns out that this is not an isolated example: actually, several arithmetic functions of interest also have a twin in the world of function fields (see *e.g.*, [Pap23, § 5.4]).

As an example, we present here the function field analogue of the Riemann zeta function, the so-called *Carlitz zeta function*. It is defined by

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

where A_+ denotes the subset of $A = \mathbb{F}_q[T]$ consisting of monic polynomials.

Similarly to the case of number fields, the Carlitz zeta function can be expressed as an Euler product

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

where the product runs over all irreducible monic polynomials $\mathfrak{p}$ of A. As in the classical case, navigating between the expressions (10) and (11) boils down to writing down the decomposition of each $\mathfrak{a} \in A_+$ as the product of irreducible factors, and factorising the resulting formula.

SageMath example 2.3. The following code directly computes the value of the Carlitz zeta function.

```
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 proved in [Car35] that, whenever s is a multiple of $q-1$, one has

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

which appears to be an analogue of the Euler formula expressing the values of the Riemann zeta function at positive even numbers. In Equation (12), the constant $\tilde{\pi}$ is the Carlitz period we already encountered at the end of Subsection 2.2. The notation BC_s refers to the Bernoulli–Carlitz numbers, while $\Pi(s)$ is the Carlitz factorial [Gos96, Chapter 9].

SageMath example 2.4. We check Formula (12) for $s = q-1$, using the following explicit congruence for $\tilde{\pi}^{q-1}$ derived from Equation (9):

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

```
sage: # here q = 7
sage: 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 * π6
1 + T^-42 + 6*T^-48 + T^-84 + 6*T^-90 + O(T^-100)
```

3 Drinfeld modules and their Anderson motives

In Section 2, we have extended the construction of the exponential function in the function field setting by building explicitly an isomorphism $C_\infty/\widetilde{\pi}A \to {}^{\phi}C_\infty$, mimicking the standard bijection $\mathbb{C}/2i\pi\mathbb{Z} \xrightarrow{\exp} \mathbb{C}^\times$. In the classical setting, quotienting out $\mathbb{C}$ by lattices of rank 2 is also very fruitful as it leads to the theory of elliptic curves. The exponential function is then replaced by the Weierstraß $\wp$ function, inducing the map

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

which identifies $\mathbb{C}/\Lambda$ with the complex points of an elliptic curve. In the world of function fields, a similar construction occurs: one can consider a general lattice $\Lambda \subset C_\infty$, and the quotient C_∞/Λ with its natural structure of A-module. Here, we require Λ to be discrete, in order to get a suitable topology on the quotient, even though it can be of arbitrary rank, given that, contrary to the classical case, the extension C_∞/K is infinite. Nonetheless, all the constructions we carried out in Subsection 2.2 extend *verbatim*: to each such lattice Λ (of any rank), one can associate an exponential map e_Λ defined by

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

which sits in the exact sequence

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

Moreover, for each $a \in A$, the function e_Λ satisfies the functional equation

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

where ϕ_a is a polynomial of the form $\phi_a(x) = ax + c_1x^q + \cdots + c_rx^{q^r}$ (with $c_i \in C_\infty$ and $c_r \neq 0$) explicitly defined by

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

The family $(\phi_a)_{a\in A}$ endows C_∞ with a structure of A-module denoted by ${}^{\phi}C_\infty$ and given, for any $a \in A$ and $z \in {}^{\phi}C_\infty$, by $a \star z = \phi_a(z)$, as in Equation (7). It is what we call a *Drinfeld module* of rank r over C_∞. Via the exponential map e_Λ, we get an isomorphism of A-modules $C_\infty/\Lambda \simeq {}^{\phi}C_\infty$.

Similarly to the case of elliptic curves, a decisive advantage of the description coming from the ϕ_a is its algebraicity: the ϕ_a are not general analytic functions, but polynomials. Consequently, they make sense over a general base and working over C_∞ is no longer required. The general definition of Drinfeld modules follows from this basic observation. We will write it down precisely in Subsection 3.2, after some introduction to Ore polynomials carried out in Subsection 3.1. We then continue in Subsection 3.3 by comparing the algebraic definition with the analytic one. Finally, in Subsection 3.4, we explain how to associate an Anderson module to a Drinfeld module: this will allow us to use characteristic polynomials and reduction theorems at a later stage.

3.1 Ore polynomials

As mentioned above, the algebraic definition of Drinfeld modules will be captured by the data set of polynomials $\{\phi_a\}_{a\in A}$. In this preliminary subsection, we introduce the ring formed by those polynomials and collect their basic properties.

Clearly, the functions ϕ_a as defined in Equation (13) have a distinctive form: they define $\mathbb{F}_q$-linear functions, which amounts to saying that they only involve terms of the form $c_i x^{q^i}$ with $i \in \mathbb{N}$. In some sense, the ϕ_a are polynomials in the q-Frobenius endomorphism $x \mapsto x^q$. This property is captured by the notion of Ore polynomials, defined below.

Definition 3.1 (Ore polynomials)**.** Let F be an $\mathbb{F}_q$-algebra. We denote by $F\{\tau\}$ the noncommutative ring of *Ore polynomials* (also known as *skew polynomials*, or *twisted polynomials*)

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

with the classical additive law, and the multiplication defined by $\tau c = c^q \tau$ for every $c \in F$.

Writing $f = \sum_i c_i \tau^i$, we define the *τ-degree* (resp. *τ-valuation*) of f as the largest (resp. smallest) integer i such that $c_i \neq 0$.

In Definition 3.1, the letter τ is just a formal variable, without further signification. However, it should of course be understood as the Frobenius endomorphism: Ore polynomials then correspond to polynomials in the q-Frobenius as claimed previously. The noncommutative multiplication law is also reminiscent of this interpretation; indeed, applying the multiplication by a scalar c and then the q-Frobenius amounts to applying first the q-Frobenius and then the multiplication by c^q.

SageMath example 3.1. In SageMath, the ring of Ore polynomials can be constructed as follows.

```
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
```

We showcase the noncommutativity of $F\{\tau\}$:

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

A nice feature of Ore polynomials is that their ring, despite being noncommutative, is left-Euclidean with respect to the *τ-degree* [Ore33b]. This means that right-Euclidean division can be performed, and that left-ideals all have a unique monic generator. For a nonempty family S of Ore polynomials, one can compute their *right-greatest common divisor* (or *right-gcd*, for short) $\mathrm{rgcd}(S)$ and their *left-least common multiple* (or *left-lcm*, for short) $\mathrm{llcm}(S)$. In practice, variants of the long division and Euclidean algorithms can be used; complexity statements can be found in [LS24, § 3.1]. More advanced primitives have been described in [CLB17b, CLB17a]: they are based on faster algorithms for the multiplication of two Ore polynomials with coefficients in a finite field.

SageMath example 3.2. Right-gcds can be easily computed as follows:

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

We underline that having a common factor on the left does not imply the nontriviality of the right-gcd:

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

3.1.1 Kernels of Ore polynomials

To carry on the identification of τ to the q-Frobenius, we interpret the Ore polynomials in $F\{\tau\}$ as actual endomorphisms, namely on a separable closure F^{s} of F: to an element $f = \sum_{i=0}^{n} c_i \tau^i \in F\{\tau\}$, we associate the transformation

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

that, in a slight abuse of notation, we continue to denote by f. This transformation is $\mathbb{F}_q$-linear and F-*algebraic* in the sense that it is given by a polynomial over F. One proves that any $\mathbb{F}_q$-linear algebraic endomorphism of F^{s} comes from a uniquely determined Ore polynomial [Pap23, Lemma 3.1.4]. Another nice illustration of this correspondence is given by the following proposition.

Proposition 3.2. *There is a bijection:*

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

We refer to [Gos96, § 1.2] for a proof of the proposition. Here, we just mention that the inverse bijection can be explicitly described as follows. Given a subspace $V \subset F^{\mathrm{s}}$, we form the (classical) polynomial

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

The stability under the Galois action ensures that $\widetilde{f}$ has coefficients in F. Besides, a calculation shows that it defines an $\mathbb{F}_q$-linear function. Thus, the classical polynomial $\widetilde{f} \in F[x]$ can be seen as an Ore polynomial in $F\{\tau\}$. This Ore polynomial is the inverse image of V under the bijection of Proposition 3.2.

Proposition 3.3. *The bijection of Proposition 3.2 is increasing in the sense that f right-divides g if and only if* $\ker f \subset \ker g$*. This implies, in particular, that right-gcds (resp. left-lcms) of Ore polynomials on the left-hand side correspond to intersections (resp. sums) of subspaces on the right-hand side.*

Remark 3.4. Restricting to Ore polynomials with a constant term equal to 1 in Proposition 3.2 is important for two reasons. First, it permits normalising the Ore polynomials as, of course, f and cf (for $c \in F^\times$) have the same kernel. Secondly, it permits discarding all Ore polynomials with vanishing constant terms. Indeed, we observe that f and $f\tau$ also share the same kernel, given that the q-Frobenius induces a bijection on each Galois-stable $\mathbb{F}_q$-linear subspace of F^{s}.

Remark 3.5. The polynomial $\widetilde{f}$ defined above can be expressed in terms of elementary symmetric functions. If we look at $\widetilde{f}$ as a regular polynomial, most of its coefficients are zero; we would also want root-coefficients relations defining $\widetilde{f}$ to be given as expressions in the sole kernel basis elements. Consequently, we introduce the following objects. Consider an integer $n \geqslant 0$, and formal variables $X_1, \dots, X_n, X$. The *Moore determinant* of the family $(X_1, \dots, X_n)$ is defined as

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

It is a polynomial in $X_1, \dots, X_n$, and was introduced by Moore [Moo96] as an $\mathbb{F}_q$-linear analogue of the classical *Vandermonde determinant*. This polynomial satisfies (see [Ore33a, Theorem 10] or [Elk99, Proposition 1])

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

which means that a family $(x_1, \dots, x_n)$ is $\mathbb{F}_q$-linearly dependant, if and only if, $\Delta(x_1, \dots, x_n) = 0$. In particular, if $(\omega_1, \dots, \omega_n)$ is a basis of $\ker f$, the univariate polynomial $\Delta(x, \omega_1, \dots, \omega_n)$ vanishes exactly on $\ker f$. After renormalisation, we obtain

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

Similarly, the unique monic separable polynomial whose set of zeros is $\ker f$ is given by

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

Expanding the determinants, one proves the existence of universal polynomials $\lambda_0^{(n)}, \dots, \lambda_n^{(n)} \in \mathbb{F}_q[X_1, \dots, X_n]$ such that $\bar{f}(x) = \sum_{i=0}^n \lambda_i^{(n)} x^{q^i}$. Each $\lambda_i^{(n)}$ is homogeneous of degree $q^n - q^i$. Altogether, they form the set of $\mathbb{F}_q$-linear elementary symmetric functions.

3.2 Algebraic Drinfeld modules

We are now ready to define Drinfeld modules over a general base, which might be different from C_∞. The definition is of an algebraic nature. Roughly speaking, a Drinfeld module over a field F is the datum of an algebraic structure of A-module on F. Here, algebraicity means that the multiplication by any element $a \in A$ is given by an Ore polynomial $\phi_a \in F\{\tau\}$.

We start by introducing the base fields we will be interested in.

Definition 3.6. An *A-field* is a field F equipped with a ring homomorphism $\gamma : A \to F$. The *A–characteristic* of F is the ideal of A defined by $\mathrm{char}_A(F) = \ker \gamma$.

Throughout the article, we set $z = \gamma(T)$. Since we suppose that $A = \mathbb{F}_q[T]$, the datum of z completely determines γ. Beyond $F = C_\infty$, the most important A-fields considered in the literature are the following.

- F is a finite extension of $\mathbb{F}_q(T)$ and $\gamma : A \to F$ is the canonical injection (so the A-characteristic is zero); this choice leads to the theory of *rational* Drinfeld modules.
- F is a finite extension of $\mathbb{F}_q$ and $\gamma : A \to F$ is a presentation of F as a quotient of $A = \mathbb{F}_q[T]$ (so the A-characteristic is nonzero, it is the defining polynomial of F); this choice leads to the theory of *finite* Drinfeld modules.

We will come back to these two particular bases and Drinfeld modules over them in Section 5.

Definition 3.7. A *Drinfeld module* over a A-field (F, γ) is a homomorphism of $\mathbb{F}_q$-algebras

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

such that:

(i) ϕ_a is nonconstant for at least one element $a \in A$,

(ii) for all $a \in A$, the constant coefficient of ϕ_a is $\gamma(a)$.

Condition (i) in Definition 3.7 is not essential: it simply eliminates trivial cases, which may be a source of problems at some point. On the other hand, Condition (ii) is a normalisation condition which reflects the fact that the derivative of the exponential map (at 0) is 1 (compare with Equation (13)). In some sense, it says that the action of ϕ_a on the tangent space, *i.e.*, the action of the derivative of $\phi_a(x)$, should be the multiplication by a. This requirement is a standard fact in the theory of elliptic curves (or, more generally, abelian varieties) where the multiplication by a on the curve always acts on the Lie algebra by scalar multiplication by a.

Remark 3.8. It is also possible to define Drinfeld modules without referring to γ and define γ afterwards by setting $\gamma := \phi \bmod \tau$. However, it is more standard to proceed as we did in Definition 3.7. This point of view also has the advantage of underlining the importance of the tangent action.

Since we assume that $A = \mathbb{F}_q[T]$, a Drinfeld module ϕ is entirely determined by the Ore polynomial $\phi_T \in F\{\tau\}$. Conversely, any choice of ϕ_T with positive degree and constant term equal to z gives rise to a unique Drinfeld module over A.

The τ-degree of ϕ_T is called the *rank* of ϕ, and we denote it by r. For any $a \in A$, it can be shown that the degree of ϕ_a in τ is equal to $r \deg a$.

SageMath example 3.3. In SageMath, we create a Drinfeld module by specifying the polynomial ring A and the coefficients of ϕ_T (we recall that z was defined in SageMath Example 3.1 as a generator of $\mathbb{F}_{7^2}$).

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

A Drinfeld module $\phi : A \to F\{\tau\}$ defines a structure of A-module over any F-algebra $\mathcal{F}$ through the formula $a \star x = \phi_a(x)$ for $a \in A$ and $x \in \mathcal{F}$. We will use the notation ${}^{\phi}\mathcal{F}$ for $\mathcal{F}$ equipped with this exotic action[1].

3.3 Analytic uniformisation

When $F = \mathbb{C}_\infty$, we have two concurrent viewpoints on Drinfeld modules: the first is analytic, as depicted in Section 2 and the introduction of this section, while the second is algebraic, as described in Subsection 3.2. Here, we aim to reconcile these viewpoints and explain that they both, indeed, define the same objects.

The direction "analytic to algebraic" has already been discussed in the introduction of Section 3. We summarise it by the following theorem.

Theorem 3.9 ([Pap23, Proposition 5.2.2])**.** *Let Λ be a discrete A-submodule of $\mathbb{C}_\infty$ and let*

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

be the corresponding exponential function. Then, the function e_Λ is entire, surjective and $\mathbb{F}_q$-linear. Its zeros consist exactly of Λ, and are all simple. Moreover, for every $a \in A$, there exists a unique Ore polynomial $\phi_a^\Lambda \in \mathbb{C}_\infty\{\tau\}$ such that

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

Finally, the map

$$\begin{array}{rccl} \phi^\Lambda : & A & \to & \mathbb{C}_\infty\{\tau\} \\ & a & \mapsto & \phi_a^\Lambda \end{array} \tag{15}$$

is a Drinfeld module over $\mathbb{C}_\infty$ and its rank is equal to the rank of Λ as an A-module.

The opposite direction "algebraic to analytic" is the so-called *analytic uniformization* theorem for Drinfeld modules. It can be stated as follows.

Theorem 3.10. *Let $\phi : A \to \mathbb{C}_\infty\{\tau\}$ be a Drinfeld module over $\mathbb{C}_\infty$. Then, there exists a lattice Λ in $\mathbb{C}_\infty$ such that $\phi = \phi^\Lambda$.*

[1] In the literature, we often find the notation $\phi(\mathcal{F})$ instead; however, for this survey, we prefer using ${}^{\phi}\mathcal{F}$ in order to minimize the risk of confusion.

Sketch of the proof. The first step is to reconstruct the exponential function e_Λ as an Ore series over C_∞, *i.e.*, an element of the form

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

To find the coefficients c_n, we come back to the functional Equation (14) with $a = T$. In our language, it reads $e_\Lambda T = \phi_T e_\Lambda$ as an equality in the ring of formal Ore power series $C_\infty\{\{\tau\}\}$. Writing

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

and identifying the coefficients (taking care of the noncommutativity relation), we end up with the relation

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

which allows one to compute recursively all the c_n (starting with $c_0 = 1$). Finally, once we know the function e_Λ, we can reconstruct Λ by taking its kernel. The details of the proof can be found in [Pap23, Theorem 5.2.8]. □

The proof of Theorem 3.10 provides an algebraic perspective on the exponential function, which extends to any base of A-characteristic zero. Precisely, if $\phi : A \to F\{\tau\}$ is a Drinfeld module over (F, γ), one defines the exponential function e_ϕ as the Ore series

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

where the coefficients $c_n \in F$ are determined by the recurrence relation

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

The fact that F has A-characteristic zero ensures that the denominator

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

never vanishes.

Similarly, one can define a *logarithm* function $\ell_\phi = \sum_{n=1}^{\infty} \ell_n \tau^n \in F\{\{\tau\}\}$ as the solution of the equation $\ell_\phi \phi_T = z\ell_\phi$. Identifying the coefficients, we now find the relation

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

which again is enough to compute recursively all the ℓ_n. In addition to the identities

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

which hold true for all $a \in A$, we have the formal relation $e_\phi \ell_\phi = \ell_\phi e_\phi = 1$ in $F\{\{\tau\}\}$.

SageMath example 3.4. The exponential and the logarithm are implemented in SageMath. However, since Ore series do not exist in SageMath, the result is given by an actual series where τ^n is replaced by x^{q^n}.

```
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)
```

We can check that they are inverse to each other.

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

3.4 Realisations of Drinfeld modules: Tate modules and Anderson motives

The definition of Drinfeld modules may sound quite disconcerting because they are not in any case modules over a ring. Even worse, they are not "parents" in the sense of SageMath, meaning that they have no elements we can pick and work with.

In this subsection, we explain how to associate Drinfeld modules with actual objects of linear algebra. Beyond making us more comfortable, this will allow us afterwards to easily import classical tools from linear algebra, such as characteristic polynomials, reduction theorems, *etc*.

3.4.1 Torsion points and Tate modules

The first construction we are going to present is the Tate module: it is the straightforward analogue in our context of the classical Tate module of an elliptic curve. We start by defining torsion points.

Definition 3.11. Let $\phi : A \to F\{\tau\}$ be a Drinfeld module over (F, γ). For an ideal $\mathfrak{a} \subset A$, the $\mathfrak{a}$-*torsion* of ϕ is defined as the $\mathfrak{a}$-torsion of ${}^{\phi}F^{\mathrm{s}}$, namely

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

Remark 3.12. Since $A = \mathbb{F}_q[T]$ in our setting, every ideal $\mathfrak{a}$ of A is principal, *i.e.*, $\mathfrak{a} = aA$, and the $\mathfrak{a}$-torsion is simply the set of roots of ϕ_a. The polynomial ϕ_a is sometimes called the *Ore polynomial of a-division* of ϕ.

The $\mathfrak{a}$-torsion $\phi[\mathfrak{a}]$ is naturally a A-submodule of ${}^{\phi}F^{\mathrm{s}}$ which is annihilated by $\mathfrak{a}$, hence, it is a module over the quotient ring $A/\mathfrak{a}$. Besides, it is equipped with an action of the Galois group $\mathrm{Gal}(F^{\mathrm{s}}/F)$. It then gives rise to a $A/\mathfrak{a}$-linear representation of $\mathrm{Gal}(F^{\mathrm{s}}/F)$.

Proposition 3.13 ([Pap23, Corollary 3.5.3])**.** *Let $\phi : A \to F\{\tau\}$ be a Drinfeld module of rank r. Let $\mathfrak{l}$ be a prime ideal of A, which is different from the A-characteristic of ϕ. Then, for all nonnegative integer n, $\phi[\mathfrak{l}^n]$ is free of rank r over $A/\mathfrak{l}^n$.*

Remark 3.14. When $\mathfrak{l} = \mathfrak{p}$ equals the A-characteristic of ϕ, it is still true that $\phi[\mathfrak{p}^n]$ is free over $A/\mathfrak{p}^n$ but its rank is always smaller than r. The defect $\mathrm{h}(\phi) := r - \mathrm{rk}_{A/\mathfrak{p}^n}(\phi[\mathfrak{p}^n])$ does not depend on n and is called the *Frobenius height* of ϕ, often referred to simply as *height*. It can also be interpreted as the τ-valuation of the Ore polynomial $\phi_{\mathfrak{p}}$ divided by the degree of $\mathfrak{p}$. This notion of height is different from the other heights attached to Drinfeld modules.

Passing to the inverse limit, we obtain a family of free modules over $A_{\mathfrak{l}}$.

Definition 3.15. Let $\phi : A \to F\{\tau\}$ be a Drinfeld module and let $\mathfrak{l}$ be a maximal ideal of A. The *Tate module* of ϕ at $\mathfrak{l}$ is

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

It follows that the Tate module of ϕ at $\mathfrak{l}$ has rank r over $A_{\mathfrak{l}}$ when $\mathfrak{l}$ is different from the A-characteristic of ϕ, and has rank $r - h(\phi)$ otherwise.

3.4.2 Anderson motives

The second important construction is that of Anderson motives. As we shall see, it is a very powerful notion which captures all the information encapsulated in a Drinfeld module and, at the same time, is easy to handle and work with, especially from an algorithmic perspective. From a more abstract viewpoint, Anderson motives should be considered as motives of Drinfeld modules in Grothendieck's vision. So far, no analogue is known in the framework of elliptic curves and abelian varieties.

Definition 3.16. Let $\phi : A \to F\{\tau\}$ be a Drinfeld module. Its *Anderson motive* $\mathbf{M}(\phi)$ is $F\{\tau\}$ endowed with the following extra structures:

- a structure of A-module given by:

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

  where the product on the right-hand side is the multiplication in $F\{\tau\}$,
- a structure of F-module given by:

  $$\forall \lambda \in F, \forall m \in \mathbf{M}(\phi), \quad \lambda \bullet m = \lambda m,$$
- an operator $\tau_{\mathbf{M}(\phi)} : \mathbf{M}(\phi) \to \mathbf{M}(\phi)$ defined by $m \mapsto \tau m$.

In what follows, we will omit the sign $\bullet$ and simply write am or λm. We note that being at the same time a A-module and a F-module is equivalent to being a module over $A \otimes_{\mathbb{F}_q} F$. In addition, since $A = \mathbb{F}_q[T]$ in our setting, we have $A \otimes_{\mathbb{F}_q} F \simeq F[T]$. Therefore, the motive $\mathbf{M}(\phi)$ is no more than a $F[T]$ module equipped with an additional endomorphism $\tau_{\mathbf{M}(\phi)}$. We notice, moreover, that the latter is semilinear in the sense that

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

where $\tau : F[T] \to F[T]$ is the ring homomorphism acting trivially on T and raising all the coefficients to the q-th power.

Proposition 3.17. *If $\phi : A \to F\{\tau\}$ is a Drinfeld module of rank r, then $\mathbf{M}(\phi)$ is free of rank r over $F[T]$ with basis $(1, \tau, \ldots, \tau^{r-1})$.*

Proof. We explain how to decompose an element $m \in \mathbf{M}(\phi)$ in the given basis. We recall that, by definition, m is an Ore polynomial in $F\{\tau\}$. The latter being right Euclidean, we can decompose m in the basis ϕ_T as follows:

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

for some nonnegative integer k and some uniquely determined $m_0, \ldots, m_k \in F\{t\}$ of degree at most $r-1$ where $r = \deg_\tau \phi_T$ is the rank of ϕ. Indeed, m_0 is obtained as the remainder in the right division of m by ϕ_T and the next m_i are obtained similarly by dividing the successive quotients. Now writing

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

we get the formula:

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

which turns out to be the decomposition of m in the basis $(1, \tau, \ldots, \tau^{r-1})$.

The previous calculation shows that the family $(1, \tau, \ldots, \tau^{r-1})$ generates $\mathbf{M}(\phi)$. Proving that it is free is left as an easy exercise for the reader. □

We say that $(1, \tau, \ldots, \tau^{r-1})$ is the *canonical basis* of $\mathbf{M}(\phi)$. The proof we have detailed above shows that writing an element of $\mathbf{M}(\phi)$ in the canonical basis is not a difficult task, which can definitely be implemented on a computer.

SageMath example 3.5. One can create the motive attached to a Drinfeld module as follows.

```
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
```

Now, we can create an element of $\mathbf{M}(\phi)$ by passing in an Ore polynomial and observe that the software automatically decomposes it on the canonical basis.

```
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)
```

Having a canonical basis of $\mathbf{M}(\phi)$ allows us to represent linear morphisms with matrices. Following the SageMath convention, we shall write vectors in row—in particular, the matrix $\mathrm{Mat}(f)$ of a morphism f will be defined as the matrix whose ith row are the coefficients of the image by f of the ith element of the basis.

Using the very same definition, it is also possible to attach a matrix to semilinear operators, and especially to the endomorphism $\tau_{\mathbf{M}(\phi)}$. A simple computation shows that, if $\phi_T = z + g_1\tau + \cdots + g_r\tau^r$, then

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

SageMath example 3.6. We have access to the above matrix using the following syntax.

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

Example 3.18. An essential example is the motive of the Carlitz module (see Section 2.2). Recall briefly that the corresponding Carlitz module is the Drinfeld module of rank 1 given by the morphism $c : A \to F\{\tau\}$, $T \mapsto z + \tau$. Its motive $\mathbf{M}(c)$ is then a $F[T]$-module of rank 1, *i.e.*, as a module one has $\mathbf{M}(c) = F[T]\mathbf{e}$ where we used the letter $\mathbf{e}$ to denote the canonical basis of $\mathbf{M}(c)$. In addition, applying Equation (16), one finds that the matrix of $\tau_{\mathbf{M}(c)}$ is simply $\left(T - z\right)$. Therefore, the operator $\tau_{\mathbf{M}(c)}$ is explicitly given by

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

3.4.3 Comparison between Anderson motives and Tate modules

The two constructions we have presented previously are, in some sense, dual to each other. To properly settle this, we consider the bilinear map

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

For all ideals $\mathfrak{a}$ of A, one checks that it induces a second bilinear map at the level of torsion points as follows:

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

It then turns out that the above map is a "perfect duality" in the sense that it makes appear $\phi[\mathfrak{a}]$ as the dual of $\mathbf{M}(\phi)/\mathfrak{a}\mathbf{M}(\phi)$ and *vice versa*. Precisely, we have the following theorem.

Theorem 3.19. *Let $\phi : A \to F\{\tau\}$ be a Drinfeld module and let $\mathfrak{a}$ be an ideal of A. If the A-characteristic of ϕ is not zero, we assume that $\mathfrak{a}$ is coprime with it. Then the bilinear map* (17) *induces an isomorphism*

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

where $\operatorname{Hom}_{F,\tau}(\cdot,\cdot)$ *denotes the A-module of F-linear maps commuting with the τ-action, where τ acts on F^{s} by $x \mapsto x^q$.*

Proof. See [Gos96, §5.4], or [CL26, §2.1] for a more pedestrian approach. □

Remark 3.20. Theorem 3.19 can be seen as a realization of Katz's famous equivalence of categories between Galois representations and Frobenius modules [Kat73, Proposition 4.1.1]: it precisely says that $\phi[\mathfrak{a}]$ and $\mathbf{M}(\phi)/\mathfrak{a}\mathbf{M}(\phi)$ are in correspondence under this equivalence.

Passing to the limit, we deduce from Theorem 3.19 a formula for the Tate module $\mathbf{T}_{\mathfrak{l}}(\phi)$ in terms of $\mathbf{M}(\phi)$. To write it down in a simple form, it is convenient to introduce the dual motive $\mathbf{M}(\phi)^\vee$ of $\mathbf{M}(\phi)$. It is defined by the usual formula

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

The τ-action on it (in the canonical dual basis) is defined by the matrix

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

We observe, nonetheless, that the latter does not assume coefficients in $F[T]$ but in $F[T][\frac{1}{T-z}]$. This means that $\tau_{\mathbf{M}(\phi)^\vee}$ is *not* an endomorphism of $\mathbf{M}(\phi)^\vee$ but only defines a mapping

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

We say that $\mathbf{M}(\phi)^\vee$ is *noneffective*.

For a maximal ideal $\mathfrak{l}$ of A, which is different from the A-characteristic of ϕ, we now have an isomorphism

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

which is compatible with the τ-action (after inverting $T-z$ on the codomain). We finally recover a formula for $\mathbf{T}_{\mathfrak{l}}(\phi)$ by taking the fixed points under the τ-action.

4 Morphisms of Drinfeld modules

In this section, we keep the notation from Subsection 3.2. In particular, we recall that F is an A-field via the ring homomorphism $\gamma : A \to F$ and we set $z = \gamma(T)$.

4.1 The formal definition

Drinfeld modules over (F, γ) are designed to model algebraic structures of A-modules on F-algebras, and likewise, morphisms between two Drinfeld modules correspond to A-linear mappings which are algebraic, *i.e.*, encoded by Ore polynomials.

The formal definition of a morphism between Drinfeld modules only retains the underlying Ore polynomial and can be phrased as follows.

Definition 4.1. Let $\phi, \psi : A \to F\{\tau\}$ be two A-Drinfeld modules over (F, γ). A *morphism* $u : \phi \to \psi$ is an Ore polynomial $u \in F\{\tau\}$ such that $u\phi_a = \psi_a u$ for all $a \in A$. An *isogeny* is a nonzero morphism.

We let $\mathrm{Hom}(\phi, \psi)$ denote the set of morphisms from ϕ to ψ. When $\phi = \psi$, we simply write $\mathrm{End}(\phi)$ for $\mathrm{Hom}(\phi, \phi)$.

Since A is $\mathbb{F}_q[T]$, the condition of Definition 4.1 is equivalent to requiring that $u\phi_T = \psi_T u$, in other words, it is sufficient to check the condition for $a = T$ only. Another remarkable fact is that two isogenous Drinfeld modules necessarily have the same rank. Indeed, the relation $u\phi_T = \psi_T u$ implies on the τ-degrees that $\deg u + \deg \phi_T = \deg \psi_T + \deg u$, and thus that $\deg \phi_T = \deg \psi_T$.

Remark 4.2. We warn the reader that multiple conventions are possible for denoting the sets of morphisms and of endomorphisms. For example, when one has to distinguish between ordinary and supersingular Drinfeld modules (which we will define in Subsection 5.1.4), it is useful to consider morphisms defined on the separable closure, *i.e.*, elements $u \in F^{\mathrm{s}}\{\tau\}$ such that $u\phi_T = \psi_T u$. We would then write $\mathrm{Hom}_{F^{\mathrm{s}}}(\phi, \psi)$ for their set, and $\mathrm{End}_{F^{\mathrm{s}}}(\phi) = \mathrm{Hom}_{F^{\mathrm{s}}}(\phi, \phi)$. This notation differs from the one introduced in [Pap23, Proposition 3.3.10], but aligns with the SageMath implementation (see SageMath Example 5.4).

We observe that, when only ϕ and u are given, it is easy to infer the codomain ψ by solving the equation $u\phi_T = \psi_T u$. This remark also leads to the following proposition.

Proposition 4.3. *Let $\phi : A \to F\{\tau\}$ be a Drinfeld module. Let $u \in F\{\tau\}$ be a nonzero Ore polynomial. Then u defines an isogeny with domain ϕ if, and only if, u right-divides $u\phi_T$.*

Proof. We assume that the condition of the proposition is fulfilled. We define the Ore polynomial ψ_T by the relation $u\phi_T = \psi_T u$. Looking at the coefficient of least degree on the right-hand side, we find that the constant coefficient of ψ_T is z. Hence ψ_T can be prolonged to a Drinfeld module $\psi : A \to F\{\tau\}$ and u defines an isogeny from ϕ to ψ. The converse is proved similarly. □

SageMath example 4.1. One can create a morphism by simply passing the Ore polynomial defining it: if the codomain is not given, it is automatically computed.

```
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
```

Arithmetic operations on morphisms. All basic arithmetic operations on morphisms are defined by importing the standard arithmetic on Ore polynomials. Precisely, morphisms can be:

- Summed. If $u, v : \phi \to \psi$ are two morphisms, then the Ore polynomial $u+v$ also defines a morphism. Indeed, we have
$$(u + v) \cdot \phi_T = u\phi_T + v\phi_T = \psi_T u + \psi_T v = \psi_T \cdot (u + v).$$
- Multiplied by scalars in $\mathbb{F}_q$. Note that since $\mathbb{F}_q$ is in the centre of $F\{\tau\}$, for any isogeny u on ϕ, and any scalar $\lambda \in \mathbb{F}_q$, then λu and $u\lambda$ define the same isogeny.
- Multiplied by elements in A. Given $u : \phi \to \psi$ and $a \in A$, the product au is defined by the Ore polynomial $u\phi_a = \psi_a u$; we easily check that it is again an isogeny from ϕ to ψ.

- Composed. Given $u : \phi \to \psi$ and $v : \psi \to \mu$, the product of Ore polynomials uv defines a morphism from ϕ to μ. Indeed, one instantly checks that $uv\phi_T = u\psi_T v = \mu_T uv$. The identity morphism also makes sense: it is represented by the constant Ore polynomial 1.

One can summarize the above properties by saying that Drinfeld modules over a fixed base (F, γ) form a A-*linear category*, meaning in particular that the sets $\mathrm{Hom}(\phi, \psi)$ are modules over A and that the $\mathrm{End}(\phi)$ are algebras over A.

SageMath example 4.2. We create another isogeny v and compose it with u.

```
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
```

In the code above, the last two lines check that the composites $u \circ v$ and $v \circ u$ are both the scalar multiplications by $T-1$. We observe, nevertheless, that the Ore polynomials defining them are different. Indeed, the first one is ψ_{T-1} (since $u \circ v$ is an endomorphism of ψ), while the second one is ϕ_{T-1}. We shall see later on in Subsection 4.4.3 that $T-1$ is the norm of u, and v is its dual isogeny.

Proposition 4.4. *Let $\phi : A \to F\{\tau\}$ be a Drinfeld module. Let $u_1, \ldots, u_n$ be isogenies with domain ϕ. Then, the Ore polynomials* $\mathrm{rgcd}(u_1, \ldots, u_n)$ *and* $\mathrm{llcm}(u_1, \ldots, u_n)$ *both define isogenies with domain ϕ.*

Proof. We let ψ_i denote the codomain of each isogeny u_i ($1 \leqslant i \leqslant n$). For every index i, we have the relation $u_i\phi_T = \psi_{i,T}u_i$.

We now write $u = \mathrm{rgcd}(u_1, \ldots, u_n)$. Given that $F\{\tau\}$ is left-euclidean, there exists a Bézout relation $u = \sum_{i=1}^n m_i u_i$ with $m_i \in F\{\tau\}$. We deduce that $u\phi_T = \sum_{i=1}^n m_i \psi_{i,T} u_i$. Hence $u\phi_T$ is in the left-ideal generated by the u_i, and so that it is right-divided by their right-gcd u. We conclude that u defines an isogeny with domain ϕ by invoking Proposition 4.3.

Let now $v = \mathrm{llcm}(u_1, \ldots, u_n)$. By definition u_i right-divides v. Thus, we can write $v = m_i u_i$ with $m_i \in F\{\tau\}$ and obtain the relation $v\phi_T = m_i u_i \phi_T = m_i \psi_{T,i} u_i$ which proves that u_i also right-divides $v\phi_T$. Since this holds for all u, we find that v also right-divides $v\phi_T$. Again, we conclude using Proposition 4.3. □

The action on the F^{s}-points. Another option to approach morphisms of Drinfeld modules is to study their action on F-algebras. Indeed, any morphism of Drinfeld modules $u : \phi \to \psi$ in the previous sense induces maps, which we will still denote by u

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

for every F-algebra $\mathcal{F}$. This construction is particularly relevant when $\mathcal{F}$ is F^{s}. Indeed, one can prove that two isogenies $u, v : \phi \to \psi$ are equal if, and only if, they induce the same morphisms ${}^{\phi}F^{\mathrm{s}} \to {}^{\psi}F^{\mathrm{s}}$.

We will elaborate more on this viewpoint in Subsection 4.4 below.

4.2 Separability

Regarding isogenies of elliptic curves, there is an important distinction between separable and nonseparable ones: the former correspond to finite subgroups, whereas the latter are typically modelled by the Frobenius morphism. Such a dichotomy is also relevant in the case of Drinfeld modules, as we will discuss now.

4.2.1 Separable isogenies and their kernels

We start by defining the notion of separability in the context of Drinfeld modules.

Definition 4.5. An isogeny $u : \phi \to \psi$ is *separable* if its τ-valuation is zero, *i.e.*, its constant coefficient does not vanish when viewed as an Ore polynomial.

We recall from Proposition 3.2 that we have defined the kernel of a morphism u by

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

It is an A-submodule of ${}^{\phi}F^{\mathrm{s}}$, which is finite if, and only if, u is an isogeny. Besides, as a subset of F^{s}, it is equipped with an action of $\mathrm{Gal}(F^{\mathrm{s}}/F)$.

Proposition 4.6. *Let $\phi : A \to F\{\tau\}$ be a Drinfeld module. Let G be an A-submodule of ${}^{\phi}F^{\mathrm{s}}$ which is finite and stable by the action of* $\mathrm{Gal}(F^{\mathrm{s}}/F)$. *Then, there exists a Drinfeld module $\psi : A \to F\{\tau\}$ and a separable isogeny $u : \phi \to \psi$ such that* $\ker u = G$.

Proof. Applying Proposition 3.2, we find an Ore polynomial $u \in F\{\tau\}$ with constant term 1 such that $\ker u = G$. Moreover, the fact that G is a A-submodule ensures that $\phi_T(G) \subset G$, from what we derive $\ker u \subset \ker(u\phi_T)$. Thus, it follows from Remark 3.3 that u right-divides $u\phi_T$, *i.e.*, there exists an Ore polynomial $\psi_T \in F\{\tau\}$ such that $u\phi_T = \psi_T u$. This Ore polynomial ψ_T defines a Drinfeld module ψ for which u becomes an isogeny $\phi \to \psi$. □

Remark 4.7. The isogeny ψ of Proposition 4.6 is uniquely determined up to an isomorphism of ψ, *i.e.*, multiplication by a nonzero element of $\mathbb{F}_q$ (see Subsection 4.3). We can then normalise it by requiring either that it has a constant coefficient 1 (as in Proposition 3.2) or that it is monic.

It is interesting to reinterpret Proposition 4.4 in light of what precedes. Indeed, we recall from Proposition 3.3 that right-gcds (resp. left-lcms) correspond to taking intersections (resp. sums). Therefore, when the isogenies u_i are separable, the Ore polynomials $\mathrm{rgcd}(u_1, \ldots, u_n)$ and $\mathrm{llcm}(u_1, \ldots, u_n)$ define the isogenies having $\ker(u_1) \cap \cdots \cap \ker(u_n)$ and $\ker(u_1) + \cdots + \ker(u_n)$ as kernel, respectively.

4.2.2 Nonseparable isogenies and the Frobenius morphism

When the A-characteristic of F is zero, one checks that all isogenies are separable and thus correspond to finite A-submodules of ${}^{\phi}F^{s}$.

On the contrary, when the A-characteristic of F is a maximal ideal $\mathfrak{p}$, inseparable isogenies do exist. Indeed, from the fact that $\mathrm{char}_A(F) = \mathfrak{p}$, we derive that $z^{q^{\deg \mathfrak{p}}} = z$. Therefore, if we write $\phi_T = z + g_1\tau + \cdots + g_r\tau^r$, the Ore polynomial $\tau^{\deg \mathfrak{p}} \in F\{\tau\}$ satisfies the following commutation relation:

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

where

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

In other words, $\tau^{\deg \mathfrak{p}}$ defines a nonseparable isogeny from ϕ to the Drinfeld module ϕ' defined by Equation (20).

Definition 4.8. The isogeny $\tau^{\deg(\mathfrak{p})} : \phi \to \phi'$ is called the *relative Frobenius morphism* of ϕ.

SageMath example 4.3. In the example below, we have $\gamma(T) = 1$, so the relative Frobenius is represented by the Ore polynomial τ.

```
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
```

On the contrary, when $\gamma(T)$ generates F, the relative Frobenius is an endomorphism. It is the so-called *Frobenius endomorphism*, which will be discussed in more detail in Subsection 5.1.1.

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

It turns out that the Frobenius morphism is the prototypical example of nonseparable isogenies, as underlined by the following proposition.

Proposition 4.9. *Any nonseparable isogeny $u : \phi \to \psi$ between Drinfeld modules of A-characteristic $\mathfrak{p}$ factors through the relative Frobenius of ϕ, i.e., there exists an isogeny $u' : \phi' \to \psi$ such that $u = u'\tau^{\deg \mathfrak{p}}$.*

Any isogeny $u : \phi \to \psi$ can be written $u = v\tau^{m \deg \mathfrak{p}}$ where v is separable and m is a nonnegative integer.

Proof. It is enough to show that the τ-valuation of u is at least $\deg \mathfrak{p}$. This follows by writing down the commutation relation $u\phi_T = \psi_T u$ and comparing the coefficients of the smallest degree. The second statement follows by repeatedly applying the first one. □

Remark 4.10. We stress that the factorisation in the opposite direction, namely $u = \tau^{\deg \mathfrak{p}}u'$ may fail in full generality. However, it does always exist when F is a finite field.

As in the case of elliptic curves, the Frobenius morphism plays a primary role in the study of Drinfeld modules over finite fields. We will elaborate more on this in Subsection 5.1.

4.3 Isomorphisms and j-invariants

An important family of morphisms is, of course, that of isomorphisms. Coming back to the definition, we see that an isomorphism $u : \phi \to \psi$ is encoded by an invertible Ore polynomial u. In virtue of the additivity of the degrees, it turns out that invertible Ore polynomials are just nonzero constant ones. Hence, isomorphisms are simply given by elements in $F^\times$. That being said, it is possible to consider isomorphisms over any extension F'/F: constant Ore polynomials u of $F'\{\tau\}$ such that $u\phi_T = \psi_T u$. In this subsection, we describe a procedure to test isomorphism, and give invariants to encode isomorphism classes (over F^{s}).

4.3.1 Deciding whether two Drinfeld modules are isomorphic

Let us fix a Drinfeld module $\phi : A \to F\{\tau\}$ of rank r and write

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

Any element $u \in (F^{\mathrm{s}})^\times$ now defines an isogeny $u : \phi \to \psi$ where ψ is the Drinfeld module of rank r which is explicitely defined by

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

Another consequence of this calculation is a procedure to decide if two Drinfeld modules ϕ and ψ are isomorphic: it is the case if, and only if, the coefficients of ψ_T can be deduced by those of ϕ_T by multiplying by u^{1-q^i} (where i is the corresponding τ-degree). Although this criterion looks quite easy to check, one needs to be careful with the possible vanishing of the coefficients. However, paying attention to properly handling this somewhat annoying case, one ends up with an efficient algorithm to check isomorphism (see also [Leu24, § 3.2.3.5] for additional details).

SageMath example 4.4. The isomorphism test we mentioned is implemented. This method even allows us to decide if the Drinfeld modules are isomorphic over the base field, or over the separable closure, the former being the default.

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

Here, we can check by hand that the isomorphism is given by the constant Ore polynomial $z + 1$.

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

Below is a second example where ϕ and ψ are not isomorphic over the ground A-field F, but are over F^{s}.

```
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-invariants

An important fact is that isomorphism classes over F^{s} can be captured by algebraic invariants. In rank 1, the situation is trivial: all Drinfeld modules of rank 1 are isomorphism to the Carlitz module $T \mapsto z + \tau$ over F^{s}.

Rank-2 Drinfeld modules. It follows from what we did in Subsection 4.3.1 that two Drinfeld modules ϕ and ψ of rank 2 defined by

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

are F^{s}-isomorphic if, and only if, there exists $u \in (F^{\mathrm{s}})^\times$ such that $h_1 = u^{q-1} g_1$ and $h_2 = u^{q^2-1} g_2$. Raising the first equation to the power $q+1$, we get $h_1^{q+1} = u^{q^2-1} g_1^{q+1}$, and combining now with the second equation, we get the necessary condition

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

It turns out that this condition is also sufficient. Indeed, if $g_1 \neq 0$ (and so $h_1 \neq 0$ as well), we solve the first equation $h_1 = u^{q-1} g_1$ and verify that any solution is also a solution of the second one. On the contrary, if $g_1 = h_1 = 0$, we just solve the second equation, the first one being automatically fulfilled.

Definition 4.11. The quantity g_1^{q+1}/g_2 appearing in Equation (21) is called the *j-invariant* of ϕ and is denoted by $j(\phi)$.

It characterises the isomorphism class of ϕ over F^{s}.

SageMath example 4.5. We reuse the isomorphic (over the separable closure, but not the base field) Drinfeld modules of SageMath Example 4.4, and verify that they have the same j-invariant.

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

Remark 4.12. For any j in K, let $\phi_T = z + \tau^2$ if $j = 0$ or $\phi_T = z + \tau + j^{-1}\tau^2$ otherwise. Then the Drinfeld module $A \to F\{\tau\}$ defined by ϕ_T has j-invariant j.

Higher rank Drinfeld modules. Isomorphism invariants for Drinfeld modules of higher ranks were introduced by Potemine [Pot98].

Definition 4.13. Let $\phi : A \to F\{\tau\}$ be a Drinfeld module of rank r. Write $\phi_T = z + g_1\tau + \cdots + g_r\tau^r$ with $g_r \neq 0$. Let $\ell < r$ and $\boldsymbol{k} = (k_1, \ldots, k_\ell)$ be a multi-index with $1 \leqslant k_1 \leqslant \ldots \leqslant k_\ell \leqslant r-1$ and let $\boldsymbol{s} = (s_1, \ldots, s_\ell, s_r)$ be a $(\ell+1)$–tuple of integers such that the following hold:

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

The *Potemine J-invariant* of ϕ of index $(\boldsymbol{k}, \boldsymbol{s})$ is

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

There is *a priori* an infinite number of acceptable pairs $(\boldsymbol{k}, \boldsymbol{s})$. Nevertheless, changing $\boldsymbol{s}$ into $n\boldsymbol{s}$ (with $n \in \mathbb{N}$) results in raising the corresponding J-invariant to the power n. For this reason, it is safe to restrict ourselves to the so-called *basic* parameters, that are the parameters $(\boldsymbol{k}, \boldsymbol{s})$ satisfying the extra condition $\gcd(s_1, \ldots, s_\ell, s_r) = 1$.

Although the list of basic parameters gets rapidly very long when r increases, it always remains finite. As an extreme case, when $r = 2$, there is one unique basic parameter, namely $\boldsymbol{k} = (1)$ and $\boldsymbol{s} = (q+1, 1)$. The corresponding Potemine J-invariant is the j-invariant we have introduced in Definition 4.11.

SageMath example 4.6. SageMath has methods to build the list of basic parameters and to compute the corresponding J-invariants in any rank. We already see in the example below that the complete list of Potemine J-invariants can be very long, even in rank 3.

```
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)
```

Remark 4.14. We warn the reader that different naming conventions may be employed for the invariants. We chose to follow that of Potemine, which is also used in SageMath. Papikian uses a different notation: the j-invariants, respectively the *basic* j-invariants, of [Pap23] correspond to the basic j-invariants of Potemine, respectively to the Potemine J-invariant associated to the parameters $\boldsymbol{k} = (k)$ and $\boldsymbol{s} = \frac{1}{q^{\gcd(k,r)-1}} \cdot (q^r - 1, q^k - 1)$, namely

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

These invariants characterise the isomorphism classes of Drinfeld modules over the algebraic closure, as can be seen in the following theorem.

Theorem 4.15 ([Pap23, Theorem 3.8.11])**.** *Let $\phi, \psi : A \to F\{\tau\}$ be two Drinfeld modules of the same rank. We assume that F is separably closed. Then ϕ and ψ are isomorphic if and only if they have the same basic Potemine J-invariants.*

4.4 Action on Anderson motives and consequences

We have already said previously that a morphism $u : \phi \to \psi$ between Drinfeld modules can be realised as an actual A-linear map $u : {}^{\phi}F^{s} \to {}^{\psi}F^{s}$. However, the structure of A-module of ${}^{\phi}F^{s}$ is not easy to describe and to work with; for example, it is usually not of finite type (see [Poo95]). One can work around this issue by substituting the Tate module $\mathbf{T}_{\mathfrak{l}}(\phi)$ to ${}^{\phi}F^{s}$. Choosing correctly the prime ideal $\mathfrak{l}$, we then know that $\mathbf{T}_{\mathfrak{l}}(\phi)$ is a free module over $A_{\mathfrak{l}}$ of rank $r := \mathrm{rank}(\phi)$. Although this modification definitely allows for many nice applications, it still has the unpleasant disadvantage of introducing an auxiliary prime $\mathfrak{l}$ and the associated completion $A_{\mathfrak{l}}$. In what follows, we will show that considering Anderson motives (introduced in Subsection 3.4.2) instead of Tate modules elegantly resolves all these issues.

Given an isogeny $u : \phi \to \psi$, we define

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

where the product mu is computed in $F\{\tau\}$. One readily checks that $\mathbf{M}(u)$ is $F[T]$-linear and commutes with the τ-action, *i.e.*, it satisfies

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

We emphasize that the construction is contravariant, *i.e.*, the direction of the arrows is reversed: if u goes from ϕ to ψ, then $\mathbf{M}(u)$ goes from $\mathbf{M}(\psi)$ to $\mathbf{M}(\phi)$.

Given that $\mathbf{M}(u)$ is a linear map, one can consider its matrix in the canonical bases of $\mathbf{M}(\psi)$ and $\mathbf{M}(\phi)$, respectively. Concretely, the ith row of $\mathrm{Mat}(\mathbf{M}(u))$ is formed by the coefficients of $\tau^i u$ in $\mathbf{M}(\phi)$.

SageMath example 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 Full faithfulness theorems

The first important result about Anderson motives is the following theorem, which tells that the functor $\mathbf{M}$ is fully faithful.

Theorem 4.16. *Let $\phi, \psi : A \to F\{\tau\}$ be two Drinfeld modules. Then, there is a canonical bijection*

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

where $\mathrm{Hom}_{F[T],\tau}$ consists of all $F[T]$-linear maps commuting with the τ-action.

Proof. It suffices to prove that the inverse map is given by $f \mapsto f(1)$, which is a straightforward verification. □

Using the fact that the Anderson motive determines the Tate modules (see Equation (19)), we deduce from Theorem 4.16 a full faithfulness result at the level of Tate modules, which can be seen as an analogue of Tate's theorem on abelian varieties.

Theorem 4.17. *Let $\mathfrak{l}$ be a maximal ideal of A which is different from the A-characteristic of (F, γ). Then, for all Drinfeld modules $\phi, \psi : A \to F\{\tau\}$, the canonical map*

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

is injective and its image consists exactly of the morphisms $\mathbf{T}_{\mathfrak{l}}(\phi) \to \mathbf{T}_{\mathfrak{l}}(\psi)$ which are equivariant under the action of $\operatorname{Gal}(F^s/F)$*.*

4.4.2 Characteristic polynomials

Anderson modules are also quite useful to import classical constructions of linear algebra and attach meaningful invariants to morphisms of Drinfeld modules. A typical example in this line is the construction of the characteristic polynomial of an endomorphism of a Drinfeld module, which can be defined as follows.

Definition 4.18. Let u be an endomorphism of a Drinfeld module ϕ. The *characteristic polynomial* of u, denoted by χ_u, is defined as the characteristic polynomial of the $F[T]$-linear map $\mathbf{M}(u) : \mathbf{M}(\phi) \to \mathbf{M}(\phi)$, *i.e.*,

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

It follows from the definition that $\chi_u(X)$ is a polynomial of degree r, the rank of ϕ. It has *a priori* coefficients in $F[T] \simeq A \otimes_{\mathbb{F}_q} F$, but one actually derives from the fact that $\mathbf{M}(u)$ commutes with the τ-action that $\chi_u(X)$ takes coefficients in A. Besides, the Cayley–Hamilton theorem asserts that $\chi_u(\mathbf{M}(u)) = 0$, which implies that $\chi_u(u) = 0$ by Theorem 4.16.

Definition 4.18, coupled with Proposition 3.17, directly leads to an algorithm to compute characteristic polynomials of endomorphisms. This is currently the default method in SageMath. More details, including complexity statements and various optimisations, are provided in [CL26].

SageMath example 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
```

Below, we decompose the computation of χ in two steps: first, we compute the matrix of the Frobenius endomorphism acting on $\mathbf{M}(\phi)$ and second, we compute its characteristic polynomial.

```
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
```

One can check on this example that the characteristic polynomial χ indeed annihilates u.

```
sage: χ(u)
Endomorphism of Drinfeld module T |--> τ^2 + z*τ + z
  Defn: 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 + z
  Defn: 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)
0
```

Remark 4.19. Musleh and Schost also proposed a general method for computing characteristic polynomials of endomorphisms [MS23]. Instead of relying on Anderson motives, they rely on the *crystalline cohomology* of the Drinfeld module [Ang97] (see also [Mus23, Chapter 5]). Both methods involve computing the characteristic polynomial as the classical characteristic polynomial of a polynomial matrix. These two families of algorithms were the first to achieve computation of characteristic polynomials of endomorphisms of Drinfeld modules in a relatively large context, whereas previous methods used to restrict to the sole Frobenius endomorphism case, as we will discuss in Subsection 5.1.2.

After Equation (19) comparing Anderson motives and Tate modules, one also finds that, for any prime ideal $\mathfrak{l}$ different from the A-characteristic, $\chi_u(X)$ equals the characteristic polynomial of $\mathbf{T}_\mathfrak{l}(u)$ acting on the Tate module $\mathbf{T}_\mathfrak{l}(\phi)$. This reinterpretation is actually the classical definition in the framework of elliptic curves, where the notion of Anderson motive is missing. We then see clearly here the benefit of Anderson motives: they allow for a simpler definition which, on the one hand, does not depend on an auxiliary prime $\mathfrak{l}$ (and so avoids proving independence results on $\mathfrak{l}$) and, on the other hand, is much more suitable for computations. In particular, it does not involve the separable closure of F, which cannot be easily handled on computers.

4.4.3 Norms and duals of isogenies

In a similar fashion, one can also define norms and dual isogenies.

Definition 4.20. Let $u : \phi \to \psi$ be a morphism of Drinfeld modules over (F, γ). The *norm* of u is defined by

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

where the determinant is computed over $F[T]$ and lc refers to the leading coefficient.

We underline that $\mathbf{M}(u)$ goes from $\mathbf{M}(\psi)$ to $\mathbf{M}(\phi)$, so it is not an endomorphism in general. Hence, taking its determinant requires some precaution since its value depends *a priori* on the choices of bases of the domain and the codomain. However, changing the bases only modifies the determinant by multiplication by an element of $F[T]^\times = F^\times$. Then the quotient of the determinant by its leading coefficient is well-defined. In practice, we can carry out the computations by picking the canonical bases of $\mathbf{M}(\phi)$ and $\mathbf{M}(\psi)$ given by Proposition 3.17.

Remark 4.21. When A is not $\mathbb{F}_q[T]$, it is no longer possible to divide by the leading coefficient of $\det \mathbf{M}(u)$. Instead, one may consider the ideal of A generated by $\det \mathbf{M}(u)$, which remains canonically defined.

As in the case of characteristic polynomials, one proves that the norm of u always lies in A. Moreover, the norm is multiplicative with respect to the composition of isogenies.

Besides, in the same manner as for characteristic polynomials, Definition 4.20 directly leads to an algorithm for computing norms. We again refer to [CL26] for detailed complexity statements.

SageMath example 4.9. We compute the norm of u defined previously and observe that it is the constant coefficient of χ_u. We note that the function `norm` of SageMath returns the ideal, and not a generator (see Remark 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
```

Contrary to characteristic polynomials, the norm continues to make sense for isogenies between different Drinfeld modules. In the example below, we recover the computation we did by hand in the SageMath Example 4.2.

```
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
```

As in the case of elliptic curves, the norm of an isogeny u is related to its kernel

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

and, more precisely, to its Fitting ideal $|\ker u|$ (see Subsection 1.2 for the definition).

Proposition 4.22. *Let u be an isogeny of Drinfeld modules defined over (F, γ).*

1. *If u is separable, then we have an equality of ideals*

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

2. *If u is not separable, then*

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

where h is the τ-valuation of u, and $\mathfrak{p}$ is the A-characteristic of (F, γ).

Sketch of the proof. When u is separable, the formula follows from Theorem 3.19 applied with an ideal $\mathfrak{a}$ annihilating $\ker u$. The general case is deduced from the previous one by factoring out as many times as possible $\tau^{\deg\mathfrak{p}}$ in u (see also Proposition 4.9 in the next section) and showing independently that $\mathrm{norm}(\tau^{\deg\mathfrak{p}}) = \mathfrak{p}$. We refer to [CL26, Theorem 3.2] for more details. □

Proposition 4.23. *Let ϕ and ψ be two Drinfeld modules over (F, γ), and $u : \phi \to \psi$ be an isogeny with norm a. Then there exists an isogeny $\hat{u} : \psi \to \phi$ such that $\hat{u}u = \phi_a$ and $u\hat{u} = \psi_a$.*

Sketch of the proof. The isogeny $\hat{u}$ is defined using Theorem 4.16 by letting $\mathbf{M}(\hat{u})$ be the adjoint (that is, the transpose of the matrix of cofactors) of $\mathbf{M}(u)$. □

The isogeny $\hat{u}$ is called the *dual isogeny* of u. Again, computing it is easily performed: one computes the norm and recovers the dual isogeny via Ore Euclidean division.

SageMath example 4.10. We compute the dual isogeny of the isogeny u of SageMath Example 4.8 and we recognize the isogeny v we already introduced in the SageMath Example 4.2.

```
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
```

Remark 4.24. The dual isogeny is the analogue to the classical *dual isogeny* in the context of elliptic curves: if $\varphi : E \to E'$ is an isogeny with norm n between two elliptic curves, there exists an isogeny $\hat{\varphi} : E' \to E$ that has norm n such that $\hat{\varphi}\varphi$ (resp. $\varphi\hat{\varphi}$) is the endomorphism of multiplication by n on E (resp. E').

We conclude this subsection by noticing that the existence of dual isogenies ensures that "being isogenous" is an equivalence relation.

4.4.4 Structure of Hom spaces and endomorphism rings

Anderson motives also help to describe the structure of the spaces of morphisms between two Drinfeld modules.

Theorem 4.25 ([Pap23, Theorem 3.4.1])**.** *Let ϕ and ψ be two Drinfeld modules over a field F, both of rank r. Then,* $\mathrm{Hom}(\phi, \psi)$ *is a free A-module of rank at most r^2.*

Sketch of the proof. We know from Theorem 4.16 that $\mathrm{Hom}(\phi, \psi)$ is isomorphic to $\mathrm{Hom}_{F[T],\tau}\big(\mathbf{M}(\psi), \mathbf{M}(\phi)\big)$, which itself lives in $\mathrm{Hom}_{F[T]}\big(\mathbf{M}(\psi), \mathbf{M}(\phi)\big)$ which is a free module of rank r^2 over $F[T]$. In order to descend from $F[T]$ to $A = \mathbb{F}_q[T]$, the key observation is that the natural morphism

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

is injective, which is a classical general result about τ-modules. We refer to [Pap23, Proposition 3.4.6] for more details. □

Remark 4.26. Not only does the above proof elucidate the structure of $\mathrm{Hom}(\phi, \psi)$, but it also translates to efficient algorithmic methods for computing this hom space. Indeed, representing $F[T]$-linear morphisms $\mathbf{M}(\psi) \to \mathbf{M}(\phi)$ by $r \times r$ matrices, we are reduced to solving the equation

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

where $M \in F[T]^{r \times r}$ is the unknown and the two other matrices are given by Equation (16). When F is a finite field, it provides efficient algorithms for computing this Hom space. We will give more details on this in Subsection 5.1.3.

Definition 4.27. Given a Drinfeld module ϕ, we set

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

where we recall that $K = \mathbb{F}_q(T)$ is the fraction field of A.

The existence of dual isogenies ensures that $\mathrm{End}^0(\phi)$ is a division algebra; indeed, the inverse in $\mathrm{End}^0(\phi)$ of an isogeny $u : \phi \to \phi$ having norm a and dual $\hat{u}$ is simply $a^{-1}\hat{u}$. Moreover, Theorem 4.25 tells us that $\mathrm{End}^0(\phi)$ has dimension at most r^2 over K, and that $\mathrm{End}(\phi)$ can be seen as an order inside it. The same is true for $\mathrm{End}^0_{F^{\mathrm{s}}}(\phi)$. We will go in further details on the structures of $\mathrm{End}^0(\phi)$ and $\mathrm{End}^0_{F^{\mathrm{s}}}(\phi)$ when F is a finite field in Subsection 5.1.5.

5 Arithmetic aspects of Drinfeld modules

The study of elliptic curves follows quite different branches depending on the base we work on. Roughly speaking, there are three main cases.

- Over $\mathbb{C}$, the main tools are the Weierstraß uniformisation theorem and analytic geometry.
- Over finite fields, the Frobenius endomorphism plays a central role.
- Over number fields, an elliptic curve can be regarded as an elliptic curve over $\mathbb{C}$, but it can also be reduced modulo primes to give elliptic curves over finite fields. This case thus takes advantage of the two previous ones.

In the theory of Drinfeld modules, a similar trichotomy occurs. We have already discussed the analytic theory (see Subsection 3.3), *i.e.*, Drinfeld modules over C_∞. In this section, we develop the theory in the two remaining cases: Drinfeld modules over finite fields and Drinfeld modules over function fields.

5.1 Over finite fields

We assume that F is a finite extension of the finite field $\mathbb{F}_q$. This implies that the morphism $\gamma : A \to F$ associated to the A-characteristic (see Definition 3.6) is not injective. We write $\mathfrak{p} = \mathrm{char}_A(F)$, which is a prime ideal. We denote by $\mathbb{F}_{\mathfrak{p}}$ the quotient $A/\mathfrak{p}$, which is a finite field with $q^{\deg \mathfrak{p}}$ elements, and we have a tower of extensions

$$\begin{tikzcd} \mathbb{F}_q \arrow[r, "\pi_{\mathfrak{p}}"] \arrow[rr, bend right, "\gamma"'] & \mathbb{F}_{\mathfrak{p}} \arrow[r, "\iota_{\mathfrak{p}}"] & F \arrow[r, "\iota_F"] & F^{\mathrm{s}} \end{tikzcd} ,$$

where $\iota_{\mathfrak{p}}$ and ι_F are injections. We also let d denote the degree of F over $\mathbb{F}_q$. It is then a multiple of $\deg \mathfrak{p}$. Throughout this subsection, we also fix a rank-r Drinfeld module $\phi : A \to F\{\tau\}$ defined by $\phi_T = z + g_1\tau + \cdots + g_r\tau^r$ with $g_i \in F$.

5.1.1 The Frobenius endomorphism and its characteristic polynomial

We recall that the Ore polynomial $\tau^{\deg \mathfrak{p}}$ defines an isogeny with domain ϕ, which is called the relative Frobenius of ϕ (see Definition 4.8).

Proposition 5.1. *The isogeny τ^d is an endomorphism of ϕ, which is called the* Frobenius endomorphism *of ϕ.*

The endomorphism τ^d is generally denoted by π.

As we shall see, one invariant of primary importance attached to ϕ is the characteristic polynomial of π. With a slight abuse of notation, due to its central role, we will denote it by $\chi_\phi(X)$ instead of $\chi_\pi(X)$ (see Definition 4.18).

Example 5.2. We recall that the Carlitz module c over (F, γ) is defined by $c_T = z + \tau$ where, as usual, $z = \gamma(T)$. We have seen in Example 3.18 that the Anderson motive of c is one-dimensional over $F[T]$, namely $\mathbf{M}(c) = F[T]{\cdot}\mathbf{e}$, with the τ-action explicitly given by the formula $\tau_{\mathbf{M}(c)}(\mathbf{e}) = (T{-}z)\mathbf{e}$. Using the semi-linearity of $\tau_{\mathbf{M}(c)}$, we deduce by induction that

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

for all positive integers n. Therefore

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

where $d = [F : \mathbb{F}_q]$. In particular, if z generates F over $\mathbb{F}_q$, we find that $\chi_c(X) = X - \mathfrak{p}$ where $\mathfrak{p}$ is a generator of the A-characteristic of (F, γ). More generally, we always have $\chi_c(X) = X - \mathfrak{p}^m$ with $m = [F : \mathbb{F}_q(z)]$.

We observe, in particular, that $\chi_c(1)$ is somehow related to the local factors defining the Carlitz zeta function (see Equation (11)). We will come back to this observation later on, when we will present the theory of L-series (see Subsection 5.2.1).

SageMath example 5.1. We compute the characteristic polynomial of the Frobenius of the Carlitz module and observe that we indeed find the formula found in Example 5.2 above.

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

Below is another example with a Drinfeld module of higher rank. We observe that the T-degrees of the coefficients increase slowly; this is a general phenomenon, as stated below in Theorem 5.4.

```
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
```

The three following theorems underline the importance of χ_ϕ. The first one is an analogue of a famous theorem on elliptic curves stating that the number of rational points is obtained by evaluating the characteristic polynomial of the Frobenius endomorphism at 1 [Sil09, Chapter V, Theorem 2.3.1]. In the case of Drinfeld modules, the role of the group of rational points is played by the A-module ${}^\phi F$. Contrary to abelian varieties, the underlying subset is always the same, that is, F itself. However, its structure as an A-module can vary.

Theorem 5.3 ([Gek91, Theorem 5.1])**.** *The Euler-Poincaré characteristic $|{}^{\phi}F|$ is the principal ideal generated by $\chi_\phi(1)$.*

SageMath example 5.2. Theorem 5.3 implies in particular that all elements in ${}^{\phi}F$ are of $\chi_\phi(1)$-torsion. We check it below with an example.

```
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, 0, 0]
```

The second theorem can be interpreted as an analogue of Hasse's theorem for elliptic curves [Sil09, Chapter V, Theorem 1.1].

Theorem 5.4. *Write $\chi_\phi(X) = \sum_{i=0}^{r} a_i X^r$, with $a_0, \ldots, a_r \in A = \mathbb{F}_q[T]$. For any positive integer $i < r$, we have*

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

In the particular case of the Frobenius norm*, that is, the coefficient a_0, we have an explicit formula: if $p \in A$ denotes the monic generator of $\mathfrak{p}$, we have*

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

It should be noted that, contrary to the case of elliptic curves, Theorem 5.4 is quite easy to establish in the framework of Drinfeld modules, since it follows directly from writing down explicitly the matrix of $\mathbf{M}(\tau^d)$ acting on $\mathbf{M}(\phi)$ and estimating the degrees of its coefficients. Besides, combining Theorem 5.3 and Theorem 5.4 gives the bound

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

for any Drinfeld module ϕ of rank 2 of the form $\phi_T = z + g_1\tau + \tau^2$ with $F = \mathbb{F}_q(z)$. This is the analogue of Weil's bound on the number of rational points of a curve of genus 1.

Theorem 5.5 ([Pap23, Theorem 4.3.2])**.** *Two Drinfeld modules over (F, γ) are F-isogenous if, and only if, they have the same characteristic polynomial of the Frobenius endomorphism.*

5.1.2 Review of methods for computing the characteristic polynomial of the Frobenius endomorphism

We now reflect on the computation of characteristic polynomials of endomorphisms, with a focus on the Frobenius case. This problem is a staple of elliptic curve and isogeny-based cryptography. For elliptic curves over a finite field, the number of rational points is given by the trace of the Frobenius endomorphism. The first deterministic algorithm to compute this quantity was proposed by Schoof [Sch85]. Schoof's algorithm works by computing the trace modulo various distinct prime numbers with division polynomials and recovering it via the Chinese remainder theorem.

A Drinfeld module analogue of this method was proposed, among others, by Musleh and Schost [MS19, Mus18, Mus23]. They describe two versions: a deterministic method, as well as a Monte–Carlo method that is more efficient. We stress that these only work for rank-2 Drinfeld modules. This restriction allows us to directly transpose algorithms from the classical case of elliptic curves.

Previous methods also include one by Gekeler, which involved solving a linear system directly coming from the identity $\chi_\phi(\pi) = 0$ [Gek08], where π is the Frobenius endomorphism of ϕ. It was generalised and implemented by Musleh for higher ranks in [Mus23, § 4.4.1]. On the other hand, Narayanan proposed a method based on the minimal polynomial of sequences [Nar18]. Musleh and Schost expressed doubts on the validity of some of the assumptions made by Narayanan, and suggested a workaround in [MS19, § 5].

In [CL26, § 4], the authors proposed a method for the Frobenius endomorphism in arbitrary rank. It is based on the observation that the Frobenius endomorphism is not only a remarkable element of ϕ, but one of $F\{\tau\}$ as well: setting $d = [F : \mathbb{F}_q]$, the element τ^d is central in $F\{\tau\}$, and the center of $F\{\tau\}$ is given by $\mathbb{F}_q\{\tau\}$. One can then show that the characteristic polynomial of π is the reduced characteristic polynomial of $\phi_T \in F\{\tau\}$, where $F\{\tau\}$ is embedded in a central simple algebra of degree d^2 over its centre.

The methods mentioned in Remark 4.19 also provide a way to compute the characteristic polynomial of the Frobenius endomorphism using Anderson motives. Interestingly, with their optimisations and subsequent variants, all the methods described above have their own benefits, depending on the relative sizes of the input parameters. They are compared in [CL26, Figure 1].

One takeaway message from these computations is that while elliptic curves shed a familiar light on Drinfeld modules, understanding Drinfeld modules as a theory on their own was the key to developing algorithms in much greater generality than the restricted case of the Frobenius endomorphism in rank 2.

Furthermore, those same Ore polynomials give a structure of a central simple algebra, allowing for the computation of the characteristic polynomial of the Frobenius. These objects bypass the need for the computation of torsion elements and Tate modules, thanks to Theorem 3.19.

For more extensive studies on the subject, we refer to Section 4.4 (Frobenius endomorphism in the rank-2 case only) or Section 6.4 (general case) of [Mus23] or [MS19, § 4]. We refer to [CL26, Appendix A] for direct comparison between asymptotic complexities, and to [LS24, § 4.4.2, 5.4.2, 6.4.1] and [ACLM23] for reproducible benchmarks.

5.1.3 Computing isogenies

In contrast with the situation of elliptic curves, isogenies of Drinfeld modules over a finite field can be computed in polynomial time. Indeed, as highlighted by Equation (22), computing $\mathrm{Hom}(\phi, \psi)$ reduces to solving a linear system over A, which is finite dimensional when F is a finite field. Wesolowski [Wes24] and Musleh [Mus23, § 7.3] develop this idea, leading to the following theorem.

Theorem 5.6 ([Mus23, Theorem 7.3.1]). *Let ϕ, ψ be two Drinfeld modules of rank r. There exist algorithms for computing*

1. *an $\mathbb{F}_q$-basis of isogenies of degree at most N in $\mathrm{Hom}(\phi, \psi)$ with quasi-cubic complexity in N and in d, and quasi-linear complexity in r,*

2. *an* $\mathbb{F}_q[\tau^d]$*-basis of* $\mathrm{Hom}(\phi, \psi)$ *with quasi-sextic complexity in* d*, and quasi-linear complexity in* r*,*

3. *an* A*-basis of* $\mathrm{Hom}(\phi, \psi)$ *with quasi-cubic complexity in* d *and in* r*.*

Remark 5.7. Musleh [Mus23] gives, in fact, slightly better complexity involving the exponent of matrix multiplication.

SageMath example 5.3. We compute the hom space between two Drinfeld modules ϕ and ψ. In this case, we further observe that the hom space contains an isogeny defined by a constant Ore polynomial, so ϕ and ψ are isomorphic.

```
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 Supersingularity

Let p again denote the monic generator of $\mathfrak{p} = \ker\gamma$. Recall from Remark 3.14 and Definition 3.15 that the Tate module of ϕ at $\mathfrak{p}$ has rank $r - \mathrm{h}(\phi)$ over $A_{\mathfrak{p}}$, where r is the rank of ϕ, and $\mathrm{h}(\phi)$ is the Frobenius height.

Definition 5.8. One says that ϕ is *ordinary* when $\mathrm{h}(\phi) = 1$, and that ϕ is *supersingular* when $\mathrm{h}(\phi) = r$.

Theorem 5.9 ([Pap23, Corollary 4.2.14, Theorem 4.4.1])**.** *The following properties are all equivalent:*

- *ϕ is supersingular;*
- *$\phi[\mathfrak{p}]$ is trivial;*
- *ϕ_p is purely inseparable;*
- *$\mathrm{End}_{F^s}(\phi)$ has maximal A-rank, i.e., r^2;*
- *$\chi_\phi \equiv X^r \pmod{\mathfrak{p}}$.*

SageMath example 5.4. We illustrate the fact that Theorem 5.9 does not hold if one replaces $\mathrm{End}_{F^s}(\phi)$ by $\mathrm{End}(\phi)$ in the fourth item.

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

We first compute $\mathrm{End}(\phi)$ and see that it has dimension 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]
```

However, more isogenies do exist over an extension. In our example, they show up over $L = F[\sqrt[8]{z}] = \mathbb{F}_{7^{16}}$.

```
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]
```

Remark 5.10. In rank two, the third item of Theorem 5.9 shows that ϕ is supersingular if, and only if, the coefficient of $\tau^{\deg(p)}$ in ϕ_p vanishes. By analogy with the theory of elliptic curves, this coefficient is sometimes called the *Hasse invariant* of ϕ. In [Gek08, Equation 3.6 and Proposition 3.7], Gekeler observed that the Hasse invariant can be computed *via* a recursive procedure as follows. Writing $\phi_T = z + g\tau + \Delta\tau^2$, we set $r_{\phi,0} = 1$, $r_{\phi,1} = g$, and for any integer $k \geqslant 2$, we recursively define

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

Then the Hasse invariant of ϕ is $r_{\phi,\deg(p)}$.

In any rank, the characteristic polynomial of a supersingular Drinfeld module ϕ has a very particular shape: over $\overline{\mathbb{F}}_q[T, X]$, we have the factorization

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

where $\frac{a}{b}$ is the irreducible form of the fraction $\frac{r}{d \deg(\mathfrak{p})}$ and the c_i lie in $\overline{\mathbb{F}}_q$. After Theorem 5.5, this implies in particular that two supersingular Drinfeld modules of the same rank become isogenous over F^{s}.

SageMath example 5.5. We continue the previous example and check that the characteristic polynomial of ϕ has the expected form (here $a = b = 1$, $p = T - 1$, $c_1 = 5z$ and $c_2 = 2z + 5$).

```
sage: χ = φ.frobenius_charpoly()
sage: χ = χ.change_ring(F['T'])  # we extend scalars to F
sage: χ.factor()
(X + 2*z*T + 5*z) * (X + (5*z + 2)*T + 2*z + 5)
```

We pick another supersingular Drinfeld module which is not isogenous to ϕ.

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

But we check that they become isogenous over the extension of F of degree $q^2 - 1 = 48$.

```
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
```

To conclude, we mention the following proposition, which implies in particular that there are only finitely many supersingular Drinfeld modules of a given rank over F^{s}.

Proposition 5.11 ([Gek91, Proposition 4.2])**.** *Let $\phi : A \to F^{\mathrm{s}}\{\tau\}$ be a supersingular Drinfeld module of rank r. Then ϕ is F^{s}-isomorphic to a Drinfeld module defined over a degree r-extension of $\mathbb{F}_{\mathfrak{p}}$.*

5.1.5 The endomorphism ring in rank two

Assuming rank 2, information on supersingularity can also be read on the structure of the endomorphism ring. An elliptic curve over a finite field is ordinary if, and only if, its endomorphism ring over the algebraic closure is commutative [Sil09, Chapter V,

§ 3]. In that case, the endomorphism ring of the elliptic curve is an order in a quadratic number field. Otherwise, it is a maximal order in a quaternion algebra. This is also true for rank-2 Drinfeld modules. Recall that $K = \mathrm{Frac}(A)$ and $\mathrm{End}^0(\phi) = K \otimes_A \mathrm{End}(\phi)$ (Definition 4.27).

Theorem 5.12 ([Car18, Theorem 6.4.2])**.** *Let $\phi : A \to F\{\tau\}$ be an ordinary Drinfeld module of rank 2. Then $\mathrm{End}^0(\phi)$ is an imaginary quadratic function field generated by the Frobenius endomorphism of ϕ. In other words, we have an isomorphism of A-algebras*

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

After Theorem 5.12, we see that, in the ordinary case, $\mathrm{End}(\phi)$ appears as an order in an imaginary quadratic function field. We recall that such fields contain a unique maximal order: their ring of integers, which is also the unique order that is a Dedekind domain. If we denote it by $\mathcal{O}_{\mathrm{End}^0(\phi)}$, the other orders are exactly the sets of the form $\mathcal{O} = A + f\mathcal{O}_{\mathrm{End}^0(\phi)}$ for f in A. The polynomial f is called the *conductor* of $\mathcal{O}$. It is such that $\mathcal{O}$ has index $q^{\deg(f)}$ in $\mathcal{O}_{\mathrm{End}^0(\phi)}$.

SageMath example 5.6. We consider the following ordinary Drinfeld module of rank 2

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

and compute its endomorphism ring

```
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]
```

Noticing that the second endomorphism of the outputted basis is $T - \pi$, we conclude that $\mathrm{End}(\phi)$ is generated by the Frobenius, that is

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

This is a more precise statement than Theorem 5.12 which only gives this isomorphism after scalar extension to K.

In our example, one can check in addition that the discriminant of $\chi_\phi(X)$ is squarefree, implying that $\mathrm{End}(\phi)$ is the maximal order of $\mathrm{End}^0(\phi)$.

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

On the contrary, when ϕ is supersingular, $\mathrm{End}^0(\phi)$ continues to contain the quadratic field generated by the Frobenius endomorphism, but it might be strictly larger. It actually has degree 2 or 4 In the latter case, it is a quaternion algebra over K, *i.e.*, a central simple K-algebra of dimension 4, and $\mathrm{End}(\phi)$ is an order in $\mathrm{End}^0(\phi)$. SageMath Example 5.4 illustrates this situation.

In any case, while $\mathrm{End}(\phi)$ might be commutative and ϕ be supersingular, the following holds as a consequence of Theorem 5.9 and Theorem 5.12.

Proposition 5.13. *A rank-2 Drinfeld module ϕ is supersingular if, and only if,* $\mathrm{End}_{F^s}(\phi)$ *is noncommutative.*

This study is very theoretical. For explicit computations, we have to turn to a completely different point of view, by computing bases with linear algebra methods (see Subsection 5.1.3).

5.1.6 The action of the Picard group

We build on the classification established in Subsection 5.1.5 to present a situation in which the endomorphism and its class group are described in terms of hyperelliptic curves. Ordinary elliptic curves over finite fields and (some) ordinary rank-2 Drinfeld modules over finite fields share a common property: the class group of the endomorphism ring acts freely and transitively on a set of isomorphism classes. Such actions allow us to realise isogenies of Drinfeld modules as ideal classes, whose description can be made very explicit. We now explain how to compute a particular instance of this group action, using imaginary hyperelliptic curves.

As previously, let us still assume that F is a finite field, and that ϕ is a rank-2 Drinfeld module over (F, γ). Let $\chi_\phi \in A[X]$ be the characteristic polynomial of the Frobenius endomorphism. We have $\chi_\phi(X) = X^2 + aX + b$ where, thanks to Theorem 5.4, we know that the polynomials a, $b \in A = \mathbb{F}_q[T]$ verify $\deg(a) \leqslant d/2$ and $\deg(b) = d$. As a and b both lie in $\mathbb{F}_q[T]$, the polynomial χ_ϕ can be seen as a bivariate polynomial in T and X. As such, it defines an algebraic variety. We make the following assumptions.

- We assume that ϕ is ordinary. This implies that a is nonzero (see Theorem 5.9), so that χ_ϕ defines a hyperelliptic curve that we denote by $\mathcal{H}$
- We assume $\mathcal{H}$ to be smooth, and d to be odd. In that case, $\mathcal{H}$ is *imaginary*, with genus $g = \frac{d-1}{2}$.

It turns out that these hypotheses fully determine the F-endomorphism ring of ϕ, and that of all Drinfeld modules F-isogenous to ϕ. Indeed, letting $A_{\mathcal{H}} = A[X]/(\chi_\phi(X))$ denote the coordinate ring of $\mathcal{H}$, the map

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

factors through $A_{\mathcal{H}}$, giving rise to an injective morphism $A_{\mathcal{H}} \to \mathrm{End}(\phi)$. Since $A_{\mathcal{H}}$ is a Dedekind domain, and as such, it is the maximal order of the quadratic function field it lives in, we conclude that $\mathrm{End}(\phi) \simeq A_{\mathcal{H}}$. Crucially, this explicit ring isomorphism yields an explicit group isomorphism

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

where $\mathrm{Pic}^0(\mathcal{H})$ is the degree–0 Picard group of $\mathcal{H}$.

Abstract definition of the action. For an ideal $\mathfrak{a}$ of the endomorphism ring $\mathrm{End}(\phi)$, we define $u_{\mathfrak{a}} = \mathrm{rgcd}(\{a \in \mathfrak{a}\})$, the right-gcd of the Ore polynomials that live in $\mathfrak{a}$. Let ψ be a Drinfeld module F-isogenous to ϕ. By Proposition 4.4, $u_{\mathfrak{a}}$ defines an isogeny from ψ to a Drinfeld module that we denote by $\psi^{\mathfrak{a}}$, and we write

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

If $\mathfrak{a}$ is a principal ideal, meaning that it is generated by an endomorphism of ψ, then $u_{\mathfrak{a}}$ is one of the generators of $\mathfrak{a}$, and ψ equals $\mathfrak{a} * \psi$.

SageMath example 5.7. We illustrate the above constructions with the Drinfeld module ϕ of SageMath Example 5.6. Unfortunately, manipulations of ideals in $\mathrm{End}(\phi)$ are not yet implemented in SageMath. We overcome this issue as follows: we reconstruct the ring $\mathrm{End}(\phi)$ as the quotient $E = A[X]/(\chi_\phi(X))$ and define a function `endomorphism` to convert elements of E into actual endomorphisms.

```
sage: E.<X> = A.extension(χ)
sage: def endomorphism(elt, ψ):   # ψ is a Drinfeld module isogenous to φ
....:     π = ψ.frobenius_endomorphism()
....:     return E(elt).lift()(π)
```

Now, we can write a function `action` by simply following the definition.

```
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()
```

We consider the ideal $\mathfrak{a} = \langle T+4, X+3 \rangle$ and compute $\psi = \mathfrak{a} * \phi$.

```
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
```

We notice that $\mathfrak{a}^2$ is the principal ideal generated by $T+4$. Therefore it acts trivially on ϕ, meaning that $\mathfrak{a} * \psi = \mathfrak{a}^2 * \phi = \phi$. We check this below.

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

It follows from what precedes that the map $*$ defines a group action of $\mathrm{Cl}(\mathrm{End}(\phi))$ on the set of isomorphism classes of Drinfeld modules that are isogenous to ϕ. In a slight abuse of notation, the group action of $\mathrm{Cl}(\mathrm{End}(\phi))$ will still be denoted by $*$. The latter is free and transitive. This can be proven directly by means of tedious computations. A more conceptual approach, which is out of the scope of this document, consists in "reducing modulo $\mathfrak{p}$" a similar group action (known to be free and transitive) that exists for Drinfeld modules over C_∞ and in the context of the class field theory of function fields (see [Hay11, Theorem 9.3] or [LS24, § 2.3]).

Practical computation of the group action. We saw in SageMath Example 5.7 that computing the action of ideals of $\mathrm{End}(\phi)$ can be easily implemented. To go further and compute the action of $\mathrm{Cl}(\mathrm{End}(\phi))$, it only remains to find an efficient representation for the elements of $\mathrm{Cl}(\mathrm{End}(\phi))$. Given that $\mathrm{End}(\phi)$ is isomorphic to $A_{\mathcal{H}}$, and that $A_{\mathcal{H}}$ is the coordinate ring of an imaginary hyperelliptic curve, we have an explicit group isomorphism

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

where $\mathrm{Pic}^0(\mathcal{H})$ is the group of divisors of $\mathcal{H}$ of degree 0 up to rational equivalence. Besides, the elements of $\mathrm{Pic}^0(\mathcal{H})$ can be represented by *Mumford coordinates* [CFA+12, Theorem 14.5], *i.e.*, pairs of polynomials $(u, v) \in A^2$ that verify

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

where $g = \frac{d-1}{2}$ is the genus of the curve $\mathcal{H}$. The element represented by (u, v) is the ideal class of $\langle u, X - v\rangle$. In terms of $\mathrm{End}(\phi)$, this means that (u, v) represents the ideal class generated by the endomorphisms ϕ_u and $\pi - \phi_v$.

Going back to the definition of the group action $*$, Mumford coordinates allow us to represent elements of the acting group by two explicit generators. If (u, v) are the Mumford coordinates representing the class of an ideal $\mathfrak{a}$, computing $\mathfrak{a} * \psi$ simply amounts to computing the right-gcd of the Ore polynomials ψ_u and $\pi - \psi_v$. This can be done, for example, with a variant of the Euclidean algorithm, as discussed in §3.2. This means that computing the group action merely amounts to computing a right-gcd of two Ore polynomials and a right-Euclidean division of Ore polynomials. Explicit complexity statements, as well as an implementation, are presented in [LS24].

Comparison with elliptic curves. The ease with which the group action $*$ is computed suggests a profound fracture with what happens for elliptic curves. In the case of elliptic curves, the group action is defined in terms of kernels of isogenies. If E is an ordinary elliptic curve over the finite field $\mathbb{F}_q$, the isogenies for the group action are defined as follows. Let I be an ideal in $\mathrm{End}(E)$, and consider

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

The kernels are not restricted to rational points. Therefore, V_I is a subgroup of the group of points of E (but not necessarily $E(\mathbb{F}_q)$). Consequently, there exists an elliptic curve E^I, as well as an isogeny ι_I from E to E^I, whose kernel is exactly V_I.

In the end, computing the group action is, as of the time of writing this survey, rather complex [DFKS18]. This is because the computation requires manipulating torsion points that live in possibly large extensions of the base field. With this in mind, we suggest two reasons to explain why the computation of the group action is easy in the case of Drinfeld modules, but not in the case of elliptic curves.

1. The first reason is the manipulation of Ore polynomials (objects defined with information contained in F), rather than their kernels (objects that may live in large extensions of F). The existence of Ore polynomials as a latent space to the theory of Drinfeld modules allows us to take advantage of efficient Ore polynomial arithmetics in virtually all computational aspects of Drinfeld modules. In the case of manipulating kernels of isogenies of Drinfeld modules, this is compatible with the arithmetic of Ore polynomials, in the sense that the intersection of kernels of a family of Ore polynomials is the kernel of the right-gcd of the family.

2. The second reason is related to the arithmetic of function fields. As we have seen, the characteristic polynomial of the Frobenius endomorphism, in the case of Drinfeld modules, defines an algebraic variety. Under our assumptions, this variety was

an imaginary hyperelliptic curve, which allowed us to manipulate the class group of the endomorphism ring of a Drinfeld module as the degree-0 Picard group of the curve. This is a direct example of the benefits of using function field arithmetics.

Remark 5.14. We now explain how the group action presented here is an instance of a more general construction. In the introduction, we stated that Drinfeld modules can be defined over a given ring A' of functions on a curve over a finite field. We also add hypotheses on the curve to make A' a Dedekind ring. Our case $A = \mathbb{F}_q[T]$ corresponds to picking the curve $\mathbb{P}^1_{\mathbb{F}_q}$. But more generally, one can study Drinfeld modules over A', which are called *Drinfeld A'-modules*. In that framework, it is a classical result that the class group of A' acts freely and transitively on the set of isomorphism classes of rank-1 Drinfeld A'-modules defined over C_∞. As shorthand, we are going to call that group action $\mathrm{GA}(A')$.

In our case, the class group of $\mathbb{F}_q[T]$ is trivial, and all Drinfeld A-modules with rank one are isomorphic. One can prove that there exists an equivalence of categories between rank-1 Drinfeld $A_\mathcal{H}$-modules over (F, γ), and rank-2 Drinfeld A-modules on (F, γ) whose endomorphism ring is $A_\mathcal{H}$. Using this correspondence, we recover the group action computed in this section (the class group of $A_\mathcal{H}$ acts on the isomorphism classes of rank-2 Drinfeld modules whose endomorphism ring is $A_\mathcal{H}$) by "reducing" $\mathrm{GA}(A_\mathcal{H})$ modulo a prime ideal.

The general group action is very explicit: for an ideal $\mathfrak{a}$ of A' and a Drinfeld A'-module ϕ, the corresponding isogeny is $\mathrm{rgcd}(\{\phi_a : a \in \mathfrak{a}\})$.

5.2 Over global function fields

We now consider the case where the base field is $F = \mathbb{F}_q(z)$, where z is a formal variable, and $\gamma : A \to F$ is the ring homomorphism taking T to z. Although F is of course isomorphic to $\mathbb{F}_q(T)$ itself, it will be quite important in what follows to use a different variable name on F to avoid confusion in notation, especially when we will consider Anderson motives.

This case is undoubtedly closely related to that of finite fields, since any Drinfeld module over K can be reduced modulo almost all places $\mathfrak{p}$ of K, giving rise to a Drinfeld module over a finite field. On the other hand, it is also related to the analytic theory (see Subsection 3.3) since, given that F embeds into C_∞, a Drinfeld module over F can be viewed as a Drinfeld module over C_∞.

5.2.1 *L*-series

We start with a Drinfeld module $\phi : A \to F\{\tau\}$ and write

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

with $g_i \in F$ for all i. For almost all places $\mathfrak{p}$ of F, it makes sense to reduce all the g_i, and thus ϕ, modulo $\mathfrak{p}$. We let $\phi \bmod \mathfrak{p} : A \to \mathbb{F}_\mathfrak{p}\{\tau\}$ be this reduction. Here $\mathbb{F}_\mathfrak{p}$ denotes the residue field at $\mathfrak{p}$, which is a finite extension of $\mathbb{F}_q$, hence a finite field. One can therefore consider the characteristic polynomial of its Frobenius endomorphism: we denote it by $\chi_{\phi \bmod \mathfrak{p}}(X)$.

The L-series of ϕ is built by putting together all these characteristic polynomials. For simplicity, we assume that all the g_i lie in A. Under this extra assumption, the reduction

ϕ mod $\mathfrak{p}$ is well defined for all places $\mathfrak{p}$ and so $\chi_{\phi \bmod \mathfrak{p}}(X)$ is. The L-series is then given by the following infinite product:

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

The numerator in the fraction above is a normalisation factor: it ensures that all the factors have constant coefficient 1. The convergence of the series holds because there is only a finite number of places $\mathfrak{p}$ of degree bounded by any given constant. Indeed, the two previous observations imply that $L(\phi; X)$ mod X^n is given by a *finite* product for all n; hence the convergence in $K[[X]]$.

One proves that $L(\phi; X)$ is not merely a formal series, but that it moreover converges on C_∞; in other words, it defines an analytic entire function. It turns out that, similarly to the number field case, the value $L(\phi; 1)$ and, more generally the Taylor expansion of $L(\phi; X)$ at $X = 1$, encode a lot of arithmetic information. The example below is a first striking illustration of this yoga.

Example 5.15. We compute the L-series of the Carlitz module c defined by $c_T = z + \tau$. By Example 5.2, we know that $\chi_{c \bmod \mathfrak{p}}(X) = X - \mathfrak{p}$. Plugging this into the definition of the L-series, we find

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

where the product runs over all places of F, that are all irreducible monic polynomials over F. We now observe that the above formula looks very similar to the Euler product of Equation (11) defining the Carlitz zeta function, and indeed, we have the relation $L(c; 1) = \zeta_C(1)$.

The previous example suggests incorporating the variable s in the general definition of the L-series as follows:

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

Indeed, with this definition, the relation $L(c; 1, s) = \zeta_C(s + 1)$ now holds for all $s \in \mathbb{Z}$.

Taelman's class formula. Beyond the example of the Carlitz module, Taelman showed in [Tae12] that, for any Drinfeld module $\phi : A \to F\{\tau\}$, the value $L(\phi; 1)$ has a wonderful arithmetic interpretation in the spirit of the classical class number formula. We recall briefly that this formula relates the special value of the Dedekind zeta function of a number field to several of its invariants of arithmetical nature: the discriminant, the group of roots of unity, the class number and the regulator. We refer to [Neu99, Chapter VII, Corollary 5.11] for a precise statement and a proof of this formula.

Taelman's formula involves function field analogues of the class number and the regulator. Both of them are defined by means of the exponential function e_ϕ we have introduced in Subsection 3.3. Let us recall briefly that e_ϕ is an Ore series in $F\{\{\tau\}\}$. Moreover, letting $F_\infty := \mathbb{F}_q((1/z))$, the restriction of e_ϕ to K_∞ still defines an analytic function $e_\phi : F_\infty \to F_\infty$ satisfying the functional equation

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

In other words, it defines an A-linear map $F_\infty \to {}^\phi F_\infty$ where the structure of A-module on the domain is induced by γ and we recall that ${}^\phi F_\infty$ is F_∞ endowed with its structure of A-module coming from ϕ. The *class module* of ϕ is defined as the quotient A-module

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

where we have set $R := \mathbb{F}_q[z] \subset F$. Taelman [Tae12, Proposition 5] proves that H_ϕ is a finite A-module, and thus we can consider its Euler–Poincaré characteristic $|H_\phi|$ (see Subsection 1.2).

To define the analogue of the regulator, we introduce the module of *Taelman units*:

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

Taelman [Tae12, Theorem 1] proves that U_ϕ is an R-line in F_∞ and we denote by $u_\phi \in K_\infty$ an element such that $\gamma(u_\phi)$ generates U_ϕ. Taelman's theorem now reads as follows.

Theorem 5.16 (Taelman's class formula). *For all Drinfeld modules $\phi : A \to F\{\tau\}$, we have*

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

Example 5.17. When ϕ is the Carlitz module, the class module H_ϕ is trivial, so that we have $|H_\phi| = A$. We deduce from Theorem 5.16 that the Taelman lattice U_ϕ is generated by $L(\phi; 1) = \zeta_C(1)$. Coming back to the definition, we conclude that the image of $\zeta_C(1)$ under the exponential map e_ϕ is a polynomial; it is actually the constant polynomial 1, *i.e.*, we have $e_\phi\big(\zeta_C(1)\big) = 1$. Taking care of domains of convergence, we deduce that $\zeta_C(1) = \ell_\phi(1)$ where ℓ_ϕ is the logarithm of the Carlitz module.

SageMath example 5.8. We can check what precedes in SageMath as follows.

```
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()  # we remove the O(·) to be able to evaluate
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)
```

According to Taelman's theorem, we observe that the previous value agrees with the value at $s = 1$ of the Carlitz zeta function we computed in the SageMath Example 2.3.

Anderson's formula. Taelman's formula and many achievements on L-series of Drinfeld modules are corollaries of a beautiful formula due to Anderson [And00] which, roughly speaking, expresses $L(\phi; X)$ as the cocharacteristic polynomial of a *single* operator σ as follows:

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

The drawback is that the space on which σ acts is not finite-dimensional; hence, defining its cocharacteristic polynomial requires some caution and produces a series and not a polynomial. There actually exist several variations of Anderson's formula. In what follows, we briefly present the motivic version where the operator σ is cooked up from the Anderson motive $\mathbf{M}(\phi)$ attached to ϕ.

We recall that $\mathbf{M}(\phi)$ is a module over $F[T]$. We consider the dual motive $M := \mathbf{M}(\phi)^\vee$ (see Subsection 3.4.3). We further introduce the space $\Omega^1_{F/\mathbb{F}_q}$ of *Kähler differentials* and the *q-Cartier operator* S acting on it. Since $F = \mathbb{F}_q(z)$, we simply have $\Omega^1_{F/\mathbb{F}_q} = F{\cdot}dz$. The q-Cartier operator also has a very explicit description: on polynomials, it is given by

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

and it is extended to $\Omega^1_{F/\mathbb{F}_q}$ thanks to the formula $S(ab^{-1}dz) = S(ab^{q-1})b^{-1}dz$ with $a, b \in \mathbb{F}_q[z]$. We also consider the space $F[T]{\cdot}dz$ and extend S to it by T-linearity[2].

We are now ready to define the operator σ appearing in Equation (24). It acts on the space

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

by

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

Like S, the operator σ is linear with respect to the variable T, but semi-linear with respect to z in the sense that it satisfies $\sigma(z^q f) = z{\cdot}\sigma(f)$ for any $f \in M^\star$. The latter property is the key fact which enables us to define the cocharacteristic polynomial of σ. Roughly speaking, the fact that σ decreases the powers on the variable z implies that the contribution of large positive and negative powers of z will be negligible. Hence, one can approximate the cocharacteristic polynomial of σ by looking at its action on larger and larger finite-dimensional spaces of the form $\langle z^i \rangle_{|i| \leqslant N}$; passing to the limit on N, we finally get the desired result.

In [And00], Anderson managed to give solid foundations to this rough idea and paved the road towards a complete proof of the Equality (24).

It is worth noticing that Anderson's formula is also quite explicit and very well-suited for implementation on computers: in [CG24], the authors turn it into an actual fast algorithm for computing the L-series $L(\phi; X)$–and more generally $L(\phi; X, s)$–attached to a Drinfeld module ϕ.

SageMath example 5.9. This algorithm is implemented in SageMath and performs very well in practice, being able to compute in a couple of seconds thousands of terms of any L-series.

```
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)   # value at 1
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 Triptych: rank-2 Drinfeld modules, elliptic curves over number fields, elliptic curves over function fields

In this paragraph, we gather and compare upper bounds on the minimal degree of isogenies in three classical settings: elliptic curves over number fields, Drinfeld modules

[2] For a general A, we should instead consider $\Omega^1_{A\otimes F/A} = A \otimes \Omega^1_{F/\mathbb{F}_q}$, to which S can be extended by A-linearity in a similar fashion.

of rank 2, and elliptic curves over function fields. We hope the reader will get a feeling for why, at least in this particular case, the best analogue in the function field setting for elliptic curves over number fields, are in fact Drinfeld modules of rank 2, and not elliptic curves over function fields.

The estimates we will study are of two types: upper bounds on the minimal degree of an isogeny between two objects, and an estimate on the height of the relevant j-invariant in any isogeny class.

Let L be a number field. We will use h to denote the *logarithmic Weil height*, which for an element $\alpha \in L$ is defined as

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

where M_L is the set of places of L, and for $v \in M_L$ we write $\| \cdot \|_v$ for the associated absolute value and L_v for the completion of L at v.

Theorem 5.18 ([GR14]). *Let E and E' be two $\overline{L}$-isogenous elliptic curves. Then, there exists an $\overline{L}$-isogeny $f : E \to E'$ such that*

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

where j is the j-invariant of the elliptic curve E.

We underline that there are many isogenies between E and E' which do not satisfy the degree bound from Theorem 5.18. In contrast, the following theorem, which addresses a different but related question, is valid for any isogeny, with a bound that is sharper for minimal degree isogenies.

Theorem 5.19 ([Paz19, Theorem 1.1]). *Let $f : E \to E'$ be an $\overline{L}$-isogeny between two elliptic curves E and E' of j-invariant j and j', respectively. Then*

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

The Northcott property for the Weil height says that a set of algebraic numbers with bounded height and bounded degree is finite. Thus, combined with the two previous theorems, we get that within an isogeny class, there are only finitely many $\overline{L}$-isomorphism classes of elliptic curves over a fixed number field.

The goal of the rest of this subsection is to present similar results for Drinfeld modules and for elliptic curves defined over function fields. The results presented in this subsection are summed up in Figure 2.

Recall that $A = \mathbb{F}_q[T]$ and $K = \mathbb{F}_q(T)$. Let M_K denote the set of places of K. For a place $v \in M_K$ we denote by $\| \cdot \|_v$ the absolute value normalised as follows: if $\mathfrak{p} \in A$ is finite corresponding to v, then $\|x\|_v = q^{-\deg(p)\cdot \mathrm{val}_{\mathfrak{p}}(x)}$, if $\mathfrak{p} \in A$ is infinite corresponding to v, then $\|x\|_v = q^{deg(x)}$. Let F/K be a finite extension of K. For a place $v \in M_F$ extending a place $w \in M_K$, we denote by $\| \cdot \|_v$ the associated absolute value such that for any $x \in K$ we have $\|x\|_v = \|x\|_w$. For a n-tuple $x = (x_1, \ldots, x_n)$ of elements in F we define its logarithmic Weil height h as

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

Remark 5.20. The logarithmic Weil height of Equation (25) is a completely different concept from the Frobenius height used in Definition 5.8. These are both called "height" in the literature, and are both denoted $h(\cdot)$. The context is generally clear.

Theorem 5.21 ([DD99, Theorem 1.3])**.** *Let ϕ and ϕ' be two F^s-isogenous Drinfeld modules of rank r defined over F. Then, there exists an F^s-isogeny $f : \phi \to \phi'$ such that*

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

where $h(\phi')$ is the height of the tuple of Potemine invariants of the Drinfeld module ϕ' (see Definition 4.13).

Theorem 5.22 ([BPR21, Theorem 3.1])**.** *Let $f : \phi \to \phi'$ be an F^s-isogeny between two Drinfeld modules of rank r. Suppose* $\ker f \subseteq \phi[N]$*. Then*

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

where $h(\phi)$ and $h(\phi')$ are the height of the tuple of Potemine invariants of the Drinfeld modules ϕ and ϕ', respectively.

Moreover, if $r = 2$, then we have

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

where j and j' are the j-invariant of the Drinfeld module ϕ and ϕ', respectively.

Again, combining the two previous theorems with the Northcott property, we get that isogeny classes of Drinfeld modules of rank 2 contain finitely many isomorphism classes.

Remark 5.23. In the case of isogenies in parallelogram configurations, there are finer results, see the recent article [BGP25].

Finally, let F be the function field of a smooth projective and geometrically irreducible curve of genus g defined over a perfect field. For elliptic curves defined over F, the following hold.

Theorem 5.24 ([GP22, Theorem B])**.** *Let E and E' be two F^s-isogenous elliptic curves with j-invariant j and j', respectively. Then, there exists an F^s-isogeny $f : E \to E'$ such that*

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

where $\deg_{ins}$ *denotes the inseparability degree.*

Theorem 5.25 ([GP22, Theorem A])**.** *Let $f : E \to E'$ be an F^s-isogeny between two elliptic curves E and E' with j-invariant j and j', respectively. Then,*

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

where $\deg_{ins}$ *denotes the inseparability degree.*

The situation of isogeny classes of elliptic curves over function fields is very different from the two previous settings. These isogeny classes contain infinitely many isomorphism classes! We refer the reader to [GP22] for more details. Taking a look at Theorem 5.25, Theorem 5.22, and Theorem 5.19, it appears that isogeny classes of elliptic curves over number fields behave more like isogeny classes of Drinfeld modules of rank 2, than like isogeny classes of elliptic curves over function fields!

<table>
<tr><th>Drinfeld modules of rank 2</th><th>Elliptic curves over a number field</th><th>Elliptic curves over a function field</th></tr>
<tr><td>Let $f : \phi \to \phi'$ be an isogeny between two <em>Drinfeld modules</em> ϕ and ϕ' <em>of rank</em> 2 on $A = \mathbb{F}_q[t]$.</td><td>Let $f : E \to E'$ be a $\overline{K}$–isogeny between two elliptic curves E and E' over the <em>number field</em> K.</td><td>Let $f : E \to E'$ be a $\overline{K}$–isogeny between two elliptic curves E and E' over a <em>function field</em> K of a smooth projective and geometrically irreducible curve of genus g over a perfect field.</td></tr>
<tr><td colspan="3">Then we can assume that the degree of the isogeny f is at most...</td></tr>
<tr><td>$c_0(q)(h(j)[K:F])^{10\cdot 3^7}$
[DD99, Theorem 1.3]</td><td>$c_0 \cdot [K:\mathbb{Q}] \cdot h(j)$.
[GR14]</td><td>$49 \cdot \max\{1, g\} \cdot \max\left\{\frac{\deg_{ins} j}{\deg_{ins} j'}, \frac{\deg_{ins} j'}{\deg_{ins} j}\right\}.$
[GP22, Theorem B]</td></tr>
<tr><td colspan="2">Then $|h(j) - h(j')|$ is bounded from above by</td><td rowspan="2">$h(j') = \frac{\deg_{ins} f}{\deg_{ins} \hat{f}} \cdot h(j).$
[GP22, Theorem A]</td></tr>
<tr><td>$q + \frac{q^2-1}{2}(\log\deg f + \log(1 + \frac{1}{q}h(j'))\Big)$
[BPR21]</td><td>$10 + 12\log(\deg f)$
[Paz19, Theorem 1.1]</td></tr>
</table>

Figure 2: Isogenies of small degree and height of invariants for elliptic curves and Drinfeld modules of rank 2.

6 Some applications of Drinfeld modules

This section aims to give a glimpse of various applications of Drinfeld modules. We first discuss their use in polynomial factorisation in Subsection 6.1. Some attempts of cryptosystems based on computational problems involving Drinfeld modules, which were believed to be hard enough to ensure security, are presented in Subsection 6.2. Both of these applications leverage the analogies of Drinfeld modules with elliptic curves. Finally, in Subsection 6.3, we present the links between Drinfeld modules and coding theory.

6.1 Drinfeld modules meet computer algebra

Elliptic curves play a pivotal role in computer algebra. They are used for primality testing (*Elliptic Curve Primality Proving* method, developed by Goldwasser–Killian, refined by Altkin and Morain, see [GK86, AM93]) or integer factorization (*Elliptic Curve Method*, developed by H. Lenstra [Len87]). Integer factorisation is a notoriously hard problem, for which the best algorithms (like the *General Number Field Sieve* [Len87]) only attain sub-exponential complexity. On the other hand, factorizing polynomials in $A = \mathbb{F}_q[T]$ can be done very efficiently using probabilistic methods. Some of them rely on Drinfeld modules.

In Subsections 6.1.1–6.1.3 below, we present an algorithm proposed by Doliskani, Narayanan, and Schost [DNS21]. It utilises many of the tools we have presented in the previous sections (supersingularity, structure of the endomorphism ring), and matches the asymptotic complexity of the best methods (as of 2025). Finally, in Subsection 6.1.4, we give an overview of other factorisations algorithms, and compare their performances.

6.1.1 Supersingular reductions

Recall that K is $\mathrm{Frac}(A) = \mathbb{F}_q(T)$, and let $\gamma : A \to K$ be the canonical injection. We let $\phi : A \to K\{\tau\}$ be a Drinfeld module of rank 2 defined by

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

As ϕ is not defined over a finite field, it does not have a Frobenius endomorphism. It thus cannot be supersingular. However, one can wonder if it becomes so upon reducing it at a prime polynomial $f_i \in A$ (see Subsection 5.2.1 for reductions of Drinfeld modules). In that case, we say that ϕ has *supersingular reduction* at f_i. By Theorem 5.9 and Remark 5.10, this is easy to check: one computes the Hasse invariant of ϕ mod f_i. In order to do so, we define the sequence $(r_{\phi,k})_{k\geqslant 0}$ by $r_{\phi,0} = 1$, $r_{\phi,1} = g$ and the recurrence relation

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

Then, the Hasse invariant of ϕ mod f_i is the image of $r_{\phi,\deg(f_i)}$ in A/f_iA.

SageMath example 6.1. The following function computes the Hasse sequence $r_{\phi,k}$ modulo the given modulus up to $k = n$ (recall that $q = 7$).

```
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
```

We compute the $r_{\phi,2}$ mod $T^{7^2} - T$ for $\phi_T = T + T\tau + (T{+}1)\tau^2$.

```
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)
```

The irreducible factors of h of degree 2 are exactly the irreducible polynomials of degree 2 modulo which ϕ has supersingular reduction. We check it below in two cases.

```
sage: F1.<U1> = F7.extension(T^2 + 2*T + 2) # $U_1$ is the image of $T$ modulo $T^2+2T+2$
sage: ϕ1 = DrinfeldModule(A, [U1, U1, U1 + 1])
sage: ϕ1.is_supersingular()
True
sage: F2.<U2> = F7.extension(T^2 + 1)       # $U_2$ is the image of $T$ modulo $T^2+1$
sage: ϕ2 = DrinfeldModule(A, [U2, U2, U2 + 1])
sage: ϕ2.is_supersingular()
False
```

In the second case, we check moreover that the image of h in F_2 is the Hasse invariant of ϕ_2, that is the coefficient in τ^2 of $\phi_2(T^2+1)$.

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

In our use case, the f_i will be the irreducible factors of a given polynomial f, and so their degrees are *a priori* not known, which prevents computing the Hasse invariant. However, building on the fact that the sequence $(r_{\phi,k})_{k\geqslant 0}$ satisfies a recurrence of order 2, one can prove the following alternative characterisation, which only involves the degree of f.

Proposition 6.1 ([DNS21, Lemma 6])**.** *For $f \in A$, $f \neq 0$, we define*

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

Let f_i be an irreducible divisor of f where ϕ has good reduction. Then, ϕ has supersingular reduction at f_i if, and only if, f_i divides $\overline{h}_{\phi,f}$.

Proposition 6.1 readily suggests a method for factoring f: we compute the gcd of f and $\overline{h}_{\phi,f}$ and hope that it yields a nontrivial divisor of f. This will actually occur as soon as f has two irreducible divisors f_1 and f_2 such that ϕ has ordinary reduction modulo f_1 and supersingular reduction modulo f_2.

6.1.2 Drinfeld modules with complex multiplications

To ensure that the previous event will occur with good probability, one must carefully choose ϕ. Indeed, picking it randomly would not work. However, this changes a lot when considering Drinfeld modules with complex multiplications, defined as follows.

Definition 6.2. A Drinfeld module $\phi : A \to K\{\tau\}$ of rank 2 has *complex multiplications* if its endomorphism algebra $\operatorname{End}^0_{K^s}(\phi) = \operatorname{End}_{K^s}(\phi) \otimes_A K$ (see Subsection 5.1.5) is isomorphic, as an A-algebra, to an imaginary quadratic function field.

Drinfeld modules with complex multiplications are scarcer than other Drinfeld modules (those whose endomorphism algebra is isomorphic to K), but they enjoy extra criteria for supersingular reduction. Namely, if f_i is unramified in $\operatorname{End}^0_{K^s}(\phi)$, then ϕ has good supersingular reduction at f_i if, and only if, f_i is inert in $\operatorname{End}^0_{K^s}(\phi)$. Together with Proposition 6.1, this gives the following.

Proposition 6.3. *We assume that ϕ has complex multiplications, and that the irreducible divisors of f are all unramified in $\operatorname{End}^0_{K^s}(\phi)$. Then $\operatorname{gcd}(\overline{h}_{\phi,f}, f)$ is the product of all monic prime factors f_i of f that are inert in $\operatorname{End}^0_{K^s}(\phi)$.*

Our task now is thus to find an explicit Drinfeld module $\phi : A \to K\{\tau\}$ with complex multiplications. We explain how to do so when q is odd; when q is even, we refer to [DNS21, Remark 7]. Picking an element $a \in \mathbb{F}_q$, we consider the field $K(\omega)$, where ω is a square root of $T{-}a$, together with the Drinfeld module $\psi : A \to K(\omega)\{\tau\}$ defined by

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

One readily checks that the Ore polynomial $\tau + \omega$ defines an endomorphism u of ψ whose square is the scalar multiplication by $T{-}a$. We thus get a ring homomorphism $K(\omega) \to \operatorname{End}^0(\psi)$, $\omega \mapsto u$, proving that ψ has complex multiplications. Nonetheless, ψ is not defined over K. We fix this issue by noticing that its j-invariant (see Subsection 4.3) is

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

and so it lies in K given that q is odd. We can then consider the Drinfeld module

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

It is isomorphic to ψ over K^{s}; hence it has complex multiplications as well.

SageMath example 6.2. Doliskani, Narayanan, and Schost's algorithm can be easily implemented as follows.

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

In what precedes, we use Equation (26) for the definition of j, and a is a parameter in the ground field $\mathbb{F}_7$. Depending on the value of a, the function may or may not output a nontrivial divisor. Below, we see that a nontrivial divisor of

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

is found when $a = 1$.

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

Indeed, when $a = 1$, we check that the corresponding Drinfeld module has ordinary reduction modulo the first factor of f, but has supersingular reduction modulo the second one.

```
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
```

We use Equation (26) again for the definition of j, and Remark 4.12 for the Drinfeld modules.

6.1.3 Implementation details and complexity

Turning the strategy presented above into an actual efficient algorithm requires some additional arguments and optimisations.

First of all, one needs to estimate the probability of success of the algorithm. By Proposition 6.3, it can be estimated by studying the proportions of polynomials of A that remain inert in the imaginary quadratic function field $K(\sqrt{T})$. This, in turn, can be done using standard results from the arithmetic of function fields, such as the Chebotarev density theorem or the Riemann–Hurwitz genus formula. All in all, one finally finds that the probability of success in one round of the algorithm is at least $\frac{1}{4}$ (see [DNS21, Lemma 8] and the discussion starting after Lemma 6 in [DNS21]).

Another important ingredient is a fast method for computing $\overline{h}_{\phi,f}$. Indeed, a direct naive method is not performant enough for the overall factorisation algorithm to match the complexity of the state-of-the-art. A crucial contribution of Doliskani, Narayanan and Schost is actually a new procedure to compute $\overline{h}_{\phi,f}$. It relies on modular composition and fast multiplication of two-by-two matrices with entries in A/fA.

Regarding modular composition, the current algorithm with the best asymptotic complexity is that of Kedlaya and Umans [KU01]. One of the innovations of this algorithm was to perform bit operations, as opposed to only algebraic operations. However, no efficient implementation of this algorithm yet exists. For these reasons, the authors of [DNS21] elect to give two kinds of complexity analyses: one using only algebraic algorithms (even for modular composition) and counting operations in $\mathbb{F}_q$, the second using the Kedlaya–Umans algorithm, and counting bit operations. In the second case, one obtains a total bit complexity which grows in $n^{\frac{3}{2}+o(1)}$ (see [DNS21, Theorem 2] for more general statements).

6.1.4 Comparison with other algorithms

For comparing algorithms, it is important to look at both the asymptotic complexity and the practical efficiency. These usually largely differ. In the case of factorisation of polynomials in A, the asymptotically best (as of 2025) algorithm is the combination of the Kaltofen–Schoup factorization algorithm [KS95] with the Kedlaya–Umans algorithm for modular composition [KU01]. This leads to an asymptotic complexity, for factorising a polynomial in A of degree n, of $n^{\frac{3}{2}+o(1)}$ bit operations. As mentioned, this algorithm is highly impractical and would only theoretically become gainful for inputs of significant size. Therefore, the Cantor–Zassenhaus algorithm [CZ81], which leverages ideas developed by Berlekamp [Ber67], is often the preferred method for implementation. It factors a polynomial with almost quadratic complexity (counted in operations in $\mathbb{F}_q$) with respect to n.

We also mention that all polynomial-time methods are probabilistic. The problem of finding a deterministic polynomial algorithm for the factorisation of polynomials on a finite field is still open.

Methods using Drinfeld modules. The known factorisation methods using Drinfeld modules are as follows.

- The method of van der Heiden [vdH04b, vdH04a] is an analogue of Lenstra's *Elliptic Curve Method* method for factorising integers [Len87]. Running the algorithm on a polynomial of degree n costs $O(n^2 \log q + dn^3)$ arithmetic operations in $\mathbb{F}_q$ [vdH04b, Proposition 4.3]. The method requires f to be given as a product of k distinct prime polynomials with a certain degree d. Finding d and normalising accordingly can be achieved by computing gcd's and derivatives following the first steps of the Berlekamp [Ber67] and Cantor–Zassenhaus [CZ81] algorithms. The method of van der Heiden is based on the identification of certain prime factors in the characteristic polynomial of the endomorphism $x\phi_T(x)$ of K, where K is a given finite field and ϕ a random Drinfeld module with rank d. We can therefore use the independent works of Reiner [Rei61] and Gerstenhaber [Ger61] to compute the probability of finding a factor of f in one step [vdH04b, Remark 4.5]. Knowing bounds on the proportion of d-by-d matrices with coefficients in $\mathbb{F}_q$ that have an irreducible characteristic polynomial, van der Heiden shows that by picking ϕ randomly, the success probability is about $1 - \frac{(d-1)^k+1}{d^k}$, provided that q is sufficiently large (see [vdH04b, Proposition 4.3] for a general statement). We also mention the survey of Randrianarisoa, which specifically targets the work of van der Heiden [Ran14].

- While van der Heiden proposed the first known complexity and success analysis of a factorisation method based on Drinfeld modules, the ideas behind his algorithm can be traced back to the work of Potemine and Panchishkin [Pot97, Section 4.3], [Pan93]. This was acknowledged by van der Heiden [vdH04a]. In [Pan93], Panchiskin also mentions that one could adapt classical methods (*Elliptic Curve Primality Proving*) for primality testing in A using Drinfeld modules. Panchishkin also discusses a possible analogue of the Schoof point counting algorithm [Sch85]. One is now known to be described in [MS19, Section 6] (see Subsection 5.1.2).

- Shortly before the work of Doliskani, Narayanan and Schost, Narayanan proposed two factorisation methods using Drinfeld modules [Nar18].

  - The first one is not a factorisation algorithm *per se*, but an algorithm to compute the degree of the smallest prime factor of f. Knowing this information allows for significant speed-ups in the Kedlaya–Umans version of the Kaltofen–Schoup: the bit asymptotic complexity falls to $n^{1+o(1)}(\log q)^{2+o(1)}$. Narayanan reads this smallest degree on the "number of points" (see Theorem 5.3) of a random rank-2 Drinfeld module over a finite field.
  - The second method is a tweaked version of the Berlekamp algorithm, in which the action of a Frobenius endomorphism is replaced by the action of a Drinfeld module. No complexity analysis is provided by the author.

Among these methods, only that of Doliskani, Narayanan and Schost [DNS21] matches the asymptotic state of the art. It is also the only method among those that does not use general random Drinfeld modules, but random Drinfeld modules with complex multiplications. The authors have developed an implementation using the NTL C++ library [Sho90], which uses more straightforward methods for modular composition. It is slower than the default NTL function by a constant factor, due to the manipulation of two-by-two polynomial matrices, according to the authors.

6.2 Drinfeld modules meet cryptography

Cryptography relies on computationally hard problems, be them used in encryption, key exchange, signature or authentication protocols. Classical computationally hard problems include factoring integers, computing discrete logarithms on finite fields and elliptic curves over finite fields, or computing isogenies between elliptic curves over finite fields. These are used in the RSA [RSA78], Diffie-Hellman [DH76], Elliptic Curve Diffie-Hellman [Kob87, Mil86], and SQIsign cryptosystems [DFKL$^+$20], respectively.

In the hope of gaining efficiency with function field arithmetics, there have been many attempts at introducing cryptosystems based on Drinfeld modules, inspired by the aforementioned classical constructions. Unfortunately, all these attempts have failed so far.

- In [Sca01], Scanlon defined the *Drinfeld module discrete logarithm problem*, and the *Drinfeld module inversion problem*, in the hope of building Drinfeld module analogues of the RSA and Diffie-Hellman cryptosystems. He proved the computational ease of these problems in the same paper.

- In [JN19], Joux and Narayanan derived analogues of the SIDH [JDF11] and CSIDH [CLM$^+$18] cryptosystems, and claimed their weakness.

- In [LS22], Leudière and Spaenlehauer proposed an analogue of the CRS cryptosystem. The work of Wesolowski on the computation of isogenies of Drinfeld modules

(Subsection 5.1.3) proved that this new construction, as well as that of Joux and Narayanan, cannot be used safely.

Remark 6.4. We mention that the SIDH cryptosystem was broken in 2022, following a series of attacks started by Castryck and Decru [CD23], Maino and Martindale [MM22], and that culminated in the unconditional cryptanalysis of Robert [Rob23]. As of 2025, CSIDH has not proven insecure. However, the ideas behind SIDH and CSIDH were adapted in the construction of SQISign, a signature protocol in the NIST competition for standardising post-quantum cryptosystems.

Let ϕ be a Drinfeld module defined over a finite A-field (F, γ). Given $x, y \in F$, the *Drinfeld module discrete logarithm problem* consists in finding, if it exists, an element $a \in A$ such that $\phi_a(x) = y$. As far as it is concerned, the *Drinfeld module inversion problem* asks, given $a \in A$ such that ϕ_a is a bijective $\mathbb{F}_q$-linear endomorphism of K, to find $b \in A$ such that ϕ_b (as an $\mathbb{F}_q$-linear endomorphism of K) is the compositional inverse of $\iota(\phi_a)$. Scanlon shows that both problems can be solved using linear algebra techniques: the maps $a \mapsto \phi_a(x)$ and $x \mapsto \phi_a(x)$ are both $\mathbb{F}_q$-linear. In [GLPR03], Gillard, Leprévost, Panchishkin and Roblot proposed a fix for the *Drinfeld module inversion problem.* Their proposal was proven insecure later, by Blackburn, Cid and Galbraith, in [BCG06].

As far as the constructions of Joux–Narayanan and Leudière–Spaenlehauer are concerned, these are all insecure because one can efficiently compute isogenies between Drinfeld modules over a finite field, thanks to the work of Wesolowski (see Subsection 5.1.3).

The common point of these attacks is a finite-dimensional vector space over $\mathbb{F}_q$. No such thing exists in the classical case, because no field lies beneath the ring of integers. We refer to [Leu24, Appendix A] for details on these attempts.

Remark 6.5. It may not be obvious that the Drinfeld module inversion problem is related to the RSA cryptosystem. Yet, there are important symmetries between the two constructions. Both involve a module (over $\mathbb{Z}$ or over A). In each case, we have an encryption cryptosystem, and we now explain (see Table 1) that the encryption function can be seen as a linear endomorphism on a torsion space of this module. For simplicity, let us assume that we work with rank-1 Drinfeld modules, and that we only consider elements ϕ_a when a is away from the A-characteristic.

	Classical RSA	**Drinfeld module RSA**
Module	$\mathbb{Z}$-module defined by: $\mathbb{Z} \times \mathbb{Q}^* \to \mathbb{Q}^*$ $(n, x) \mapsto n * x = x^n$	A-module defined by: $A \times F \to F$ $(a, x) \mapsto a * x = \phi_a(x)$
Torsion	n-torsion (in $\overline{\mathbb{Q}}$): $\mathbb{Z}/n\mathbb{Z}$	a-torsion (in F^{s}): A/aA
Encryption function	Linear automorphism $\mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ $x \mapsto e * x$ with e carefully chosen	Linear automorphism $F \to F$ $x \mapsto a * x$ with a carefully chosen

Table 1: Comparison between the classical RSA setting and its Drinfeld analogue.

One might wonder why the Drinfeld module RSA encryption function would not be defined on A/aA. In the classical case, the isomorphism between the n-torsion and $\mathbb{Z}/n\mathbb{Z}$ is explicit, and given by primitive n-th roots of unity. This allows us to view the multiplicative law $*$ directly on $\mathbb{Z}/n\mathbb{Z}$. No such explicit isomorphism is given in the construction of the Drinfeld module case (see Proposition 3.13). That being said, given that F is finite, all elements of ${}^{\phi}F$ are torsion elements, namely, they are all of $\chi_\phi(1)$-torsion—where χ_ϕ is the characteristic polynomial of the Frobenius endomorphism—by Theorem 5.3, and ${}^{\phi}F$ can be seen as an A-submodule of a torsion space.

These similarities between the classical and Drinfeld module RSA construction come from the constructions of cyclotomic number fields and function fields. As we saw in Subsection 2.3, cyclotomic number fields are obtained by adding roots of unity to $\mathbb{Q}$, while cyclotomic function fields are obtained by adding to $\mathbb{F}_q(T)$ the a-torsion of a rank-1 Drinfeld module defined over C_∞.

6.3 Drinfeld modules meet linear codes

Error-correcting codes are mathematical tools designed to detect and correct errors in transmitted or stored data. A data item is encoded by adding redundancy before being transmitted or stored. Then the original data can be recovered through a decoding operation, even if it has been corrupted during transmission in space and time. The most widely studied model of error-correcting codes is that of *linear codes*.

In this section, we present some known connections between Drinfeld modules and coding theory. Drinfeld modules played a significant role in the construction of asymptotically good codes, which historically gave algebraic geometry its credentials in coding theory. We briefly review this piece of history in Subsection 6.3.2. Very recently, Drinfeld modules have reemerged in coding theory to design locally recoverable codes in the rank metric [BDM24]. We present this construction in Subsection 6.3.3, which originally relies on Carlitz modules, and we discuss its generalisation to higher-rank Drinfeld modules.

6.3.1 Linear codes in the Hamming and the rank metrics

A *linear code* is a $\mathbb{F}_q$-vector subspace of some finite-dimensional $\mathbb{F}_q$-linear ambient space. The efficiency of a linear code is captured by three main parameters, which are its *length*, defined as the dimension of the ambient space in which the code sits, its *dimension* as a vector space, and its *minimum distance*, which depends on the metric put on the ambient space. Notably, the dimension of a code represents the quantity of data that one can encode with it, the length is the size of the transmitted message, which includes the redundancy added to the raw data, while the minimum distance is related to the error detection and correction capacity. Indeed, it is well known that a code with minimum distance d can correct up to $\frac{d-1}{2}$ errors or $d-1$ erasures.

Traditionally, linear codes are defined as $\mathbb{F}_q$-vector subspaces of $\mathbb{F}_q^n$ endowed with the *Hamming distance*, which measures the number of positions in which two codewords, seen as vectors in $\mathbb{F}_q^n$, differ.

Definition 6.6 (Codes in the Hamming metric)**.** The *Hamming distance* between $x, y \in \mathbb{F}_q^n$ is defined as

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

A *code in the Hamming metric* $\mathcal{C}$ is an $\mathbb{F}_q$-linear subspace of $\mathbb{F}_q^n$ endowed with the Hamming distance. Its *dimension* k is $\dim_{\mathbb{F}_q} \mathcal{C}$, its *minimum distance* is defined as

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

We call a code $\mathcal{C} \subseteq \mathbb{F}_q^n$ of dimension k and minimum distance $d(\mathcal{C}) = d$ a $[n,k,d]_q$-code.

A large family of codes in the Hamming metric is composed of so-called *evaluation codes*, which are built, as the name suggests, by evaluating a space of functions at a set of elements. This is the case of *Reed–Solomon* [RS60] and *Reed–Muller codes* [Ree54, Mul54], where one evaluates polynomials in one or m variables at distinct elements of $\mathbb{F}_q$ or $\mathbb{F}_q^m$, respectively, and of *Algebraic Geometry codes* [Gop81], obtained by evaluating rational functions at points over an algebraic curve. A $[n,k,d]_q$-code in the Hamming metric respects the so-called *Singleton bound* $k+d \leqslant n+1$. Codes attaining this bound are called *Maximum Distance Separable* (MDS). The aforementioned Reed–Solomon code, described below, provides an example of an MDS code.

Definition 6.7. Let $k \leqslant n \leqslant q$ be integers. Let $\mathbf{x} = (x_1, \dots, x_n)$ be a tuple of pairwise distinct elements of the finite field $\mathbb{F}_q$. The *Reed–Solomon code* of support $\mathbf{x}$ and dimension k is defined as

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

It is an $[n, k, n-k+1]_q$-code.

More recently, metrics other than that of Hamming have been considered for error-correcting codes, better suited to address specific information theory problems. Among them is the *rank metric* [Del78].

Definition 6.8 (Codes in the rank metric)**.** Let $\mathbb{F}_q^{n\times m}$ denote the space of $n \times m$ matrices with coefficients in $\mathbb{F}_q$. The *rank distance* between $M, N \in \mathbb{F}_q^{n\times m}$ is defined as

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

A *rank metric code* $\mathcal{C}$ is an $\mathbb{F}_q$-linear subspace of $\mathbb{F}_q^{n\times m}$ endowed with the rank distance. Its dimension k is $\dim_{\mathbb{F}_q} \mathcal{C}$, its minimum rank distance is defined as

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

We call a code $\mathcal{C} \subseteq \mathbb{F}_q^{n\times m}$ of dimension k and minimum distance $d := d_{\mathrm{rk}}(\mathcal{C})$ an $[nm, k, d]_q$ *rank-metric code*.

Remark 6.9. Here, we present rank-metric codes in the formalism of matrices to comply with the notation of [BDM24], a paper we will present in Subsection 6.3.3. However, rank-metric codes can also be seen as spaces of linear morphisms. Let V be a $\mathbb{F}_q$-subspace of $\mathbb{F}_{q^m}$ of dimension n. The *rank distance* between $f, g \in \mathrm{Hom}(V, \mathbb{F}_{q^m})$ can naturally be defined as $d_{\mathrm{rk}}(f,g) = \mathrm{rk}(f-g)$. A *rank metric code* $\mathcal{C}$ is then an $\mathbb{F}_q$-linear subspace of $\mathrm{Hom}(V, \mathbb{F}_{q^m})$ endowed with the rank distance. One can recover the matrix point of view by fixing $\mathbb{F}_q$-bases for V and $\mathbb{F}_{q^m}$.

A particular case of rank-metric codes that we will focus on is the so-called *vector rank metric codes*. After choosing an $\mathbb{F}_q$-basis of $\mathbb{F}_{q^m}$, one can associate to any vector $x \in \mathbb{F}_{q^m}^n$ a matrix $M_x \in \mathbb{F}_q^{n\times m}$. Then any vector subspace of $\mathbb{F}_{q^m}^n$ can be endowed with the rank metric and be regarded as a matrix code. Compared to matrix rank-metric codes, they naturally come with the extra property of $\mathbb{F}_{q^m}$-linearity.

Definition 6.10. A *(vector) rank metric code* $\mathcal{C}$ is an $\mathbb{F}_{q^m}$-linear subspace of $\mathbb{F}_{q^m}^n$ endowed with the rank distance. Its dimension k is $\dim_{\mathbb{F}_{q^m}} \mathcal{C}$, its minimum rank distance is defined as

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

We call a code $\mathcal{C} \subseteq \mathbb{F}_{q^m}^n$ of dimension k and minimum distance $d_{\mathrm{rk}}(\mathcal{C}) = d$ an $[n,k,d]_{q^m}$ *rank-metric code*.

Rank-metric codes are particularly effective in contexts where errors may affect entire rows or columns rather than isolated symbols, such as in network coding, space-time coding, and cryptography. The interested reader can consult [BHL$^+$22] for a survey on the applications of rank metric codes.

The theory of Ore polynomials allowed the construction of evaluation codes in the rank metric, leading to the analogues of all the aforementioned codes [Del78, ALR18, ACLN21, BC25, BC24]. In particular, the counterparts of Reed–Solomon codes in the rank metric world are Gabidulin codes, introduced by Delsarte [Del78] and Gabidulin [Gab85].

Definition 6.11. For a positive integer $\kappa \leqslant m$ and a $\mathbb{F}_q$-linear subspace W of $\mathbb{F}_{q^m}$ of dimension n, the associated *Gabidulin code* is defined as the image of the map

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

where $\mathbb{F}_{q^m}\{\tau\}_{\leqslant \kappa-1}$ is the vector space of Ore polynomials of degree bounded by $\kappa - 1$, and we recall from Subsection 3.1.1 that, in a slight abuse of notation, we continue to write f for the induced linear map on $\mathbb{F}_{q^m}$.

The Gabidulin code is an $[mn, m\kappa, n{+}1{-}\kappa]_q$ rank-metric code. One can look at a Gabidulin code as an $\mathbb{F}_{q^m}$-linear subspace of $\mathbb{F}_{q^m}^n$, thus obtaining a $[n, \kappa, n{+}1{-}\kappa]_{q^m}$ (vector) rank-metric code.

The parameters of rank-metric codes satisfy the rank-Singleton bound [Gor21, Theorem 3.5]:

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

Codes whose parameters reach this bound are called *Maximum Rank Distance* (MRD) codes. Gabidulin codes provide examples of MRD codes.

While Ore polynomials have been successfully applied in coding theory in the last forty years, Drinfeld modules have not been used in this context until very recently, when Carlitz modules were exploited to construct codes in the rank metric with optimal properties for distributed storage [BDM24], giving so-called locally recoverable codes. This construction will be described in Subsection 6.3.3. Before that, in the next section, we briefly discuss the importance of Drinfeld modular curves for codes in the Hamming metric.

6.3.2 Modular curves for asymptotically good codes in the Hamming metric

Given a sequence of codes $(C_s)_{s\in\mathbb{N}}$ of parameters $[n_s, k_s, d_s]_q$, we define its *rate* $R := \lim_{s\to\infty} k_s/n_s$ and its relative distance $\delta := \lim_{s\to\infty} d_s/n_s$. A sequence of codes $(C_s)_{s\in\mathbb{N}}$ is said to form a family of *asymptotically good codes* if $R > 0$ and $\delta > 0$.

The *asymptotic Gilbert–Varshamov bound* [Sti09, Proposition 8.4.4] states that families of increasingly long random codes achieve $R > 1 - h_q(\delta) + o(1)$ where h_q is the q-ary entropy function defined by

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

For a long time, it was believed that the Gilbert–Varshamov bound was indeed a bound, that is, no family of structured codes could achieve a better rate and relative distance than random codes, until Tsfasman, Vlăduţ, and Zink constructed Algebraic Geometry codes that beat the Gilbert–Varshamov bound [TVZ82]. The parameters of an Algebraic Geometry code constructed from a curve $\mathcal{X}$ depend on the geometry of $\mathcal{X}$. For instance, the length is bounded from above by the number of $\mathbb{F}_q$-points $\#\mathcal{X}(\mathbb{F}_q)$ of $\mathcal{X}$. Tsfasman, Vlăduţ, and Zink's construction relies on an asymptotically good tower of curves.

A *tower of curves* is an infinite sequence of curves and surjective maps

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

which are all defined over a finite field $\mathbb{F}_q$ and whose genera $g(\mathcal{X}_s)$ satisfy

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

By the Hasse–Weil theorem, the number of $\mathbb{F}_q$-points of each curve $\mathcal{X}_s$ is bounded by

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

The tower is said to be *asymptotically good* if the number of $\mathbb{F}_q$-points on the curves $\mathcal{X}_s$ grows significantly faster than their genera, *i.e.*,

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

From the Hasse-Weil bound, we know that $\frac{\#\mathcal{X}_n(\mathbb{F}_q)}{g(\mathcal{X}_n)} \leqslant 2\sqrt{q}$. Ihara [Iha81] noticed that this bound is far from being met for large-genus curves and introduced the quantity

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

now called *Ihara's constant*. He proved that $A(q) \geqslant \sqrt{q} - 1$ when q is a square. Later, Vlăduţ and Drinfeld proved that $A(q) \leqslant \sqrt{q} - 1$ [VD83], meaning that $A(q) = \sqrt{q} - 1$ when q is a square. A tower $(\mathcal{X}_n)$ is said to be *optimal* if

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

Modular curves provide asymptotically good towers of curves, which are essential for constructing Algebraic Geometry codes with strong asymptotic performance. The classical modular curves $X_0(N)$, parametrising elliptic curves with cyclic N-isogenies, form asymptotically good towers over $\mathbb{F}_{p^2}$, for prime p. This was leveraged by Tsfasman, Vlăduţ, and Zink to construct Algebraic Geometry codes beating the Gilbert–Varshamov bound [TVZ82]. The curious reader is invited to read [Cou23] for a detailed introduction to this topic.

Similarly, Drinfeld modular curves, which parametrise rank-2 Drinfeld modules with level structures, also yield asymptotically good towers over any quadratic field $\mathbb{F}_{q^2}$ [BBN15], and more generally any non-prime field. These curves are particularly useful over finite fields $\mathbb{F}_q$ where q is a square, as seen in the optimal towers constructed by Garcia and Stichtenoth [GS95]. Elkies gave a modular interpretation for certain recursive towers previously studied in coding theory, such as the Garcia-Stichtenoth towers, providing a deeper structural explanation for their optimality [Elk01]. More precisely, he showed that the tame case corresponds to classical modular curves [Elk97], while the wild case corresponds to Drinfeld modular curves [Elk01]. Subsequently, many explicitly known recursively defined towers have been given a modular interpretation. Bassa, Beelen and Nguyen [BBN14, BBN15] showed that the defining equations for these (classical or Drinfeld) modular towers can be read off directly from the modular polynomial. The theory of modular curves is therefore considered an efficient machinery to produce explicitly defined families of curves, particularly good and optimal towers of curves. We refer the reader to Beelen's survey [Bee22] for more details.

6.3.3 Locally recoverable codes in the rank metric

One main application of coding theory is data recovery in distributed storage systems. Originally, data replication was used to ensure reliability against node (*e.g.,* individual machine) failures. In the last decades, distributed storage systems have been transitioning to the use of *erasure codes* as they offer higher reliability at significantly lower storage costs. One can easily check that an $[n, k, d]$ linear code can recover up to $d - 1$ erasures. For instance, in 2014, Facebook deployed a version of the Hadoop Distributed File System (HDFS) that relies on a $[14, 10, 5]$ Reed–Solomon code and can thus resist as many as 4 node failures. However, this requires accessing the 10 other nodes and performing high-degree polynomial interpolation.

Locally recoverable codes are a class of error-correcting codes designed to efficiently address this issue by allowing each symbol in a codeword to be recovered by accessing only a small subset of other symbols. Locally recoverable codes were originally introduced in the Hamming metric [GHSY12, PD14]. We recall their definition below.

Definition 6.12. [BTV17, Definition 2] A code $\mathcal{C} \subseteq \mathbb{F}_q^n$ is *locally recoverable* with *locality* (t, δ) if for every coordinate index $i \in \{1, \ldots, n\}$ there exists a subset $\Gamma[i] \subseteq \{1, \ldots, n\}$ containing i such that $|\Gamma(i)| \leqslant t + \delta - 1$ and the code $\mathcal{C}|_{\Gamma(i)}$ obtained by restricting $\mathcal{C}$ to the coordinates in $\Gamma(i)$ has minimumdistance $d(\mathcal{C}|_{\Gamma(i)}) \geqslant \delta$.

The definition was generalised to the rank metric in [KERDS16] in the following way.

Definition 6.13. A rank metric code $\mathcal{C} \subseteq \mathbb{F}_q^{n \times m}$ is *locally recoverable* with *rank-locality* (t, δ) if, for every column index $i \in \{1, \ldots, m\}$, there exists a set of columns $\Gamma[i] \subseteq \{1, \ldots, m\}$ containing i such that $|\Gamma(i)| \leqslant t + \delta - 1$ and the code $\mathcal{C}|_{\Gamma(i)}$ obtained by restricting $\mathcal{C}$ to the coordinates in $\Gamma(i)$ has minimum rank distance $d_{\mathrm{rk}}(\mathcal{C}|_{\Gamma(i)}) \geqslant \delta$.

Remark 6.14. The above definition is a natural extension of the one originally introduced in the Hamming metric. In particular, when the rank-metric code $\mathcal{C}$ is $\mathbb{F}_{q^m}$-linear, it coincides exactly with the classical definition of locally recoverable codes in the Hamming setting. The notion of locality relates to code puncturings. A puncturing of a rank-metric matrix code is a projection onto a coordinate subspace that, in opposition to the Hamming setting, can be precomposed with a rank-preserving isomorphism $A \in GL_n(\mathbb{F}_q)$ [Ner19, Definition 2.15]. Definition 6.13 only involves puncturings with trivial isomorphisms $A = I_n$. Therefore, the current notion of locality in the rank metric does not fully leverage the richness of the rank metric and may be considered somewhat unsatisfactory. However, since this is the definition used in [BDM24], we will stick to it.

A locally recoverable rank-metric code $\mathcal{C} \subseteq \mathbb{F}_q^{n \times m}$ of dimension $m \cdot k$ and with rank-locality (t, δ) satisfies the following Singleton-type bound [KERDS19, Theorem 1]

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

In what follows, we present the construction of locally recoverable codes in the rank metric from Carlitz modules as outlined in [BDM24], while generalising it to Drinfeld modules of any rank.

Let $\phi : \mathbb{F}_q[T] \to \mathbb{F}_{q^m}\{\tau\}$ be a Drinfeld Module of rank r with $\phi_T := z + g_1\tau + \cdots + g_r\tau^r$. We consider the message space to be

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

For some positive integer ℓ such that $\ell \geqslant s+1$ we choose $a_1, \ldots, a_\ell \in \mathbb{F}_q^*$ and build the polynomial $h = \prod_{i=1}^{\ell}(T - a_i)$. Considering the h-torsion $\phi[h]$ as defined in Section 3.4.1, we have $\phi[h] \simeq \oplus_{i=1}^{\ell}\phi[T-a_i]$. We formulate the following hypothesis:

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

By Proposition 3.13, we know that $\dim_{\mathbb{F}_q} \phi[T-a_i] = r$.

Definition 6.15. Consider the encoding map

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

where the last isomorphism is given after the choice of bases of $\phi[T-a_i]$, for all $i \in \{1, \ldots, \ell\}$. We define the code $\mathcal{C}(\phi, h)$ as the image $\text{enc}(\mathcal{M})$.

The parameters of the locally recoverable codes in the rank metric obtained with Drinfeld modules of rank 1 are given in [BDM24, Theorem 3.4]. Here, we largely follow their proof to show, in the following theorem, that our generalised construction with Drinfeld modules of higher rank has the same parameters.

Theorem 6.16. *Let s, ℓ be two integers such that $s+1 \leqslant \ell$. For t, δ two integers such that $t \geqslant 1$ and $\delta \geqslant 2$, consider a Drinfeld module ϕ of rank $r = t + \delta - 1 > 0$. Then $\mathcal{C}(\phi, h)$ is a $[m\ell r,\ m(s{+}1)t,\ \ell r{-}rs{-}t{+}1]$ code with rank-locality (t, δ). Furthermore, the code is optimal, that is, it attains the Singleton-type bound.*

Proof. By construction, the elements in $\mathbb{F}_{q^m}^{\ell r}$ are matrices of size $m \cdot \ell r$. As for the dimension, note that an Ore polynomial of degree $sr + t - 1 < (s+1)r$ cannot be the zero map on the space $\mathbb{F}_{q^m}^{\ell r}$ of $\mathbb{F}_{q^m}$-dimension $\ell r \geqslant (s+1)r$, hence the encoding map is injective. Since $\mathcal{M}$ has $\mathbb{F}_{q^m}$-dimension $(s+1) \cdot t$, the code has $\mathbb{F}_q$-dimension $m \cdot (s+1) \cdot t$. Now, observe that $\mathcal{M}$ is contained in the ring of Ore polynomials of degree at most $sr + t - 1$. Therefore, $\mathcal{C}(\phi, h)$ is a subcode of a Gabidulin code of parameters $(\ell r, sr + t)$. Since Gabidulin codes are MRD, we obtain

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

We now want to establish the rank-locality property according to Definition 6.13. For each $i \in \{1, \ldots, r\}$, let $\Lambda(i)$ be the set of column indices corresponding to the summand $\operatorname{Hom}_{\mathbb{F}_q}(\phi[T-a_i], \mathbb{F}_{q^m}) \simeq \mathbb{F}_{q^m}^r$. We have $|\Lambda(i)| = \dim \phi[T-a_i] = r = t + \delta - 1$. Besides, for any $f \in \mathcal{M}$ and any $x \in \phi[T-a_i]$, we have

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

where $f_k(x) \in \mathbb{F}_{q^m}\{\tau\}_{\leqslant t-1}$. We conclude that $\mathcal{C}(\phi, h)|_{\Lambda(i)}$ is included in a $[r, t]_{q^m}$ Gabidulin code, hence, it has minimum distance at least $r + 1 - t = \delta$. Now, if

$\gamma \in \{1, \dots, \ell r\}$ is a column index, we set $\Gamma(\gamma) := \Lambda(i)$ for the unique index i such that $\gamma \in \Lambda(i)$. By what precedes, $\mathcal{C}(\phi, h)|_{\Gamma(\gamma)}$ has minimum distance at least δ, proving that $\mathcal{C}(\phi, h)$ has (t, δ) rank-locality. From the Singleton-type bound of Equation (28) we entail that

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

which, together with Equation (29), finally gives $d_{\mathrm{rk}}(\mathcal{C}(\phi, h)) = \ell r - rs - t + 1$. □

A key ingredient in the construction of locally recoverable codes in any metric is the choice of a *good* polynomial respecting some conditions which allow the recovery of the lost pieces of data (see, for instance, [TB14, Section A]). The present construction of LR codes in the rank metric makes no exception. Here, the evaluation points of Definition 6.15 are carefully chosen by selecting a polynomial $h \in \mathbb{F}_q[T]$ so that the h-torsion is defined over $\mathbb{F}_{q^m}$, to satisfy (**H**). For Drinfeld modules of rank 1, the existence of such a polynomial h is guaranteed using an effective version of Dirichlet's Theorem [BDM24, § 5]. It would be interesting to study under which conditions such a polynomial h exists when generalising the construction to Drinfeld modules of any rank. This question could be approached by developing an explicit Chebotarev density theorem for Drinfeld modules, using the theory of L-series presented in Subsection 5.2.1 as a main tool.

Acknowledgements

This presentation is inspired by the talks given in the second edition of the *Coding theory, cryptogrAphy, arIthmetic geometry, and comPuter Algebra Itinerant* symposium[3]. The authors are very grateful to the sponsors of this edition, namely the Mathematics Institute of Marseille (I2M – UMR7373) and the FRUMAM research federation (FR 2291 - CNRS). CA was supported by ANR *Jinvariant* (ANR-20-CE40-0003) and ANR *PadLEfAn* (ANR-22-CE40-0013). EB was supported by the grant ANR-22-CPJ2-0047-01. XC and AL are grateful to the ANR *PadLEfAn* (ANR-22-CE40-0013) for supporting several "research in pairs" devoted to code development. AL gratefully acknowledges that this research was supported in part by the Pacific Institute for the Mathematical Sciences. JN is supported by the French government *Investissements d'Avenir* program ANR-11-LABX-0020-01. FP was supported by ANR *Jinvariant* (ANR-20-CE40-0003), and is grateful to the University of Bordeaux for the hospitality. This work was partially funded by the grant ANR-21-CE39-0009-BARRACUDA.

References

[ACLM23] David Ayotte, Xavier Caruso, Antoine Leudière, and Joseph Musleh. Drinfeld modules in SageMath. *ACM Communications in Computer Algebra*, 57(2):65–71, 2023.

[ACLN21] Daniel Augot, Alain Couvreur, Julien Lavauzelle, and Alessandro Neri. Rank-metric codes over arbitrary Galois extensions and rank analogues of Reed–Muller codes. *SIAM Journal on Applied Algebra and Geometry*, 5(2):165–199, 2021.

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

[ALR18] Daniel Augot, Pierre Loidreau, and Gwezheneg Robert. Generalized Gabidulin codes over fields of any characteristic. *Designs, Codes and Cryptography*, 86:1807–1848, 2018.

[AM93] Arthur Oliver Lonsdale Atkin and François Morain. Elliptic curves and primality proving. *Mathematics of Computation*, 61(203):29–68, 1993.

[And00] Greg Anderson. An elementary approach to L-functions mod p. *Journal of Number Theory*, 80(2):291–303, 2000.

[Ang97] Bruno Anglès. On some characteristic polynomials attached to finite Drinfeld modules. *manuscripta mathematica*, 93(1):369–379, 1997.

[Ayo23] David Ayotte. *Arithmetic and computational aspects of modular forms over global fields*. PhD thesis, Concordia University, 2023.

[BBN14] Alp Bassa, Peter Beelen, and Nhut Nguyen. Good towers of function fields. *Algebraic Curves and Finite Fields, Radon Series on Computational and Applied Mathematics*, pages 23–40, 2014.

[BBN15] Alp Bassa, Peter Beelen, and Nhut Nguyen. Good families of Drinfeld modular curves. *LMS Journal of Computation and Mathematics*, 18(1):699–712, 2015.

[BC24] Elena Berardini and Xavier Caruso. Algebraic Geometry codes in the sum–rank metric. *IEEE Transactions on Information Theory*, 70(5):3345–3356, 2024.

[BC25] Elena Berardini and Xavier Caruso. Reed–Muller codes in the sum-rank metric. *Journal of Algebra and Its Applications*, page 2541019, 2025.

[BCG06] Simon Blackburn, Carlos Cid, and Steven Galbraith. Cryptanalysis of a cryptosystem based on drinfeld modules. *Information Security, IEE Proceedings*, 153:12–14, 2006.

[BDM24] Luca Bastioni, Mohamed O Darwish, and Giacomo Micheli. Optimal rank-metric codes with rank-locality from Drinfeld modules. *preprint arXiv:2407.06081*, 2024.

[Bee22] Peter Beelen. A survey on recursive towers and Ihara's constant. *preprint arXiv:2203.03310*, 2022.

[Ber67] Elwyn Berlekamp. Factoring polynomials over finite fields. *The Bell System Technical Journal*, 46(8):1853–1859, 1967.

[BGP25] Liam Baker, Richard Griffon, and Fabien Pazuki. A parallelogram height inequality for Drinfeld modules. *preprint arXiv:2512.09526*, 2025.

[BHL$^+$22] Hannes Bartz, Lukas Holzbaur, Hedongliang Liu, Sven Puchinger, Julian Renner, and Antonia Wachter-Zeh. Rank-metric codes and their applications. *Foundations and Trends® in Communications and Information Theory*, 19(3):390–546, 2022.

[BP20] W. Dale Brownawell and Matthew A. Papanikolas. A rapid introduction to drinfeld modules, t-modules, and t-motives. In *t-Motives: Hodge Structures, Transcendence and Other Motivic Aspects*, pages 3–30. European Mathematical Society - EMS - Publishing House GmbH, 2020. ISSN: 2523-515X, 2523-5168.

[BPR21] Florian Breuer, Fabien Pazuki, and Mahefason Heriniaina Razafinjatovo. Heights and isogenies of Drinfeld modules. *Acta Arithmetica*, 197:111–128, 2021.

[BTV17] Alexander Barg, Itzhak Tamo, and Serge Vlăduţ. Locally recoverable codes on algebraic curves. *IEEE Transactions on Information Theory*, 63(8):4928–4939, 2017.

[Car35] Leonard Carlitz. On certain functions connected with polynomials in a Galois field. *Duke Mathematical Journal*, 1(2):137–168, 1935.

[Car18] Perlas Caranay. *Computing Isogeny Volcanoes of Rank Two Drinfeld Modules*. PhD thesis, University of Calgary, 2018.

[CD23] Wouter Castryck and Thomas Decru. An efficient key recovery attack on SIDH. In Carmit Hazay and Martijn Stam, editors, *Advances in Cryptology – EUROCRYPT 2023*, pages 423–447. Springer Nature Switzerland, 2023.

[CFA+12] Henri Cohen, Gerhard Frey, Roberto Avanzi, Christophe Doche, Tanja Lange, Kim Nguyen, and Frederik Vercauteren. *Handbook of Elliptic and Hyperelliptic Curve Cryptography.* Chapman & Hall/CRC, 2nd edition, 2012.

[CG24] Xavier Caruso and Quentin Gazda. Computation of classical and v-adic l-series of t-motives. *preprint arXiv:2401.12618*, 2024.

[CG25] Xavier Caruso and Quentin Gazda. Computation of classical and v-adic l-series of t-motives. *Research in Number Theory*, 11(1):35, 2025.

[CGS20] Perlas Caranay, Matthew Greenberg, and Renate Scheidler. Computing modular polynomials and isogenies of rank two Drinfeld modules over finite fields. In *75 Years of Mathematics of Computation: Symposium on Celebrating 75 Years of Mathematics of Computation, November 1-3, 2018, the Institute for Computational and Experimental Research in Mathematics (ICERM)*, volume 754, page 283. American Mathematical Soc., 2020.

[CL26] Xavier Caruso and Antoine Leudière. Algorithms for computing norms and characteristic polynomials on general drinfeld modules. *Mathematics of Computation*, 95(357), 2026.

[CLB17a] Xavier Caruso and Jérémy Le Borgne. Fast multiplication for skew polynomials. In *Proceedings of the 2017 ACM on International Symposium on Symbolic and Algebraic Computation*, ISSAC '17, pages 77–84. Association for Computing Machinery, 2017.

[CLB17b] Xavier Caruso and Jérémy Le Borgne. A new faster algorithm for factoring skew polynomials over finite fields. *Journal of Symbolic Computation*, 79:411–443, 2017.

[CLM+18] Wouter Castryck, Tanja Lange, Chloe Martindale, Lorenz Panny, and Joost Renes. CSIDH: An efficient post-quantum commutative group action. In Thomas Peyrin and Steven Galbraith, editors, *Advances in Cryptology – ASIACRYPT 2018*, pages 395–427. Springer International Publishing, 2018.

[Cou23] Alain Couvreur. Codes and modular curves. *preprint arXiv:2301.03569*, 2023.

[CZ81] David Cantor and Hans Zassenhaus. A new algorithm for factoring polynomials over finite fields. *Mathematics of Computation*, 36(154):587–592, 1981. Publisher: American Mathematical Society.

[DD99] Sinnou David and Laurent Denis. Isogénie minimale entre modules de Drinfeld. *Mathematische Annalen*, 315:97–140, 1999.

[Del78] Philippe Delsarte. Bilinear forms over a finite field, with applications to coding theory. *Journal of combinatorial theory, Series A*, 25(3):226–241, 1978.

[DFKL$^+$20] Luca De Feo, David Kohel, Antonin Leroux, Christophe Petit, and Benjamin Wesolowski. SQISign: Compact post-quantum signatures from quaternions and isogenies. In Shiho Moriai and Huaxiong Wang, editors, *Advances in Cryptology – ASIACRYPT 2020*, pages 64–93. Springer International Publishing, 2020.

[DFKS18] Luca De Feo, Jean Kieffer, and Benjamin Smith. Towards practical key exchange from ordinary isogeny graphs. In Thomas Peyrin and Steven Galbraith, editors, *Advances in Cryptology – ASIACRYPT 2018*, Lecture Notes in Computer Science, pages 365–394. Springer International Publishing, 2018.

[DH76] Whitfield Diffie and Martin Hellman. New directions in cryptography. *IEEE Transactions on Information Theory*, 22(6):644–654, 1976.

[DNS21] Javad Doliskani, Anand Kumar Narayanan, and Éric Schost. Drinfeld modules with complex multiplication, Hasse invariants and factoring polynomials over finite fields. *Journal of Symbolic Computation*, 105:199–213, 2021.

[Dri74] Vladimir Drinfeld. Elliptic modules. *Mathematics of the USSR-Sbornik*, 23(4):561, 1974.

[Dri77] Vladimir Drinfeld. Commutative subrings of certain noncommutative rings. *Functional Analysis and Its Applications*, 11(1):9–12, 1977.

[Dri80] Vladimir Drinfeld. Langlands' conjecture for GL(2) over functional fields. In *Proceedings of the International Congress of Mathematicians (Helsinki, 1978)*, volume 2, pages 565–574, 1980.

[Elk97] Noam Elkies. Explicit modular towers. In *Proceedings of the Thirty-Fifth Annual Allerton Conference on Communication, Control and Computing*, 1997.

[Elk99] Noam Elkies. Linearized algebra and finite groups of Lie type. I. Linear and symplectic groups. In *Applications of curves over finite fields*, volume 245 of *Contemporary Mathematics*, pages 77–107, 1999.

[Elk01] Noam Elkies. Explicit towers of Drinfeld modular curves. In Carles Casacuberta, Rosa Maria Miró-Roig, Joan Verdera, and Sebastià Xambó-Descamps, editors, *European Congress of Mathematics*, pages 189–198, Basel, 2001. Birkhäuser Basel.

[Gab85] Ernest Mukhamedovich Gabidulin. Theory of codes with maximum rank distance. *Problemy Peredachi Informatsii*, 21(1):3–16, 1985.

[Gek91] Ernst-Ulrich Gekeler. On finite Drinfeld modules. *Journal of Algebra*, 141(1):187–203, 1991.

[Gek08] Ernst-Ulrich Gekeler. Frobenius distributions of Drinfeld modules over finite fields. *Transactions of the American Mathematical Society*, 360(4):1695–1721, 2008. Publisher: American Mathematical Society.

[Ger61] Murray Gerstenhaber. On the number of nilpotent matrices with coefficients in a finite field. *Illinois Journal of Mathematics*, 5(2):330–333, 1961. Publisher: Duke University Press.

[GHSY12] Parikshit Gopalan, Cheng Huang, Huseyin Simitci, and Sergey Yekhanin. On the locality of codeword symbols. *IEEE Transactions on Information theory*, 58(11):6925–6934, 2012.

[GK86] Shafi Goldwasser and Joe Kilian. Almost all primes can be quickly certified. In *Proceedings of the eighteenth annual ACM symposium on Theory of computing*, STOC '86, pages 316–329. Association for Computing Machinery, 1986.

[GKK25] Filip Głoch, Dawid E. Kędzierski, and Piotr Krasoń. Algorithms for determination of t-module structures on some extension groups. *International Journal of Number Theory*, 21(8):1889–1922, 2025.

[GLPR03] Rolland Gillard, Franck Leprévost, Alexei Panchishkin, and Xavier-François Roblot. Utilisation des modules de Drinfeld en cryptologie. *Comptes Rendus Mathematique*, 336(11):879–882, 2003.

[Gop81] Valerii Denisovich Goppa. Codes on algebraic curves. In *Sov. Math.-Dokl*, volume 24, pages 170–172, 1981.

[Gor21] Elisa Gorla. Rank-metric codes. In *Concise Encyclopedia of Coding Theory*, pages 227–250. Chapman and Hall/CRC, 2021.

[Gos96] David Goss. *Basic structures of function field arithmetic*, volume 35 of *Ergebnisse der Mathematik und ihrer Grenzgebiete (3) [Results in Mathematics and Related Areas (3)]*. Springer-Verlag, Berlin, 1996.

[GP22] Richard Griffon and Fabien Pazuki. Isogenies of elliptic curves over function fields. *International Mathematics Research Notices*, 2022(19):14697–14740, 2022.

[GR96] Ernst-Ulrich Gekeler and Marc Reversat. Jacobians of Drinfeld modular curves. *Journal für die Reine und Angewandte Mathematik*, 476:27–93, 1996.

[GR14] Éric Gaudron and Gaël Rémond. Théorème des périodes et degrés minimaux d'isogénies. *Commentarii Mathematici Helvetici*, 89(2):343–403, 2014.

[GS95] Arnaldo Garcia and Henning Stichtenoth. A tower of Artin-Schreier extensions of function fields attaining the Drinfeld-Vladut bound. *Inventiones mathematicae*, 121(1):211–222, 1995.

[Hay74] David Hayes. Explicit class field theory for rational function fields. *Transactions of the American Mathematical Society*, 189(0):77–91, 1974.

[Hay11] David Hayes. A brief introduction to Drinfeld Modules. In *A Brief Introduction to Drinfeld Modules*, pages 1–32. De Gruyter, 2011.

[Iha81] Yasutaka Ihara. Some remarks on the number of rational points of algebraic curves over finite fields. *Journal of the Faculty of Science, University of Tokyo*, 28(3):721–724, 1981.

[JDF11] David Jao and Luca De Feo. Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies. In Bo-Yin Yang, editor, *Post-Quantum Cryptography*, pages 19–34. Springer, 2011.

[JN19] Antoine Joux and Anand Kumar Narayanan. Drinfeld modules may not be for isogeny based cryptography, 2019.

[Kat73] Nicholas Katz. *p-adic properties of modular schemes and modular forms*, volume Vol. 350 of *Lecture Notes in Math.* Springer, Berlin-New York, 1973.

[Ked01] Kiran Kedlaya. The algebraic closure of the power series field in positive characteristic. *Proceedings of the American Mathematical Society*, 129(12):3461–3470, 2001.

[KERDS16] Swanand Kadhe, Salim El Rouayheb, Iwan Duursma, and Alex Sprintson. Rank-metric codes with local recoverability. In *2016 54th Annual Allerton Conference on Communication, Control, and Computing (Allerton)*, pages 1033–1040. IEEE, 2016.

[KERDS19] Swanand Kadhe, Salim El Rouayheb, Iwan Duursma, and Alex Sprintson. Codes with locality in the rank and subspace metrics. *IEEE Transactions on Information Theory*, 65(9):5454–5468, 2019.

[Kob87] Neal Koblitz. Elliptic curve cryptosystems. *Mathematics of Computation*, 48(177):203–209, 1987.

[KS95] Erich Kaltofen and Victor Shoup. Subquadratic-time factoring of polynomials over finite fields. In *Proceedings of the twenty-seventh annual ACM symposium on Theory of computing*, STOC '95, pages 398–406. Association for Computing Machinery, 1995.

[KU01] Kiran Kedlaya and Christopher Umans. Fast polynomial factorization and modular composition. *SIAM Journal on Computing*, 40(6):1767–1802, 2011-01. Publisher: Society for Industrial and Applied Mathematics.

[Laf02] Laurent Lafforgue. Chtoucas de Drinfeld et correspondance de Langlands. *Inventiones mathematicae*, 147:1–241, 2002.

[Lan02] Serge Lang. *Algebra*, volume 211 of *Graduate Texts in Mathematics*. Springer, 2002.

[Len87] Henrik Lenstra. Factoring integers with elliptic curves. *The Annals of Mathematics*, 126(3):649, 1987.

[Leu24] Antoine Leudière. *Morphisms of Drinfeld Modules and their Algorithms*. PhD thesis, Université de Lorraine, 2024.

[LS22] Antoine Leudière and Pierre-Jean Spaenlehauer. Hard homogeneous spaces from the class field theory of imaginary hyperelliptic function fields. *Cryptology ePrint Archive*, 2022.

[LS24] Antoine Leudière and Pierre-Jean Spaenlehauer. Computing a group action from the class field theory of imaginary hyperelliptic function fields. *Journal of Symbolic Computation*, 125:102311, 2024.

[Mil86] Victor Miller. Use of elliptic curves in cryptography. In Hugh C. Williams, editor, *Advances in Cryptology — CRYPTO '85 Proceedings*, pages 417–426. Springer, 1986.

[MM22] Luciano Maino and Chloe Martindale. An attack on sidh with arbitrary starting curve. *Cryptology ePrint Archive*, 2022.

[Moo96] Eliakim Hastings Moore. A two-fold generalization of Fermat's theorem. *Bulletin of the American Mathematical Society*, 2(7):189–199, 1896.

[MS19] Yossef Musleh and Éric Schost. Computing the characteristic polynomial of a finite rank two Drinfeld module. *Proceedings of the 2019 on International Symposium on Symbolic and Algebraic Computation*, pages 307–314, 2019.

[MS23] Yossef Musleh and Éric Schost. Computing the characteristic polynomial of endomorphisms of a finite Drinfeld module using crystalline cohomology. In *Proceedings of the 2023 International Symposium on Symbolic and Algebraic Computation*, ISSAC '23, pages 461–469. Association for Computing Machinery, 2023.

[Mul54] David Muller. Application of boolean algebra to switching circuit design and to error detection. *Transactions of the IRE professional group on electronic computers*, EC-3(3):6–12, 1954.

[Mus18] Yossef Musleh. Fast algorithms for finding the characteristic polynomial of a rank-2 Drinfeld module, 2018. Masters thesis.

[Mus23] Yossef Musleh. *Algorithms for Drinfeld Modules*. PhD thesis, University of Waterloo, 2023.

[Nar18] Anand Kumar Narayanan. Polynomial factorization over finite fields by computing Euler–Poincaré characteristics of Drinfeld modules. *Finite Fields and Their Applications*, 54:335–365, 2018.

[Ner19] Alessandro Neri. *Algebraic theory of rank-metric codes : representations, invariants and density results*. PhD thesis, University of Zurich (Switzerland), 2019.

[Neu99] Jürgen Neukirch. *Algebraic number theory. Transl. from the German by Norbert Schappacher*, volume 322 of *Grundlehren Math. Wiss.* Berlin: Springer, 1999.

[Ore33a] Øystein Ore. On a special class of polynomials. *Transactions of the American Mathematical Society*, 35(3):559–584, 1933.

[Ore33b] Øystein Ore. Theory of non-commutative polynomials. *Annals of Mathematics. Second Series*, 34:480–508, 1933.

[Pan93] Alexei Panchishkin. Algorithmes rapides pour factorisation des nombres et des polynômes, test de primalité, courbes elliptiques et modules de Drinfeld. *Séminaire de théorie des nombres de l'université de Caen*, Fascicule de l'année 1992-1993:1–7, 1993.

[Pap23] Mihran Papikian. *Drinfeld modules*, volume 296 of *Grad. Texts Math.* Cham: Springer, 2023.

[Paz19] Fabien Pazuki. Modular invariants and isogenies. *International Journal of Number Theory*, 15(03):569–584, 2019.

[PD14] Dimitris Papailiopoulos and Alexandros Dimakis. Locally repairable codes. *IEEE Transactions on Information Theory*, 60(10):5843–5855, 2014.

[Poo95] Bjorn Poonen. Local height functions and the Mordell-Weil theorem for Drinfeld modules. *Compositio Mathematica*, 97(3):349–368, 1995.

[Poo22] Bjorn Poonen. Introduction to drinfeld modules. *Arithmetic, Geometry, Cryptography, and Coding Theory*, 779, 2022.

[Pot97] Igor Potemine. *Arithmétique des corps globaux de fonctions et géométrie des schémas modulaires de Drinfeld*. PhD thesis, Université Joseph Fourier, 1997.

[Pot98] Igor Potemine. Minimal terminal $\mathbf{Q}$-factorial models of Drinfeld coarse moduli schemes. *Mathematical Physics, Analysis and Geometry. An International Journal Devoted to the Theory and Applications of Analysis and Geometry to Physics*, 1(2):171–191, 1998.

[Ran14] Tovohery Hajatiana Randrianarisoa. The number of matrices over $\mathbb{F}_q$ with irreducible characteristic polynomial. *preprint arXiv:1402.2794*, 2014.

[Ree54] Irving Reed. A class of multiple-error-correcting codes and the decoding scheme. *Transactions of the IRE Professional Group on Information Theory*, 4(4):38–49, 1954.

[Rei61] Irving Reiner. On the number of matrices with given characteristic polynomial. *Illinois Journal of Mathematics*, 5(2):324–329, 1961. Publisher: Duke University Press.

[Rob23] Damien Robert. Breaking SIDH in polynomial time. In Carmit Hazay and Martijn Stam, editors, *Advances in Cryptology – EUROCRYPT 2023*, pages 472–503. Springer Nature Switzerland, 2023.

[Ros02] Michael Rosen. *Number theory in function fields*, volume 210. Springer Science & Business Media, 2002.

[RS60] Irving Reed and Gustave Solomon. Polynomial codes over certain finite fields. *Journal of the society for industrial and applied mathematics*, 8(2):300–304, 1960.

[RSA78] Ronald Rivest, Adi Shamir, and Leonard Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, 21(2):120–126, 1978.

[Sca01] Thomas Scanlon. Public key cryptosystems based on Drinfeld modules are insecure. *Journal of Cryptology*, 14(4):225–230, 2001.

[Sch85] René Schoof. Elliptic curves over finite fields and the computation of square roots mod p. *Mathematics of Computation*, 44(170):483–494, 1985.

[Sho90] Victor Shoup. NTL: A library for doing number theory, 1990.

[Sil09] Joseph Silverman. *The Arithmetic of Elliptic Curves*, volume 106 of *Graduate Texts in Mathematics*. Springer, 2009.

[Sti09] Henning Stichtenoth. *Algebraic function fields and codes*. Springer, 2009.

[Tae12] Lenny Taelman. Special L-values of Drinfeld modules. *Annals of Mathematics. Second Series*, 175(1):369–391, 2012.

[TB14] Itzhak Tamo and Alexander Barg. A family of optimal locally recoverable codes. *IEEE Transactions on Information Theory*, 60(8):4661–4676, 2014.

[Tha04] Dinesh Thakur. *Function field arithmetic*. River Edge, NJ: World Scientific, 2004.

[TVZ82] Michael Tsfasman, Sergey Vlădutx, and Thomas Zink. Modular curves, Shimura curves, and Goppa codes, better than Varshamov-Gilbert bound. *Mathematische Nachrichten*, 109(1):21–28, 1982.

[VD83] Sergei Georgievich Vlăduţ and Vladimir Gershonovich Drinfeld. Number of points of an algebraic curve. *Funktsional'nyi Analiz i ego Prilozheniya*, 17(1):68–69, 1983.

[vdH04a] Gert-Jan van der Heiden. Addendum to "Factoring polynomials over finite fields with Drinfeld modules". *Mathematics of Computation*, 73(248):2109–2109, 2004.

[vdH04b] Gert-Jan van der Heiden. Factoring polynomials over finite fields with Drinfeld modules. *Mathematics of Computation*, 73(245):317–322, 2004.

[Wad41] Luther Irwin Wade. Certain quantities transcendental over GF(p^n, x). *Duke Mathematical Journal*, 8:701–720, 1941.

[Wes24] Benjamin Wesolowski. Computing isogenies between finite Drinfeld modules. *IACR Communications in Cryptology*, 1(1), 2024.